

iC9200 Series

CPU | PMC921xEx | Betriebsanleitung

HB700 | CPU | PMC921xEx | de | 24-04

IEC 61131 CPU iC921xM-x - Hardware



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.	7
1.1	Copyright © YASKAWA Europe GmbH.	7
1.2	Über dieses Handbuch.	8
1.3	Sicherheitshinweise.	10
1.4	Sicherheitshinweis für den Benutzer.	12
1.5	Bestimmungsgemäße Verwendung.	13
1.6	Verantwortung des Betreibers.	13
1.7	Schutzeinrichtungen.	14
1.7.1	Hinweise zur Security.	14
1.8	Ausbildung des Personals.	14
1.8.1	Qualifikation.	15
1.9	Persönliche Schutzausrüstung.	15
1.10	Besondere Gefahren.	16
1.11	Feuerbekämpfung.	17
1.12	Elektrische Sicherheit.	17
1.13	Sicherheitseinrichtungen.	18
1.14	Verhalten bei Gefahren und Unfällen.	18
1.15	Beschilderung.	19
1.15.1	Hinweisschilder.	19
1.16	Sicherheitshinweise.	19
1.17	Zulassungen, Richtlinien, Normen.	20
1.18	Einsatz unter erschwerten Betriebsbedingungen.	22
2	Grundlagen und Montage.	23
2.1	Sicherheitshinweise für den Benutzer.	23
2.1.1	Handhabung und Transport.	24
2.2	Systemvorstellung.	25
2.2.1	Übersicht.	25
2.2.2	Komponenten.	26
2.2.3	Hardware-Ausgabestand.	30
2.3	Abmessungen.	30
2.4	Montage.	32
2.4.1	Montage CPU.	32
2.4.2	Montage Peripherie-Module.	34
2.5	Verdrahtung.	35
2.5.1	Verdrahtung CPU.	36
2.5.2	Verdrahtung System SLIO Peripherie.	37
2.6	Demontage.	44
2.6.1	Demontage CPU.	44
2.6.2	Demontage 8x-Peripherie-Module.	46
2.6.3	Demontage 16x-Peripherie-Module.	48
2.7	Gerätetausch und Reparatur.	50
2.7.1	Gerätetausch.	50
2.7.2	Reparatur und Gerätedefekt.	51

2.8	Industrielle Sicherheit und Aufbaurichtlinien.	52
2.8.1	Industrielle Sicherheit in der Informationstechnologie.	52
2.8.2	Aufbaurichtlinien.	54
2.9	Allgemeine Daten für iC9200 Series.	57
2.9.1	Einsatz unter erschwerten Betriebsbedingungen.	58
3	Hardwarebeschreibung.	59
3.1	Leistungsmerkmale.	59
3.2	Aufbau.	60
3.2.1	CPU iC921xM-x.	60
3.2.2	Schnittstellen.	61
3.2.3	Speicher.	64
3.2.4	Pufferungsmechanismen.	64
3.2.5	LEDs.	64
3.2.6	DIP-Schalter.	69
3.2.7	Betriebsartenschalter.	69
3.3	Technische Daten.	70
3.3.1	iC9212M-EC - PMC9212E0.	70
3.3.2	iC9216M-EC - PMC9216E0.	73
3.3.3	iC9212M-FSoE - PMC9212ES.	77
3.3.4	iC9216M-FSoE - PMC9216ES.	81
4	Einsatz CPU iC921xM-EC.	86
4.1	Sicherheitshinweise.	86
4.2	Montage.	87
4.3	Lizenzhinweise zu Open Source Software.	87
4.4	Programmierung und Dateisystem.	87
4.4.1	iCube Engineer installieren.	88
4.4.2	iCube Engineer Benutzeroberfläche.	88
4.4.3	Neues Projekt erstellen.	90
4.5	Inbetriebnahme.	90
4.5.1	Hinweise zur Inbetriebnahme.	90
4.5.2	Online-Zugriff auf die CPU.	91
4.6	Speichermanagement.	94
4.6.1	Interner Speicher.	94
4.6.2	Steckplatz für Yaskawa SD-Karte.	96
4.7	MRESET und Rücksetzen auf Werkseinstellungen.	98
4.8	Firmware-Update.	99
4.9	Safe Mode.	99
4.10	Systemvariablen und Zustandsinformationen.	101
4.10.1	Allgemeines.	101
4.10.2	Systemvariablen.	102
5	Einsatz CPU iC921xM-FSoE.	110
5.1	Sicherheitshinweise.	110
5.2	Montage.	112
5.3	Lizenzhinweise zu Open Source Software.	112

5.4	Programmierung und Dateisystem.	112
5.4.1	iCube Engineer installieren.	113
5.4.2	iCube Engineer Benutzeroberfläche.	113
5.4.3	Neues Projekt erstellen.	115
5.4.4	Parametrierung der sicheren Parameter.	115
5.4.5	Sichere Prozessdaten zuordnen.	117
5.5	Inbetriebnahme.	118
5.5.1	Hinweise zur Inbetriebnahme.	118
5.5.2	Online-Zugriff auf die CPU.	120
5.5.3	Validation des Systems.	123
5.5.4	Abgleich der Prüfsummen.	125
5.6	Speichermanagement.	126
5.6.1	Interner Speicher.	126
5.6.2	Steckplatz für Yaskawa SD-Karte.	128
5.7	MRESET und Rücksetzen auf Werkseinstellungen.	130
5.8	Firmware-Update.	131
5.9	Safe Mode.	132
5.10	Temperaturverhalten.	132
5.11	Fail Safe Zustände.	133
5.12	Reaktionszeiten.	134
5.12.1	Fehlerfreier Fall.	134
5.12.2	Vorhandensein eines Fehlers.	135
5.12.3	Beliebige Laufzeiten bei Einzelfehler.	136
5.12.4	Maximal zulässige Watchdog-Zeiten.	137
5.12.5	Zykluszeit T_{CL} Safety-CPU.	137
5.12.6	Zyklusüberwachungszeit T_{CL_MAX} Safety-CPU.	137
5.12.7	Bezeichnungen.	138
5.13	Applikationsbeispiel.	139
5.13.1	Voraussetzung.	139
5.13.2	Projektierung im iCube Engineer.	140
5.13.3	Modifikation.	152
5.14	Funktionale Sicherheit - Sicherheitsrelevante Kenngrößen.	159
5.15	Systemvariablen und Zustandsinformationen.	161
5.15.1	Allgemeines.	161
5.15.2	Systemvariablen.	162
5.15.3	FSoE-Systemvariablen.	170
5.15.4	FSoE-Diagnosevariablen.	176
6	Web-based Management - WBM.	179
6.1	Übersicht und erste Schritte.	179
6.2	Übersicht.	181
6.2.1	Allgemeine Daten.	181
6.2.2	Cockpit.	181
6.3	Diagnose.	182
6.3.1	Achsenraster.	182
6.3.2	EtherCAT.	183
6.3.3	Bewegungsalarme.	183

6.3.4	Benachrichtigungen.	184
6.3.5	PROFINET - optional.	186
6.3.6	SliceBus.	189
6.3.7	SliceBus Module.	190
6.4	Konfiguration.	191
6.4.1	Netzwerk.	191
6.4.2	Datum und Uhrzeit.	191
6.4.3	Systemdienste.	193
6.4.4	Webdienste.	193
6.5	Security.	195
6.5.1	Zertifikatauthentifizierung.	195
6.5.2	Firewall.	199
6.5.3	SD-Karte.	203
6.5.4	Syslog-Konfiguration.	205
6.5.5	Benutzerauthentifizierung.	207
6.6	Verwaltung.	213
6.6.1	iCube Apps.	213
6.6.2	Firmware-Update.	215
6.6.3	Lizenzmanagement.	216
7	Anhang.	219
	Checklisten - Einsatz CPU iC921xM-FSoE.	221
A	Checkliste Planung.	223
B	Checkliste Installation.	224
C	Checkliste Inbetriebnahme, Parametrierung und Validation.	225
D	Checkliste Betrieb.	226
E	Checkliste Modifikation und Nachrüstung.	227
F	Checkliste Außerbetriebnahme.	228

1 Allgemein

1.1 Copyright © YASKAWA Europe GmbH

All Rights Reserved

Dieses Dokument enthält geschützte Informationen von Yaskawa und darf außer in Übereinstimmung mit anwendbaren Vereinbarungen weder offengelegt noch benutzt werden.

Dieses Material ist durch Urheberrechtsgesetze geschützt. Ohne schriftliches Einverständnis von Yaskawa und dem Besitzer dieses Materials darf dieses Material weder reproduziert, verteilt, noch in keiner Form von keiner Einheit (sowohl Yaskawa-intern als auch -extern) 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

EG-Konformitätserklärung

Hiermit erklärt YASKAWA Europe GmbH, dass die Produkte und Systeme mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften übereinstimmen. Die Übereinstimmung ist durch CE-Zeichen gekennzeichnet.

Informationen zur Konformitätserklärung

Für weitere Informationen zur CE-Kennzeichnung und Konformitätserklärung wenden Sie sich bitte an Ihre Landesvertretung der YASKAWA Europe GmbH.

Warenzeichen

SLIO ist ein eingetragenes Warenzeichen der YASKAWA Europe GmbH.

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 ein eingetragenes Warenzeichen der Beckhoff Automation GmbH.

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 alle Anstrengungen unternommen, um sicherzustellen, dass die in diesem Dokument enthaltenen Informationen zum Zeitpunkt der Veröffentlichung vollständig und richtig sind. Fehlerfreiheit kann nicht garantiert werden, das Recht auf Änderungen der Informationen bleibt jederzeit vorbehalten. Eine Informationspflicht gegenüber dem Kunden über etwaige Änderungen besteht nicht. Der Kunde ist aufgefordert, seine Dokumente aktiv aktuell zu halten. Der Einsatz der Produkte mit zugehöriger Dokumentation hat immer in Eigenverantwortung des Kunden unter Berücksichtigung der geltenden Richtlinien und Normen zu erfolgen.

Die vorliegende Dokumentation beschreibt alle heute bekannten Hardware-Einheiten und Funktionen. Es ist möglich, dass Einheiten beschrieben sind, die beim Kunden nicht vorhanden sind. Der genaue Lieferumfang 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

Über dieses Handbuch

Technischer Support

Wenden Sie sich an Ihre Landesvertretung der YASKAWA Europe GmbH, wenn Sie Probleme oder Fragen zu dem Produkt haben. Steht eine solche Stelle nicht zur Verfügung, erreichen Sie den YASKAWA Kundenservice über folgenden Kontakt:

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

YASKAWA America, Inc.
2121 Norman Drive South, Waukegan, IL 60085
Tel.: 1-800-YASKAWA (927-5292) oder 1-847-887-7457 (Hotline)
E-Mail: technical_support@yaskawa.com

1.2 Über dieses Handbuch

Zielsetzung und Inhalt

Dieses Handbuch ist das Originaldokument!

Das Handbuch beschreibt die CPU PMC921xEx der iC9200 Series.

- Beschrieben wird Aufbau, Projektierung und Anwendung.
- Das Handbuch ist geschrieben für Anwender mit Grundkenntnissen in der Automatisierungstechnik.
- 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

Produkt	Best.-Nr.	ab Version:	
CPU iC921xM-x	PMC921xEx	CPU-HW: 1	CPU-FW: V2022.9.1

Piktogramme Signalwörter

Besonders wichtige Textteile sind mit folgenden Piktogrammen und Signalworten ausgezeichnet:

**GEFAHR**

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

**WARNUNG**

Gefährliche Situation für Leben und Gesundheit von Personen. Nichtbeachten kann Tod oder schwerste Verletzungen zur Folge haben.

**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

Haftungsbeschränkung

Alle Angaben und Hinweise in dieser Betriebsanleitung wurden unter Berücksichtigung der geltenden Normen und Vorschriften, dem Stand der Technik sowie unserer langjährigen Erkenntnisse und Erfahrungen zusammengestellt.

Der Hersteller übernimmt keine Haftung für Schäden aufgrund von:

- Nichtbeachtung der Betriebsanleitung
- Nichtbestimmungsgemäßer Verwendung
- Einsatz von nicht ausgebildetem Personal

Der tatsächliche Lieferumfang kann bei Sonderausführungen, der Inanspruchnahme zusätzlicher Bestelloptionen oder aufgrund neuester technischer Änderungen von den hier beschriebenen Erläuterungen und Darstellungen abweichen.

Der Benutzer trägt die Verantwortung für die Durchführung von Service und Inbetriebnahme gemäß den Sicherheitsvorschriften der geltenden Normen und allen anderen relevanten staatlichen oder örtlichen Vorschriften betreffend Leiterdimensionierung und Schutz, Erdung, Trennschalter, Überstromschutz usw.

Für Schäden, die bei der Montage oder beim Anschluss entstehen, haftet derjenige, der die Montage oder Installation ausgeführt hat.

Der Inhalt dieser Druckschrift wurde auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass für die vollständige Übereinstimmung keine Gewähr übernommen wird. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, und notwendige Korrekturen sind in den nachfolgenden Ausgaben enthalten.

Für Verbesserungsvorschläge sind wir dankbar.

Für Schäden, die durch fehlende oder unzureichende Kenntnisse der Betriebsanleitung entstehen, ist jegliche Haftung des Herstellers ausgeschlossen.

Für den Betreiber ist es deshalb ratsam, sich die Einweisung des Personals schriftlich bestätigen zu lassen.

Umbauten oder funktionelle Veränderungen am Produkt sind aus Sicherheitsgründen nicht gestattet. Nicht ausdrücklich vom Hersteller genehmigte Umbauten am Produkt führen deshalb zum Verlust jeglicher Haftungsansprüche gegen den Hersteller. Das gilt ebenfalls, wenn nicht originale bzw. nicht zugelassene Teile oder Ausstattungen verwendet werden.

Urheberschutz

Die Betriebsanleitung vertraulich behandeln. Sie ist ausschließlich für die mit dem Produkt beschäftigten Personen bestimmt. Die Überlassung der Betriebsanleitung an Dritte ohne schriftliche Genehmigung des Herstellers ist unzulässig.



Die inhaltlichen Angaben, Texte, Zeichnungen, Bilder und sonstige Darstellungen sind urheberrechtlich geschützt und unterliegen den gewerblichen Schutzrechten. Jede missbräuchliche Verwertung ist strafbar.

Sicherheitshinweise

Nutzung dieses Handbuchs

Dieses Sicherheitshandbuch enthält Informationen für den bestimmungsgemäßen Gebrauch der iC9200 Series CPUs.

Die Kenntnis von Vorschriften und die technisch einwandfreie Umsetzung der in diesem Handbuch enthaltenen Sicherheitshinweise durch qualifiziertes Personal sind Voraussetzung für die gefahrlose Installation, Inbetriebnahme und die Sicherheit bei Betrieb und Instandhaltung der iC9200 Series CPUs. → "*Ausbildung des Personals*"...Seite 14

Bei nicht qualifizierten Eingriffen in die Geräte, bei Abschalten oder Umgehen von Sicherheitsfunktionen oder bei Nichtbeachtung von Hinweisen dieses Handbuches können schwere Personen-, Sach- oder Umweltschäden eintreten, für die Yaskawa keine Haftung übernimmt.

Die Sicherheitskomponenten und Systeme werden unter Beachtung geltender Sicherheitsnormen entwickelt, gefertigt und geprüft. Sie dürfen nur mit den spezifizierten Umgebungsbedingungen und nur in Verbindung mit zugelassenen Fremdgeräten verwendet werden.

Die Betriebsanleitung enthält Sicherheitshinweise, Beschreibungen der Module und Informationen über die Lebenszyklusphasen.

Mitgeltende Unterlagen

In den Safety-CPU's sind möglicherweise Komponenten anderer Hersteller eingebaut. Für diese Zukaufteile sind von den jeweiligen Herstellern Gefährdungsbeurteilungen durchgeführt worden. Die Übereinstimmung der Konstruktionen mit den geltenden europäischen und nationalen Vorschriften wurde von den jeweiligen Herstellern der Komponenten erklärt.

Garantiebestimmungen

Die Garantiebestimmungen befinden sich in den "Allgemeinen Geschäftsbedingungen" unter → www.yaskawa.eu.com.

1.3 Sicherheitshinweise**Bestimmungsgemäße Verwendung****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 CPU iC921xM-x ist konstruiert und gefertigt für:

- den industriellen Einsatz.
- allgemeine Steuerungs- und Automatisierungsaufgaben.
- industrielle Netzwerkkommunikation, Maschinen- und Prozesskontrolle.
- die Anbindung an EtherCAT und PROFINET (optional).
- den Einbau in einen Schaltschrank mit der Schutzart IP54 oder besser.
- den Betrieb innerhalb der in den technischen Daten spezifizierten Umgebungsbedingungen.

**GEFAHR**

Das Gerät ist nicht zugelassen für den Einsatz:

- in explosionsgefährdeten Umgebungen (EX-Zone)

Dokumentation

Handbuch zugänglich machen für:

- Projektierung
- Installation
- Inbetriebnahme
- Betrieb

**VORSICHT**

Vor Inbetriebnahme und Betrieb der in diesem Handbuch beschriebenen Komponenten unbedingt beachten:

- Änderungen am Automatisierungssystem nur im spannungslosen Zustand vornehmen!
- Anschluss und Änderung nur durch ausgebildetes Elektro-Fachpersonal
- Nationale Vorschriften und Richtlinien im jeweiligen Verwenderland beachten und einhalten (Installation, Schutzmaßnahmen, EMV ...)

Wartung

Wenn Sie die vorgeschriebenen Umgebungsbedingungen einhalten, ist die CPU wartungsfrei.

→ *"Zulassungen, Richtlinien, Normen" ...Seite 20*

Ersatzteile

Bitte verwenden Sie nur Originalersatzteile von Yaskawa.

**WARNUNG**

Falsche oder fehlerhafte Ersatzteile können zu Beschädigungen, Fehlfunktionen oder Totalausfall führen sowie die Sicherheit beeinträchtigen.

Versand

Verwenden Sie für den Versand immer die Originalverpackung.

Entsorgung

Zur Entsorgung des Geräts nationale Vorschriften beachten!

Restrisiken**WARNUNG**

Die CPU iC921xM-x wurde entsprechend der in den herangezogenen Normen beschriebenen Vorgehensweise als Baugruppe für die funktionale Sicherheit entwickelt. Die erforderliche Risikominimierung wurde sowohl konstruktiv umgesetzt als auch entsprechende Warnungen und Anforderungen an den Benutzer in diesem Handbuch beschrieben. Bitte beachten Sie, dass trotz dieser Maßnahmen ein geringes Restrisiko für eine Gefährdung für Leben und Gesundheit von Personen verbleibt und berücksichtigen Sie das im Rahmen der Risikobewertung für die Maschine/Anlage in der die CPU iC921xM-x eingesetzt wird.

Sicherheitshinweis für den Benutzer

1.4 Sicherheitshinweis für den Benutzer

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 Baugruppe 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.

Messen und Ändern von elektrostatisch gefährdeten Baugruppen

Bei Messungen an elektrostatisch gefährdeten Baugruppen sind folgende Dinge zu beachten:

- Potenzialfreie Messgeräte sind kurzzeitig zu entladen.
- Verwendete Messgeräte sind zu erden.

**VORSICHT**

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

1.5 Bestimmungsgemäße Verwendung

Allgemein

Das Produkt ist ausschließlich für den in diesem Handbuch beschriebenen bestimmungsgemäßen Verwendungszweck konzipiert und konstruiert. Sie verwenden das Produkt dann bestimmungsgemäß, wenn Sie alle Hinweise und Informationen dieser Betriebsanleitung beachten.



WARNUNG

Gefahr durch nicht bestimmungsgemäße Verwendung!

Jede über die bestimmungsgemäße Verwendung hinausgehende bzw. andersartige Benutzung des Produktes kann zu gefährlichen Situationen führen.

Deshalb

- Das Produkt nur bestimmungsgemäß verwenden.
- Das Produkt nur in Verbindung mit den empfohlenen Komponenten verwenden.
- Alle Angaben in diesem Handbuch beachten.
- Dafür sorgen, dass ausschließlich qualifiziertes Personal mit/an diesem Produkt arbeitet. → ["Ausbildung des Personals"...Seite 14](#)
- Bei der Projektierung dafür sorgen, dass das Produkt immer innerhalb seiner Spezifikationen betrieben wird.
- Dafür sorgen, dass die Spannungsversorgung den vorgegebenen Spezifikationen entspricht.
- Das Produkt nur im technisch einwandfreien Zustand betreiben.
- Das Produkt nur in Kombination mit freigegebenen Komponenten betreiben.
- Das Produkt nur in Umgebungen zweiter Art (Industrienumgebung) betreiben. Das Produkt ist so entwickelt worden, dass dieses die Anforderungen der Kategorie C3 erfüllt. Für den Betrieb ist eine zugelassene Spannungsversorgung (SELV/PELV) erforderlich. Beim Betrieb des Produktes in einer Umgebung erster Art der Kategorie C2/C1 (Wohn-, Geschäfts- und Gewerbebereich ohne Zwischentransformator direkt an einem öffentlichen Niederspannungsnetz), sind durch den Schaltschrankbauer spezielle Maßnahmen zur Reduktion der Störaussendung (leitungsgelassen und gestrahlt) vorzusehen und nachzuweisen, da es ohne Zusatzmaßnahmen zu EMV-Störungen kommen kann. Ob ein hier beschriebenes Produkt selbst mit Zusatzmaßnahmen die Kategorie C2/C1 erreicht, kann nicht gewährleistet werden.

Veränderungen und Umbauten am Produkt

Zur Vermeidung von Gefährdungen und zur Sicherung der optimalen Leistung dürfen an dem Produkt weder Veränderungen noch An- und Umbauten vorgenommen werden, die durch den Hersteller nicht ausdrücklich genehmigt worden sind.

1.6 Verantwortung des Betreibers

Allgemein

Das Produkt wird im gewerblichen Bereich eingesetzt. Der Betreiber des Produkts unterliegt daher den gesetzlichen Pflichten zu Arbeitssicherheit. Neben den Arbeitssicherheits Hinweisen in dieser Betriebsanleitung müssen die für den Einsatzbereich des Moduls gültigen Sicherheits-, Unfallverhütungs- und Umweltschutzvorschriften eingehalten werden. Dabei gilt insbesondere:

- Der Betreiber muss sich über die geltenden Arbeitsschutzbestimmungen informieren und in einer Gefährdungsbeurteilung zusätzlich Gefahren ermitteln, die sich durch die speziellen Arbeitsbedingungen am Einsatzort des Produktes ergeben. Diese muss er in Form von Betriebsanweisungen für den Betrieb des Produktes umsetzen.
- Diese Betriebsanleitung muss in unmittelbarer Umgebung des Produktes aufbewahrt werden und den an und mit dem Produkt beschäftigten Personen jederzeit zugänglich sein.
- Die Angaben der Betriebsanleitung sind vollständig und uneingeschränkt zu befolgen!
- Das Produkt darf nur in technisch einwandfreiem Zustand betrieben werden.

Ausbildung des Personals

1.7 Schutzeinrichtungen

Schutzart

Der Einbauort der CPU muss für Geräte nach IP20 geeignet sein.

**WARNUNG****Schwere Gefahren durch unsachgemäßen Einsatz**

Schwere Gefahren für den Anwender und/oder Sachschäden drohen durch unsachgemäßen oder nicht bestimmungsgemäßen Einsatz sowie Manipulation der CPU.

**HINWEIS****Sachschäden durch Fehlbeanspruchung**

Die Schutzart IP20 (IEC 60529/EN 60529) der CPU ist für eine saubere und trockene Umgebung vorgesehen.

- Setzen Sie die CPU keiner mechanischen und/oder thermischen Beanspruchung aus, welche die beschriebenen Grenzen überschreitet.
- Beachten Sie, dass Sie die CPU für einen einwandfreien Betrieb zwingend in ein abschließbares Gehäuse oder einen abschließbaren Schaltschrank mit mindestens Schutzart IP54 einbauen müssen.

1.7.1 Hinweise zur Security

**HINWEIS****Nicht autorisierte physikalische Zugriffe**

Durch nicht autorisierte physikalische Zugriffe besteht die Gefahr von Manipulationen an der CPU.

- Schützen Sie Ihr System vor unbefugten physikalischen Zugriffen. Verwenden Sie z.B. einen abschließbaren Schaltschrank.

**HINWEIS****Unerlaubte(r) Löschung/Austausch des sicherheitsbezogenen Projekts möglich**

- Geben Sie die Rollen zur Benutzerauthentifizierung "Admin", "Commissioner" und "Engineer" nur denjenigen Anwendern bekannt, die zur Programmierung der sicherheitsbezogenen Steuerung berechtigt sind. Anderenfalls ist der unerlaubte Austausch oder die Löschung des sicherheitsbezogenen Projekts durch den Anwender nicht auszuschließen. Benutzerrollen können Sie im Web-based Management einstellen.
→ ["Benutzerauthentifizierung"...Seite 207](#)
- Bauen Sie die CPU und die angereichten Module zwingend in ein abschließbares Gehäuse oder einen abschließbaren Schaltschrank ein. Das Gerätegehäuse ist nicht gegen Manipulationen geschützt, der Zugriff auf die CPU ist nicht validierbar. Der Zugriff auf die SD-Karte ist möglich, sodass Daten gelesen und manipuliert werden können. Wir empfehlen, den Schacht des Parametrierungsspeichers (SD-Karte) an der CPU mit einem Siegel gegen Manipulation zu schützen.

1.8 Ausbildung des Personals

**WARNUNG****Verletzungsgefahr bei unzureichender Qualifikation!**

Unsachgemäßer Umgang kann zu erheblichen Personen- und Sachschäden führen.

Deshalb: Besondere Tätigkeiten nur durch die in den jeweiligen Kapiteln dieser Betriebsanleitung benannten Personen durchführen lassen.

1.8.1 Qualifikation

In der Betriebsanleitung werden folgende Qualifikationen für verschiedene Tätigkeitsbereiche benannt:

Bedienungspersonal

Die Bedienung des Automatisierungssystems darf nur von Personen durchgeführt werden, die dafür ausgebildet, eingewiesen und befugt sind. Störungsbeseitigung, Instandhaltung, Reinigung, Wartung und Austausch darf nur durch geschultes oder eingewiesenes Personal durchgeführt werden. Diese Personen müssen die Betriebsanleitung kennen und danach handeln. Inbetriebnahme und Einweisung dürfen nur vom qualifizierten Personal durchgeführt werden.

Qualifiziertes Personal

Vom Hersteller autorisierte Elektro-Ingenieure und Elektro-Fachkräfte des Kunden oder Dritter, die Installation und Inbetriebnahme vom Hersteller erlernt haben und berechtigt sind, Stromkreise und Geräte gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen. Qualifiziertes Personal verfügt über eine Ausbildung oder Unterweisung gemäß den örtlich jeweils gültigen Standards der Sicherheitstechnik in Pflege und Gebrauch angemessener Sicherheitsausrüstung.

1.9 Persönliche Schutzausrüstung

Allgemein

Bei der Arbeit ist das Tragen von persönlicher Schutzausrüstung erforderlich, um die Gesundheitsgefahren zu minimieren.

- Die für die jeweilige Arbeit notwendige Schutzausrüstung während der Arbeit stets tragen.
- Im Arbeitsbereich vorhandene Schilder zur persönlichen Sicherheit beachten!

Arbeitsschutzkleidung



ist eng anliegende Arbeitskleidung mit geringer Reißfestigkeit, mit engen Ärmeln und ohne abstehende Teile. Je nach Einsatzgebiet soll damit verhindert werden, dass der Träger sich während der Arbeit ernsthafte Verletzungen zuzieht oder dass er gesundheitlichen Belastungen ausgesetzt ist. Aus Gründen der Verletzung sollte kein Schmuck wie Ringe und Ketten getragen werden.

Schutzhelm



zum Schutz vor herabfallenden und umherfliegenden Teilen.

Sicherheitsschuhe



zum Schutz vor schweren herabfallenden Teilen.

Schutzhandschuhe



zum Schutz der Hände vor Reibung, Abschürfungen, Einstichen oder Verletzungen, sowie vor Berührung mit heißen Gegenständen.

Besondere Gefahren

Bei besonderen Arbeiten tragen: Schutzbrille



zum Schutz der Augen vor umherfliegenden Teilen und Flüssigkeitsspritzern.

1.10 Besondere Gefahren

Allgemein

Im folgenden Abschnitt werden die Restrisiken benannt. Die hier aufgeführten Sicherheitshinweise und die Warnhinweise in den weiteren Kapiteln dieser Anleitung beachten, um Gesundheitsgefahren zu reduzieren und gefährliche Situationen zu vermeiden.

Elektrischer Strom



GEFAHR

Lebensgefahr durch elektrischen Strom!

Bei Berührung mit spannungsführenden Teilen besteht unmittelbare Lebensgefahr. Beschädigung der Isolation oder einzelner Bauteile kann lebensgefährlich sein.

Deshalb: Bei Beschädigung der Isolation Spannungsversorgung sofort abschalten. Arbeiten an der elektrischen Anlage nur von qualifiziertem Personal ausführen lassen. Bei allen Arbeiten an der elektrischen Anlage diese spannungslos schalten und vor Wiedereinschalten sichern.

Gefahren durch Restenergie



GEFAHR

Lebensgefahr durch elektrischen Strom!

Nach dem Trennen eines Gerätes vom Netz dürfen spannungsführende Teile wie z.B. Leistungsanschlüsse erst dann berührt werden, wenn die Kondensatoren im Gerät entladen sind.

Deshalb: Entladezeit der Kondensatoren berücksichtigen und spannungsführende Teile vorher nicht berühren. Entsprechende Hinweise auf dem Gerät beachten. Wenn Sie zusätzliche Kondensatoren am Zwischenkreis angeschlossen haben, kann die Zwischenkreisentladung auch erheblich länger dauern. In diesem Fall müssen Sie die nötige Wartezeit selbst ermitteln bzw. messen, ob das Gerät spannungsfrei ist.

Bewegte Bauteile



WARNUNG

Verletzungsgefahr durch bewegte Bauteile!

Rotierende bzw. linear bewegte Bauteile können schwere Verletzungen verursachen.

Deshalb: Während des Betriebs nicht in bewegte Bauteile eingreifen. Abdeckungen im Betrieb nicht öffnen. Die mechanische Restenergie ist von der Applikation abhängig. Angetriebene Bauteile drehen bzw. bewegen sich auch nach dem Abschalten der Energieversorgung noch für eine bestimmte Zeit. Sorgen Sie für angemessene Sicherheitseinrichtungen.

1.11 Feuerbekämpfung



GEFAHR

Lebensgefahr durch elektrischen Strom!

Stromschlag bei Verwendung eines leitenden Feuerbekämpfungsmittels.



Deshalb folgendes Feuerbekämpfungsmittel verwenden:
ABC-Pulver / CO₂

1.12 Elektrische Sicherheit

Allgemein

Die CPU ist gemäß IEC61131-2 für Verschmutzungsgrad 2 ausgelegt. Das bedeutet, dass zur Betriebszeit nur nichtleitfähige Verschmutzungen auftreten dürfen. Kurzzeitige Leitfähigkeit durch Betauung ist nur zulässig, wenn das Modul außer Betrieb ist.



WARNUNG

Verletzungsgefahr durch leitfähige Verschmutzungen!

Es dürfen während der Betriebszeit keine leitfähigen Verschmutzungen auftreten.

Deshalb: Vor der Installation des Systems prüfen und gegebenenfalls durch zusätzliche Maßnahmen sicherstellen, dass Verschmutzungsgrad 2 nicht überschritten wird (z.B. Einbau in Schaltschrank mit Schutzart IP54 oder besser).

Installation und Projektierung



WARNUNG

Bei fehlerhafter Installation und Nachrüstung können schwere Gefahren drohen

- Geräte und deren Installationen im System sind nach diesen Anforderungen auszulegen.
- Bestehende Anlagen und Systeme, welche nachgerüstet werden, sind ebenfalls diesbezüglich zu überprüfen.

Verhalten bei Gefahren und Unfällen

Hinweis zur Spannungsversorgung

**WARNUNG****Verletzungsgefahr durch elektrischen Strom!**

An die CPU dürfen nur Geräte angeschlossen werden, die eine sichere Trennung zum 230V Netz aufweisen. Das Netzteil zur Erzeugung der 24V-Versorgung muss den Anforderungen für PELV/SELV gemäß EN 50178 entsprechen.

**WARNUNG****Gefährliche Körperströme und Verlust der funktionalen Sicherheit**

Die Nichtbeachtung der Hinweise zur elektrischen Sicherheit kann zum Auftreten von gefährlichen Körperströmen und zum Verlust der funktionalen Sicherheit führen.

Beachten Sie zur Gewährleistung der elektrischen Sicherheit die folgenden Punkte:

- Direktes/indirektes Berühren
- Sichere Trennung

Direktes/indirektes Berühren

Gewährleisten Sie für alle am System angeschlossenen Komponenten den Schutz gegen direktes und indirektes Berühren nach VDE 0100 Teil 410 (IEC 60364-4-41). Im Fehlerfall darf es zu keiner gefahrbringenden Spannungsverschleppung kommen (Einfehlersicherheit!). Dies gilt auch für Geräte und Komponenten mit gefährlichen Berührungsspannungen, die an Netzwerk- und/oder Diagnose-Schnittstellen der verwendeten Geräte dauerhaft angeschlossen sind.

Sichere Trennung

Setzen Sie ausschließlich Geräte mit sicherer Trennung ein, wenn deren Anschlüsse im normalen Betriebsfall oder durch einen Isolationsfehler verursacht, gefährliche Berührungsspannungen führen können.

1.13 Sicherheitseinrichtungen

**WARNUNG****Lebensgefahr durch nicht funktionierende Sicherheitseinrichtungen!**

Sicherheitseinrichtungen sorgen für ein Höchstmaß an Sicherheit im Betrieb. Auch wenn durch Sicherheitseinrichtungen Arbeitsprozesse umständlicher werden, dürfen Sie keinesfalls außer Kraft gesetzt werden. Die Sicherheit ist nur bei intakten Sicherheitseinrichtungen gewährleistet.

Deshalb: Vor Arbeitsbeginn prüfen, ob die Sicherheitseinrichtungen funktionstüchtig und richtig installiert sind.

1.14 Verhalten bei Gefahren und Unfällen

Vorbeugende Maßnahmen

- Stets auf Unfälle oder Feuer vorbereitet sein!
- Erste-Hilfe-Einrichtungen (Verbandskasten, Decken usw.) und Feuerlöscher griffbereit aufbewahren.
- Personal mit Unfallmelde-, Erste-Hilfe- und Rettungseinrichtungen vertraut machen.

Im Fall der Fälle: Richtig handeln

- Gerät durch Not-Stopp sofort außer Betrieb setzen.
- Erste-Hilfe-Maßnahmen einleiten.
- Personen aus der Gefahrenzone bergen.
- Verantwortlichen am Einsatzort informieren.
- Arzt und / oder Feuerwehr alarmieren.
- Zufahrtswege für Rettungsfahrzeuge frei machen.

1.15 Beschilderung



WARNUNG

Verletzungsgefahr durch unleserliche Symbole!

Im Laufe der Zeit können Aufkleber und Symbole auf den Geräten verschmutzen oder auf andere Weise unkenntlich werden.

Deshalb: Alle Sicherheits-, Warn- und Bedienungshinweise am Gerät in stets gut lesbarem Zustand halten.

1.15.1 Hinweisschilder

Die folgenden Symbole und Hinweisschilder befinden sich im Arbeitsbereich. Sie beziehen sich auf die unmittelbare Umgebung in der sie angebracht sind.

Elektrische Spannung



GEFAHR

Lebensgefahr durch elektrischen Strom!

Entladezeit > 1 Minute

Gespeicherte elektrische Ladung

Deshalb: Entladezeit der Kondensatoren berücksichtigen und spannungsführende Teile vorher nicht berühren. Entsprechende Hinweise auf dem Gerät beachten. Wenn Sie zusätzliche Kondensatoren am Zwischenkreis angeschlossen haben, kann die Zwischenkreisentladung auch erheblich länger dauern. In diesem Fall müssen Sie die nötige Wartezeit selbst ermitteln bzw. messen, ob das Gerät spannungsfrei ist.

1.16 Sicherheitshinweise

Die CPU entspricht dem heutigen Stand der Technik und erfüllen die geltenden Sicherheitsbestimmungen und die entsprechenden harmonisierten, europäischen Normen (EN).

Ergänzend gelten für den Anwender die:

- einschlägigen Unfallverhütungsvorschriften
- EG-Richtlinien oder sonstige länderspezifische Bestimmungen
- allgemein anerkannten sicherheitstechnischen Regeln
- allgemeinen ESD-Vorschriften

Störungen jeglicher Art oder sonstige Schäden sind einer zuständigen Person zu melden. Schutz- und Sicherheitseinrichtungen dürfen nicht umgangen oder überbrückt werden. Demontierte Sicherheitseinrichtungen sind vor einer erneuten Inbetriebnahme wieder anzubauen und müssen einem Funktionstest unterzogen werden. Die Module sind gegen missbräuchliche oder versehentliche Benutzung zu sichern. Original angebrachte Hinweisschilder, Beschriftungen, Aufkleber oder ähnliches sind immer zu beachten und in einem lesbaren Zustand zu halten.

Zulassungen, Richtlinien, Normen

1.17 Zulassungen, Richtlinien, Normen

Konformität und Approbation		
Konformität		
CE	2014/30/EU	EMV-Richtlinie
	2006/42/EG	Maschinenrichtlinie
RoHS (EU)	2011/65/EU	Beschränkung der Verwendung bestimmter gefährlicher Stoffe
UKCA	2016 No. 1091	Electromagnetic Compatibility Regulations
	2008 No. 1597	Supply of Machinery (Safety) Regulation
RoHS (UK)	2012 No. 3032	Use of Certain Hazardous Substances
Personenschutz und Geräteschutz		
Schutzart	-	IP20
Potenzialtrennung		
Zum Feldbus	-	Galvanisch entkoppelt
Zur Prozessebene	-	Galvanisch entkoppelt
Isolationsfestigkeit	EN 61131-2	-
Isolationsspannung gegen Bezugserde		
Eingänge / Ausgänge	-	AC / DC 50V, bei Prüfspannung AC 500V
Schutzmaßnahmen	-	gegen Kurzschluss
Umgebungsbedingungen gemäß EN 61131-2		
Klimatisch		
Lagerung /Transport	EN 60068-2-14	-40...+70°C
Betrieb		
Horizontaler Einbau hängend	EN 61131-2	0...+60°C
Vertikaler Einbau	EN 61131-2	0...+55°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, 9Hz ... 150Hz
Schock	EN 60068-2-27	15g, 11ms
Montagebedingungen		
Einbauort	-	Im Schaltschrank (IP54 oder besser)
Einbaulage	-	Horizontal und vertikal → <i>"Montagemöglichkeiten"...</i> Seite 34

EMV	Norm	Bemerkungen	
Störaussendung	EN 61000-6-4	Class A (Industriebereich)	
Störfestigkeit Zone B	EN 61000-6-2	Industriebereich	
		EN 61000-4-2	ESD 8kV bei Luftentladung (Schärfegrad 3), 4kV bei Kontaktentladung (Schärfegrad 2)
		EN 61000-4-3	HF-Einstrahlung (Gehäuse) 80MHz ... 1000MHz, 10V/m 1,4GHz ... 6,0GHz, 3V/m
		EN 61000-4-6	HF-Leitungsgeführt 150kHz ... 80MHz, 10V
		EN 61000-4-4	Burst, Schärfegrad 3
		EN 61000-4-5	Surge, Schärfegrad 3 ¹

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

Beispiele für Blitzschutzableiter

Anwendung	Hersteller	Artikel	Beschreibung
Einspeisung	Dehn	BLITZDUCTOR VT BVT AVD 24	Blitzschutz extern (DC24V/10A)
Digital Eingänge, Testpuls-Ausgänge	Dehn	DEHNconnect RK DCO RK ME 24	Blitzschutz extern (DC24V/0,5A)
Digital Ausgänge	Dehn	DEHNconnect RK DCO RK D 5 24	Blitzschutz extern (DC24V/10A)
EtherCAT-Schnittstelle	Dehn	DEHNpatch DPA M CLE RJ45B 48	Blitzschutz extern (RJ45/48V)

Normen und Standards

DIN EN 61508 Teile 1-7	Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer, programmierbarer Systeme
DIN EN ISO 13849-1	Sicherheit von Maschinen, sicherheitsbezogene Teile von Steuerungen
DIN EN 61784-3	Funktional sichere Übertragung bei Feldbussen - Allgemeine Regeln und Profilstellungen
DIN EN 60204-1	Elektrische Ausrüstung von Maschinen
DIN EN 61131-2	Speicherprogrammierbare Steuerungen, Teil 2: Betriebsmittelanforderungen und Prüfungen
DIN EN 61000-4-11	Spannungsvariation
Reihe SN 29500	Ausfallrate, Bauelement, Erwartungswert, Zuverlässigkeit
DIN EN 61496-1	Berührungslos wirkende Schutzvorrichtungen

Einsatz unter erschwerten Betriebsbedingungen

Anforderungen an Luft- und Kriechstromstrecken und System-Spannungsversorgungen

DIN EN 61131-2	Die Festlegung der Luft- und Kriechstromstrecken erfolgt gemäß EN 61131-2. Für die sicheren Feldbus-Koppler werden Überspannungskategorie 2 und Verschmutzungsgrad 2 zugrunde gelegt.
DIN EN 13849	Die Annahme von Fehlerausschlüssen für Kurzschlüsse zwischen benachbarten Leiterbahnen oder für Kurzschlüsse zwischen benachbarten Bauteilen muss weitestgehend durch geeignete Schaltungs- und Layoutmaßnahmen vermieden werden. Ist ein Fehlerausschluss unumgänglich, sind Maßnahmen gemäß EN 13849 Teil 2 anzuwenden.
DIN EN 50178	Das Gerät wird entwickelt für den Betrieb an 24V-Netzteilen, die den PELV-/SELV-Bestimmungen gemäß EN 50178 entsprechen.
DIN EN 61508	Die normativen Anforderungen der EN 61508 (erhöhte EMV Anforderungen und Anforderungen bezüglich Potenzialtrennung) sind auch für die gemeinsame Spannungszuführung des SLIO Systems zu erfüllen.
DIN EN 50178	Damit die elektrischen Werte für Kleinspannung mit sicherer Trennung auf den sicheren Feldbus-Koppler nicht überschritten werden können, werden für das System ausschließlich 24V-Netzteile eingesetzt, die den PELV-/SELV-Bestimmungen gemäß EN 50178 entsprechen.
	Um die sicheren Feldbus-Koppler vor Überspannung zu schützen, wird ein geeigneter Überspannungsschutz vorgesehen.
DIN EN 60204-1	Das 24V-Netzteil muss die in der EN 60204-1 definierte Spannungsunterbrechung beherrschen.

Anforderungen an Umwelt- und EMV-Prüfungen

DIN EN 61131-2	Speicherprogrammierbare Steuerungen, Teil 2: Betriebsmittelanforderungen und Prüfungen
DIN EN DIN EN 61326-3-1:2017	Für die erhöhte EMV-Störfestigkeits-Prüfungen wird die DIN EN 61326-3-1:2017 angewendet.

1.18 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 Grundlagen und Montage

2.1 Sicherheitshinweise für den Benutzer



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 die CPU entsprechend der Bestimmung eingesetzt wird.
- Beachten Sie die Sicherheitsvorschriften der Elektrotechnik und der Berufsgenossenschaft!
- Führen Sie alle Arbeiten an der CPU im spannungslosen Zustand durch!
- Die CPU darf nur unter Beachtung der zugehörigen Dokumentation und unter Einhaltung der darin angegebenen Vorgaben von Fachpersonal montiert werden.
- Elektrische Arbeiten dürfen nur von Elektrofachkräften durchgeführt werden.
- Die CPU 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 erforderlichen Vorsichtsmaßnahmen bei der Handhabung elektrostatisch gefährdeter Bauelemente (EN 61340-5-1, IEC 61340-5-1)!
- Reparaturen an der CPU, insbesondere das Öffnen des Gehäuses, dürfen nur vom Hersteller vorgenommen werden.
- Bewahren Sie die Betriebsanleitung auf!
- Der Betreiber der CPU bzw. der Anlage unterliegt den gesetzlichen Pflichten zu Arbeitssicherheit. In diesem Zusammenhang ist die Maschinenrichtlinie zu berücksichtigen.



GEFAHR

Schutz vor gefährlichen Spannungen

- Beim Einsatz der CPU muss der Anwender vor dem Berühren von gefährlichen Spannung geschützt werden.
- Sie müssen daher ein Isolationskonzept für Ihre Anlage erstellen, das eine sichere Trennung der Potentialbereiche von ELV und von gefährlichen Spannung umfasst.
- Beachten Sie dabei, die bei den Baugruppen angegebenen Isolationsspannungen zwischen den Potentialbereichen und treffen Sie geeignete Maßnahmen, wie z.B. die Verwendung von PELV/SELV Stromversorgungen für die Baugruppen.

**WARNUNG****Sicherheitshinweise für den Start von Applikationen**

Berücksichtigen Sie bei der Konfiguration der Startbedingungen für Ihre Anlage:

- Der Start der Maschine oder Anlage darf nur dann erfolgen, wenn sichergestellt ist, dass sich keine Person im Gefahrenbereich befindet.
- Halten Sie die Anforderungen der EN ISO 13849-1 in Bezug auf die manuelle Rückstellungsfunktion ein. So darf keine Maschinenbewegung selbst eingeleitet bzw. Gefährdungssituation hervorgerufen werden, bedingt durch z.B.:
 - Einschalten von Teilnehmern
 - Quittieren von Gerätefehlermeldungen
 - Quittieren von Bausteinfehlermeldungen in der Applikation
 - Aufhebung von Anlaufsperrern

Berücksichtigen Sie diese Hinweise auch, um einen unerwarteten Maschinenanlauf nach Quittierung mit einem "Operator Acknowledgement" auszuschließen!

2.1.1 Handhabe und Transport

Handhabung elektrostatisch gefährdeter Baugruppen

**HINWEIS****Elektrostatische Entladung**

Die CPU enthält Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können.

- Beachten Sie beim Umgang mit der CPU die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) gemäß EN 61340-5-1 und IEC 61340-5-1.

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.

**HINWEIS****Sachschaden durch Nichtbeachtung der ESD-Hinweise**

Wenn Sie die ESD-Hinweise beim Aus- und Einpacken nicht beachten, kann es zu Schäden an der CPU kommen.

- Beachten Sie beim Aus- und Einpacken der CPU die ESD-Hinweise.

Messen und Ändern von elektrostatisch gefährdeten Baugruppen

Bei Messungen an elektrostatisch gefährdeten Baugruppen sind folgende Dinge zu beachten:

- Potenzialfreie Messgeräte sind kurzzeitig zu entladen.
- Verwendete Messgeräte sind zu erden.

Bei Änderungen an elektrostatisch gefährdeten Baugruppen ist darauf zu achten, dass ein geerdeter Lötkolben verwendet wird.

**VORSICHT**

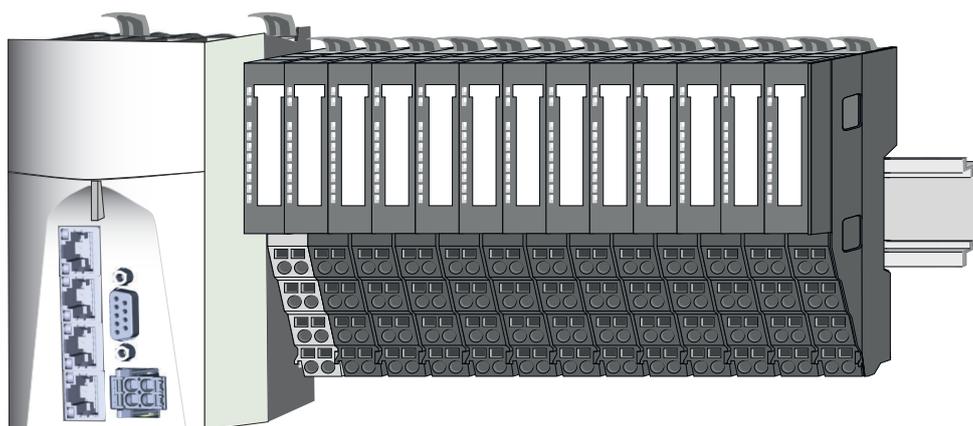
Bei Arbeiten mit und an elektrostatisch gefährdeten Baugruppen ist auf ausreichende Erdung des Menschen und der Arbeitsmittel zu achten.

2.2 Systemvorstellung**2.2.1 Übersicht**

iC9200 Series ist ein Automatisierungssystem für die Montage auf einer 35mm Tragschiene. Durch die Kompatibilität zum System SLIO von Yaskawa können Sie durch Einsatz der System SLIO Peripherie-Module in 2-, 4-, 8- und 16-Kanalausführung dieses System passgenau an Ihre Automatisierungsaufgaben adaptieren. Ein zusätzlich vorhandener PCIe-Bus macht das System für zukünftige Erweiterungen zukunftssicher.



Nähere Informationen zum Einsatz der System SLIO Module finden Sie im entsprechenden Handbuch im "Download Center" von www.yaskawa.eu.com unter der entsprechenden Best.-Nr.



2.2.2 Komponenten

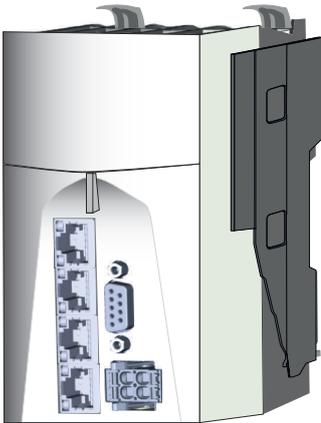
- CPU (Kopf-Modul)
- Power-Module
- 8x-Peripherie-Module
- 16x-Peripherie-Module
- Zubehör



VORSICHT

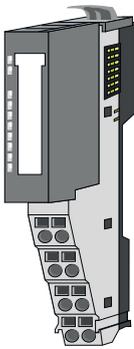
Beim Einsatz dürfen nur Yaskawa-Module kombiniert werden. Ein Mischbetrieb mit Modulen von Fremdherstellern ist nicht zulässig!

CPU iC921xM-x



Bei der CPU iC921xM-x sind CPU-Elektronik und Spannungsversorgung in ein Gehäuse integriert. Programmiert und konfiguriert wird die CPU mit iCube Engineer von Yaskawa unter IEC 61131-3. Die CPU besitzt auf der linken Seite einen PCIe-Bus für zukünftige Erweiterungen. Auf der rechten Seite können Sie über *SliceBus* System SLIO Peripherie-Module von Yaskawa anbinden. Als Kopf-Modul werden über die integrierte Spannungsversorgung sowohl die CPU-Elektronik, als auch die Elektronik der über den *SliceBus* angebotenen Peripherie-Module versorgt. Zum Anschluss der Spannungsversorgung besitzt die CPU einen abnehmbaren Steckverbinder. Zur Leistungsversorgung der angebotenen Peripherie-Module müssen Sie immer direkt nach der CPU das Power-Modul 007-1AB00 - DC 24V 10A stecken.

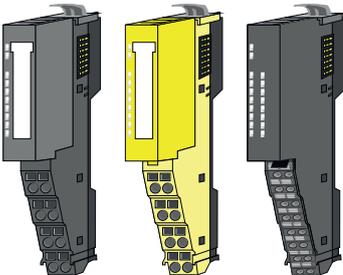
Power-Module



Beim Einsatz von System SLIO Modulen müssen Sie immer das Power-Modul 007-1AB00 - DC 24V 10A montieren, da die CPU systembedingt keine Leistungsversorgung bereit stellt.

Die farblich abgesetzten Power-Module setzen Sie ein, wenn keine Leistungsversorgung von der CPU bereitgestellt wird, wie bei der CPU iC921xM-x. Auch sind diese zu verwenden, wenn die Leistungsversorgung der I/O-Ebene nicht mehr ausreicht bzw. wenn die Elektronikversorgung nicht mehr ausreicht. Je nach eingesetztem Power-Modul haben Sie die Möglichkeit Potenzialgruppen zu bilden. Die Power-Module sind extern mit DC 24V zu versorgen. Jedes Power-Modul besitzt einen Überspannungs- und Verpol-schutz.

Peripherie-Module

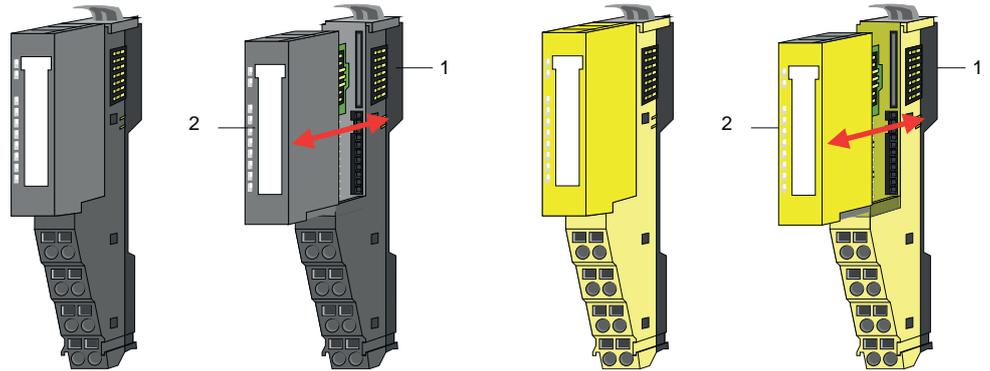


Die Peripherie-Module gibt es in folgenden Ausführungen, wobei jedes der Elektronik-Teile bei stehender Verdrahtung getauscht werden kann:

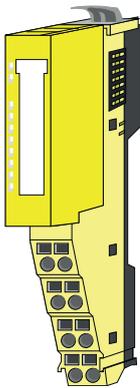
- 8x-Peripherie-Module für maximal 8 Kanäle.
 - Standard-Peripherie-Module
 - Safety-Peripherie-Module
- 16x-Peripherie-Module für maximal 16 Kanäle.

8x-Peripherie-Module

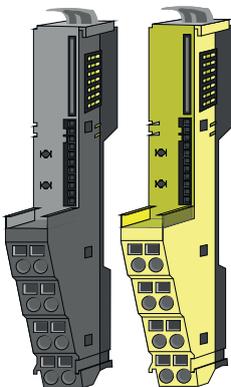
Jedes 8x-Peripherie-Modul besteht aus einem *Terminal-* und einem *Elektronik-Modul*.



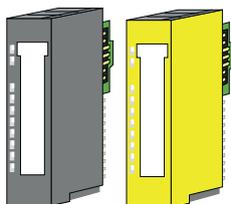
- 1 Terminal-Modul
- 2 Elektronik-Modul



Die *Safety-Peripherie-Module* aus dem System SLIO entsprechen in Aufbau und Abmessungen den Standard Peripherie-Modulen. Zur besseren Unterscheidung haben die *Safety-Peripherie-Module* ein gelbes Gehäuse. Bitte beachten Sie, dass das *Safety-Elektronik-Modul* ausschließlich auf einem gelben *Safety-Terminal-Modul* betrieben werden darf! Der Betrieb auf mechanisch kompatiblen Terminal-Modulen ist nicht zulässig.

Terminal-Modul

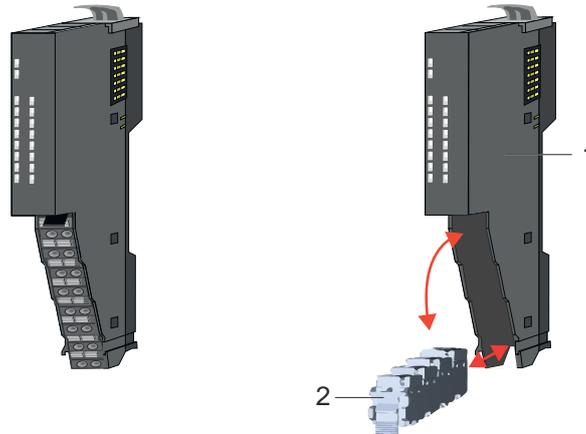
Das *Terminal-Modul* bietet die Aufnahme für das *Elektronik-Modul*, beinhaltet den Rückwandbus mit Spannungsversorgung für die Elektronik, die Anbindung an die DC 24V Leistungsversorgung und den treppenförmigen Klemmblock für die Verdrahtung. Zusätzlich besitzt das *Terminal-Modul* ein Verriegelungssystem zur Fixierung auf einer Tragschiene. Mittels dieser Verriegelung können Sie Ihr System außerhalb Ihres Schaltschranks aufbauen und später als Gesamtsystem im Schaltschrank montieren.

Elektronik-Modul

Über das *Elektronik-Modul*, welches durch einen sicheren Schiebemechanismus mit dem *Terminal-Modul* verbunden ist, wird die Funktionalität eines Peripherie-Moduls definiert. Im Fehlerfall können Sie das defekte *Elektronik-Modul* gegen ein funktionsfähiges Modul tauschen. Hierbei bleibt die Verdrahtung bestehen. Auf der Frontseite befinden sich LEDs zur Statusanzeige. Für die einfache Verdrahtung finden Sie bei jedem *Elektronik-Modul* auf der Front und an der Seite entsprechende Anschlussinformationen.

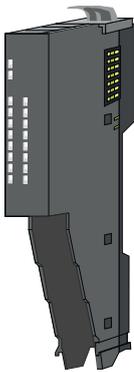
16x-Peripherie-Module

Jedes 16x-Peripherie-Modul besteht aus einer *Elektronik-Einheit* und einem *Terminal-Block*.



- 1 Elektronik-Einheit
- 2 Terminal-Block

Elektronik-Einheit



Über den Terminal-Block, welcher durch einen sicheren Klappmechanismus mit der *Elektronik-Einheit* verbunden ist, wird die Funktionalität eines 16x-Peripherie-Moduls definiert. Im Fehlerfall können Sie bei stehender Verdrahtung die defekte Elektronik-Einheit gegen eine funktionsfähige Einheit tauschen. Auf der Frontseite befinden sich LEDs zur Statusanzeige. Für die einfache Verdrahtung finden Sie bei jeder Elektronik-Einheit an der Seite entsprechende Anschlussinformationen. Die Elektronik-Einheit bietet die Aufnahme für den Terminal-Block für die Verdrahtung und beinhaltet den Rückwandbus mit Spannungsversorgung für die Elektronik und die Anbindung an die DC 24V Leistungsversorgung. Zusätzlich besitzt die Elektronik-Einheit ein Verriegelungssystem zur Fixierung auf einer Tragschiene. Mittels dieser Verriegelung können Sie Ihr System außerhalb Ihres Schalt-schranks aufbauen und später als Gesamtsystem im Schaltschrank montieren.

Terminal-Block



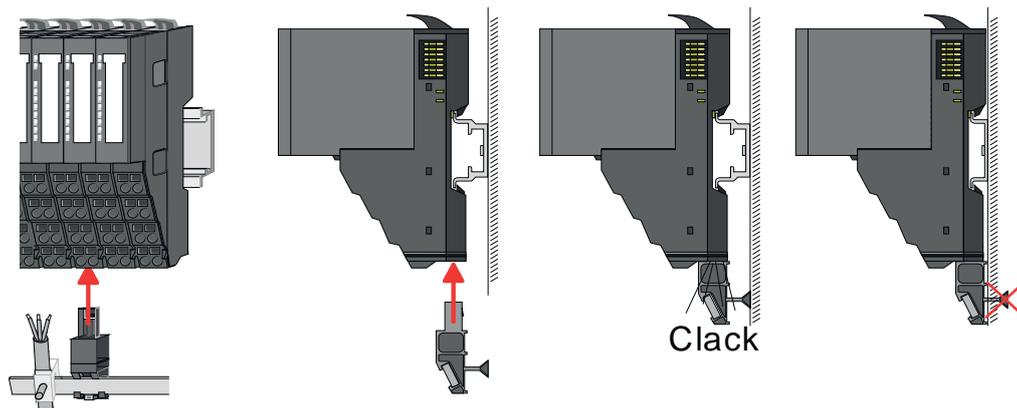
Über den *Terminal-Block* werden Signal- und Versorgungsleitungen mit dem Modul verbunden. Bei der Montage des Terminal-Block wird dieser an der Unterseite der Elektronik-Einheit eingehängt und zur Elektronik-Einheit geklappt, bis dieser einrastet. Bei der Verdrahtung kommt eine "push-in"-Federklemmtechnik zum Einsatz. Diese ermöglicht einen werkzeuglosen und schnellen Anschluss Ihrer Signal- und Versorgungsleitungen. Das Abklemmen erfolgt mittels eines Schraubendrehers.

**2.2.2.1 Zubehör
Schirmschienen-Träger**

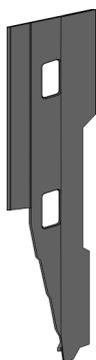


i Bitte beachten Sie, dass an der CPU iC921xM-x und einem 16x-Peripherie-Modul kein Schirmschienen-Träger montiert werden kann!

Der Schirmschienen-Träger (Best.-Nr.: 000-0AB00) dient zur Aufnahme von Schirmschienen (10mm x 3mm) für den Anschluss von Kabelschirmen. Schirmschienen-Träger, Schirmschiene und Kabelschirmbefestigungen sind nicht im Lieferumfang enthalten, sondern ausschließlich als Zubehör erhältlich. Der Schirmschienen-Träger wird unterhalb des Klemmblocks in das Terminal-Modul gesteckt. Bei flacher Tragschiene können Sie zur Adaption die Abstandshalter am Schirmschienen-Träger abrechnen.



Bus-Blende



Bei jedem Kopf-Modul gehört zum Schutz der Bus-Kontakte eine Bus-Blende zum Lieferumfang. Vor der Montage von System SLIO Modulen ist die Bus-Blende am Kopf-Modul zu entfernen. Zum Schutz der Bus-Kontakte müssen Sie die Bus-Blende immer am äußersten Modul montieren. Die Bus-Blende hat die Best.-Nr. 000-0AA00.

Kodier-Stecker



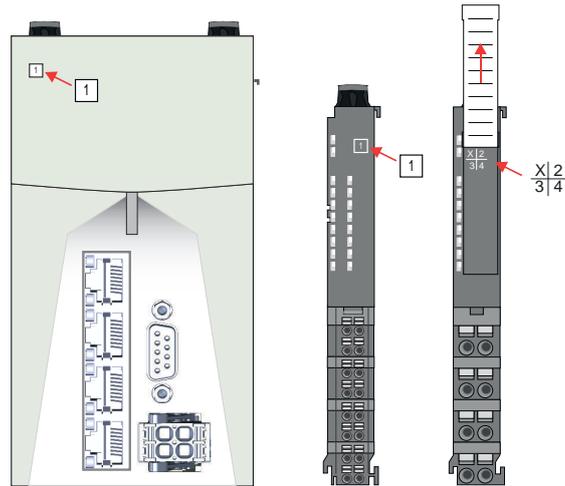
Bitte beachten Sie, dass an einem 16x-Peripherie-Modul kein Kodier-Stecker montiert werden kann! Hier müssen Sie selbst dafür Sorge tragen, dass bei einem Tausch der Elektronik-Einheit der zugehörige Terminal-Block wieder gesteckt wird.

Sie haben die Möglichkeit die Zuordnung von Terminal- und Elektronik-Modul zu fixieren. Hierbei kommen Yaskawa-Kodier-Stecker (Best-Nr.: 000-0AC00) zum Einsatz. Die Kodier-Stecker bestehen aus einem Kodierstift-Stift und einer Kodier-Buchse, wobei durch Zusammenfügen von Elektronik- und Terminal-Modul der Kodier-Stift am Terminal-Modul und die Kodier-Buchse im Elektronik-Modul verbleiben. Dies gewährleistet, dass nach Austausch des Elektronik-Moduls nur wieder ein Elektronik-Modul mit der gleichen Kodierung gesteckt werden kann.

Abmessungen

2.2.3 Hardware-Ausgabestand

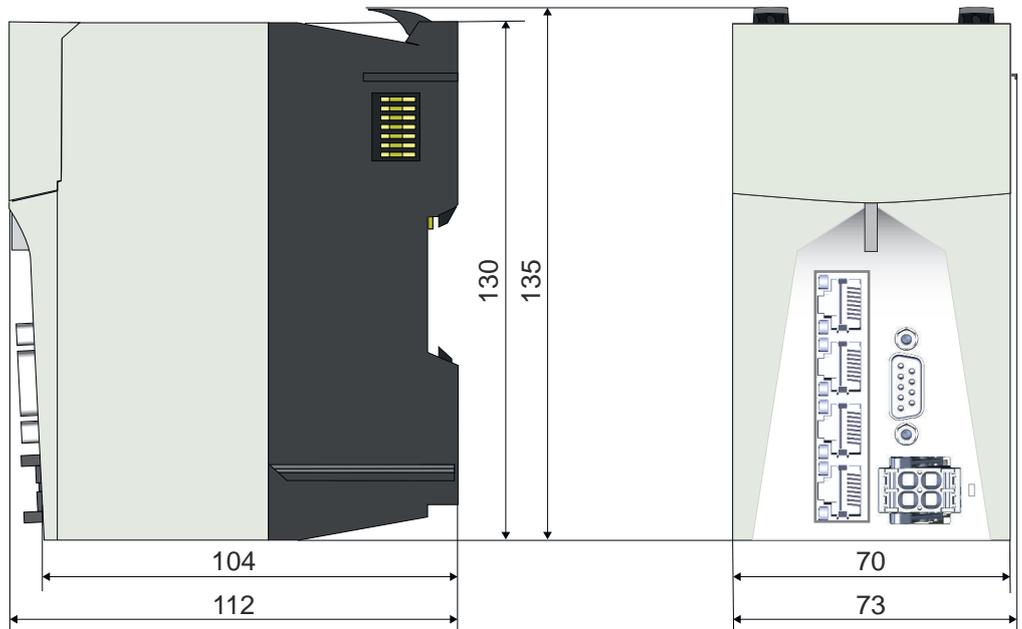
- Auf jedem Modul ist der Hardware-Ausgabestand aufgedruckt.
- Da ein System SLIO 8x-Peripherie-Modul aus Terminal- und Elektronik-Modul besteht, finden Sie auf diesen jeweils einen Hardware-Ausgabestand aufgedruckt.
- Maßgebend für den Hardware-Ausgabestand eines System SLIO Moduls ist der Hardware-Ausgabestand des Elektronik-Moduls. Dieser befindet sich immer unter dem Beschriftungsstreifen des entsprechenden Elektronik-Moduls.
- Abhängig vom Modultyp gibt es folgende 2 Varianten für die Darstellung beispielsweise von Hardware Ausgabestand 1:
 - Mit aktueller Beschriftung befindet sich eine **1** auf der Front.
 - Mit älterer Beschriftung ist auf einem Zahlenraster die 1 mit "X" gekennzeichnet.



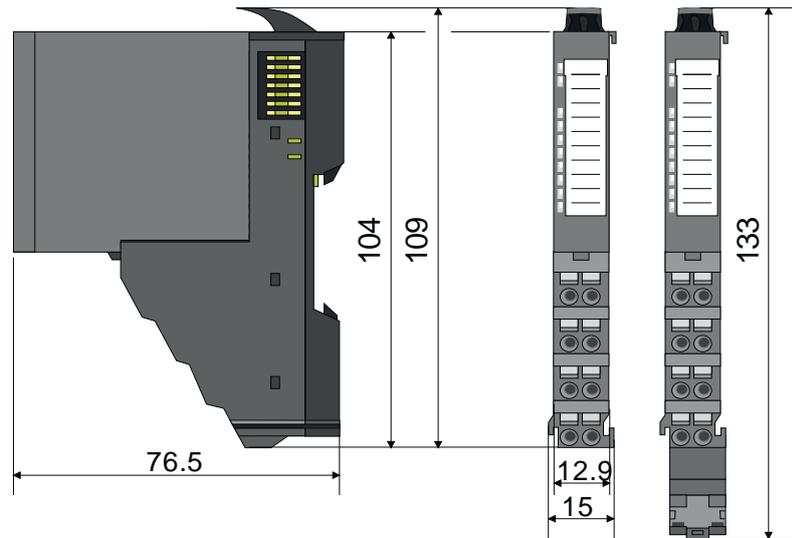
2.3 Abmessungen

CPU iC921xM-x

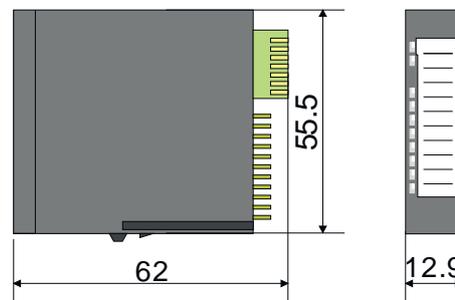
Alle Maße sind in mm angegeben.



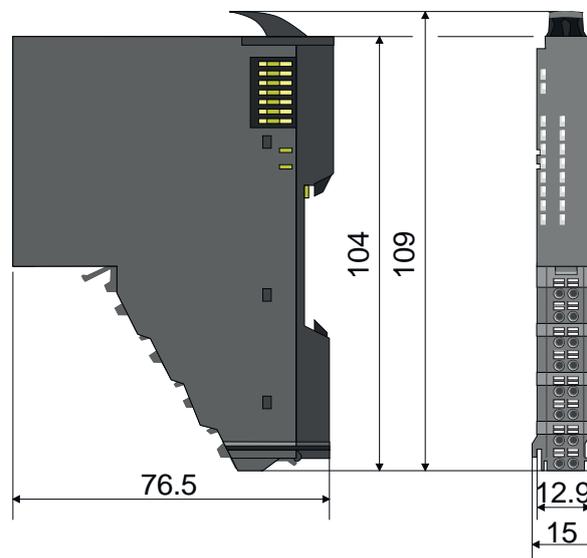
8x-Peripherie-Modul



Elektronik-Modul



16x-Peripherie-Modul



2.4 Montage



WARNUNG

Unbeabsichtigter Maschinenanlauf

- Führen Sie die Montage bzw. Demontage nicht unter Spannung durch!
- Schalten Sie vor der Montage bzw. Demontage die CPU spannungsfrei und sichern Sie die Spannung gegen Wiedereinschalten!
- Schalten Sie die Spannung erst zu, wenn das System vollständig aufgebaut ist. Beachten Sie hierbei Diagnoseanzeigen und eventuelle Diagnosesmeldungen.
- Der Start der Maschine/Anlage darf erst dann erfolgen, wenn keine Gefährdung von der Maschine/Anlage ausgehen kann.



