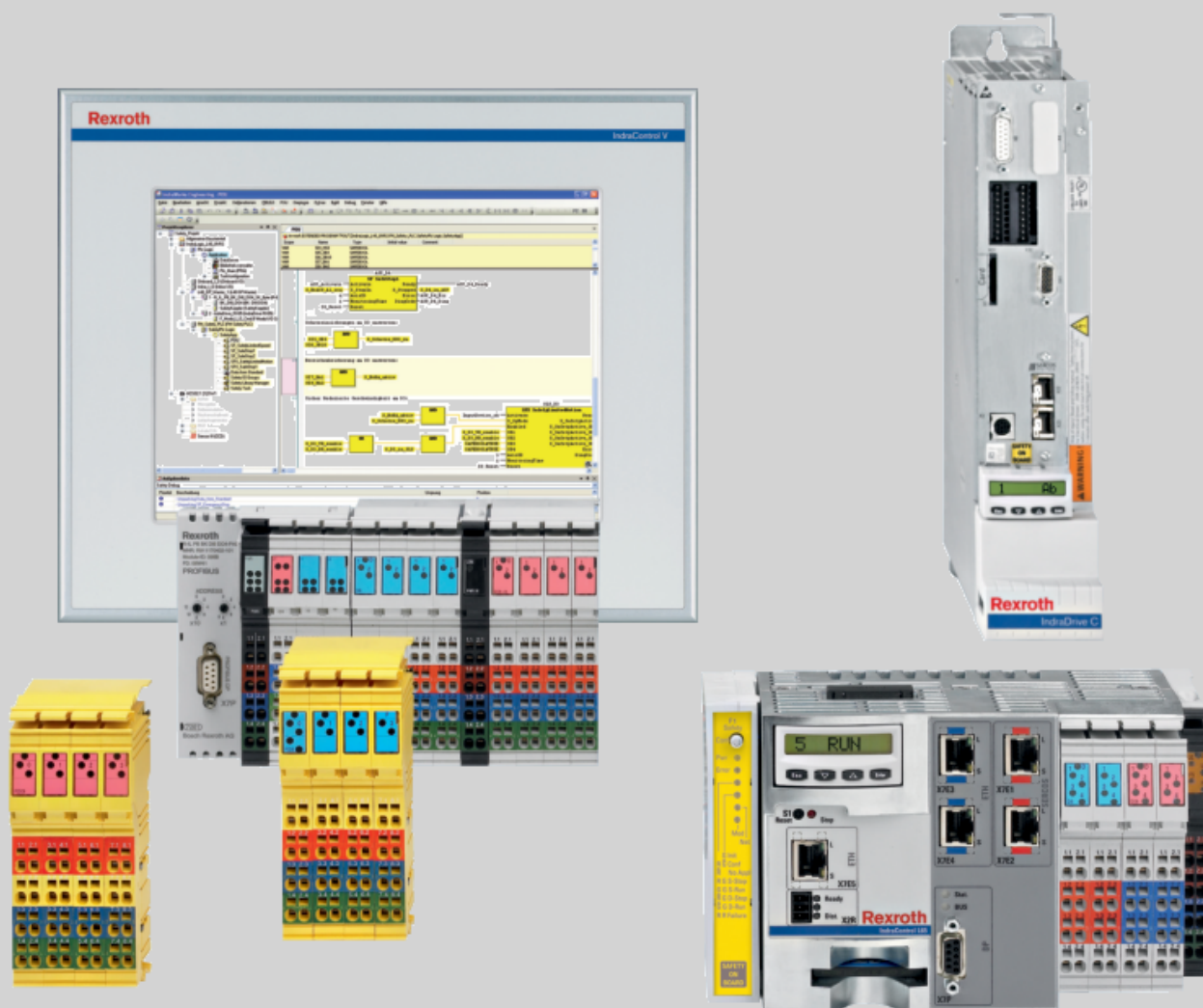


IndraMotion MTX 14VRS

SafeLogic Systemübersicht

Projektierungsbeschreibung
R911341697

Ausgabe 04



Titel	IndraMotion MTX 14VRS SafeLogic Systemübersicht
Art der Dokumentation	Projektierungsbeschreibung
Dokumentations-Type	DOK-MTX***-SL**SYS*V14-PR04-DE-P
Interner Ablagevermerk	RS-06aaa101c4b1bcdd0a6846a500e45f55-4-de-DE-8
Änderungsverlauf	Ausgabe 04, 2019-04 Siehe Tab. 1-1 "Änderungsverlauf" auf Seite 1
Schutzvermerk	© Bosch Rexroth AG 2019 Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.
Verbindlichkeit	Die angegebenen Daten dienen allein der Produktbeschreibung und sind nicht als zugesicherte Eigenschaften im Rechtssinne zu verstehen. Änderungen im Inhalt der Dokumentation und Liefermöglichkeiten der Produkte sind vorbehalten.
Redaktion	Lösungsintegration Strg.-Hardware, SPS- und Sicherheits-Steuerungen, AnSt (MiNi)

Inhaltsverzeichnis

	Seite
1 Über diese Dokumentation.....	1
1.1 Gültigkeit der Dokumentation.....	1
1.2 Gliederung der Dokumentation.....	6
1.3 Darstellung von Informationen.....	7
1.3.1 Sicherheitshinweise.....	7
1.3.2 Verwendete Symbole.....	8
1.3.3 Bezeichnungen und Abkürzungen.....	8
1.3.4 Kundenfeedback.....	8
2 Zur Sicherheit.....	9
2.1 Allgemeines.....	9
2.2 Befähigte Personen.....	9
2.3 Verwendungsbereiche der Geräte.....	9
2.4 Bestimmungsgemäße Verwendung.....	9
2.5 Allgemeine Sicherheitshinweise und Schutzmaßnahmen.....	10
2.6 Umweltgerechtes Verhalten.....	10
2.6.1 Allgemeines.....	10
2.6.2 Entsorgung.....	10
2.6.3 Werkstofftrennung.....	10
3 Einführung in die Sicherheitstechnik.....	13
3.1 Sicherheitstechnische Kenngrößen.....	13
3.1.1 Übersicht.....	13
3.1.2 Allgemeines.....	14
3.1.3 Bewertung nach IEC 61508.....	17
3.1.4 Bewertung nach IEC 62061.....	18
3.1.5 Bewertung nach ISO 13849-1.....	19
3.2 Entwurf des sicherheitsbezogenen Steuerungssystems.....	23
3.2.1 Topologie.....	23
3.2.2 Systementwurf.....	24
3.2.3 Entwurf der Teilsysteme.....	26
3.3 Bestimmung der erreichten Sicherheitsintegrität.....	28
3.4 Bestimmung der garantierten Abschaltzeit.....	28
3.4.1 Reaktionszeit.....	28
3.4.2 Überprüfung der geforderten Abschaltzeit.....	31
3.5 Adressvergabe/Namen.....	32
3.6 Beispielanwendung.....	32
3.6.1 Überblick.....	32
3.6.2 Anforderungen.....	33
3.6.3 Sicherheitsfunktion.....	34
3.6.4 Aufbau und Verdrahtung.....	35
3.6.5 Komponenten.....	35
3.6.6 Parametrierung.....	37

	Seite
3.6.7	Betrachtete Sicherheitskette..... 40
3.6.8	Bestimmen des erreichten PL-Wertes nach EN ISO 13849-1..... 40
3.6.9	Bestimmen des erreichten SIL nach EN 62061..... 40
3.6.10	Ermitteln des erforderlichen Sicherheitsabstands..... 41
3.6.11	Weitere Vorgehensweise..... 43
4	Systemübersicht..... 45
4.1	Überblick..... 45
4.2	Einsatzgebiete..... 46
4.3	Systemvoraussetzungen..... 46
4.4	Sicherheitssteuerungen..... 47
4.4.1	SafeLogic compact..... 47
4.4.2	SafeLogic..... 50
4.5	Sichere Kommunikation..... 52
4.6	Systemaufbau..... 52
4.7	IndraMotion MTX – Systemlösung..... 55
5	Sichere Bussysteme..... 57
5.1	Überblick..... 57
5.2	Allgemeines zur sicheren Datenübertragung..... 57
5.3	Hardware für das Rexroth Inline-System..... 59
5.4	Hardware für das Rexroth IndraControl S20 System..... 62
5.5	Antriebssystem Rexroth IndraDrive..... 68
5.5.1	Was versteht man unter "Integrierter Sicherheitstechnik (Safe Motion)"?..... 68
5.5.2	Unterstützte Sicherheitstechnikfunktionen..... 69
5.6	Profibus-DP bzw. PROFINET mit PROFISafe..... 73
5.6.1	Allgemeines..... 73
5.6.2	Anwendung von PROFISafe..... 74
5.6.3	Fehlerreaktion am PROFISafe..... 79
5.6.4	Diagnoseeigenschaften von PROFISafe..... 80
5.7	Sercos III mit "CIP Safety on Sercos"..... 81
5.7.1	Allgemeines..... 81
5.7.2	Anwendung von "CIP Safety on Sercos"..... 81
5.8	Sichere Querkommunikation über Ethernet..... 84
5.8.1	Allgemeines..... 84
5.8.2	Anwendung der sicheren Querkommunikation..... 85
6	Entwicklungsoberfläche..... 89
6.1	Überblick..... 89
6.2	SafeLogic compact (SafeLogic Designer)..... 89
6.2.1	Lizenz..... 89
6.2.2	Standardansichten..... 89
6.2.3	Logikprogrammierung..... 92
6.3	SafeLogic..... 94
6.3.1	Lizenz..... 94

	Seite
6.3.2 Projektstruktur.....	96
6.3.3 Logikprogrammierung.....	98
6.3.4 I/Os.....	101
7 Inbetriebnahme.....	103
7.1 Überblick.....	103
7.2 Ablauf der Installation und Inbetriebnahme.....	104
7.3 Auspacken.....	105
7.4 Montage und Installation.....	105
7.4.1 Gerätemontage des Safety-Funktionsmoduls.....	105
7.4.2 Gerätemontage der SafeLogic compact.....	106
7.4.3 Installation der Verdrahtung.....	109
7.4.4 Überprüfung.....	109
7.5 Inbetriebnahme der Komponenten.....	110
7.5.1 Vor dem Einschalten.....	110
7.5.2 Zuschalten der Versorgungsspannung.....	110
7.5.3 Funktionstest und Fehlersuche.....	110
7.5.4 Inbetriebnahme SafeLogic.....	112
7.5.5 Technische Inbetriebnahme SafeLogic compact.....	116
7.5.6 Modifikationen.....	117
8 Diagnose und Störungsbeseitigung.....	119
8.1 Diagnosekonzept.....	119
8.2 Logbuch der SafeLogic compact.....	120
8.3 Logbuch des Safety-Funktionsmoduls.....	121
8.4 Logbuch der Standardsteuerung.....	122
8.5 Gerätediagnose der Standardsteuerung.....	122
8.6 Diagnose in der Standard-SPS.....	123
8.7 Funktionsbausteine "CSosOriginator" und "ProfisafeHost".....	124
9 Service und Support.....	127
Index.....	129

1 Über diese Dokumentation

Ausgaben dieser Dokumentation

Ausgabe	Stand	Bemerkung
Ausgabe 01	2014-09	Erstausgabe
Ausgabe 02	2016-07	Überarbeitung, Ergänzungen
Ausgabe 03	2017-07	Überarbeitung der Kap. "Sichere Bussysteme", "Entwicklungsoberfläche"
Ausgabe 04	2019-04	Überarbeitung: - Überarbeitung "Anwahl der Safe Motion Sicherheitsfunktionen", siehe "Anwahl der Funktion" auf Seite 69 - Ergänzung Sicherheitsfunktionen, siehe Kap. 5.5.2 "Unterstützte Sicherheitstechnikfunktionen" auf Seite 69

Tab. 1-1: Änderungsverlauf

1.1 Gültigkeit der Dokumentation

Übersicht über Zielgruppen und Produktphasen

In der folgenden Grafik beziehen sich die umrandeten Aktivitäten, Produktphasen und Zielgruppen auf die vorliegende Dokumentation.

Beispiel: In der Produktphase "Auswahl" kann die Zielgruppe "Konstrukteur" mit Hilfe dieser Dokumentation die Aktivitäten "auswählen, zusammenstellen, auslegen und konstruieren" ausführen.

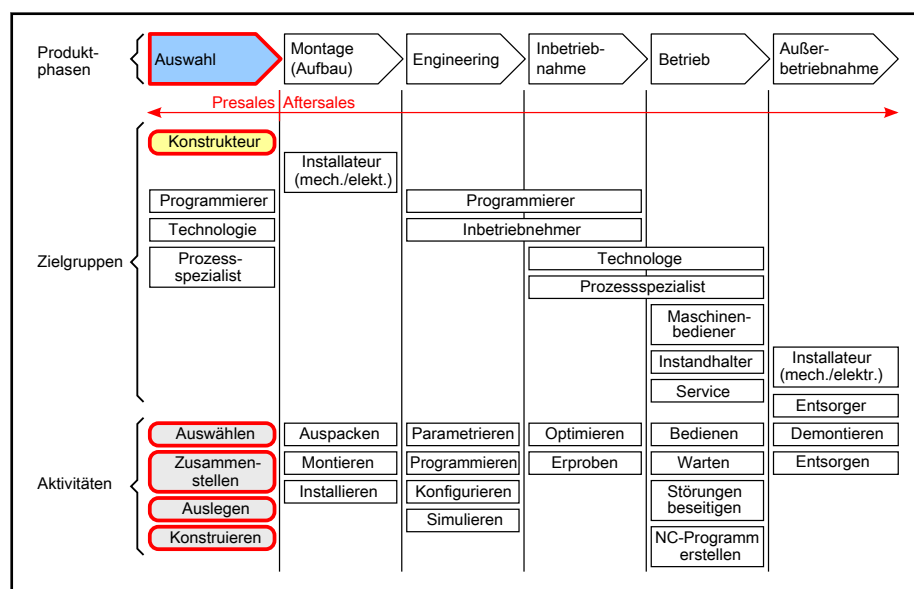


Abb. 1-1: Zuordnung der vorliegenden Dokumentation zu den Zielgruppen, Produktphasen und den Aktivitäten der Zielgruppe

Zweck

Diese Projektierungsbeschreibung stellt eine Übersicht der sicherheitstechnischen Systemlösungen von Bosch Rexroth dar. Diese Projektierungsbeschreibung beschreibt die Sicherheitssteuerung SafeLogic compact und das Safety-Funktionsmodul.

Über diese Dokumentation

Das Safety-Funktionsmodul von Bosch Rexroth ist ein Sicherheitsbauteil, das nur in Verbindung mit einer Rexroth IndraControl L Steuerung ein sicherheitsgerichtetes Steuerungssystem (IndraLogic XLC SafeLogic, IndraMotion MLC SafeLogic, IndraMotion MTX SafeLogic) bildet.

Die SafeLogic compact ist eine modular skalierbare Sicherheitssteuerung, die unabhängig von einer übergeordneten Steuerung ist.

Diese Projektierungsbeschreibung ist nur gültig in Verbindung mit anderen Betriebs-, Projektierungs- und Montageanleitungen, siehe auch nachfolgende Tabelle. Diese Projektierungsbeschreibung unterstützt den Anwender bei der Auswahl, Konfiguration und Auslegung der Sicherheitssteuerung.

Diese Projektierungsbeschreibung leitet nicht zur Bedienung der Maschine an, in die eine Sicherheitssteuerung integriert ist. Informationen hierzu enthält die Betriebsanleitung der jeweiligen Maschine.

Qualifikation Erforderliche Qualifikationen: Person, die aufgrund ihrer fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie Kenntnis der einschlägigen Normen und Bestimmungen die ihr übertragenen Arbeiten beurteilen und mögliche Gefahren erkennen kann.

Verfügbarkeit Diese Projektierungsbeschreibung ist nicht Bestandteil einer Produktlieferung.

Weiterführende Dokumente

Dokument	Materialnummer, Dokumentart	Beschreibung
IndraWorks 14VRS Software-Installation	R911344285 Inbetriebnahmebeschreibung	Die Dokumentation beschreibt den Installationsprozess von IndraWorks
IndraWorks 14VRS Engineering	R911343564 Anwendungsbeschreibung	Diese Dokumentation beschreibt die Verwendung von IndraWorks, in das sich die Rexroth Engineering-Tools integrieren
IndraWorks 14VRS SPS-Programmiersystem IndraLogic 2G	R911343570 Anwendungsbeschreibung	Diese Dokumentation beschreibt das SPS-Programmierungswerkzeug IndraLogic 2G und seine Verwendung.
IndraWorks 14VRS Basis-Bibliotheken, IndraLogic 2G	R911343918 Bibliothek	Das vorliegende Handbuch beschreibt die systemübergreifenden SPS-Bibliotheken
IndraWorks 14VRS Feldbusse	R911341484 Anwendungsbeschreibung	Die Dokumentation dient der Beschreibung der von den Systemen IndraLogic XLC, IndraMotion MLC und IndraMotion MTX unterstützten Feldbus- und lokalen Peripherieanschlüssen
Rexroth IndraWorks 14VRS HMI	R911343567 Anwendungsbeschreibung	Diese Dokumentation beschreibt die Funktionen, die Konfiguration und die Bedienung der Bedienoberflächen IndraWorks HMI Engineering und IndraWorks HMI Operation

Dokument	Materialnummer, Dokumentart	Beschreibung
IndraWorks IndraMotion Service Tool	R911341382 Anwendungsbeschreibung	Diese Dokumentation beschreibt das IndraMotion Service Tool (IMST). Das IMST ermöglicht OEMs, Endanwendern und Kundenbetreuern von überall auf ein System zuzugreifen und Ferndiagnosen zu stellen. Die folgenden Steuerungs-Varianten werden unterstützt: • IndraMotion MLC L25/L45/L65 • IndraLogic XLC L25/L45/L65/VEP
Rexroth IndraDrive Service Tools IMST/IDST	R911342651 Referenz	Die Dokumentation beschreibt das IndraMotion Service Tool (IMST) und das IndraDrive Service Tool (IDST). Diese Service Tools ermöglichen OEMs, Endanwendern und Kundenbetreuern von überall auf ein System zuzugreifen und Ferndiagnosen zu stellen
IndraWorks 14VRS Feldbus-Bibliotheken	R911343574 Bibliothek	Diese Dokumentation dient der Beschreibung der Feldbus-Bibliotheken für die Systeme IndraLogic XLC, IndraMotion MLC und IndraMotion MTX
IndraWorks SafeLogic 14VRS Die ersten Schritte	R911341519 Inbetriebnahmebeschreibung	Diese Dokumentation enthält eine Beschreibung zur Erstellung eines 14VRS Steuerungs-Projektes und zur Inbetriebnahme einer SafeLogic-Steuerung
IndraWorks SafeLogic 14VRS Projektkonfiguration	R911341693 Anwendungsbeschreibung	Diese Dokumentation beschreibt die Erstellung und Programmierung von SafeLogic Projekten in IndraWorks Engineering
IndraControl CFL01.1-F1 Safety-Funktionsmodul	R911336575 Betriebsanleitung	Diese Betriebsanleitung leitet das technische Personal des Maschinenherstellers zur sicheren Montage und Elektroinstallation des Safety-Funktionsmoduls an
IndraLogic XLC IndraMotion MLC 14VRS SafeLogic Systemübersicht	R911341695 Projektierungsbeschreibung	Diese Projektierungsbeschreibung beschreibt die Sicherheitssteuerung SafeLogic compact und das Safety- Funktionsmodul bei Einsatz mit einer IndraMotion MLC und IndraLogic XLC
IndraMotion MTX 14VRS SafeLogic Systemübersicht	R911341697 Projektierungsbeschreibung	Diese Projektierungsbeschreibung beschreibt die Sicherheitssteuerung SafeLogic compact und das Safety- Funktionsmodul bei Einsatz mit einer IndraMotion MTX
Rexroth Inline-Buskoppler für PROFINET mit digitalen Eingängen und Ausgängen R-IL PN BK DI8 DO4-PAC	R911328681 Datenblatt	Enthält die technischen Daten des Rexroth Inline-Buskopplers R-IL PN BK DI8 DO4-PAC
Rexroth Inline-Buskoppler für PROFIBUS-DP R-IL PB BK DI8 DO4/CN-PAC	R911324348 Anwendungsbeschreibung	Diese Dokumentation beschreibt den Rexroth Inline-Buskoppler R-IL PB BK DI8 DO4/CN-PAC

Über diese Dokumentation

Dokument	Materialnummer, Dokumentart	Beschreibung
Rexroth Inline-Buskoppler für PROFIBUS-DP mit digitalen Ein- und Ausgängen R-IL PB BK DI8 DO4/CN-PAC	R911324350 Datenblatt	Enthält die technischen Daten des Rexroth Inline-Buskopplers R-IL PB BK DI8 DO4/CN-PAC
Rexroth Inline-Modul mit sicheren digitalen Eingängen R-IB IL 24 PSDI 8-PAC	R911326025 Anwendungsbeschreibung	Diese Dokumentation beschreibt das Rexroth Inline-Modul R-IB IL 24 PSDI 8-PAC
Rexroth Inline-Modul mit sicheren digitalen Ausgängen R-IB IL 24 PSDO 8-PAC	R911326027 Anwendungsbeschreibung	Diese Dokumentation beschreibt das Rexroth Inline-Modul R-IB IL 24 PSDO 8-PAC
Rexroth Inline-Modul mit sicheren digitalen Ausgängen R-IB IL 24 PSDO 4/4-PAC	R911336652 Anwendungsbeschreibung	Diese Dokumentation beschreibt das Rexroth Inline-Modul R-IB IL 24 PSDO 4/4-PAC
Rexroth Inline-Modul mit sicheren digitalen Relaisausgängen R-IB IL 24 PSDOR 4-PAC	R911336650 Anwendungsbeschreibung	Diese Dokumentation beschreibt das Rexroth Inline-Modul R-IB IL 24 PSDOR 4-PAC
Rexroth IndraControl S20-Buskoppler für PROFINET	R911342783 Datenblatt	Diese Dokumentation beschreibt den Rexroth S20 PROFINET Buskoppler S20-PN-BK+
IndraControl S20-Modul mit sicheren digitalen Ausgängen S20-PSDO-8/3	R911369166 Anwendungsbeschreibung	Diese Dokumentation beschreibt das Rexroth S20-Modul S20-PSDO-8/3
IndraControl S20-Modul mit sicheren digitalen Eingängen S20-PSDI-8/4	R911369170 Anwendungsbeschreibung	Diese Dokumentation beschreibt das Rexroth S20-Modul S20-PSDI 8/4
Rexroth IndraControl S20-Buskoppler für Sercos	R911342781 Datenblatt	Diese Dokumentation beschreibt den Rexroth S20 Sercos Buskoppler S20-S3-BK+
IndraControl S20-Modul mit sicheren digitalen Ausgängen S20-SSDO-8/3	R911342481 Anwendungsbeschreibung	Diese Dokumentation beschreibt das Rexroth S20-Modul S20-SSDO-8/3
IndraControl S20-Modul mit sicheren digitalen Eingängen S20-SSDI-8/4	R911342479 Anwendungsbeschreibung	Diese Dokumentation beschreibt das Rexroth S20-Modul S20-SSDI 8/4

Dokument	Materialnummer, Dokumentart	Beschreibung
Rexroth IndraDrive Integrierte Sicherheitstechnik "Safe Torque Off" (ab MPx-16)	R911332633 Anwendungsbeschreibung	Diese Dokumentation beschreibt die in IndraDrive integrierte Sicherheitstechnik "Safe Torque Off"
Rexroth IndraDrive Integrierte Sicherheitstechnik "Safe Motion" (ab MPx-18)	R911338919 Anwendungsbeschreibung	Diese Dokumentation beschreibt die in IndraDrive integrierte Sicherheitstechnik "Safe Motion"

Tab. 1-2: Dokumentationen zu SafeLogic

Dokument	Materialnummer, Dokumentart	Beschreibung
IndraControl SafeLogic compact Designer Software	R911332748 Betriebsanleitung	Leitet das technische Personal des Maschinenherstellers zu Software-Konfiguration, Betrieb und Diagnose eines SafeLogic compact Systems mit der Software SafeLogic Designer an
IndraControl SafeLogic compact Hardware	R911332745 Betriebsanleitung	Leitet das technische Personal des Maschinenherstellers und Maschinenbetreibers zur sicheren Montage, Elektroinstallation, Inbetriebnahme sowie zur Wartung der SafeLogic compact Diagnose Gateways an
Rexroth IndraControl SafeLogic compact Diagnose Gateways	R911332751 Betriebsanleitung	Beschreibt die SafeLogic compact Diagnose Gateways und deren Funktionen im Detail
IndraControl SafeLogic compact Sercos Gateway	R911338435 Projektierungsbeschreibung	Leitet das technische Personal des Maschinenherstellers und Maschinenbetreibers zur sicheren Montage, Konfiguration, Elektroinstallation, Inbetriebnahme sowie zum Betrieb und zur Wartung des SafeLogic compact Sercos Gateways an
Sicherheitssteuerungen Netzwerk-Lösungen SafeLogic compact	R911332754 Sicherheitshinweise	Diese Sicherheitshinweise informieren den Planer, Entwickler und Betreiber sowie die Personen, die die Schutzeinrichtung in eine Maschine/Anlage einbauen, erstmals in Betrieb nehmen und bedienen

Dokument	Materialnummer, Dokumentart	Beschreibung
SLC-3-GS3S00300 SafeLogic compact Sercos Gateway	R911339569 Montageanleitung	Diese Montageanleitungen beschreiben die Montage der Module einer Sicherheitssteuerung SafeLogic compact
SLC-0-GPNT00300 SafeLogic compact Ethernet-Gateway Profinet IO	R911332744 Montageanleitung	
SLC-0-GPRO00300 SafeLogic compact Profibus Gateway	R911332743 Montageanleitung	
SLC-3-MOC000300 SafeLogic compact Motion-Control-Modul	R911343757 Montageanleitung	
SLC-3-CPU000300/ SLC-3-CPU130302/ SLC-3-CPU320302 SafeLogic compact Hauptmodule	R911332742 Montageanleitung	
SLC-3-XTDI80302/SLC-3-XTIO84302/ SLC-3-XTDS84302/SLC-0-STIO68302 SafeLogic compact Erweiterungsmodule	R911332741 Montageanleitung	
SLC-A-UE410-2RO4/ SLC-A-UE410-4RO4 SafeLogic compact Ausgangsmodule	R911332740 Montageanleitung	
SLC-A-MOC-MFSB-RX/ SLC-A-MOC-DECB-RX SafeLogic compact Geber-Anschlussboxen	R911343760 Montageanleitung	

Tab. 1-3: Dokumentationen zu SafeLogic compact

1.2 Gliederung der Dokumentation

Der erste Teil des Dokuments enthält wichtige Gebrauchs- und Sicherheitshinweise ([Kap. 2 "Zur Sicherheit" auf Seite 9](#)).

[Kap. 3 "Einführung in die Sicherheitstechnik" auf Seite 13](#) gibt eine kurze Einführung in die Sicherheitstechnik.

[Kap. 4 "Systemübersicht" auf Seite 45](#) enthält eine Übersicht über die SafeLogic Komponenten.

Das Kapitel gliedert sich in:

- Einsatzgebiete
- Systemvoraussetzungen
- Sicherheitssteuerungen

- Sichere Kommunikation
- Systemaufbau
- Systemlösungen

Kap. 5 "Sichere Bussysteme" auf Seite 57 beschreibt die sichere Datenübertragung bei Bosch Rexroth-Sicherheitssystemen.

Kap. 6 "Entwicklungsoberfläche" auf Seite 89 beschreibt die verfügbaren Entwicklungsoberflächen für Projektierung und Inbetriebnahme.

Kap. 7 "Inbetriebnahme" auf Seite 103 enthält Informationen zur Inbetriebnahme der SafeLogic Komponenten.

Kap. 8 "Diagnose und Störungsbeseitigung" auf Seite 119 beschreibt Möglichkeiten zur Diagnose und Störungsbeseitigung für ein Sicherheitssystem.

Kap. 9 "Service und Support" auf Seite 127 enthält Informationen zu unserem Kundendienst-Helpdesk.

1.3 Darstellung von Informationen

1.3.1 Sicherheitshinweise

Die Sicherheitshinweise, soweit sie in der vorliegenden Anwendungsdokumentation vorhanden sind, beinhalten bestimmte Signalwörter ("Gefahr", "Warnung", "Vorsicht", "Hinweis") und ggf. eine Signalgrafik (nach ANSI Z535.6-2006).

Das Signalwort soll die Aufmerksamkeit auf den Sicherheitshinweis lenken und bezeichnet die Schwere der Gefährdung.

Die Signalgrafik (Warndreieck mit Ausrufezeichen), welche den Signalwörtern "Gefahr", "Warnung" und "Vorsicht" vorangestellt wird, weist auf Gefährdungen für Personen hin.

Sicherheitshinweise in dieser Dokumentation werden wie folgt dargestellt:

GEFAHR

Bei Nichtbeachtung dieses Sicherheitshinweises **werden** Tod oder schwere Körpervverletzung eintreten.

WARNUNG

Bei Nichtbeachtung dieses Sicherheitshinweises **können** Tod oder schwere Körpervverletzung eintreten.

VORSICHT

Bei Nichtbeachtung dieses Sicherheitshinweises können mittelschwere oder leichte Körpervverletzung eintreten.

HINWEIS

Bei Nichtbeachtung dieses Sicherheitshinweises können Sachschäden eintreten.

1.3.2 Verwendete Symbole

Hinweis Hinweise werden wie folgt dargestellt:



Das ist ein Hinweis für den Anwender.

Tipp Tipps werden wie folgt dargestellt:



Das ist ein Tipp für den Anwender.

1.3.3 Bezeichnungen und Abkürzungen

Begriff	Erklärung
IndraWorks Engineering Framework	Projektierungs- und Inbetriebnahmetool von Bosch Rexroth
SafeLogic Designer	Projektierungs- und Inbetriebnahmetool von Bosch Rexroth für die SafeLogic compact Komponenten
DTM	Device Type Manager Ist in der Automatisierungstechnik ein herstellerübergreifendes Konzept, welches die Parametrierung von Feldgeräten verschiedener Hersteller mit nur einem Programm ermöglicht
IEC	International Electrotechnical Commission (Normungsgremium für Elektrotechnik)
IEEE	Institute of Electrical and Electronics Engineers
DIN	Deutsches Institut für Normung e. V.
ISO	Internationale Organisation für Normung
IndraDrive	Antriebsregelgerät
Sercos	Sercos (Serial Realtime Communication System) interface ist eine weltweit genormte digitale Schnittstelle zur Kommunikation zwischen Steuerungen und Antrieben

Tab. 1-4: Verwendete Bezeichnungen und Abkürzungen

1.3.4 Kundenfeedback

Anregungen, Wünsche oder Verbesserungen von unseren Kunden haben bei uns einen hohen Stellenwert. Senden Sie uns Ihre Anmerkungen zu den Dokumentationen per E-Mail an Feedback.Documentation@boschrexroth.de. Sie können direkt im elektronischen PDF-Dokument Kommentare einfügen und uns die PDF-Datei zusenden.

2 Zur Sicherheit

2.1 Allgemeines

Dieses Kapitel dient Ihrer Sicherheit und der Sicherheit der Anlagenbediener.

Bitte lesen Sie dieses Kapitel sorgfältig, bevor Sie mit der Sicherheitssteuerung oder mit einer durch eine Sicherheitssteuerung geschützten Maschine arbeiten.

2.2 Befähigte Personen

Eine Sicherheitssteuerung darf nur von befähigten Personen montiert, in Betrieb genommen und gewartet werden.

Befähigt ist, wer ...

- über eine geeignete technische Ausbildung verfügt

und

- vom Maschinenbetreiber in der Bedienung und den gültigen Sicherheitsrichtlinien unterwiesen wurde

und

- Zugriff auf die Betriebs-, Projektierungs- und Montageanleitungen zur Sicherheitssteuerung und diese Betriebs-, Projektierungs- und Montageanleitungen gelesen und zur Kenntnis genommen hat

und

- Zugriff auf die Betriebsanleitungen zu den mit der Sicherheitssteuerung verbundenen Schutzeinrichtungen (z. B. Lichtgitter) und diese Betriebsanleitungen gelesen und zur Kenntnis genommen hat

2.3 Verwendungsbereiche der Geräte

Die modulare Sicherheitssteuerung SafeLogic compact sowie das Safety-Funktionsmodul CFL01.1-F1 sind einsetzbar ...

- gemäß IEC 61 508 bis SIL3
- gemäß EN 62 061 bis SILCL3
- gemäß EN ISO 13 849-1 bis Kategorie 4 und Performance Level e

Der tatsächlich erreichte Sicherheitsgrad hängt von der Außenbeschaltung, der Ausführung der Verdrahtung, der Parametrierung, der Wahl der Befehlsgeber und deren Anordnung an der Maschine ab.

2.4 Bestimmungsgemäße Verwendung



Die Sicherheitssteuerungen erfüllen gemäß der Fachgrundnorm "Störaussendung" die Voraussetzung der Klasse A (Industrieanwendungen).

Die Sicherheitssteuerungen sind daher nur für den Einsatz im industriellen Umfeld und nicht im Privatbereich geeignet.

HINWEIS

Sachschäden an Komponenten der Sicherheitssteuerungen!

Die Sicherheitssteuerungen dürfen nur in ihren spezifizierten Betriebsgrenzen (Spannung, Temperatur etc.) verwendet werden.

Bei jeder anderen Verwendung sowie bei Veränderungen am Gerät – auch im Rahmen von Montage und Installation – verfällt jeglicher Gewährleistungsanspruch gegenüber der Bosch Rexroth AG.

Die externe Spannungsversorgung der Geräte muss gemäß EN 60 204 einen kurzzeitigen Netzausfall von 20 ms überbrücken. Geeignete PELV- und SELV-fähige Netzteile sind bei Bosch Rexroth als Zubehör erhältlich.

2.5 Allgemeine Sicherheitshinweise und Schutzmaßnahmen

Beachten Sie die Sicherheitshinweise und Schutzmaßnahmen!

Beachten Sie die nachfolgenden Punkte, um die bestimmungsgemäße Verwendung der Sicherheitssteuerung zu gewährleisten:

- Beachten Sie bei Montage, Installation und Anwendung der Sicherheitssteuerung die in Ihrem Land gültigen Normen und Richtlinien
- Für Einbau und Verwendung der Sicherheitssteuerung sowie für die Inbetriebnahme und wiederkehrende technische Überprüfung gelten die nationalen und internationalen Rechtsvorschriften, insbesondere
 - die Maschinenrichtlinie 2006/42/EG
 - die EMV-Richtlinie 2004/108/EG
 - die Arbeitsmittelbenutzungsrichtlinie 2009/104/EG
 - die Niederspannungsrichtlinie 2006/95/EG
 - die Unfallverhütungsvorschriften und Sicherheitsregeln
- Hersteller und Betreiber der Maschine, an der eine Sicherheitssteuerung verwendet wird, müssen alle geltenden Sicherheitsvorschriften und -regeln in eigener Verantwortung mit der für Sie zuständigen Behörde abstimmen und einhalten
- Die Hinweise, insbesondere die Prüfhinweise der Betriebs-, Projektierungs- und Montageanleitungen (wie z. B. zum Einsatz, zur Montage, Installation oder Einbindung in die Maschinensteuerung), sind unbedingt zu beachten
- Die Prüfungen sind von befähigten Personen bzw. von eigens hierzu befugten und beauftragten Personen durchzuführen und in jederzeit von Dritten nachvollziehbarer Weise zu dokumentieren

2.6 Umweltgerechtes Verhalten

2.6.1 Allgemeines

Die Sicherheitssteuerungen sind so konstruiert, dass die Umwelt so wenig wie möglich belastet wird. Die Sicherheitssteuerungen verbrauchen nur ein Minimum an Energie und Ressourcen.

- Handeln Sie auch am Arbeitsplatz immer mit Rücksicht auf die Umwelt

2.6.2 Entsorgung

Die Entsorgung unbrauchbarer oder irreparabler Geräte sollte immer gemäß den jeweils gültigen landesspezifischen Abfallbeseitigungsvorschriften (z. B. Europäischer Abfallschlüssel 16 02 14) erfolgen.

Gerne sind wir Ihnen bei der Entsorgung dieser Geräte behilflich. Sprechen Sie uns an.

2.6.3 Werkstofftrennung

Die Werkstofftrennung darf nur von befähigten Personen ausgeführt werden!

Bei der Demontage der Geräte ist Vorsicht geboten. Es besteht die Möglichkeit von Verletzungen.

Bevor Sie die Geräte dem umweltgerechten Recycling-Prozess zuführen können, ist es notwendig, die verschiedenen Werkstoffe des Safety-Funktionsmoduls voneinander zu trennen.

- Trennen Sie das Gehäuse von den restlichen Bestandteilen (insbesondere von der Leiterplatte)
- Führen Sie die getrennten Bestandteile dem entsprechenden Recycling zu (siehe nachfolgende Tabelle)

Bestandteile	Entsorgung
Produkt • Gehäuse • Leiterplatten, Kabel, Stecker und elektrische Verbindungsstücke	Kunststoff-Recycling Elektronik-Recycling
Verpackung • Karton, Papier	Papier- und Kartonage-Recycling

Tab. 2-1: Übersicht der Entsorgung nach Bestandteilen

3 Einführung in die Sicherheitstechnik

3.1 Sicherheitstechnische Kenngrößen

3.1.1 Übersicht

Im Hinblick auf den Steuerungsteil der Maschine oder Anlage bezieht sich die Projektierung auf die Automatisierungsaufgaben selbst, die zusätzlichen prozessbedingten Überwachungsaufgaben und die Aufgaben zur Funktionalen Sicherheit der Maschine.

Dieses Kapitel beschäftigt sich ausschließlich mit den Aufgaben zur funktionalen Sicherheit und beschreibt die vorbereitenden Aktivitäten zur Realisierung des Sicherheitssystems bzw. die Ermittlung der erforderlichen Strukturen und Parameter, die dann für die Umsetzung mit dem Engineeringtool die entsprechenden Eingangsgrößen liefern. Das Engineeringtool selbst wird beschrieben in [Kap. 6 "Entwicklungsoberfläche"](#) auf Seite 89.

Planung der funktionalen Sicherheit

Zu Beginn der Projektierung des Sicherheitssystems steht die Erstellung eines Plans der funktionalen Sicherheit. Die Planung erfasst alle Management-Aktivitäten und technischen Aktivitäten, beginnend von der Konzepterstellung bis hin zur Validierung.

Im Rahmen der Planung der funktionalen Sicherheit sind unter anderem:

- alle für ihre Maschine oder Anlage zutreffenden Normen und Vorschriften festzustellen
- die Grenzen der Maschine oder Anlage zu bestimmen. Dies sind:
 - räumliche Grenzen
 - Einsatzort
 - geplante Lebensdauer
 - Funktionen und Betriebsarten
 - zu erwartende Fehlfunktionen und Störungen
 - vorhersehbare Fehlanwendungen
- eine Risikoanalyse durchzuführen und auf deren Basis nachfolgend eine Risikobewertung. Daraus resultieren der erforderliche Safety-Integritätslevel SIL bei Anwendung von IEC 61508/IEC 62061 oder der erforderliche Performance Level PL bei Anwendung von EN ISO 13849-1 für die Sicherheitsfunktionen
- alle Schutzmaßnahmen zur Risikominderung festzulegen. Dies sind:
 - Sicheres Gestalten
 - Technische Schutzmaßnahmen
 - Benutzerinformation über Restrisiken
- alle Sicherheitsfunktionen die von dem Sicherheitssystem auszuführen sind, zu benennen und zu beschreiben
- alle Schutzeinrichtungen auszuwählen und ihre Anwendung unter Berücksichtigung der zutreffenden Normen festzulegen
- für jede Sicherheitsfunktion die Reaktionszeitanforderungen zu ermitteln, unter Berücksichtigung der vorgesehenen Sicherheitsabstände
- alle Sicherheitsmaßnahmen zum Stillsetzen im Notfall (Not-Halt, Not-Aus) auszuwählen und zu konzipieren

3.1.2 Allgemeines

Prüfgrundlagen/Normen

Als allgemeine Basisnorm zur funktionalen Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Systeme gilt international die siebenteilige Normenreihe IEC 61508, die auch der Entwicklung und Validierung des Bosch Rexroth Sicherheitssystems und dessen Komponenten zugrunde liegt.

Für die Maschinenindustrie wurde als Sektornorm zur IEC 61508 die IEC 62061 veröffentlicht, die im Umfeld von Maschinen speziell die funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme behandelt.

Parallel dazu entstand als Nachfolger der europäischen EN 954 (Teile 1 und 2) die internationale ISO 13849 (Teile 1 und 2) die sich mit der Gestaltung und Validierung sicherheitsbezogener Teile von Maschinensteuerungen befasst.

Alle Maschinen, die innerhalb des europäischen Wirtschaftsraumes in Verkehr gebracht werden, müssen die EG-Maschinenrichtlinie einhalten. Beide Normen, IEC 62061 und ISO 13849-1 sind in ihrer europäischen Umsetzung als EN 62061 bzw. EN ISO13849-1 im Amtsblatt der europäischen Union gelistet. Ihre Anwendung gilt als Übereinstimmung mit den grundlegenden Anforderungen der Maschinenrichtlinie (Vermutungswirkung). Diesbezüglich sind beide Normen gleichberechtigt anwendbar. Sie enthalten beide eine Tabelle zur Entscheidungsfindung hinsichtlich ihrer Eignung zur Realisierung einer Anwendung.

Im Gegensatz zur IEC 62061 behandelt ISO13849-1 auch nicht elektrische, sicherheitsbezogene Teile und ermöglicht damit durchgängig technologieübergreifende Betrachtungen. Neben diesem zwingenden Argument zur Wahl der ISO13849-1 zur Realisierung eines sicherheitsbezogenen Systems kann deren vereinfachter Quantifizierungsansatz, unter Verwendung der vorgesehenen und aus der EN 954-1 bekannten Architekturen, genannt werden. IEC 62061 ist durch ihre Nähe zur Basisnorm IEC 61508 eher prädestiniert zur Betrachtung komplexer programmierbarer elektronische Systeme und geeignet für alle Architekturen. Die IEC 61508 ist bei Anwendungen außerhalb des Maschinenbereichs in Betracht zu ziehen.

Risikobetrachtung

Zu Beginn der Sicherheitsbetrachtung einer Maschine ist nach ISO 12100-1 (Sicherheit von Maschinen - Grundbegriffe, allgemeine Gestaltungsleitsätze - Teil 1: Grundsätzliche Terminologie, Methodologie) eine Risikoanalyse und Risikobewertung gefordert. Dies ist Basis einer Strategie zur Risikominde- rung mit dem Ziel, das Risiko durch Schutzmaßnahmen auf ein tolerierbares Maß zu reduzieren.

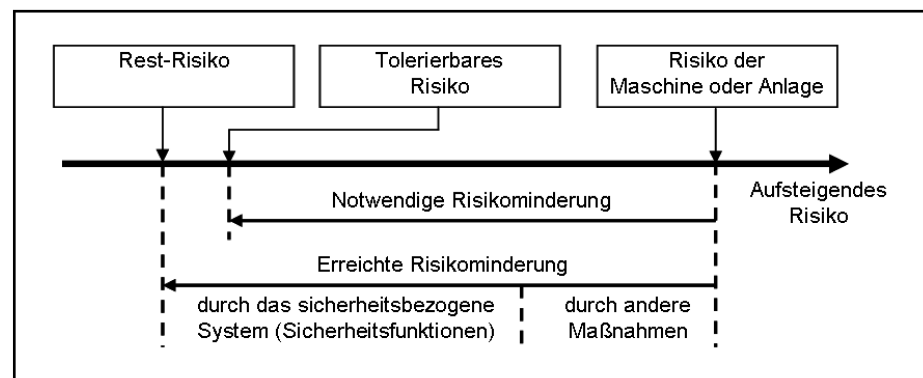


Abb. 3-1: Risikominderung

Sicherheitsfunktionen

Neben anderen Schutzmaßnahmen wird die Risikominderung durch Realisierung von Sicherheitsfunktionen erreicht, die durch das sicherheitsbezogene Steuerungssystem technisch umgesetzt werden.

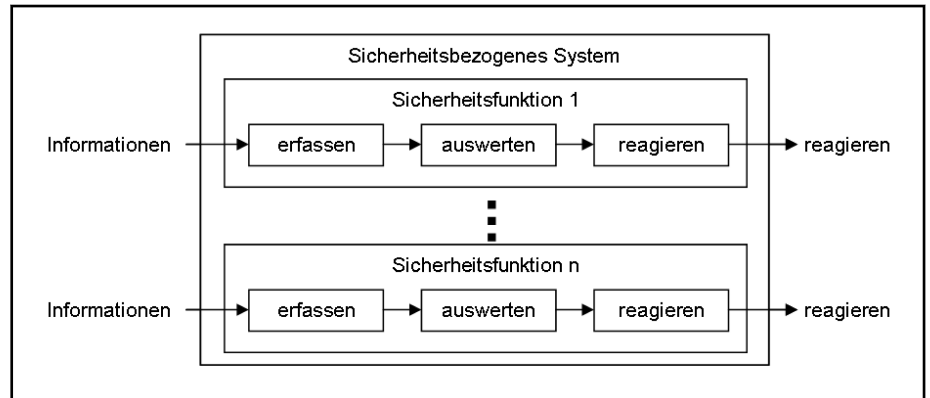


Abb. 3-2: Sicherheitsfunktionen im sicherheitsbezogenen Steuerungssystem

Für jede einzelne Sicherheitsfunktion wird die erforderliche Qualität der Risikoreduzierung je nach der herangezogenen Norm durch unterschiedliche sicherheitstechnische Kenngrößen charakterisiert.

