

Steckkarten

PCIe | YRCP32F0 | Handbuch

HB170 | PCIe | YRCP32F0 | de | 25-10

Steckkarte PCI Express - YRCP-MP4P



YASKAWA Europe GmbH
Philipp-Reis-Str. 6
65795 Hattersheim
Deutschland
Tel.: +49 6196 569-300
Fax: +49 6196 569-398
E-Mail: info@yaskawa.eu
Internet: www.yaskawa.eu.com

Inhaltsverzeichnis

1	Allgemein.	5
1.1	Über dieses Handbuch.	5
1.2	Copyright © YASKAWA Europe GmbH.	6
2	Hardwarebeschreibung.	8
2.1	Leistungsmerkmale.	8
2.2	Abmessungen.	8
2.3	Aufbau.	9
2.3.1	YRCP-MP4P.	9
2.3.2	Schnittstellen.	10
2.3.3	LEDs.	13
2.3.4	Schalter.	15
2.4	Zulassungen, Richtlinien, Normen.	16
2.5	Einsatz unter erschwerten Betriebsbedingungen.	17
2.6	Technische Daten.	17
3	Einsatz	21
3.1	Sicherheitshinweise.	21
3.2	Montage.	24
3.3	Gerätetausch und Reparatur.	24
3.4	Industrielle Sicherheit in der Informationstechnologie.	24
3.4.1	Absicherung von Hardware und Applikationen.	26
3.4.2	Absicherung von PC-basierter Software.	27
3.5	Lizenzhinweise zu Open Source Software.	28
3.6	Rücksetzen auf Werkseinstellung Typ 1.	28
3.7	Firmware-Update.	29
3.8	Safe Mode.	30
4	Einsatz unter PROFINET.	31
4.1	Einsatz als PROFINET-IO-Controller.	31
4.1.1	2CON installieren.	31
4.1.2	2CON Benutzeroberfläche.	31
4.1.3	Konfiguration.	33
4.2	Einsatz als PROFINET-Device.	37
5	Einsatz unter EtherCAT.	38
5.1	Bezeichnungen.	38
5.2	Einsatz als EtherCAT-SubDevice.	38
6	Web-based Management - WBM.	39
6.1	Übersicht und erste Schritte.	39
6.2	Übersicht.	41
6.2.1	Allgemeine Daten.	41
6.2.2	Cockpit.	42

6.3	Diagnose.	43
6.3.1	Benachrichtigungen.	43
6.3.2	PROFINET.	44
6.4	Konfiguration.	48
6.4.1	Netzwerk.	48
6.4.2	Datum und Uhrzeit.	49
6.4.3	Webdienste.	51
6.5	Security.	54
6.5.1	Zertifikatauthentifizierung.	54
6.5.2	Firewall.	58
6.5.3	Benutzerauthentifizierung.	63
6.6	Verwaltung.	67
6.6.1	Firmware-Update.	67

1 Allgemein

1.1 Über dieses Handbuch

- Zielsetzung und Inhalt**
- Das Handbuch beschreibt die PCIe Steckkarte YRCP32F0.

 - Beschrieben wird Aufbau, Projektierung und Anwendung.
 - Das Handbuch ist geschrieben für Anwender mit guten Grundkenntnissen in der Automatisierungstechnik.
 - Das Handbuch ersetzt keine ausreichenden Grundkenntnisse in der Automatisierungstechnik sowie die ausreichende Befassung mit dem betroffenen Produkt.
 - Das Handbuch ist in Kapitel gegliedert. Jedes Kapitel beschreibt eine abgeschlossene Thematik.
 - Als Orientierungshilfe stehen im Handbuch zur Verfügung:
 - Gesamt-Inhaltsverzeichnis am Anfang des Handbuchs
 - Verweise mit Seitenangabe

Gültigkeit der Dokumentation

Typ	Best.-Nr.	ab Version:	
YRCP-MP4P	YRCP32F0	PCIe-HW: 1	PCIe-FW: V2024.0

- Dokumentation**
- Das Handbuch ist im Rahmen der Nutzung des einschlägigen Yaskawa Produktes zugänglich zu machen für das einschlägige Fachpersonal in:

 - Projektierung
 - Installation
 - Inbetriebnahme
 - Betrieb

Piktogramme und Signalwörter

Wichtige Textteile sind mit folgenden Piktogrammen und Signalwörtern hervorgehoben:



GEFAHR

- Unmittelbar drohende Gefahr für Leben und Gesundheit von Personen.
- Bei Nichtbeachten sind Tod oder schwerste Verletzungen die Folge.



VORSICHT

- Möglicherweise gefährliche Situation. Wenn sie nicht gemieden wird, können leichte Verletzungen die Folge sein.
- Dieses Symbol wird auch als Warnung vor Sachschäden benutzt.



HINWEIS

- Bezeichnet eine möglicherweise schädliche Situation.
- Das Nichtbeachten kann das Produkt oder etwas in seiner Umgebung beschädigen.



Zusätzliche Informationen und nützliche Tipps.

1.2 Copyright © YASKAWA Europe GmbH

All rights reserved

Dieses Dokument enthält geschützte Informationen von Yaskawa und darf außerhalb einer mit Yaskawa im Vorfeld getroffenen Vereinbarung und nur in Übereinstimmung mit dieser, weder offengelegt noch benutzt werden.

Dieses Dokument ist durch Urheberrechtsgesetze geschützt. Ohne schriftliches Einverständnis von Yaskawa und dem Besitzer dieses Dokuments darf dieses Dokument bzw. dürfen Ausschnitte hiervon weder reproduziert, verteilt, noch geändert werden, es sei denn in Übereinstimmung mit anwendbaren Vereinbarungen, Verträgen oder Lizenzen.

Zur Genehmigung von Vervielfältigung oder Verteilung wenden Sie sich bitte an:
YASKAWA Europe GmbH, European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Deutschland

Tel.: +49 6196 569 300

Fax.: +49 6196 569 398

E-Mail: info@yaskawa.eu

Internet: www.yaskawa.eu.com

Download Center

Im *"Download Center"* unter www.yaskawa.eu.com finden Sie unter Angabe der Produkt-Best.-Nr. die hierfür einschlägigen Handbücher, Datenblätter, Konformitätserklärungen, Zertifikate und weitere hilfreiche Informationen zu Ihrem Produkt.

Warenzeichen

Alle genannten Microsoft Windows, Office und Server-Produkte sind eingetragene Warenzeichen von Microsoft Inc., USA.

Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

PLCnext Technology ist ein eingetragenes Warenzeichen von Phoenix Contact.

EtherCAT® ist eine eingetragene Marke und patentierte Technologie, lizenziert durch die Beckhoff Automation GmbH, Deutschland.

PROFINET ist ein eingetragenes Warenzeichen der PROFIBUS and PROFINET International (PI).

Alle anderen erwähnten Firmennamen und Logos sowie Marken- oder Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Eigentümer.

Allgemeine Nutzungsbedingungen

Es wurden von Yaskawa alle Anstrengungen unternommen, dass die in diesem Dokument enthaltenen Informationen zum Zeitpunkt der Veröffentlichung vollständig und richtig sind. Gleichwohl sind die darin enthaltenen Information von Yaskawa nur so geschuldet, wie diese bei Yaskawa vorliegen. Fehlerfreiheit wird von Yaskawa nicht gewährleistet, das Recht auf Änderungen der hierin enthaltenen Informationen bleibt Yaskawa jederzeit vorbehalten. Eine Informationspflicht gegenüber dem Kunden über etwaige Änderungen besteht nicht. Der Kunde ist aufgefordert, diese Dokumentation aktiv aktuell zu halten. Der Einsatz der von diesen Hinweisen erfassten Produkte mit zugehöriger Dokumentation hat immer in Eigenverantwortung des Kunden unter Berücksichtigung der geltenden Richtlinien und Normen zu erfolgen. Die vorliegende Dokumentation beschreibt die Hard- und Software-Einheiten und Funktionen des Produkts. Es ist möglich, dass Einheiten beschrieben sind, die beim Kunden nicht vorhanden sind. Der genaue Lieferumfang des Produkts ist im jeweiligen Kaufvertrag beschrieben.

Dokument-Support

Wenden Sie sich an Ihre Landesvertretung der YASKAWA Europe GmbH, wenn Sie Fehler anzeigen oder inhaltliche Fragen zu diesem Dokument stellen möchten. Sie können YASKAWA Europe GmbH über folgenden Kontakt erreichen:

E-Mail: Documentation.HER@yaskawa.eu

Technischer Support

Wenden Sie sich an Ihre Landesvertretung der YASKAWA Europe GmbH, wenn Sie Probleme mit dem Produkt haben oder Fragen zum Produkt stellen möchten. Ist eine solche Stelle nicht erreichbar, können Sie den Yaskawa Kundenservice über folgenden Kontakt erreichen:

YASKAWA Europe GmbH,
European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Deutschland
Tel.: +49 6196 569 500 (Hotline)
E-Mail: support@yaskawa.eu

2 Hardwarebeschreibung

2.1 Leistungsmerkmale

YRCP-MP4P

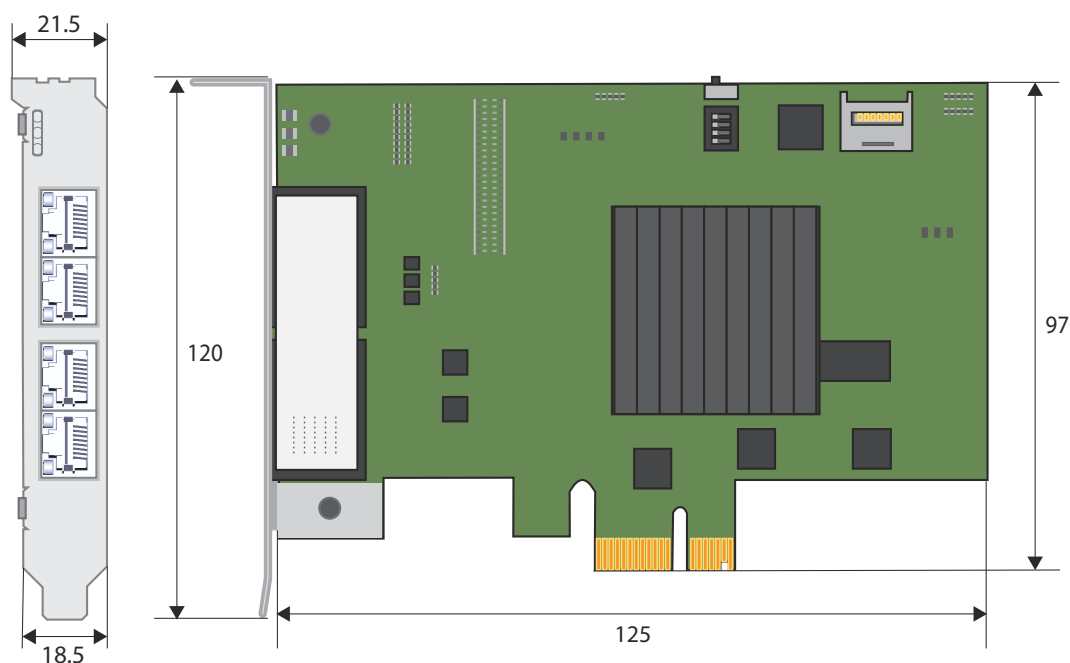
- Die YRCP-MP4P ist eine PCIe x1 Gen1 Steckkarte für die Montage in einem Robot-Controller mit PCI Express Steckplatz.
- Der auf der PCIe-Steckkarte integrierte Kommunikations-Prozessor ermöglicht die ethernet-basierte Anbindung an PROFINET und EtherCAT.
- Unterstützt werden PROFINET-IO-Controller/Device- bzw. EtherCAT SubDevice-Funktionalitäten.
- Die Konfiguration des PROFINET-IO-Controllers erfolgt mit dem Programmierwerkzeug 2CON von Yaskawa.
- Bei Einsatz in einem Robot-Controller von Yaskawa erfolgt die Kommunikation und der Datenaustausch mit der Steckkarte durch direkten Zugriff auf den Speicherbereich. Dieser wird der Steckkarte durch das Betriebssystem direkt zugeordnet. Hierbei kommt auf Host-Seite eine User-API zum Einsatz, welche alle Funktionalitäten der Steckkarte zur Verfügung stellt.

Bestelldaten

Typ	Best.-Nr.	Beschreibung
YRCP-MP4P	YRCP32F0	PCIe x1 Gen1 Steckkarte

2.2 Abmessungen

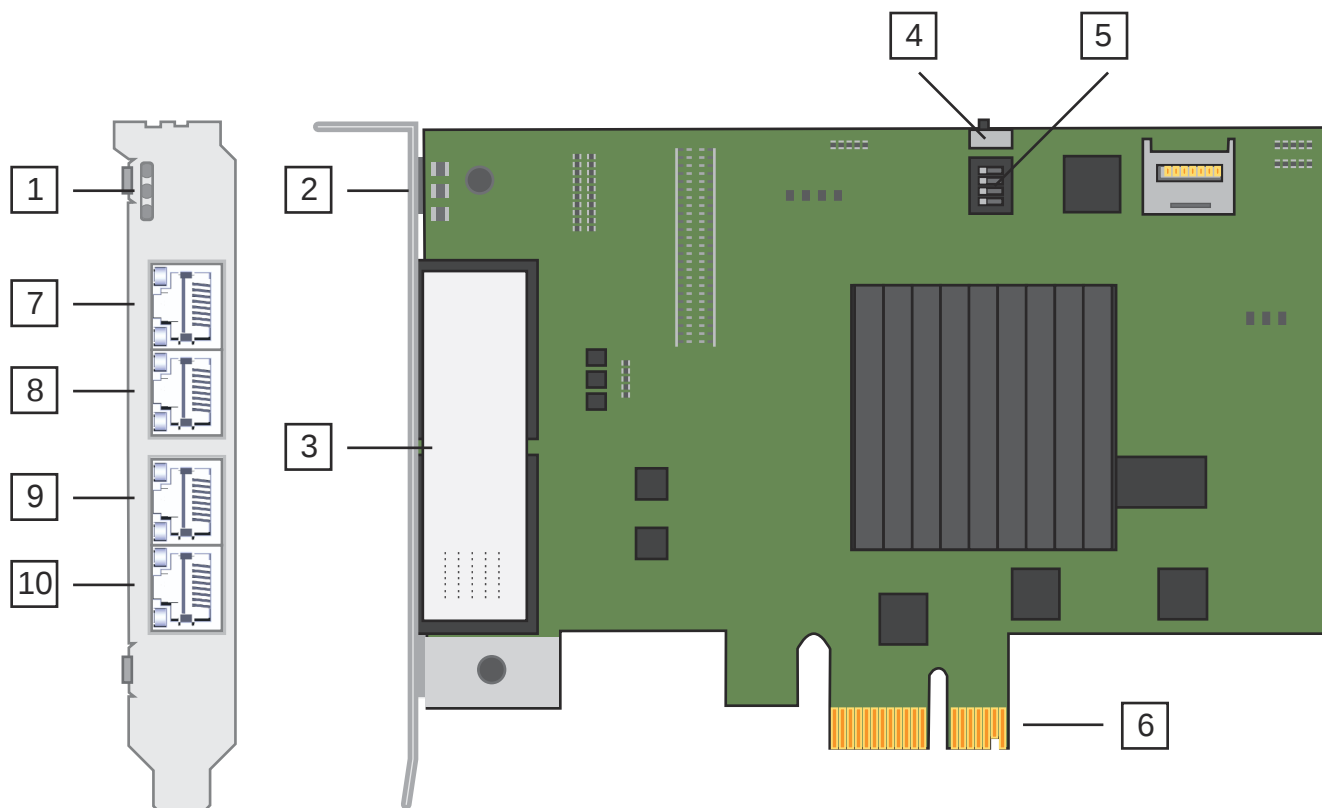
Alle Maße sind in mm angegeben.



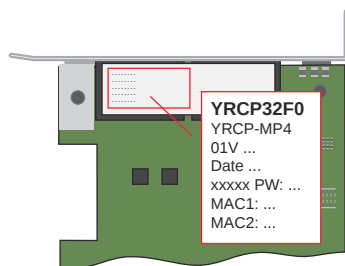
2.3 Aufbau

2.3.1 YRCP-MP4P

Übersicht



- 1** LED-Leiste
- 2** Slot-Blech
- 3** Spezifische Informationen
- 4** S1: Schiebeschalter
- 5** S2: DIP-Schalter
- 6** PCI Express Schnittstelle
- PROFINET aktiviert (default)**
- 7** X1: PROFINET-Device (intern geswitched mit X2)
- 8** X2: PROFINET-Device (intern geswitched mit X1)
- 9** X3: PROFINET-IO-Controller / Ethernet-Port (intern geswitched mit X4)
- 10** X4: PROFINET-IO-Controller / Ethernet-Port (intern geswitched mit X3)
- EtherCAT aktiviert**
- 7** X1: EtherCAT-Port - SubDevice IN
- 8** X2: EtherCAT-Port - SubDevice OUT
- 9** X3: Ethernet-Port (intern geswitched mit X4)
- 10** X4: Ethernet-Port (intern geswitched mit X3)

Spezifische Informationen 3

Folgende Informationen sind auf der Steckkarte aufgedruckt:

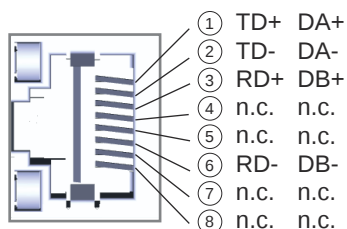
- YRCP32F0 - Bestellnummer
- YRCP-MP4 - Typ
- 01V - Hardware-Ausgabestand
 - Das Beispiel zeigt den Hardware-Ausgabestand 1.
 - Diesen finden Sie auch im WBM unter *"Übersicht"...*[Seite 41](#).
- Date
 - Produktionsdatum
- xxxxx - Seriennummer
- PW - Passwort
 - Das Passwort mit der Bezeichnung "PW:" ist für die Erstanmeldung für den "Admin"-Benutzer im *"Web-based Management - WBM"...*[Seite 39](#) erforderlich.
- MAC1/MAC2 - MAC-Adressen
 - "MAC1" für die Schnittstellen X3/X4 (default: 192.168.1.1).
 - "MAC2" für die Schnittstellen X1/X2 (default: 192.168.3.1).



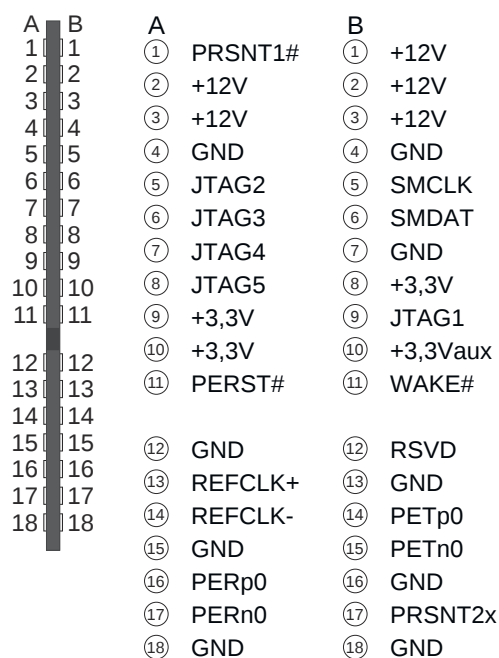
Es ist ratsam, das Passwort aufzuschreiben, bevor Sie die Steckkarte einbauen.

2.3.2 Schnittstellen

X1/X2 X3/X4



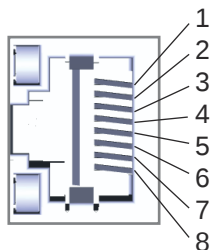
PCIe



X1/X2/X3/X4: PROFINET



Für die Projektierung in einem PROFINET-IO-Controller finden Sie im "Download Center" von www.yaskawa.eu.com die zugehörige "GSDML-V...-YASKAWA-YRCP-MP4P-....xml". Installieren Sie diese in Ihrem PROFINET-Konfigurationstool.