HINWEIS

Elektronikschaden durch ungenügende externe Absicherung – Kein sicheres Auslösen im Fehlerfall

Durch eine ungenügende externe Absicherung entstehen Elektronikschäden an der CPU.

- Sichern Sie die Versorgungsspannung entsprechend der angeschlossenen Last (Anzahl der System SLIO F-Teilnehmer/Summe der Stromaufnahmen jedes Teilnehmers) extern ab.
- Gewährleisten Sie ein sicheres Auslösen der externen Sicherung.
- Falls Sie eine Schmelzsicherung verwenden, muss das Netzteil den vierfachen Nennstrom der Schmelzsicherung liefern können. Damit ist ein sicheres Auslösen im Fehlerfall gewährleistet.



HINWEIS

Beschädigung durch unsachgemäße Handhabung

- Gehen Sie sorgfältig mit der CPU und den Komponenten um!
- Beachten Sie bei der Installation der CPU und der Komponenten, dass mechanische Beschädigungen vermieden werden!



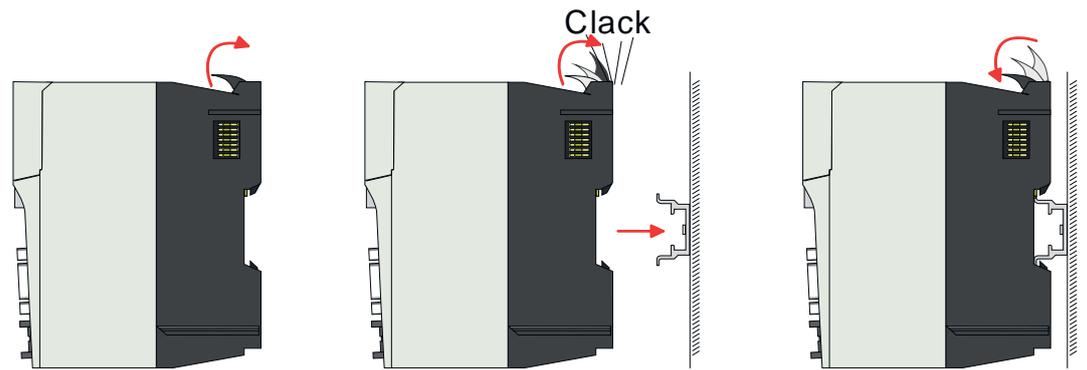
Hinweis zur Montage

- *Montieren Sie die CPU im geschlossenen Schaltschrank oder Schaltkasten der Schutzart IP54 oder höher auf einer 35 mm Standardtragschiene.*
- *Verwenden Sie eine Tragschiene nach EN 60715.*

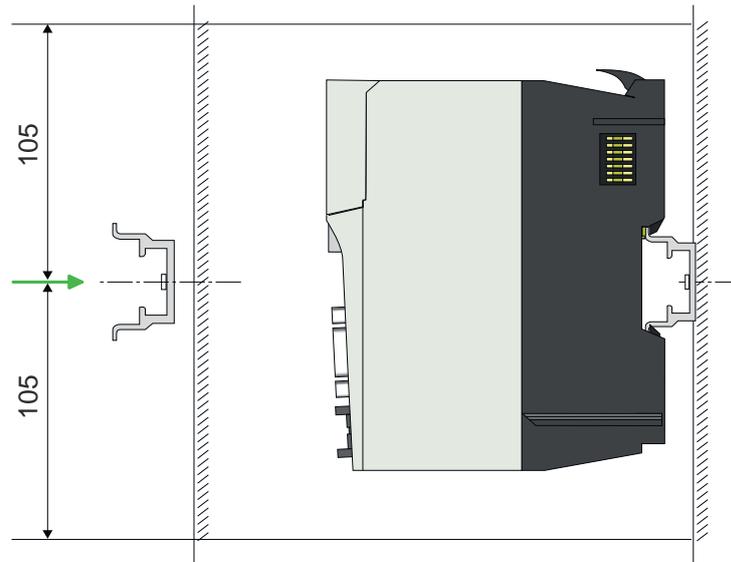
2.4.1 Montage CPU

Funktionsprinzip

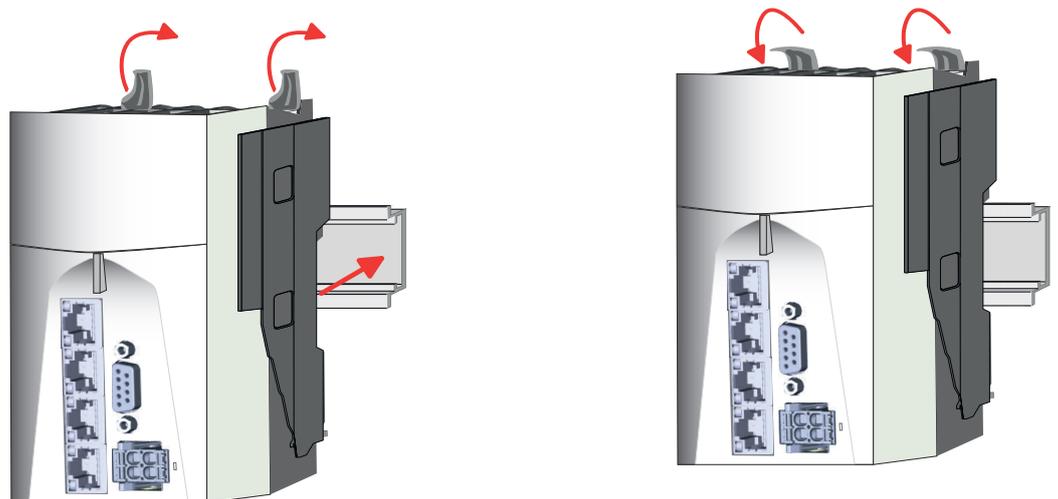
Die CPU besitzt Verriegelungshebel an der Oberseite. Zur Montage und Demontage sind diese Hebel nach oben zu drücken, bis diese einrasten. Stecken Sie die CPU auf die Tragschiene. Durch Klappen der Verriegelungshebel nach unten wird die CPU auf der Tragschiene fixiert. Die CPU wird direkt auf eine Tragschiene montiert. Sie können bis zu 64 System SLIO Module stecken. Über die Verbindung mit dem Rückwandbus wird die Elektronikversorgung für die Module angebunden. Für die Leistungsversorgung der Module ist immer das Power-Modul 007-1AB00 zu montieren.



Vorgehensweise



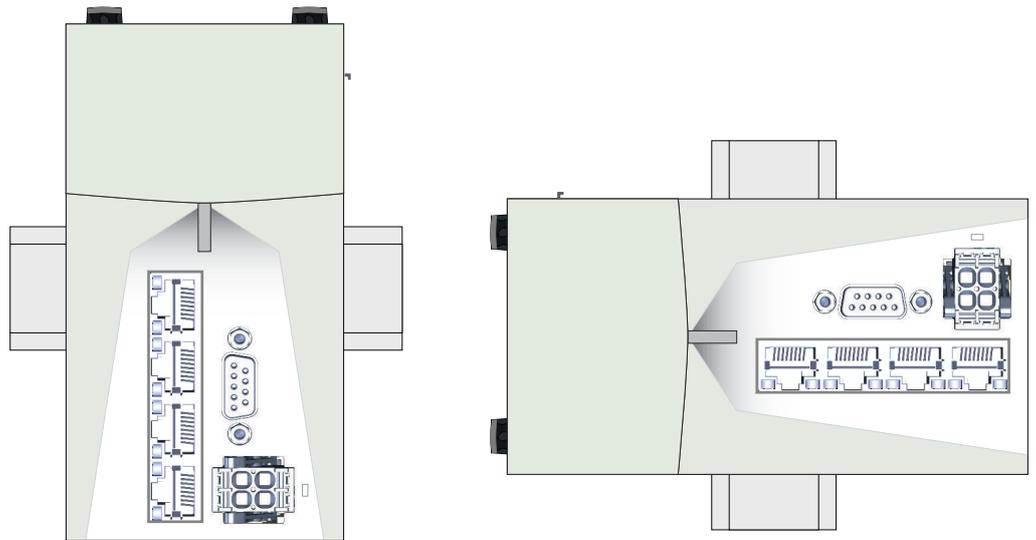
1. → Montieren Sie die Tragschiene! Bitte beachten Sie, dass Sie von der Mitte der Tragschiene nach oben und nach unten einen Montageabstand von mindestens 105mm einhalten.



2. → Klappen Sie die Verriegelungshebel der CPU nach oben, stecken Sie die CPU auf die Tragschiene und klappen Sie die Verriegelungshebel wieder nach unten.
 - ➔ Sofern Sie die CPU ohne Peripherie-Module betreiben möchten, können Sie diese jetzt verdrahten.

Montagemöglichkeiten

Horizontal hängend oder vertikal hängend:

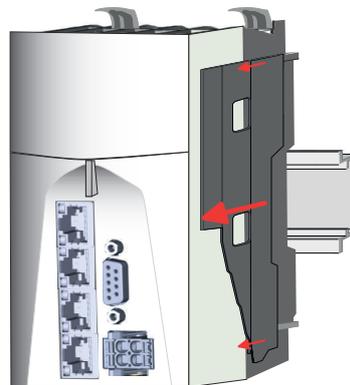


2.4.2 Montage Peripherie-Module

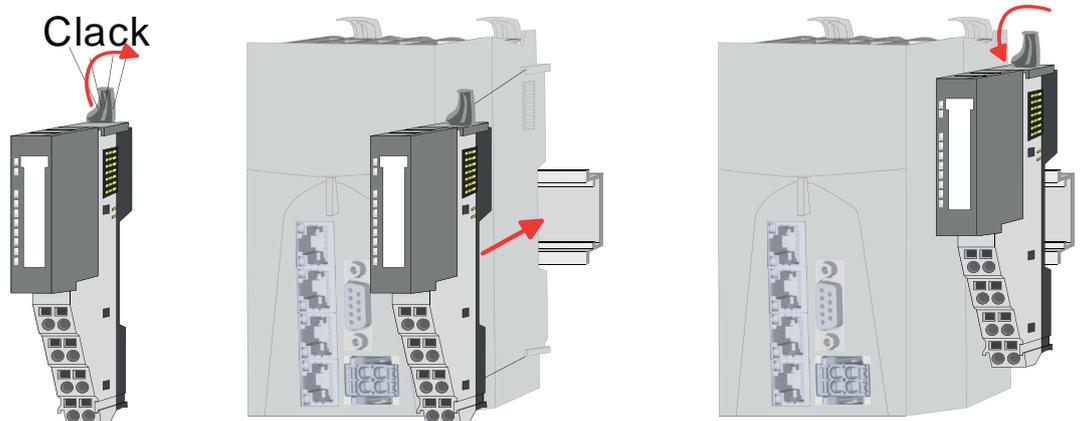


Beim Einsatz von System SLIO Modulen müssen Sie immer das Power-Modul 007-1AB00 - DC 24V 10A montieren, da die CPU systembedingt keine Leistungsversorgung bereit stellt.

Montage Power Modul 007-1AB00



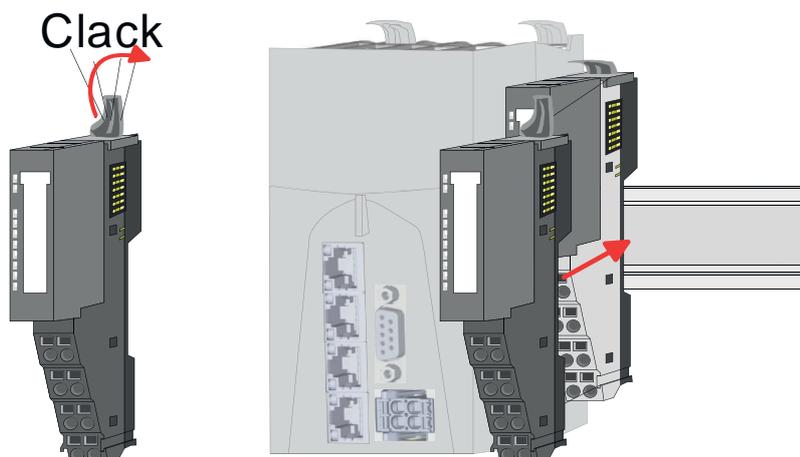
1. Entfernen Sie vor der Montage der Peripherie-Module die Bus-Blende auf der rechten Seite der CPU, indem Sie diese nach vorn abziehen. Bewahren Sie die Blende für spätere Montage auf.



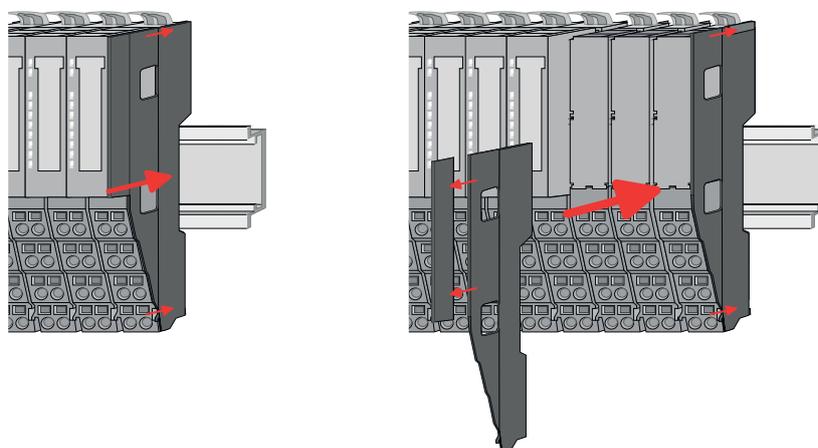
2. Montieren Sie die gewünschten Peripherie-Module.

Montage Peripherie-Module

Die Vorgehensweise ist für 8x- und 16x-Peripherie-Module identisch.



1. → Montieren Sie die gewünschten Peripherie-Module.



2. → Nachdem Sie Ihr Gesamt-System montiert haben, müssen Sie zum Schutz der Bus-Kontakte die Bus-Blende am äußersten Modul wieder stecken. Handelt es sich bei dem äußersten Modul um ein Klemmen-Modul, so ist zur Adaption der obere Teil der Bus-Blende abzubrechen.

→ Das System kann jetzt verdrahtet werden.

2.5 Verdrahtung**VORSICHT****Temperatur externer Kabel beachten!**

Aufgrund der Wärmeableitung des Systems kann die Temperatur externer Kabel ansteigen. Aus diesem Grund muss die Spezifikation der Temperatur für die Verkabelung 5°C über der Umgebungstemperatur gewählt werden!

**VORSICHT****Elektrische Sicherheit - Verlust der Sicherheitsfunktion beim Einsatz nicht geeigneter Stromversorgungen**

- An die CPU dürfen nur Geräte angeschlossen werden, die eine sichere Trennung zum 230V Netz aufweisen.
- Das Netzteil zur Erzeugung der DC 24V Versorgung muss den Anforderungen für PELV/SELV gemäß EN 50178 entsprechen. In diesen wird ein Kurzschluss zwischen Primär- und Sekundärseite ausgeschlossen.

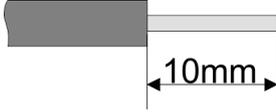
Verdrahtung > Verdrahtung CPU

2.5.1 Verdrahtung CPU

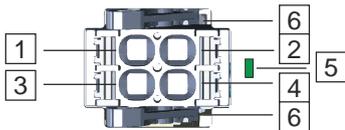
CPU-Steckverbinder

Für die Spannungsversorgung besitzt die CPU einen abnehmbaren Steckverbinder. Bei der Verdrahtung des Steckverbinders kommt eine "push-in"-Federklemmtechnik zum Einsatz. Diese ermöglicht einen werkzeuglosen und schnellen Anschluss Ihrer Versorgungsleitungen. Das Abklemmen der Leitungen erfolgt mittels eines Schraubendrehers.

Daten

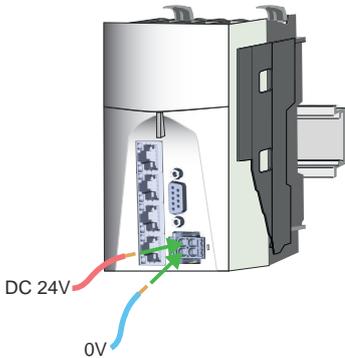


U_{max}	30V DC
I_{max}	10A
Querschnitt	0,08 ... 1,5mm ² (AWG 28 ... 16)
Abisolierlänge	10mm



- 1, 2 Pluspol DC 24V Spannungsversorgung, im Stecker gebrückt.
- 3, 4 Masse DC 24V Spannungsversorgung, im Stecker gebrückt.
- 5 LED-Anzeige für Spannungsversorgung.
- 6 Entriegelung

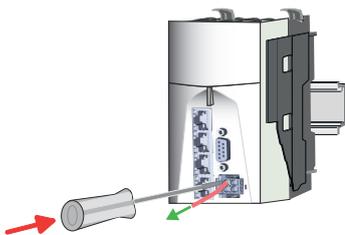
Draht stecken



Die Verdrahtung erfolgt werkzeuglos.

1. Führen Sie durch die runde Anschlussöffnung des entsprechenden Kontakts Ihren vorbereiteten Draht bis zum Anschlag ein, so dass dieser fixiert wird.
 - ➔ Durch das Einschieben öffnet die Kontaktfeder und sorgt somit für die erforderliche Anpresskraft.
2. Ermitteln Sie gemäß Pinbelegung die Anschlussposition.
3. Schließen Sie an Pin 1 oder Pin 2 den Plus-Pol (+) Ihrer externen DC 24V Spannungsversorgung an.
4. Schließen Sie an Pin 3 oder Pin 4 den Minus-Pol (0V) Ihrer externen DC 24V Spannungsversorgung an.
 - ➔ Sobald die CPU mit Spannung versorgt wird, leuchtet die zugehörige LED.

Draht entfernen

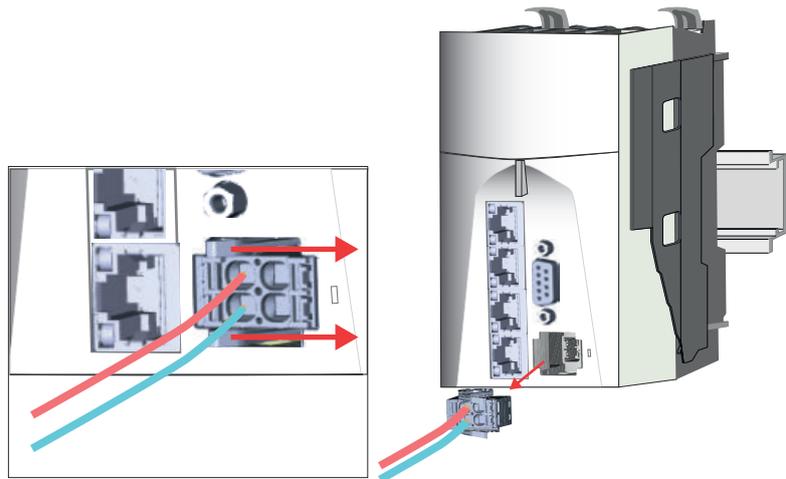


Das Entfernen eines Drahtes erfolgt mittels eines Schraubendrehers mit 2,5mm Klingbreite.

1. Drücken Sie mit dem Schraubendreher senkrecht auf die Entriegelung.
 - ➔ Die Kontaktfeder gibt den Draht frei.
2. Ziehen Sie den Draht aus der runden Öffnung heraus.

Steckverbinder entfernen

Sie haben die Möglichkeit z.B. für einen Modulwechsel bei stehender Verdrahtung den Steckverbinder der Spannungsversorgung zu entfernen. Hierzu besitzt dieser eine Entriegelung. Das Entfernen des Steckverbinders erfolgt nach folgender Vorgehensweise:



1. Steckverbinder entfernen:
Durch Betätigen der Entriegelung wie gezeigt wird der Steckverbinder gelöst und kann entnommen werden.
2. Steckverbinder stecken:
Indem Sie den Steckverbinder direkt stecken und einrasten, kehren die Entriegelungshebel in die Ursprungslage zurück.

2.5.2 Verdrahtung System SLIO Peripherie



Beim Einsatz von System SLIO Modulen müssen Sie immer das Power-Modul 007-1AB00 - DC 24V 10A montieren, da die CPU systembedingt keine Leistungsversorgung bereit stellt.

2.5.2.1 Verdrahtung Power-Modul

Terminal-Modul Anschlussklemmen

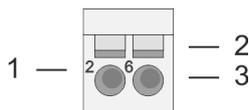
Bei der Verdrahtung des Power-Moduls kommen Anschlussklemmen mit Federklemmtechnik zum Einsatz. Die Verdrahtung mit Federklemmtechnik ermöglicht einen schnellen und einfachen Anschluss Ihrer Versorgungsleitungen. Im Gegensatz zur Schraubverbindung ist diese Verbindungsart erschütterungssicher.

Daten

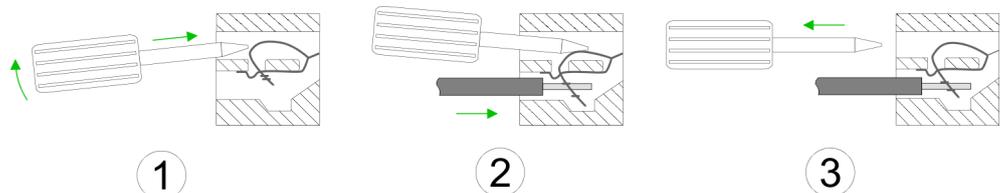


U_{max}	30V DC
I_{max}	10A
Querschnitt	0,08 ... 1,5mm ² (AWG 28 ... 16)
Abisolierlänge	10mm

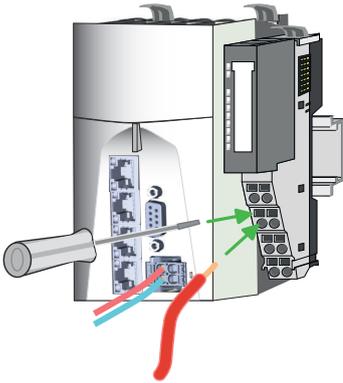
Verdrahtung Vorgehensweise



- 1 Pin-Nr. am Steckverbinder
- 2 Entriegelung für Schraubendreher
- 3 Anschlussöffnung für Draht

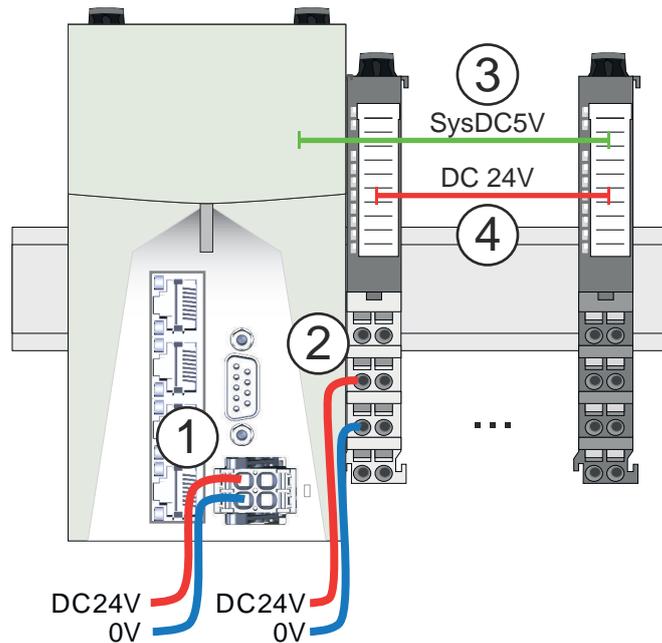


Verdrahtung > Verdrahtung System SLIO Peripherie



1. ➔ Zum Verdrahten stecken Sie, wie in der Abbildung gezeigt, einen passenden Schraubendreher leicht schräg in die rechteckige Öffnung. Zum Öffnen der Kontaktfeder müssen Sie den Schraubendreher in die entgegengesetzte Richtung drücken und halten.
2. ➔ Führen Sie durch die runde Öffnung Ihren abisolierten Draht ein. Sie können Drähte mit einem Querschnitt von 0,08mm² bis 1,5mm² anschließen.
3. ➔ Durch Entfernen des Schraubendrehers wird der Draht über einen Federkontakt sicher mit der Anschlussklemme verbunden.

Standard-Verdrahtung



- (1) DC 24V Versorgung CPU:
DC 5V Elektronikversorgung I/O-Ebene (max. 2A)
- (2) Power-Modul 007-1AB00:
DC 24V Leistungsversorgung I/O-Ebene (max. 10A)
- (3) DC 5V Elektronikversorgung der I/O-Ebene
- (4) DC 24V Leistungsversorgung der I/O-Ebene



VORSICHT

Da die Leistungsversorgung keine interne Absicherung besitzt, ist diese extern mit einer Sicherung entsprechend dem Maximalstrom abzusichern, d.h. max. 10A mit einer 10A-Sicherung (flink) bzw. einem Leitungsschutzschalter 10A Charakteristik Z!

Absicherung

- Die Leistungsversorgung ist extern mit einer Sicherung entsprechend dem Maximalstrom abzusichern, d.h. max. 10A mit einer 10A-Sicherung (flink) bzw. einem Leitungsschutzschalter 10A Charakteristik Z.
- Es wird empfohlen die Elektronikversorgung für die CPU und die I/O-Ebene extern mit einer 2A-Sicherung (flink) bzw. einem Leitungsschutzschalter 2A Charakteristik Z abzusichern.

Zustand der Elektronikversorgung über LEDs

Nach PowerON leuchtet an jedem System SLIO Modul die RUN- bzw. MF-LED, sofern der Summenstrom für die Elektronikversorgung den Maximalwert nicht übersteigt. Bei der CPU beträgt dieser 3A. Ist der Summenstrom größer als der Maximalwert, werden die LEDs nicht mehr angesteuert. Hier müssen Sie zwischen Ihre Peripherie-Module das Power-Modul mit der Best.-Nr. 007-1AB10 platzieren.

2.5.2.2 Verdrahtung 8x-Peripherie-Module

Terminal-Modul Anschlussklemmen



VORSICHT

Keine gefährliche Spannungen anschließen!

Sofern dies nicht ausdrücklich bei der entsprechenden Modulbeschreibung vermerkt ist, dürfen Sie an dem entsprechenden Terminal-Modul keine gefährlichen Spannungen anschließen!



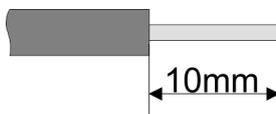
VORSICHT

Verletzungsgefahr durch Stromschlag und Beschädigung der CPU bzw. der Module möglich!

Setzen Sie das iC9200 Series in einen sicheren, spannungslosen Zustand, bevor Sie mit der Montage, Demontage oder Verdrahtung der iC9200 Series Module beginnen!

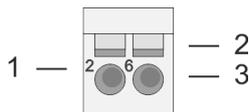
Bei der Verdrahtung von Terminal-Modulen kommen Anschlussklemmen mit Federklemmtechnik zum Einsatz. Die Verdrahtung mit Federklemmtechnik ermöglicht einen schnellen und einfachen Anschluss Ihrer Signal- und Versorgungsleitungen. Im Gegensatz zur Schraubverbindung ist diese Verbindungsart erschütterungssicher.

Daten

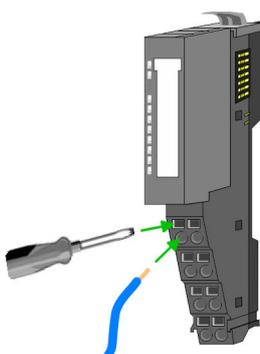
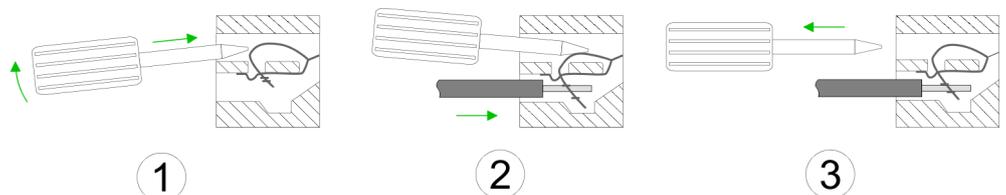


U_{max}	240V AC / 30V DC
I_{max}	10A
Querschnitt	0,08 ... 1,5mm ² (AWG 28 ... 16)
Abisolierlänge	10mm

Verdrahtung Vorgehensweise



- 1 Pin-Nr. am Steckverbinder
- 2 Entriegelung für Schraubendreher
- 3 Anschlussöffnung für Draht

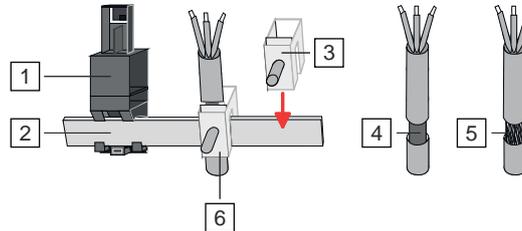


1. Zum Verdrahten stecken Sie, wie in der Abbildung gezeigt, einen passenden Schraubendreher leicht schräg in die rechteckige Öffnung. Zum Öffnen der Kontaktfeder müssen Sie den Schraubendreher in die entgegengesetzte Richtung drücken und halten.
2. Führen Sie durch die runde Öffnung Ihren abisolierten Draht ein. Sie können Drähte mit einem Querschnitt von 0,08mm² bis 1,5mm² anschließen.
3. Durch Entfernen des Schraubendrehers wird der Draht über einen Federkontakt sicher mit der Anschlussklemme verbunden.

2.5.2.2.1 Schirmung

Übersicht

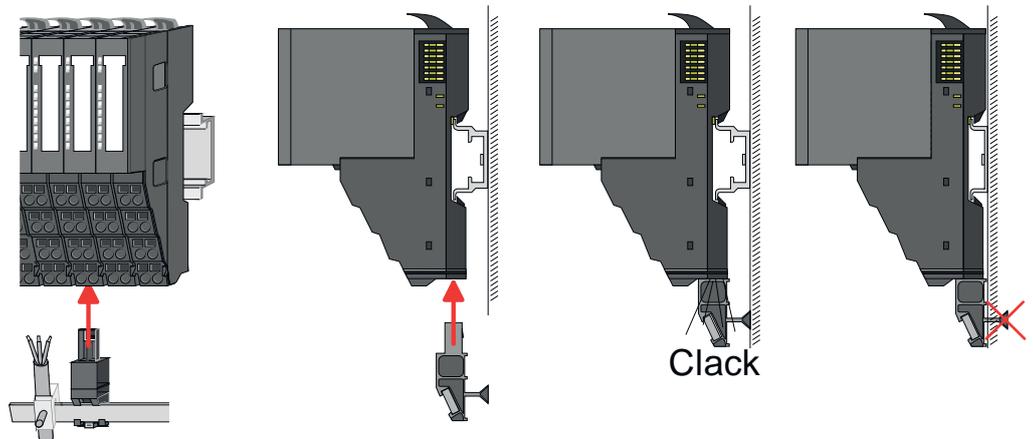
Für eine störungsfreie Signalübertragung ist eine Schirmung erforderlich. Hierdurch werden elektrisch, magnetische oder elektromagnetische Störfelder geschwächt. Zur Schirmaufgabe ist die Montage von Schirmschienen-Trägern erforderlich. Der Schirmschienen-Träger (als Zubehör erhältlich) dient zur Aufnahme der Schirmschiene für den Anschluss von Kabelschirmen. → "Aufbaurichtlinien"...Seite 54



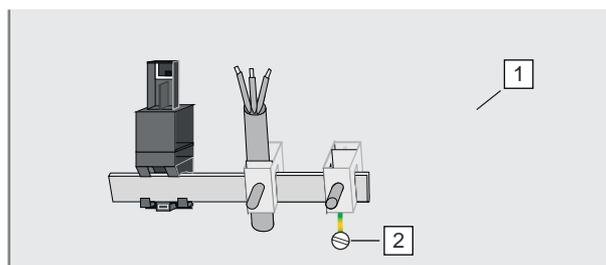
- 1 Schirmschienen-Träger
- 2 Schirmschiene (10mm x 3mm)
- 3 Schirmanschlussklemme
- 4 Kabelschirm mit Metallfolie
- 5 Kabelschirm mit Drahtgeflecht (engmaschig)
- 6 Kabelschirm mit Schirmanschlussklemme montiert

Schirm auflegen

1. Jedes iC9200 Series 8x-Peripherie-Modul besitzt an der Unterseite Aufnehmer für Schirmschienen-Träger. Stecken Sie Ihre Schirmschienen-Träger, bis diese am Modul einrasten. Bei flacher Tragschiene können Sie zur Adaption den Abstandshalter am Schirmschienen-Träger abbrechen.
2. Legen Sie Ihre Schirmschiene in den Schirmschienen-Träger ein.



3. Legen Sie ihre Kabel mit dem entsprechend abisolierten Kabelschirm auf und verbinden Sie diese über die Schirmanschlussklemme mit der Schirmschiene.
4. Die Schirmschiene ist immer zu erden. Halten Sie alle Kabel-Verbindung möglichst kurz. Zur Erdung der Schirmschiene schließen Sie einen PE-Leiter über eine Schirmanschlussklemme an der Schirmschiene an und verschrauben Sie diesen möglichst nahe und impedanzarm mit der Grundplatte.



- 1 Grundplatte
- 2 PE-Leiter verschraubt mit Grundplatte

2.5.2.3 Verdrahtung 16x-Peripherie-Module

Terminal-Block Anschlussklemmen

**VORSICHT****Keine gefährliche Spannungen anschließen!**

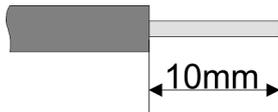
Sofern dies nicht ausdrücklich bei der entsprechenden Modulbeschreibung vermerkt ist, dürfen Sie an dem entsprechenden Terminal-Block keine gefährlichen Spannungen anschließen!

**VORSICHT****Verletzungsgefahr durch Stromschlag und Beschädigung der CPU bzw. der Module möglich!**

Setzen Sie das iC9200 Series in einen sicheren, spannungslosen Zustand, bevor Sie mit der Montage, Demontage oder Verdrahtung der iC9200 Series Module beginnen!

- Für die Verdrahtung besitzt das 16x-Peripherie-Modul einen abnehmbaren Terminal-Block.
- Bei der Verdrahtung des Terminal-Blocks kommt eine "push-in"-Federklemmtechnik zum Einsatz. Diese ermöglicht einen werkzeuglosen und schnellen Anschluss Ihrer Signal- und Versorgungsleitungen.
- Das Abklemmen erfolgt mittels eines Schraubendrehers.
- Bitte verwenden Sie ausschließlich Kupferdraht!

Daten



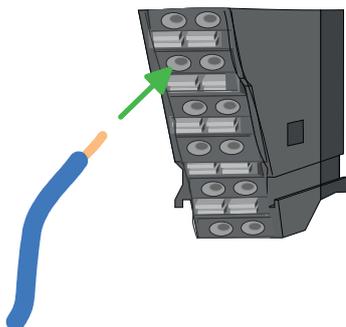
U_{max}	30V DC
I_{max}	10A
Querschnitt fester Draht	0,25 ... 0,75mm ²
Querschnitt mit Aderendhülse	0,14 ... 0,75mm ²
Drahttyp	CU
AWG	24 ... 16
Abisolierlänge	10mm

Verdrahtung Vorgehensweise

- 1 Entriegelung
- 2 Anschlussöffnung für Draht



Draht stecken



Die Verdrahtung erfolgt werkzeuglos.

1. Ermitteln Sie gemäß der Gehäusebeschriftung die Anschlussposition.
2. Führen Sie durch die runde Anschlussöffnung des entsprechenden Kontakts Ihren vorbereiteten Draht bis zum Anschlag ein, so dass dieser fixiert wird.
 - ➔ Durch das Einschieben öffnet die Kontaktfeder und sorgt somit für die erforderliche Anpresskraft.

Draht entfernen



Das Entfernen eines Drahtes erfolgt mittels eines Schraubendrehers mit 2,5mm Klingbreite.

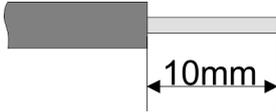
1. Drücken Sie mit dem Schraubendreher senkrecht auf die Entriegelung.
 - ➔ Die Kontaktfeder gibt den Draht frei.
2. Ziehen Sie den Draht aus der runden Öffnung heraus.

2.5.2.4 Verdrahtung Power-Module

Terminal-Modul Anschlussklemmen

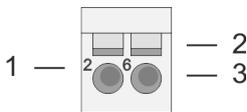
Power-Module können zwischen die Peripherie-Module gesteckt werden. Bei der Verdrahtung von Power-Modulen kommen Anschlussklemmen mit Federklemmtechnik zum Einsatz. Die Verdrahtung mit Federklemmtechnik ermöglicht einen schnellen und einfachen Anschluss Ihrer Signal- und Versorgungsleitungen. Im Gegensatz zur Schraubverbindung ist diese Verbindungsart erschütterungssicher.

Daten

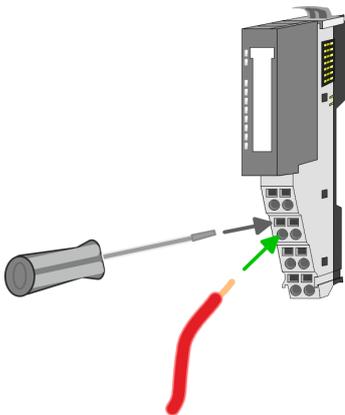
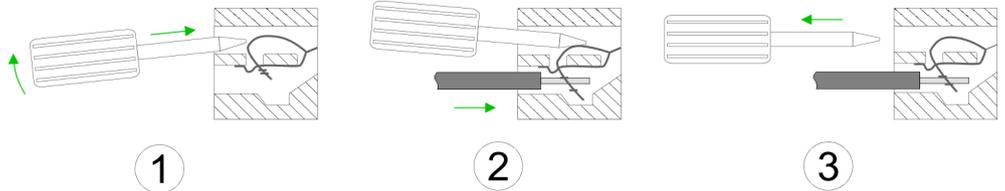


U_{max}	30V DC
I_{max}	10A
Querschnitt	0,08 ... 1,5mm ² (AWG 28 ... 16)
Abisolierlänge	10mm

Verdrahtung Vorgehensweise



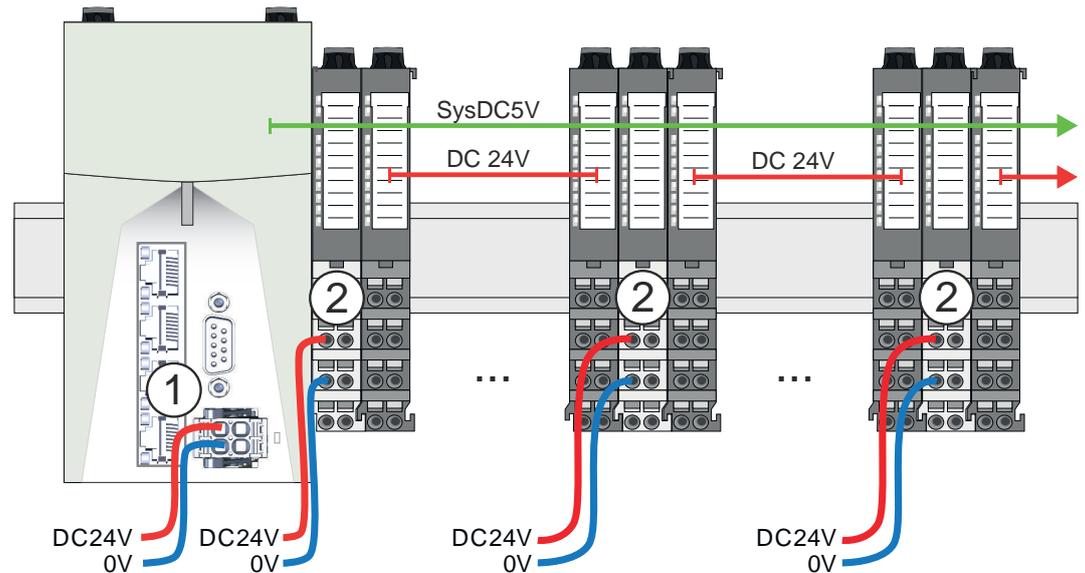
- 1 Pin-Nr. am Steckverbinder
- 2 Entriegelung für Schraubendreher
- 3 Anschlussöffnung für Draht



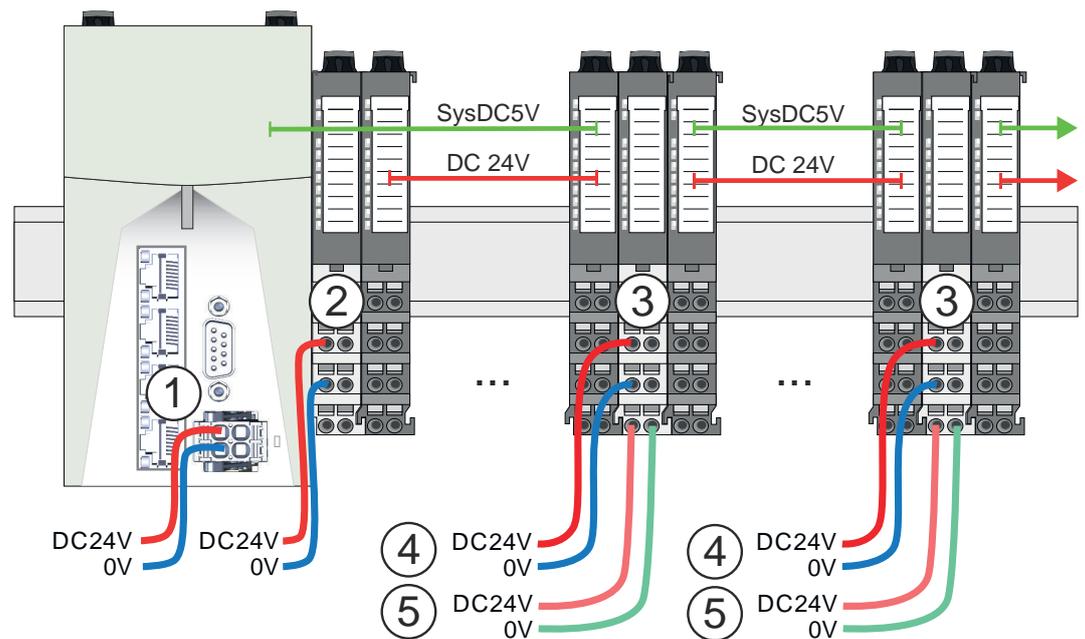
1. Zum Verdrachten stecken Sie, wie in der Abbildung gezeigt, einen passenden Schraubendreher leicht schräg in die rechteckige Öffnung. Zum Öffnen der Kontaktfeder müssen Sie den Schraubendreher in die entgegengesetzte Richtung drücken und halten.
2. Führen Sie durch die runde Öffnung Ihren abisolierten Draht ein. Sie können Drähte mit einem Querschnitt von 0,08mm² bis 1,5mm² anschließen.
3. Durch Entfernen des Schraubendrehers wird der Draht über einen Federkontakt sicher mit der Anschlussklemme verbunden.

Einsatz von Power-Modulen

- Die CPU stellt keine Leistungsversorgung für die Peripherie-Module bereit. Durch Stecken des Power-Moduls mit der Best.-Nr. 007-1AB00 erhalten die nachfolgenden Peripherie-Module eine DC 24V Leistungsversorgung mit max. 10A. Reichen die 10A nicht mehr aus, ist ein weiteres Power-Modul zu stecken. Sie haben so auch die Möglichkeit, Potenzialgruppen zu bilden.
- Die Peripherie-Module erhalten Ihre Elektronikversorgung von der CPU mit max. 3A. Das Power-Modul mit der Best.-Nr. 007-1AB10 setzen Sie ein, wenn die 3A für die Elektronikversorgung am Rückwandbus nicht mehr ausreichen. Zusätzlich erhalten Sie eine neue Potenzialgruppe für die DC 24V Leistungsversorgung mit max. 4A.
- Durch Stecken des Power-Moduls 007-1AB10 können am nachfolgenden Rückwandbus Module gesteckt werden mit einem maximalen Summenstrom der Leistungsversorgung von 2A. Danach ist wieder ein Power-Modul zu stecken. Zur Sicherstellung der Spannungsversorgung dürfen die Power-Module beliebig gemischt eingesetzt werden.

Power-Modul 007-1AB00

- (1) DC 24V Versorgung CPU:
DC 5V Elektronikversorgung I/O-Ebene (max. 2A)
- (2) Power-Modul 007-1AB00:
DC 24V Leistungsversorgung I/O-Ebene (max. 10A)

Power-Modul 007-1AB10

- (1) DC 24V Versorgung CPU:
DC 5V Elektronikversorgung I/O-Ebene (max. 2A)
- (2) Power-Modul 007-1AB00:
DC 24V Leistungsversorgung I/O-Ebene (max. 10A)
- (3) Zusätzliches Power-Modul 007-1AB10:
- (4) DC 24V Leistungsversorgung I/O-Ebene (max. 4A)
- (5) DC 5V Elektronikversorgung I/O-Ebene (max. 2A)

**VORSICHT**

Da die Leistungsversorgung keine interne Absicherung besitzt, ist diese extern mit einer Sicherung entsprechend dem Maximalstrom abzusichern, d.h. max. 10A mit einer 10A-Sicherung (flink) bzw. einem Leitungsschutzschalter 10A Charakteristik Z!



Die Elektronikversorgung ist intern gegen zu hohe Spannung durch eine Sicherung geschützt. Die Sicherung befindet sich innerhalb des Power-Moduls. Wenn die Sicherung ausgelöst hat, muss das Elektronik-Modul getauscht werden!

Absicherung

- Die Leistungsversorgung ist extern mit einer Sicherung entsprechend dem Maximalstrom abzusichern, d.h. max. 10A mit einer 10A-Sicherung (flink) bzw. einem Leitungsschutzschalter 10A Charakteristik Z.
- Es wird empfohlen die Elektronikversorgung für die CPU und die I/O-Ebene extern mit einer 2A-Sicherung (flink) bzw. einem Leitungsschutzschalter 2A Charakteristik Z abzusichern.

Zustand der Elektronikversorgung über LEDs

Nach PowerON leuchtet an jedem System SLIO Modul die RUN- bzw. MF-LED, sofern der Summenstrom für die Elektronikversorgung den Maximalwert nicht übersteigt. Bei der CPU beträgt dieser 3A. Ist der Summenstrom größer als der Maximalwert, werden die LEDs nicht mehr angesteuert. Hier müssen Sie zwischen Ihre Peripherie-Module das Power-Modul mit der Best.-Nr. 007-1AB10 platzieren.

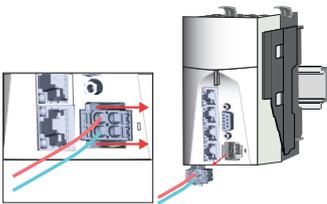
2.6 Demontage

2.6.1 Demontage CPU

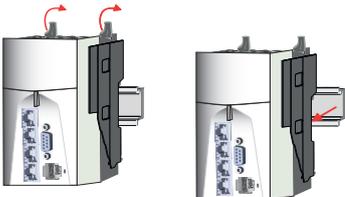
Demontage im Standalone-Betrieb



1. → Machen Sie Ihr System stromlos.

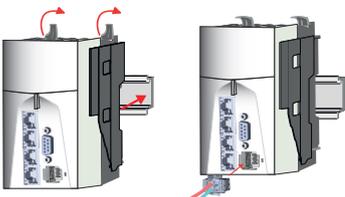


2. → Entfernen Sie den Steckverbinder der Spannungsversorgung der CPU. Durch Betätigen der Entriegelung wie gezeigt wird der Steckverbinder gelöst und kann entnommen werden.



3. → Klappen Sie die Verriegelungshebel der CPU nach oben.

4. → Ziehen Sie die CPU nach vorne ab.



5. → Klappen Sie die Verriegelungshebel der zu montierenden CPU nach oben, stecken Sie die CPU auf die Tragschiene und klappen Sie die Verriegelungshebel wieder nach unten.

6. → Stecken Sie wieder den Steckverbinder der Spannungsversorgung.

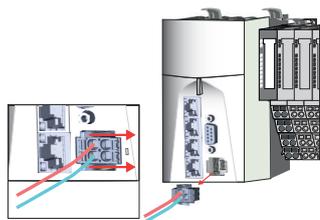


7. → Jetzt können Sie Ihr System wieder in Betrieb nehmen.

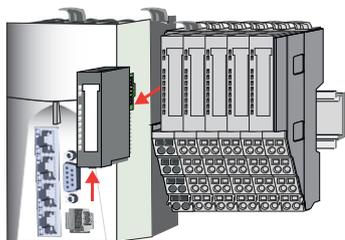
Demontage am System SLIO



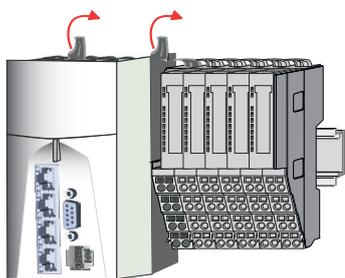
1. → Machen Sie Ihr System stromlos.



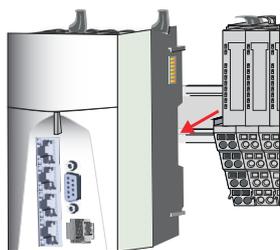
2. ➔ Entfernen Sie den Steckverbinder der Spannungsversorgung der CPU. Durch Betätigen der Entriegelung wie gezeigt wird der Steckverbinder gelöst und kann entnommen werden.



3. ➔ Aus montagetechnischen Gründen müssen Sie das Elektronik-Modul des rechts neben der CPU befindlichen Power-Moduls entfernen. Betätigen Sie hierzu die Entriegelung an der Unterseite des Power-Moduls und ziehen Sie dieses nach vorne ab.

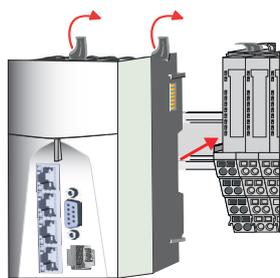


4. ➔ Klappen Sie alle Verriegelungshebel der zu tauschenden CPU nach oben.



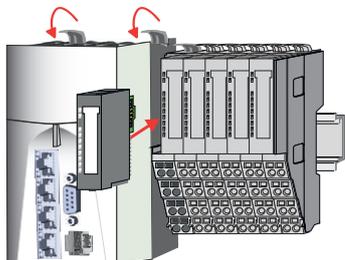
5. ➔ Ziehen Sie die CPU nach vorne ab.

6. ➔ Zur Montage klappen Sie alle Verriegelungshebel der zu montierenden CPU nach oben.



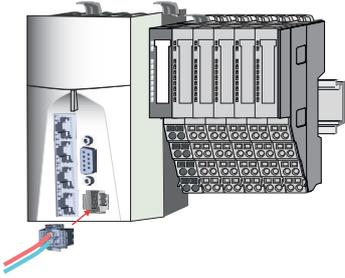
7. ➔ Stecken Sie die zu montierende CPU an das linke Modul und schieben Sie die CPU, geführt durch die Führungsleisten, auf die Tragschiene.

8. ➔ Klappen Sie alle Verriegelungshebel wieder nach unten.



9. ➔ Stecken Sie wieder das zuvor entnommene Elektronik-Modul. Für die Montage schieben Sie das Elektronik-Modul in die Führungsschiene, bis dieses an der Unterseite am Terminal-Modul einrastet.

Demontage > Demontage 8x-Peripherie-Module



11. ➔ Stecken Sie wieder den Steckverbinder der Spannungsversorgung.



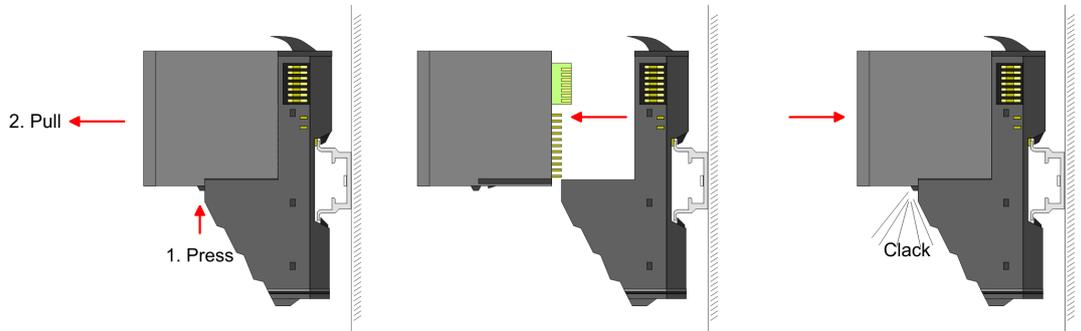
12. ➔ Jetzt können Sie Ihr System wieder in Betrieb nehmen.

2.6.2 Demontage 8x-Peripherie-Module

Vorgehensweise

Austausch eines Elektronik-Moduls

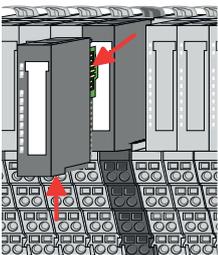
1. ➔ Machen Sie Ihr System stromlos.



2. ➔ Zum Austausch eines Elektronik-Moduls können Sie das Elektronik-Modul, nach Betätigung der Entriegelung an der Unterseite, nach vorne abziehen.

3. ➔ Für die Montage schieben Sie das neue Elektronik-Modul in die Führungsschiene, bis dieses an der Unterseite am Terminal-Modul einrastet.
➔ Jetzt können Sie Ihr System wieder in Betrieb nehmen.

Austausch eines Peripherie-Moduls



1. ➔ Machen Sie Ihr System stromlos.

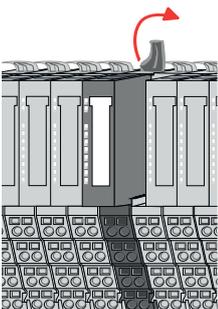
2. ➔ Entfernen Sie falls vorhanden die Verdrahtung am Modul.

3. ➔

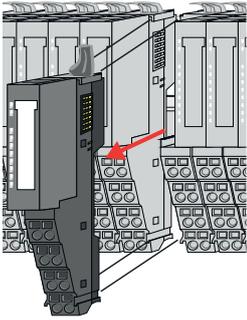


Bei der Demontage und beim Austausch eines (Kopf)-Moduls oder einer Modulgruppe müssen Sie aus montagetechnischen Gründen immer das rechts daneben befindliche Elektronik-Modul entfernen! Nach der Montage kann es wieder gesteckt werden.

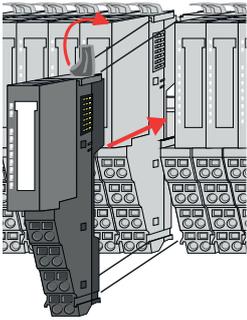
Betätigen Sie die Entriegelung an der Unterseite des rechts daneben befindlichen Elektronik-Moduls und ziehen Sie dieses nach vorne ab.



4. ➔ Klappen Sie den Verriegelungshebel des zu tauschenden Moduls nach oben.

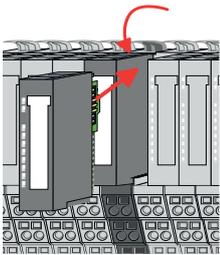


5. Ziehen Sie das Modul nach vorne ab.
6. Zur Montage klappen Sie den Verriegelungshebel des zu montierenden Moduls nach oben.



7. Stecken Sie das zu montierende Modul in die Lücke zwischen die beiden Module und schieben Sie das Modul, geführt durch die Führungsleisten auf beiden Seiten, auf die Tragschiene.

8. Klappen Sie den Verriegelungshebel wieder nach unten.

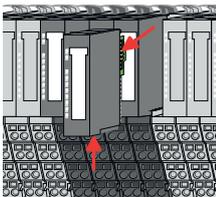


9. Stecken Sie wieder das zuvor entnommene Elektronik-Modul.

10. Verdrahten Sie Ihr Modul.

➔ Jetzt können Sie Ihr System wieder in Betrieb nehmen.

Austausch einer Modulgruppe



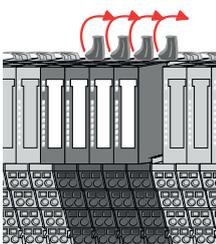
1. Machen Sie Ihr System stromlos.
2. Entfernen Sie falls vorhanden die Verdrahtung an der Modulgruppe.
- 3.



Bei der Demontage und beim Austausch eines (Kopf)-Moduls oder einer Modulgruppe müssen Sie aus montage-technischen Gründen immer das rechts daneben befindliche Elektronik-Modul entfernen! Nach der Montage kann es wieder gesteckt werden.

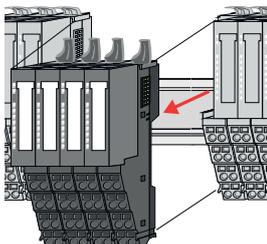
Betätigen Sie die Entriegelung an der Unterseite des rechts neben der Modulgruppe befindlichen Elektronik-Moduls und ziehen Sie dieses nach vorne ab.

4. Klappen Sie alle Verriegelungshebel der zu tauschenden Modulgruppe nach oben.

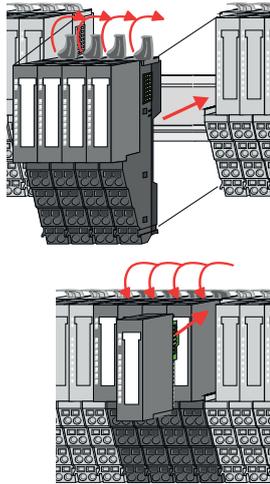


5. Ziehen Sie die Modulgruppe nach vorne ab.

6. Zur Montage klappen Sie alle Verriegelungshebel der zu montierenden Modulgruppe nach oben.



Demontage > Demontage 16x-Peripherie-Module



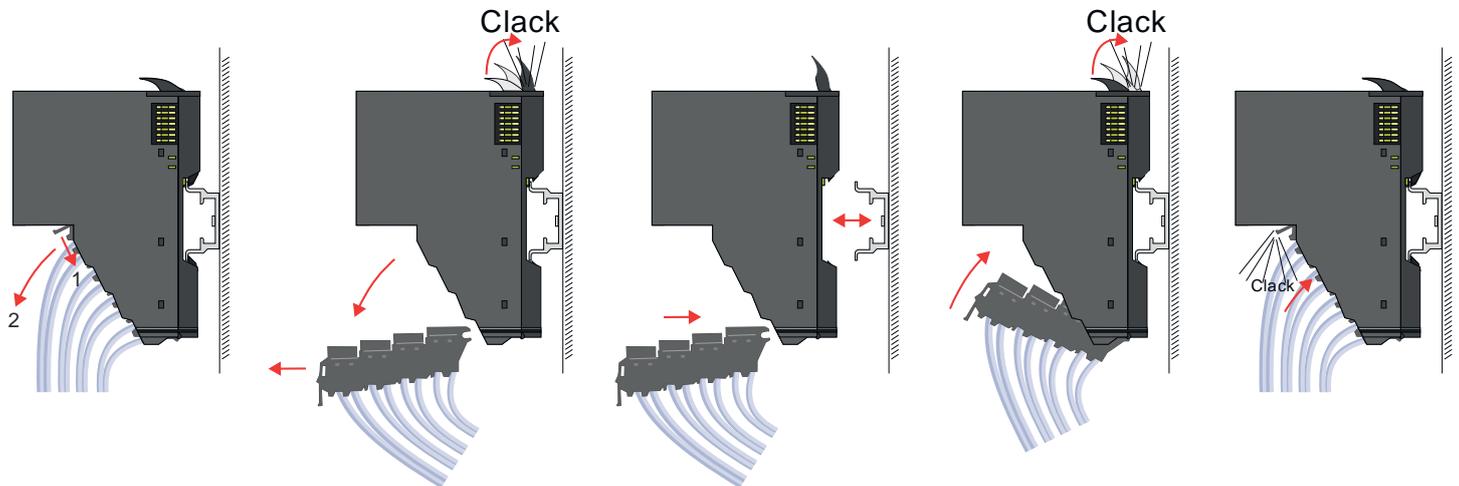
7. ➔ Stecken Sie die zu montierende Modulgruppe in die Lücke zwischen die beiden Module und schieben Sie die Modulgruppe, geführt durch die Führungsleisten auf beiden Seiten, auf die Tragschiene.
8. ➔ Klappen Sie alle Verriegelungshebel wieder nach unten.
9. ➔ Stecken Sie wieder das zuvor entnommene Elektronik-Modul.
10. ➔ Verdrahten Sie Ihre Modulgruppe.
 - ➔ Jetzt können Sie Ihr System wieder in Betrieb nehmen.

2.6.3 Demontage 16x-Peripherie-Module

Vorgehensweise

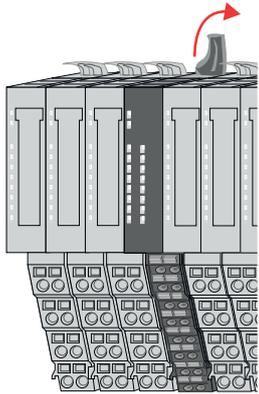
Austausch einer Elektronik-Einheit

1. ➔ Machen Sie Ihr System stromlos.
2. ➔ Zum Austausch einer Elektronik-Einheit können Sie den Terminal-Block nach Betätigung der Entriegelung nach unten klappen und abziehen.
Für die Montage des Terminal-Blocks wird dieser horizontal an der Unterseite der Elektronik-Einheit eingehängt und zur Elektronik-Einheit geklappt, bis dieser einrastet.
➔ Jetzt können Sie Ihr System wieder in Betrieb nehmen.



Austausch eines 16x-Peripherie-Moduls

1. ➔ Machen Sie Ihr System stromlos.
2. ➔ Entfernen Sie falls vorhanden die Verdrahtung am Modul bzw. den verdrahteten Terminal-Block.

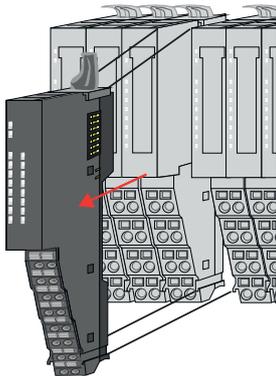


3. →



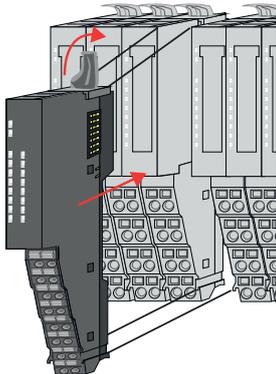
Im Gegensatz zu 8x-Peripherie-Modulen können Sie 16x-Peripherie-Module direkt demontieren und montieren.

Clappen Sie den Verriegelungshebel des zu tauschenden Moduls nach oben.

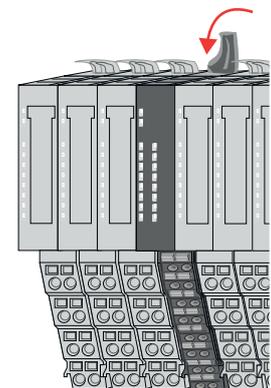


4. → Ziehen Sie das Modul nach vorne ab.

5. → Zur Montage klappen Sie den Verriegelungshebel des zu montierenden Moduls nach oben.



6. → Stecken Sie das zu montierende Modul in die Lücke zwischen die beiden Module und schieben Sie das Modul, geführt durch die Führungsleisten auf beiden Seiten, auf die Tragschiene.



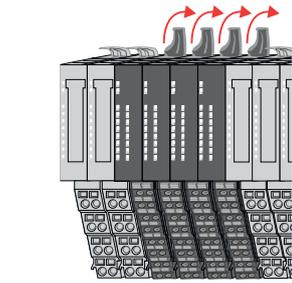
7. → Klappen Sie den Verriegelungshebel wieder nach unten.

8. → Verdrahten Sie Ihr Modul bzw. stecken Sie wieder den verdrahteten Terminal-Block.
➔ Jetzt können Sie Ihr System wieder in Betrieb nehmen.

Austausch einer Modulgruppe

1. → Machen Sie Ihr System stromlos.

2. → Entfernen Sie falls vorhanden die Verdrahtung an der Modulgruppe bzw. die verdrahteten Terminal-Blocks.

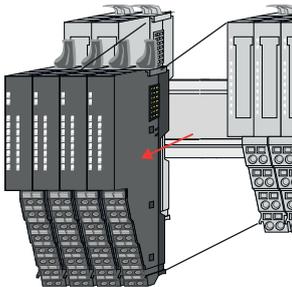


3. →



Im Gegensatz zu 8x-Peripherie-Modulen können Sie 16x-Peripherie-Module direkt demontieren und montieren.

Klappen Sie alle Verriegelungshebel der zu tauschenden Modulgruppe nach oben.

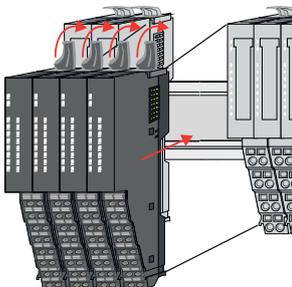


4. →

Ziehen Sie die Modulgruppe nach vorne ab.

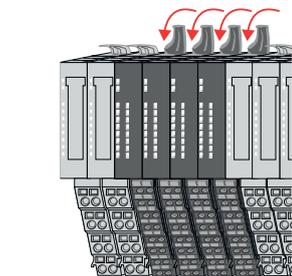
5. →

Zur Montage klappen Sie alle Verriegelungshebel der zu montierenden Modulgruppe nach oben.



6. →

Stecken Sie die zu montierende Modulgruppe in die Lücke zwischen die beiden Module und schieben Sie die Modulgruppe, geführt durch die Führungsleisten auf beiden Seiten, auf die Tragschiene.



7. →

Klappen Sie alle Verriegelungshebel wieder nach unten.

8. →

Verdrahten Sie Ihre Modulgruppe bzw. stecken Sie wieder die verdrahteten Terminal-Blocks.

➔ Jetzt können Sie Ihr System wieder in Betrieb nehmen.

2.7 Gerätetausch und Reparatur

2.7.1 Gerätetausch

Hinweise



HINWEIS

Beim Gerätetausch einer Safety-CPU ist immer die zugehörige Checkliste zu beachten!

➔ ["Checkliste Modifikation und Nachrüstung"...](#)Seite 227



HINWEIS

Der Austausch gegen ein inkompatibles Gerät ist nicht erlaubt!



Wenn die Firmware-Version der CPU neuer ist als die Firmware-Version der zu ersetzenden CPU, müssen Sie möglicherweise Ihr Anwenderprogramm in iCube Engineer neu kompilieren. Wenn dies erforderlich ist, werden Sie mit der entsprechenden Firmware-Version informiert.

Vorgehensweise

Die neue CPU muss folgende Bedingungen erfüllen:

- Gleicher Gerätetyp.
- Gleicher oder höherer Firmwarestand.
- 1.  Demontieren Sie die zu tauschende CPU. [↪ "Demontage"...Seite 44](#)
- 2.  Entnehmen Sie, falls vorhanden, die Yaskawa SD-Karte.
- 3.  Montieren Sie die neue CPU. [↪ "Montage"...Seite 32](#)
- 4.  Falls vorhanden können Sie durch Stecken der Yaskawa SD-Karte Ihr Projekt mit allen Zugangsdaten und IP-Adresse in die neue CPU übernehmen.
- 5.  Zum Abschluss des Gerätetauschs verfahren Sie jetzt nach Vorgabe der Checkliste. [↪ "Checkliste Modifikation und Nachrüstung"...Seite 227](#)

2.7.1.1 Modultausch FSoE-Slave**HINWEIS**

Beachten Sie, dass beim Modultausch eines FSoE-Slave alle Anforderungen des Herstellers eingehalten werden!

2.7.2 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 möglichst die Originalverpackung.

2.8 Industrielle Sicherheit und Aufbaurichtlinien

2.8.1 Industrielle Sicherheit in der Informationstechnologie

Aktuellste Version	Dieses Kapitel finden Sie auch als Leitfaden " <i>Industrielle IT-Sicherheit</i> " im " <i>Download Center</i> " unter ↪ www.yaskawa.eu.com
Gefahren	<p>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:</p> <ul style="list-style-type: none">■ 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	<p>Die wichtigsten Schutzmaßnahmen vor Manipulation und Verlust der Datensicherheit im industriellen Umfeld sind:</p> <ul style="list-style-type: none">■ Verschlüsselung des Datenverkehrs mittels Zertifikate.■ 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	<p>Nähere Informationen zu den Maßnahmen finden Sie auf den folgenden Webseiten:</p> <ul style="list-style-type: none">■ Bundesamt für Informationstechnik ↪ www.bsi.bund.de■ Cybersecurity & Infrastructure Security Agency ↪ us-cert.cisa.gov■ VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik ↪ www.vdi.de

2.8.1.1 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.
 - 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.
- Deaktivieren Sie inaktive Kommunikations-Ports bzw. Protokolle.
 - Es sollten immer nur die Kommunikations-Ports aktiviert sein, über die auch kommuniziert wird.
 - Es sollten immer nur die Kommunikations-Protokolle aktiviert sein, über die auch kommuniziert wird.
- 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.
- Beschränken Sie den Einsatz von externen Datenträgern.
 - Über externe Datenträger wie USB-Speichersticks oder SD-Speicherkarten kann Schadsoftware unter Umgehung einer Firewall direkt in eine Anlage gelangen.
 - Externe Datenträger bzw. deren Steckplätze müssen z.B. unter Verwendung eines abschließbaren Schaltschranks vor unbefugtem physischem Zugriff geschützt werden.
 - Stellen Sie sicher, dass nur befugte Personen Zugriff haben.
 - Stellen Sie bei der Entsorgung von Datenträgern sicher, dass diese sicher zerstört werden.
- 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.