Neben ihrer Funktion hat die Sicherheitsfunktion folgende Eigenschaften:

- Ihr Ausfall führt zu einer unmittelbaren Erhöhung des Risikos
- die Sicherheitsfunktion ist durch ihre Sicherheitsintegrität gekennzeichnet, d. h. die Wahrscheinlichkeit, dass das sicherheitsbezogene Steuerungssystem die Sicherheitsfunktion unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt. Die wesentliche Kenngröße für die Sicherheitsintegrität ist der Ausfallgrenzwert, d. h. der Grenzwert der Wahrscheinlichkeit gefährbringender Ausfallarten. Der Ausfallgrenzwert gilt für die gesamte Sicherheitsfunktion
- die Sicherheitsfunktion erstreckt sich von einer Eingangsschnittstelle bis zu einer Ausgangsschnittstelle des sicherheitsbezogenen Steuerungssystems
- Ihre technische Umsetzung wird in Teilsysteme gegliedert

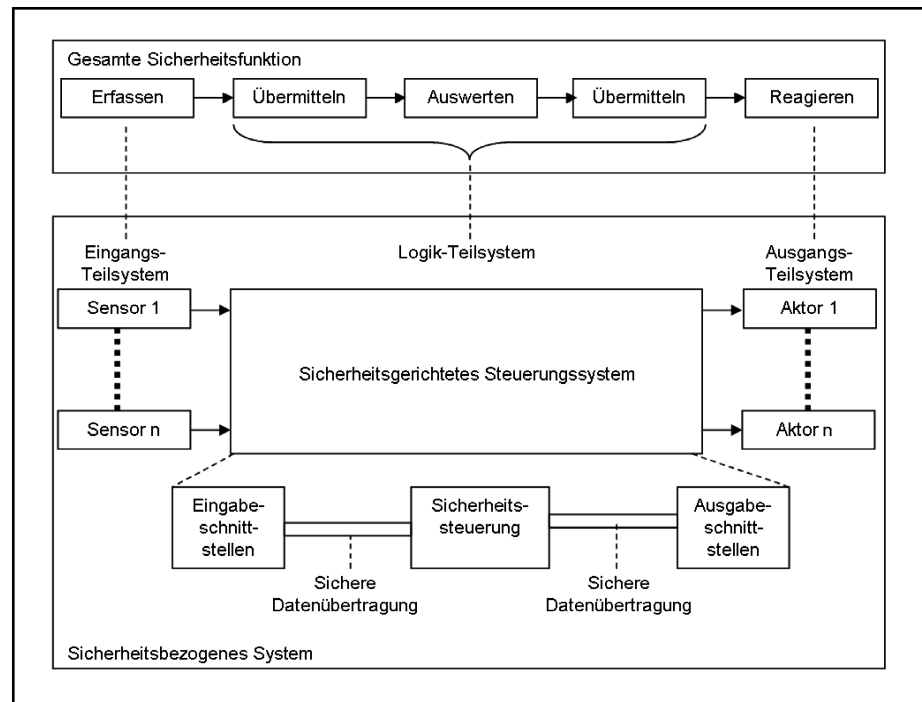


Abb. 3-3: Umsetzung der Sicherheitsfunktion im sicherheitsbezogenen System

Für jede Sicherheitsfunktion ist die bei der Risikoanalyse und Risikobewertung festgelegte Sicherheitsintegrität zu gewährleisten.

Für die bei einer Sicherheitsfunktion üblicherweise vorhandenen Teilsysteme wird der Ausfallgrenzwert nach folgender Konvention verteilt:

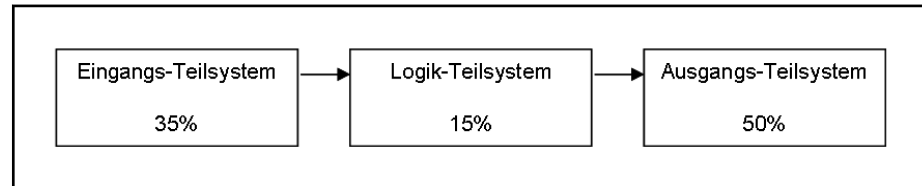


Abb. 3-4: Aufteilung des Ausfallgrenzwertes

Die Sicherheitsintegrität einer Sicherheitsfunktion verringert sich in Abhängigkeit von der technischen Umsetzung des sicherheitsbezogenen Systems bzw. seiner Teilsysteme im Laufe der Zeit, z. B. durch Verschleiß.

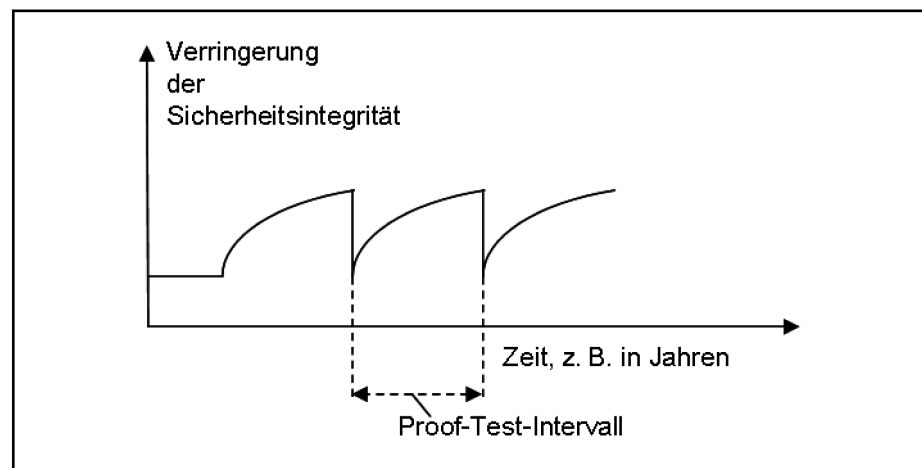


Abb. 3-5: Proof-Test-Intervall

Für jede Sicherheitsfunktion muss die maximale Gebrauchsdauer der einzelnen Teilsysteme (Zeit, in der das Teilsystem im Einsatz sein darf) und das vorgegebene Proof-Test-Intervall berücksichtigt werden.

Nach Ablauf des Proof-Test-Intervalls ist ein Proof-Test durchzuführen. Der Proof-Test kann Fehler oder eine Verschlechterung im Sicherheitssystem und seinen Teilsystemen erkennen. Durch entsprechende Maßnahmen kann das sicherheitsbezogene System dann in einen Auslieferungszustand gebracht werden.

3.1.3 Bewertung nach IEC 61508

IEC 61508 stellt den Wert der Sicherheitsintegrität durch vier Integritätslevel SIL1 (niedrigste Stufe) bis SIL4 (höchste Stufe) dar.

In der allgemeinen Automationstechnik und im Maschinenbereich sind nur die Integritätslevel SIL1 bis SIL3 relevant.

Um für eine Sicherheitsfunktion den in der Risikoanalyse ermittelten notwendigen SIL zu erreichen, müssen von dem sicherheitsgerichteten System folgende Anforderungen erfüllt sein:

1. Alle an der Ausführung der Sicherheitsfunktion beteiligten Teilsysteme müssen einzeln alle Anforderungen der IEC 61508 für den erforderlichen SIL erfüllen. Dies bezieht sich insbesondere auf die Anforderungen zur Vermeidung und Beherrschung von systematischen Fehlern.
2. Die Wahrscheinlichkeit unentdeckter, gefährlicher Ausfälle der gesamten Sicherheitsfunktion muss kleiner als der vorgegebene Ausfallgrenzwert für den erforderlichen SIL sein.

SIL3 nach IEC 61508

Das Safety-Funktionsmodul und die SafeLogic compact sind für den Einsatz in Anwendungen bis SIL3 nach IEC 61508 geeignet.

Die Gebrauchsdauer des Safety-Funktionsmoduls und der SafeLogic compact sind für einen Zeitraum von 20 Jahren ausgelegt. In dieser Zeit (ausgehend vom Herstelldatum) ist kein Proof-Test erforderlich. Nach Ablauf dieser Zeit ist das Safety-Funktionsmodul und die SafeLogic compact durch ein neues Gerät zu ersetzen.

Der Ausfallgrenzwert ist nach IEC 61508 abhängig von der Betriebsart der Sicherheitsfunktion. IEC61508 unterscheidet die Betriebsart mit niedriger Anforderungsrate (nicht mehr als eine Anforderung pro Jahr) und die Betriebsart mit hoher (mehr als eine Anforderung pro Jahr) oder kontinuierlicher Anforderungsrate.

Je nach SIL sind für die gesamte Sicherheitsfunktion festgelegt:

SIL	PFD _{avg}
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$

PFD_{avg} mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion

Tab. 3-1: Ausfallgrenzwerte für niedrige Anforderungsrate

SIL	PFH
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

PFH mittlere Häufigkeit eines gefahrbringenden Ausfalls pro Stunde

Tab. 3-2: Ausfallgrenzwerte für hohe oder kontinuierliche Anforderungsrate

Für die vorgesehene Umsetzung der Sicherheitsfunktion muss also in Abhängigkeit von der Betriebsart die Ausfallwahrscheinlichkeit für die gesamte Sicherheitsfunktion unter Berücksichtigung aller Teilsysteme ermittelt werden. Diese Ausfallwahrscheinlichkeit muss kleiner als der Ausfallgrenzwert für den angestrebten SIL sein.

In der allgemeinen Automationstechnik und im Maschinenbereich liegt in der Regel eine Betriebsart mit hoher oder kontinuierlicher Anforderungsrate vor. Für diesen Fall addieren Sie die Häufigkeit eines gefahrbringenden Ausfalls (pro Stunde) aller an der Sicherheitsfunktion beteiligten Teilsysteme entsprechend der folgenden allgemeinen Formel:

$$PFH_D = \sum_1^n PFH_{DS} + \sum_1^m PFH_{DSDI} + PFH_{DSIS} + \sum_1^i PFH_{DSDO} + \sum_1^k PFH_{DA}$$

PFH_D Wahrscheinlichkeit eines gefahrbringenden Ausfalls (pro Stunde) der gesamten Sicherheitsfunktion

PFH_{DS} PFH-Wert eines an der Sicherheitsfunktion beteiligten Sensors

PFH_{DSDI} PFH-Wert eines an der Sicherheitsfunktion beteiligten Eingangsgeräts

PFH_{DSIS} PFH-Werte der Sicherheitssteuerung und der sicheren Übertragung

PFH_{DSDO} PFH-Wert eines an der Sicherheitsfunktion beteiligten sicheren Ausgangsgeräts

PFH_{DA} PFH-Wert eines an der Sicherheitsfunktion beteiligten Aktors

Abb. 3-6: Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde

Diese Berechnung muss für jede Sicherheitsfunktion durchgeführt werden. Bei Sicherheitsfunktionen mit niedriger Anforderungsrate berechnen Sie den Wert PFD_D auf die gleiche Weise.

Entnehmen Sie die Ausfallraten der sicherheitsbezogenen Komponenten den Gerätehandbüchern.

Die Ausfallwahrscheinlichkeiten von Standardkomponenten werden bei der Betrachtung des Ausfallgrenzwertes einer Sicherheitsfunktion nicht berücksichtigt, da die Ausfallwahrscheinlichkeiten keinen sicherheitsrelevanten Beitrag zur Umsetzung der Sicherheitsfunktion leisten.

3.1.4 Bewertung nach IEC 62061

Als Sektornorm zur IEC 61508 verlangt IEC 62061 die gleiche, wie oben beschriebene Betrachtungsweise.

Auch hier ist der Zielparameter der Safety Integrity Level SIL. Aufgrund ihres auf Maschinen eingeschränkten Anwendungsbereichs der Norm kommen nur SIL1 bis SIL3 in Betracht. Die jeweils geforderten Ausfallgrenzwerte entsprechen denen der IEC 61508, es wird jedoch nur die Betriebsart mit hoher oder kontinuierlicher Anforderungsrate berücksichtigt. Die Betriebsart mit niedriger

Anforderungsrate wird für die Anwendung von sicherheitsbezogenen Systemen an Maschinen als nicht relevant betrachtet.

Wesentliche Unterschiede bestehen teilweise in der Terminologie und einem streng systematisch gegliederten Ablauf zu dem Entwurf des sicherheitsgerichteten Steuerungssystems (SRECS = Safety-Related Electrical Control System), beginnend mit der Erstellung eines Sicherheitsplans bis hin zur Durchführung der Gesamt-Validierung. Die für jede Phase dieses Ablaufs formulierten Anforderungen der Norm sind entsprechend des angestrebten SIL zu erfüllen.

Als SILCL (SIL Claim Limit) bezeichnet IEC 62061 die SILAnspruchsgrenze für ein Teilsystem. Dabei handelt es sich um den maximalen SIL, der für ein SRECS-Teilsystem zur Umsetzung einer Sicherheitsfunktion (SRCF = Safety-Related Control Function) in Bezug auf vorgegebene strukturelle Einschränkungen und systematische Sicherheitsintegrität beansprucht werden kann. In diesem Sinne erfüllen das Safety-Funktionsmodul und die SafeLogic compact den SILCL für SIL3.

Bei der Bewertung eines SRECS nach IEC 62061 können für das Safety-Funktionsmodul und die SafeLogic compact die oben genannten sicherheitsbezogenen Kennwerte angesetzt werden.

3.1.5 Bewertung nach ISO 13849-1

Die Bewertung eines sicherheitsbezogenen Steuerungssystems oder sicherheitsbezogener Teile einer Steuerung (SRP/CS) nach ISO 13849-1 verwendet den Performance Level PL als Bezugsgröße.

Wie der SIL ist der PL ein Maß für die Qualität der Risiko-Reduzierung einer Sicherheitsfunktion und die Sicherheitsintegrität der steuerungstechnischen Umsetzung. Die Norm definiert 5 verschiedene PL-Stufen (a bis e), die jeweils mit einem Wertebereich der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde korrespondierten.

Performance Level PL	mittlere Häufigkeit eines gefahrbringenden Ausfalls pro Stunde (PFH in 1/h)
a	$\geq 10^{-5}$ bis $< 10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ bis $< 10^{-5}$
c	$\geq 10^{-6}$ bis $< 3 \cdot 10^{-6}$
d	$\geq 10^{-7}$ bis $< 10^{-6}$
e	$\geq 10^{-8}$ bis $< 10^{-7}$

Tab. 3-3: Performance Level

Für jede Sicherheitsfunktion wird als Resultat der Risikobewertung der erforderliche Performance Level PL_r (r = required) festgelegt.

Der von den sicherheitsbezogenen Teilen der Steuerung für diese Sicherheitsfunktion zu erreichende PL bestimmt sich aus:

- der zahlenmäßigen Bestimmung der Ausfallwahrscheinlichkeit ($MTTF_d$ = Mean Time To Dangerous Failure)
- der Wirksamkeit der Diagnose (Selbsttests) = DC_{avg} (average diagnostic coverage = Diagnosedeckungsgrad)
- der Fehlertoleranz der Struktur mit Bezug zu den Kategorien der EN 954-1

Das Säulendiagramm der ISO13849 ist ein einfaches graphisches Verfahren zur Bestimmung des PL-Wertes. Das Säulendiagramm beruht auf komplexen Berechnungen und Abschätzungen zur sicheren Seite.

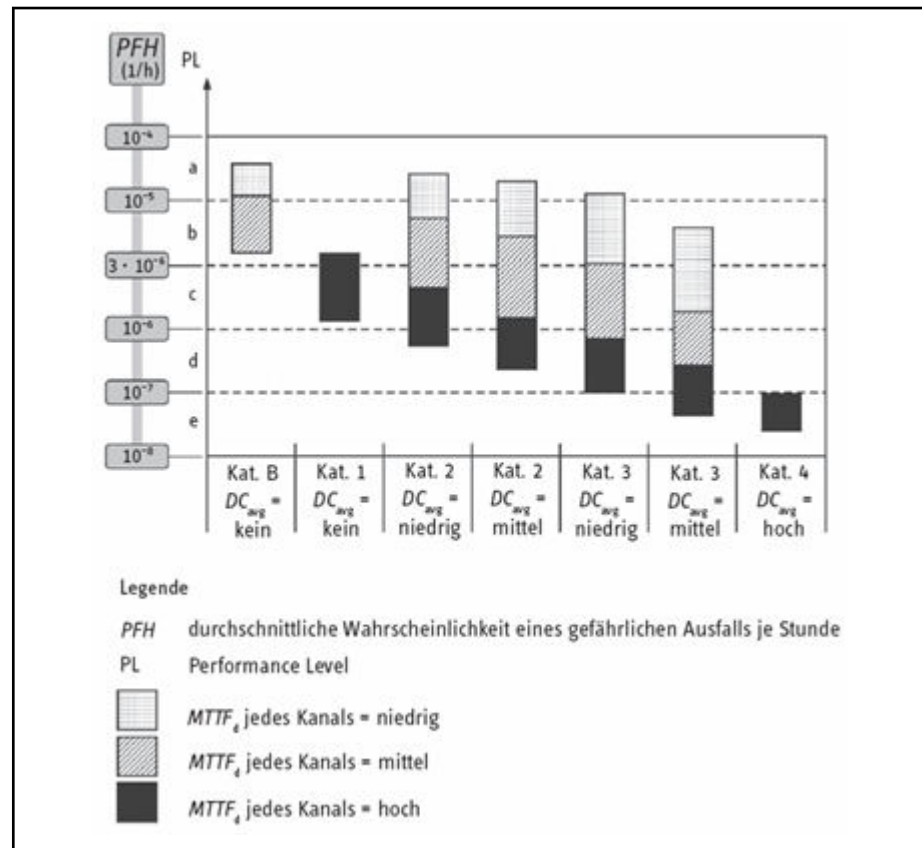


Abb. 3-7: Säulendiagramm zur PL-Bestimmung

Vorgehensweise:

1. Bestimmen Sie die relevante Säule auf der horizontalen Achse durch Einbeziehen der erreichten Kategorie und der erreichten DC_{avg} -Klasse.
2. Die Höhe der von den SRP/CS erreichten $MTTF_d$ auf der ausgewählten Säule legt den auf der vertikalen Achse abzulesenden PL fest.

Mit dieser Methode ist auch ohne genaue quantitative Daten eine schnelle qualitative Abschätzung des erreichten PL möglich. Falls genauere PFH-Werte gefragt sind, bietet die Norm in ihrem Anhang K eine Numerische Darstellung des Säulendiagramms an.

Die Verwendung des Säulendiagramms setzt allerdings noch einige Bedingungen voraus:

- Bei den Kategorien 2, 3 und 4 werden ausreichende Maßnahmen gegen Fehler gemeinsamer Ursache (Common Cause Fehler = CCF) vorausgesetzt. ISO 13849-1 bietet dazu eine Checkliste aus acht wichtigen Gegenmaßnahmen an, die mittels eines Punkte-Schemas unterschiedlich bewertet werden. Aus erreichbaren 100 Punkten fordert ISO 13849-1 für die Kategorien 2, 3 und 4 eine Mindestsumme von 65 Punkten und setzt dies einer Verschlechterung der $MTTF_d$ um 2 % gleich. Diesem Faktor wird implizit in dem Säulendiagramm Rechnung getragen
- Als Gebrauchsdauer für das SRP/CS werden 20 Jahre unterstellt. Verschleißbehaftete Bauteile, die diese Bedingung nicht erfüllen, müssen vorsorglich zu einem festgelegten Zeitpunkt ausgetauscht werden

- Bei den Säulen für Kategorie 2 wird unterstellt, dass die Testhäufigkeit mindestens 100-mal größer ist als die mittlere Häufigkeit der Anforderung der Sicherheitsfunktion und dass außerdem die Testeinrichtung mindestens halb so zuverlässig ist wie die Logik
- Außer dem quantitativen Aspekt der Ausfallwahrscheinlichkeit müssen zum Erreichen eines bestimmten PL auch qualitative Aspekte beachtet werden. Zu diesen Aspekten gehören systematische Ausfälle und Softwarefehler

Die vorstehenden Betrachtungen beziehen sich auf eine SRP/CS, die sich als ganzes auf eine Kategorie bzw. Architektur mit einem vorgesehenen PL abbilden lässt. Im Prinzip gilt das auch für die Zusammenschaltung von Subsystemen mit jeweils dem gleichen PL, jeweils unter Berücksichtigung der genauen Definition des Anteils eines Subsystems an der Sicherheitsfunktion und der genauen Definition der Schnittstellen an die weitere Subsysteme angeschlossen werden können. Auch für die Zusammenschaltung mit unterschiedlichen PL-Werten bietet die Norm Verfahren zur Bestimmung des resultierenden PL einer Sicherheitsfunktion.

Liegen für alle Subsysteme die PFH-Werte vor, so kann daraus durch Aufaddieren der für den Gesamt-PL relevante Wert berechnet werden. Die PFH-Werte können dabei auch nach IEC 61508 oder IEC 62061 berechnet sein.

Da alle Subsystem-PL immer mindestens so groß sind wie der Gesamt-PL, ist auch gewährleistet, dass bei der Kombination alle Maßnahmen zu nicht quantifizierbaren, qualitativen Aspekten (z. B. systematische Ausfälle oder Software) in ausreichendem Maße berücksichtigt sind.

Besonderes Augenmerk ist jedoch zusätzlich auf die Schnittstellen der Subsysteme zu richten:

- Alle Verbindungen (z. B. Leitungen oder Datenkommunikation durch Bussysteme müssen im PL eines der beteiligten Subsysteme bereits berücksichtigt sein oder Fehler in den Verbindungen müssen ausgeschlossen oder vernachlässigt werden können
- Jeder Ausgangsstatus eines ansteuernden Subsystems, der die Anforderung der Sicherheitsfunktion signalisiert, muss als auslösendes Ereignis für die Einleitung des sicheren Zustands des nachgeordneten Subsystems geeignet sein

Diese Bedingungen sind für die Schnittstellen zwischen den sicherheitsbezogenen Komponenten des Bosch Rexroth Sicherheitssystems erfüllt.

Das Safety-Funktionsmodul ist für den Einsatz in Sicherheitsfunktionen bis $PL_r = e$ geeignet und trägt mit folgenden Kenngrößen zum Gesamt-PL bei:

	CFL01.1-F1
Sicherheitsintegritätslevel SIL	SIL 3 (IEC, DIN EN 61 508), SILCL 3 (IEC, DIN EN 62 061)
Performance Level PL	PL e (DIN EN ISO 13 849-1)
Kategorie	Kategorie 4 (DIN EN ISO 13849-1)
PFH (mittlere Häufigkeit eines gefahrbringenden Ausfalls pro Stunde)	$4,5 \times 10^{-10}$ 1/h
PFD_{avg} (mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung)	$3,9 \times 10^{-5}$
Gebrauchsdauer T_M	20 Jahre (DIN EN ISO 13849); kein Proof-Test erforderlich

	CFL01.1-F1
MTTF _d (mittlere Zeit bis zum gefahrbringenden Ausfall)	2500 Jahre
DC _{avg} (durchschnittlicher Diagnosedetektionsgrad)	99 % ± hoch

Tab. 3-4: *Safety-Funktionsmodul*

Bei der Sicherheitsteuerung SafeLogic compact gelten für die CPUs folgende Kennwerte:

	SLC-3-CPU0	SLC-3-CPU1/SLC-3-CPU3
Sicherheitstechnische Kenngrößen		
Diese Angaben beziehen sich auf eine Umgebungstemperatur von +40 °C, die üblicherweise zur statistischen Berechnung der Werte angenommen wird.		
Sicherheits-Integritäts-level ¹⁾	SIL3 (IEC 61 508)	
SIL-Anspruchsgrenze ¹⁾	SILCL3 (EN 62 061)	
Kategorie	Kategorie 4 (EN ISO 13 849-1)	
Performance Level ¹⁾	PL e (EN ISO 13 849-1)	
PFHd	1,07 × 10 ⁻⁹ 1/h	1,69 × 10 ⁻⁹ 1/h
PFHd für Flexi Line Station ²⁾	–	0,40 × 10 ⁻⁹ 1/h

- 1) Für detaillierte Informationen zur Sicherheitsauslegung Ihrer Maschine/Anlage setzen Sie sich bitte mit Ihrer zuständigen Niederlassung von Bosch Rexroth in Verbindung
 2) nur SLC-3-CPU3

Tab. 3-5: *SafeLogic compact SLC-3-CPU0, SLC-3-CPU1, SLC-3-CPU3*



Bosch Rexroth bietet die umfangreiche Broschüre

"Mit Rexroth auf der sicheren Seite: 10 Schritte zum Performance Level"

zur Umsetzung der funktionalen Sicherheit nach ISO 13849 an. Die Broschüre ist ein praxistaugliches Hilfsmittel für die Konstruktion sicherer Maschinen (Bestellnummer der deutschen Version: R961006998, ISBN-Nummer 978-3-9814879-1-6, 264 Seiten).

Das Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung IFA (ehemals BGIA) bietet Anwendern der Norm ISO 13849-1 folgende Unterstützung an:

- BGIA-Report 2/2008: Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO13849 - Hier werden alle Aspekte zur Anwendung der Norm ausführlich dargestellt

- **SISTEMA©**

Dieses Software-Tool dient zur Ermittlung des erforderlichen Performance Level (PL_r) und erlaubt eine automatisierte Berechnung der resultierenden Quantifizierungswerte. Die IFA stellt das Tool als Freeware kostenlos zur Verfügung

Rexroth bietet für bestimmte Technologien ständig wachsende SISTEMA-Bibliotheken an. Diese Bibliotheken können ab Version 1.1.1 genutzt werden. Sie finden die SISTEMA-Bibliotheken unter:

<http://www.boschrexroth.com/de/de/trends-und-themen/maschinensicherheit/rexroth-safety-on-board-unsere-loesung/sistema/sistema>

Um die Handhabung der SISTEMA-Software zu vereinfachen, steht die offene Reihe der SISTEMA-Kochbücher kostenlos zum Download zur Verfügung

- Ebenfalls kostenlos kann bei der IFA der "Performance Level Calculator©" bezogen werden. Bei diesem "Performance Level Calculator" handelt sich um eine praktische Rechenscheibe zur Bestimmung des Performance Levels gemäß ISO 13849

3.2 Entwurf des sicherheitsbezogenen Steuerungssystems

3.2.1 Topologie

Die grundlegende Topologie des sicherheitsbezogenen Steuerungssystems ist im Prinzip unabhängig von dem Aufbau der Maschine oder Anlage.

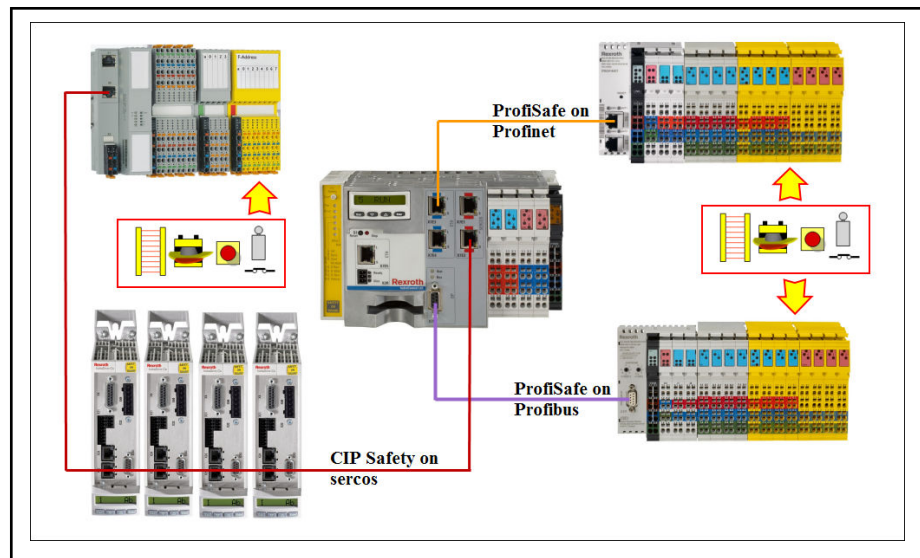


Abb. 3-8: Topologie eines sicherheitsbezogenen Steuerungssystems

Für die Anwendungsbereiche IndraMotion MTX ergeben die Risikobeurteilungen in der Regel die sicherheitsbezogene Anforderung SIL2 (bei Anwendung von IEC 61508 oder IEC 62061) oder PL d (bei Anwendung der EN ISO 13849-1).

Bei SPS-Applikationen unter Verwendung der Systemlösung IndraLogic (IL) sind häufig auch Sicherheitsfunktionen der Qualität SIL3 bzw. PL e gefordert.

Das Safety-Funktionsmodul als Kernelement des sicherheitsbezogenen Steuerungssystems ist generell einsetzbar zur Realisierung von Sicherheitsfunktionen bis SIL3 oder PL e. Hinsichtlich der Ein-/Ausgangsbaugruppen bietet Bosch Rexroth eine Auswahl von Safety-I/Os für alle Anwendungen an, die über Profibus und Profinet via PROFISafe bzw. über Sercos via CIP Safety on Sercos (CSOs) angebunden werden. Eine Übersicht finden Sie unter [Kap. 5.3 "Hardware für das Rexroth Inline-System" auf Seite 59](#).

Die SafeLogic compact ist ebenfalls einsetzbar zur Realisierung von Sicherheitsfunktionen bis SIL3 oder PL e. Eine Übersicht der unterstützten Haupt- und Erweiterungsmodule finden Sie unter ["CPU-Module" auf Seite 48](#) und ["Erweiterungsmodule" auf Seite 48](#).

3.2.2 Systementwurf

Obwohl die grundsätzliche Topologie des Sicherheitssystems von dem Anwendungsbereich unabhängig ist, stellen die Eigenschaften des Standard-Automatisierungssystems wesentliche Randbedingungen für den Entwurf des Sicherheitssystems dar. Diese Eigenschaften sind per Definition nicht für die Sicherheit, wohl aber für die Performance des Sicherheitssystems, insbesondere für die Reaktionszeit der Sicherheitsfunktionen von Bedeutung.

Einflüsse des Standardsystems

Zu berücksichtigen sind

- die verwendete Standardsteuerung
 - Hardware
 - Software
- die Größe der Standardapplikation
- das (oder die) eingesetzte(n) Bussystem(e), in Frage kommen:
 - Profibus-DP
 - Sercos III

	• die Auslastung des Bussystems – Anzahl der Busteilnehmer – Datenbreite der Standardtelegramme – Verwendung von azyklischen Übertragungsdiensten (Parameter- oder Diagnosekanäle) • die verwendeten Antriebe (einschließlich Motoren)
Schaltschrank-Einbau	Alle Sicherheitskomponenten mit Schutzart < IP 54 müssen in einen Schaltschrank eingebaut werden, dessen Schutzart mindestens IP 54 beträgt. Dies trifft sowohl für die SafeLogic compact als auch für das Safety-Funktionsmodul und die Sicherheits-I/O-Komponenten (SIL2, SIL3) von Bosch Rexroth zu. Diese Komponenten haben die Schutzart IP 20.
Spannungsversorgung	Planen Sie die Spannungsversorgung des Sicherheitssystems nach den Vorgaben in DIN EN 60204-1. Es dürfen nur Netzteile mit sicherer Trennung nach EN 50178 (oder Stromquellen mit gleichem Sicherheitsgrad) mit PELV-Spannung nach EN 61131-2 eingesetzt werden. Weitere Geräte dürfen an diesen Netzteilen nur angeschlossen werden, wenn die Geräte ebenfalls der PELV-Spezifikation genügen.
EMV	Die elektrische Ausrüstung der Maschine muss so gestaltet werden, dass die Maschine den Anforderungen zur Elektromagnetischen Verträglichkeit genügt, insbesondere den zu erwartenden Störungen standhält. Auch wenn alle Einzelgeräte der europäischen EMV-Richtlinie genügen und die einzelnen Sicherheitskomponenten zusätzlich für erhöhte Störfestigkeitspegel qualifiziert sind, müssen Sie bei der Gestaltung der elektrischen Ausrüstung der Maschine einen möglichst EMV-gerechten Aufbau anstreben. Folgende Grundregeln sind geeignet, EMV-Probleme zu vermeiden: • Durchgängiger Potentialausgleich zwischen Maschinen- und Anlagenteilen • Räumliche Trennung zwischen Versorgung, Leistungsteilen und Steuerungen • Schirme kurz und vollflächig auflegen • Potentialausgleichsströme über den Schirm vermeiden • Vorhandene Funktionserdeanschlüsse beschalten • Alle Kommunikationsleitungen nach Vorgabe entsprechend abschließen
	 Beachten Sie genau die Installationsanweisungen aller Komponenten, insbesondere auch die der Feldbussysteme.
Architekturentwurf	Die Architektur des sicherheitsbezogenen Steuerungssystems zur Umsetzung der vorgesehenen Sicherheitsfunktionen lässt sich allgemein, wie in der nachfolgenden Abbildung gezeigt, darstellen. Das Sicherheitssystem kann mehrere Sicherheitsfunktionen zur Risikominderung beinhalten. Jede einzelne Sicherheitsfunktion wird unter Verwendung sequentiell angeordneter Teilsysteme innerhalb dieser Grundarchitektur umgesetzt.

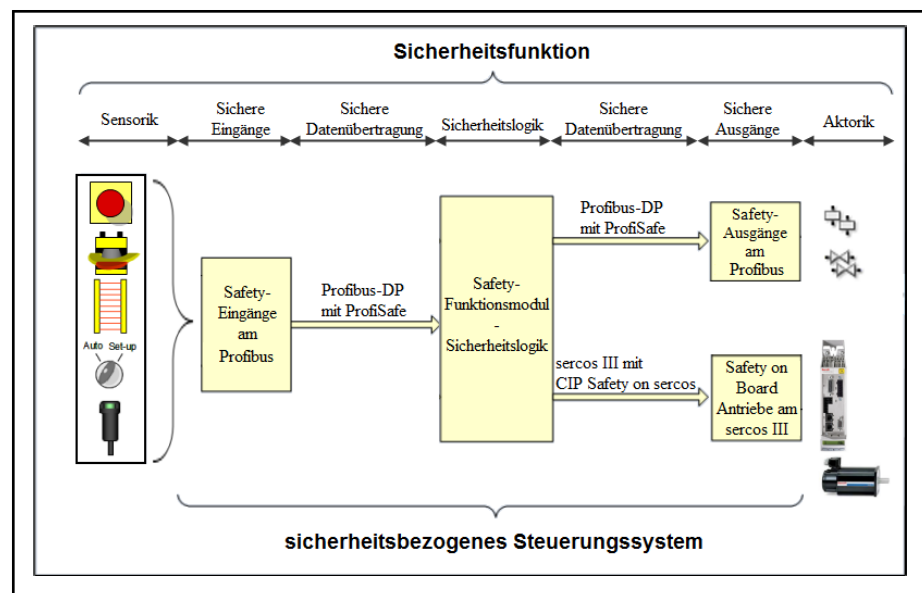


Abb. 3-9: Sicherheitsbezogenes Steuerungssystem

3.2.3 Entwurf der Teilsysteme

Bei dem Entwurf der Teilsysteme zur Umsetzung der Sicherheitsfunktionen und bei der abschließenden Beurteilung der Sicherheitsintegrität für jede Sicherheitsfunktion ist generell zu berücksichtigen:

Sichere Ein-/Ausgänge

- Auswahl der Ein-/Ausgangsmodule unter Berücksichtigung des geforderten Sicherheits-Levels (je nach angewandeter Norm) für die Sicherheitsfunktion
 - SIL2 bzw. PL d
 - SIL3 bzw. PL e



Werden zur Umsetzung einer Sicherheitsfunktion verschiedene, parallel angeordnete Eingangsmodule oder verschiedene, parallel angeordnete Ausgangsmodule verwendet, müssen alle für den angestrebten SIL oder PL geeignet sein.

- Auswahl der Ein-/Ausgangsmodule unter Berücksichtigung der Reaktionszeitanforderungen für die Sicherheitsfunktion



Werden zur Umsetzung einer Sicherheitsfunktion verschiedene, parallel angeordnete Eingangs- oder Ausgangsmodule verwendet, muss zur Ermittlung der resultierenden Reaktionszeit die im Hinblick auf Laufzeit, und Fehlerreaktionszeit jeweils langsamste Komponente herangezogen werden.

Zu berücksichtigen sind dabei auch die unterschiedlich parametrisierten Überwachungszeiten für die sichere Buskommunikation.

- Ausbau der dezentralen I/O-Stationen unter Berücksichtigung der Reaktionszeitanforderungen. Der Ausbau einer dezentralen Station mit sicherheitsbezogenen und nichtsicheren Modulen hat Einfluss auf die Signallaufzeit. Für zeitkritische Signale empfiehlt sich möglicherweise der Einsatz einer eigenen I/O-Station

- Zusammenfassen von funktional zusammengehörenden Ein-/Ausgängen. Die Sicherheitssteuerung bietet dazu ein Verfahren zur Gruppenkoordinierung z. B. zur Realisierung eines gemeinsamen Abschaltverhaltens an. Fehlerreaktionen beziehen sich in der Regel auf ganze Module und sind nicht signal-granular. Ziehen Sie bei der Zuordnung von Aktoren zu den Ausgängen in Betracht, dass bei Fehlerreaktionen möglicherweise alle Ausgänge eines Moduls abgeschaltet werden können
- Anschluss der Eingänge unter Berücksichtigung der Eingangsdynamisierung. Sicherheitsbezogene Eingänge müssen in der Regel dynamisiert werden, um "schlafende" Fehler im Eingangskanal und bei der Eingangsverdrahtung zu erkennen. Sichere Eingangsmodule stellen hierzu Testausgänge zur Eingangsdynamisierung zur Verfügung. Diese Testsignale müssen in die Eingangsbeschaltung einbezogen und bei der Eingangsparametrierung berücksichtigt werden

Sichere Ein-/Ausgangsgeräte von Bosch Rexroth sind als dezentrale Module sowohl für PROFISafe als auch für CIP Safety on Sercos erhältlich.



Alle Informationen zur Sicherheitsintegrität, zum Zeitverhalten und zur Parametrierung der sicheren Ein-Ausgangsgeräte entnehmen Sie den jeweiligen Gerätebeschreibungen.

Sichere Antriebe

Bosch Rexroth Antriebssysteme der Baureihe IndraDrive können optional mit integrierter Sicherheitstechnik ausgerüstet werden. Mit ihnen aufgebaute Sicherheitsanwendungen unterscheiden sich von Systemen mit konventioneller Sicherheitstechnik dadurch, dass die Sicherheitsfunktionen direkt in die intelligenten Antriebe in Form von Hard- bzw. Software integriert sind. Dies führt in allen Betriebsarten bei maximaler Sicherheit zu besonders kurzen Reaktionszeiten. Zudem entfallen unter anderem folgende Komponenten der konventionellen Sicherheitstechnik:

- Motorstillstandswächter zur Überwachung des sicheren Halts
- Drehzahlwächter zur Überwachung sicher reduzierter Geschwindigkeiten
- Leistungsschütze zwischen Regelgeräten und Motoren
- Endschalter bzw. Positionsnocken zur Bereichserkennung



Alle Informationen zur Integrierten Sicherheitstechnik bei Rexroth IndraDrive entnehmen Sie bitte folgenden Dokumentationen:

- "Rexroth IndraDrive Integrierte Sicherheitstechnik "Safe Torque Off" (ab MPx-16)" ([R911332633](#))
- "Rexroth IndraDrive Integrierte Sicherheitstechnik nach IEC 61508" ([R911327663](#))

Sichere Datenübertragung

Die sichere Datenübertragung bei Bosch Rexroth Sicherheitssystemen erfolgt zusammen mit der Standard-Prozessdatenübertragung über die nachfolgend genannten Bussysteme unter Verwendung der sicherheitsbezogenen Übertragungsprofile PROFISafe bzw. CIP Safety on Sercos, die beide sicherheitsbezogene Anwendungen bis SIL 3 bzw. PL e ermöglichen.

- Profibus-DP
- Profinet-IO
- Sercos III

Zur Projektierung der Datenübertragung sind die Installationsanweisungen für die Feldbusse, insbesondere die speziellen Vorgaben für die sicheren

Übertragungsprofile zwingend einzuhalten. Lesen Sie hierzu [Kap. 5 "Sichere Bussysteme" auf Seite 57](#).

An der sicheren Datenübertragung für unterschiedliche Ein-/Ausgangsmodul innerhalb einer Sicherheitsfunktion können eingangs- und ausgangsseitig beide Bussysteme beteiligt sein.

Zur Ermittlung der resultierenden Reaktionszeit der Sicherheitsfunktion muss die im Hinblick auf Laufzeit, Überwachungszeit und Fehlerreaktionszeit jeweils langsamste Datenverbindung herangezogen werden. Dabei sind der physikalische Aufbau, die Vorgabe der Übertragungsparameter (z. B. Baudrate) und der Ausbau der Bussysteme mit sicherheitsbezogenen und nicht-sicheren Teilnehmern in die Kalkulation mit einzubeziehen.

3.3 Bestimmung der erreichten Sicherheitsintegrität

Nach der Festlegung des Entwurfs des Sicherheitssystems und der Umsetzung der Sicherheitsfunktionen müssen Sie die damit erzielte Sicherheitsintegrität, d. h. den erreichten SIL bzw. PL ermitteln und feststellen, ob Sie den aufgrund der Risikobeurteilung erforderlichen SIL bzw. PL unter Berücksichtigung der vorgesehenen Gebrauchsdauer der Maschine oder Anlage erreichen.

Diese Bestimmung führen Sie nach den Vorgaben der Norm durch, die Sie der Betrachtung Ihres Sicherheitssystems zugrunde legen.

Sie benötigen dazu die sicherheitsbezogenen Kenngrößen der einzelnen Komponenten des Sicherheitssystems. Für das Safety-Funktionsmodul oder die SafeLogic compact Steuerung finden Sie die erforderlichen Angaben in [Kap. 4.4.2 "SafeLogic" auf Seite 50](#) dieser Dokumentation. Die nicht-sicheren Standardkomponenten des Automatisierungssystems haben per Definition keinen Einfluss auf die Sicherheitsintegrität und müssen nicht berücksichtigt werden.

Falls mit dem vorliegenden Entwurf des Sicherheitssystems die erforderliche Sicherheitsintegrität für alle Sicherheitsfunktionen nicht erreicht wird, muss der Systementwurf so lange angepasst werden, bis alle Anforderungen erfüllt sind. Dieser iterative Prozess muss unter Umständen mehrfach durchlaufen werden.

3.4 Bestimmung der garantierten Abschaltzeit

3.4.1 Reaktionszeit

Sicherheitsprozesse sind Abläufe, die eine zuverlässige und kalkulierbare Abschaltung in sehr kurzer Zeit veranlassen müssen. Nicht selten bleibt zwischen dem Erkennen des gefährlichen Eingriffs und der notwendigen Abschaltung nur eine kurze Zeitspanne. Die Planung eines Sicherheitssystems erfordert daher kalkulierbare Reaktions- und Abschaltzeiten.

Sicherheitsabstand

Sicherheitsabstände an einer Maschine, z. B. der Abstand eines Lichtgitters von der gefahrbringenden Bewegung, resultieren aus der Risikoanalyse und der Beschaffenheit der Maschine. Neben der Zutrittsgeschwindigkeit ist die Abschaltzeit der Maschine der maßgebende Parameter zu ihrer Bemessung.

Die allgemeine Formel für den Sicherheitsabstand lautet:

$$S = K \times T + C$$

S	Sicherheitsabstand in mm
K	Zutrittsgeschwindigkeit in mm/s
T	Abschaltzeit [s]
C	Zuschlag in mm

Abb. 3-10: Sicherheitsabstand nach EN 999

Die Zutrittsgeschwindigkeit ist abgeleitet von den Möglichkeiten und der Art der Annäherung.

Die Abschaltzeit T bezeichnet die Zeit vom Auslösen der Sensorfunktion bis zur Beendigung der gefahrbringenden Bewegung.

Der Zuschlag C ist ein zusätzlicher Abstand, der das Eindringen in den Gefahrenbereich vor Auslösen der Sicherheitsfunktion berücksichtigt.

Zur Berechnung des Sicherheitsabstandes sind je nach Art der Zugangsabsicherung weitere Parameter zu berücksichtigen.



Hilfe bei der Berechnung des Sicherheitsabstandes finden Sie in der Norm: DIN EN 999: "Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen".

Geforderte Abschaltzeit Bei vorgegebener Zutrittsgeschwindigkeit ergibt sich zur Erreichung des notwendigen Sicherheitsabstandes die Forderung nach einer maximalen Abschaltzeit für die Sicherheitsfunktion.

Typische Reaktionszeit Die typische Reaktionszeit des Sicherheitssystems ist die Zeit, die vom Anlegen des Signals an die sichere Eingangsklemme bis zur Reaktion an der sicheren Ausgangsklemme vergeht. Diese Zeit kann im ungestörten Betrieb des Sicherheitssystems typisch erreicht und gemessen werden.

Die typische Reaktionszeit des Sicherheitssystems ist zur Ermittlung der garantierten Abschaltzeit und damit zur Auslegung von Sicherheitsabständen nicht relevant und nicht geeignet.

Die Verarbeitungszeiten der Standard-Steuerung sind zum Ermitteln der typischen Reaktionszeit des Sicherheitssystems nicht relevant.

Garantierte Abschaltzeit Die garantierte Abschaltzeit der Sicherheitsfunktion entspricht der maximalen Reaktionszeit der Maschine. Die Abschaltzeit wird im Rahmen einer Worst Case-Betrachtung ermittelt und berücksichtigt unbedingt auch Fehlerfälle in der Sicherheitskette der Sicherheitsfunktion.

Die garantierte Abschaltzeit setzt sich aus der längsten Verarbeitungszeit der an der Sicherheitsfunktion beteiligten Eingänge, Ausgänge, Kommunikationsverbindungen und der Sicherheitslogik zusammen. Die maximalen Verarbeitungszeiten der einzelnen Komponenten kann den entsprechenden Datenblättern entnommen werden. Die garantierte Abschaltzeit muss kleiner sein als die geforderte Abschaltzeit sein.

Eine wichtige Projektierungsaufgabe ist nun, festzustellen, dass an der vorliegenden Maschine von dem entworfenen Sicherheitssystem für alle Sicherheitsfunktionen Abschaltzeiten erreicht werden, die garantiert kleiner sind als die geforderte maximale Abschaltzeit und dies nicht nur im fehlerfreien Fall sondern auch bei Vorliegen eines Fehlers.

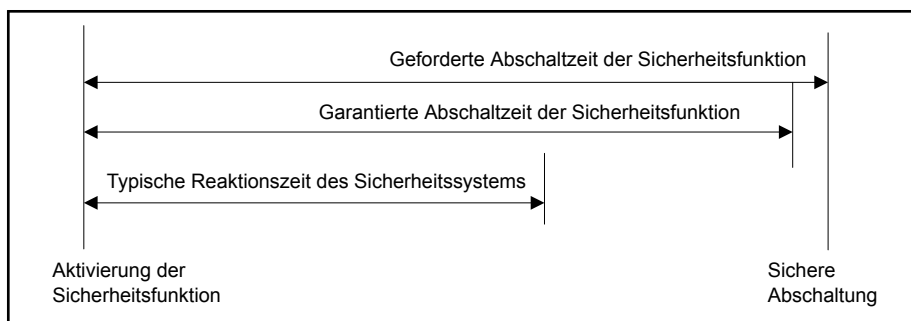
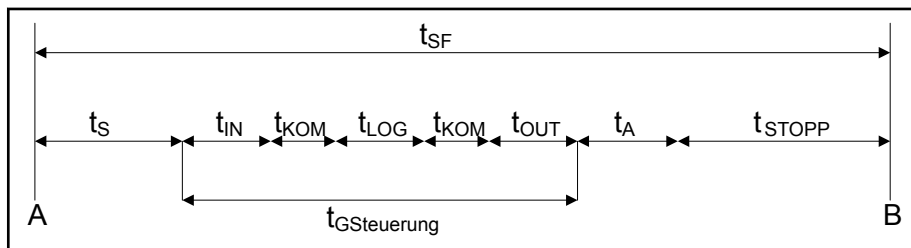


Abb. 3-11: Typische Reaktionszeit - Garantierte Abschaltzeit

Im fehlerfreien Fall

Die Abschaltzeit im fehlerfreien Fall bestimmen Sie durch Laufzeitbetrachtungen der einzelnen Teilabschnitte der Sicherheitsfunktion.