8polige RJ45-Buchse:

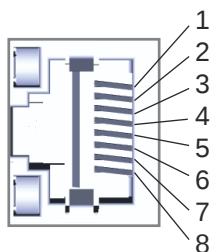
Pin	Signal	Beschreibung
1	DA+	Bidirektionales Paar A + (Daten senden +)
2	DA-	Bidirektionales Paar A - (Daten senden -)
3	DB+	Bidirektionales Paar B + (Daten empfangen +)
4	n.c.	reserviert
5	n.c.	reserviert
6	DB-	Bidirektionales Paar B - (Daten empfangen -)
7	n.c.	reserviert
8	n.c.	reserviert

- Die Steckkarte hat einen Ethernet Kommunikationsprozessor mit PROFINET-IO-Controller und PROFINET-Device integriert.
- Über X1/X2 (default: 192.168.3.1, "MAC2") binden Sie die Steckkarte als PROFINET-Device an einen PROFINET-IO-Controller an.
- Über X3/X4 (default: 192.168.1.1, "MAC1") binden Sie PROFINET-Devices an den PROFINET-IO-Controller der Steckkarte an.
- Über Ethernet haben Sie über diese Schnittstellen Zugriff auf das "[Web-based Management - WBM](#)"...[Seite 39](#) der Steckkarte.

X1/X2: EtherCAT-Port



Für die Projektierung in einem EtherCAT-MainDevice finden Sie im "Download Center" von www.yaskawa.eu.com die zugehörige "ESI-V...-YASKAWA-YRCP-MP4P-....xml". Installieren Sie diese in Ihrem EtherCAT-Konfigurationstool und aktivieren Sie die EtherCAT-Kommunikation für X1/X2 mittels der User-API für Ihr Hostsystem.

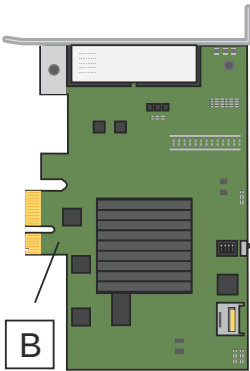


8polige RJ45-Buchse:

Pin	Signal	Beschreibung
1	TD+	Daten senden +
2	TD-	Daten senden -
3	RD+	Daten empfangen +
4	n.c.	reserviert
5	n.c.	reserviert
6	RD-	Daten empfangen -
7	n.c.	reserviert
8	n.c.	reserviert

- Die Steckkarte hat einen Ethernet Kommunikationsprozessor mit EtherCAT-SubDevice integriert.
- Der Anschluss an ein übergeordnetes EtherCAT-MainDevice erfolgt über X1: EtherCAT-Port - SubDevice IN.
- Der Anschluss an ein nachfolgendes EtherCAT-SubDevice erfolgt über X2: EtherCAT-Port - SubDevice OUT.
- EtherCAT verwendet als Übertragungsmedium Ethernet. Es kommen Standard CAT5-Kabel zum Einsatz. Hierbei sind Leitungslängen von bis zu 100m zwischen zwei Teilnehmern möglich.
- Ein EtherCAT-Netz besteht immer aus einem EtherCAT-MainDevice und einer beliebigen Anzahl an EtherCAT-SubDevices (Koppler).
- Jedes EtherCAT-SubDevice besitzt eine RJ45-Buchse für das ankommende EtherCAT-Kabel aus Richtung des MainDevices (hier X1) und eine RJ45-Buchse zur Anbindung an den nachfolgenden Teilnehmer (hier X2). Beim jeweiligen letzten Teilnehmer bleibt die ausgehende Buchse frei.

PCI Express Schnittstelle



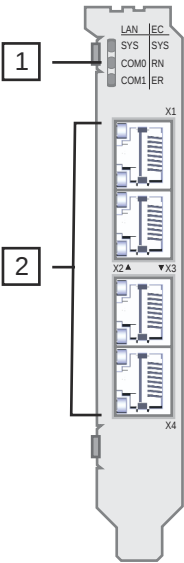
PCIe

A	B
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16
17	17
18	18

Die PCI Express Schnittstelle dient zur Anbindung an einen Robot-Controller mit PCI Express Steckplatz. Die Schnittstelle hat folgende Pinbelegung:

Pin	Seite A		Seite B	
	Name	Beschreibung	Name	Beschreibung
1	PRSNT1#	Hot-plug presence detect	+12V	DC 12V power
2	+12V	DC 12V power	+12V	DC 12V power
3	+12V	DC 12V power	+12V	DC 12V power
4	GND	Ground	GND	Ground
5	JTAG2	nicht verwendet	SMCLK	nicht verwendet
6	JTAG3	nicht verwendet	SMDAT	nicht verwendet
7	JTAG4	nicht verwendet	GND	nicht verwendet
8	JTAG5	nicht verwendet	+3,3V	nicht verwendet
9	+3,3V	nicht verwendet	JTAG1	nicht verwendet
10	+3,3V	DC 3,3V power	+3,3Vaux	DC 3,3V auxiliary power
11	PERST#	Fundamental reset	WAKE#	Signal for link activation
12	GND	Ground	RSVD	nicht verwendet
13	REFCLK+	Reference clock input (differential pair)	GND	Ground
14	REFCLK-		PETp0	Transmitter
15	GND	Ground	PETn0	(differential pair)
16	PERp0	Receiver (differential pair)	GND	Ground
17	PERn0	Receiver (differential pair)	PRSNT2x	Hot-plug presence detect
18	GND	Ground	GND	Ground

2.3.3 LEDs



- 1 LED-Leiste
- 2 LEDs RJ45-Buchsen

LED-Leiste ¹

Bootvorgang nach NetzEIN und Betrieb

SYS	COM0/RN	COM1/ER	Beschreibung
 grün	 grün/rot	 grün/rot	
	 grün		Applikation wird geladen.
	 grün	 grün	Kernel konnte erfolgreich kopiert werden.
	 rot 2Hz	 rot	Fehler beim Kopieren des Kernels.
 grün 2Hz	 rot 2Hz	 rot 2Hz	Applikation wurde gestoppt. Führen Sie einen Powercycle durch.
 grün 2Hz			Firmware wird geladen.
	 rot 0,5Hz	 rot 0,5Hz	Applikation konnte nicht geladen werden. Führen Sie einen Powercycle durch.
	 rot 2Hz	 rot 2Hz	Speicherüberlauf Flash-Speicher.
 grün			Applikation wurde erfolgreich geladen und initialisiert.
	 grün 2Hz	 grün 2Hz	Anforderung Powercycle nach <i>"Rücksetzen auf Werkseinstellung Typ 1"...</i> Seite 28.
	 grün 2Hz	 grün 2Hz	Firmware-Update wird durchgeführt.
	 rot 2Hz	 grün	Ungültige Schalterstellung DIP-Schalter S2 <i>"Schalter"...</i> Seite 15.

PROFINET-Betrieb ¹

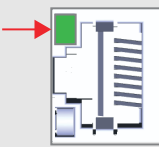
SYS	COM0	COM1	Beschreibung
 grün	 grün/rot	 grün/rot	
 grün 1Hz	X	X	Dient zur Geräteidentifizierung.
PROFINET-IO-Controller meldet			
X	X		- Der PROFINET-IO-Controller hat eine aktive Kommunikationsverbindung zu jedem projektierten PROFINET-Device aufgebaut. - Der PROFINET-IO-Controller ist nicht konfiguriert.
X	X		- Busfehler, kein Link vorhanden. - Falsche Übertragungsgeschwindigkeit. - Vollduplexübertragung ist nicht aktiviert.
X	X		Linkstatus ist vorhanden, zu mindestens einem PROFINET-Device besteht keine Kommunikationsverbindung.
PROFINET-Device meldet			
X		X	Das PROFINET-Device hat eine aktive Kommunikationsverbindung zum PROFINET-IO-Controller aufgebaut.
X		X	- Busfehler, kein Link vorhanden. - Keine Kommunikationsverbindung zum PROFINET-IO-Controller.
X		X	Linkstatus ist vorhanden, es besteht keine Kommunikationsverbindung zum PROFINET-IO-Controller.
nicht relevant: X			

EtherCAT-Betrieb ¹

SYS	RN	ER	Beschreibung
 grün	 grün/rot	 grün/rot	
X	 grün 2,5Hz	X	EtherCAT-SubDevice befindet sich im Zustand PreOp.
X	 grün 0,2/1s	X	EtherCAT-SubDevice befindet sich im Zustand SafeOp.
X	 grün	X	EtherCAT-SubDevice befindet sich im Zustand Op.
X		X	EtherCAT-SubDevice befindet sich im Zustand Init bzw. ist nicht konfiguriert.
X	X		EtherCAT-SubDevice meldet keinen Fehler.
X	X	 rot 2,5Hz	EtherCAT-SubDevice meldet fehlerhafte Konfiguration.
X	X	 rot 0,2/1s	EtherCAT-SubDevice meldet lokalen Fehler und wechselt in den Zustand SafeOp.
X	X	 rot 2x2,5Hz/1s	EtherCAT-SubDevice meldet eine Watchdog-Zeitüberschreitung z.B. Syncmanager-Timeout.
nicht relevant: X			

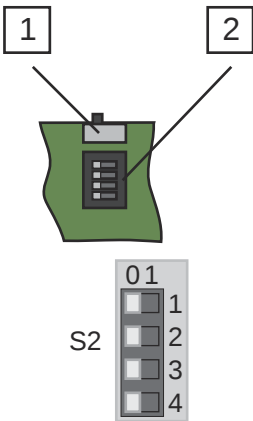
LEDs RJ45-Buchsen ²

Es kommt ausschließlich die grüne LED (oben) zum Einsatz. Die LED unten ist ohne Funktion.

LED	Farbe	Funktion
	 grün	Die entsprechende RJ45-Buchse ist physikalisch mit dem Ethernet verbunden.
	 grün flackernd	Bei Datenverkehr flackert die LED.

2.3.4 Schalter

S1: Schiebeschalter
S2: DIP-Schalter



S1: Schiebeschalter ¹

Der Schiebeschalter S1 wird intern verwendet und ist für Kundenanwendungen nicht relevant. Belassen Sie diesen in der abgebildeten Schiebe-Stellung links.

S2: DIP-Schalter ²

Es darf sich immer nur ein Schalter in Stellung "ON" befinden. Hierbei können Sie folgende Aktionen auslösen:

Schalter	Aktion
S2-1	0 (OFF): Reserviert - Defaulteinstellung
S2-2	0 (OFF): Reserviert - Defaulteinstellung
S2-3	0 (OFF): Nach PowerON startet die Steckkarte im <i>Standard Mode</i> - Defaulteinstellung. 1 (ON): Nach PowerON startet die Steckkarte im <i>"Safe Mode"...</i>Seite 30. - Kommunikation ausschließlich über <i>"Web-based Management - WBM"...</i>Seite 39. - Keine Kommunikation über PROFINET bzw. EtherCAT.
S2-4	0 (OFF): Nach PowerON startet die Steckkarte - Defaulteinstellung. 1 (ON): Nach PowerON führt die Steckkarte <i>"Rücksetzen auf Werkseinstellung Typ 1"...</i>Seite 28 durch.

2.4 Zulassungen, Richtlinien, Normen

Konformität und Approbation

Konformität

CE	2014/30/EU	EMV-Richtlinie
----	------------	----------------

Approbation

UL	UL 61010-2-201	
KC	KSC C IEC 61131-2	
UKCA	2016 No. 1091	The Electromagnetic Compatibility Regulations 2016
	2012 No. 3032	The Restriction of the use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulation 2012

Sonstiges

RoHS	2011/65/EU	Richtlinie zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten
ChinaRoHS	SJ/T 11363-2006	Use of Certain Hazardous Substances
WEEE	2012/19/EU	Rücknahme von Elektro(nik)geräten in der EU

Personenschutz und Geräteschutz

Schutzart	-	IP00
Potenzialtrennung		
zum Feldbus	-	galvanisch entkoppelt
zur Prozessebene	-	galvanisch entkoppelt
Isulationsfestigkeit	EN 61010-2-201	-
Isolationsspannung		
RJ45-Buchse X1, X2, X3, X4	-	DC 1000V (getestet für 60s)
Schutzmaßnahmen	-	-

Umgebungsbedingungen gemäß EN 61131-2

Klimatisch		
Lagerung / Transport	EN 60068-2-14	-40...+85°C
Betrieb	EN 61131-2	0...+60°C
Luftfeuchtigkeit	EN 60068-2-30	RH1 (ohne Betauung, relative Feuchte 10...95%)
Verschmutzung	EN 61131-2	Verschmutzungsgrad 2
Aufstellhöhe max.	-	2000m
Mechanisch		
Schwingung	EN 60068-2-6	1g, 9...150Hz
Schock	EN 60068-2-27	15g, 11ms

Montagebedingungen		
Einbauort	-	PCI Express Slot in Robot-Controller

EMV	Norm	Bemerkungen
Störaussendung	EN 61000-6-4	Class A (Industriebereich)
Störfestigkeit Zone B	EN 61000-6-2	Industriebereich
		ESD
		8kV bei Luftentladung (Schärfegrad 3)
		4kV bei Kontaktentladung (Schärfegrad 2)
		HF-Einstrahlung (Gehäuse)
		80...1000MHz, 10V/m, 80% AM (1kHz) 1,4...6,0GHz, 3V/m, 80% AM (1kHz)
		HF-Leitungsgeführt
		150kHz...80MHz, 10V, 80% AM (1kHz)
		Burst
		Surge ¹

1) Aufgrund der energiereichen Einzelimpulse ist bei Surge eine angemessene externe Beschaltung mit Blitzschutzelementen wie z.B. Blitzstromableitern und Überspannungsableitern erforderlich.

2.5 Einsatz unter erschwerten Betriebsbedingungen



Ohne zusätzlich schützende Maßnahmen dürfen die Produkte nicht an Orten mit erschwerten Betriebsbedingungen; z.B. durch:

- Staubentwicklung
- chemisch aktive Substanzen (ätzende Dämpfe oder Gase)
- starke elektrische oder magnetische Felder

eingesetzt werden!

2.6 Technische Daten

Artikelnr.	YRCP32F0
Bezeichnung	YRCP-MP4P
Modulkennung	-
Stromversorgung über PCIe	
Spannung	+3,3 V DC ±5 %
Spannung	+12,0 V DC ±5 %
Typische Stromaufnahme	
3V3@25°C	0,7 A
3V3@60°C	1,3 A
12V@25°C	10 mA

Technische Daten

Artikelnr.	YRCP32F0
Maximal Stromaufnahme	
3V3@25°C	1,3 A
3V3@60°C	2,3 A
12V@25°C	20 mA
Hardware	
CPU	TRITON (ARM Cortex-A17)
CPU-Kerne	3
Frequenz	1,26 GHz
RAM	512 MB
eMMC	8 GB
Bedienelemente	LEDs, DIP-Schalter (S2)
Integrierte SliceBus-Versorgung	-
Anschlüsse	
Serial Com (Sub-D)	-
SliceBus	-
Anzahl RJ45-Schnittstellen	4
Betriebssystem	
Betriebssystem	Linux mit RT Kernel
Overlay filesystem auf interner eMMC	✓
Overlay filesystem auf interner eMMC, Kapazität	1500 MB
Overlay filesystem auf externer SD-Karte	-
Overlay filesystem auf externer SD-Karte, Kapazität	-
Firewall	✓
SSH/SFTP	-
Synchronisation über Ethernet (NTP)	✓
DNS	✓
Web-based Management (WBM)	✓
PROFINET System	
VendorID	0x0111
DeviceID	0x047C
Spezifikation	Version 2.4
PROFINET-fähige Anschlüsse	X1/X2 Device, X3/X4 Controller
Controller	✓
- Max. Anzahl Devices	64@16ms, 32@8ms, 16@4ms, 8@2ms, 4@1ms
- Max. Anzahl E/A-Daten (inkl. IOxS)	8192 Byte
- Zykluszeit	1 ms .. 512 ms
- Systemredundanz	-
- Fast Startup	✓

Artikelnr.	YRCP32F0
- Fast Startup, Max. Anzahl Devices	32
- Topologie	✓
Device	✓
Device I/O Daten	2 Byte / 2 Byte 512 Byte / 512 Byte 4 Byte / 4 Byte 8 Byte / 8 Byte 16 Byte / 16 Byte 32 Byte / 32 Byte 64 Byte / 64 Byte 128 Byte / 128 Byte 256 Byte / 256 Byte 436 Byte / 436 Byte
- Zykluszeit	1 ms .. 512 ms
- MRP Client Unterstützung	✓
EtherCAT SubDevice	
E/A PDO Mapping	2 Byte / 2 Byte 512 Byte / 512 Byte 4 Byte / 4 Byte 8 Byte / 8 Byte 16 Byte / 16 Byte 32 Byte / 32 Byte 64 Byte / 64 Byte 128 Byte / 128 Byte 256 Byte / 256 Byte 436 Byte / 436 Byte
Aktualisierungszeit	1 ms .. 512 ms
EoE Unterstützung	-
CoE Unterstützung	✓
FoE Unterstützung	-
Distributed Clock Unterstützung	-
Gehäuse	
Material	Edelstahl
Befestigung	Steckkarte
Mechanische Daten	
Abmessungen (BxHxT)	21,6 mm x 120,8 mm x 138,4 mm
Gewicht Netto	105 g
Gewicht inklusive Zubehör	105 g
Gewicht Brutto	180 g

Technische Daten

Artikelnr.	YRCP32F0
Umgebungsbedingungen	
Betriebstemperatur	0 °C bis 60 °C
Lagertemperatur	-40 °C bis 85 °C
Zertifizierungen	
Zertifizierung nach UL	ja
Zertifizierung nach KC	ja
Zertifizierung nach UKCA	ja
Zertifizierung nach ChinaRoHS	ja

3 Einsatz

3.1 Sicherheitshinweise



GEFAHR

Sicherheitshinweise

Beachten Sie die folgenden Sicherheitshinweise! Werden die Sicherheitsvorschriften nicht beachtet, kann Tod, schwere Körperverletzung oder hoher Sachschaden die Folge sein!

- Personen- und Sachschutz sind nur dann gewährleistet, wenn das Gerät entsprechend seiner Bestimmung eingesetzt wird.
- Beachten Sie die Sicherheitsvorschriften der Elektrotechnik und der Berufsgenossenschaft!
- Führen Sie alle Arbeiten am Gerät im spannungslosen Zustand durch!
- Das Gerät darf nur unter Beachtung der zugehörigen Dokumentation und unter Einhaltung der darin angegebenen Vorgaben von Fachpersonal montiert werden.
- Elektrische Arbeiten dürfen nur Elektrofachkräfte durchführen.
- Das Gerät darf nur von einer für die Sicherheit der Anlage zuständigen Person in Betrieb genommen werden. Den Anschluss der Versorgungsspannung darf nur diese Person vornehmen.
- Beachten Sie die Vorsichtsmaßnahmen bei der Handhabe elektrostatisch gefährdeter Bauelemente (EN 61340-5-1, IEC 61340-5-1)!
- Reparaturen am Gerät darf nur der Hersteller durchführen.
- Bewahren Sie die Betriebsanleitung auf!
- Der Betreiber des Geräts bzw. der Anlage unterliegt den gesetzlichen Pflichten zu Arbeitssicherheit. In diesem Zusammenhang ist die Maschinenrichtlinie zu berücksichtigen.



VORSICHT

Bei Arbeiten mit und an elektrostatisch gefährdeten Baugruppen ist auf ausreichende Erdung des Menschen und der Arbeitsmittel zu achten.



HINWEIS

Geräteausfall durch Betrieb außerhalb des zulässigen Umgebungstemperaturbereichs

Wenn Sie die Steckkarte außerhalb des zulässigen Umgebungstemperaturbereichs betreiben, kann dies zu Fehlfunktionen bis hin zum Geräteausfall führen. *"Zulassungen, Richtlinien, Normen" ...Seite 16*

- Achten Sie darauf, dass Sie die Steckkarte im zugelassenen Umgebungstemperaturbereich betreiben.



HINWEIS

Geräteausfall durch Betrieb oberhalb der zulässigen Angaben für Vibration und Schock

Wenn Sie die Steckkarte oberhalb der zulässigen Angaben für Vibration und Schock betreiben, kann dies zu Fehlfunktionen bis hin zum Geräteausfall führen. *"Zulassungen, Richtlinien, Normen" ...Seite 16*

- Achten Sie darauf, dass beim Betrieb der Steckkarte die zulässigen Angaben für Vibration und Schock eingehalten werden.