2.8.1.2 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 unbekanntem 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.

2.8.2 Aufbaurichtlinien

Allgemeines

Die Aufbaurichtlinien enthalten Informationen über den störstabilen Aufbau eines SPS-Systems. Es werden die Wege beschrieben, wie Störungen in Ihre Steuerung gelangen können, wie die elektromagnetische Verträglichkeit (EMV) sicher gestellt werden kann und wie bei der Schirmung vorzugehen ist.

Was bedeutet EMV?

Unter Elektromagnetischer Verträglichkeit (EMV) versteht man die Fähigkeit eines elektrischen Gerätes, in einer vorgegebenen elektromagnetischen Umgebung fehlerfrei zu funktionieren, ohne vom Umfeld beeinflusst zu werden bzw. das Umfeld in unzulässiger Weise zu beeinflussen.

Die Komponenten sind für den Einsatz in Industrieumgebungen entwickelt und erfüllen hohe Anforderungen an die EMV. Trotzdem sollten Sie vor der Installation der Komponenten eine EMV-Planung durchführen und mögliche Störquellen in die Betrachtung einbeziehen.

Mögliche Störeinwirkungen

Elektromagnetische Störungen können sich auf unterschiedlichen Pfaden in Ihre Steuerung einkoppeln:

- Elektromagnetische Felder (HF-Einkopplung)
- Magnetische Felder mit energietechnischer Frequenz
- Bus-System
- Stromversorgung
- Schutzleiter

Je nach Ausbreitungsmedium (leitungsgebunden oder -ungebunden) und Entfernung zur Störquelle gelangen Störungen über unterschiedliche Kopplungsmechanismen in Ihre Steuerung.

Man unterscheidet:

- galvanische Kopplung
- kapazitive Kopplung
- induktive Kopplung
- Strahlungskopplung

Grundregeln zur Sicherstellung der EMV

Häufig genügt zur Sicherstellung der EMV das Einhalten einiger elementarer Regeln. Beachten Sie beim Aufbau der Steuerung deshalb die folgenden Grundregeln.

- Achten Sie bei der Montage Ihrer Komponenten auf eine gut ausgeführte flächenhafte Massung der inaktiven Metallteile.
 - Stellen Sie eine zentrale Verbindung zwischen der Masse und dem Erde/Schutzleitersystem her.
 - Verbinden Sie alle inaktiven Metallteile großflächig und impedanzarm.
 - Verwenden Sie nach Möglichkeit keine Aluminiumteile. Aluminium oxidiert leicht und ist für die Massung deshalb weniger gut geeignet.
- Achten Sie bei der Verdrahtung auf eine ordnungsgemäße Leitungsführung.
 - Teilen Sie die Verkabelung in Leitungsgruppen ein. (Starkstrom, Stromversorgungs-, Signal- und Datenleitungen).
 - Verlegen Sie Starkstromleitungen und Signal- bzw. Datenleitungen immer in getrennten Kanälen oder Bündeln.
 - Führen Sie Signal- und Datenleitungen möglichst eng an Masseflächen (z.B. Tragholme, Metallschienen, Schrankbleche).
- Achten Sie auf die einwandfreie Befestigung der Leitungsschirme.
 - Datenleitungen sind geschirmt zu verlegen.
 - Analogleitungen sind geschirmt zu verlegen. Bei der Übertragung von Signalen mit kleinen Amplituden kann das einseitige Auflegen des Schirms vorteilhaft sein.
 - Leitungen für Frequenzumrichter, Servo- und Schrittmotore sind geschirmt zu verlegen.
 - Legen Sie die Leitungsschirme direkt nach dem Schrankeintritt großflächig auf eine Schirm-/Schutzleiterschienen auf, und befestigen Sie die Schirme mit Kabelschellen.
 - Achten Sie darauf, dass die Schirm-/Schutzleiterschienen impedanzarm mit dem Schrank verbunden ist.
 - Verwenden Sie für geschirmte Datenleitungen metallische oder metallisierte Steckergehäuse.

- Setzen Sie in besonderen Anwendungsfällen spezielle EMV-Maßnahmen ein.
 - Erwägen Sie bei Induktivitäten den Einsatz von Löschgliedern.
 - Beachten Sie, dass bei Einsatz von Leuchtstofflampen sich diese negativ auf Signalleitungen auswirken können.
- Schaffen Sie ein einheitliches Bezugspotenzial und erden Sie nach Möglichkeit alle elektrischen Betriebsmittel.
 - Achten Sie auf den gezielten Einsatz der Erdungsmaßnahmen. Das Erden der Steuerung dient als Schutz- und Funktionsmaßnahme.
 - Verbinden Sie Anlagenteile und Schränke mit Ihrer SPS sternförmig mit dem Erde/Schutzleitersystem. Sie vermeiden so die Bildung von Erdschleifen.
 - Verlegen Sie bei Potenzialdifferenzen zwischen Anlagenteilen und Schränken ausreichend dimensionierte Potenzialausgleichsleitungen.

Schirmung von Leitungen

Elektrische, magnetische oder elektromagnetische Störfelder werden durch eine Schirmung geschwächt; man spricht hier von einer Dämpfung. Über die mit dem Gehäuse leitend verbundene Schirmschiene werden Störströme auf Kabelschirme zur Erde hin abgeleitet. Hierbei ist darauf zu achten, dass die Verbindung zum Schutzleiter impedanzarm ist, da sonst die Störströme selbst zur Störquelle werden.

Bei der Schirmung von Leitungen ist folgendes zu beachten:

- Verwenden Sie möglichst nur Leitungen mit Schirmgeflecht.
- Die Deckungsdichte des Schirmes sollte mehr als 80% betragen.
- In der Regel sollten Sie die Schirme von Leitungen immer beidseitig auflegen. Nur durch den beidseitigen Anschluss der Schirme erreichen Sie eine gute Störunterdrückung im höheren Frequenzbereich. Nur im Ausnahmefall kann der Schirm auch einseitig aufgelegt werden. Dann erreichen Sie jedoch nur eine Dämpfung der niedrigen Frequenzen. Eine einseitige Schirmanbindung kann günstiger sein, wenn:
 - die Verlegung einer Potenzialausgleichsleitung nicht durchgeführt werden kann.
 - Analogsignale (einige mV bzw. μA) übertragen werden.
 - Folienschirme (statische Schirme) verwendet werden.
- Benutzen Sie bei Datenleitungen für serielle Kopplungen immer metallische oder metallisierte Stecker. Befestigen Sie den Schirm der Datenleitung am Steckergehäuse. Schirm nicht auf den PIN 1 der Steckerleiste auflegen!
- Bei stationärem Betrieb ist es empfehlenswert, das geschirmte Kabel unterbrechungsfrei abzuisolieren und auf die Schirm-/Schutzleiterschiene aufzulegen.
- Benutzen Sie zur Befestigung der Schirmgeflechte Kabelschellen aus Metall. Die Schellen müssen den Schirm großflächig umschließen und guten Kontakt ausüben.
- Legen Sie den Schirm direkt nach Eintritt der Leitung in den Schrank auf eine Schirmschiene auf.



VORSICHT

Bitte bei der Montage beachten!

Bei Potenzialdifferenzen zwischen den Erdungspunkten kann über den beidseitig angeschlossenen Schirm ein Ausgleichsstrom fließen.

Abhilfe: Potenzialausgleichsleitung.

2.9 Allgemeine Daten für iC9200 Series

Konformität und Approbation		
Konformität		
CE	2014/30/EU	EMV-Richtlinie
Approbation		
UL	UL 61010-2-201	UL befindet sich in Vorbereitung
Sonstiges		
RoHS	2011/65/EU	Richtlinie zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten
Personenschutz und Geräteschutz		
Schutzart	-	IP20
Potenzialtrennung		
zum Feldbus	-	galvanisch entkoppelt
zur Prozessebene	-	galvanisch entkoppelt
Isolationsfestigkeit	EN 61010-2-201	-
Isolationsspannung gegen Bezugserde		
Eingänge / Ausgänge	-	AC / DC 50V, bei Prüfspannung AC 500V
Schutzmaßnahmen	-	gegen Kurzschluss
Umgebungsbedingungen gemäß EN 61131-2		
Klimatisch		
Lagerung / Transport	EN 60068-2-14	-40...+85°C
Betrieb		
Horizontaler Einbau hängend	EN 61131-2	0...+60°C
Horizontaler Einbau liegend	EN 61131-2	0...+55°C
Vertikaler Einbau	EN 61131-2	0...+40°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	-	Schaltschrank oder Schaltkasten der Schutzart IP54 oder höher auf einer 35- mm-Standardtragschiene
Einbaulage	-	Horizontal und vertikal → "Montagemöglichkeiten"...Seite 34

Allgemeine Daten für iC9200 Series > Einsatz unter erschwerten Betriebsbedingungen

EMV	Norm	Bemerkungen	
Störaussendung	EN 61000-6-4	Class A (Industriebereich)	
Störfestigkeit Zone B	EN 61000-6-2	Industriebereich	
		EN 61000-4-2	ESD 8kV bei Luftentladung (Schärfegrad 3), 4kV bei Kontaktentladung (Schärfegrad 2)
		EN 61000-4-3	HF-Einstrahlung (Gehäuse) 80...1000MHz, 10V/m, 80% AM (1kHz) 1,4...6,0GHz, 3V/m, 80% AM (1kHz)
		EN 61000-4-6	HF-Leitungsgeführt 150kHz...80MHz, 10V, 80% AM (1kHz)
		EN 61000-4-4	Burst, Schärfegrad 3
		EN 61000-4-5	Surge, Schärfegrad 3 ¹

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

2.9.1 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!

3 Hardwarebeschreibung

3.1 Leistungsmerkmale

CPU

iC9212M-EC - PMC9212E0

iC9216M-EC - PMC9216E0

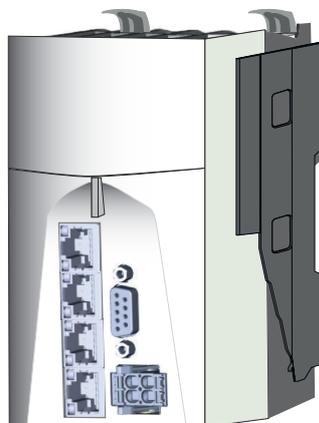
iC9212M-FSoE - PMC9212ES

iC9216M-FSoE - PMC9216ES

- Programmierbar in IEC 61131 über Yaskawa iCube Engineer.
- Steckplatz für externe Yaskawa SD-Karte.
- Status-LEDs für Betriebszustand und Diagnose.
- X1: EtherCAT-Master Funktionalität (nur PMC921xE0).
- X1: EtherCAT FSoE-Master Funktionalität (nur PMC921xES).
- X2: Ethernet-Schnittstelle für zukünftige Erweiterungen.
- X3/X4: Ethernet (Switch) - PROFINET optional.
- Über *SliceBus* bis zu 64 System SLIO Module ankopelbar.

Speicher

- Nur PMC9212Ex:
 - 2GB Arbeitsspeicher (RAM).
 - 12MB Programmspeicher.
 - 32MB Datenspeicher.
 - 512kB permanenter Datenspeicher.
- Nur PMC9216Ex:
 - 2GB Arbeitsspeicher (RAM).
 - 12MB Programmspeicher.
 - 32MB Datenspeicher.
 - 3072kB permanenter Datenspeicher.



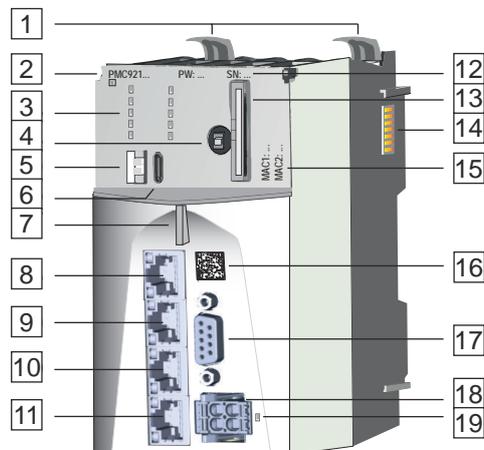
Bestelldaten

Typ	Bestellnummer	Beschreibung
CPU iC9212M-EC	PMC9212E0	CPU iC9212M-EC mit EtherCAT-Master.
CPU iC9216M-EC	PMC9216E0	CPU iC9216M-EC mit EtherCAT-Master und erweitertem Speicher.
CPU iC9212M-FSoE	PMC9212ES	CPU iC9212M-FSoE mit EtherCAT FSoE-Master.
CPU iC9216M-FSoE	PMC9216ES	CPU iC9216M-FSoE mit EtherCAT FSoE-Master und erweitertem Speicher.

Aufbau > CPU iC921xM-x

3.2 Aufbau

3.2.1 CPU iC921xM-x



- 1 Verriegelungshebel
 - 2 Bestellnummer und Hardware-Ausgabestand
 - 3 LED-Leisten
 - 4 Betriebsarten-Schalter CPU
 - 5 S1: DIP-Schalter
 - 6 X7: USB-C-Buchse
 - 7 Status-LED
 - 8 X1: EtherCAT-Port
 - 9 X2: Optional
 - 10 X3: Ethernet-Port (intern geswitched mit X4) - PROFINET optional
 - 11 X4: Ethernet-Port (intern geswitched mit X3) - PROFINET optional
 - 12 Passwort und Seriennummer
 - 13 Steckplatz für Yaskawa SD-Karte
 - 14 *SliceBus* für System SLIO Module
 - 15 MAC1: MAC-Adresse für X3/X4, MAC2: MAC-Adresse für X1/X2
 - 16 QR-Code
 - 17 X5: reserviert
 - 18 X6: Stecker DC 24V Spannungsversorgung
 - 19 LED DC 24V Spannungsversorgung
- 2)...6, 12, 13 und 15 befinden sich unter der Frontklappe.

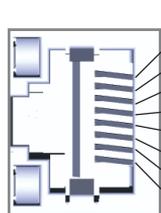


Direktzugriff auf Produktinformationen

Über den QR-Code 16 auf der Frontseite gelangen Sie auf die produkt-spezifische Webseite. Dort finden Sie alle Informationen für den Einsatz und Betrieb der CPU.

3.2.2 Schnittstellen

X1/X2 X3/X4



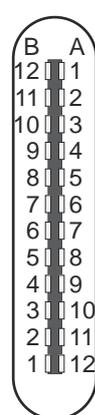
①	TD+	DA+
②	TD-	DA-
③	RD+	DB+
④	n.c.	DC+
⑤	n.c.	DC-
⑥	RD-	DB-
⑦	n.c.	DD+
⑧	n.c.	DD-

X6



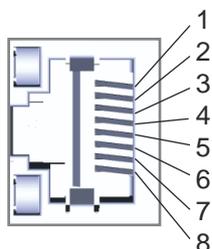
①	+ DC 24V
②	+ DC24V
③	0V
④	0V

X7



A	B
①	① GND
②	② TX1+
③	③ TX1-
④	④ VBUS
⑤	⑤ CC1
⑥	⑥ D+
⑦	⑦ D-
⑧	⑧ n.c.
⑨	⑨ VBUS
⑩	⑩ RX2-
⑪	⑪ RX2+
⑫	⑫ GND

X1: EtherCAT-Port



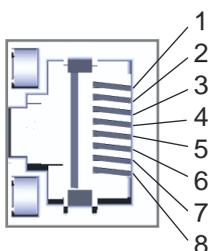
8polige RJ45-Buchse:

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 CPU hat einen Ethernet Kommunikationsprozessor mit EtherCAT-Controller integriert.
- Den EtherCAT-Controller können Sie in einem EtherCAT-System einsetzen als:
 - EtherCAT-Master (nur PMC921xE0)
 - EtherCAT FSoE-Master (nur PMC921xES)
- Der Anschluss erfolgt über den integrierten EtherCAT-Port X1.
- Verbinden Sie diese Schnittstellen mit der RJ45-Buchse "IN" Ihrer EtherCAT Slave-Station.
- 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-Master und einer beliebigen Anzahl an EtherCAT-Slaves (Koppler)
- Jeder EtherCAT-Slave besitzt eine RJ45-Buchse "IN" und "OUT". Das ankommende EtherCAT-Kabel aus Richtung des Masters ist in die mit "IN" bezeichnete Buchse zu stecken. Die mit "OUT" bezeichnete Buchse ist mit dem nachfolgenden Teilnehmer zu verbinden. Beim jeweiligen letzten Teilnehmer bleibt die "OUT"-Buchse frei.

Aufbau > Schnittstellen

X3/X4: Ethernet-Port

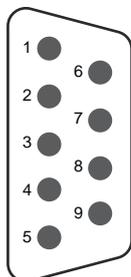


8polige RJ45-Buchse:

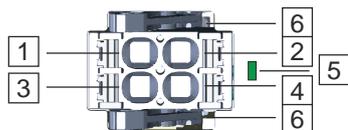
Pin	Signal	Beschreibung
1	DA+	Bidirektionales Paar A + (Daten senden +)
2	DA-	Bidirektionales Paar A - (Daten senden -)
3	DB+	Bidirektionales Paar B + (Daten empfangen +)
4	DC+	Bidirektionales Paar C +
5	DC-	Bidirektionales Paar C -
6	DB-	Bidirektionales Paar B - (Daten empfangen -)
7	DD+	Bidirektionales Paar D +
8	DD-	Bidirektionales Paar D -

- Die CPU hat einen Ethernet Kommunikationsprozessor integriert.
- Der Anschluss erfolgt über einen integrierten 2-fach Switch (X3/X4).
- Über Ethernet (default: 192.168.1.1, "MAC1") haben Sie Zugriff auf:
 - Programmierung/Fernwartung der CPU.
 - Web-based Management WBM der CPU.
 - OPC UA-Kommunikation der CPU.
- In der optional freisichtbaren Betriebsart "PROFINET-IO-Controller" können Sie hier Ihre PROFINET-Devices anbinden.
- In der optional freisichtbaren Betriebsart "PROFINET I-Device" können Sie hier Ihre CPU als PROFINET I-Device an einen PROFINET-IO-Controller anbinden.

X5: reserviert



Die Schnittstelle ist für zukünftige Erweiterungen reserviert.

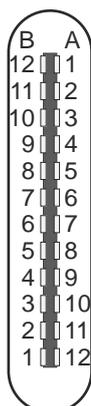
X6: Spannungsversorgung**2poliger Stecker:**

Pos.	Signal	Beschreibung
1, 2	DC 24V	Pluspol DC 24V Spannungsversorgung, im Stecker gebrückt.
3, 4	0V	Masse DC 24V Spannungsversorgung, im Stecker gebrückt.

- 5 LED-Anzeige für Spannungsversorgung.
- 6 Entriegelung

Die CPU besitzt ein eingebautes Netzteil:

- Das Netzteil ist mit DC 24V, max 1,5A zu versorgen. Hierzu dient der DC 24V Anschluss.
- Mit der Versorgungsspannung können sowohl die CPU-Elektronik als auch die Elektronik der über den *SliceBus* angebundene System SLIO Peripherie-Module versorgt werden. Für die Leistungsversorgung der System SLIO Peripherie-Module ist ein zusätzliches Power-Modul erforderlich.
- Das Netzteil ist gegen Verpolung und Überstrom geschützt.
- Sie haben die Möglichkeit z.B. für einen Modulwechsel bei stehender Verdrahtung den Steckverbinder der Spannungsversorgung zu entfernen. Hierzu besitzt der Steckverbinder eine Entriegelung. → "[Verdrahtung CPU](#)"...Seite 36
- Zur einfachen Verdrahtung ist jeder Pol am Steckverbinder 2-fach ausgelegt.

X7: USB-C**24polige USB-C-Buchse:**

Pin A	Signal	Beschreibung	Pin B	Signal	Beschreibung
1	GND	Masse	1	GND	Masse
2	TX1+	High Speed Datenpfad 1 +	2	TX2+	High Speed Datenpfad 2 +
3	TX1-	High Speed Datenpfad 1 -	3	TX2-	High Speed Datenpfad 2 -
4	VBUS	Spannung +5V	4	VBUS	Spannung +5V
5	CC1	Kontroll-Kanal 1 für Steckerorientierung	5	CC2	Kontroll-Kanal 2 für Steckerorientierung
6	D+	USB 2.0 Daten +	6	D+	USB 2.0 Daten +
7	D-	USB 2.0 Daten -	7	D-	USB 2.0 Daten -
8	n.c.	reserviert	8	n.c.	reserviert
9	VBUS	Spannung +5V	9	VBUS	Spannung +5V
10	RX2-	High Speed Datenpfad 2 -	10	RX1-	High Speed Datenpfad 1 -
11	RX2+	High Speed Datenpfad 2 +	11	RX1+	High Speed Datenpfad 1 +
12	GND	Masse	12	GND	Masse

- Die Schnittstelle befindet sich unter der Frontklappe.
- Die Schnittstelle ist für Kundenanwendungen nicht relevant.
- Die Schnittstelle unterstützt das USB 2.0 Protokoll und dient ausschließlich als Service-Schnittstelle.

Aufbau > LEDs

3.2.3 Speicher

Interner Speicher

Die CPU hat einen Speicher integriert. Angaben zu den Speichergrößen finden Sie in den technischen Daten. → ["Technische Daten"...Seite 70](#)

Der Speicher gliedert sich in folgende Teile:

- *Arbeitsspeicher* für temporäre Daten und Teile des Anwenderprogramms.
- *Parametrierungsspeicher* für aktuelle Firmware und überlagerndes Dateisystem mit Firmwareanpassungen, Anwenderprogramm und -Daten.
- Nichtflüchtiger Speicher für remanente Daten.

→ ["Speichermanagement"...Seite 94](#)

Steckplatz für Yaskawa SD-Karte

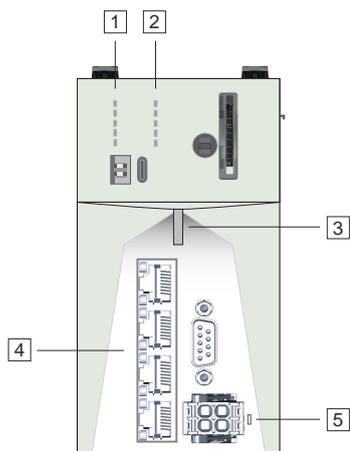
Die CPU besitzt einen Steckplatz für eine Yaskawa SD-Karte. Hier können Sie als externen Speicher eine Yaskawa SD-Karte einsetzen und das *überlagernde Dateisystem* der CPU auf die Karte auslagern.

→ ["Steckplatz für Yaskawa SD-Karte"...Seite 96](#)

3.2.4 Pufferungsmechanismen

- Die iC9200 Series CPU besitzt auf Kondensatorbasis einen Mechanismus zur Sicherung der internen Uhr bei Stromausfall für max. 28 Tage.
- Die bei der Projektierung definierten remanenten Daten werden bei Stromausfall automatisch im nichtflüchtigen Speicher gespeichert.

3.2.5 LEDs



- 1 LED-Leiste 1
 - 2 LED-Leiste 2
 - 3 Status-LED
 - 4 LEDs RJ45-Buchsen
 - 5 LED Spannungsversorgung
- 1 und 2 befinden sich unter der Frontklappe.

LED-Leiste 1/2 ¹, ²

LED	Farbe	Funktion
LED-Leiste 1 ¹		
RN	 grün	Die CPU befindet sich im Zustand RUN ohne Fehler.
ER	 rot	Es ist ein Fehler in der CPU aufgetreten.
IO ER	 rot	Es ist ein Fehler am <i>SliceBus</i> aufgetreten.
EC RN	 grün	EtherCAT-Master - Status. ↔ 68
EC_ER	 rot	EtherCAT-Master - Fehler. ↔ 68
LED-Leiste 2 ²		
PMC921xE0 und PMC921xES		
PN-C ER	 rot	PROFINET-Controller - Busfehler. ↔ 68
PN-D ER	 rot	PROFINET-Device - Busfehler. ↔ 68
IO DIAG	 rot	Es ist eine Diagnose am <i>SliceBus</i> aufgetreten.
Nur PMC921xES		
SF RN	 grün	EtherCAT FSoE-Master - Status. ↔ 67
SF ER	 rot	EtherCAT FSoE-Master - Fehler. ↔ 67

Status-LED ³

LED	Farbe	Funktion
	grün	Die CPU befindet sich im Zustand RUN ohne Fehler.
	rot	Die CPU befindet sich im Zustand STOP mit Fehler.
	grün/rot 1Hz	Die CPU befindet sich im Zustand RUN mit Fehler.
	rot 2Hz	Es liegt ein Systemfehler vor. Starten Sie die CPU neu.
	gelb	Die CPU befindet sich im Zustand STOP ohne Fehler.
	gelb 1Hz	Dient zur Anzeige von Sonderfunktionen.
	gelb 2Hz	Dient zur Anzeige von Sonderfunktionen.

Aufbau > LEDs

LEDs CPU [1](#), [2](#), [3](#)

Status LED	RN grün	ER rot	IO ER rot	PN-C ER rot	PN-D ER rot	IO DIAG rot	Beschreibung
Bootvorgang nach NetzEIN - sobald die CPU mit DC 24V versorgt wird, leuchtet die  grüne LED der Spannungsversorgung.							
 rot	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Fehler beim Kopieren des Kernels.
 rot	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	X	<input type="checkbox"/>	<input type="checkbox"/>	Laufzeitsystem wurde gestoppt. Führen Sie einen Powercycle durch.
 rot 2Hz	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Yaskawa SD-Karte wurde nicht erkannt.
 rot 2Hz	<input type="checkbox"/>	 1Hz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Zertifikat der Yaskawa SD-Karte ist fehlerhaft bzw. wurde während des Betriebs unerlaubt entnommen. Führen Sie einen Powercycle durch.
 gelb 1Hz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Laufzeitsystem wird geladen.
 rot 2Hz	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Laufzeitsystem konnte nicht geladen werden. Führen Sie einen Powercycle durch.
Betrieb							
 gelb	 0,5Hz	X	X	X	X	X	CPU befindet sich im Zustand STOP.
 rot	 2Hz	 2Hz	X	X	X	X	System-Watchdog wurde ausgelöst und die CPU neu gestartet. Führen Sie über iCube Engineer einen Reboot durch oder versetzen Sie Ihre CPU in den Zustand RUN.
 grün	<input checked="" type="checkbox"/>	<input type="checkbox"/>	X	X	X	X	CPU befindet sich ohne Fehler im Zustand RUN.
 rot	 0,5Hz	<input checked="" type="checkbox"/>	X	X	X	X	Fehler im Anwenderprogramm. CPU befindet sich im Zustand READY/STOP/HALT mit Fehler.
 rot 2Hz	<input type="checkbox"/>	 1Hz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Zertifikat der Yaskawa SD-Karte ist fehlerhaft bzw. wurde während des Betriebs unerlaubt entnommen. Führen Sie einen Powercycle durch.
 rot 2Hz	<input type="checkbox"/>	 2Hz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Das überlagernde Dateisystem im Parametrierungsspeicher meldet einen Speicherüberlauf. → "Speicherüberlauf beheben"... Seite 95
 gelb 2Hz	 1Hz	 1Hz	 1Hz	 1Hz	 1Hz	 1Hz	Die CPU fordert einen Powercycle an z.B. nach Rücksetzen auf <i>Werkseinstellung Typ 1</i> mittels DIP-Schalter.
SliceBus							
X	X	X	<input type="checkbox"/>	X	X	X	Es gibt keine Fehler am <i>SliceBus</i> .
 rot ¹	X	X	<input checked="" type="checkbox"/>	X	X	X	Konfigurationsfehler am <i>SliceBus</i> .
	X	X	X	X	X	<input checked="" type="checkbox"/>	<i>SliceBus</i> meldet eine Diagnose. → "SliceBus"... Seite 189
nicht relevant: X							
1) Der Zustand ist abhängig vom Betriebszustand der CPU.							

LEDs CPU [1](#), [2](#), [3](#)

Status LED	RN grün	ER rot	IO ER rot	PN-C ER rot	PN-D ER rot	IO DIAG rot	Beschreibung
Rücksetzen auf Werkseinstellung							
 gelb 1Hz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Anforderung Rücksetzen auf <i>Werkseinstellung Typ 1</i> .
 gelb 2Hz	<input checked="" type="checkbox"/> 1Hz	<input checked="" type="checkbox"/> 1Hz	<input checked="" type="checkbox"/> 1Hz	<input checked="" type="checkbox"/> 1Hz	<input checked="" type="checkbox"/> 1Hz	<input checked="" type="checkbox"/> 1Hz	Die CPU fordert nach Rücksetzen auf <i>Werkseinstellung Typ 1</i> mittels DIP-Schalter einen Powercycle an.
 gelb 2Hz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Anforderung Rücksetzen auf <i>Werkseinstellung Typ 2</i> .
Firmwareupdate							
 gelb 1Hz	<input checked="" type="checkbox"/> 0,2s/1s	<input type="checkbox"/>	Firmwareupdate wird durchgeführt.				

LEDs Safety [2](#)

SF RN grün	SF ER rot	Beschreibung
<input type="checkbox"/>	<input type="checkbox"/>	Die Safety-CPU ist nicht bereit für Operationen.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Die Safety-CPU befindet sich im Zustand SAFE-RUN. Das sicherheitsbezogene Anwenderprogramm wird ausgeführt.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Die Safety-CPU befindet sich Fail Safe Zustand <i>Hard Fail Safe</i> . → " Fail Safe Zustände "...Seite 133 Überprüfen Sie Ihren Hardware-Aufbau und führen Sie einen Powercycle durch.
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1Hz	Die Safety-CPU befindet sich Fail Safe Zustand <i>Soft Fail Safe</i> . → " Fail Safe Zustände "...Seite 133 Das sicherheitsbezogene Anwenderprogramm wird nicht ausgeführt. Es ist ein Fehler aufgetreten.
<input checked="" type="checkbox"/> 1Hz	<input type="checkbox"/>	Abhängig von der Betriebsart wird folgender Zustand angezeigt: <ul style="list-style-type: none"> ■ NetzEIN - Initialisierung <ul style="list-style-type: none"> - Die Safety-CPU befindet sich im Zustand SAFE-STOP. - Projektdaten werden vom Parametrierungsspeicher in den internen Speicher der Safety-CPU übernommen. ■ Datentransfer <ul style="list-style-type: none"> - Mit iCube Engineer wird ein Projekt in die Safety-CPU übertragen. ■ Debug <ul style="list-style-type: none"> - Die Safety-CPU befindet sich im Zustand DEBUG-STOP. - Die Safety-CPU befindet sich im Zustand DEBUG-HALT.
<input checked="" type="checkbox"/> 2Hz	<input type="checkbox"/>	Die Safety-CPU befindet sich im Zustand DEBUG-RUN.



Nähere Informationen zum DEBUG-Betrieb finden Sie im Handbuch zum iCube Engineer.

Aufbau > LEDs

LEDs EtherCAT ¹

Status LED	EC RN  grün	EC ER  rot	Beschreibung
X	<input type="checkbox"/>	X	<ul style="list-style-type: none"> Der EtherCAT-Master befindet sich im Zustand INIT. Der EtherCAT-Master ist nicht konfiguriert.
X	<input checked="" type="checkbox"/> 2,5Hz	X	<ul style="list-style-type: none"> Der EtherCAT-Master befindet sich im Zustand PreOp.
X	<input checked="" type="checkbox"/> 0,2s/1s	X	<ul style="list-style-type: none"> Der EtherCAT-Master befindet sich im Zustand SafeOp.
X	X	<input type="checkbox"/>	<ul style="list-style-type: none"> Der EtherCAT-Master meldet keinen Fehler.
 rot ¹	X	<input checked="" type="checkbox"/> 2,5Hz	<ul style="list-style-type: none"> Die Slaves am EtherCAT-Master sind konfiguriert und verbunden aber die Topologie ist fehlerhaft.
 rot ¹	X	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> Die Slaves am EtherCAT-Master sind konfiguriert aber nicht verbunden.

nicht relevant: X

1) Der Zustand ist abhängig vom Betriebszustand der CPU.

LEDs PROFINET ²
PROFINET optional

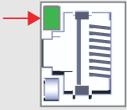
Bitte beachten Sie, dass für den Einsatz von PROFINET eine gesonderte Lizenz erforderlich ist, welche entsprechend zu aktivieren ist!

Status LED	PN-C ER  rot	PN-D ER  rot	Beschreibung
X	<input type="checkbox"/>	X	PROFINET-IO-Controller meldet: <ul style="list-style-type: none"> Der PROFINET-IO-Controller hat eine aktive Kommunikationsverbindung zu jedem projektierten PROFINET-IO-Device aufgebaut. Der PROFINET-IO-Controller ist nicht konfiguriert.
 rot ¹	<input checked="" type="checkbox"/>	X	PROFINET-IO-Controller meldet: <ul style="list-style-type: none"> Busfehler, kein Link vorhanden. Falsche Übertragungsgeschwindigkeit. Vollduplexübertragung ist nicht aktiviert.
	<input checked="" type="checkbox"/> 1Hz	X	PROFINET-IO-Controller meldet: <ul style="list-style-type: none"> Linkstatus ist vorhanden, zu mindestens einem PROFINET-IO-Device besteht keine Kommunikationsverbindung.
X	X	<input type="checkbox"/>	Ein PROFINET-IO-Controller hat eine aktive Kommunikationsverbindung zum CPU iC921xM-x I-Device aufgebaut.
X	X	<input checked="" type="checkbox"/>	PROFINET I-Device meldet: <ul style="list-style-type: none"> Busfehler, keine Verbindung zu PROFINET-IO-Controller.
	X	<input checked="" type="checkbox"/> 1Hz	PROFINET I-Device meldet: <ul style="list-style-type: none"> Link-Status vorhanden aber keine Kommunikationsverbindung zu PROFINET-IO-Controller.
 gelb 1Hz	X	X	Dient zur Geräteidentifizierung.

nicht relevant: X

1) Der Zustand ist abhängig vom Betriebszustand der CPU.

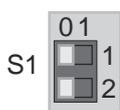
LEDs RJ45-Buchsen ⁴

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

LED Spannungsversorgung ⁵

LED	Farbe	Funktion
	 grün	Die CPU wird mit Spannung versorgt.

3.2.6 DIP-Schalter



Mit dem 2-fach DIP-Schalter unter der Frontklappe können Sie folgende Aktionen der CPU auslösen:

S1	S1-1	S1-2	Aktion
 01	OFF	OFF	Nach PowerON startet die CPU im <i>Standard Mode</i> - Defaulteinstellung.
 1	OFF	ON	Nach PowerON führt die CPU <i>Rücksetzen auf Werkseinstellung Typ 1</i> durch. → " Rücksetzen auf Werkseinstellung Typ 1 "...Seite 98
 2	ON	OFF	Nach PowerON startet die CPU im <i>Safe Mode</i> . → " Safe Mode "...Seite 99

3.2.7 Betriebsartenschalter



- Mit dem Betriebsartenschalter können Sie bei der CPU zwischen den Betriebsarten ST (**STOP**) und RN (**RUN**) wählen.
- Mit der Tasterstellung MR (**Memory Reset**) können Sie einen Reset der CPU in verschiedenen Stufen anfordern. → "[MRESET und Rücksetzen auf Werkseinstellungen](#)"...Seite 98

Technische Daten > iC9212M-EC - PMC9212E0

3.3 Technische Daten

3.3.1 iC9212M-EC - PMC9212E0

Artikelnr.	PMC9212E0
Bezeichnung	iC9212M-EC
Modulkennung	-
Technische Daten Stromversorgung	
Versorgungsspannung (Nennwert)	DC 24 V
Versorgungsspannung (zulässiger Bereich)	DC 20,4...28,8 V
Verpolschutz	✓
Stromaufnahme (im Leerlauf)	0,2 A
Stromaufnahme (Nennwert)	1,5 A
Einschaltstrom	1 A
I ² t	0,3 A ² s
max. Stromabgabe am Rückwandbus	3 A
max. Stromabgabe Lastversorgung	-
Verlustleistung	12 W
Hardware	
CPU	Triton (ARM A17)
CPU-Kerne	3
Frequenz	1,26 GHz
RAM	2 GB
eMMC	8 GB
Bedienelemente	LEDs, Dreipunktschalter, DIP-Schalter
Integrierte SliceBus-Versorgung	✓
Anschlüsse	
Serial Com (Sub-D)	-
SliceBus	✓
Anzahl RJ45-Schnittstellen	4 Ports
Externe SD-Karte	
Externe SD-Karte	✓
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	abhängig von SD-Karte
Firewall	✓

Artikelnr.	PMC9212E0
SSH/SFTP	✓
Synchronisation über Ethernet (NTP)	✓
DNS	✓
IEC 61131 runtime system	
Programmspeicher	12 MB
Datenspeicher	32 MB
Remanenter Speicher	512 KB
Echtzeituhr	
Echtzeituhr	✓
Genauigkeit Echtzeituhr	1 Minute Abweichung pro Monat
Pufferungsdauer	28 Tage @ 25°C
Execution and Synchronization Manager (ESM)	
Execution and Synchronization Manager (ESM)	✓
Min. Taskzykluszeit (ESM)	500 µs
ESM-Kerne	1
Maximum Anzahl parallele Tasks	16
SliceBus	
Prozessdaten pro Modul	bis zu 60 Bytes
Max. Moduleanzahl	64
Zykluszeit [ms]	500 µs .. 512 ms
OPC UA	
OPC UA	✓
Server	✓
Max. Anzahl parallele Verbindungen	5
Samplingraten	100 ms .. 5 s
Encryption suite Basic128Rsa15	✓
Encryption suite Basic256	✓
Encryption suite Basic256Sha256	✓
Encryption suite Aes256Sha256RsaPss	✓
Encryption suite Aes128Sha256RsaOaep	✓
Programmierung	
IEC 61131-3	✓
Web Based Management (WBM)	
Web Based Management (WBM)	✓
Ethernet	
Ethernet-fähige Anschlüsse	X3/X4: 2 Ports x 10/100 Mbit/s (Halb-/Voll duplex)

Artikelnr.	PMC9212E0
EtherCAT Master	
Anzahl der EtherCAT-Slaves	512
Aktualisierungszeit	500 µs .. 512 ms
EoE Unterstützung	-
CoE Unterstützung	✓
FoE Unterstützung	-
Distributed Clock Unterstützung	✓
Hotconnect Slaves	✓
Taktsynchronität	✓
Funktionale Sicherheit	
Minimale Zykluszeit	-
Maximale Zykluszeit	-
Programmspeicher sicheres Programm	-
Datenspeicher	-
Safety Protokoll	-
Anzahl FSoE-Teilnehmer	-
Sicherheitsbezogene Eingangsdaten	-
Sicherheitsbezogene Ausgangsdaten	-
Standardeingangsdaten	-
Standardausgangsdaten	-
Max. Anzahl FB-Instanzen	-
Sicherheitsanforderungen	-
Motion	
Basis Achsanzahl	4 (Servo) + 4 (virtuell)
Zyklische Motion Aktualisierungsrate	bis zu 4 Achsen bei 250µs bis zu 16 Achsen bei 500µs bis zu 32 Achsen bei 1ms bis zu 64 Achsen bei 2ms bis zu 128 Achsen bei 4ms
Kaskadentiefe	bis zu 4
Anzahl Achsgruppen	bis zu 16 Achsen Gruppen bis zu 32 Achsen pro Gruppe
PROFINET System	
VendorID	0x0111
DeviceID	0x0368
Spezifikation	Version 2.3
PROFINET-fähige Anschlüsse	X3/X4 (lizensierbar)

Artikelnr.	PMC9212E0
Controller	✓
- Max. Anzahl Devices	64@16ms, 32@8ms, 16@4ms, 8@2ms, 4@1ms
- Zykluszeit	1 ms .. 512 ms
- Systemredundanz	✓
- Fast Startup	✓
- Fast Startup, Max. Anzahl Devices	32
- Topologie	✓
Device	✓
- Device I/O Daten	512 Byte / 512 Byte
- Zykluszeit	1 ms .. 512 ms
- MRP Client Unterstützung	✓
Gehäuse	
Material	PC
Befestigung	Profilschiene 35mm
Mechanische Daten	
Abmessungen (BxHxT)	72 mm x 134 mm x 112 mm
Gewicht Netto	488 g
Gewicht inklusive Zubehör	503 g
Gewicht Brutto	621 g
Umgebungsbedingungen	
Betriebstemperatur	0 °C bis 60 °C
Lagertemperatur	-40 °C bis 70 °C
Zertifizierungen	
Zertifizierung nach UL	-
Zertifizierung nach KC	-
Zertifizierung nach UKCA	ja
Zertifizierung nach ChinaRoHS	ja

3.3.2 iC9216M-EC - PMC9216E0

Artikelnr.	PMC9216E0
Bezeichnung	iC9216M-EC
Modulkennung	-
Technische Daten Stromversorgung	
Versorgungsspannung (Nennwert)	DC 24 V
Versorgungsspannung (zulässiger Bereich)	DC 20,4...28,8 V
Verpolschutz	✓

Technische Daten > iC9216M-EC - PMC9216E0

Artikelnr.	PMC9216E0
Stromaufnahme (im Leerlauf)	0,2 A
Stromaufnahme (Nennwert)	1,5 A
Einschaltstrom	1 A
I ² t	0,3 A ² s
max. Stromabgabe am Rückwandbus	3 A
max. Stromabgabe Lastversorgung	-
Verlustleistung	12 W
Hardware	
CPU	Triton (ARM A17)
CPU-Kerne	3
Frequenz	1,26 GHz
RAM	2 GB
eMMC	8 GB
Bedienelemente	LEDs, Dreipunktschalter, DIP-Schalter
Integrierte SliceBus-Versorgung	✓
Anschlüsse	
Serial Com (Sub-D)	-
SliceBus	✓
Anzahl RJ45-Schnittstellen	4 Ports
Externe SD-Karte	
Externe SD-Karte	✓
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	abhängig von SD-Karte
Firewall	✓
SSH/SFTP	✓
Synchronisation über Ethernet (NTP)	✓
DNS	✓
IEC 61131 runtime system	
Programmspeicher	12 MB
Datenspeicher	32 MB
Remanenter Speicher	3072 KB
Echtzeituhr	

Artikelnr.	PMC9216E0
Echtzeituhr	✓
Genauigkeit Echtzeituhr	1 Minute Abweichung pro Monat
Pufferungsdauer	28 Tage @ 25°C
Execution and Synchronization Manager (ESM)	
Execution and Synchronization Manager (ESM)	✓
Min. Taskzykluszeit (ESM)	500 µs
ESM-Kerne	1
Maximum Anzahl parallele Tasks	16
SliceBus	
Prozessdaten pro Modul	bis zu 60 Bytes
Max. Moduleanzahl	64
Zykluszeit [ms]	500 µs .. 512 ms
OPC UA	
OPC UA	✓
Server	✓
Max. Anzahl parallele Verbindungen	5
Samplingraten	100 ms .. 5 s
Encryption suite Basic128Rsa15	✓
Encryption suite Basic256	✓
Encryption suite Basic256Sha256	✓
Encryption suite Aes256Sha256RsaPss	✓
Encryption suite Aes128Sha256RsaOaep	✓
Programmierung	
IEC 61131-3	✓
Web Based Management (WBM)	
Web Based Management (WBM)	✓
Ethernet	
Ethernet-fähige Anschlüsse	X3/X4: 2 Ports x 10/100 Mbit/s (Halb-/Voll duplex)
EtherCAT Master	
Anzahl der EtherCAT-Slaves	512
Aktualisierungszeit	500 µs .. 512 ms
EoE Unterstützung	-
CoE Unterstützung	✓
FoE Unterstützung	-
Distributed Clock Unterstützung	✓
Hotconnect Slaves	✓

Technische Daten > iC9216M-EC - PMC9216E0

Artikelnr.	PMC9216E0
Taktsynchronität	✓
Funktionale Sicherheit	
Minimale Zykluszeit	-
Maximale Zykluszeit	-
Programmspeicher sicheres Programm	-
Datenspeicher	-
Safety Protokoll	-
Anzahl FSoE-Teilnehmer	-
Sicherheitsbezogene Eingangsdaten	-
Sicherheitsbezogene Ausgangsdaten	-
Standardeingangsdaten	-
Standardausgangsdaten	-
Max. Anzahl FB-Instanzen	-
Sicherheitsanforderungen	-
Motion	
Basis Achsanzahl	4 (Servo) + 4 (virtuell)
Zyklische Motion Aktualisierungsrate	bis zu 4 Achsen bei 250µs bis zu 16 Achsen bei 500µs bis zu 32 Achsen bei 1ms bis zu 64 Achsen bei 2ms bis zu 128 Achsen bei 4ms
Kaskadentiefe	bis zu 4
Anzahl Achsgruppen	bis zu 16 Achsen Gruppen bis zu 32 Achsen pro Gruppe
PROFINET System	
VendorID	0x0111
DeviceID	0x0368
Spezifikation	Version 2.3
PROFINET-fähige Anschlüsse	X3/X4 (lizensierbar)
Controller	✓
- Max. Anzahl Devices	64@16ms, 32@8ms, 16@4ms, 8@2ms, 4@1ms
- Zykluszeit	1 ms .. 512 ms
- Systemredundanz	✓
- Fast Startup	✓
- Fast Startup, Max. Anzahl Devices	32
- Topologie	✓
Device	✓

Artikelnr.	PMC9216E0
- Device I/O Daten	512 Byte / 512 Byte
- Zykluszeit	1 ms .. 512 ms
- MRP Client Unterstützung	✓
Gehäuse	
Material	PC
Befestigung	Profilschiene 35mm
Mechanische Daten	
Abmessungen (BxHxT)	72 mm x 134 mm x 112 mm
Gewicht Netto	488 g
Gewicht inklusive Zubehör	503 g
Gewicht Brutto	621 g
Umgebungsbedingungen	
Betriebstemperatur	0 °C bis 60 °C
Lagertemperatur	-40 °C bis 70 °C
Zertifizierungen	
Zertifizierung nach UL	-
Zertifizierung nach KC	-
Zertifizierung nach UKCA	ja
Zertifizierung nach ChinaRoHS	ja

3.3.3 iC9212M-FSoE - PMC9212ES

Artikelnr.	PMC9212ES
Bezeichnung	iC9212M-FSoE
Modulkennung	-
Technische Daten Stromversorgung	
Versorgungsspannung (Nennwert)	DC 24 V
Versorgungsspannung (zulässiger Bereich)	DC 20,4...28,8 V
Verpolschutz	✓
Stromaufnahme (im Leerlauf)	0,2 A
Stromaufnahme (Nennwert)	1,5 A
Einschaltstrom	1 A
I ² t	0,3 A ² s
max. Stromabgabe am Rückwandbus	3 A
max. Stromabgabe Lastversorgung	-
Verlustleistung	12 W
Hardware	

Technische Daten > iC9212M-FSoE - PMC9212ES

Artikelnr.	PMC9212ES
CPU	Triton (ARM A17)
CPU-Kerne	3
Frequenz	1,26 GHz
RAM	2 GB
eMMC	8 GB
Bedienelemente	LEDs, Dreipunktschalter, DIP-Schalter
Integrierte SliceBus-Versorgung	✓
Anschlüsse	
Serial Com (Sub-D)	-
SliceBus	✓
Anzahl RJ45-Schnittstellen	4 Ports
Externe SD-Karte	
Externe SD-Karte	✓
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	abhängig von SD-Karte
Firewall	✓
SSH/SFTP	✓
Synchronisation über Ethernet (NTP)	✓
DNS	✓
IEC 61131 runtime system	
Programmspeicher	12 MB
Datenspeicher	32 MB
Remanenter Speicher	512 KB
Echtzeituhr	
Echtzeituhr	✓
Genauigkeit Echtzeituhr	1 Minute Abweichung pro Monat
Pufferungsdauer	28 Tage @ 25°C
Execution and Synchronization Manager (ESM)	
Execution and Synchronization Manager (ESM)	✓
Min. Taskzykluszeit (ESM)	500 µs
ESM-Kerne	1
Maximum Anzahl parallele Tasks	16

Artikelnr.	PMC9212ES
SliceBus	
Prozessdaten pro Modul	bis zu 60 Bytes
Max. Moduleanzahl	64
Zykluszeit [ms]	500 µs .. 512 ms
OPC UA	
OPC UA	✓
Server	✓
Max. Anzahl parallele Verbindungen	5
Samplingraten	100 ms .. 5 s
Encryption suite Basic128Rsa15	✓
Encryption suite Basic256	✓
Encryption suite Basic256Sha256	✓
Encryption suite Aes256Sha256RsaPss	✓
Encryption suite Aes128Sha256RsaOaep	✓
Programmierung	
IEC 61131-3	✓
Web Based Management (WBM)	
Web Based Management (WBM)	✓
Ethernet	
Ethernet-fähige Anschlüsse	X3/X4: 2 Ports x 10/100 Mbit/s (Halb-/Voll duplex)
EtherCAT Master	
Anzahl der EtherCAT-Slaves	512
Aktualisierungszeit	500 µs .. 512 ms
EoE Unterstützung	-
CoE Unterstützung	✓
FoE Unterstützung	-
Distributed Clock Unterstützung	✓
Hotconnect Slaves	✓
Taktsynchronität	✓
Funktionale Sicherheit	
Minimale Zykluszeit	5 ms
Maximale Zykluszeit	15 ms
Programmspeicher sicheres Programm	64 KB
Datenspeicher	16 KB
Safety Protokoll	FSoE
Anzahl FSoE-Teilnehmer	32

Technische Daten > iC9212M-FSoE - PMC9212ES

Artikelnr.	PMC9212ES
Sicherheitsbezogene Eingangsdaten	512 Byte
Sicherheitsbezogene Ausgangsdaten	512 Byte
Standardeingangsdaten	128 Byte
Standardausgangsdaten	128 Byte
Max. Anzahl FB-Instanzen	512
Sicherheitsanforderungen	SIL CL 3, PL e, Kat 4
Motion	
Basis Achsanzahl	4 (Servo) + 4 (virtuell)
Zyklische Motion Aktualisierungsrate	bis zu 4 Achsen bei 250µs bis zu 16 Achsen bei 500µs bis zu 32 Achsen bei 1ms bis zu 64 Achsen bei 2ms bis zu 128 Achsen bei 4ms
Kaskadentiefe	bis zu 4
Anzahl Achsgruppen	bis zu 16 Achsen Gruppen bis zu 32 Achsen pro Gruppe
PROFINET System	
VendorID	0x0111
DeviceID	0x0368
Spezifikation	Version 2.3
PROFINET-fähige Anschlüsse	X3/X4 (lizensierbar)
Controller	✓
- Max. Anzahl Devices	64@16ms, 32@8ms, 16@4ms, 8@2ms, 4@1ms
- Zykluszeit	1 ms .. 512 ms
- Systemredundanz	✓
- Fast Startup	✓
- Fast Startup, Max. Anzahl Devices	32
- Topologie	✓
Device	✓
- Device I/O Daten	512 Byte / 512 Byte
- Zykluszeit	1 ms .. 512 ms
- MRP Client Unterstützung	✓
Gehäuse	
Material	PC
Befestigung	Profilschiene 35mm
Mechanische Daten	
Abmessungen (BxHxT)	72 mm x 134 mm x 112 mm

Artikelnr.	PMC9212ES
Gewicht Netto	488 g
Gewicht inklusive Zubehör	503 g
Gewicht Brutto	621 g
Umgebungsbedingungen	
Betriebstemperatur	0 °C bis 60 °C
Lagertemperatur	-40 °C bis 70 °C
Zertifizierungen	
Zertifizierung nach UL	-
Zertifizierung nach KC	-
Zertifizierung nach UKCA	ja
Zertifizierung nach ChinaRoHS	ja

3.3.4 iC9216M-FSoE - PMC9216ES

Artikelnr.	PMC9216ES
Bezeichnung	iC9216M-FSoE
Modulkennung	-
Technische Daten Stromversorgung	
Versorgungsspannung (Nennwert)	DC 24 V
Versorgungsspannung (zulässiger Bereich)	DC 20,4...28,8 V
Verpolschutz	✓
Stromaufnahme (im Leerlauf)	0,2 A
Stromaufnahme (Nennwert)	1,5 A
Einschaltstrom	1 A
I ² t	0,3 A ² s
max. Stromabgabe am Rückwandbus	3 A
max. Stromabgabe Lastversorgung	-
Verlustleistung	12 W
Hardware	
CPU	Triton (ARM A17)
CPU-Kerne	3
Frequenz	1,26 GHz
RAM	2 GB
eMMC	8 GB
Bedienelemente	LEDs, Dreipunktschalter, DIP-Schalter
Integrierte SliceBus-Versorgung	✓
Anschlüsse	

Technische Daten > iC9216M-FSoE - PMC9216ES

Artikelnr.	PMC9216ES
Serial Com (Sub-D)	-
SliceBus	✓
Anzahl RJ45-Schnittstellen	4 Ports
Externe SD-Karte	
Externe SD-Karte	✓
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	abhängig von SD-Karte
Firewall	✓
SSH/SFTP	✓
Synchronisation über Ethernet (NTP)	✓
DNS	✓
IEC 61131 runtime system	
Programmspeicher	12 MB
Datenspeicher	32 MB
Remanenter Speicher	3072 KB
Echtzeituhr	
Echtzeituhr	✓
Genauigkeit Echtzeituhr	1 Minute Abweichung pro Monat
Pufferungsdauer	28 Tage @ 25°C
Execution and Synchronization Manager (ESM)	
Execution and Synchronization Manager (ESM)	✓
Min. Taskzykluszeit (ESM)	500 µs
ESM-Kerne	1
Maximum Anzahl parallele Tasks	16
SliceBus	
Prozessdaten pro Modul	bis zu 60 Bytes
Max. Moduleanzahl	64
Zykluszeit [ms]	500 µs .. 512 ms
OPC UA	
OPC UA	✓
Server	✓
Max. Anzahl parallele Verbindungen	5

Artikelnr.	PMC9216ES
Samplingraten	100 ms .. 5 s
Encryption suite Basic128Rsa15	✓
Encryption suite Basic256	✓
Encryption suite Basic256Sha256	✓
Encryption suite Aes256Sha256RsaPss	✓
Encryption suite Aes128Sha256RsaOaep	✓
Programmierung	
IEC 61131-3	✓
Web Based Management (WBM)	
Web Based Management (WBM)	✓
Ethernet	
Ethernet-fähige Anschlüsse	X3/X4: 2 Ports x 10/100 Mbit/s (Halb-/Voll duplex)
EtherCAT Master	
Anzahl der EtherCAT-Slaves	512
Aktualisierungszeit	500 µs .. 512 ms
EoE Unterstützung	-
CoE Unterstützung	✓
FoE Unterstützung	-
Distributed Clock Unterstützung	✓
Hotconnect Slaves	✓
Taktsynchronität	✓
Funktionale Sicherheit	
Minimale Zykluszeit	5 ms
Maximale Zykluszeit	15 ms
Programmspeicher sicheres Programm	64 KB
Datenspeicher	16 KB
Safety Protokoll	FSoE
Anzahl FSoE-Teilnehmer	32
Sicherheitsbezogene Eingangsdaten	512 Byte
Sicherheitsbezogene Ausgangsdaten	512 Byte
Standardeingangsdaten	128 Byte
Standardausgangsdaten	128 Byte
Max. Anzahl FB-Instanzen	512
Sicherheitsanforderungen	SIL CL 3, PL e, Kat 4
Motion	
Basis Achsanzahl	4 (Servo) + 4 (virtuell)

Artikelnr.	PMC9216ES
Zyklische Motion Aktualisierungsrate	bis zu 4 Achsen bei 250µs bis zu 16 Achsen bei 500µs bis zu 32 Achsen bei 1ms bis zu 64 Achsen bei 2ms bis zu 128 Achsen bei 4ms
Kaskadentiefe	bis zu 4
Anzahl Achsgruppen	bis zu 16 Achsen Gruppen bis zu 32 Achsen pro Gruppe
PROFINET System	
VendorID	0x0111
DeviceID	0x0368
Spezifikation	Version 2.3
PROFINET-fähige Anschlüsse	X3/X4 (lizensierbar)
Controller	✓
- Max. Anzahl Devices	64@16ms, 32@8ms, 16@4ms, 8@2ms, 4@1ms
- Zykluszeit	1 ms .. 512 ms
- Systemredundanz	✓
- Fast Startup	✓
- Fast Startup, Max. Anzahl Devices	32
- Topologie	✓
Device	✓
- Device I/O Daten	512 Byte / 512 Byte
- Zykluszeit	1 ms .. 512 ms
- MRP Client Unterstützung	✓
Gehäuse	
Material	PC
Befestigung	Profilschiene 35mm
Mechanische Daten	
Abmessungen (BxHxT)	72 mm x 134 mm x 112 mm
Gewicht Netto	488 g
Gewicht inklusive Zubehör	503 g
Gewicht Brutto	621 g
Umgebungsbedingungen	
Betriebstemperatur	0 °C bis 60 °C
Lagertemperatur	-40 °C bis 70 °C
Zertifizierungen	
Zertifizierung nach UL	-

Artikelnr.	PMC9216ES
Zertifizierung nach KC	-
Zertifizierung nach UKCA	ja
Zertifizierung nach ChinaRoHS	ja

4 Einsatz CPU iC921xM-EC

4.1 Sicherheitshinweise



Einsatz Safety-CPU → ["Einsatz CPU iC921xM-FSoE"...Seite 110.](#)



WARNUNG

Bei unsachgemäßem Einsatz der CPU können in Abhängigkeit von der Applikation schwere Gefahren für den Anwender drohen

Beachten Sie beim Umgang mit der CPU alle in diesem Kapitel aufgeführten Sicherheitshinweise.



HINWEIS

Sachschäden durch Fehlbeanspruchung

Die Schutzart IP20 (IEC 60529/EN 60529) der CPU ist für eine saubere und trockene Umgebung vorgesehen.

- Setzen Sie die CPU keiner mechanischen und/oder thermischen Beanspruchung aus, welche die beschriebenen Grenzen überschreitet.
- Beachten Sie, dass Sie die CPU für einen einwandfreien Betrieb zwingend in ein abschließbares Gehäuse oder einen abschließbaren Schaltschrank mit mindestens Schutzart IP54 einbauen müssen.



HINWEIS

Elektrostatische Entladung

Die CPU enthält Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können.

- Beachten Sie beim Umgang mit der CPU die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) gemäß EN 61340-5-1 und IEC 61340-5-1.



HINWEIS

Geräteausfall durch Fremdkörper im Gerät

Fremdkörper in der CPU können zu Fehlfunktionen bis hin zum Geräteausfall führen.

- Achten Sie darauf, dass keine Fremdkörper in die CPU (z.B. in die Lüftungsöffnungen) gelangen.



HINWEIS

Geräteausfall durch Betrieb außerhalb des zulässigen Umgebungstemperaturbereichs

Wenn Sie die CPU außerhalb des zulässigen Umgebungstemperaturbereichs betreiben, kann dies zu Fehlfunktionen bis hin zum Geräteausfall führen.

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

→ ["Zulassungen, Richtlinien, Normen"...Seite 20](#)

**HINWEIS****Geräteausfall durch Betrieb oberhalb der zulässigen Angaben für Vibration und Schock**

Wenn Sie die CPU oberhalb der zulässigen Angaben für Vibration und Schock betreiben, kann dies zu Fehlfunktionen bis hin zum Geräteausfall führen.

- Achten Sie darauf, dass beim Betrieb der CPU die zulässigen Angaben für Vibration und Schock eingehalten werden.
→ *"Zulassungen, Richtlinien, Normen"...*Seite 20

**HINWEIS****Gerätedefekt durch Verpolung**

Das Verpolen stellt für die Elektronik eine Belastung dar und kann zum Defekt der CPU führen.

- Vermeiden Sie zum Schutz der CPU eine Verpolung der DC 24V-Versorgung.

4.2 Montage



Nähere Informationen zur Montage und zur Verdrahtung → *"Grundlagen und Montage"...*Seite 23.

4.3 Lizenzhinweise zu Open Source Software

- Die CPU 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 179
- 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).*

4.4 Programmierung und Dateisystem

PLCnext Technology

- Die CPU basiert auf PLCnext Technology® von Phoenix Contact.
- Die CPU arbeitet mit einem Linux Betriebssystem.

Programmierung

- Die CPU können Sie mit iCube Engineer nach IEC 61131-3 konfigurieren und programmieren.

Firewall



- Im Auslieferungszustand ist die Firewall in der CPU deaktiviert!
- Sicherheitsempfehlung: Aktivieren Sie die Firewall!
- Im WBM können Sie unter "Security → Firewall" die Firewall aktivieren.
→ "Firewall"...Seite 199
- Bitte beachten Sie, dass Sie ausschließlich als Administrator Zugriff auf die Firewall-Einstellungen haben!

4.4.1 iCube Engineer installieren

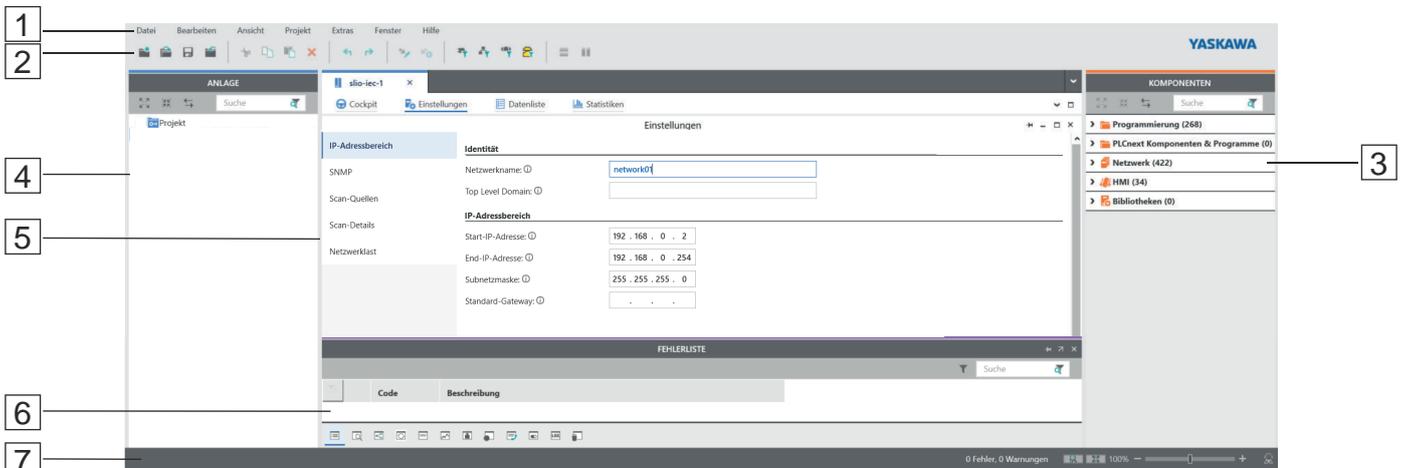
Installation

Für die Inbetriebnahme der CPU ist die Software iCube Engineer erforderlich.

1. → Laden Sie die Software iCube Engineer 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 iCube Engineer jetzt starten.

4.4.2 iCube Engineer Benutzeroberfläche

Übersicht



- | | |
|-------------------------|-----------------------------------|
| 1 Menüleiste | 5 Editorenbereich |
| 2 Symbolleiste | 6 Funktionsübergreifender Bereich |
| 3 "Komponenten"-Bereich | 7 Statusleiste |
| 4 "Anlage"-Bereich | |

Menüleiste

Die Menüleiste ermöglicht den Zugriff auf eine Reihe von projektbezogenen Befehlen, die sich nicht explizit auf eine bestimmte Engineering-Aufgabe beziehen.

Symbolleiste

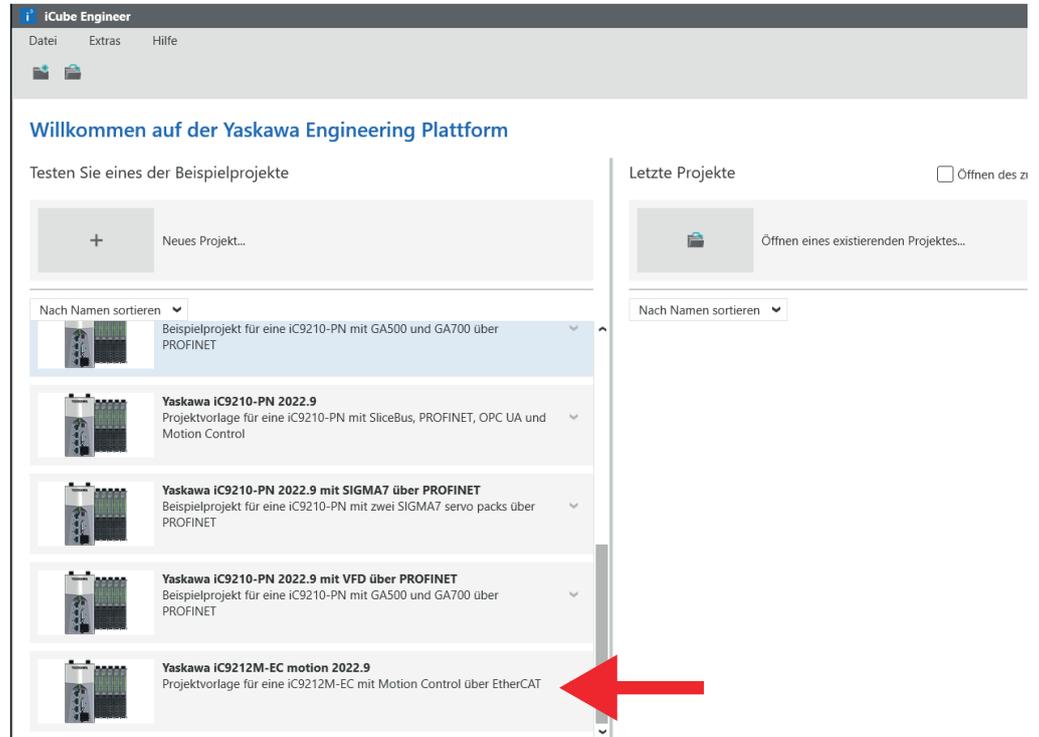
Die Symbolleiste ermöglicht den Zugriff auf eine Reihe projektbezogener Befehle, welche sich nicht explizit auf eine bestimmte Engineering-Aufgabe beziehen. Zusätzlich bieten die verschiedenen Bereiche und Editoren ihre eigenen spezifischen Symbolleisten.

"Komponenten"-Bereich	<p>Der Bereich <i>"Komponenten"</i> beinhaltet alle für das Projekt verfügbaren Komponenten. Die Komponenten lassen sich anhand ihrer Funktion in folgende Typen unterteilen:</p> <ul style="list-style-type: none"> ■ 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	<p>Im Bereich <i>"Anlage"</i> bilden Sie alle physischen und logischen Komponenten Ihrer Applikation in Form einer hierarchischen Baumstruktur ab.</p>
Editorenbereich	<ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> - Blau: Editor aus dem Bereich <i>"Anlage"</i>. - Orange: Editor aus dem Bereich <i>"Komponenten"</i>.
Funktionsübergreifender Bereich	<p>Der funktionsübergreifende Bereich beinhaltet Funktionen, welche sich über Ihr gesamtes Projekt erstrecken.</p> <ul style="list-style-type: none"> ■ FEHLERLISTE <ul style="list-style-type: none"> - Hier werden alle Fehler, Warnungen und Nachrichten des aktuellen Projekts angezeigt. ■ GLOBAL SUCHEN UND ERSETZEN <ul style="list-style-type: none"> - Hier können Sie Text im Projekt suchen und ersetzen. ■ QUERVERWEISE <ul style="list-style-type: none"> - Hier werden alle Querverweise innerhalb des Projekts angezeigt wie z.B. die Verwendung und Deklaration aller Variablentypen. ■ WATCH-FENSTER <ul style="list-style-type: none"> - Debug-Tool - hier werden im Online-Modus die aktuellen Werte der hinzugefügten Variablen angezeigt. ■ BREAKPOINTS <ul style="list-style-type: none"> - Debug-Tool - hier können Sie zur Fehlersuche Breakpoints setzen und rücksetzen. ■ CALL STACKS <ul style="list-style-type: none"> - Debug-Tool - hier wird die Reihenfolge der Aufrufe bei Ausführung des Codes angezeigt und es werden Kommandos für das Debuggen mit Breakpoints zur Verfügung gestellt. ■ LOGIKANALYSE <ul style="list-style-type: none"> - Hier lassen sich Variablenwerte zur Laufzeit aufzeichnen und visualisieren. ■ PROTOKOLL <ul style="list-style-type: none"> - Hier werden alle Fehler, Warnungen und Nachrichten ausgegeben. <ul style="list-style-type: none"> <i>"Online"</i>: Nachrichten der Laufzeitumgebung sowie andere Fehler und Warnungen, welche die Online-Kommunikation betreffen. <i>"Engineering"</i>: Nicht projektbezogene Nachrichten über Ereignisse, welche die Software betreffen wie z.B. Gerätedateien GSDML usw. ■ PAPIERKORB <ul style="list-style-type: none"> - 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 gelöschte Elemente wiederherstellen.
Statusleiste	<p>Erkannte Fehler und Warnungen werden hier angezeigt. Zusätzlich haben Sie hier bei grafischen Anwendungen eine Zoomfunktion.</p>

4.4.3 Neues Projekt erstellen

Vorgehensweise

1. Starten Sie iCube Engineer.
2. Klicken Sie auf der Startleiste auf eine Projektvorlage, welche Ihrer Firmware-Version entspricht, wie z.B. Yaskawa CPU iC921xM-x



➔ Die Projektvorlage für eine leere CPU iC921xM-x wird geöffnet.