A	Anforderung der Sicherheitsfunktion
B	Sicherer Zustand der Anlage
t_{SF}	Garantierte Abschaltzeit für die Sicherheitsfunktion
t_S	Reaktionszeit des Sensors
t_{IN}	Verarbeitungszeit des Eingangs
t_{KOM}	Übertragungszeit
t_{LOG}	Logik-Bearbeitungszeit
t_{OUT}	Abschaltzeit des Ausgangs
t_A	Reaktionszeit des Aktors
t_{STOPP}	Anhaltezeit der Maschine
$t_{GSteuerung}$	Zeitanteil des Sicherheitssystems

Abb. 3-12: Übersicht über die Abschaltzeiten

Kalkulieren Sie die garantierte Abschaltzeit nach folgender Formel:

$$t_{SF} = t_{S_{\max}} + t_{GSteuerung_{\max}} + t_{A_{\max}} + t_{STOPP_{\max}}$$

Abb. 3-13: Garantierte Abschaltzeit für eine Sicherheitsfunktion

Die maximalen Reaktionszeiten der Sensoren und Aktoren entnehmen Sie den jeweiligen Gerätebeschreibungen. Zur Ermittlung der Anhaltezeit der Maschine sind Sie in der Regel auf zuverlässige Messungen angewiesen.



Wenn an der Sicherheitsfunktion mehrere Sensoren oder Aktoren beteiligt sind, fließt in die Berechnung die längste Reaktionszeit der beteiligten Geräte ein.

Den maximalen Zeitanteil des Steuerungssystems berechnen Sie unter Berücksichtigung der folgenden Faktoren auch unter Berücksichtigung von Fehlerfällen im Worst Case für Ihren Anwendungsfall:

- Verwendete Ein-/Ausgangskomponenten und deren Parametrierung
- Verwendetes Bussystem (verwendete Bussysteme) für die sichere Datenübertragung und dessen Parametrierung und Konfiguration (Buszykluszeit, Anzahl Busteilnehmer, Anzahl Nutzdatenbytes) Bei der Kalku-

lation der Laufzeiten der sicheren Datenübertragungen ist auch die Auslegung des Standard-Automatisierungssystems von Bedeutung:

- Standardauslastung und Zeitverhalten der Busse
- Standardauslastung und Zeitverhalten der dezentralen Stationen
- Zeitverhalten der Standardapplikation
- Verwendung asynchroner Übertragungsdienste zur Parametrierung oder Diagnose
- Die Bearbeitungszeit der Sicheren Logik

Sind sequentielle Teilabschnitte des Sicherheitssystems nicht untereinander synchronisiert, sind die von ihnen beigesteuerten Zeitanteile zweifach in die Berechnung einzusetzen (Worst Case)

$$t_{GSteuerung} = 2 \cdot t_{IN_{max}} + 4 \cdot t_{KOM_{max}} + 2 \cdot t_{LOG} + 2 \cdot t_{OUT_{max}}$$

Abb. 3-14: Berechnung des maximalen Zeitanteils des Steuerungssystems



Wenn an der Sicherheitsfunktion mehrere Eingänge oder Ausgänge oder unterschiedliche Kommunikationspfade beteiligt sind, dann fließt in die Berechnung die längste Verarbeitungszeit der beteiligten Komponenten oder Teilsysteme ein.

Im Fehlerfall

Im Fehlerfall werden an den Ausgängen der sicherheitsgerichteten Komponenten "Failstate-Werte" ausgegeben. Diese Werte können gemeinsam mit entsprechenden Fehlermeldungen über das Kommunikationssystem übertragen werden. Ist das Kommunikationssystem nicht mehr verfügbar, greifen parametrierbare Zeitüberwachungen auf den Sicherheitskomponenten, die den sicheren Zustand der Ausgänge in den Sicherheitskomponenten bewirken. Die Time-Out-Werte werden bei der Parametrierung der Sicherheitskomponenten so eingestellt, dass die garantierten Abschaltzeiten erreicht werden, ohne dass die Verfügbarkeit der Anlage unnötig beeinträchtigt wird.

Bearbeitungszeit der sicheren Logik

Die Bearbeitungszeit der sicheren Logik ist dadurch gegeben, dass die Bearbeitungszeit im Rahmen einer zyklischen Task mit fester Tasklaufzeit ausgeführt wird. Die Bearbeitungszeit können Sie bei der Parametrierung der Safety-Task festlegen. Einstellbar ist ein Wert zwischen 2 ms und 500 ms. Die Einhaltung der Tasklaufzeit wird im Safety-Funktionsmodul überwacht, eine Überschreitung der Zeit führt zu einer Fehlerreaktion und zum sicheren Zustand des Sicherheitssystems.

Die SafeLogic compact verfügt über keine parametrierbare Safety-Task. Die Zykluszeit hängt von der Anzahl der verwendeten Funktionsblöcke ab und liegt zwischen 4 ms und 40 ms.

3.4.2 Überprüfung der geforderten Abschaltzeit

Führen Sie für jede Sicherheitsfunktion folgende Überprüfung durch:

- Wird mit der ermittelten garantierten Abschaltzeit die geforderte Abschaltzeit für die Sicherheitsfunktion erreicht?
- Ist der ermittelte Wert größer als die geforderte Abschaltzeit für die Sicherheitsfunktion t_{SF} , dann müssen Sie an einem der Parameter Veränderungen vornehmen, weil unter den gegebenen Bedingungen die die Sicherheit der Maschine nicht in jedem Fall gewährleistet ist
- Ist der ermittelte Wert kleiner als t_{SF} , dann können Sie die Überwachungszeiten der an der Sicherheitskette beteiligten Einheiten mit den vorgesehenen Werten parametrieren. Ist der ermittelte Wert wesentlich kleiner als t_{SF} , dann können Sie den Wert für die Überwachungszeiten

auch vergrößern, um die Verfügbarkeit zu erhöhen. Führen Sie die Überprüfung für den neuen Wert der parametrisierten Abschaltzeit durch!



Führen Sie die vorstehenden Überprüfungen für jede Sicherheitsfunktion durch.

3.5 Adressvergabe/Namen

Komponenten können durch zusätzliche Adressen innerhalb ihrer eindeutigen Kommunikationsbeziehungen eindeutig identifiziert werden. Die Art und Weise der Einstellung dieser Adressen ist gerätespezifisch. Folgende Möglichkeiten sind bekannt:

- Manuelle Einstellung mittels DIP-Schalter oder über eine Geräte-Tool
- Automatische Einstellung durch Parametrierung von der Sicherheitssteuerung aus

Diese zusätzlichen Adressen sind unabhängig von der Standardadressierung. Die Adressen werden bei der Parametrierung der Sicherheitskomponenten in der Sicherheitsapplikation hinterlegt (z. B. F-Parameter bei PROFISafe) und im zyklischen Betrieb zur Verifikation der Kommunikationsbeziehung herangezogen.

3.6 Beispielanwendung

3.6.1 Überblick

Das Beispiel ist fiktiv und erhebt keinen Anspruch auf Authentizität im Hinblick auf eine konkrete Anwendung. In diesem Sinne sind die hier angenommenen Abstände und Zeiten auch nur größenordnungsmäßig zu verstehen. Deshalb ist es nicht möglich, Daten aus diesem Beispiel in eine konkrete Applikation zu übertragen.



Auf dem Datenträger der SafeLogic compact Designer Software (R911334897) befinden sich Applikationsbeispiele aus verschiedenen Branchen.

Das nachfolgende Beispiel beschreibt eine Antriebsapplikation in Verbindung mit dem Safety-Funktionsmodul, bei der die Bewegung einer Motorenachse als einzige Gefährdung (neben der allgemeinen elektrischen) identifiziert wurde. Nach eingehender Analyse soll die erforderliche Risikoreduzierung dadurch erreicht werden, dass die Gefahrenstelle durch einen vertikal angeordneten Lichtvorhang gegen einen Zugriff mit Hand bzw. Arm abgesichert wird.

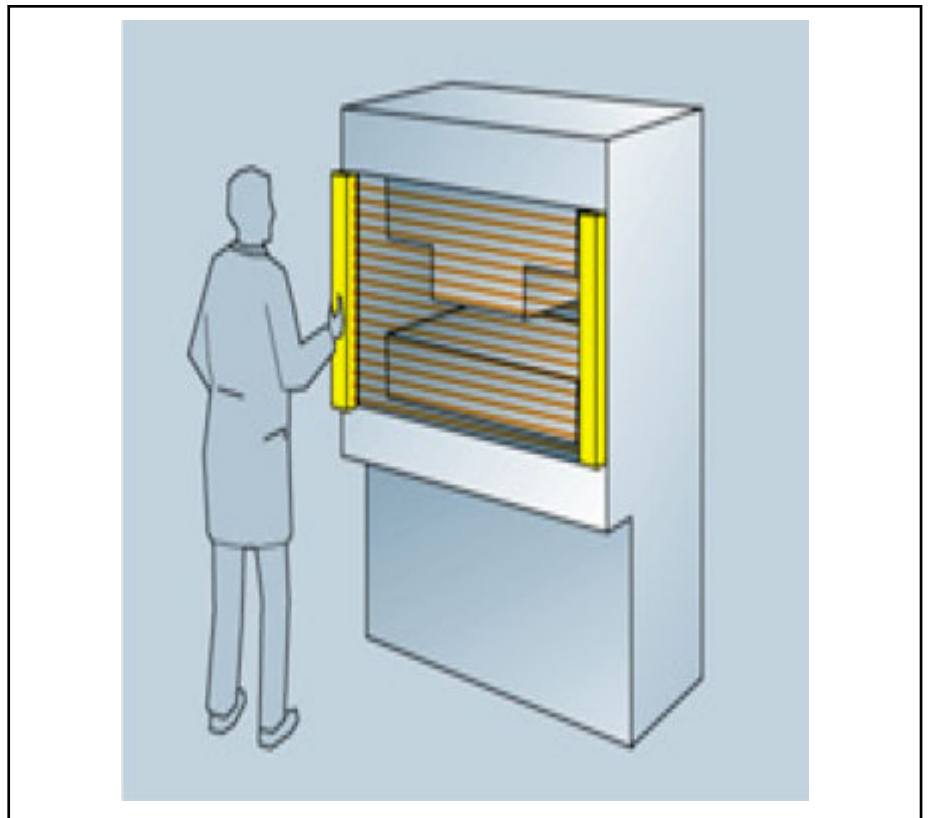


Abb. 3-15: Projektierungsbeispiel

3.6.2 Anforderungen

Für diese Maschine sind folgende Normen und Vorschriften als zutreffend erachtet worden:

- Maschinenrichtlinie 2006/42/EG
- EMV-Richtlinie 2004/108/EG
- Arbeitsmittelbenutzungsrichtlinie 2009/104/EG
- Niederspannungsrichtlinie 2006/95/EG
- Unfallverhütungsvorschriften/Sicherheitsregeln
- DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen
- IEC 61496-2: Aktive optoelektronische Schutzeinrichtungen
- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen
- EN 999: Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen

Die sicherheitstechnische Bewertung soll sowohl nach EN 62061 als auch nach EN ISO 13849-1 durchgeführt werden.

Aufgrund einer Risikobeurteilung unter Berücksichtigung der Grenzen der Maschine wurde als erforderliches Sicherheitsniveau festgelegt:

- SIL 2 nach EN 62061
- PL d nach EN ISO 13849-1

3.6.3 Sicherheitsfunktion

Die funktionale Sicherheit der Maschine wird durch Realisierung einer einzigen Sicherheitsfunktion erreicht:

SF1: "Wenn der Lichtvorhang unterbrochen wird, muss der Motor gesteuert in Stopp gehen, die Energiezufuhr soll beibehalten werden (Stopp-Kategorie 2 nach EN 60204-1)".

Das immer notwendige Stillsetzen im Notfall (Not-Halt) ist eine ergänzende Schutzmaßnahme und kein primäres Mittel zur Risikominderung. Daher wird diese Funktion nicht als eigentliche Sicherheitsfunktion angesehen und in diesem Beispiel nicht weiter betrachtet. Diese Funktion muss jedoch über einen Stopp der Kategorie 0 oder 1 nach EN 60204-1 die Maschine in den sicheren Stillstand bringen.

SF1 kann in Teilsicherheitsfunktionen unterteilt werden:

SF1:	"Wenn der Lichtvorhang unterbrochen wird, muss der Motor in Stopp gehen"		
Teilsicherheitsfunktionen:	Sensor	Logik und Datenübertragung	Aktor
Aufgaben:	Erfassen	Übermitteln und Auswerten	Reagieren
Einheiten:	Lichtvorhang	Safety-Funktionsmodul, Sichere Eingänge (SIL2 I/O-System), PROFISafe	Sichere Antriebssteuerung, Motor

Tab. 3-6: Sicherheitsfunktion

3.6.4 Aufbau und Verdrahtung

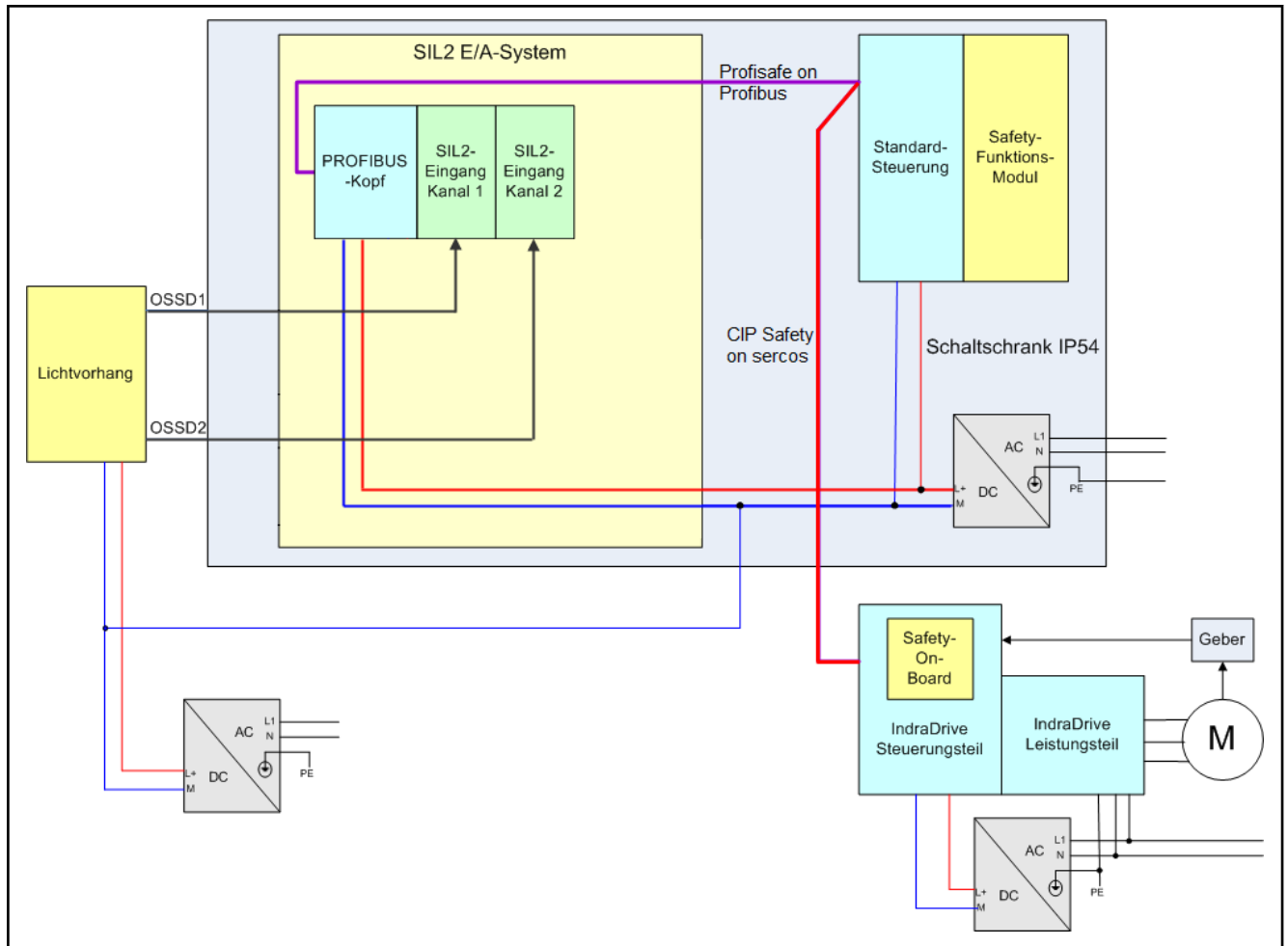


Abb. 3-16: Schematischer Aufbau eines Beispielsystems

Ohne auf den detaillierten Aufbau und die detaillierte Verdrahtung näher einzugehen, sind folgende Anforderungen zu erfüllen:

- Die Stromversorgung für den Lichtvorhang darf keine weiteren Teile der Maschine mit Spannung versorgen. Diese Stromversorgung benötigt die gleiche Masse wie die der Steuerungskomponenten
- Die Stromversorgungen werden mit 230V AC (Überspannungskategorie II) versorgt
- Alle Netzteile liefern Sicherheitskleinspannung PELV (protective extra-low voltage)
- Alle Steuerungskomponenten müssen in einem Schaltschrank mit Schutzart IP54 installiert werden

3.6.5 Komponenten

- Lichtvorhang**
- An das sichere Steuerungssystem ist der Lichtvorhang über die Signale OSSD1 und OSSD2 angeschlossen

OSSD1 und OSSD2 sind sicherheitsrelevante Schaltausgänge (Output Signal Switching Devices). Die beiden Schaltausgänge werden an ein sicherheitsgerichtetes digitales Eingabemodul (F-DI) angeschlossen und im Eingabemodul ausgewertet (2v2-Auswertung). Bei unterbroche-

nem Lichtvorhang liest die sicherheitsgerichtete Steuerung ein "0"-Signal von der F-DI. Das Sicherheitsprogramm in der Sicherheitssteuerung sorgt dann für den Stopp der Anwendung

- Um einen Zugriff mit Hand bzw. Arm sicher zu erkennen, muss ein geeigneter Lichtvorhang eine physikalische Auflösung von 30 Millimetern aufweisen.

Die Annäherung soll konstruktionsbedingt rechtwinklig erfolgen. Durch die Konstruktion ist auch gewährleistet, dass die Gefahrenstelle nur durch das Schutzfeld erreichbar ist; Übergreifen, Untergreifen und Hintertreten ist nicht möglich. Zu beachten ist auch der Abstand zu reflektierenden Flächen wie in IEC 61496-2 ("Aktive optoelektronische Schutzeinrichtungen") beschrieben

- Um die SIL-Anspruchsgrenze SIL2 zu erreichen, muss der Lichtvorhang mindestens eine BWS vom Typ 3 nach EN 61496-1 sein. Bei Lichtvorhängen handelt es sich um optoelektronische Geräte, die diffuse Reflektion nutzen (AOPDDR). Eine solche BWS erfüllt eine Reihe spezieller Anforderungen, insbesondere:
 - besitzt die BWS zwei unabhängige Halbleiterausgänge (24V) OSSD1 und OSSD2 als Verbindung zum sicheren Steuerungssystem
 - führt die BWS mindestens alle 5 s und bei jedem Rücksetzen interne Tests durch
- Als Lichtvorhang verwendet wird eine BWS TYP 4 nach EN 61496-1
 SILCL nach EN 62061 = 3
 PL nach EN ISO 13849-1 = e
 PFH = $2,5 \times 10^{-8}$
 Dies unterteilt sich in:
 PFH (Empfänger) = 2×10^{-8} PFH (Sender) = 5×10^{-9}
 Maximale Reaktionszeit: 15 ms

Sichere Eingänge

Bosch Rexroth SIL2 I/O-System

- SIL2 I/O-System in Minimal-Konfiguration, bestehend aus Profibus-Koppler und 2 Safety-Eingangsbaugruppen
- Der Anschluss der Ausgänge OSSD1 und OSSD2 des Lichtvorhangs erfolgt zweikanalig

Für das SIL2 I/O-System kann den technischen Daten entnommen werden:

SILCL nach EN 62061 = 2

PL nach EN ISO 13849-1 = d

PFH = 2×10^{-8}

Zykluszeit des SIL2 I/O-Systems bei dieser Minimalkonfiguration wird zu 10 ms ermittelt.

Sichere Datenübertragung

Als sichere Datenübertragung wird Profibus mit PROFISafe verwendet.

PROFISafe ist einsetzbar bis SIL3 bzw. PL e. Als PFH-Wert kann 10^{-9} angesetzt werden.

Der Profibus wird mit 12 Mbaud betrieben. Unter der Annahme, dass der Profibus mit weiteren 32 Profibus-Teilnehmern belastet wird, kann als Buszykluszeit 1,5 ms eingesetzt werden.

Sicherheitssteuerung

Das Safety-Funktionsmodul CFL01.1-F1 ist einsetzbar bis SIL3- bzw. PL e-Anwendungen.

PFH: $4,5 \times 10^{-10}$

Als Zykluszeit der Sicherheitsapplikation werden 10 ms parametrier.

Antriebssteuerung

Bosch Rexroth Antriebssteuerung mit Safety on Board.

Mit der Option Safety on Board ist der Antrieb für geberabhängige Sicherheitsfunktionen bis SIL2 oder PL d einsetzbar. Geberunabhängige Sicherheitsfunktionen erfüllen SIL3.

Die Reaktionszeit auf eine Sicherheitsanforderung beträgt 2 ms.

Zusammen mit dem Geber wird als PFH-Wert $2,5 \times 10^{-8}$ angesetzt.

Motor

Es wird angenommen, dass der Motor eine Anhaltezeit von 100 ms aufweist (Zeit bis zum sicheren Stillstand).

3.6.6 Parametrierung

Von der Vielzahl der einzustellenden bzw. einstellbaren Parameter der unterschiedlichen Komponenten werden hier nur die dargestellt, die für die Umsetzung der Beispiel-Sicherheitsfunktion relevant und von Interesse sind.

Komponente	Parameter	Wert	Bedeutung
Lichtvorhang	Keine		
SIL2-Eingänge	Profibus:		
	Stationsadresse	1	
	F-Parameter:		
	F_Slot Number	1	
	F_Check_SegNr	No Check	
	F_Check_iPar	No Check	
	F_SIL	SIL2	SIL2
	F_CRC_Length	2 Byte CRC	
	F_Block_ID	0	
	F_Par_Version	V1mode	PROFISafe-Version 1
	F_Source_Add	1	PROFISafe-Adressen mit Bezug zur Profibus-Stationsnummer
	F_Dest_Add	8	
	F_WD_Time	50	Überwachungszeit (ms)
	F_Par_CRC	27761	Automatisch erstellt

Komponente	Parameter	Wert	Bedeutung
	I-Parameter:		
	Inline Module 1	IL 24 DI8	2 Eingangsmodule
	Inline Module 2	IL 24 DI8	
	Inline Module 3	No Module	
	Startmodule Input Channel 1	Module 1	
	Startmodule Input Channel 2	Module 2	
	Startmodule Feed-back	No Module	Keine Ausgänge mit Rückmeldung
	Startmodule Output	No Module	
	Input 0	Aktiv	
	Input 0 Channel	Two Channel	Eingangskanal 1 monovalent
	Input 0 Type	Monovalent	
	Input 0 discrepancy	5 ms	Diskrepanzzeit zu Kanal 2: 5 ms
	Input 0 Filter	0 ms	Kein Eingangsfilter
	...		
	Input 8	Aktiv	
	Input 8 Channel	Two Channel	Eingangskanal 1 monovalent
	Input 8 Type	Monovalent	
	Input 8 discrepancy	5 ms	Diskrepanzzeit zu Kanal 2: 5 ms
	Input 8 Filter	0 ms	Kein Eingangsfilter
Profibus-Master	Stationsadresse	0	
	Höchste Stationsadresse	2	
	Baudrate	12 000 kBit/s	
	Max. Anzahl von Wiederholungen im Fehlerfall	2	
	...		

Komponente	Parameter	Wert	Bedeutung
Sicherheitssteuerung	Safety Task:		
	Priorität	1	Gegenüber den Standard-Tasks
	Typ	Extern ereignis-gesteuert	Event_Safety Interrupt
	Cycle Time	10 ms	Zykluszeit der Sicherheitslogik
	...		
Antrieb mit Safety on Sercos	Sercos Adresse	1	
	Safety Network Number(SNN)	0x00060000xxxx	Date/Time-Format: Date konstant 0x0006, Time von 0x0001..270F frei konfigurierbar. Alle Targets müssen die gleiche SNN haben wie der CSos Originator
	Safety Device ID (SDID)	0x1	Sichere Adresse für die CIP Safety Konfiguration. Alle Targets und Originator müssen unterschiedliche Adressen haben
	Network Time Expectation (NTE)	50	Übertragungszeit im ungünstigsten Fall vom Producer zum Consumer
	Expected Packet Interval (EPI)	10	Zykluszeit der CIP Safety Verbindungen
	Timeout Multiplier (TiMu)	2	Der TiMu bestimmt die Anzahl der CIP Safety Telegramme, die verloren gehen dürfen, bevor die CIP Safety Verbindung geschlossen wird. Ein TiMu von 1 bedeutet, dass kein Telegramm verloren gehen darf, bei einem TiMu von 2 darf 1 Telegramm verloren gehen, usw.
	Ping Interval EPI Multiplier (PIEM)	19	Es wird als Vielfaches der EPI angegeben, in welchem Intervall eine Zeitkoordinierung gesendet werden soll
	Time Coord. Msg. Min Multiplier (TCMM)	2	Übertragungszeit, die für eine Zeitkoordinierung mindestens erforderlich ist

Komponente	Parameter	Wert	Bedeutung
	Max fault number	5	Anzahl korrupter Telegramme, die innerhalb einer Stunde auftreten dürfen
	Timeout	1000	Zeitüberwachung Verbindungsaufbau (Forward Open timeout)

Tab. 3-7: Parametrierung der sicherheitsgerichteten Komponenten

3.6.7 Betrachtete Sicherheitskette

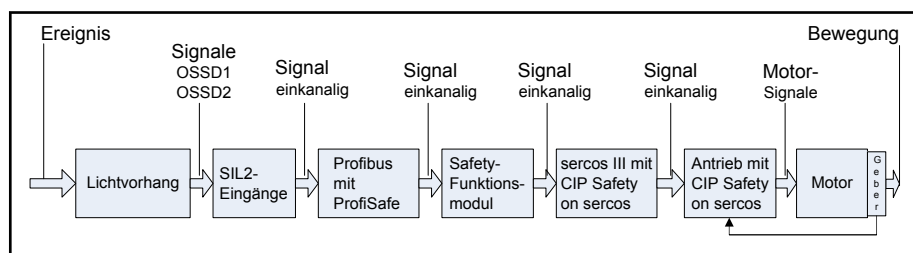


Abb. 3-17: Betrachtete Sicherheitskette

3.6.8 Bestimmen des erreichten PL-Wertes nach EN ISO 13849-1

Die EN 13849-1 gestattet hierzu ein vereinfachtes Verfahren, wenn die einzelnen Performance Level der Teilsysteme bekannt sind. Die Norm stellt dazu eine Tabelle zur Verfügung aus der man den resultierenden PL-Wert auslesen kann, nachdem man den niedrigsten PL der Sicherheitskette festgestellt (PL low) und dessen Häufigkeit in der Sicherheitskette bestimmt hat.

PL (low) (niedrigster PL eines Teilsystems)	n (low) (Anzahl der Teilsysteme mit diesem PL)	PL (Maximal erreichbarer PL)
a	> 3	–
	≤ 3	a
b	> 2	a
	≤ 2	b
c	> 2	b
	≤ 2	c
d	> 3	c
	≤ 3	d
e	> 3	d
	≤ 3	e

Abb. 3-18: PL-Bestimmung Sicherheitsfunktion (vereinfachtes Verfahren)

Nach den Informationen zu den Teilfunktionen ist der PL (low) = "d". Dieser PL kommt in der gesamten Sicherheitskette 2-mal vor, sodass der Gesamt-PL der Sicherheitsfunktion nach der Tabelle bei PL "d" bleibt. Die eingangsseitig spezifizierte Forderung ist damit erfüllt.

3.6.9 Bestimmen des erreichten SIL nach EN 62061

Bei der Betrachtung der gesamten Sicherheitsfunktion wird die Sicherheitsintegrität der Hardware dadurch bestimmt, dass

- der niedrigste SILCL eines Teilsystems den maximal erreichbaren SIL des Gesamtsystems einschränkt
- der PFH_D der gesamten Kette aus der Summe der einzelnen PFH ermittelt und der Sicherheitsintegritätslevel aus der folgenden Tabelle abgelesen wird

Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH)
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

Tab. 3-8: Sicherheitsintegritätslevel aus EN 62061

Die Rechnung ergibt: $\text{PFH}_D = 0,7 \times 10^{-7}$

Unter der Voraussetzung, dass zusätzlich alle Anforderungen der EN 62061 zur systematischen Sicherheitsintegrität erfüllt sind, genügt die Sicherheitsfunktion SF1 der Forderung SIL2 nach EN 62061.

3.6.10 Ermitteln des erforderlichen Sicherheitsabstands

ausreichendem Sicherheitsabstand montiert werden. Die Berechnungsformeln für den Sicherheitsabstand sind abhängig von der Art der Absicherung. Anbausituationen und Berechnungsformeln finden sich in der Norm EN 999 ("Anordnung von Schutzeinrichtungen in Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen").

Nach EN 999 fällt der verwendete Lichtvorhang unter die Kategorie: "Berührungslos wirkende Schutzeinrichtungen bei Verwendung aktiver opto-elektronischer Schutzeinrichtungen mit einem Detektionsvermögen von maximal 40 mm Durchmesser".

Allgemeine Gleichung für den Mindestabstand vom Schutzfeld zum Gefahrenbereich:

$$S = (K \cdot T) + C$$

- S** Mindestabstand in mm, gemessen vom Gefahrenbereich zum Schutzfeld
- K** Nach EN 999 anzunehmende Annäherungsgeschwindigkeit in mm/Sek.
- T** Nachlauf des Gesamtsystems in Sek.
- C** Zusätzlicher Abstand in mm, der das Eindringen in den Gefahrenbereich vor Auslösen der Schutzeinrichtung zugrunde legt.

Abb. 3-19: Mindestabstand

Dabei ist für die vorliegende Konstellation:

- $K = 2000 \text{ mm/s}$
- $C = 8 (d - 14 \text{ mm})$, jedoch nicht kleiner als 0

d ist dabei das Detektionsvermögen der Einrichtung in Millimetern, also hier 30 mm.

$T = T$ wird allgemein aufgeteilt in

- t_1 : die maximale Zeit zwischen dem Auslösen der Sensorfunktion und dem Zeitpunkt ist, bis die Schutzeinrichtung das Ausgangssignal in den AUS-Zustand geschaltet hat

- t_2 : die Ansprechzeit der Maschine ist, d. h. die zum Stillsetzen der Maschine oder zur Beseitigung der Risiken benötigte Zeit, nachdem das Ausgangssignal von der Schutzeinrichtung übergeben wurde

Somit wird:

- $S = (2000 \text{ mm/s} \times T) + 128 \text{ mm}$

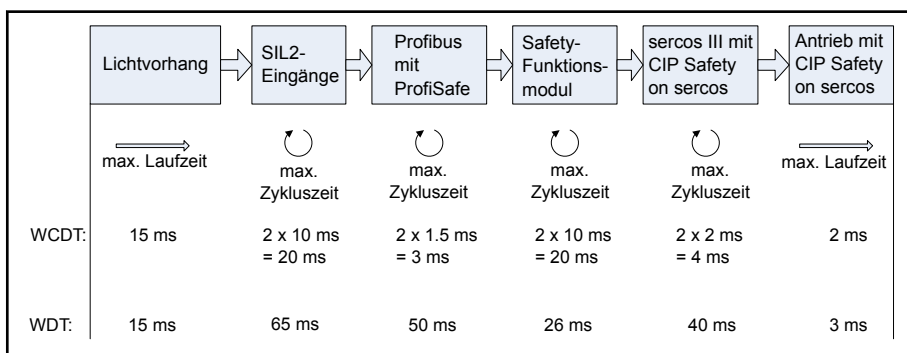
Diese Gleichung gilt für alle Mindestabstände S bis einschließlich 500 mm. Der Mindestwert von S darf nicht kleiner als 100 mm sein.

Zur Kalkulation des notwendigen Sicherheitsabstandes ist nun die Zeit T zu ermitteln:

- $T = t_1 + t_2$

Die Zeit " t_2 " stellt die maximale Anhaltezeit des Motors dar und beinhaltet die Rückmeldung des sicheren Stillstands über Geber zur Sicherheitslogik im Antrieb und unter Berücksichtigung einer möglicherweise notwendigen Fehlerreaktion. Die Zeit ist abhängig von dem verwendeten Motor und dem verwendeten Geber. Ihre Ermittlung wird hier nicht weiter ausgeführt. Für " t_2 " ist im vorliegenden Beispiel 150 ms ermittelt.

Die Zeit " t_1 " ist aus den Einzelzeiten der Teilsysteme der Sicherheitskette vom Lichtvorhang bis zur Eingangsschnittstelle der integrierten Sicherheitsfunktion im Antrieb zusammengesetzt, im Worst Case, unter Berücksichtigung aller asynchronen Vorgänge und unter Berücksichtigung eines möglichen Fehlers an beliebiger Stelle im Verlauf der Sicherheitskette. Zur Ermittlung geht man zunächst von der Worst Case Laufzeit im fehlerfreien Fall aus.



Laufzeit Einmalige sequentiell zu berücksichtigende Laufzeit

Zykluszeit Zykluszeit einer asynchronen Einheit

WCDT Worst Case Laufzeit

WDT Fehlerüberwachungszeit

Abb. 3-20: Zur Zeitkalkulation der Sicherheitsfunktion

Dabei ist WCDT die Worst Case Laufzeit jedes Gliedes der Sicherheitskette und WDT die Fehlerüberwachungszeit bzw. Fehlererkennungszeit jedes Gliedes der Sicherheitskette. Bei Lichtvorhang und Relais gibt es keine internen Überwachungen, bzw. entspricht die maximale Laufzeit im Fehlerfall der maximalen Laufzeit im fehlerfreien Fall.

WDT bei den SIL2-Eingängen umfasst die Zeit von der Erkennung eines Eingangs-Signalfehlers unter Berücksichtigung der parametrisierten Diskrepanz- und Filterzeit sowie der Zeit für die interne Fehlerdiagnose.

Die PROFISafe-Fehlerreaktionszeiten sind für die Eingangs- und Ausgangsübertragung unterschiedlich und berücksichtigen neben den eigentlichen Buslaufzeiten, der maximalen Zyklus- und Bearbeitungszeit der beteiligten PROFISafe-Master- bzw. Slave-Instanz ganz wesentlich die parametrisierte F-Watchdog-Time, ein sogenannter F-Parameter für PROFISafe.

Bei der Einstellung der F-Watchdog-Time ist über den Sicherheitsaspekt hinaus auf eine ausreichende Verfügbarkeit der Übertragung zu achten, die z. B. von Umgebungsbedingungen und EMV-Aspekten abhängt.

Für das Safety-Funktionsmodul kann die Zykluszeit der Applikation parametrisiert werden. Dieser Zyklus beinhaltet bereits die Zeit der internen Fehlerüberwachung, so dass auch im Fehlerfall die Worst Case-Zykluszeit gültig bleibt.

Der Zeitbedarf für die Fehlerbehandlung im Antrieb ist bei der für "t2" angesetzten Zeit von 150 ms bereits berücksichtigt. Für "t1" ist daher nur noch die Reaktionszeit des Antriebs im fehlerfreien Fall einzurechnen.

Nach diesen Betrachtungen ergibt sich "t1" nach der allgemeinen Formel:

$$t_1 = \sum_{i=1}^n WCDT_i + \max_{12..n} (WDT_i - WCDT_i) = 63 + 50 - 3 = 110$$

Abb. 3-21: Reaktionszeit der Sicherheitskette

Damit ergibt sich T zu: 110 ms + 150 ms = 260 ms = 0,26 s

In dieser Zeit ist auf jeden Fall mit einer fehlerhaften Antriebsbewegung zu rechnen. Eingesetzt in die Formel für den erforderlichen Sicherheitsabstand ergibt das Ergebnis:

- $S = (2000 \text{ mm/s} \times 0,26 \text{ s}) + 128 \text{ mm} = 648 \text{ mm}$

Für den Fall, dass sich "S" nach dieser Formel, wie hier geschehen, > 500 mm ergibt, kann die angenommene Annäherungsgeschwindigkeit auf 1600 mm/s reduziert werden. Der Abstand darf jedoch 500 mm nicht unterschreiten.

Es würde sich dann ergeben:

- $S = (1600 \text{ mm/s} \times 0,26 \text{ s}) + 128 \text{ mm} = 544 \text{ mm}$

Der Lichtvorhang muss also in einem Abstand von 544 mm von der Gefahrenstelle entfernt angebracht werden. Nur dann ist gewährleistet, dass ein Bediener beim Eindringen in den Lichtvorhang auch im Fehlerfall nicht gefährdet ist.

3.6.11 Weitere Vorgehensweise

Die bei der Projektierung festgelegten Strukturen, Adressen und Parameter stellen nun alle Eingangsgrößen für die Konfiguration des Sicherheitssystems, die Parametrierung der Komponenten und die Erstellung des Applikationsprogramms im Safety-Funktionsmodul dar.



Lesen Sie hierzu das Dokument "Rexroth IndraWorks 14VRS SafeLogic Projektkonfiguration" (siehe [Tab. 1-2 "Dokumentationen zu SafeLogic" auf Seite 2](#)).

4 Systemübersicht

4.1 Überblick

Die Sicherheitslösungen "SafeLogic" und "SafeLogic compact" ermöglichen eine frei programmierbare, sichere Logikverarbeitung.

Das **SafeLogic compact** Sicherheitssystem setzt sich im Wesentlichen aus folgenden Komponenten zusammen:

- Safety-CPU
- Sicherheits-I/O
- Sicherheits-Gateway für Sercos
- sichere Antriebe

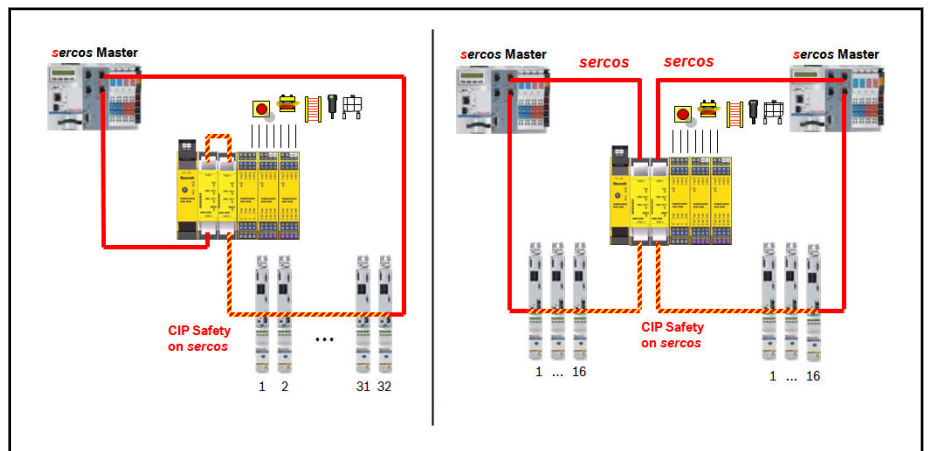


Abb. 4-1: Beispieltopologien der SafeLogic compact mit Sercos

Das **SafeLogic** Sicherheitssystem setzt sich im Wesentlichen aus folgenden Komponenten zusammen:

- Safety-Funktionsmodul als Komponente von Rexroth Steuerungen
- Sicherheits-I/O über Profibus, Profinet und Sercos
- sichere Antriebe über Sercos
- Sichere Netzwerkvariablen

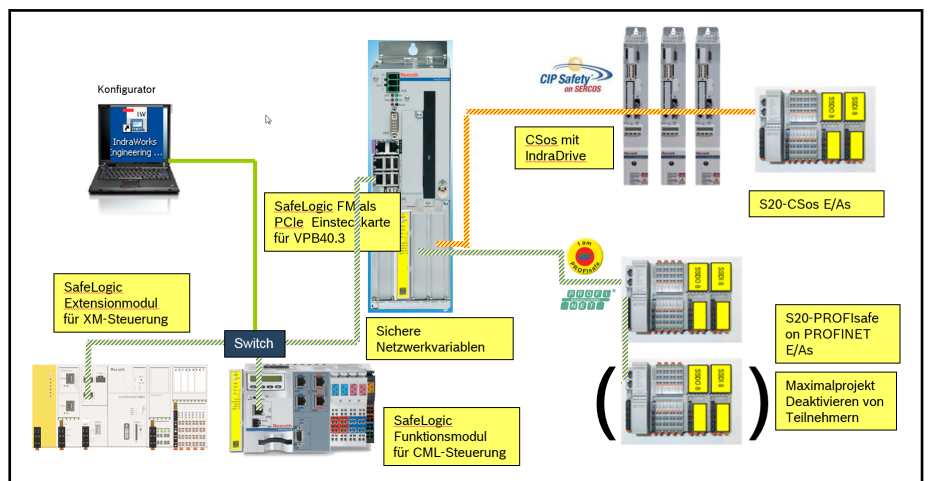


Abb. 4-2: Systemübersicht SafeLogic

4.2 Einsatzgebiete

Sowohl die SafeLogic, als auch die SafeLogic compact, sind für den Einsatz in der Fabrikautomatisierung vorgesehen. Beide Systeme arbeiten nach dem Ruhestromprinzip.

Der energielose Zustand ist der sichere Zustand:

- Ausgänge abgeschaltet
- Eingänge melden "Null" an die Steuerung

Die **SafeLogic compact** ist nach IEC 61508 und EN ISO 13849-1 zertifiziert und für den folgenden Einsatz zugelassen:

- bis SIL3 nach EN 61508:2010
- bis SILCL3 nach EN 62061:2005
- bis PLe nach EN ISO 13849-1:2006

Das Safety-Funktionsmodul der **SafeLogic** ist nach IEC 61508 und EN ISO 13849-1 zertifiziert und für den folgenden Einsatz zugelassen:

- bis SIL3 nach EN 61508:2010
- bis SILCL3 nach EN 62061:2005
- bis PLe nach EN ISO 13849-1:2006



Sicherheitsfunktionen erstrecken sich vom Sensor bis zum Aktor. Entsprechend der Risikoklassifizierung durch die Risikoanalyse müssen die Sicherheitsfunktionen eine ausreichende Widerstandsfähigkeit gegen den Verlust der Sicherheitsfunktion aufweisen. Sowohl das Safety-Funktionsmodul als auch die SafeLogic compact sind nur ein Teil der gesamten Sicherheitsfunktion.

Der tatsächlich erreichte Sicherheitsgrad hängt von der Außenbeschaltung, der Ausführung der Verdrahtung, der Parametrierung, der Wahl der Befehlsgeber und deren Anordnung an der Maschine ab.

4.3 Systemvoraussetzungen

Für die Installation und den Betrieb der **SafeLogic compact**-Entwicklungswerkzeuge müssen die folgenden Mindestvoraussetzungen erfüllt sein:

- Betriebssystem: Windows XP, Windows Vista oder Windows 7 mit 32 Bit oder 64 Bit
- Speicher: 1 GB RAM
- Festplattenspeicher: 300 MB
- Bildschirmauflösung: 1024 x 768

Für die Installation und den Betrieb der **SafeLogic**-Entwicklungswerkzeuge müssen die folgenden Mindestvoraussetzungen erfüllt sein:

- Betriebssystem: Windows 7 mit 64 Bit
- Speicher: 2 GB RAM (empfohlen ≥ 4 GB)
- Festplattenspeicher: 5 GB
- Bildschirmauflösung: 1024 x 768

4.4 Sicherheitssteuerungen

4.4.1 SafeLogic compact

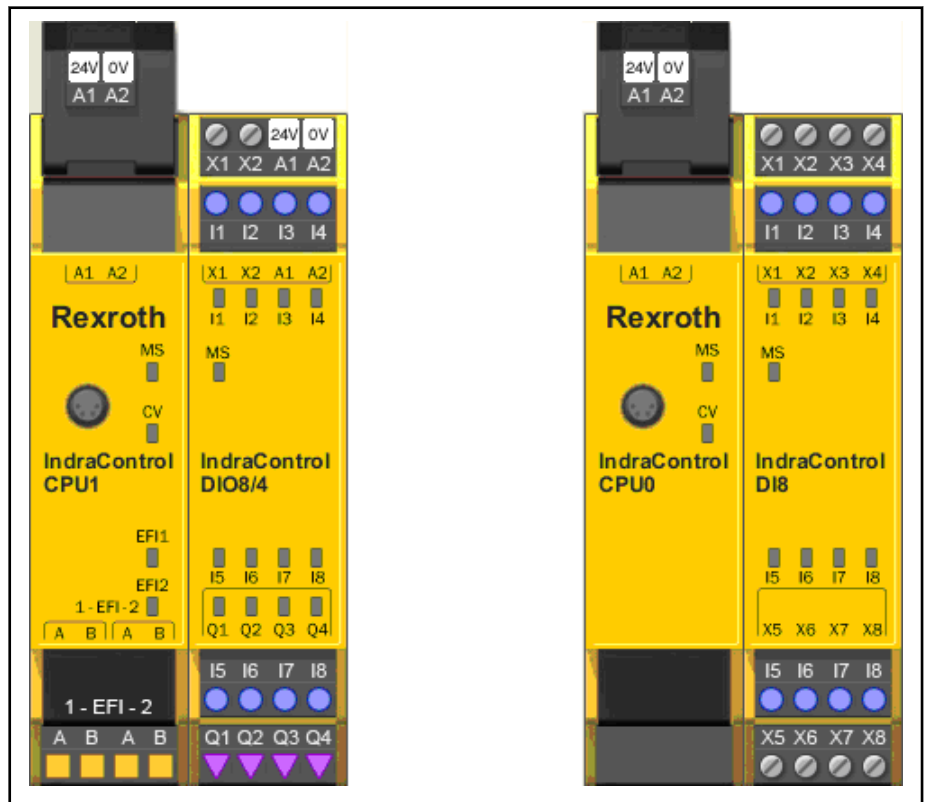


Abb. 4-3: Beispiele für Minimalaufbau SafeLogic compact System mit CPU0 und XTIO oder CPU1 und XTIO

Die SafeLogic compact eignet sich für Safety-Projekte mit einer lokal begrenzten Anzahl sicherer I/O.