**Bestimmungsgemäße
Verwendung**

- Es liegt in der Verantwortung des Kunden, die Konformität des Produkteinsatzes mit allen einschlägigen Standards, Vorschriften oder Bestimmungen zu erfüllen, auch solche, die gelten, wenn das Yaskawa-Produkt in Kombination mit anderen Produkten verwendet wird.
- Der Kunde muss sich vergewissern, dass das Yaskawa-Produkt für die vom Kunden verwendeten Anlagen, Maschinen und Geräte geeignet ist.
- Wenn das Yaskawa-Produkt auf eine Art und Weise verwendet wird, welche nicht in diesem Handbuch beschrieben ist, kann der durch das Yaskawa-Produkt gebotene Schutz beeinträchtigt werden und es bei dem Einsatz zu materiellen und immateriellen Schäden kommen.
- Wenden Sie sich an Yaskawa, um festzustellen, ob der Einsatz in den folgenden Anwendungen zulässig ist. Ist der Einsatz in der jeweiligen Anwendung zulässig, so ist das Yaskawa-Produkt unter Berücksichtigung zusätzlicher Risikobewertungen und Spezifikationen zu verwenden, und es sind Sicherheitsmaßnahmen vorzusehen, um die Gefahren im Fehlerfall zu minimieren. Besondere Vorsicht ist geboten und Schutzmaßnahmen sind zu treffen bei:
 - Verwendung im Freien, Verwendung mit möglicher chemischer Verunreinigung oder elektrischer Störung oder Verwendung unter Bedingungen oder in Umgebungen, welche nicht in Produktkatalogen oder Handbüchern beschrieben sind
 - Steuerungssysteme für Kernenergie, Verbrennungssysteme, Eisenbahnsysteme, Luftfahrtsysteme, Fahrzeugsysteme, medizinische Geräte, Vergnügungsmaschinen und Anlagen, welche gesonderten Industrie- oder Regierungsvorschriften unterliegen
 - Systeme, Maschinen und Geräte, die eine Gefahr für Leben oder Eigentum darstellen können
 - Systeme, die ein hohes Maß an Zuverlässigkeit erfordern, wie z. B. Systeme zur Gas-, Wasser- oder Stromversorgung oder Systeme, die 24 Stunden am Tag in Betrieb sind
 - Andere Systeme, die ein ähnlich hohes Maß an Sicherheit erfordern
- Verwenden Sie das Yaskawa-Produkt niemals für eine Anwendung, die eine ernsthafte Gefahr für Körper, Leben, Gesundheit oder Eigentum darstellt, ohne vorher sicherzustellen, dass das System so ausgelegt ist, dass es das erforderliche Sicherheitsniveau mit Risikowarnungen und Redundanz zur Vermeidung der Realisierung solcher Gefahren gewährleistet und dass das Yaskawa-Produkt ordnungsgemäß ausgelegt und installiert ist.
- Die in den Produktkatalogen und Handbüchern von Yaskawa beschriebenen Schaltungsbeispiele und sonstigen Anwendungsbeispiele dienen als Referenz. Überprüfen Sie die Funktionalität und Sicherheit der tatsächlich zu verwendenden Geräte und Anlagen, bevor Sie das Yaskawa-Produkt einsetzen.
- Lesen und verstehen Sie alle Verwendungsverbote und Vorsichtsmaßnahmen, und bedienen Sie das Yaskawa-Produkt korrekt, um versehentliche Schäden Dritter zu vermeiden.

Einsatzbereich

**WARNUNG****Gefahr durch nicht bestimmungsgemäße Verwendung!**

Jede über die bestimmungsgemäße Verwendung hinausgehende und/oder andersartige Benutzung des Produktes kann zu gefährlichen Situationen führen und ist untersagt.

Die YRCP-MP4P ist konstruiert und gefertigt für:

- den industriellen Einsatz.
- allgemeine Steuerungs- und Automatisierungsaufgaben.
- industrielle Netzwerkkommunikation, Maschinen- und Prozesskontrolle.
- die Anbindung an PROFINET und EtherCAT (optional).
- den Einbau in einen Robot-Controller.
- den Betrieb innerhalb der in den technischen Daten spezifizierten Umgebungsbedingungen.

**GEFAHR**

Das Gerät ist nicht zugelassen für den Einsatz:

- in explosionsgefährdeten Umgebungen (EX-Zone)

Haftungsausschluss

(1) Die vertragliche und gesetzliche Haftung von Yaskawa sowie der gesetzlichen Vertreter und Erfüllungsgehilfen von Yaskawa für Schadensersatz und Aufwendungsersatz, in Bezug auf den Inhalt dieser Dokumentation, wird wie folgt ausgeschlossen beziehungsweise beschränkt:

(a) Für die leicht fahrlässige Verletzung *Wesentlicher Vertragspflichten* aus dem Schuldverhältnis haftet Yaskawa der Höhe nach begrenzt auf den vertragstypischen und vorhersehbaren Schaden. "*Wesentliche Vertragspflichten*" sind solche Verpflichtungen, deren Erfüllung den Vertrag prägt und auf die der Kunde von Yaskawa vertrauen durfte.

(b) Für (i) die leicht fahrlässige Verletzung von Pflichten aus dem Schuldverhältnis, die nicht *Wesentliche Vertragspflichten* sind, sowie (ii) höhere Gewalt, d.h. von außen kommende, keinen betrieblichen Zusammenhang aufweisende und auch durch äußerste vernünftigerweise zu erwartender Sorgfalt nicht abwendbare Ereignisse, haftet Yaskawa jeweils nicht.

(2) Die vorgenannte Haftungsbeschränkung gilt nicht (i) in den Fällen zwingender gesetzlicher Haftung (insbesondere nach dem Produkthaftungsgesetz), (ii) wenn und soweit Yaskawa eine Garantie oder ein garantiegleiches Beschaffungsrisiko nach § 276 BGB übernommen hat, (iii) für schuldhaft verursachte Verletzungen von Leben, Körper und/oder Gesundheit, auch durch Vertreter oder Erfüllungsgehilfen, sowie (iv) im Falle des Verzuges bei einem fixen Leistungstermin.

(3) Eine Umkehr der Beweislast ist mit den vorstehenden Regelungen nicht verbunden.

Handhabung elektrostatisch gefährdeter Baugruppen

Die Baugruppen sind mit hochintegrierten Bauelementen in MOS-Technik bestückt. Diese Bauelemente sind hoch empfindlich gegenüber Überspannungen, die z.B. bei elektrostatischer Entladung entstehen. Zur Kennzeichnung dieser gefährdeten Baugruppen wird nachfolgendes Symbol verwendet:



Das Symbol befindet sich auf Baugruppen, Baugruppenträgern oder auf Verpackungen und weist so auf elektrostatisch gefährdete Baugruppen hin. Elektrostatisch gefährdete Baugruppen können durch Energien und Spannungen zerstört werden, die weit unterhalb der Wahrnehmungsgrenze des Menschen liegen. Hantiert eine Person, die nicht elektrisch entladen ist, mit elektrostatisch gefährdeten Baugruppen, können Spannungen auftreten und zur Beschädigung von Bauelementen führen und so die Funktionsweise der Baugruppen beeinträchtigen oder die Baugruppen unbrauchbar machen. Auf diese Weise beschädigte Baugruppen werden in den wenigsten Fällen sofort als fehlerhaft erkannt. Der Fehler kann sich erst nach längerem Betrieb einstellen. Durch statische Entladung beschädigte Bauelemente können bei Temperaturänderungen, Erschütterungen oder Lastwechseln zeitweilige Fehler zeigen. Nur durch konsequente Anwendung von Schutzeinrichtungen und verantwortungsbewusste Beachtung der Handhabungsregeln lassen sich Funktionsstörungen und Ausfälle an elektrostatisch gefährdeten Baugruppen wirksam vermeiden.

Versenden von Baugruppen

Verwenden Sie für den Versand immer die Originalverpackung.

3.2 Montage

Die Steckkarte ist in einem Robot-Controller mit PCI Express Steckplatz zu montieren. Die Vorgehensweise zur Montage finden Sie im entsprechenden Handbuch des Robot-Controllers.

3.3 Gerätetausch und Reparatur

Gerätetausch

Bei einem Gerätetausch müssen alle Kommunikationseinstellungen erneut vorgenommen werden. Informationen zur Vorgehensweise bei der Demontage finden Sie im entsprechenden Handbuch des Robot-Controllers.

Reparatur und Gerätedefekt

Reparaturen dürfen ausschließlich von Yaskawa vorgenommen werden.

- Kontaktieren Sie vor der Rücksendung immer Ihre Landesvertretung von Yaskawa.
- Senden Sie defekte Geräte zur Reparatur oder zum Erhalt eines Ersatzgeräts an die Landesvertretung von Yaskawa zurück.
- Verwenden Sie bei Rücksendung immer die Originalverpackung.

Entsorgung

Zur Entsorgung des Geräts nationale Vorschriften beachten!

3.4 Industrielle Sicherheit in der Informationstechnologie

Aktuellste Version

Dieses Kapitel finden Sie auch als Leitfaden *"Industrielle IT-Sicherheit"* im *"Download Center"* unter www.yaskawa.eu.com

Gefahren

Datensicherheit und Zugriffsschutz wird auch im industriellen Umfeld immer wichtiger. Die fortschreitende Vernetzung ganzer Industrieanlagen mit den Unternehmensebenen und die Funktionen zur Fernwartung führen zu höheren Anforderungen zum Schutz der Industrieanlagen. Gefährdungen können entstehen durch:

- Innere Manipulation wie technische Fehler, Bedien- und Programmfehler und vorsätzliche Programm- bzw. Datenmanipulation.
- Äußere Manipulation wie Software-Viren, -Würmer und Trojaner.
- Menschliche Unachtsamkeit wie z.B. Passwort-Phishing.

Schutzmaßnahmen

Die wichtigsten Schutzmaßnahmen vor Manipulation und Verlust der Datensicherheit im industriellen Umfeld sind:

- Verschlüsselung des Datenverkehrs mittels Zertifikaten.
- Filterung und Kontrolle des Datenverkehrs durch VPN - "Virtual Private Networks".
- Identifizierung der Teilnehmer durch "Authentifizierung" über sicheren Kanal.
- Segmentierung in geschützte Automatisierungszellen, so dass nur Geräte in der gleichen Gruppe Daten austauschen können.
- Deaktivierung überflüssiger Hard- und Software.

Weiterführende Informationen

Nähere Informationen zu den Maßnahmen finden Sie auf den folgenden Webseiten:

- Bundesamt für Informationstechnik ➔ www.bsi.bund.de
- Cybersecurity & Infrastructure Security Agency ➔ us-cert.cisa.gov
- VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik ➔ www.vdi.de

3.4.1 Absicherung von Hardware und Applikationen

Maßnahmen

- Integrieren Sie keine Komponenten bzw. Systeme in öffentliche Netzwerke.
 - Setzen Sie bei Einsatz in öffentlichen Netzwerken VPN "Virtual Private Networks" ein. Hiermit können Sie den Datenverkehr entsprechend kontrollieren und filtern.
- Halten Sie Ihre Systeme immer auf dem neuesten Stand.
 - Verwenden Sie immer den neuesten Firmwarestand für alle Geräte.
 - Führen Sie regelmäßige Updates Ihrer Bedien-Software durch.
- Schützen Sie Ihre Systeme durch eine Firewall.
 - Die Firewall schützt Ihre Infrastruktur nach innen und nach außen.
 - Hiermit können Sie Ihr Netzwerk segmentieren und ganze Bereiche isolieren.
- Sichern Sie den Zugriff auf Ihre Anlagen über Benutzerkonten ab. *"Benutzerauthentifizierung"...Seite 63*
 - Verwenden Sie nach Möglichkeit ein zentrales Benutzerverwaltungssystem.
 - Legen Sie für jeden Benutzer, für den eine Autorisierung unbedingt erforderlich ist, ein Benutzerkonto an.
 - Halten Sie die Benutzerkonten immer aktuell und deaktivieren Sie nicht verwendete Benutzerkonten.
- Schützen Sie den Zugriff auf Ihre Anlagen durch sichere Passwörter.
 - Ändern Sie das Passwort einer Standard-Anmeldung nach dem ersten Start.
 - Verwenden Sie sichere Passwörter bestehend aus Groß-/Kleinschreibung, Zahlen und Sonderzeichen. Der Einsatz eines Passwort-Generators bzw. -Managers wird empfohlen.
 - Ändern Sie die Passwörter gemäß den für Ihre Anwendung geltenden Regeln und Vorgaben.
- Berücksichtigen Sie bei der Anlagenplanung und Absicherung mögliche Verteidigungsstrategien.
 - Die alleinige Isolation von Komponenten ist nicht ausreichend für einen umfassenden Schutz. Hier ist ein Gesamt-Konzept zu entwerfen, welches auch Verteidigungsmaßnahmen im Falle eines Cyber-Angriffs vorsieht.
 - Führen Sie in regelmäßigen Abständen Bedrohungsanalysen durch. Unter anderem erfolgt hier eine Gegenüberstellung zwischen den getroffenen zu den erforderlichen Schutzmaßnahmen.
- Verwenden Sie sichere Zugriffspfade wie HTTPS bzw. VPN für den Remote-Zugriff auf Ihre Anlage.
- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung gemäß der gültigen Sicherheitsrichtlinie und den gesetzlichen Anforderungen zum Datenschutz.

3.4.2 Absicherung von PC-basierter Software

Maßnahmen

Da PC-basierte Software zur Programmierung, Konfiguration und Überwachung verwendet wird, können hiermit auch ganze Anlagen oder einzelne Komponenten manipuliert werden. Hier ist besondere Vorsicht geboten!

- Verwenden Sie Benutzerkonten auf Ihren PC-Systemen.
 - Verwenden Sie nach Möglichkeit ein zentrales Benutzerverwaltungssystem.
 - Legen Sie für jeden Benutzer, für den eine Autorisierung unbedingt erforderlich ist, ein Benutzerkonto an.
 - Halten Sie die Benutzerkonten immer aktuell und deaktivieren Sie nicht verwendete Benutzerkonten.
- Schützen Sie Ihre PC-Systeme durch sichere Passwörter.
 - Ändern Sie das Passwort einer Standard-Anmeldung nach dem ersten Start.
 - Verwenden Sie sichere Passwörter bestehend aus Groß-/Kleinschreibung, Zahlen und Sonderzeichen. Der Einsatz eines Passwort-Generators bzw. -Managers wird empfohlen.
 - Ändern Sie die Passwörter gemäß den für Ihre Anwendung geltenden Regeln und Vorgaben.
- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung gemäß der gültigen Sicherheitsrichtlinie und den gesetzlichen Anforderungen zum Datenschutz.
- Schützen Sie Ihre PC-Systeme durch Sicherheitssoftware.
 - Installieren Sie auf Ihren PC-Systemen Virens Scanner zur Identifikation von Viren, Trojanern und anderer Malware.
 - Installieren Sie Software, die Phishing-Attacken erkennen und aktiv verhindern kann.
- Halten Sie Ihre Software immer auf dem neuesten Stand.
 - Führen Sie regelmäßige Updates Ihres Betriebssystems durch.
 - Führen Sie regelmäßige Updates Ihrer Software durch.
- Führen Sie regelmäßige Datensicherungen durch und lagern Sie die Datenträger an einem sicheren Ort.
- Führen Sie regelmäßige Neustarts Ihrer PC-Systeme durch. Starten Sie nur von Datenträgern, welche gegen Manipulation geschützt sind.
- Setzen Sie Verschlüsselungssysteme auf Ihren Datenträgern ein.
- Führen Sie regelmäßig Sicherheitsbewertungen durch, um das Manipulationsrisiko zu verringern.
- Verwenden Sie nur Daten und Software aus zugelassenen Quellen.
- Deinstallieren Sie Software, welche nicht verwendet wird.
- Deaktivieren Sie nicht verwendete Dienste.
- Aktivieren Sie an Ihrem PC-System eine passwortgeschützte Bildschirmsperre.
- Sperren Sie Ihre PC-Systeme immer, sobald Sie den PC-Arbeitsplatz verlassen.
- Klicken Sie auf keine Links, welche von unbekannten Quellen stammen. Fragen Sie ggf. nach, z.B. bei E-Mails.
- Verwenden Sie sichere Zugriffspfade wie HTTPS bzw. VPN für den Remote-Zugriff auf Ihr PC-System.

3.5 Lizenzhinweise zu Open Source Software

- Die Steckkarte arbeitet mit einem Linux-Betriebssystem.
- Lizenzinformationen zu den einzelnen Linux-Paketen können Sie im Web-based Management (WBM) über die Schaltfläche *"Rechtliche Hinweise"* abrufen. *"Web-based Management - WBM"...Seite 39*
- Jede Open Source Software, die im Produkt verwendet wird, unterliegt den jeweiligen Lizenzbestimmungen, die von den Yaskawa-Software-Lizenzbedingungen (**Software License Terms - SLT**) für das Produkt nicht berührt werden.
- Der Lizenznehmer kann die jeweilige Open Source Software entsprechend den geltenden Lizenzbestimmungen ändern.



Original-Hinweise zu OpenSSL

- *This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (↪ <http://www.openssl.org/>).*
- *This product includes cryptographic software written by Eric Young (↪ eay@cryptsoft.com).*

3.6 Rücksetzen auf Werkseinstellung Typ 1



Bitte beachten Sie, dass durch Rücksetzen auf Werkseinstellung Typ 1 alle Einstellungen der Steckkarte auf Ihre Standardwerte zurückgesetzt werden. Dies betrifft auch alle Einstellungen, welche über das WBM durchgeführt wurden.

Nach Rücksetzen auf Werkseinstellung Typ 1 besitzt die Steckkarte folgende Kommunikationseinstellungen:

- Die Kommunikation über PROFINET ist aktiviert.
 - X1/X2 (default: 192.168.3.1, "MAC2"): PROFINET-Device
 - X3/X4 (default: 192.168.1.1, "MAC1"): PROFINET-IO-Controller
- Die Kommunikation über EtherCAT ist deaktiviert.
- *"Web-based Management - WBM"...Seite 39* ist erreichbar über:
 - X1/X2 (default: 192.168.3.1, "MAC2")
 - X3/X4 (default: 192.168.1.1, "MAC1")

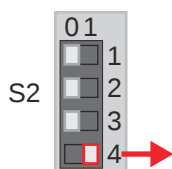
Mit DIP-Schalter S2

Mittels DIP-Schalter S2 "*Schalter*"...Seite 15 können Sie ein *Rücksetzen auf Werkseinstellung Typ 1* nach folgender Vorgehensweise durchführen.

1. Schalten Sie die Spannungsversorgung der Steckkarte aus.

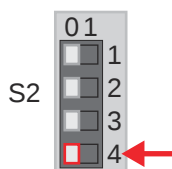
**VORSICHT**

Beim Abschalten der Spannungsversorgung der Steckkarte ist das übergeordnete System auszuschalten. Bitte beachten Sie hierbei die Vorgehensweisen und Sicherheitshinweise in der zugehörigen Dokumentation!



2. Bringen Sie den DIP-Schalter S2-4 in Stellung 1 (ON).
3. Schalten Sie die Spannungsversorgung der Steckkarte wieder ein.
 - ➔ Die Steckkarte wird auf ihre Standardeinstellungen zurückgesetzt.
4. Sobald die LEDs folgendes Verhalten zeigen, schalten Sie die Spannungsversorgung der Steckkarte aus:

SYS	COM0	COM1	Beschreibung
☐	☒ grün 2Hz	☒ grün 2Hz	Anforderung Powercycle.



5. Bringen Sie den DIP-Schalter S2-4 in Stellung 0 (OFF).
6. Schalten Sie die Spannungsversorgung der Steckkarte wieder ein.
 - ➔ Die Steckkarte arbeitet nun mit den Standardeinstellungen.

Mit WBM

Mittels der Symbolleiste von "*Cockpit*"...Seite 42 können Sie ein *Rücksetzen auf Werkeinstellung Typ 1* nach folgender Vorgehensweise durchführen.

1. Klicken Sie in der Symbolleiste auf .
 - ➔ Die Steckkarte wird auf ihre Standardeinstellungen zurückgesetzt.
2. Sobald die LEDs folgendes Verhalten zeigen, schalten Sie die Spannungsversorgung der Steckkarte aus:

SYS	COM0	COM1	Beschreibung
☐	☒ grün 2Hz	☒ grün 2Hz	Anforderung Powercycle.

3. Schalten Sie die Spannungsversorgung der Steckkarte wieder ein.
 - ➔ Die Steckkarte arbeitet nun mit den Standardeinstellungen.