3. Öffnen Sie "Datei → Speichern unter", vergeben Sie einen aussagekräftigen Namen für Ihr Projekt und schließen Sie den Dialog mit [Speichern].

4.5 Inbetriebnahme

4.5.1 Hinweise zur Inbetriebnahme



WARNUNG

Automatischen Anlauf verhindern

- Stellen Sie durch geeignete Maßnahmen sicher, dass ein automatischer Anlauf Ihrer Anlage/Maschine verhindert wird.



HINWEIS

Akklimatisierung vor Inbetriebnahme

Stellen Sie sicher, dass die Inbetriebnahme erst nach Akklimation der CPU und der zugehörigen Module erfolgt!



HINWEIS

Beschädigung durch unsachgemäße Handhabung

- Gehen Sie sorgfältig mit der CPU und den Komponenten um!
- Beachten Sie bei der Installation der CPU und der Komponenten, dass mechanische Beschädigungen vermieden werden!

**HINWEIS****Anlauf der CPU nicht sichergestellt**

- Für den ordnungsgemäßen Anlauf der CPU ist das Einschalten der Versorgungsspannung frühestens 30 Sekunden nach Erlöschen der Geräte-LEDs erlaubt.

**HINWEIS****Unerlaubter Zugriff auf die SD-Karte möglich**

Der Zugriff auf die SD-Karte ist möglich, sodass Daten gelesen und manipuliert werden können.

- Beachten Sie → ["Hinweise zur Security" ...Seite 14](#), besonders hinsichtlich eines Zugriffsschutzes für die SD-Karte.



Bedienung und Programmierung dürfen ausschließlich von qualifiziertem Personal durchgeführt werden!

4.5.2 Online-Zugriff auf die CPU

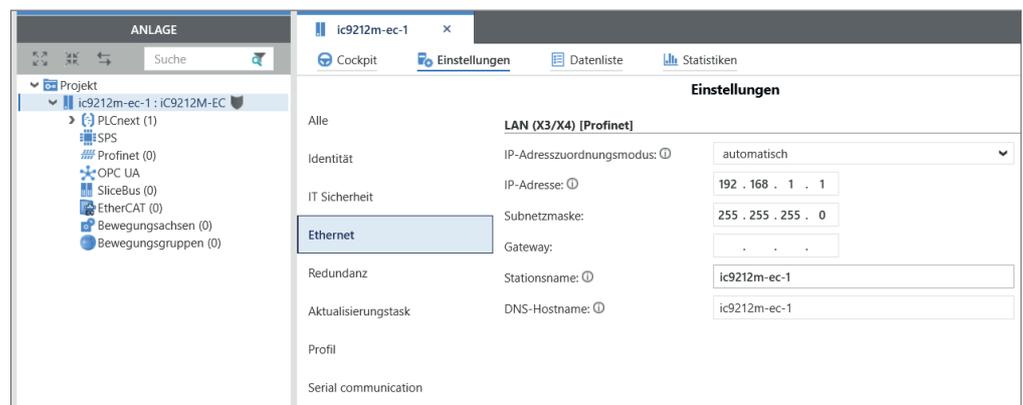
IP-Adress-Parameter für die Kommunikation

Im Auslieferungszustand sind in der Projektvorlage der CPU folgende IP-Adress-Parameter für die Kommunikation voreingestellt:

- Ethernet-Port (X3/X4): 192.168.1.1
- Subnetzmaske: 255.255.255.0
- Gateway: -

Sollte Ihre CPU andere IP-Adress-Parameter besitzen, können Sie diese für iCube Engineer nach folgender Vorgehensweise anpassen:

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



4. Die IP-Adress-Parameter für die Verbindung über den Ethernet-Port (X3/X4) können Sie unter **"LAN (X3/X4)"** einstellen.
 - ➔ Beim Aufbau einer Ethernet-Verbindung zur CPU verwendet iCube Engineer die hier angegebenen IP-Adress-Parameter für die entsprechende Schnittstelle.

Mit der CPU verbinden



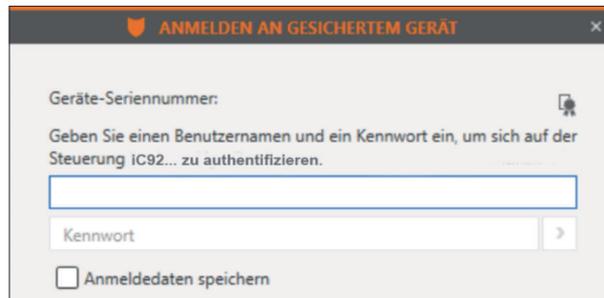
Bitte beachten Sie, dass die Online-Suche aktuell nur vom Port X3/X4 unterstützt wird!

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

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



- ➔ Eine Verbindung zwischen iCube Engineer und Ihrer CPU wird, unter Verwendung der IP-Adress-Parameter, aufgebaut und der Anmeldedialog zur Authentifizierung geöffnet.



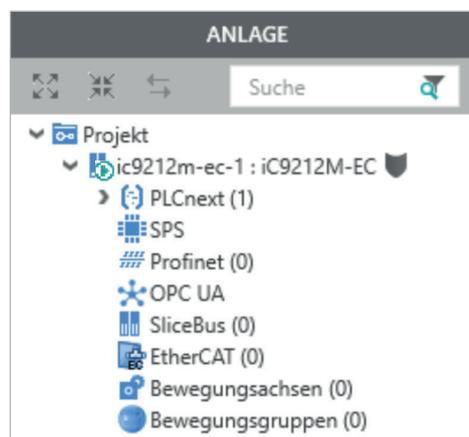
3. ➔ Geben Sie Ihre Zugangsdaten an und klicken Sie auf .



Im Auslieferungszustand sind folgende Zugangsdaten mit Administratorrechten voreingestellt:

- *Benutzername: admin*
- *Das Passwort befindet sich unter der Frontklappe auf die Frontseite der CPU aufgedruckt.*

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



4.5.2.1 Neue IP-Adress-Parameter zuweisen

Zuweisung über WBM

Sobald Sie online mit der CPU 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].



Im Auslieferungszustand sind folgende Zugangsdaten mit Administratorrechten voreingestellt:

- *Benutzername: admin*
- *Das Passwort befindet sich unter der Frontklappe auf die Frontseite der CPU aufgedruckt.*

- ➔ Sie haben jetzt Zugriff auf das WBM der CPU 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.

TCP/IP (LAN 1) - Separated Mode	Status	Konfiguration
IP-Adresse	192.168.1.11	<input type="text" value="192.168.1.11"/>
Subnetzmaske	255.255.255.0	<input type="text" value="255.255.255.0"/>
Standard-Gateway	192.168.1.1	<input type="text" value="192.168.1.1"/>
DNS-Serveradressen	8.8.8.8	<input type="text" value="8.8.8.8"/>
	8.8.4.4	<input type="text" value="8.8.4.4"/>
MAC-Adresse	BE:FA:66:E9:FD:76	<input type="text"/>
Port X1		
Datenrate	100 Mbit/s	<input type="text"/>
Duplexmodus	Voll duplex	<input type="text"/>
Link-Status	Linkup	<input type="text"/>

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 CPU übertragen und zur Aktivierung die CPU automatisch neu gestartet.



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

4.6 Speichermanagement

4.6.1 Interner Speicher

Übersicht



Bitte beachten Sie, dass abhängig von der Firmware und den eingesetzten Komponenten, nicht der komplette Speicherbereich zur Verfügung steht.

Speicher

- Nur PMC9212Ex:
 - 2GB Arbeitsspeicher (RAM).
 - 12MB Programmspeicher.
 - 32MB Datenspeicher.
 - 512kB permanenter Datenspeicher.
- Nur PMC9216Ex:
 - 2GB Arbeitsspeicher (RAM).
 - 12MB Programmspeicher.
 - 32MB Datenspeicher.
 - 3072kB permanenter Datenspeicher.

Arbeitsspeicher

- Während des Betriebs legt das Betriebssystem temporäre Daten und Teile des Anwenderprogramms im *Arbeitsspeicher* ab.
- Durch MRESET können Sie ohne Powercycle die CPU in den Zustand *Ready* versetzen. Hierbei wird u.a. der Arbeitsspeicher entladen. ➔ ["MRESET"...Seite 98](#)

Parametrierungsspeicher

Der *Parametrierungsspeicher* als Summe aus Programm- und Datenspeicher bietet Speicher für:

- Aktuelle Firmware-Version
- *Überlagerndes Dateisystem* für Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen.

Verwendung des *überlagernden Dateisystems*:

- Sobald Sie die CPU projektieren bzw. Änderungen an der aktuellen Firmware-Version vornehmen, werden Daten im *überlagernden Dateisystem* erzeugt.
- Durch *"Rücksetzen auf Werkseinstellung Typ 1"* können Sie u.a. das *überlagernde Dateisystem* löschen. Hierbei bleibt die aktuelle Firmware-Version bestehen, aber alle Änderungen daran werden verworfen. ➔ ["Rücksetzen auf Werkseinstellung Typ 1"...Seite 98](#)
- Durch *"Rücksetzen auf Werkseinstellung Typ 2"* können Sie u.a. das *überlagernde Dateisystem* und die aktuelle Firmware-Version löschen. Hierbei wird die aktuelle Firmware-Version durch die ursprüngliche Firmware-Version überschrieben und somit der Auslieferungszustand der CPU wieder hergestellt. ➔ ["Rücksetzen auf Werkseinstellung Typ 2"...Seite 99](#)

**VORSICHT****Beschädigung des internen Parametrierungsspeichers durch hohen Datenverkehr!**

- Durch häufige Schreibzugriffe bei Applikationen mit hohem Datenverkehr wie z.B. Data-Logger-Applikationen auf das überlagernde Dateisystem kann der interne Parametrierungsspeicher der CPU langfristig beschädigt werden und zu einem Gerätedefekt führen.
- Nutzen Sie für Applikationen mit hohem Datenverkehr eine externe Yaskawa SD-Karte als Speichermedium für das überlagernde Dateisystem.

Nichtflüchtiger Speicher für remanente Daten

- Hier werden alle Daten, welche bei der Projektierung in iCube Engineer als remanent gekennzeichnet wurden, dauerhaft abgelegt.
- Bei Stromausfall werden remanente Daten automatisch gesichert.
- Durch MRESET bzw. Rücksetzen auf Werkseinstellung Typ 1/2 können Sie u.a. den nichtflüchtigen Speicher für remanente Daten löschen.

Speicherüberlauf beheben

Sollte es während des Betriebs bzw. beim Anlaufen der CPU zu der Fehlermeldung kommen, dass der Speicher des überlagernden Dateisystems im Parametrierungsspeicher übergelaufen ist, können Sie die CPU über den *Safe Mode* nach folgender Vorgehensweise wieder starten:

1. Schalten Sie die Spannungsversorgung der CPU aus.
2. Bringen Sie die DIP-Schalter S1 unter der Frontklappe in folgende Stellung:

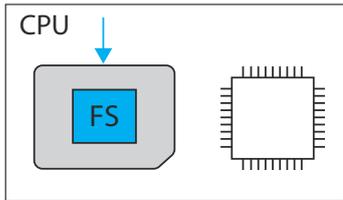
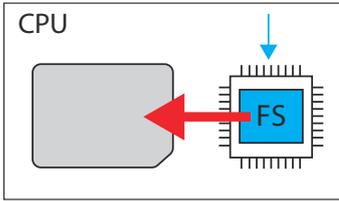
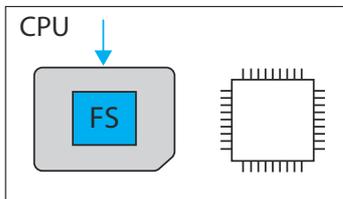
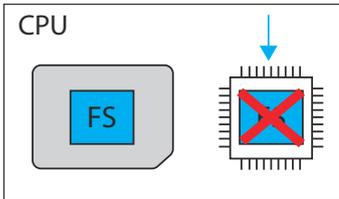
S1	S1-1	S1-2	Aktion
01 	ON	OFF	Nach PowerON startet die CPU im <i>Safe Mode</i> .

3. Schalten Sie die Spannungsversorgung der CPU wieder ein.
 - ➔ Die CPU startet im *"Safe Mode"...*Seite 99. Hierbei wird ein ausschließlich für den *Safe Mode* reservierter Speicherbereich freigegeben, der es ermöglicht, dass die CPU bei einem Speicherüberlauf wieder anlaufen kann. Im *Safe Mode* startet die CPU mit einem Default-Projekt, Ihr Anwenderprogramm ist aber weiterhin im Dateisystem vorhanden.
4. Überprüfen Sie Ihr Anwenderprogramm nach Dateien auf dem Dateisystem, welche das System zum Überlauf bringen wie z.B. Log-Dateien, Rezepte, Bewegungsdaten. Verwenden Sie für den Zugriff auf das Dateisystem einen SSH-Client und löschen Sie ggf. die verursachenden Dateien. Starten Sie danach wieder im *Standard Mode*.
5. Schalten Sie hierzu die Spannungsversorgung der CPU aus.
6. Bringen Sie die DIP-Schalter S1 in die Default-Stellung:

S1	S1-1	S1-2	Aktion
01 	OFF	OFF	Nach PowerON startet die CPU im <i>Standard Mode</i> - Defaulteinstellung.

7. Schalten Sie die Spannungsversorgung der CPU wieder ein.
 - ➔ Die CPU startet wieder im *Standard Mode*. Wurde im *Safe Mode* ein Projekt geladen, wird dieses im Betriebszustand RUN ausgeführt.

4.6.2 Steckplatz für Yaskawa SD-Karte

Power 0 → 1 Power 0 → 1 

- Auf diesem Steckplatz können Sie ausschließlich eine Yaskawa SD-Karte mit gültiger Lizenzdatei stecken.
- Im WBM können Sie unter "Security → SD-Karte" den Einsatz der SD-Karte aktivieren bzw. deaktivieren und Informationen über diese abrufen. Per Default ist der Einsatz der SD-Karte aktiviert. → "SD-Karte"...Seite 203
- Eine gesteckte Yaskawa SD-Karte wird ausschließlich nach NetzEIN von der CPU erkannt.
- Wird nach NetzEIN eine neue noch unbenutzte Yaskawa SD-Karte erkannt, wird das *überlagernde Dateisystem*  mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen vom internen Parametrierungsspeicher auf die Yaskawa SD-Karte verschoben und im internen Parametrierungsspeicher gelöscht. Von nun an verwendet die CPU das überlagernde Dateisystem auf der Yaskawa SD-Karte.
- Wird nach NetzEIN eine Yaskawa SD-Karte erkannt, auf der sich schon ein *überlagerndes Dateisystem*  befindet, so wird das überlagernde Dateisystem im internen Parametrierungsspeicher gelöscht, ohne dieses zu verschieben. Von nun an verwendet die CPU das vorhandene überlagernde Dateisystem auf der Yaskawa SD-Karte.

**WARNUNG**

Datenverlust - Kartenentnahme nur bei ausgeschalteter Spannungsversorgung!

Entnehmen Sie die Yaskawa SD-Karte nur dann, wenn die Versorgungsspannung der CPU ausgeschaltet ist. Ansonsten führt dies zu Datenverlust!

**Generelle Hinweise zum Einsatz der Yaskawa SD-Karte**

- Es werden ausschließlich Yaskawa SD-Karten unterstützt.
- Die Karten sind vorformatiert (ext4-Format) für den Einsatz in CPUs der iC9200 Series.
- Durch eine erneute Formatierung gehen bestimmte Informationen auf der Yaskawa SD-Karte verloren, welche für den Einsatz in den CPUs der iC9200 Series erforderlich sind.
- Schließen Sie aus, dass die Yaskawa SD-Karte formatiert wird.
- Die Yaskawa SD-Karte kann jederzeit mit einem herkömmlichen SD-Kartenleser gelesen werden. Sensible Daten auf der Yaskawa SD-Karte können ausgelesen werden, wenn Sie diese nicht physisch vor unbefugtem Zugriff schützen.
- Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die Yaskawa SD-Karte haben.



Bitte beachten bei Einsatz ohne Yaskawa SD-Karte!

- Per Default ist die Unterstützung der Yaskawa SD-Karte aktiviert.
- Deaktivieren Sie die Unterstützung der Yaskawa SD-Karte, wenn Sie die CPU ohne Yaskawa SD-Karte betreiben möchten.
- Bleibt die Unterstützung der Yaskawa SD-Karte aktiviert und wird die CPU ohne Yaskawa SD-Karte betrieben, besteht die Gefahr von Datendiebstahl oder Datenmanipulation.
 - Unbefugte Personen können eine Yaskawa SD-Karte einsetzen und die CPU neu starten.
 - Wird nach NetzEIN eine neue noch unbenutzte Yaskawa SD-Karte erkannt, wird das überlagernde Dateisystem mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen, vom internen Parametrierungsspeicher auf die Yaskawa SD-Karte verschoben und im internen Parametrierungsspeicher gelöscht. Dort gespeicherte Projekte und IP-Konfigurationen sind dann nicht mehr verfügbar!
- Beim Wechsel zum Betrieb ohne Yaskawa SD-Karte wird nach NetzEIN der CPU das überlagernde Dateisystem des internen Parametrierungsspeichers aktiviert und von nun an verwendet. Bitte beachten Sie, dass hierbei *keine* Daten von der Yaskawa SD-Karte übernommen werden. Auch gibt es keine Funktion zur Rückübertragung von der Yaskawa SD-Karte auf den internen Parametrierungsspeicher.

Yaskawa SD-Karte



Die Yaskawa SD-Karte besitzt folgende Beschriftung und Bedienelemente:

- 1 Bestellnummer
- 2 Produktversion
- 3 Seriennummer
- 4 Schieber für Schreibschutz - hier deaktiviert dargestellt.
- 5 Speichergröße
- 6 Bezeichnung

- 1 In dieser Position ist der Schreibschutz deaktiviert - Auslieferungszustand.
- 2 In dieser Position ist der Schreibschutz aktiviert und die SD-Karte vor versehentlichem Überschreiben geschützt.

MRESET und Rücksetzen auf Werkseinstellungen

4.7 MRESET und Rücksetzen auf Werkseinstellungen

MRESET

- Die CPU wird in den Zustand *Ready* gebracht.
 - Der Arbeitsspeicher wird entladen, hierbei bleibt das Anwenderprogramm im überlagernden Dateisystem erhalten.
 - Der nichtflüchtige Speicher für remanente Daten wird gelöscht.
1. Bringen Sie Ihre CPU in STOP.
 2. Drücken Sie den Betriebsartenschalter nach unten in Stellung MR.
 3. Lassen Sie den Betriebsartenschalter nach 3 Sekunden los und drücken Sie diesen innerhalb von 3 Sekunden wieder in Stellung MR.
 4. Lassen Sie den Betriebsartenschalter nach 3 Sekunden wieder los.
 - ➔ ■ Die CPU führt jetzt ein MRESET durch.
 - Zur Bestätigung erhalten Sie eine Diagnose-Meldung, dass ein MRESET durchgeführt wurde. Diese können Sie z.B. in iCube Engineer über "Benachrichtigungen" im Editor "Cockpit" ausgeben lassen.

Rücksetzen auf Werkseinstellung Typ 1

- Das überlagernde Dateisystem mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen wird gelöscht.
- Der nichtflüchtige Speicher für remanente Daten wird gelöscht.
- Die aktuelle Firmware-Version bleibt bestehen, aber alle Änderungen daran werden verworfen.

Mit Betriebsartenschalter

1. Schalten Sie die Spannungsversorgung der CPU aus.
2. Drücken und halten Sie den Betriebsartenschalter in Stellung MR und schalten Sie die Spannungsversorgung der CPU wieder ein.
3. Sobald nach dem Anlauf die LEDs folgendes Verhalten zeigen, lassen Sie den Betriebsartenschalter wieder los:

Status	RN	ER	IO ER	PN-C ER	PN-D ER	IO DIAG
gelb 1Hz	grün	rot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- ➔ Die CPU führt jetzt ein Rücksetzen auf *Werkseinstellung Typ 1* durch.

Mit DIP-Schalter S1

1. Schalten Sie die Spannungsversorgung der CPU aus.
2. Bringen Sie die DIP-Schalter S1 unter der Frontklappe in folgende Stellung:

S1	S1-1	S1-2	Aktion
01 1 2	OFF	ON	Nach PowerON führt die CPU Rücksetzen auf <i>Werkseinstellung Typ 1</i> durch.

3. Schalten Sie die Spannungsversorgung der CPU wieder ein.
Nach dem Hochlauf der CPU führt diese ein Rücksetzen auf *Werkseinstellung Typ 1* durch und zeigt folgendes LED-Verhalten:

Status	RN	ER	IO ER	PN-C ER	PN-D ER	IO DIAG
gelb 1Hz	grün	rot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Nach dem Rücksetzen auf *Werkseinstellung Typ 1* fordert die CPU einen Power-cycle an:

Status	RN	ER	IO ER	PN-C ER	PN-D ER	IO DIAG
gelb 2Hz	1Hz	1Hz	1Hz	1Hz	1Hz	1Hz

4. Schalten Sie die Spannungsversorgung der CPU aus.
5. Bringen Sie die DIP-Schalter S1 in die Default-Stellung:

S1	S1-1	S1-2	Aktion
	OFF	OFF	Nach PowerON startet die CPU im <i>Standard Mode</i> - Defaulteinstellung.

6. Schalten Sie die Spannungsversorgung der CPU wieder ein.
 - ➔ Die CPU startet wieder im *Standard Mode*.

Rücksetzen auf Werkseinstellung Typ 2

- Das überlagernde Dateisystem mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen wird gelöscht.
- Der nichtflüchtige Speicher für remanente Daten wird gelöscht.
- Die aktuelle Firmware-Version wird durch die ursprüngliche Firmware-Version überschrieben und somit der Auslieferungszustand der CPU wieder hergestellt.

1. Schalten Sie die Spannungsversorgung der CPU aus.
2. Drücken und halten Sie den Betriebsartenschalter in Stellung MR und schalten Sie die Spannungsversorgung der CPU wieder ein.
3. Sobald nach dem Anlauf die LEDs folgendes Verhalten zeigen, lassen Sie den Betriebsartenschalter wieder los (Dauer ca. 30s):

Status	RN	ER	IO ER	PN-C ER	PN-D ER	IO DIAG
 gelb 2Hz	 grün	 rot	 rot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- ➔ Die CPU führt jetzt ein Rücksetzen auf *Werkseinstellung Typ 2* durch und befindet sich danach im Auslieferungszustand.

4.8 Firmware-Update

Ein Firmware-Update können Sie über Web-based Management WBM durchführen.
 ➔ ["Firmware-Update"...Seite 215](#)



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

4.9 Safe Mode

Starten im Safe Mode

Mittels der DIP-Schalter "S1" unter der Frontklappe können Sie Ihre CPU im *Safe Mode* starten lassen. Hierbei startet die CPU mit folgendem Verhalten:

- Die CPU geht in RUN mit dem Default-Projekt.
- Ein Projekt kann geladen aber nicht ausgeführt werden.
- Der SliceBus wird abgeschaltet.
- Alle Feldbusse werden deaktiviert.
- Der Parametrierungsspeicher mit der aktuellen Firmware-Version und dem überlagernden Dateisystem bleibt unverändert.
- Beim Online-Zugriff erhalten Sie eine Information, dass sich die CPU im *Safe Mode* befindet.
- Der *nichtflüchtige Speicher* für remanente Daten bleibt unverändert.

Safe Mode

- Die CPU ist ausschließlich über die Default-IP-Adresse erreichbar.
- Zusätzlich wird ein ausschließlich für den *Safe Mode* reservierter Speicherbereich freigegeben, der es ermöglicht, dass die CPU bei einem Speicherüberlauf wieder anlaufen kann.

1. Schalten Sie die Spannungsversorgung der CPU aus.

2. Bringen Sie die DIP-Schalter S1 unter der Frontklappe in folgende Stellung:

S1	S1-1	S1-2	Aktion
01 	ON	OFF	Nach PowerON startet die CPU im <i>Safe Mode</i> .

3. Schalten Sie die Spannungsversorgung der CPU wieder ein.

- ➔ Die CPU startet im *Safe Mode* und zeigt dies ausschließlich beim Online-Zugriff an.

Starten im *Standard Mode*

1. Schalten Sie die Spannungsversorgung der CPU aus.

2. Bringen Sie die DIP-Schalter S1 in die Default-Stellung:

S1	S1-1	S1-2	Aktion
01 	OFF	OFF	Nach PowerON startet die CPU im <i>Standard Mode</i> - Defaulteinstellung.

3. Schalten Sie die Spannungsversorgung der CPU wieder ein.

- ➔ Die CPU startet wieder im *Standard Mode*. Wurde im *Safe Mode* ein Projekt geladen, wird dieses im Betriebszustand RUN ausgeführt.

4.10 Systemvariablen und Zustandsinformationen

4.10.1 Allgemeines

Zugriff auf Systemvariablen und Datenstrukturen

- In diesem Kapitel werden Systemvariablen beschrieben, die für die CPU zur Verfügung stehen.
- Die CPU besitzt einen Registersatz, der zur Diagnose und zur einfachen Steuerung der CPU eingesetzt wird.
- Die Diagnosedaten werden im Diagnose-Statusregister und im Diagnose-Parameterregister abgelegt. Diese Register stehen dem Anwendungsprogramm als Systemvariablen (Systemmerker, globale Variablen) zur Verfügung.
- Einige Systemvariablen der CPU sind als Datenstrukturen organisiert. Die Datenstruktur einer solchen Systemvariable beinhaltet dabei weitere Systemvariablen.
- Im *"Init-Werteeditor"* von iCube Engineer können Sie einsehen, welche Systemvariablen im Einzelnen zu einer als Datenstruktur organisierten Systemvariable gehören.

Um den *"Init-Werteeditor"* für eine als Datenstruktur organisierten Systemvariable zu öffnen, gehen Sie wie folgt vor:

1.  Doppelklicken Sie im Bereich Anlage auf den Knoten SPS.
 - ➔ Die Editorengruppe der CPU/SPS wird geöffnet.
2.  Wählen Sie den Editor Datenliste.



Alternativ können Sie den Editor Datenliste im Bereich Anlage über den Knoten der CPU öffnen.

3.  Öffnen Sie den Bereich Systemvariablen.
4.  Klicken Sie in der Spalte Variable (SPS) auf den Pfeil, zur Anzeige der erweiterten Informationen.
 - ➔ In der Spalte Typ der erweiterten Informationen wird der Datentyp der Systemvariablen angezeigt.
5.  Markieren Sie die Zeile der als Datenstruktur organisierten Systemvariable, deren zugehörige Systemvariablen Sie einsehen möchten. Klicken Sie hierzu auf die erste Spalte in der Zeile der als Datenstruktur organisierten Systemvariable.
6.  Klicken Sie auf die Schaltfläche .
 - ➔ Der *"Init-Werteeditor"* der gewählten als Datenstruktur organisierten Systemvariable wird unterhalb des Editors Datenliste geöffnet.

The screenshot shows the 'Datenliste' window with the following table:

Variable (SPS)	Typ	Verw.	Kommentar	Init.
PND_S1_OUTPUTS	PND_IO_...	Global	Output proc...	
PND_S1_INPUTS	PND_IO_...	Global	Input proces...	
PND_IO_DRIVEN_BY_PLC	INT	Global		INT#0
ESM_DATA	ESM_DAT	Global		
RTC	RTC_TYPE	Global		
DEVICE_STATE	DEVICE_S...	Global		
USER_PARTITION	PARTITIO...	Global		

The 'Init-Werteeditor' window shows the following table:

Elementname	Init-Wert Element
HOURS	USINT#0
MINUTES	USINT#0
SECONDS	USINT#0
DAY	USINT#0
MONTH	USINT#0
YEAR	UINT#0

Im "Init-Werteeditor" werden in der Spalte Elementname alle Systemvariablen aufgelistet, welche in der als Datenstruktur organisierten Systemvariable enthalten sind.

4.10.2 Systemvariablen

Systemzeit

- Die Systemvariable RTC ist eine als Datenstruktur organisierte Systemvariable.
- Mit der Systemvariable RTC können Sie Informationen zur Systemzeit der geräteinternen Echtzeituhr abrufen.

Systemvariable	Typ - Beschreibung
RTC	RTC_TYPE - Datenstruktur
HOURS	USINT - Systemzeit (Stunden)
MINUTES	USINT - Systemzeit (Minuten)
SECONDS	USINT - Systemzeit (Sekunden)
DAY	USINT - Systemzeit (Tag)
MONTH	USINT - Systemzeit (Monat)
YEAR	UINT - Systemzeit (Jahr)

Funktionsbausteine
TLS_SOCKET_2
UDP_SOCKET_2

- Mit dem Funktionsbaustein TLS_SOCKET_2 öffnen und schließen Sie IP-Sockets für die IP-Kommunikation über TCP (Transmission Control Protocol - nicht sicher) oder TLS (Transport Layer Security - sicher). Mit dem Eingabeparameter START_TLS können Sie dies steuern (FALSE: TCP, TRUE: TLS).
- Mit dem Baustein UDP_SOCKET_2 öffnen und schließen Sie IP-Sockets für die IP-Kommunikation über UDP (User Datagram Protocol).
- Die Anzahl der geöffneten IP-Sockets können Sie mit den folgenden Systemvariablen abrufen:

Systemvariable	Typ - Beschreibung
IP_ACTIVE_SOCKETS	UINT - Anzahl der mit den Funktionsbausteinen TLS_SOCKET_2 und UDP_SOCKET_2 geöffneten TCP/UDP-Sockets.
TLS_ACTIVE_SOCKETS	UINT - Anzahl der mit dem Funktionsbaustein TLS_SOCKET geöffneten TLS-Sockets.

Gerätestatus

- Die Systemvariable DEVICE_STATE ist eine als Datenstruktur organisierte Systemvariable.
- Mit der Systemvariable DEVICE_STATE können Sie verschiedene Informationen zum Gerätestatus der CPU abrufen.

Systemvariable	Typ - Beschreibung
DEVICE_STATE	DEVICE_STATE_X152_TYPE - Datenstruktur
BOARD_TEMPERATURE	SINT - Temperatur im Gehäuseinneren (in °C).
reserved1	BOOL - reserviert
reserved2	USINT - reserviert
CPU_LOAD_ALL_CORES	USINT - durchschnittliche aktuelle Auslastung aller Prozessorkerne (in %).
CPU_LOAD_PER_CORE	CPU_LOAD_PER_CORE_ARRAY - Informationen zur Auslastung je Prozessorkern.
[1]	USINT - aktuelle Auslastung Prozessorkern 1 (in %).
[2]	USINT - aktuelle Auslastung Prozessorkern 2 (in %).

Systemvariablen und Zustandsinformationen > Systemvariablen

Partition

- Die Systemvariable USER_PARTITION ist eine als Datenstruktur organisierte Systemvariable.
- Mit der Systemvariable USER_PARTITION können Sie verschiedene Informationen und Speicherstatistiken zur Anwenderpartition (überlagerndes Dateisystem) abrufen.
- Die Partition kann sich auf der externen Yaskawa SD-Karte oder auf dem internen Speicher befinden.
- Der Speicher ist in Blöcken organisiert.
- Ein Block hat eine konstante, festgelegte Größe und eine Datei belegt immer einen oder mehrere Blöcke.
- Eine bestimmte Anzahl an Blöcken ist im Linux-System für den Root-Benutzer reserviert. Diese reservierten Blöcke sind ausschließlich für den Root-Benutzer verfügbar und sichern dessen Handlungsfähigkeit auch bei belegtem Speicher (z.B. für Log-Ausgaben).

Systemvariable	Typ - Beschreibung
USER_PARTITION	PARTITION_INFO - Datenstruktur
MEM_TOTAL	ULINT - Gesamtspeicher der Partition in Bytes (inklusive reservierter Blöcke).
MEM_FREE	ULINT - freier, zur Verfügung stehender Speicher in Bytes (ohne reservierte Blöcke).
MEM_USED	ULINT - belegter Speicher in Bytes (inklusive reservierter Blöcke).
MEM_USAGE	ULINT - genutzter Speicher in % (ohne reservierte Blöcke).

Task-Handling

- Programme und Programmteile werden in iCube Engineer als Tasks behandelt.
- Die Koordination und Abarbeitung der einzelnen Tasks übernimmt der **Execution & Synchronization Manager (ESM)**.
- Mit der Systemvariable ESM_DATA können Sie Informationen über das Task-Handling des ESM abrufen.
- ESM_DATA ist eine als Datenstruktur organisierte Systemvariable.

Systemvariable	Typ - Beschreibung
ESM_DATA	ESM_DAT - Datenstruktur
ESM_COUNT	USINT - Anzahl der ESM (jeweils ein ESM pro Prozessorkern).
ESM_INFOS	ESM_INFO_ARRAY
[1] ... [2]	ESM_INFO - Informationen zu den ESM [1 ... 2] ² .
TASK_COUNT	UINT - Anzahl der Tasks, die für den ESM projiziert wurden.
TICK_COUNT	UDINT - immer 0.
TICK_INTERVAL	UDINT - immer 0.
TASK_INFOS	TASK_INFO_ARRAY
[1] ... [16]	TASK_INFO - Informationen zu den Tasks [1 ... 16].
INTERVAL ¹	LINT - Zeitintervall <ul style="list-style-type: none"> ■ Bei zyklischen Tasks: Zeitintervall in µs ■ Bei azyklischen Tasks: 0
PRIORITY ¹	INT - Priorität der Task

Systemvariable	Typ - Beschreibung
WATCHDOG ¹	LINT - Watchdog-Zeit in μs (0 = kein Watchdog). <ul style="list-style-type: none"> Watchdog-Zeit, die Sie für die Summe aus Ausführungsdauer und Verzögerungszeit definieren. Wird die Watchdog-Zeit überschritten, löst der Watchdog aus.
LAST_EXEC_DURATION	LINT - Ausführungsdauer der Task im vorigen Zyklus in μs . <ul style="list-style-type: none"> Dies schließt auch Unterbrechungen durch höherpriorie Tasks ein.
MIN_EXEC_DURATION	LINT - Minimale Ausführungsdauer der Task in μs . <ul style="list-style-type: none"> Dies schließt auch Unterbrechungen durch höherpriorie Tasks ein.
MAX_EXEC_DURATION	LINT - Maximale Ausführungsdauer der Task in μs . <ul style="list-style-type: none"> Dies schließt auch Unterbrechungen durch höherpriorie Tasks ein.
LAST_ACTIVATION_DELAY	LINT - Verzögerungszeit der Task im vorigen Zyklus in μs . <ul style="list-style-type: none"> Eine Verzögerung entsteht, wenn zum Zeitpunkt der Task-Aktivierung höherpriorie Tasks anstehen.
MIN_ACTIVATION_DELAY	LINT - Minimale Verzögerungszeit der Task in μs . <ul style="list-style-type: none"> Eine Verzögerung entsteht, wenn zum Zeitpunkt der Task-Aktivierung höherpriorie Tasks anstehen.
MAX_ACTIVATION_DELAY	LINT - Maximale Verzögerungszeit der Task in μs . <ul style="list-style-type: none"> Eine Verzögerung entsteht, wenn zum Zeitpunkt der Task-Aktivierung höherpriorie Tasks anstehen.
EXEC_TIME_THRESHOLD ¹	LINT - Schwellwert, den Sie für die Summe aus Ausführungsdauer und Verzögerungszeit definieren können.
EXEC_TIME_THRESHOLD_CNT	UDINT - Wenn der definierte Schwellwert EXEC_TIME_THRESHOLD überschritten wird, wird der Wert der Variable EXEC_TIME_THRESHOLD_CNT inkrementiert.
NAME ¹	STRING - Name der Task.
EXCEPTION_COUNT	USINT - Anzahl der Ausnahmen.
EXCEPTION_INFOS	ESM_EXCEPTION_INFO_ARRAY
[1] ... [2]	ESM_EXCEPTION_INFO - Informationen zu den Ausnahmen [1 ... 2] ² .
TYPE_ID	UDINT - ID der Ausnahme.
SUB_TYPE	STRING512 - Typ der Ausnahme.
SUB_TYPE_ID	UDINT - ID der Task, in der die Ausnahme aufgetreten ist.
TASK_NAME	STRING - Name der Task, in der die Ausnahme aufgetreten ist.
PROGRAM_NAME	STRING512 - Name der Programminstanz, in der die Ausnahme aufgetreten ist.
INFORMATION	STRING512 - Informationen zur aufgetretenen Ausnahme.

1) Sie können die Systemvariable in der Software iCube Engineer im Editor Tasks und Events einstellen.

2) Bitte beachten Sie, dass manche CPUs nur ESM1 unterstützen. ➔ ["Technische Daten"...Seite 70](#)

SliceBus Systemvariablen



- Bitte beachten Sie, dass die System SLIO Power- und Klemmen-Module keine Typ-Kennung besitzen. Diese können nicht erkannt werden und werden somit bei der Auflistung bzw. Zuordnung der Steckplätze nicht berücksichtigt.
- Die Zählung der Steckplätze beginnt bei 1, d.h. der 1. Steckplatz entspricht Bit 0 im entsprechenden Diagnose-Register.
- Ein Diagnosealarm wird nicht automatisch quittiert. Die Quittierung erfolgt durch Lesen der Diagnose. Solange ein Diagnosealarm nicht quittiert ist, wird auf diesem Steckplatz kein weiterer Diagnosealarm ausgegeben.

Behandlung von Diagnosealarmen

- Sobald ein Modul über den Rückwandbus einen Diagnosealarm meldet, wird dieser von der CPU automatisch erkannt und das dem Steckplatz entsprechende Register-Bit in `SB_DIAG_ALARM_STATUS` gesetzt.
- Für das Modul muss im iCube Engineer der Diagnosealarm aktiviert sein.
- Durch Lesen von Datensatz 0x00 (Diagnose) bzw. 0x01 (erweiterte Diagnose) vom entsprechenden Steckplatz können Sie eine Diagnosemeldung quittieren. Informationen zum Aufbau der Diagnose-Datensätze finden Sie im Handbuch zum entsprechenden System SLIO Modul.
- In iCube Engineer können Sie mit dem Baustein `Y_SB_DataRecordRead` aus der Systembibliothek den entsprechenden Datensatz lesen. Hierzu müssen Sie zuvor Ihrem Projekt die Systembibliothek "`Y_SliceBus.pcwlx`" hinzufügen.

Systemvariable	Typ - Beschreibung
SB_DATA_VALID	BOOL - Busaktivität <ul style="list-style-type: none"> ■ Diese Variable ist gesetzt, wenn der Datentransfer über den <i>SliceBus</i> aktiv ist.
SB_TOPOLOGY_OK	BOOL - Bus-Topologie <ul style="list-style-type: none"> ■ Diese Variable ist gesetzt, wenn die gesteckten Module am <i>SliceBus</i> mit der Konfiguration übereinstimmen.
SB_DIAG_ALARM_STATUS	ULINT - Diagnose-Status der Module <ul style="list-style-type: none"> ■ Sobald ein Modul am <i>SliceBus</i> einen Diagnosealarm meldet, wird zur entsprechenden Steckplatzposition das zugehörige Bit im 64Bit großen Register gesetzt.
SB_DIAG_ALARM_ACK_PENDING	ULINT - Quittierung Diagnose-Status der Module <ul style="list-style-type: none"> ■ Sobald ein Modul am <i>SliceBus</i> eine Quittierung des Diagnosealarms anfordert, wird zur entsprechenden Steckplatzposition das zugehörige Bit im 64Bit großen Register gesetzt.

EtherCAT-Systemvariablen

Nachfolgend sind die Systemvariablen zur Diagnose des EtherCAT-Master und der angebotenen EtherCAT-Slaves aufgeführt.

Systemvariable	Beschreibung
EC_MASTER_STATE	BYTE - Master-Zustand <ul style="list-style-type: none"> ■ Gibt den Zustand des EtherCAT-Master zurück: <ul style="list-style-type: none"> - 00h: Der Zustand ist unbekannt - 01h: INIT - 02h: PreOP - 04h: SafeOp - 08h: OP

Systemvariablen und Zustandsinformationen > Systemvariablen

Systemvariable	Beschreibung
EC_MASTER_LINK_CONNECTED	BOOL - physikalische Verbindung <ul style="list-style-type: none"> ■ Gesetzt, wenn ein Ethernet-Kabel am EtherCAT-Master angeschlossen ist.
EC_TOPOLOGY_OK	BOOL - Topologie OK <ul style="list-style-type: none"> ■ Gesetzt, wenn aktuelle Topologie und konfigurierte Topologie übereinstimmen.
EC_DC_IN_SYNC	BOOL - verteilte Uhren <ul style="list-style-type: none"> ■ Gesetzt wenn die verteilten Uhren synchronisiert sind.
EC_CYCLIC_LOST_FRAMES	DWORD - fehlende Frames (zyklisch) <ul style="list-style-type: none"> ■ Gibt die Anzahl der während der zyklischen Kommunikation verlorenen Frames zurück.
EC_ACYCLIC_LOST_FRAMES	DWORD - fehlende Frames (azyklisch) <ul style="list-style-type: none"> ■ Gibt die Anzahl der während der azyklischen Kommunikation verlorenen Frames zurück.
EC_NUM_CONFIGURED_SLAVES	WORD - konfigurierte Slaveanzahl <ul style="list-style-type: none"> ■ Gibt die Anzahl der konfigurierten EtherCAT-Slaves zurück.
EC_NUM_AVAILABLE_SLAVES	WORD - Slaveanzahl im Netzwerk <ul style="list-style-type: none"> ■ Gibt die Anzahl der EtherCAT-Slaves zurück, welche bei der Suche im EtherCAT-Netzwerk gefunden wurden.
EC_SLAVES_IN_MASTER_STATE	BOOL - EtherCAT-Slaves im Master-Zustand <ul style="list-style-type: none"> ■ Gesetzt, wenn alle am EtherCAT-Master befindlichen EtherCAT-Slaves den Zustand des EtherCAT-Master haben.
EC_SLAVE_STATION_ADDRESS	ARRAY[0...512] OF WORD ¹⁾ - Slave-Adressen <ul style="list-style-type: none"> ■ Gibt alle Adressen der an den EtherCAT-Master angebundenen EtherCAT-Slaves zurück.
EC_SLAVE_STATE	ARRAY[0...512] OF BYTE ¹⁾ - Slave-Zustände <ul style="list-style-type: none"> ■ Gibt die Zustände der an den EtherCAT-Master angebundenen EtherCAT-Slaves zurück: <ul style="list-style-type: none"> - 00h: Unknown - der Zustand ist unbekannt - 01h: INIT - 02h: PreOP - 03: Bootstrap - 04h: SafeOp - 08h: OP
EC_SLAVE_LAST_AL_STATUS_CODE	ARRAY[0...512] OF WORD ¹⁾ - Slave AL Status Codes <ul style="list-style-type: none"> ■ Gibt den zuletzt gelesenen AL Status Code der an den EtherCAT-Master angebundenen EtherCAT-Slaves zurück.

1) Index 0 ist reserviert. Der 1. EtherCAT-Slave ist dem Index 1 zugeordnet.

PROFINET Systemvariablen
optional

Bitte beachten Sie, dass für den Einsatz von PROFINET eine gesonderte Lizenz erforderlich ist, welche entsprechend zu aktivieren ist!

PROFINET-Systemvariablen - PROFINET-Controller-Funktionalität

Systemvariable	Typ - Beschreibung
PNIO_SYSTEM_BF	<p>BOOL - Fehlende Verbindung zu einem projektierten PROFINET-Device.</p> <ul style="list-style-type: none"> Im PROFINET-Netzwerk ist ein Fehler aufgetreten, d.h. zu mindestens einem projektierten PROFINET-Device konnte keine Verbindung aufgebaut werden. Dieser Wert wird nicht gesetzt, wenn bei einem PROFINET-Device der Parameter "BF ansteuern" auf FALSE gesetzt wurde. Das PROFINET-Device wurde damit aus der Verbindungsüberwachung herausgenommen.
PNIO_SYSTEM_SF	<p>BOOL - Diagnosealarm auf einem projektierten PROFINET-Device.</p> <ul style="list-style-type: none"> Mindestens ein PROFINET-Device meldet einen Systemfehler als Diagnosealarm oder Maintenance-Alarm. Die Fehlerpriorität kann den Variablen PNIO_DIAG_AVAILABLE, PNIO_MAINTENANCE_DEMANDED und PNIO_MAINTENANCE_REQUIRED entnommen werden.
PNIO_MAINTENANCE_DEMANDED	<p>BOOL - Wartungsanforderung</p> <ul style="list-style-type: none"> Mindestens ein PROFINET-Device meldet bei aktiver Verbindung eine "Wartungsanforderung" - Maintenance-Alarm mit hoher Priorität. Mit Hilfe des Diagnosebausteins RALRM kann das PROFINET-Device identifiziert werden.
PNIO_MAINTENANCE_REQUIRED	<p>BOOL - Wartungsbedarf</p> <ul style="list-style-type: none"> Mindestens ein PROFINET-Device meldet bei aktiver Verbindung einen "Wartungsbedarf" - Maintenance-Alarm mit niedriger Priorität. <p>Mit Hilfe des Diagnosebausteins RALRM kann das PROFINET-Device identifiziert werden.</p>
PNIO_FORCE_FAILSAFE	<p>BOOL - Alle PROFINET-Devices werden zum Setzen ihrer projektierten Ersatzwerte aufgefordert.</p> <ul style="list-style-type: none"> Die Systemvariable kann bei Bedarf aus dem Programm beschrieben/gesetzt werden.
PNIO_CONFIG_STATUS	WORD - Konfigurationsstatus des PROFINET-Controllers.
PNIO_CONFIG_STATUS_READY	<p>BOOL - PROFINET-Controller initialisiert.</p> <ul style="list-style-type: none"> Diese Variable ist gesetzt, wenn der PROFINET-Controller fehlerfrei initialisiert werden konnte. Es ist noch keine Sollkonfiguration von iCube Engineer geladen worden.
PNIO_CONFIG_STATUS_ACTIVE	<p>BOOL - Sollkonfiguration geladen.</p> <ul style="list-style-type: none"> Diese Variable ist gesetzt, wenn eine Sollkonfiguration zum PROFINET-Controller geladen wurde. In diesem Zustand versucht der PROFINET-Controller, zyklisch zu allen Geräten der Sollkonfiguration eine Verbindung aufzubauen.

Systemvariable	Typ - Beschreibung
PNIO_CONFIG_STATUS_CFG_FAULT	<p>BOOL - Fehler Sollkonfiguration.</p> <ul style="list-style-type: none"> Die Sollkonfiguration des PROFINET-Controllers wurde aufgrund eines schwerwiegenden Fehlers nicht übernommen. Kontaktieren Sie bitte unseren Support!
PNIO_FORCE_PRIMARY	<p>BOOL - Diese Variable wird von Funktionsbausteinen für applikative Redundanz genutzt um die SRL-Rolle des PROFINET-Controllers vorzugeben.</p>

PROFINET-Systemvariablen - PROFINET-Device-Funktionalität

Systemvariable	Typ - Beschreibung
PND_S1_PLC_RUN	<p>BOOL - Status des überlagerten PROFINET-Controllers.</p> <ul style="list-style-type: none"> Information, ob der überlagerte PROFINET-Controller aktiv ist. Der Wert ist TRUE, wenn sich der überlagerte PROFINET-Controller im Zustand RUN befindet und das Programm abgearbeitet wird. Die Anzeige ist nur bei bestehender PROFINET-Verbindung gültig (PND_S1_VALID_DATA_CYCLE).
PND_S1_VALID_DATA_CYCLE	<p>BOOL - Überlagerter PROFINET-Controller hat die Verbindung aufgebaut.</p> <ul style="list-style-type: none"> Information, ob eine Verbindung besteht und zyklische Daten zwischen PROFINET-Controller und PROFINET-Device ausgetauscht werden und der zuletzt empfangene Frame gültige Daten enthielt.
PND_S1_OUTPUT_STATUS_GOOD	<p>BOOL - IOP-Status des überlagerten PROFINET-Controllers.</p> <ul style="list-style-type: none"> Information, ob das PROFINET-Device die Eingangsprozessdaten (PND_S1_INPUTS) mit dem Status "gültig" empfangen hat. Der Wert ist TRUE, wenn die Ausgangsdaten des überlagerten PROFINET-Controllers gültig sind (Provider-Status).
PND_S1_INPUT_STATUS_GOOD	<p>BOOL - IOC-Status des überlagerten PROFINET-Controllers.</p>
PND_S1_DATA_LENGTH	<p>WORD - Prozessdatenlänge, die für das PROFINET-Device konfiguriert wurde.</p>
PND_S1_OUTPUTS	<p>PND_IO_512 - Ausgangsprozessdaten</p> <ul style="list-style-type: none"> Speicherbereich für Ausgangsprozessdaten, die das PROFINET-Device zum überlagerten PROFINET-Controller sendet.
PND_S1_INPUTS	<p>PND_IO_512 - Eingangsprozessdaten</p> <ul style="list-style-type: none"> Speicherbereich für Eingangsprozessdaten, die das PROFINET-Device von dem überlagerten PROFINET-Controller empfängt.
PND_IO_DRIVEN_BYPLC	<p>INT - Applikative Systemredundanz</p> <ul style="list-style-type: none"> Nummer des aktuell mit dem PROFINET-Device verbundenen PROFINET-Controllers. Angabe, von welchem überlagerten PROFINET-Controller die Daten im PROFINET-Device stammen: <ul style="list-style-type: none"> 0: Kein PROFINET-Controller 1: PROFINET-Controller A 2: PROFINET-Controller B

5 Einsatz CPU iC921xM-FSoE

5.1 Sicherheitshinweise



WARNUNG

Bei unsachgemäßem Einsatz der CPU können in Abhängigkeit von der Applikation schwere Gefahren für den Anwender drohen

Beachten Sie beim Umgang mit der CPU alle in diesem Kapitel aufgeführten Sicherheitshinweise.



WARNUNG

Gefahr vermeiden – Ausgänge können gesetzt werden

- Stellen Sie durch geeignete Maßnahmen sicher, dass von Ihrer Anlage/Maschine keine Gefahr ausgeht.
- Im Zustand "DEBUG-RUN" können Variablen überschrieben werden. Diese werden dann auch zu den FSoE-Ausgangsgeräten übertragen und ausgegeben.
- Quittieren Sie einen Operator-Acknowledge-Request nicht automatisch aus dem Anwenderprogramm heraus. Die Quittierung muss durch eine bewusste Anwenderhandlung ausgelöst werden.
- Wenn Sie passivierte FSoE-Teilnehmer reintegrieren, können sicherheitsbezogene Ausgänge gesetzt werden! Stellen Sie durch geeignete Maßnahmen sicher, dass von Ihrer Anlage/Maschine keine Gefahr ausgeht, wenn passivierte FSoE-Teilnehmer reintegriert werden.



WARNUNG

Verlust der elektrischen Sicherheit sowie der Sicherheitsfunktion beim Einsatz nicht geeigneter Stromversorgungen

Die CPU ist ausschließlich für den Betrieb mit Schutzkleinspannung (PELV) nach EN 60204-1 ausgelegt. Nur Schutzkleinspannungen nach genannter Norm dürfen zur Versorgung verwendet werden. Für den Netzwerkverbund (FSoE und System SLIO) und die darin eingesetzten I/O-Geräte gilt:

- Setzen Sie ausschließlich Stromversorgungen ein, welche die EN 61204 erfüllen, mit sicherer Trennung mit PELV-Spannung nach IEC 61010-2-201 (PELV). In diesen wird ein Kurzschluss zwischen Primär- und Sekundärseite ausgeschlossen.



HINWEIS

Unterstützende Checklisten beachten

Die im Anhang aufgeführten Checklisten dienen zur Unterstützung bei Planung, Montage und elektrischer Installation, Inbetriebnahme und Parametrierung sowie Validierung der Safety-CPU und des FSoE-Systems.



HINWEIS

Geräteidentifikation / Anzahl der sicheren Geräte

- Beachten Sie, dass jede F-Adresse innerhalb eines Netzwerks eindeutig sein muss und Überschneidungen nicht zulässig sind.



HINWEIS

"Watchdog" darf Ti/TO_{FSoEWD_MAX} max nicht überschreiten

- Der in iCube Engineer unter "Watchdog" angegebene Wert darf $Ti/TO_{FSoEWD_MAX} \rightarrow$ "Maximal zulässige Watchdog-Zeiten"...Seite 137 aus \rightarrow "Reaktionszeiten"...Seite 134 nicht überschreiten!

**HINWEIS****Anforderung an die Verfügbarkeit**

Die CPU ist nicht geeignet für Applikationen, welche erhöhte Anforderungen an die Verfügbarkeit erfordern, da im Fehlerfall der Betrieb eingestellt wird.

**HINWEIS****Sachschäden durch Fehlbeanspruchung**

Die Schutzart IP20 (IEC 60529/EN 60529) der CPU ist für eine saubere und trockene Umgebung vorgesehen.

- Setzen Sie die CPU keiner mechanischen und/oder thermischen Beanspruchung aus, welche die beschriebenen Grenzen überschreitet.
- Beachten Sie, dass Sie die CPU für einen einwandfreien Betrieb zwingend in ein abschließbares Gehäuse oder einen abschließbaren Schaltschrank mit mindestens Schutzart IP54 einbauen müssen.

**HINWEIS****Elektrostatische Entladung**

Die CPU enthält Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können.

- Beachten Sie beim Umgang mit der CPU die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) gemäß EN 61340-5-1 und IEC 61340-5-1.

**HINWEIS****Geräteausfall durch Fremdkörper im Gerät**

Fremdkörper in der CPU können zu Fehlfunktionen bis hin zum Geräteausfall führen.

- Achten Sie darauf, dass keine Fremdkörper in die CPU (z.B. in die Lüftungsöffnungen) gelangen.

**HINWEIS****Geräteausfall durch Betrieb außerhalb des zulässigen Umgebungstemperaturbereichs**

Wenn Sie die CPU außerhalb des zulässigen Umgebungstemperaturbereichs betreiben, kann dies zu Fehlfunktionen bis hin zum Geräteausfall führen.

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

→ ["Zulassungen, Richtlinien, Normen"...Seite 20](#)

**HINWEIS****Geräteausfall durch Betrieb oberhalb der zulässigen Angaben für Vibration und Schock**

Wenn Sie die CPU oberhalb der zulässigen Angaben für Vibration und Schock betreiben, kann dies zu Fehlfunktionen bis hin zum Geräteausfall führen.

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

→ ["Zulassungen, Richtlinien, Normen"...Seite 20](#)

**HINWEIS****Gerätedefekt durch Verpolung**

Das Verpolen stellt für die Elektronik eine Belastung dar und kann zum Defekt der CPU führen.

- Vermeiden Sie zum Schutz der CPU eine Verpolung der DC 24V-Versorgung.

5.2 Montage



Nähere Informationen zur Montage und zur Verdrahtung → "Grundlagen und Montage"...Seite 23.

5.3 Lizenzhinweise zu Open Source Software

- Die CPU 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 179
- 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).

5.4 Programmierung und Dateisystem

PLCnext Technology

- Die CPU basiert auf PLCnext Technology® von Phoenix Contact.
- Die CPU arbeitet mit einem Linux Betriebssystem.

Programmierung

- Die CPU darf ausschließlich mit iCube Engineer nach IEC 61131-3 konfigurieren und programmiert werden.



Der Sprachumfang des Safety Funktionsplans und die sichere Funktionsbausteinbibliothek ist in der Dokumentation des iCube Engineer enthalten.

Firewall



- Im Auslieferungszustand ist die Firewall in der CPU deaktiviert!
- Sicherheitsempfehlung: Aktivieren Sie die Firewall!
- Im WBM können Sie unter "Security → Firewall" die Firewall aktivieren.
→ "Firewall"...Seite 199
- Bitte beachten Sie, dass Sie ausschließlich als Administrator Zugriff auf die Firewall-Einstellungen haben!

5.4.1 iCube Engineer installieren

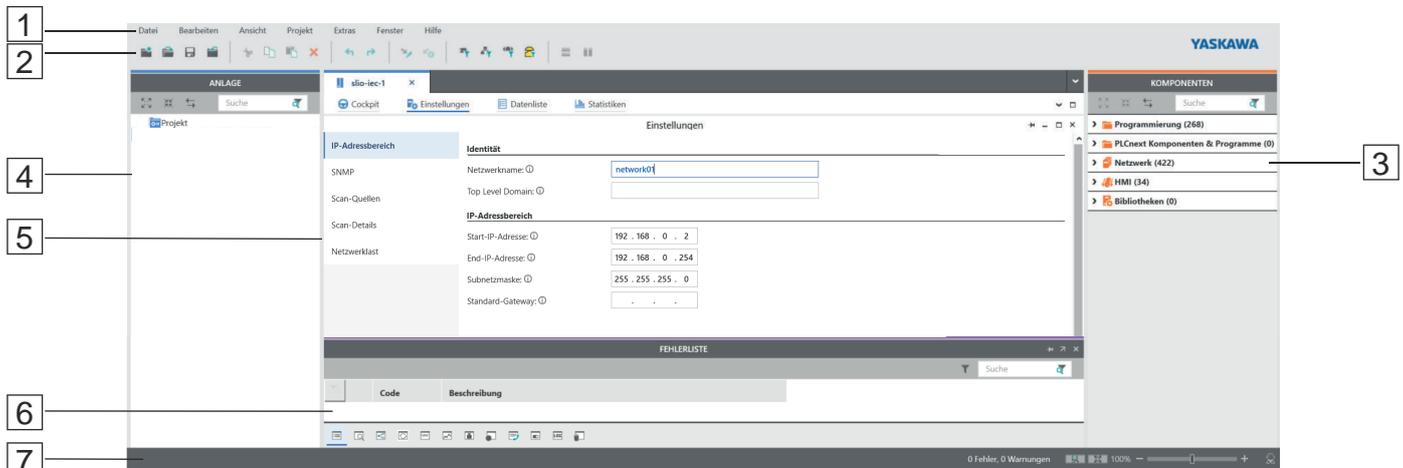
Installation

Für die Inbetriebnahme der CPU ist die Software iCube Engineer erforderlich.

1. ➔ Laden Sie die Software iCube Engineer 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 iCube Engineer jetzt starten.

5.4.2 iCube Engineer Benutzeroberfläche

Übersicht



- | | |
|-------------------------|-----------------------------------|
| 1 Menüleiste | 5 Editorenbereich |
| 2 Symbolleiste | 6 Funktionsübergreifender Bereich |
| 3 "Komponenten"-Bereich | 7 Statusleiste |
| 4 "Anlage"-Bereich | |

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	<p>Der Bereich "<i>Komponenten</i>" beinhaltet alle für das Projekt verfügbaren Komponenten. Die Komponenten lassen sich anhand ihrer Funktion in folgende Typen unterteilen:</p> <ul style="list-style-type: none"> ■ 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	<p>Im Bereich "<i>Anlage</i>" bilden Sie alle physischen und logischen Komponenten Ihrer Applikation in Form einer hierarchischen Baumstruktur ab.</p>
Editorenbereich	<ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> - Blau: Editor aus dem Bereich "<i>Anlage</i>". - Orange: Editor aus dem Bereich "<i>Komponenten</i>".
Funktionsübergreifender Bereich	<p>Der funktionsübergreifende Bereich beinhaltet Funktionen, welche sich über Ihr gesamtes Projekt erstrecken.</p> <ul style="list-style-type: none"> ■ FEHLERLISTE <ul style="list-style-type: none"> - Hier werden alle Fehler, Warnungen und Nachrichten des aktuellen Projekts angezeigt. ■ GLOBAL SUCHEN UND ERSETZEN <ul style="list-style-type: none"> - Hier können Sie Text im Projekt suchen und ersetzen. ■ QUERVERWEISE <ul style="list-style-type: none"> - Hier werden alle Querverweise innerhalb des Projekts angezeigt wie z.B. die Verwendung und Deklaration aller Variablentypen. ■ WATCH-FENSTER <ul style="list-style-type: none"> - Debug-Tool - hier werden im Online-Modus die aktuellen Werte der hinzugefügten Variablen angezeigt. ■ BREAKPOINTS <ul style="list-style-type: none"> - Debug-Tool - hier können Sie zur Fehlersuche Breakpoints setzen und rücksetzen. ■ CALL STACKS <ul style="list-style-type: none"> - Debug-Tool - hier wird die Reihenfolge der Aufrufe bei Ausführung des Codes angezeigt und es werden Kommandos für das Debuggen mit Breakpoints zur Verfügung gestellt. ■ LOGIKANALYSE <ul style="list-style-type: none"> - Hier lassen sich Variablenwerte zur Laufzeit aufzeichnen und visualisieren. ■ PROTOKOLL <ul style="list-style-type: none"> - Hier werden alle Fehler, Warnungen und Nachrichten ausgegeben. <ul style="list-style-type: none"> "<i>Online</i>": Nachrichten der Laufzeitumgebung sowie andere Fehler und Warnungen, welche die Online-Kommunikation betreffen. "<i>Engineering</i>": Nicht projektbezogene Nachrichten über Ereignisse, welche die Software betreffen wie z.B. Gerätedateien GSDML usw. ■ PAPIERKORB <ul style="list-style-type: none"> - 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 gelöschte Elemente wiederherstellen.
Statusleiste	<p>Erkannte Fehler und Warnungen werden hier angezeigt. Zusätzlich haben Sie hier bei grafischen Anwendungen eine Zoomfunktion.</p>

5.4.3 Neues Projekt erstellen

Vorgehensweise



HINWEIS

Die Parametrierung der sicheren Parameter wird durch ein Safety-Passwort abgesichert, welches Sie bei der Anlage eines Projekts mit Sicherheits-Komponenten zu vergeben haben. Sorgen Sie für den entsprechenden Schutz des Safety-Passworts und geben Sie das Safety-Passwort nur an autorisiertes Personal weiter!

1. Starten Sie iCube Engineer.
2. Klicken Sie auf "*Neues Projekt ...*".
 - ➔ Die iCube Engineer-Benutzeroberfläche wird angezeigt.
3. Wählen Sie unter "*Komponenten*" die entsprechende Safety-CPU aus und ziehen Sie diese per Drag&Drop auf "*Anlage*" "*Projekt*".
 - ➔ Für den Zugriff auf den sicherheitsbezogenen Bereich müssen Sie jetzt ein Safety-Passwort vergeben.
 - Verwenden Sie sichere Passwörter bestehend aus Groß-/Kleinschreibung, Zahlen und Sonderzeichen.
 - Der Einsatz eines Passwort-Generators bzw. -Managers wird empfohlen.
 - In den Vorlagen desiCube Engineer lautet das Passwort "safety".
 - Nach der Passwortvergabe wird die CPU in Ihr Projekt übernommen.
4. Speichern Sie Ihr Projekt über "*Datei* → *Speichern unter*". Vergeben Sie einen aussagekräftigen Namen für Ihr Projekt und schließen Sie den Dialog mit [Speichern].

5.4.4 Parametrierung der sicheren Parameter

Sicherheitshinweise



HINWEIS

Auf der CPU befindet sich ein Speicherbereich für Safety Variablen-Verknüpfungen. Bitte berücksichtigen Sie hierbei folgende Begrenzungen:

- Jede in die Prozessdaten gemappte Safety Variablen-Verknüpfungen belegt 16 Byte.
- Jede in die Prozessdaten gemappte Variablen-Verknüpfungen belegt 8 Byte.
- Die Summe aller in die Prozessdaten gemappten Variablen-Verknüpfungen darf 19980 Byte nicht überschreiten.



HINWEIS

Bitte beachten Sie, dass die "*FSoE Device-Adresse*" bzw. "*F-Adresse*" der lokalen und über Ethernet angebotenen Safety-Module eindeutig ist und nur einmalig vergeben sein darf!



HINWEIS

Die Parametrierung der sicheren Parameter wird durch ein Safety-Passwort abgesichert, welches Sie bei der Anlage des Projekt angegeben haben. Sorgen Sie für den entsprechenden Schutz des Safety-Passworts und geben Sie das Safety-Passwort nur an autorisiertes Personal weiter!



HINWEIS

Bitte beachten Sie, dass die Safety-CPU grundsätzlich 2-kanalige Sicherheitsfunktionen unterstützt. Berücksichtigen Sie bei der Auslegung der Sicherheitsfunktionen inwieweit die angebotenen Sicherheitskomponenten 2-kanalige Sicherheitsfunktionen zur Verfügung stellen. In der Safety-CPU gibt es keine Information hierzu. Nähere Informationen hierzu finden Sie in der zugehörigen Hersteller-Dokumentation der Safety-Komponente.



Zur Erreichung von SIL3/Kat.4/PLe ist 2-Kanaligkeit erforderlich. Für SIL2/Kat.3/PLd ist 1-Kanaligkeit ausreichend. Bitte berücksichtigen Sie hierbei die Vorgaben für die Testrate und Anforderungsrate. Nähere Informationen hierzu finden Sie in der zugehörigen Hersteller-Dokumentation der Safety-Komponente.



Sofern eine angebundene Sicherheitskomponente ausschließlich 1-kanalige Sicherheitsfunktionen bereit stellt, können Sie mittels der Hantierungsbausteine "SF_Antivalent..." und "SF_Equivalent..." aus zwei 1-kanaligen Signalen ein 2-kanaliges Signal generieren. Die Bausteine finden Sie in der "SF Library", welche ggf zu installieren ist. Informationen zum Einsatz der Bausteine finden Sie in der zugehörigen Onlinehilfe.

Vorbereitung

Führen Sie die Hardwarekonfiguration Ihres Systems durch, indem sie in Ihrem Projekt unter "Anlage" zu der entsprechenden Komponente durch Doppelklick navigieren und im Editor den entsprechenden "Typ" wählen. Wählen Sie auf diese Weise auch Ihre Safety-Module aus.



Durch Eingabe von Teilen der Bestellnummer bzw. der Modulbezeichnung erhalten Sie während der Eingabe eine Modul-Auswahlliste, welche sich während der Eingabe dynamisch anpasst.

1. ➔ Projektieren Sie, falls vorhanden, die System SLIO Module, welche lokal am Rückwandbus angebunden sind. Doppelklicken Sie hierzu unter "Anlage" auf "SliceBus".
 - ➔ Der Editor "SliceBus" wird geöffnet. Hier können Sie unter "Typ" das Modul für den entsprechenden Steckplatz vorgeben.
2. ➔ Zur Projektierung Ihres EtherCAT FSoE-Systems doppelklicken Sie unter "Anlage" auf "EtherCAT".
 - ➔ Der Editor "EtherCAT → Geräteliste" wird geöffnet.
3. ➔ Wählen Sie den entsprechenden EtherCAT-Koppler aus.
 - ➔ Unter "Anlage → EtherCAT" wird der entsprechende EtherCAT-Koppler angelegt.
4. ➔ Doppelklicken unter "Anlage → EtherCAT" auf den neu eingefügten EtherCAT-Koppler.
 - ➔ Der Editor "Modulliste" wird geöffnet. Hier können Sie unter "Typ" das Modul für den entsprechenden Steckplatz vorgeben.

5.4.4.1 Parametrierung Sprachumschaltung



Bitte beachten Sie, dass systembedingt die Parametrierung der sicheren Parameter aktuell nur in der englischen Sprachsicht durchgeführt werden kann.

1. ➔ Zur Sprachumschaltung öffnen sie im iCube Engineer über "Extras → Optionen" den Optionen-Dialog.
2. ➔ Wählen Sie unter "Lokalisierung" als Sprache "Englisch".
3. ➔ Speichern Sie Ihr Projekt und starten Sie den iCube Engineer mit Ihrem Projekt neu.

Vergabe der F-Adresse

**HINWEIS**

Bitte beachten Sie, dass die "FSoE Device-Adresse" bzw. "F-Adresse" der lokalen und über Ethernet angebotenen Safety-Module eindeutig ist und nur einmalig vergeben sein darf!

1. Stellen sie die F-Adresse an Ihrem F-Device ein. Näheres zur Vorgehensweise hierzu finden Sie in der zugehörigen Dokumentation.
2. Starten Sie iCube Engineer mit Ihrem Projekt.
3. Navigieren Sie unter Anlage zu Ihrem F-Device.
4. Doppelklicken Sie in Ihrem Projekt auf das entsprechende F-Device.
➔ Der "Safety Parameters"-Editor wird geöffnet.
5. Geben Sie, nach Abfrage des Passworts für den Safety-Bereich, unter "FSoE Device-Adresse" die F-Adresse an, welche Sie an Ihrem F-Device eingestellt haben.

Einstellung der sicheren Parameter

1. Unter "Safety Parameters" können Sie die gewünschten Safety-Parameter einstellen, welche vom F-Device bereitgestellt werden.
2. Speichern Sie Ihr Projekt und übertragen Sie dieses in die Safety-CPU.



Nähere Informationen zu den Vorgehensweisen finden Sie unter [↔ "Applikationsbeispiel"...](#)Seite 139.

5.4.5 Sichere Prozessdaten zuordnen

**HINWEIS****Beschaltung von Sensoren und Aktoren**

Stellen Sie bei der Beschaltung von Sensoren und Aktoren sicher, dass:

- die richtigen sicherheitsbezogenen Sensoren und Aktoren korrekt angeschlossen sind.
- die Parametrierung der Ein- und Ausgänge sowie aller Geräte bzw. Module korrekt ist.
- die Verknüpfung der Baustein-Eingänge bzw. -Ausgänge mit den Signalen der sicherheitsbezogenen Sensoren bzw. Aktoren 1-/2-kanalig korrekt ist.
- Querschuss- und Leitungsbruchüberwachung in Ihrer Anwendung umgesetzt ist, wenn dies erforderlich ist.
- alle sicherheitsbezogenen Funktionsbausteine und Funktionen im sicherheitsbezogenen Code korrekt beschaltet sind.