Systemeigenschaften

- Modularer Aufbau: 1 Hauptmodul, bis zu 2 unterschiedliche Gateways und bis zu 12 Ein-/Ausgangserweiterungsmodule mit je 22,5 mm Baubreite
- 8 bis 96 einkanalige Eingänge und 4 bis 48 einkanalige Ausgänge
- Programmierbar
- Verwendung von bis zu 255 Standard- und applikationsspezifischen Logikblöcken
- Standard-Logikblöcke, z. B.:
 - AND
 - OR
 - NOT
 - XNOR
 - XOR
- Applikationsspezifische Logikblöcke, z. B.:
 - Not-Halt
 - Zweihand
 - Muting

Systemübersicht

- Pressen
- Nachlauferkennung
- Betriebsartenwahlschalter
- Reset
- Restart
- Mit Gateways in unterschiedliche Feldbusse integrierbar
 - Profinet-IO Gateway zur Diagnose
 - Profibus-DP Gateway zur Diagnose
 - Sercos Gateway zur Anbindung von bis zu 16 CIP Safety on Sercos Targets (Antriebe/IndraDrive) an einem Sercos Gateway. Somit entfällt die diskrete Verdrahtung zu den Antrieben

CPU-Module Die folgenden CPU-Module stehen zur Verfügung:

Typ	Bezeichnung	Ein- gänge	Aus- gänge	Max. Anzahl im System	Materialnummer
SLC-3-CPU0	Hauptmodul	–	–	1	R911172284
SLC-3-CPU1	Hauptmodul	2 x EFI	–		R911172285
SLC-3-CPU3	Hauptmodul	2 x EFI 2 x Flexi Line	–		R911173402

Tab. 4-1: SafeLogic compact CPUs

Erweiterungsmodule An das CPU-Modul können weitere Module angereicht werden. Die folgenden Module werden unterstützt:

Typ	Bezeichnung	Ein- gänge	Aus- gänge	Max. Anzahl im System	Materialnummer
SLC-0-GPNT	Profinet-IO Gateway	2	–	2	R911172290
SLC-0-GPRO	Profibus-DP Gateway	1	–		R911172287
SLC-3-GS3S	Sercos Gateway	2	–		R911172765
SCL-3-XTIO	Ein-/Ausgangs- erweiterung	8	4	12	R911172291
SLC-3-XTDI	Eingangserwei- terung	8	–		R911172292
SLC-3-XTDS	Acht sichere Eingänge und vier bzw. sechs nicht sichere Ausgänge	8	4/6	12	R911173404

Typ	Bezeichnung	Ein- gänge	Aus- gänge	Max. Anzahl im System	Materialnummer
SLC-3-STIO	Sechs bzw. acht nicht sichere Eingänge, sechs bzw. acht nicht sichere Ausgänge	6/8	6/8	12	R911173405
SLC-3-MOCx	Anschluss und sichere Auswertung von zwei Gebern	2	–	6	R911173406
UE410-2RO	Relais-Ausgangserweiterung	–	2	8 ¹⁾	R911172293
UE410-4RO	Relais-Ausgangserweiterung	–	4	4 ¹⁾	R911172294

1) In Kombination max. 16RO

Tab. 4-2: Erweiterungsmodule für SafeLogic compact CPU

EFI-Link

EFI-Link ermöglicht es Ihnen, bis zu vier SafeLogic compact Stationen über EFI zum **sicheren Datenaustausch** zu kombinieren. In einem EFI-Link-System können nur SLC-3-CPU1-Module benutzt werden; der Anschluss von SLC-3-CPU0-Modulen ist nicht möglich. Die Prozessdaten jeder Station (Eingänge und Ausgänge, Logikergebnisse usw.) können allen anderen Stationen im EFI-Link-System zur Verfügung gestellt werden. Die Teachfunktion ermöglicht es, einzelne Stationen vorübergehend zu deaktivieren, ohne die Funktion des Gesamtsystems zu beeinträchtigen.

Weiterhin ist es möglich EFI-kompatible Sicherheitsensoren der Fa. SICK anzuschließen (z. B. Sicherheits-Laserscanner, Lichtvorhänge).

Das XTIO-Erweiterungsmodul bietet die Möglichkeit des "Fast-Shut-Off". Durch direkte Abschaltung auf dem Erweiterungsmodul können - unabhängig von der Logik-Zykluszeit - Abschaltzeiten von 8 ms erreicht werden.

Ist zum Anschluss der EFI-Geräte z. B. aus EMV-Gründen eine Schirmung erforderlich, verwenden Sie dazu eine Erdungsklemme, die im Schaltschrank nahe dem SafeLogic compact Hauptmodul platziert ist. Verbinden Sie diese Erdungsklemme mit der Schirmung.

Flexi Line

Flexi Line ermöglicht es Ihnen, bis zu 32 SafeLogic compact Stationen sicher zu vernetzen. In einem Flexi Line System können nur SLC-3-CPU3-Module benutzt werden. Der Anschluss aller anderen Hauptmodule (SLC-3-CPU0, SLC-3-CPU1) ist nicht möglich.

Die EFI-Schnittstelle bleibt uneingeschränkt verfügbar.

Das Prozessabbild kann bis zu 12 Byte bzw. 96 Bits umfassen.

Die maximale Leitungslänge zwischen 2 Stationen beträgt 1000 Meter. Die mögliche Gesamtlänge eines Systems mit 32 Stationen beträgt somit 31 Kilometer.

Technische Daten der CPUx

Sicherheitsintegritätslevel SIL	SIL 3 (DIN EN 61508), SILCL 3 (DIN EN 62061)
Performance Level PL	PL e (DIN EN ISO 13849-1)

Kategorie	Kategorie 4 (DIN EN ISO 13849-1)
PFH _d	CPU0: $1,07 \times 10^{-9}$ 1/h CPU1/CPU3: $1,69 \times 10^{-9}$ 1/h
PFD _d für Flexi Line Stationen	CPU3: $0,40 \times 10^{-9}$ 1/h
Gebrauchsdauer T _M	20 Jahre (DIN EN ISO 13849)
Versorgungsspannung	24 V DC (16,8 ... 24 ... 30 V DC)

Tab. 4-3: Sicherheitstechnische Kenngrößen

Weiterführende Dokumentation

Weiterführende Dokumente finden Sie in "[Weiterführende Dokumente](#)" auf Seite 2.

4.4.2 SafeLogic

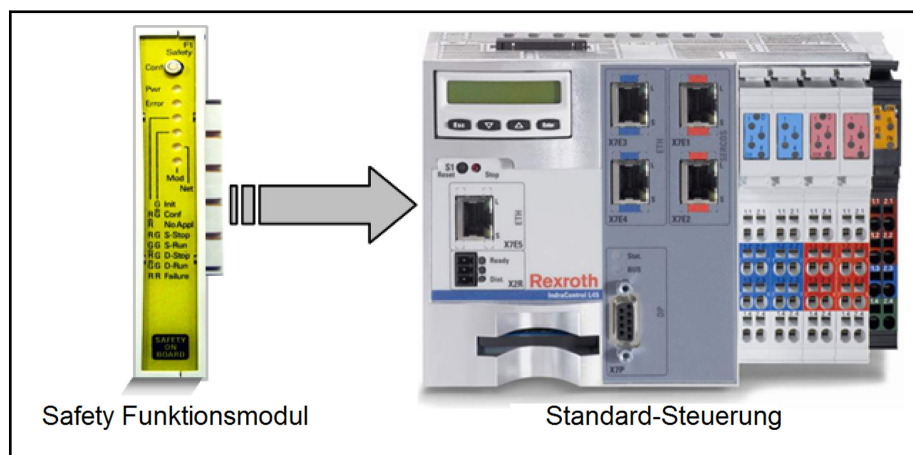
Die SafeLogic-Steuerung stellt die Ressource für die Verarbeitung von sicherheitsgerichteten Applikationsprogrammen zur Verfügung. Sie erweitert die Funktionssteuerung zur Sicherheitssteuerung und ermöglicht die Abarbeitung sowohl der funktionalen als auch der Sicherheitsapplikation auf ein und derselben Steuerung. Die SafeLogic-Steuerung ist in mehreren Bauformen für die Steuerungstypen IndraControl L45 / L75 / L85 erhältlich.

Standard- und Safety-Peripherie (Safety-IO, Sichere Antriebe, ..) können an ein und demselben Kommunikationssystem betrieben werden. Die Übertragung der sicheren Daten erfolgt über entsprechende Safety-Protokolle.

Die Rexroth SafeLogic-Steuerung unterstützt folgende sichere Peripheriekomponenten:

- Rexroth SIL3 I/O-System
- Rexroth IndraDrive mit integrierter Sicherheitstechnik

Ausprägungen der SafeLogic-Steuerung:



- Standard-Logikblöcke
 - AND
 - OR
 - NOT
 - XOR
- über die Steuerung mit unterschiedlichen Feldbussen verbunden
 - Profibus-DP über PROFISafe on Profibus
 - ProfiNetIO über PROFISafe on ProfiNet
 - Sercos über CIP Safety on Sercos
 - sichere Querkommunikation

Technische Daten

Nennspannung	DC 24V
Toleranz	-15 %, +20 % (ohne Restwelligkeit)
Restwelligkeit	±5 %
U _{max}	30 V
U _{min}	19,2 V

Tab. 4-4: Spannungsversorgung IndraControl L

Safety-Funktions-modul	Spannung	Typische Stromaufnahme	Typische Leistungsaufnahme
	3,3 V	0,12 A	0,4 W
	5 V	0,6 A	3 W

Tab. 4-5: Spannung, Strom- und Leistungsaufnahme

Sicherheitsintegritätslevel SIL	SIL 3 (DIN EN 61508), SILCL 3 (DIN EN 62061)
Performance Level PL	PL e (DIN EN ISO 13849-1)
Kategorie	Kategorie 4 (DIN EN ISO 13849-1)
PFH (mittlere Häufigkeit eines gefahrbringenden Ausfalls pro Stunde)	$4,5 \times 10^{-10}$ 1/h
PFD _{avg} (mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung)	$3,9 \times 10^{-5}$
Gebrauchsdauer T _M	20 Jahre (DIN EN ISO 13849); kein Proof-Test erforderlich
MTTF _d (mittlere Zeit bis zum gefahrbringenden Ausfall)	2500 Jahre
DC _{avg} (durchschnittlicher Diagnosedeckungsgrad)	99 % ± hoch

Tab. 4-6: Sicherheitstechnische Kenngrößen

Weiterführende Dokumentation

Weiterführende Dokumente finden Sie in ["Weiterführende Dokumente"](#) auf [Seite 2](#).

Hardware-Portfolio

Weitere Informationen zur Hardware des Rexroth Inline-Systems finden Sie in [Kap. 5 "Sichere Bussysteme"](#) auf [Seite 57](#).

4.5 Sichere Kommunikation

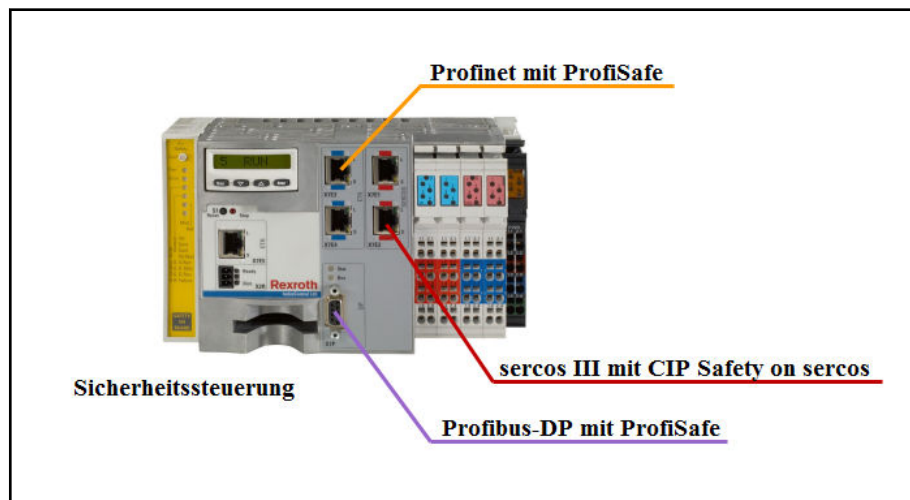


Abb. 4-5: Schnittstellen zur sichereren Kommunikation

Zur Übertragung der sicheren Daten werden folgende Sicherheitsprotokolle verwendet:

- CIP Safety on Sercos
- PROFISafe ²⁾
- Sichere Querkommunikation ³⁾

Als physikalische Übertragungsmedien können genutzt werden:

- Profibus-DP ⁴⁾
- Profinet-IO ⁵⁾
- Sercos ⁶⁾
- Ethernet ⁷⁾

4.6 Systemaufbau

SafeLogic compact

Ein SafeLogic compact System besteht aus folgenden Modulen:

- ein Speicherstecker SLC-3-MPL
- ein Hauptmodul SLC-3-CPU0, SLC-3-CPU1 oder SLC-3-CPU3
- bis zu 2 Gateways
- bis zu 12 zusätzliche IO-Erweiterungsmodule, z. B. SLC-3-XTIO, SLC-3-XTDI und SLC-0-STIO
- zusätzlich bis zu 8 Relais-Ausgangsmodule UE410-2RO und/oder 4 Relais-Ausgangsmodule UE410-4RO (d. h. max. 16 sichere Relais-Ausgänge)

²⁾ nur Safety-Funktionsmodul

³⁾ nur Safety-Funktionsmodul

⁴⁾ mit PROFISafe

⁵⁾ mit PROFISafe

⁶⁾ mit CIP

⁷⁾ mit sicherer Querkommunikation

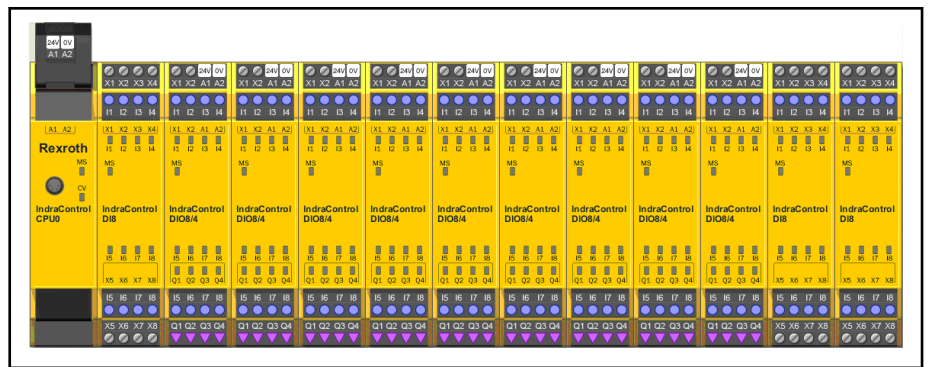


Abb. 4-6: Maximalaufbau SafeLogic compact System (ohne Relais-Ausgangs-erweiterungen und Gateways)

Die direkt am CPU-Modul angereichten sicheren I/O sind durch den internen Bus abgesichert.

SafeLogic

Das Safety-Funktionsmodul steht als optionales Erweiterungsmodul der Standard-Steuerung alle Ressourcen für die sichere Logikverarbeitung zur Verfügung. Zwischen den Endteilnehmern einer Datenverbindung, z. B. zwischen Safety-Funktionsmodul und Safety-I/O wird die Information in Form von sicheren Datentelegrammen ausgetauscht. Erkennen die Teilnehmer, dass die empfangenen Daten nicht korrekt sind bzw. die Übertragung gestört ist, gehen die Teilnehmer in einen definierten, sicheren Fehlerreaktionszustand. Die Übertragungsstrecke wird somit zum "Black Channel" und spielt für die Sicherheit keine Rolle – unabhängig davon welches Medium bzw. welche Übertragungsstrecke gewählt wird.

Als Sicherheitsprotokoll werden unterstützt:

- PROFISafe
- CIP Safety on Sercos
- Sichere Querkommunikation

Beide Protokolle werden parallel unterstützt, so dass sowohl CIP Safety als auch PROFISafe Teilnehmer gleichzeitig betrieben werden können.

Das Safety-Funktionsmodul verfügt über keine eigenen Schnittstellen, sondern nutzt die der Standard-Steuerung. Damit ist der Betrieb von sicheren und nicht sicherheitsrelevanten Teilnehmern an ein und demselben Kommunikationsmedium möglich.

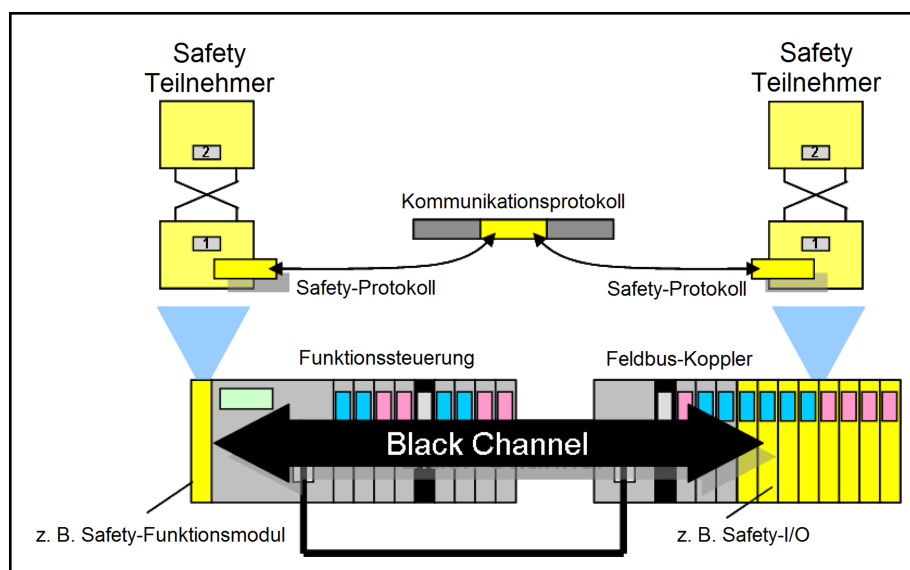


Abb. 4-7: Funktionsprinzip

Entsprechend der Anforderungen der zugrunde gelegten Sicherheitsnormen, wird die Sicherheitsapplikation gekapselt von der Standard-Applikation auf dem Safety-Funktionsmodul zweikanalig abgearbeitet. Das Engineeringssystem bietet dem Anwender eine durchgängige Sicht auf das Projekt und stellt den Datenaustausch zwischen sicherheitsrelevanter und nicht sicherheitsrelevanter Applikation bereit.

Das Safety-Funktionsmodul kontrolliert exklusiv die Safety-Teilnehmer und wirkt als Zustimmungseinheit der Prozesssteuerung. Es wird ein Sicherheitsausgang nur dann "TRUE" wenn sowohl Prozess- als auch Sicherheits-Signal "TRUE" sind.

4.7 IndraMotion MTX – Systemlösung

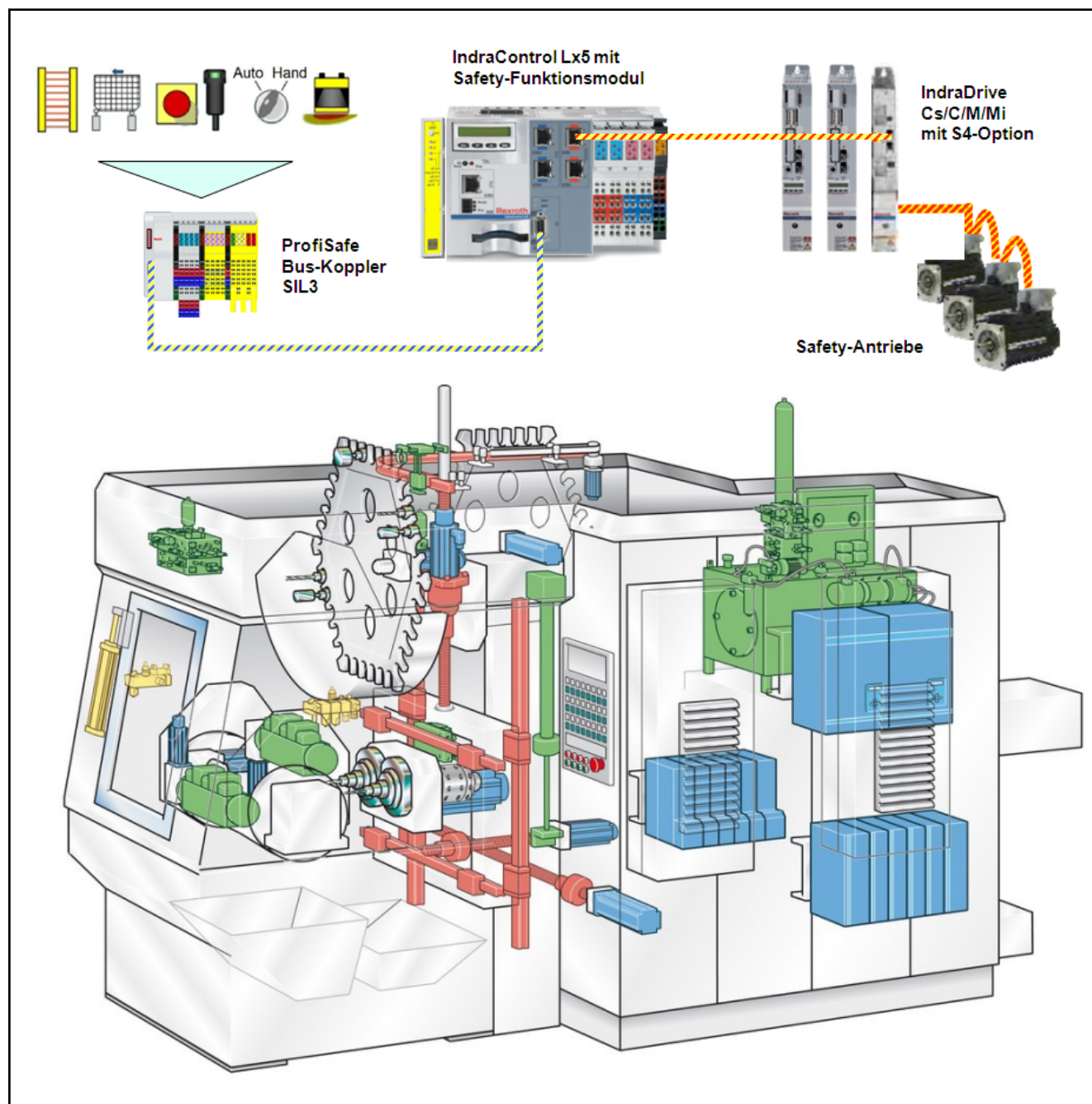


Abb. 4-8: Beispiel IndraMotion MTX Bearbeitungszentrum

Das Beispiel zeigt die Applikation der Sicherheitstechnik eines Bearbeitungszentrums im Werkzeugmaschinenbau. Der Arbeitsbereich ist durch trennende Schutzeinrichtungen abgesichert. Der Bediener benötigt Zugang, um Prozess- bzw. Materialstörungen zu beseitigen, bzw. den Werkzeugwechsler z. B. für neue Produktionsaufträge einzurichten. Die Verknüpfung der Peripheriesignale (Not-Halt, Türüberwachung, Lichtschranken, usw.) erfolgt auf dem Safety-Funktionsmodul, das integraler Bestandteil der Systemlösung ist. Sichere Bewegungsfunktionen werden durch die sichere Antriebstechnik bereitgestellt. Mit dem Sicherheitssystem "Safety on Board" lassen sich die Anforderungen, wie z. B. der ISO 10218, sicher und einfach umsetzen.

Folgende Funktions- und Anwendungsbeschreibungen stehen im Umfeld der Sicherheitstechnik zum Thema IndraMotion MTX zur Verfügung:

Dokument	Materialnummer, Dokumentart	Beschreibung
IndraMotion MTX 14VRS Systembeschreibung	R911342639 Projektierungsbeschreibung	Diese Dokumentation beschreibt das Steuerungssystem Rexroth IndraMotion MTX. Beschrieben werden die Ausführungen, Technischen Daten, Schnittstellen und die Konfiguration der Steuerungsbaugruppen
IndraMotion MTX 14VRS Maschinenparameter	R911342629 Referenz	Das vorliegende Handbuch beschreibt das Handling, den Aufbau und die Anpassung der verfügbaren Parameter der Rexroth IndraMotion MTX. Ebenfalls beschrieben werden Funktion und Bedienung des NC-Konfigurators
IndraMotion MTX 14VRS SPS-Interface	R911342621 Projektierungsbeschreibung	Das vorliegende Handbuch beschreibt die Interface-Signale und die Programmbausteine für die integrierte SPS
IndraMotion MTX 14VRS Funktionsbeschreibung - Grundlagen	R911342625 Referenz	Diese Dokumentation beschreibt die Funktionen der Rexroth IndraMotion MTX. Erläutert werden grundlegende Inbetriebnahmeschritte und die Funktionen der Steuerung als Beschreibung und Handlungsanweisung
IndraMotion MTX 14VRS Funktionsbeschreibung - Erweiterung	R911342627 Referenz	Diese Dokumentation beschreibt die Funktionen der Rexroth IndraMotion MTX. Erläutert werden grundlegende Inbetriebnahmeschritte und die Funktionen der Steuerung als Beschreibung und Handlungsanweisung
IndraMotion MTX 14VRS Funktionsbeschreibung - Sonderfunktionen	R911342623 Referenz	Diese Dokumentation beschreibt Sonderfunktionen der Rexroth IndraMotion MTX. Erläutert werden grundlegende Inbetriebnahmeschritte und die Funktionen der Steuerung als Beschreibung und Handlungsanweisung.
IndraMotion MTX 14VRS Inbetriebnahme	R911342619 Inbetriebnahmebeschreibung	Diese Dokumentation beschreibt die Inbetriebnahme der Steuerung IndraMotion MTX. Neben einer Gesamtübersicht werden die Inbetriebnahme und Konfiguration der Achsen und Bedienoberfläche und der SPS-Daten erläutert
Rexroth IndraMotion MTX 11VRS Diagnosemeldungen	R911332310 Referenz	Diese Dokumentation dient der Übersicht von Fehlern, Warnungen und Meldungen innerhalb des Steuerungssystems Rexroth IndraMotion MTX
Rexroth IndraMotion MTX 13VRS Automation Interface	R911337273 Anwendungsbeschreibung	Diese Dokumentation beschreibt den scriptbasierten Zugriff auf IndraWorks-Projektdaten über die Schnittstelle des Automation Interfaces. Beschrieben werden die verschiedenen Objekte, einschließlich Code-Beispielen. Eine Beschreibung des Automation Builders schließt sich an

Tab. 4-7: Dokumentationen zu SafeLogic



Weitere Dokumentangaben finden Sie in "[Weiterführende Dokumente](#)" auf Seite 2.

5 Sichere Bussysteme

5.1 Überblick

Standard-Bussysteme

Die sichere Datenübertragung bei Bosch Rexroth-Sicherheitssystemen erfolgt über die Bussysteme Sercos und/oder Profibus-DP und/oder Profinet-IO, jeweils gemeinsam mit der Standard-Prozessdatenübertragung.

Profibus-DP ist festgelegt in IEC 61158 und IEC 61784. Weitere Informationen zu Profibus-DP erhalten Sie bei der Profibus Nutzerorganisation e. V. (PNO).

Profinet wird durch Profibus & Profinet International (PI) definiert und ist seit 2003 Teil der Normen IEC 61158 und IEC 61784-2.

Sercos ist die dritte Generation der Sercos Interface Reihe nach IEC/EN 61491 auf der Basis von Standard-Ethernet IEEE 802.3. Sercos ist Teil der internationalen Standards IEC 61800-7, IEC 617843 und IEC 611584. Weitere Informationen zu Sercos erhalten Sie bei der Nutzerorganisation Sercos International e. V. (SI).

Sichere Datenübertragung

Die sichere Datenübertragung wird über sicherheitsgerichtete Applikationsprofile in die Standard-Bussysteme eingegliedert.

PROFISafe ist das sicherheitsgerichtete Applikationsprofil für Profibus-DP und Profinet und international in der IEC 61784-3-3 standardisiert.

Sercos Safety ist das sicherheitsgerichtete Applikationsprofil für Sercos. Basis ist CIPsafety, die sicherheitsgerichtete Erweiterung des Common Industrial Protokolls (CIP), das von der ODVA (Open DeviceNet Vendor Association) für Ethernet-IP und DeviceNet spezifiziert wurde.

5.2 Allgemeines zur sicheren Datenübertragung

Wesentliche Merkmale der sicheren Datenübertragung unabhängig von dem verwendeten Bussystem sind:

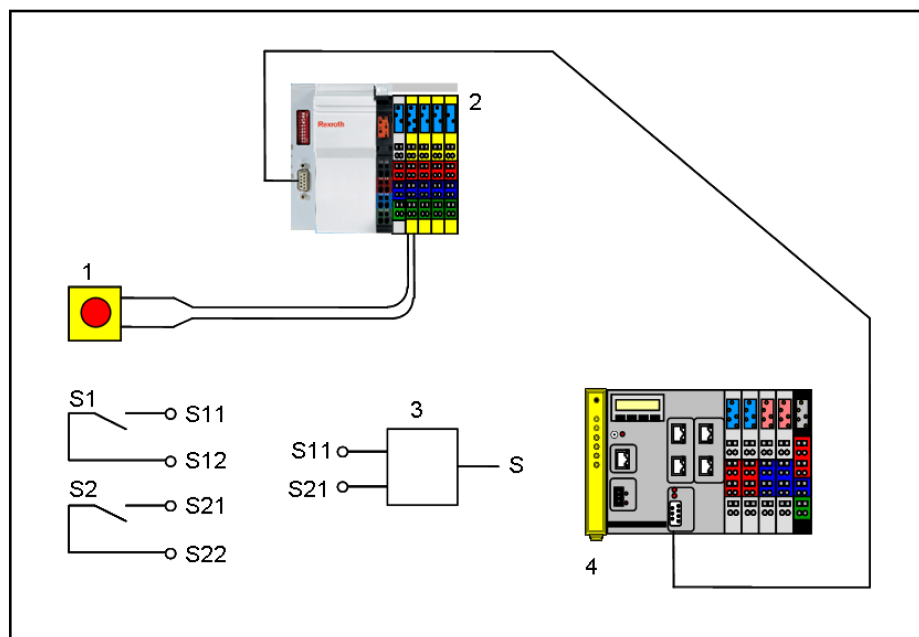
- Die sichere Datenübertragung zwischen dem Safety-Funktionsmodul (Host) bzw. dem SafeLogic compact CPU-Modul und den sicherheitsbezogenen Busteilnehmern (Slaves) beruht immer auf einer individuellen, eindeutigen, zeitlich überwachten Kommunikationsbeziehung
- Die sicherheitsbezogenen Daten sind in Form abgesicherter Daten-Container in den Nutzdatenstrom der Busprotokolle eingegliedert. Die Protokollmechanismen der Busse werden zur Erzeugung der Sicherheit nicht herangezogen. Die sicherheitsbezogenen Daten werden daher weder verändert noch erweitert und entsprechen den Standardprotokollen. Sichere Datenübertragung und Standarddatenübertragung erfolgen rückwirkungsfrei in Koexistenz
- Telegramme mit sicheren Daten und solche mit Standarddaten nutzen die gleiche Übertragungsphysik. Die Übertragungskanäle, angefangen von der Elektronik über die Steckverbinder bis hin zu den Übertragungskabeln haben keinerlei Einfluss auf die Sicherheit. Diese Übertragungskanäle werden als schwarze Kanäle bezeichnet und können in dieser Eigenschaft als beliebig fehlerbehaftet angenommen werden, ohne dass die Sicherheit dadurch beeinträchtigt wird. Die an die sichere Datenübertragung gestellten hohen Verfügbarkeitsanforderungen werden von den Standard-Bussystemen bei Einhaltung der spezifizierten Umgebungsbedingungen erfüllt
- Die Sicherheit wird ausschließlich von der sicheren Software in dem Safety-Funktionsmodul (Safety Host Layer) und der sicheren Software in

den sicheren Teilnehmern (Safety Slave Layer) gewährleistet. Sicherheit der Übertragung bedeutet die Freiheit von den anzunehmenden Übertragungsfehlern:

- Verlust von Telegrammen
- Fehlerhafte Wiederholung von Telegrammen
- Einfügung von Telegrammen
- Falsche Abfolge
- Unzulässige Verzögerung der Daten
- Verzögerung von Daten

Die Maßnahmen zur Beherrschung dieser Fehler sind von Sicherheits-Bus zu Sicherheitsbus durchaus unterschiedlich

- Die Safety-Layer sind als Zusatzschicht des ISO-OSI-Modells (Open Systems Interconnection Reference Model) oberhalb der Anwendungsschicht ausgebildet. Im Safety-Funktionsmodul gibt es für jede Kommunikationsbeziehung einen eigenen Safety-Host-Layer, der als Funktionsbaustein-Instanz in das sichere Programm einzubinden ist und dessen Ein-/Ausgangsparameter die Schnittstelle zur Sicherheitslogik darstellen
- Die sichere Datenübertragung erfolgt immer einkanalig, unabhängig davon, ob Sensoren oder Aktoren ein- oder zweikanalig angeschlossen werden. Bei diesem Ein-Bit-Prinzip werden zwei Bits zweier Peripheriekanäle auf ein sicheres Übertragungsbit abgebildet. Das Ein-Bit-Prinzip setzt sich über die Datenkommunikation bis in die Sicherheitslogik fort. In der Sicherheitslogik wurde dem Ein-Bit-Prinzip durch die Einführung der neuen Variablen-Typen Safe-Bool, Safe-Byte, Safe-Int,... Rechnung getragen



- 1 NOT-HALT-Bediengerät, zweikanaliger Anschluss
 2 Sicheres Eingangsgerät, zwei Eingangsklemmen beschaltet
 3 Logik-Verarbeitung im sicheren Eingangsgerät (zwei Eingangsbits werden sicher zu einem Übertragungsbit (SafeBool) zusammengefasst)
 4 IndraControl L mit Safety-Funktionsmodul mit Sicherheitslogik

Abb. 5-1: Ein-Bit-Prinzip

5.3 Hardware für das Rexroth Inline-System

Einführung Das Rexroth Inline-System dient zur Einbindung von I/O-Modulen (Inline-Klemmen) des IndraControl Inline-Busses.

Sichere Inline-Klemmen sind in gelber Farbe ausgeführt. Die sichere Kommunikation erfolgt über PROFISafe.

Profibus Inline-Buskoppler

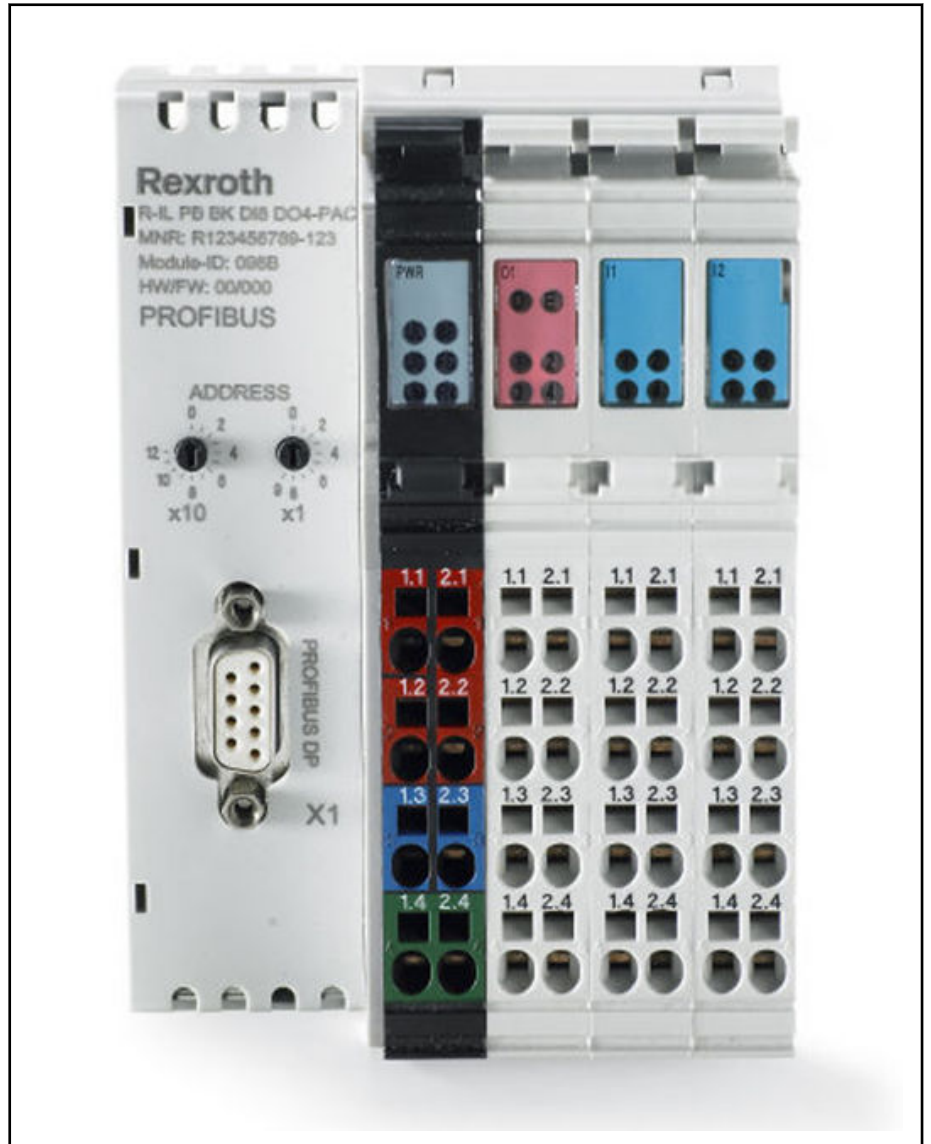


Abb. 5-2: Rexroth Profibus Inline-Buskoppler

Der Profibus Inline-Buskoppler dient zur Einbindung von I/O-Modulen des IndraControl Inline-Bus in Profibus-DP. Profibus lässt strukturell den Anschluss von bis zu 125 Feldbus-Kopplern mit je 61 zusätzlichen I/O-Modulen zu. Die maximale Anzahl ist abhängig vom eingesetzten DP-Master und den zur Verfügung gestellten Nutzdaten der angeschlossenen I/O-Module.

Typenschlüssel: R-IL PB BK DI8 DO4/CN-PAC

Materialnummer: R911172194

Überblick der Feldbus-Koppler-Eigenschaften:

- acht digitale Eingänge, Typ 1, 24 V DC
- vier digitale Ausgänge, 24 V DC, 0,5 A

- modular erweiterbar um bis zu 61 externe I/O-Module
- bis zu 6 sichere I/O-Module anschließbar (die max. Anzahl ergibt sich aus der Anzahl der belegten Bytes im Konfigurationskanal (max. 230 Bytes), siehe Tab. 5-2 "PROFISafe-Kanalbelegung durch Safety Inline-Klemmen" auf Seite 62). Jedes sichere IO-Modul besitzt einen PCP-Kanal
- Bis zu 16 PCP-Teilnehmer anschließbar. Jedes sichere Inline-I/O-Modul stellt einen PCP-Teilnehmer dar
- maximal 244 Byte je Datenrichtung Prozessdaten
- Parametrierung und Konfiguration mittels GSD inkl. Diagnose

Eine ausführliche Beschreibung finden Sie in der Dokumentation

- "Rexroth Inline-Buskoppler für Profibus-DP R-IL PB BK DI8 DO4/CN-PAC", Materialnummer [R911324348](#)



- PROFISafe-Geräte auf Basis Profibus dürfen nur am on-Board Profibus-Master der Standard-Steuerungen CML45/75/85 betrieben werden. Der Betrieb von PROFISafe-Geräten am Profibus-Master-Funktionsmodul (CFL01.1-TP) ist nicht freigegeben.

Profinet Inline-Buskoppler

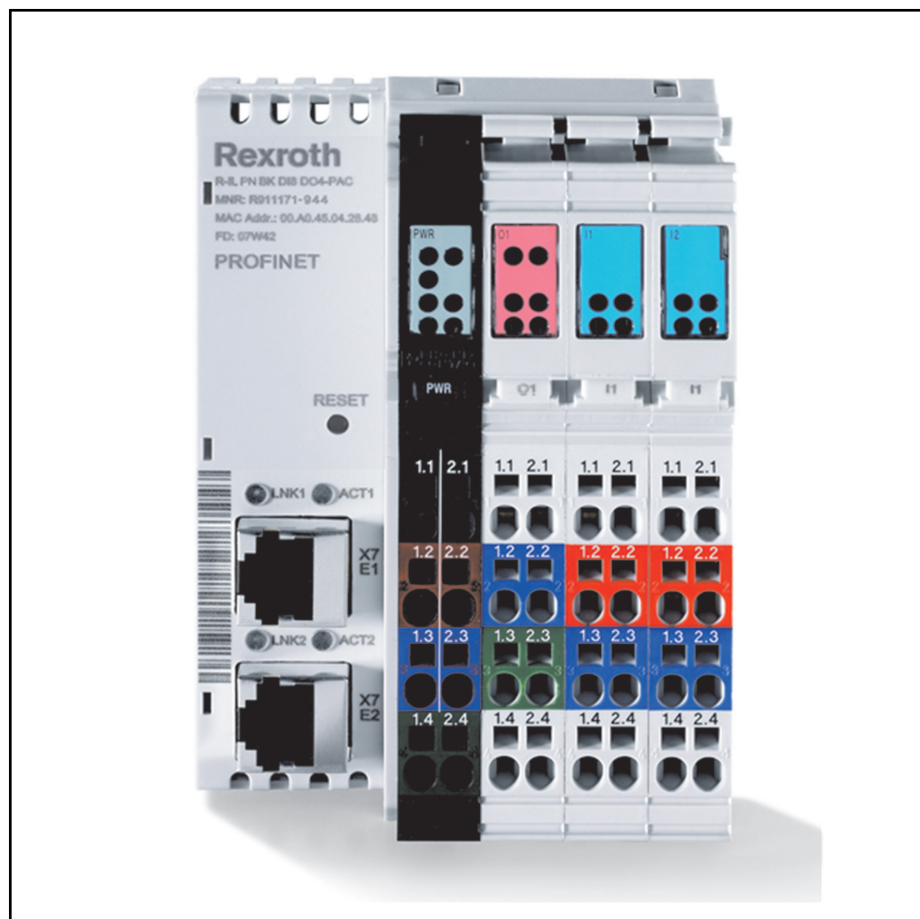


Abb. 5-3: Rexroth Profinet Inline-Buskoppler

Der Profinet Inline-Buskoppler dient zur Einbindung von I/O-Modulen des IndraControl Inline-Bus in Profinet. Profinet lässt strukturell den Anschluss von bis zu 125 Feldbus-Kopplern mit je 61 zusätzlichen I/O-Modulen zu. Die

maximale Anzahl ist abhängig vom eingesetzten Profinet-Master und den zur Verfügung gestellten Nutzdaten der angeschlossenen I/O-Module.

Typenschlüssel: R-IL PN BK DI8 DO4-PAC

Materialnummer: R911171944

Überblick der Feldbus-Koppler-Eigenschaften:

- acht digitale Eingänge, Typ 1, 24 V DC
- vier digitale Ausgänge, 24 V DC, 0,5 A
- modular erweiterbar um bis zu 61 externe I/O-Module
- bis zu 16 sichere I/O-Module anschließbar
- Maximal 16 PCP-Teilnehmer anschließbar. Jedes sichere Inline-I/O-Modul stellt einen PCP-Teilnehmer dar
- typ. 512 Byte je Datenrichtung Prozessdaten
- Parametrierung und Konfiguration mittels GSDML inkl. Diagnose

Eine ausführliche Beschreibung finden Sie in der Dokumentation

- "Rexroth Inline-Buskoppler für Profinet mit digitalen Eingängen und Ausgängen R-IL PN BK DI8 DO4-PAC", Materialnummer [R911328681](#)



- Für die Verwendung der Inline-PROFISafe-Module (PSDx) muss der Profinet Inline-Buskoppler mindestens die Firmware-Version 3.30 haben
- PROFISafe-Geräte auf Basis Profinet dürfen nur am on-Board Profinet-IO-Controller der Standard-Steuerungen CML45/75/85 betrieben werden.

Der Betrieb von PROFISafe-Geräten am Profinet-IO-Controller-Funktionsmodul (CFL01.1-TP) ist nicht freigegeben.

Inline-Module

Das Rexroth Inline System für Profibus und Profinet besteht aus folgenden PROFISafe-fähigen Komponenten:

Typenschlüssel	Kurzbeschreibung	Materialnummer
R-IB IL 24 PSDI 8-PAC	PROFISafe Modul mit 8 sicheren digitalen Eingängen; DC 24 V	R911172846
R-IB IL 24 PSDI 16-PAC	PROFISafe Modul mit 16 sicheren digitalen Eingängen; DC 24 V	R911173314
R-IB IL 24 PSDO 8-PAC	PROFISafe Modul mit 8 sicheren digitalen Ausgängen; DC 24 V	R911172847
R-IB IL 24 PSDOR 4-PAC	PROFISafe Modul mit 4 sicheren Relais-Ausgängen	R911172848
R-IB IL 24 PSDO 4/4-PAC	PROFISafe Module mit 4 sicheren digitalen Ausgängen; konfigurierbar plus- oder minusschaltend	R911172849

Tab. 5-1: Übersicht PROFISafe-I/O-Module



Abb. 5-4: PROFISafe-fähige I/O-Module

Die Inline-Klemmen belegen die folgende Anzahl Bytes im Konfigurationskanal:

Safety Inline-Klemme	Kommunikationsdaten	Anzahl der Bytes im Konfigurationskanal
R-IB IL 24 PSDI 8	8	54
R-IB IL 24 PSDI 16	16	36
R-IB IL 24 PSDO 8	8	60
R-IB IL 24 PSDO 4/4	8	48
R-IB IL 24 PSDOR 4	8	48

Tab. 5-2: PROFISafe-Kanalbelegung durch Safety Inline-Klemmen

Diese PROFISafe Inline-Module können an die oben aufgeführten Inline-Buskoppler angereicht werden.

5.4 Hardware für das Rexroth IndraControl S20 System

Einführung IndraControl S20 von Bosch Rexroth ist ein High-Speed Realtime-I/O-System.

Die Kommunikation zum übergeordneten System erfolgt über ein Ethernet-basierendes Protokoll (z. B. Profinet oder Sercos).

Innerhalb der Produktfamilie IndraControl S20 stehen Module mit verschiedenen Funktionen zur Verfügung, z. B. Buskoppler, Standard Ein- und Ausgabemodule, sichere Ein- und Ausgabemodule, Module zur Temperaturerfassung etc..

Sichere IndraControl S20 Klemmen sind in gelber Farbe ausgeführt. Die sichere Kommunikation erfolgt über "CIP Safety on Sercos" (CSos).

Sercos Buskoppler S20-S3-BK+

Abb. 5-5: Rexroth Sercos Buskoppler S20-S3-BK+

Der Buskoppler ist zum Einsatz innerhalb eines Sercos Netzwerks der dritten Generation vorgesehen und stellt das Bindeglied zum IndraControl S20 System dar.

Er ist modular erweiterbar mit S20 Modulen. An ein bestehendes Sercos Netzwerk können Sie mit Hilfe des Buskopplers bis zu 63 S20 Teilnehmer anschließen.