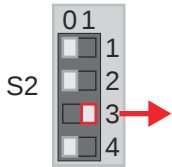
3.7 Firmware-Update



Ein Firmware-Update der Steckkarte können Sie ausschließlich über "*Web-based Management - WBM*"...Seite 39 durchführen.
 "*Firmware-Update*"...Seite 67

3.8 Safe Mode

Starten im *Safe Mode*

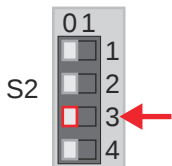


Mittels DIP-Schalter S2 "*Schalter*"...Seite 15 können Sie Ihre Steckkarte im *Safe Mode* starten lassen. Im Safe Mode startet die Steckkarte mit folgendem Verhalten:

- Die Kommunikation über PROFINET ist deaktiviert.
- Die Kommunikation über EtherCAT ist deaktiviert.
- Sie können ausschließlich über "*Web-based Management - WBM*"...Seite 39 mit der Steckkarte kommunizieren. Der Zugriff ist ausschließlich über die Default IP-Adressen möglich.
 - X1/X2 (default: 192.168.3.1, "*MAC2*")
 - X3/X4 (default: 192.168.1.1, "*MAC1*")
- Die aktuelle Firmware-Version bleibt unverändert.

1. Schalten Sie die Spannungsversorgung der Steckkarte aus.
2. Bringen Sie den DIP-Schalter S2-3 in Stellung 1 (ON).
3. Schalten Sie die Spannungsversorgung der Steckkarte wieder ein.
 - ➔ Die Steckkarte startet im *Safe Mode*.

Starten im *Standard Mode*



1. Schalten Sie die Spannungsversorgung der Steckkarte aus.
2. Bringen Sie den DIP-Schalter S2-3 in Stellung 0 (OFF).
3. Schalten Sie die Spannungsversorgung der Steckkarte wieder ein.
 - ➔ Die Steckkarte startet im *Standard Mode*.

4 Einsatz unter PROFINET

4.1 Einsatz als PROFINET-IO-Controller

PLCnext Technology



- Die Steckkarte basiert auf PLCnext Technology® von Phoenix Contact.
- Die Steckkarte arbeitet mit einem Linux Betriebssystem.
- Den integrierten PROFINET-IO-Controller können Sie ausschließlich mit 2CON konfigurieren.

Firewall



- Im Auslieferungszustand ist die Firewall auf der Steckkarte deaktiviert!
- Sicherheitsempfehlung: Aktivieren Sie die Firewall!
- Im WBM können Sie unter "Security → Firewall" die Firewall aktivieren.
["Firewall"...Seite 58](#)
- Bitte beachten Sie, dass Sie ausschließlich als Administrator Zugriff auf die Firewall-Einstellungen haben!

4.1.1 2CON installieren

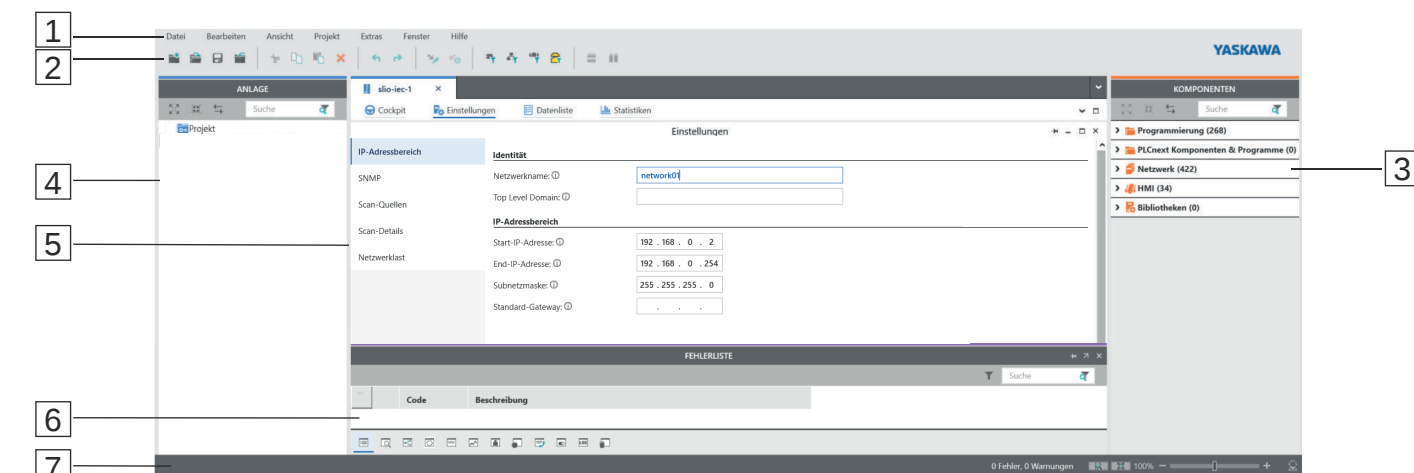
Installation

Für den Einsatz des PROFINET-IO-Controllers ist die Software 2CON erforderlich.

1. Laden Sie die Software 2CON auf Ihren PC herunter. Sie finden diese unter www.yaskawa.eu.com im "Download Center".
2. Entpacken Sie die Datei in Ihr Arbeitsverzeichnis und starten Sie die Installation per Doppelklick auf die exe-Datei.
3. Folgen Sie den Anweisungen des Installationsassistenten.
 - ➔ Die Installation wird gestartet.
4. Starten Sie, wenn Sie dazu aufgefordert werden, Ihr System neu.
 - ➔ Die Installation wird fertig gestellt. Sie können 2CON jetzt starten.

4.1.2 2CON Benutzeroberfläche

Übersicht



- 1 Menüleiste
- 2 Symbolleiste
- 3 "Komponenten"-Bereich
- 4 "Anlage"-Bereich

- 5 Editorenbereich
- 6 Funktionsübergreifender Bereich
- 7 Statusleiste

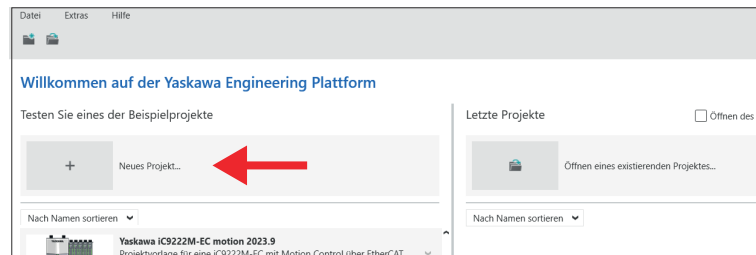
Menüleiste	Die Menüleiste ermöglicht den Zugriff auf eine Reihe von projektbezogenen Befehlen, die sich nicht explizit auf eine bestimmte Engineering-Aufgabe beziehen.
Symbolleiste	Die Symbolleiste ermöglicht den Zugriff auf eine Reihe projektbezogener Befehle, welche sich nicht explizit auf eine bestimmte Engineering-Aufgabe beziehen. Zusätzlich bieten die verschiedenen Bereiche und Editoren ihre eigenen spezifischen Symbolleisten.
"Komponenten"-Bereich	Der Bereich <i>"Komponenten"</i> beinhaltet alle für das Projekt verfügbaren Komponenten. Die Komponenten lassen sich anhand ihrer Funktion in folgende Typen unterteilen: ■ Programmcode entwickeln (Datentypen, Programme, Funktionen und Funktionsbausteine). ■ Alle für den Bereich <i>"Anlage"</i> verfügbaren Geräte anzeigen bzw. hinzufügen. ■ Bibliotheken einfügen wie Firmware-Bibliotheken, IEC-Nutzerbibliotheken usw.
"Anlage"-Bereich	Im Bereich <i>"Anlage"</i> bilden Sie alle physischen und logischen Komponenten Ihrer Applikation in Form einer hierarchischen Baumstruktur ab.
Editorenbereich	■ Über einen Doppelklick auf einen Knoten im Bereich <i>"Anlage"</i> oder auf ein Element im Bereich <i>"Komponenten"</i> öffnet sich im Editorenbereich die zugehörige Editorengruppe. ■ Editorengruppen werden immer in der Mitte der Benutzeroberfläche angezeigt. ■ Jede Editorengruppe beinhaltet mehrere Editoren, welche über Schaltflächen in der Editorengruppe geöffnet und geschlossen werden können. ■ Anhand der farblichen Darstellung der Editorengruppe können Sie den entsprechenden Editor identifizieren: – Blau: Editor aus dem Bereich <i>"Anlage"</i>. – Orange: Editor aus dem Bereich <i>"Komponenten"</i>.
Funktionsübergreifender Bereich	Der funktionsübergreifende Bereich beinhaltet Funktionen, welche sich über Ihr gesamtes Projekt erstrecken. ■ Hier werden alle Fehler, Warnungen und Nachrichten des aktuellen Projekts angezeigt. ■ Elemente, welche Sie aus den Bereichen <i>"Anlage"</i> oder <i>"Komponenten"</i> kürzlich gelöscht haben, werden in den Papierkorb verschoben. Bei Bedarf können Sie hier gelöschte Elemente wiederherstellen.
	 Näheres hierzu finden Sie in der zugehörigen Onlinehilfe von 2CON.
Statusleiste	Erkannte Fehler und Warnungen werden hier angezeigt. Zusätzlich haben Sie hier bei grafischen Anwendungen eine Zoomfunktion.

4.1.3 Konfiguration

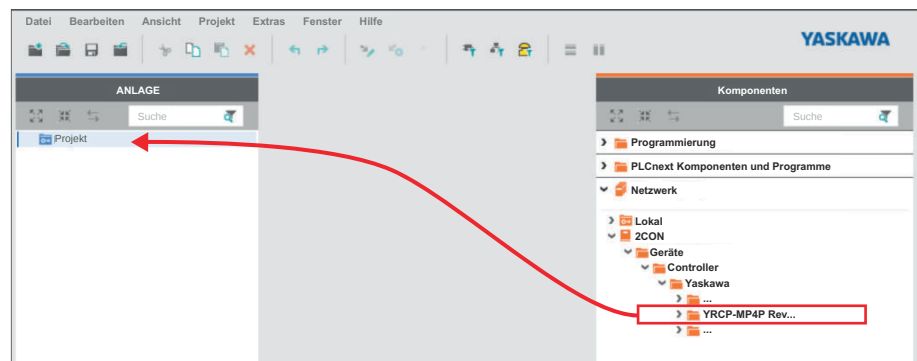
4.1.3.1 Neues Projekt erstellen

Vorgehensweise

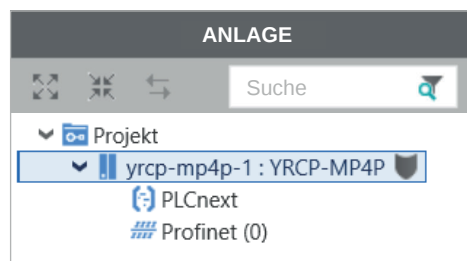
1. Starten Sie 2CON.



2. Klicken Sie auf "Neues Projekt...".
➔ Eine leere Projektvorlage wird geöffnet.
3. Navigieren Sie im "Komponenten"-Bereich über "Netzwerk" zur Steckkarte YRCP-MP4P..., welche der Hardware- bzw. der Firmwareversion entspricht. ["Spezifische Informationen" \[3\] "...Seite 10"](#)



4. Ziehen Sie die Auswahl auf "Projekt" im "Anlage"-Bereich.
➔ Die ausgewählte Steckkarte wird dem Projekt hinzugefügt.



5. Öffnen Sie "Datei → Speichern unter", vergeben Sie einen aussagekräftigen Namen für Ihr Projekt und schließen Sie den Dialog mit [Speichern].
➔ Das Projekt für die Steckkarte wird gespeichert.

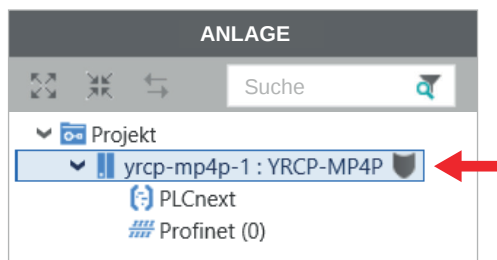
4.1.3.2 Online-Zugriff auf die Steckkarte

IP-Adress-Parameter für die Kommunikation

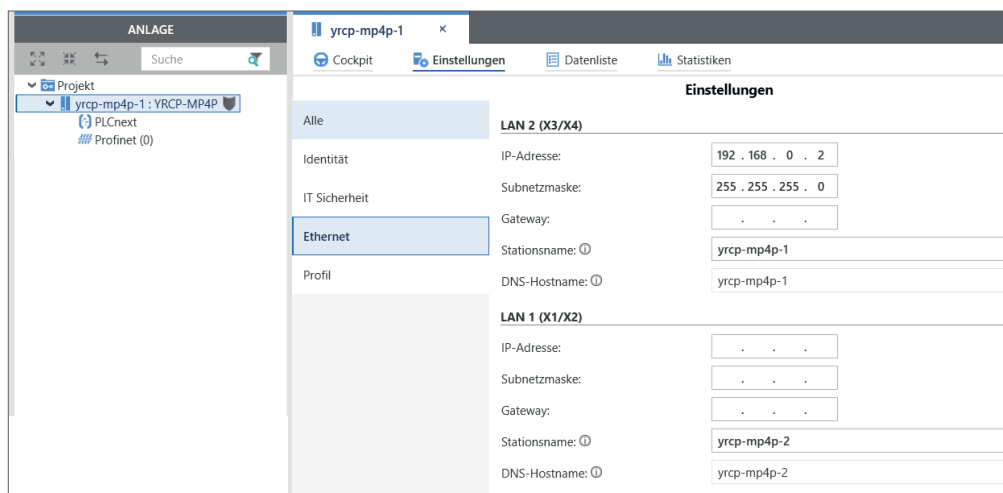
Im Auslieferungszustand besitzt die Steckkarte folgende Zugangsparameter für den Online-Zugriff:

- X1/X2 (default: 192.168.3.1, "MAC2"): PROFINET-Device
- X3/X4 (default: 192.168.1.1, "MAC1"): PROFINET-IO-Controller
- X1/X2/X3/X4: Zugriff auf *"Web-based Management - WBM"...* [Seite 39](#)
- Subnetzmaske: 255.255.255.0
- Gateway: -

Für den Onlinezugriff aus 2CON können Sie die IP-Adress-Parameter nach folgender Vorgehensweise anpassen:



1. ➤ Doppelklicken Sie im Bereich "Anlage" auf den Knoten der Steckkarte.
➔ Die Editorengruppe der Steckkarte wird geöffnet.
2. ➤ Wählen Sie den Editor "Einstellungen".
3. ➤ Wählen Sie die Ansicht "Ethernet".

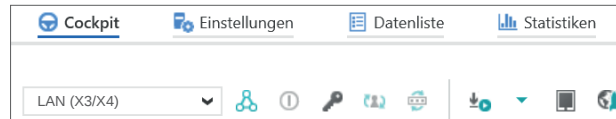


4. ➤ Geben Sie unter "LAN ..." die IP-Adress-Parameter für die Verbindung über den entsprechenden Ethernet-Port (X...) an.
➔ Beim Aufbau einer Ethernet-Verbindung zur Steckkarte verwendet 2CON die hier angegebenen IP-Adress-Parameter für die entsprechende Schnittstelle.

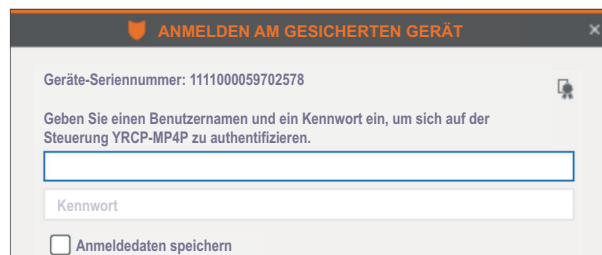
Mit der Steckkarte verbinden

Verbinden Sie beispielsweise den Port X3 oder X4 mit der Ethernet-Schnittstelle Ihres PCs. Bitte beachten Sie, dass sich zur Kommunikation über 2CON die Netzwerkkarte des PCs und die Ethernet-Schnittstelle der Steckkarte im gleichen IP-Kreis befinden. Kontaktieren Sie hierzu ggf. Ihren Netzwerkadministrator.

1. ➤ Wählen Sie in der Editorengruppe der Steckkarte den Editor "Cockpit".
2. ➤ Stellen Sie die Schnittstelle "LAN (X3/X4)" ein und klicken Sie auf .



- ➔ Eine Verbindung zwischen 2CON und Ihrer Steckkarte wird, unter Verwendung der IP-Adress-Parameter, aufgebaut und der Anmeldedialog zur Authentifizierung geöffnet.

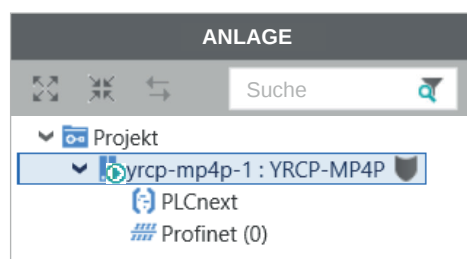


3. ➤ Geben Sie Ihre Zugangsdaten an und klicken Sie auf .



- Per Default ist die Benutzerauthentifizierung aktiviert. Im Auslieferungszustand ist der "Admin"-Benutzer bereits mit Administratorrechten angelegt.
- Bitte beachten Sie, dass Sie durch Deaktivierung der Benutzerauthentifizierung die Sicherheit Ihres Systems gegen unerlaubten Zugriff sehr gefährden!
- Das Administrator-Passwort mit der Bezeichnung "PW:" befindet sich auf der Steckkarte. [Spezifische Informationen](#) ³ "...Seite 10"
- Verwenden Sie das Administrator-Passwort ausschließlich für die Erstanmeldung am WBM.
- Nachdem Sie sich erfolgreich angemeldet haben, sollten Sie aus Sicherheitsgründen das Administrator-Passwort ändern.

- ➔ Sie haben jetzt Zugriff auf Ihre Steckkarte. Eine bestehende Verbindung wird im Bereich "Anlage" am Knoten der Steckkarte durch  angezeigt.

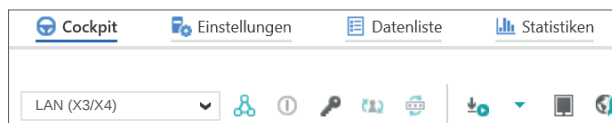


4.1.3.3 Neue IP-Adress-Parameter zuweisen

Zuweisung über WBM

Sobald Sie online mit der Steckkarte verbunden sind, können Sie dieser über WBM (Web-based Management) neue IP-Adress-Parameter zuweisen.

1. ➤ Zum Aufruf des WBM klicken Sie im Editor "Cockpit" auf .



- ➔ Die Anmeldeseite von WBM wird geöffnet.

2. ➤ Geben Sie Ihre Zugangsdaten an und klicken Sie auf [Anmelden].



- Per Default ist die Benutzerauthentifizierung aktiviert. Im Auslieferungszustand ist der "Admin"-Benutzer bereits mit Administratorrechten angelegt.
- Bitte beachten Sie, dass Sie durch Deaktivierung der Benutzerauthentifizierung die Sicherheit Ihres Systems gegen unerlaubten Zugriff sehr gefährden!
- Das Administrator-Passwort mit der Bezeichnung "PW:" befindet sich auf der Steckkarte. ["Spezifische Informationen" 3 "...Seite 10"](#)
- Verwenden Sie das Administrator-Passwort ausschließlich für die Erstanmeldung am WBM.
- Nachdem Sie sich erfolgreich angemeldet haben, sollten Sie aus Sicherheitsgründen das Administrator-Passwort ändern.

- ➔ Sie haben jetzt Zugriff auf das WBM der Steckkarte mit den Ihnen zugewiesenen Zugriffsrechten.

3. ➤ Navigieren Sie zu "Netzwerk" im Bereich "Konfiguration".

- ➔ Hier können Sie in der Spalte "Konfiguration" die aktuellen IP-Adress-Parameter ändern.

LAN 1 (X1/X2)	Status	Konfiguration
IP-Adresse	192.168.3.1	192.168.3.1
Subnetzmaske	255.255.255.0	255.255.255.0
Standard-Gateway	0.0.0.0	0.0.0.0
DNS-Serveradressen	8.8.8.8	8.8.8.8
	8.8.4.4	8.8.4.4
MAC-Adresse	00:20:B5:2E:CE:7E	

Port X1		
Datenrate		
Duplexmodus		
Link-Status	Link Down	

4. → Geben Sie in der Spalte "Konfiguration" Ihre neuen IP-Adress-Parameter ein.