Entnehmen Sie weiterführende Informationen zur Parametrierung von Ein- und Ausgängen sowie aller Geräte bzw. Module der gerätespezifischen Anwenderdokumentation.



Die detaillierte Vorgehensweise zur E/A-Zuordnung von Prozessdaten ist im Applikationsbeispiel beschrieben. [↔ "Applikationsbeispiel"...](#)Seite 139

5.5 Inbetriebnahme

5.5.1 Hinweise zur Inbetriebnahme



WARNUNG

Automatischen Anlauf verhindern

- Stellen Sie durch geeignete Maßnahmen sicher, dass ein automatischer Anlauf Ihrer Anlage/Maschine verhindert wird.



WARNUNG

Gefahr vermeiden während Inbetriebnahme

- Stellen Sie durch geeignete Maßnahmen sicher, dass während der Inbetriebnahme und Validierung von Ihrer Anlage/Maschine keine Gefahr ausgeht.



WARNUNG

Sicherheitsfunktion erst nach Validierung gegeben

- Die geplante Sicherheitsfunktion der Anlage/Maschine ist erst nach Validierung gegeben.



WARNUNG

Organisatorische oder technische Maßnahmen zum Abgleich der CRC-Prüfsumme erforderlich

Treffen Sie technische oder organisatorische Maßnahmen um sicherzustellen, dass das für die vorliegende Applikation passende Projekt in der CPU anläuft, indem ein Abgleich der CRC-Prüfsumme stattfindet:

→ ["Abgleich der Prüfsummen"...](#)Seite 125

- Nach der Übertragung eines Projekts in die CPU.
 - Ein gültiges aber für die Applikation falsches Projekt könnte eingespielt werden.
- Nach dem Entfernen der SD-Karte.
 - Im internen Speicher könnte sich ein gültiges aber für die Applikation falsches Projekt befinden.
- Nach Stecken bzw. Wechsel der SD-Karte.
 - Auf der SD-Karte könnte sich ein gültiges aber für die Applikation falsches Projekt befinden.

Falls Sie eine technische Maßnahme zur Prüfung der CRC-Prüfsumme einsetzen, muss diese so umgesetzt werden, dass die Prüfung von einer dritten technischen Instanz außerhalb der Safety-CPU erfolgt.



WARNUNG

Sicherheit und Verfügbarkeit der Anlage/Maschine

- Stellen Sie durch geeignete Wahl der Watchdog-Zeit FSoE_WD_Time die Sicherheit und die Verfügbarkeit Ihrer Anlage/Maschine sicher.
- Wählen Sie die Watchdog-Zeit so hoch, dass die Sicherheit Ihrer Anlage/Maschine bei höchstmöglicher Verfügbarkeit noch garantiert ist.



WARNUNG

Gefahr vermeiden, die durch ein zu spätes Auslösen der Sicherheitsfunktion hervorgerufen werden kann

- Stellen Sie sicher, dass die maximal zulässigen Werte T_{FSoEWD_MAX} und TO_{FSoEWD_MAX} nicht überschritten werden. → ["Maximal zulässige Watchdog-Zeiten"...](#)Seite 137

**WARNUNG****Debug-Betrieb**

- In den Debug-Betrieb wechseln bedeutet, den normalen Betrieb zu verlassen.
- Stellen Sie sicher, dass im Debug-Betrieb von Ihrer Anlage/Maschine keine Gefährdungen für Personen ausgehen und Schäden nicht verursacht werden können.

**HINWEIS****Akklimatisierung vor Inbetriebnahme**

Stellen Sie sicher, dass die Inbetriebnahme erst nach Akklimatisierung der CPU und der zugehörigen Module erfolgt!

**HINWEIS****Beschädigung durch unsachgemäße Handhabung**

- Gehen Sie sorgfältig mit der CPU und den Komponenten um!
- Beachten Sie bei der Installation der CPU und der Komponenten, dass mechanische Beschädigungen vermieden werden!

**HINWEIS****Anlauf der CPU nicht sichergestellt**

- Für den ordnungsgemäßen Anlauf der CPU ist das Einschalten der Versorgungsspannung frühestens 30 Sekunden nach Erlöschen der Geräte-LEDs erlaubt.

**HINWEIS****Online-Verifizierung in der Inbetriebnahmephase erforderlich**

In der Inbetriebnahmephase sind die in der Planungsphase offline ermittelten Werte für Programmlaufzeit und Zykluszeit online zu verifizieren.



Berücksichtigen Sie bei der Inbetriebnahme immer die zugehörige Checkliste.

→ "Checkliste Inbetriebnahme, Parametrierung und Validation"...Seite 225



Bedienung und Programmierung dürfen ausschließlich von qualifiziertem Personal durchgeführt werden!



Die Bedienung und Programmierung darf ausschließlich über iCube Engineer erfolgen!



Sorgen Sie während der ganzen Betriebszeit dafür, dass immer ein PC-System mit lauffähigem iCube Engineer zur Verfügung steht!

Ansonsten können keine nachträglichen Modifikationen durchgeführt werden.



Sorgen Sie für eine rechtssichere Dokumentation und Archivierung Ihres Engineering-Projekts!

5.5.1.1 Hinweise zur Erstinbetriebnahme



WARNUNG

Sicherheitsbezogene Arbeitsschritte

Die folgenden Arbeitsschritte beinhalten sicherheitsbezogene Tätigkeiten in der Software iCube Engineer und die Sicherheitsvalidierung des FSoE-Systems.

- Beachten Sie auch für die folgenden Arbeitsschritte die im Anhang aufgeführten Checklisten.
- Beachten Sie zusätzlich die Online-Hilfe des iCube Engineer.



WARNUNG

Verifikation entsprechend Sicherheitsnormen durchführen

- Führen Sie für alle Schritte zur Erstellung des Sicherheitsprogramms für Ihre Applikation eine Verifikation entsprechend der für Ihre Applikation gültigen Sicherheitsnormen durch.



HINWEIS

Unerlaubter Zugriff auf die SD-Karte möglich

Der Zugriff auf die SD-Karte ist möglich, sodass Daten gelesen und manipuliert werden können.

- Beachten Sie → ["Hinweise zur Security"...](#)Seite 14, besonders hinsichtlich eines Zugriffsschutzes für die SD-Karte.

5.5.2 Online-Zugriff auf die CPU

IP-Adress-Parameter für die Kommunikation

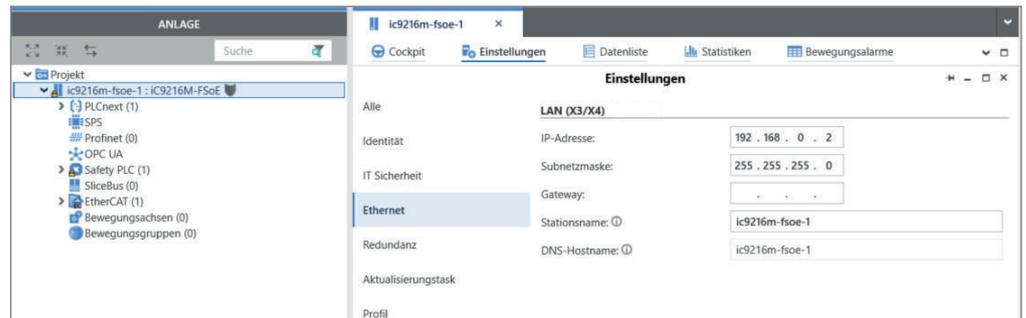
Im Auslieferungszustand sind in der Projektvorlage der CPU folgende IP-Adress-Parameter für die Kommunikation voreingestellt:

- Ethernet-Port (X3/X4): 192.168.1.1
- Subnetzmaske: 255.255.255.0
- Gateway: -

Sollte Ihre CPU andere IP-Adress-Parameter besitzen, können Sie diese für iCube Engineer nach folgender Vorgehensweise anpassen:

1. Öffnen Sie Ihr Projekt.
2. Doppelklicken Sie im Bereich *"Anlage"* auf den Knoten der CPU.
 - ➔ Die Editorengruppe der CPU wird geöffnet.
3. Wählen Sie den Editor *"Einstellungen"*.

4. ➔ Wählen Sie die Ansicht "Ethernet".



5. ➔ Die IP-Adress-Parameter für die Verbindung über den Ethernet-Port (X3/X4) können Sie unter "LAN (X3/X4)" einstellen.

- ➔ Beim Aufbau einer Ethernet-Verbindung zur CPU verwendet iCube Engineer die hier angegebenen IP-Adress-Parameter für die entsprechende Schnittstelle.

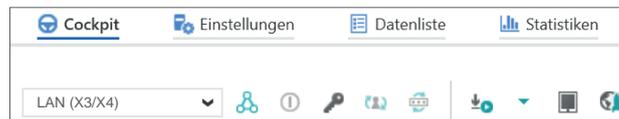
Mit der CPU verbinden



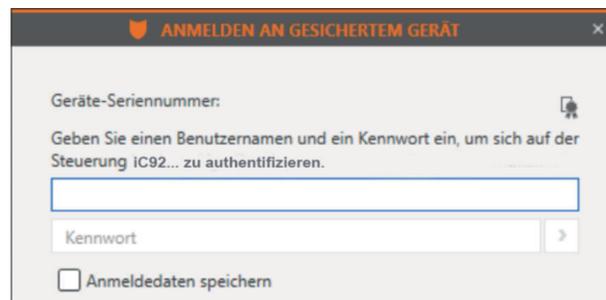
Bitte beachten Sie, dass die Online-Suche aktuell nur vom Port X3/X4 unterstützt wird!

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

1. ➔ Öffnen Sie Ihr Projekt.
2. ➔ Wählen Sie in der Editorengruppe der CPU den Editor "Cockpit".
3. ➔ Stellen Sie die Schnittstelle "LAN (X3/X4)" ein und klicken Sie auf .



- ➔ Eine Verbindung zwischen iCube Engineer und Ihrer CPU wird, unter Verwendung der IP-Adress-Parameter, aufgebaut und der Anmeldedialog zur Authentifizierung geöffnet.



Inbetriebnahme > Online-Zugriff auf die CPU

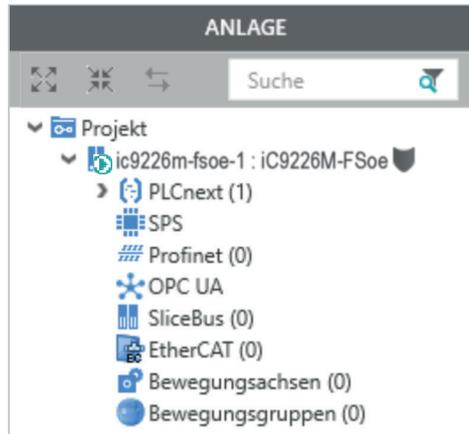
4. Geben Sie Ihre Zugangsdaten an und klicken Sie auf .



Im Auslieferungszustand sind folgende Zugangsdaten mit Administratorrechten voreingestellt:

- Benutzername: admin
- Das Passwort befindet sich unter der Frontklappe auf die Frontseite der CPU aufgedruckt.

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

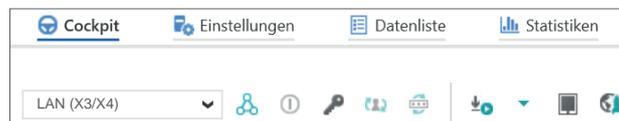


5.5.2.1 Neue IP-Adress-Parameter zuweisen

Zuweisung über WBM

Sobald Sie online mit der CPU 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.

YASKAWA

Bitte melden Sie sich mit Ihrem Benutzernamen und Ihrem Passwort an.

Benutzername

Passwort

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



Im Auslieferungszustand sind folgende Zugangsdaten mit Administratorrechten voreingestellt:

- Benutzername: admin
- Das Passwort befindet sich unter der Frontklappe auf die Frontseite der CPU aufgedruckt.

- ➔ Sie haben jetzt Zugriff auf das WBM der CPU 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.

YASKAWA

IC92...
PMC92...

Konfiguration
Netzwerk

Informationen
Diagnose
Konfiguration
Netzwerk
Datum und Uhrzeit
Systemdienste
Webdienste
Security
Verwalten

LAN-Schnittstellen

TCP/IP (LAN 1) - Separated Mode	Status	Konfiguration
IP-Adresse	192.168.1.11	192.168.1.11
Subnetzmaske	255.255.255.0	255.255.255.0
Standard-Gateway	192.168.1.1	192.168.1.1
DNS-Serveradressen	8.8.8.8 8.8.4.4	8.8.8.8 8.8.4.4
MAC-Adresse	BE:FA:66:E9:FD:76	
Port X1		
Datenrate	100 Mbit/s	
Duplexmodus	Voll duplex	
Link-Status	LinkUp	

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 CPU übertragen und zur Aktivierung die CPU automatisch neu gestartet.



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

5.5.3 Validation des Systems

Allgemein

Mit der Erstinbetriebnahme müssen sämtliche Sicherheitsfunktionen und die einwandfreie Funktion des installierten und programmierten Systems getestet werden. Die Prüfung des Systems muss dokumentiert werden.



WARNUNG

Gefahr bei der Inbetriebnahme!

Das Steuerungssystem darf ausschließlich nach erfolgreicher Prüfung durch einen Sachkundigen in Betrieb genommen werden.

- Führen Sie einen vollständigen Funktionstest durch, prüfen Sie dabei die korrekte Zuordnung der verknüpften Sicherheitskomponenten.
- Führen Sie die Validation des Systems gemäß der Checkliste durch und dokumentieren Sie die Durchführung entsprechend. → ["Checkliste Inbetriebnahme, Parametrierung und Validation"...](#) Seite 225
- Stellen Sie sicher, dass das Bedienpersonal in die Handhabung des Steuerungssystems eingewiesen wird.

5.5.3.1 Funktionstest

Übersicht

Der Funktionstest ist wesentlicher Bestandteil der Validation des Gesamtsystems. Durch den Funktionstest können die einwandfreie Zuordnung der Sicherheitskomponenten des Netzwerks und die programmierte Logik des Systems festgestellt werden. Je nach

Komplexität der Verknüpfungslogik des jeweiligen Projektes ist empfohlen, abgestufte Funktionstests durchzuführen. Folgende Vorgehensweise wird bei der Durchführung von Funktionstests empfohlen:

- Verbinden Sie die Aktoren und Antriebe mit den sicheren Ausgangsklemmen erst dann, wenn bei der Überprüfung der Verdrahtung keine Fehler festgestellt wurden.
- Führen Sie einen vollständigen I/O-Test durch. Das bedeutet, dass Sie der Reihe nach einzeln jeden Sensor in alle seiner möglichen Schaltzustände bringen (in der Regel an und aus, bzw. betätigt nicht betätigt).
 - Prüfen Sie dabei, ob der spezifizierte und erwartete Signalzustand auch dem realen Zustand entspricht.
 - Prüfen Sie außerdem, ob sich in der angeschlossenen Sicherheits-SPS der zugeordnete Variablenzustand auch entsprechend ändert.
 - Ebenso ist bei der Ansteuerung der Aktoren über die Safety-Ausgabemodule zu verfahren. Auch hier ist jeder in der Sicherheitsapplikation spezifizierte Prozesszustand zu testen.
- Führen Sie einen vollständigen Funktionstest mit allen Sensoren (Initiatoren), Schaltern, Aktoren und Antrieben durch.
- Dokumentieren Sie das Ergebnis des Funktionstests.
- Lösen Sie zur Durchführung des Funktionstests sämtliche Sicherheitsfunktionen nacheinander aus und dokumentieren Sie die Reaktion des Systems. Prüfen Sie, ob die Reaktion dem erwarteten Verhalten entspricht.

Im iCube Engineer unterstützen Sie folgende Funktionen beim Funktionstest:

- Monitoring-Modus
- Debug-Modus



Nähere Informationen hierzu finden Sie in der Onlinehilfe des iCube Engineer.

Onlinezugriff

Beim Online-Zugriff wird zwischen sicherheitsgerichteter Funktionalität und Standard-Funktionalität unterschieden. Den Zugriff steuern Sie durch Doppelklick auf den entsprechenden Knoten unter "Anlage". Über den Knoten "Safety PLC" haben Sie Zugriff auf das Cockpit der sicherheitsgerichteten CPU. Der Zugriff ist durch das von Ihnen vergebene Safety-Passwort geschützt.

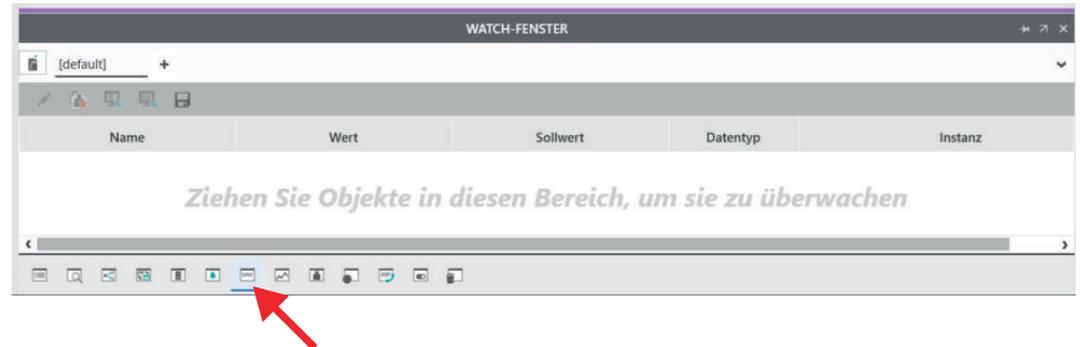
Monitoring-Modus



Der Monitoring-Modus ermöglicht Nur-Lese-Zugriff auf die sicherheitsbezogene SPS. Da die Ausführung der Applikation nicht durch Debug-Befehle beeinflusst werden kann, wird der Monitoring-Modus als sicherer Modus betrachtet.

1. Laden Sie Ihr Projekt.
2. Doppelklicken Sie im Bereich "Anlage" auf den "Safety PLC"-Knoten.
 - ➔ Das Cockpit der sicheren SPS wird geöffnet.
3. Gehen Sie über mit Ihrer Safety-CPU online.

4.  Klicken Sie im *Funktionsübergreifenden Bereich* in der Symbolleiste unten auf .



- ➔ Es öffnet sich das "Watch-Fenster". Im Watch-Fenster können Sie Variablen sammeln und die Online-Werte während der Ausführung der Applikation übersichtlich anzeigen und überwachen. Innerhalb des WATCH-Fensters können Sie mehrere Watch-Listen anlegen. Jede Liste kann gespeichert und geladen werden. Zusätzlich kann der aktuelle Online-Wert von Listenelementen von der Steuerung geladen und als *Sollwert* verwendet werden.
5.  Ziehen Sie die zu überwachenden Variablen in das Watch-Fenster.
6.  Aktivieren Sie mit  den Monitoring-Modus.
- ➔ Sie haben jetzt Lesezugriff auf die Variablen in Ihrem Projekt.

Debug-Modus



GEFAHR

Unbeabsichtigter Betriebszustand der CPU

Im Gegensatz zum Monitoring-Modus gewährt der Debug-Modus schreibenden Zugriff auch auf die sicherheitsbezogene SPS. Da die Ausführung der Applikation durch Debug-Befehle beeinflusst werden kann, wird der Debug-Modus als nicht-sicherer Modus betrachtet.

- Stellen Sie sicher, dass durch beabsichtigte oder unbeabsichtigte Operationen der sicherheitsbezogenen SPS keine Gefährdung entstehen kann.
- Bitte beachten Sie auch die ["Hinweise zur Inbetriebnahme"...](#)Seite 90.

1.  Laden Sie Ihr Projekt.
2.  Doppelklicken Sie im Bereich "Anlage" auf den "SafetyPLC"-Knoten.
 - ➔ Das Cockpit der sicheren SPS wird geöffnet.
3.  Gehen Sie über  mit Ihrer Safety-CPU online.
4.  Aktivieren Sie mit  den Debug-Modus.
 - ➔ Sie haben jetzt die Möglichkeit Ihr Anwenderprogramm zu debuggen und Variablen zu steuern. Zur fixen Vorgabe von Variablenwerten können Sie die Force-Funktion verwenden. Zum Anhalten Ihres Anwenderprogramms können Sie Breakpoints setzen.

5.5.4 Abgleich der Prüfsummen

Vorgehensweise

Sobald Sie in Ihrem Projekt Safety-Komponenten platzieren, wird für Ihr Sicherheits-Projekt automatisch eine Prüfsumme berechnet. Nach der Projektübertragung müssen die Prüfsumme Ihres Projekts und der online verbundenen CPU identisch sein. Die Überprüfung erfolgt nach folgender Vorgehensweise:

1.  Stellen Sie eine Online-Verbindung zu Ihrer CPU her.
2.  Doppelklicken Sie auf "SafetyPLC".

3. ➤ Wählen Sie den Editor "Cockpit Sichere SPS" und klicken Sie auf "Übersicht".
 - ➔ Folgende Prüfsummen müssen identisch sein:
 - Prüfsumme CPU: "Projektinformationen sicherheitsbezogene SPS"
 - Prüfsumme Projekt: "Engineering Projektinformation"

5.6 Speichermanagement

5.6.1 Interner Speicher

Übersicht



Bitte beachten Sie, dass abhängig von der Firmware und den eingesetzten Komponenten, nicht der komplette Speicherbereich zur Verfügung steht.

Speicher

- Nur PMC9212Ex:
 - 2GB Arbeitsspeicher (RAM).
 - 12MB Programmspeicher.
 - 32MB Datenspeicher.
 - 512kB remanenter Datenspeicher.
- Nur PMC9216Ex:
 - 2GB Arbeitsspeicher (RAM).
 - 12MB Programmspeicher.
 - 32MB Datenspeicher.
 - 3072kB remanenter Datenspeicher.

Arbeitsspeicher

- Während des Betriebs legt das Betriebssystem temporäre Daten und Teile des Anwenderprogramms im *Arbeitsspeicher* ab.
- Durch MRESET können Sie ohne Powercycle die CPU in den Zustand *Ready* versetzen. Hierbei wird u.a. der Arbeitsspeicher entladen. ➔ "[MRESET](#)"...Seite 130

Parametrierungsspeicher

Der *Parametrierungsspeicher* als Summe aus Programm- und Datenspeicher bietet Speicher für:

- Aktuelle Firmware-Version
- *Überlagerndes Dateisystem* für Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen.

Verwendung des *überlagernden Dateisystems*:

- Sobald Sie die CPU projektieren bzw. Änderungen an der aktuellen Firmware-Version vornehmen, werden Daten im *überlagernden Dateisystem* erzeugt.
- Durch "[Rücksetzen auf Werkseinstellung Typ 1](#)" können Sie u.a. das *überlagernde Dateisystem* löschen. Hierbei bleibt die aktuelle Firmware-Version bestehen, aber alle Änderungen daran werden verworfen. ➔ "[Rücksetzen auf Werkseinstellung Typ 1](#)"...Seite 130
- Durch "[Rücksetzen auf Werkseinstellung Typ 2](#)" können Sie u.a. das *überlagernde Dateisystem* und die aktuelle Firmware-Version löschen. Hierbei wird die aktuelle Firmware-Version durch die ursprüngliche Firmware-Version überschrieben und somit der Auslieferungszustand der CPU wieder hergestellt. ➔ "[Rücksetzen auf Werkseinstellung Typ 2](#)"...Seite 131

**VORSICHT****Beschädigung des internen Parametrierungsspeichers durch hohen Datenverkehr!**

- Durch häufige Schreibzugriffe bei Applikationen mit hohem Datenverkehr wie z.B. Data-Logger-Applikationen auf das überlagernde Dateisystem kann der interne Parametrierungsspeicher der CPU langfristig beschädigt werden und zu einem Gerätedefekt führen.
- Nutzen Sie für Applikationen mit hohem Datenverkehr eine externe Yaskawa SD-Karte als Speichermedium für das überlagernde Dateisystem.

Nichtflüchtiger Speicher für remanente Daten

- Hier werden alle Daten, welche bei der Projektierung in iCube Engineer als remanent gekennzeichnet wurden, dauerhaft abgelegt.
- Bei Stromausfall werden remanente Daten automatisch gesichert.
- Durch MRESET bzw. Rücksetzen auf Werkseinstellung Typ 1/2 können Sie u.a. den nichtflüchtigen Speicher für remanente Daten löschen.

Speicherüberlauf beheben

Sollte es während des Betriebs bzw. beim Anlaufen der CPU zu der Fehlermeldung kommen, dass der Speicher des überlagernden Dateisystems im Parametrierungsspeicher übergelaufen ist, können Sie die CPU über den *Safe Mode* nach folgender Vorgehensweise wieder starten:

1. Schalten Sie die Spannungsversorgung der CPU aus.

2. Bringen Sie die DIP-Schalter S1 unter der Frontklappe in folgende Stellung:

S1	S1-1	S1-2	Aktion
01 	ON	OFF	Nach PowerON startet die CPU im <i>Safe Mode</i> .

3. Schalten Sie die Spannungsversorgung der CPU wieder ein.

- ➔ Die CPU startet im *"Safe Mode"...*Seite 132. Hierbei wird ein ausschließlich für den *Safe Mode* reservierter Speicherbereich freigegeben, der es ermöglicht, dass die CPU bei einem Speicherüberlauf wieder anlaufen kann. Im *Safe Mode* startet die CPU mit einem Default-Projekt, Ihr Anwenderprogramm ist aber weiterhin im Dateisystem vorhanden.

4. Überprüfen Sie Ihr Anwenderprogramm nach Dateien auf dem Dateisystem, welche das System zum Überlauf bringen wie z.B. Log-Dateien, Rezepte, Bewegungsdaten. Verwenden Sie für den Zugriff auf das Dateisystem einen SSH-Client und löschen Sie ggf. die verursachenden Dateien. Starten Sie danach wieder im *Standard Mode*.

5. Schalten Sie hierzu die Spannungsversorgung der CPU aus.

6. Bringen Sie die DIP-Schalter S1 in die Default-Stellung:

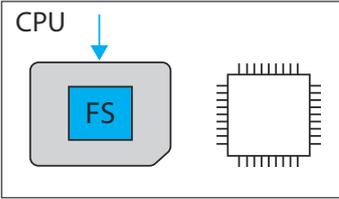
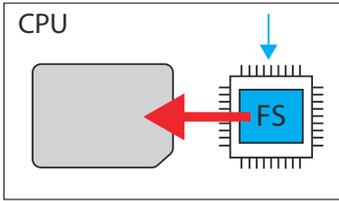
S1	S1-1	S1-2	Aktion
01 	OFF	OFF	Nach PowerON startet die CPU im <i>Standard Mode</i> - Defaulteinstellung.

7. Schalten Sie die Spannungsversorgung der CPU wieder ein.

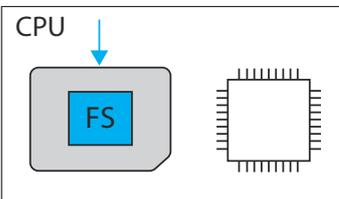
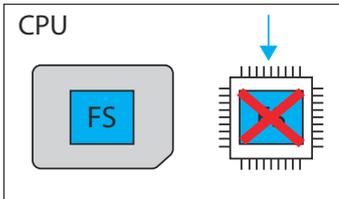
- ➔ Die CPU startet wieder im *Standard Mode*. Wurde im *Safe Mode* ein Projekt geladen, wird dieses im Betriebszustand RUN ausgeführt.

5.6.2 Steckplatz für Yaskawa SD-Karte

Power 0 → 1 



Power 0 → 1 



- Auf diesem Steckplatz können Sie ausschließlich eine Yaskawa SD-Karte mit gültiger Lizenzdatei stecken.
- Im *WBM* können Sie unter "Security → SD-Karte" den Einsatz der SD-Karte aktivieren bzw. deaktivieren und Informationen über diese abrufen. Per Default ist der Einsatz der SD-Karte aktiviert. → "SD-Karte"...Seite 203
- Eine gesteckte Yaskawa SD-Karte wird ausschließlich nach NetzEIN von der CPU erkannt.
- Wird nach NetzEIN eine neue noch unbenutzte Yaskawa SD-Karte erkannt, wird das *überlagernde Dateisystem*  mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen vom internen Parametrierungsspeicher auf die Yaskawa SD-Karte verschoben und im internen Parametrierungsspeicher gelöscht. Von nun an verwendet die CPU das überlagernde Dateisystem auf der Yaskawa SD-Karte.
- Wird nach NetzEIN eine Yaskawa SD-Karte erkannt, auf der sich schon ein *überlagerndes Dateisystem*  befindet, so wird das überlagernde Dateisystem im internen Parametrierungsspeicher gelöscht, ohne dieses zu verschieben. Von nun an verwendet die CPU das vorhandene überlagernde Dateisystem auf der Yaskawa SD-Karte.



WARNUNG

Datenverlust - Kartenentnahme nur bei ausgeschalteter Spannungsversorgung!

- Entnehmen Sie die Yaskawa SD-Karte nur dann, wenn die Versorgungsspannung der CPU ausgeschaltet ist. Ansonsten führt dies zu Datenverlust!
- Wenn Sie die SD-Karte im laufenden Betrieb entnehmen, schaltet die Safety-CPU in den sicheren Zustand (Failure State).



HINWEIS

Projektlöschung bei Einsetzen der SD-Karte möglich

- Beachten Sie folgende Punkte für den Fall, dass Sie nur den internen Flash-Speicher der CPU verwenden:
- Treffen Sie zwingend organisatorische Maßnahmen, welche die Löschung des sicherheitsbezogenen und des nicht sicherheitsbezogenen Projekts verhindern.
 - Falls Sie im laufenden Betrieb der Safety-CPU eine SD-Karte stecken, wird nach einem Spannungs-Reset oder einem Neustart des Systems, das auf dem internen Flash-Speicher vorhandene sicherheitsbezogene und nicht sicherheitsbezogene Projekt gelöscht. Außerdem könnte ein auf der SD-Karte möglicherweise vorhandenes sicherheitsbezogenes Projekt mit einer anderen CRC-Prüfsumme in die Safety-CPU geladen werden.



Generelle Hinweise zum Einsatz der Yaskawa SD-Karte

- Es werden ausschließlich Yaskawa SD-Karten unterstützt.
- Die Karten sind vorformatiert (ext4-Format) für den Einsatz in CPUs der iC9200 Series.
- Durch eine erneute Formatierung gehen bestimmte Informationen auf der Yaskawa SD-Karte verloren, welche für den Einsatz in den CPUs der iC9200 Series erforderlich sind.
- Schließen Sie aus, dass die Yaskawa SD-Karte formatiert wird.
- Die Yaskawa SD-Karte kann jederzeit mit einem herkömmlichen SD-Kartenleser gelesen werden. Sensible Daten auf der Yaskawa SD-Karte können ausgelesen werden, wenn Sie diese nicht physisch vor unbefugtem Zugriff schützen.
- Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die Yaskawa SD-Karte haben.



Bitte beachten bei Einsatz ohne Yaskawa SD-Karte!

- Per Default ist die Unterstützung der Yaskawa SD-Karte aktiviert.
- Deaktivieren Sie die Unterstützung der Yaskawa SD-Karte, wenn Sie die CPU ohne Yaskawa SD-Karte betreiben möchten.
- Bleibt die Unterstützung der Yaskawa SD-Karte aktiviert und wird die CPU ohne Yaskawa SD-Karte betrieben, besteht die Gefahr von Datendiebstahl oder Datenmanipulation.
 - Unbefugte Personen können eine Yaskawa SD-Karte einsetzen und die CPU neu starten.
 - Wird nach NetzeIN eine neue noch unbenutzte Yaskawa SD-Karte erkannt, wird das überlagernde Dateisystem mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen, vom internen Parametrierungsspeicher auf die Yaskawa SD-Karte verschoben und im internen Parametrierungsspeicher gelöscht. Dort gespeicherte Projekte und IP-Konfigurationen sind dann nicht mehr verfügbar!
- Beim Wechsel zum Betrieb ohne Yaskawa SD-Karte wird nach NetzeIN der CPU das überlagernde Dateisystem des internen Parametrierungsspeichers aktiviert und von nun an verwendet. Bitte beachten Sie, dass hierbei keine Daten von der Yaskawa SD-Karte übernommen werden. Auch gibt es keine Funktion zur Rückübertragung von der Yaskawa SD-Karte auf den internen Parametrierungsspeicher.

Yaskawa SD-Karte



Die Yaskawa SD-Karte besitzt folgende Beschriftung und Bedienelemente:

- 1 Bestellnummer
- 2 Produktversion
- 3 Seriennummer
- 4 Schieber für Schreibschutz - hier deaktiviert dargestellt.
- 5 Speichergröße
- 6 Bezeichnung

MRESET und Rücksetzen auf Werkseinstellungen



- 1 In dieser Position ist der Schreibschutz deaktiviert - Auslieferungszustand.
- 2 In dieser Position ist der Schreibschutz aktiviert und die SD-Karte vor versehentlichem Überschreiben geschützt.

5.7 MRESET und Rücksetzen auf Werkseinstellungen

MRESET

- Die CPU wird in den Zustand *Ready* gebracht.
- Der Arbeitsspeicher wird entladen, hierbei bleibt das Anwenderprogramm im überlagernden Dateisystem erhalten.
- Der nichtflüchtige Speicher für remanente Daten wird gelöscht.

1. ➔ Bringen Sie Ihre CPU in STOP.
2. ➔ Drücken Sie den Betriebsartenschalter nach unten in Stellung MR.
3. ➔ Lassen Sie den Betriebsartenschalter nach 3 Sekunden los und drücken Sie diesen innerhalb von 3 Sekunden wieder in Stellung MR.
4. ➔ Lassen Sie den Betriebsartenschalter nach 3 Sekunden wieder los.
 - ➔ ■ Die CPU führt jetzt ein MRESET durch.
 - Zur Bestätigung erhalten Sie eine Diagnose-Meldung, dass ein MRESET durchgeführt wurde. Diese können Sie z.B. in iCube Engineer über "Benachrichtigungen" im Editor "Cockpit" ausgeben lassen.

Rücksetzen auf Werkseinstellung Typ 1

- Das überlagernde Dateisystem mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen wird gelöscht.
- Der nichtflüchtige Speicher für remanente Daten wird gelöscht.
- Die aktuelle Firmware-Version bleibt bestehen, aber alle Änderungen daran werden verworfen.

Mit Betriebsartenschalter

1. ➔ Schalten Sie die Spannungsversorgung der CPU aus.
2. ➔ Drücken und halten Sie den Betriebsartenschalter in Stellung MR und schalten Sie die Spannungsversorgung der CPU wieder ein.
3. ➔ Sobald nach dem Anlauf die LEDs folgendes Verhalten zeigen, lassen Sie den Betriebsartenschalter wieder los:

Status	RN	ER	IO ER	PN-C ER	PN-D ER	IO DIAG
 gelb 1Hz	 grün	 rot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- ➔ Die CPU führt jetzt ein Rücksetzen auf *Werkseinstellung Typ 1* durch.

Mit DIP-Schalter S1

1. ➔ Schalten Sie die Spannungsversorgung der CPU aus.
2. ➔ Bringen Sie die DIP-Schalter S1 unter der Frontklappe in folgende Stellung:

S1	S1-1	S1-2	Aktion
01 	OFF	ON	Nach PowerON führt die CPU Rücksetzen auf <i>Werkseinstellung Typ 1</i> durch.

3. Schalten Sie die Spannungsversorgung der CPU wieder ein.
Nach dem Hochlauf der CPU führt diese ein Rücksetzen auf *Werkseinstellung Typ 1* durch und zeigt folgendes LED-Verhalten:

Status	RN	ER	IO ER	PN-C ER	PN-D ER	IO DIAG
 gelb 1Hz	 grün	 rot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Nach dem Rücksetzen auf *Werkseinstellung Typ 1* fordert die CPU einen Power-cycle an:

Status	RN	ER	IO ER	PN-C ER	PN-D ER	IO DIAG
 gelb 2Hz	 1Hz	 1Hz	 1Hz	 1Hz	 1Hz	 1Hz

4. Schalten Sie die Spannungsversorgung der CPU aus.
5. Bringen Sie die DIP-Schalter S1 in die Default-Stellung:

S1	S1-1	S1-2	Aktion
01 	OFF	OFF	Nach PowerON startet die CPU im <i>Standard Mode</i> - Defaulteinstellung.

6. Schalten Sie die Spannungsversorgung der CPU wieder ein.
➔ Die CPU startet wieder im *Standard Mode*.

Rücksetzen auf Werkseinstellung Typ 2

- Das überlagernde Dateisystem mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen wird gelöscht.
- Der nichtflüchtige Speicher für remanente Daten wird gelöscht.
- Die aktuelle Firmware-Version wird durch die ursprüngliche Firmware-Version überschrieben und somit der Auslieferungszustand der CPU wieder hergestellt.

1. Schalten Sie die Spannungsversorgung der CPU aus.
2. Drücken und halten Sie den Betriebsartenschalter in Stellung MR und schalten Sie die Spannungsversorgung der CPU wieder ein.
3. Sobald nach dem Anlauf die LEDs folgendes Verhalten zeigen, lassen Sie den Betriebsartenschalter wieder los (Dauer ca. 30s):

Status	RN	ER	IO ER	PN-C ER	PN-D ER	IO DIAG
 gelb 2Hz	 grün	 rot	 rot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

➔ Die CPU führt jetzt ein Rücksetzen auf *Werkseinstellung Typ 2* durch und befindet sich danach im Auslieferungszustand.

5.8 Firmware-Update

Ein Firmware-Update können Sie über Web-based Management WBM durchführen.
➔ "[Firmware-Update](#)"...Seite 215



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

Temperaturverhalten

5.9 Safe Mode

Starten im *Safe Mode*

Mittels der DIP-Schalter "S1" unter der Frontklappe können Sie Ihre CPU im *Safe Mode* starten lassen. Hierbei startet die CPU mit folgendem Verhalten:

- Die CPU geht in RUN mit dem Default-Projekt.
- Ein Projekt kann geladen aber nicht ausgeführt werden.
- Der SliceBus wird abgeschaltet.
- Alle Feldbusse werden deaktiviert.
- Der Parametrierungsspeicher mit der aktuellen Firmware-Version und dem *überlagernden Dateisystem* bleibt unverändert.
- Beim Online-Zugriff erhalten Sie eine Information, dass sich die CPU im *Safe Mode* befindet.
- Der *nichtflüchtige Speicher* für remanente Daten bleibt unverändert.
- Die CPU ist ausschließlich über die Default-IP-Adresse erreichbar.
- Zusätzlich wird ein ausschließlich für den *Safe Mode* reservierter Speicherbereich freigegeben, der es ermöglicht, dass die CPU bei einem Speicherüberlauf wieder anlaufen kann.

1. Schalten Sie die Spannungsversorgung der CPU aus.

2. Bringen Sie die DIP-Schalter S1 unter der Frontklappe in folgende Stellung:

S1	S1-1	S1-2	Aktion
01 	ON	OFF	Nach PowerON startet die CPU im <i>Safe Mode</i> .

3. Schalten Sie die Spannungsversorgung der CPU wieder ein.

- ➔ Die CPU startet im *Safe Mode* und zeigt dies ausschließlich beim Online-Zugriff an.

Starten im *Standard Mode*

1. Schalten Sie die Spannungsversorgung der CPU aus.

2. Bringen Sie die DIP-Schalter S1 in die Default-Stellung:

S1	S1-1	S1-2	Aktion
01 	OFF	OFF	Nach PowerON startet die CPU im <i>Standard Mode</i> - Defaulteinstellung.

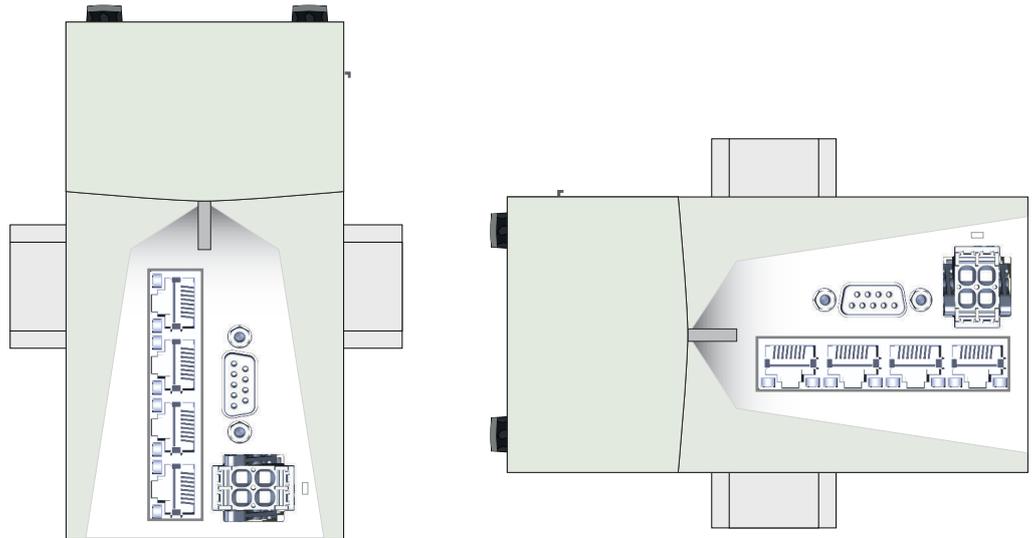
3. Schalten Sie die Spannungsversorgung der CPU wieder ein.

- ➔ Die CPU startet wieder im *Standard Mode*. Wurde im *Safe Mode* ein Projekt geladen, wird dieses im Betriebszustand RUN ausgeführt.

5.10 Temperaturverhalten

Die Safety-CPU hat eine Temperaturüberwachung integriert. Hier gibt es folgende Temperatur-Bereiche bzw. -Grenzen:

- 0°C bis 55°C/60°C: Betriebstemperatur
- < -2°C und > 78°C: Warngrenze
- < -7°C und > 83°C: Fehlergrenze

Betriebstemperatur

Horizontal hängend oder vertikal hängend besitzt die CPU folgende Temperaturbereiche:

- Horizontal hängend: 0°C bis 60°C
- Vertikal hängend: 0°C bis 55°C

Warngrenzen

Werden -2°C unterschritten bzw. 78°C überschritten, wird eine Warnmeldung in den Fehlerstack und das Logfile der sicherheitsbezogenen CPU eingetragen.

Fehlergrenze

Werden -7°C unterschritten bzw. 83°C überschritten, geht die Safety-CPU in den Hard Fail Safe Zustand über. → "[Fail Safe Zustände](#)"...Seite 133

5.11 Fail Safe Zustände**Verhalten im Fehlerfall**

Alle detektierten, schwerwiegenden Fehler in der CPU, welche zum Verlust oder zur Beeinträchtigung der programmierten Sicherheitsfunktion führen können, haben einen Übergang in den sicheren Zustand (Fail Safe Zustand) zur Folge. Hierbei wird zwischen den Zuständen *Soft Fail Safe* und *Hard Fail Safe* unterschieden. Hierbei zeigt die CPU unterschiedliches Verhalten:

- Zustand *Soft Fail Safe*

Verhalten

- Die sicheren Ausgänge der F-Devices werden auf Null (FALSE) gesetzt.
- Die rote SF_ER-LED blinkt mit 1Hz.
- Falls Sie im Fehlerfall online mit dem iCube Engineer verbunden sind, werden Informationen zum Fehlerfall auch in der Software angezeigt.

Mögliche Ursache

- Parametrierungsfehler

Quittierung

- Fehlerbeseitigung im Projekt und neuem Upload.

- Zustand *Hard Fail Safe*

Verhalten

- Die sicheren Ausgänge der F-Devices werden auf Null (FALSE) gesetzt.
- Die rote SF_ER-LED leuchtet.
- Eine Kommunikation mit der CPU ist nicht mehr möglich.

Mögliche Ursache

- Hardwarefehler, Überschreiten der Abschaltsschwellen der Temperaturgrenzen.

Quittierung

- Überprüfen Sie Ihren Hardware-Aufbau und führen Sie einen Powercycle durch.

**HINWEIS**

Sollte sich Ihre CPU nach einem Powercycle weiterhin im Zustand *Hard Fail Safe* befinden und dies sich auch nach einem Reset → *"MRESET und Rücksetzen auf Werkseinstellungen"...*Seite 130 nicht ändern, kontaktieren Sie bitte die Yaskawa Hotline.

5.12 Reaktionszeiten

5.12.1 Fehlerfreier Fall

Im fehlerfreien Fall wird angenommen, dass keine der Zeitüberwachungen anspricht und der Durchlauf eines Signals von der Eingangsklemme eines Safety Eingabe-Moduls bis zur Ausgangsklemme eines Safety Ausgabe-Moduls betrachtet:



Maximal zu erwartende Reaktionszeit im fehlerfreien Fall

$$T_{\max\text{NF}} = T_{\text{Ist}} + T_{\text{IWCDT}} + T_{\text{ISlave}} + T_{\text{IBUS}} + T_{\text{CL}} + T_{\text{FPROG}} + T_{\text{OBUS}} + T_{\text{OSlave}} + T_{\text{OWCDT}}$$

→ *"Bezeichnungen"...*Seite 138

$T_{\max\text{NF}}$	Max. Reaktionszeit im fehlerfreien Fall (max No Fault).
T_{Ist}	Eingangsglättungszeit der Eingänge des Safety SDI (S oothing T ime).
$T_{\text{I/OWCDT}}$	Max. Reaktionszeit im fehlerfreien Fall (W orst C ase D elay T ime).
T_{ISlave}	Max. Reaktionszeit des dezentralen Peripheriesystems, d.h. Verzögerung durch den FSoE EtherCAT-Koppler und den Rückwandbus.
T_{IBUS}	EtherCAT-Zykluszeit für die EtherCAT Busübertragung. Die EtherCAT-Zykluszeit ergibt sich aus den Zykluszeiten aller angebenen EtherCAT-Slaves.
T_{CL}	Zykluszeit der Safety-CPU.
T_{FPROG}	Zykluszeit Sicherheitsprogramm.

Für die Anlagenplanung sind auch noch die Sensor- und Aktorlaufzeiten zu berücksichtigen:

$$T_{\max\text{NFSA}} = T_{\text{SensorDly}} + T_{\max\text{NF}} + T_{\text{ActuatorDly}}$$

→ *"Bezeichnungen"...*Seite 138

$T_{\max\text{NFSA}}$	Max. Reaktionszeit im fehlerfreien Fall mit Sensor und Aktor (max No Fault Sensor Actuator).
$T_{\text{SensorDly}}$	Verzögerungszeit des Sensors. (S ensor D e L a Y).
$T_{\max\text{NF}}$	Max. Reaktionszeit im fehlerfreien Fall (max No Fault).
$T_{\text{ActuatorDly}}$	Verzögerungszeit des Aktors (A ctuator D e L a Y).

5.12.2 Vorhandensein eines Fehlers

Mögliche Einzelfehler

Bei Vorhandensein eines Fehlers wird angenommen, dass eine Zeitüberwachung anspricht und die entsprechende Fehlerreaktion auslöst. Mögliche Ursachen wären Fehler des Systems, falsche Laufzeit-Angabe in der Dokumentation des Standard-Systems oder eine Verlängerung der Laufzeit über den bei der Berechnung verwendeten Wert hinaus durch Änderung der Projektierung des Standard-Systems. Die Gesamtreaktionszeit im fehlerfreien Fall erhöht sich um die maximale Zeitdauer der möglichen Einzelfehler:

- Diskrepanzfehler im Safety SDI. Hier muss die Diskrepanzzeit zusätzlich berücksichtigt werden: (T_{DIS})
- Ein Einzelfehler tritt im Safety SDI auf. Hier muss nun die evtl. größere max. Reaktionszeit bei Vorhandensein eines Fehlers (T_{IOFDT}) als die max. Reaktionszeit im fehlerfreien Fall (T_{IWCDT}) berücksichtigt werden: ($T_{IOFDT} - T_{IWCDT}$)
- Einmalige oder dauerhafte Kommunikationsunterbrechung zwischen dem Safety SDI und der Safety-CPU. Hier muss die FSoE Watchdog Time des Safety SDI und die projektierte Zykluszeit der Steuerung berücksichtigt werden: ($T_{IFSoEWD} + T_{CL}$)
- Einmalige oder dauerhafte Kommunikationsunterbrechung zwischen dem Safety SDO und der Safety-CPU bzw. Ausfall der Safety-CPU. Hier muss die FSoE Watchdog Time des Safety SDO und Quittungszeit seitens des Safety SDO berücksichtigt werden: ($T_{OFSOEWd} + T_{DAT}$)
- Ein Einzelfehler tritt im Safety SDO auf. Hier muss nun die evtl. größere max. Reaktionszeit bei Vorhandensein eines Fehlers (T_{OOFDT}) als die max. Reaktionszeit im fehlerfreien Fall (T_{OWCDT}) berücksichtigt werden: ($T_{OOFDT} - T_{OWCDT}$)

Maximale Reaktionszeit bei einem Fehler

$$T_{\max OF} = T_{\max NF} + \text{MAX}((T_{DIS}), (T_{IOFDT} - T_{IWCDT}), (T_{IFSoEWD} + T_{CL}), (T_{OFSOEWd} + T_{DAT}), (T_{OOFDT} - T_{OWCDT}))$$

→ "Bezeichnungen"...Seite 138

$T_{\max OF}$	Max. Reaktionszeit bei Vorhandensein eines Fehlers (max One Fault).
$T_{\max NF}$	Max. Reaktionszeit im fehlerfreien Fall (max No Fault).
T_{DIS}	Bei 2-kanaliger Auswertung Diskrepanzzeit, ansonsten 0 (DIScrepancy).
T_{I}/T_{OOFDT}	Max. Reaktionszeit bei Vorhandensein eines Fehlers (One Fault Delay Time).
T_{I}/T_{OWCDT}	Max. Reaktionszeit im fehlerfreien Fall (Worst Case Delay Time).
$T_{I}/T_{OFSOEWd}$	Projektierte FSoE Watchdog Time (FSoE WatchDog).
T_{CL}	Zykluszeit der Safety-CPU.
T_{DAT}	Max. Quittierungszeit (Device Acknowledgement Time).

Für die Anlagenplanung sind auch noch die Sensor- und Aktorlaufzeiten zu berücksichtigen:

$$T_{\max OFSA} = T_{\text{SensorDLY}} + T_{\max OF} + T_{\text{ActuatorDLY}}$$

→ "Bezeichnungen"...Seite 138

$T_{\max OFSA}$	Max. Reaktionszeit bei Vorhandensein eines Fehlers mit Sensor und Aktor (max One Fault SensorActuator).
$T_{\text{SensorDLY}}$	Verzögerungszeit des Sensors (Sensor DeLaY).
$T_{\max OF}$	Max. Reaktionszeit bei Vorhandensein eines Fehlers (max One Fault).
$T_{\text{ActuatorDLY}}$	Verzögerungszeit des Aktors (Actuator DeLaY).

Reaktionszeiten > Beliebige Laufzeiten bei Einzelfehler

5.12.3 Beliebige Laufzeiten bei Einzelfehler

Zu berücksichtigende Zeiten Bei beliebigen Laufzeiten des Standard-Systems wird zusätzlich zum Vorhandensein eines Fehlers angenommen, dass alle relevanten Laufzeiten an der Grenze der Zeitüberwachung liegen.

- Die maximale Verarbeitungszeit zum und im Safety SDI:
($T_{IST} + T_{DIS} + T_{WCDT} + T_{FSoEWD}$)
- Die kleinste aller möglichen Überwachungszeiten, ab diesem Moment greift das definierte Verhalten für einen Fehler:
($\text{MIN}(T_{FSoEWD}, T_{CL_MAX}, T_{OFSOEWDT})$)
- Die maximale Verarbeitungszeit zum und im Safety SDO:
($T_{WCDT} + T_{OFSOEWDT}$)
- Die eventuell größeren Verarbeitungszeiten im Fehlerfall innerhalb der Safety-Module, hierbei aber nur die größere der beiden, da von einem Einzelfehler ausgegangen wird:
($\text{MAX}((T_{IOFDT} - T_{WCDT}), (T_{OOFDT} - T_{WCDT}))$)
- Für die gesamte Verarbeitungskette kann gerade vorher noch ein gutes FSoE-Telegramm an das Safety SDI oder -SDO verschickt worden sein. Hierfür muss noch das größere der beiden Timeouts berücksichtigt werden:
($\text{MAX}(T_{FSoEWD}, T_{OFSOEWDT})$)

Maximale Reaktionszeit bei beliebigen Laufzeiten bei einem Fehler

$$\begin{aligned}
 T_{\max RT} &= T_{IST} + T_{DIS} + T_{WCDT} + T_{FSoEWD} \\
 &+ \text{MIN}(T_{FSoEWD}, T_{CL_MAX}, T_{OFSOEWDT}) \\
 &+ T_{WCDT} + T_{OFSOEWDT} \\
 &+ \text{MAX}((T_{IOFDT} - T_{WCDT}), (T_{OOFDT} - T_{WCDT})) \\
 &+ \text{MAX}(T_{FSoEWD}, T_{OFSOEWDT})
 \end{aligned}$$

↪ "Bezeichnungen"...Seite 138

$T_{\max RT}$	Max. Reaktionszeit bei Vorhandensein eines Fehlers mit maximaler Laufzeit (max RunTime).
T_{IST}	Eingangsglättungszeit der Eingänge des Safety SDI (S oothing T ime).
T_{DIS}	Bei 2-kanaliger Auswertung Diskrepanzzeit, ansonsten 0 (DIS crepancy).
$T_{I}/T_{O_{WCDT}}$	Max. Reaktionszeit im fehlerfreien Fall (W orst C ase D elay T ime).
$T_{I}/T_{O_{FSoEWD}}$	Projektierte FSoE Watchdog Time (FSoE W atch D og).
T_{CL_MAX}	Zyklusüberwachungszeit der Safety-CPU.
$T_{I}/T_{O_{OFDT}}$	Max. Reaktionszeit bei Vorhandensein eines Fehlers (O ne F ault D elay T ime).

Für die Anlagenplanung sind auch noch die Sensor- und Aktorlaufzeiten zu berücksichtigen:

$$T_{\max RTSA} = T_{\text{SensorDLY}} + T_{\max RT} + T_{\text{ActuatorDLY}}$$

↪ "Bezeichnungen"...Seite 138

$T_{\max RTSA}$	Max. Reaktionszeit bei Vorhandensein eines Fehlers mit maximaler Laufzeit mit Sensor und Aktor (max RunTime S ensor A ctuator).
$T_{\text{SensorDLY}}$	Verzögerungszeit des Sensors (S ensor D e L a Y).
$T_{\max RT}$	Max. Reaktionszeit bei Vorhandensein eines Fehlers mit maximaler Laufzeit (max RunTime).
$T_{\text{ActuatorDLY}}$	Verzögerungszeit des Aktors (A ctuator D e L a Y).

5.12.4 Maximal zulässige Watchdog-Zeiten

Auslegung

Zur Auslegung von TI/TO_{FSoEWD_MAX} im FSoE-System gilt folgende Formel:

$$TI_{FSoEWD_MAX} + TO_{FSoEWD_MAX} \leq T_{maxRTSA} - TI_{WCDT} - TO_{WCDT}$$

→ "Bezeichnungen"...Seite 138

TI/TO_{FSoEWD_MAX} Maximal zulässige FSoE Watchdog Time (FSoE WatchDog MAXimum).

$T_{maxRTSA}$ Max. Reaktionszeit bei Vorhandensein eines Fehlers mit maximaler Laufzeit mit Sensor und Aktor (max RunTime Sensor Actuator).

TI/TO_{WCDT} Max. Reaktionszeit im fehlerfreien Fall (Worst Case Delay Time).



Berücksichtigen Sie anhand der Angaben in der gerätespezifischen Anwenderdokumentation der F-Devices, ob weitere Angaben zu Watchdog-Zeiten innerhalb der internen Gerätefunktion vorhanden sind. Ebenfalls in der Berechnung sind Timer-Funktionen zu berücksichtigen, welche im sicherheitsbezogenen Anwendungsprogramm innerhalb der Sicherheitsfunktion verwendet werden.



Nähere Informationen zur Berechnung und Optimierung der Watchdog-Zeit finden Sie in der Dokumentation zum iCube Engineer.

5.12.5 Zykluszeit T_{CL} Safety-CPU

Auslegung

iCube Engineer:

Für die Zykluszeit gilt folgende Formel:

$$T_{CL} = T_{FPROG} / 0,7$$

T_{FPROG} ist abzuschätzen. Es gelten folgende Vorgaben für die Summierung:

- Pro F-Device sind 70µs zu addieren.
- Pro sicherheitsbezogenen Funktionsbaustein-Instanzen sind 20µs zu addieren.

In iCube Engineer ist der Wert anzugeben unter "Anlage → Safety PLC": "Tasks und Events → Intervall" im Bereich von 5 ... 15ms.

→ "Bezeichnungen"...Seite 138

T_{CL} Zykluszeit der Safety-CPU.

T_{FPROG} Zykluszeit Sicherheitsprogramm.

5.12.6 Zyklusüberwachungszeit T_{CL_MAX} Safety-CPU

Auslegung

Für die Zyklusüberwachungszeit gilt folgende Formel:

$$T_{CL_MAX} \geq T_{FPROG} / 0,7$$

T_{FPROG} ist abzuschätzen. Es gelten folgende Vorgaben für die Summierung:

- Pro F-Device sind 70µs zu addieren.
- Pro sicherheitsbezogenen Funktionsbaustein-Instanzen sind 20µs zu addieren.

In iCube Engineer ist der Wert anzugeben unter "Anlage → Safety PLC": "Tasks und Events → Watchdog"

→ "Bezeichnungen"...Seite 138

T_{CL_MAX} Zyklusüberwachungszeit der Safety-CPU.

T_{FPROG} Zykluszeit Sicherheitsprogramm.

Reaktionszeiten > Bezeichnungen

5.12.7 Bezeichnungen

Abkürzungen nach Komponenten sortiert

Komponente	Zeit ¹	Beschreibung	Woher
Sensor	$T_{\text{SensorDLY}}$	Verzögerungszeit des Sensors (Sensor DeLaY).	Dokumentation des Sensors.
Safety SDI	T_{IST}	Eingangsglättungszeit der Eingänge des Safety SDI (Smoothing Time).	Projektierung der F-Peripherie, abgestimmt auf den eingesetzten Sensor.
Safety SDI	T_{DIS}	Bei 2-kanaliger Auswertung Diskrepanzzeit, ansonsten 0 (DIScrepancy).	Projektierung der F-Peripherie, abgestimmt auf den eingesetzten Sensor.
Safety SDI Safety SDO	T_{IWCDT} T_{OWCDT}	Max. Reaktionszeit im fehlerfreien Fall (Worst Case Delay Time).	Dokumentation Safety-Modul.
Safety SDI Safety SDO	T_{IOFDT} T_{OOFDT}	Max. Reaktionszeit bei Vorhandensein eines Fehlers (One Fault Delay Time).	Dokumentation Safety-Modul.
Safety SDI Safety SDO	T_{IDAT} T_{ODAT}	Max. Quittierungszeit (Device Acknowledgement Time).	Dokumentation Safety-Modul.
Safety SDI Safety SDO	T_{IFSoEWD} T_{OFSoEWD}	Projektierte FSoE Watchdog Time (FSoE WatchDog).	Dokumentation Safety-Modul.
Safety SDI Safety SDO	$T_{\text{IFSoEWD_MAX}}$ $T_{\text{OFSoEWD_MAX}}$	Maximal zulässige FSoE Watchdog Time (FSoE WatchDog MAXimum).	siehe Formel
Bus-Koppler	T_{ISlave} T_{OSlave}	Max. Reaktionszeit des dezentralen Peripheriesystems, d.h. Verzögerung durch den FSoE EtherCAT-Koppler und den Rückwandbus.	Dokumentation FSoE EtherCAT-Koppler
EtherCAT Feldbus	T_{IBUS} T_{OBUS}	EtherCAT-Zykluszeit für die EtherCAT Busübertragung. Die EtherCAT-Zykluszeit ergibt sich aus den Zykluszeiten aller angebundenen EtherCAT-Slaves.	Dokumentation EtherCAT-Slave iCube Engineer: Wert ist anzugeben unter: "Anlage → EtherCAT": "Einstellungen → Zykluszeit"
F-SPS / F-Logik	T_{CL}	Zykluszeit der Safety-CPU. $T_{\text{CL}} = T_{\text{FPROG}}/0,7$	iCube Engineer: Wert anzugeben unter "Anlage → Safety PLC": "Tasks und Events → Intervall" im Bereich von 5 ... 15ms.
F-SPS / F-Logik	$T_{\text{CL_MAX}}$	Zyklusüberwachungszeit der Safety-CPU. $T_{\text{CL_MAX}} \geq T_{\text{FPROG}}/0,7$	iCube Engineer: Wert ist anzugeben unter "Anlage → Safety PLC": "Tasks und Events → Watchdog".

Komponente	Zeit ¹	Beschreibung	Woher
F-SPS / F-Logik	T_{FPROG}	Zykluszeit Sicherheitsprogramm. Dieser Wert ist abzuschätzen. Hierbei gelten folgende Vorgaben für die Summierung: <ul style="list-style-type: none"> ■ Pro F-Device sind 70µs zu addieren. ■ Pro sicherheitsbezogenen Funktionsbaustein-Instanzen sind 20µs zu addieren. 	Wert wird abgeschätzt.
Aktor	$T_{ActuatorDLY}$	Verzögerungszeit des Aktors.	Dokumentation des Aktors
Gesamt Eingabe bis Ausgabe	T_{maxNF}	Max. Reaktionszeit im fehlerfreien Fall (max No Fault).	Siehe Formel
Gesamt Sensor bis Aktor	$T_{maxNFSA}$	Max. Reaktionszeit im fehlerfreien Fall mit Sensor und Aktor (max No Fault Sensor Actuator).	Siehe Formel
Gesamt Eingabe bis Ausgabe	T_{maxOF}	Max. Reaktionszeit bei Vorhandensein eines Fehlers (max One Fault).	Siehe Formel
Gesamt Sensor bis Aktor	$T_{maxOFSA}$	Max. Reaktionszeit bei Vorhandensein eines Fehlers mit Sensor und Aktor (max One Fault Sensor Actuator).	Siehe Formel
Gesamt Eingabe bis Ausgabe	T_{maxRT}	Max. Reaktionszeit bei Vorhandensein eines Fehlers mit maximaler Laufzeit (max RunTime).	Siehe Formel
Gesamt Sensor bis Aktor	$T_{maxRTSA}$	Max. Reaktionszeit bei Vorhandensein eines Fehlers mit maximaler Laufzeit mit Sensor und Aktor (max RunTime Sensor Actuator).	Siehe Formel

1) "I" oder "O" hinter dem "T" stehen jeweils für Eingabe oder Ausgabe.

5.13 Applikationsbeispiel

5.13.1 Voraussetzung

Hard- und Software

In diesem Applikationsbeispiel wird der Einsatz der iC9212M-FSoE über EtherCAT beschrieben. Für das Applikationsbeispiel ist folgende Hard- und Software erforderlich:

Hardware	Gerät / Modul	Bezeichnung / Bestellnummer
Zentralgerät	iCube CPU mit integriertem EtherCAT (FSoE) Safety Master	iC9212M-FSoE
Lokale SLIO-Module	System SLIO DI	SM 021 (021-1BF00)
	System SLIO DO	SM 021 (022-1BF00)
	System SLIO Safety DI	SM 021 (021-1SD10)
	System SLIO Safety DO	SM 022 (022-1SD10)
EtherCAT Slave-System	System SLIO Buskoppler	IM 053EC Slave (053-1EC01)
	System SLIO DI	SM 021 (021-1BF00)
	System SLIO DO	SM 022 (022-1BF00)

Applikationsbeispiel > Projektierung im iCube Engineer

Hardware	Gerät / Modul	Bezeichnung / Bestellnummer
	System SLIO Safety DI	SM 021 (021-1SD10)
	System SLIO Safety DO	SM 022 (022-1SD10)
Software	Funktion	
iCube Engineer	iCube Engineer unterstützt die Programmierung und Konfiguration von Steuerungen der iC9200 Series-Generation und deren FSoE-Varianten.	

F-Adressen

Stellen Sie vor dem Aufbau an folgenden Modulen per DIP-Schalter die entsprechende F-Adresse ein:

Modul	F-Adresse dezimal	Schalterstellung
System SLIO DI lokal	1	0000 0000 0001
System SLIO DO lokal	2	0000 0000 0010
System SLIO DI EtherCAT	3	0000 0000 0011
System SLIO DO EtherCAT	4	0000 0000 0100

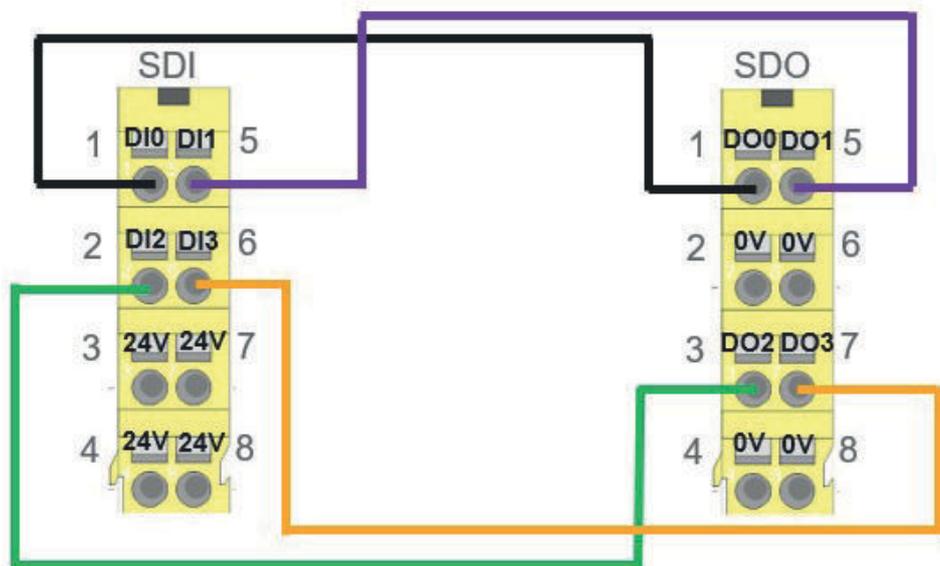


HINWEIS

Bitte beachten Sie, dass die "FSoE Device-Adresse" bzw. "F-Adresse" der lokalen und über Ethernet angebotenen Safety-Module eindeutig ist und nur einmalig vergeben sein darf!

Verdrahtung FSoE-Module

Verdrahten Sie die FSoE-Module gemäß folgender Abbildung:



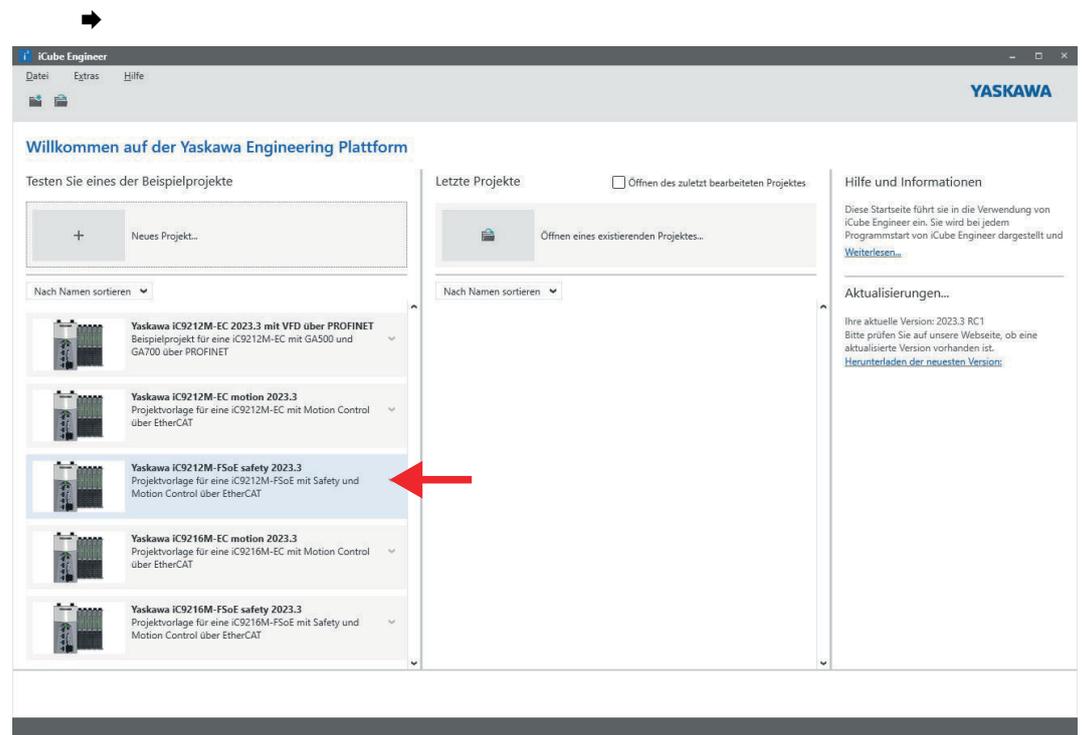
5.13.2 Projektierung im iCube Engineer

Vorgehensweise

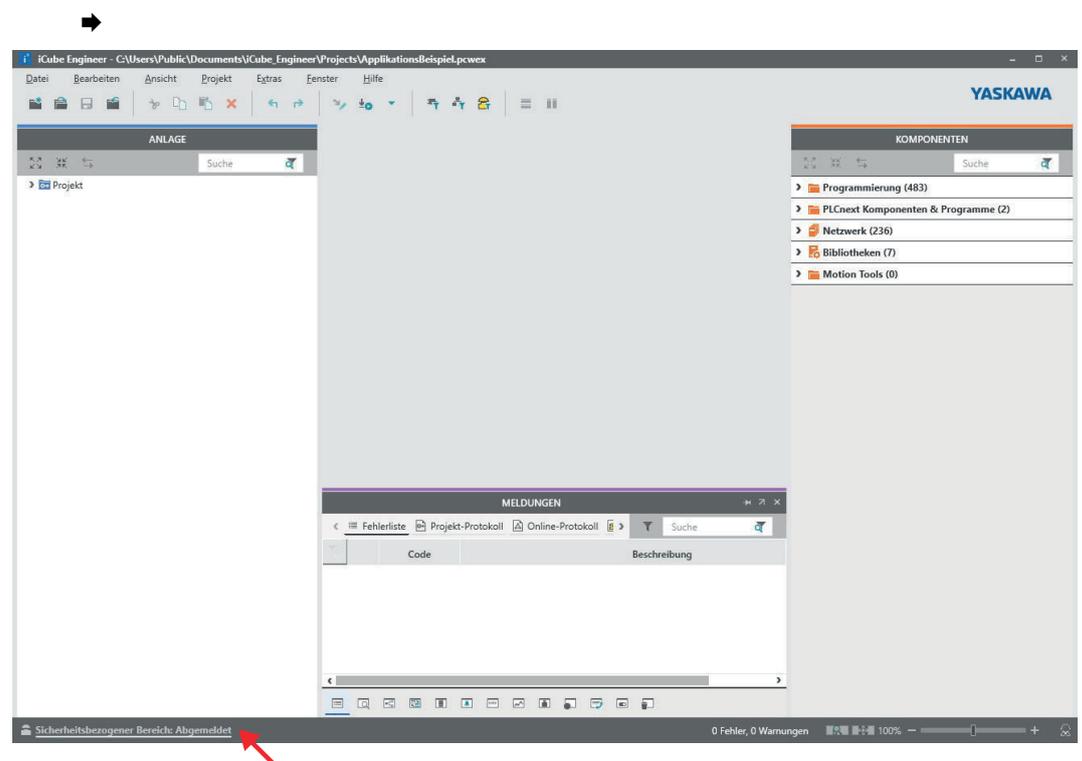


Weitere Informationen zur Vorgehensweise finden Sie unter [↔ "Programmierung und Dateisystem" ...Seite 87.](#)

1. Öffnen Sie iCube Engineer und wählen Sie die Vorlage für Ihre Safety-CPU.