Typenschlüssel: S20-S3-BK+

Materialnummer: R911173318

Überblick der Feldbus-Koppler-Eigenschaften:

- 2 Ethernet-Ports
- Übertragungsrate 100 MBit/s bei einer minimalen Sercos Zykluszeit von 31,25 µs
- Sercos Diagnose-LED
- Unterstützung von bis zu 63 Safety-I/O-Module (CSos-IO-Module)

Die Anzahl der anschließbaren CSos-I/O-Module ist begrenzt durch die Stromaufnahme aus der Logikspannung des Buskopplers

Folgende CSos-I/O-Module lassen sich am Sercos Buskoppler S20-S3-BK+ betreiben:

Typenschlüssel	Kurzbeschreibung	Materialnummer
S20-SSDI-8/4	8 einkanalige oder 4 zweikanalige sichere Eingänge in 4-Leiter-Anschlussstechnik	R911173191
S20-SSDO-8/3	8 einkanalige oder 4 zweikanalige sichere Ausgänge in 3-Leiter-Anschlussstechnik	R911173192

Tab. 5-3: Übersicht CSos-I/O-Module



Abb. 5-6: Sercos CSos I/O-Module

Eine ausführliche Beschreibung finden Sie in den Dokumentationen:

- "Rexroth IndraControl S20-Buskoppler für Sercos", Materialnummer [R911342781](#)
- Anwendungsbeschreibung "Rexroth IndraControl S20: System und Installation", Materialnummer [R911335987](#)
- Anwendungsbeschreibung "IndraControl S20-Modul mit sicheren digitalen Eingängen S20-SSDI-8/4", Materialnummer [R911342479](#)
- Anwendungsbeschreibung "IndraControl S20-Modul mit sicheren digitalen Ausgängen S20-SSDO-8/3", Materialnummer [R911342481](#)

Profibus Buskoppler S20-PB-BK



Abb. 5-7: Rexroth Profibus Buskoppler S20-PB-BK

Der Buskoppler ist zum Einsatz innerhalb eines Profibus-Netzwerks vorgesehen und stellt das Bindeglied zum IndraControl S20 System dar.

Er ist modular erweiterbar mit S20 Modulen. An ein bestehendes Profibus-Netzwerk können Sie mit Hilfe des Buskopplers bis zu 63 S20 Teilnehmer anschließen.

Typenschlüssel: S20-PB-BK

Materialnummer: R911173247

Überblick der Feldbus-Koppler-Eigenschaften:

- RS-485 für PROFIBUS
 - Übertragungsrate 9,6 kBit/s bis zu 12 MBit/s (automatische Erkennung)
 - Diagnose-LED
 - Unterstützung von bis zu 4 Safety-I/O-Module (PROFIsafe-IO-Module)
- Die Anzahl der anschließbaren PROFIsafe-I/O-Module ist begrenzt durch die Stromaufnahme aus der Logikspannung des Buskopplers

Folgende PROFIsafe-I/O-Module lassen sich am Profibus Buskoppler S20-PB-BK betreiben:

Typenschlüssel	Kurzbeschreibung	Materialnummer
S20-PSDI-8/4	8 einkanalige oder 4 zweikanalige sichere Eingänge in 4-Leiter-Anschlussstechnik	R911173254
S20-PSDO-8/3	8 einkanalige oder 4 zweikanalige sichere Ausgänge in 3-Leiter-Anschlussstechnik	R911173255

Tab. 5-4: Übersicht PROFIsafe-I/O-Module



Abb. 5-8: PROFINET PROFIsafe I/O-Module

Eine ausführliche Beschreibung finden Sie in den Dokumentationen:

- "Rexroth IndraControl S20-Buskoppler für PROFINET", Materialnummer [R911342783](#)
- Anwendungsbeschreibung "Rexroth IndraControl S20: System und Installation", Materialnummer [R911335987](#)
- Anwendungsbeschreibung "IndraControl S20-Modul mit sicheren digitalen Eingängen S20-PSDI-8/4", Materialnummer [R911369170](#)
- Anwendungsbeschreibung "IndraControl S20-Modul mit sicheren digitalen Ausgängen S20-PSDO-8/3", Materialnummer [R911369166](#)

PROFINET Buskoppler S20-PN-BK+



Abb. 5-9: Rexroth PROFINET Buskoppler S20-PN-BK+

Der Buskoppler ist zum Einsatz innerhalb eines PROFINET-Netzwerks vorgesehen und stellt das Bindeglied zum IndraControl S20 System dar.

Er ist modular erweiterbar mit S20 Modulen. An ein bestehendes PROFINET-Netzwerk können Sie mit Hilfe des Buskopplers bis zu 63 S20 Teilnehmer anschließen.

Typenschlüssel: S20-PN-BK+

Materialnummer: R911173359

Überblick der Feldbus-Koppler-Eigenschaften:

- 2 Ethernet-Ports
- Übertragungsrate 100 MBit/s
- Diagnose-LED
- Unterstützung von bis zu 63 Safety-I/O-Module (PROFIsafe-I/O-Module)
Die Anzahl der anschließbaren PROFIsafe-I/O-Module ist begrenzt durch die Stromaufnahme aus der Logikspannung des Buskopplers

Folgende PROFIsafe-I/O-Module lassen sich am PROFINET Buskoppler S20-PN-BK+ betreiben:

Typenschlüssel	Kurzbeschreibung	Materialnummer
S20-PSDI-8/4	8 einkanalige oder 4 zweikanalige sichere Eingänge in 4-Leiter-Anschlusstechnik	R911173254
S20-PSDO-8/3	8 einkanalige oder 4 zweikanalige sichere Ausgänge in 3-Leiter-Anschlusstechnik	R911173255

Tab. 5-5: Übersicht PROFIsafe-I/O-Module



Abb. 5-10: PROFINET PROFIsafe I/O-Module

Eine ausführliche Beschreibung finden Sie in den Dokumentationen:

- "Rexroth IndraControl S20-Buskoppler für PROFINET", Materialnummer [R911342783](#)
- Anwendungsbeschreibung "Rexroth IndraControl S20: System und Installation", Materialnummer [R911335987](#)
- Anwendungsbeschreibung "IndraControl S20-Modul mit sicheren digitalen Eingängen S20-PSDI-8/4", Materialnummer [R911369170](#)
- Anwendungsbeschreibung "IndraControl S20-Modul mit sicheren digitalen Ausgängen S20-PSDO-8/3", Materialnummer [R911369166](#)

5.5 Antriebssystem Rexroth IndraDrive

5.5.1 Was versteht man unter "Integrierter Sicherheitstechnik (Safe Motion)"?

IndraDrive Cs Die Steuerteile der Antriebsfamilie IndraDrive Cs können mit den Optionsmodulen "S4", "S5" und "SB" ausgerüstet werden.

Durch die genannten Optionsmodule wird IndraDrive Cs mit integrierter Sicherheitstechnik ausgestattet, die dem Anwender eine universell parametrierbare sichere Bewegungs- bzw. Stillstandsüberwachung bietet.

Die **geberabhängigen** Sicherheitsfunktionen sind gemäß ISO 13849-1 Kategorie 3, PL d und IEC 62061 SIL 2 und die **geberunabhängigen** Sicherheitsfunktionen gemäß ISO 13849-1 Kategorie 4, PL e und IEC 62061 SIL 3 für den Personenschutz an Maschinen anwendbar.

Mit dem optionalen Erweiterungspaket "SIL3-MOTION" bzw. "SIL3-PLUS" können auch die **geberabhängigen** Sicherheitsfunktionen gemäß IEC 62061 SIL 3 für den Personenschutz an Maschinen angewendet werden.

IndraDrive Mi Die Antriebssysteme IndraDrive Mi mit dem motorintegrierten Servoantrieb KSM02 und dem motornahen Servoantrieb KMS02 können mit dem Optionsmodul "S3" [Safe Motion (ohne SBC)] ausgerüstet werden.

Durch das Optionsmodul "S3" wird IndraDrive Mi mit integrierter Sicherheitstechnik ausgestattet, die dem Anwender eine universell parametrierbare sichere Bewegungs- bzw. Stillstandsüberwachung bietet.

Die Antriebssysteme IndraDrive Mi mit dem motorintegrierten Servoantrieb KSM02 und den motornahen Servoantrieben KMS02 / KMS03 können mit dem Optionsmodul "SD" [Safe Motion (mit SBC)] ausgerüstet werden.

Die **geberabhängigen** Sicherheitsfunktionen sind gemäß ISO 13849-1 Kategorie 3, PL d und IEC 62061 SIL 2 und die **geberunabhängigen** Sicherheitsfunktionen gemäß ISO 13849-1 Kategorie 4, PL e und IEC 62061 SIL 3 für den Personenschutz an Maschinen anwendbar.

Mit dem optionalen Erweiterungspaket "SIL3-MOTION" bzw. "SIL3-PLUS" können auch die **geberabhängigen** Sicherheitsfunktionen gemäß IEC 62061 SIL 3 für den Personenschutz an Maschinen angewendet werden.

Mit der Ansteuerelektronik KCU02.2 sind die Sicherheitsfunktionen gemäß ISO 13849-1 Kategorie 3, PL d und IEC 62061 SIL 3 für den Personenschutz an Maschinen anwendbar.

Mit der Ansteuerelektronik KCU02.3 sind die Sicherheitsfunktionen gemäß ISO 13849-1 Kategorie 4, PL e und IEC 62061 SIL 3 für den Personenschutz an Maschinen anwendbar.



Für die Nutzung der integrierten Sicherheitstechnik "S3"/"SD" muss mindestens die Ausführung "2" oder höher der Ansteuerelektronik KCU02 verwendet werden.

**IndraDrive ML / IndraDrive M /
IndraDrive C**

Die Steuerteile Cxx02 der Antriebsfamilie IndraDrive ML / IndraDrive M / IndraDrive C können mit den Optionsmodulen "S4", "S5" und "SB" ausgerüstet werden.

Durch die genannten Optionsmodule wird IndraDrive ML / IndraDrive M / IndraDrive C mit integrierter Sicherheitstechnik ausgestattet, die dem Anwender eine universell parametrierbare sichere Bewegungs- bzw. Stillstandsüberwachung bietet.

Die **geberabhängigen** Sicherheitsfunktionen sind gemäß ISO 13849-1 Kategorie 3, PL d und IEC 62061 SIL 2 und die **geberunabhängigen** Sicherheitsfunktionen gemäß ISO 13849-1 Kategorie 4, PL e und IEC 62061 SIL 3 für den Personenschutz an Maschinen anwendbar.

gigen Sicherheitsfunktionen gemäß ISO 13849-1 Kategorie 4, PL e und IEC 62061 SIL 3 für den Personenschutz an Maschinen anwendbar.

Mit dem optionalen Erweiterungspaket "SIL3-MOTION" bzw. "SIL3-PLUS" können auch die **geberabhängigen** Sicherheitsfunktionen gemäß IEC 62061 SIL 3 für den Personenschutz an Maschinen angewendet werden.

Anwahl der Funktion

Die Sicherheitsfunktionen können wie folgt angewählt werden:

- zentral über 24 V-Eingänge eines Sicherheitszonenmoduls (HSZ01) (bei IndraDrive Mi nicht möglich)
- über die sichere Buskommunikation
- ab MPx-21: über die als sichere Eingänge konfigurierten Eingänge der Sicherheitstechnik-Optionsmodule "S3", "S4", "S5" und "SD"

Zertifizierung

Die Sicherheitstechnik ist vom TÜV Rheinland ® zertifiziert worden; eine NRTL-Listung durch den TÜV Rheinland of North America ist in Vorbereitung.



Zertifikate sind auf "[Certipedia](#)", der Zertifikatsdatenbank des TÜV Rheinland ® erhältlich.

Realisierbare Anforderungen

Die integrierte Sicherheitstechnik ist unabhängig von der Art der Führungskommunikation, der übergeordneten Steuerung und der Versorgungsmodule. Sie wird als funktionale Ausprägung zum Standard-Antriebssystem angeboten. Folgende Anforderungen sind in der Maschine oder in der Anlage realisierbar:

- Maßnahmen nach ISO 12100-2, wenn der Zugang zum Gefahrenbereich, beispielsweise zum Einrichten, Teachen oder Materialentnahme notwendig wird.
- Anforderungen für sicherheitsbezogene Teile von Steuerungen gemäß ISO 13849-1 Kategorie 4, PL e und IEC 62061 SIL 3, wie gefordert in EN 1010-1 (Druck- u. Papierverarbeitungsmaschinen), ISO 23125 (Drehmaschinen) und EN 12417 (Bearbeitungszentren).
- Steuerfunktionen im Fehlerfall gemäß IEC 60204-1 ("homogene Redundanz").

5.5.2 Unterstützte Sicherheitstechnikfunktionen

Die folgende Tabelle zeigt die Abhängigkeit von Sicherheitsfunktionen, SIL und der Verfügbarkeit bei den Sicherheitsoptionsmodulen.

Sichere Bussysteme

Sicherheitstechnikfunktion	Verfügbarkeit bei Sicherheitstechnik-Optionsmodul					SIL	Bemerkung
	IndraDrive Mi		IndraDrive Cs, IndraDrive M / IndraDrive C (Steuerteil Cxx02) und IndraDrive ML				
	S3 (KMS02 und KSM02)	SD (KSM02, KMS02 und KMS03)	S4	S5	SB		
Sichere Zonenquittierung [Safety Zone Acknowledge (SZA)] Die Sicherheitstechnikfunktion ist nur in Verbindung mit Sicherheitszonenmodul (HSZ01) nutzbar. Mit Hilfe von "Sichere Zonenquittierung" und dem Sicherheitszonenmodul "HSZ" kann die Sicherheit einer Sicherheitszone von einem Quittungsmaster überwacht und an eine übergeordnete Steuerung quittiert werden. Es ist ebenfalls möglich, dass der Quittungsmaster der Sicherheitszone direkt eine an das Sicherheitszonenmodul angeschlossene Schutztürverriegelung ansteuert.	–	–	✓	✓	–	3	
Sichere Schutztürzuhaltung [Safe Door Locking (SDL)] Die Sicherheitstechnikfunktion ist nur in Verbindung mit Sicherheitszonenmodul (HSZ01) nutzbar. Es wird die Zuhaltung einer verriegelten trennenden Schutzeinrichtung zweikanalig angesteuert, wenn die sichere Zonenquittierung "Sicherheit" meldet und der Anwender per Taster das Entriegeln der Schutztür anfordert. Es findet eine sichere Überwachung der Stellung der Verriegelung statt.	–	–	✓	✓	–	3	
Sichere Zonenfehler [Safe Zone Error (SZE)] Die Sicherheitstechnikfunktion ist nur in Verbindung mit Sicherheitszonenmodul (HSZ01) nutzbar. Die Funktion "Sicherer Zonenfehler" ist eine Teilfunktion der Sicherheitsfunktion "Sichere Zonenquittierung". Die Funktion "Sicherer Zonenfehler" ermöglicht den Zonenteilnehmern lokal anstehende Sicherheitstechnikfehler über einen sicheren Ausgang an alle Zonenteilnehmer zu melden und individuelle Fehlerreaktionen auszulösen. Es ist ebenfalls möglich, dass der Quittungsmaster einer Sicherheitszone Zonenfehler über die sichere Kommunikation an die übergeordnete Steuerung meldet.	–	–	✓	✓	–	3	
Sicher abgeschaltetes Moment [Safe Torque Off (STO)] Die Energieversorgung zum Antrieb ist sicher unterbrochen. Der Antrieb kann kein Drehmoment/keine Kraft und somit keine gefährlichen Bewegungen erzeugen.	✓	✓	✓	✓	✓	3	
Sicherer Betriebshalt [Safe Operating Stop (SOS)] Bei der Sicherheitsfunktion "Sicherer Betriebshalt" befindet sich der Antrieb im geregelten Stillstand; d. h. alle Regelfunktionen zwischen der elektronischen Steuerung und dem Antrieb bleiben erhalten. Mittels einer zweikanaligen Überwachung wird verhindert, dass der Antrieb aufgrund von Fehlern gefährliche Bewegungen ausführen kann, obwohl die Energieversorgung nicht unterbrochen wird.	✓	✓	✓	✓	✓	2 / 3*	* nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht

Sicherheitstechnikfunktion	Verfügbarkeit bei Sicherheitstechnik-Optionsmodul					SIL	Bemerkung
	IndraDrive Mi		IndraDrive Cs, IndraDrive M / IndraDrive C (Steuerteil Cxx02) und IndraDrive ML				
	S3 (KMS02 und KSM02)	SD (KSM02, KMS02 und KMS03)	S4	S5	SB		
Sichere Bremsenansteuerung [Safe Brake Control (SBC)] Bei der Sicherheitsfunktion "Sichere Bremsenansteuerung" wird die angeschlossene Bremse sicher (2-kanalig) abgeschaltet.	✓ ^{1) 2)}	✓	✓ ²⁾	✓ ²⁾	✓ ²⁾	3	¹⁾ ab MPx-21 verfügbar ²⁾ Die Sicherheitstechnikfunktion ist bei IndraDrive M / IndraDrive C (Steuerteil Cxx02), IndraDrive ML und IndraDrive Mi mit Sicherheitstechnik-Optionsmodul "S3" nur in Verbindung mit einer Ansteuereinheit (HAT02.1) nutzbar.
Sicheres Brems- und Haltesystem [Safe Braking and Holding System (SBS)] Bei der Sicherheitsfunktion "Sicheres Brems- und Haltesystem" werden ungewollte Achsbewegungen (z. B. bei Vertikalachsen) sicher verhindert, auch wenn sich der Antrieb nicht in Regelung befindet.	–	✓	✓	✓	–	3	ab MPx-21 verfügbar mit Firmware-Option (FWS) "SAFETY-PLUS" oder "SIL3-PLUS" Sicherheitsfunktion "SBT" wird benötigt
Sichere maximale Geschwindigkeit [Safe Maximum Speed (SMS)] Bei der Sicherheitsfunktion "Sichere maximale Geschwindigkeit" wird durch eine zweikanalige Überwachung verhindert, dass der Antrieb den vorgegebenen Geschwindigkeitsgrenzwert überschreitet.	✓	✓	✓	✓	✓	2 / 3*	* nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht
Sichere Bewegungsrichtung [Safe Direction (SDI)] Bei der Sicherheitsfunktion "Sichere Bewegungsrichtung" wird durch eine zweikanalige Überwachung gewährleistet, dass eine Bewegung nur in eine Richtung möglich ist.	✓	✓	✓	✓	✓	2 / 3*	* nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht
Sicher begrenzte Geschwindigkeit [Safely-Limited Speed (SLS)] Bei der Sicherheitsfunktion "Sicher begrenzte Geschwindigkeit" wird zweikanalig überwacht, dass der Antrieb eine zuvor festgelegte Begrenzung des Geschwindigkeitsfensters nicht überschreitet.	✓	✓	✓	✓	✓	2 / 3*	* nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht
Sicher überwachttes Einschwingen [Safely-Monitored Transient Oscillation (SLS-LT)] Bei der Sicherheitsfunktion "Sicher überwachttes Einschwingen" wird mit Hilfe eines Geschwindigkeitsfenster und einer Toleranzzeit das Einschwingen auf eine "Sicher begrenzte Geschwindigkeit" überwacht.	✓	✓	✓	✓	✓	2 / 3*	* nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht
Sicher begrenztes Schrittmaß [Safely-Limited Increment (SLI)] Bei der Sicherheitsfunktion "Sicher begrenztes Schrittmaß" wird zweikanalig überwacht, dass der Antrieb sich nur innerhalb des maximalen Schrittmaßes bewegt.	✓	✓	✓	✓	✓	2 / 3*	* nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht

Sichere Bussysteme

Sicherheitstechnikfunktion	Verfügbarkeit bei Sicherheitstechnik-Optionsmodul					SIL	Bemerkung
	IndraDrive Mi		IndraDrive Cs, IndraDrive M / IndraDrive C (Steuerteil Cxx02) und IndraDrive ML				
	S3 (KMS02 und KSM02)	SD (KSM02, KMS02 und KMS03)	S4	S5	SB		
Sicherer Stopp 1 (SS1) Wird die Überföhrfunktion "Sicherer Stopp 1 (SS1)" aktiviert, so wird der Antrieb sicher überwacht stillgesetzt. Nach Abschluss des Stillsetzvorgangs wird die Sicherheitsfunktion "Sicher abgeschaltetes Moment (STO)" aktiviert und die Energieversorgung zum Motor wird sicher unterbrochen. Der Motor kann kein Drehmoment/keine Kraft und somit keine gefährlichen Bewegungen erzeugen.	✓	✓	✓	✓	✓	3 2 / 3*	SS1, zeitüberwacht SS1, Überwachung der Verzögerung * nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht
Sicherer Stopp 2 [Safe Stop 2 (SS2)] Wird die Überföhrfunktion "Sicherer Stopp 2" aktiviert, so wird der Antrieb sicher überwacht stillgesetzt. Nach Abschluss des Stillsetzvorgangs wird die Sicherheitsfunktion "Sicherer Betriebshalt" aktiviert und sicher verhindert, dass der Motor um mehr als einen festgelegten Betrag von der Halteposition abweicht.	✓	✓	✓	✓	✓	2 / 3*	* nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht
Sicher überwachte Verzögerung [Safely-Monitored Deceleration (SMD)] Bei der Sicherheitsfunktion "Sicher überwachte Verzögerung" wird bei einem Betriebszustandswechsel oder einer Fehlerreaktion zweikanalig überwacht, ob die Istgeschwindigkeit des Antriebs innerhalb einer parametrisierten Geschwindigkeits-Hüllkurve liegt.	✓	✓	✓	✓	✓	2 / 3*	* nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht
Sicher überwachte Position [Safely Monitored Position (SMP)] Bei der Sicherheitsfunktion "Sicher überwachte Position" wird überwacht, ob der parametrisierte Lagebereich in positiver oder negativer Richtung überschritten wird.	✓	✓	✓	✓	✓	2	ab MPx-20V06 verfügbar mit Firmware-Option (FWS) "SAFETY-PLUS" oder "SIL3-PLUS"
Sicher begrenzte Position [Safely Limited Position (SLP)] Bei der Sicherheitsfunktion "Sicher begrenzte Position" wird zweikanalig überwacht, dass der Antrieb mit der aktuellen Geschwindigkeit und der parametrisierten minimalen Verzögerung noch innerhalb der parametrisierten Lagegrenzen stillgesetzt werden kann.	✓	✓	✓	✓	✓	2	ab MPx-20V06 verfügbar mit Firmware-Option (FWS) "SAFETY-PLUS" oder "SIL3-PLUS"
Sicher begrenzte Endlage [Safely Limited End Position (SLE)] Bei der Sicherheitsfunktion "Sicher begrenzte Endlage" wird zweikanalig überwacht, dass der Antrieb mit der aktuellen Geschwindigkeit und der parametrisierten minimalen Verzögerung noch innerhalb der parametrisierten Endlage-Grenzwert stillgesetzt werden kann.	✓	✓	✓	✓	✓	2	ab MPx-20V06 verfügbar mit Firmware-Option (FWS) "SAFETY-PLUS" oder "SIL3-PLUS"
Sichere Nocken [Safe CAM (SCA)] Bei der Sicherheitsfunktion "Sichere Nocken" wird zweikanalig überwacht, ob sich die Achse innerhalb eines definierten Positionsbereich (Nockenbereich) befindet. Das Ergebnis wird über Statuswörter zur Verfügung gestellt.	✓	✓	✓	✓	✓	2	ab MPx-20V08 verfügbar mit Firmware-Option (FWS) "SAFETY-PLUS" oder "SIL3-PLUS"

Sicherheitstechnikfunktion	Verfügbarkeit bei Sicherheits- technik-Optionsmodul					SIL	Bemerkung
	IndraDrive Mi		IndraDrive Cs, IndraDrive M / IndraDrive C (Steuerteil Cxx02) und IndraDrive ML				
	S3 (KMS02 und KSM02)	SD (KSM02, KMS02 und KMS03)	S4	S5	SB		
Sicherer Geschwindigkeitswächter [Safe Speed Monitor (SSM)] Bei der Sicherheitsfunktion "Sicherer Geschwindigkeitswächter" wird zweikanalig beobachtet, ob sich die Achse innerhalb eines definierten Geschwindigkeitsbereichs befindet. Das Ergebnis wird über Statuswörter zur Verfügung gestellt.	✓	✓	✓	✓	✓	2 / 3*	ab MPx-21 verfügbar * nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht
Sicheres Referenzieren (Safe Homing Procedure) Bei der Hilfsfunktion "Sicheres Referenzieren" wird im Anschluss an das funktionale Referenzieren, an einer separaten Position ein weiteres Referenzereignis erwartet. Das zweite Referenzereignis dient zum Plausibilisieren des funktionalen Referenzierens.	✓	✓	✓	✓	✓	2	ab MPx-20V06 verfügbar
Sicherer Bremsentest [Safe Brake Test (SBT)] Bei der Hilfsfunktion "Sicherer Bremsentest" wird regelmäßig zweikanalig überprüft, ob eine oder zwei über SBC angesteuerte Bremsen noch funktionsfähig sind und ein definiertes Haltemoment aufbringen.	✓	✓	✓	✓	✓	2 / 3*	ab MPx-21 verfügbar * nur mit Firmware-Option (FWS) "SIL3-MOTION" oder "SIL3-PLUS" wird SIL 3 erreicht

Tab. 5-6: Funktionen zur sicheren Bewegungs- bzw. Stillstandsüberwachung



Sicherheitstechnik-Optionsmodule können "im Feld" weder nachgerüstet noch getauscht werden; d. h. Antriebsregelgeräte müssen ab Werk mit der benötigten Sicherheitstechnik-Option bestellt werden.

5.6 Profibus-DP bzw. PROFINET mit PROFISafe

5.6.1 Allgemeines

PROFISafe wurde 1999 in der Version V1 als sicherheitsbezogenes Profil ausschließlich für Profibus-DP spezifiziert und mittlerweile (2004) in der Release V1.3 veröffentlicht.

PROFISafe gibt es in den Versionen V1 (bis 2004, ausschließlich für Profibus-DP) und V2 für Profibus-DP und Profinet.

PROFISafe in Version V2 ist in der internationalen Norm IEC 61784-3-3 standardisiert.



Weitergehende Informationen zu PROFISafe enthalten Sie bei der Profibus Nutzer Organisation (PNO).

Achten Sie darauf, dass Sie immer die aktuellsten Dokumente zu Profibus-DP bzw. Profinet und PROFISafe verwenden.

Das Safety-Funktionsmodul unterstützt sowohl die Anwendung von PROFISafe V2-Geräten. Das Programmiersystem unterscheidet dies bei der Konfiguration anhand der GSD-Datei (Generic Station Description).

5.6.2 Anwendung von PROFISafe

Aufbau und Umgebungsbedingungen

Bei der Anwendung von PROFISafe am Profibus-DP bzw. PROFINET müssen Sie bei der Projektierung Ihrer Maschine oder Anlage die allgemeinen Anforderungen von Profibus bzw. Profinet und die speziellen Anforderungen von PROFISafe an den Aufbau, die Systemgrenzen und die Umgebungsbedingungen des Profibus- bzw. Profinet-Systems berücksichtigen.



Achten Sie darauf, dass Sie immer die aktuellsten Dokumente zu Profibus-DP bzw. Profinet und PROFISafe verwenden.

Bei Einhaltung aller Vorgaben können Sie die PROFISafe-Datenkommunikation bis SIL3 nach IEC 61508 bzw. IEC 62061 oder PL e nach EN ISO 31849-1 einsetzen. Für die Berechnung der Ausfallraten Ihres Systems bzw. ihrer Sicherheitsfunktionen können Sie für die sichere Datenkommunikation mit PROFISafe die folgende Restfehlerrate einsetzen:

$$\Lambda = 3 \cdot 10^{-10}$$

Abb. 5-11: Restfehlerrate PROFISafe

Konfiguration

Fügen Sie zunächst ihre sicheren PROFISafe-Geräte in die Topologie Ihres Profibus-DP- und/oder Profinet-Systems ein. Dazu entnehmen Sie wie bei Standard-Geräten die einzusetzenden PROFISafe-Geräte der Gerätebibliothek des Programmiersystems und binden die PROFISafe-Geräte an den gewünschten Positionen in den Gerätebaum Ihrer Applikation ein. Die Geräte sind durch ihre GSD- bzw. GSDML-Dateien beschrieben und mit einer Grundparametrierung versehen.

Aufgrund dieser Informationen stellt Ihnen das Programmiersystem für jedes PROFISafe-Gerät eine Reihe von Konfigurations- und Parametrierungsfenster zur Verfügung, in deren Rahmen Sie alle Konfigurations- und Parametrierungseinstellungen vornehmen können.

- Safety Parameter (PROFISafe F-Parameter)
- Safety Mapping (I/O-Kanäle)
- I-Parameter (individuelle Parameter, falls vorhanden)
- Status (Anzeige von Geräte-Diagnosemeldungen)
- Information (allgemeine Information über das Gerät, welche der Gerätebeschreibung entnommen sind: Name, Hersteller, Version, Bestellnummer, Beschreibung, Bild)

Im Fenster "I/O-Abbild" ordnen Sie die I/O-Kanäle des Gerätes den symbolischen Variablen zu, die Sie in Ihrer Sicherheitslogik verwenden.

Parametrierung

Die PROFISafe-Spezifikation beschreibt zwei unterschiedliche Parameterarten für PROFISafe-Geräte.

F-Parameter dienen speziell zur Parametrierung der sicheren Kommunikation. Die F-Parameter sind in der Profil-Spezifikation (V1/V2) bzw. in der IEC 61784-3-3 spezifiziert und werden von jedem PROFISafe-Gerät umgesetzt. Die F-Parameter werden bei der Initialisierung im Rahmen des Standard-Profibus-Parametrierungsdialogs an das PROFISafe-Gerät übermittelt. Nach Empfang des gültigen F-Parameter-Satzes sendet ein PROFISafe-Gerät an den Eingängen zur Sicherheitssteuerung Prozessdaten, an den Ausgängen zur Peripherie zunächst Fail-safe-Werte bis von der Sicherheitslogik andere

Werte vorgegeben werden. Die Einträge der F-Parameter im Konfigurationsfenster werden mit den Werten in dem sicheren Gerät verglichen, im Falle der Adressen und der Überwachungszeit sogar ständig während der zyklischen Kommunikation. Unterschiede führen zu einer Fehlerreaktion und Diagnosemeldung.

Gerätespezifische Parameter werden als I-Parameter bezeichnet. Die I-Parameter werden in den einzelnen Gerätebeschreibungen beschrieben.

Allgemeine Beschreibung der F-Parameter

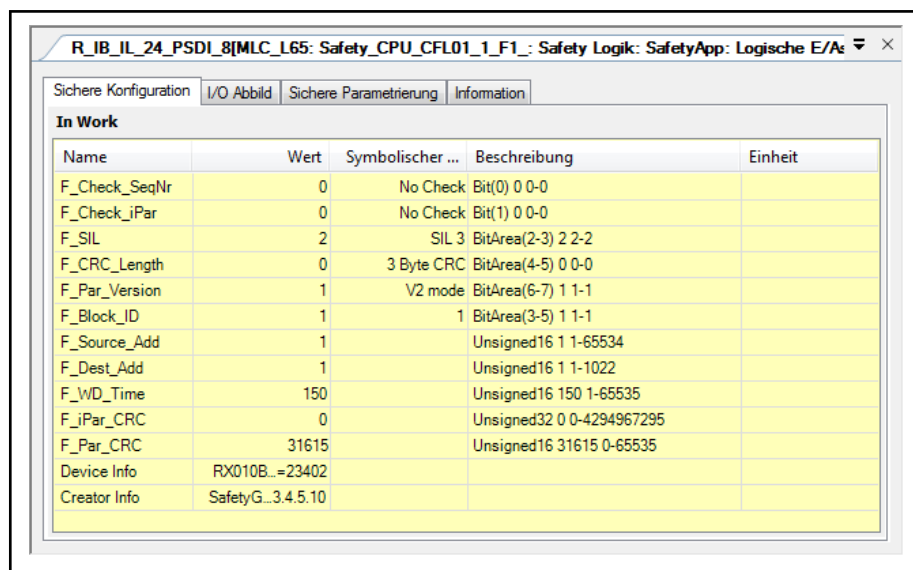
Parameter	Bedeutung	Wertebereich
F_SlotNumber	Modul-Nummer innerhalb einer modularen Profibus- bzw. Profinet-Station	Geräteabhängig
F_Check_SeqNr	Wird die Consecutive-Number in die CRC2-Signature eingerechnet oder nicht? Nur relevant für V1. Bei V2 immer 0, Eintrag ist Don't care In der Regel 0 (No Check)	0: nein 1: ja
F_Check_iPar	Verwendung Gerätespezifisch. Siehe Gerätebeschreibung In der Regel 0 (No Check)	0: nein 1: ja
F_SIL	Das sichere Gerät vergleicht seinen SIL mit dem hier zugewiesenen	00: SIL1 01: SIL2 10: SIL3 11: No SIL
F_CRC_Length	Die CRC2-Signatur kann unterschiedliche Länge haben: 2 Byte (nur im V1-Mode) 3 Byte (nur im V2-Mode) 4 Byte (optional im V1- oder V2-Mode)	00: 3 Byte 01: 2 Byte 10: 4 Byte 11: reserviert
F_Block_ID	F-Parameter-Typidentifikation: 0 = keine F-iPar_CRC im F-Parameterblock 1 = F-iPar_CRC im F-Parameterblock	0-1
F_Par_Version	Versionsnummer des F-Parameter-Sets 0 = gültig für V1-Mode 1 = gültig für V2-Mode	0-1

Parameter	Bedeutung	Wertebereich
F_Source_Add	Quell-Adresse des Kommunikationskanals; hier PROFISafe-Adresse des Safety-Funktionsmoduls	Unsigned 16
F_Dest_Add	Ziel-Adresse des Kommunikationskanals	Unsigned 16
F_WD_Time	Überwachungszeit für die zyklische Kommunikation, Zeitbasis 1 ms	Geräteabhängig
F_Par_CRC	CRC1-Signatur über die F-Parameter, muss aus der sicheren Parametrierung übernommen werden	Unsigned 16
F_iPar_CRC	CRC-Signatur über die I-Parameter, wird von IndraWorks berechnet und eingetragen	Unsigned 32

Tab. 5-7: Liste der F-Parameter

Die Einträge der F-Parameter im Konfigurationsfenster werden mit den Werten in dem sicheren Gerät verglichen, im Falle der Adressen und der Überwachungszeit sogar ständig während der zyklischen Kommunikation.

Unterschiede führen zu einer Fehlerreaktion und Diagnosemeldung.



The screenshot shows a software window titled 'R_IB_IL_24_PSDI_8[MLC_L65: Safety_CPU_CFL01_1_F1_: Safety Logik: SafetyApp: Logische E/A'. It has tabs for 'Sichere Konfiguration', 'I/O Abbild', 'Sichere Parametrierung', and 'Information'. The 'Sichere Konfiguration' tab is active, showing a table of parameters under the heading 'In Work'.

Name	Wert	Symbolischer ...	Beschreibung	Einheit
F_Check_SeqNr	0	No Check	Bit(0) 0 0-0	
F_Check_iPar	0	No Check	Bit(1) 0 0-0	
F_SIL	2	SIL 3	BitArea(2-3) 2 2-2	
F_CRC_Length	0	3 Byte CRC	BitArea(4-5) 0 0-0	
F_Par_Version	1	V2 mode	BitArea(6-7) 1 1-1	
F_Block_ID	1	1	BitArea(3-5) 1 1-1	
F_Source_Add	1		Unsigned16 1 1-65534	
F_Dest_Add	1		Unsigned16 1 1-1022	
F_WD_Time	150		Unsigned16 150 1-65535	
F_iPar_CRC	0		Unsigned32 0 0-4294967295	
F_Par_CRC	31615		Unsigned16 31615 0-65535	
Device Info	RX010B...=23402			
Creator Info	SafetyG...3.4.5.10			

Abb. 5-12: Beispiel: Konfigurationsfenster und F-Parameter in der SafeLogic

Schnittstelle zur Sicherheitslogik

Die Schnittstelle zwischen PROFISafe-Kanal und Sicherheitslogik wird durch die Ein-/Ausgangsparameter des PROFISafe-Layer-Funktionsbausteins gebildet, der für jeden PROFISafe-Kanal instanziiert wird. Über diese Parameter kann die Sicherheitslogik die PROFISafe-Kommunikation dieses Kanals steuern oder ihren Status abfragen.

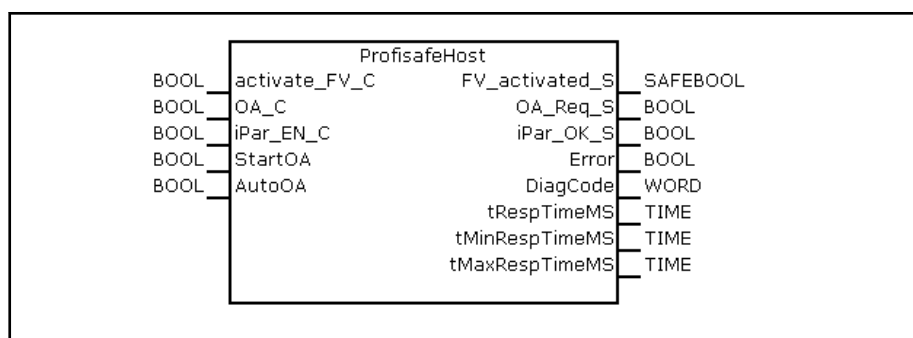


Abb. 5-13: Interface ProfisafeHost-Funktionsbaustein

Sichere Bussysteme

I/O-Typ	Name	Datentyp	Beschreibung
VAR_INPUT	activate_FV_C	BOOL	Eingang nach PROFISafe-Spezifikation, Kapitel 6.1: Aktivierung der Fail-safe Werte TRUE: Die Verwendung von Fail-safe Werten wird erzwungen: Der ProfisafeHost-Stack liefert als Eingangssignale die Fail-safe Werte an die Applikation und schreibt fail-safe Werte als Ausgangssignale an das F-Device FALSE: Die Verwendung von fail-safe Werten wird nicht erzwungen. Es sollen im Normalfall Prozessdaten übertragen werden Vorsicht: Das Rücksetzen dieses Eingangs von TRUE auf FALSE kann zur sofortigen Übertragung der Prozessdaten führen! Stellen Sie durch geeignete Maßnahmen sicher, dass von Ihrer Anlage/Maschine keine Gefahr ausgeht! Default-Wert: FALSE
	OA_C	BOOL	Eingang nach PROFISafe-Spezifikation, Kapitel 6.1: Operator Acknowledgement Mit einer steigenden Flanke des Eingangs wird die Wiederaufnahme der Sicherheitsfunktion nach einem Fehler bestätigt. Nach einer Bestätigung muss der Eingang mindestens einen vollen Zyklus auf FALSE stehen, bevor der nächste Fehler bestätigt werden kann Hinweis: Wenn sowohl "StartOA", als auch "AutoOA" auf TRUE gesetzt sind, wird der Eingang "OA_C" nicht ausgewertet, da alle Anfragen zur Aufnahme der Sicherheitsfunktion automatisch bestätigt werden Default-Wert: FALSE
	iPar_EN_C	BOOL	Eingang nach PROFISafe-Spezifikation, Kapitel 6.1: Aktivierung der I-Parametrierung des F-Device. Dieser Eingang wird im Kontext einer gerätespezifischen I-Parametrierung unter Nutzung eines Proxy-FB verwendet. Falls erforderlich, sollte auch der Eingang "activate_FV_C" auf "1" gesetzt werden. Details entnehmen Sie der Dokumentation des F-Device TRUE: Die I-Parametrierung des F-Device wird aktiviert FALSE: Die I-Parametrierung des F-Device wird nicht aktiviert Default-Wert: FALSE
	StartOA	BOOL	Verhalten nach einem Fehler während der Anlaufphase des F-Device. Die Wirksamkeit des Eingangs "StartOA" erstreckt sich vom erster Start der Applikation bis das F-Device einmal die Sicherheitsfunktion aufgenommen hat TRUE: Automatische Bestätigung zur Aufnahme der Sicherheitsfunktion nach einem Fehler FALSE: Manuelle Bestätigung am Eingang "OA_C" zur Aufnahme der Sicherheitsfunktion des F-Device nach einem Fehler notwendig Default-Wert: TRUE Hinweis: "StartOA" ist keine Anlaufverriegelung!
	AutoOA	BOOL	Wiederanlaufverhalten nach einem Fehler. Vorbedingung: Das F-Device ist erfolgreich angelaufen und hat mindestens einmal die Sicherheitsfunktion aufgenommen TRUE: Automatische Bestätigung zur Wiederaufnahme der Sicherheitsfunktion nach einem Fehler FALSE: Manuelle Bestätigung am Eingang "OA_C" zur Wiederaufnahme der Sicherheitsfunktion des F-Device nach einem Fehler notwendig Default-Wert: FALSE Hinweis: Sind "StartOA" und "AutoOA" TRUE, so werden Fehler immer automatisch bestätigt. Dies ist nur in absoluten Ausnahmefällen sinnvoll

I/O-Typ	Name	Datentyp	Beschreibung
VAR_OUTPUT	FV_activated_S	SAFE- BOOL	Ausgang nach PROFISafe-Spezifikation, Kapitel 6.1: Anzeige Aktivierung der Fail-safe Werte TRUE: Der ProfisafeHost-Stack liefert Fail-safe Werte FALSE: Der ProfisafeHost-Stack liefert Prozessdaten Hinweis: Der Ausgang wechselt auf TRUE, entweder auf Anweisung des Stacks oder aufgrund Übertragungsfehler zum F-Device bzw. interner Fehler im F-Device oder falls der Eingang "activate_FV_C" gleich TRUE ist
	OA_Req_S	BOOL	Ausgang nach PROFISafe-Spezifikation, Kapitel 6.1: Anzeige Operator Acknowledgement Request TRUE: Das F-Device benötigt eine Bestätigung durch den Bediener (Operator Acknowledgement), um die Sicherheitsfunktion wieder aufzunehmen FALSE: Das F-Device benötigt derzeit keine Bestätigung durch den Bediener (Operator Acknowledgement)
	iPar_OK_S	BOOL	Ausgang nach PROFISafe-Spezifikation, Kapitel 6.1: Anzeige Ende I-Parametrierung des F-Device Dieser Ausgang wird im Kontext einer gerätespezifischen I-Parametrierung unter Nutzung eines Proxy-FB verwendet. Details entnehmen Sie der Dokumentation des F-Device TRUE: Das F-Device hat neue I-Parameter erhalten FALSE: Das F-Device hat keine neuen I-Parameter erhalten
	Error	BOOL	Fehleranzeige TRUE: Es liegt ein Fehler vor (DiagCode = 16#Cxxx) FALSE: Es liegt kein Fehler vor (DiagCode = 16#8xxx)
	DiagCode	WORD	Verwendung des Ausganges DiagCode als Diagnose-Code, Initialwert 16#0000
	tRespTimeMS	TIME	Ausgang, der die aktuelle Durchlaufzeit für eine Nachricht angibt
	tMinRespTimeMS	TIME	Ausgang, der die minimale Durchlaufzeit für eine Nachricht angibt. Ermittelt seit der letzten steigenden Flanke von "OA_C" oder Systemstart
	tMaxRespTimeMS	TIME	Ausgang, der die maximale Durchlaufzeit für eine Nachricht angibt. Ermittelt seit der letzten steigenden Flanke von "OA_C" oder Systemstart

Tab. 5-8: Schnittstelle ProfisafeHost

5.6.3 Fehlerreaktion am PROFISafe

Alle schwerwiegenden Fehler, die zum Verlust oder zur Beeinträchtigung der Sicherheitsfunktion führen können, bewirken den sicheren Zustand des PROFISafe-Gerätes. Das Gerät liefert an Ein- und Ausgängen Fail-State-Werte und meldet dies über den Bus an die Safety-Applikation. In der Sicherheitslogik können Sie programmtechnisch reagieren. Nach der Fehlerbeseitigung können Sie von der Sicherheitslogik aus durch Ausgabe eines gezielten Quittierungssignals ("Operator Acknowledge") das Gerät wieder aktiv in die Sicherheitsfunktion eingliedern.

Das Fehlerverhalten im Einzelnen ist von dem Gerätetyp abhängig, ebenso Diagnosemeldungen zur Sicherheitssteuerung. Entnehmen Sie Einzelheiten bitte der jeweiligen Gerätebeschreibung. In der Regel wird die Fehlermeldung

am Gerät über LED-Anzeigen dargestellt. Die Übertragung von Diagnosemeldungen zur Sicherheitssteuerung ist nicht sicherheitsgerichtet.

5.6.4 Diagnoseeigenschaften von PROFISafe

Bei der Systeminitialisierung erkennt die Sicherheitssteuerung die folgenden PROFISafe-spezifischen Fehler und stellt im Programmiersystem (Online-Betrieb) entsprechende Diagnoseinformationen zur Verfügung.

- Fehlerhafte PROFISafe-Adresse am Gerät
- Ungültig parametrierte PROFISafe-Adresse
- Ungültig parametrierte Überwachungszeit
- Ungültig parametrierte SIL-Klasse
- Ungültige CRC-Länge
- Ungültige Version des F-Parametersatzes

Im Betrieb erhält die dem Gerät zugeordnete Host-Layer-Instanz im Safety-Funktionsmodul im Rahmen des Status-Bytes der Protokolldaten (PDU) die folgenden Meldungen:

- Fail-save-values
Die sicheren Ausgänge des Gerätes nehmen den sicheren Zustand an, die sicheren Eingänge melden den sicheren Zustand zum Host
- Communication failure
Überschreiten der parametrierten Überwachungszeit (WD-Timeout), Datenverfälschung (CRC) oder Fehler bei der Telegrammabfolge (Consecutive Number)
- Failure exists in Fslave or Fmodule
Von dem PROFISafe-Gerät erkannte Peripherie- und Gerätefehler werden über das zyklische PROFISafe-Telegramm mitgeteilt. Hierzu gehören Drahtbruch, Kurzschluss, Divergenzzeitüberschreitung und anderes, sofern die Komponente diese Fehler erkennt und weiterleitet

Voraussetzung zur Übertragung der Diagnosemeldungen ist eine funktionsfähige Komponente und zumindest zeitweise eine funktionsfähige Kommunikation. Ist dies nicht gewährleistet, erkennt die F-Host-Instanz ein Kommunikations-TimeOut.

Die Fehlermeldungen werden zum einen als Diagnoseinformationen an dem Programmiersystem gemeldet, zum anderen "Oder"-verknüpft über die PROFISafe-Layerschnittstelle der Applikation zur programmtechnischen Auswertung zur Verfügung gestellt.

Erweiterte Diagnose kann je nach Diagnosefähigkeit des Gerätes über azyklische Dienste an die Standardsteuerung übermittelt und über das Programmiersystem angezeigt werden. Siehe hierzu die Gerätebeschreibungen.

Sichere Eingänge	An sicheren Eingängen können je nach Gerätetyp und Parametrierung folgende Fehler erkannt werden: • Kurzschluss • Querschuss • Überlast/Kurzschluss der Taktausgänge Bei Erkennung eines Fehlers wird für diesen Eingang der sichere Zustand eingenommen d. h. in den Eingangsdaten eine "0" übertragen.
Sichere Ausgänge	An sicheren Ausgängen können in Abhängigkeit vom Gerätetyp und von der Parametrierung folgende Fehler erkannt werden: • Kurzschluss

- Querschluss
- Überlast
- Verletzung der parametrisierten Abschaltzeit

Bei Erkennung eines solchen Fehlers wird der betroffene Ausgang abgeschaltet ("0" = aus = sicherer Zustand).