**VORSICHT**

Bitte beachten Sie bei der Vergabe der IP-Adress-Parameter, dass sich sofern vorhanden die Nummernkreise der IP-Adressen von X1/X2 und X3/X4 nicht überschneiden dürfen!

5. → Klicken Sie auf [Anwenden und neu starten].

- Die Einstellungen werden übernommen, an die Steckkarte übertragen und zur Aktivierung die Steckkarte automatisch neu gestartet.



Die Steckkarte ist jetzt ausschließlich über die neuen IP-Adress-Parameter erreichbar. Bitte beachten Sie, dass diese neuen Daten aktuell nicht automatisch in die Einstellungen von 2CON übernommen werden. Diese müssen Sie dort manuell in den Einstellungen anpassen.



Weitere Informationen zur Konfiguration des PROFINET-IO-Controllers und zur Integration in Ihr PROFINET-Netzwerk finden Sie in der Onlinehilfe von 2CON.

4.2 Einsatz als PROFINET-Device

Übersicht

- Die Funktionalität *PROFINET-Device* erlaubt es, Daten mit einem übergeordneten PROFINET-IO-Controller auszutauschen.
- Das PROFINET-Device ist als IO-Device über X1/X2 (default: 192.168.3.1, "MAC2") an einen PROFINET-IO-Controller anzubinden.
- Für die Projektierung in einem PROFINET-IO-Controller finden Sie im "Download Center" von www.yaskawa.eu.com die zugehörige "GSDML-V...-YASKAWA-YRCP-MP4P-....xml".
- Für die Kommunikation über PROFINET müssen Sie Ihrem PROFINET-Device einen Namen vergeben. Die Vergabe erfolgt mit dem Engineering Tool des übergeordneten PROFINET-IO-Controllers.



Nähere Informationen hierzu finden Sie im Handbuch zu Ihrem übergeordneten PROFINET-IO-Controller.

5 Einsatz unter EtherCAT

5.1 Bezeichnungen

MainDevice (MDevice)

Das MDevice ist die zentrale Steuereinheit unter EtherCAT. Es übernimmt die Rolle des übergeordneten Geräts, welches den Kommunikationsablauf koordiniert und Befehle an die angebundenen SubDevices sendet.

**SubordinateDevice
(SubDevice)**

Das SubDevice ist ein untergeordnetes Gerät unter EtherCAT. Dieses empfängt die Anweisungen vom MDevice und reagiert entsprechend hierauf. Das YRCP32F0 ist ein SubDevice.

5.2 Einsatz als EtherCAT-SubDevice

Übersicht

- Für die Projektierung in einem EtherCAT-MainDevice finden Sie im *"Download Center"* von www.yaskawa.eu.com die zugehörige *"ESI-V...-YASKAWA-YRCP-MP4P-....xml"*. Installieren Sie diese in Ihrem EtherCAT-Konfigurationstool.
- Aktivieren Sie in Ihrem Robot-Controller die EtherCAT-Kommunikation mittels der User-API für X1/X2.
- Der Anschluss an ein übergeordnetes EtherCAT-MainDevice erfolgt über X1: EtherCAT-Port - SubDevice IN.
- Der Anschluss an ein nachfolgendes EtherCAT-SubDevice erfolgt über X2: EtherCAT-Port - SubDevice OUT.
- Stellen Sie die gewünschten PDO-Größen ein. Hierbei werden ausschließlich die PDO-Größen unterstützt, welche in den *"Technische Daten" ...Seite 17* aufgeführt sind.



Nähere Informationen hierzu finden Sie im Handbuch zu Ihrem übergeordneten EtherCAT-MainDevice.

EtherCAT[®]
Conformance tested

6 Web-based Management - WBM

6.1 Übersicht und erste Schritte

Zugriff auf WBM

- Die Steckkarte verfügt über ein webbasiertes Management (WBM). Im WBM können Sie auf statische und dynamische Informationen zugreifen und bestimmte Einstellungen ändern. Sie können WBM über die Ethernet-Schnittstellen der Steckkarte aufrufen.
 - Sie können WBM nur aufrufen, wenn die Steckkarte über eine gültige IP-Adresse verfügt.
 - Im Auslieferungszustand hat die Steckkarte die IP-Adressen:
 - X1/X2 (default: 192.168.3.1, "MAC2")
 - X3/X4 (default: 192.168.1.1, "MAC1")
1. ➔ Stellen Sie für die Erstinbetriebnahme eine gesicherte Verbindung zwischen Konfigurations-PC und Steckkarte her, wie z.B. eine Punkt-zu-Punkt-Verbindung über Ethernet.
 2. ➔ Über die Suche in 2CON können Sie die IP-Adresse der entsprechenden Ethernet-Schnittstelle ermitteln. Navigieren Sie hierzu in 2CON zu "PROFINET" im "Anlage"-Bereich und wählen Sie "Online devices".
 3. ➔ Öffnen Sie den Webbrowser auf Ihrem Konfigurations-PC.
 4. ➔ Geben Sie im Adressfeld die URL ein wie z.B. https://192.168.1.1
 - ➔ Für die sichere Kommunikation verwendet der Webserver ein selbstsigniertes TLS-Zertifikat, das bei der Inbetriebnahme automatisch auf der Steckkarte generiert wird. Systembedingt erhalten Sie eine Sicherheitsmeldung bzgl. des Zertifikats, da dieses auf dem Konfigurations-PC noch nicht installiert ist. Nach der Anmeldungen können Sie das entsprechende Zertifikat der Steckkarte als vertrauenswürdigen Zertifikat auf Ihrem Konfigurations-PC installieren (siehe unten). Hiermit authentifiziert sich die Steckkarte gegenüber dem Webbrowser auf dem Konfigurations-PC.
 5. ➔ Nehmen Sie die Sicherheitsmeldung zur Kenntnis und fahren Sie nur fort, wenn zwischen Konfigurations-PC und Steckkarte eine gesicherte Verbindung und kein Zugriff Dritter besteht!
 - ➔ Die Anmeldeseite von WBM wird geöffnet.
 6. ➔ Geben Sie Ihre Zugangsdaten an und klicken Sie auf [Anmelden].



- Per Default ist die Benutzerauthentifizierung aktiviert. Im Auslieferungszustand ist der "Admin"-Benutzer bereits mit Administratorrechten angelegt.
- Bitte beachten Sie, dass Sie durch Deaktivierung der Benutzerauthentifizierung die Sicherheit Ihres Systems gegen unerlaubten Zugriff sehr gefährden!
- Das Administrator-Passwort mit der Bezeichnung "PW:" befindet sich auf der Steckkarte. ["Spezifische Informationen \[3\]"...Seite 10](#)
- Verwenden Sie das Administrator-Passwort ausschließlich für die Erstanmeldung am WBM.
- Nachdem Sie sich erfolgreich angemeldet haben, sollten Sie aus Sicherheitsgründen das Administrator-Passwort ändern.

- ➔ Sie haben jetzt Zugriff auf das WBM der Steckkarte mit den Ihnen zugewiesenen Zugriffsrechten.

Zertifikat installieren

**Erstzugriff über TLS-Zertifikat**

- Bei der Erstinbetriebnahme wird während der Startphase auf der Steckkarte ein TLS-Zertifikat erzeugt.
- Das Zertifikat wird für alle Ethernet-Schnittstellen der Steckkarte verwendet und beinhaltet alle IP-Adressen.
- Bei Rücksetzen auf Werkseinstellungen wird automatisch ein neues Zertifikat erzeugt.

Zur Absicherung der Kommunikation sollte im Konfigurations-PC und auf der Steckkarte das gleiche Sicherheits-Zertifikat installiert sein. Ansonsten erhalten Sie eine Warnmeldung. Das generierte Zertifikat übertragen Sie nach folgender Vorgehensweise auf Ihren Konfigurations-PC:

1. Nach der Anmeldung im WBM können Sie über *"Konfiguration → Websdienste"* die Inhalte des automatisch generierten Zertifikats einsehen bzw. anpassen und dieses mit [HTTPS-Zertifikat neu generieren] neu generieren. *"Websdienste"...Seite 51*



Sobald Sie eine der IP-Adressen auf der Steckkarte ändern, müssen Sie über [HTTPS-Zertifikat neu generieren] das Zertifikat neu generieren.

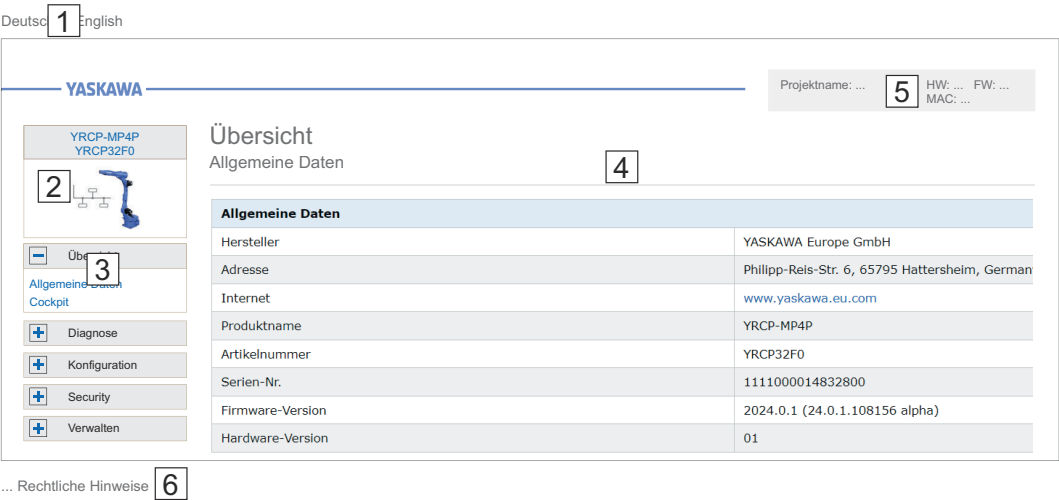
2. Navigieren Sie über *"Security → Zertifikatauthentifizierung"* zu den Zertifikaten.
3. Wechseln Sie in das Register IdentityStore.
 - ➔ Hier haben Sie Zugriff auf das generierten Zertifikat.
4. Laden Sie mit  das gewünschte HTTPS-Zertifikat auf Ihren Konfigurations-PC. Hier können Sie auch ein eigenes schon bestehendes HTTPS-Zertifikat auf die Steckkarte übertragen. *"Zertifikatauthentifizierung"...Seite 54*
5. Installieren Sie das Zertifikat gemäß Ihrem Betriebssystem als vertrauenswürdige Stammzertifizierungsstelle. Kontaktieren Sie hierzu Ihren Systemadministrator.
 - ➔ Nach der Installation erfolgt die Kommunikation zwischen Konfigurations-PC und Steckkarte als *"gesicherte Verbindung"*.

**VORSICHT**

Sollte während des Betriebs die Kommunikation zwischen Konfigurations-PC und Steckkarte als *"nicht sichere Verbindung"* deklariert werden, hat sich entweder das Zertifikat geändert z.B. durch IP Adress-Änderung oder Ihr System wurde durch Dritte kompromittiert! Sorgen Sie immer dafür, dass auf dem Konfigurations-PC entweder das aktuelle Zertifikat der Steckkarte oder, falls vorhanden, ein zugehöriges übergeordnetes Zertifikat installiert ist!

Struktureller Aufbau

Das WBM gliedert sich in folgende Bereiche:

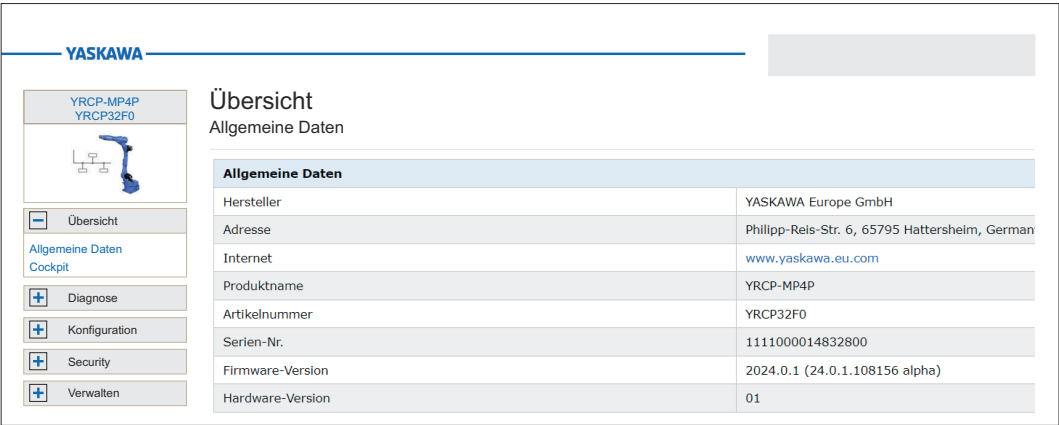


- 1 Sprachumschaltung zwischen "Deutsch" und "Englisch".
- 2 Symbolbild der Robotsteuerung mit Typ- und Bestellbezeichnung.
- 3 Menüspalte für die Navigation.
- 4 Bereich für Informationsausgabe und Eingabe-Dialoge.
- 5 Ausgabe von Projektname (falls vorhanden), aktueller Hardware-/Firmware-Version und MAC-Adresse der Steckkarte.
- 6 Zugriff auf die Yaskawa-Software-Lizenzbedingungen (Software License Terms - SLT) und die Lizenzinformationen zu den einzelnen Linux-Paketen.

6.2 Übersicht

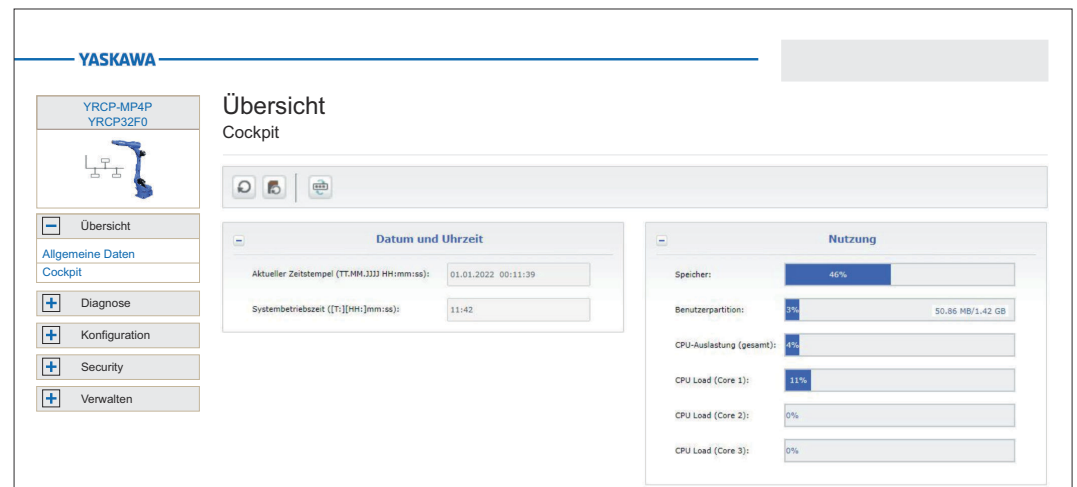
6.2.1 Allgemeine Daten

Hier finden Sie allgemeine Details zur Steckkarte, z.B. Hardware- und Firmware-Versionen, Bestellnummer sowie Herstellerangaben.



6.2.2 Cockpit

Hier finden Sie die Cockpit-Symboleiste und Informationen über Uhrzeit, Status und Auslastung der Steckkarte.



Cockpit-Symboleiste

Die Symbolleiste bietet Zugriff auf folgende Funktionen:

- : Neustart - Führt einen Neustart der Steckkarte durch. Die Operation entspricht einem Aus-/Einschaltvorgang. Die Steckkarte startet mit den zuletzt gespeicherten Einstellungen neu.
- : Reset - Führt auf der Steckkarte "[Rücksetzen auf Werkseinstellung Typ 1](#)"...Seite 28 aus. Hierbei werden alle Kommunikationseinstellungen auf die Standardeinstellungen zurückgesetzt.
- : Passwort ändern - Hiermit können Sie das Passwort des aktuellen Nutzerkontos für den Online-Zugriff auf die Steckkarte ändern.



Bitte beachten Sie, dass durch Rücksetzen auf Werkseinstellung Typ 1 alle Einstellungen der Steckkarte auf Ihre Standardwerte zurückgesetzt werden. Dies betrifft auch alle Einstellungen, welche über das WBM durchgeführt wurden.

Datum und Uhrzeit

Über Aktueller Zeitstempel wird die aktuelle Systemzeit angezeigt. Systembetriebszeit zeigt die aktuelle Laufzeit seit PowerON. Die Einstellung von Datum und Uhrzeit erfolgt über "[Datum und Uhrzeit](#)"...Seite 49.

Nutzung

Hier werden Speicherbelegung und die Last der Steckkarte ausgegeben.

6.3 Diagnose

6.3.1 Benachrichtigungen

Jeder Benutzer mit Zugriffsrechten kann hier Meldeeinträge anzeigen und herunterladen. Die Seite beinhaltet Schaltflächen für Filterfunktionen und für den CSV-Export der Meldungen, sowie eine Übersichtstabelle aller Meldungen und eine Volltextanzeige einer ausgewählten Meldung. Diese Informationen werden einmal pro Sekunde aktualisiert.

YASKAWA

YRCP-MP4P
YRCP32F0

Übersicht

Diagnose

Benachrichtigungen

Profinet

Konfiguration

Security

Verwalten

Diagnose

Benachrichtigungen

Filter

Archivname

<Alle Archive>

Schweregrad

>= Intern

Sender

Maximale Anzahl von Benachrichtigungen

1024

Zeit von

TT.MM.JJJJ

HH:mm:ss

Zeit bis

TT.MM.JJJJ

HH:mm:ss

Filter anwenden

CSV exportieren

Benachrichtigungen

Schweregrad	Zeit	Sender	Name	Benachrichtigung
1	03.01.2022 18:02:23.284	PROFINET Device	Arp.Io.PhD.ResetToFactoryDefaults	This station is reset to factory defaults.
1	03.01.2022 17:51:53.022	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 2, port 2, status Up
1	03.01.2022 17:51:53.022	Device Interface	Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 2, port 2, status: Up
1	03.01.2022 17:51:53.022	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 2, port 1, status Up
1	03.01.2022 17:51:53.022	Device Interface	Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 2, port 1, status: Up
1	03.01.2022 17:51:50.811	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 2, port 2, status Down
1	03.01.2022 17:51:50.811	Device Interface	Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 2, port 2, status: Down
1	03.01.2022 17:51:50.811	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 2, port 1, status Down
1	03.01.2022 17:51:50.811	Device Interface	Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 2, port 1, status: Down
1	03.01.2022 17:51:44.580	Device Interface	Security.Arp.Device.Interface.EthernetLinkStateChan	Link state changed: interface 2, port 1, status Up

Benachrichtigung

Verbindung: Online

Status: Ok

Sortierkriterien für die Meldeeinträge

Standardmäßig werden in der Tabelle die Meldeeinträge in absteigender Reihenfolge basierend auf dem Zeitstempel sortiert. Sie haben die Möglichkeit die einzelnen Spalten als Sortierkriterium zu verwenden, indem Sie auf die entsprechende Spalte klicken. Die Pfeile an den Spaltenüberschriften haben hierbei folgende Bedeutung:

- Doppelpfeil - Die Tabelle wird nicht nach dieser Spalte sortiert.
- Pfeil nach oben - Die Tabelle wird nach dieser Spalte in aufsteigender Reihenfolge sortiert.
- Pfeil nach unten - Die Tabelle wird nach dieser Spalte in absteigender Reihenfolge sortiert.

Volltextanzeige

Unterhalb der Tabelle befindet sich die Volltextanzeige eines gewählten Meldeintrags in der Tabelle. Ist keine Meldung ausgewählt, bleibt die Volltextanzeige leer.