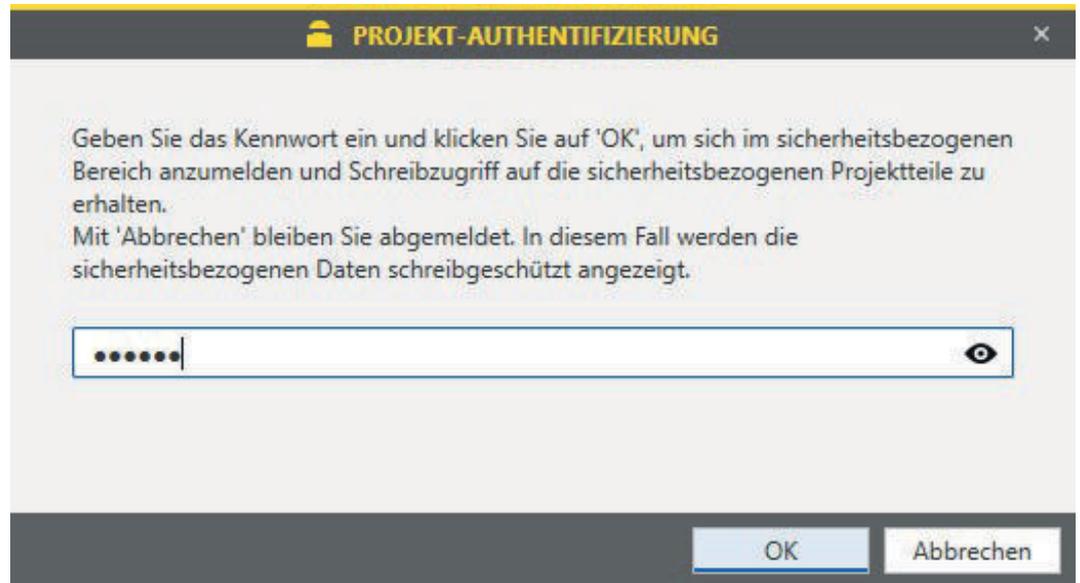


2. Speichern Sie das Projekt unter einem passenden Projektnamen. Lassen Sie den Projektpfad unverändert.

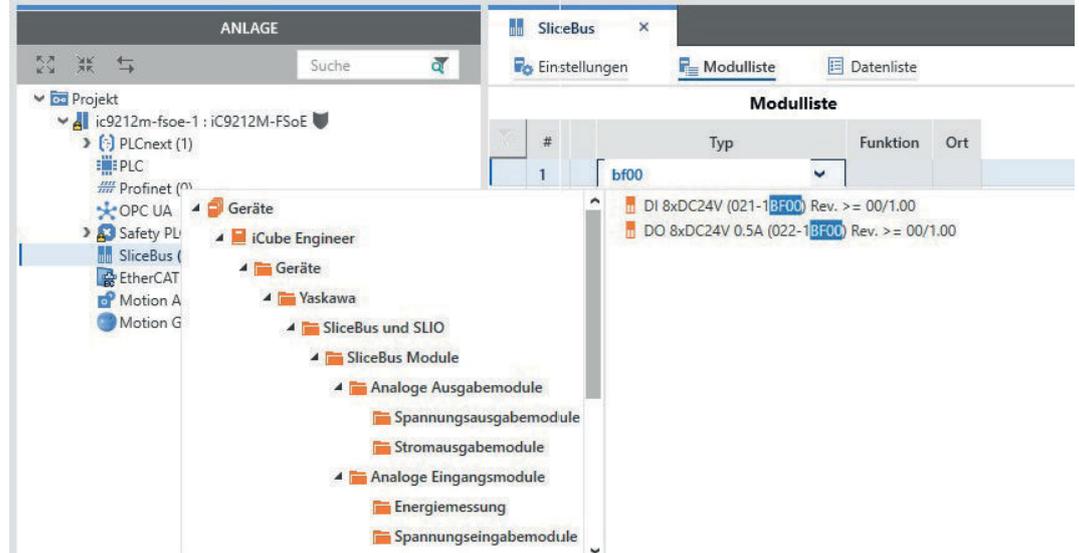


Applikationsbeispiel > Projektierung im iCube Engineer

3. → Klicken Sie auf *"Sicherheitsbezogener Bereich"* und geben Sie das Safety-Passwort ein. In der Vorlage wird das Passwort "safety" verwendet.
Klicken Sie auf [OK].



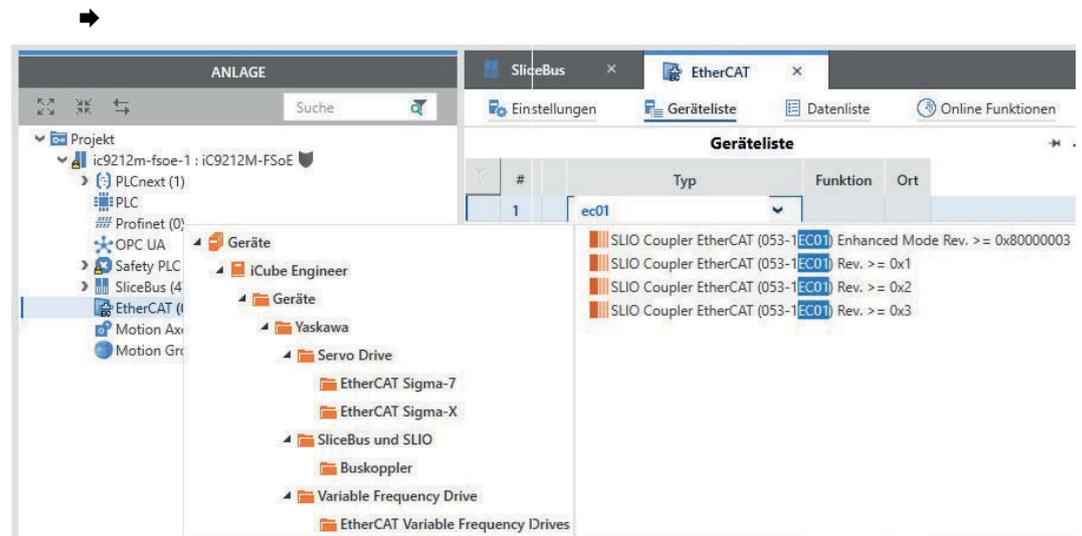
4. → Doppelklicken Sie unter *"Anlage"* in Ihrem Projekt auf *"SliceBus"* und ergänzen Sie Ihre lokalen SLIO Module indem Sie einen relevanten Teil des Namens eingeben und auf ein vorgeschlagenes Modul klicken.



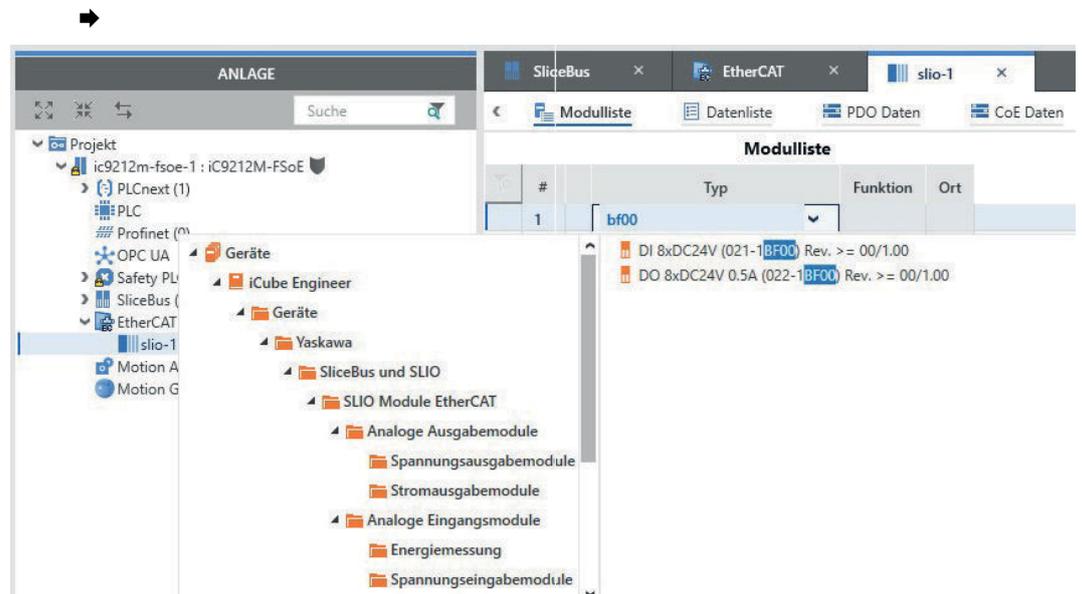
5. → Doppelklicken Sie unter "Anlage" in Ihrem Projekt auf "EtherCAT" und ergänzen Sie Ihren Koppler, indem Sie einen relevanten Teil des Namens eingeben und auf eine vorgeschlagene Version bzw. den Koppler mit Enhanced Mode klicken.



Alternativ können Sie über die rechte Maustaste einen "EtherCAT Bus Scan" durchführen. Hierbei darf iCube Engineer nicht zusätzlich online mit der Safety-CPU verbunden sein.



6. → Beim Bus-Scan werden die Module direkt eingefügt. Zur manuellen Platzierung doppelklicken Sie unter "Anlage" auf den EtherCAT-Koppler in Ihrem Projekt und ergänzen Sie ihre SLIO Module, indem Sie einen relevanten Teil des Namens eingeben und auf ein vorgeschlagenes Modul klicken.



7. → Ihre Hardware Konfiguration ist jetzt vollständig. Speichern Sie ihr Projekt.

Applikationsbeispiel > Projektierung im iCube Engineer

8. →



Bitte beachten Sie, dass systembedingt die Parametrierung der sicheren Modulparameter aktuell nur in der englischen Sprachsicht durchgeführt werden kann.

Zur Sprachumschaltung öffnen Sie im Menü "Extras → Optionen" und stellen unter "Lokalisierung" die Sprache auf "Englisch" ein.



9. → Speichern Sie Ihr Projekt.

10. → Starten Sie iCube Engineer neu mit Ihrem Projekt.

11. → Zur Einstellung der Modulparameter doppelklicken Sie auf das lokale Safety DI-Modul.

12. Geben Sie das Safety-Passwort ein und stellen Sie folgende Modulparameter ein:

- *Input evaluation: 1 channel*
- *Input signal-smoothing: 5ms*
- *Testpuls activation: deactivated*



The screenshot shows the iCube Engineer software interface. The left sidebar displays a project tree with the following structure:

- Project
 - ic9212m-fsoe-1 : iC9212M
 - PLCnext (1)
 - PLC
 - Profinet (0)
 - OPC UA
 - Safety PLC (1)
 - SliceBus (4)
 - di-1 : DI 8xDC24V/0.5A
 - do-1 : DO 8xDC24V/0.5A
 - di-2 : DI 4xDC24V/0.5A
 - do-2 : DO 4xDC24V/0.5A
 - EtherCAT (1)
 - sluo-1 : SLIO C
 - di-1 : DI 8xDC24V/0.5A
 - do-1 : DO 8xDC24V/0.5A
 - di-2 : DI 4xDC24V/0.5A
 - do-2 : DO 4xDC24V/0.5A
 - Motion Axes (0)
 - Motion Groups (0)

The main window displays the 'Safety Parameters' configuration for the 'FSoE' module. The 'FSoE Device Address' is set to 1. The 'FSoE Parameter Set' is configured as follows:

Parameter	Value
ComParameterLength:	2
Watchdog Time:	150
AppParameterLength:	16
Ch0,1: Re-integration after discrepancy fault:	Test 0-signal required
Ch0,1: Signal polarity:	equivalent
Ch0,1: Input evaluation:	1 channel
Ch0,1: Test pulse activation:	deactivated
Ch0,1: Activation:	activated
Ch2,3: Re-integration after discrepancy fault:	Test 0-signal required
Ch2,3: Signal polarity:	equivalent
Ch2,3: Input evaluation:	1 channel
Ch2,3: Test pulse activation:	deactivated
Ch2,3: Activation:	activated
Parameter change mode:	normal
Diagnostic Interrupt:	activated
Behaviour after Channel Errors:	Passivate the entire module
Ch0,1: Input signal-smoothing [ms]:	5
Ch0,1: Discrepancy timeout [ms]:	20
Ch2,3: Input signal-smoothing [ms]:	5
Ch2,3: Discrepancy timeout [ms]:	20

13. Zur Einstellung der Modulparameter doppelklicken Sie auf das lokale Safety DO-Modul.

Applikationsbeispiel > Projektierung im iCube Engineer

14. Stellen Sie folgende Modulparameter ein:

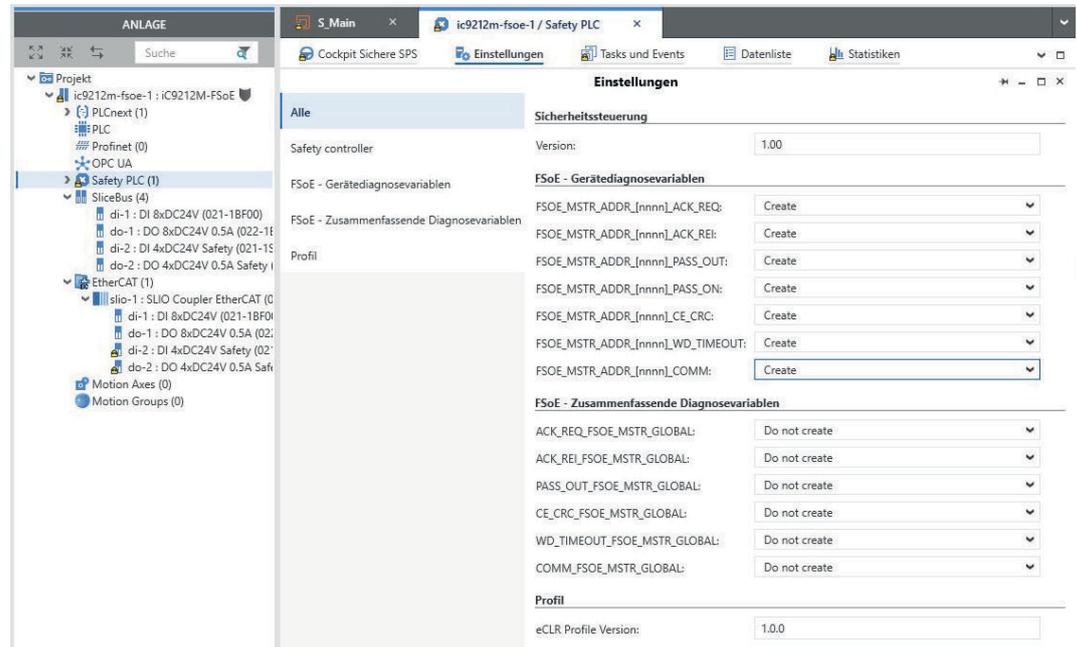
- *Activation Mode*: 1 channel
- *Test pulse length*: 2ms



Safety Parameters	
All	FSoE
FSoE	FSoE Device Address: 2
FSoE Parameter Set	FSoE Parameter Set
	ComParameterLength: 2
	Watchdog Time: 150
	ApplParameterLength: 16
	Ch0: Wire break recognition: deactivated
	Ch1: Wire break recognition: deactivated
	Ch0,1: Activation mode: 1 channel
	Ch0,1: Activation: activated
	Ch2: Wire break recognition: deactivated
	Ch3: Wire break recognition: deactivated
	Ch2,3: Activation mode: 1 channel
	Ch2,3: Activation: activated
	Parameter change mode: normal
	Diagnostic Interrupt: activated
	Ch0: Test pulse length [us]: 2ms
	Ch1: Test pulse length [us]: 2ms
	Ch2: Test pulse length [us]: 2ms
	Ch3: Test pulse length [us]: 2ms

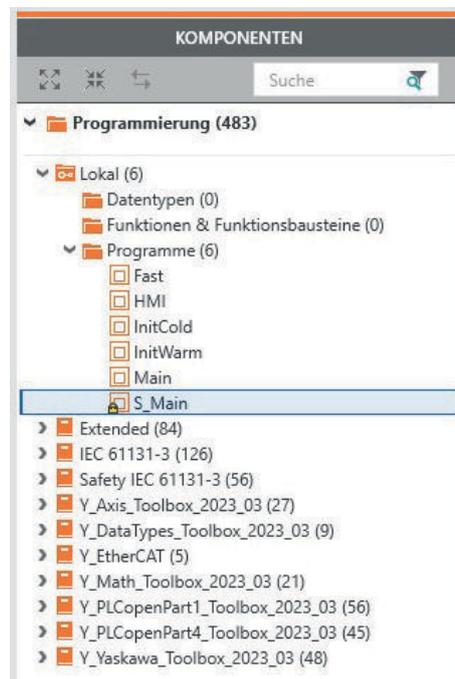
15. Wiederholen Sie die Parametrierung für die Safety Module am FSoE EtherCAT Koppler.**16.** Doppelklicken Sie unter "Anlage" auf die "Safety PLC" in Ihrem Projekt und öffnen Sie die Einstellungen.

17. Aktivieren Sie dort alle "FSoE-Gerätediagnosevariablen", indem Sie "Create" aktivieren.



➔ Ihre Parametrierung ist jetzt vollständig.

18. Speichern Sie ihr Projekt.



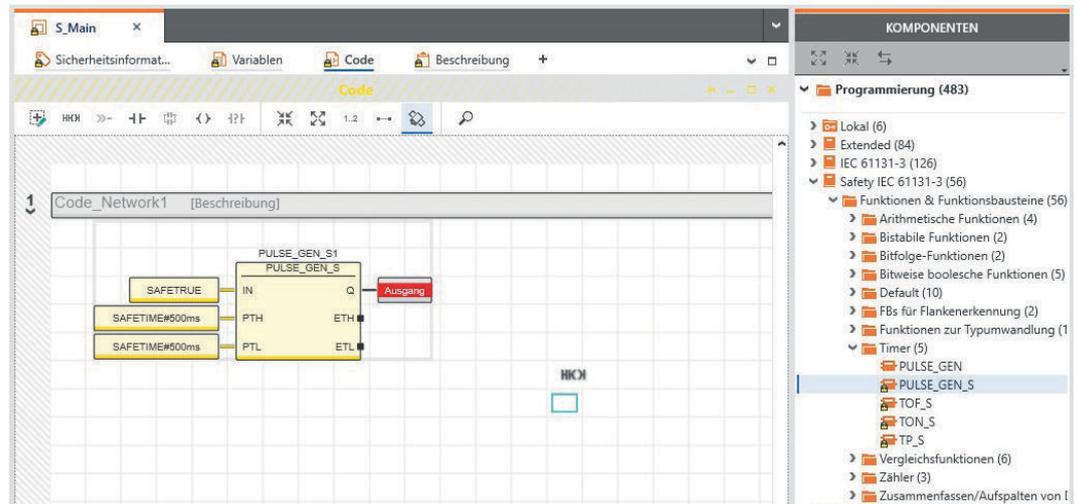
19. Navigieren Sie unter "Komponenten" zu "Programmierung → Lokal → Programme" und öffnen Sie "S_Main".

➔ Der Programm-Editor für Ihre Safety-Applikation wird geöffnet.

20. Geben Sie das Safety-Passwort ein und klicken Sie auf [OK].

Applikationsbeispiel > Projektierung im iCube Engineer

21. Programmieren Sie Ihre Applikation in folgender Reihenfolge:
- Ziehen Sie einen *PULSE_GEN_S* in den Editor.
 - Versorgen Sie den Eingangsparameter *IN* mit *SAFETRUE*.
 - Versorgen Sie die beiden Zeitparameter mit *SAFETIME#500ms*.
 - Geben Sie dem Ausgang *Q* den Namen *Ausgang*.
 - Legen Sie mit Rechtsklick auf *Ausgang* "Neue Variable anlegen → Lokal" eine neue lokale Variable an.

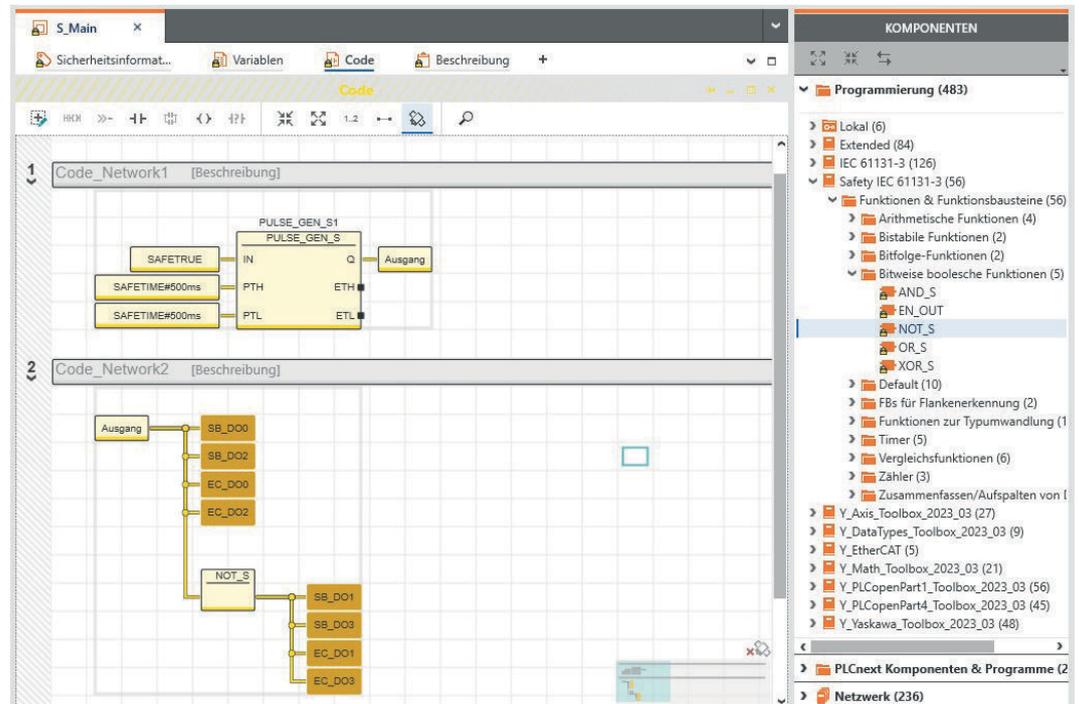


22. Wechseln Sie in den Reiter "Variablen" und legen Sie 8 externe Variablen an, welche später mit den Ausgängen verknüpft werden. Hierbei können Sie die angelegten Variablen kopieren.



Name	Typ	Verw.	Kommentar	Init	Rückkoppl
PULSE_GEN_S1	PULSE_GEN_S	Lokal			
Ausgang	SAFEBOOL	Lokal		SAFEFALSE	<input type="checkbox"/>
SB_DO0	SAFEBOOL	Extern			
SB_DO1	SAFEBOOL	Extern			
SB_DO2	SAFEBOOL	Extern			
SB_DO3	SAFEBOOL	Extern			
EC_DO0	SAFEBOOL	Extern			
EC_DO1	SAFEBOOL	Extern			
EC_DO2	SAFEBOOL	Extern			
EC_DO3	SAFEBOOL	Extern			
Geben Sie hier einen V...					<input type="checkbox"/>

23. Wechseln Sie in den Reiter "Code", fügen Sie die Variable *Ausgang* ein und verbinden Sie diese mit der Ausgangs-Variable mit gerader Nummerierung. Invertieren Sie die Variable *Ausgang* mit einem *NOT_S* und verbinden Sie diese mit der Ausgangs-Variable mit ungerader Nummerierung.



24. Doppelklicken Sie auf die "Safety PLC" und wechseln Sie in den Reiter "Datenliste".



Variable (Sichere SPS)	Variable (SPS)	Prozessdaten-Element
SB_DO0	Variable (SPS) auswählen	Prozessdaten-Element ausw...
SB_DO1	Variable (SPS) auswählen	Prozessdaten-Element ausw...
SB_DO2	Variable (SPS) auswählen	Prozessdaten-Element ausw...
SB_DO3	Variable (SPS) auswählen	Prozessdaten-Element ausw...
EC_DO0	Variable (SPS) auswählen	Prozessdaten-Element ausw...
EC_DO1	Variable (SPS) auswählen	Prozessdaten-Element ausw...
EC_DO2	Variable (SPS) auswählen	Prozessdaten-Element ausw...
EC_DO3	Variable (SPS) auswählen	Prozessdaten-Element ausw...
Variablenname eingeben	Variable (SPS) auswählen	Prozessdaten-Element ausw...
System Variables		

Applikationsbeispiel > Projektierung im iCube Engineer

25. Klicken Sie in das Feld "Prozessdaten-Element" der ersten Ausgangs-Variable und wählen Sie für eine bessere Filterung das Safety DO am "SliceBus" aus.



The screenshot shows the 'Datenliste' window in iCube Engineer. The 'Prozessdaten-Element' column is selected, and the 'do-2 : DO 4xDC24V 0.5A Safety (022-1SD10)' is highlighted in the tree view. The tree view shows the following structure:

- Projekt
 - ic9212m-fsoe-1 : iC9212M-FSoE
 - SliceBus
 - di-2 : DI 4xDC24V Safety (021-1SD10)
 - do-2 : DO 4xDC24V 0.5A Safety (022-1SD10)
 - EtherCAT
 - slio-1 : SLIO Coupler EtherCAT (053-1EC01) Enhanced Mode
 - di-2 : DI 4xDC24V Safety (021-1SD10)
 - do-2 : DO 4xDC24V 0.5A Safety (022-1SD10)

26. Ordnen Sie alle 8 Safety-Ausgänge zu.

The screenshot shows the 'Datenliste' window in iCube Engineer. The 'Prozessdaten-Element' column is selected, and the 'Funktion' column is empty. The table shows the following data:

Variable (Sichere SPS)	Variable (SPS)	Prozessdaten-Element	Funktion
SB_DO0	Variable (SPS) auswählen	do-2 / DO0	
SB_DO1	Variable (SPS) auswählen	do-2 / DO1	
SB_DO2	Variable (SPS) auswählen	do-2 / DO2	
SB_DO3	Variable (SPS) auswählen	do-2 / DO3	
EC_DO0	Variable (SPS) auswählen	slio-1 / do-2 / DO0	
EC_DO1	Variable (SPS) auswählen	slio-1 / do-2 / DO1	
EC_DO2	Variable (SPS) auswählen	slio-1 / do-2 / DO2	
EC_DO3	Variable (SPS) auswählen	slio-1 / do-2 / DO3	

➔ Sie erhalten folgende Fehlermeldung:

The screenshot shows the 'MELDUNGEN' window in iCube Engineer. The 'Fehlerliste' tab is selected, and the following error messages are displayed:

Code	Beschreibung
SBIO0008	Das Modul ic9212m-fsoe-1 / di-2 hat keine verbundenen Eingänge.
EC1007	Das Modul ic9212m-fsoe-1 / slio-1 / di-2 hat keine verbundenen Eingänge.

27. Zur Vermeidung der Fehlermeldungen erstellen Sie 8 externe Variablen in "S_Main", welche Sie mit den Safety-Eingängen verknüpfen.
28. Nachdem das Mapping der Prozessdaten fertig ist, speichern und übersetzen Sie das Projekt mit "Projekt → Neu erzeugen".

29. Mit *Speichern und Übersetzen* ist nun die Anzahl der Warnungen gestiegen. Doppelklicken Sie auf die erste Meldung, in der die Adresse des Anwenders nicht validiert ist.
 ➔ Der Cursor springt auf die erste Variable in der Datenliste der "Safety PLC".
30. Zum Einblenden weitere Tabellenspalten klicken Sie auf das ">" im Tabellenkopf.
31. Navigieren Sie zur Spalte "*Bestätigen*" und aktivieren Sie die Kontrollkästchen aller 16 Variablen.
 ➔

Variable (Sichere SPS)	Typ	Verw.	I/Q/M	Kommentar	Init	Bestätigen
SB_DO0	SAFEBOOL	Global	Q		SAFEFALSE	<input checked="" type="checkbox"/>
SB_DO1	SAFEBOOL	Global	Q		SAFEFALSE	<input type="checkbox"/>
SB_DO2	SAFEBOOL	Global	Q		SAFEFALSE	<input type="checkbox"/>
SB_DO3	SAFEBOOL	Global	Q		SAFEFALSE	<input type="checkbox"/>
EC_DO0	SAFEBOOL	Global	Q		SAFEFALSE	<input type="checkbox"/>
EC_DO1	SAFEBOOL	Global	Q		SAFEFALSE	<input type="checkbox"/>
EC_DO2	SAFEBOOL	Global	Q		SAFEFALSE	<input type="checkbox"/>
EC_DO3	SAFEBOOL	Global	Q		SAFEFALSE	<input type="checkbox"/>
SB_DI0	SAFEBOOL	Global	I		SAFEFALSE	<input type="checkbox"/>
SB_DI1	SAFEBOOL	Global	I		SAFEFALSE	<input type="checkbox"/>
SB_DI2	SAFEBOOL	Global	I		SAFEFALSE	<input type="checkbox"/>
SB_DI3	SAFEBOOL	Global	I		SAFEFALSE	<input type="checkbox"/>
EC_DI0	SAFEBOOL	Global	I		SAFEFALSE	<input type="checkbox"/>
EC DI1	SAFEBOOL	Global	I		SAFEFALSE	<input type="checkbox"/>

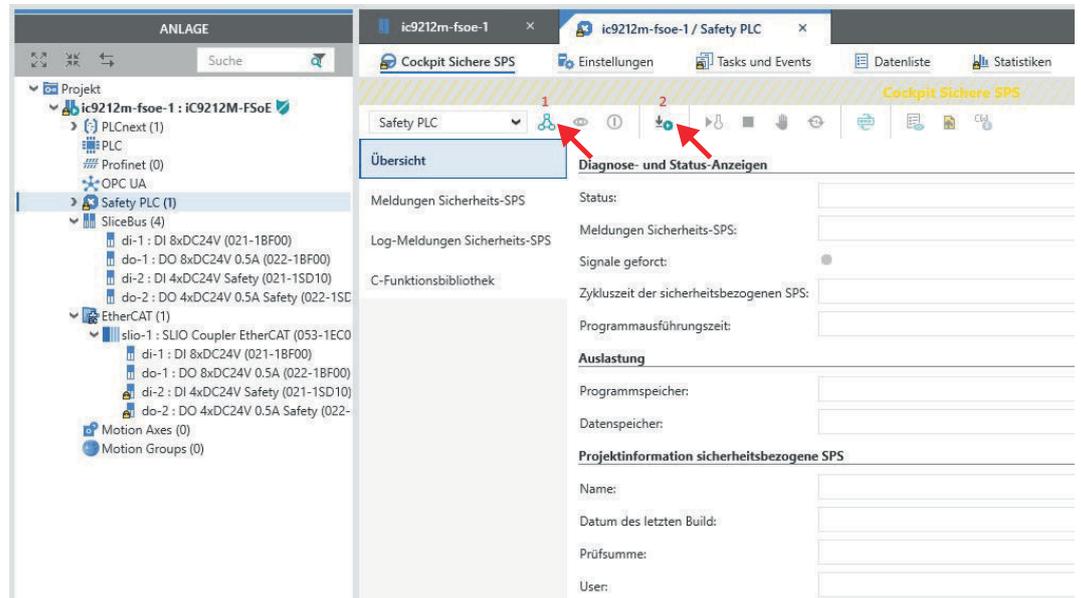
32. Doppelklicken Sie im Bereich "*Anlage*" auf den Controller in Ihrem Projekt und wechseln Sie in den Reiter "*Cockpit*".
 ➔

The screenshot shows the 'ANLAGE' tree on the left with the 'ic9212m-fsoe-1' project selected. The 'Cockpit' window on the right is active, showing the 'LAN (X3/X4)' interface. Red arrows point to the online symbol (1) and the download symbol (2).

33. Gehen Sie über das Symbol online.
34. Geben Sie den Namen "Admin" und das aufgedruckte Geräte-Passwort ein.
35. Übertragen Sie mit Symbol das Projekt in die Standard-Komponente der Safety-CPU.

Applikationsbeispiel > Modifikation

36. Doppelklicken Sie im Bereich "Anlage" auf ihre "Safety PLC" und wechseln Sie in den Reiter "Cockpit Sichere SPS".



37. Gehen Sie mit dem  Symbol online.

38. Mit dem  Symbol übertragen Sie das Projekt in die Safety-Komponente der Safety-CPU.

- ➔ Es erscheint eine Passwortabfrage der Safety-CPU. Vergeben Sie ein neues Passwort oder geben Sie ein Passwort ein, das Sie berechtigt das Projekt auf der Safety-CPU zu überschreiben.

5.13.3 Modifikation

- Auswertung der FSoE-Gerätediagnosevariablen
- Zurücksetzen einer Passivierung

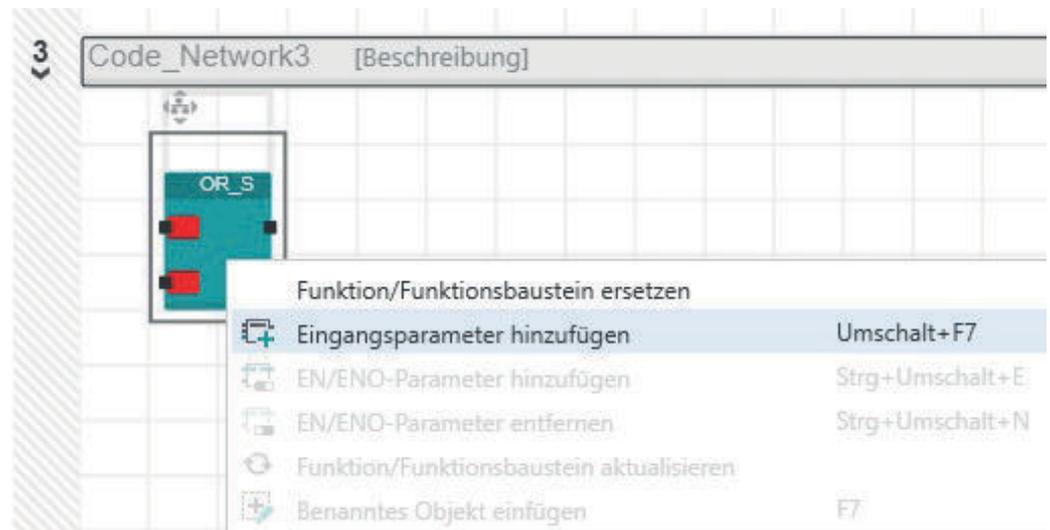
1. Öffnen Sie den Reiter "Variablen" in "S_Main" und ergänzen Sie folgende Variablen:

- *FSoE_ACK_REQ*
- *FSoE_PASS_OUT*
- *FSoE_ACK_REI*
- *FSoE_PASS_ON*

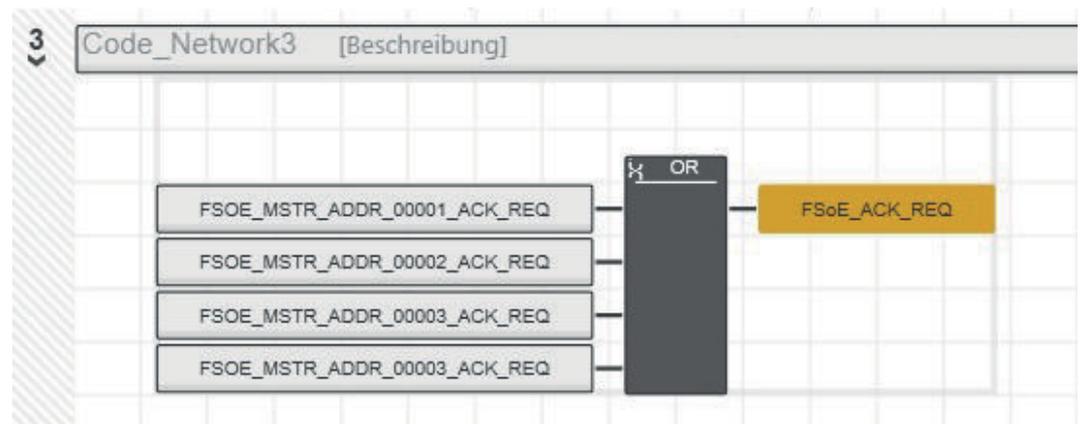


Name	Typ	Verw.	Kommentar
FSoE_ACK_REQ	BOOL	Extern	
FSoE_PASS_OUT	BOOL	Extern	
FSoE_ACK_REI	BOOL	Extern	
FSoE_PASS_ON	BOOL	Extern	

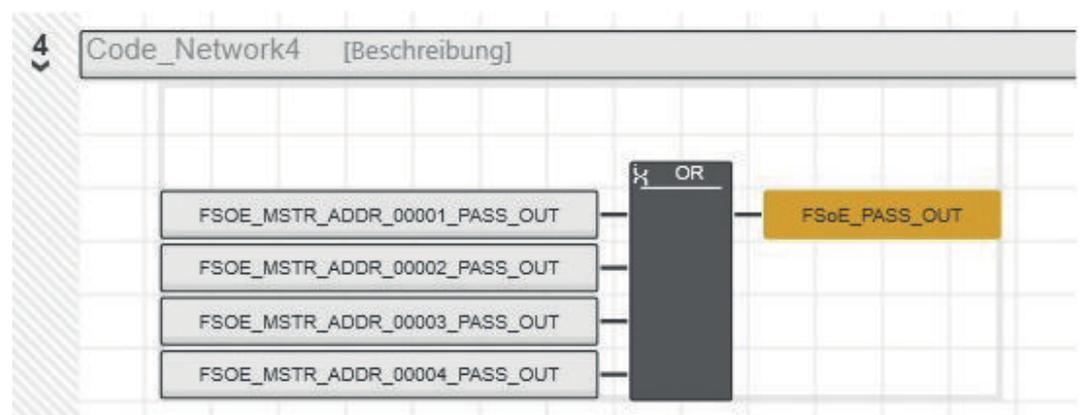
2. Öffnen Sie den Reiter "Code" in "S_Main", ziehen Sie ein OR hinein und ergänzen Sie zwei weitere Eingangsparameter.



3. Fügen Sie über "Eingangsparameter hinzufügen" die Eingangsparameter *FSoE_MSTR_ADDR_0000x_ACK_REQ* hinzu und den Ausgang *FSoE_ACK_REQ*.

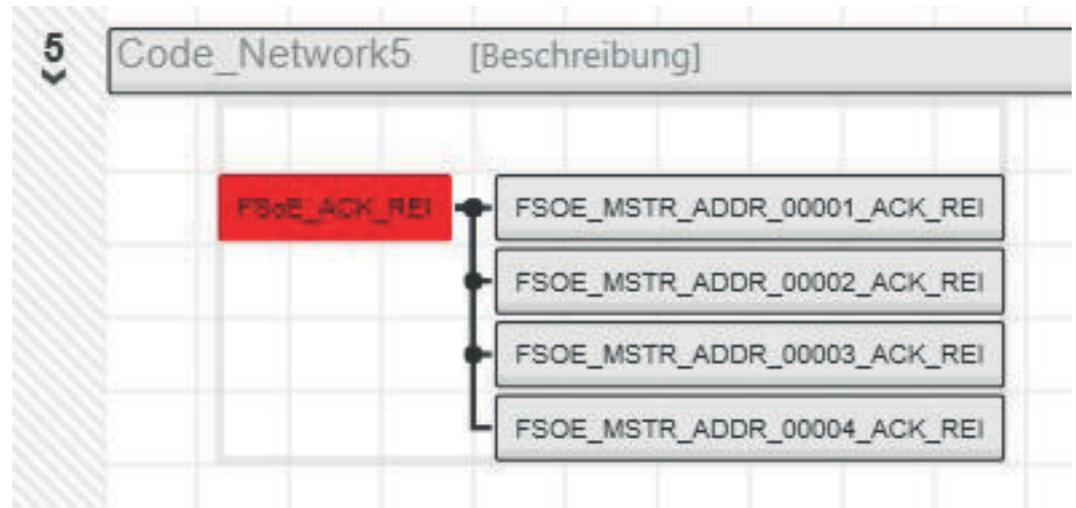


4. Fügen Sie ein weiteres OR hinzu und verfahren Sie mit *FSoE_MSTR_ADDR_0000x_PASS_OUT* und *FSoE_PASS_OUT* auf die gleiche Weise.

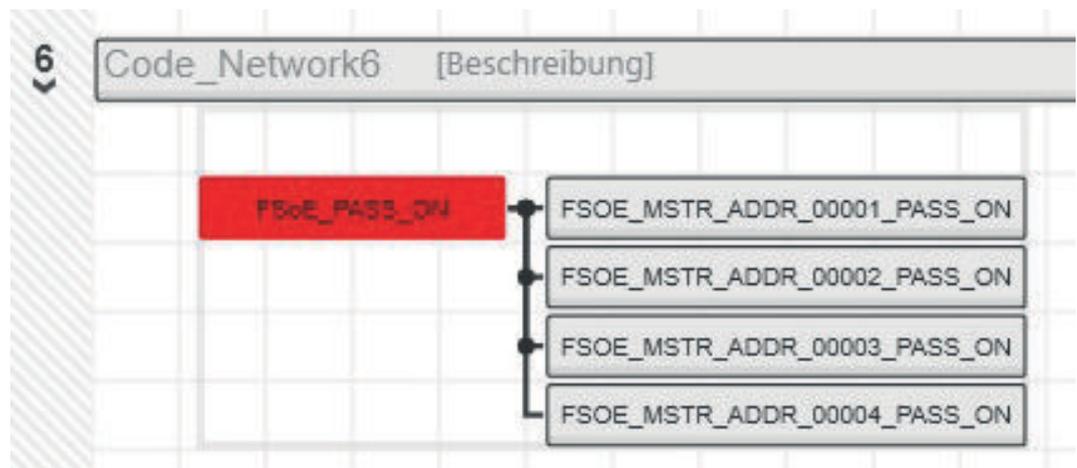


Applikationsbeispiel > Modifikation

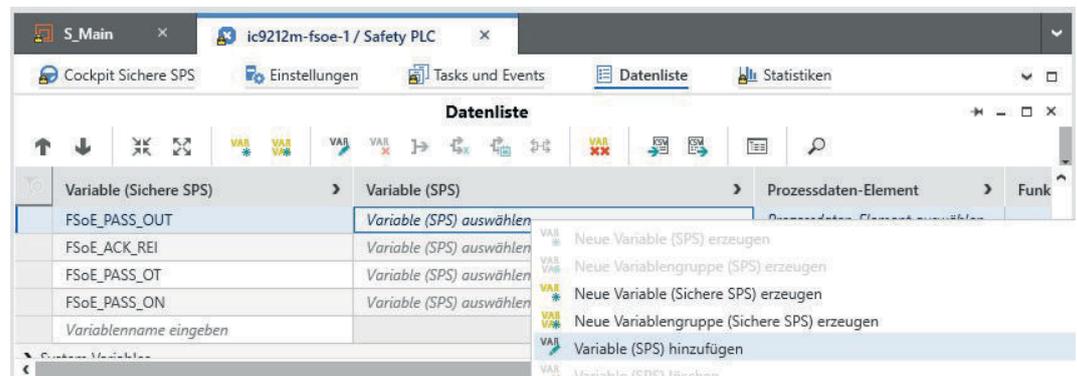
5. Fügen Sie *FSoE_ACK_REI* ein und verbinden Sie es mit allen *FSoE_MSTR_ADDR_0000x_ACK_REI*.



6. Fügen Sie *FSoE_PASS_ON* ein und verbinden Sie es mit allen *FSoE_MSTR_ADDR_0000x_PASS_ON*.



7. Öffnen Sie die "Datenliste" der "Safety PLC" und fügen Sie über "Variable (SPS) hinzufügen" die vier FSoE-Variablen der Standard-Komponente der Safety-CPU hinzu.



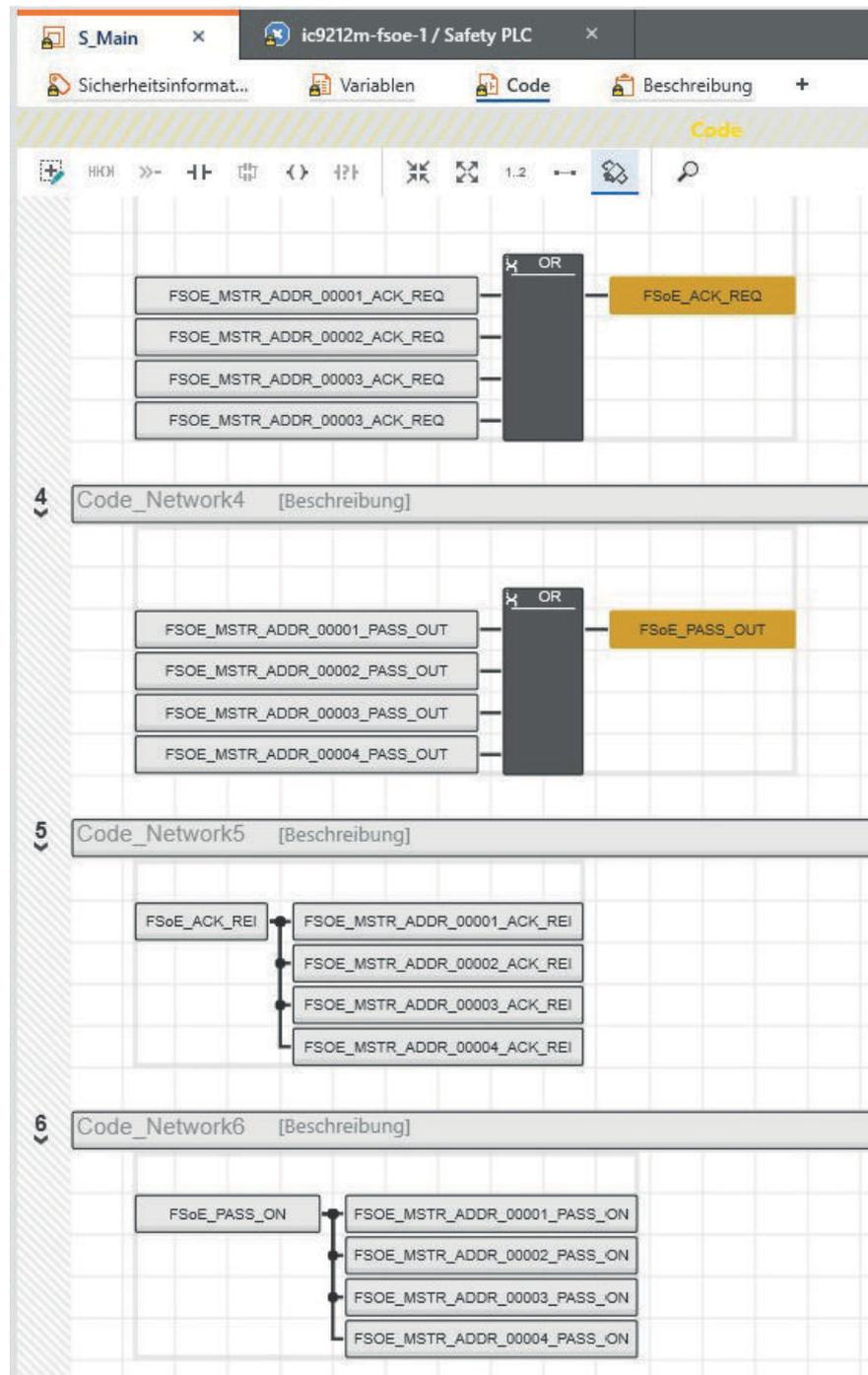
8. → Wählen Sie unter "I/Q/M" die Datenrichtung, "Q" für Ausgang und "I" für Eingang.



Variable (Sichere SPS)	Typ	Verw.	I/Q/M	Kommentar	Init	Bestätigen	Variable (SPS)
EC_DI3	SAFEBOOL	Global	I		SAFEFALSE	<input checked="" type="checkbox"/>	Variable (SPS) ausw
FSoE_ACK_REQ	BOOL	Global	Q		FALSE		FSoE_ACK_REQ
FSoE_PASS_OUT	BOOL	Global	Q		FALSE		FSoE_PASS_OUT
FSoE_ACK_REI	BOOL	Global	I		FALSE		FSoE_ACK_REI
FSoE_PASS_ON	BOOL	Global	I		FALSE		FSoE_PASS_ON
Variablename eingeben	SAFEBOOL	Global				<input type="checkbox"/>	

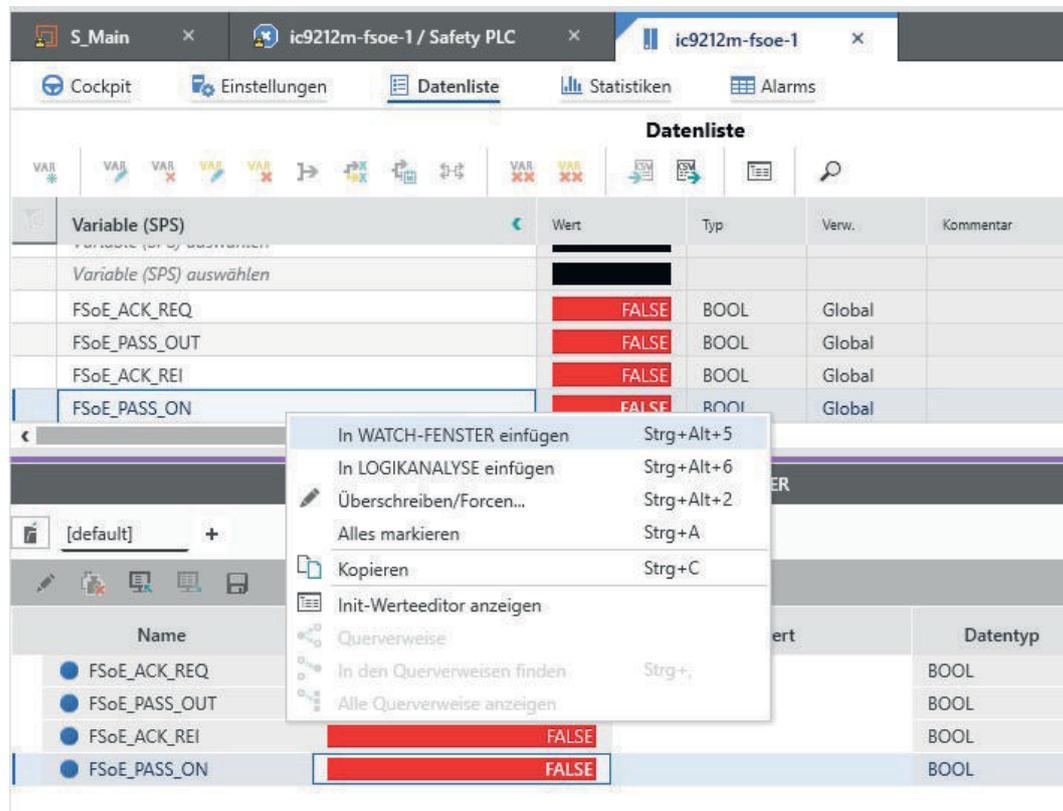
Applikationsbeispiel > Modifikation

9. Im Code von "S_Main" sollte jetzt nichts mehr rot markiert sein.

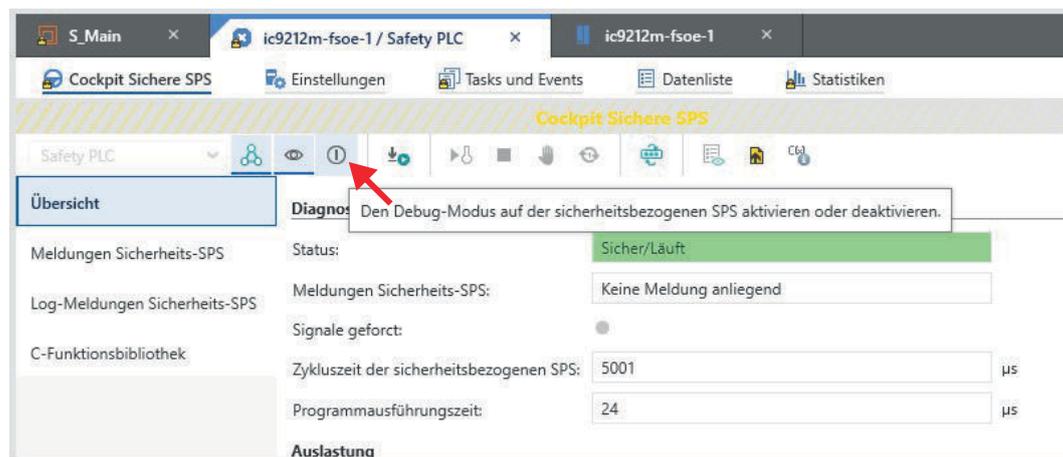


10. Speichern Sie ihr Projekt und übertragen Sie dies.

11. Fügen Sie über "In Watch-Fenster einfügen" alle vier Variablen dem "Watch-Fenster" hinzu.



12. Öffnen Sie das "Cockpit" der Safety PLC "Cockpit Sichere SPS" und überprüfen Sie ob Sie online sind und schalten Sie zusätzlich über  den Debug-Modus ein.



13. Öffnen Sie in Ihrer "Safety PLC" "S_Main:S_Main".

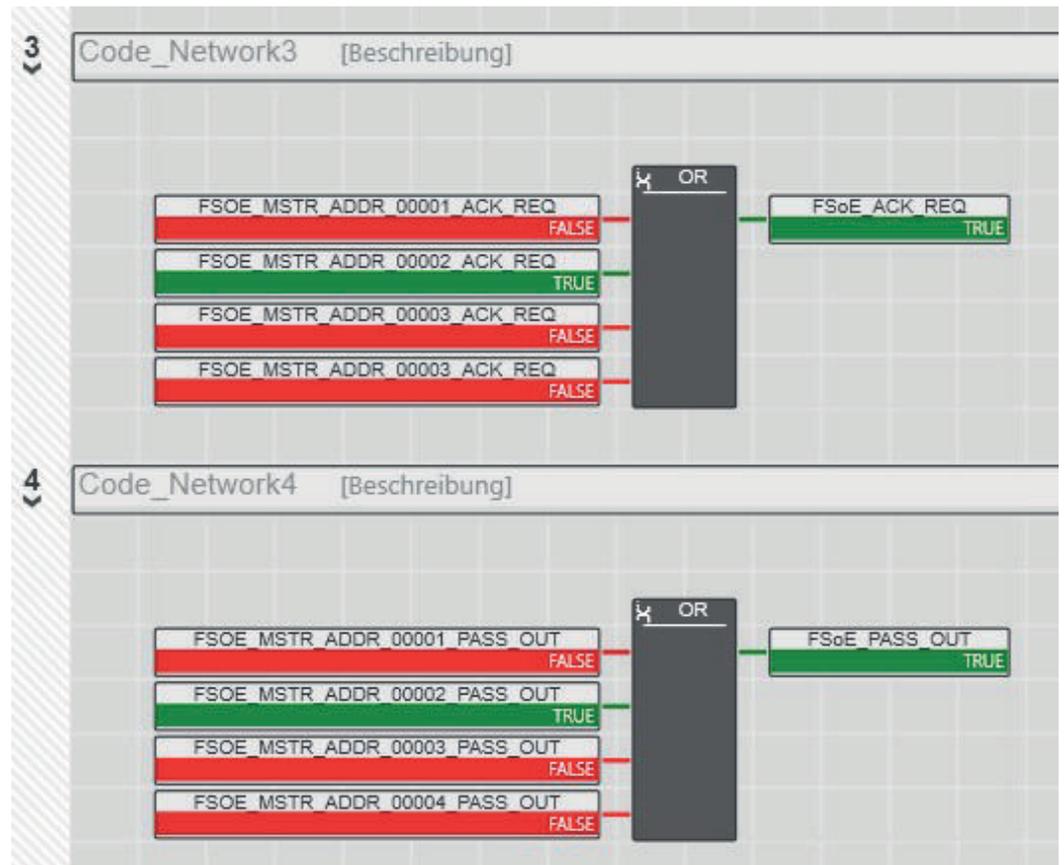


Name	Wert	Sollwert
FSoE_ACK_REQ	FALSE	
FSoE_PASS_OUT	FALSE	
FSoE_ACK_REI	FALSE	
FSoE_PASS_ON	FALSE	

Sicherheitsbezogener Bereich: Angemeldet Sicherheitsbezogene SPS: Debug-Modus aktiv

14. Schalten Sie kurz die DC 24V Leistungsversorgung der IO-Module am Rückwandbus aus und wieder ein.

➔ Das Safety-DO wird passiviert.



15. Zur Reintegration setzen Sie *FSoE_ACK_REI* im "Watch-Fenster" auf *True*.



Name	Wert
● FSoE_ACK_REQ	TRUE
● FSoE_PASS_OUT	TRUE
● FSoE_ACK_REI	FALSE
● FSoE_PASS_ON	TRUE

16. Sobald die Reintegration erfolgreich ist, setzen Sie *FSoE_ACK_REI* im "Watch-Fenster" wieder auf *False*.

5.14 Funktionale Sicherheit - Sicherheitsrelevante Kenngrößen

Allgemein

In diesem Kapitel werden Kenngrößen im Zusammenhang mit funktionaler Sicherheit beschrieben. Unter Sicherheit ist gemäß IEC 61508 zunächst zu verstehen, dass das Gesamtsystem eine Restfehlerwahrscheinlichkeit kleiner als die in der Norm vorgegebenen Grenzen hat. Bezogen auf die Gesamtanwendung müssen interne sicherheitsrelevante Gerätefehler erkannt werden und zu einem sicheren Zustand führen.

Funktionale Sicherheit - Sicherheitsrelevante Kenngrößen

Sicherheitsrelevante Kenngrößen

Die hier angegebenen Werte beziehen sich ausschließlich auf die in diesem Handbuch angegebenen Safety-CPU. Sicherheitsrelevante Kenngrößen finden Sie immer in den entsprechenden Handbüchern zu den Modulen.

**HINWEIS**

Nach Ablauf der Gerätelebensdauer muss die Safety-CPU außer Betrieb genommen und an den Hersteller gesendet werden!

Kenngrößen gemäß DIN EN ISO 13849-1	Wert	Bedeutung
Performance Level	max. e	Maß für die Zuverlässigkeit einer Sicherheitsfunktion.
Kategorie	max 4	Maß für die Widerstandsfähigkeit gegen Fehler.
PFH _D	1 * 10 ⁻⁹ /h	Probability of Failure per Hour: Restfehlerrate für einen gefährlichen Fehler pro Stunde.
DCavg	99%	Diagnostic Coverage average: Mittlerer Diagnosedeckungsgrad.
MTTF _D	> 80 Jahre	Mean Time To dangerous Failure: Mittlere Zeit bis zu einem gefährlichen Ausfall.

Kenngrößen gemäß IEC 62061	Wert	Bedeutung
SIL CL:	max. 3	Safety Integrity Level Claim Limit Sicherheitsanforderungsstufe zur Klassifizierung der funktionalen Sicherheit des Teilsystems.
PFH _D	1 * 10 ⁻⁹ /h	Probability of Failure per Hour: Restfehlerrate für einen gefährlichen Fehler pro Stunde.
HFT	1	Hardware Fault Tolerance Anzahl Fehler, welche zu einem Verlust der Sicherheitsfunktion führen können.
Lifetime	300 Monate	Gerätelebensdauer Während der erwarteten Gerätelebensdauer ist keine Wartung erforderlich.
SFF	99%	Safe Failure Fraction: Anteil der Ausfälle, die in den sicheren Zustand führen.

Kenngrößen gemäß IEC 61508	Wert	Bedeutung
SIL	max. 3	Safety Integrity Level Sicherheitsanforderungsstufe zur Klassifizierung der funktionalen Sicherheit.
PFH _D	1 * 10 ⁻⁹ /h	Probability of Failure per Hour: Restfehlerrate für einen gefährlichen Fehler pro Stunde.
HFT	1	Hardware Fault Tolerance Anzahl Fehler, welche zu einem Verlust der Sicherheitsfunktion führen können.
Lifetime	300 Monate	Gerätelebensdauer Während der erwarteten Gerätelebensdauer ist keine Wartung erforderlich.

5.15 Systemvariablen und Zustandsinformationen

5.15.1 Allgemeines

Zugriff auf Systemvariablen und Datenstrukturen

- In diesem Kapitel werden Systemvariablen beschrieben, die für die CPU zur Verfügung stehen.
- Die CPU besitzt einen Registersatz, der zur Diagnose und zur einfachen Steuerung der CPU eingesetzt wird.
- Die Diagnosedaten werden im Diagnose-Statusregister und im Diagnose-Parameterregister abgelegt. Diese Register stehen dem Anwendungsprogramm als Systemvariablen (Systemmerker, globale Variablen) zur Verfügung.
- Einige Systemvariablen der CPU sind als Datenstrukturen organisiert. Die Datenstruktur einer solchen Systemvariable beinhaltet dabei weitere Systemvariablen.
- Im *"Init-Werteeditor"* von iCube Engineer können Sie einsehen, welche Systemvariablen im Einzelnen zu einer als Datenstruktur organisierten Systemvariable gehören.

Um den *"Init-Werteeditor"* für eine als Datenstruktur organisierten Systemvariable zu öffnen, gehen Sie wie folgt vor:

1.  Doppelklicken Sie im Bereich Anlage auf den Knoten SPS.
 - ➔ Die Editorengruppe der CPU/SPS wird geöffnet.
2.  Wählen Sie den Editor Datenliste.



Alternativ können Sie den Editor Datenliste im Bereich Anlage über den Knoten der CPU öffnen.

3.  Öffnen Sie den Bereich Systemvariablen.
4.  Klicken Sie in der Spalte Variable (SPS) auf den Pfeil, zur Anzeige der erweiterten Informationen.
 - ➔ In der Spalte Typ der erweiterten Informationen wird der Datentyp der Systemvariablen angezeigt.
5.  Markieren Sie die Zeile der als Datenstruktur organisierten Systemvariable, deren zugehörige Systemvariablen Sie einsehen möchten. Klicken Sie hierzu auf die erste Spalte in der Zeile der als Datenstruktur organisierten Systemvariable.
6.  Klicken Sie auf die Schaltfläche .
 - ➔ Der *"Init-Werteeditor"* der gewählten als Datenstruktur organisierten Systemvariable wird unterhalb des Editors Datenliste geöffnet.

The screenshot displays the 'Datenliste' window with the following table:

Variable (SPS)	Typ	Verw.	Kommentar	Init.
PND_S1_OUTPUTS	PND_IO_...	Global	Output proc...	
PND_S1_INPUTS	PND_IO_...	Global	Input proces...	
PND_IO_DRIVEN_BY_PLC	INT	Global		INT#0
ESM_DATA	ESM_DAT	Global		
RTC	RTC_TYPE	Global		
DEVICE_STATE	DEVICE_S...	Global		
USER_PARTITION	PARTITIO...	Global		

Below the 'Datenliste' window is the 'Init-Werteeditor' window, which contains the following table:

Elementname	Init-Wert Element
HOURS	USINT#0
MINUTES	USINT#0
SECONDS	USINT#0
DAY	USINT#0
MONTH	USINT#0
YEAR	UINT#0

Im "Init-Werteeditor" werden in der Spalte Elementname alle Systemvariablen aufgelistet, welche in der als Datenstruktur organisierten Systemvariable enthalten sind.

5.15.2 Systemvariablen

Systemzeit

- Die Systemvariable RTC ist eine als Datenstruktur organisierte Systemvariable.
- Mit der Systemvariable RTC können Sie Informationen zur Systemzeit der geräteinternen Echtzeituhr abrufen.

Systemvariable	Typ - Beschreibung
RTC	RTC_TYPE - Datenstruktur
HOURS	USINT - Systemzeit (Stunden)
MINUTES	USINT - Systemzeit (Minuten)
SECONDS	USINT - Systemzeit (Sekunden)
DAY	USINT - Systemzeit (Tag)
MONTH	USINT - Systemzeit (Monat)
YEAR	UINT - Systemzeit (Jahr)

Funktionsbausteine
TLS_SOCKET_2
UDP_SOCKET_2

- Mit dem Funktionsbaustein TLS_SOCKET_2 öffnen und schließen Sie IP-Sockets für die IP-Kommunikation über TCP (Transmission Control Protocol - nicht sicher) oder TLS (Transport Layer Security - sicher). Mit dem Eingabeparameter START_TLS können Sie dies steuern (FALSE: TCP, TRUE: TLS).
- Mit dem Baustein UDP_SOCKET_2 öffnen und schließen Sie IP-Sockets für die IP-Kommunikation über UDP (User Datagram Protocol).
- Die Anzahl der geöffneten IP-Sockets können Sie mit den folgenden Systemvariablen abrufen:

Systemvariable	Typ - Beschreibung
IP_ACTIVE_SOCKETS	UINT - Anzahl der mit den Funktionsbausteinen TLS_SOCKET_2 und UDP_SOCKET_2 geöffneten TCP/UDP-Sockets.
TLS_ACTIVE_SOCKETS	UINT - Anzahl der mit dem Funktionsbaustein TLS_SOCKET geöffneten TLS-Sockets.

Gerätestatus

- Die Systemvariable DEVICE_STATE ist eine als Datenstruktur organisierte Systemvariable.
- Mit der Systemvariable DEVICE_STATE können Sie verschiedene Informationen zum Gerätestatus der CPU abrufen.

Systemvariable	Typ - Beschreibung
DEVICE_STATE	DEVICE_STATE_X152_TYPE - Datenstruktur
BOARD_TEMPERATURE	SINT - Temperatur im Gehäuseinneren (in °C).
reserved1	BOOL - reserviert
reserved2	USINT - reserviert
CPU_LOAD_ALL_CORES	USINT - durchschnittliche aktuelle Auslastung aller Prozessorkerne (in %).
CPU_LOAD_PER_CORE	CPU_LOAD_PER_CORE_ARRAY - Informationen zur Auslastung je Prozessorkern.
[1]	USINT - aktuelle Auslastung Prozessorkern 1 (in %).
[2]	USINT - aktuelle Auslastung Prozessorkern 2 (in %).

Systemvariablen und Zustandsinformationen > Systemvariablen

Partition

- Die Systemvariable USER_PARTITION ist eine als Datenstruktur organisierte Systemvariable.
- Mit der Systemvariable USER_PARTITION können Sie verschiedene Informationen und Speicherstatistiken zur Anwenderpartition (überlagerndes Dateisystem) abrufen.
- Die Partition kann sich auf der externen Yaskawa SD-Karte oder auf dem internen Speicher befinden.
- Der Speicher ist in Blöcken organisiert.
- Ein Block hat eine konstante, festgelegte Größe und eine Datei belegt immer einen oder mehrere Blöcke.
- Eine bestimmte Anzahl an Blöcken ist im Linux-System für den Root-Benutzer reserviert. Diese reservierten Blöcke sind ausschließlich für den Root-Benutzer verfügbar und sichern dessen Handlungsfähigkeit auch bei belegtem Speicher (z.B. für Log-Ausgaben).

Systemvariable	Typ - Beschreibung
USER_PARTITION	PARTITION_INFO - Datenstruktur
MEM_TOTAL	ULINT - Gesamtspeicher der Partition in Bytes (inklusive reservierter Blöcke).
MEM_FREE	ULINT - freier, zur Verfügung stehender Speicher in Bytes (ohne reservierte Blöcke).
MEM_USED	ULINT - belegter Speicher in Bytes (inklusive reservierter Blöcke).
MEM_USAGE	ULINT - genutzter Speicher in % (ohne reservierte Blöcke).