5.7 Sercos III mit "CIP Safety on Sercos"

5.7.1 Allgemeines

"CIP Safety on Sercos" ist das in Kooperation mit der ODVA (Open DeviceNet Vendor Association) definierte und nach IEC 61508 bis SIL 3 zertifizierte Protokoll auf Basis der CIP Safety Sicherungsmechanismen zur Übertragung sicherheitsrelevanter Signale über Sercos interface. Ein zusätzlicher Sicherheitsbus entfällt, denn die sicheren Daten werden einfach neben den Standard-Daten des Sercos interface Netzwerks echtzeitfähig eingetaktet. Die Integration von Antriebs-, Peripherie- und Sicherheitsbus sowie Standard Ethernet in einem einzigen Netzwerk vereinfacht die Handhabung und reduziert Hardware- und Installationskosten. Integrierte Sicherheitssteuerungen und homogene Sicherheitslösungen lassen sich so einfach umsetzen.

5.7.2 Anwendung von "CIP Safety on Sercos"

Kurzbeschreibung "CIP Safety on Sercos" ist das Protokoll zur Übertragung sicherheitsrelevanter Signale über Sercos Interface. Die sichere Buskommunikation über "CIP Safety on Sercos" zeichnet sich durch folgende Merkmale aus:

- Die Konsumenten- und Produzenten-Verbindungen sind nicht frei konfigurierbar. Es können nur fest definierte Vorzugskonfigurationen verwendet werden
- Alle notwendigen Informationen zur Verbindungsherstellung werden der Steuerung über die Gerätebeschreibungsdatei (SDDML) zur Verfügung gestellt
- Der erreichbare Sicherheitslevel ist von den verwendeten Sicherheitsfunktionen abhängig

Konfiguration Fügen Sie zunächst ihre sicheren CSos-fähigen Geräte in die Topologie Ihres Sercos-Systems ein. Dazu entnehmen Sie wie bei Standard-Geräten die einzusetzenden CSos-fähigen Geräte der Gerätebibliothek des Programmiersystems und binden Sie diese Geräte an den gewünschten Positionen in den Gerätebaum Ihrer Applikation ein. Die Geräte sind durch ihre SDDML-Dateien beschrieben und mit einer Grundparametrierung versehen.

Aufgrund dieser Informationen stellt Ihnen das Programmiersystem für jedes CSos-Gerät eine Reihe von Konfigurations- und Parametrierungs-Fenster zur Verfügung, in deren Rahmen Sie alle Konfigurations- und Parametrierungseinstellungen vornehmen können, u. a.:

- Safety Parameter (PROFISafe F-Parameter)
- Safety Mapping (I/O-Kanäle)
- I-Parameter (individuelle Parameter, falls vorhanden)
- Information (allgemeine Information über das Gerät, welche der Gerätebeschreibung entnommen sind: Name, Hersteller, Version, Bestellnummer, Beschreibung, Bild)

Analog zur PROFISafe-Anwendung ordnen Sie im Fenster "I/O-Abbild" die I/O-Kanäle des Gerätes den symbolischen Variablen zu, die Sie in Ihrer Sicherheitslogik verwenden.

Parametrierung Die Parametrierung geschieht analog zu den PROFISafe-Geräte.

F-Parameter dienen speziell zur Parametrierung der sicheren Kommunikation, siehe "[Allgemeine Beschreibung der F-Parameter](#)" auf Seite 75. Die gerätespezifische Parameter werden als I-Parameter bezeichnet und werden in den einzelnen Gerätebeschreibungen beschrieben.

Schnittstelle zur Sicherheitslogik

Der Funktionsbaustein CSosOriginator überwacht den Verbindungsaufbau und die zyklische Kommunikation eines sicheren Sercos-Teilnehmers. Der Funktionsbaustein stellt Diagnosen zur Verfügung und ermöglicht das Quittieren von aufgetretenen Meldungen. Mit dem logischen CSos-Gerät wird eine Kontrollinstanz dieses Funktionsbaustein automatisch der Sicherheitsapplikation hinzugefügt. Jede Eingangs- und Ausgangsgruppe benötigt eine Kontrollinstanz dieses Funktionsbaustein

Legt man einen IndraDrive mit einem SafeLogic Safety-Profil an, wird automatisch je eine Kontrollinstanz für Control (Ausgänge) und Status (Eingänge) angelegt. Je S20 CSos-I/O-Modul wird eine Instanz angelegt.

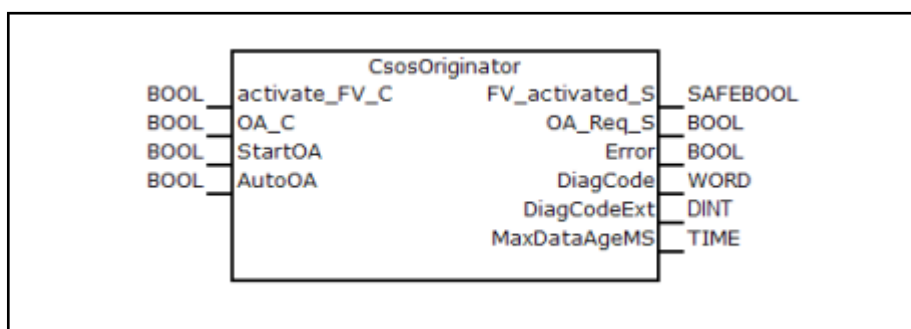


Abb. 5-14: Interface CSosOriginator-Funktionsbaustein

I/O-Typ	Name	Datentyp	Beschreibung
VAR_INPUT	activate_FV_C	BOOL	Eingang nach PROFISafe-Spezifikation, Kapitel 6.1: Aktivierung der Fail-safe Werte TRUE: Die Verwendung von Fail-safe Werten wird erzwungen: Der ProfisafeHost-Stack liefert als Eingangssignale die Fail-safe Werte an die Applikation und schreibt fail-safe Werte als Ausgangssignale an das F-Device FALSE: Die Verwendung von fail-safe Werten wird nicht erzwungen. Es sollen im Normalfall Prozessdaten übertragen werden Vorsicht: Das Rücksetzen dieses Eingangs von TRUE auf FALSE kann zur sofortigen Übertragung der Prozessdaten führen! Stellen Sie durch geeignete Maßnahmen sicher, dass von Ihrer Anlage/Maschine keine Gefahr ausgeht! Default-Wert: FALSE
	OA_C	BOOL	Eingang nach PROFISafe-Spezifikation, Kapitel 6.1: Operator Acknowledgement Mit einer steigenden Flanke des Eingangs wird die Wiederaufnahme der Sicherheitsfunktion nach einem Fehler bestätigt. Nach einer Bestätigung muss der Eingang mindestens einen vollen Zyklus auf FALSE stehen, bevor der nächste Fehler bestätigt werden kann Hinweis: Wenn sowohl "StartOA", als auch "AutoOA" auf TRUE gesetzt sind, wird der Eingang "OA_C" nicht ausgewertet, da alle Anfragen zur Aufnahme der Sicherheitsfunktion automatisch bestätigt werden Default-Wert: FALSE
	StartOA	BOOL	Verhalten nach einem Fehler während der Anlaufphase des F-Device. Die Wirksamkeit des Eingangs "StartOA" erstreckt sich vom erster Start der Applikation bis das F-Device einmal die Sicherheitsfunktion aufgenommen hat TRUE: Automatische Bestätigung zur Aufnahme der Sicherheitsfunktion nach einem Fehler FALSE: Manuelle Bestätigung am Eingang "OA_C" zur Aufnahme der Sicherheitsfunktion des F-Device nach einem Fehler notwendig Default-Wert: TRUE Hinweis: "StartOA" ist keine Anlaufverriegelung!
	AutoOA	BOOL	Wiederanlaufverhalten nach einem Fehler. Vorbedingung: Das F-Device ist erfolgreich angelaufen und hat mindestens einmal die Sicherheitsfunktion aufgenommen TRUE: Automatische Bestätigung zur Wiederaufnahme der Sicherheitsfunktion nach einem Fehler FALSE: Manuelle Bestätigung am Eingang "OA_C" zur Wiederaufnahme der Sicherheitsfunktion des F-Device nach einem Fehler notwendig Default-Wert: FALSE Hinweis: Sind "StartOA" und "AutoOA" TRUE, so werden Fehler immer automatisch bestätigt. Dies ist nur in absoluten Ausnahmefällen sinnvoll

I/O-Typ	Name	Datentyp	Beschreibung
VAR_OUTPUT	FV_activated_S	SAFE- BOOL	Ausgang nach PROFISafe-Spezifikation, Kapitel 6.1: Anzeige Aktivierung der Fail-safe Werte TRUE: Der ProfisafeHost-Stack liefert Fail-safe Werte FALSE: Der ProfisafeHost-Stack liefert Prozessdaten Hinweis: Der Ausgang wechselt auf TRUE, entweder auf Anweisung des Stacks oder aufgrund Übertragungsfehler zum F-Device bzw. interner Fehler im F-Device oder falls der Eingang "activate_FV_C" gleich TRUE ist
	OA_Req_S	BOOL	Kommunikationsfehler TRUE: Es ist ein Kommunikationsfehler aufgetreten FALSE: Es liegt kein Kommunikationsfehler vor
	Error	BOOL	Fehleranzeige TRUE: Es liegt ein Fehler vor (DiagCode = 16#Cxxx) FALSE: Es liegt kein Fehler vor (DiagCode = 16#8xxx)
	DiagCode	WORD	Diagnose-Code 16#8000 : Normale Operation
	DiagCodeExt	DINT	Erweiterter DiagnoseCode
	MaxDataAgeMS	TIME	Maximales Datenalter

Tab. 5-9: Schnittstelle CSosOriginator

5.8 Sichere Querkommunikation über Ethernet

5.8.1 Allgemeines

Die sichere Querkommunikation ermöglicht den Austausch von sicheren SPS-Variablen zwischen mehreren SafeLogic-Steuerungen über Ethernet-basierte Bussysteme. Die Daten werden mittels des IP-Kommunikationsprotokolls übertragen und sind zwischen den Steuerungen mit Ende-zu-Ende Sicherungsmechanismen abgesichert. Die Integration von Antriebs-, Peripherie- und Sicherheitsbus sowie Standard Ethernet in einem einzigen Netzwerk vereinfacht die Handhabung und reduziert Hardware- und Installationskosten. Integrierte Sicherheitssteuerungen und homogene Sicherheitslösungen lassen sich so einfach umsetzen.

Der Verbindungsaufbau erfolgt nach dem Subscriber-Prinzip. Die sendende SafeLogic-Steuerung stellt die Daten bereit. Die empfangene SafeLogic-Steuerung nimmt Verbindung zur sendenden Steuerung auf. Mehrere Empfänger können sich auf einen Sender verbinden. Hierfür muss die sendende SafeLogic-Steuerung eine einstellbare Verbindungsanzahl vorhalten.

Mit der sicheren Querkommunikation werden Daten sicher auf demselben Medium und mit derselben Anschaltung übertragen wie die Standard-Kommunikation. Sichere Kommunikation ist zwischen allen Netzwerk-Ebenen möglich, auch bei direkter Querkommunikation und netzwerkübergreifender Kommunikation. Die sicherheitsrelevanten Daten werden in Form eines über sichere Kommunikationsprotokolle abgesicherten UDP-Pakets über die IP-Schicht übertragen.

Den logischen Datenverbindungen sind dabei keine Grenzen gesetzt, da die sichere Querkommunikation voll routingfähig ist. So kann sich ein Safety-Netzwerk über mehrere IP-fähige Netzwerke erstrecken. Überschreitet je-

doch die Übertragungszeit den Maximalwert, so wird die Verbindung in den sicheren Zustand versetzt.

5.8.2 Anwendung der sicheren Querkommunikation

Kurzbeschreibung

Die sichere Querkommunikation dient zur Übertragung sicherheitsrelevanter Signale über Ethernet-basierte Bussysteme. Die sichere Querkommunikation zeichnet sich durch folgende Merkmale aus:

- Die übertragenen sicheren Variablen können frei definiert werden
- Alle notwendigen Informationen zur Verbindungsherstellung werden der Steuerung des Safety-Projekts zur Verfügung gestellt
- Der erreichbare Sicherheitslevel ist SIL 3

Die folgenden sicheren Datentypen können über die sichere Querkommunikation übertragen werden:

- SAFEBOOL
- SAFEINT
- SAFEWORD

Konfiguration

Fügen Sie auf der sendenden SafeLogic-Steuerung einen "Safety-NVL-Sender" (sichere Netzwerkvariablenliste) ein. Definieren Sie dann die zu übertragenden Variablen. Setzen Sie die Safety-Adresse der Senderliste. Fügen Sie dann auf der empfangenden SafeLogic-Steuerung einen "Safety-NVL-Receiver" ein. Danach können die beiden Listen durch die Auswahl des zugeordneten Senders im "Safety-NVL-Receiver" verbunden werden.

Schnittstelle zur Sicherheitslogik

Der Funktionsbaustein NetVarSender stellt die sicheren Variablen bereit. Mit dem Safety-NVL-Sender wird eine Kontrollinstanz dieses Funktionsbausteins automatisch der Sicherheitsapplikation hinzugefügt. Jede Sendeliste benötigt eine Kontrollinstanz dieses Funktionsbausteins.

Der Funktionsbaustein NetVarSender hat keinerlei überwachende Funktion. Es gibt keine Möglichkeit zu prüfen, ob Empfänger mit der Netzwerkliste verbunden sind. Über den Eingang S_ActivateOut wird die Übertragung von Prozessdaten aktiviert. Ist S_ActivateOut FALSE, werden Failsafe-Werte übertragen.

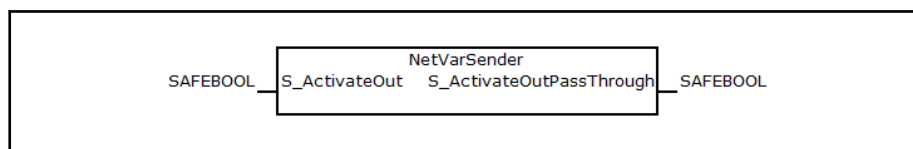


Abb. 5-15: Interface NetVarSender

I/O-Typ	Name	Datentyp	Beschreibung
VAR_INPUT	S_ActivateOut	SAFE- BOOL	Aktiviert die Übertragung von Prozessdaten TRUE: Es werden Prozessdaten übertragen. Die Werte der sicheren Austauschvariablen werden an die Gegenstelle übertragen. FALSE: Es werden Failsafe-Werte übertragen. SAFEBOOL-Variablen sind FALSE, SAFEINT- und SAFEWORD-Variablen sind 0. Default-Wert: FALSE
VAR_OUTPUT	S_ActivateOut- PassThrough	SAFE- BOOL	Übertragung von Prozessdaten aktiv. TRUE: Es werden Prozessdaten übertragen FALSE: Es werden Failsafe-Werte übertragen

Tab. 5-10: Schnittstelle NetVarSender

Der Funktionsbaustein NetVarReceiver überwacht den Verbindungsaufbau und die zyklische Kommunikation einer Safety Netzwerkvariablen-Empfangsliste. Der Funktionsbaustein stellt Diagnosen zur Verfügung und ermöglicht das Quittieren von aufgetretenen Meldungen. Mit dem Safety-NVL-Receiver wird eine Kontrollinstanz dieses Funktionsbausteins automatisch der Sicherheitsapplikation hinzugefügt. Jede Empfangsliste benötigt eine Kontrollinstanz dieses Funktionsbausteins.

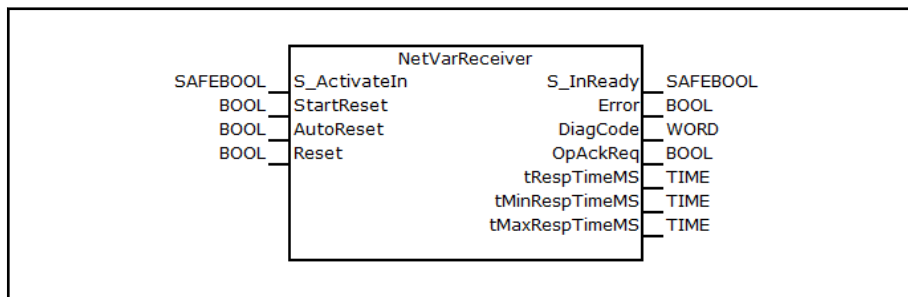


Abb. 5-16: Interface NetVarReceiver-Funktionsbaustein

I/O-TYP	Name	Datentyp	Beschreibung
VAR_INPUT	S_ActivateIn	SAFEBOOL	Aktivierung der Prozessdaten FALSE: Die Verwendung von Fail-safe Werten wird erzwungen: Alle Werte werden mit 0 bzw. False übertragen TRUE: Die Verwendung von fail-safe Werten wird nicht erzwungen. Es sollen im Normalfall Prozessdaten übertragen werden. Vorsicht: Das Setzen dieses Eingangs von FALSE auf TRUE kann zur sofortigen Übertragung der Prozessdaten führen! Stellen Sie durch geeignete Maßnahmen sicher, dass von Ihrer Anlage/Maschine keine Gefahr ausgeht! Default-Wert: TRUE
	StartReset	BOOL	Verhalten nach einem Fehler während der Anlaufphase: Die Wirksamkeit des Eingangs StartReset erstreckt sich vom erster Start der Applikation bis die NVL einmal die Sicherheitsfunktion aufgenommen hat. (z.B. nach einem Reset kalt oder einem Neustart der Bootapplikation bzw. PowerON) Der Eingang "StartReset" entspricht dem Eingang <auto-Quitt-Anlauffehler> zur automatischen Quittierung von Fehlern beim Anlauf. TRUE: Automatische Bestätigung zur Aufnahme der Sicherheitsfunktion nach einem Fehler. FALSE: Manuelle Bestätigung am Eingang Reset zur Aufnahme der Sicherheitsfunktion nach einem Fehler notwendig. Default-Wert: TRUE

I/O-TYP	Name	Datentyp	Beschreibung
	AutoReset	BOOL	Wiederanlaufverhalten nach einem Fehler. Vorbedingung: Die NVL ist erfolgreich angelaufen und hat mindestens einmal die Sicherheitsfunktion aufgenommen. Der Eingang "AutoReset" entspricht dem Eingang <auto-Quitt-Unterbrechung> zur automatischen Quittierung nach Unterbrechungen. TRUE: Automatische Bestätigung zur Wiederaufnahme der Sicherheitsfunktion nach einem Fehler. FALSE: Manuelle Bestätigung am Eingang Reset zur Wiederaufnahme der Sicherheitsfunktion der NVL nach einem Fehler notwendig. Default-Wert: FALSE
	Reset	BOOL	Mit einer steigenden Flanke des Eingangs wird die Wiederaufnahme der Sicherheitsfunktion nach einem Fehler bestätigt. Nach einer Bestätigung muss der Eingang mindestens einen vollen Zyklus auf FALSE stehen, bevor der nächste Fehler bestätigt werden kann. Der Eingang "Reset" entspricht dem Eingang <Quitt-Flanke> zur manuellen Quittierung. Hinweis: Wenn sowohl StartReset, als auch AutoReset auf TRUE gesetzt sind, wird der Eingang Reset nicht ausgewertet, da alle Anfragen zur Aufnahme der Sicherheitsfunktion automatisch bestätigt werden. Hinweise: Reset ist ein Eingang zur Bestätigung durch den Anwender. Er soll mit einem Eingangssignal verbunden werden und nicht programmatisch generiert werden. Default-Wert: FALSE Hinweis: Wenn aktuell keine Quittierung (OpAckReq ist FALSE) angefordert ist, wird der Eingang ignoriert: Deshalb kann das gleiche Signal mit dem Eingang zur Quittierungsflanke aller FB-Instanzen verbunden werden, um eine unspezifische Bestätigung von Kommunikationsproblemen zu realisieren.
VAR_OUTPUT	S_InReady	SAFEBOOL	Anzeige Aktivierung von Prozessdaten TRUE: Es werden Prozessdaten der NVL übertragen FALSE: Es werden failsafe-Werte übertragen Hinweis: Der Ausgang wechselt auf FALSE, entweder auf Anweisung des Stacks oder aufgrund Übertragungsfehler bzw. interner Fehler in der NVL oder falls der Eingang S_AktiviertIn gleich FALSE ist.
	Error	BOOL	Fehleranzeige TRUE: Es liegt ein Fehler vor (DiagCode = 16#Cxxx). FALSE: Es liegt kein Fehler vor (DiagCode = 16#8xxx).
	DiagCode	WORD	Verwendung des Ausganges DiagCode als Diagnose-Code, Initialwert 16#0000

I/O-TYP	Name	Datentyp	Beschreibung
	OpAckReq	BOOL	Anzeige Operator Acknowledgement Request TRUE: Die NVL benötigt eine Bestätigung durch den Bediener (Operator Acknowledgement), um die Sicherheitsfunktion wieder aufzunehmen. FALSE: Die NVL benötigt derzeit keine Bestätigung durch den Bediener (Operator Acknowledgement). Hinweis: Dass eine Verbindung eine Bestätigung durch den Bediener benötigt, wird durch OpAckReq = TRUE signalisiert. Normalerweise wird dies dem Bediener gemeldet, Die entsprechende Logic muss in der Applikation programmiert werden.
	tRespTimeMS	TIME	Ausgang, der die aktuelle Durchlaufzeit für eine Nachricht angibt.
	tMinRespTimeMS	TIME	Ausgang, der die minimale Durchlaufzeit für eine Nachricht angibt. Ermittelt seit der letzten steigenden Flanke von Reset oder Systemstart.
	tMaxRespTimeMS	TIME	Ausgang, der die maximale Durchlaufzeit für eine Nachricht angibt. Ermittelt seit der letzten steigenden Flanke von Reset oder Systemstart.

Tab. 5-11: Schnittstelle NetVarReceiver

6 Entwicklungsoberfläche

6.1 Überblick

Die beiden Safety Programmiersysteme "SafeLogic" und "SafeLogic compact" nutzen unterschiedliche Entwicklungsoberflächen. Während die SafeLogic-Komponenten durchgängig in IndraWorks integriert sind, kann die SafeLogic compact sowohl als Stand alone, als auch als in IndraWorks integriertes DTM genutzt werden. Voraussetzung für die DTM-Nutzung ist IndraWorks 12V06 oder höher.

Im folgenden werden Benutzeroberflächen beider Programmiersysteme vorgestellt.

- [Kap. 6.2 "SafeLogic compact \(SafeLogic Designer\)" auf Seite 89](#)
- [Kap. 6.3 "SafeLogic" auf Seite 94](#)

6.2 SafeLogic compact (SafeLogic Designer)

6.2.1 Lizenz

Der SafeLogic Designer ist nicht lizenzpflichtig.

6.2.2 Standardansichten

Der SafeLogic Designer hat die folgenden Ansichten, die über Karteireiter unterhalb der Menüleiste erreicht werden können.

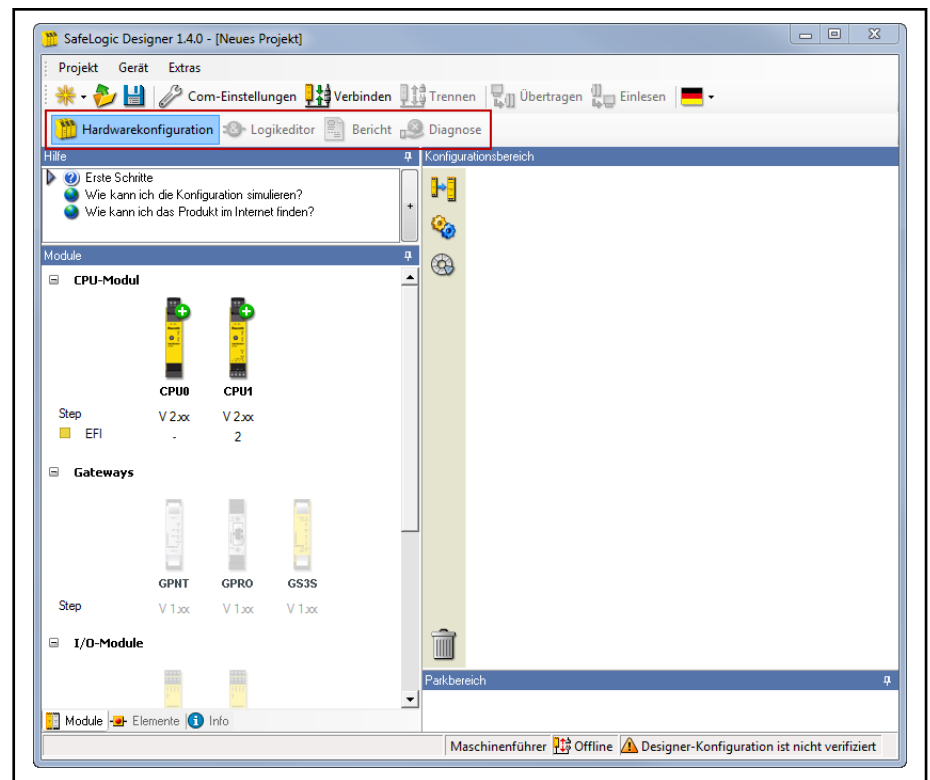


Abb. 6-1: Die Ansichten sind unterhalb der Menüleiste wählbar

- In der Ansicht **Hardwarekonfiguration** wird der Aufbau eines SafeLogic compact Systems aus verschiedenen Hardwaremodulen sowie die Konfiguration der Ein- und Ausgänge und der angeschlossenen Elemente festgelegt

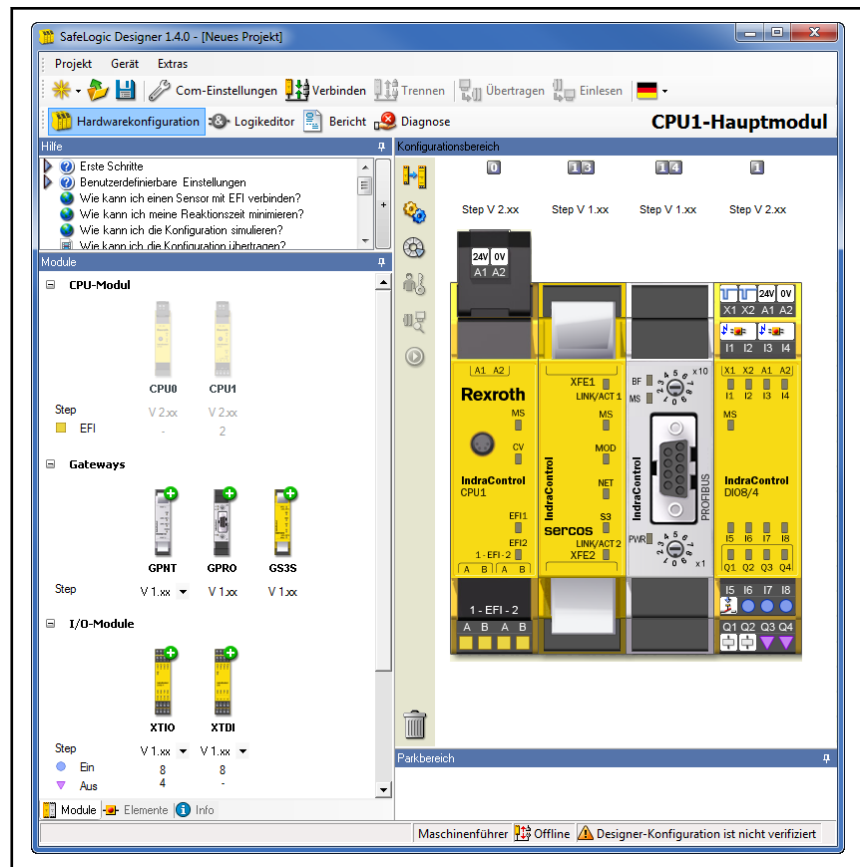


Abb. 6-2: Ansicht "Hardwarekonfiguration"

- In der Ansicht **Logikeditor** kann die Funktionslogik mit Hilfe von logischen Funktionsblöcken und applikationsspezifischen Funktionsblöcken konfiguriert werden. Diese Ansicht ist erst dann verfügbar, wenn vorher ein Hauptmodul in der Hardwarekonfiguration ausgewählt wurde

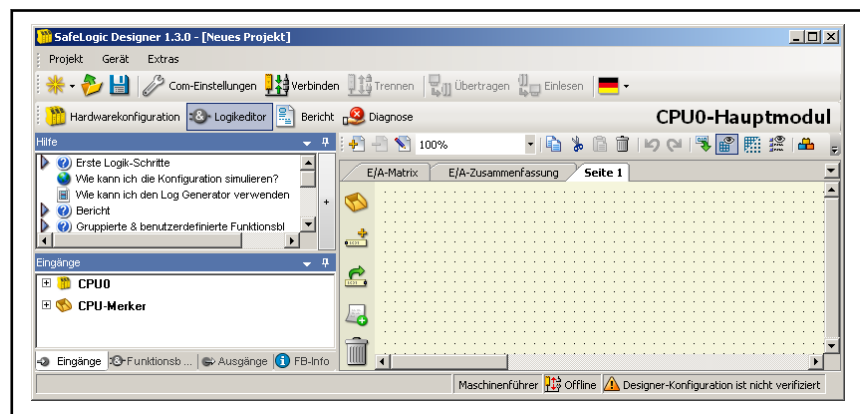


Abb. 6-3: Ansicht "Logikeditor"

- Wenn das Projekt mindestens ein SafeLogic compact Diagnose Gateway enthält oder wenn die RS-232-Kommunikation aktiviert ist, dann ist die Ansicht **Gateways** verfügbar. Diese Ansicht dient zur Konfiguration der SafeLogic compact Diagnose Gateways und der Daten, die mit dem Netzwerk ausgetauscht werden

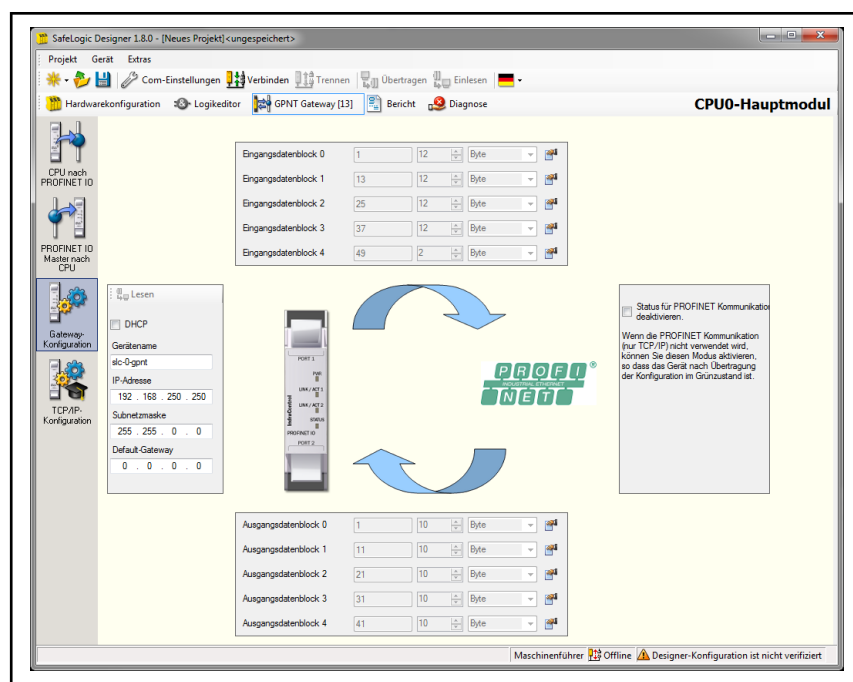


Abb. 6-4: Ansicht "Gateway"

- In der Ansicht **Bericht** stehen vollständige Informationen zu dem aktuell geladenen Projekt und allen Einstellungen einschließlich der Logikprogrammierung und Verdrahtungsdiagrammen zur Verfügung. Außerdem können zusätzliche Angaben zum Projekt eingegeben werden. Alle Informationen können in Standard-Dateiformaten gespeichert und ausgedruckt werden. Der Berichtsumfang kann je nach Auswahl individuell zusammengestellt werden



Abb. 6-5: Ansicht "Bericht"

- In der Ansicht **Diagnose** werden die gespeicherten Fehlermeldungen als Historie eines angeschlossenen SafeLogic compact Systems angezeigt

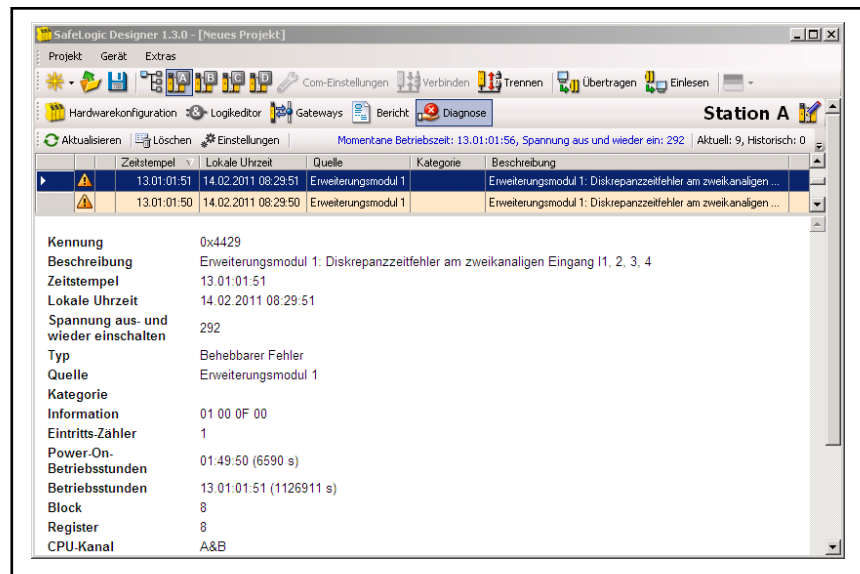


Abb. 6-6: Ansicht "Diagnose"

6.2.3 Logikprogrammierung

Die Funktionslogik des SafeLogic compact Systems wird mit Hilfe von Funktionsblöcken programmiert. Diese Funktionsblöcke sind für den Einsatz in sicherheitsrelevanten Funktionen zertifiziert, wenn bei der Implementierung alle Sicherheitsnormen eingehalten werden. Die folgenden Abschnitte informieren über wichtige Aspekte der Verwendung von Funktionsblöcken im SafeLogic compact System.

Funktionsblöcke

Das SafeLogic compact System unterstützt bis zu 255 Funktionsblöcke in einer gegebenen Anwendung. Die Logik-Zykluszeit ergibt sich aus der Anzahl der verwendeten Funktionsblöcken und liegt zwischen 4 ms und 40 ms.

Die folgenden Funktionsblöcke sind im System SafeLogic compact verfügbar:

- *Logik*
 - AND
 - OR
 - XOR
 - XNOR
 - NOT
 - RS Flip-Flop
 - JK Flip-Flop
 - Binär-Decodierer
 - Binär-Codierer
 - Routing 1:N
 - Routing N:N
 - Mehrfach-Freigabe
 - Mehrfach-Speicher
- *Start/Flanke*
 - Reset
 - Restart
 - Anlaufwarnung

- Flankenerkennung
- *Verzögerungen*
 - Einschaltverzögerung
 - Ausschaltverzögerung
 - Einstellbare Einschaltverzögerung
 - Einstellbare Ausschaltverzögerung
- *Zähler und Takt*
 - Zähler (Aufwärts, Abwärts, Auf- und Abwärts)
 - Taktgenerator
 - Nachlauferkennung
 - Log-Generator
 - Frequenzüberwachung
- *EDM/Ausgangsbausteine*
 - EDM
 - Ventilüberwachung
 - Fast Shut Off mit Bypass
 - Fast Shut Off
- *Muting/Pressen*
 - Sequenziell-Muting
 - Parallel-Muting
 - Kreuz-Muting
 - Kontaktmonitor Universal-Pressen
 - Presse Einzelhub
 - Presse einrichten
 - Presse Automatik
 - Taktbetrieb
 - Kontaktmonitor Exzenterpresse
- *Andere*
 - Betriebsartenwahlschalter
 - Not-Halt
 - Schalter-Auswertung
 - Magnetschalter
 - Lichtgitter-Auswertung
 - Zweihand Typ IIIA
 - Zweihand Typ IIIC
 - Mehrfach-Zweihand
 - Schaltersynchronisation
 - Fehler-Ausgangskombination
 - Tolerante Zweikanaligkeitsauswertung
- *Benutzerdefinierte Funktionsblöcke*
 - Gruppiertes Funktionsblock
 - Benutzerdefinierter Funktionsblock

Funktionsblockeigenschaften

Funktionsblöcke verfügen über eine Reihe verschiedener Eigenschaften, auf die Sie zugreifen können. Die konfigurierbaren Parameter sind je nach Funktionsblock unterschiedlich. Sie können mit einem Doppelklick auf den Funktionsblock auf die konfigurierbaren Parameter zugreifen und die Karteikarte mit den gewünschten Eigenschaften anwählen. Das folgende Beispiel zeigt den Funktionsblock "Schalter-Auswertung":

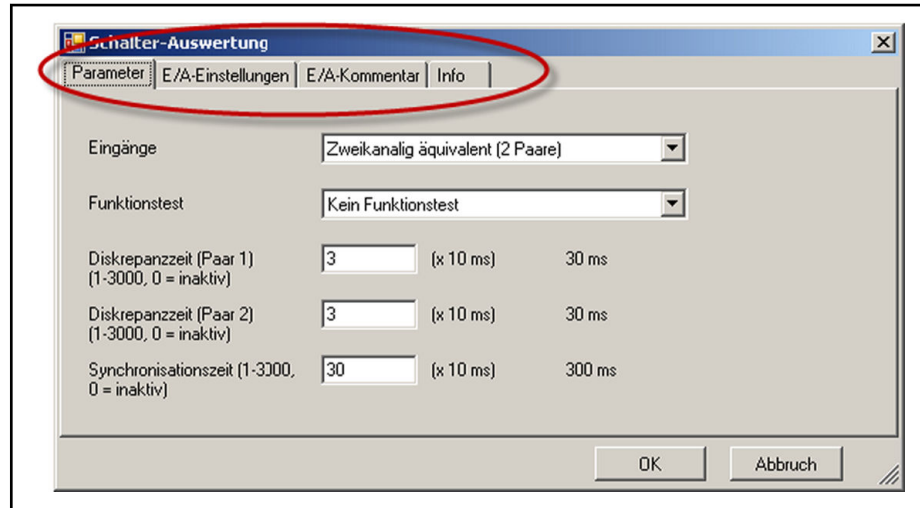


Abb. 6-7: Konfigurierbare Parameter von Funktionsblöcken

Funktionsblock-Eingänge

Mögliche Quellen für Funktionsblockeingänge sind alle Eingangselemente, die im Auswahlbaum der Eingänge des Logikeditors aufgelistet sind sowie Ausgänge von Funktionsblöcken.

Funktionsblock-Ausgänge

Funktionsblöcke stellen verschiedene Ausgangssignalanschlüsse zum Anschluss an physikalische Ausgänge oder an andere Funktionsblöcke bereit.

I/O-Module

Die I/O-Erweiterungsmodule (z. B. XTIO oder XTDI) können eine zweikanalige Auswertung vornehmen, wenn vordefinierte Eingangselemente aus dem Elementfenster (z. B. RE27, C4000, ...) daran angeschlossen werden. Wenn ein solches Eingangselement ausgewählt wird, dann benötigen Sie keinen separaten Funktionsblock für die zweikanalige Auswertung (z. B. "Lichtgitter-Auswertung", "Schalter-Auswertung" oder "Magnetschalter"). Der zweikanalig ausgewertete Eingang wird als "einkanaliger" Signalpfad im Logikeditor konfiguriert.

Die zweikanalige Auswertung prüft die korrekte Abfolge der zwei Eingangssignale. Wenn eines der beiden Signale eine Abschaltung bewirkt hat, dann wird erwartet, dass das andere Signal entsprechend folgt. Welche Werte die beiden Signale haben müssen, hängt von der Art der zweikanaligen Auswertung ab. Es gibt zwei Möglichkeiten:

- Äquivalente Auswertung
- Antivalente Auswertung

Optional kann eine "Diskrepanzzeit" konfiguriert werden. Die Diskrepanzzeit bestimmt, wie lange die zwei Eingänge diskrepante Werte haben dürfen, nachdem eines der beiden Eingangssignale seinen Wert geändert hat, ohne dass dies als Fehler gewertet wird.

6.3 SafeLogic

6.3.1 Lizenz

IndraWorks SafetyManager-Lizenz

Es gibt zwei Arten von SafetyManager-Lizenzen:

- IndraWorks SafetyManager (R911322463)
Diese Lizenz wird zum Entwickeln von Safety-Programmen benötigt.
Sie ermöglicht:
 - das Einloggen in die Safety-Steuerung inklusive aller Debug-Handlungen
 - das Setzen von Passwörtern
 - das Herunterladen von Safety-Programmen
 - das Erzeugen von Bootprojekten
 - das Abrufen des Steuerungslogbuchs
 - den Firmwareupdate
- IndraWorks SafetyManager Lite (R911383338)
Diese Lizenz wird für die Ferndiagnose bzw. den Service von Safety-Applikationen benötigt.
Sie ermöglicht:
 - das Einloggen in die Steuerung über den Fernwartungszugang
 - das Debuggen ohne die Möglichkeit, Werte zu ändern
 - das Abrufen des Steuerungslogbuchs

Die Lizenzen werden wie folgt installiert:

1. Lizenzübersicht öffnen

Die Lizenzübersicht ist über **Extras ► Optionen...** und dann im Baum unter **Allgemein ► Softwarelizenzen** erreichbar.

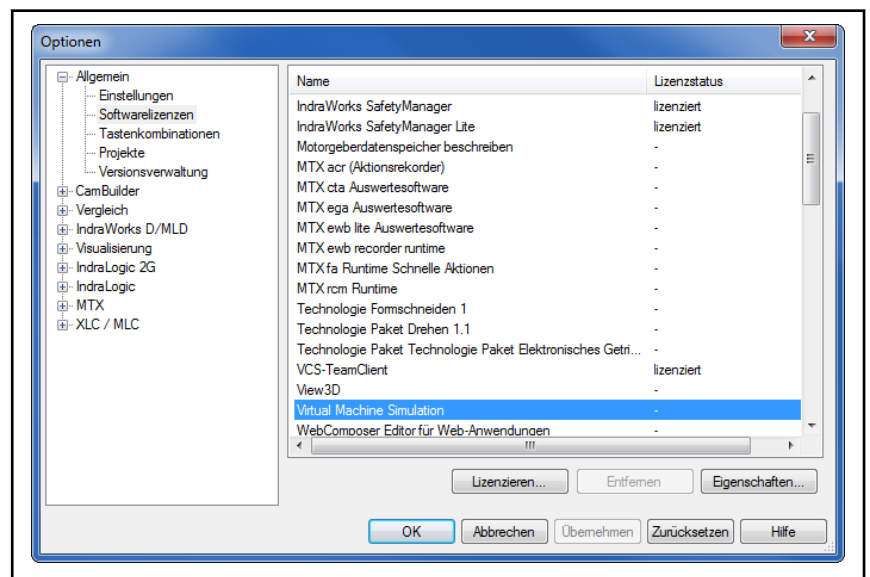


Abb. 6-8: Lizenzübersicht

2. Lizenzieren

Über die Schaltfläche **Lizenzieren...** gelangt man in den Lizenzdialog. Hier kann der Aktivierungsschlüssel eingetragen werden.

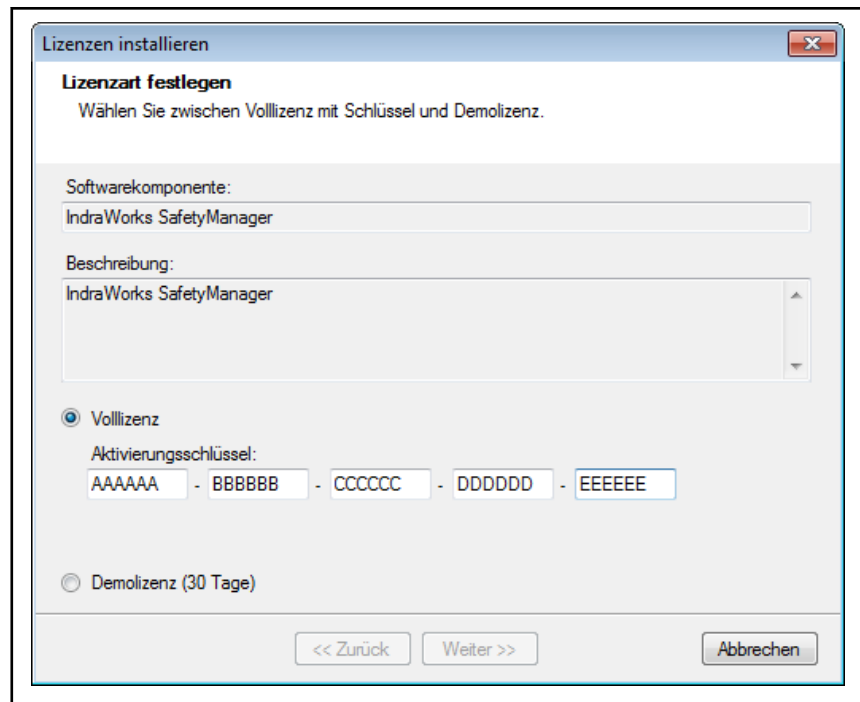


Abb. 6-9: Lizenzdialog

Nach der Bestätigung mit **Weiter >>** wird der Aktivierungsschlüssel geprüft und die Lizenz übernommen.

Die IndraWorks SafetyManager-Lizenz (Lite) ist jetzt installiert und aktiviert.

6.3.2 Projektstruktur

Das SafeLogic-System ist vollständig in IndraWorks integriert. Sämtliche Komponenten sind über IndraWorks Standardfunktionalität zu erreichen.

Im Folgenden werden die Struktur des Projektbaums und die Projektbaum-Objekte beschrieben, welche für die Erstellung einer sicheren Applikation mit Safety gemäß der Richtlinien IEC 61508 und ISO 13849 zur Verfügung stehen.

Das Anlegen eines Projekts und die Bedienung der Oberfläche erfolgt nach dem Bedienkonzept von IndraWorks. Befehle von IndraWorks, die in Safety nicht zur Verfügung stehen, sind sichtbar, aber nicht aktivierbar.

Nach dem Einfügen des Safety-Funktionsmoduls unterhalb der Steuerung, werden unterhalb des Safety-Funktionsmodul-Knotens die erforderlichen Objekte für die Applikationserstellung automatisch erzeugt.

Gelbe Safety-Strukturen

Durch gelbe Strukturen werden die Safety-Objekte in der Projektstruktur und die Safety-Editoren deutlich hervorgehoben und unterscheiden sich dadurch optisch klar von den entsprechenden Standard-Objekten und Standard-Editoren.

Zusätzlich sind die sicheren Signalflüsse ebenfalls gelb markiert. Dies unterstützt und erleichtert die Tätigkeiten bei der Entwicklung, Verifikation und Abnahme der Safety Applikation.