Benachrichtigungen

Schweregrad	Zeit	Sender	Name	Benachrichtigung
1	02.08.2021 15:38:13.659	System Manager	Arp.System.Acf.SystemManager.StateChanged	SystemManager state changed: Running, error=false, warnin...
1	02.08.2021 15:38:13.506	PLC Manager	Arp.Plc.Domain.PlcManager.StateChanged	Plc state changed: Stop (warm) ==> Running
1	02.08.2021 15:38:13.493	Device Interface	Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 1, port 1, status: Up
1	02.08.2021 15:38:13.483	System Manager	Arp.System.Acf.SystemManager.StateChanged	SystemManager state changed: Stop, error=false, warning...
1	02.08.2021 15:38:13.286	PLC Manager	Arp.Plc.Domain.PlcManager.StateChanged	Plc state changed: Ready ==> Stop (warm)
1	02.08.2021 15:38:13.072	System Manager	Arp.System.Acf.SystemManager.StateChanged	SystemManager state changed: Ready, error=false, warnin...
1	02.08.2021 15:38:07.857	System Manager	Arp.System.Acf.SystemManager.StateChanged	SystemManager state changed: None, error=false, warnin...

Benachrichtigung

SystemManager state changed: Running, error=false, warning=false

HB170 | PCIe | YRCP32F0 | de | 25-10

43

Filterfunktionen

Geben Sie die Filtereinstellungen vor. Mit Klick auf [Filter anwenden] werden die zuvor durchgeführten Filtereinstellungen aktiviert und die Tabelle mit den Meldeeinträgen entsprechend aktualisiert.

Sie haben folgende Filtermöglichkeiten:

- Archivname
 - Hier können Sie die Meldeeinträge durch Angabe eines Archivnamens filtern.
- Schweregrad
 - Hier können Sie die Meldeeinträge aufgrund deren Schweregrad eingrenzen.
 - Die Eingrenzung erfolgt nach folgender Staffellung für den minimalsten Schweregrad:
Intern → Information → Warnung → Fehler → Kritische Fehler → Fataler Fehler
 Beispielsweise werden bei *Intern* alle Schweregrade gelistet. Mit der Einstellung *Fehler* werden alle *Fehler*, *Kritische Fehler* und *Fataler Fehler* gelistet.
- Sender
 - Hier können Sie die Meldeeinträge durch Eingabe oder Auswahl eines Absenders im Auswahlfeld eingrenzen.
 - Maßgebend für die Namen im Auswahlfeld ist immer die aktuell dargestellte Liste der Meldeeinträge.
 - Bei Eingabe eines Namens bzw. Teil des Namens werden mit Klick auf [Filter anwenden] Meldungen von Absendern gelistet, welche mit dem gesuchten Namen übereinstimmen bzw. teilweise übereinstimmen.
- Maximale Anzahl von Benachrichtigungen
 - Hier können Sie die Anzahl der anzuzeigenden Meldeeinträge begrenzen.
 - Per Default sind 1024 eingestellt, 4000 sind maximal erlaubt.
- Zeit von, Zeit bis
 - Hier können Sie durch Eingabe von Datum und Uhrzeit den Zeitraum der Meldeeinträge entsprechend eingrenzen.
 - Zeit von: Listet alle Meldeeinträge, welche nicht älter sind als der vorgegebene Zeitpunkt.
 - Zeit bis: Listet alle Meldeeinträge, die älter sind als der vorgegebene Zeitpunkt.
 - Bei Filterung durch Zeitvorgabe ist die Eingabe eines Datums immer erforderlich und kann um eine Uhrzeit ergänzt werden.

6.3.2 PROFINET**Reiter: "Übersicht"**

Hier finden Sie Informationen zur aktuellen PROFINET-Funktion auf der Steckkarte und deren IP-Einstellungen.

YASKAWA

Diagnose Profinet

Übersicht ...

Profinet-Controller

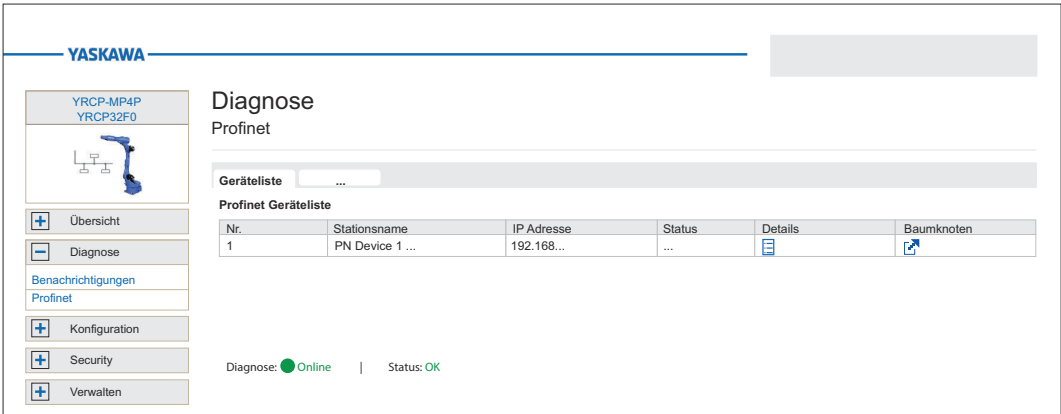
Status	
Profinet-Controller-Funktion	Aktiviert
Profinet-Device-Funktion	Aktiviert

Controller-Details

Gerätetyp	YRCP-MP4P
IP-Adresse	192.168.1.11
Subnetzmaske	255.255.255.0
Standard-Gateway	192.168.1.1
Echtzeitklasse	RT

Diagnose: ● Online | Status: OK

Reiter: "Geräteliste"

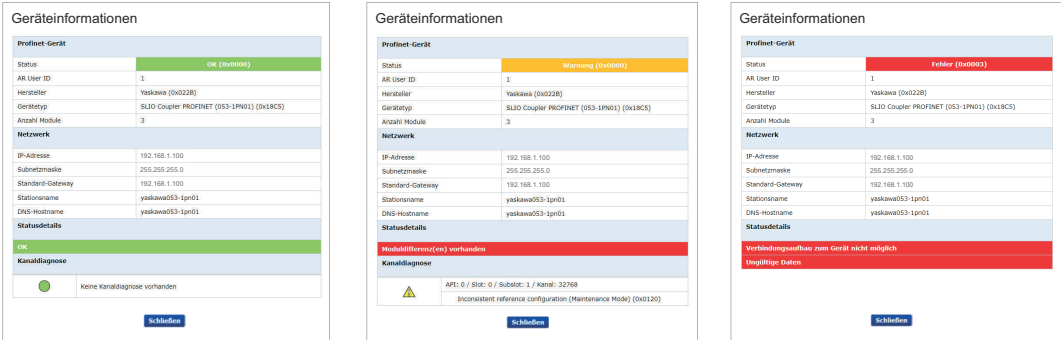


WBM eines PROFINET-Device öffnen

- ➔ Zur Anzeige des WBM eines PROFINET-Device klicken Sie in der Spalte Stationsname auf das entsprechende PROFINET-Gerät.
- ➔ Das WBM des PROFINET-Device wird im Webbrowser in einem neuen Tab geöffnet.

Details öffnen

- Für das entsprechende PROFINET-Device finden Sie unter Details Informationen zu IP-Einstellungen und Diagnose. Diese Informationen werden einmal pro Sekunde aktualisiert.
- ➔ Zur Anzeige der Geräteinformation eines PROFINET-Device klicken Sie in der Spalte Details auf
 - ➔ Die Ansicht Geräteinformation mit den aktuellen Informationen zu IP-Einstellungen und Diagnose wird geöffnet.

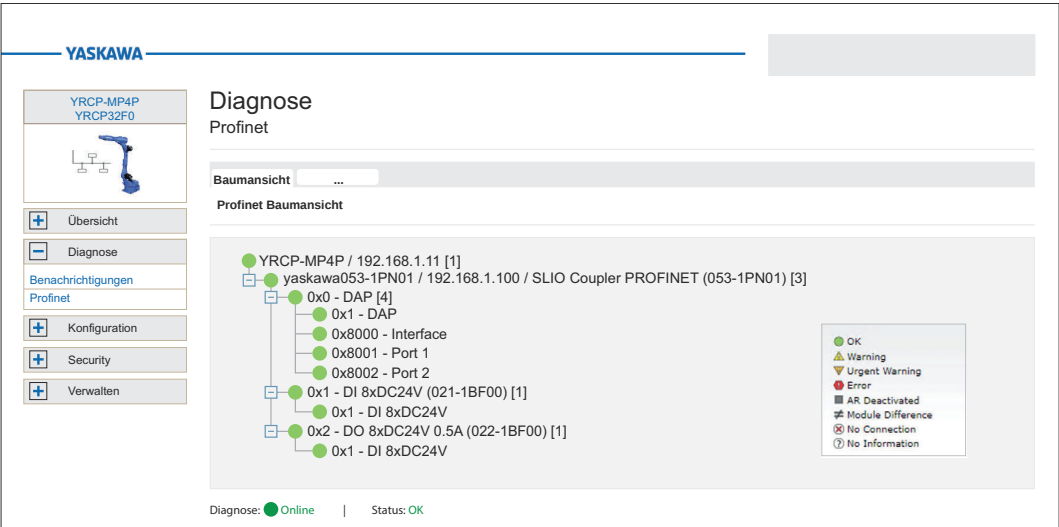


Baumknoten öffnen

- Für das entsprechende PROFINET-Device finden Sie unter Baumknoten die zugehörige Ansicht des Baumknotens. Diese Informationen werden einmal pro Sekunde aktualisiert.
- ➔ Zur Anzeige des Baumknotens eines PROFINET-Device klicken Sie in der Spalte Baumknoten auf
 - ➔ Die Baumansicht des angewählten Device wird geöffnet.

Reiter: "Baumansicht"

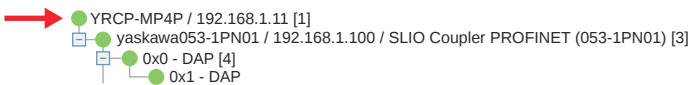
Hier haben Sie eine Baumansicht über alle konfigurierten PROFINET-Devices. Die Übersicht enthält die Gerätenamen der PROFINET-Devices, deren aktuelle IP-Einstellungen sowie den Diagnosezustand der Geräte und Module. Über [+] und [-] können Sie die nächste Ebene der Baumansicht öffnen oder schließen.



Controller-Ebene

Auf der Ebene der PROFINET-IO-Controller finden Sie folgende Informationen:

- Controller-Bezeichnung
- IP-Adresse des Controllers
- Anzahl der PROFINET-Devices



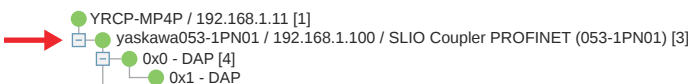
Stations-Ebene

Auf Stations-Ebene finden Sie folgende Informationen zu den PROFINET-Devices:

- Stations-Name
- IP-Adresse der Station
- Stations-Bezeichnung
- Anzahl der angebenen Module

Folgende Symbole informieren über den Diagnosestatus des PROFINET-Device:

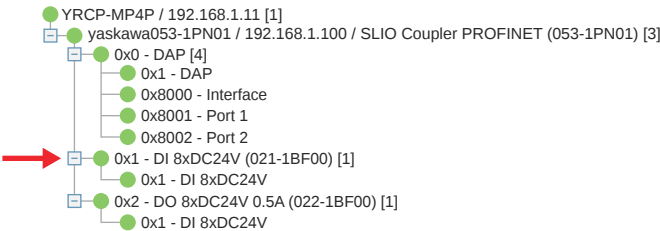
Symbol	Diagnosestatus
	OK
	Warnung
	Fehler



Modul-Ebene

Auf Modul-Ebene finden Sie folgende Informationen:

- Steckplatz-Nr.
- Modul-Bezeichnung
- Anzahl der Submodule



Submodul-Ebene

Auf Submodul-Ebene finden Sie folgende Informationen:

- Submodul-Nr.
- Submodul-Bezeichnung



6.3.2.1 PROFINET Diagnosecode

Hier können Sie den Status einer Verbindung mit einem IO-Controller (Application Relation - AR) bitcodiert anzeigen lassen.

Status AR

Bit	Beschreibung und Handlungsempfehlung
0	Bit 0 ist gesetzt, wenn keine Verbindung besteht. - Der PROFINET-IO-Controller konnte keine Verbindung mit dem PROFINET-Device herstellen oder die AR wurde deaktiviert. - Bitte überprüfen Sie die Ethernet-Verbindung und den PROFINET-Gerätenamen mit Ihrem Projekttool 2CON. - Prüfen Sie außerdem, ob die AR in den Geräteeinstellungen von PROFINET deaktiviert wurde.
1	Bit 1 ist gesetzt, wenn die Daten ungültig sind. - Das PROFINET-Device ist mit dem PROFINET-IO-Controller verbunden, aber die Prozessdaten wurden aufgrund eines Fehlers als ungültig markiert. Die Prozessdaten wurden nicht in das Prozessabbild übertragen. - Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.
2	Bit 2 ist gesetzt, wenn eine Diagnosemeldung ansteht. - Das PROFINET-Device meldet eine Diagnose. - Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.
3	Bit 3 ist gesetzt, wenn das Modul vom konfigurierten Modul abweicht. - Bei der Initialisierung der PROFINET-Verbindung wurde eine Abweichung zwischen Soll- und Istkonfiguration festgestellt. - Bitte überprüfen Sie die Konfiguration des PROFINET-Device. In der Standardeinstellung von 2CON bleibt die Verbindung im Falle eines Konfigurationsunterschieds hergestellt.
4	Bit 4 ist gesetzt, wenn die AR deaktiviert ist. - Das PROFINET-Device ist im Projekt konfiguriert, aber die AR wurde deaktiviert. - Überprüfen Sie die PROFINET-Geräteeinstellungen und aktivieren Sie die AR.

Bit	Beschreibung und Handlungsempfehlung
5	Bit 5 ist gesetzt, wenn keine Nachbarinformationen verfügbar sind. ■ Im verwendeten Netzwerk sind keine Nachbarinformationen verfügbar. – Dies ist in der Regel auf den Einsatz von Komponenten zurückzuführen, die nicht mindestens PROFINET Conformance Class-B (CC-B) kompatibel sind. Für ein stabiles PROFINET-Netzwerk sollten Sie ausschließlich CC-B- bzw. CC-C-konforme PROFINET-Devices verwenden.
6	Bit 6 ist gesetzt, wenn Nachbarinformationen nicht einheitlich sind. ■ Im verwendeten Netzwerk sind Nachbarinformationen verfügbar, aber nicht eindeutig. Das bedeutet, dass mehr als zwei PROFINET-Devices an einem Port von mindestens einem Switch erkannt werden können. Dies ist nicht zulässig und kann dazu führen, dass der automatische Gerätewechsel nicht zuverlässig funktioniert. – Dies ist in der Regel auf die Verwendung von Komponenten zurückzuführen, die nicht mindestens PROFINET Conformance Class-B (CC-B) kompatibel sind (z.B. unmanaged Switches).
7	Bit 7 ist gesetzt, wenn der Aliasname eines gesuchten Geräts bereits von einem AR verwendet wird. ■ Eine DCP-Identifizierungsanforderung (Alias) wurde an das Netzwerk gesendet. Der Aliasname eines gesuchten Geräts wird jedoch bereits von einem AR verwendet. – Diese Information ist nur ein Hinweis darauf, dass das Steuerungsprogramm wahrscheinlich versucht, eine Verbindung mit einem Gerät herzustellen, obwohl eine Verbindung noch aktiv ist.
8	Bit 8 ist gesetzt, wenn ein Wartungsbedarf ansteht. ■ Das PROFINET-Device hat eine Wartungsanfrage (Wartungsalarm) übermittelt. – Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.
9	Bit 9 ist gesetzt, wenn eine hochpriorie Wartungsanforderung ansteht. ■ Das PROFINET-Device hat eine hochpriorie Wartungsanfrage (Wartungsalarm) übermittelt. – Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.
10	Bit 10 ist gesetzt wenn eine hersteller- bzw. kanalspezifische Diagnose ansteht. ■ Das PROFINET-Device hat eine hersteller- bzw. kanalspezifische Diagnose übermittelt. – Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.

6.4 Konfiguration

6.4.1 Netzwerk

Benutzer mit Leseberechtigung

Hier können Sie die Ethernet-Einstellungen der Steckkarte anzeigen.

YRCF-MP4P
YRCF32F0

Übersicht

Diagnose

Konfiguration

Netzwerk

Datum und Uhrzeit

Webdienste

Security

Verwalten

Konfiguration

Netzwerk

LAN-Schnittstelle

LAN 1 (X1/X2)	Status	Konfiguration
IP-Adresse	192.168.3.1	192.168.3.1
Subnetzmaske	255.255.255.0	255.255.255.0
Standard-Gateway	0.0.0.0	0.0.0.0
DNS-Serveradressen	8.8.8.8	8.8.8.8
	8.8.4.4	8.8.4.4
MAC-Adresse	00:20:B5:2E:CE:7E	00:20:B5:2E:CE:7E
Port X1		
Datenrate		
Duplexmodus		
Link-Status	Link Down	

Benutzer mit Schreibberechtigung

Wenn Sie mit Administratorrechten angemeldet sind, können Sie hier die Ethernet-Einstellungen Ihrer Steckkarte anzeigen. Zusätzlich können Sie in der Spalte "Konfiguration" die aktuellen Netzwerkeinstellungen ändern.

YASKAWA

YRCP-MP4P
YRCP32F0

Konfiguration
Netzwerk

LAN-Schnittstelle ...

LAN 1 (X1/X2)	Status	Konfiguration
IP-Adresse	192.168.3.1	192.168.3.1
Subnetzmaske	255.255.255.0	255.255.255.0
Standard-Gateway	0.0.0.0	0.0.0.0
DNS-Serveradressen	8.8.8.8	8.8.8.8
	8.8.4.4	8.8.4.4
MAC-Adresse	00:20:B5:2E:CE:7E	

Port X1

Datenrate

Duplexmodus

Link-Status

Zur Änderung der Netzwerkeinstellungen gehen Sie wie folgt vor:

1. Geben Sie in der Spalte "Konfiguration" Ihre neuen Einstellungen ein.
2. Klicken Sie auf [Anwenden und neu starten].
 - ➔ Die Einstellungen werden übernommen, an die Steckkarte übertragen und zur Aktivierung die Steckkarte automatisch neu gestartet.



Sie können die Netzwerkeinstellungen auch über 2CON konfigurieren. Näheres hierzu finden Sie in der zugehörigen Onlinehilfe.

6.4.2 Datum und Uhrzeit

Die Seite Datum und Uhrzeit bietet Zugriff auf die NTP-Client-Konfiguration. NTP steht für **N**etwork **T**ime **P**rotocol und ist ein in RFC 958 beschriebener Standard zur Uhrzeit-Synchronisation in über Netzwerk bzw. Internet verbundenen Endgeräten. NTP baut auf dem verbindungslosen UDP-Protokoll auf (Port 123). Zur Synchronisation setzt NTP auf die Coordinated Universal Time (UTC) auf, welche von den einzelnen Clients und Servern in einem hierarchischen System bezogen wird.



Die Steckkarte verwendet als Default-Einstellung UTC0, welche der koordinierten Weltzeit UTC $\pm 00:00$ entspricht.

Hier können Sie den NTP-Client konfigurieren, indem Sie neue NTP-Servereinträge hinzufügen.

1. Klicken Sie hierzu unterhalb der Tabelle auf

➔ Das Dialogfenster zum Hinzufügen eines NTP-Servers wird geöffnet.

2. Passen Sie die entsprechenden Parameter an.

- Server-Hostname
 - Geben Sie die IP-Adresse an, unter welcher der NTP-Server im Netzwerk zu erreichen ist.
- Min. Aktualisierungszeit und Max. Aktualisierungszeit
 - Geben Sie hier den Bereich an, innerhalb dessen die Zeit mit dem NTP-Server synchronisiert werden soll mit dem Ziel mit möglichst geringer Netzlast eine hohe Genauigkeit zu erreichen. Die voreingestellten Werte sind Standardwerte.
- Kommentar
 - Hier können Sie für den NTP-Server eine interne Bezeichnung vergeben.

3. Klicken Sie auf [OK].

➔ Der Dialog wird geschlossen und der NTP-Server in der Tabelle aufgeführt.
Mit können Sie Einträge entfernen und mit bearbeiten.

4. Klicken Sie auf [Anwenden].

➔ Hierbei erhalten Sie einen Hinweis, dass das Anwenden der neuen NTP-Daemon-Konfiguration einen Neustart des NTP-Daemons erfordert und dies zur Verletzung der Echtzeit führen kann. Mit [OK] werden die in der Tabelle aufgeführten NTP-Server zur Uhrzeitsynchronisation übernommen und der NTP-Daemon wird neu gestartet.

6.4.3 Webdienste

Die Seite bietet Zugriff auf die Konfiguration von Web Services, z.B. HTTPS-Zertifikat, das für den NGINX-Webserver verwendet wird.



Das HTTPS-Zertifikat und der zugehörige private Schlüssel befinden sich als Dateien im Dateisystem der Steckkarte und werden als symbolische Links auf der Webseite aufgeführt. Bei einem Firmware-Update werden die vorhandenen Zertifikats- und Schlüsseldateien in ein Backup-Verzeichnis verschoben und symbolische Links erstellt, die auf diese Sicherung verweisen.

6.4.3.1 NGINX Webserver

TLS-Konfiguration

TLS (Transport Layer Security) ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet zwischen Benutzer und Webseite. Der Einsatz in der NGINX-Konfiguration erfolgt nach folgender Vorgehensweise:

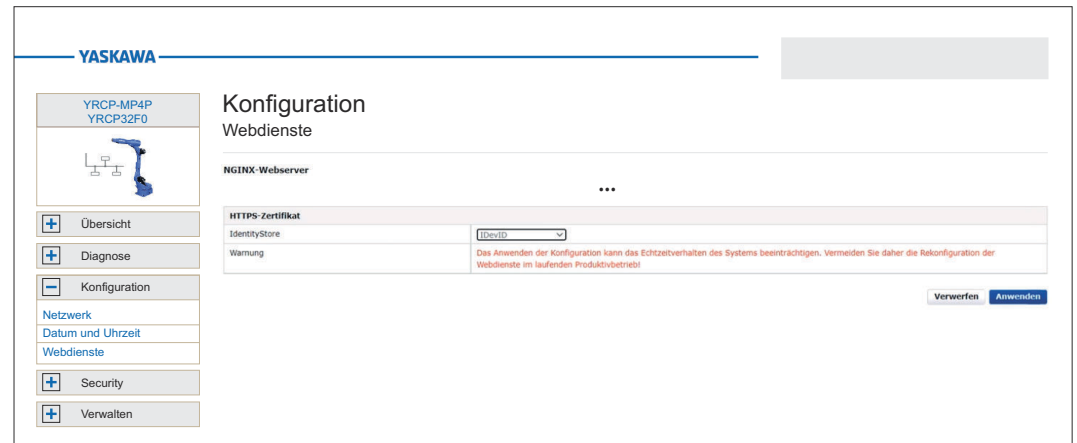
1. ➔ Aktivieren Sie "TLSv1.3". Aktivieren Sie immer eine und immer die aktuellste TLS-Version.
2. ➔ Wählen Sie unter "Cipher suits" eine vordefinierte Verschlüsselungssammlung aus.
3. ➔ Klicken Sie auf [Anwenden].
 - ➔ TLS wird für die Authentifizierung in der Konfiguration verwendet.



Bitte beachten Sie, dass durch eine Rekonfiguration des Web-Services das Echtzeitverhalten Ihres Systems beeinflusst werden kann. Vermeiden Sie dies während des Produktivbetriebs.

Ausgewähltes HTTPS-Zertifikat

Das HTTPS-Zertifikat dient zur Authentifizierung der Steckkarte gegenüber dem Webserver.



In der Konfigurationstabelle für den NGINX Webserver haben Sie die Möglichkeit, das HTTPS-Zertifikat aus einem der auf der Steckkarte hinterlegten Identity Stores auszuwählen.

1. ➔ Wählen Sie den entsprechenden Identity Store.
 - ➔ Das entsprechende HTTPS-Zertifikat wird ausgewählt.
2. ➔ Klicken Sie auf [Anwenden].
 - ➔ Das Zertifikat wird für die Authentifizierung in der Konfiguration verwendet.



Bitte beachten Sie, dass durch eine Rekonfiguration des Web-Services das Echtzeitverhalten Ihres Systems beeinflusst werden kann. Vermeiden Sie dies während des Produktivbetriebs.

Selbst-signiertes HTTPS-Zertifikat

Neben den auf der Steckkarte gespeicherten HTTPS-Zertifikaten haben Sie auch die Möglichkeit, ein von der Firmware erstelltes selbstsigniertes Zertifikat auszuwählen.

1. Wählen Sie hierzu im Auswahlfeld "HTTPS-self-signed".

- Die Konfiguration des selbst-signierten HTTPS-Zertifikats wird tabellarisch aufgeführt. Dieses können Sie entsprechend anpassen und mit [Anwenden] neue Zertifikatsdateien generieren.

2. Passen Sie die entsprechenden Parameter an.

- Distinguished Name**
 - Tragen Sie hier zur Identifikation Ihre Firmeninformationen ein.
- Gültigkeit**
 - Geben Sie hier Datum im Format TT.MM.JJJJ und Uhrzeit in hh:mm:ss an.
 - Ist bei "Gültig ab" das Eingabefeld leer, wird das aktuelle Datum verwendet.
 - Ist bei "Gültig bis" das Eingabefeld leer, wird das Datum 31.12.9999 und die Uhrzeit 23:59:59 verwendet.
- Subjektalternativname**
 - Die IP-Adressen aus der Netzwerkkonfiguration der Steckkarte werden standardmäßig vorgeschlagen.
 - Sie haben die Möglichkeit, diese zu erweitern, anzupassen oder einen DNS-Namen vorzugeben. Mit + fügen Sie einen Eintrag hinzu. Mit X können Sie einen Eintrag entfernen.



Soll der Webserver über verschiedene IP-Adressen ohne Fehlermeldung erreichbar sein, müssen Sie alle IP-Adressen als Subjektalternativname vom Typ IP-Adresse angeben. Ist die Steckkarte über DNS-Namen erreichbar, müssen Sie auch diese angeben!

3. Damit die Änderungen übernommen werden, klicken Sie auf [HTTPS-Zertifikat neu generieren].

- Das Zertifikat wird neu erzeugt. Hierbei wird ein bestehendes selbst-signiertes HTTPS-Zertifikat überschrieben.

4. Klicken Sie auf [Anwenden].

- ➔ Das Zertifikat wird für die Authentifizierung in der NGINX-Konfiguration verwendet.



Bitte beachten Sie, dass durch eine Rekonfiguration des Web-Services das Echtzeitverhalten Ihres Systems beeinflusst werden kann. Vermeiden Sie dies während des Produktivbetriebs.

6.5 Security

Die sicherheitsrelevanten Einstellungen für die Steckkarte sind im Bereich "Security" des WBM zu konfigurieren.

6.5.1 Zertifikatauthentifizierung

Unter "Zertifikatauthentifizierung" können Sie Ihre Zertifikate für die sichere Kommunikation mit der Steckkarte verwalten. Die "Zertifikatauthentifizierung" teilt sich in folgende Register:

- TrustStores
 - Hier werden vertrauenswürdige Zertifikate und Sperrlisten möglicher Kommunikationspartner gespeichert.
- IdentityStores
 - Hier werden die persönlich erstellten Zertifikate gespeichert.



- Der Name für jeden Store kann mit den Schnittstellen für die TLS-Kommunikation verwendet werden.
- Bei den Namen der Stores wird zwischen Groß- und Kleinschreibung unterschieden.

Register: TrustStores

Jeder TrustStore wird im WBM durch zwei Tabellen definiert:

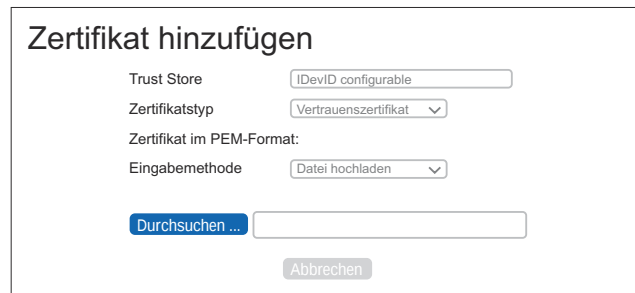
- Tabelle *"Zertifikate"*
 - In dieser Tabelle können Sie vertrauenswürdige Zertifikate und Ausstellerzertifikate verwalten.
- Tabelle *"Sperrlisten"*
 - In dieser Tabelle können Sie die Sperrlisten für den entsprechenden TrustStore verwalten. Indem Sie hier nicht vertrauenswürdige Zertifikate und Ausstellerzertifikate hinterlegen.

TrustStore erstellen

1. ➔ Zum Erstellen eines TrustStore klicken Sie am Ende der Tabelle auf die Schaltfläche .
- ➔ Es öffnet sich der Eingabe-Dialog zur Eingabe eines Namens für den TrustStore.
2. ➔ Geben Sie einen Namen an.
3. ➔ Klicken Sie auf [Hinzufügen].
- ➔ Der Dialog wird geschlossen und der neue TrustStore hinzugefügt.
- Mit  können Sie diesen wieder entfernen und mit  umbenennen.

Zertifikat hinzufügen

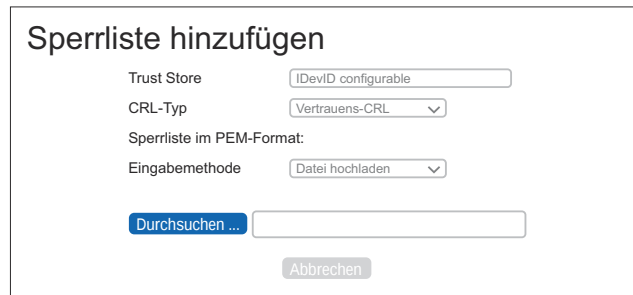
1. ➔ Mit  unterhalb der Tabelle *"Zertifikate"* können Sie über den Dialog ein Zertifikat hinzufügen.



- ➔ ■ TrustStore
 - Name des TrustStore.
 - Zertifikatstyp
 - Geben Sie hier an, ob es sich um ein vertrauenswürdiges bzw. nicht vertrauenswürdige Zertifikat handelt.
 - Zertifikat im PEM-Format
 - Zertifikat-Dateien können ausschließlich im PEM-Format verarbeitet werden.
 - Eingabemethode
 - Hier können Sie angeben, in welcher Form das Zertifikat hinzugefügt werden soll.
 - Sie haben die Auswahl zwischen Text und Datei (PEM-Format).
2. ➔ Zum Hinzufügen eines Zertifikats in Textform wählen Sie unter *"Eingabemethode"* den Parameter *"Textinhalt einfügen"* aus, geben den Text in das Eingabefeld ein und klicken Sie auf [Hinzufügen].
 - ➔ Der Eingabe-Dialog wird geschlossen und das Zertifikat in Textform hinzugefügt.
 3. ➔ Zum Hinzufügen eines Zertifikats in Dateiform wählen Sie unter *"Eingabemethode"* den Parameter *"Datei hochladen"* aus, navigieren Sie über [Durchsuchen...] zu Ihrem Zertifikat im PEM-Format und klicken Sie auf [Hinzufügen].
 - ➔ Der Eingabe-Dialog wird geschlossen und das Zertifikat als PEM-Datei hinzugefügt.

Sperrliste hinzufügen

→ Mit  unterhalb der Tabelle *"Sperrlisten"* können Sie über den Dialog eine Sperrliste hinzufügen.



- ➔ ■ TrustStore
 - Name des TrustStore.
- CRL-Typ
 - Geben Sie hier an, ob es sich um eine vertrauenswürdige bzw. nicht vertrauenswürdige Sperrliste handelt.
- Sperrliste im PEM-Format
 - Sperrlisten-Dateien können ausschließlich im PEM-Format verarbeitet werden.
- Eingabemethode
 - Hier können Sie angeben, in welcher Form die Sperrliste hinzugefügt werden soll.
 - Sie haben die Auswahl zwischen Text und Datei (PEM-Format).

Löschen von Zertifikaten und Sperrlisten

1. → Zum Löschen eines Zertifikats oder einer Sperrliste klicken Sie auf die Schaltfläche  des jeweiligen Zertifikats oder der Sperrliste.
2. → Klicken Sie im Abfrage-Dialog auf *"Entfernen"*.

Detailansicht

Die Detailansichten bieten detaillierte Informationen zu jedem Zertifikat und jeder Sperrliste:

1. → Zum Öffnen der Detailansicht klicken Sie auf .
 - ➔ Die Detailansicht wird geöffnet.
2. → Mit [Schließen] wird diese wieder geschlossen.

Register: IdentityStores

- Im Register "IdentityStores" können Sie mehrere Identity Stores erstellen und verwalten.
- Jeder IdentityStore enthält in der Regel ein RSA-Schlüsselpaar und das entsprechende Schlüsselzertifikat.
- Optional können Sie einem Identity Store weitere Ausstellerzertifikate hinzufügen.
- Der IDevID Identity Store ist Teil des Systems und wird mit der Steckkarte geliefert.

IdentityStore hinzufügen

1. Mit **+** unterhalb der Tabelle "IdentityStore" können Sie über den Dialog einen IdentityStore hinzufügen.

- ➔ ■ **Name**
 - Name für den IdentityStore.
 - **Schlüsselpaar**
 - Geben Sie hier an, wie das Schlüsselpaar hinzugefügt werden soll.
 - Das Schlüsselpaar können Sie eingeben oder generieren lassen.
 - **Schlüsselpaar im PEM-Format**
 - Schlüssel-Dateien können ausschließlich im PEM-Format verarbeitet werden.
 - **Eingabemethode**
 - Hier können Sie angeben, in welcher Form das Schlüsselpaar hinzugefügt werden soll.
 - Sie haben die Auswahl zwischen Text und Datei (PEM-Format).
2. Zum Hinzufügen eines Schlüsselpaars in Textform wählen Sie unter "Schlüsselpaar" den Parameter "Eingeben" und unter "Eingabemethode" den Parameter "Textinhalt einfügen" aus, geben den Text in das Eingabefeld ein und klicken Sie auf [Hinzufügen].
 - ➔ Der Eingabe-Dialog wird geschlossen und das Schlüsselpaar in Textform hinzugefügt.

3. ➔ Zum Hinzufügen eines Schlüsselpaars in Dateiform wählen Sie unter "**Schlüsselpaar**" den Parameter "**Eingeben**" und unter "**Eingabemethode**" den Parameter "**Datei hochladen**" aus, navigieren Sie über [Durchsuchen...] zu Ihrer Schlüsselpaar-Datei im PEM-Format und klicken Sie auf [Hinzufügen].
 - ➔ Der Eingabe-Dialog wird geschlossen und das Schlüsselpaar als PEM-Datei hinzugefügt.
4. ➔ Zum Hinzufügen eines auf der Steckkarte generierten Schlüsselpaars wählen Sie unter "**Schlüsselpaar**" den Parameter "**Generieren**" aus, wählen Sie unter "**Schlüsseltyp**" die Verschlüsselungsmethode aus und klicken Sie auf [Hinzufügen].
 - ➔ Der Eingabe-Dialog wird geschlossen und das automatisch auf der Steckkarte generierte Schlüsselpaar hinzugefügt.

Sie können Schlüsselpaare bzw. Zertifikate hinzufügen, umbenennen, festlegen und entfernen, indem Sie folgende Schaltflächen im entsprechenden Tabelleneintrag verwenden:

- : Neues Element - Fügt ein neues Schlüsselpaar bzw. Zertifikat hinzu.
- : Element löschen - Löscht mit Klick auf "**Entfernen**" das ausgewählte Schlüsselpaar bzw. Zertifikat oder wenn ausgewählt den IdentityStore.
- : Details - Zeigt die Detailansicht des entsprechenden Elements.
- : Herunterladen - Sie können den Inhalt des öffentlichen Schlüssels eines Schlüsselpaars als PEM-Datei herunterladen.
 - Sofern ein Schlüsselzertifikat verfügbar ist, können Sie dies als CRT-Datei herunterladen.
 - Speichern Sie die Datei in einem Verzeichnis Ihrer Wahl oder öffnen Sie die Datei direkt mit einem geeigneten Tool.
- : Umbenennen - Abhängig von der Position innerhalb einer Tabelle, können Sie hiermit das entsprechende Element umbenennen.

6.5.2 Firewall

Die Steckkarte wird mit einer voreingestellten Firewall ausgeliefert. Hierbei kommt die Linux® Firewall "**nftables**" zum Einsatz. Sie können wie nachfolgend beschrieben, Regeln aus vordefinierten Grundregeln erstellen oder eigene Regeln neu erzeugen.



- *Im Auslieferungszustand ist die Firewall deaktiviert!*
- *Bitte beachten Sie, dass Sie ausschließlich als Administrator Zugriff auf die Firewall-Einstellungen haben!*

Zugriff auf die Firewall

1. ➔ Melden Sie sich als Administrator am WBM an.
2. ➔ Navigieren Sie zu "**Security → Firewall**".
 - ➔ Die Konfigurationsseite für die Firewall wird geöffnet.

YASKAWA

YRCP-MP4P
YRCP32F0

Security
Firewall

Systemnachricht
Konfigurationsstatus = OK

Systemstatus
Liste der aktiven Firewall-Regeln [Regeln anzeigen](#)

Generelle Einstellungen
Status: (Aktuell: gestoppt)
Aktivierung: ☐
Aktiviert: Die Firewall wird dauerhaft gestartet. Nach einem Systemneustart ist diese aktiv.
Deaktiviert: Die Firewall wird dauerhaft gestoppt. Nach einem Systemneustart ist diese inaktiv.

Basis-Konfigurationen Benutzer-Konfigurationen

ICMP-Einstellungen
Eingehende ICMP-Anfragen zulassen: ☒ Wenn deaktiviert: Der Controller ist über einen Ping-Befehl nicht erreichbar.
Ausgehende ICMP-Anfragen zulassen: ☒ Wenn deaktiviert: Vom Controller aus können keine Ping-Befehle abgesetzt werden.

Basisregeln

Seq.	Richtung	Protokoll	Nach Port	Kommentar	Aktion
1	Eingang	UDP	123	NTP (Network Time Protocol)	Annehmen
2	Eingang	TCP	41100	Remoting (z.B. iCube Engineer)	Annehmen
3	Eingang	TCP	22	SSH	Annehmen
4	Eingang	TCP	80	HTTP	Annehmen
5	Eingang	TCP	443	HTTPS	Annehmen
6	Eingang	TCP	4840	OPC UA	Annehmen

[Verwerfen](#) [Anwenden](#)

[Anwenden] und [Verwerfen]

- Mit der Schaltfläche [Anwenden] werden die geänderten Firewall-Einstellungen auf die Steckkarte übertragen.
- Mit der Schaltfläche [Verwerfen] werden nach einer Sicherheitsabfrage die getätigten Einstellungen verworfen und die WBM-Seite wird neu geladen.

"Systemnachricht"

Unter "Systemnachricht" werden Meldungen bezüglich der Übertragung von Firewall-Einstellungen an die Steckkarte angezeigt. Hierbei können folgende Systemmeldungen auftreten:

- Konfigurationsstatus = OK
 - Die konfigurierten Firewall-Einstellungen wurden erfolgreich auf die Steckkarte übertragen.
- Warnung
 - Die Steckkarte meldet eine Warnung, z.B. wenn eine oder mehrere zusätzliche Filterkonfigurationen im System vorhanden sind. Die Warnung enthält die Bezeichnungen aller zusätzlich geladenen Filtertabellen.
- Fehler
 - Mindestens eine Firewall-Konfiguration ist fehlerhaft.

"Systemstatus"

- Bei aktivierter Firewall können Sie über die Schaltfläche [Regeln anzeigen] eine Übersicht aller aktivierten Firewall-Regeln als txt-Datei anzeigen lassen.
- Mit [Datei speichern] können Sie die Datei lokal auf Ihrem PC als txt-Datei speichern.

"Generelle Einstellungen"

Unter *"Generelle Einstellungen"* können Sie den aktuellen Firewall-Status einsehen und diesen temporär oder dauerhaft einstellen.

Temporäre Aktivierung

1. ➤ Wählen Sie unter *"Status"* den Eintrag *"Starten"* oder *"Neu starten"* aus.
2. ➤ Klicken Sie auf [Anwenden].
 - ➔ Die Firewall wird aktiviert. Nach einem Neustart der Steckkarte ist die Firewall wieder deaktiviert.

Temporäre Deaktivierung

1. ➤ Wählen Sie unter *"Status"* den Eintrag *"Stoppen"* aus.
2. ➤ Klicken Sie auf [Anwenden].
 - ➔ Die Firewall wird deaktiviert. Nach einem Neustart der Steckkarte ist die Firewall wieder aktiviert.

Dauerhafte Aktivierung

1. ➤ Aktivieren Sie das Auswahlfeld *"Aktivierung"*.
2. ➤ Klicken Sie auf [Anwenden].
 - ➔ Die Firewall wird aktiviert und bleibt auch nach einem Neustart aktiviert.

Dauerhafte Deaktivierung

1. ➤ Deaktivieren Sie das Auswahlfeld *"Aktivierung"*.
2. ➤ Klicken Sie auf [Anwenden].
 - ➔ Die Firewall wird deaktiviert und bleibt auch nach einem Neustart deaktiviert.



Durch Deaktivierung der Firewall gefährden Sie die Sicherheit Ihrer Anlage, insbesondere wenn diese über das Internet erreicht werden kann! Die Firewall sollte nur temporär zu Testzwecken deaktiviert werden wie z.B. bei der Fehlersuche.

Konfiguration

Die Konfiguration der Firewall-Regeln teilt sich in folgende Register:

- Basis-Konfigurationen
 - Hier finden Sie vordefinierte Firewall-Regeln, welche Sie aktivieren bzw. deaktivieren können.
- Benutzer-Konfigurationen
 - Hier können Sie eigene Firewall-Regeln nach definierten Vorgaben erstellen, aktivieren bzw. deaktivieren.

In beiden Registern gibt es die Spalte *"Aktion"*. Mit der Schaltfläche [Anwenden] werden die Firewall-Einstellungen übernommen. Für die Spalte *"Aktion"* haben Sie folgende Einstellungsmöglichkeiten:

- Annehmen
 - Die entsprechende Verbindung und Verbindungsanforderung wird akzeptiert.
 - Die entsprechende Verbindung kann hergestellt werden.
- Verwerfen
 - Die entsprechende Verbindung wird unterbrochen.
 - Es gibt keine Antwort auf die entsprechende Anfrage.
 - Das entsprechende Paket wird verworfen.
- Abweisen
 - Die entsprechende Verbindung wird abgelehnt.
 - Der Absender erhält eine Antwort auf die entsprechende Anfrage.
- Überspringen
 - Die Regel wird nicht ausgeführt.
 - Hiermit können Sie z.B. eine Regel in der *"Basis-Konfigurationen"* überspringen und stattdessen eine Regel in der *"Benutzer-Konfigurationen"* erstellen und dort aktivieren.

Register: Basis-Konfigurationen**"ICMP-Einstellungen"**

- **"Eingehende ICMP-Anfragen zulassen"**
 - aktiviert: Eingehende ICMP-Echoanforderungen werden akzeptiert. Die Steckkarte kann mit einer Ping-Anforderung erreicht werden.
 - deaktiviert: Eingehende ICMP-Echoanforderungen werden blockiert. Die Steckkarte kann nicht mit einer Ping-Anforderung erreicht werden.
- **"Ausgehende ICMP-Anfragen zulassen"**
 - aktiviert: Ausgehende ICMP-Echoanforderungen werden akzeptiert. Ping-Anforderungen von der Steckkarte werden übermittelt.
 - deaktiviert: Ausgehende ICMP-Echoanforderungen werden blockiert. Ping-Anforderungen von der Steckkarte werden blockiert.

"Basisregeln"

- Hier finden Sie vordefinierte Firewall-Regeln für die entsprechend eingehenden Verbindungen. Deren Anwendung können Sie über **"Aktion"** entsprechend steuern.
- Die Einstellungen sind für alle Ethernet-Schnittstellen gültig. Zur individuellen Anpassung können Sie stattdessen eine Regel in der **"Benutzer-Konfigurationen"** erstellen und dort aktivieren.

**Sperren des WBM-Zugangs**

- Der Zugriff auf das WBM erfolgt bei der Steckkarte über TCP-Port 443.
- Durch Blockieren dieses Ports bei dauerhaft aktivierter Firewall, haben Sie auch nach einem Neustart keinen Zugriff mehr auf das WBM der Steckkarte.
- Durch Rücksetzen auf Werkseinstellung wird unter anderem auch die Firewall auf ihre Defaulteinstellungen zurückgesetzt. Auf diese Weise bekommen Sie wieder Zugriff auf das WBM der Steckkarte mit den ursprünglichen Zugangsdaten.

Register: Benutzer-Konfigurationen

- Zusätzlich oder alternativ zu den **"Basisregeln"** können Sie hier eigene benutzerspezifische Firewall-Regeln für verschiedene Filterkategorien definieren und aktivieren.
- Firewall-Regeln für die Ausgabe legen Sie im Register **"Ausgangsregeln"** an.
- Firewall-Regeln für die Eingabe legen Sie im Register **"Eingangsregeln"** an.
- Mit der Reihenfolge der Firewall-Regeln in der Tabelle bestimmen Sie die Priorität für die Anwendung dieser.
- Sie können neue Regeln erstellen, Regeln löschen oder die Reihenfolge der Regeln ändern, indem Sie folgende Schaltflächen am Ende der Tabelle verwenden:
 - : Neue Regel - Fügt eine neue Firewall-Regel hinzu.
 - : Regel löschen - Löscht die ausgewählte Firewall-Regel.
 - : Regel nach oben - Die Regel wird nach oben verschoben.
 - : Regel nach unten - Die Regel wird nach unten verschoben.
- Mit der Schaltfläche [Anwenden] werden die Firewall-Regeln übernommen und aktiviert. Eine bereits vorhandene Konfiguration wird hierbei überschrieben.

Neben **"Aktion"** gibt es noch folgende Parameter zur Vorgabe einer Firewall-Regel:

- **"Seq."**
 - Nummeriert die Reihenfolge für die Priorität, nach der die Firewall-Regeln angewendet werden.
 - Die Regeln werden von 1 aufsteigend angewendet.
 - Mit und können Sie die Firewall-Regeln entsprechend verschieben.

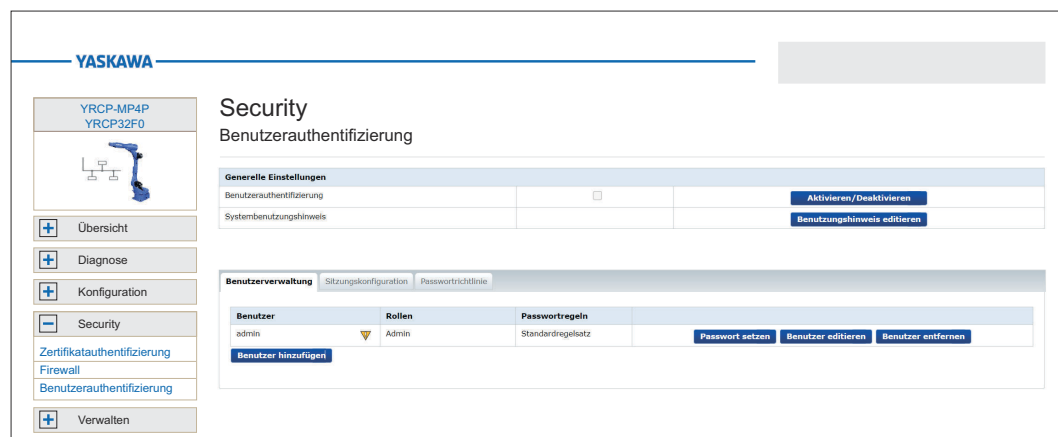
- **"Schnittstelle"**
 - Im Reiter *"Eingangsregeln"* können Sie aus einer Auswahlliste eine einzelne Schnittstelle auswählen, für welche die Regel angewendet werden soll.
 - Im Reiter *"Ausgangsregeln"* haben Sie keine Auswahlmöglichkeit. Hier gilt die Regel für alle Schnittstellen.
- **"Protokoll"**
 - Geben Sie das Protokoll an, für welches die Regel angewendet werden soll.
- **"Von IP"**
 - Geben Sie die IP-Adresse für Verbindungen an, die von dieser Adresse empfangen werden.
- **"Von Port"**
 - Geben Sie den Port für Verbindungen an, die über diesen Port empfangen werden.
 - Sie können alle Ports, ausgewählte Ports oder einen Wertebereich angeben.
- **"Nach IP"**
 - Geben Sie die IP-Adresse für Verbindungen an, die an diese Adresse gesendet werden.
- **"Nach Port"**
 - Geben Sie den Port für Verbindungen an, die über diesen Port gesendet werden.
 - Sie können alle Ports, ausgewählte Ports oder einen Wertebereich angeben.
- **"Kommentar"**
 - Hier können Sie Ihre Filterregel entsprechend kommentieren.

6.5.3 Benutzerauthentifizierung

- Unter *"Benutzerauthentifizierung"* können Sie die Benutzerauthentifizierung aktivieren bzw. deaktivieren.
- Bei aktivierter Benutzerauthentifizierung haben Sie ausschließlich durch Angabe von Benutzername und Kennwort Zugriff auf definierbare Komponenten der Steckkarte und Funktionen in 2CON.
- Bei deaktivierter Benutzerauthentifizierung erfolgt der Zugriff ohne Benutzer-Abfrage. Die Bereiche für den Administrator bleiben weiterhin durch Passwort geschützt.



- *Per Default ist die Benutzerauthentifizierung aktiviert. Im Auslieferungszustand ist der "Admin"-Benutzer bereits mit Administratorrechten angelegt.*
- *Bitte beachten Sie, dass Sie durch Deaktivierung der Benutzerauthentifizierung die Sicherheit Ihres Systems gegen unerlaubten Zugriff sehr gefährden!*
- *Das Administrator-Passwort mit der Bezeichnung "PW:" befindet sich auf der Steckkarte. ["Spezifische Informationen \[3\]"...Seite 10](#)*
- *Verwenden Sie das Administrator-Passwort ausschließlich für die Erstanmeldung am WBM.*
- *Nachdem Sie sich erfolgreich angemeldet haben, sollten Sie aus Sicherheitsgründen das Administrator-Passwort ändern.*



Benutzerauthentifizierung aktivieren/deaktivieren

1. Klicken Sie auf die Schaltfläche [Aktivieren/Deaktivieren] neben Benutzerauthentifizierung.
 - ➔ Das Dialogfenster für die Benutzerauthentifizierung wird geöffnet.
2. Hier können Sie über das Kontrollfeld durch Anwahl bzw. Abwahl die Benutzerauthentifizierung aktivieren bzw. deaktivieren.
3. Mit [Speichern] werden die Änderungen übernommen und der Dialog wird geschlossen.

Systembenutzungshinweis ändern

Bei jeder Anmeldung an der Steckkarte über WBM oder 2CON, erfolgt die Anzeige des Systembenutzungshinweis. Zur individuellen Anpassung können Sie diesen Text bearbeiten. Die Anzeige erfolgt unabhängig von der verwendeten Sprache der Benutzeroberfläche. Sie sollten daher bei der Bearbeitung alle erforderlichen Sprachen berücksichtigen.

1. Zur Bearbeitung klicken Sie auf [Benutzungshinweis editieren] neben Systembenutzungshinweis.
 - ➔ Das Dialogfenster zur Bearbeitung des Textes wird geöffnet.
2. Passen Sie entsprechend Ihren Text an.
3. Mit [Speichern] werden die Änderungen übernommen und der Dialog wird geschlossen.

Benutzerverwaltung

Über die Benutzerauthentifizierung werden die Zugangsdaten aller Benutzer, die berechtigt sind auf die Steckkarte zuzugreifen, verwaltet und jedem Benutzer die erforderlichen Zugriffsberechtigungen zugewiesen. Hierbei werden die Benutzerdaten der neu angelegten Benutzer intern in der Steckkarte abgelegt.

Benutzer hinzufügen

1. ➤ Klicken Sie auf die Schaltfläche [Benutzer hinzufügen].
 - ➔ Das Dialogfenster zum Anlegen eines neuen Benutzers wird geöffnet.
2. ➤ Geben Sie Benutzername und Passwort an.



Beachten Sie beim Zuweisen von Benutzername und Passwort die Längenbeschränkung von 127 Byte für Passwörter und 63 Byte für Benutzernamen. Die Zeichen werden mit UTF-8 codiert und die Anzahl der verwendeten Bytes hängt davon ab, welche Zeichen eingegeben werden. Für normale Zeichen (Buchstaben a-z oder Ziffern 0-9) wird 1 Byte je Zeichen verwendet. Für Sonderzeichen und Umlaute werden bis zu 4 Byte pro Zeichen verwendet. Die Längenbegrenzung begrenzt daher die Anzahl der Bytes und nicht die Anzahl der Zeichen.

3. ➤ Mit [Hinzufügen] wird der neue Benutzer in die Liste aufgenommen und der Dialog geschlossen.

Benutzer entfernen

1. ➤ Klicken Sie in der Tabelle hinter dem Benutzereintrag, welchen Sie entfernen möchten, auf die Schaltfläche [Benutzer entfernen].
 - ➔ Es folgt eine Sicherheitsabfrage zur Entfernung des Benutzereintrags.
2. ➤ Mit [Entfernen] wird der Benutzereintrag aus der Tabelle entfernt und der Dialog geschlossen.

Passwort ändern

1. ➤ Klicken Sie in der Tabelle hinter dem Benutzereintrag, dessen Passwort Sie ändern möchten, auf die Schaltfläche [Passwort setzen].
 - ➔ Das Dialogfenster zur Passworteingabe für den entsprechenden Benutzereintrag wird geöffnet.
2. ➤ Tragen Sie Ihr neues Passwort in die 2 Eingabefelder ein.
3. ➤ Mit [Speichern] wird das neue Passwort für den Benutzereintrag übernommen und der Dialog geschlossen.

Ändern von Benutzerrollen

Sie können für jeden Benutzereintrag eine oder mehrere Benutzerrollen mit unterschiedlichen Berechtigungen auswählen. Diese Berechtigungen steuern den Zugriff auf:

- 2CON
- Web-based Management - WBM

1. ➤ Klicken Sie in der Tabelle hinter dem Benutzereintrag, dessen Rolle Sie ändern möchten, auf die Schaltfläche [Benutzer editieren].
 - ➔ Das Dialogfenster zur Zuweisung von Rollen für den entsprechenden Benutzereintrag wird geöffnet.
2. ➤ Weisen Sie durch Auswahl die entsprechenden Rollen dem Benutzereintrag zu.
3. ➤ Mit [Speichern] werden die ausgewählten Rollen für den Benutzereintrag übernommen und der Dialog geschlossen.

Benutzerrollen und deren Zugriffsrechte

2CON	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
Cockpitausgabe (z.B. Auslastung)	✓	✓	✓			✓	✓	✓	✓	✓	✓		
Steckkarte-Neustart (Reboot)	✓												
Steckkarte Reset (Default Typ 1)	✓												
Steckkarte Status lesen	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Geräteinformationen lesen	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Zugriff auf WBM	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
Übersicht - Allgemeine Daten	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Übersicht - Cockpit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnose - Benachrichtigungen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnose - PROFINET (optional)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Konfiguration - Netzwerk	✓	✓	✓ ¹			✓ ¹	✓ ¹	✓ ¹					
Konfiguration - Datum und Uhrzeit	✓	✓	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹		
Konfiguration - Webdienste	✓	✓											
Security - Zertifikatauthentifizierung	✓	✓		✓									
Security - Firewall	✓	✓											
Security - Benutzerauthentifizierung	✓	✓			✓								
Verwaltung - Firmware-Update	✓	✓											

¹) Nur Lesezugriff

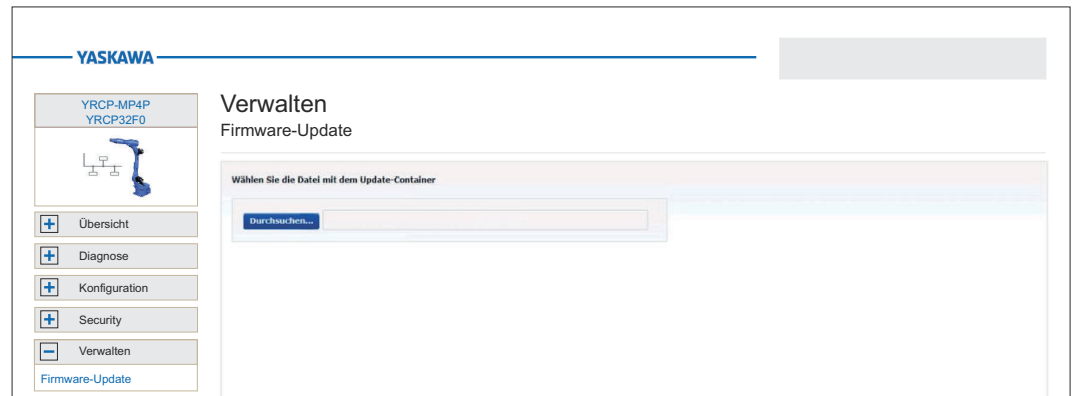
6.6 Verwaltung

6.6.1 Firmware-Update

Hier können Sie ein Firmware-Update auf Ihrer Steckkarte durchführen.



Bitte beachten Sie, dass Sie ausschließlich mit Administratorrechten ein Firmware-Update durchführen können!



Vorgehensweise



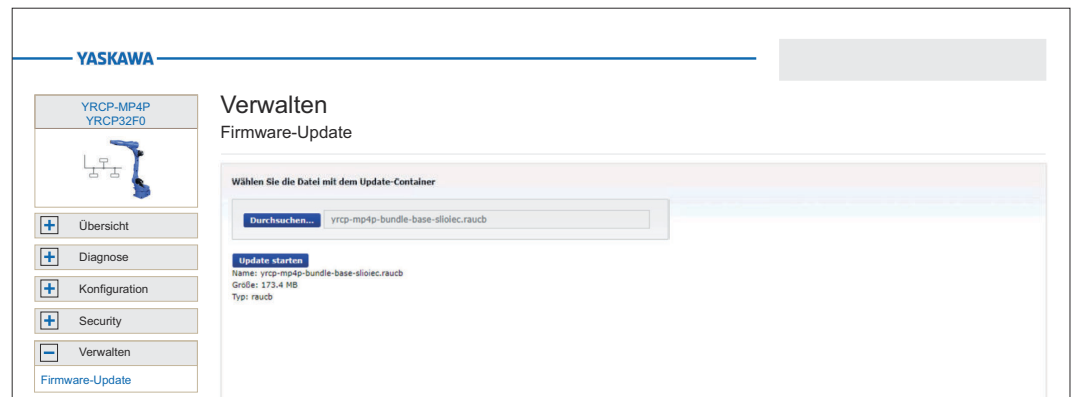
VORSICHT

Beim Aufspielen einer neuen Firmware ist äußerste Vorsicht geboten. Unter Umständen kann Ihre Steckkarte unbrauchbar werden, wenn beispielsweise während der Übertragung die Spannungsversorgung unterbrochen wird oder die Firmware-Datei fehlerhaft ist. Setzen Sie sich in diesem Fall mit unserem Support in Verbindung!

Den aktuell installierten Firmware-Stand Ihrer Steckkarte finden Sie im WBM unter *"Übersicht → Allgemeine Daten"*. Hier können Sie auch überprüfen, ob das Firmware-Update erfolgreich war. *"Allgemeine Daten" ...Seite 41*

1. ➔ Im *"Download Center"* von www.yaskawa.eu.com finden Sie immer die aktuellste Firmware unter der entsprechenden Best.-Nr.
Laden Sie die aktuelle Firmware-Datei in Ihr Arbeitsverzeichnis.
2. ➔ Entpacken Sie die zip-Datei.
3. ➔ Gehen Sie zurück in das WBM zu *"Firmware-Update"* und klicken Sie auf [Durchsuchen...].
➔ Ein Dateiauswahlfenster wird geöffnet.

4. Navigieren Sie zur entpackten raucb-Datei und klicken Sie auf [Öffnen].
 - ➔ Die Firmware-Datei, welche installiert werden soll, wird geladen und im WBM angezeigt.



5. Klicken Sie auf [Update starten].
 - ➔ Die Firmware-Datei wird auf die Steckkarte übertragen und das Firmware-Update gestartet. Hierbei werden der Status der Dateiübertragung und der Status des Aktualisierungsprozesses im WBM als Fortschrittsbalken angezeigt.
6. Während des Firmware-Updates wird die Verbindung zur Steckkarte unterbrochen. Nach dem Hochlauf der Steckkarte müssen Sie sich neu am WBM der Steckkarte anmelden. Hierdurch werden die WBM-Seiten aktualisiert.
7. Zur Überprüfung des Firmware-Updates rufen Sie im WBM die Seite "Übersicht → Allgemeine Daten" auf. *"Allgemeine Daten"...Seite 41*
 - ➔ Hier sollte die neue Firmware-Version aufgeführt sein. Ansonsten starten Sie das Update erneut. Sollte das Update nicht gelingen, kontaktieren Sie bitte unseren Support.