Task-Handling

- Programme und Programmteile werden in iCube Engineer als Tasks behandelt.
- Die Koordination und Abarbeitung der einzelnen Tasks übernimmt der **Execution & Synchronization Manager (ESM)**.
- Mit der Systemvariable ESM_DATA können Sie Informationen über das Task-Handling des ESM abrufen.
- ESM_DATA ist eine als Datenstruktur organisierte Systemvariable.

Systemvariable	Typ - Beschreibung
ESM_DATA	ESM_DAT - Datenstruktur
ESM_COUNT	USINT - Anzahl der ESM (jeweils ein ESM pro Prozessorkern).
ESM_INFOS	ESM_INFO_ARRAY
[1] ... [2]	ESM_INFO - Informationen zu den ESM [1 ... 2] ² .
TASK_COUNT	UINT - Anzahl der Tasks, die für den ESM projektiert wurden.
TICK_COUNT	UDINT - immer 0.
TICK_INTERVAL	UDINT - immer 0.
TASK_INFOS	TASK_INFO_ARRAY
[1] ... [16]	TASK_INFO - Informationen zu den Tasks [1 ... 16].
INTERVAL ¹	LINT - Zeitintervall <ul style="list-style-type: none"> ■ Bei zyklischen Tasks: Zeitintervall in µs ■ Bei azyklischen Tasks: 0
PRIORITY ¹	INT - Priorität der Task

Systemvariable	Typ - Beschreibung
WATCHDOG ¹	LINT - Watchdog-Zeit in μs (0 = kein Watchdog). <ul style="list-style-type: none"> Watchdog-Zeit, die Sie für die Summe aus Ausführungsdauer und Verzögerungszeit definieren. Wird die Watchdog-Zeit überschritten, löst der Watchdog aus.
LAST_EXEC_DURATION	LINT - Ausführungsdauer der Task im vorigen Zyklus in μs . <ul style="list-style-type: none"> Dies schließt auch Unterbrechungen durch höherpriorie Tasks ein.
MIN_EXEC_DURATION	LINT - Minimale Ausführungsdauer der Task in μs . <ul style="list-style-type: none"> Dies schließt auch Unterbrechungen durch höherpriorie Tasks ein.
MAX_EXEC_DURATION	LINT - Maximale Ausführungsdauer der Task in μs . <ul style="list-style-type: none"> Dies schließt auch Unterbrechungen durch höherpriorie Tasks ein.
LAST_ACTIVATION_DELAY	LINT - Verzögerungszeit der Task im vorigen Zyklus in μs . <ul style="list-style-type: none"> Eine Verzögerung entsteht, wenn zum Zeitpunkt der Task-Aktivierung höherpriorie Tasks anstehen.
MIN_ACTIVATION_DELAY	LINT - Minimale Verzögerungszeit der Task in μs . <ul style="list-style-type: none"> Eine Verzögerung entsteht, wenn zum Zeitpunkt der Task-Aktivierung höherpriorie Tasks anstehen.
MAX_ACTIVATION_DELAY	LINT - Maximale Verzögerungszeit der Task in μs . <ul style="list-style-type: none"> Eine Verzögerung entsteht, wenn zum Zeitpunkt der Task-Aktivierung höherpriorie Tasks anstehen.
EXEC_TIME_THRESHOLD ¹	LINT - Schwellwert, den Sie für die Summe aus Ausführungsdauer und Verzögerungszeit definieren können.
EXEC_TIME_THRESHOLD_CNT	UDINT - Wenn der definierte Schwellwert EXEC_TIME_THRESHOLD überschritten wird, wird der Wert der Variable EXEC_TIME_THRESHOLD_CNT inkrementiert.
NAME ¹	STRING - Name der Task.
EXCEPTION_COUNT	USINT - Anzahl der Ausnahmen.
EXCEPTION_INFOS	ESM_EXCEPTION_INFO_ARRAY
[1] ... [2]	ESM_EXCEPTION_INFO - Informationen zu den Ausnahmen [1 ... 2] ² .
TYPE_ID	UDINT - ID der Ausnahme.
SUB_TYPE	STRING512 - Typ der Ausnahme.
SUB_TYPE_ID	UDINT - ID der Task, in der die Ausnahme aufgetreten ist.
TASK_NAME	STRING - Name der Task, in der die Ausnahme aufgetreten ist.
PROGRAM_NAME	STRING512 - Name der Programminstanz, in der die Ausnahme aufgetreten ist.
INFORMATION	STRING512 - Informationen zur aufgetretenen Ausnahme.

1) Sie können die Systemvariable in der Software iCube Engineer im Editor Tasks und Events einstellen.

2) Bitte beachten Sie, dass manche CPUs nur ESM1 unterstützen. ➔ ["Technische Daten"...Seite 70](#)

SliceBus Systemvariablen



- Bitte beachten Sie, dass die System SLIO Power- und Klemmen-Module keine Typ-Kennung besitzen. Diese können nicht erkannt werden und werden somit bei der Auflistung bzw. Zuordnung der Steckplätze nicht berücksichtigt.
- Die Zählung der Steckplätze beginnt bei 1, d.h. der 1. Steckplatz entspricht Bit 0 im entsprechenden Diagnose-Register.
- Ein Diagnosealarm wird nicht automatisch quittiert. Die Quittierung erfolgt durch Lesen der Diagnose. Solange ein Diagnosealarm nicht quittiert ist, wird auf diesem Steckplatz kein weiterer Diagnosealarm ausgegeben.

Behandlung von Diagnosealarmen

- Sobald ein Modul über den Rückwandbus einen Diagnosealarm meldet, wird dieser von der CPU automatisch erkannt und das dem Steckplatz entsprechende Register-Bit in `SB_DIAG_ALARM_STATUS` gesetzt.
- Für das Modul muss im iCube Engineer der Diagnosealarm aktiviert sein.
- Durch Lesen von Datensatz 0x00 (Diagnose) bzw. 0x01 (erweiterte Diagnose) vom entsprechenden Steckplatz können Sie eine Diagnosemeldung quittieren. Informationen zum Aufbau der Diagnose-Datensätze finden Sie im Handbuch zum entsprechenden System SLIO Modul.
- In iCube Engineer können Sie mit dem Baustein `Y_SB_DataRecordRead` aus der Systembibliothek den entsprechenden Datensatz lesen. Hierzu müssen Sie zuvor Ihrem Projekt die Systembibliothek "`Y_SliceBus.pcwlx`" hinzufügen.

Systemvariable	Typ - Beschreibung
SB_DATA_VALID	BOOL - Busaktivität <ul style="list-style-type: none"> ■ Diese Variable ist gesetzt, wenn der Datentransfer über den <i>SliceBus</i> aktiv ist.
SB_TOPOLOGY_OK	BOOL - Bus-Topologie <ul style="list-style-type: none"> ■ Diese Variable ist gesetzt, wenn die gesteckten Module am <i>SliceBus</i> mit der Konfiguration übereinstimmen.
SB_DIAG_ALARM_STATUS	ULINT - Diagnose-Status der Module <ul style="list-style-type: none"> ■ Sobald ein Modul am <i>SliceBus</i> einen Diagnosealarm meldet, wird zur entsprechenden Steckplatzposition das zugehörige Bit im 64Bit großen Register gesetzt.
SB_DIAG_ALARM_ACK_PENDING	ULINT - Quittierung Diagnose-Status der Module <ul style="list-style-type: none"> ■ Sobald ein Modul am <i>SliceBus</i> eine Quittierung des Diagnosealarms anfordert, wird zur entsprechenden Steckplatzposition das zugehörige Bit im 64Bit großen Register gesetzt.

EtherCAT-Systemvariablen

Nachfolgend sind die Systemvariablen zur Diagnose des EtherCAT-Master und der ange-bundenen EtherCAT-Slaves aufgeführt.

Systemvariable	Beschreibung
EC_MASTER_STATE	BYTE - Master-Zustand <ul style="list-style-type: none"> ■ Gibt den Zustand des EtherCAT-Master zurück: <ul style="list-style-type: none"> - 00h: Der Zustand ist unbekannt - 01h: INIT - 02h: PreOP - 04h: SafeOp - 08h: OP

Systemvariablen und Zustandsinformationen > Systemvariablen

Systemvariable	Beschreibung
EC_MASTER_LINK_CONNECTED	BOOL - physikalische Verbindung <ul style="list-style-type: none"> ■ Gesetzt, wenn ein Ethernet-Kabel am EtherCAT-Master angeschlossen ist.
EC_TOPOLOGY_OK	BOOL - Topologie OK <ul style="list-style-type: none"> ■ Gesetzt, wenn aktuelle Topologie und konfigurierte Topologie übereinstimmen.
EC_DC_IN_SYNC	BOOL - verteilte Uhren <ul style="list-style-type: none"> ■ Gesetzt wenn die verteilten Uhren synchronisiert sind.
EC_CYCLIC_LOST_FRAMES	DWORD - fehlende Frames (zyklisch) <ul style="list-style-type: none"> ■ Gibt die Anzahl der während der zyklischen Kommunikation verlorenen Frames zurück.
EC_ACYCLIC_LOST_FRAMES	DWORD - fehlende Frames (azyklisch) <ul style="list-style-type: none"> ■ Gibt die Anzahl der während der azyklischen Kommunikation verlorenen Frames zurück.
EC_NUM_CONFIGURED_SLAVES	WORD - konfigurierte Slaveanzahl <ul style="list-style-type: none"> ■ Gibt die Anzahl der konfigurierten EtherCAT-Slaves zurück.
EC_NUM_AVAILABLE_SLAVES	WORD - Slaveanzahl im Netzwerk <ul style="list-style-type: none"> ■ Gibt die Anzahl der EtherCAT-Slaves zurück, welche bei der Suche im EtherCAT-Netzwerk gefunden wurden.
EC_SLAVES_IN_MASTER_STATE	BOOL - EtherCAT-Slaves im Master-Zustand <ul style="list-style-type: none"> ■ Gesetzt, wenn alle am EtherCAT-Master befindlichen EtherCAT-Slaves den Zustand des EtherCAT-Master haben.
EC_SLAVE_STATION_ADDRESS	ARRAY[0...512] OF WORD ¹⁾ - Slave-Adressen <ul style="list-style-type: none"> ■ Gibt alle Adressen der an den EtherCAT-Master angebundenen EtherCAT-Slaves zurück.
EC_SLAVE_STATE	ARRAY[0...512] OF BYTE ¹⁾ - Slave-Zustände <ul style="list-style-type: none"> ■ Gibt die Zustände der an den EtherCAT-Master angebundenen EtherCAT-Slaves zurück: <ul style="list-style-type: none"> - 00h: Unknown - der Zustand ist unbekannt - 01h: INIT - 02h: PreOP - 03: Bootstrap - 04h: SafeOp - 08h: OP
EC_SLAVE_LAST_AL_STATUS_CODE	ARRAY[0...512] OF WORD ¹⁾ - Slave AL Status Codes <ul style="list-style-type: none"> ■ Gibt den zuletzt gelesenen AL Status Code der an den EtherCAT-Master angebundenen EtherCAT-Slaves zurück.

1) Index 0 ist reserviert. Der 1. EtherCAT-Slave ist dem Index 1 zugeordnet.

PROFINET Systemvariablen
optional

Bitte beachten Sie, dass für den Einsatz von PROFINET eine gesonderte Lizenz erforderlich ist, welche entsprechend zu aktivieren ist!

PROFINET-Systemvariablen - PROFINET-Controller-Funktionalität

Systemvariable	Typ - Beschreibung
PNIO_SYSTEM_BF	<p>BOOL - Fehlende Verbindung zu einem projektierten PROFINET-Device.</p> <ul style="list-style-type: none"> Im PROFINET-Netzwerk ist ein Fehler aufgetreten, d.h. zu mindestens einem projektierten PROFINET-Device konnte keine Verbindung aufgebaut werden. Dieser Wert wird nicht gesetzt, wenn bei einem PROFINET-Device der Parameter "BF ansteuern" auf FALSE gesetzt wurde. Das PROFINET-Device wurde damit aus der Verbindungsüberwachung herausgenommen.
PNIO_SYSTEM_SF	<p>BOOL - Diagnosealarm auf einem projektierten PROFINET-Device.</p> <ul style="list-style-type: none"> Mindestens ein PROFINET-Device meldet einen Systemfehler als Diagnosealarm oder Maintenance-Alarm. Die Fehlerpriorität kann den Variablen PNIO_DIAG_AVAILABLE, PNIO_MAINTENANCE_DEMANDED und PNIO_MAINTENANCE_REQUIRED entnommen werden.
PNIO_MAINTENANCE_DEMANDED	<p>BOOL - Wartungsanforderung</p> <ul style="list-style-type: none"> Mindestens ein PROFINET-Device meldet bei aktiver Verbindung eine "Wartungsanforderung" - Maintenance-Alarm mit hoher Priorität. Mit Hilfe des Diagnosebausteins RALRM kann das PROFINET-Device identifiziert werden.
PNIO_MAINTENANCE_REQUIRED	<p>BOOL - Wartungsbedarf</p> <ul style="list-style-type: none"> Mindestens ein PROFINET-Device meldet bei aktiver Verbindung einen "Wartungsbedarf" - Maintenance-Alarm mit niedriger Priorität. <p>Mit Hilfe des Diagnosebausteins RALRM kann das PROFINET-Device identifiziert werden.</p>
PNIO_FORCE_FAILSAFE	<p>BOOL - Alle PROFINET-Devices werden zum Setzen ihrer projektierten Ersatzwerte aufgefordert.</p> <ul style="list-style-type: none"> Die Systemvariable kann bei Bedarf aus dem Programm beschrieben/gesetzt werden.
PNIO_CONFIG_STATUS	<p>WORD - Konfigurationsstatus des PROFINET-Controllers.</p>
PNIO_CONFIG_STATUS_READY	<p>BOOL - PROFINET-Controller initialisiert.</p> <ul style="list-style-type: none"> Diese Variable ist gesetzt, wenn der PROFINET-Controller fehlerfrei initialisiert werden konnte. Es ist noch keine Sollkonfiguration von iCube Engineer geladen worden.
PNIO_CONFIG_STATUS_ACTIVE	<p>BOOL - Sollkonfiguration geladen.</p> <ul style="list-style-type: none"> Diese Variable ist gesetzt, wenn eine Sollkonfiguration zum PROFINET-Controller geladen wurde. In diesem Zustand versucht der PROFINET-Controller, zyklisch zu allen Geräten der Sollkonfiguration eine Verbindung aufzubauen.

Systemvariable	Typ - Beschreibung
PNIO_CONFIG_STATUS_CFG_FAULT	<p>BOOL - Fehler Sollkonfiguration.</p> <ul style="list-style-type: none"> Die Sollkonfiguration des PROFINET-Controllers wurde aufgrund eines schwerwiegenden Fehlers nicht übernommen. Kontaktieren Sie bitte unseren Support!
PNIO_FORCE_PRIMARY	<p>BOOL - Diese Variable wird von Funktionsbausteinen für applikative Redundanz genutzt um die SRL-Rolle des PROFINET-Controllers vorzugeben.</p>

PROFINET-Systemvariablen - PROFINET-Device-Funktionalität

Systemvariable	Typ - Beschreibung
PND_S1_PLC_RUN	<p>BOOL - Status des überlagerten PROFINET-Controllers.</p> <ul style="list-style-type: none"> Information, ob der überlagerte PROFINET-Controller aktiv ist. Der Wert ist TRUE, wenn sich der überlagerte PROFINET-Controller im Zustand RUN befindet und das Programm abgearbeitet wird. Die Anzeige ist nur bei bestehender PROFINET-Verbindung gültig (PND_S1_VALID_DATA_CYCLE).
PND_S1_VALID_DATA_CYCLE	<p>BOOL - Überlagerter PROFINET-Controller hat die Verbindung aufgebaut.</p> <ul style="list-style-type: none"> Information, ob eine Verbindung besteht und zyklische Daten zwischen PROFINET-Controller und PROFINET-Device ausgetauscht werden und der zuletzt empfangene Frame gültige Daten enthielt.
PND_S1_OUTPUT_STATUS_GOOD	<p>BOOL - IOP-Status des überlagerten PROFINET-Controllers.</p> <ul style="list-style-type: none"> Information, ob das PROFINET-Device die Eingangsprozessdaten (PND_S1_INPUTS) mit dem Status "gültig" empfangen hat. Der Wert ist TRUE, wenn die Ausgangsdaten des überlagerten PROFINET-Controllers gültig sind (Provider-Status).
PND_S1_INPUT_STATUS_GOOD	<p>BOOL - IOC-Status des überlagerten PROFINET-Controllers.</p>
PND_S1_DATA_LENGTH	<p>WORD - Prozessdatenlänge, die für das PROFINET-Device konfiguriert wurde.</p>
PND_S1_OUTPUTS	<p>PND_IO_512 - Ausgangsprozessdaten</p> <ul style="list-style-type: none"> Speicherbereich für Ausgangsprozessdaten, die das PROFINET-Device zum überlagerten PROFINET-Controller sendet.
PND_S1_INPUTS	<p>PND_IO_512 - Eingangsprozessdaten</p> <ul style="list-style-type: none"> Speicherbereich für Eingangsprozessdaten, die das PROFINET-Device von dem überlagerten PROFINET-Controller empfängt.
PND_IO_DRIVEN_BYPLC	<p>INT - Applikative Systemredundanz</p> <ul style="list-style-type: none"> Nummer des aktuell mit dem PROFINET-Device verbundenen PROFINET-Controllers. Angabe, von welchem überlagerten PROFINET-Controller die Daten im PROFINET-Device stammen: <ul style="list-style-type: none"> 0: Kein PROFINET-Controller 1: PROFINET-Controller A 2: PROFINET-Controller B

5.15.3 FSoE-Systemvariablen

Systemvariable SPLC

- Die Systemvariable SPLC ist eine als Datenstruktur organisierte Systemvariable.
- Die Systemvariable SPLC stellt mit Hilfe der Datenstruktur SPNSV2_TYPE folgende Informationen zur Safety-CPU zur Verfügung.

Systemvariable	Typ - Beschreibung
SPLC	SPNSV2_TYPE - Datenstruktur
PRJ	
Name	STRING - Name des iCube Engineer-Projekts.
CRC	DWORD - Projekt-CRC (32-Bit) des Safety-CPU Boot-Projekts.
EXEC_TIME	UDINT - Laufzeit des Safety-CPU Programm-Zyklus in µs.
HAS_PRJ	BOOL - Gesetzt wenn sicherheitsbezogenes Anwendungsprogramm und Programmquellen im Speicher der Safety-CPU vorhanden sind.
DIAG	
STATUS_REG	WORD - Diagnose-Statusregister der Safety-CPU. <ul style="list-style-type: none"> ■ Enthält die Statusinformationen der Safety-CPU. Es spiegelt zu jeder Zeit den Zustand der Safety-CPU inklusive eventuell aufgetretener Fehlerzustände der Safety-CPU wider. ■ Zusatzinformationen und Fehlerparameter, insbesondere im Zustand Fail Safe, sind in den zugehörigen Diagnose-Parameterregistern der Safety-CPU (Elemente SPNS.DIAG.PARAM_REG und SPNS.DIAG.PARAM_2_REG) enthalten. → <i>"Diagnose-Statusregister SPLC.DIAG.STATUS_REG.xxx"...</i> Seite 172
PARAM_REG	WORD - Diagnose-Parameterregister 1 der Safety-CPU (Fehlercode).
PARAM_2_REG	WORD - Diagnose-Parameterregister 2 der Safety-CPU (ergänzende Fehlermeldungen für Service/Support).
EXT_PARAM_REG	DWORD - Erweitertes Diagnose-Parameterregister der Safety-CPU (ergänzende Fehlermeldungen für Service/Support).
CH2_PARAM_REG	WORD - Diagnose-Parameterregister 1 der Safety-CPU Kanal 2 (CH2) (Fehlercode).
CH2_PARAM_2_REG	WORD - Diagnose-Parameterregister 2 der Safety-CPU Kanal 2 (CH2) (ergänzende Fehlermeldungen für Service/Support).
CH2_EXT_PARAM_REG	DWORD - Erweitertes Diagnose-Parameterregister der Safety-CPU Kanal 2 (CH2) (ergänzende Fehlermeldungen für Service/Support).
INFO	
CYCLE_TIME	UDINT - Safety-CPU-Zyklus in µs.
TEMP	
TEMP_CURRENT	INT - Aktuell gemessene Temperatur der Safety-CPU.
TEMP_MIN	INT - Minimale gemessene Temperatur der Safety-CPU seit dem letzten NetzEIN des Geräts.
TEMP_MAX	INT - Maximale gemessene Temperatur der Safety-CPU seit dem letzten NetzEIN des Geräts.

Systemvariable	Typ - Beschreibung
STATUS_REG	WORD - Safety-CPU Temperatur-Statusregister. <ul style="list-style-type: none"> 0x0000: Die Temperatur der Safety-CPU ist im unkritischen Bereich. 0x0080: Die Temperatur der Safety-CPU ist im kritischen Bereich nahe der Toleranzgrenze. Die CPU bleibt im Zustand RUN und gibt parallel eine Warnung mit dem Fehlercode 0xFA41 aus. 0x8000: Die Temperatur der Safety-CPU ist über dem zulässigen Bereich. Die Safety-CPU wechselt in den sicheren Zustand und gibt parallel einen Fehler mit dem Fehlercode 0x924D aus.
CPU	
LOAD_CURRENT	INT - Aktuelle CPU-Auslastung der Safety-CPU.
LOAD_MIN	INT - Minimale CPU-Auslastung der Safety-CPU seit dem letzten NetZEIN des Geräts.
LOAD_MAX	INT - Maximale CPU-Auslastung der Safety-CPU seit dem letzten NetZEIN des Geräts.
STATUS_REG	WORD - CPU-Statusregister der Safety-CPU.
FW_VERSION	
VERSION_MAJOR	BYTE - Hauptversion der Safety-CPU Firmware (Major-Version).
VERSION_MINOR	BYTE - Nebenversion der Safety-CPU Firmware (Minor-Version).
VERSION_BUILD	WORD - Build-Nummer der Safety-CPU Firmware.
FPGA_VERSION	
VERSION_MAJOR	BYTE - Hauptversion des Safety-CPU Hardware-FPGAs (Major-Version).
VERSION_MINOR	BYTE - Nebenversion des Safety-CPU Hardware-FPGAs (Minor-Version).
VERSION_BUILD	WORD - Build-Nummer des Safety-CPU Hardware-FPGAs.
FW_UPDATE_STATUS	UINT - Status des sicherheitsbezogenen Firmware-Updates.
SOFT_RESET_REG	WORD - Software-Reset-Register der Safety-CPU.

**HINWEIS**

Der Warnschwellwert der CPU-Auslastung beträgt 70%, der Abschaltswellwert 90%. Bei Überschreiten der 90% CPU-Auslastung schaltet die Safety-CPU ab.

Systemvariablen und Zustandsinformationen > FSoE-Systemvariablen

**Diagnose-Statusregister
SPLC.DIAG.STATUS_REG.
xxx**

- Die folgende Tabelle beschreibt die Informationen der einzelnen Bits (0 ... 15) im Diagnose-Statusregister (SPLC.DIAG.STATUS_REG.xxx).

Systemvariable/Elemente		Typ - Beschreibung
SPLC		SPNSV2_TYPE - Datenstruktur
DIAG		
STATUS_REG		
	DBG ²	BOOL - Nicht sicherer Debug-Betrieb der Safety-CPU. <ul style="list-style-type: none"> Die Safety-CPU befindet sich in einem der beiden DEBUG-Zustände (DEBUG-RUN oder DEBUG-STOP/DEBUG-HALT).
	EST	BOOL - Ein Eintrag im Fehlerspeicher des sicheren Betriebssystems (Error-Stack) der Safety-CPU liegt vor. Diagnose- und Fehlermeldungen vom sicheren Betriebssystem der Safety-CPU liegen vor. <ul style="list-style-type: none"> Diese Meldungen können durch iCube Engineer ausgelesen und ausgewertet werden. Die Variable hat immer dann den Wert TRUE, wenn mindestens ein Eintrag im Fehlerspeicher des sicheren Betriebssystems enthalten ist. Sobald der Fehlerspeicher über iCube Engineer ausgelesen und dadurch geleert wurde, wechselt der Wert der Variable auf FALSE.
	FS	BOOL - Failure State der Safety-CPU. <ul style="list-style-type: none"> Ein Fehler wurde erkannt, der die Safety-CPU in den Zustand Fail Safe versetzt. → "Fail Safe Zustände" ... Seite 133 Der zugehörige, weitergehende Fehler-Code ist in diesem Zustand in den Diagnose-Parameterregistern der Safety-CPU (SPLC.DIAG.PARAM_REG und SPLC.DIAG.PARAM_2_REG) enthalten.
	INIT ¹	BOOL - Initialisierung der Safety-CPU. <ul style="list-style-type: none"> Die Initialisierung der Safety-CPU Firmware (sicheres Betriebssystem) wurde fehlerfrei durchlaufen und ist abgeschlossen.
	IO ¹	BOOL - Initialisierung des Safety I/O-Kanal-Kommunikation. <ul style="list-style-type: none"> Die Initialisierung der FSoE-Kommunikation zu den I/O-Geräten wurde fehlerfrei abgeschlossen.
	PON ¹	BOOL - NetzEIN-Vorgang. <ul style="list-style-type: none"> Die Safety-CPU ist mit Spannung versorgt. Die Firmware wurde in den RAM-Speicher der Safety-CPU geladen und ist hochgelaufen. Die Selbsttest-Routinen der Safety-CPU wurden fehlerfrei abgeschlossen.
	POST	BOOL - NetzEIN-Selbsttest der Safety-CPU (POWER ON SELF TEST). <ul style="list-style-type: none"> Selbsttest der Safety-CPU nach NetzEIN aktiv.
	PRO ¹	BOOL - Laden und Starten des sicherheitsbezogenen Anwendungsprogramms. <ul style="list-style-type: none"> Das mit iCube Engineer erstellte sicherheitsbezogene Anwendungsprogramm wurde fehlerfrei in das sichere Betriebssystem der Safety-CPU geladen und gestartet.

Systemvariable/Elemente			Typ - Beschreibung
		RUN ²	BOOL - Ausführung des sicherheitsbezogenen Anwendungsprogramms (RUN). <ul style="list-style-type: none"> Die Safety-CPU führt das sicherheitsbezogene Anwendungsprogramm aus und befindet sich in einem der beiden RUN-Zustände (SAFE-RUN oder DEBUG-RUN).
		SYN ¹	BOOL - Synchronisierung Safety- und Standard-Komponenten innerhalb der Safety-CPU. <ul style="list-style-type: none"> Die Synchronisierung der Safety- und Standard-Komponenten innerhalb der Safety-CPU wurde erfolgreich durchgeführt.
		WARN	BOOL - Warnung der Safety-CPU. <ul style="list-style-type: none"> Eine Sammel-Warnungsmeldung der Safety-CPU liegt vor.

- 1) Die Variablen geben den Anlaufstatus der Safety-CPU wieder. Die Anlaufsequenz hat folgenden Ablauf:
 - NetzeIN-Vorgang
 - Initialisierung der Safety-CPU.
 - Laden und Starten des sicherheitsbezogenen Anwendungsprogramms.
 - Synchronisierung von Safety- und Standard-Komponenten innerhalb der Safety-CPU.
 - Initialisierung Safety I/O-Kanal-Kommunikation.
- 2) Die Variablen zeigen die Betriebszustände RUN und DEBUG Safety-CPU an.

Bedeutung der Bits

Das Diagnose-Statusregister SPLC.DIAG.STATUS_REG enthält die Statusinformationen der Safety-CPU. Es spiegelt zu jeder Zeit den Zustand der Safety-CPU inklusive eventuell aufgetretener Fehlerzustände der Safety-CPU wider. Zusatzinformationen und Fehlerparameter, insbesondere im Zustand Fail Safe (FS), sind in den zugehörigen Diagnose-Parameterregistern der Safety-CPU (SPLC.DIAG.PARAM_REG und SPLC.DIAG.PARAM_2_REG) und im erweiterten Diagnose-Parameterregister (SPLC.DIAG.EXT_PARAM_REG) enthalten.

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
FS	POST	res.	EST	res.	res.	res.	res.	WARN	DBG	RUN	I/O	SYN	PRO	INIT	PON

- Bit 4 ... 0: Anlaufstatus der Safety-CPU:
 - PON - Power-ON-Vorgang abgeschlossen.
Dieses Bit wird gesetzt, sobald die Safety-CPU mit Spannung versorgt ist. Die Firmware wurde in den RAM-Speicher der Safety-CPU geladen und ist hochgelaufen. Die Selbsttest-Routinen der Safety-CPU sind erfolgreich abgeschlossen.
 - INIT - Initialisierung der Safety-CPU abgeschlossen.
Dieses Bit wird gesetzt, sobald die Initialisierung der Safety-CPU Firmware (sicheres Betriebssystem) fehlerfrei durchlaufen wurde und abgeschlossen ist.
 - PRO - Sicherheitsbezogenes Anwenderprogramm geladen und gestartet.
Dieses Bit wird gesetzt, sobald das sicherheitsbezogene Anwenderprogramm, welches mit iCube Engineer erstellt wurde, fehlerfrei in das sichere Betriebssystem der Safety-CPU geladen und gestartet wurde.
 - SYN - Synchronisierung von Safety- und Standard_Komponenten der Safety-CPU.
Das Bit wird gesetzt, wenn Safety- und Standard-Komponenten der Safety-CPU synchronisiert sind.
 - I/O - I/O-Channel-Kommunikation initialisiert.
Dieses Bit wird gesetzt, sobald die Initialisierung der Safety I/O-Kanal-Kommunikation fehlerfrei abgeschlossen ist.
- Bit 6, 5: Betriebsstatus der Safety-CPU:
 - RUN - RUN-Betrieb der Safety-CPU.

Systemvariablen und Zustandsinformationen > FSoE-Systemvariablen

Dieses Bit ist gesetzt, wenn die Safety-CPU das sicherheitsbezogene Anwenderprogramm ausführt und sich in einem der beiden RUN-Zustände (SAFE-RUN oder DEBUG-RUN) befindet.

- DBG - Nicht sicherer Debug-Betrieb der Safety-CPU.

Dieses Bit ist gesetzt, wenn sich die Safety-CPU in einem der beiden DEBUG-Zustände (DEBUG-RUN oder DEBUG-STOP/DEBUG-HALT) befindet. In den Zuständen SAFE-STOP und SAFE-RUN ist dieses Bit nicht gesetzt.

- Bit 7: Warnung
 - WARN - Das gesetzte Bit WARN (WARNING) zeigt eine Sammel-Warnungsmeldung der Safety-CPU an.
- Bit 11 ... 8: reserviert
- Bit 12: Error-Stack
 - EST - Das Bit EST (Error-Stack) zeigt an, dass Diagnose- und Fehlermeldungen vom sicheren Betriebssystem der Safety-CPU vorliegen.
Dieses Bit ist gesetzt, wenn mindestens ein Eintrag im Fehlerspeicher des sicheren Betriebssystems enthalten ist. Diese Meldungen können durch iCube Engineer ausgelesen und ausgewertet werden. Sobald der Fehlerspeicher über iCube Engineer ausgelesen und dadurch geleert wurde, wird dieses Bit automatisch zurückgesetzt.
- Bit 13: reserviert
- Bit 14: POST
 - POST - POWER ON SELF TEST
Dieses Bit ist für die Dauer des **Power-ON-SelbstTests** der Safety-CPU gesetzt. Nach Abschluss des Selbsttests wird dieses zurückgesetzt.
- Bit 15: Fail Safe Zustand
 - FS - Failure State
Dieses Bit wird gesetzt, sobald ein Fehler erkannt wurde, welcher die Safety-CPU in den Zustand *Fail Safe* versetzt. → "[Fail Safe Zustände](#)"...Seite 133
Der zugehörige weiterführende Fehler-Code ist in diesem Zustand in den Diagnose-Parameterregistern der Safety-CPU (SPLC.DIAG.PARAM_REG und SPLC.DIAG.PARAM_2_REG) enthalten.

Systemvariablen SPLC_CONTROL_COMMAND und SPLC_CONTROL_CONFIRM

- Mit der Systemvariablen SPLC_CONTROL_COMMAND wird aus dem nicht sicherheitsbezogenen Projekt das Zurücksetzen von Diagnosewerten angefordert.
- Über die Systemvariable SPLC_CONTROL_CONFIRM bestätigt die Safety-CPU im nicht sicherheitsbezogenen Projekt, dass die Diagnosewerte zurückgesetzt wurden.

SPLC_CONTROL_COMMAND

Systemvariable	Typ - Beschreibung
SPLC_CONTROL_COMMAND	SPLC_CONTROL_TYPE - Datenstruktur mit 32 Bits zum Aktivieren von Funktionen der Safety-CPU.
CODE	<ul style="list-style-type: none"> ■ DWORD - Bit 0: Anforderung Zurücksetzen der minimalen und maximalen Safety-Roundtrip-Zeiten (SRT_MIN, SRT_MAX). <ul style="list-style-type: none"> - Datenrichtung innerhalb der Safety-CPU: Standard-Komponente → Safety-Komponente
PARAM	<ul style="list-style-type: none"> ■ DWORD - Bit 31 ... 1: Reserviert

SPLC_CONTROL_CONFIRM

Systemvariable	Typ - Beschreibung
SPLC_CONTROL_CONFIRM	SPLC_CONTROL_TYPE - Datenstruktur mit 32 Bits zum Bestätigen von Funktionen der Safety-CPU, die über die Variable SPLC_CONTROL_COMMAND angefordert wurden.

Systemvariable	Typ - Beschreibung
CODE	<ul style="list-style-type: none"> ■ DWORD - Bit 0: Bestätigung Rücksetzen der minimalen und maximalen Safety-Roundtrip-Zeiten (SRT_MIN, SRT_MAX). <ul style="list-style-type: none"> - Datenrichtung innerhalb der Safety-CPU: Safety-Komponente → Standard-Komponente
PARAM	<ul style="list-style-type: none"> ■ DWORD - Bit 31 ... 1: Reserviert

Systemvariablen FDEV_INx und FDEV_OUTx (x = 0 ... 7)

Diese Systemvariablen werden für den Datenaustausch zwischen der Standard- und der Safety-Komponente der Safety-CPU verwendet.

- Die Systemvariablen FDEV_IN0 bis FDEV_IN7 beinhalten die Eingangsprozessdaten (8 * 1 Byte) der Safety-Komponente der Safety-CPU.
- Die Systemvariablen FDEV_OUT0 bis FDEV_OUT7 beinhalten die Ausgangsprozessdaten (8 * 1 Byte) der Safety-Komponente der Safety-CPU.

Datenrichtung:

- FDEV_INx = I
- FDEV_OUTx = Q

FDEV_INx und FDEV_OUTx (x = 0 ... 7)

Systemvariable	Typ - Beschreibung
FDEV_IN0 ... FDEV_IN7	SAFEBYTE - Eingangsprozessdaten der Safety-Komponente der Safety-CPU.
FDEV_OUT0 ... FDEV_OUT7	SAFEBYTE - Ausgangsprozessdaten der Safety-Komponente der Safety-CPU.

5.15.4 FSoE-Diagnosevariablen

Allgemein

Für jede FSoE-Master-Verbindung werden Statusinformationen in den SafeOS Diag IN (DI) Bereich geliefert. Die FSoE-Master-Verbindung kann durch den SafeOS Diag OUT (DQ) Bereich gesteuert werden. Es gibt verbindungs-spezifische Diagnosevariablen pro FSoE-Verbindung und globale Diagnosevariablen. In der folgenden Tabelle werden die verbindungs-spezifische Diagnosevariablen pro FSoE-Verbindung aufgeführt. Der Platzhalter xxxxx steht für die jeweilige projektierte FSoE-Adresse.

FSoE-verbindingsspezifische Diagnosevariablen

Variablenname	Datenrichtung
FSOE_MSTR_ADDR_xxxxx_ACK_REQ	DI
Acknowledge Request	
<ul style="list-style-type: none"> ■ 1: Variable wird auf 1 gesetzt, wenn ein vorher aufgetretener FSoE-Kommunikationsfehler behoben ist und quittiert werden kann. Dies wird durch einen Flankenwechsel in <code>SAPL_DataValidChangedClbk()</code> von <i>FailSafeData</i> auf <i>ProcessData</i> erkannt. Solange Variable = 1, <ul style="list-style-type: none"> – werden Fail Safe Werte in das SafeOS Prozessabbild der Eingänge für diese Kommunikationsinstanz geliefert. Dies gilt auch, wenn die Kommunikationsinstanz schon vorher Prozessdaten liefert (signalisiert durch <code>SAPL_DataValidChangedClbk()</code> <i>ProcessData</i>). – wird die ausgehende PDU für die Kommunikationsinstanz über <code>SSD_IoDataCmdSet()</code> in den Fail Safe Status gesetzt. ■ 0: Variable wird auf 0 gesetzt, wenn der Acknowledge Request durch <code>FSOE_MSTR_ADDR_xxxx_ACK_REI = 1</code> bestätigt wird. Solange Variable = 0, <ul style="list-style-type: none"> – werden die <i>SafeData</i> (<i>FailSafeData</i> auf <i>ProcessData</i>) für diese Kommunikationsinstanz direkt in das SafeOS Prozessabbild Eingänge übernommen. 	
FSOE_MSTR_ADDR_xxxxx_ACK_REI	DQ
Acknowledge Reintegration	
<ul style="list-style-type: none"> ■ 1: Die Variable <code>FSOE_MSTR_ADDR_xxxx_ACK_REQ</code> auf wird 0 gesetzt. ■ 0: Keine Aktion wird ausgeführt. 	
FSOE_MSTR_ADDR_xxxxx_PASS_OUT	DI
Passivierung aktiviert eingangsseitig: Der angeschlossene FSoE-Slave sendet Fail Safe auf dieser FSoE-Verbindung.	
<ul style="list-style-type: none"> ■ 1: Die Variable wird auf 1 gesetzt, wenn <code>SAPL_DataValidChangedClbk()</code> <i>FailSafeData</i> liefert. ■ 0: Variable wird auf 0 gesetzt, wenn <code>SAPL_DataValidChangedClbk()</code> <i>ProcessData</i> liefert. 	
FSOE_MSTR_ADDR_xxxxx_PASS_ON	DQ
Passivierung aktiviert ausgangsseitig: Der FSoE-Master sendet Fail Safe auf dieser FSoE-Verbindung.	
<ul style="list-style-type: none"> ■ 1: Wenn die Variable = 1, wird die Ausgangsnachricht dieser Kommunikationsinstanz auf <i>FailSafeData</i> gesetzt. Zusätzlich wird <code>FSOE_MSTR_ADDR_xxxx_PASS_OUT = 1</code> gesetzt (Eingangsdaten auf Fail Safe). ■ 0: Wenn die Variable = 0, wird die Ausgangsnachricht dieser Kommunikationsinstanz <i>ProcessData</i> gesetzt. 	



WARNUNG

Rücksetzen von `FSOE_MSTR_ADDR_xxxxx_PASS_ON`

Das Rücksetzen dieser Variable führt zur sofortigen Übertragung der sicheren Ein- und Ausgangsdaten. Stellen Sie durch geeignete Maßnahmen sicher, dass von Ihrer Anlage/Maschine keine Gefahr ausgeht, wenn die Passivierung des F-Devices zurückgenommen wird.

Variablenname	Datenrichtung
FSOE_MSTR_ADDR_XXXXX_CE_CRC	DI
<p>CRC-Fehler eingangsseitig: Der FSoE-Master hat in der eingehenden FSoE-PDU einen CRC-Fehler erkannt.</p> <ul style="list-style-type: none"> ■ 1: Variable wird auf 1 gesetzt, wenn <code>SAPL_FsoeErrorClbk()</code> folgenden Fehler liefert: <code>FSOE_k_COMM_ERR_INV_CRC</code> ■ 0: Variable wird auf 0 gesetzt, wenn <ul style="list-style-type: none"> - <code>SAPL_DataValidChangedClbk()</code> <i>ProcessData</i> liefert. - <code>SAPL_FsoeStateChangedClbk()</code> signalisiert, dass der <i>Data state</i> verlassen wurde. 	
FSOE_MSTR_ADDR_XXXXX_WD_TIMEOUT	DI
<p>Watchdog Timeout eingangsseitig: Der FSoE-Master hat für die eingehende FSoE-PDU einen Watchdog Timeout.</p> <ul style="list-style-type: none"> ■ 1: Variable wird auf 1 gesetzt, wenn <code>SAPL_FsoeErrorClbk()</code> folgenden Fehler liefert: <code>FSOE_k_COMM_ERR_WD_EXPIRED</code>. ■ Variable wird auf 0 gesetzt, wenn <ul style="list-style-type: none"> - <code>SAPL_DataValidChangedClbk()</code> <i>ProcessData</i> liefert. - <code>SAPL_FsoeStateChangedClbk()</code> signalisiert, dass der <i>Data state</i> verlassen wurde. 	
FSOE_MSTR_ADDR_XXXXX_COMM	DI
<p>Alle weiteren wiederherstellbaren FSoE-Kommunikationsfehler:</p> <ul style="list-style-type: none"> ■ 1: Variable wird auf 1 gesetzt, wenn <code>SAPL_FsoeErrorClbk()</code> folgenden Fehler liefert: <ul style="list-style-type: none"> - <code>FSOE_K_COMM_ERR_LOCAL_RESET_OR_ACK</code> - <code>FSOE_K_COMM_ERR_INV_CMD</code> - <code>FSOE_K_COMM_ERR_UNK_CMD</code> - <code>FSOE_K_COMM_ERR_INV_CONNID</code> - <code>FSOE_K_COMM_ERR_INV_ADDRESS</code> - <code>FSOE_K_COMM_ERR_INV_DATA</code> - <code>FSOE_K_COMM_ERR_INV_COMMPARALEN</code> - <code>FSOE_K_COMM_ERR_INV_COMPARA</code> - <code>FSOE_K_COMM_ERR_INV_USRPARALEN</code> - <code>FSOE_K_COMM_ERR_INV_USRPARA</code> - <code>FSOE_K_COMM_ERR_INV_SAFEPARA_START</code> ■ 0: Variable wird auf 0 gesetzt, wenn <ul style="list-style-type: none"> - <code>SAPL_DataValidChangedClbk()</code> <i>ProcessData</i> liefert. - <code>SAPL_FsoeStateChangedClbk()</code> signalisiert, dass der <i>Data state</i> verlassen wurde. 	

Systemvariablen und Zustandsinformationen > FSoE-Diagnosevariablen

Globale Diagnosevariablen

Variablenname	Datenrichtung
ACK_REQ_FSOE_MSTR_GLOBAL	DI
Acknowledge Request: Mindestens eine FSoE-Verbindung wartet auf einen Operator-Acknowledge-Request z.B. nach einem Wechsel von Fail Safe zur Prozessdatenkommunikation. <ul style="list-style-type: none"> ■ Globales Äquivalent zu FSOE_MSTR_ADDR_xxxx_ACK_REQ. ■ Mindestens eine Kommunikationsinstanz verhält sich wie in FSOE_MSTR_ADDR_xxxx_ACK_REQ beschrieben. 	
ACK_REI_FSOE_MSTR_GLOBAL	DQ
Acknowledge Reintegration: Alle vorherigen ACK_REQ für diese FSoE-Verbindung werden bestätigt. <ul style="list-style-type: none"> ■ Globales Äquivalent zu FSOE_MSTR_ADDR_xxxx_ACK_REI. ■ Setze alle Kommunikationsinstanzen wie in FSOE_MSTR_ADDR_xxxx_ACK_REI beschrieben. ■ Wenn ein spezifisches ACK_REI gesetzt wird, darf das globale ACK_REI nicht mit aktiviert werden. 	
PASS_OUT_FSOE_MSTR_GLOBAL	DI
Passivierung aktiviert eingangsseitig: Mindestens eine FSoE-Verbindung sendet Fail Safe. <ul style="list-style-type: none"> ■ Globales Äquivalent zu FSOE_MSTR_ADDR_xxxx_PASS_OUT. ■ Mindestens eine Kommunikationsinstanz verhält sich wie in FSOE_MSTR_ADDR_xxxx_PASS_OUT beschrieben. 	
CE_CRC_FSOE_MSTR_GLOBAL	DI
CRC-Fehler eingangsseitig: Mindestens eine FSoE-Verbindung hat in der eingehenden FSoE-PDU einen CRC-Fehler erkannt. <ul style="list-style-type: none"> ■ Globales Äquivalent zu FSOE_MSTR_ADDR_xxxx_CE_CRC. ■ Mindestens eine Kommunikationsinstanz verhält sich wie in FSOE_MSTR_ADDR_xxxx_CE_CRC beschrieben. 	
WD_TIMEOUT_FSOE_MSTR_GLOBAL	DI
Watchdog Timeout eingangsseitig: Mindestens eine FSoE-Verbindung hat einen Watchdog Timeout. <ul style="list-style-type: none"> ■ Globales Äquivalent zu FSOE_MSTR_ADDR_xxxx_WD_TIMEOUT. ■ Mindestens eine Kommunikationsinstanz verhält sich wie in FSOE_MSTR_ADDR_xxxx_WD_TIMEOUT beschrieben. 	
COMM_FSOE_MATR_GLOBAL	DI
<ul style="list-style-type: none"> ■ Globales Äquivalent zu FSOE_MSTR_ADDR_xxxx_COMM. ■ Mindestens eine Kommunikationsinstanz verhält sich wie in FSOE_MSTR_ADDR_xxxx_COMM beschrieben. 	

6 Web-based Management - WBM

6.1 Übersicht und erste Schritte

Zugriff auf WBM

- Die CPU 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 CPU aufrufen.
 - Die Kommunikation zwischen PC und CPU erfolgt über ein Sicherheits-Zertifikat, welches sich auf CPU und PC befinden muss.
 - Sie können WBM nur aufrufen, wenn die CPU über eine gültige IP-Adresse verfügt.
 - Im Auslieferungszustand hat die CPU die IP-Adresse 192.168.1.1 über Ethernet-Port (X3/X4).
1. ➔ Stellen Sie für die Erstinbetriebnahme eine gesicherte Verbindung zwischen PC und CPU her, wie z.B. eine Punkt-zu-Punkt-Verbindung über Ethernet.
 2. ➔ Öffnen Sie den Webbrowser auf Ihrem PC.
 3. ➔ Über die Suche in iCube Engineer können Sie die IP-Adresse der entsprechenden Ethernet-Schnittstelle ermitteln.
Geben Sie im Adressfeld die URL ein wie z.B. https://192.168.1.1
 - ➔ Für die sichere Kommunikation verwendet der CPU-Webserver ein selbstsigniertes TLS-Zertifikat, das bei der Inbetriebnahme automatisch von der CPU generiert wird. Systembedingt erhalten Sie eine Sicherheitsmeldung bzgl. des Zertifikats, da dieses auf dem PC noch nicht installiert ist. Nach der Anmeldung können Sie das entsprechende Zertifikat von der CPU als vertrauenswürdigen Zertifikat auf Ihrem PC installieren (siehe unten). Hiermit authentifiziert sich die CPU gegenüber dem Webbrowser auf dem PC.
 4. ➔ Nehmen Sie die Sicherheitsmeldung zur Kenntnis und fahren Sie nur fort, wenn zwischen PC und CPU eine gesicherte Verbindung und kein Zugriff Dritter besteht!
 - ➔ Die Anmeldeseite von WBM wird geöffnet.

5. ➔ Geben Sie Ihre Zugangsdaten an und klicken Sie auf [Anmelden].



Im Auslieferungszustand sind folgende Zugangsdaten mit Administratorrechten voreingestellt:

- *Benutzername: admin*
- *Das Passwort befindet sich unter der Frontklappe auf die Frontseite der CPU aufgedruckt.*

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

Zertifikat installieren



Erstzugriff über TLS-Zertifikat

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

Übersicht und erste Schritte

Zur Absicherung der Kommunikation muss in PC und CPU das gleiche Sicherheits-Zertifikat installiert sein. Das von der CPU generierte Zertifikat übertragen Sie nach folgender Vorgehensweise auf Ihren PC:

1. Nach der Anmeldung im WBM können Sie über *"Konfiguration → Webdienste"* die Inhalte des automatisch generierten Zertifikats einsehen bzw. anpassen und dieses mit [Regeneriere HTTPS-Zertifikat] neu generieren. → *"Webdienste"...Seite 193*



– Sobald Sie eine der IP-Adressen der CPU ändern, müssen Sie über [Regeneriere HTTPS-Zertifikat] das Zertifikat neu generieren.

2. Navigieren Sie über *"Security → Zertifikatauthentifizierung"* zu den Zertifikaten.
3. Wechseln Sie in das Register Identity Store.
 - ➔ Hier haben Sie Zugriff auf das generierten Zertifikat.
4. Laden Sie mit  das gewünschte HTTPS-Zertifikat auf Ihren PC. Hier können Sie auch ein eigenes schon bestehendes HTTPS-Zertifikat in die CPU übertragen. → *"Zertifikatauthentifizierung"...Seite 195*
5. Installieren Sie das Zertifikat gemäß Ihrem Windows-System als vertrauenswürdige Stammzertifizierungsstelle.
 - ➔ Nach der Installation erfolgt die Kommunikation zwischen PC und CPU als *"gesicherte Verbindung"*.

**VORSICHT**

Sollte während des Betriebs die Kommunikation zwischen PC und CPU 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 PC entweder das aktuelle Zertifikat der CPU oder, falls vorhanden, ein zugehöriges übergeordnetes Zertifikat installiert ist!

Struktureller Aufbau

Das WBM gliedert sich in folgende Bereiche:

Deutsch **1** English

HW: ... FW: ... **5**
MAC: ...

YASKAWA

2 

3  Information
Allgemeine Daten

 Diagnose

 Konfiguration

 Security

 Verwalten

Information
Allgemeine Daten **4**

Allgemeine Daten	
Hersteller	Yaskawa Europe GmbH
Adresse	Hauptstr. 185, 65760 Eschborn, Germany
Internet	AMERICA: http://www.yaskawa.com EUROPE: http://www.yaskawa.eu.com
Gerätetyp	iC921...
Bestell-Nr.	PMC921...
Serien-Nr.	000000000000
Firmware-Version	9999.0 (99.0.0.26818)
Hardware-Version	00

... Rechtliche Hinweise **6**

- 1 Sprachumschaltung zwischen *"Deutsch"* und *"Englisch"*.
- 2 Frontansicht der CPU mit Typ- und Bestellbezeichnung.
- 3 Menüspalte für die Navigation.
- 4 Bereich für Informationsausgabe und Eingabe-Dialoge
- 5 Ausgabe der aktuellen Hardware-/Firmware-Version und MAC-Adresse der CPU.
- 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 CPU, z.B. Hardware- und Firmware-Versionen, Bestellnummer sowie Herstellerangaben.

The screenshot shows the 'Übersicht' (Overview) page for a YASKAWA CPU. The page title is 'Übersicht Allgemeine Daten'. On the left, there is a navigation menu with options: Übersicht, Allgemeine Daten (selected), Cockpit, Diagnose, Konfiguration, Security, and Verwalten. The main content area displays a table of general data:

Allgemeine Daten	
Hersteller	Yaskawa Europe GmbH
Adresse	Hauptstr. 185, 65760 Eschborn, Germany
Internet	AMERICA: http://www.yaskawa.com EUROPE: http://www.yaskawa.eu.com
Gerätetyp	iC921...
Bestell-Nr.	PMC921...
Serien-Nr.	000000000000
Firmware-Version	9999.0 (99.0.0.26818)
Hardware-Version	00

6.2.2 Cockpit

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

The screenshot shows the 'Übersicht Cockpit' page for a YASKAWA CPU. The page title is 'Übersicht Cockpit'. On the left, there is a navigation menu with options: Übersicht, Allgemeine Daten, Cockpit (selected), Diagnose, Konfiguration, Security, and Verwalten. The main content area displays the Cockpit section, which includes a toolbar with icons for Stop, Warmstart, Kaltstart, Speicher Download, Speicher Upload, and Neustart. Below the toolbar, there are two main sections:

- Datum und Uhrzeit**: Shows the current time and system uptime.

Aktueller Zeitstempel (TT:MM:JJJ HH:mm:ss):	01.01.2022 00:11:39
Systembetriebszeit ([T]:[H]:[mm]:ss):	11:42
- Nutzung**: Shows resource usage metrics.

Speicher:	40%
Benutzerpartition:	3% (50.86 MB / 1.42 GB)
CPU-Auslastung (gesamt):	6%
CPU Load (Core 1):	11%
CPU Load (Core 2):	0%
CPU Load (Core 3):	0%

Cockpit-Symboleiste

Die Symboleiste bietet Zugriff auf folgende Funktionen:

- ■: Stopp - Stoppt die Programmausführung auf der CPU.
- ▶: Heißstart - Führt einen Heißstart durch. Hierbei wird die CPU neu gestartet und das Programm ohne Initialisierung der Variablen fortgesetzt.
- ▶: Warmstart - Führt einen Warmstart durch. Hierbei wird die CPU neu gestartet und das Programm mit Initialisierung der Variablen fortgesetzt. Die Werte der Variablen, welche in iCube Engineer mit "Retain" gekennzeichnet sind, bleiben erhalten.
- ▶: Kaltstart - Führt einen Kaltstart durch. Hierbei wird die CPU neu gestartet und das Programm mit Initialisierung aller Variablen fortgesetzt.
- 📄: Speicher Download - Speichert die Retain-Daten lokal in einer Datei.
- 📄: Speicher Upload - Stellt die gespeicherten Retain-Daten wieder her.
- 🔄: Neustart - Führt einen Neustart durch. Die Operation entspricht einem Aus-/Einschaltvorgang. Die geladene Applikation (Code und Netzwerkkonfiguration) wird aus dem RAM gelöscht. Die Steuerung startet mit den zuletzt gespeicherten Einstellungen neu und lädt, falls vorhanden, das Bootprojekt aus dem Flash-Speicher.

- : Reset - Setzt die CPU auf die Werkseinstellungen zurück. Ähnlich wie beim Befehl "Neustart", wird die geladene Applikation (Code und Netzwerkkonfiguration) aus dem RAM aber auch aus dem Flash-Speicher (Bootprojekt) gelöscht. Zusätzlich werden alle Kommunikationseinstellungen auf die Standardeinstellungen rückgesetzt.
- : Passwort ändern - Hiermit können Sie das Passwort des aktuellen Nutzerkontos für den Online-Zugriff auf die CPU ändern.

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 191](#).

Nutzung

Hier werden CPU-Speicherbelegung und die CPU-Last ausgegeben.

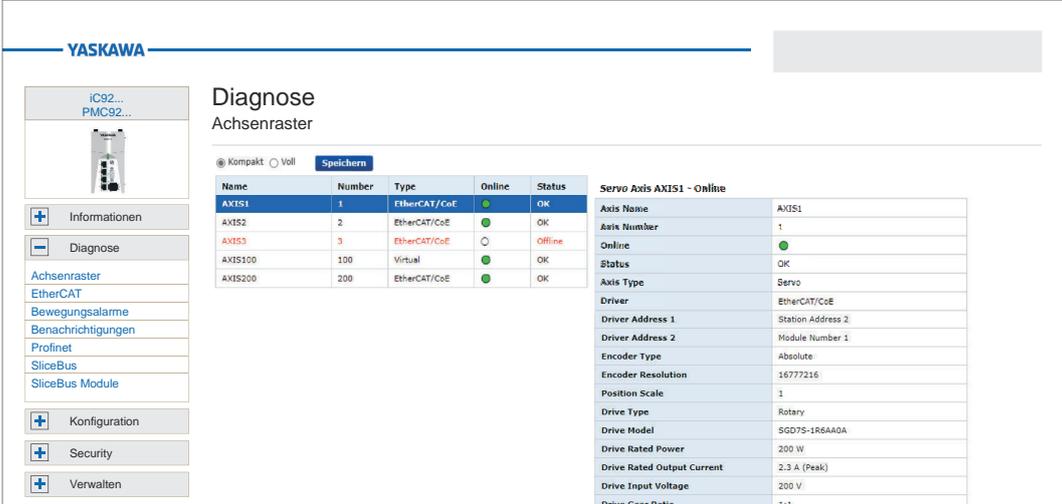
SPS-Laufzeitsystem

Hier werden der CPU-Status und die Speicherbelegung im SPS-Laufzeitsystem ausgegeben.

6.3 Diagnose

6.3.1 Achsenraster

Hier finden Sie grundlegende Informationen zur Konfiguration Ihrer Achsen wie z.B. Servoantriebe.



The screenshot shows the 'Diagnose Achsenraster' page in the YASKAWA WBM interface. The page is divided into a left sidebar with navigation options (Informationen, Diagnose, Achsenraster, EtherCAT, Bewegungsalarme, Benachrichtigungen, Profinet, SliceBus, SliceBus Module, Konfiguration, Security, Verwalten) and a main content area. The main content area has a 'Diagnose Achsenraster' title and a 'Speichern' button. Below the title is a table with columns: Name, Number, Type, Online, Status. The table lists four axes: AXIS1 (Number 1, Type EtherCAT/CoF, Online, Status OK), AXIS2 (Number 2, Type EtherCAT/CoE, Online, Status OK), AXIS3 (Number 3, Type EtherCAT/CoE, Offline, Status Offline), and two virtual axes (AXIS100 and AXIS200, both Online, Status OK). To the right of this table is a detailed configuration table for 'Servo Axis AXIS1 - Online', listing parameters such as Axis Name, Axis Number, Online status, Status, Axis Type, Driver, Driver Address 1, Driver Address 2, Encoder Type, Encoder Resolution, Position Scale, Drive Type, Drive Model, Drive Rated Power, Drive Rated Output Current, Drive Input Voltage, and Drive Gear Ratio.

Name	Number	Type	Online	Status
AXIS1	1	EtherCAT/CoF	●	OK
AXIS2	2	EtherCAT/CoE	●	OK
AXIS3	3	EtherCAT/CoE	○	Offline
AXIS100	100	Virtual	●	OK
AXIS200	200	EtherCAT/CoE	●	OK

Servo Axis AXIS1 - Online	
Axis Name	AXIS1
Axis Number	1
Online	●
Status	OK
Axis Type	Servo
Driver	EtherCAT/CoE
Driver Address 1	Station Address 2
Driver Address 2	Module Number 1
Encoder Type	Absolute
Encoder Resolution	16777216
Position Scale	1
Drive Type	Rotary
Drive Model	SGD7S-1R6AA0A
Drive Rated Power	200 W
Drive Rated Output Current	2.3 A (Peak)
Drive Input Voltage	200 V
Drive Gear Ratio	1:1

Zur Anzeige haben Sie folgende Möglichkeiten:

- Kompakt
 - Hier werden alle in der CPU konfigurierten Achsen und deren Zustände in einer kompakten Tabelle aufgeführt.
 - Durch Anwahl einer Achse erhalten Sie in der daneben befindlichen Tabelle alle Informationen zu der entsprechenden Achse.
- Voll
 - Hier werden alle in der CPU konfigurierten Achsen mit allen Informationen in einer Tabelle aufgelistet.
 - Durch Anwahl von EtherCAT/CoE bzw. Virtuell können Sie die Auflistung auf über FSoE angebundene Achsen bzw. virtuelle Achsen begrenzen.
- Mit [Speichern] können Sie die Achs-Informationen als CSV-Datei auf Ihrem PC speichern.

6.3.2 EtherCAT

Hier finden Sie grundlegende Informationen über die EtherCAT Slave-Stationen, welche über das EtherCAT-Netzwerk verbunden sind. Hier werden nur Informationen angezeigt, wenn das EtherCAT-Netzwerk korrekt konfiguriert ist und sich die EtherCAT Slave-Stationen im Zustand *OP*, *PreOP* oder *SafeOP* befinden. Ansonsten erhalten Sie den Hinweis "*Ungültige Netzwerkkonfiguration oder Netzwerk nicht betriebsbereit*".

YASKAWA

Diagnose
EtherCAT

Gefundene Slaves: 3
Konfigurierte Slaves: 3

	Stationsadresse	Konfigurierter Stationsalias	Gerätename	Gerätetyp	Hersteller ID	Produktcode	Revisionsnummer	Seriennummer	Status
1	1	0	053-1EC01	0x00001389	0x0000022B	0x0531EC01	0x80000003	2050	OP
2	2	1	SGD7S-1R6AA0A	0x00020192	0x00000539	0x02200301	0x00080014	D02080258710018	OP
3	3	2	SGD7S-1R6AA0A	0x00020192	0x00000539	0x02200301	0x00080014	D02080258720033	OP

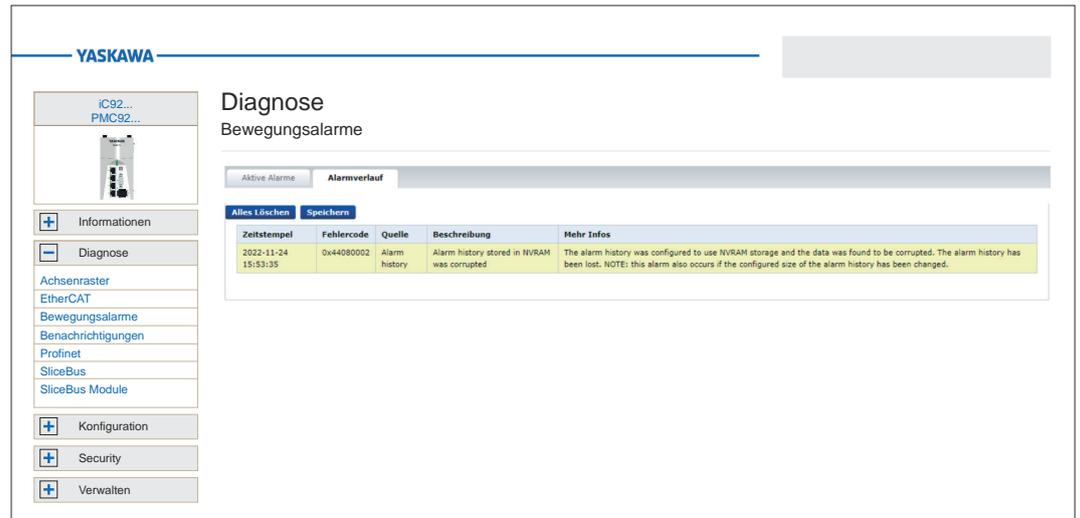
EtherCAT-Geräteinformationen sind nur verfügbar, wenn die folgenden Kriterien erfüllt sind:
 1. Netzwerk ist konfiguriert und betriebsbereit
 2. ESM-Status des Geräts ist OP, SAFEOP oder PREOP

Folgende Informationen werden tabellarisch aufgeführt:

- Stationsadresse und Station Alias
- Stationsname, -Typ und Hersteller
- Produkt-Code, Revisionsnummer und Seriennummer
- "State": ESM-Status der entsprechenden EtherCAT Slave-Station:
 - OP
Die EtherCAT Slave-Station befindet sich im Zustand *Operational* und tauscht zyklisch Prozessdaten aus.
 - PreOP
Die EtherCAT Slave-Station befindet sich im Zustand *Pre-Operational*. Prozessdaten werden nicht ausgetauscht.
 - SafeOP
Die EtherCAT Slave-Station befindet sich im Zustand *Safe-Operational*. Hierbei werden die Eingangsprozessdaten zyklisch aktualisiert aber die Ausgänge sind deaktiviert.

6.3.3 Bewegungsalarme

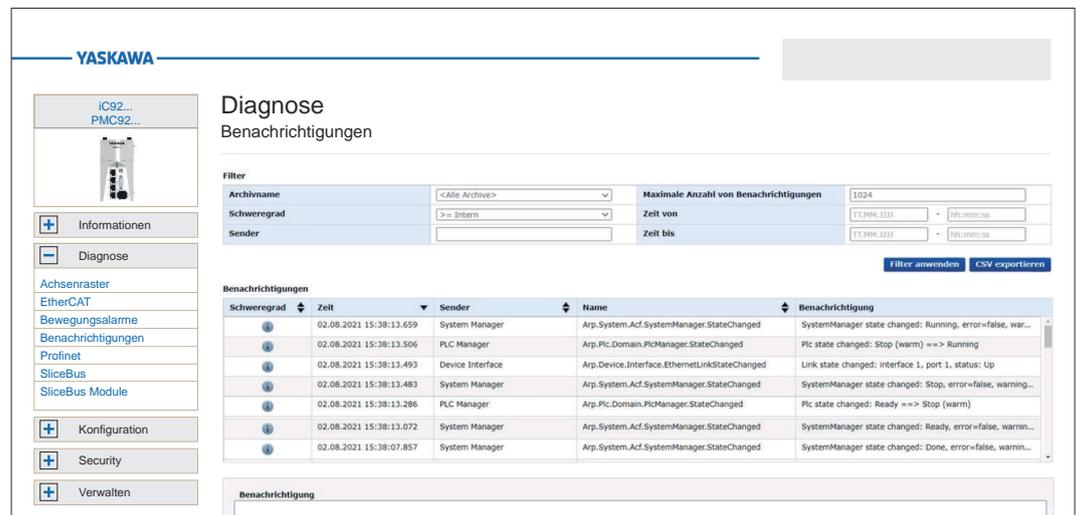
Sofern Sie einen Antrieb an Ihre CPU angebunden haben, finden Sie hier die aktuellen Bewegungsalarme und deren Verlauf.



- **"Aktive Alarme"**
 - Hier werden alle aktuell anstehenden Bewegungsalarme aufgelistet.
 - Die Tabelle beinhaltet Fehlercode, Quelle, Beschreibung und nähere Informationen zu dem entsprechenden Bewegungsalarm.
- **"Alarmverlauf"**
 - Hier werden die letzten 100 Bewegungsalarme aufgelistet.
 - Die Tabelle beinhaltet Datum, Uhrzeit, Fehlercode, Quelle, Beschreibung und nähere Informationen zu dem entsprechenden Bewegungsalarm.

6.3.4 Benachrichtigungen

Jeder Benutzer mit Zugriffsrechten kann hier Meldeinträge 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.



Sortierkriterien für die Meldeinträge

Standardmäßig werden in der Tabelle die Meldeinträge 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 Meldeeintrags 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...
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

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:

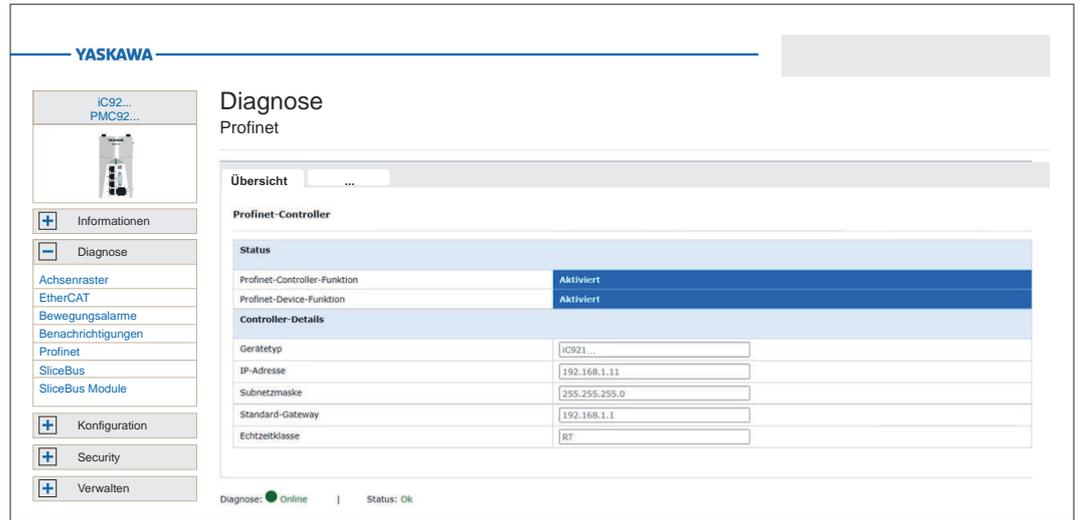
- Archivname
 - Hier können Sie die Meldeeinträge durch Angabe eines Archivnamens filtern.
- Schweregrad
 - Hier können Sie die Meldeeinträge aufgrund deren Schweregrad eingrenzen.
 - Die Eingrenzung erfolgt nach folgender Staffelung für den minimalsten Schweregrad:
Intern → Information → Warnung → Fehler → Kritische Fehler → Schwerwiegende Fehler
 Beispielsweise werden bei *Intern* alle Schweregrade gelistet. Mit der Einstellung *Fehler* werden alle *Fehler*, *Kritische Fehler* und *Schwerwiegende 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 ist 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.