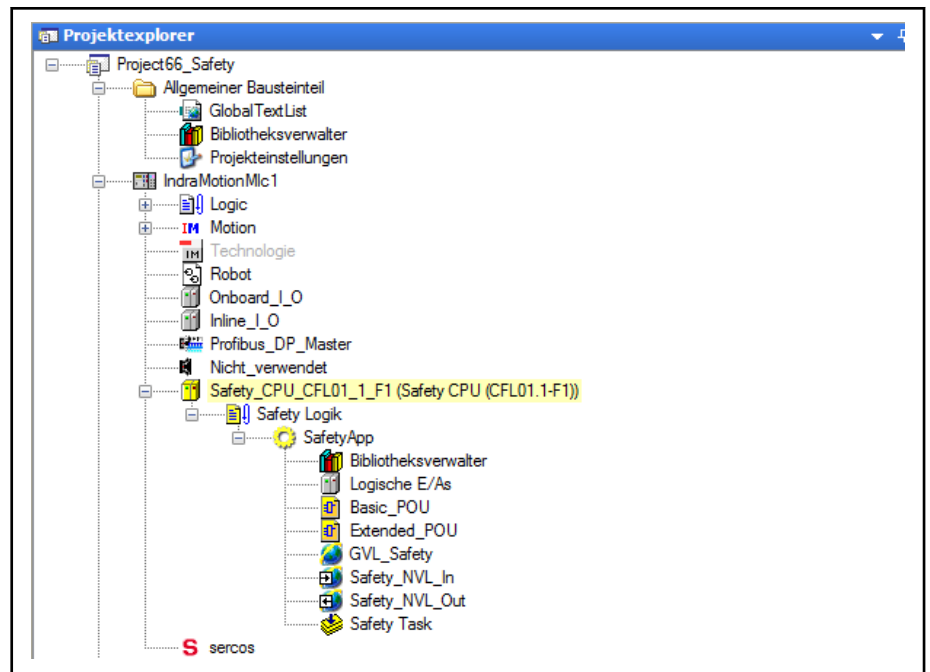


Abb. 6-10: Safety-Applikation im Projektexplorer eines Steuerungs-Projekts

Die Objekte unterhalb des Safety-Funktionsmoduls unterliegen den folgenden Einschränkungen:

- Es ist nur eine Applikation erlaubt. Diese Applikation wird automatisch angelegt
- Es gibt nur eine Task. Diese Task wird automatisch angelegt
- Der Bibliotheksverwalter wird automatisch eingefügt

Die folgenden Objekte bzw. Knotenpunkte sind unterhalb des Safety-Funktionsmoduls genau einmal vorhanden:

- Safety Logik:
Logischer Knotenpunkt der Sicherheitssteuerung, unter den genau eine Safety-Applikation eingehängt werden kann
- SafetyApp:
Knotenpunkt, unter dem die zur Safety-Applikation gehörenden Objekte liegen.

Objekt, das die Ausführungsversion des Codes und den aktuell festgehaltene Stand (Pin) der Applikation festlegt (siehe [Kap. "Pinnen" auf Seite 113](#)).

Der Editor des Objekts verwaltet die Liste der aktuell zur Safety Applikation gehörenden Objekte:

- Bibliotheksverwalter:
Enthält die auf der eingefügten Sicherheitssteuerung zur Verfügung stehenden Bibliotheken (siehe [Kap. 6.3.2 "Projektstruktur" auf Seite 96](#))
- Logische E/As:
Knotenpunkt, dem logische I/O-Objekte hinzugefügt werden können. Diese hinzugefügten logischen I/O dienen dem Austausch von Daten mit der Standardsteuerung (siehe [Kap. 6.3.2 "Projektstruktur" auf Seite 96](#))
- Safety Task:

Dieses Objekt listet alle Programme auf, die auf die Steuerung geladen und ausgeführt werden können

Die folgenden Objekte können unterhalb der Applikation hinzugefügt werden (siehe [Kap. 6.3.2 "Projektstruktur" auf Seite 96](#)):

- Basic_POU (Safety):
POU (Programm oder Funktionsbaustein) mit Programmierlevel Basic
- Extended_POU (Safety):
POU (Programm oder Funktionsbaustein) mit Programmierlevel Extended
- GVL_Safety (Globale Variablenliste Safety):
Deklaration der nur innerhalb der Safety Applikation gültigen globalen Variablen

Alle Objekte können über die Benutzerverwaltung vor unberechtigtem Zugriff geschützt werden (siehe [Kap. 7 "Inbetriebnahme" auf Seite 103](#)).

6.3.3 Logikprogrammierung

Die Programmierung einer Safety-Applikation erfolgt in POU (Programm-Organisations-Einheiten), GVLs (Globale Variablenlisten) und dem Task-Objekt. In den POU wird der Programmcode in der IEC 61131-3 Sprache FUP (Funktionsplan) implementiert. FUP zeichnet sich durch Eindeutigkeit, leichtes Erkennen von Programmierfehlern und klaren Datenfluss aus.

Die Bedienoberfläche und Handhabung des SafeLogic FUP-Editors entspricht in seiner Bedienoberfläche und in der Handhabung dem FUP-Editor der Standard-Steuerung.

Sprachumfang Der Sprachumfang von FUP wird entsprechend der in PLCopen definierten Sprachteilmengen "Basic" und "Extended" eingeschränkt. Die entsprechende Auswahl für den Sprachumfang "Basic Level" oder "Extended Level" wird beim Neuanlegen einer POU (Programm oder Funktionsbaustein) durch den Entwickler festgelegt:

- im **Basic Level** kann durch Verknüpfung der bereits zertifizierten Bausteine der PLCopen-Bibliothek (SafetyPLCopen) mit relativ geringem Aufwand eine Safety-Applikation implementiert und anschließend verifiziert werden
- der **Extended Level** bietet dem Entwickler zusätzliche Operatoren (boolesche, mathematische und andere) und bedingte Sprünge/Returns, um umfangreichere Safety-Applikationen zu erstellen. Diese Operatoren und bedingte Sprünge/Returns erfordern im Anschluss an die Entwicklung einen entsprechend aufwendigeren Verifikationsprozess.

Datentypen Die folgenden Datentypen stehen in der SafeLogic zur Verfügung:

- *Standard-Datentypen*
 - BOOL
 - INT
 - DINT
 - BYTE
 - WORD
 - DWORD
 - TIME

- *Safety-Datentypen*

- SAFEBOOL
- SAFEINT
- SAFEDINT
- SAFEBYTE
- SAFEWORD
- SAFEDWORD
- SAFETIME

Operatoren Die SafeLogic stellt die folgenden Operatoren zur Verfügung:
Operatoren im "Basic Level"

- AND
- OR

Operatoren im "Extended Level"

- *Boolesche Operatoren*

- AND
- OR
- XOR
- NOT

- *Mathematische Operatoren*

- ADD
- SUB
- DIV
- MUL
- NE
- LE
- GE
- GT
- LT
- EQ
- NE

- *Andere Operatoren*

- SEL
- MUX

Sicherer Datenfluss Der sichere Datenfluss der FUP-Programmierung wird in SafeLogic folgendermaßen hervorgehoben:

- Konstanten und konstant deklarierte Variablen werden gelb hinterlegt
- Variablen mit sicherem Datentyp (SAFExxx) werden gelb hinterlegt
- Datenfluss von SAFE-Werten in SAFE-Variablen und Eingänge hinein wird durch dicke gelbe Linien dargestellt
- Funktionsbausteine werden gelb dargestellt, wenn die Funktionsbausteine mindestens einen SAFE-Ausgang haben
- Operator-Aufrufboxen werden gelb ausgefüllt, wenn der Ausgang SAFE ist. Dies ist unter folgenden Bedingungen der Fall:

- bei Operator AND: der Ausgang ist SAFE, wenn mindestens 1 Eingang SAFE ist
- alle anderen Operatoren, inklusiv Konvertierungen: der Ausgang ist SAFE, wenn alle Eingänge SAFE sind

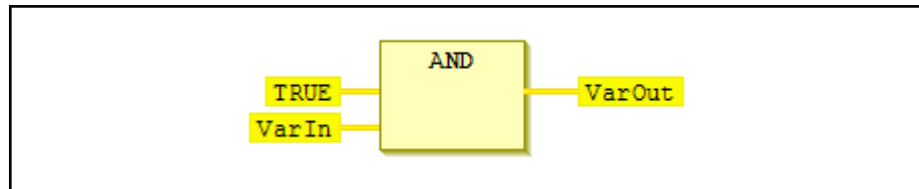


Abb. 6-11: Beispiel für sicheren Datenfluss: Operator AND mit Konstante: TRUE, SAFE-Variablen: VarIn und VarOut

Funktionsbausteine

In SafeLogic stehen dem Entwickler neben den "Operatoren" auf Seite 99 Bibliotheken mit diversen Funktionsbausteinen zur Verfügung. Die für das Safety-Funktionsmodul verfügbaren Bibliotheken sind im Editorfenster der Bibliotheksverwaltung der Sicherheitsapplikation einsehbar.

Die folgenden Funktionsbausteine werden durch Bibliotheken zur Verfügung gestellt:

- *SafetyStandard*
 - SF_RS
 - SF_SR
 - SF_CTD
 - SF_CTU
 - SF_CTUD
 - SF_TOF
 - SF_TON
 - SF_TP
 - SF_F_TRIG
 - SF_R_TRIG
- *SafetyUtilities*
 - SF_ClockGenerator
 - SF_StartupWarning
 - SF_IOConfig
 - SF_IOConfigCntl
 - BinaryDecoder_4_16
 - BinaryEncoder_16_4
 - SF_BinaryDecoder_4_16
 - SF_BinaryEncoder_16_4
 - BoolToByte
 - BoolToWord
 - BoolToDWord
 - SF_BoolToByte
 - SF_BoolToWord
 - SF_BoolToDWord
 - ByteToBool
 - WordToBool

- DWordToBool
 - SF_ByteToBool
 - SF_WordToBool
 - SF_DWordToBool
- *SafetyPLCopen*
 - SF_Antivalent
 - SF_Equivalent
 - SF_EmergencyStop
 - SF_EnableSwitch
 - SF_ESPE
 - SF_EDM
 - SF_GuardLocking
 - SF_GuardMonitoring
 - SF_ModeSelector
 - SF_MutingPar
 - SF_MutingPar_2Sensor
 - SF_MutingSeq
 - SF_OutControl
 - SF_SafetyRequest
 - SF_TestableSafetySensor
 - SF_TwoHandControlTypell
 - SF_TwoHandControlTypelll
- *SafetyDriveMotion*
 - SF_MotionEmergencyStop
 - SF_MotionSafeStop
 - SF_SMMSelector
 - SF_AxisGroup
- *SafetyPLCopenPress*
 - SF_PressControl
 - SF_CamShaftMonitor
 - SF_CamMonitoring
 - SF_CycleControl
 - SF_SingleValveMonitoring
 - SF_SingleValveCycleMonitoring
 - SF_DoubleValveMonitoring
 - SF_ValveGroupControl

6.3.4 I/Os

Das Safety-Funktionsmodul verfügt über keine Anschlussmöglichkeiten für Peripherie-Geräte. Die Safety taugliche Peripherie wird an den Bussystemen der Standardsteuerung angeschlossen.

Im Programmiersystem wird konfiguriert, welche I/O-Signale auf dem Safety-Funktionsmodul verarbeitet werden sollen. Die Eingangssignale die für das Safety-Funktionsmodul bestimmt sind, werden auf der Standardsteuerung aus dem Pool der Gesamt-I/O-Daten herausgefiltert und zum Safety-Funkti-

onsmodul transportiert. Umgekehrt werden die Ausgangssignale vom Safety-Funktionsmodul an die Standardsteuerung übertragen und von der Standardsteuerung in den Pool der Gesamt-I/O-Daten hineingemischt. Es ist somit erforderlich, dass sowohl auf der Standardsteuerung als auch auf der Safety-Steuerung eine konsistente I/O-Konfiguration abliegt. Für den Fall, dass die I/O-Konfiguration nicht identisch ist wird dies im IndraWorks Projekt-Explorer am Knoten des Safety-Funktionsmodul durch ein auf das Steuerungs-Icon überlagertes "Achtung-Symbol" dargestellt.



Im Fall von I/O-Konfigurationsinkonsistenz erfolgt kein Datenaustausch zwischen der Peripherie und dem Safety-Funktionsmodul.

Der Datenaustausch zwischen der Standardsteuerung und dem Safety-Funktionsmodul erfolgt über den gleichen Mechanismus wie der Datenaustausch mit der Peripherie. Das bedeutet, dass bei I/O-Konfigurationsinkonsistenz auch keine Daten zwischen der Standardsteuerung und dem Safety-Funktionsmodul ausgetauscht werden.

I/O-Zugriffe

Die Mapping-Variablen werden auf der "Mapping-Seite" der logischen I/Os editiert und stehen für die Code-Implementierung als Variable der Kategorie "Globale Variablen" zur Verfügung.

7 Inbetriebnahme

7.1 Überblick

Zur Installation und Inbetriebnahme Ihres Automatisierungssystems beachten Sie bitte die Installations- und Inbetriebnahmehinweise in den Anwenderhandbüchern zu den eingesetzten Geräten.

Verantwortlichkeiten

Klären Sie vorab die Verantwortlichkeiten für Installation und Inbetriebnahme:

- Gesamtverantwortung
- Verantwortung für die einzelnen Teilbereiche (Elektrik, Mechanik)
- Verantwortung für das Einschalten



Bitte beachten Sie: Installation und Inbetriebnahme darf nur durch qualifiziertes Personal durchgeführt werden. Diese Personen sind im Hinblick auf die einschlägigen Normen, Bestimmungen, Unfallverhütungsvorschriften und Betriebsverhältnisse unterrichtet und dadurch in der Lage, die erforderlichen Tätigkeiten auszuführen und mögliche Gefahren zu erkennen und zu vermeiden.

Benutzerverwaltung der SafeLogic

Die Benutzerverwaltung ermöglicht Ihnen, die Zugriffsrechte auf eine sicherheitsgerichtete Applikation zu strukturieren und zu verwalten.

Zum Öffnen eines Projektes benötigen Sie:

- Benutzername
- Passwort
- Gruppenzugehörigkeit

Folgende Benutzergruppen werden von dem Programmiersystem angeboten:

- Wartung
- Inbetriebnahme
- Entwickler
- Administrator

Die einzelnen Rechte, die mit diesen Benutzergruppen verbunden sind, entnehmen Sie bitte der Beschreibung des Programmiersystems.

Bei der initialen Aktivierung der Benutzerverwaltung haben Sie zunächst Administrator-Status. Sie sind dann in der Lage:

- Benutzer anzulegen
- Benutzergruppen zu definieren
- Benutzer den verschiedenen Benutzergruppen zuzuordnen

Ein Benutzer kann Mitglied bei mehreren Benutzergruppen sein. Jede Änderung der Benutzerverwaltung wird durch einen Logbucheintrag dokumentiert.

Benutzerverwaltung SafeLogic compact

Die Benutzerverwaltung bietet Benutzergruppen, die unterschiedliche Berechtigungen zum Übertragen von Konfigurationen an die Geräte haben:

- Maschinenführer
- Instandhalter
- Autorisierter Kunde

Die einzelnen Rechte, die mit diesen Benutzergruppen verbunden sind, entnehmen Sie bitte der Beschreibung des Programmiersystems.

Es kann für jede Benutzergruppe ein Passwort vergeben oder geändert werden.

7.2 Ablauf der Installation und Inbetriebnahme

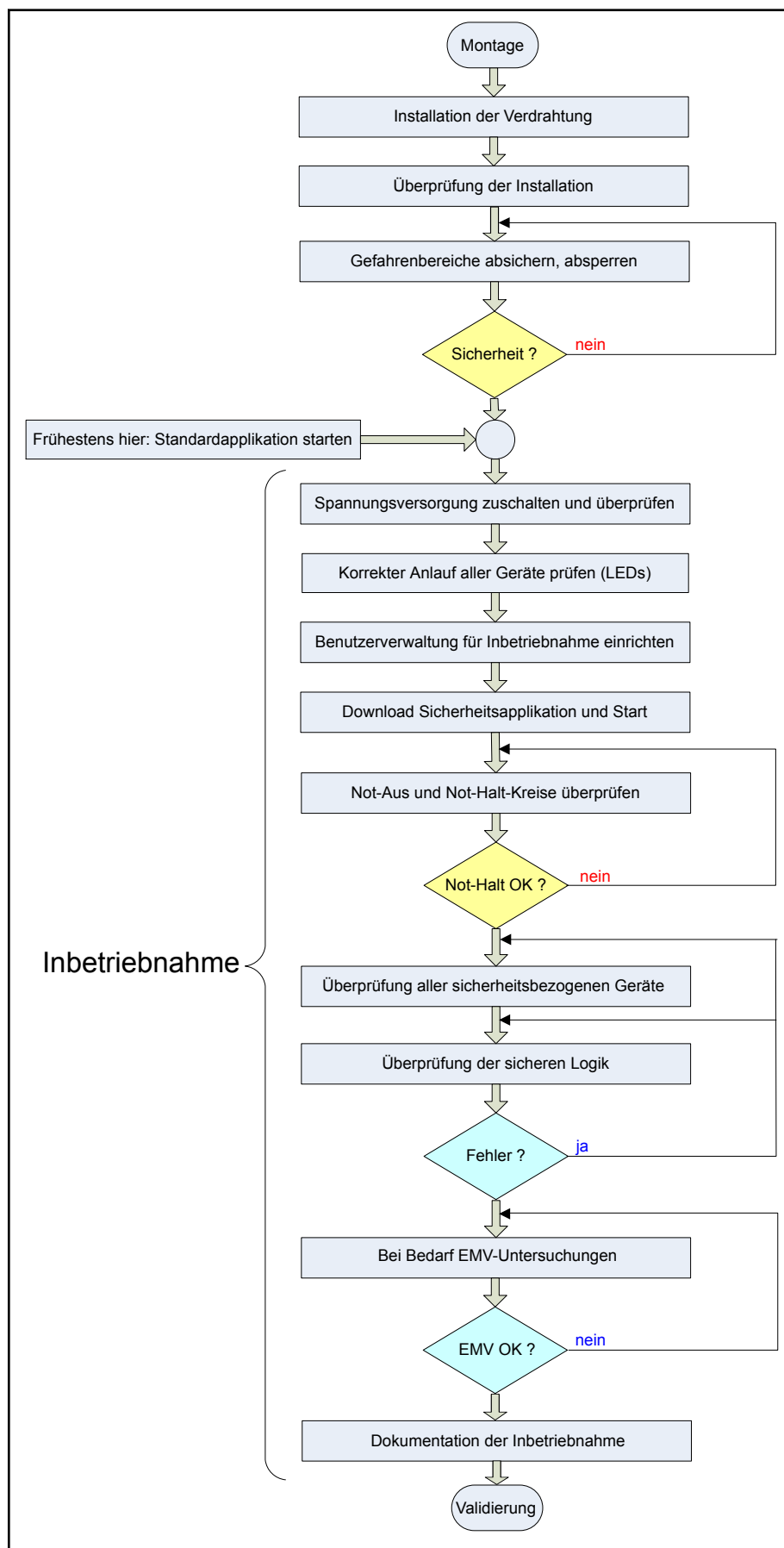


Abb. 7-1: Ablauf Installation und Inbetriebnahme

7.3 Auspacken

Beachten Sie beim Auspacken und Handhaben der elektronischen Komponenten:

HINWEIS

Schäden am Gerät durch elektrostatische Entladungen!

Halten Sie beim Umgang mit Baugruppen und Bauelementen alle Vorkehrungen zum ESD-Schutz ein! Vermeiden Sie elektrostatische Entladungen!

Verpackung Entsorgen Sie die Verpackung entsprechend den nationalen Bestimmungen Ihres Landes.

7.4 Montage und Installation

7.4.1 Gerätemontage des Safety-Funktionsmoduls

Montieren Sie die Sicherheitssteuerung, die sicheren und nicht sicheren I/O-Geräte, die Sensoren und Aktoren nach den Installationsvorschriften der einzelnen Geräte. Berücksichtigen Sie die Maßangaben für die Geräte.



Bauen Sie die Sicherheitssteuerung waagrecht in einen Schaltschrank oder ein entsprechendes Gehäuse mit Schutzart IP54 nach IEC 60529 ein.

Standard-Steuerung und Inline-Module

Zur Montage der Steuerung hängen Sie die Standardsteuerung von oben auf die Hutschiene und rasten die Steuerung dann mit leichtem Druck auf den unteren Teil des Gehäuses ein. Bei Bedarf reihen Sie nun auf der rechten Seite Rexroth Inline-Module an.

Funktionsmodule

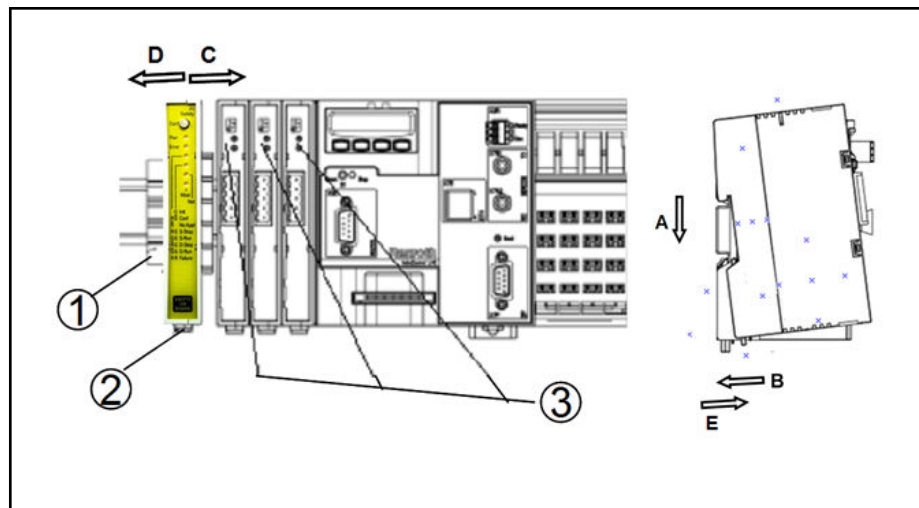
An der linken Seite der Standard-Steuerung können nun über den an der Steuerung angebrachten Funktionsmodul-Stecker eine Anzahl Erweiterungsmodule angeschlossen werden. Die Anzahl und Art der unterstützten Funktionsmodule sind von der verwendeten Standardsteuerung abhängig.



Entnehmen Sie alle Informationen zur Montage der Standardsteuerung, der Inline-Module und der Funktionsmodule bitte dem jeweiligen Handbuch.

Safety-Funktionsmodul

Das Safety-Funktionsmodul wird als letztes Modul eingesetzt. Aus diesem Grund entfällt hier die Einstellmöglichkeit für die Steckplatznummer.



- 1 Endhalter
 2 Montageschienenverriegelung
 3 Funktionsmodul-Steckplatznummern
 A-D Vorgehen bei Montage und Demontage (siehe Text)

Abb. 7-2: Montage Safety-Funktionsmodul

Funktionsmodul aufstecken:

Hängen Sie das Funktionsmodul auf die Montageschiene (A) und kippen (B) Sie das Funktionsmodul gegen die Montageschiene, bis die Verriegelung einrastet.

Danach schieben (C) Sie das Modul auf die linke 120-polige Buchse der Steuerung oder des benachbarten Funktionsmoduls bis eine sichere Verbindung über den PCIPLUS-Bus hergestellt ist. Ggf. verfahren Sie in der gleichen Weise mit weiteren Funktionsmodulen, die nacheinander aufgereiht werden, bis als letztes das Safety-Funktionsmodul montiert wird. Arretieren Sie das Safety-Funktionsmodul mit dem Endhalter auf der Montageschiene.

Funktionsmodul demontieren:

Entfernen Sie den Endhalter. Ziehen Sie das Funktionsmodul nach links (D) von der Steuerung oder dem Nachbarmodul weg. Ziehen Sie mit einem Schraubendreher die Montageschienenverriegelung nach unten und kippen Sie das Funktionsmodul nach vorne (E).



Bei Veränderungen am Gerät – auch im Rahmen von Montage und Installation – verfällt jeglicher Gewährleistungsanspruch gegenüber der Bosch Rexroth AG.

7.4.2 Gerätemontage der SafeLogic compact

Montage und Demontage

Allgemeines

Dieses Kapitel beschreibt die Montage der Module der Sicherheits-Steuerung SafeLogic compact.

Schritte zur Montage von Modulen

⚠ VORSICHT

Das SafeLogic compact System muss in einem Schaltschrank mit mindestens der Schutzart IP 54 montiert werden!

- In einem SafeLogic compact System befindet sich das Hauptmodul SLC-3-CPU0, SCL-3-CPU1 oder SLC-3-CPU3 ganz links
- Die beiden optionalen Gateways folgen unmittelbar rechts vom Hauptmodul
- Montieren Sie weitere SafeLogic compact Erweiterungsmodule (z. B. SLC-3-XTI, SLC-3-XTDIO oder SLC-0-STIO) rechts von den Gateways oder rechts vom Hauptmodul, wenn kein Gateway verwendet wird
- Montieren Sie zusätzliche Relaismodule (UE410-2RO oder UE410-4RO) ganz rechts im SafeLogic compact System
- Die Module sind in einem 22,5 mm breiten Aufbaugehäuse für 35 mm Normschienen nach EN 60 715 untergebracht
- Die Verbindung zwischen den Modulen erfolgt über die in das Gehäuse integrierte FLEXBUS+-Steckverbindung. Berücksichtigen Sie, dass für einen Modultauch die SafeLogic compact Module ca. 10 mm auseinandergeschoben werden müssen, bevor das entsprechende Modul von der Normschiene entfernt werden kann
- Montieren Sie die Module gemäß EN 50 274
- Achten Sie bei der Montage auf geeignete ESD-Schutzmaßnahmen. Andernfalls kann es zu Schäden am Bus FLEXBUS+ kommen
- Treffen Sie geeignete Maßnahmen, damit keine Fremdkörper in die Steckeröffnungen gelangen, insbesondere in die für den Speicherstecker
- Module mit Lüftungsschlitzen müssen vertikal so montiert werden, dass eine vertikale Luftzirkulation möglich ist; d. h. die Lüftungsschlitze müssen oben und unten positioniert sein

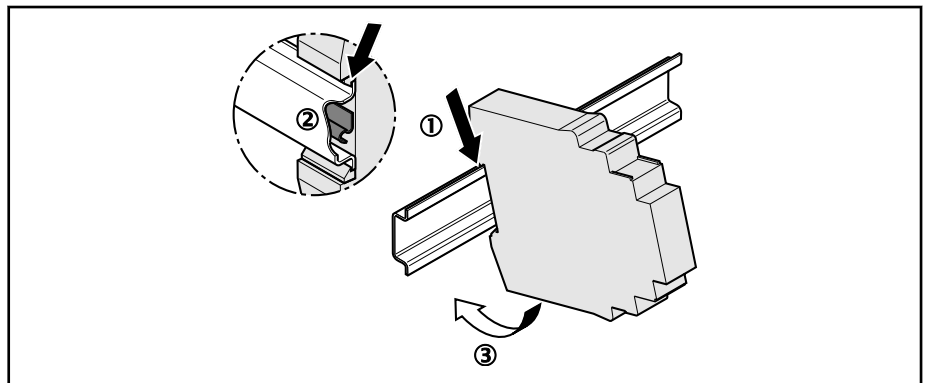


Abb. 7-3: Modul auf Normschiene hängen

- Stellen Sie sicher, dass die Betriebsspannung des SafeLogic compact Systems ausgeschaltet ist
- Hängen Sie das Gerät auf die Normschiene ①
- Achten Sie dabei auf korrekten Sitz der Erdungsfeder ②. Die Erdungsfeder des Moduls muss sicher und elektrisch gut leitend auf der Normschiene aufliegen
- Rasten Sie das Modul mit leichtem Druck in Pfeilrichtung auf der Normschiene ein ③

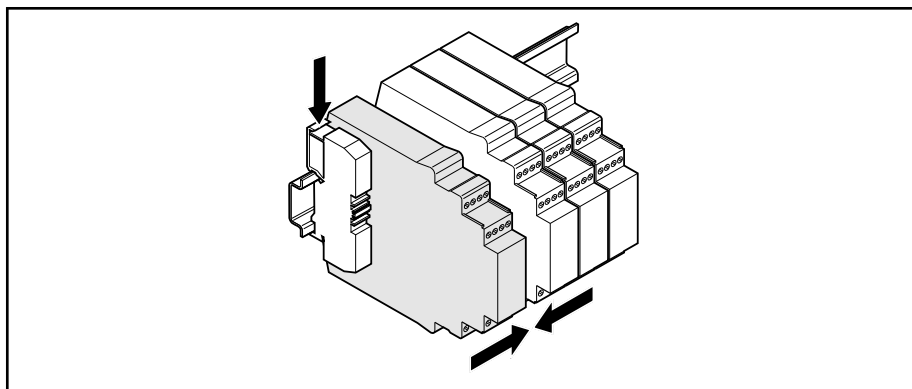


Abb. 7-4: Endklammern installieren

- Sind mehrere Module vorhanden, schieben Sie die Module in Pfeilrichtung einzeln zusammen, bis die seitliche Steckverbindung einrastet
- Installieren Sie links und rechts Endklammern

Im Anschluss an die Montage sind folgende Schritte notwendig:

- Herstellen der elektrischen Anschlüsse
- Konfiguration (siehe Betriebsanleitung "Rexroth IndraLogic SafeLogic compact Designer Software")
- Prüfen der Installation

Schritte zur Demontage von Modulen

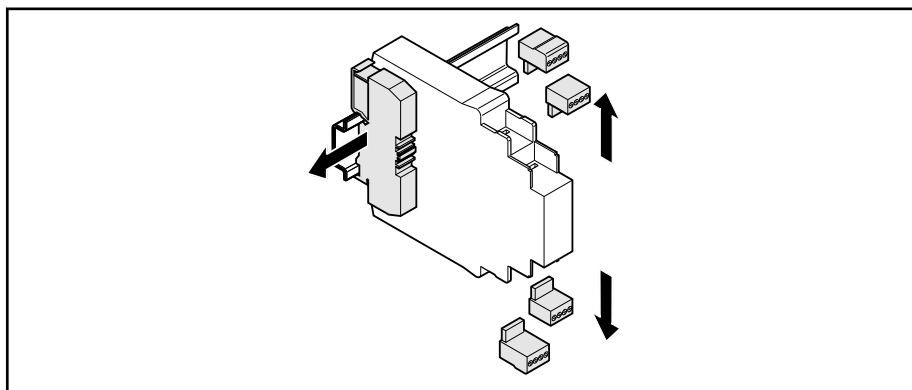


Abb. 7-5: Steckbare Klemmenblöcke entfernen

- Entfernen Sie die steckbaren Klemmenblöcke mit der Verdrahtung und die Endklammern

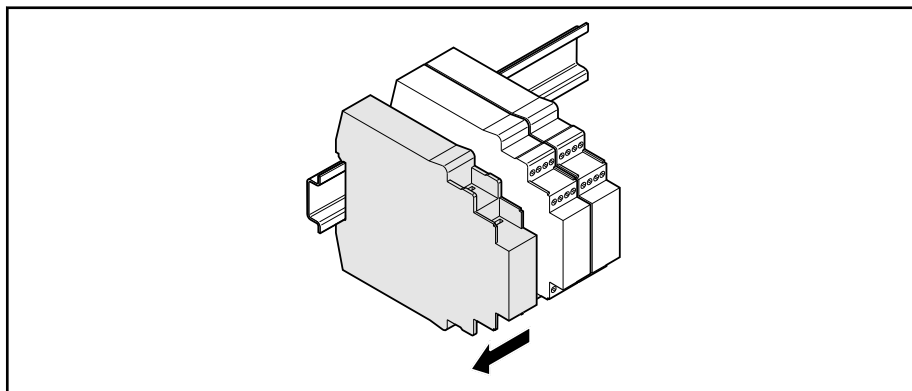


Abb. 7-6: Steckverbindung trennen

- Sind mehrere Module vorhanden, schieben Sie die Module in Pfeilrichtung einzeln auseinander, bis die seitliche Steckverbindung getrennt ist

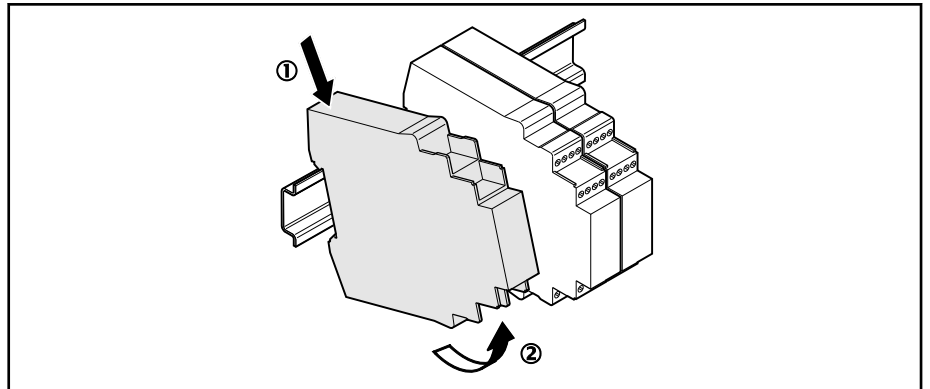


Abb. 7-7: Modul von der Normschiene nehmen

- Drücken Sie das Modul hinten herunter ① und nehmen Sie das Modul im heruntergedrückten Zustand in Pfeilrichtung von der Normschiene ②

7.4.3 Installation der Verdrahtung

Installieren Sie die Verdrahtung nach den vorgegebenen Verdrahtungsplänen und den Installationshinweisen in den einzelnen Gerätebeschreibungen.

Berücksichtigen Sie auch die Installationsvorschriften für die Bussysteme, insbesondere auch die speziellen Anforderungen an die Installation bei Verwendung der sicherheitsbezogenen Profile der Bussysteme für die sichere Datenkommunikation.

Vergewissern Sie sich, dass die Querschnitte der Leitungen den Vorgaben entsprechen.

Kennzeichnen Sie alle Verbindungen (Anschlussleitungen und Steckverbinder) an der Sicherheitssteuerung klar und eindeutig, um Verwechslungen zu vermeiden.

Spannungsversorgung

Beachten Sie:

Die Spannungsversorgung der Sicherheitssteuerung darf nur aus Netzteilen mit sicherer Trennung nach EN 50178 (oder Stromquellen mit gleichem Sicherheitsgrad) mit PELV- Spannung nach EN 61131-2 entnommen werden.

Da das Safety-Funktionsmodul über keine eigene Spannungsversorgung verfügt, beachten Sie bezüglich der elektrischen Installation bitte die Vorgaben im Handbuch der Standardsteuerung.

Geräte

Verdrahten Sie die sicheren und unsicheren I/O-Geräte, die Sensoren und Aktoren und die Sicherheitssteuerung.

Feldbusse

Verkabeln Sie die Feldbusse nach den Installationsanweisungen von Profibus-DP und/oder Sercos III.

- Verwenden Sie nur die zugelassenen Kabel
- Berücksichtigen Sie die Installationshinweise bezüglich EMV
- Installieren Sie die Not-Aus bzw. Not-Halt-Kreise

7.4.4 Überprüfung

Überprüfen Sie die korrekte Montage und Verdrahtung.

Überprüfen Sie die Verdrahtung nach den vorgegebenen Verdrahtungsplänen. Es empfiehlt sich, im Sicherheitsplan die Erstellung eines Abnahmeprotokolls für die Verkabelung vorzuschreiben.

- Achten Sie auf Kurz- und Querschläüssen bei allen Leitungen

- Führen Sie Messungen mit einem Multimeter durch
- Überprüfen Sie, ob die Erdung sicher ausgeführt ist

7.5 Inbetriebnahme der Komponenten

7.5.1 Vor dem Einschalten

Beachten Sie:

Die Inbetriebnahme aller Komponenten ist solange untersagt, bis festgestellt wurde, dass die Maschine oder Anlage, in der diese Komponenten eingebaut sind, den länderspezifischen Bestimmungen, Sicherheitsvorschriften und Normen der Anwendung entspricht.

Sorgen sie für Anlagensicherheit!

- Stellen Sie vor der Inbetriebnahme sicher, dass sich niemand im Gefahrenbereich aufhält!
- Vor der Inbetriebnahme, auch zu Versuchszwecken stets den Schutzleiter anschließen oder mit Erdleiter verbinden. Auf Gehäusen können sonst hohe Spannungen auftreten, die elektrischen Schlag verursachen
- Not-Halt-Schalter leicht zugänglich in unmittelbarer Nähe anordnen
- Verhindern Sie Gefährdungen durch zusätzliche Zugangsabsicherungen, solange nicht alle Sicherheitsfunktionen in Betrieb genommen sind. In Frage kommen mechanische Abdeckungen, Barrieren oder Hindernisse, sogenannte trennende Schutzeinrichtungen
- Spezielle mechanische Vorkehrungen sind vorzusehen, wenn aus Maschinen Teile herausgeschleudert werden können
- Als weitere Maßnahme ist die Begrenzung der Bewegungsgeschwindigkeit, -kraft oder Bewegungsdauer (Tippbetrieb) unter Verwendung einer manuellen Bedienstation mit Zustimmschalter und +/- -Tasten vorteilhaft, sofern die dazugehörenden Sicherheitsfunktionen bereits in Betrieb genommen sind
- Ergänzende Maßnahmen zu den klassischen Sicherheitsfunktionen sind Verriegelungsanzeigen, Leuchten und andere Anlaufwarneinrichtungen



Schalten Sie die Spannung erst zu, wenn das System vollständig aufgebaut ist.

Der Start der Anlage darf erst dann erfolgen, wenn keine Gefährdung von der Anlage ausgehen kann.

7.5.2 Zuschalten der Versorgungsspannung

Überprüfen Sie die korrekte Spannungsversorgung aller Komponenten anhand Ihrer Projektierungsvorgaben.

Überprüfen Sie als nächstes die Funktion der Not-Aus-/Not-Halt-Einrichtung, bevor Sie die Inbetriebnahme fortsetzen.



Die Maschine oder Anlage bei Fehlfunktion der Not-Aus/Not-Halt-Einrichtung nicht betreiben.

7.5.3 Funktionstest und Fehlersuche

Untersuchen Sie das Sicherheitssystem systematisch nach:

- Installationsfehler
- Fehler durch Störungen (EMV-Einflüsse)

- Fehler durch Störungen in der Versorgungsspannung, Spannungseinbruch oder Spannungsausfall
- Einwirkungen auf die Netzwerkverdrahtungen und Kommunikation
- Applikationsfehler

Durch die Komponentendiagnose und das Programmiersystem werden Sie bei dieser Aufgabe unterstützt.

Das Programmiersystem bietet dafür folgende Funktionalitäten:

- Monitoring von Variablen
- Forcen von Variablen
- Debugging und Ablaufkontrolle
- Online-Änderungen von Variablen, Funktionsblöcken, Parameter

EMV Vermeiden Sie den Betrieb von Hochfrequenz-, Fernsteuer- und Funkgeräten in der Nähe der Geräteelektronik und deren Zuleitungen. Wenn ein Gebrauch dieser Geräte unvermeidlich ist, müssen Sie das System auf mögliche Fehlfunktionen prüfen.

Die einzelnen Komponenten sind durch Typprüfungen hinsichtlich der Einhaltung der einzuhaltenden Normen (Fachgrundnormen für den Industriebereich und/oder EMV-Produktnormen) geprüft und erfüllen die EG-EMV-Richtlinie.

Die eingehaltenen Grenzwerte und Normen sind der Dokumentation zu dem jeweiligen Produkt zu entnehmen. Die Prüfungen erfolgten an einem systemtypischen Aufbau auf einem normkonformen Messplatz.

Die Prüfergebnisse sind jedoch nicht in allen Fällen auf den eingebauten Zustand im Endprodukt, der Maschine oder Anlage übertragbar. Im Bedarfsfalle ist eine spezielle EMV-Prüfung der Anlage notwendig.

Anlauf der Geräte

- Überprüfen Sie anhand der Anzeige-LEDs, ob alle Geräte und Module korrekt anlaufen oder ob Fehler angezeigt werden

Überprüfung der Geräteanschlüsse

- Überprüfen Sie den korrekten Anschluss der sicheren Geräte an die zugeordneten Sensoren und Aktoren

Überprüfung der Ein-/Ausgänge

- Messen Sie die Ein-/Ausgangsspannungen um festzustellen, dass die Spannungen im zulässigen Bereich liegen
- Messen Sie falls möglich die Wellenform der Signale um das dynamische Verhalten den Erwartungen entspricht
- Sind bei Eingängen, die zweikanalig beschaltet werden, beide Kanäle zueinander passen parametrisiert?
- Ist bei Eingängen die Zuordnung zu den richtigen Taktausgängen parametrisiert?

Überprüfung der Konfiguration

- Verifizierung der Variablenverknüpfung zwischen den Funktionsbausteinen und den Ein-/Ausgängen

Überprüfung der Datenkommunikation

- Verifizieren Sie die Kommunikationsparameter der Buskommunikation
- Haben Sie alle Adressen korrekt vorgegeben?
- Haben Sie die richtige Übertragungsgeschwindigkeit eingestellt?

7.5.4 Inbetriebnahme SafeLogic

Inbetriebnahme der Applikation

Inbetriebnahmeschritte des Safety-Funktionsmoduls

1. Standard-SPS herunterladen und starten.
2. Motion herunterladen und in P4 bringen.
3. Sicherheits-SPS herunterladen und starten.
4. ggf. Anlauffehler der Bussysteme quittieren.

Debug-Mode

Zum Testen der Funktionalität des Applikationsprogramms und zur Fehlersuche ist der Debug-Mode vorteilhaft einzusetzen. In diesem Betriebszustand ist die Sicherheitssteuerung in Betrieb und arbeitet das Anwendungsprogramm ab. Der Debug-Mode bietet jedoch umfangreiche Inbetriebnahmemöglichkeiten, angefangen vom Forcen von Eingängen bis hin zum Einzelschrittbetrieb, insbesondere auch die Möglichkeit, die Applikation Online zu ändern.

Damit können nicht nur Fehler im Applikationsprogramm diagnostiziert werden sondern das Sicherheits-System und die Sicherheitsfunktionen schrittweise in Betrieb genommen werden. Dieser Betriebszustand ist aufgrund der erweiterten Möglichkeiten nicht sicher, Debug-Kommandos potenziell gefährbringend.



Stellen Sie im Betriebszustand "Debug" durch organisatorische Maßnahmen sicher, dass kein Schaden durch beabsichtigte oder fehlerhafte Funktion der Sicherheitssteuerung entstehen kann.

In den Debug-Modus können nur Personen gelangen, die als Administrator oder Programmierer in der Benutzerverwaltung für die Sicherheitssteuerung angemeldet sind.

Gewährleisten Sie, dass sich kein Mensch im Gefahrenbereich aufhält und auch niemand den Gefahrenbereich betreten kann.

Inbetriebnahme der Sicherheitsfunktionen

Testen Sie die Funktion der Sicherheitsfunktionen. Diese technische Prüfung darf nur durch befähigte Personen erfolgen.

Die technische Prüfung umfasst folgende Prüfpunkte:

- Kennzeichnen Sie alle Anschlussleitungen und Steckverbinder eindeutig, um Verwechslungen zu vermeiden. Sie müssen sicherstellen, dass gelöste Anschlussleitungen nicht am falschen Anschluss wieder angeschlossen werden
- Führen Sie eine vollständige Verifizierung der Sicherheitsfunktionen der Anlage in jeder Betriebsart und eine Fehlersimulation durch. Beachten Sie insbesondere die Ansprechzeiten der einzelnen Applikationen
- Überprüfen Sie die Signalpfade und die korrekte Einbindung in übergeordnete Steuerungen
- Prüfen Sie die korrekte Datenübertragung von und zur Sicherheitssteuerung
- Prüfen Sie das Logik-Programm der Sicherheitssteuerung
- Dokumentieren Sie vollständig die Konfiguration der Anlage, der einzelnen Geräte und das Ergebnis der Sicherheitsprüfung
- Prüfen Sie die Sicherheitsfunktionen der Maschine oder Anlage vollständig und stellen Sie sicher, dass die Sicherheitsfunktionen einwandfrei funktionieren

- Überprüfen Sie die an die Sicherheitssteuerung angeschlossenen Geräte entsprechend den Prüfhinweisen in den zugehörigen Betriebsanleitungen
- Um ein unbeabsichtigtes Überschreiben der Konfiguration zu verhindern, aktivieren Sie den Schreibschutz

Inbetriebnahme-Dokumentation

Logbuch des Safety-Funktionsmoduls

Die während der Inbetriebnahme dokumentierten Informationen müssen einschließen:

- Die Dokumentation der Inbetriebnahmetätigkeiten
- Hinweise auf Berichte zu Ausfällen
- Die Behebung von Ausfällen und Inkompatibilitäten

Das Safety-Funktionsmodul unterstützt Sie bei der Inbetriebnahmedokumentation durch das Führen eines Logbuchs, das im Online-Betrieb am Programmersystem angezeigt wird.

Dieses Logbuch protokolliert eine Reihe von Ereignissen in der Sicherheitssteuerung mit Datum und Uhrzeit des Auftretens, ausführende Person (identifiziert über die Benutzerverwaltung), Typ (Information, Warnung, Fehler, Exception) und weiteren typabhängigen Klartextinformationen.

Die folgenden Ereignisse werden eingetragen:

- Login/Logout
- Download einer Applikation
- Stop-/Run-Umschaltung
- Forcen von Eingängen
- Bootapplikation erstellen
- Abnahmevermerk
- Systemfehlermeldungen
- Urlöschen (Löschen der Applikation und der Benutzerverwaltung)

Das Logbuch ist als Ringbuffer organisiert und bietet Kapazität für mehrere tausend Einträge. Das Logbuch kann nicht gelöscht werden, so dass die im Rahmen der Kapazität letzten Einträge unwiderruflich dokumentiert sind.

Pinnen

Vorbereitende Maßnahme für die Verifikation

Für die Verifikation der Sicherheitsapplikation muss der Entwickler vorbereitende Maßnahmen treffen. Ein wesentlicher Aspekt hierbei ist es, den zur Verifikation vorgesehenen Stand der Sicherheitsapplikation festzusetzen und somit sicherzustellen, dass immer nur genau dieser Stand der Sicherheitsapplikation für die Verifikation, Validierung und anschließende Abnahme verwendet wird.

Speziell hierfür bietet der IndraWorks Safety Manager die Funktion **Pinnen**.



Bevor die programmierte oder geänderte Sicherheitsapplikation verifiziert wird, ist die Sicherheitsapplikation neu zu pinnen.

Verifikation und Abnahme darf nur bei gepinnten Applikationen durchgeführt werden. Kein Objekt der Applikation darf den Status "In Work" aufweisen.

Die Prüfung auf "In Work" erfolgt bei den einzelnen Verifikationsschritten.

	 Eine gepinnte Applikation darf erst nach der Verifikation (siehe Kap. 7.5.4 "Inbetriebnahme SafeLogic" auf Seite 112) als überprüft angesehen werden.
Was ist Pinnen	Pinnen bedeutet, dass ein Referenzpunkt auf den aktuellen Stand einer Sicherheitsapplikation gesetzt wird, der den konkreten Stand der Sicherheitsapplikation und der dazugehörigen Objekte identifiziert. Mittels Pin ist es möglich, einen bestimmten Stand der Applikation im Projekt, eines Objekts im Editor und einer Bootapplikation auf der Sicherheitssteuerung zu identifizieren. Außerdem kann der Verifizierende – basierend auf dem Pin – jederzeit Änderungen in der Applikationsstruktur, im Inhalt ihrer Objekte und in den angezogenen Bibliotheksbausteinen erkennen.
	 Durch das Setzen eines Pins wird ein konkreter Stand identifizierbar gemacht, es wird dabei jedoch keine Kopie des konkreten Standes erzeugt!
	 Ein gepinntes Objekt kann durch Export/Import auf eine andere Applikation übertragen werden, ohne das Objekt erneut verifizieren zu müssen. Es muss lediglich die Objekt-Pin geprüft werden.
Vergleichsansicht	Die Pin-Funktionen sind im Editor des Applikationsobjekts zu finden. Dazu wird im Projektbaum das Safety-Applikationsobjekt selektiert und über den Kontextmenü-Befehl Öffnen geöffnet. Die Registerkarte Objekte zeigt die Vergleichsansicht, welche die Version und die Prüfsumme der Objekte des aktuellen Projekts und des gepinnten Projekts darstellt.
	 Weitere Informationen finden Sie in Kapitel "Pinnen" der Dokumentation "Rexroth IndraWorks 14VRS SafeLogic Projektkonfiguration".

Verifikation

Als Voraussetzung muss der Anwender in früheren Entwicklungsphasen spezifiziert haben, was sein gewünschtes Verhalten der Software-Applikation ist (Software-Spezifikation) und was seine gewünschten Regeln von Programmierung und Kommentierung (Programmierrichtlinien) sind.

Mit dem Prozess der Software-Verifikation wird nachgewiesen, dass die Spezifikation und die Programmierrichtlinien erfüllt und damit verifiziert sind. Die Software-Verifikation erfolgt durch die Kombination von statischen und dynamischen Verifikationsmethoden (toolbasierte Checks, Codereview, Tests).

Der Software-Verifikation folgt als weiterer Verifikationsschritt die Validierung der programmierten Sicherheitsfunktionen in der aufgebauten Maschine.

Beides sind Voraussetzungen für die Abnahme von Maschine und Sicherheitsapplikation.


 Verifikation und Abnahme darf nur auf gepinnten Sicherheitsapplikationen durchgeführt werden. Kein Objekt der Applikation darf den Status "In Work" aufweisen.


 Der gelbe Datenfluss ist als Unterstützung für Verifikation, Validierung und Abnahme nicht geeignet.



Die IndraWorks-Standard-Projektansicht ist für die Verifikation und Abnahme einer Sicherheitsapplikation **nicht geeignet**. Zum Nachweis, welche Objekte zur Sicherheitsapplikation gehören muss die Vergleichsansicht verwendet werden.



Der IndraWorks-Standard-Projektvergleich ist für die Verifikation und Abnahme einer Sicherheitsapplikation **nicht geeignet**. Der Projektvergleich kann lediglich als Hilfsfunktion verwendet werden, um die Vergleichseditoren geänderter Objekte zu öffnen.



Um den gesamten Prozess der Verifikation und Validierung zu vereinfachen und damit zu beschleunigen, stellt SafeLogic die bereits validierten und zertifizierten PLCopen-Bausteine und die Bausteine der SafetyStandard-Bibliothek zur Verfügung.



Weitere Informationen finden Sie in Kapitel "Verifikation" der Dokumentation "Rexroth IndraWorks 14VRS SafeLogic Projektkonfiguration".

Abnahme

Abnahme, Einleitung



Während des gesamten Prozesses von der Entwicklung bis zur Abnahme einer Sicherheitsapplikation muss von Anwenderseite dafür gesorgt werden, dass die richtigen Objektstände, die richtigen Bibliotheken und richtigen Gerätebeschreibungsdateien verwendet werden (siehe [Kap. "Pinnen" auf Seite 113](#)).



Der Anwender ist dafür verantwortlich, dass bei der Abnahme der Sicherheitsapplikation alle dafür relevanten Normen eingehalten werden.



Für die Beurteilung der richtigen Verwendung der FB-Schnittstelle ist die zu dieser Steuerung gehörende Anwenderdokumentation für diesen FB in der nachgewiesenen Version heranzuziehen.



Die IndraWorks-Standard-Projektansicht ist für die Verifikation und Abnahme einer Sicherheitsapplikation **nicht geeignet**. Zum Nachweis, welche Objekte zur Sicherheitsapplikation gehören muss die Vergleichsansicht verwendet werden.



Der IndraWorks-Standard-Projektvergleich ist für die Verifikation und Abnahme einer Sicherheitsapplikation **nicht geeignet**. Der Projektvergleich kann lediglich als Hilfsfunktion verwendet werden, um die Vergleichseditoren geänderter Objekte zu öffnen.

Voraussetzungen und Nachweise für die Abnahme



Der Anwender muss vor der Abnahme seiner Sicherheitsapplikation verifizieren, dass die vorliegende Applikation, aus der tatsächlich die Bootapplikation erzeugt wird, gepinnt ist, die richtige Pin-Kennung angezeigt wird, und dass keine Abweichung des Projektstandes vom gepinnten Stand gemeldet wird.



Für die Abnahme ist vom Anwender zu prüfen, ob im Projekt tatsächlich die zum Gerät in der Maschine passende Gerätebeschreibung zum Einsatz kommt.



Weitere Informationen finden Sie in Kapitel "Abnahme" der Dokumentation "Rexroth IndraWorks 14VRS SafeLogic Projektkonfiguration".

7.5.5 Technische Inbetriebnahme SafeLogic compact

Allgemeines

Bevor Sie mit der technischen Inbetriebnahme beginnen, muss die Konfiguration des SafeLogic compact Systems abgeschlossen sein.

Verdrahtung und Spannungsversorgung

⚠ VORSICHT

Beachten Sie beim Anschluss des SafeLogic compact Systems die technischen Daten in der Betriebsanleitung "Rexroth IndraControl SafeLogic compact Hardware"!

- Schließen Sie die einzelnen Feldgeräte an die entsprechenden Signalanschlüsse an und prüfen Sie für jeden Sicherheitseingang, Test/Signalausgang und Sicherheitsausgang, ob sich diese Ein/Ausgänge wie für die Applikation erforderlich verhalten. Diagnoseinformationen der SafeLogic compact LEDs unterstützen Sie bei der Validierung der einzelnen Feldsignale. Prüfen Sie, ob die Außenbeschaltung, die Ausführung der Verdrahtung, die Wahl der Befehlsgeber und deren Anordnung an der Maschine dem geforderten Sicherheitsniveau entspricht
- Beheben Sie eventuelle Störungen (z. B. falsche Verdrahtung oder gekreuzte Signale) an jedem Sicherheitseingang, Test/Signalausgang oder Sicherheitsausgang, bevor Sie mit dem nächsten Schritt fortfahren
- Schalten Sie die Spannungsversorgung ein. Sobald an den Anschlüssen "A1" und "A2" der Controller-Module CPU0/CPU1/CPU3 bzw. der XTIO/XTDS/STIO-Modulen die Versorgungsspannung anliegt, führt das SafeLogic compact System automatisch die folgenden Schritte aus:
 - interner Selbsttest
 - Laden der gespeicherten Konfiguration
 - Test der geladenen Konfiguration auf Gültigkeit

Das System geht nicht in Betrieb, wenn die oben beschriebenen Schritte nicht erfolgreich durchgeführt werden konnten. Im Fehlerfall erfolgt eine entsprechende LED-Anzeige (siehe Projektierungshandbuch SafeLogic compact Hardware) und das SafeLogic compact System setzt alle übermittelten Werte auf Low.

Übertragen der Konfiguration

Nachdem Sie die Hardware und die Logik im SafeLogic compact System konfiguriert und auf Richtigkeit geprüft haben, übertragen Sie die Konfiguration über den SafeLogic Designer an das SafeLogic compact System.

Technische Prüfung und Inbetriebnahme

Die Maschine oder Anlage, die durch eine Sicherheits-Steuerung SafeLogic compact geschützt wird, darf nur nach einer erfolgreichen technischen Prüfung sämtlicher Sicherheitsfunktionen in Betrieb genommen werden. Die technische Prüfung darf nur durch befähigte Personen erfolgen.

Die technische Prüfung umfasst folgende Prüfpunkte:

- Kennzeichnen Sie alle Anschlussleitungen und Steckverbinder am SafeLogic compact System eindeutig, um Verwechslungen zu vermeiden. Da das SafeLogic compact System mehrere Anschlüsse gleicher Bauform besitzt, müssen Sie sicherstellen, dass gelöste Anschlussleitungen nicht am falschen Anschluss wieder angeschlossen werden
- Verifizieren Sie die Konfiguration des SafeLogic compact Systems
- Überprüfen Sie die Signalpfade und die korrekte Einbindung in übergeordnete Steuerungen
- Prüfen Sie die korrekte Datenübertragung von und zur Sicherheits-Steuerung SafeLogic compact
- Prüfen Sie das Logik-Programm der Sicherheits-Steuerung
- Dokumentieren Sie vollständig die Konfiguration der gesamten Anlage, der einzelnen Geräte und die Ergebnisse der Sicherheitsprüfung
- Prüfen Sie die Sicherheitsfunktionen der Maschine oder Anlage vollständig und stellen Sie sicher, dass die Sicherheitsfunktionen einwandfrei funktionieren
- Um ein unbeabsichtigtes Überschreiben der Konfiguration zu verhindern, aktivieren Sie den Schreibschutz der Konfigurationsparameter des SafeLogic compact Systems. Veränderungen sind jetzt erst wieder möglich, wenn der Schreibschutz aufgehoben wurde

7.5.6 Modifikationen

Bei Hinzufügen oder Austauschen von Komponenten oder anderen Veränderungen des bereits in Betrieb genommenen Sicherheitssystems oder Teilsystemen davon ist die Inbetriebnahme aller betroffenen Teile und Sicherheitsfunktionen zu wiederholen.

Modulwechsel

Führen Sie Modulwechsel nicht unter Spannung durch. Vergewissern Sie sich, dass das neue Gerät den richtigen Typ und die richtige Version hat.

- **SLc**

Die Systemkonfiguration des gesamten SafeLogic compact Systems ist nur im Speicherstecker gespeichert. Dies bietet beim Austausch von Erweiterungsmodulen den Vorteil, dass das SafeLogic compact System nicht neu konfiguriert werden muss

- **SL**

Beim Austausch des SafeLogic-Funktionsmoduls kann die Memory-Card des alten Funktionsmoduls übernommen werden. Die Memory-Card enthält:

- Applikationsprogramm (Bootapplikation)
- Daten zur Benutzerverwaltung

- Logbuch
- Firmware des Safety-Funktionsmoduls

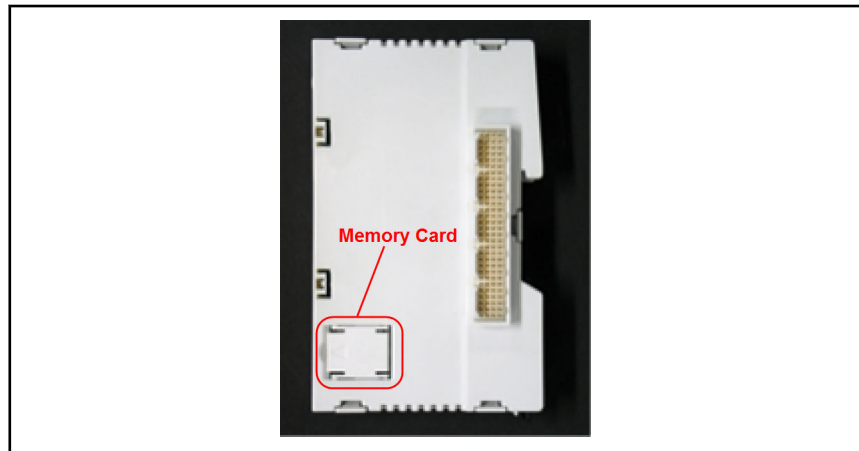


Abb. 7-8: Position der Memory-Card auf dem SafeLogic-Funktionsmodul

- **Profibus Inline-Buskoppler**

Beim Austausch des Profibus-Kopplers muss die Profibus-Adresse am Koppler wieder eingestellt werden. Beim Tausch der PROFISafe-I/O muss die DIP-Schalterstellung vom alten Modul übernommen werden.

- **Profinet Inline-Buskoppler**

Beim Tausch der PROFISafe-I/Os muss die DIP-Schalterstellung vom alten Modul übernommen werden.

Weitere Informationen zum Gerätetausch des Profinet Inline-Buskopplers finden Sie in der Dokumentation "Rexroth IndraWorks 14VRS Feldbusse", Kapitel "PROFINET IO", Unterkapitel "PROFINET IO, Topologie und Gerätetausch" (siehe ["Weiterführende Dokumente" auf Seite 2](#)).

- **Sercos Buskoppler**

Beim Tausch der CSos S20-I/Os muss die DIP-Schalterstellung vom alten Modul übernommen werden.

Weitere Informationen zum Gerätetausch des Sercos S20-S3-BK+ - Buskopplers finden Sie in der Dokumentation "Rexroth IndraWorks 14VRS Feldbusse", Kapitel "Sercos III IO", Unterkapitel "Sercos III Master, Slave hinzufügen" (siehe ["Weiterführende Dokumente" auf Seite 2](#)).

- **IndraDrive**

Beim IndraDrive sind alle Parameter inkl. SafeMotion im Display gesichert. Beim Tausch wird das Display auf den neuen Antrieb übernommen. Beim Bootvorgang des Antriebs erscheint im Display "Load New Safety". Die Funktion des Antriebs ist zu prüfen.

8 Diagnose und Störungsbeseitigung

8.1 Diagnosekonzept

Innerhalb des Sicherheitssystems haben Sie umfassende Möglichkeiten zur Diagnose.

Zunächst werden die Betriebs- und Fehlerzustände über die LED-Anzeigen an den Geräten selbst dargestellt. Ihre Bedeutungen entnehmen Sie bitte den jeweiligen Gerätebeschreibungen. Das Safety-Funktionsmodul sowie die SafeLogic compact sind in [Kap. 4.4 "Sicherheitssteuerungen" auf Seite 47](#) beschrieben.

Darüber hinaus werden Fehlermeldungen und Statusinformationen im Online-Betrieb des Programmiersystems dargestellt. Diese Diagnosemeldungen sind nicht sicherheitsrelevant und werden über die Standardkanäle an das Programmiersystem gesendet.

Gerätediagnose des Safety-Funktionsmoduls

Der Gerätedialog zeigt Status-Informationen (z. B. "Running", "Stopped") und spezifische Diagnosemeldungen aus dem jeweiligen Gerät und dem Bussystem. Diese Informationen werden im Anzeigefeld "Status" des Geräteeeditors dargestellt.

Name	Wert	Beschreibung
SafetyFM-Diagnose		
Elektronisches Typenschild		
Typ	CFL01.1-F1	
Seriennummer	6983074	
Materialnummer	R911170129	
Materialindex	AD1	
SafetyFM-Versionen		
Bootlader	SMRB 01V04.14	Version des Bootladers
Firmware	SMFW 02V04.0569	Version der Firmware
Hardware	72	
FPGA	0x2050000	
Status		
Zustand der IO-Konfiguration	IO Config: Error	
ID der IO-Konfiguration		
Safety-Konfigurations-Id	0xCDFFA052	
Standard-Konfigurations-Id	0x693FDE10	
Eingestellte Safety-Zykluszeit	10 ms	
Auslastung der Safety-Zykluszeit	13 %	
Safety-Zyklen ohne Quittung	0	
Safety-Zyklen mit Kollision	0	
Bearbeitungszeit		
Gesamtbearbeitungszeit		

Abb. 8-1: Anzeige Gerätestatus (Beispiel: Safety-Funktionsmodul)

Welche Diagnoseinformationen zur Verfügung stehen, sind geräteabhängig. Es können Statusmeldungen oder Fehlermeldungen und weiterführende Informationen dazu sein. Fehlermeldungen können sich auf Baugruppenfehler, Kommunikationsfehler bis hin zu Peripheriefehlern, wie z. B. Kurzschluss oder Diskrepanzzeitverletzungen, beziehen.

Sicherheitssteuerung Der aktuelle Baugruppenstatus für Standardsteuerung und Safety-Funktionsmodul wird im Online-Betrieb am Programmiersystem angezeigt. In Logbüchern (Safety-Modul und Standardsteuerung separat) werden Fehler, Warnungen, Ausnahmen und weitere Informationen mit Datum und Hinweisen zur Lokalisierung registriert und gespeichert. Diese weiteren Informationen beziehen sich auf die CPU, die Baugruppenfirmware, das Ablaufverhalten und den Online-Dialog.

Programmdiagnose Zur Diagnostizierung des Verhaltens Ihrer Applikation stellt das Programmiersystem verschiedene Debug-Dienste zur Verfügung. Neben anderen sind hervorzuheben:

- Darstellung des aktuellen Variablenzustands
- Informationen über das Task-Verhalten (Zyklen, Zykluszeiten, Status)
- Dynamische Bausteinanalyse (Ausführungszeiten, Anzahl der Aufrufe, nicht durchlaufene Codezeilen)

Durch die Möglichkeiten, Haltepunkte zu setzen, können Sie Ihr Applikationsprogramm Schritt für Schritt systematisch analysieren.

Lesen Sie hierzu die Dokumentationen zum Programmiersystem "SafeLogic Designer" und "IndraWorks" (siehe ["Weiterführende Dokumente" auf Seite 2](#)).

8.2 Logbuch der SafeLogic compact

Wenn Sie eine Verbindung zu Ihrem SafeLogic compact System hergestellt haben, haben Sie die Möglichkeit, eine Diagnose Ihres Systems durchzuführen. In der Ansicht "Diagnose" steht Ihnen in der oberen Hälfte des Fensters eine Liste aller Meldungen, Informationen, Warnungen und Fehlermeldungen Ihres Systems zur Verfügung. Wenn Sie auf einen der Einträge in der Liste klicken, werden Ihnen in der unteren Hälfte des Fensters Details zu der ausgewählten Meldung angezeigt.

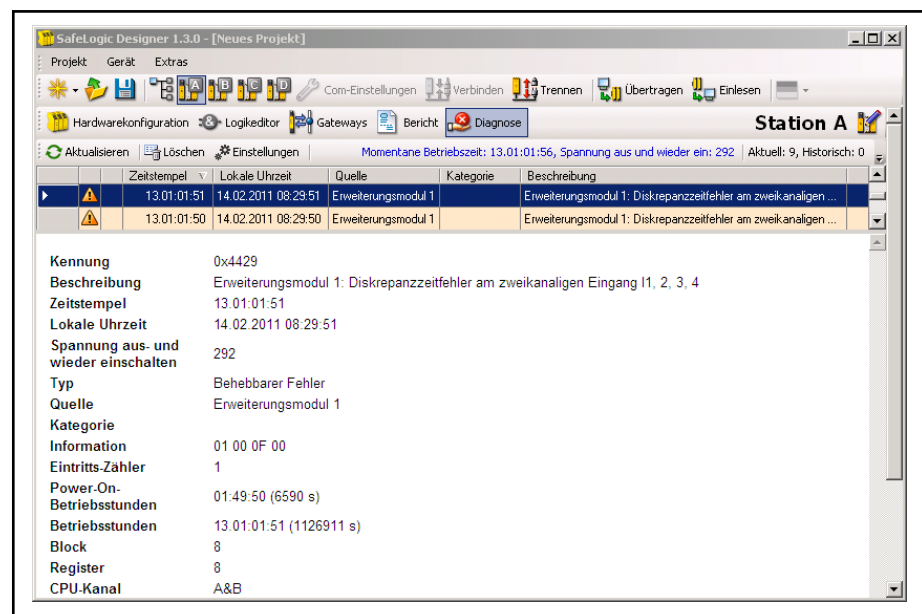
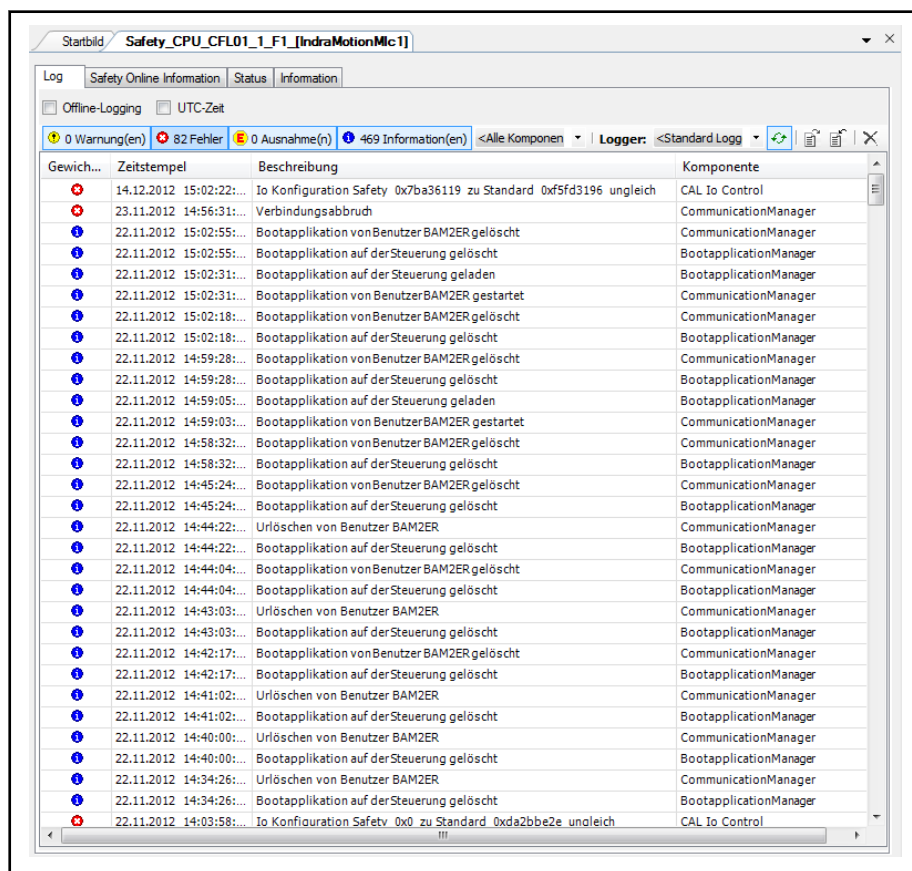


Abb. 8-2: Diagnoseübersicht

8.3 Logbuch des Safety-Funktionsmoduls



Gewich...	Zeitstempel	Beschreibung	Komponente
✖	14.12.2012 15:02:22:...	Io Konfiguration Safety 0x7ba36119 zu Standard 0xf5fd3196 ungleich	CAL Io Control
✖	23.11.2012 14:56:31:...	Verbindungsabbruch	CommunicationManager
ⓘ	22.11.2012 15:02:55:...	Bootapplikation von Benutzer BAM2ER gelöscht	CommunicationManager
ⓘ	22.11.2012 15:02:55:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 15:02:31:...	Bootapplikation auf der Steuerung geladen	BootapplicationManager
ⓘ	22.11.2012 15:02:31:...	Bootapplikation von Benutzer BAM2ER gestartet	CommunicationManager
ⓘ	22.11.2012 15:02:18:...	Bootapplikation von Benutzer BAM2ER gelöscht	CommunicationManager
ⓘ	22.11.2012 15:02:18:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:59:28:...	Bootapplikation von Benutzer BAM2ER gelöscht	CommunicationManager
ⓘ	22.11.2012 14:59:28:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:59:05:...	Bootapplikation auf der Steuerung geladen	BootapplicationManager
ⓘ	22.11.2012 14:59:03:...	Bootapplikation von Benutzer BAM2ER gestartet	CommunicationManager
ⓘ	22.11.2012 14:58:32:...	Bootapplikation von Benutzer BAM2ER gelöscht	CommunicationManager
ⓘ	22.11.2012 14:58:32:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:45:24:...	Bootapplikation von Benutzer BAM2ER gelöscht	CommunicationManager
ⓘ	22.11.2012 14:45:24:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:44:22:...	Ulröschen von Benutzer BAM2ER	CommunicationManager
ⓘ	22.11.2012 14:44:22:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:44:04:...	Bootapplikation von Benutzer BAM2ER gelöscht	CommunicationManager
ⓘ	22.11.2012 14:44:04:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:43:03:...	Ulröschen von Benutzer BAM2ER	CommunicationManager
ⓘ	22.11.2012 14:43:03:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:42:17:...	Bootapplikation von Benutzer BAM2ER gelöscht	CommunicationManager
ⓘ	22.11.2012 14:42:17:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:41:02:...	Ulröschen von Benutzer BAM2ER	CommunicationManager
ⓘ	22.11.2012 14:41:02:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:40:00:...	Ulröschen von Benutzer BAM2ER	CommunicationManager
ⓘ	22.11.2012 14:40:00:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
ⓘ	22.11.2012 14:34:26:...	Ulröschen von Benutzer BAM2ER	CommunicationManager
ⓘ	22.11.2012 14:34:26:...	Bootapplikation auf der Steuerung gelöscht	BootapplicationManager
✖	22.11.2012 14:03:58:...	Io Konfiguration Safetyv 0x0 zu Standard 0xda2bbe2e ungleich	CAL Io Control

Abb. 8-3: Logbuch der Sicherheitssteuerung

Das Logbuch wird in der Registerkarte **Log** der Sicherheitssteuerung angezeigt und dient als Protokoll und zur Diagnose von Laufzeitfehlern der Applikation und Systemfehlern. Es kann helfen, die Ursache eines Fehlers in der SPS oder in der Applikation zu finden.

In IndraWorks stehen zwei Logbücher zur Verfügung:

- Geräte-Logbuch
- Applikations-Logbuch

Das Geräte-Logbuch gehört zum Gerät und ist für Einträge gedacht, die das Gerät betreffen, z. B. Systemfehler, Erzeugen neuer Bootapplikationen.

Das Applikations-Logbuch gehört zur IEC-Applikation und ist für Einträge gedacht, die die Applikation betreffen, z. B. Laufzeitfehler, Fehler beim Laden der Bootapplikation, Fehler bei der Online-Kommunikation.

Das Applikations-Logbuch ist das Default-Logbuch der Sicherheitssteuerung. Das Geräte-Logbuch steht erst dann zur Verfügung, wenn das Default-Logbuch (Applikations-Logbuch) geladen ist.

Durch Betätigen der Schaltfläche  werden alle zur Verfügung stehenden Logbücher (Geräte- und Applikations-Logbuch) zyklisch von der Steuerung geladen und können in Fenster **Logger** selektiert werden.

Die in den Logbüchern angezeigten Informationen sind folgendermaßen strukturiert:

- Gewichtung (Information, Warnung, Fehler, Ausnahme)

- Zeitstempel
- Fehlerbeschreibung
- Komponente (Erzeuger)

8.4 Logbuch der Standardsteuerung

Das Logbuch der Standardsteuerung zeichnet unter anderem Probleme beim Verbindungsaufbau und bei der Datenübertragung von und zu sicheren Bus-teilnehmern auf. Das Logbuch kann durch einen Doppelklick auf die Steuerung und nachfolgender Auswahl der Registerkarte **Log** erreicht werden.

Das Logbuch der Standard-SPS befindet sich in RAM der Steuerung. Das Logbuch geht beim Aus- und wieder Einschalten der Steuerung verloren.

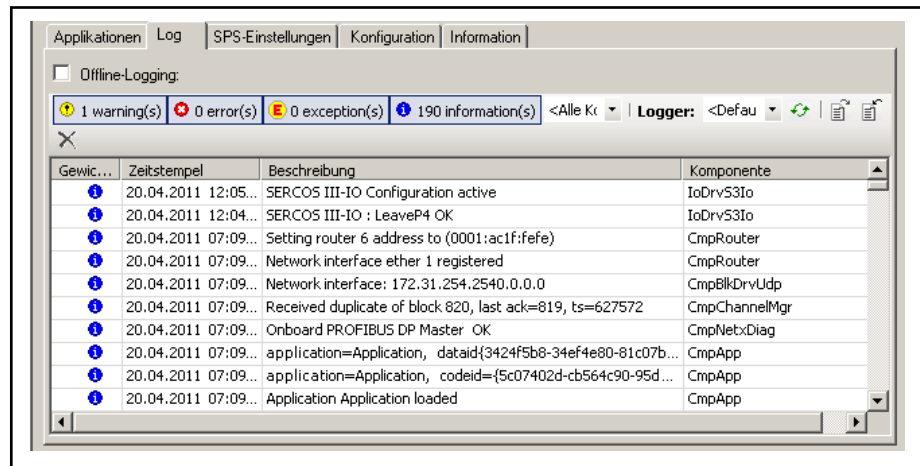


Abb. 8-4: Geräte-Editor, Log



Das Logbuch muss über **Extras ► Optionen...** im Dialog **IL2G ► Allgemeine Einstellungen** freigeschaltet werden.

8.5 Gerätediagnose der Standardsteuerung

IndraMotion MTX

Der Dialog "Gerätediagnose" muss über **Diagnose ► Gerätediagnose** aktiviert werden und gibt einen Überblick über alle Diagnosemeldungen der Steuerung und der angeschlossenen Geräte. Dabei werden die Diagnosemeldungen automatisch so sortiert, dass die neusten Meldungen in der Liste oben stehen. Alle Meldungen der Standard-SPS werden im "Fehler-/Diagnosespeicher" ebenfalls abgelegt.

Die Logbucheinträge werden remanent auf der Steuerung gespeichert und stehen somit auch nach Aus- und wieder Einschalten der Steuerung noch zur Verfügung. Der Speicher der Gerätediagnose ist auf 1000 Einträge begrenzt.

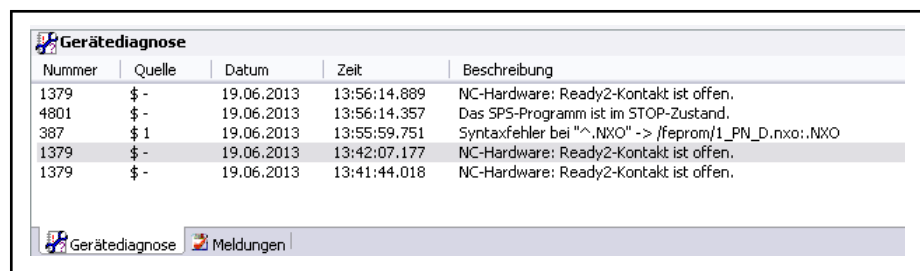


Abb. 8-5: Beispiel für die Darstellung der MTX-Gerätediagnose

Dieser Dialog kann nur online angezeigt werden.

8.6 Diagnose in der Standard-SPS

Das Sichere Steuerungssystem SafeLogic bietet den Zugriff auf Diagnoseinformationen der sicheren Steuerung und der sicheren I/O-Daten in der SPS der Standard-Steuerung. Hierdurch lassen sich für Diagnosen benötigte Daten leicht auslesen und im SPS-Programm verwenden.

Als Einstiegspunkt dient die SPS-Datenstruktur `SafetyData`. Diese globale Variable wird beim Übersetzen der Standard-Steuerung automatisch generiert, wenn sich unterhalb der Hauptsteuerung eine SafeLogic befindet.

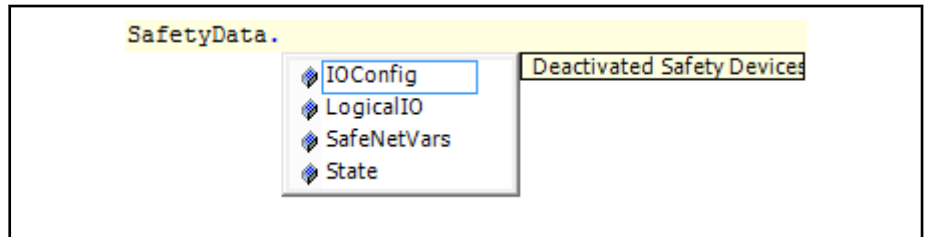


Abb. 8-6: Oberste Ebene der globalen Variable `SafetyData`.

`SafetyData` enthält die folgenden Einträge:

- `SafetyFM` - Statusinformationen der Safety-Steuerung:

Dieser Eintrag enthält allgemeine Diagnoseinformationen der SafeLogic-Steuerung

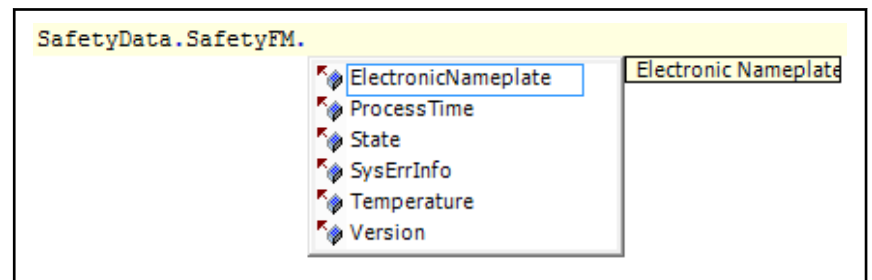


Abb. 8-7: Unterpunkte des Eintrags `SafetyData.SafetyFM`

- `LogicalIO` - Zugriff auf die sicheren Verbindungen:

Dieser Eintrag ermöglicht den Zugriff auf die sicheren Verbindungen. Er bildet die Geräte unterhalb des Knotens "Logische I/Os" der Safety-Steuerung hierarchisch ab. Neben dem Zugriff auf die übertragenen Variablen stehen zusätzlich Verbindungsinformationen zur Verfügung.

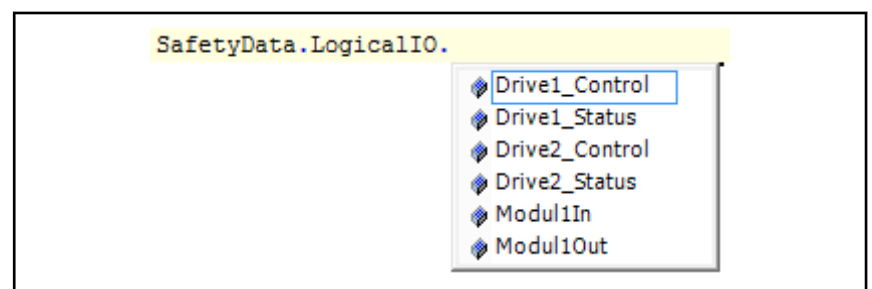


Abb. 8-8: Beispiel für die Logischen I/Os unterhalb des Eintrags `SafetyData.LogicalIO`

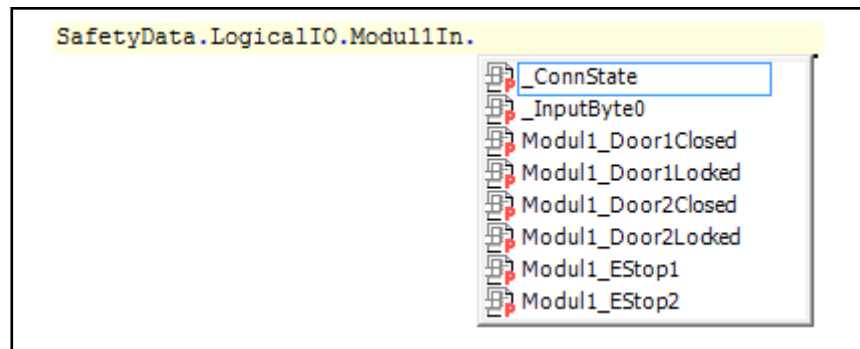


Abb. 8-9: Beispiel für einen Logischen I/O-Knoten unterhalb des Eintrags *SafetyData.LogicalIO*

- **SafeNetVars** - Zugriff auf die sicheren Netzwerkvariablen:
Dieser Eintrag stellt alle der sicheren Steuerung bekannten sicheren Netzwerkvariablenlisten (siehe [Kap. 5.8 "Sichere Querkommunikation über Ethernet" auf Seite 84](#)) zur Verfügung. Bei Senderlisten ist jede konfigurierte Verbindung einzeln sichtbar. Neben dem Zugriff auf die übertragenen sicheren Variablen wird zusätzlich der Verbindungsstatus angezeigt.
- **IoConfig** - Deaktivierte sichere Teilnehmer:
Dieser Eintrag bildet die Funktionalität zum Einlernen deaktivierter sicherer Teilnehmer ab. Neben der Prüfsumme (CRC) der aktuell eingelesenen Konfiguration ist auch der Zugriff auf die Deaktivierungsbits möglich.

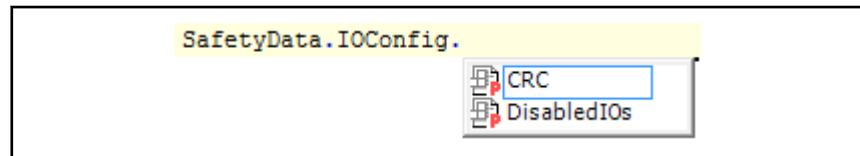


Abb. 8-10: Unterpunkte des Eintrags *SafetyData.IOConfig*

8.7 Funktionsbausteine "CSosOriginator" und "ProfisafeHost"

Sämtliche Fehlermeldungen im Bereich der Konfiguration werden an den DiagCode- bzw. DiagCodeExt-Ausgängen der Funktionsbausteine "CSosOriginator" bzw. "ProfisafeHost" ausgegeben.

Beispielaufwurf in der Applikation:

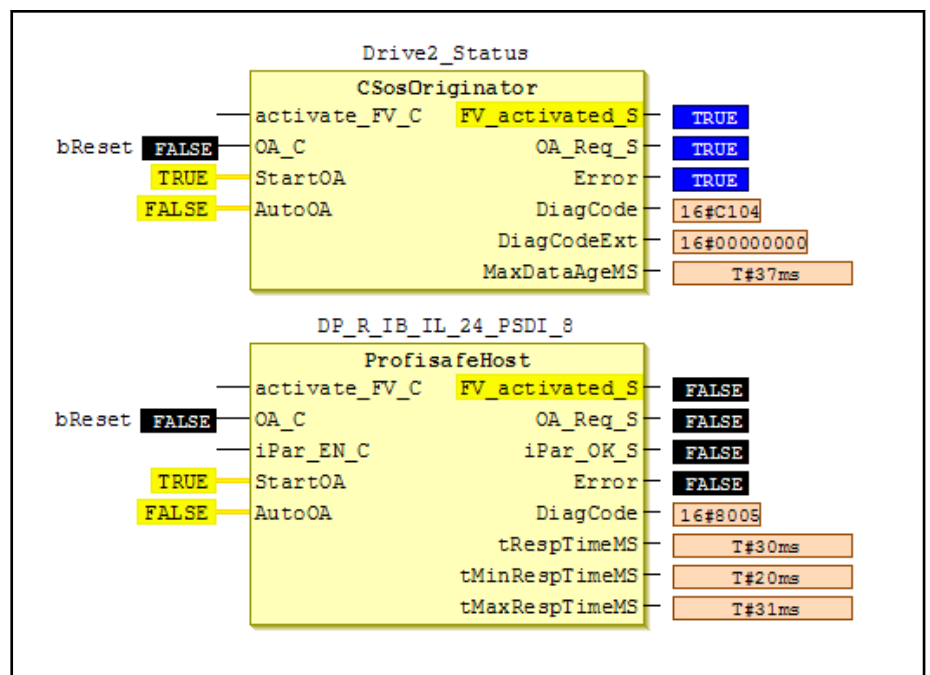


Abb. 8-11: Beispielaufzug des CSosOriginator- und des ProfisafeHost-Funktionsbausteins

DiagCode/DiagCodeExt

DiagCode	DiagCodeExt	Beschreibung
16#C104	0	Quittierung durch Bediener angefordert
16#8005	-	"Prepare Message" (Datenaustausch): Vorbereitung der nächsten Nachricht für das F-Device

Tab. 8-1: DiagCode/DiagCodeExt

9 Service und Support

Für Ihre schnelle und optimale Unterstützung verfügen wir über ein dichtes weltweites Servicenetz. Unsere Experten stehen Ihnen mit Rat und Tat zur Seite. Sie erreichen uns täglich **rund um die Uhr – auch an Wochenenden und Feiertagen**.

Service Deutschland Unser technologieorientiertes Competence Center in Lohr deckt alle Belange rund um den Service für elektrische Antriebe und Steuerungen ab.

Sie erreichen unsere **Service-Hotline** und unseren **Service-Helpdesk** unter:

Telefon: **+49 9352 40 5060**
Fax: **+49 9352 18 4941**
E-Mail: service.svc@boschrexroth.de
Internet: <http://www.boschrexroth.com>

Auf unseren Internetseiten finden Sie ergänzende Hinweise zu Service, Reparatur (z. B. Anlieferadressen) und Training.

Service weltweit Außerhalb Deutschlands nehmen Sie bitte zuerst Kontakt mit Ihrem Ansprechpartner auf. Die Hotline-Rufnummern entnehmen Sie bitte den Vertriebsadressen im Internet.

Vorbereitung der Informationen Wir können Ihnen schnell und effizient helfen, wenn Sie folgende Informationen bereithalten:

- Eine detaillierte Beschreibung der Störung und der Umstände
- Angaben auf dem Typenschild der betreffenden Produkte, insbesondere Typenschlüssel und Seriennummern
- Ihre Kontaktdaten (Telefon-, Faxnummer und E-Mail-Adresse)

Index

A

Abkürzungen.....	8
Ablauf der Installation und Inbetriebnahme.....	104
Abnahme.....	115
Abnahmedokumentation.....	115
Adressvergabe/Namen.....	32
Anregungen.....	8
Anwahl der Funktion.....	69
Anwendung der sicheren Querkommunikation.....	85
Anwendung von CIP Safety on Sercos.....	81
Anwendung von PROFISafe.....	74

B

Beispielanwendung.....	32
Anforderungen.....	33
Aufbau und Verdrahtung.....	35
Bestimmen des erreichten PL-Wertes nach EN ISO 13849-1.....	40
Bestimmen des erreichten SIL nach EN 62061.....	40
Betrachtete Sicherheitskette.....	40
Ermitteln des erforderlichen Sicherheitsabstands.....	41
Komponenten.....	35
Parametrierung.....	37
Sicherheitsfunktion.....	34
Weitere Vorgehensweise.....	43
Benutzerverwaltung der SafeLogic.....	103
Benutzerverwaltung SafeLogic compact.....	103
Beschwerde.....	8
Bestimmung der erreichten Sicherheitsintegrität.....	28
Bestimmung der garantierten Abschaltzeit.....	28
Reaktionszeit.....	28
Überprüfung der geforderten Abschaltzeit.....	31
Bestimmungsgemäße Verwendung.....	9
Bezeichnungen und Abkürzungen.....	8
Bussysteme.....	57

D

Darstellung von Informationen.....	7
Datentypen.....	98
DCavg.....	51
Demontage.....	106
Diagnose in der Standard-SPS.....	123
Diagnose und Störungsbeseitigung.....	119
Diagnoseeigenschaften von PROFISafe.....	80
Diagnosekonzept.....	119
Dokumentation	
Änderungsverlauf.....	1
Dokumente, weiterführende.....	2

E

Einführung in die Sicherheitstechnik.....	13
---	----

Einsatzgebiete.....	46
EMV.....	111
Entsorgung.....	10
Entwicklungsoberfläche.....	89
Entwurf des sicherheitsbezogenen Steuerungssystems.....	23
Entwurf der Teilsysteme.....	26
Systementwurf.....	24
Topologie.....	23

F

Feedback.....	8
Fehlerreaktion am PROFISafe.....	79
Funktion anwählen.....	69
Funktionsbausteine.....	100
Funktionsbausteine CSosOriginator und ProfisafeHost.....	124
Funktionsblöcke.....	92
Funktionstest und Fehlersuche.....	110

G

Gebrauchsdauer TM.....	50, 51
Gerätediagnose der Standardsteuerung.....	122
Gerätediagnose des Safety-Funktionsmoduls.....	119
Gerätemontage des Safety-Funktionsmoduls.....	105
Gliederung der Dokumentation.....	6
Gültigkeit der Dokumentation.....	1

H

Helpdesk.....	127
Hotline.....	127

I

I/O-Module.....	94
I/Os.....	101
Inbetriebnahme.....	103
Inbetriebnahme der Applikation.....	112
Inbetriebnahme der Komponenten.....	110
Inbetriebnahme SafeLogic.....	112
Inbetriebnahme-Dokumentation.....	113
IndraControl S20 System.....	62
IndraWorks SafetyManager-Lizenz.....	94
Installation der Verdrahtung.....	109

K

Kategorie.....	50, 51
Konfiguration	
übertragen.....	117
Kritik.....	8
Kundenfeedback.....	8

L

Lizenz.....	89, 94
Logbuch der SafeLogic compact.....	120
Logbuch der Standardsteuerung.....	122
Logbuch des Safety-Funktionsmoduls.....	121
Logikprogrammierung.....	92, 98

M

Modifikationen.....	117
Modulmontage.....	106
Montage.....	106
Montage und Installation.....	105

O

Operatoren.....	99
-----------------	----

P

Performance Level PL.....	49, 51
PFDavg.....	51
PFH.....	51
Pinnen.....	113
Profibus-DP bzw. PROFINET mit PROFISafe....	73
Projektstruktur.....	96

R

Realisierbare Anforderungen.....	69
Rexroth Inline-System.....	59

S

SafeLogic.....	50, 94
SafeLogic compact.....	47
SafeLogic compact (SafeLogic Designer).....	89
Safety	
IndraWorks SafetyManager-Lizenz.....	94
Safety Pinnen.....	114
Safety-Abnahme	
Voraussetzungen und Nachweise.....	116
Schutzmaßnahmen.....	10
Sercos III mit CIP Safety on Sercos.....	81
Service-Hotline.....	127
Sichere Bussysteme.....	57
Sichere Datenübertragung.....	57
Sichere Kommunikation.....	52
Sichere Querkommunikation über Ethernet.....	84
Sicherer Datenfluss.....	99
Sicherheits-Integritätslevel SIL.....	49, 51
Sicherheitshinweise.....	7, 9, 10
Sicherheitssteuerungen.....	47
Sicherheits technikfunktionen.....	69
Sicherheitstechnische Kenngrößen.....	13
Bewertung nach IEC 61508.....	17
Bewertung nach IEC 62061.....	18
Bewertung nach ISO 13849-1.....	19
Spannungsversorgung.....	116
Standardansichten.....	89
Support.....	127
Systemaufbau.....	52

Systemlösung.....	55
Systemübersicht.....	45

T

Technische Inbetriebnahme SafeLogic compact.....	116
Technische Prüfung.....	117

U

Überprüfung der Installation.....	109
Umweltgerechtes Verhalten.....	10

V

Verdrahtung.....	116
Verifikation.....	114
Verwendete Symbole.....	8
Verwendungsbereiche.....	9
Vor dem Einschalten.....	110

W

Werkstofftrennung.....	10
------------------------	----

Z

Zertifizierung.....	69
Zielgruppen.....	1
Zuschalten der Versorgungsspannung.....	110

Notizen

Bosch Rexroth AG

Electric Drives and Controls

Postfach 13 57

97803 Lohr, Deutschland

Bgm.-Dr.-Nebel-Str. 2

97816 Lohr, Deutschland

Tel. +49 9352 18 0

Fax +49 9352 18 8400

www.boschrexroth.com/electrics



R911341697