6.3.5 PROFINET - optional

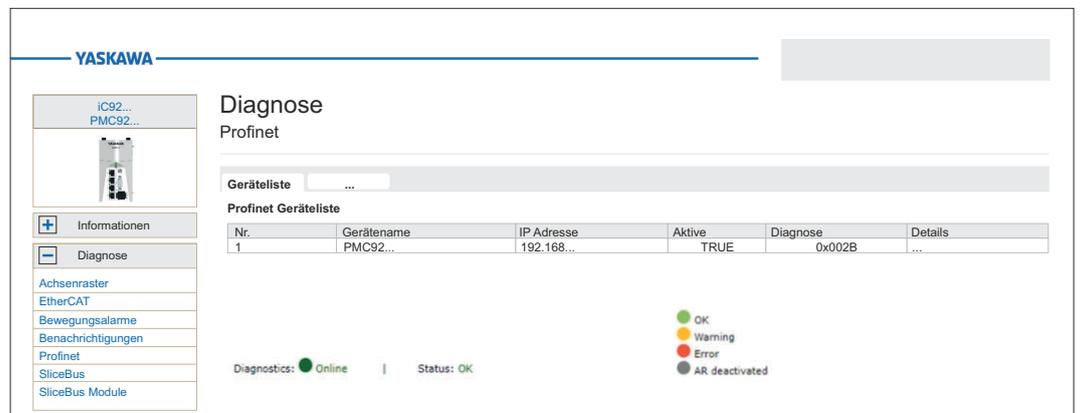
Reiter: "Übersicht"

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

 *Bitte beachten Sie, dass für den Einsatz von PROFINET eine gesonderte Lizenz erforderlich ist, welche entsprechend zu aktivieren ist!*



Reiter: "Geräte-Liste"



WBM eines PROFINET-Device öffnen

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

Geräteinformation öffnen

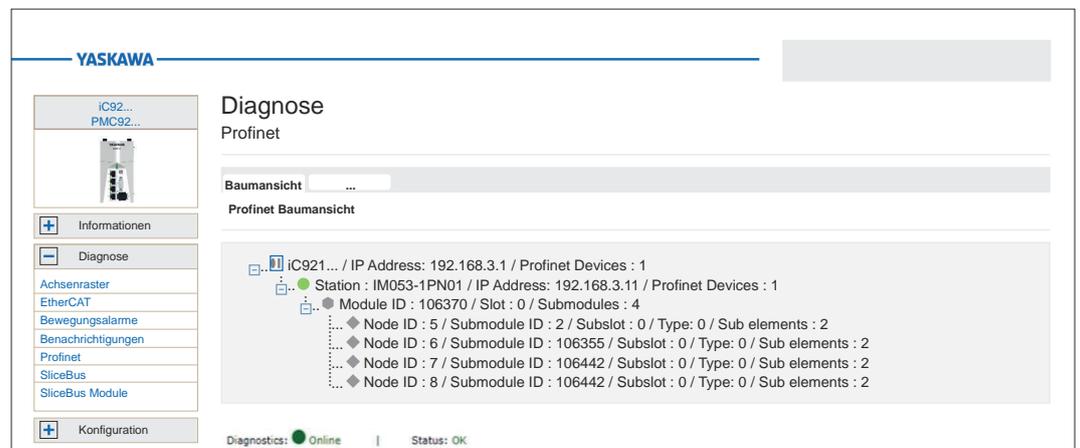
Für das entsprechende PROFINET-Device finden Sie unter Geräteinformation Informationen zu IP-Einstellungen und Diagnose. Diese Informationen werden einmal pro Sekunde aktualisiert.

- ➔ 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.



Reiter: "Baumansicht"

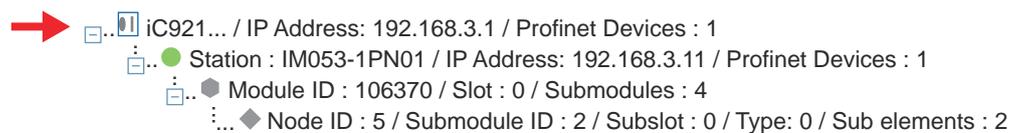
Hier haben Sie eine Baumansicht über alle konfigurierten PROFINET-Devices. Die Übersicht enthält die Gerätenamen der PROFINET-Devices, deren aktuelle IP-Einstellungen sowie den Diagnosezustand der Geräte und Module. Über [+] und [-] können Sie die nächste Ebene der Baumansicht öffnen oder schließen.



Controller-Ebene

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

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



Stations-Ebene

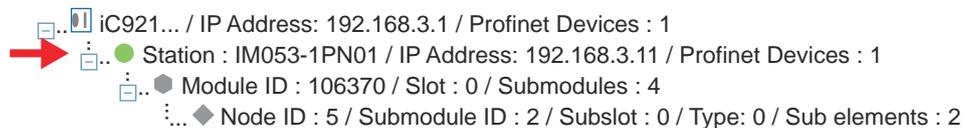
Auf Stations-Ebene finden Sie folgende Informationen zu den PROFINET-Devices:

- Stationsname
- IP Address - IP-Adresse der Station
- Vendor ID - die ID des Herstellers
- Device ID - die ID des Geräts
- Modules - Anzahl der Module

Die folgenden Symbole geben Auskunft über den aktuellen Diagnosezustand des PROFINET-Device:

Symbol	Diagnosestatus
	OK
	Warnung

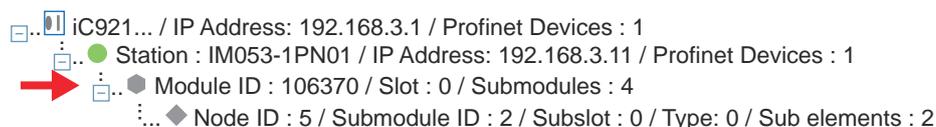
Symbol	Diagnosestatus
	Fehler



Modul-Ebene

Auf Modul-Ebene finden Sie folgende Informationen:

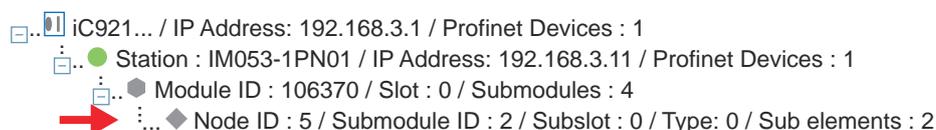
- Module ID - die ID des Moduls
- Slot - Steckplatz des Moduls
- Submodules - die Anzahl der Submodule



Submodul-Ebene

Auf Submodul-Ebene finden Sie folgende Informationen:

- Node ID - node ID des Submoduls
- Submodule ID
- Subslot
- Type
- Sub Elements - Anzahl der Submodul-Elemente



6.3.5.1 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	<p>Bit 0 ist gesetzt, wenn keine Verbindung besteht.</p> <ul style="list-style-type: none"> ■ Der PROFINET-Controller konnte keine Verbindung mit dem PROFINET-Device herstellen oder die AR wurde deaktiviert. <ul style="list-style-type: none"> - Bitte überprüfen Sie die Ethernet-Verbindung und den PROFINET-Gerätenamen mit Ihrem Projekttool iCube Engineer. - Prüfen Sie außerdem, ob die AR in den Geräteeinstellungen von PROFINET deaktiviert wurde.
1	<p>Bit 1 ist gesetzt, wenn die Daten ungültig sind.</p> <ul style="list-style-type: none"> ■ Das PROFINET-Device ist mit dem PROFINET-Controller verbunden, aber die Prozessdaten wurden aufgrund eines Fehlers als ungültig markiert. Die Prozessdaten wurden nicht in das Prozessabbild übertragen. <ul style="list-style-type: none"> - Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.
2	<p>Bit 2 ist gesetzt, wenn eine Diagnosemeldung ansteht.</p> <ul style="list-style-type: none"> ■ Das PROFINET-Device meldet eine Diagnose. <ul style="list-style-type: none"> - Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.

Bit	Beschreibung und Handlungsempfehlung
3	<p>Bit 3 ist gesetzt, wenn das Modul vom konfigurierten Modul abweicht.</p> <ul style="list-style-type: none"> ■ Bei der Initialisierung der PROFINET-Verbindung wurde eine Abweichung zwischen Soll- und Istkonfiguration festgestellt. <ul style="list-style-type: none"> – Bitte überprüfen Sie die Konfiguration des PROFINET-Device. In der Standardeinstellung von iCube Engineer bleibt die Verbindung im Falle eines Konfigurationsunterschieds hergestellt.
4	<p>Bit 4 ist gesetzt, wenn die AR deaktiviert ist.</p> <ul style="list-style-type: none"> ■ Das PROFINET-Device ist im Projekt konfiguriert, aber die AR wurde deaktiviert. <ul style="list-style-type: none"> – Überprüfen Sie die PROFINET-Geräteeinstellungen und aktivieren Sie die AR.
5	<p>Bit 5 ist gesetzt, wenn keine Nachbarinformationen verfügbar sind.</p> <ul style="list-style-type: none"> ■ Im verwendeten Netzwerk sind keine Nachbarinformationen verfügbar. <ul style="list-style-type: none"> – 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	<p>Bit 6 ist gesetzt, wenn Nachbarinformationen nicht einheitlich sind.</p> <ul style="list-style-type: none"> ■ 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. <ul style="list-style-type: none"> – 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	<p>Bit 7 ist gesetzt, wenn der Aliasname eines gesuchten Geräts bereits von einem AR verwendet wird.</p> <ul style="list-style-type: none"> ■ Eine DCP-Identifizierungsanforderung (Alias) wurde an das Netzwerk gesendet. Der Aliasname eines gesuchten Geräts wird jedoch bereits von einem AR verwendet. <ul style="list-style-type: none"> – 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	<p>Bit 8 ist gesetzt, wenn ein Wartungsbedarf ansteht.</p> <ul style="list-style-type: none"> ■ Das PROFINET-Device hat eine Wartungsanfrage (Wartungsalarm) übermittelt. <ul style="list-style-type: none"> – Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.
9	<p>Bit 9 ist gesetzt, wenn eine hochpriorie Wartungsanforderung ansteht.</p> <ul style="list-style-type: none"> ■ Das PROFINET-Device hat eine hochpriorie Wartungsanfrage (Wartungsalarm) übermittelt. <ul style="list-style-type: none"> – Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.
10	<p>Bit 10 ist gesetzt wenn eine hersteller- bzw. kanalspezifische Diagnose ansteht.</p> <ul style="list-style-type: none"> ■ Das PROFINET-Device hat eine hersteller- bzw. kanalspezifische Diagnose übermittelt. <ul style="list-style-type: none"> – Bitte überprüfen Sie die Diagnose des PROFINET-Device und wenden Sie sich ggf. an den Hersteller des PROFINET-Device.

6.3.6 SliceBus

Hier finden Sie Informationen zum Rückwandbus und den angebundenen Modulen.

6.4 Konfiguration

6.4.1 Netzwerk

Benutzer mit Leseberechtigung

Hier können Sie die Ethernet-Einstellungen Ihrer CPU, anzeigen. Sie haben ausschließlich Lesezugriff.

The screenshot shows the 'Konfiguration Netzwerk' page. On the left is a navigation menu with options: Informationen, Diagnose, Konfiguration, Netzwerk, Datum und Uhrzeit, Systemdienste, Webdienste, Security, and Verwalten. The main content area displays network settings for 'LAN-Schnittstellen' (TCP/IP LAN 1 - Separated Mode) and 'Port X1'. The 'Konfiguration' column contains input fields for IP-Adresse, Subnetzmaske, Standard-Gateway, DNS-Serveradressen, and MAC-Adresse, but they are disabled for editing.

TCP/IP (LAN 1) - Separated Mode	Status	Konfiguration
IP-Adresse	192.168.1.11	192.168.1.11
Subnetzmaske	255.255.255.0	255.255.255.0
Standard-Gateway	192.168.1.1	192.168.1.1
DNS-Serveradressen	8.8.8.8	8.8.8.8
	8.8.4.4	8.8.4.4
MAC-Adresse	8E:FA:66:E9:FD:76	
Port X1		
Datenrate	100 Mbit/s	
Duplexmodus	VollDuplex	
Link-Status	LinkUp	

Benutzer mit Schreibberechtigung

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

The screenshot shows the same 'Konfiguration Netzwerk' page, but the 'Konfiguration' column is now active, allowing for editing of the network settings. At the bottom right, there are buttons for 'Verwerfen' and 'Anwenden und neu starten'.

TCP/IP (LAN 1) - Separated Mode	Status	Konfiguration
IP-Adresse	192.168.1.11	192.168.1.11
Subnetzmaske	255.255.255.0	255.255.255.0
Standard-Gateway	192.168.1.1	192.168.1.1
DNS-Serveradressen	8.8.8.8	8.8.8.8
	8.8.4.4	8.8.4.4
MAC-Adresse	8E:FA:66:E9:FD:76	
Port X1		
Datenrate	100 Mbit/s	
Duplexmodus	VollDuplex	
Link-Status	LinkUp	

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 CPU übertragen und zur Aktivierung die CPU automatisch neu gestartet.



Sie können die Netzwerkeinstellungen auch über iCube Engineer 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 verbunden 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.



Alle iC9200 Series CPUs verwenden 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 Host Name
 - Geben Sie die Adresse an, unter welcher der NTP-Server im Netzwerk zu erreichen ist.
- Kommentar
 - Hier können Sie für den NTP-Server eine interne Bezeichnung vergeben.
- Die übrigen Parameter dienen der Information und können nicht geändert werden.

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 Systemdienste

Hier finden Sie Statusinformationen zu den aktivierten und deaktivierten Systemdiensten, sowie deren werkseitige Standardeinstellungen. Durch die Deaktivierung nicht benötigter Dienste können Sie die Leistungsfähigkeit Ihres Systems steigern.



- Vor der Deaktivierung eines standardmäßig aktivierten Dienstes, sollten Sie sicherstellen, dass dieser auch für das Gesamtsystem nicht erforderlich ist.
- Bitte beachten Sie auch, dass bei der Änderung einer Einstellung immer die gesamten Systemdienste-Einstellungen überschrieben werden.
- Bei der Deaktivierung von PROFINET (optional) wird auch das DCP-Protokoll deaktiviert, welches für die Identifikation und IP-Adresszuweisung für Teilnehmer im PROFINET-Netzwerk verwendet wird.

Dienst-ID	Dienstname	Auslieferungszustand	Aktivierung
DATALOGGER	Data Logger	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FWM	Firewall Manager	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IEC	IEC 61131-3 Runtime for iCube Engineer	<input type="checkbox"/>	<input checked="" type="checkbox"/>
LINUX SYSLOG	Linux Syslog Adapter	<input type="checkbox"/>	<input type="checkbox"/>
---	---	<input type="checkbox"/>	<input type="checkbox"/>
---	---		

Systemdienst aktivieren/deaktivieren

1. → Durch Anwahl bzw. Abwahl des entsprechenden Kontrollfelds aktivieren bzw. deaktivieren Sie einen Systemdienst in der Liste.
2. → Mit der Schaltfläche [Anwenden und neu starten] werden die Einstellungen für die Systemdienste übernommen.
 - ➔ Nach einer Sicherheitsabfrage werden die Einstellungen für die Systemdienste übernommen und die CPU wird neu gestartet.

6.4.4 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 CPU und werden als symbolische Links auf der Webseite aufgeführt. Bei einem Firmwareupdate werden die vorhandenen Zertifikats- und Schlüsseldateien in eine Backup-Verzeichnis verschoben und symbolische Links erstellt, die auf diese Sicherung verweisen.

Konfiguration > Webdienste

6.4.4.1 NGINX Webserver

Ausgewähltes HTTPS-Zertifikat

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

In der Konfigurationstabelle für den NGINX Webserver haben Sie die Möglichkeit, das HTTPS-Zertifikat aus einem der auf der CPU 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 Produktiv-Betriebs.

Selbst-signiertes HTTPS-Zertifikat

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

1. ➤ Wählen Sie hierzu im Auswahlfeld "HTTPS selbst-signiert".
 - ➔ Die Konfiguration des selbst-signierten HTTPS-Zertifikats wird tabellarisch aufgeführt. Diese 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 CPU werden standardmäßig vorgeschlagen.
 - Sie haben die Möglichkeit, diese zu erweitern, anzupassen oder einen DNS-Namen vorzugeben. Mit  fügen Sie einen Eintrag hinzu. Mit  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 CPU über DNS-Namen erreichbar, müssen Sie auch diese angeben!

3.  Damit die Änderungen übernommen werden, klicken Sie auf [Regeneriere HTTPS-Zertifikat].
 - ➔ Das Zertifikat wird neu erzeugt. Hierbei wird ein bestehendes selbst-signierte 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 CPU sind im Bereich "Security" des WBM zu konfigurieren.

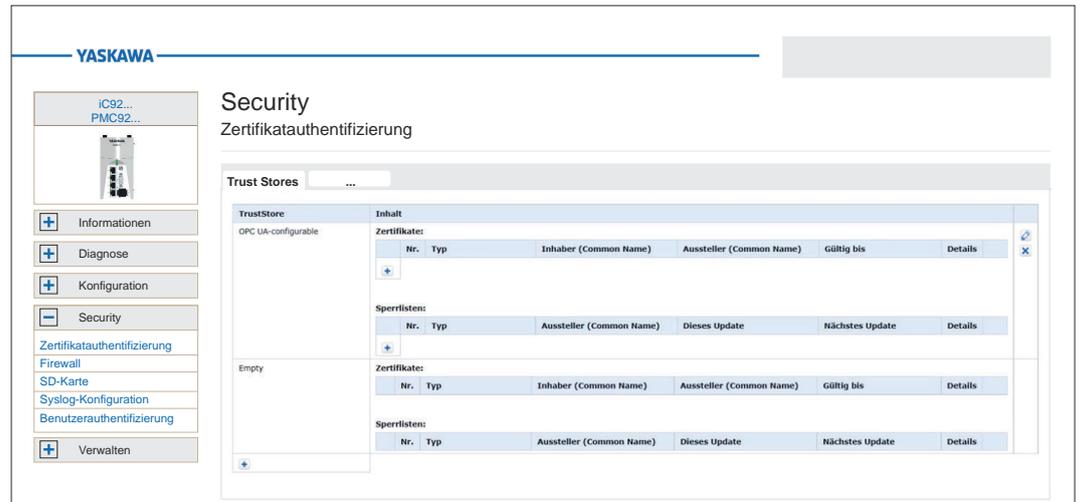
6.5.1 Zertifikatauthentifizierung

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

- Trust Store
 - Hier werden vertrauenswürdige Zertifikate und Sperrlisten möglicher Kommunikationspartner gespeichert.
- Identity Store
 - Hier werden die persönlich erstellten Zertifikate gespeichert.



- *Der Name für jeden Store kann mit den Schnittstellen für die TLS-Kommunikation verwendet werden, z.B. TLS_SOCKET Block in IEC 61131-3 oder TlsSocket-Klasse in C++ oder C#.*
- *Bei den Namen der Stores wird zwischen Groß- und Kleinschreibung unterschieden.*



Register: Trust Store

Jeder Trust Store 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 Trust Store verwalten. Indem Sie hier nicht vertrauenswürdige Zertifikate und Ausstellerzertifikate hinterlegen.

Trust Store erstellen

1. ➔ Zum Erstellen eines Trust Store klicken Sie am Ende der Tabelle auf die Schaltfläche **+**.
 - ➔ Es öffnet sich der Eingabe-Dialog zur Eingabe eines Namens für den Trust Store.
2. ➔ Geben Sie einen Namen an.
3. ➔ Klicken Sie auf [Hinzufügen].
 - ➔ Der Dialog wird geschlossen und der neue Trust Store 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.

Zertifikat hinzufügen

Trust Store

Zertifikatstyp

Zertifikat im PEM-Format:

Eingabemethode

- ➔ ■ Trust Store
 - Name des Trust Store.
- Zertifikattyp
 - Geben Sie hier an, ob es sich um eine vertrauenswürdige bzw. nicht vertrauenswürdige Zertifikat handelt.
- Zertifikat im PEM-Format

- Zertifikat-Dateien können ausschließlich im PEM-Format verarbeitet werden.
 - Eingabe Methode
 - 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 "*Eingabe Methode*" den Parameter "*Textinhalt*" aus, geben den Text in das Eingabefeld ein und klicken Sie auf [Hinzufügen].
- ➔ Der Eingabedialog wird geschlossen und das Zertifikat in Textform hinzugefügt.
3. ➔ Zum Hinzufügen eines Zertifikats in Dateiform wählen Sie unter "*Eingabe Methode*" den Parameter "*Datei hochladen*" aus, navigieren Sie über [Durchsuchen...] zu Ihrem Zertifikat im PEM-Format und klicken Sie auf [Hinzufügen].
- ➔ Der Eingabedialog wird geschlossen und das Zertifikat als PEM-Datei hinzugefügt.
- ➔ Mit unterhalb der Tabelle "*Sperrlisten*" können Sie über den Dialog eine Sperrliste hinzufügen.

Sperrliste hinzufügen

Sperrliste hinzufügen

Trust Store

CRL-Typ

Sperrliste im PEM-Format:

Eingabemethode

- ➔ ■ Trust Store
- Name des Trust Store.
- CRL-Typ
- Geben Sie hier an, ob es sich um eine vertrauenswürdige bzw. nicht vertrauenswürdige Sperrliste handelt.
- Zertifikat im PEM-Format
- Sperrlisten-Dateien können ausschließlich im PEM-Format verarbeitet werden.
- Eingabe Methode
- 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*".

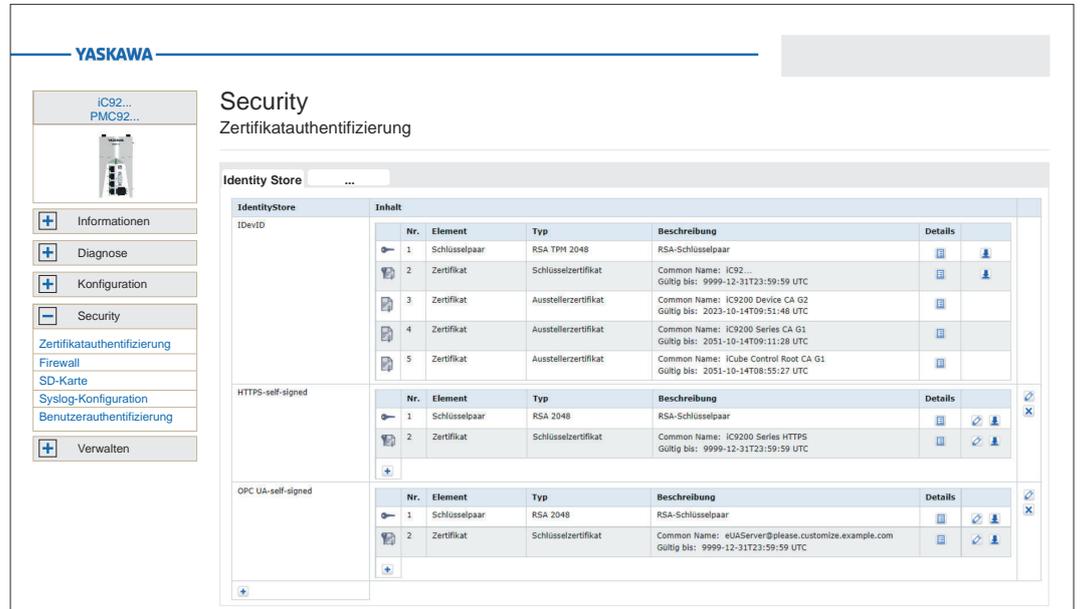
Detailansicht

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: Identity Store

- Im Register "Identity Store" können Sie mehrere Identity Stores erstellen und verwalten.
- Jeder Identity Store enthält in der Regel ein RSA-Schlüsselpaar und das entsprechende Schlüsselzertifikat.
- Optional können Sie einem Identity Store weitere Ausstellerzertifikate hinzufügen.
- Die IDDevID- und OPC UA-self-signed-Identity Stores sind Teil des Systems und werden mit der CPU geliefert.



Identity Store hinzufügen

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

Identity Store hinzufügen

Bezeichnung

Zertifikatstyp

Schlüsselpaar im PEM-Format:

Eingabemethode

- ➔ ■ Name
 - Name für den Identity Store.
- 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.
- Eingabe Methode
 - 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 "Eingabe Methode" den Parameter "Textinhalt" aus, geben den Text in das Eingabefeld ein und klicken Sie auf [Hinzufügen].
 - ➔ Der Eingabedialog wird geschlossen und das Schlüsselpaar in Textform hinzugefügt.
3. ➔ Zum Hinzufügen eines Schlüsselpaars in Dateiform wählen Sie unter "Schlüsselpaar" den Parameter "Eingeben" und unter "Eingabe Methode" den Parameter "Datei hochladen" aus, navigieren Sie über [Durchsuchen...] zu Ihrer Schlüsselpaar-Datei im PEM-Format und klicken Sie auf [Hinzufügen].
 - ➔ Der Eingabedialog wird geschlossen und das Schlüsselpaar als PEM-Datei hinzugefügt.
4. ➔ Zum Hinzufügen eines durch die CPU generierten Schlüsselpaares wählen Sie unter "Schlüsselpaar" den Parameter "Generieren" aus, wählen Sie im Dialog die Verschlüsselungsmethode aus und klicken Sie auf [Hinzufügen].
 - ➔ Der Eingabedialog wird geschlossen und das automatisch von der CPU 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 Identity Store.
- : Details - Zeigt die Detailansicht des entsprechenden Elements.
- : Herunterladen - Sie können den Inhalt des öffentlichen Schlüssels eines Schlüsselpaares 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 CPU 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.

The screenshot shows the YASKAWA WBM Security Firewall configuration interface. The main heading is 'Security Firewall'. Below it, there's a 'Systemnachricht' section showing 'Konfigurationsstatus = OK'. The 'Systemstatus' section indicates 'Liste der aktiven Firewall-Regeln' with a button 'Regeln anzeigen'. The 'Generelle Einstellungen' section shows the status as 'Stoppen' (Aktuell: gestoppt) and an 'Aktivierung' checkbox. Below this, there are 'Basis-Konfigurationen' and 'Benutzer-Konfigurationen' tabs. The 'ICMP-Einstellungen' section has checkboxes for 'Eingehende ICMP-Anfragen zulassen' and 'Ausgehende ICMP-Anfragen zulassen'. The 'Basisregeln' table is as follows:

Seq.	Richtung	Protokoll	Nach Port	Kommentar	Aktion
1	Eingang	UDP	123	NTP (Network Time Protocol)	Annehmen
2	Eingang	TCP	41100	Remoting (e.g. 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
7	Eingang	UDP	161	SNMP (Simple Network Management Protocol)	Annehmen
8	Eingang	UDP	34962-34964	Profinet Uni-/Multicast Ports	Annehmen

[Anwenden] und [Verwerfen]

- Mit der Schaltfläche [Anwenden] werden die geänderten Firewall-Einstellungen in die CPU 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 CPU angezeigt. Hierbei können folgende Systemmeldungen auftreten:

- Status = OK
 - Die konfigurierten Firewall-Einstellungen wurden erfolgreich auf die CPU übertragen.
- Warnung
 - Die CPU 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 "Neustarten" aus.

2. ➤ Klicken Sie auf [Anwenden].

- ➔ Die Firewall wird aktiviert. Nach einem Neustart der CPU 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 CPU 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-Konfiguration
 - Hier finden Sie vordefinierte Firewall-Regeln, welche Sie aktivieren bzw. deaktivieren können.
- Benutzer-Konfiguration
 - 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 Einstellmöglichkeiten:

- 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-Konfiguration" überspringen und stattdessen eine Regel in der "Benutzer-Konfiguration" erstellen und dort aktivieren.

Register: Basis-Konfiguration

"ICMP-Einstellungen"

- "Eingehende ICMP-Anfragen zulassen"
 - aktiviert: Eingehende ICMP-Echoanforderungen werden akzeptiert. Die CPU kann mit einer Ping-Anforderung erreicht werden.
 - deaktiviert: Eingehende ICMP-Echoanforderungen werden blockiert. Die CPU kann nicht mit einer Ping-Anforderung erreicht werden.

- **"Ausgehende ICMP-Anfragen zulassen"**
 - aktiviert: Ausgehende ICMP-Echoanforderungen werden akzeptiert. Ping-Anforderungen von der CPU werden übermittelt.
 - deaktiviert: Ausgehende ICMP-Echoanforderungen werden blockiert. Ping-Anforderungen von der CPU werden blockiert.

"Basisregeln"

- Hier finden Sie vordefinierten 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-Konfiguration"** erstellen und dort aktivieren.

**Sperrung des WBM-Zugangs**

- Der Zugriff auf das WBM erfolgt bei der CPU 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 CPU.
- 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 CPU mit den ursprünglichen Zugangsdaten.

**Einsatz als PROFINET-Controller (optional)**

- Verbindungen zu PROFINET Devices können nur aufgebaut werden, wenn Sie für die Regel **"PROFINET unicast/multicast ports"** (UDP-Ports 34962 - 34964) **"Annehmen"** anwählen.

Register: Benutzer-Konfiguration

- 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.
- **"Interface"**
 - 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.
- **"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 SD-Karte

Unter SD-Karte können Sie den Einsatz von Yaskawa SD-Karten aktivieren und Informationen über diese abrufen.



WARNUNG

Datenverlust - Kartenentnahme nur bei ausgeschalteter Spannungsversorgung!

- Entnehmen Sie die Yaskawa SD-Karte nur dann, wenn die Versorgungsspannung der CPU ausgeschaltet ist. Ansonsten führt dies zu Datenverlust!
- Wenn Sie die SD-Karte im laufenden Betrieb entnehmen, schaltet die Safety-CPU in den sicheren Zustand (Failure State).



Generelle Hinweise zum Einsatz der Yaskawa SD-Karte

- Es werden ausschließlich Yaskawa SD-Karten unterstützt.
- Die Karten sind vorformatiert (ext4-Format) für den Einsatz in CPUs der iC9200 Series.
- Durch eine erneute Formatierung gehen bestimmte Informationen auf der Yaskawa SD-Karte verloren, welche für den Einsatz in den CPUs der iC9200 Series erforderlich sind.
- Schließen Sie aus, dass die Yaskawa SD-Karte formatiert wird.
- Die Yaskawa SD-Karte kann jederzeit mit einem herkömmlichen SD-Kartenleser gelesen werden. Sensible Daten auf der Yaskawa SD-Karte können ausgelesen werden, wenn Sie diese nicht physisch vor unbefugtem Zugriff schützen.
- Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die Yaskawa SD-Karte haben.

- **Status**
 - Hier wird der Status zum aktuell verwendeten Filesystem der CPU angezeigt.
 - **Konfiguration**
 - Hier können Sie die Unterstützung der Yaskawa SD-Karte durch die CPU aktivieren (Defaulteinstellung) oder deaktivieren.
 - **Systemnachricht**
 - Hier werden Informationen zur aktuellen Konfiguration und Hinweise zu potenziellen Sicherheitsrisiken angezeigt.
 - **[Anwenden] und [Verwerfen]**
 - Mit der Schaltfläche [Anwenden] wird die Auswahl unter Konfiguration gespeichert und nach einem Neustart der CPU übernommen.
 - Mit der Schaltfläche [Verwerfen] können Sie Ihre Auswahl verwerfen.
- Einsatz SD-Karte aktivieren**
1. ➤ Aktivieren Sie den Parameter "Unterstützung der externen SD-Karte".
 2. ➤ Klicken Sie auf [Anwenden].
 - ➔ Die Einstellung wird gespeichert und erst übernommen, wenn Sie die CPU neu starten.

3. Starten Sie die CPU neu.
 - ➔ ■ Der Einsatz der Yaskawa SD-Karte wird aktiviert.
 - Wird während der Initialisierungsphase eine neue Yaskawa SD-Karte erkannt, wird das überlagernde Dateisystem mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen, vom internen Parametrierungsspeicher auf die Yaskawa SD-Karte verschoben und im internen Parametrierungsspeicher gelöscht.
 - Von nun an verwendet die CPU das überlagernde Dateisystem auf der Yaskawa SD-Karte.
 - Unter "Status" wird "Externe SD-Karte" angezeigt.



Bitte beachten bei Einsatz ohne Yaskawa SD-Karte!

- Per Default ist die Unterstützung der Yaskawa SD-Karte aktiviert.
- Deaktivieren Sie die Unterstützung der Yaskawa SD-Karte, wenn Sie die CPU ohne Yaskawa SD-Karte betreiben möchten.
- Bleibt die Unterstützung der Yaskawa SD-Karte aktiviert und wird die CPU ohne Yaskawa SD-Karte betrieben, besteht die Gefahr von Datendiebstahl oder Datenmanipulation.
 - Unbefugte Personen können eine Yaskawa SD-Karte einsetzen und die CPU neu starten.
 - Wird nach NetzEIN eine neue noch unbenutzte Yaskawa SD-Karte erkannt, wird das überlagernde Dateisystem mit Anwenderprogramm, Konfigurationen, Anwenderdaten und Firmwareanpassungen, vom internen Parametrierungsspeicher auf die Yaskawa SD-Karte verschoben und im internen Parametrierungsspeicher gelöscht. Dort gespeicherte Projekte und IP-Konfigurationen sind dann nicht mehr verfügbar!
- Beim Wechsel zum Betrieb ohne Yaskawa SD-Karte wird nach NetzEIN der CPU das überlagernde Dateisystem des internen Parametrierungsspeichers aktiviert und von nun an verwendet. Bitte beachten Sie, dass hierbei keine Daten von der Yaskawa SD-Karte übernommen werden. Auch gibt es keine Funktion zur Rückübertragung von der Yaskawa SD-Karte auf den internen Parametrierungsspeicher.

Einsatz SD-Karte deaktivieren

1. Deaktivieren Sie den Parameter "Unterstützung der externen SD-Karte".
2. Klicken Sie auf [Anwenden].
 - ➔ Die Einstellung wird gespeichert und erst übernommen, wenn Sie die CPU neu starten.
3. Starten Sie die CPU neu.
 - ➔ ■ Der Einsatz der Yaskawa SD-Karte wird deaktiviert.
 - Die Yaskawa SD-Karte wird während der Initialisierungsphase von der CPU nicht erkannt und das überlagernde Dateisystem des internen Parametrierungsspeichers aktiviert.
 - Von nun an verwendet die CPU ausschließlich den internen Parametrierungsspeicher.
 - Unter "Status" wird "Interne SD-Karte" angezeigt.

6.5.4 Syslog-Konfiguration

Hier können Sie Syslog-Server konfigurieren. Syslog bzw. Syslog-ng ist ein Standard zur Übermittlung von Log-Meldungen in einem Netzwerk.

Syslog-Server-Ziel anlegen

1. Zum Erstellen eines Syslog Server-Ziels klicken Sie am Ende der Tabelle auf die Schaltfläche **+**.

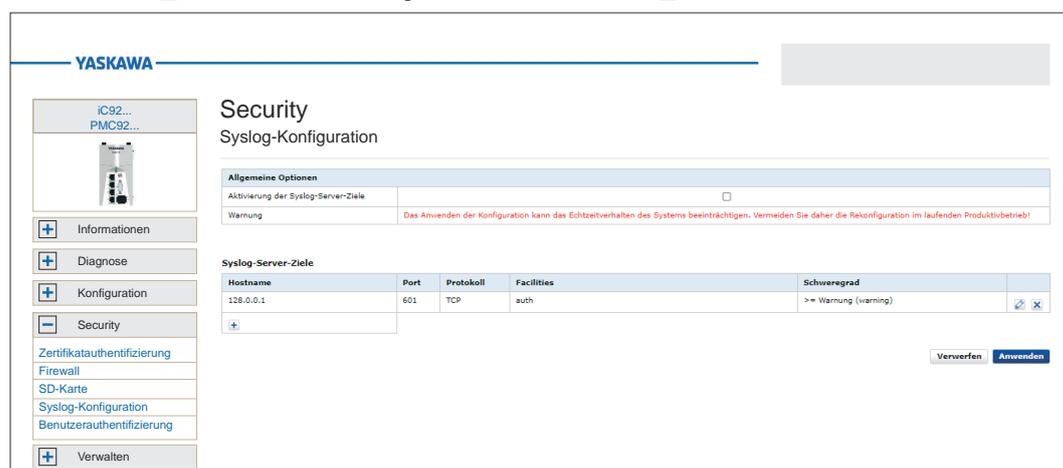
➔ Es öffnet sich der Dialog zur Konfiguration eines Syslog Server-Ziels.

2. Geben Sie unter "Allgemeine Optionen" folgende Parameter an:

- Hostname
 - Hostname bzw. IP-Adresse des Syslog-Server, an welchen die Log-Daten zu senden sind.
- Protokoll
 - Übertragungsprotokoll zum Server. Für eine sichere Übertragung wird TLS empfohlen, hierzu ist ein Trust Store zur Überprüfung zu definieren. Diesen können Sie über ["Zertifikatauthentifizierung"...Seite 195](#). Den entsprechenden Trust Store können Sie unter "Trust Store" angeben.
- Port
 - Port über den die Kommunikation mit dem Syslog-Server stattfinden soll. Stellen Sie sicher, dass der Port in den Firewall-Einstellungen für ausgehende Anforderungen aktiviert ist. ["Firewall"...Seite 199](#)

3. Geben Sie unter Filteroptionen folgende Parameter an:
 - Facilities
 - Hier spezifizieren Sie den Systemtyp der Log-Daten.
 - Schweregrad
 - Bestimmen Sie hier den Schweregrad, ab welchem die Log-Daten an den Syslog-Server gesendet werden.
 - Stufe 1: >= Intern (debug): Alle Meldungen werden gesendet.
 - Stufe 2: >= Information (info): Meldungen >= Stufe 2 werden gesendet.
 - Stufe 3: >= Warnung (warning): Meldungen >= Stufe 3 werden gesendet.
 - Stufe 4: >= Fehler (err): Meldungen >= Stufe 4 werden gesendet.
 - Stufe 5: >= Kritischer Fehler (crit): Meldungen >= Stufe 5 werden gesendet.
 - Stufe 6: >= Fataler Fehler (alert): Meldungen >= Stufe 6 werden gesendet.
 - Stufe 7: Notfall (emerg): Ausschließlich Notfall-Meldungen werden gesendet.
4. Klicken Sie auf [OK].
 - ➔ Der Dialog wird geschlossen und der Syslog-Server in der Tabelle aufgeführt.
 - Mit  können Sie Einträge entfernen und mit  bearbeiten.

Syslog-Konfiguration aktivieren bzw. deaktivieren



YASKAWA

Security
Syslog-Konfiguration

Allgemeine Optionen

Aktivierung der Syslog-Server-Ziele

Warnung Das Anwenden der Konfiguration kann das Echtzeitverhalten des Systems beeinträchtigen. Vermeiden Sie daher die Rekonfiguration im laufenden Produktivbetrieb!

Syslog-Server-Ziele

Hostname	Port	Protokoll	Facilities	Schweregrad
128.0.0.1	601	TCP	auth	>= Warnung (warning)

Verwerfen Anwenden

1. Durch Anwahl bzw. Abwahl des Kontrollfelds von "Aktivierung der Syslog-Server-Ziele" unter "Syslog-Konfiguration" aktivieren bzw. deaktivieren Sie die in der Tabelle angegebenen Syslog Server-Ziele.
2. Klicken Sie auf [Anwenden].
 - ➔ Die Einstellungen werden übernommen.

6.5.5 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 CPU und Funktionen in iCube Engineer.
- 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!
- Verwenden Sie das auf der CPU aufgedruckte 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.

System Verwendungshinweis ändern

Bei jeder Anmeldung an der CPU über WBM oder iCube Engineer, erfolgt die Anzeige des System Verwendungshinweis. 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 [Benachrichtigung bearbeiten] neben System Verwendungshinweis.
 - ➔ 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 CPU zuzugreifen, verwaltet und jedem Benutzer die erforderlichen Zugriffsberechtigungen zugewiesen. Hierbei werden die Benutzerdaten der neu angelegten Benutzer intern in der CPU 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.

Benutzer entfernen

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

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:

- SD-Karte/Parametrierungsspeicher (Param. Speicher) der CPU
- Betriebssystem
- iCube Engineer
- Web-based Management - WBM
- OPC UA Server der CPU

1. → Klicken Sie in der Tabelle hinter dem Benutzereintrag, dessen Rolle Sie ändern möchten, auf die Schaltfläche [Rolle ändern].

➔ 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

Zugriff auf SD-Karte/ Param. Speicher	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
<p>SFTP-Zugriff auf das Filesystem mit einem FTP-Client</p> <p>Bitte beachten:</p> <p>Für den SFTP-Zugriff ist immer eine Authentifizierung mit Benutzername und Passwort erforderlich, auch wenn die Benutzerauthentifizierung deaktiviert ist.</p>	✓												
Zugriff auf das Betriebssystem	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
<p>SSH-Zugriff auf das Betriebssystem</p> <p>Bitte beachten:</p> <p>Für den SSH-Zugriff ist immer eine Authentifizierung mit Benutzername und Passwort erforderlich, auch wenn die Benutzerauthentifizierung deaktiviert ist.</p>	✓												

iCube Engineer	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
Werte in Cockpit anzeigen (z.B. Auslastung).	✓	✓	✓			✓	✓	✓	✓	✓	✓		
Projekt in die CPU transferieren.	✓					✓	✓						
CPU-Stop / CPU Kalt-/ Warm-/ Neustart	✓					✓	✓	✓					
CPU-Neustart (Reboot).	✓												
CPU-Reset (Default Typ 1).	✓												
Online-Variablen lesen.	✓	✓	✓			✓		✓	✓	✓	✓		
Variablen überschreiben.	✓					✓		✓		✓			
Haltepunkte setzen und löschen.	✓					✓		✓					
CPU-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
Information - Allgemeine Daten	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnose - EtherCAT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnose - Bewegungsalarme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnose - Benachrichtigungen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		

Security > Benutzerauthentifizierung

Zugriff auf WBM	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
Diagnose - PROFINET (optional)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnose - SliceBus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnose - SliceBus Module	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Konfiguration - Netzwerk	✓	✓	✓ ¹			✓ ¹	✓ ¹	✓ ¹					
Konfiguration - Datum und Uhrzeit	✓	✓	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹	✓ ¹		
Konfiguration - Systemdienste	✓	✓											
Konfiguration - Webdienste	✓	✓											
Security - Zertifikatauthentifizierung	✓	✓		✓									
Security - Firewall	✓	✓											
Security - SD-Karte	✓	✓											
Security - Syslog-Konfiguration	✓	✓											
Security - Benutzerauthentifizierung	✓	✓			✓								
Verwaltung - iCube Apps	✓	✓				✓							
Verwaltung - Firmware-Update	✓	✓											
Verwaltung - Lizenzmanagement	✓	✓											

Zugriff auf OPC UA Server	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Chan ger	View er	File Reader	File Writer
Online-Variablen lesen.	✓	✓				✓		✓	✓	✓	✓		
Online-Variablen schreiben.	✓					✓		✓		✓			
Dateien lesen.	✓											✓ ²	
Dateien schreiben.	✓												✓ ³

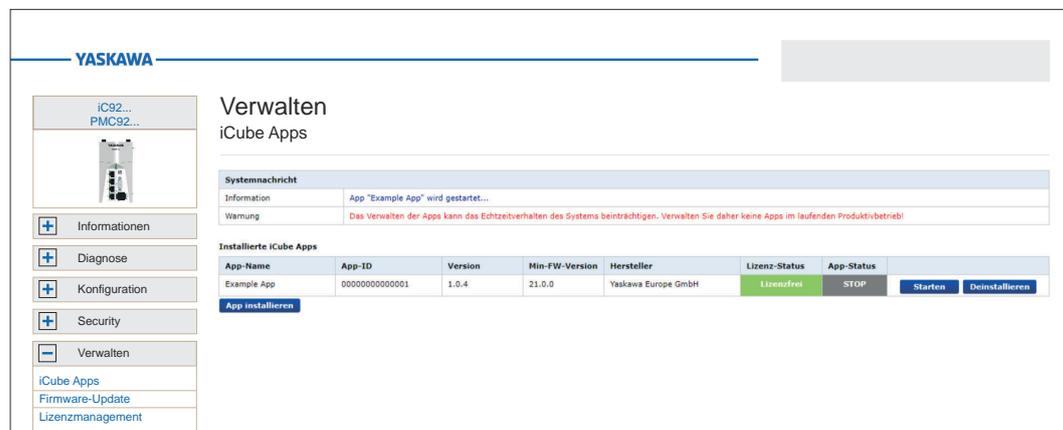
- 1) Nur lesender Zugriff.
- 2) FileReader kann Dateien nur dann über einen OPC UA Client lesen, wenn die OPC UA Dateiübertragung in iCube Engineer aktiviert ist. Näheres hierzu finden Sie in der Onlinehilfe von iCube Engineer.
- 3) FileWriter kann Dateien nur dann über einen OPC UA Client schreiben, wenn die OPC UA Dateiübertragung in iCube Engineer aktiviert ist. Näheres hierzu finden Sie in der Onlinehilfe von iCube Engineer.

6.6 Verwaltung

6.6.1 iCube Apps

Installierte iCube Apps

Hier können Sie Apps installieren und deinstallieren. Nach erfolgreicher Installation können Sie die Apps auch von hier aus starten und stoppen. iCube Apps sind Softwareanwendungen von Bibliotheken bis hin zu kompletten Programmen, die Ihnen von Yaskawa bereitgestellt werden.



In der Tabelle werden alle installierten Apps mit weiteren App-spezifischen Informationen aufgelistet.

- App-Name
 - Name der App.
- App-ID
 - Eindeutige Kennung der App.
- Version
 - Version der App
- Min-FW-Version
 - Firmware-Version der CPU, ab der die App eingesetzt werden kann.
- Hersteller
 - Hersteller der App.
- Lizenz-Status

- Lizenz-Status der App.

Informationen und Warnmeldungen werden unter "Systemnachricht" aufgeführt.



- *Zusätzliche Apps können sich negativ auf das Echtzeitverhalten auswirken.*
- *Bitte beachten Sie, dass für die Installation bzw. den Einsatz ggf. eine Lizenz erforderlich ist.*

Installation einer App

Zur Installation einer App gehen Sie wie folgt vor:

1. Klicken Sie auf [App installieren].
2. Wählen Sie im sich öffnenden Datei-Explorer die zu installierende App (*.app) aus.
3. Klicken Sie auf [Öffnen].
 - ➔ Der ausgewählte App-Container wird nun an den Controller gesendet und installiert. Nach erfolgreicher Installation wird die App in der Tabelle Installierte iCube Apps angezeigt.

Starten einer App

- Zum Starten einer App klicken Sie in der Tabelle "Installierte iCube Apps" auf [Starten] hinter der entsprechenden App.
 - ➔ Die App wird gestartet und der App-Status "RUN" in der Spalte "App Status" angezeigt.



Bitte beachten Sie, dass das Starten mehrerer Apps einen Neustart der CPU erfordern kann. Hierbei werden Sie über den bevorstehenden Neustart durch einen sich öffnenden Dialog informiert.

Beenden einer App

- Zum Beenden einer App klicken Sie in der Tabelle "Installierte iCube Apps" auf [Stoppen] hinter der entsprechenden App.
 - ➔ Die App wird beendet und der App-Status "Stoppen" in der Spalte "App Status" angezeigt.

Deinstallation einer App

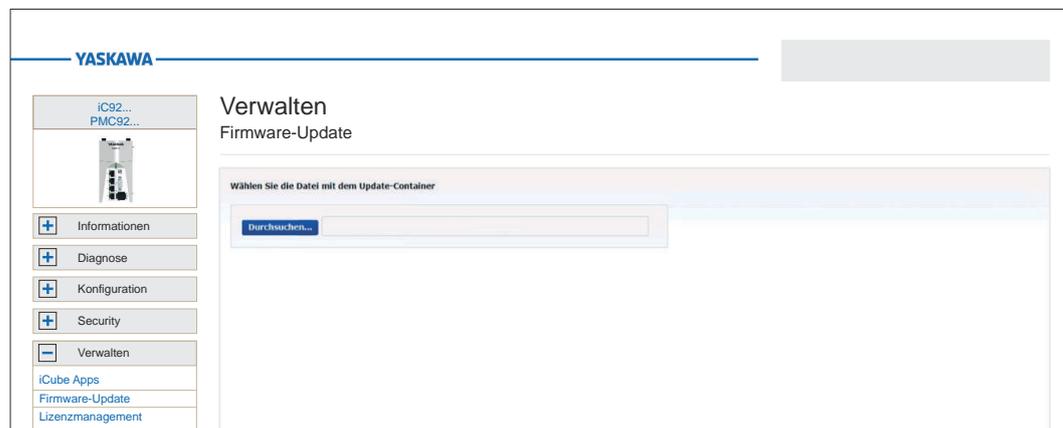
1. Zur Deinstallation einer App müssen Sie diese zuvor beenden. Klicken Sie hierzu in der Tabelle "Installierte iCube Apps" auf [Stoppen] hinter der entsprechenden App.
2. Zur Deinstallation klicken Sie in der Tabelle "Installierte iCube Apps" auf [Deinstallieren] hinter der entsprechenden App.
 - ➔ Nach einer entsprechenden Sicherheitsabfrage wird die entsprechende App deinstalliert.

6.6.2 Firmware-Update

Hier können Sie ein Firmwareupdate auf Ihrer CPU durchführen.



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



Vorgehensweise

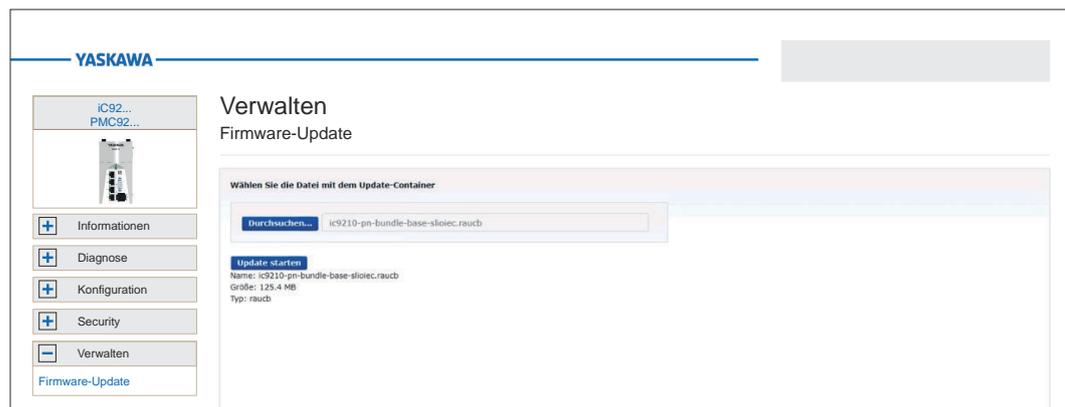


VORSICHT

Beim Aufspielen einer neuen Firmware ist äußerste Vorsicht geboten. Unter Umständen kann Ihre CPU 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 Firmwarestand Ihrer CPU finden Sie im WBM unter *"Information → Allgemeine Daten"*. Hier können Sie auch überprüfen, ob das Firmwareupdate erfolgreich war. → *"Allgemeine Daten"...Seite 181*

1. Im *"Download Center"* von www.yaskawa.eu.com finden Sie immer die aktuellste Firmware unter der entsprechenden Best.-Nr.
Laden Sie die aktuelle Firmwaredatei 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 Firmwaredatei, welche installiert werden soll, wird geladen und im WBM angezeigt.

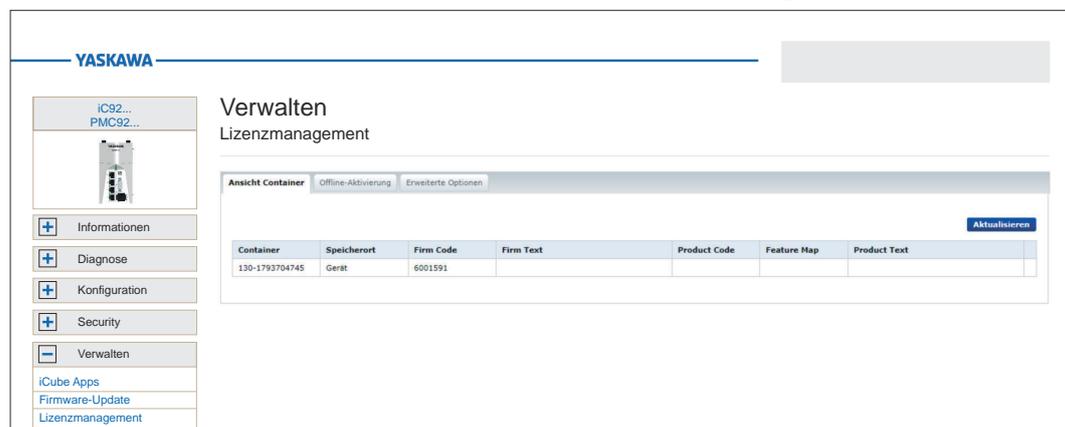


5. Klicken Sie auf [Update starten].
 - ➔ Die Firmwaredatei wird auf die CPU übertragen und das Firmwareupdate gestartet. Hierbei werden der Status der Dateiübertragung und der Status des Aktualisierungsprozesses im WBM als Fortschrittsbalken angezeigt.
6. Während des Firmwareupdates wird die Verbindung zur CPU unterbrochen. Nach dem Hochlauf der CPU müssen Sie sich neu am WBM der CPU anmelden. Hierdurch werden die WBM-Seiten aktualisiert.
7. Zur Überprüfung des Firmwareupdate rufen Sie im WBM die Seite "Information → Allgemeine Daten" auf. ➔ "[Allgemeine Daten](#)"...Seite 181
 - ➔ Hier sollte die neue Firmware-Version aufgeführt sein. Ansonsten starten Sie das Update erneut. Sollte das Update nicht gelingen, kontaktieren Sie bitte unseren Support.

6.6.3 Lizenzmanagement

Reiter: "Ansicht Container"

Hier können Sie die Lizenzen anzeigen und verwalten, welche auf der CPU installiert sind. Mehrere Lizenzen können in einem "Container" zusammen gefasst werden.



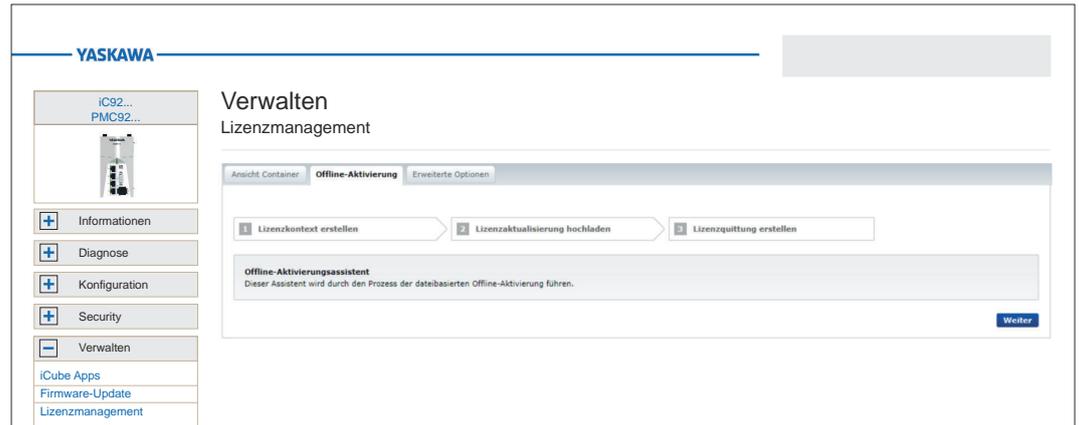
In der Tabelle werden alle Container mit den Lizenzen aufgelistet. Mit der Schaltfläche [Aktualisieren] wird die Liste neu geladen.

- Container
 - Seriennummer des Containers, in welchem die Lizenzen verwaltet werden.
- Speicherort
 - Speicherort, an dem der Container gespeichert wird.
- Firm Code
 - Identifikationsnummer des Lizenzgebers.
- Firm Text
 - Beschreibung des Lizenzgebers.
- Product Code
 - Eindeutiger Identifikationscode der lizenzierten Software.

- Feature Map
 - Angaben zum Funktionsumfang der Software.
- Product Text
 - Beschreibung der Lizenz.

Reiter: "Offline-Aktivierung"

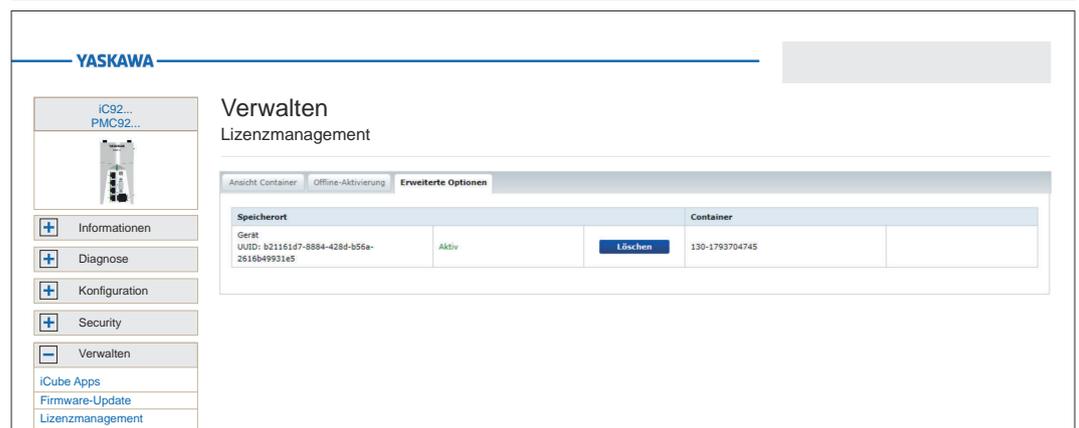
Hier können Sie eine zuvor erworbene Lizenz mittels einer Lizenzdatei offline aktivieren. Der Begriff "offline" bedeutet in diesem Zusammenhang, dass die CPU, auf der die lizenzierte Software läuft, nicht mit dem Internet verbunden sein muss. Der Offline-Aktivierungsassistent führt Sie durch den Aktivierungsprozess und bietet weitere Informationen.

**Reiter: "Erweiterte Optionen"**

Mit der Schaltfläche [Container erzeugen] können Sie für Ihre Lizenzdateien einen neuen Lizenzcontainer anlegen. Zum Löschen des entsprechenden Containers klicken Sie auf die zugehörige Schaltfläche [Löschen].



Bitte beachten Sie, dass Sie das Löschen eines Lizenzcontainers nicht wieder rückgängig machen können! Sie sollten diese Aktion nur auf Anweisung des Yaskawa-Supports durchführen!

**Schritte der Aktivierung**

Sie haben einen Lizenz-Schlüssel von Yaskawa erhalten. Die Aktivierung der Lizenz in Ihrer CPU erfolgt nach folgender Vorgehensweise:

1. ➤ Legen Sie, falls noch kein Container für Lizenzen besteht, unter "Verwaltung → Lizenzmanagement → Reiter: Erweiterte Optionen" mit der Schaltfläche [Container erzeugen] einen neuen Container an. Verwenden Sie hierbei folgende Angaben:
2. ➤ Gehen Sie in den Reiter: "Offline-Aktivierung".

3.  Laden Sie mit die zugehörige "Lizenzkontext"-Datei *.WibuCmRaC auf Ihren PC und starten Sie den Aktivierungsprozess über die Schaltfläche [Weiter].
4.  Öffnen Sie auf Ihrem PC die Webseite [↪ https://lc.codemeter.com/74390/depot/index.php](https://lc.codemeter.com/74390/depot/index.php).
5.  Tragen Sie unter Ticket Ihren Lizenz-Schlüssel ein und klicken Sie auf [Weiter].
 - ➔ Ihre Lizenz wird aufgelistet.
6.  Klicken Sie auf [Lizenzen aktivieren].
 - ➔ Es öffnet sich der Assistent für die Aktivierung mittels Dateiübertragung.
7.  Markieren Sie mit die gewünschte Lizenz.
8.  Wählen Sie die zuvor geladene "Lizenzkontext"-Datei *.WibuCmRaC aus und klicken Sie auf [Aktivierung jetzt starten].
9.  Klicken Sie auf [Download License Update File Now] und speichern Sie die "Lizenzaktualisierung" als *.WibuCmRaU-Datei auf Ihrem PC.
10.  Wechseln Sie wieder zum Reiter "Offline-Aktivierung" im WBM, wählen Sie die *.WibuCmRaU-Datei an und klicken Sie auf [Hochladen].
 - ➔ Die Lizenzaktualisierung wird dem Lizenzcontainer hinzugefügt.
11.  Laden Sie mit die "Lizenzquittung" als *.WibuCmRaR-Datei auf Ihren PC.
12.  Wechseln Sie wieder zum Assistenten von [↪ https://lc.codemeter.com/74390/depot/index.php](https://lc.codemeter.com/74390/depot/index.php).
13.  Wählen Sie die *.WibuCmRaR-Datei an und klicken Sie auf [Upload Receipt Now] und klicken Sie auf [Weiter].
 - ➔ Die Lizenz wird freigeschaltet und unter "My Licenses" als "Activated" aufgeführt.
14.  Starten Sie Ihre CPU neu.
 - ➔ Nach dem Hochlauf stehen Ihnen die mittels Lizenz freigeschaltete Funktionalitäten zur Verfügung.



Bitte beachten Sie, dass Sie bei einer erworbenen PROFINET-Lizenz nach der Aktivierung die PROFINET-Funktionalität in WBM in der Konfiguration entsprechend aktivieren müssen. [↪ "Systemdienste"...Seite 193](#)

7 Anhang

Checklisten - Einsatz CPU iC921xM-FSoE

A	Checkliste Planung.	223
B	Checkliste Installation.	224
C	Checkliste Inbetriebnahme, Parametrierung und Validation.	225
D	Checkliste Betrieb.	226
E	Checkliste Modifikation und Nachrüstung.	227
F	Checkliste Außerbetriebnahme.	228

A Checkliste Planung

Checkliste

Lfd. Nr.	Anforderung	erfüllt		Bemerkung
		ja	nein	
1	Planung			
1.1	Ist eine Risikobeurteilung durchgeführt worden und wurden die erforderlichen SIL und Performance-Level gemäß DIN EN ISO 13849-1 oder IEC 62061 bestimmt?			
1.2	Werden ausschließlich Netzteile gem. Spezifikation PELV/SELV verwendet?			
1.3	Erfolgt die Leitungsverlegung nach geltenden Normen und Richtlinien?			
1.4	Ist die Spannungsversorgung für lokale I/O-Module und Feldbuskomponenten richtig dimensioniert?			
1.5	Erfüllen alle sicherheitsgerichteten Systemkomponenten die Anforderungen des ermittelten SIL (IEC 61508), Performance Levels (DIN EN ISO 13849-1) und Sicherheitskategorie (DIN EN 954-1)?			
1.6	Entspricht die Verdrahtung der Sicherheitskomponenten den Anforderungen der zuvor festgelegten Sicherheitseinstufung?			
1.7	Entsprechen die Leistungsdaten der Safety-CPU den Vorgaben der Applikation? → "Technische Daten"...Seite 70			
1.8	Erfüllen die Komponenten die in der Applikation herrschenden Umgebungsbedingungen?			
1.9	Erfüllt das System die erforderliche Schutzart?			
1.10	Wird Verschmutzungsgrad 2 eingehalten?			
1.11	Wurde die maximal zulässige Reaktionszeit der Sicherheitsfunktionen durch eine Gefährdungsanalyse ermittelt?			
1.12	Wird die maximal zulässige Reaktionszeit erreicht? Wurde der rechnerische Nachweis erbracht?			
1.13	Ist das System vor mechanischer Überlastung geschützt?			
1.14	Ist das System vor aggressiven Medien geschützt?			
1.15	Werden die spezifizierten elektrischen Werte der Ausgangsklemmen eingehalten?			
1.16	Werden sämtliche elektromechanische Sensoren mit Taktsignalen zur Erkennung von Kurzschlüssen versorgt?			
1.17	Wurde eine Liste der einzustellenden Geräte-Parameter erstellt und sämtliche Parameter festgelegt?			

Nähere Informationen finden Sie unter → ["Applikationsbeispiel"...Seite 139](#).

Datum:.....Name:Unterschrift:

B Checkliste Installation

Checkliste

Lfd. Nr.	Anforderung	erfüllt		Bemerkung
		ja	nein	
2	Installation			
2.1	Erfüllen die Komponenten die in der Applikation herrschenden Umgebungsbedingungen?			
2.2	Erfüllt das System die erforderliche Schutzart?			
2.3	Wird Verschmutzungsgrad 2 eingehalten?			
2.4	Ist das System vor aggressiven Medien geschützt?			
2.5	Werden ausschließlich Netzteile gem. Spezifikation PELV/SELV verwendet?			
2.6	Ist sichergestellt, dass keine Kurzschlüsse durch Verdrahtung der Ein- und Ausgangsklemmen vorliegen?			
2.7	Ist sichergestellt, dass Sicherheitsschaltgeräte nicht durch Verdrahtungsfehler überbrückt sind?			
2.8	Wurde eine Verdrahtungskontrolle gemäß Installationsplan durchgeführt?			
2.9	Sind sämtliche Anschlussstecker entsprechend ihrer Zuordnung gekennzeichnet?			
2.10	Sind die Anschlussklemmen mit dem vorgegebenen Anzugsmoment beaufschlagt?			
2.11	Ist sichergestellt, dass die Isolation der Leitungen zu keiner fehlerhaften Kontaktierung führt?			
2.12	Wurden die Zuverlässigkeit sämtlicher Klemmverbindungen durch mechanische Zugbelastung kontrolliert?			
2.13	Wurde eine Sichtkontrolle auf etwaige mechanische Beschädigungen der installierten Komponenten durchgeführt?			
2.14	Wurden erforderliche Einbauabstände zu anderen Komponenten eingehalten?			

Datum:.....Name:Unterschrift:

C Checkliste Inbetriebnahme, Parametrierung und Validation

Checkliste

Lfd. Nr.	Anforderung	erfüllt		Bemerkung
		ja	nein	
3	Inbetriebnahme			
3.1	Ist sichergestellt, dass alle sicheren Kommunikationsteilnehmer eines Systems eine eindeutige sichere Geräteadresse (F-Adresse) haben? Dies gilt auch für Teilnehmer, die zu unterschiedlichen Sicherheitssteuerungen gehören, wenn die Steuerungen über Gateways (z.B. Ethernet) miteinander verbunden sind.			
3.2	Wurde die Zykluszeit T_{Cl} der Safety-CPU ermittelt und in der Safety-CPU eingestellt? → "Zykluszeit T_{Cl} Safety-CPU" ...Seite 137			
3.3	Wurde die maximale Reaktionszeit mit der eingestellten Zykluszeit T_{Cl} rechnerisch nachgewiesen? → "Reaktionszeiten" ...Seite 134			
3.4	Wurden die Geräteparameter der Safety E/A-Module validiert? → "Validation des Systems" ...Seite 123			
3.5	Wurde das richtige Projekt ausgewählt?			
3.6	Wurde ein Review des Sicherheitsprogramms durchgeführt?			
3.7	Wurden die Projektdaten auf eine Speicherkarte kopiert?			
3.8	Wurde ein vollständiger Funktionstest durchgeführt und dokumentiert?			
3.9	Wurde Ihr Engineering-Projekt rechtssicher dokumentiert und archiviert?			
3.10	Wurde das Bedienpersonal in die Handhabung des Steuerungssystems eingewiesen?			
Datum:Name:Unterschrift:				

D Checkliste Betrieb

Checkliste

Lfd. Nr.	Anforderung	erfüllt		Bemerkung
		ja	nein	
4	Betrieb			
4.1	Ist sichergestellt, dass während des Betriebs der Safety-CPU keine Änderungen an der Systemkonfiguration durchgeführt werden?			
4.2	Ist sichergestellt, dass vor der Erweiterung des Systems, dem Entfernen einzelner Systemkomponenten und Änderungen in der Verdrahtung die Steuerung durch sachkundiges Personal in einen von der Anwendung abhängigen sicheren Zustand gesetzt wird?			
4.3	Werden die in den Technischen Daten angegebenen Umgebungsbedingungen eingehalten? ↪ <i>"Technische Daten" ...Seite 70</i>			
4.4	Wird die vom Hersteller angegebene Lebensdauer aller sicherheitsrelevanten Geräte eingehalten?			
4.5	Ist sichergestellt, dass eine Inbetriebsetzung erst nach einer Akklimatisierung der Safety-CPU und der Safety-Module erfolgt?			
4.6	Ist sichergestellt, dass während der ganzen Betriebszeit ein PC-System mit lauffähigem iCube Engineer zur Verfügung steht?			

Datum:.....Name:Unterschrift:

E Checkliste Modifikation und Nachrüstung

Checkliste

Lfd. Nr.	Anforderung	erfüllt		Bemerkung
		ja	nein	
5	Modifikation und Nachrüstung			
5.1	Ist die Modifikation/Nachrüstung des Systems kompatibel? Werden weiterhin sämtliche Anforderungen der folgenden Checklisten erfüllt? ➔ " <i>Checkliste Planung</i> "...Seite 223 ➔ " <i>Checkliste Installation</i> "...Seite 224 ➔ " <i>Checkliste Inbetriebnahme, Parametrierung und Validation</i> "...Seite 225			
5.2	Wurde die zu tauschende Sicherheitskomponente gegen eine kompatible Sicherheitskomponente getauscht?			
5.3	Ist bei Änderungen von nicht-safety Komponenten die Prüfsumme unverändert?			
5.4	Wurde das richtige Sicherheitsprojekt eingespielt?			
5.5	Werden die berechneten Reaktionszeiten nach der Modifikation/Nachrüstung weiterhin eingehalten? Nachweis erforderlich!			
5.6	Wurden die Projektdaten auf eine Speicherkarte kopiert?			
5.7	Wurde ein vollständiger Funktionstest durchgeführt und dokumentiert?			
Datum:.....Name:Unterschrift:				

F Checkliste Außerbetriebnahme

Checkliste

Lfd. Nr.	Anforderung	erfüllt		Bemerkung
		ja	nein	
6	Außerbetriebnahme			
6.1	Ist sichergestellt, dass die Außerbetriebnahme durch autorisiertes und qualifiziertes Personal erfolgt?			
6.2	Wurde die Spannungsversorgung an dem außer Betrieb zu nehmenden Gerät abgeschaltet?			
6.3	Wurde die Verdrahtung an dem außer Betrieb zu nehmenden Gerät entfernt?			
	Wurde die Demontage gemäß der Demontagebeschreibung durchgeführt? → "Demontage"...Seite 44			
6.4	Ist sichergestellt, dass das außer Betrieb genommene defekte Gerät an Yaskawa zur Entsorgung in der Originalverpackung gesendet werden?			

Datum:.....Name:Unterschrift: