OCTOGON

HANDBUCH

ESMD

PROGRAMMIERBARE SICHERHEITSSTEUERUNG SIL3 / PL e

Installationshandbuch



Dokument	Version	Datum	Gilt für
Installationshandbuch	V00x	10/2026	ESMD, Ausführungen 10 / 20 / 30, mit Erweiterungs- und Kommunikationsbaugruppen

Dieses Installationshandbuch beschreibt Sicherheit, Gerätetypen, sicherheitstechnische Merkmale, Anschluss und Installation, Reaktionszeiten, Inbetriebnahme, sicherheitstechnische Prüfung und Wartung der programmierbaren Sicherheitssteuerung ESMD und ihrer Erweiterungs- und Kommunikationsbaugruppen.

octogon GmbH · Roseggerstrasse 16 · 8700 Leoben · Austria · office@octogon.org

www.octogon.org

Inhalt

1 Wichtige Hinweise ... 3
1.1 Begriffsbestimmungen ... 3
1.2 Mit geltende Dokumente ... 4
1.3 Verwendete Abkürzungen ... 4
1.4 Gerät ... 5
2 Sicherheitshinweise ... 6
2.1 Bestimmungsgemäße Verwendung ... 6
2.2 Verwendung in Regionen mit UL/CSA-Anforderung ... 6
2.3 Allgemeine Sicherheitshinweise ... 7
2.4 Betrieb und Service ... 7
2.5 Transport/Einlagerung ... 7
3 Gerätetypen ... 8
3.1 Baugruppenübersicht ... 8
3.2 Gerätekenndaten ... 8
3.2.1 Basisbaugruppen ... 8
3.2.2 Zentrale Erweiterungsbaugruppen ... 10
3.2.3 Kommunikationsbaugruppen ... 11
3.3 Kennzeichnung ... 12
3.3.1 Typenschild ... 12
3.3.2 Lieferumfang ... 13
4 Sicherheitstechnische Merkmale ... 14
4.1 Allgemeiner Aufbau, sicherheitstechnische Architektur und Kenndaten ... 14
4.2 Sicherheitstechnische Kenndaten und Beschaltung für angeschlossene Sensorik ... 15
4.2.1 Digitale Sensoren ... 15
4.2.2 Analogsensoren ... 23
4.3 Sicherheitstechnische Kenndaten und Beschaltung der Ausgänge ... 25
4.3.1 Charakteristik der Ausgangselemente ... 25
4.3.2 Diagnosen im Abschaltkreis ... 26
4.3.3 Zulässige kapazitive und induktive Last an sicheren Ausgängen ... 27
4.3.4 Digitale Ausgänge ... 28
4.3.5 Digitale Ausgänge I/Os (EAAx) ... 30
5 Anschluss und Installation ... 38
5.1 Allgemeine Installationshinweise ... 38
5.2 Einbau und Montage der Baugruppe ... 38
5.3 Montage Rückwandbus ... 38
5.4 Montage der Baugruppen ... 39
5.4.1 Montage auf C-Schiene ... 39
5.4.2 Montage auf Rückwandbus ... 40
5.4.3 Installation I/O-Erweiterungen ... 41
5.5 Klemmenbelegung ... 42
5.5.1 Klemmenbelegung ESMD ... 42
5.5.2 Klemmenbelegung Erweiterungsbaugruppe ... 43
5.5.3 Klemmenbelegung Kommunikationsbaugruppen ... 43
5.6 Externe 24-VDC-Spannungsversorgung ... 44
5.7 Anschluss der Digitaleingänge ... 45
5.8 Anschluss Analogeingänge ... 45
6 Reaktionszeiten des ESMD ... 46
6.1 Reaktionszeiten im Standardbetrieb ... 46
6.2 Reaktionszeiten für FAST_CHANNEL ... 47
6.3 Reaktionszeiten für Fehlerdistanzüberwachung ... 47
6.4 Reaktionszeiten bei Verwendung der Erweiterungsbaugruppe ... 48
7 Inbetriebnahme ... 50
7.1 Vorgehensweise ... 50
7.2 Einschaltsequenzen ... 50
7.3 Reset-Verhalten ... 50
7.3.1 Resettypen und auslösendes Element ... 50
7.3.2 Reset-Timing ... 51
7.3.3 Reset-Funktion ... 51
7.4 LED-Anzeige ... 54
7.5 Parametrierung ... 54
7.6 Funktionsprüfung ... 54

7.7 Validierung....54
8 Sicherheitstechnische Prüfung....55
9 Wartung....55
9.1 Modifikation / Umgang mit Änderungen am Gerät....55
9.2 Tausch einer Baugruppe....55
9.3 Wartungsintervalle....55
10 Technische Daten....56
10.1 Umweltbedingungen....56
10.2 Sicherheitstechnische Kenndaten....56
10.3 Abmessungen....56
10.4 Anschlussbeispiel....57
11 Schaltertypen....58
12 Hinweise für Entwurf, Programmieren, Validieren und Testen von sicherheitstechnischen Applikationen. 3
12.1 Risikobetrachtung....64
12.2 Erforderliche technische Unterlagen....65
12.3 Erforderliche Schritte zu Entwurf, Realisierung und Prüfung....66
12.3.1 Phasen des V-Modells....67
12.3.2 Spezifikation der Sicherheitsanforderungen (Gliederungsschema)....67
12.3.3 Spezifikation des funktionalen Sicherheitssystems....69
12.3.4 Softwarespezifikation....71
12.3.5 Hardwarespezifikation....72
12.3.6 Hard- und Softwaredesign....74
12.3.7 Prüfung des HW-Designs....74
12.3.8 Verifikation Software (Programm) und Parameter....77
12.3.9 Durchführung der Systemtests / FIT (fault injection test)....80
Anhang A Einstufung der Schaltertypen....81

1 Wichtige Hinweise

Gültigkeit

Installationsanleitung für die Geräte ESMD, ESMD Ausführung 20 (FSoE) und ESMD Ausführung 30 (PROFIsafe) der Baureihe ESMD und deren Erweiterungsbaugruppen (Erweiterungsbaugruppe, Kommunikationsbaugruppen).

Die Ausführungen 20 und 30 sind Optionen für ESMD:

- Ausführung 20: Standard-Feldbus und Safety-Protokoll FSoE
- Ausführung 30: Standard-Feldbus und Safety-Protokoll PROFISAFE

Hinweis Die deutsche Version ist die Originalausführung der Installationsanleitung.

Gültig ab FW-Release 2.0.2.46. Technische Änderungen vorbehalten.

Definition der einzelnen Zielgruppen

Zielgruppe	Personal
Projektanten sicherer Antriebssysteme	Ingenieure und Techniker
Montage, Elektroinstallation, Wartung und Gerätetausch	Betriebselektriker und Servicetechniker
Inbetriebnahme, Bedienung und Konfiguration	Techniker und Ingenieure

1.1 Begriffsbestimmungen

Die Bezeichnung ESMD wird als Oberbegriff für alle Derivate der Produktlinie gebraucht. Wird in der Beschreibung auf ein bestimmtes Derivat Bezug genommen, so wird jeweils die vollständige Bezeichnung verwendet.

Der nachfolgend verwendete Begriff „sicher“ bezieht sich jeweils auf die Einordnung als sichere Funktion zur Anwendung bis PL e nach EN ISO 13849-1 bzw. SIL3 nach IEC 61508:2010.

Die Systemsoftware (Programmiersoftware) dient zur Konfiguration und Programmierung der Baugruppen.

Intern sind die Baugruppen der Baureihe aus zwei unabhängigen Verarbeitungseinheiten aufgebaut. Diese werden nachfolgend auch als System A und System B bezeichnet.

1.2 Mit geltende Dokumente

Beschreibung	Referenz
Konfiguration der Baugruppe für Standalone-Anwendungen ohne Feldbusanschaltung mit der Programmiersoftware	Programmierhandbuch der Programmiersoftware (System-CD)
Validierungsreport der implementierten Parametrierung und des PLC-Programms	Sicherheitstechnische Prüfung mit Abnahmeprotokoll
Abnahme für allgemeine sicherheitstechnische Applikationen	Zertifikat zur Typprüfung für Sicherheitssteuerung nach Maschinenrichtlinie 2006/42/EG für die Produktbaugruppen ESMD, ESMD Ausführung 20 und 30, Erweiterungsbaugruppe

Hinweis

- Lesen Sie Handbücher sorgfältig durch, bevor Sie mit der Installation und der Inbetriebnahme der Baugruppe beginnen.
- Die Beachtung der Dokumentation ist die Voraussetzung für einen störungsfreien Betrieb und die Erfüllung eventueller Garantieansprüche.

1.3 Verwendete Abkürzungen

Abkürzung	Bedeutung
AC	Wechselspannung
AWL	Anweisungsliste
BG	Berufsgenossenschaft
CLK	Clock (Takt)
CPU	Central Processing Unit
DC	Gleichspannung
I1..I14	Digital Input (Digitaler Eingang)
DIN	Deutsches Institut für Normung
DO	Digital Output (Digitaler Ausgang)
EMU	Emergency Monitoring Unit
EMV	Elektromagnetische Verträglichkeit
ELC	Emergency Limit Control
EN	Europäische Norm
HISIDE	Nach Plus schaltender Ausgang mit 24 VDC Nominalpegel
IP20	Schutzart für Gehäuse
ISO	International Organisation for Standardisation
LED	Light Emitting Diode
LOSIDE	Nach Bezugspotential schaltender Ausgang
OLC	Operational Limit Control
PAA	Prozessabbild der Ausgänge
PAE	Prozessabbild der Eingänge
SMMC	Safe Master-Master Communication
P1, P2	Pulsausgänge
PLC	Programmable Logic Controller
POR	Power on Reset
PSC	Position Supervision Control
SELV	Safety Extra Low Voltage
SSI	Synchron Serielles Interface
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik e. V.
SDDC	Safe Device-Device Communication
DOx.y (1)	Hilfsausgang
G. P.	Allgemeine Verwendung
(1)	Module address x = 0 ... 2, Channel address y = 1 ... 40

1.4 Gerät

Merkmal	Ausführung
Bauart	Programmierbare Sicherheitssteuerung SIL3 / PL e (Grundgerät), auf Normschiene, IP20
Ausführungen	10 Standard · 20 mit FSoE, ETHERCAT integriert · 30 mit PROFISAFE, PROFINET integriert
Zubehör	Erweiterungsbaugruppe (I/O); Kommunikationsbaugruppen CAN, Profibus-DP, Profinet, CANopen, EtherCAT; Programmiersoftware; Programmiereinheit; Rückwandbusverbinder (Standard- und Unterbrecherausführung)
Typbezeichnung des Herstellers	SCU-DR

2 Sicherheitshinweise

2.1 Bestimmungsgemäße Verwendung

Die Geräte der Baureihe ESMD sind programmierbare Sicherheitssteuerungen zur Herstellung von Sicherheitsabschaltungen und -funktionen. Die Geräte sind bestimmt zum Einsatz

- in NOT-AUS-Einrichtungen,
- als Sicherheitsbauteil im Sinne der EG-Maschinenrichtlinie 2006/42/EG,
- als PES für zur Risikoreduzierung im Sinne der IEC 61508,
- in Sicherheitsstromkreisen nach EN 60204-1 u. EN 60204-32,
- als PES für funktionale Sicherheit im Sinne der EN 62061,
- als SRP/CS im Sinne der EN ISO 13849-1,
- als Gerät zur Herstellung der Sicherheitsfunktionen nach EN 61800-5-2,
- als Logikeinheit zur Signalwandlung und -verarbeitung in Zweihandschaltung nach EN 574.

Die Geräte der Baureihe ESMD inkl. Erweiterungsbaugruppe sind Sicherheitsbauteile gemäß Anhang IV EG-Maschinenrichtlinie 2006/42/EG. Sie wurden entwickelt, konstruiert und gefertigt in Übereinstimmung mit der o. g. Richtlinie sowie der EU-Richtlinie EU-EMV-Richtlinie 2014/30/EU.

2.2 Verwendung in Regionen mit UL/CSA-Anforderung

Bei Baugruppen der Baureihe, die keine UL/CSA-Zulassung haben, kann unter Beachtung folgender Randbedingungen in den USA und Kanada eingesetzt werden:

- die Schaltspannung der Ausgangsrelais ist auf max. 24 V zu begrenzen.
- die Spannungsversorgung der Baugruppen und deren Ein- und Ausgänge muss mit einem Netzteil erfolgen, welches der Anforderung CLASS 2 gemäß der UL 1310 entspricht.

Unter diesen Voraussetzungen ist eine UL/CSA-Zulassung nicht notwendig und die Baureihe kann in Schaltanlagen gemäß der UL 61010 eingesetzt werden.

2.3 Allgemeine Sicherheitshinweise

Sicherheitshinweis

- Zur Vermeidung von Personen- und Sachschäden darf nur qualifiziertes Personal an dem Gerät arbeiten. Qualifiziertes Personal ist Personal, das eine elektrotechnische Ausbildung besitzt und mit den gültigen Regeln und Normen der Elektrotechnik vertraut ist.
- Die qualifizierte Person muss sich mit der Betriebsanleitung vertraut machen (vgl. IEC 364, DIN VDE 0100).
- Die qualifizierte Person muss mindestens vertiefte Kenntnis der nationalen Unfallverhütungsvorschriften besitzen.
- Die Verwendung der Geräte ist auf deren bestimmungsgemäßen Gebrauch gemäß vorstehender Auflistung einzuschränken. Die Werte der im Abschnitt 3.2 Gerätekenndaten gelisteten Daten sind weiter zu beachten.
- Der Inhalt dieser Installationsanleitung ist auf die Grundfunktion der Geräte bzw. deren Installation beschränkt. Die Programmierung und Neuparametrierung der Geräte wird im Programmierhandbuch der Programmiersoftware weitergehend beschrieben. Deren genaue Kenntnis und Verständnis ist zwingende Voraussetzung für eine Neuinstallation bzw. Modifikation der Gerätefunktion oder Geräteparameter.
- Die Inbetriebnahme (d. h. die Aufnahme des bestimmungsgemäßen Betriebes) ist nur bei Einhaltung der EMV-Richtlinie erlaubt. Es werden die EMV-Prüfvorschriften EN 55011:2009 + A2:2010 und EN 61000-6-2:2005 zugrunde gelegt.
- Für Lagerung und Transport sind die Bedingungen nach EN 60068-2-6 in Bezug auf die unter Techn. Kenndaten genannten Werte einzuhalten.
- Die Verdrahtungs- und Anschlusshinweise aus dem Kapitel Anschluss und Installation sind zwingend zu beachten.
- Es sind die geltenden VDE-Vorschriften sowie weitere besondere Sicherheitsvorschriften für die gegenständliche Applikation zu beachten.
- Die konfigurierten Überwachungsfunktionen sowie deren Parameter und Verknüpfungen sind über einen Validierungsreport nachzuweisen.
- Die Implementierung der Baugruppe ist mit den Forderungen der zuständigen Abnahmestelle (z. B. TÜV oder BG) abzustimmen.
- Niemals beschädigte Produkte installieren oder in Betrieb nehmen. Beschädigungen bitte umgehend beim Transportunternehmen reklamieren.
- Niemals das Gehäuse öffnen und/oder eigenmächtig Umbauten vornehmen.
- Ein- und Ausgänge für Standardfunktionen bzw. die per Kommunikationsbaugruppen übertragenen Digital- und Analogdaten dürfen nicht für sicherheitsgerichtete Anwendungen verwendet werden.

WARNUNG **Eine Verwendung unserer Geräte entgegen den hier aufgeführten Regeln und Bedingungen kann Verletzungen oder Tod von Personen sowie Schäden an angeschlossenen Geräten und Maschinen zur Folge haben!**

Ebenso führt dies zum Verlust jeglicher Garantie- oder Schadensersatzansprüche gegen den Hersteller.

2.4 Betrieb und Service

Vor dem Ein- und Ausbau der Baugruppe oder dem Trennen von Signalleitungen ist die Baugruppe spannungsfrei zu schalten. Dazu sind sämtliche spannungsführenden Zuleitungen zum Gerät abzuschalten und auf Spannungsfreiheit zu prüfen.

Während des Ein- und Ausbaus der Baugruppe sind durch entsprechende Maßnahmen elektrostatische Entladungen auf die nach außen geführten Klemmen- und Steckverbindungen zu vermeiden. Ein Kontakt mit diesen Klemmen sollte dazu auf ein Minimum beschränkt bleiben und vorher und währenddessen sollte eine Erdung durch z. B. Erdungsarmband erfolgen.

2.5 Transport/Einlagerung

Die Hinweise für Transport, Lagerung und sachgemäße Handhabung sind zu beachten. Die klimatischen Vorgaben sind gemäß Kap. Technische Daten einzuhalten.

3 Gerätetypen

Die Baureihe ESMD besteht aus

- den Basisgeräten ESMD
- den Erweiterungsbaugruppen
- den Kommunikationsbaugruppen mit Standard-Feldbus
- der Programmiereinheit
- den integrierten Kommunikationsbaugruppen mit sicherem Feldbus ESMD Ausführung 20 und 30

Basisgeräte

Bei der Baureihe ESMD handelt es sich um eine kompakte Sicherheitssteuerung. Das Gerät ist frei programmierbar zur sicheren Verarbeitung sowohl von NOT-AUS-Taster, Zweihandbedienung, Lichtgitter, Betriebsartenwahlschalter etc. als auch von antriebsbezogenen Sicherheitsfunktionen. Für eine Vielzahl von Eingabegeräten stehen für die sicherheitsrelevante Signalvorverarbeitung vorkonfigurierte Bausteine zur Verfügung. Gleiches gilt auch für Sicherheitsfunktionen zur Antriebsüberwachung. Details sind dem Programmierhandbuch zu entnehmen.

Das Gerät verfügt in der Basisausführung über 14 sichere Eingänge und bis zu 5 sichere Abschaltkanäle.

Erweiterungsbaugruppen

Zentrale oder dezentrale I/O-Erweiterung für die Baureihe ESMD. Es können maximal 2 Erweiterungsbaugruppen verwendet werden.

Kommunikationsbaugruppen und integrierte Schnittstelle

Das Kommunikationsinterface verfügt über eine bidirektionale Datenübertragung von und zu einer übergeordneten Steuerung mittels Standard-Feldbus oder sicherem Standard-Feldbus.

3.1 Baugruppenübersicht

Bezeichnung	Basisbaugruppe ESMD	Erweiterungsbaugruppe	Kommunikationsbaugruppe
Max. Anzahl Erweiterungsbaugruppen	2*	–	–
Sichere digitale Eingänge	14	12	–
Sichere digitale I/Os	–	10	–
Sichere analoge Eingänge	2	–	–
Relaisausgänge	6	–	–
Hilfsausgänge	2	–	–
Pulsausgänge	2	–	–
Integriertes Kommunikationsinterface	Optional (Ausführung 30 und 20): Profinet-PROFIsafe, FSoE	–	–
Erw. Kommunikationsinterface	Optional (Kommunikationsbaugruppe): CAN 2.0, Profibus, Profinet, CANopen, EtherCAT	–	CAN 2.0, Profibus, Profinet, CANopen, EtherCAT
Technische Daten	Siehe technische Kenndaten der jeweiligen Baugruppe		

3.2 Gerätekenndaten

3.2.1 Basisbaugruppen

ESMD

Ausführung der Baugruppe mit folgender Peripherie:

Anzahl	Peripherie
14	Digitale Eingänge
2	Pulsausgänge
6	Relaisausgänge
2	Hilfsausgänge
2	Analogeingänge
1	Diagnose- und Konfigurationsschnittstelle
1	Funktionstaster
1	7-Segmentanzeige
1	Status-LED
14	Status-LEDs für Eingänge
2	Status-LEDs für Pulsausgänge
2	Status-LEDs für Relaisausgänge
6	Status-LEDs für Ausgänge
1	Optional: Kommunikationsinterface (Kommunikationsbaugruppe)

Eigenschaften der Baugruppe:

- Erweiterbar auf: max. 38 sichere digitale Eingänge + max. 2 sichere digitale Ausgänge; max. 20 sichere digitale I/Os; max. 12 sichere Relaisausgänge + max. 6 Hilfsausgänge
- Logikverarbeitung bis PL e nach EN ISO 13849-1 bzw. SIL 3 nach IEC 61508
- Freiprogrammierbare Kleinsteuerung für bis zu 800 AWL-Anweisungen
- Funktionsplanorientierte Programmierung
- Pulsausgänge zur Querschlusserkennung digitaler Eingangssignale
- Sicherheitsfunktion Externe Kontaktüberwachung angeschlossener Schaltgeräte
- Überwachte Relaisausgänge für sicherheitsrelevante Funktionen
- Externe Kontaktüberwachung angeschlossener Schaltgeräte (EMU)
- Parameterverwaltung für Erweiterungsbaugruppen im Grundgerät
- Vollständige geschwindigkeits- und positionsbezogene Sicherheitsfunktionen zur Antriebsüberwachung gemäß IEC 61800-5-2 in Firmware integriert; räumliche Funktionen für sichere Geschwindigkeits- und Bereichsüberwachungen möglich
- Umfangreiche Diagnosefunktionen integriert
- Codierte Statusanzeige über frontseitige 7-Segment-Anzeige und Status-LEDs
- Multifunktionstaster (Quit, Start, Reset) frontseitig bedienbar
- CAN-Kommunikation in Verbindung mit der Kommunikationsbaugruppe für Diagnose über Rückwandbus
- Montage auf Hutschiene

Technische Kenndaten ESMD

Merkmal	Wert
Sicherheitstechnische Kenndaten	
PL nach EN ISO 13849-1	PL e
PFH / Architektur	12,6 FIT / Kat 4; zzgl. 1-kanalig pro Rel 20 FIT (max. 4), 2-kanalig pro Rel 1,0 FIT (max. 2)
SIL nach IEC 61508	SIL 3
Proof-Test-Intervall	20 Jahre = max. Einsatzdauer
Allgemeine Daten	
Max. Anzahl Erweiterungsbaugruppen	2
Schnittstelle f. Erweiterungsbaugruppen	T-Busverbinder, in Hutschiene steckbar
Anzahl sichere digitale Eingänge	14 (OSSD fähig)
Anzahl Relais Ausgänge	6
Anzahl sichere analoge Eingänge	2
Anzahl Hilfsausgänge	2
Anzahl Pulsausgänge (Taktausgänge)	2
Anschlussart	Steckklemmen mit Feder- oder Schraubanschluss
Elektrische Daten	
Versorgungsspannung (Toleranz)	24 VDC; 2 A (–15 %, +20 %)
Sicherung X11.1	min. 30 VDC; max. 3,15 A
Max. Leistungsaufnahme (Logik)	2,4 W

Merkmal	Wert
Nenndaten digitale Eingänge	24 VDC; 20 mA, Typ 1 nach EN 61131-2
Nenndaten digitale Ausgänge – Hilfsausgänge	24 VDC; 250 mA
Nenndaten Pulsausgänge	24 VDC; 250 mA
Nenndaten Relais – Schließer	DC13: 24 VDC; 2 A · AC15: 230 VAC; 2 A
Nenndaten Relais – Öffner (Rücklesekontakt)	DC13: 24 VDC; 2 A
Nenndaten sichere analoge Eingänge	ESMD: 4 ... 20 mA
Umweltdaten	
Temperatur	0 °C ... +50 °C Betrieb; –25 °C ... +70 °C Lagerung, Transport
Schutzklasse	IP 20
Klimaklasse	3k3 nach DIN 60 721-3
Min-, Maximal relative Luftfeuchte (keine Betauung)	5 % – 85 %
EMV	EN 61000-6-2, EN 61000-6-4, EN 61000-6-7, EN 61800-3, EN 61326-3, EN 62061
Betriebsmitteleinsatz	2000 m
Überspannungskategorie	III
Verschmutzungsgrad	2
Mechanische Daten	
Größe (H × T × B [mm])	ESMD = 100 × 115 × 90; ESMD Ausführung 20/30 = 100 × 115 × 115
Gewicht (g)	ESMD = 500; ESMD Ausführung 20/30 = 600
Befestigung	Auf Normschiene aufschnappbar
Anzahl T-Bus	ESMD: 4; ESMD Ausführung 20 und 30: 5
Min. Anschlussquerschnitt / AWG	0,2 mm^2 / 24
Max. Anschlussquerschnitt / AWG	2,5 mm^2 / 12

3.2.2 Zentrale Erweiterungsbaugruppen

Erweiterungsbaugruppe

Ausführung der Baugruppe mit folgender Peripherie:

Anzahl	Peripherie
12	Digitale Eingänge
10	Digitale I/Os
2	Pulsausgänge
2	Hilfsausgänge
12	Status-LEDs für Eingänge
10	Status-LEDs für I/O

Eigenschaften der Baugruppe:

- Pulsausgänge zur Querschlusserkennung digitaler Eingangssignale
- Externe Kontaktüberwachung angeschlossener Schaltgeräte (EMU)
- Umfangreiche Diagnosefunktionen integriert
- Montage auf Hutschiene
- Erweiterungsbaugruppe – mit gesamt 10 I/Os

Technische Kenndaten Erweiterungsbaugruppe

Merkmal	Wert
Sicherheitstechnische Kenndaten	
PL nach EN ISO 13849-1	PL e
PFH / Architektur	9,2 FIT / Kat 4 1)
SIL nach IEC 61508	SIL 3
Proof-Test-Intervall	20 Jahre = max. Einsatzdauer
MTTFd	213 Jahre
Allgemeine Daten	
Max. Anzahl Erweiterungsbaugruppen	–
Schnittstelle f. Erweiterungsbaugruppen	T-Busverbinder, in Hutschiene steckbar
Anzahl sichere digitale Eingänge	12 (OSSD fähig)

Merkmal	Wert
Anzahl sichere digitale Ausgänge	–
Anzahl sichere digitale I/O	10
Anzahl sichere Analog-In	–
Anzahl Hilfsausgänge	2
Anzahl Pulsausgänge (Taktausgänge)	2
Anschlussart	Steckklemmen mit Feder- oder Schraubanschluss
Elektrische Daten	
Sicherung X11.1	min. 30 VDC; max. 3,15 A
Max. Leistungsaufnahme (Logik)	2,4 W
Nenndaten digitale Eingänge	24 VDC; 20 mA, Typ 1 nach EN 61131-2
Nenndaten digitale Ausgänge – Hilfsausgänge	24 VDC; 250 mA
Nenndaten digitale Ausgänge – Pulsausgänge	24 VDC; 250 mA
Nenndaten digitale Ausgänge – digitale I/O	24 VDC; 250 mA
Nenndaten Relais – Schließer	DC13: 24 VDC; 2 A · AC15: 230 VAC; 2 A
Nenndaten Relais – Öffner (Rücklesekontakt)	DC13: 24 VDC; 2 A
Nenndaten analoge Eingänge	–
Umweltdaten	
Temperatur	0 °C ... +50 °C Betrieb; –25 °C ... +70 °C Lagerung, Transport
Schutzklasse	IP 20
Klimaklasse	3k3 nach DIN 60 721-3
Min-, Maximal relative Luftfeuchte (keine Betauung)	5 % – 85 %
EMV	EN 61000-6-2, EN 61000-6-4, EN 61000-6-7, EN 61800-3, EN 61326-3, EN 62061
Betriebsmitteleinsatz	2000 m
Überspannungskategorie	III
Verschmutzungsgrad	2
Mechanische Daten	
Größe (H × T × B [mm])	100 × 115 × 45
Gewicht (g)	300
Befestigung	Auf Normschiene aufschnappbar
Anzahl T-Bus	2
Min. Anschlussquerschnitt / AWG	0,2 mm² / 24
Max. Anschlussquerschnitt / AWG	2,5 mm² / 12

1) Wert gilt nur für Erweiterungsbaugruppe. Für eine Gesamtbewertung nach EN ISO 13849-1 ist eine Serienschaltung mit dem jeweiligen Basisgerät anzusetzen => PFH Logik = PFH Basis + PFH Erweiterung

3.2.3 Kommunikationsbaugruppen

3.2.3.1 Kommunikationsbaugruppen (Standard-Feldbus)

Ausführungen der Baugruppen mit folgender Peripherie:

- 1 Feldbusschnittstelle: Kommunikationsbaugruppe CAN 2.0 oder Profibus oder Profinet oder CANopen oder EtherCAT
- 1 Rückwandbusschnittstelle
- 1 Status-LED für den Betriebszustand
- 1 Status-LED CAN-Kommunikation

Eigenschaften der Baugruppe:

- Kommunikationsmodul CAN oder Profibus oder Profinet oder CANopen oder EtherCAT
- 2 × 8 Byte PAA mit freier Zuordnung
- 32 Bit PAE
- Genauere Informationen bitte den Installationshandbüchern der jeweiligen Feldbusbaugruppen entnehmen.

Technische Kenndaten Kommunikationsbaugruppe

Merkmal	Wert
Sicherheitstechnische Kenndaten	
PL nach EN ISO 13849-1	n. a.
PFH / Architektur	n. a.

Merkmal	Wert
SIL nach IEC 61508	n. a.
Proof-Test-Intervall	n. a.
Allgemeine Daten	
Feldbusinterface	1
Anschlussart	Standard nach Feldbustyp
Max. Größe PAA	2 × 64 Bit
Max. Größe PAE	32 Bit
Typ. Updatezeit für Daten	16 ms
Elektrische Daten	
Leistungsaufnahme	Max. 2,4 W
Nenndaten Feldbus	Standard nach Feldbustyp
Umweltdaten	
Temperatur	0 °C ... +50 °C Betrieb; –25 °C ... +70 °C Lagerung, Transport
Schutzklasse	IP 20
Klimaklasse	3k3 nach DIN 60 721-3
Min-, Maximal relative Luftfeuchte (keine Betauung)	5 % – 85 %
EMV	EN 61000-6-2, EN 61000-6-4, EN 61000-6-7, EN 61800-3, EN 61326-3, EN 62061
Betriebsmitteleinsatz	2000 m
Überspannungskategorie	III
Verschmutzungsgrad	2
Mechanische Daten	
Größe (H × T × B [mm])	100 × 115 × 22,5
Gewicht (g)	110
Befestigung	Auf Normschiene aufschnappbar

3.2.3.2 ESMD Ausführung 20 / 30 (integrierter sicherer Feldbus)

Ausführungen der Baugruppen mit folgender Peripherie:

- 1 Feldbusschnittstelle: ESMD Ausführung 30 PROFISAFE über Profinet oder ESMD Ausführung 20 FSoE FailSafe over EtherCAT
- 1 Status-LED für den Betriebszustand
- 1 Status-LED interne SPI-Kommunikation
- 1 Status-LED Feldbus

Eigenschaften der Baugruppe:

- Kommunikationsmodul PROFISAFE über PROFINET oder FSoE FailSafe over EtherCAT
- Genauere Informationen bitte den Installationshandbüchern der jeweiligen Feldbusbaugruppen entnehmen.

Hinweis **Muss bei der Bestellung der Basisbaugruppe mit angegeben werden!**

3.3 Kennzeichnung

Das Typenschild ist auf der linken Seitenwand der Baugruppe angebracht und enthält folgende Informationen:

3.3.1 Typenschild

- Typenbezeichnung
- Artikelnummer
- Seriennummer
- Hardware Release Kennzeichnung
- Software Release Kennzeichnung
- Sicherheitskategorie
- Eigenschaften der Eingänge
- Eigenschaften der Ausgänge
- Herstellungsdatum (KW/Jahr)

3.3.2 Lieferumfang

Im Lieferumfang enthalten ist:

- Baugruppe: Stecker für alle Signalklemmen ohne Geberanschluss

Nicht im Lieferumfang enthalten sind:

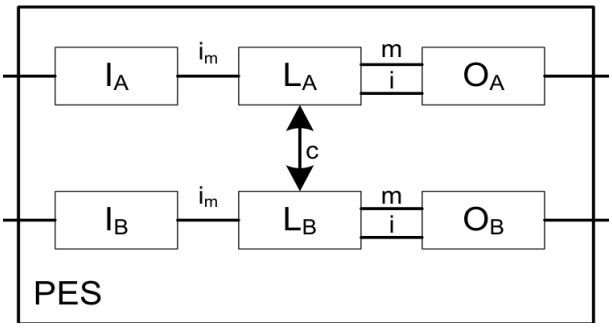
- Konfigurationssoftware-CD der Programmiersoftware mit Installationshandbuch, Programmierhandbuch und Treiber für Programmieradapter
- Programmieradapter (Programmiereinheit)
- Lizenzkey (USB-Dongle) für die Programmiersoftware
- System-CD mit Handbüchern
- Rückwandbusstecker (Erweiterungsbaugruppe und Verwendung Kommunikationsschnittstellen)

4 Sicherheitstechnische Merkmale

4.1 Allgemeiner Aufbau, sicherheitstechnische Architektur und Kenndaten

Der innere Aufbau der Baureihe besteht aus zwei getrennten Kanälen mit gegenseitigem Ergebnisvergleich. In jedem der beiden Kanäle werden hochwertige Diagnosen zur Fehlererkennung ausgeführt.

Der Aufbau entspricht in Architektur und Funktionsweise der Kategorie 4 der EN ISO 13849-1.



Interner Aufbau (PES)

Die Gesamtarchitektur zeigt damit folgenden Aufbau:



Doppeltes Einlesen jedes Eingangs und Diagnose durch Quervergleich

Die spezifischen sicherheitstechnischen Kenndaten der jeweiligen Baugruppen sind den techn. Kenndaten aus Kapitel 3 zu entnehmen.

Für die sicherheitstechnische Beurteilung von Gesamtsystemen können für das Teilsystem PES die im Kapitel 3 angegebenen Kenndaten angesetzt werden (z. B. PL e und PFH-Wert nach Tabelle für Nachweis gemäß EN ISO 13849-1).

Kenndaten

Merkmal	Wert
Max. erreichbare Sicherheitsklasse	SIL 3 gemäß IEC 61508; Kategorie 4 gemäß EN ISO 13849-1; Performance-Level e gemäß EN ISO 13849-1
Systemstruktur	2-kanalig mit Diagnose (1oo2) nach IEC 61508; Architektur Kategorie 4 nach EN ISO 13849-1
Auslegung der Betriebsart	„high demand“ gemäß IEC 61508 (hohe Anforderungsrate)
Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH-Wert); spezifische Werte gemäß Tabellen Sicherheitstechnische Kenndaten	Erweiterungsbaugruppe: PFH = 9,2 FIT; ESMD (1-kanalig): PFH = 20 FIT; ESMD (2-kanalig): PFH = 1,0 FIT
Proof-Test-Intervall (IEC 61508)	20 Jahre, danach muss die Baugruppe ersetzt werden

Sicherheitshinweis

- Die spezifischen sicherheitstechnischen Kenndaten der jeweiligen Baugruppen sind den techn. Kenndaten aus Kapitel 3 zu entnehmen.
- Bei Verwendung von mehreren Sensoren unterschiedlicher Funktion (z. B. Stellungsanzeige Zugangstür + Geschwindigkeitserfassung) für eine Sicherheitsfunktion (z. B. sicher reduzierte Geschwindigkeit bei geöffneter Zugangstür) sind diese für die sicherheitstechnische Beurteilung des Gesamtsystems als Reihenschaltung aufzufassen. Siehe hierzu Berechnungsbeispiel in Abschnitt 12.3.7.
- Die Sicherheitsvorschriften und EMV-Richtlinien müssen beachtet werden.
- In Bezug auf die getroffenen Fehlerausschlüsse ist auf die Tabellen unter D im Anhang der EN ISO 13849-2 verwiesen.
- Für die sicherheitstechnische Beurteilung des Gesamtsystems können die im Kapitel 3 angegebenen Kenndaten für das Teilsystem PES angesetzt werden (z. B. PL e und PFH-Wert nach Tabelle für Nachweis gemäß EN ISO 13849-1).

Die im Folgenden dargestellten Beispiele und deren charakteristische Architektur sind maßgeblich verantwortlich für die Zuordnung in eine Kategorie nach EN ISO 13849-1.

Die sich daraus ergebenden maximal möglichen Performance Levels nach EN ISO 13849-1 sind weiterhin abhängig von folgenden Faktoren der externen Bauteile:

- Struktur (einfach oder redundant)
- Erkennung von Fehlern gemeinsamer Ursache (CCF)
- Diagnosedeckungsgrad bei Anforderung (DCavg)
- Zeit bis zum gefährlichen Ausfall eines Kanals (MTTFd)

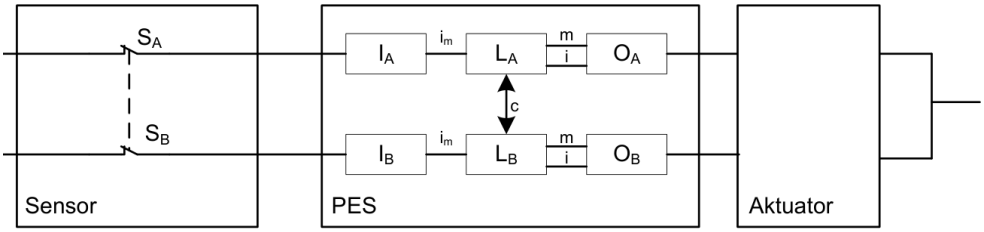
4.2 Sicherheitstechnische Kenndaten und Beschaltung für angeschlossene Sensorik

Die Baugruppen verfügen über jeweils komplett getrennte Signalverarbeitungspfade für jeden Sicherheitseingang. Dies gilt sowohl für die digitalen als auch die analogen Eingänge. Weiterhin sind jeweils Maßnahmen zur Erzielung möglichst hoher DC-Werte implementiert.

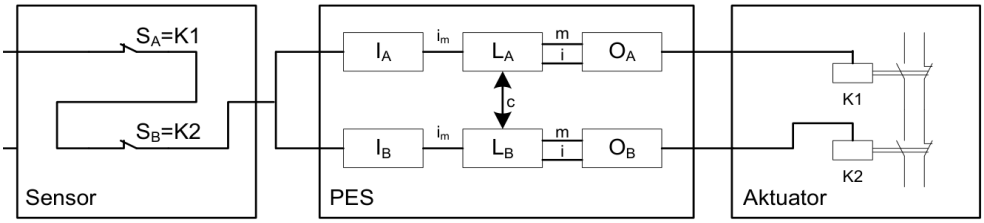
4.2.1 Digitale Sensoren

Die digitalen Eingänge sind mit Ausnahme der elektromechanischen Eingangsklemme grundsätzlich vollständig redundant ausgeführt. Nachfolgend sind die Details zur Einordnung, dem DC und dem erzielbaren PL bzw. SIL aufgelistet.

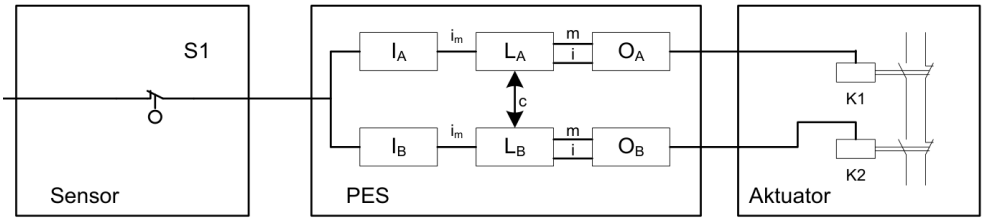
4.2.1.1 Charakteristik der Sensoren / Eingangselemente



Zweikanaliges Eingangselement in Parallelschaltung (Cat. 4, Fehlertoleranz 1) mit hohem DC durch Signalverarbeitung in zwei Kanälen und Diagnose mittels Kreuzvergleich in der PES



Zweikanaliges Eingangselement in Serienschaltung (Cat. 4, Fehlertoleranz 1) mit niedrigen bis mittleren DC durch Signalverarbeitung in zwei Kanälen und Diagnose mittels zyklischer Testung



Einkanaliges Eingangselement und zweikanalige Verarbeitung mit niedrigen bis mittleren DC durch Signalverarbeitung in zwei Kanälen und Diagnose mittels zyklischer Testung, PL / SIL abhängig von zulässigen Fehlerausschlüssen und Testrate des Eingangselements.

4.2.1.2 DC digitale Sensoren/Eingänge

Die Baugruppen gewährleisten weitreichende Diagnosefunktionen für das Eingangsteilsystem. Diese werden ständig bzw. optional (Querschlussüberwachung mittels Pulskennung, Kreuzvergleich, 2- oder mehrkanaliger Sensor mit/ohne Zeitüberwachung, Anlauftest) ausgeführt.

Ständig aktive Diagnosefunktionen:

Kreuzvergleich: Die Eingänge der Baugruppen sind grundsätzlich intern zweikanalig ausgeführt. Der Status der Eingangssignale wird ständig kreuzweise verglichen. Nur bei High-Signal in beiden Eingangsteilsystemen wird auf High-Status des Eingangs erkannt, bei Abweichung des Signalpegels zwischen beiden Kanälen wird der Eingang auf Low-Status gesetzt.

Dynamischer Test der Schaltschwellen des Eingangsteilsystems: Die Schaltschwellen für das Erkennen des High-Pegels werden zyklisch, mit hoher Rate getestet. Bei Unterschreiten des definierten Schwellwertes wird ein Baugruppen-Alarm ausgelöst.

Dynamischer Test der Schaltbarkeit des Eingangsteilsystems: Die Schaltbarkeit des Eingangsteilsystems auf Low-Pegel wird für alle Eingänge mit Ausnahme DI05 ... DI08 zyklisch, mit hoher Rate getestet. Bei Unterschreiten des definierten Schwellwertes wird ein Baugruppen-Alarm ausgelöst.

Durch Parametrierung aktivierbare Diagnosefunktionen:

Querschlusstest: Die Baugruppen verfügen über Pulssignalausgänge, welchen eine eindeutige Signatur eingeprägt wird. Bei Nutzung des Querschlusstests sind die Schaltelemente der digitalen Sensoren / Eingangselemente über die Pulssignalausgänge von der Baugruppe mit Hilfsspannung zu versorgen. Die Signatur wird somit dem High-Signalpegel der Sensoren / Eingangselemente eingeprägt und von der Baugruppe geprüft. Durch die Signaturprüfung können Kurz- oder Querschlüsse nach High-Signal erkannt werden. Mit alternierender Verwendung der Pulssignale bei Mehrfachkontakten, parallelen Signalleitungen oder benachbarter Klemmenbelegung werden Querschlüsse zwischen den entsprechenden Eingangssignalen erkannt.

Sensoren / Eingangselemente mit 2- oder mehrpoligen Kontakten ohne Zeitüberwachung: Den Sensoren/Eingangselementen können mehrere Kontakte zugeordnet werden. Diese entsprechen somit mindestens 2-kanaligen Elementen. Ein High-Pegel des Sensors/Eingangselements erfordert eine logische Reihenschaltung beider Kontakte.

Beispiel 1: Eingangselement mit 2 Öffnern: High-Pegel, wenn beide Kontakte geschlossen.

Beispiel 2: Eingangselement mit 1 Öffner und 1 Schließer: High-Pegel, wenn Schließer betätigt und Öffner unbetätigt.

Sensoren / Eingangselemente mit 2- oder mehrpoligen Kontakten mit Zeitüberwachung: Gleiche Prüfung wie vor, jedoch zusätzlich Überwachung der Eingangssignale auf Übereinstimmung der definierten Pegelzusammenhänge innerhalb eines Zeitfensters von 0,5 s. Bei Differieren der Pegel über einen Zeitraum > 0,5 s wird ein Baugruppen-Alarm ausgelöst.

Starttest: Mit jedem Einschalten der Sicherheitsbaugruppe muss ein Test des Eingangselements in Richtung Low-Signalstatus (= definierter Safe-Status) durchgeführt werden, z. B. Betätigen des Not-Aus-Tasters oder einer Türverriegelung nach Anlagenstart.

Betriebliche / Organisatorische Tests: Über die vorstehend angeführten Diagnosemaßnahmen der Baugruppen hinaus kann in der Applikation eine zyklische Testung durchgeführt werden. Diese Tests können bei der Beurteilung des DC mit herangezogen werden.

> **Hinweis** Die betrieblichen/organisatorischen Tests können auch auf eine Kombination von Hardwareeingängen und funktionalen Eingängen (über Standard-Feldbus übertragene Eingangsinformationen) angewendet werden. Eine exklusive Verwendung von funktionalen Eingängen ist in diesem Zusammenhang jedoch ausgeschlossen (Kombination aus zwei oder mehr funktionalen Eingängen).

Die Baugruppen gewährleisten somit weitreichende Diagnosefunktionen für das Eingangsteilsystem. Diese werden ständig bzw. optional (Querschlussüberwachung mittels Pulskennung) ausgeführt.

Für die sicherheitstechnische Beurteilung des Gesamtsystems können somit grundsätzlich folgende Diagnosen für die Eingangssensorik herangezogen werden:

Charakteristik Eingangselement	Quer-schluss-test	Mit Zeit-überwa-chung	Start-test	Zykl. Test im Betrieb	DC	Definition der Maßnahme	Anmerkung
Einkanalig			O	O	>60	Zyklischer Testimpuls durch dynamische Änderung der Eingangssignale	Ausreichend hohe Testrate muss gewährleistet sein
	X				90	Zyklischer Testimpuls durch dynamische Änderung der Eingangssignale	Nur wirksam, wenn Pulszuordnung aktiv

Charakteristik Eingangselement	Quer-schluss-test	Mit Zeit-überwa-chung	Start-test	Zykl. Test im Betrieb	DC	Definition der Maßnahme	Anmerkung
	X		O	O	90-99	Zyklischer Testimpuls durch dynamische Änderung der Eingangssignale	DC von Häufigkeit des Start- / zyklischen Test abhängig; DC = 90 Test nur in Abständen > 4 Wochen; DC = 99 Test mind. 1 × Tag bzw. 100-fach Anforderungsrate
Zweikanalig					90	Kreuzvergleich von Eingangssignalen mit dynamischem Test, wenn Kurzschlüsse nicht bemerkt werden können (bei Mehrfach-Ein-/Ausgängen)	Bei Fehlerausschluss Kurzschluss bis DC = 99 möglich
			O	O	90-99	Zyklischer Testimpuls durch dynamische Änderung der Eingangssignale	DC von Häufigkeit des Start- / zyklischen Test abhängig
	X				99	Kreuzvergleich von Eingangssignalen mit unmittelbarem und Zwischenergebnissen in der Logik (L) und zeitlich und logische Programmlauf überwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Eingängen)	Nur wirksam, wenn Pulszuordnung aktiv

Charakteristik Eingangselement	Quer-schluss-test	Mit Zeit-überwa-chung	Start-test	Zykl. Test im Betrieb	DC	Definition der Maßnahme	Anmerkung
		X			99	Plausibilitätsprüfung, z. B. Verwendung der Schließer- und Öffnerkontakte = antivalenter Signalvergleich von Eingangselementen	Nur wirksam in Verbindung mit aktivierter Zeitüberwachungsfunktion für Eingangselement

Sicherheitshinweis

- Für eine sicherheitstechnische Beurteilung des Teilsystems Sensorik sind die Herstellerangaben (MTTFd, FIT-Zahlen etc.) heranzuziehen.
- Die in der Tabelle angeführten DC-Werte sind konservativ anzusetzen und die Einhaltung der Randbedingungen (siehe Tabelle unter „Anmerkungen“) zu gewährleisten.
- Fehlerausschlüsse sind nach den einschlägigen Normen zulässig. Die dabei angeführten Randbedingungen sind dauerhaft zu gewährleisten.
- Wenn mehrere Sensorsysteme zur ordnungsgemäßen Funktion einer einzelnen Sicherheitsfunktion erforderlich sind, sind deren Teilwerte jeweils korrekt nach gewähltem Verfahren zusammenzuführen.

4.2.1.3 Klassifizierung der sicheren digitalen Eingänge

Digitale Eingänge DI01 ... DI14

Digitale Eingänge	Erreichbarer Performance Level	Bemerkung
DI01 ... DI04, DI09 ... DI14	PL e	Geeignet für alle Arten von Eingangselementen, mit / ohne Pulse, erreichbarer PL abhängig von MTTFd des Eingangselements sowie Fehlerausschlüssen in der externen Verkabelung
DI05 ... DI08	PL e	Einkanalig mit Pulse: – Überwiegend High-Pegel erforderlich (THigh > 100 * TLow) – Mindestens eine Anforderung/Tag durch Applikation bedingt – Fehlererkennung bei Anforderung
	PL d	Einkanalig ohne Pulse: – Fehlerausschluss Kurzschluss zwischen den Signalen und nach VCC – Fehlererkennung bei Anforderung
	PL e	Zweikanalig: – Mindestens eine Anforderung/Tag durch Applikation bedingt – Fehlererkennung bei Anforderung

Digitale Eingänge I/Os (EAEx)

Hinweis Der erzielbare PL für eine Kombination aus HW-Eingängen und funktionalen Eingängen ist abhängig von den gewählten betrieblichen/organisatorischen Tests sowie der Unabhängigkeit beider Kanäle im Systemaufbau. Für die Bestimmung des PL ist eine applikationsbezogene Analyse erforderlich.

Digitale Eingänge	Erreichbarer Performance Level	Bemerkung
EAEx		Ohne Puls, einkanalig statisches Signal -> Meldeeingang
	PL e	Ohne Puls, zweikanalig statisches Signal – Mindestens eine Anforderung/Tag durch Applikation bedingt – Fehlererkennung nur bei Anforderung
	PL d	Ohne Puls, zweikanalig statisches Signal – Weniger als eine Anforderung/Tag durch Applikation bedingt
	PL e	Einkanalig mit Pulse – Überwiegend High-Pegel erforderlich (THigh > 100 * TLow) – Mindestens eine Anforderung/Tag durch Applikation bedingt – Fehlererkennung nur bei Anforderung
	PL d	Einkanalig mit Pulse – Weniger als eine Anforderung/Tag
	PL e	Zweikanalig mit Puls1 und Puls2

4.2.1.4 Anschlussbeispiele digitale Sensoren

Einkanaliger Sensor, ohne Querschlussprüfung

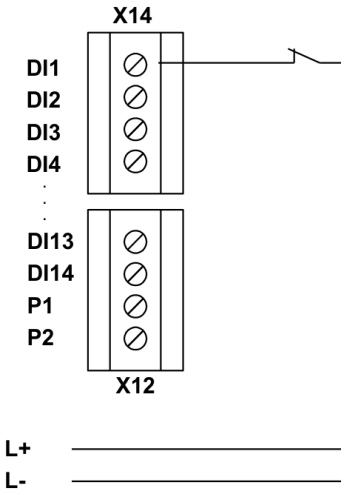


Bild: Einkanaliger Sensor, ohne Querschlussprüfung

Der einkanalige Sensor wird ohne Pulse bzw. ohne Querschlussprüfung an die Baugruppe angeschlossen. Diese Bauart ist für Sicherheitsanwendungen nicht zu empfehlen. Es kann max. PL b nach EN ISO 13849-1 erreicht werden.

Einkanaliger Sensor mit Querschlussprüfung

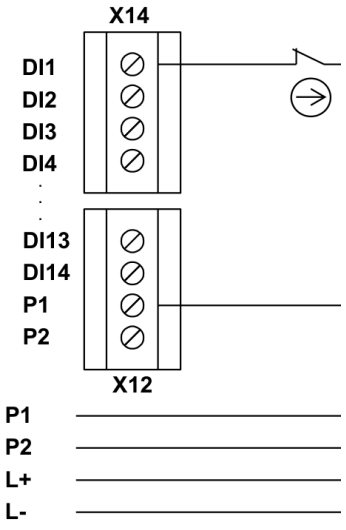


Bild: Einkanaliger Sensor mit Pulsen

Bei Einsatz eines einkanaligen Sensors mit Pulsen wird ein Versorgungsanschluss des Schaltelements an den Pulsausgang P1 oder P2 angeschlossen. Anschließend muss die Pulszuordnung auf der Baugruppe noch zugeordnet werden.

Die Verwendung eines einkanaligen Sensors mit Pulsen erkennt:

- Kurzschluss auf die Versorgungsspannung DC 24 V
- Kurzschluss auf DC 0 V
- Kabelunterbrechung (Stromunterbrechung ist sicherer Zustand!)

Vorsicht ist hingegen bei einem Kabelkurzschluss zwischen den beiden Anschlüssen des Sensors angebracht, da dieser nicht erkannt wird! Ebenfalls nicht erkannt wird ein Kurzschluss zwischen P1 und DI01.

Aufgrund des 1-kanaligen Charakters des Schaltelements / Sensors ist für dessen Versagen ein Fehlerausschluss erforderlich. Dies ist bei Verwendung von zwangstrennenden Schaltern mit korrekter zwangsläufiger Betätigung zulässig.

Dieser Anwendung gleichgestellt ist eine Reihenschaltung von 2 Schaltelementen mit entsprechendem Fehlerausschluss eines Doppelfehlers (zwei Fehler treten zum selben Zeitpunkt auf). Dies können z. B. die Sicherheitsausgänge eines elektronischen Überwachungsgeräts (Lichtvorhang, Schaltmatte) mit interner 2-kanaliger Abschaltung darstellen.

Bei Verwendung eines geeigneten Schaltelements und sorgfältiger Verkabelung des Sensors kann PL d nach EN ISO 13849-1 erreicht werden. In Sonderfällen, d. h. in Verbindung mit geeigneten Schaltelementen und zulässigen Fehlerausschlüssen, kann auch PL e nach EN ISO 13849-1 erzielt werden.

Sicherheitshinweis

- PL d oder höher nach EN ISO 13849-1 wird erreicht, wenn der Kurzschluss zwischen Eingang und zugehörigem Pulsausgang sowie der Kurzschluss zwischen den Sensoranschlüssen ausgeschlossen werden kann. Dabei ist zu beachten, dass der Schalter im Fehlerfall zwangsöffnend nach EN 60947-5-1 sein muss. Zusätzlich muss der Sensor in regelmäßigen Abständen ausgelöst und die Sicherheitsfunktion angefordert werden. Fehlerausschlüsse können gemäß EN ISO 13849-2 Tabelle D8 erzielt werden. Bei einkanaliger Verwendung der Eingänge ist das erreichbare Sicherheitsniveau auf SIL 2 bzw. PL d eingeschränkt, wenn nicht in regelmäßigen Abständen eine Anforderung der Sicherheitsfunktion erfolgt.
- Eine Reihenschaltung von 2 Schaltelementen mit Fehlerausschluss Doppelfehler bedingt eine Prüfung auf Eignung nach dem angestrebten Sicherheitsniveau für dieses Element. Auf die einschlägigen Regelungen der EG-Maschinenrichtlinie 2006/42/EG wird hingewiesen.
- Bei einkanaligen Sensoren ist grundsätzlich eine sicherheitstechnische Verwendung der Eingänge nur in Verbindung mit den Pulsausgängen vorgesehen.

Zweikanaliger Sensor ohne Zeitüberwachung mit Querschlussprüfung

Fehler werden mindestens bei Anforderung erkannt. Der DC ist mittel und kann durch Verwendung zyklischer Tests (Starttests, betriebliche/organisatorische Tests) je nach Testhäufigkeit bis zur Einstufung hoch verändert werden.

Für Sicherheitsanwendungen sind hierzu ausschließlich Öffnerkontakte zu verwenden.

PL d nach EN ISO 13849-1 kann erreicht werden bei Verwendung von Sensoren / Schaltelementen mit Fehlerausschluss für das Nichtöffnen der Schaltkontakte. Dies ist bei Verwendung von zwangstrennenden Schaltern mit korrekter zwangsläufiger Betätigung zulässig. Ebenfalls zulässig ist die Verwendung von Sensoren mit selbstüberwachenden Ausgangskontakten.

PL e nach EN ISO 13849-1 kann erreicht werden bei Verwendung von diversitären Sensoren / Eingangselementen mit ausreichend hohem MTTFd in Verbindung mit einer zeitlichen Plausibilitätsüberwachung und ausreichend hoher Änderung des Schaltzustands = dynamische Testung.

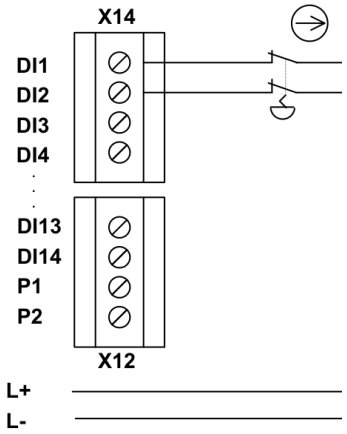


Bild: zweikanaliger Sensor homogen ohne Pulse, mit Zwangstrennung

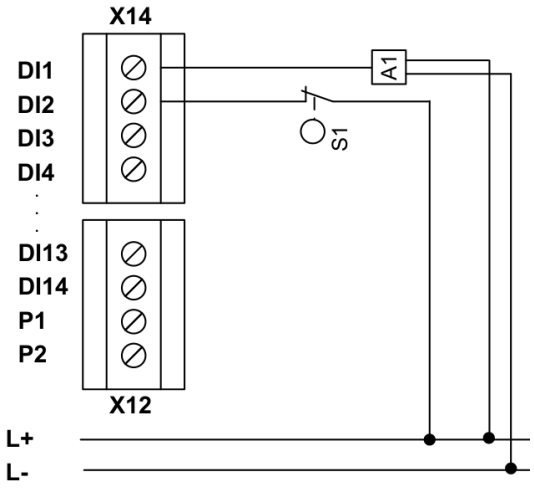


Bild: zweikanaliges Eingangselement diversitär, ohne Pulse

Sicherheitshinweis

- PL d oder höher nach EN ISO 13849-1 wird erreicht bei Verwendung von Schaltelementen / Sensoren mit zwangsöffnenden Kontakten bzw. zwangsläufiger Betätigung nach EN 60947-5-1.
- Eine Verwendung von Geräten, für deren Schaltelemente der Fehlerausschluss Doppelfehler für das angestrebte Sicherheitsniveau getroffen werden kann, ist zulässig. Auf die einschlägigen Regelungen der EU-Maschinenrichtlinie 2006/42/EG wird hingewiesen.

Zweikanaliger Sensor mit Zeitüberwachung und Querschlussprüfung

Durch Verwendung von zwei unabhängigen Pulssignalen am homogenen Sensor können alle Querschlüsse sowie Verbindungen nach DC 24 V und DC 0 V erkannt werden.

PL d oder höher nach EN ISO 13849-1 kann erreicht werden bei:

- Verwendung von Sensoren / Schaltelementen mit zwangsläufiger Betätigung.
- Verwendung von 2 Sensoren / Schaltelementen mit unabhängiger Betätigung
- dto., jedoch mit Betätigung über eine gemeinsame Betätigungseinrichtung in Zusammenhang mit einem Fehlerausschluss für diese Einrichtung.

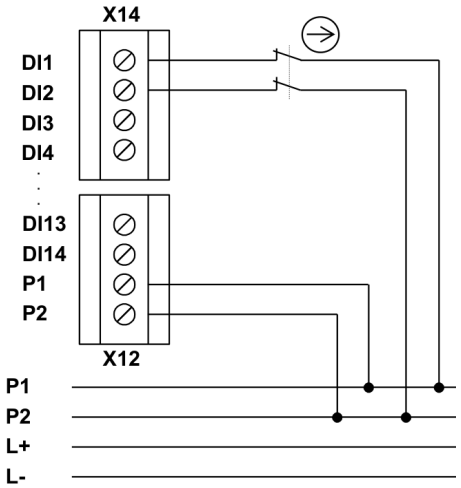


Bild: zweikanaliger Sensor homogen mit Pulsen

Sicherheitshinweis

- PL d oder höher nach EN ISO 13849-1 wird erreicht bei Verwendung von Schaltelementen / Sensoren mit zwangsläufiger Betätigung.
- Bei Verwendung von zwei unabhängigen Sensoren mit unabhängiger Betätigung kann PL d oder höher nach EN ISO 13849-1 erreicht werden.
- Bei Verwendung von gemeinsamen Elementen in der Betätigungskette ist hierfür ein Fehlerausschluss erforderlich. Die entsprechenden Einschränkungen und Kriterien nach EN ISO 13849-1 sind hierfür zu beachten.

4.2.1.5 Übersicht erreichbarer PL für digitale Sicherheitseingänge

Typ Sensor / Eingangselement	Eingang	Quer-schluss-test	Zeit-überw.	Start-test	Zykl. Test	PL	Fehlerausschluss für Eingangselement	Bedingung für Eingangselement
Einkanalig	DI01..DI14					b		Betriebsbewährtes Eingangselement
	DI01..DI14			O	O	d	Alle Fehler am Eingangselement; Kurzschluss am Eingang/Signalleitung	MTTFd = hoch; Verbindung im Schaltschrank oder geschützte Verlegung
	DI01..DI04, DI09..DI14					e	Alle Fehler am Eingangselement; Kurzschluss am Eingang/Signalleitung	Eingangselement entspricht mind. PLr; Verbindung im Schaltschrank oder geschützte Verlegung
	Alle	X				d	Hängenbleiben; Kurzschluss am Eingang/Signalleitung	Überwiegend High-Pegel erforderlich (THigh > 100 * TLow). Zwangstrennend, MTTFd = hoch; Verbindung im Schaltschrank oder geschützte Verlegung
	Alle	X		O	O	e	Alle Fehler am Eingangselement; Kurzschluss am Eingang/Signalleitung	Eingangselement entspricht mind. PLr; Verbindung im Schaltschrank oder geschützte Verlegung; MTTFd = hoch
Zweikanalig parallel	Alle					d	Kurzschluss zwischen Eingang/Signalleitung	Verbindung im Schaltschrank oder geschützte Verlegung; MTTFd = mittel

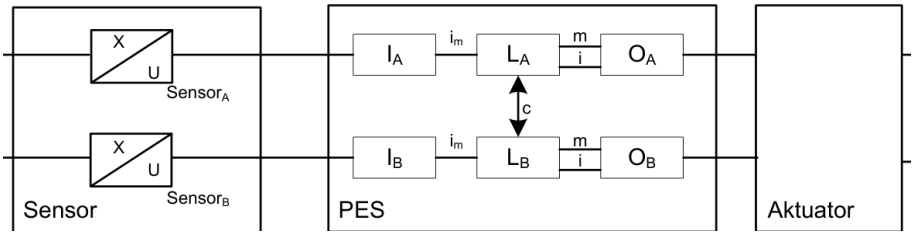
Typ Sensor / Eingangselement	Eingang	Quer-schluss-test	Zeit-überw.	Start-test	Zykl. Test	PL	Fehlerausschluss für Eingangselement	Bedingung für Eingangselement
	Alle	X				e		MTTFd = hoch
Zweikanalig parallel	Alle		X			e	Kurzschluss zwischen Eingang/Signalleitung (nur bei gleichen Schaltelementen = 2xS oder 2xÖ)	Verbindung im Schaltschrank oder geschützte Verlegung; MTTFd = hoch
Zweikanalig seriell	DI01..DI04, DI09..DI14					d	Kurzschluss am Eingang/Signalleitung; Hängenbleiben / Zwangstrennend	Verbindung im Schaltschrank oder geschützte Verlegung; MTTFd = mittel
	DI01..DI04, DI09..DI14			O	O	e	Kurzschluss am Eingang/Signalleitung	Verbindung im Schaltschrank oder geschützte Verlegung; MTTFd = hoch
	Alle			O	O	d	Kurzschluss am Eingang/Signalleitung	Verbindung im Schaltschrank oder geschützte Verlegung; MTTFd = mittel
	Alle	X		O	O	e		MTTFd = hoch

X: Diagnosemaßnahme aktiviert · O: mind. 1 Diagnosemaßnahme aktiviert · PL: erreichbarer PL nach EN ISO 13849-1

4.2.2 Analogsensoren

Die Basisbaugruppe ESMD verfügt über zwei Analogeingänge mit je zwei Eingangskanälen. Grundsätzlich sind an dieses Interface nur 2-kanalige Sensoren anzuschließen.

Die interne Signalverarbeitung erfolgt getrennt in beiden Kanälen mit Kreuzvergleich der Ergebnisse.



Zweikanaliges Sensorsystem mit getrennter Signalverarbeitung in zwei Kanälen, Diagnose durch Quervergleich in der PES

Analog zu den anderen Sensorsystemen ist eine Reihe von Diagnosemaßnahmen implementiert.

Grundsätzlich können die Diagnosemaßnahmen bezüglich ihrer Art und Wirksamkeit gemäß nachstehender Tabelle klassifiziert werden:

Diagnosen für Sensoren zur Positions- und/oder Geschwindigkeitserfassung:

Maßnahme	DC	Anmerkung	Verwendung
Kreuzvergleich von Eingangssignalen mit dynamischem Test, wenn Kurzschlüsse nicht bemerkt werden können (bei Mehrfach-Ein-/Ausgängen)	90 %	Vergleich der analogen Eingangswerte mit gleicher Charakteristik für beide Kanäle	Überwachung 2-kanaliger Systeme mit gleicher Charakteristik der Eingangssignale
Kreuzvergleich von Eingangssignalen mit unmittelbarem und Zwischenergebnissen in der Logik (L) und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Eingängen)	99 %	Vergleich der analogen Eingangswerte mit diversitärer Charakteristik der beiden Kanäle, z. B. inverser Signalverlauf etc.	Überwachung 2-kanaliger Sensorsysteme mit diversitärer Charakteristik der Eingangssignale

Sicherheitshinweis

- Für eine sicherheitstechnische Beurteilung des Teilsystems Sensorik sind die Herstellerangaben (MTTFd, FIT-Zahlen etc.) heranzuziehen.
- Die in der Tabelle angeführten DC-Werte sind konservativ anzusetzen und die Einhaltung der Randbedingungen (siehe Tabelle unter „Anmerkungen“) zu gewährleisten.
- Fehlerausschlüsse sind nach den einschlägigen Normen zulässig. Die dabei angeführten Randbedingungen sind dauerhaft zu gewährleisten.
- Wenn mehrere Sensorsysteme zur ordnungsgemäßen Funktion einer einzelnen Sicherheitsfunktion erforderlich sind, sind deren Teilwerte jeweils korrekt nach gewähltem Verfahren zusammenzuführen. Dies gilt auch für eine Kombination aus digitalen und analogen Sensoren (z. B. sicher reduzierte Geschwindigkeit bei geöffneter Schutztür = Türkontakt + Encoder für Geschwindigkeitserfassung).

Anschlussbeispiel analoge Sensoren

Durch Verwendung geeigneter Sensoren und sorgfältiger Verkabelung des Sensors kann PL e nach EN ISO 13849-1 erreicht werden.

Die analogen Stromeingänge sind jeweils mit einem festen Bürden-Widerstand von 500 Ω bestückt. Bei analogen Spannungseingängen entfällt dieser Widerstand.

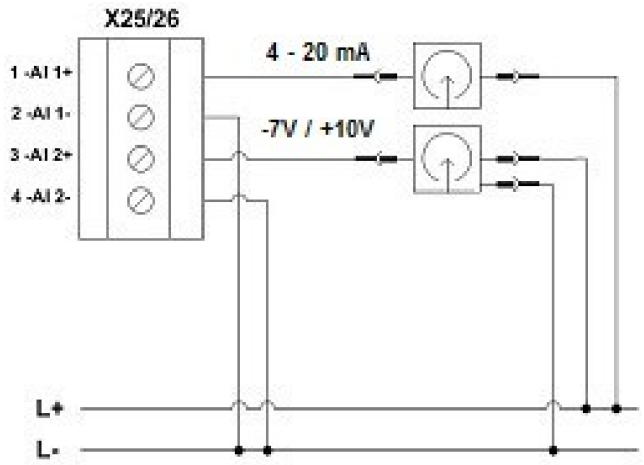


Bild: Beispiel für Anschluss analoge Sensoren

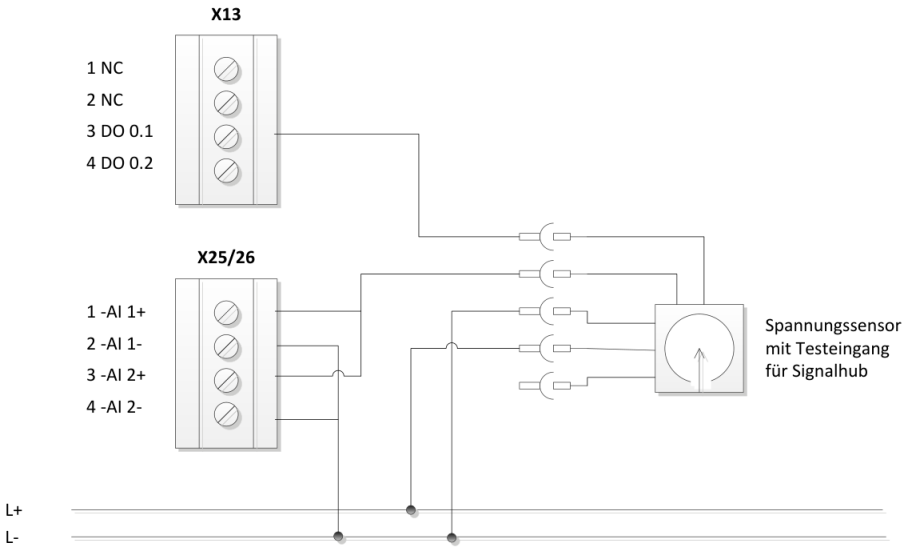


Bild: Spannungssensor mit Prüfimpuls

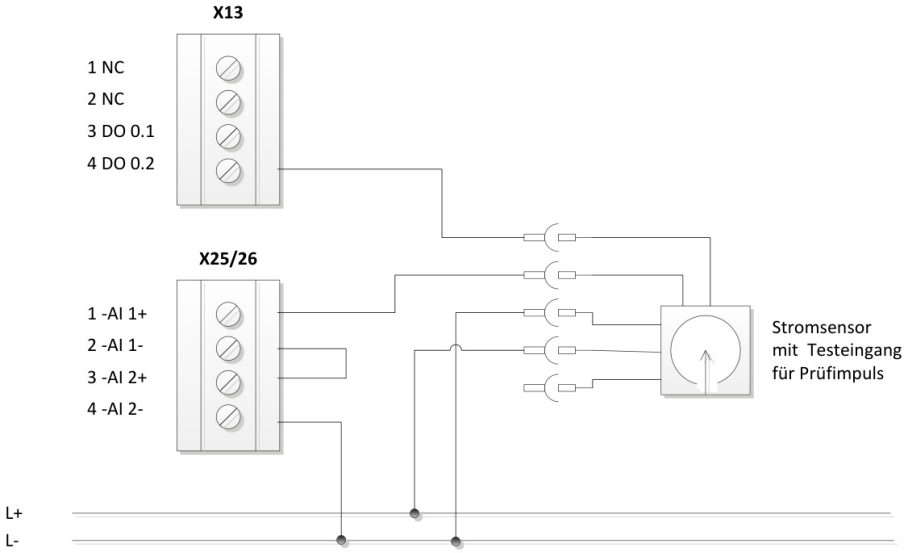


Bild: Stromsensor mit Prüfimpuls

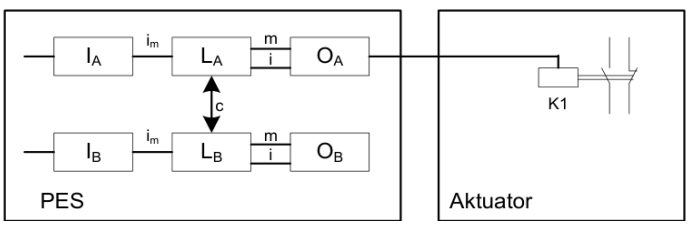
Sicherheitshinweis

– PL e nach EN ISO 13849-1 wird erreicht, wenn zwei rückwirkungsfreie Sensoren verwendet werden, für welche Common-Cause-Fehler ausgeschlossen werden können.

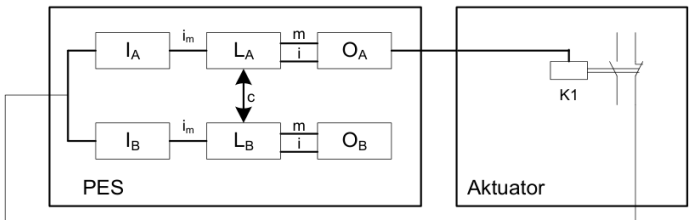
4.3 Sicherheitstechnische Kenndaten und Beschaltung der Ausgänge

Die Baugruppen verfügen jeweils über sichere Ausgänge unterschiedlichen Typs. Bei der Beschaltung ist die jeweilige Charakteristik gemäß nachstehender Beschreibung zu berücksichtigen.

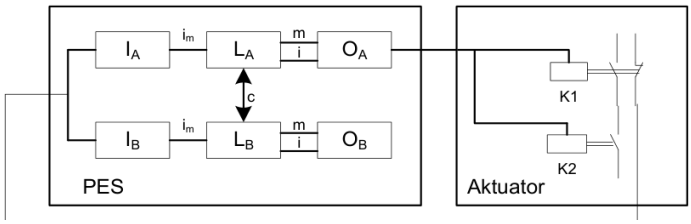
4.3.1 Charakteristik der Ausgangselemente



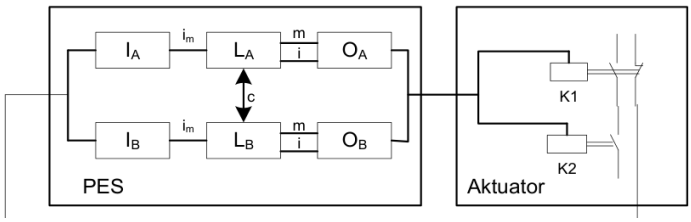
Einkanaliger Ausgang ESMD und einkanaliger Aktuator ohne Diagnose



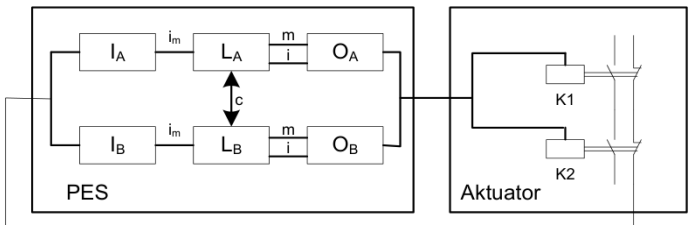
Einkanaliger Ausgang ESMD und einkanaliger Aktuator mit Diagnose



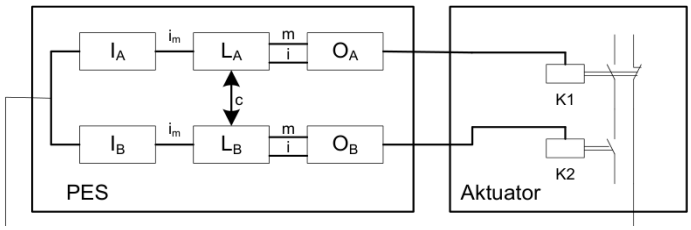
Einkanaliger Ausgang ESMD (Rel 1 / 2) und zweikanaliger Aktuator mit mind. einkanaliger Diagnose



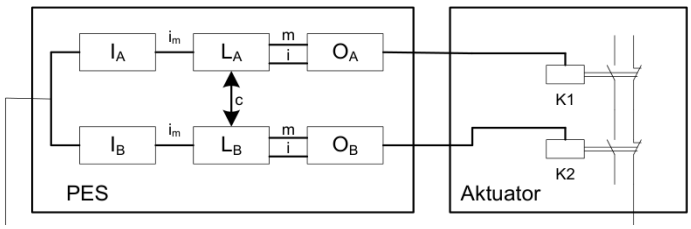
Einkanaliger Ausgang mit intern zweikanaliger Verarbeitung (EAAx) und zweikanaliger Aktuator mit mind. einkanaliger Diagnose



Einkanaliger Ausgang mit intern zweikanaliger Verarbeitung (EAAx) und zweikanaliger Aktuator mit zweikanaliger Diagnose



Zweikanaliger Ausgang ESMD und zweikanaliger Aktuator mit einkanaliger Diagnose



Zweikanaliger Ausgang ESMD und zweikanaliger Aktuator mit zweikanaliger Diagnose

4.3.2 Diagnosen im Abschaltkreis

Die Abschaltkreise verfügen über fest implementierte und parametrierbare Diagnosefunktionen. Bestimmte Diagnosefunktionen schließen auch den externen Teil des Abschaltkanals mit ein. Abhängig von der Nutzung dieser Diagnosefunktionen ergeben sich unterschiedliche DC-Werte.

4.3.2.1 Diagnosefunktionen

Fest implementierte Diagnosefunktionen:

Kreuzweises Rücklesen der Ausgänge: Sämtliche Sicherheitsausgänge werden jeweils im komplementären Kanal zurückgelesen. Fehler im internen Abschaltkreis der Baugruppe werden so mit DC = Hoch detektiert.

Testung der Abschaltfähigkeit für K1 und K2 (nur Ansteuerung des Relais): Die Abschaltfähigkeit dieser Ausgänge wird zyklisch getestet. Ein Ausfall der Abschaltmöglichkeit wird eindeutig erkannt.

Parametrierbare Diagnosefunktionen:

Rücklesen des Aktuatorstatus über Hilfskontakte, Stellungsanzeigen etc.: Der aktuelle Status des Aktuators wird durch Rücklesen von entsprechend geeigneten Hilfskontakten oder Stellungsanzeigen erfasst und mit dem Sollstatus verglichen. Eine Abweichung wird so eindeutig erkannt.

Hinweis: Der DC ist abhängig von einer einkanaligen oder zweikanaligen Diagnose sowie von der Schalthäufigkeit.

Testung der Abschaltfähigkeit für EAA, EAA1 – EAA10 (digitale Ausgänge): Die Abschaltfähigkeit dieser Ausgänge wird nach Aktivierung der Funktion zyklisch getestet. Ein Ausfall der Abschaltmöglichkeit wird eindeutig erkannt.

4.3.2.2 Übersicht DC in Bezug auf gewählte Diagnosefunktionen

Maßnahme	DC	Anmerkung	Verwendung
Überwachung der Ausgänge durch einen Kanal ohne dynamischen Test	0-90 %	DC abhängig von der Schalthäufigkeit. Bei Verwendung von Elementen zur Schaltverstärkung (externe Relais oder Schütze) nur wirksam in Verbindung mit Rücklesefunktion der Schaltkontakte	Überwachung von elektromechanischen, pneumatischen oder hydraulischen Aktuatoren / Ausgängen
Redundanter Abschaltpfad mit Überwachung eines der Antriebselemente	90 %	Bei Verwendung von Elementen zur Schaltverstärkung (externe Relais oder Schütze) nur wirksam in Verbindung mit Rücklesefunktion der Schaltkontakte	Überwachung von Ausgängen mit direkter Funktion als Sicherheitsschaltkreis oder Überwachung von Sicherheitsschaltkreisen mit Elementen zur Schaltverstärkung oder pneumatischen / hydraulischen Steuerventilen in Verbindung mit Rücklesefunktion von deren Schaltstatus
Kreuzvergleich von Ausgangssignalen mit unmittelbarem und Zwischenergebnissen in der Logik (L) und zeitlich und logische Programmlaufüberwachung und Erkennung statischer Ausfälle und Kurzschlüsse (bei Mehrfach-Ein-/Eingängen)	99 %	Bei Verwendung von Elementen zur Schaltverstärkung (externe Relais oder Schütze) nur wirksam in Verbindung mit Rücklesefunktion der Schaltkontakte. Für Applikationen mit häufiger Anforderung der Sicherheitsabschaltung sollte in kürzeren Zeitintervallen, z. B. bei Schichtbeginn, 1 × pro Woche getestet werden. Ein Test sollte jedoch mindestens zyklisch 1 × pro Jahr erfolgen.	Überwachung von Ausgängen mit direkter Funktion als Sicherheitsschaltkreis oder Überwachung von Sicherheitsschaltkreisen mit Elementen zur Schaltverstärkung oder pneumatischen / hydraulischen Steuerventilen in Verbindung mit Rücklesefunktion von deren Schaltstatus

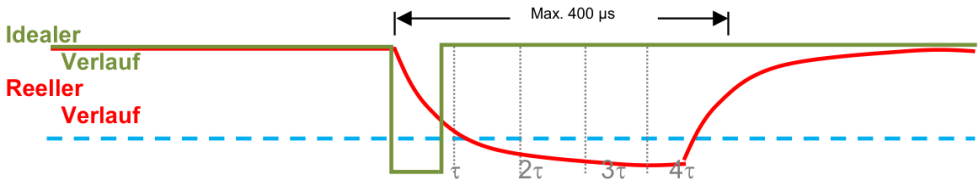
4.3.3 Zulässige kapazitive und induktive Last an sicheren Ausgängen

Die sicheren Ausgänge weisen OSSD-Charakter auf, d. h. die Ausgänge werden zum Test der Abschaltfähigkeit zyklisch abgeschaltet und der Status rückgelesen.

Die Prüfung der Abschaltfähigkeit erfolgt nach folgenden Kriterien / Funktionen:

- Nach Abschaltung des Ausgangs darf die Ausgangsspannung max. 5,6 V betragen
- Der zulässige Spannungspegel muss spätestens nach 400 µs erreicht werden
- Wird der zulässige Spannungspegel erreicht, gilt der Test als erfolgreich, der Ausgang wird ohne weitere Verzögerung wieder aktiviert
- Wird der zulässige Spannungspegel auch nach 400 µs noch nicht erreicht, wird ein Alarm ausgelöst und sämtliche sichere Ausgänge (Zweitkanal bei sicheren Ausgängen!) werden deaktiviert

Die nachstehende Darstellung zeigt den idealen (grüne Kurve) und typischen (rote Kurve) Verlauf.



Idealer und reeller Verlauf der Ausgangsspannung beim Test (max. 400 µs)

Zur Ermittlung der maximal zulässigen Kapazität oder Induktivität ist die Zeitkonstante **τ** des realen RC- bzw. RL-Glieds am Ausgang zu betrachten.

Dieses RC- bzw. RL-Glied bestimmt die reale Entladekurve:

Der Spannungspegel von max. 5,6 V wird sicher nach 3**τ** erreicht. Damit gilt: 3**τ** < 350 µs, **τ** < 100 µs.

Mit dem Zusammenhang

$$\tau = RC = \frac{L}{R}$$

kann die max. verwendbare kapazitive oder induktive Last in Verbindung mit deren ohmscher Last ermittelt werden:

$$C_{max} = \frac{\tau}{R} = \frac{10^{-4}}{R} \quad \text{bzw.} \quad L_{max} = \tau R = 10^{-4} \cdot R$$

Typische Werte für die Kapazität C sind C = 20 nF und für die Längsinduktivität L = 100 mH.

4.3.4 Digitale Ausgänge

Die Baugruppen ESMD und Erweiterungsbaugruppe verfügen jeweils über die baugleichen Ausgänge.

4.3.4.1 Kenndaten der Basisausgänge

Die Baureihe stellt verschiedene Arten von Ausgängen zur Verfügung, die entweder einzeln oder in Gruppen zusammengeschaltet werden können.

Ausgang	Architektur nach EN ISO 13849-1	Bemerkung
Kombination von 2 Relais K1 – K2	4	Vollständiger Abschaltkanal entsprechend Architektur Kategorie 4 nach EN ISO 13849-1
K1, K2	Nicht sicher	Nur funktional
DO 0.1	Nicht sicher	Hilfsausgang
DO 0.2	Nicht sicher	Hilfsausgang

Im eingeschalteten Zustand werden alle Ausgänge mit einem zyklischen Testimpuls auf korrekte Funktion geprüft. Dazu wird der Ausgang maximal für eine Testdauer TT < 500 µs (typisch 200 µs) auf den jeweils inversen Wert geschaltet.

Die Relaisausgänge werden bei jedem Schaltspiel auf Plausibilität überwacht. Zum Erhalten der Sicherheitsfunktion müssen die Relaisausgänge zyklisch geschaltet und somit getestet werden. Der Schalt-/Testzyklus ist abhängig von der Applikation festzulegen.

Sicherheitshinweis

- Für Applikationen mit häufiger Anforderung der Sicherheitsabschaltung sollte in kürzeren Zeitintervallen, z. B. bei Schichtbeginn, 1 × pro Woche getestet werden. Ein Test sollte jedoch mindestens zyklisch 1 × pro Jahr erfolgen.
- Die Testfunktion der Ausgänge wird bei Gruppen- und Einzelansteuerung ausgeführt. Die Hilfsausgänge werden nicht getestet.
- Ein Mischbetrieb bei den Relaiskontakten ist nicht erlaubt! Mischbetrieb: Ein gefährliches Berührungsspannungspotenzial darf nicht mit einer Schutzkleinspannung gemischt werden.

Beispiel FALSCH: Über K1.1 + K1.2 werden 230 VAC geschaltet und über K2.1 + K2.2 werden 24 VDC geschaltet.

Beispiel RICHTIG: Über K1.1 + K1.2 und K2.1 + K2.2 werden jeweils 230 VAC geschaltet. Oder über K1.1 + K1.2 und K2.1 + K2.2 werden jeweils 24 VDC geschaltet.

Die Ausgänge können wie folgt belastet werden:

Ausgang	Spannung	Strom
Relais Kx	24 VDC	2,0 A (DC13)
Relais Kx	230 VAC	2,0 A (AC15)
DOx	24 VDC	250 mA
EAAx	24 VDC	250 mA

Sicherheitshinweis

- Für sicherheitstechnische Anwendungen dürfen nur externe Schaltelemente mit einem minimalen Haltestrom von > 1,2 mA verwendet werden.
- Für das Ausgangssystem ist eine Reihe von Diagnosemaßnahmen implementiert. Zu beachten ist hier insbesondere die Einbeziehung von Elementen zur Schaltverstärkung wie Relais, Schütze etc. im Abschaltkreis.
- Wenn die Hilfsausgänge zu Steuerungszwecken eingesetzt werden, muss beachtet werden, dass nach einem POR (Power-on-Reset) der Steuerung die Hilfsausgänge in der Hochlaufphase in einem undefinierten Zustand sind.

4.3.4.2 Beschaltungsbeispiele Basisausgänge

Einkanalig schaltender Relais- oder Halbleiter-Ausgang ohne Prüfung

Zur Anschaltung mehrphasiger Anwendungen bzw. bei erhöhtem Strombedarf können externe Schütze verwendet werden. Bei einer einkanaligen Anschaltung ohne externe Prüfung ist zu beachten, dass ein Verkleben eines oder mehrerer externer Kontakte von der Baugruppe nicht erkannt wird. Das nachfolgende Schaltbeispiel ist für Sicherheitsanwendungen nur eingeschränkt geeignet, es kann maximal PL b nach EN ISO 13849-1 erreicht werden!

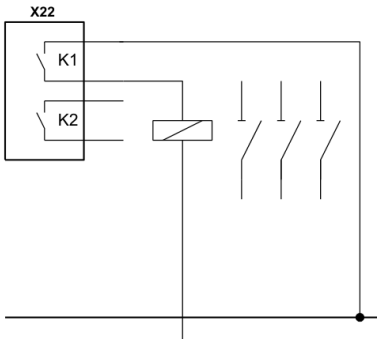


Bild: Einkanalig schaltender Relaisausgang

Sicherheitshinweis

- Nicht empfohlen für Sicherheitsanwendungen! Siehe hierzu auch Hinweise in der EN ISO 13849-1 zur Anwendung und erforderlichen Fehlerausschlüssen.

Zweikanalig schaltender Relaisausgang mit externer Überwachung – Sammelrückmeldung

Für Sicherheitsanwendungen ab PL d nach EN ISO 13849-1 kommen zwei Relais auf der Baugruppe und zwei externe Leistungsschütze zum Einsatz.

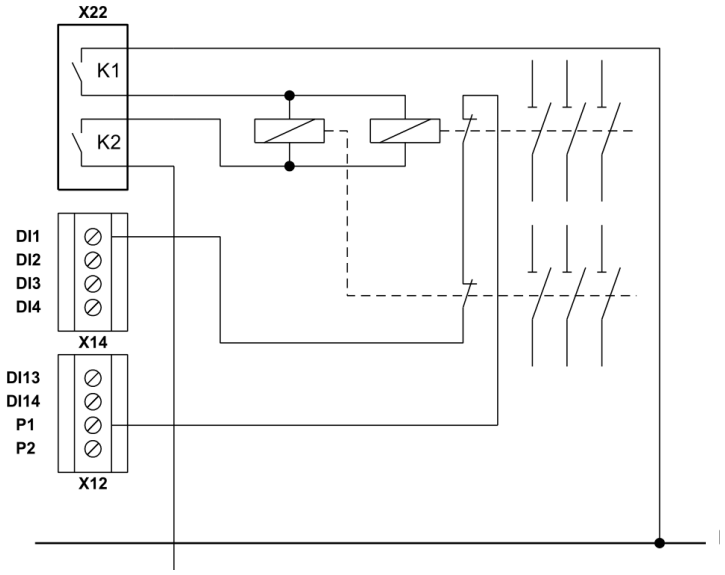


Bild: Zweikanalig schaltender Relaisausgang mit externer Überwachung – Sammelrückmeldung

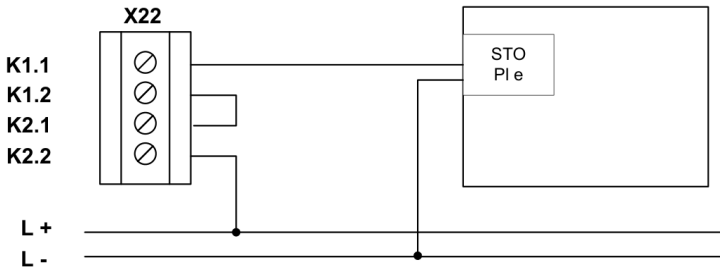
Die beiden externen Überwachungskontakte werden in Reihe geschaltet, von Pulssignal P1 gespeist und von DI01 (als EMU-Eingang konfiguriert) eingelesen. Bei erhöhten Anforderungen ist zu beachten, dass mindestens alle 24 Stunden mindestens 1 Schaltvorgang stattfinden muss.

Sicherheitshinweis

- Zur Erreichung von PL e nach EN ISO 13849-1 wird eine ausreichend hohe Testrate gefordert.
- Für Applikationen mit häufiger Anforderung der Sicherheitsabschaltung sollte in kürzeren Zeitintervallen, z. B. bei Schichtbeginn, 1 × pro Woche getestet werden. Ein Test sollte jedoch mindestens zyklisch 1 × pro Jahr erfolgen.

Zweikanaliger Ausgang mit Relaisausgang – externer Ansteuerkreis in PL e

Für Sicherheitsanwendungen ab PL d und höher nach EN ISO 13849-1. Die Ansteuerung des externen Kreises erfolgt zweikanalig über die Relaisausgänge. Für PL e nach EN ISO 13849-1 ist eine ausreichend hohe Testrate sowie PL e für den externen Kreis gefordert.



Zweikanaliger Ausgang mit Relaisausgang, externer Kreis (STO, PL e)

Beschaltung eines Hilfsausgangs

Beide auf der Baugruppe implementierten Halbleiterausgänge können für funktionale Applikationen beschaltet werden. Die Ausgänge werden nicht gepulst.

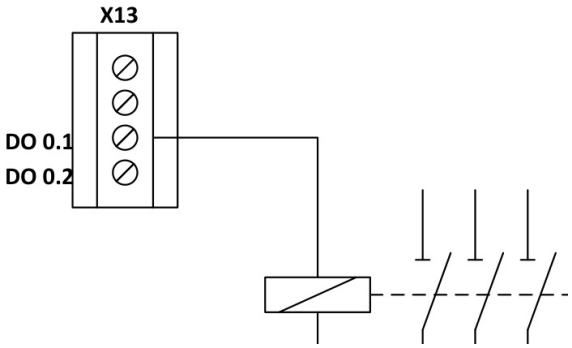


Bild: Beschaltung eines Hilfsausgangs

Sicherheitshinweis **Anwendungen mit Hilfsausgängen sind für Sicherheitsanwendungen nicht zugelassen!**

4.3.5 Digitale Ausgänge I/Os (EAAx)

Die Erweiterungsbaugruppe verfügt über konfigurierbare sichere digitale I/Os (siehe Kapitel 3 Baugruppenübersicht). Als Ausgang parametriert wirkt dieser Anschluss als sicherer digitaler pp-schaltender Ausgang (EAAx).

4.3.5.1 Klassifizierung der I/Os (EAAx) bei Verwendung als Ausgang

Klassifizierung	Erreichbarer PL nach EN ISO 13849-1	Bemerkung
Statisch einkanalig 2)	PL c	Fehlererkennung bzw. Fehlerreaktion gemäß Kat. 2
Statisch zweikanalig 2)	PL d	Gleiche Gruppe 1): – Ansteuerung zeitversetzt auf PLC-Ebene – Fehleransatz Kurzschluss an beiden Ausgängen. Unterschiedliche Gruppe 1): – Keine weitere Anforderung notwendig
	PL e	Unterschiedliche Gruppe 1)
Dynamisch einkanalig 2), Dynamisch zweikanalig 2)	PL e	Keine weitere Anforderung notwendig

Hinweis: 1) Gruppe 1: EAA01 ... EAA06; Gruppe 2: EAA07 ... EAA10. 2) Statisch: kein Pulstest am Ausgang; Dynamisch: Pulstest am Ausgang mit tTest ≤ 500 µs.

4.3.5.2 Beschaltungsbeispiele für sichere digitale Ausgänge I/Os (EAAx)

Beschaltung einkanalig ohne Testung

Bei Verwendung von einem zweikanaligen Ausgang (EAAx) in Verbindung mit einer einkanaligen externen Beschaltung ohne externe Prüfung ist zu beachten, dass ein Verkleben eines oder mehrerer externer Kontakte von der Baugruppe nicht erkannt wird. Das nachfolgende Schaltbeispiel ist für Sicherheitsanwendungen nur eingeschränkt geeignet, es kann maximal PL b nach EN ISO 13849-1 erreicht werden!

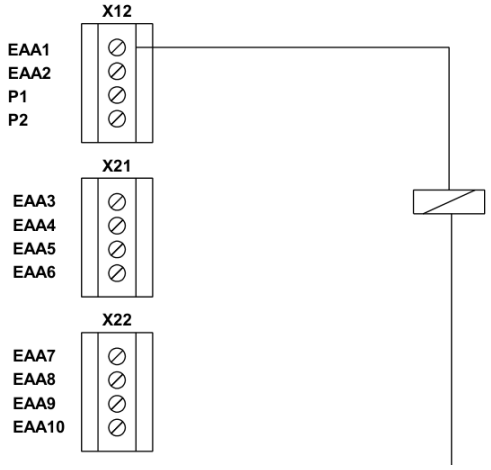


Bild: Zweikanaliger Ausgang mit einkanaliger Beschaltung ohne Testung

Sicherheitshinweis

– Nicht empfohlen für Sicherheitsanwendungen! Siehe hierzu auch Hinweise in der EN ISO 13849-1 zur Anwendung und erforderlichen Fehlerausschlüssen.

Beschaltung einkanalig mit Testung

Bei Verwendung von einem zweikanaligen Ausgang (EAAx) in Verbindung mit einer einkanaligen externen Beschaltung mit Testung sind insbesondere bei elektromechanischen Geräten zwangsgeführte Hilfskontakte bzw. für hydraulische oder pneumatische Komponenten Meldekontakte der Ventilstellung erforderlich. Weiter ist eine Melde-/Warneinrichtung zur Anzeige des Versagensfalls erforderlich. Die Melde-/Warneinrichtung muss unmittelbar dem Bediener die Gefahrensituation kenntlich machen. Der erzielbare PL ist stark von der Testrate abhängig, es kann maximal PL d nach EN ISO 13849-1 erreicht werden!

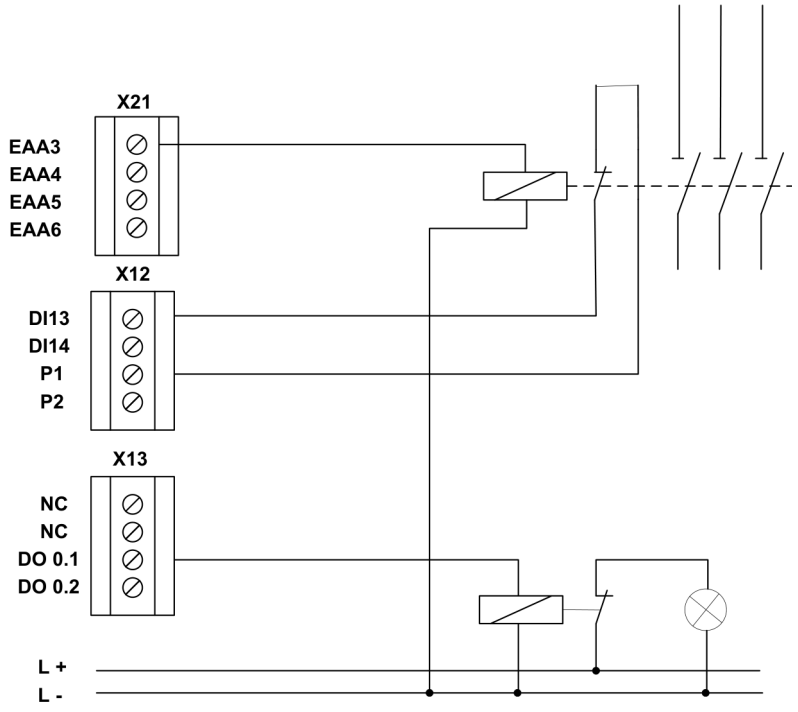


Bild: Zweikanaliger Ausgang mit einkanaliger Beschaltung mit Testung

Sicherheitshinweis

- Nur bedingt empfohlen für Sicherheitsanwendungen! Siehe hierzu auch Hinweise in der EN ISO 13849-1 zur Anwendung und erforderlichen Fehlerausschlüssen.
- Für PL c oder höher ist eine Testrate > 100 * Anforderungsrate erforderlich.
- Wird bei einem Test der Sicherheitsfunktion eine Gefahrensituation erkannt, so müssen geeignete Steuerungsmaßnahmen eingeleitet werden. Für PL d muss ein sicherer Zustand eingeleitet werden, der nicht aufgehoben werden darf, bis der Fehler beseitigt ist. Für PL bis einschließlich PL c ist es außerdem möglich, durch eine Warn- oder Meldeeinrichtung auf einen Fehler hinzuweisen, sofern ein sicherer Zustand nicht eingeleitet werden kann.

Beschaltung mit sicherem Abschaltkreis

Für Sicherheitsanwendungen ab PL c und höher nach EN ISO 13849-1. Die Ansteuerung des externen Kreises erfolgt direkt über einen zweikanaligen Ausgang. Der erzielbare PL nach EN ISO 13849-1 ist abhängig von der Verwendung der dynamischen Testung (siehe 4.3.2.1 DC) sowie dem PL des nachgeordneten Geräts.

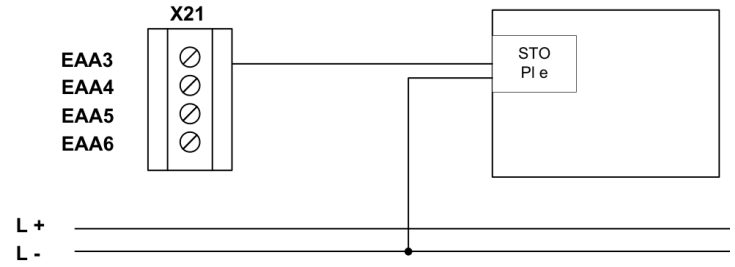


Bild: Zweikanaliger Ausgang in Verbindung mit Gerät mit geprüfter Abschaltung

Beschaltung in Verbindung mit zweikanaligem Abschaltkreis

Geeignet für PL d oder höher nach EN ISO 13849-1. Verwendung von einem Ausgang EAAx in Verbindung mit einer zweikanaligen externen Beschaltung mit Testung. Insbesondere sind hierfür bei elektromechanischen Geräten zwangsgeführte Hilfskontakte bzw. für hydraulische oder pneumatische Komponenten Meldekontakte der Ventilstellung erforderlich.

Der erzielbare PL ist von der Verwendung der dynamischen Testung sowie dem MTTFd-Wert des externen Kreises abhängig. Es kann maximal PL e nach EN ISO 13849-1 erreicht werden!

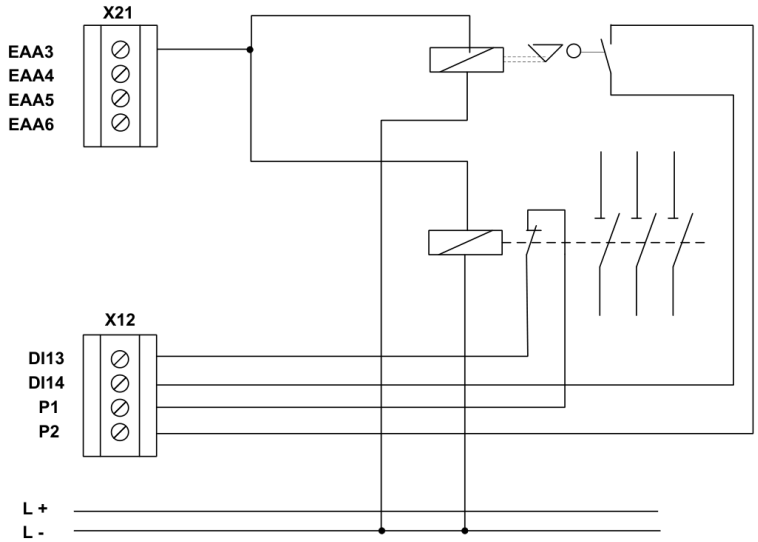


Bild: Zweikanaliger Ausgang in Verbindung mit zweikanaligem Abschaltkreis mit Testung

Redundanter zweikanaliger Ausgang

Geeignet für PL d oder höher nach EN ISO 13849-1. Verwendung von zwei Ausgängen EAAx in Verbindung mit einer zweikanaligen externen Beschaltung.

Beschaltung zweikanalig in gleicher Gruppe:

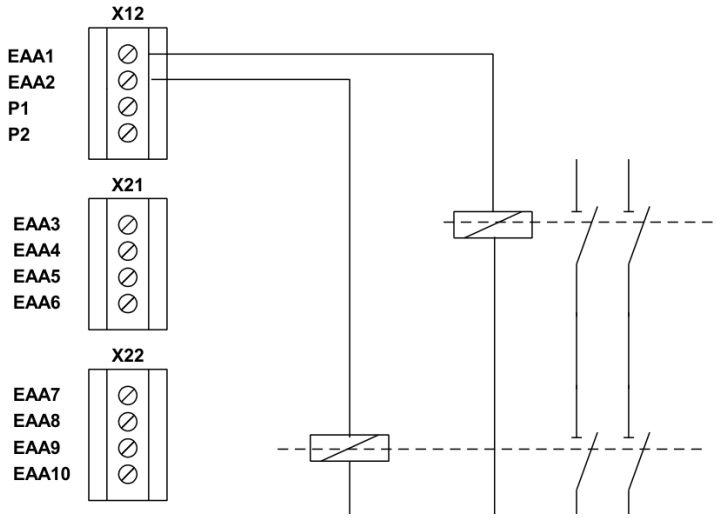


Bild: Redundante zweikanalige Ausgänge in gleicher Gruppe in Verbindung mit zweikanaligem Abschaltkreis

Beschaltung zweikanalig in unterschiedlichen Gruppen:

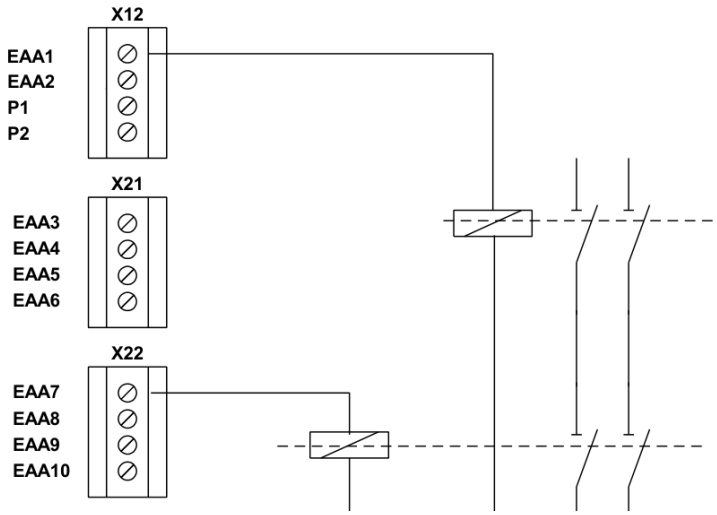


Bild: Redundante zweikanalige Ausgänge in unterschiedlichen Gruppen in Verbindung mit zweikanaligem Abschaltkreis

Sicherheitshinweis

- Für eine sicherheitstechnische Beurteilung des Teilsystems Ausgang sind bei Verwendung von externen Elementen im Abschaltkreis, z. B. zur Schaltverstärkung, deren Herstellerangaben (MTTFd, FIT-Zahlen, B10d-Wert etc.) heranzuziehen.
- Die in der Tabelle angeführten DC-Werte sind konservativ anzusetzen und die Einhaltung der Randbedingungen (siehe Tabelle unter „Anmerkungen“) zu gewährleisten.
- Fehlerausschlüsse sind nach den einschlägigen Normen zulässig. Die dabei angeführten Randbedingungen sind dauerhaft zu gewährleisten.
- Bei Verwendung von Elementen zur Schaltverstärkung in Sicherheitskreisen ist deren Funktion mittels geeigneter Rücklesekontakte etc. zu überwachen (siehe Schaltbeispiele). Geeignete Rücklesekontakte sind Kontakte, welche zwangsschaltend mit den Kontakten im Abschaltkreis verbunden sind.
- Die Schaltfähigkeit der externen Schaltverstärker ist zyklisch zu prüfen. Der Zeitraum zwischen 2 Prüfungen ist nach Anforderung durch die Applikation festzulegen und durch geeignete Maßnahmen sicherzustellen. Geeignete Maßnahmen können organisatorischer (Aus- und Einschalten bei Schichtbeginn etc.) oder technischer (automatisches, zyklisches Schalten) Natur sein.

4.3.5.3 Übersicht erreichbarer PL für digitale Sicherheitsausgänge

Ausgang ESMD	Aktuator / externer Abschaltkreis	Kat.	DC		MTTFd Aktuator	PL	Randbedingung	Fehler-ausschluss
Einkanalig ohne dynamischen Ausgangstest K1, K2, EAAx	Einkanalig Schütz, Ventil, Bremse etc. ohne direkte Rückführung zur Diagnose	Kat. B	0 %		Mittel	B	Schütz und nachgeordnete Aktuatoren geeignet ausgelegt für Sicherheitsanwendung	
	Einkanalig Schütz, Ventil, Bremse etc. mit überwachtem zwangsgeführten Hilfskontakt	Kat. 2	60-90 %	Abhängig von Schalthäufigkeit	Mittel	B	Hilfsausgang erforderlich zur Warnung bei erkannter Fehlfunktion. Schütz und nachgeordnete Aktuatoren geeignet ausgelegt für Sicherheitsanwendung	
					Hoch	C	Wie vor	
						D	Wie vor. DC = 90 % durch in Bezug auf die Applikation ausreichend hohe Testrate	
Einkanalig ohne dynamischen Ausgangstest K1 od. K2 oder Einkanalig	Zweikanalig Schütz, Ventil, Bremse etc. mit direkter Rückführung zur Diagnose mind. in einem Kanal oder Aktuator einkanalig angesteuert mit Sicherheitsfunktion Kat. 3 (z. B. STO)	Kat. 2	90 %	Überwachung nur in einem externen Abschaltkreis	Mittel	c	Hilfsausgang erforderlich zur Warnung bei erkannter Fehlfunktion. Schütz und nachgeordnete Aktuatoren geeignet ausgelegt für Sicherheitsanwendung	Kurzschluss an externer Ansteuerung
					Hoch	d		

Ausgang ESMD	Aktuator / externer Abschaltkreis	Kat.	DC		MTTFd Aktuator	PL	Randbedingung	Fehler-ausschluss
Einkanalig ohne dynamischen Ausgangstest EAA01..EAA10	Zweikanalig Schütz, Ventil, Bremse etc. mit direkter Rückführung zur Diagnose mind. in einem Kanal oder Aktuator einkanalig angesteuert mit Sicherheitsfunktion Kat. 3 (z. B. STO)	Kat. 3	90 %	Überwachung nur in einem externen Abschaltkreis	Mittel od. Hoch	d	Schütz und nachgeordnete Aktuatoren geeignet ausgelegt für Sicherheitsanwendung	Kurzschluss an externer Ansteuerung
Einkanalig mit dynamischen Ausgangstest EAA01..EAA10	Zweikanalig Schütz, Ventil, Bremse etc. mit direkter Rückführung zur Diagnose in beiden Kanälen oder Aktuator mit Sicherheitsfunktion Kat. 4 (z. B. STO)	Kat. 4	99 %	Überwachung in beiden externen Abschaltkreisen	Hoch	e	Schütz und nachgeordnete Aktuatoren geeignet ausgelegt für Sicherheitsanwendung. Überwachung elektromechanischer Komponenten durch zwangsgeführte Schalter, Stellungsüberwachung von Schaltventilen etc.	

Ausgang ESMD	Aktuator / externer Abschaltkreis	Kat.	DC		MTTFd Aktuator	PL	Randbedingung	Fehler-ausschluss
Zweikanalig ohne dynamischen Ausgangstest K1 und K2, 2 × EAA01..EAA10	Zweikanalig Schütz, Ventil, Bremse etc. mit direkter Rückführung zur Diagnose mind. in einem Kanal oder Aktuator mit Sicherheitsfunktion Kat. 4 (z. B. STO)	Kat. 3	90 %	Überwachung in beiden externen Abschaltkreisen	Mittel od. Hoch	d	Schütz und nachgeordnete Aktuatoren geeignet ausgelegt für Sicherheitsanwendung. Überwachung elektromechanischer Komponenten durch zwangsgeführte Schalter, Stellungsüberwachung von Schaltventilen etc.. Ausgänge EAA1..10 je 1 × aus unterschiedlichen Gruppen (jeweils Gruppen von 6/4 zusammenhängende EAA-Ports, z. B. EAA1..6, EAA7..10) oder Ansteuerung zeitversetzt auf PLC-Ebene	Kurzschluss an externer Ansteuerung

Ausgang ESMD	Aktuator / externer Abschaltkreis	Kat.	DC		MTTFd Aktuator	PL	Randbedingung	Fehler-ausschluss
Zweikanalig mit dynamischen Ausgangstest 2 × EAA01..EAA10	Zweikanalig Schütz, Ventil, Bremse etc. mit direkter Rückführung zur Diagnose in beiden Kanälen oder Aktuator mit Sicherheitsfunktion Kat. 4 (z. B. STO)	Kat. 4	99 %	Überwachung in beiden externen Abschaltkreisen	Hoch	e	Schütz und nachgeordnete Aktuatoren geeignet ausgelegt für Sicherheitsanwendung. Überwachung elektromechanischer Komponenten durch zwangsgeführte Schalter, Stellungsüberwachung von Schaltventilen etc.. Für Applikationen mit häufiger Anforderung der Sicherheitsabschaltung sollte in kürzeren Zeitintervallen, z. B. bei Schichtbeginn, 1 × pro Woche getestet werden. Ein Test sollte jedoch mindestens zyklisch 1 × pro Jahr erfolgen.	Kurzschluss an externer Ansteuerung in beiden Kanälen

PL: erreichbarer PL nach EN ISO 13849-1; Kat.: Kategorie nach EN ISO 13849-1.

5 Anschluss und Installation

5.1 Allgemeine Installationshinweise

Bei der Installation unbedingt die Sicherheitshinweise beachten!

Schutzart IP20

- Führen Sie alle Signalleitungen für die Anschaltung der digitalen Eingänge und Kontaktüberwachungen getrennt.
- Trennen Sie in jedem Fall 230-VAC-Spannungen von Niederspannungsleitungen, falls diese Spannungen im Zusammenhang mit der Applikation verwendet werden.

Die Kabellängen für die digitalen Eingänge und Ausgänge und sämtlicher Sensorik dürfen im Regelfall 30 m nicht überschreiten.

Falls die Kabellängen einen Wert von 30 m überschreiten, sind geeignete Maßnahmen zum Fehlerausschluss von unzulässiger Überspannung zu treffen. Geeignete Maßnahmen sind beispielsweise Blitzschutz für Außenleitungen, Überspannungsschutz der Anlage im Innenbereich, geschützte Kabelverlegung.

Maßnahmen zur elektromagnetischen Verträglichkeit (EMV)

Die Baugruppe ist für den Einsatz im Antriebsumfeld vorgesehen und erfüllt die oben genannten EMV-Anforderungen.

Weiterhin wird vorausgesetzt, dass die elektromagnetische Verträglichkeit des Gesamtsystems durch einschlägig bekannte Maßnahmen sichergestellt wird.

Sicherheitshinweis

- Es ist sicherzustellen, dass die Spannungsversorgungsleitungen der Baugruppe und „schaltenden Leitungen“ des Stromrichters getrennt voneinander verlegt werden.
- Signalleitungen und Leistungsleitungen der Stromrichter sind in getrennten Kabelkanälen zu führen. Der Abstand der Kabelkanäle sollte mindestens 10 mm betragen.
- Zum Anschluss der Positions- und Geschwindigkeitssensoren sind ausschließlich geschirmte Leitungen zu verwenden. Das Kabel zur Übertragung der Signale muss für RS-485-Standard geeignet sein (paarweise verdrillte Leitungen).
- Das richtige Auflegen des Schirms in den 9-poligen SUB-D-Steckern der Positions- und Geschwindigkeitssensoren ist zu beachten. Es sind nur metallische oder metallisierte Stecker zugelassen.
- Die Schirmung auf der Sensorseite muss nach einschlägig bekannten Methoden ausgeführt sein.
- Es ist auf eine EMV-gemäße Installation der Stromrichtertechnik im Umfeld der Baugruppe zu achten. Besondere Beachtung sollte die Kabelführung und die Verarbeitung der Schirmung für die Motorleitung und den Anschluss des Bremswiderstandes finden. Hier müssen die Installationsrichtlinien des Stromrichtergeräteherstellers unbedingt Beachtung finden.
- Alle Schütze im Umfeld des Umrichters müssen mit entsprechender Schutzbeschaltung ausgerüstet sein.
- Es sind geeignete Maßnahmen zum Schutz gegen Überspannungen zu treffen.

5.2 Einbau und Montage der Baugruppe

Der Einbau der Baugruppe erfolgt ausschließlich in Schaltschränken, die mindestens der Schutzart IP54 genügen.

Die Baugruppen müssen senkrecht auf einer Hutschiene befestigt werden.

Bei den Lüftungsschlitzen muss ein Freiraum nach oben und unten von 30 mm eingehalten werden. Eine Aneinanderreihung von Erweiterungsbaugruppen ist erlaubt. Bei benachbarten Geräten, die eine Abwärme erzeugen können, muss ein Abstand von 20 mm eingehalten werden.

Hinweis Bei Benutzung in nicht geschlossenen Räumen muss sichergestellt sein, dass die Umweltbedingungen der einzelnen Baugruppen (siehe technische Daten) eingehalten werden.

5.3 Montage Rückwandbus

Es besteht die Möglichkeit, mehrere Baugruppen (ESMD, Erweiterungsbaugruppe) auf einer Hutschiene in Verbindung mit dem Rückwandbus zu montieren. Diese Baugruppen können mit einer Kommunikationserweiterung kombiniert werden. In diesem Fall muss der Rückwandbus bei der Bestellung durch den Hersteller konfiguriert und entsprechend der vorliegenden Applikation geliefert werden.

Der Rückwandbus besteht aus einem 5-poligen Steckverbinder mit Federkontakten. Standardmäßig sind bei den Steckverbindern alle 5 Kontakte bestückt. In diesem Fall besitzt das Bauteil keine besondere Kennzeichnung. Bei einer zweiten Variante des Steckverbinders sind lediglich 3 Kontakte bestückt.

Anmerkung Erweiterungsbaugruppen verfügen über kein eigenes Netzteil und sind auf eine DC-Versorgung über den Rückwandbus angewiesen. Die Basisbaugruppe ESMD verfügt über ein verstärktes Netzteil und speist immer auf den Rückwandbus ein.

Es gibt zwei Arten von Rückwandbusverbindern:

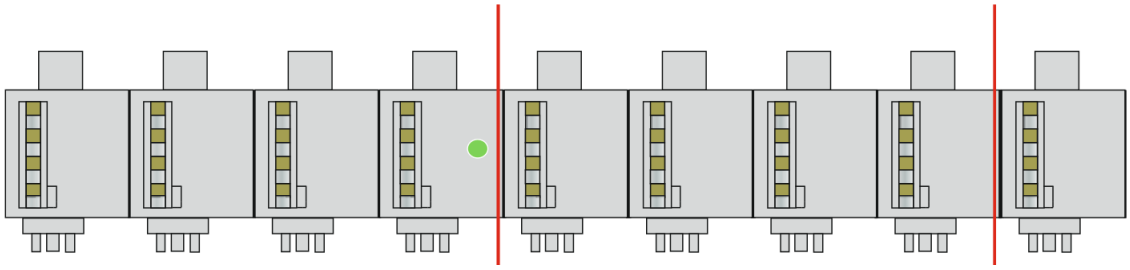
- Standardausführung (alle Kontakte sind vorhanden)
- Unterbrecherausführung (die beiden spannungsführenden Leiter sind nicht vorhanden; mit einem grünen Punkt gekennzeichnet)

Verwendung des Rückwandbusverbinders in Standardausführung: Der Rückwandbusverbinder in Standardausführung kann nur in Verbindung mit Erweiterungsbaugruppen ohne eigene Spannungsversorgung installiert werden. Eine Verbindung mehrerer Standalone-Baugruppen ist nicht möglich.

Verwendung des Rückwandbusverbinders in Unterbrecherausführung: Der Rückwandbusverbinder in Unterbrecherausführung wird immer dann eingesetzt, wenn mehrere Basisbaugruppen mit Erweiterungsbaugruppen kombiniert werden. Dies wird unter dem nachfolgenden Punkt Anordnungsbeispiele noch einmal anschaulich dargestellt.

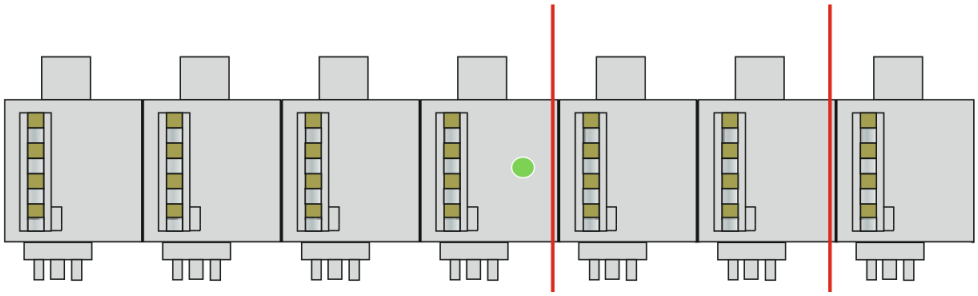
Anordnungsbeispiele

Hinweis Die Anordnungsbeispiele dienen nur zur Veranschaulichung und können mechanisch von der tatsächlichen Anordnung abweichen.



ESMD + ESMD + Kommunikationsbaugruppe (von links: Kommunikationsbaugruppe, ESMD, ESMD)

Zwischen der letzten Baugruppe ESMD und der Kommunikationsbaugruppe ist kein Rückwandbusverbinder in Unterbrecherausführung angebracht, da für die Kommunikationsbaugruppe die Spannungsversorgung über den Rückwandbus eingespeist wird.



ESMD + Erweiterungsbaugruppe + Kommunikationsbaugruppe (von links: ESMD, Erweiterungsbaugruppe, Kommunikationsbaugruppe)

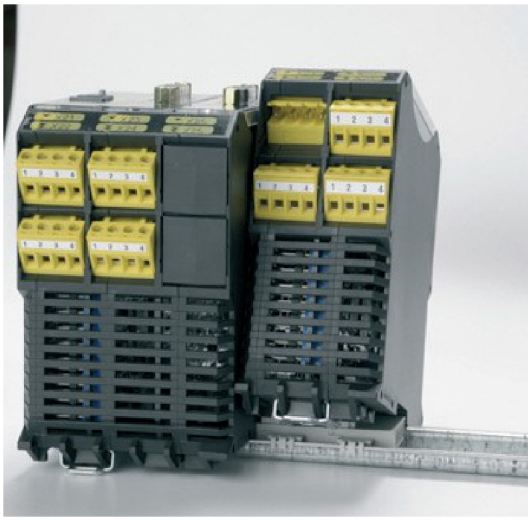
Zwischen der Erweiterungsbaugruppe und der Kommunikationsbaugruppe ist kein Rückwandbusverbinder in Unterbrecherausführung angebracht, da für die Kommunikationsbaugruppe die Spannungsversorgung über den Rückwandbus eingespeist wird.

5.4 Montage der Baugruppen

Die Montage der Baugruppen erfolgt auf C-Normschienen mittels Schnapp-Klinke.

5.4.1 Montage auf C-Schiene

Die Geräte werden schräg von oben in die Schiene eingeführt und nach unten eingeschnappt. Die Demontage erfolgt mittels eines Schraubendrehers, welcher in den Schlitz der nach unten herausgeführten Klinke eingeführt und anschließend nach oben bewegt wird.



5.4.2 Montage auf Rückwandbus

Nach Montage des Rückwandbusses kann die Gerätemontage erfolgen. Die Baugruppe hierzu von schräg oben in Steckverbindung einführen und auf der C-Schiene aufschnappen.



Baugruppe von schräg oben einführen



Nach unten auf der C-Schiene aufschnappen

Die Rückwandsteckverbindung kann nachträglich erweitert werden. Die Systemkonfiguration kann somit um zusätzliche Baugruppen erweitert werden.



Rückwandbuselement in C-Schiene einschnappen und durch Verschieben seitlich in Gegenstück einführen

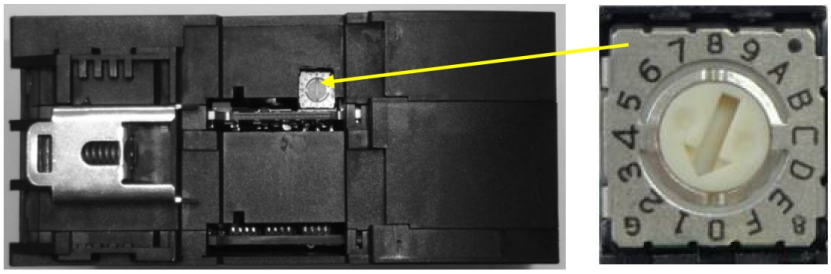
5.4.3 Installation I/O-Erweiterungen

Hinweis Max. zwei Erweiterungsbaugruppen können mit einem Basisgerät betrieben werden.

Physikalische Adresskonfiguration der Slavebaugruppen (zentral)

Auf den Erweiterungsbaugruppen muss die Busadresse mit Hilfe des Adressschalters eingestellt werden.

Die Einstellung erfolgt auf der Rückseite der Baugruppe.

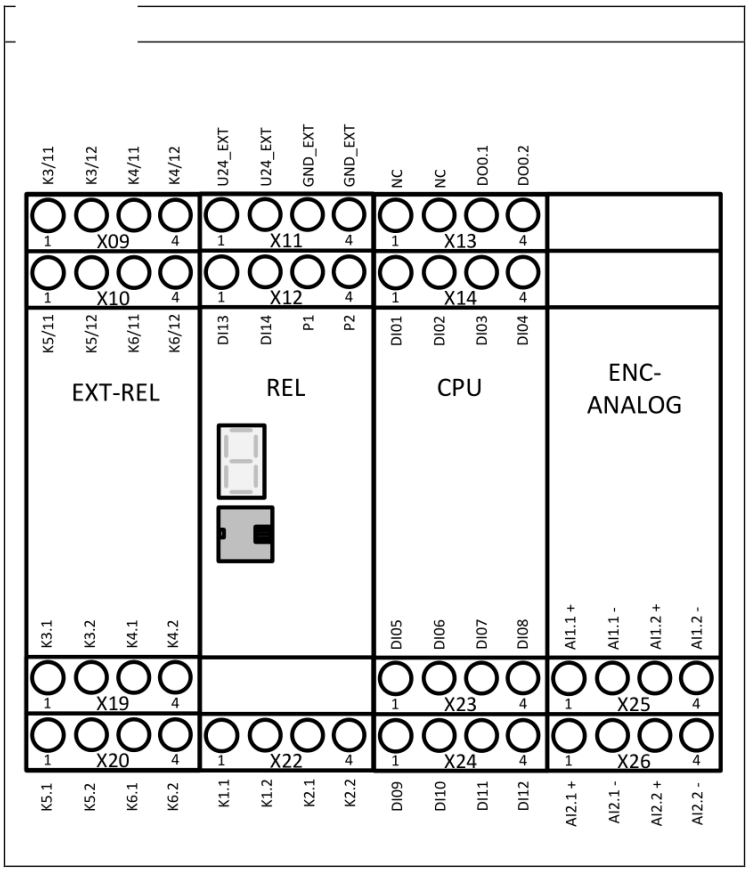


Hinweis

- Adressbereich der Erweiterungsbaugruppe von 1 ... 15.
- Adresse „0“ ist für das Basisgerät reserviert.

5.5 Klemmenbelegung

5.5.1 Klemmenbelegung ESMD

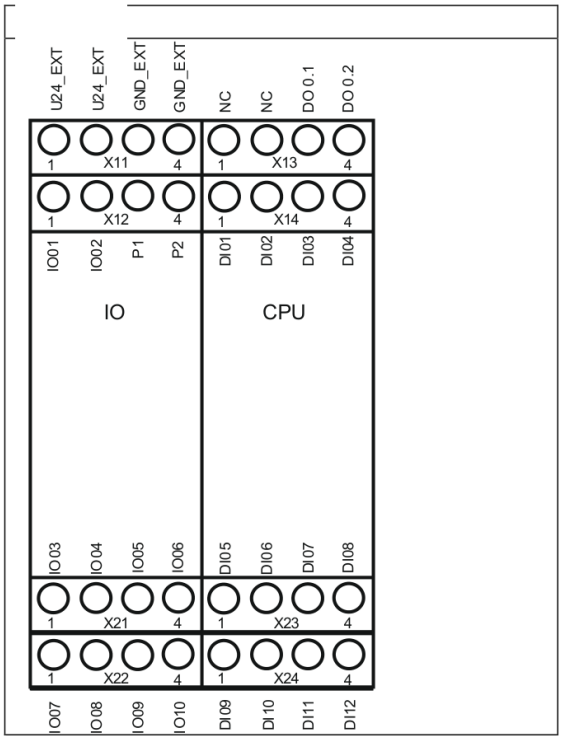


Klemmenlage ESMD

Einheit	Klemme	Pin	Beschreibung
EXT-REL	X09	1 – K3/11, 2 – K3/12	Rücklesekontakt Relais 3
		3 – K4/11, 4 – K4/12	Rücklesekontakt Relais 4
	X10	1 – K5/11, 2 – K5/12	Rücklesekontakt Relais 5
		3 – K6/11, 4 – K6/12	Rücklesekontakt Relais 6
	X19	1 – K3.1, 2 – K3.2	Sicherer Relaisausgang
		3 – K4.1, 4 – K4.2	Sicherer Relaisausgang
	X20	1 – K5.1, 2 – K5.2	Sicherer Relaisausgang
		3 – K6.1, 4 – K6.2	Sicherer Relaisausgang
REL	X11	1 – U24_EXT, 2 – U24_EXT	Spannungsversorgung Gerät +24 VDC
		3 – GND_EXT, 4 – GND_EXT	Spannungsversorgung Gerät 0 VDC
	X12	1 – DI13, 2 – DI14	Sichere digitale Eingänge
		3 – P1, 4 – P2	Pulsausgänge
	X22	1 – K1.1, 2 – K1.2	Sicherer Relaisausgang
		3 – K2.1, 4 – K2.2	Sicherer Relaisausgang
CPU	X13	1 – NC, 2 – NC	Keine Funktion
		3 – DO 0.1, 4 – DO 0.2	Hilfsausgänge
	X14	1 – DI1, 2 – DI2, 3 – DI3, 4 – DI4	Sichere digitale Eingänge
	X23	1 – DI5, 2 – DI6, 3 – DI7, 4 – DI8	Sichere digitale Eingänge
	X24	1 – DI9, 2 – DI10, 3 – DI11, 4 – DI12	Sichere digitale Eingänge

Einheit	Klemme	Pin	Beschreibung
ENC-ANALOG	X25	1 – AI 1.1+, 2 – AI 1.1–, 3 – AI 1.2+, 4 – AI 1.2–	Sicherer analoger Eingang
	X26	1 – AI 2.1+, 2 – AI 2.1–, 3 – AI 2.2+, 4 – AI 2.2–	Sicherer analoger Eingang

5.5.2 Klemmenbelegung Erweiterungsbaugruppe



Klemmenlage Erweiterungsbaugruppe

Einheit	Klemme	Pin	Beschreibung
IO	X11	1 – U24_EXT, 2 – U24_EXT	Spannungsversorgung Gerät +24 VDC Ausgänge
		3 – GND_EXT, 4 – GND_EXT	Spannungsversorgung Gerät 0 VDC
	X12	1 – IO01, 2 – IO02	Sichere digitale Ein-, Ausgänge pp-schaltend
		3 – P1, 4 – P2	Pulsausgänge
	X21	1 – IO03, 2 – IO04, 3 – IO05, 4 – IO06	Sichere digitale Ein-, Ausgänge pp-schaltend
	X22	1 – IO07, 2 – IO08, 3 – IO09, 4 – IO10	Sichere digitale Ein-, Ausgänge pp-schaltend
CPU	X13	1 – NC, 2 – NC	Keine Funktion
		3 – DO0.1, 4 – DO0.2	Hilfsausgänge
	X14	1 – DI1, 2 – DI2, 3 – DI3, 4 – DI4	Sichere digitale Eingänge
	X23	1 – DI5, 2 – DI6, 3 – DI7, 4 – DI8	Sichere digitale Eingänge
	X24	1 – DI9, 2 – DI10, 3 – DI11, 4 – DI12	Sichere digitale Eingänge

5.5.3 Klemmenbelegung Kommunikationsbaugruppen

Die Klemmenbelegungen der einzelnen Kommunikationsbaugruppen entnehmen Sie bitte den entsprechenden Installationshandbüchern.

5.6 Externe 24-VDC-Spannungsversorgung

Die Baugruppe benötigt eine Spannungsversorgung von 24 VDC (siehe hierzu SELV oder PELV, EN 50178). Bei der Projektierung und Installation des vorgesehenen Netzgerätes sind folgende Randbedingungen zu beachten:

Die minimale und maximale Toleranz der Versorgungsspannung muss unbedingt beachtet werden.

Nominalspannung	DC 24 V
Minimal: 24 VDC – 15 %	20,4 VDC
Maximal: 24 VDC + 20 %	28,8 VDC

Um eine möglichst kleine Restwelligkeit der Versorgungsspannung zu erreichen, wird der Einsatz eines 3-phasigen Netzgerätes oder eines elektronisch geregelten Gerätes empfohlen. Das Netzgerät muss den Anforderungen nach EN 61000-4-11 genügen (Spannungseinbruch).

Die Auslegung der Verbindungskabel muss entsprechend der örtlichen Vorschriften erfolgen.

Die Fremdspannungsfestigkeit der Baugruppe beträgt 32 VDC (abgesichert durch Suppressordioden am Eingang).

Sicherheitshinweis

– Die Baugruppe ist einzeln extern mit einer Vorsicherung von 3,15 A (min. 30 VDC) abzusichern. Die Sicherung muss in der Nähe der Klemmen angeordnet sein.

Empfohlener Sicherungstyp: 3,15 A-Leistungsschutzschalter (Klasse B) oder Schmelzsicherung (träge).

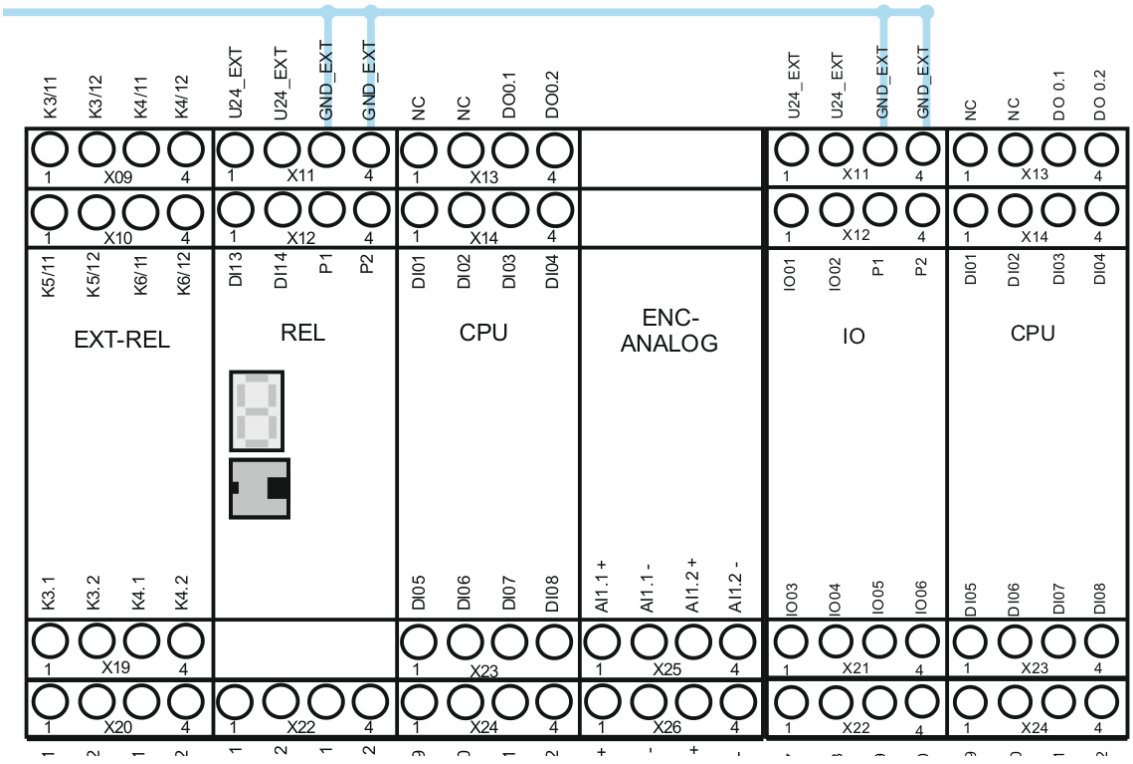
Anmerkung In jedem Fall muss die sichere galvanische Trennung zum 230-VAC- bzw. 400-VAC-Netz gewährleistet werden. Hierzu sind Netzgeräte auszuwählen, die den Vorschriften DIN VDE 0551, EN 60 742 und DIN VDE 0160 entsprechen. Neben der Auswahl des geeigneten Gerätes ist auf einen Potentialausgleich zwischen PE und 0 VDC auf der Sekundärseite zu achten.

Sicherheitshinweis

– Alle GND-Anschlüsse der Geräte, die mit den Eingängen der Baugruppe verbunden sind, müssen mit dem GND der Baugruppe (Spannungsversorgung) verbunden werden.

Eingänge der Baugruppe sind: Digitaleingänge, digitale I/Os, Analogeingänge, Geberanschlüsse.

Anmerkung Die Anschlüsse GND_ENC und AIN sind nicht intern mit GND verbunden!



GND-Verbindung ESMD und Erweiterungsbaugruppe

5.7 Anschluss der Digitaleingänge

Die Baugruppe verfügt über 14 (ESMD) bzw. 12 (Erweiterungsbaugruppe) sichere digitale Eingänge. Diese sind zum Anschluss von ein- oder zweikanaligen Signalen mit und ohne Pulse bzw. ohne Querschlussprüfung geeignet.

Die angeschlossenen Signale müssen einen „High"-Pegel von 24 VDC (+15 VDC ... +30 VDC) aufweisen und einen „Low"-Pegel von (–3 VDC ... +5 VDC, Typ 1 nach EN 61131-2). Die Eingänge sind intern mit Eingangsfiltern versehen.

Eine geräteinterne Diagnosefunktion prüft zyklisch die korrekte Funktion der Eingänge inklusive der Eingangsfilter. Ein erkannter Fehler versetzt die Baugruppe in den Alarmzustand. Gleichzeitig werden alle Ausgänge der Baugruppe passiviert.

Neben den eigentlichen Signaleingängen stellt die Baugruppe zwei Pulsausgänge P1 und P2 zur Verfügung. Bei den Pulsausgängen handelt es sich um schaltende 24-VDC-Ausgänge.

Die Pulsausgänge sind ausschließlich für die Überwachung der digitalen Eingänge (DI1 ... DI14) vorgesehen und können für keine anderen Funktionen innerhalb der Applikation Verwendung finden.

Die Schaltfrequenz beträgt 125 Hz für jeden Ausgang. Bei der Projektierung ist zu beachten, dass die Ausgänge maximal mit einem Gesamtstrom von 250 mA belastet werden dürfen.

Weiterhin können zugelassene OSSD-Ausgänge ohne Einschränkung an die Eingänge DI01 – DI14 angeschlossen werden.

Bei einkanaliger Verwendung der Eingänge ist das erreichbare Sicherheitsniveau auf SIL 2 bzw. PL d eingeschränkt, wenn in regelmäßigen Abständen eine Anforderung der Sicherheitsfunktion erfolgt.

Grundsätzlich ist eine sicherheitstechnische Verwendung der Eingänge nur in Verbindung mit den Pulsausgängen vorgesehen.

Werden die Pulsausgänge nicht verwendet, muss durch externe Maßnahmen, insbesondere eine geeignete Kabelführung, ein Kurzschluss in der externen Verdrahtung zwischen verschiedenen Eingängen und gegen die Versorgungsspannung der Baugruppe ausgeschlossen werden.

Jeder Eingang der Baugruppe kann individuell für folgende Signalquellen konfiguriert werden:

- Eingang wird Puls P1 zugeordnet
- Eingang wird Puls P2 zugeordnet
- Eingang wird 24 VDC Dauerspannung zugeordnet

5.8 Anschluss Analogeingänge

Bei den Ausführungen mit Analogverarbeitung können max. 2 Analogsignale sicher verarbeitet werden. Die Analogeingänge können wie folgt beschaltet werden:

	min.	max.
Spannung	–10 VDC	+10 VDC

Hinweis Die Baugruppen können wahlweise mit Spannungs- und/oder Stromeingängen bestellt werden.

Sicherheitshinweis

- Der GND-Anschluss AIN muss mit dem GND der Baugruppe verbunden werden!

6 Reaktionszeiten des ESMD

Die Reaktionszeit ist eine wichtige sicherheitstechnische Eigenschaft und für jede Applikation / applikative Sicherheitsfunktion zu betrachten. Im nachfolgenden Kapitel sind die Reaktionszeiten für einzelne Funktionen, u. U. auch in Abhängigkeit von weiteren Parametern, gelistet. Sind diese Angaben für eine spezifische Applikation nicht ausreichend, ist das tatsächliche Zeitverhalten gegen das Sollverhalten durch gesonderte Messungen zu validieren. Dies betrifft insbesondere auch die Verwendung von Filterfunktionen.

Sicherheitshinweis

- Die Reaktionszeiten sind für jede applikative Sicherheitsfunktion im Sollverhalten festzulegen und gegen den tatsächlichen Wert mit Hilfe der nachstehenden Angaben zu vergleichen.
- Bei Verwendung von Filterfunktionen ist besondere Vorsicht geboten. Je nach Filterlänge / -zeit kann es zu einer erheblichen Verlängerung der Reaktionszeit kommen, die bei der sicherheitstechnischen Auslegung mit zu betrachten ist.
- Bei besonders kritischen Aufgabenstellungen ist das Zeitverhalten durch Messungen zu validieren.
- Bei Geräteanlauf / Alarm- bzw. Fehler-Reset können u. U. (abhängig vom Applikationsprogramm) die Ausgänge für die Dauer der Reaktionszeit aktiv werden. Dies ist bei der Planung der Sicherheitsfunktionen zu berücksichtigen.
- Bei Verwendung von sicheren Feldbusanbindungen (z. B. PROFIsafe, FSoE) ist die Systemlaufzeit (Watchdog) mit einzuberechnen.

6.1 Reaktionszeiten im Standardbetrieb

Grundlage der Berechnung von Reaktionszeiten ist die Zykluszeit des Systems. Diese beträgt im Betrieb **T_zyklus = 8 ms**. Die angegebenen Reaktionszeiten entsprechen der jeweiligen Maximallaufzeit für den konkreten Anwendungsfall innerhalb der Baugruppe. Je nach Anwendung müssen noch weitere, applikationsabhängige Reaktionszeiten der verwendeten Sensorik und Aktuatoren hinzugerechnet werden, um die Gesamtlaufzeit zu erhalten.

Funktion	Reaktionszeit [ms]	Erläuterung
Aktivierung einer Überwachungsfunktion durch ENABLE mit anschließender Abschaltung über digitalen Ausgang	24 *)	Aktivierung einer Überwachungsfunktion durch das ENABLE-Signal.
Aktivierung einer Überwachungsfunktion durch ENABLE mit anschließender Abschaltung über Sicherheitsrelais	47 *)	Aktivierung einer Überwachungsfunktion durch das ENABLE-Signal.
Reaktion einer bereits aktivierten Überwachungsfunktion inklusive PLC-Bearbeitung bei Positions- und Geschwindigkeitsverarbeitung über digitalen Ausgang	16 *)	Bei einer bereits über ENABLE aktivierten Überwachungsfunktion benötigt die Baugruppe einen Zyklus, um den aktuellen Geschwindigkeitswert zu berechnen. Im nächsten Zyklus wird nach Berechnung der Überwachungsfunktion die Information durch die PLC weiterverarbeitet und ausgegeben, d. h. nach implementierter Logik führt dies z. B. zum Schalten eines Ausgangs.
Reaktion einer bereits aktivierten Überwachungsfunktion inklusive PLC-Bearbeitung bei Positions- und Geschwindigkeitsverarbeitung über Sicherheitsrelais	39 *)	Bei einer bereits über ENABLE aktivierten Überwachungsfunktion benötigt die Baugruppe einen Zyklus, um den aktuellen Geschwindigkeitswert zu berechnen. Im nächsten Zyklus wird nach Berechnung der Überwachungsfunktion die Information durch die PLC weiterverarbeitet und ausgegeben, d. h. nach implementierter Logik führt dies z. B. zum Schalten eines Ausgangs.
Aktivierung digitaler Ausgang über digitalen Eingang	16	Aktivierung eines Eingangs und Schalten des Ausgangs
Aktivierung Ausgang Relais über digitalen Eingang	26	Aktivierung eines Eingangs und Schalten des Ausgangs
Deaktivierung digitaler Ausgang über digitalen Eingang	16	Deaktivierung eines Eingangs und damit Deaktivierung des Ausgangs
Deaktivierung Ausgang Relais über digitalen Eingang	47	Deaktivierung eines Eingangs und damit Deaktivierung des Ausgangs

Funktion	Reaktionszeit [ms]	Erläuterung
Mittelwertfilter (Einstellung siehe Geberdialog der Programmiersoftware)	0 - 64	Gruppenlaufzeit des Mittelwertbildners. Diese Laufzeit wirkt nur auf Überwachungsfunktionen in Zusammenhang mit Position / Geschwindigkeit / Beschleunigung, jedoch nicht auf die Logikverarbeitung.
Analogfilter: 1 (2 Hz) · 2 (2 Hz) · 3 (2 Hz) · 4 (4 Hz) · 5 (6 Hz) · 6 (8 Hz) · 7 (10 Hz) · 8 (20 Hz)	760 · 760 · 760 · 512 · 268 · 143 · 86 · 56	Das Analogfilter wirkt nur auf die sicheren Analogeingänge aller Baugruppen mit Analogvarianten. Reaktionszeiten der Analogeingangsfilter bezogen auf die Eingangsfrequenz

Hinweis: *) Bei Verwendung eines Mittelwertfilters muss dessen Reaktionszeit aufaddiert werden.

6.2 Reaktionszeiten für FAST_CHANNEL

FAST_CHANNEL bezeichnet eine Eigenschaft der Baugruppe, auf Geschwindigkeitsanforderungen schneller zu reagieren, als dies mit der Bearbeitung des Sicherheitsprogramms im Normalzyklus (= 8 ms) möglich ist. Die Abtastzeit des **FAST_CHANNEL** beträgt 2 ms.

Folgende Reaktionszeiten können angegeben werden: 4 ms (Worst-Case-Bedingung)

Sicherheitshinweis

- Bei Verwendung des FAST_CHANNEL ist zu beachten, dass eine Abschaltung in der oben angegebenen Zeit für eine vorgegebene Geschwindigkeitsschwelle nur dann stattfinden kann, falls die Sensorinformation über eine ausreichende Auflösung verfügt. Die kleinste auflösbare Schaltschwelle des FAST_CHANNEL benötigt mindestens 2 Flankenwechsel am jeweils gewählten Sensorsystem innerhalb einer Zeit von 2 ms.
- Diese Funktion ist nur in Verwendung mit sicheren Halbleiterausgängen möglich.
- Der FAST_CHANNEL darf nicht auf SSI-Listener wirken.

6.3 Reaktionszeiten für Fehlerdistanzüberwachung

Für die Berechnung der Worst-Case-Bedingung ergibt sich folgendes Berechnungsschema:

Größe	Zeichen
Systemgeschwindigkeit zum Abtastzeitpunkt	V(t)
Systemgeschwindigkeit bei Reaktion der Baugruppe	VA
Schwellwert für Überwachung (SLS oder SCA)	VS = konstant für alle t
Parametrierter Filterwert	XF = konstant für alle t
Maximal mögliche Beschleunigung der Applikation	aF = konstant für alle t
Verzögerung nach Abschalten	aV = konstant für alle t
Abtastzeitpunkt für Eintritt eines Worst-Case-Ereignisses	TFehler
Reaktionszeit des Systems	tReakt

Für die Worst-Case-Betrachtung wird angenommen, dass sich der Antrieb zunächst mit einer Geschwindigkeit v(k) genau auf der parametrierten Schwelle v0 bewegt und dann mit maximal möglichem Wert a0 beschleunigt.

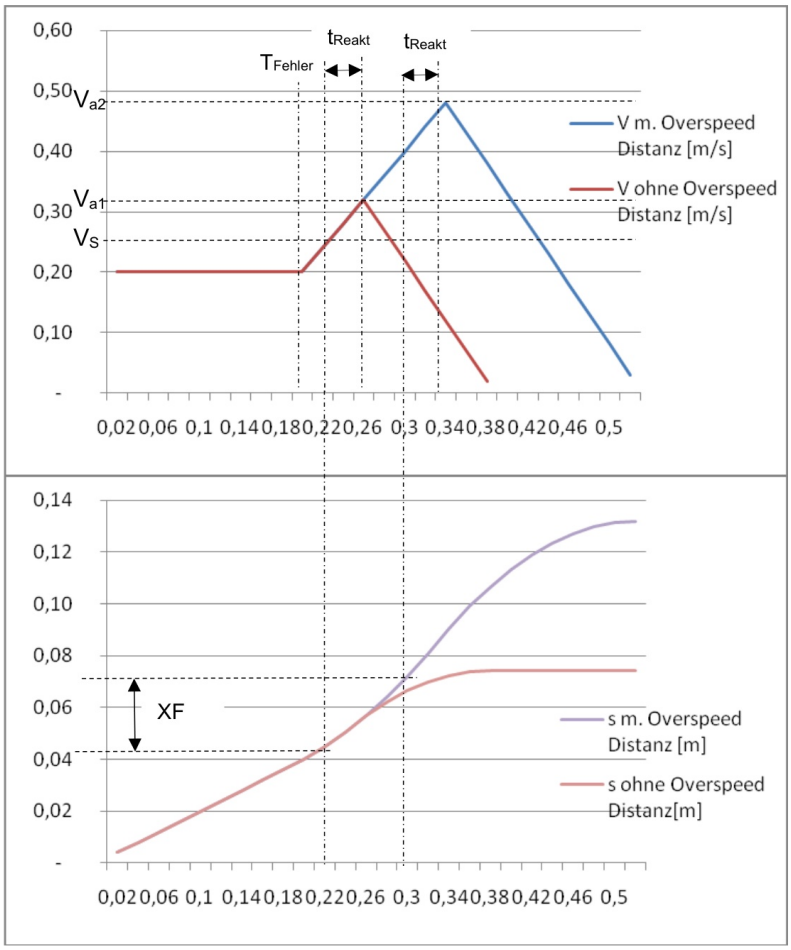


Diagramm: Verhalten des Antriebs mit / ohne Overspeed-Distanz

Für den Verlauf V und s ergeben sich **ohne** Overspeed-Distanz folgende Zusammenhänge:

Parameter	Berechnungsverfahren	Bemerkung
tReakt	Wert aus Angabe Reaktionszeit ESMD + Verzögerungszeit in externer Abschaltkette	Verzögerungszeit in externer Abschaltkette aus Angabe Relais- / Schütz-, Bremshersteller etc.
aF, aV	n. a.	Abschätzung aus Applikation
Va1	= VS + aF * tReakt	

Für den Verlauf V und s **mit** Overspeed-Distanz gilt:

Parameter	Berechnungsverfahren	Bemerkung
tReakt	Wert aus Angabe Reaktionszeit ESMD + Verzögerungszeit in externer Abschaltkette	Verzögerungszeit in externer Abschaltkette aus Angabe Relais- / Schütz-, Bremshersteller etc.
aF, aV	n. a.	Abschätzung aus Applikation
Va2	= aF * tReakt + (VS² + 2 * aF * XF)^1/2	

Der Filter verschiebt in seiner Wirkung die eingestellte Geschwindigkeitsschwelle Va um einen Betrag delta_v_filter nach oben. Für die Applikation sind die neuen Werte für die Reaktionszeit (Treact = Tscu + Tfilter) sowie die daraus resultierende Geschwindigkeit bei Abschaltung durch die Baugruppe zu berücksichtigen.

6.4 Reaktionszeiten bei Verwendung der Erweiterungsbaugruppe

Grundlage der Berechnung von Reaktionszeiten ist die Zykluszeit des Systems. Diese beträgt im Betrieb **T_zyklus = 8 ms**. Die angegebenen Reaktionszeiten entsprechen der jeweiligen Maximallaufzeit für den konkreten Anwendungsfall innerhalb der Baugruppe. Je nach Anwendung müssen noch weitere, applikationsabhängige Reaktionszeiten der verwendeten Sensorik und Aktuatoren hinzugerechnet werden, um die Gesamtlaufzeit zu erhalten.

Funktion	Benennung	Reaktionszeit [ms]	Erläuterung
Worst-case-Verzögerungszeit Eingang in der Basisbaugruppe zum PAE	**TIN_BASE**	10	z. B. Aktivierung einer Überwachungsfunktion durch ein Eingangssignal in der Basisbaugruppe
Worst-case-Verzögerungszeit Eingang Erweiterungsbaugruppe zur PAE in Basisbaugruppe	**TIN_31**	18	z. B. Aktivierung einer Überwachungsfunktion durch ein Eingangssignal in der Erweiterungsbaugruppe
Verarbeitungszeit PAE zu PAA in Basisbaugruppe	**TPLC**	8	Abschaltung durch eine Überwachungsfunktion oder durch einen Eingang im PAE
Aktivierung / Deaktivierung digitaler Ausgang in Basisbaugruppe aus PAA	**TOUT_BASE**	–	Aktivierung oder Deaktivierung eines Ausgangs in der Basisbaugruppe nach Änderung im PAA
Aktivierung / Deaktivierung digitaler Ausgang in Erweiterungsbaugruppe über PAA in Basisbaugruppe	**TOUT_31**	8	Aktivierung oder Deaktivierung eines Ausgangs in der Erweiterungsbaugruppe nach Änderung im PAA der Basisbaugruppe

Ermittlung der Gesamtreaktionszeit

TTOTAL = TIN + TPLC + TOUT

Beispiel 1: Eingang auf Erweiterungsbaugruppe, Aktivierung von SLS und Verarbeitung in PLC, Ausgang auf Basisbaugruppe
TTOTAL = TIN_31 + TPLC + TOUT_Base = 18 ms + 8 ms + 0 ms = 24 ms

Beispiel 2: Eingang auf Basisbaugruppe, Aktivierung von SLS und Verarbeitung in PLC, Ausgang auf Erweiterungsbaugruppe
TTOTAL = TIN_Base + TPLC + TOUT_31 = 10 ms + 8 ms + 8 ms = 26 ms

Beispiel 3: Eingang auf Erweiterungsbaugruppe, Aktivierung von SLS und Verarbeitung in PLC, Ausgang auf Erweiterungsbaugruppe
TTOTAL = TIN_31 + TPLC + TOUT_31 = 18 ms + 8 ms + 8 ms = 34 ms

7 Inbetriebnahme

7.1 Vorgehensweise

Sicherheitshinweis **Eine Inbetriebnahme darf nur durch qualifiziertes Personal vorgenommen werden!**
Beachten Sie bitte bei der Inbetriebnahme die Sicherheitshinweise!

7.2 Einschaltsequenzen

Nach jedem Neustart der Baugruppe werden bei fehlerfreiem Lauf folgende Phasen durchlaufen und an der frontseitigen Siebensegmentanzeige angezeigt:

7-Segment-Anzeige	Mode	Beschreibung
1	STARTUP	Synchronisation zwischen beiden Prozessorsystemen und Prüfung der Konfigurations-/Firmwaredaten
2	SENDCONFIG	Verteilung der Konfigurations-/Firmwaredaten und nochmalige Prüfung dieser Daten. Anschließend Bereichsprüfung der Konfigurationsdaten.
3	STARTUP BUS	Falls vorhanden, Initialisierung eines Bussystems
4	RUN	Normalbetrieb des Systems. Alle Ausgänge werden nach dem aktuellen Zustand der Logik geschaltet.
5	STOP	Im Stop-Mode können Parameter- und Programmdaten extern geladen werden.
A	ALARM	Alarm kann über Digitaleingang oder frontseitigen Quittierungstaster rückgesetzt werden.
E	ECS-Alarm, ICS-Alarm, ACS-Alarm	ECS-Alarm kann über Digitaleingänge oder frontseitigen Quittierungstaster rückgesetzt werden.
F	Fehler	Fehler kann nur über EIN/AUS der Baugruppe rückgesetzt werden.
.	FBus Status	Slave F-Bus (PROFIsafe/FSoE): Aus: F-Bus nicht verwendet · Langsames Blinken: F-Bus konfiguriert, keine Verbindung zum Master · Schnelles Blinken: Verbindung zum Master, F-Bus-Aktivierung ausstehend · Ein: F-Bus verbunden

7.3 Reset-Verhalten

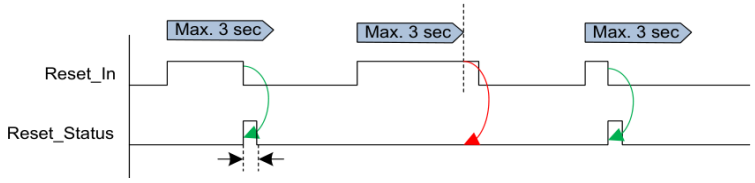
Die Resetfunktion differenziert sich in eine Anlauffunktion nach Spannungswiederkehr = General Reset und einen Status-/Alarmreset = Internal Reset. Letzterer wird über den frontseitigen Taster oder einen entsprechend konfigurierten Eingang = Resetelement mit aktivierter „Alarmreset“-Funktion ausgelöst. Nachstehende Tabelle gibt eine Übersicht zu den Resetfunktionen und deren Wirkung.

7.3.1 Resettypen und auslösendes Element

Reset-Typ	Auslösendes Element	Bemerkung
General Reset	Spannungswiederkehr / Geräteanlauf	Resetfunktion nach einem kompletten Aus- und Einschalten des Gerätes
Internal Reset	Reset-Taste (frontseitiger Taster)	Auslösen des internen Reset mittels frontseitigen Reset-Taster
	Reset-Element (konfigurierter Eingang)	Konfigurieren eines Reset-Eingangs

7.3.2 Reset-Timing

Der Reseteingang für den Internal Reset wird im „RUN"-Mode zeitlich überwacht. Ein Internal Reset wird mit der fallenden Flanke des Reset-Eingangs ausgelöst unter der Bedingung T < 3 s zwischen steigender / fallender Flanke.



Reset_In / Reset_Status, max. 3 s

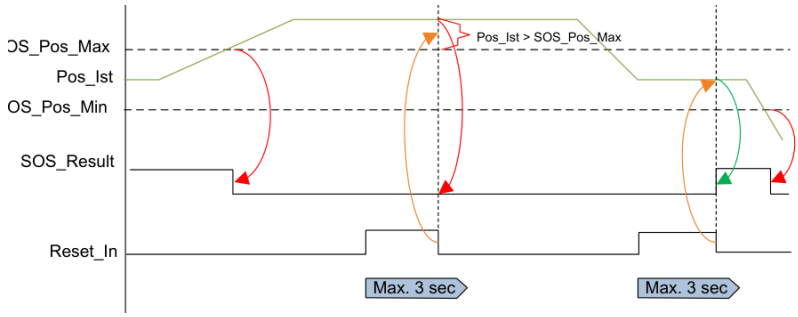
7.3.3 Reset-Funktion

Funktionseinheit	General Reset	Internal Reset	Funktion
Fatal Error	X		Rücksetzen Fehler
Alarm	X	X	Rücksetzen Alarm
Überwachungsfunktionen	X	X	Rücksetzen einer angesprochenen Überw.-Funktion
Flip-Flop	X	X	Status = Reset
Timer	X	X	Timer = 0

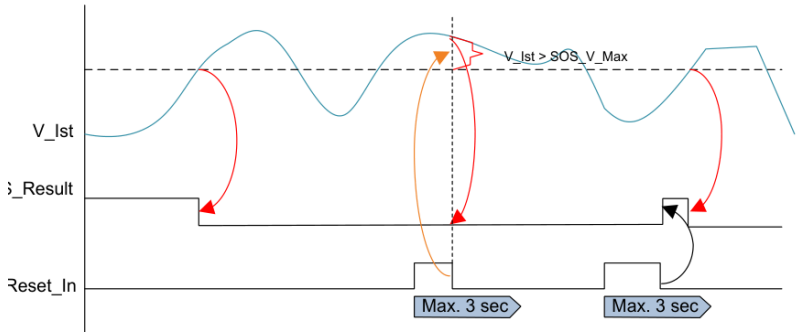
Der Status der Überwachungsfunktionen wird nach einem Reset neu gebildet:

– Prozesswerte führen bei Überschreiten der parametrierten Grenzen zu keiner Änderung des Ausgangsstatus der Überwachungsfunktion

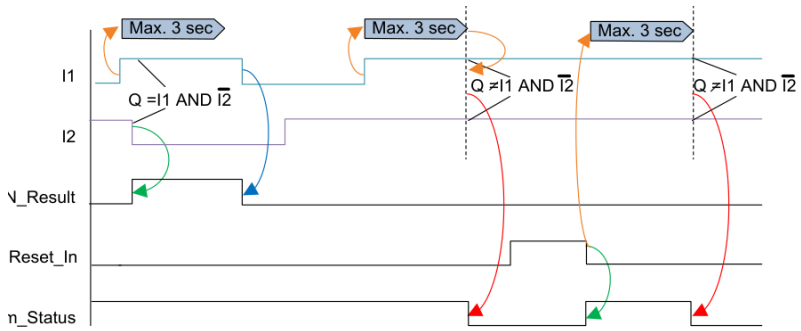
– Zeitbasierende Funktionen – Timer führen zu einem Rücksetzen des Ausgangsstatus der Überwachungsfunktion. Ein Ansprechen erfolgt nur bei neuerlichem Überschreiten der parametrierten Grenzwerte



Prozesswert (Position) => keine Änderung des Ausgangsstatus bei Reset im Alarmzustand



Prozesswert (Geschwindigkeit) => keine Änderung des Ausgangsstatus bei Reset im Alarmzustand



Zeitbasierende Funktion => Rücksetzen des Ausgangszustands, Ansprechen bei neuerlichem Überschreiten der Grenze

Sicherheitshinweis

- Bei zeitbasierenden Funktionen, z. B. zeitliche Überwachung von komplementären Eingangssignalen, wird der Ausgangszustand rückgesetzt und erst bei neuerlichem Überschreiten des (zeitlichen) Grenzwertes ein als fehlerhaft definierter Zustand detektiert.
- Zur Absicherung gegen falsche Benutzung, z. B. wiederholtes Auslösen der Resetfunktion zur Umgehung eines Alarmzustandes, müssen gegebenenfalls applikativ Maßnahmen in der PLC-Programmierung ergriffen werden.

Beispiel Reset-Funktion mit Absicherung gegen falsche Benutzung

Funktion: An einer Maschine soll eine Absicherung des Gefahrenbereichs im Normalbetrieb durch eine trennende Schutzeinrichtung und im Einrichtbetrieb durch einen Zustimmtaster in Verbindung mit Stillstandsüberwachung und sicher reduzierter Geschwindigkeit erfolgen.

Das Vorhandensein der trennenden Schutzeinrichtung wird durch einen elektrischen Sensor überwacht. Bei geöffneter Schutzeinrichtung ist ein Verfahren nur bei betätigtem Zustimmtaster möglich.

Im Programm wird dies durch eine Funktion „Schutztüre“ (2-kanalig mit Zeitüberwachung) und eine Funktion „Zustimmung“ realisiert.

Das Logiksignal „Schutztüre“ wird mittels einer Eingangsvorverarbeitung mit komplementären Eingängen und Zeitüberwachung erzeugt. Die Zeitüberwachung dieses Elements ist fest auf 3 Sekunden eingestellt.

Bei offener Schutztüre (Signal „LOW“ am Schalterausgang X23.1 und X23.2 (ID 369)) kann die Achse mit reduzierter Geschwindigkeit verfahren werden, wenn die Zustimmung X14.1 und X14.2 (ID 318) aktiv ist.

Problemstellung: Wird ein Fehler „Querschluss“ am Schutztüre-Eingang simuliert, dann zeigt die Baugruppe den Alarm 6701 an.

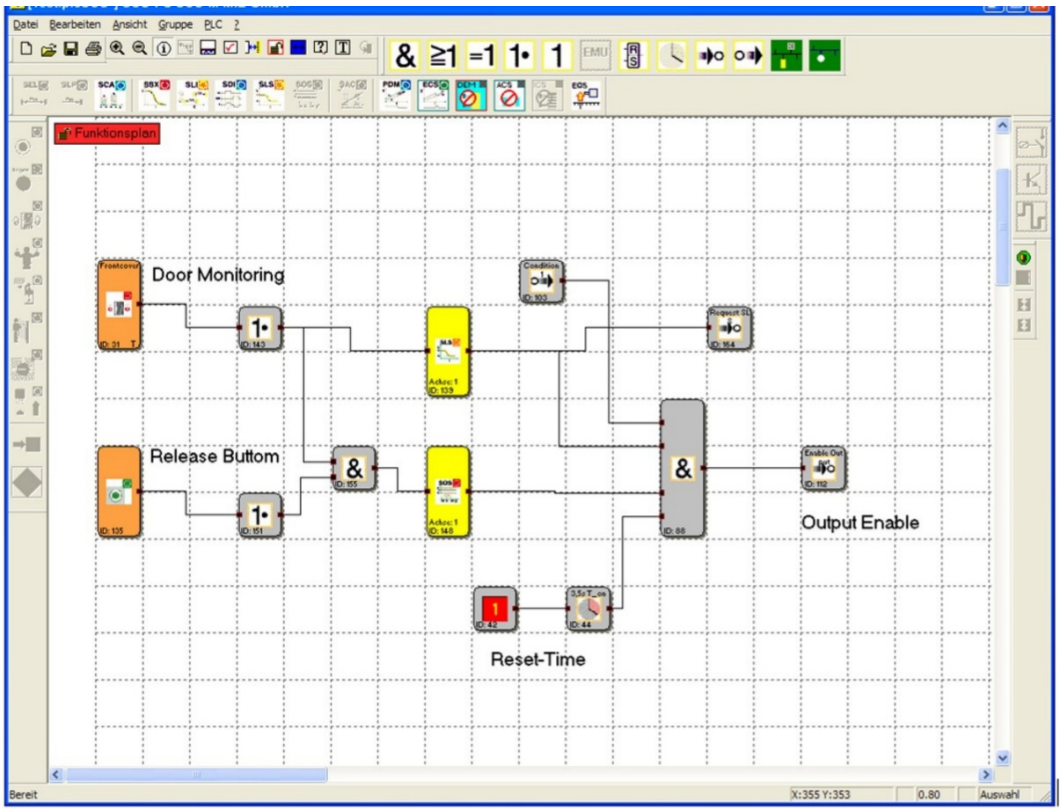
Dieser kann quittiert werden und das Signal „Schutztüre“ (ID 369) bleibt korrekterweise auf „LOW“.

Nach Ablauf der Zeitüberwachung von 3 Sekunden wird erneut der Alarm 6701 ausgelöst.

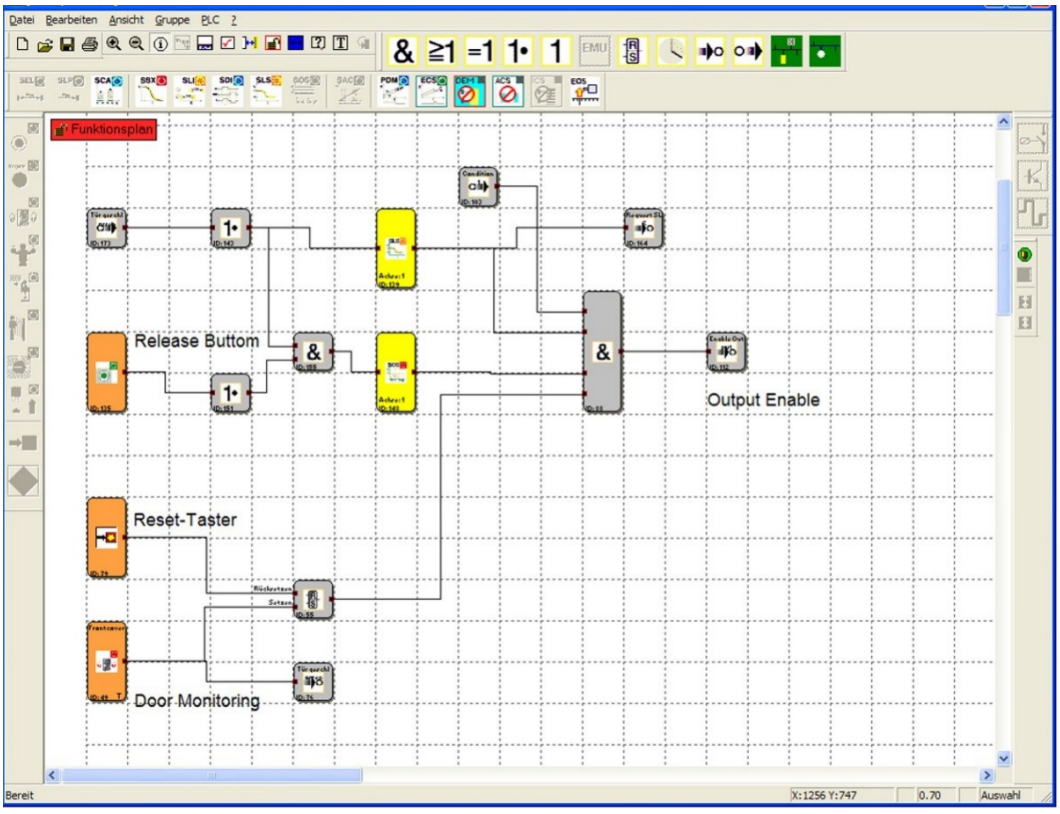
Wird in diesem Zeitraum die Zustimmung gedrückt, kann die Achse für 3 Sekunden mit reduzierter Geschwindigkeit verfahren werden.

Die Aufgabe besteht nun darin, Achsbewegungen zu verhindern, wenn der Alarm nach einem Reset möglicherweise zurückkommt.

Applikative Maßnahme: Durch Verknüpfung innerhalb des PLC-Programms der Programmiersoftware wird eine Aktivierung der Ausgänge unter zeitlicher Umgehung des Alarmzustandes verhindert.



Beispiel 1: Die Freigabefunktion der Ausgänge (ID 88) wird zusätzlich mit einem „Reset-Timer“ verknüpft. Dieser verhindert für t > 3 s die Aktivierung der Ausgänge nach einem Reset => die neuerliche Wirkung einer zeitlichen Überwachung wird sichergestellt.



Beispiel 2: Die Freigabefunktion der Ausgänge (ID 88) wird zusätzlich mit einem FF verknüpft. Dieses verhindert die Aktivierung der Ausgänge nach einem Reset und anstehenden Fehler im Eingangskreis. Erst nach 1-maligem Anlegen eines fehlerfreien Eingangssignals werden die Ausgänge freigegeben.

7.4 LED-Anzeige

Farbe	Mode	Beschreibung
grün	blinkend	System OK, Konfiguration validiert
gelb	blinkend	System OK, Konfiguration noch nicht validiert
rot	blinkend	Alarm
rot	dauerhaft	Fatal Error
gelb – rot	blinkend	System OK, Konfiguration nicht validiert, SMMC konfiguriert, aber Teilnehmer fehlt
grün – rot	blinkend	System OK, Konfiguration validiert, SMMC konfiguriert, aber Teilnehmer fehlt

Hinweis Für alle Betriebszustände außer RUN werden die Ausgänge von der Firmware passiviert, d. h. sicher abgeschaltet. Im Zustand RUN ist der Zustand der Ausgänge abhängig vom implementierten PLC-Programm.

7.5 Parametrierung

Die Parametrierung erfolgt über die Programmiersoftware. Um die Daten an die Baugruppe senden zu können, wird ein Programmieradapter benötigt, dessen Treiber vor dem Benutzen erstmals installiert werden muss.

Für die Beschreibung der Parametrierung siehe Programmierhandbuch der Programmiersoftware.

7.6 Funktionsprüfung

Um die Sicherheit der Baugruppe zu gewährleisten, muss einmal pro Jahr eine Funktionsprüfung der Sicherheitsfunktionen durchgeführt werden. Dazu müssen die in der Parametrierung verwendeten Bausteine (Eingänge, Ausgänge, Überwachungsfunktionen und Logikbausteine) hinsichtlich ihrer Funktion bzw. Abschaltung getestet werden. Siehe Programmierhandbuch der Programmiersoftware.

7.7 Validierung

Für die Sicherstellung der implementierten Sicherheitsfunktionen muss vom Anwender nach erfolgter Inbetriebnahme und Parametrierung eine Überprüfung und Dokumentation der Parameter und Verknüpfungen vorgenommen werden. Dies wird durch den Validierungsassistenten in der Programmieroberfläche unterstützt (siehe Kapitel 8 Sicherheitstechnische Prüfung).

8 Sicherheitstechnische Prüfung

Für die Sicherstellung der implementierten Sicherheitsfunktionen muss vom Anwender nach erfolgter Inbetriebnahme und Parametrierung eine Überprüfung und Dokumentation der Parameter und Verknüpfungen vorgenommen werden. Dies wird durch die Programmiersoftware unterstützt (siehe Programmierhandbuch der Programmiersoftware).

Auf den ersten zwei Seiten können allgemeine Angaben zur Anlage gemacht werden.

Auf den folgenden Seiten des Validierungsreports werden alle verwendeten Funktionen mit ihren Parametern als Einzelnachweis der sicherheitstechnischen Prüfung abgedruckt.

Nach der Übertragung der Konfigurations- und Programmdaten zur Baugruppe blinkt die Status-LED in der Farbe Gelb. Dies zeigt an, dass die Konfigurationsdaten noch nicht validiert wurden.

Mit Bestätigung der Taste „KONFIGURATION SPERREN“ am Ende des Validierungsdialogs werden die Daten als „Validiert“ gekennzeichnet und die LED blinkt in der Farbe „Grün“.

9 Wartung

9.1 Modifikation / Umgang mit Änderungen am Gerät

Wartungsarbeiten sind ausschließlich von qualifiziertem Personal vorzunehmen.

Regelmäßige Wartungsarbeiten müssen nicht durchgeführt werden.

Reparatur: Geräte sind immer komplett zu tauschen. Eine Reparatur des Gerätes kann nur im Werk durchgeführt werden.

Garantie: Mit unzulässigem Öffnen der Baugruppe erlischt die Garantie.

Hinweis **Bei Modifikation der Baugruppe erlischt die Sicherheitszulassung!**

9.2 Tausch einer Baugruppe

Beim Tausch einer Baugruppe sollte Folgendes beachtet werden:

- Stromrichter von der Hauptversorgung trennen.
- Spannungsversorgung für das Gerät ausschalten und Verbindung lösen.
- Geberstecker abziehen.
- Alle weiteren steckbaren Verbindungen entfernen.
- Baugruppe von der Hutschiene nehmen und EMV-gerecht verpacken.
- Neue Baugruppe auf der Hutschiene anbringen.
- Alle Verbindungen wiederherstellen.
- Stromrichter einschalten.
- Versorgungsspannung einschalten.
- Gerät konfigurieren.

Hinweis Grundsätzlich darf kein steckbarer Anschluss der Baugruppe unter Spannung getrennt oder wieder gesteckt werden. Insbesondere bei den angeschlossenen Positions- bzw. Geschwindigkeitssensoren besteht die Gefahr einer Zerstörung des Sensors.

9.3 Wartungsintervalle

Tätigkeit	Intervall
Austausch Baugruppe	Siehe Technische Daten (Kapitel 10)
Funktionsprüfung	Siehe Kapitel 7 Inbetriebnahme

10 Technische Daten

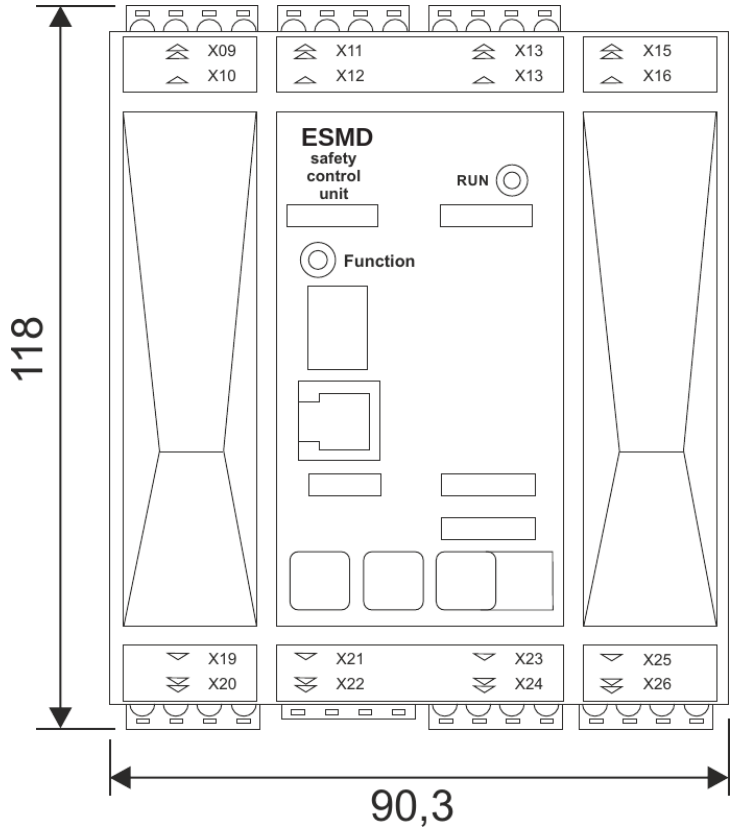
10.1 Umweltbedingungen

Merkmal	Wert
Schutzklasse	IP 20
Umgebungstemperatur	0 °C* ... 50 °C
Klimaklasse	3k3 nach DIN 60 721
Min-, Maximal relative Luftfeuchte (keine Betauung)	5 % – 85 %
Überspannungskategorie	III
Verschmutzungsgrad	2
Betriebsmitteleinsatz	2000 m
Lebensdauer	90000 h bei 50 °C Umgebung

10.2 Sicherheitstechnische Kenndaten

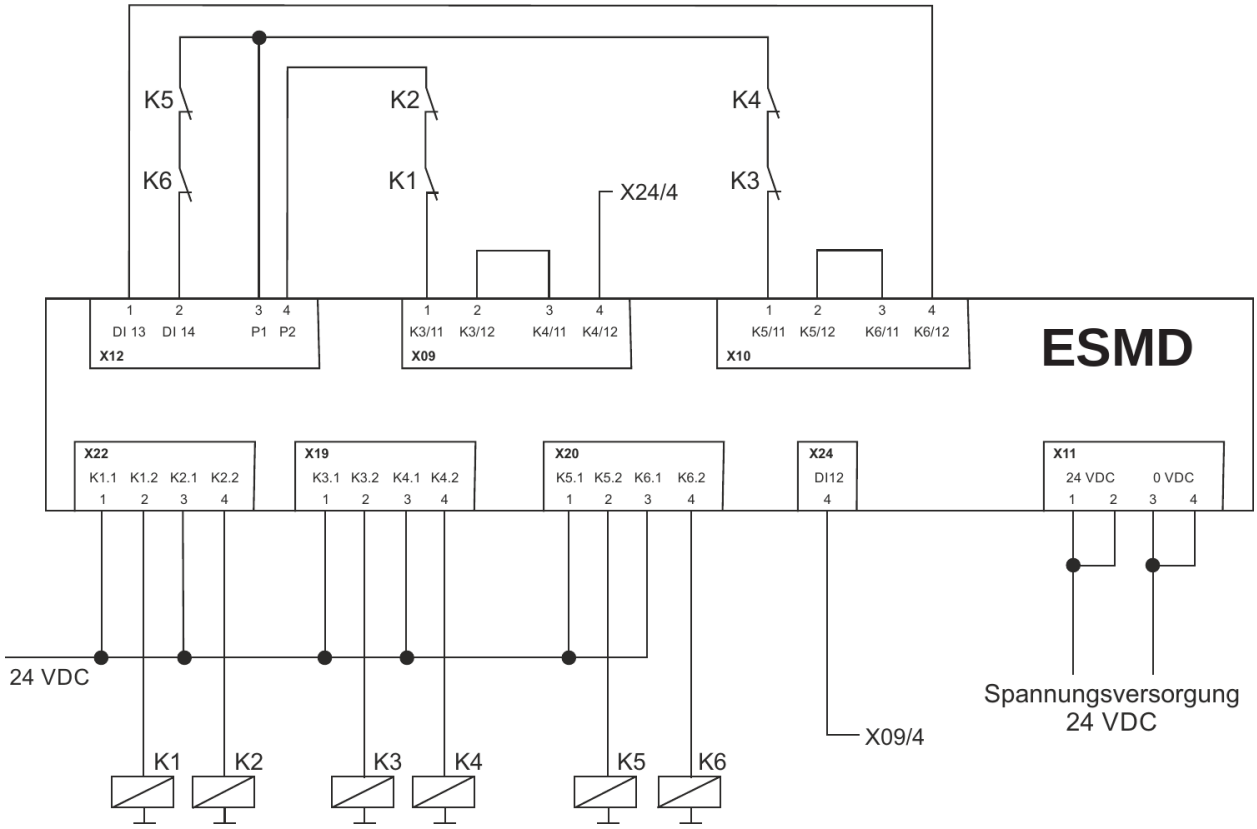
Merkmal	Wert
Max. erreichbare Sicherheitsklasse	SIL 3 gemäß IEC 61508; Kategorie 4 gemäß EN ISO 13849-1; Performance-Level e gemäß EN ISO 13849-1
Systemstruktur	2-kanalig mit Diagnose (1oo2) nach IEC 61508; Architektur Kategorie 4 nach EN ISO 13849-1
Auslegung der Betriebsart	„high demand“ gemäß IEC 61508 (hohe Anforderungsrate)
Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH-Wert); spezifische Werte gemäß Tabellen Sicherheitstechnische Kenndaten	Erweiterungsbaugruppe: PFH = 9,2 FIT; ESMD (1-kanalig): PFH = 20 FIT; ESMD (2-kanalig): PFH = 1,0 FIT; 20 Jahre, danach muss die Baugruppe ersetzt werden
Proof-Test-Intervall (IEC 61508)	20 Jahre, danach muss die Baugruppe ersetzt werden

10.3 Abmessungen



Gerätefront mit den Steckern X09 bis X26, den Tasten RUN und Function und der Statusanzeige. Maße in mm.

10.4 Anschlussbeispiel

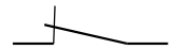


Anschlussbeispiel: sechs Relais K1 ... K6 an den Steckern X09, X10, X19, X20 und X22, mit den Rücklesekontakten K3/11 ... K6/12 zurück auf X09 und X10 und den Querschlussimpulsen P1 und P2 auf X12. Die externe Kontaktüberwachung (EMU) der angeschlossenen Schaltgeräte ist eine eingebaute Sicherheitsfunktion; eine Kontaktvervielfältigung über externe Schütze ist mit dieser Überwachung möglich.

11 Schaltertypen

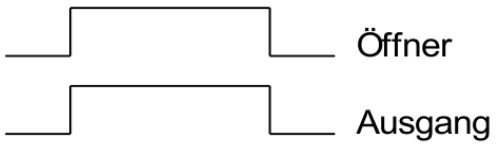
Je Schaltertyp: Schaltzeichen und Wahrheitstabelle (links) und Zeitdiagramm (rechts), darunter Logikfunktion (AWL), Funktionsblock und Funktion. Ö = Öffner, S = Schließer, A = Ausgang.

Typ 1 – eSwitch_1o



eSwitch_1o

Ö	A
0	0
1	1

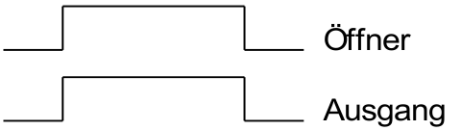


Logikfunktion	Funktionsblock	Funktion
LD E.1 **ST IE.X**		Schließer, nur in Darstellung Öffner

Typ 2 – sSwitch_1s

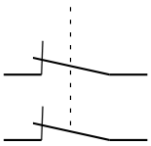
sSwitch_1s

S	A
0	0
1	1



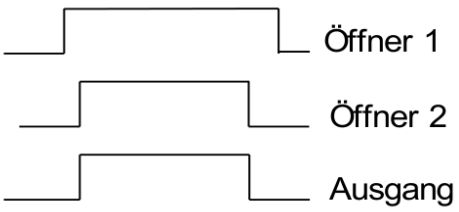
Logikfunktion	Funktionsblock	Funktion
LD E.1 **ST IE.X**		Schließer, wie Typ 1

Typ 3 – eSwitch_2o



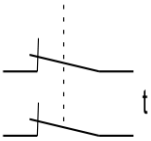
eSwitch_2o

Ö1	Ö2	A
0	0	0
1	0	0
0	1	0
1	1	1



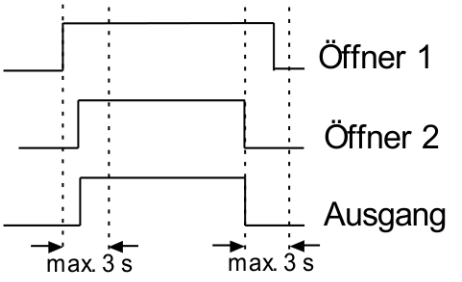
Logikfunktion	Funktionsblock	Funktion
LD E.1 **AND E.2** **ST IE.X**		UND-Verknüpfung beider Eingänge

Typ 4 – eSwitch_2oT



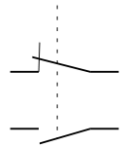
eSwitch_2oT

Ö1	Ö2	A
0	0	0
1	0	0
0	1	0
1	1	1



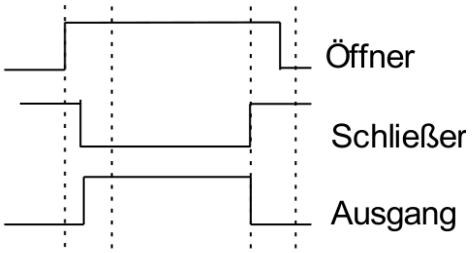
Logikfunktion	Funktionsblock	Funktion
LD E.1 **OR E.2** **ST META_EN.1** **LD E.1** **AND E.2** **ST METB_EN.1** **LD MET.1** **ST IE.X**	Zeitüberwachung MET1..MET4	Wie 3, jedoch mit zeitlicher Überwachung von Zustandsänderungen. Bei Signalwechsel an S oder Ö muss komplementäres Signal innerhalb Zeit t = 3 s folgen. Falls nicht, auf Störung erkennen und A = 0

Typ 5 – eSwitch_1s1o



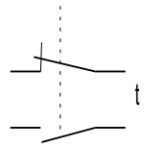
eSwitch_1s1o

S	Ö	A
0	0	0
1	0	0
0	1	1
1	1	0



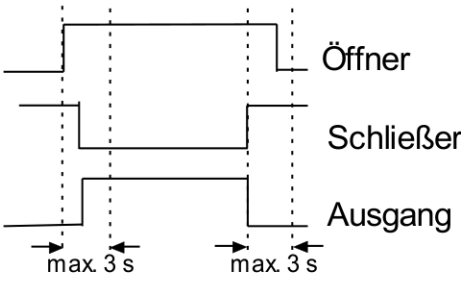
Logikfunktion	Funktionsblock	Funktion
LD E.1 **AND NOT E.2** **ST IE.X**		Überwachung auf S = inaktiv und Ö = aktiv

Typ 6 – eSwitch_1s1oT



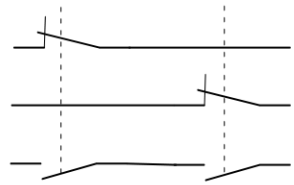
eSwitch_1s1oT

S	Ö	A
0	0	0
1	0	0
0	1	1
1	1	0

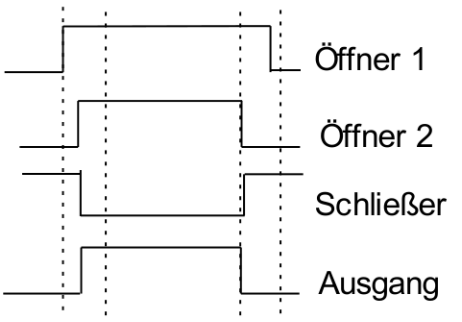


Logikfunktion	Funktionsblock	Funktion
LD E.1 **OR NOT E.2** **ST META_EN.1** **LD E1** **AND NOT E2** **ST METB_EN.1** **LD MET.1** **ST IE.X**	Zeitüberwachung MET1..MET4	Wie 5, jedoch mit zeitlicher Überwachung von Zustandsänderungen. Bei Signalwechsel an S oder Ö muss komplementäres Signal innerhalb Zeit t = 3 s folgen. Falls nicht, auf Störung erkennen und A = 0

Typ 7 – eSwitch_2s2o



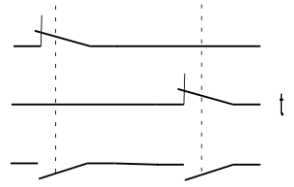
S1	Ö 1	S2	Ö2	A
1	0	1	0	0
0	1	1	0	0
0	1	0	1	1
1	0	0	1	0



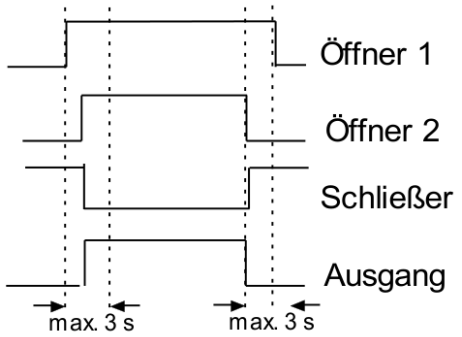
eSwitch_2s2o

Logikfunktion	Funktionsblock	Funktion
LD E.1 **AND E.2** **AND NOT E.3** **ST IE.X**		Überwachung auf S1*S2 = inaktiv und Ö1*Ö2 = aktiv

Typ 8 – eSwitch_2s2oT



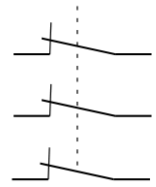
S1	Ö 1	S2	Ö2	A
1	0	1	0	0
0	1	1	0	0
0	1	0	1	1
1	0	0	1	0



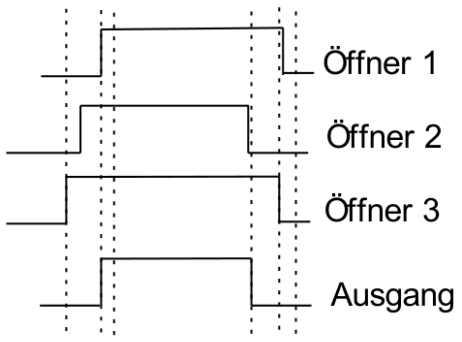
eSwitch_2s2oT

Logikfunktion	Funktionsblock	Funktion
LD E.1 **OR E.2** **OR NOT E.3** **ST META_EN.1** **LD E.1** **AND E.2** **AND NOT E.3** **ST METB_EN.1** **LD MET.1** **ST IE.X**	Zeitüberwachung MET1..MET4	Wie 6, jedoch mit zeitlicher Überwachung von Zustandsänderungen. Bei Signalwechsel an S (Achtung Sammelleitung!) oder Ö muss komplementäres Signal innerhalb Zeit t = 3 s folgen. Falls nicht, auf Störung erkennen und A = 0

Typ 9 – eSwitch_3o



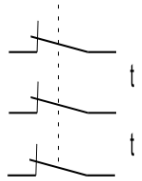
Ö1	Ö2	Ö3	A
0	0	0	0
1	0	0	0
0	1	0	0
1	1	0	0
1	1	1	1



eSwitch_3o

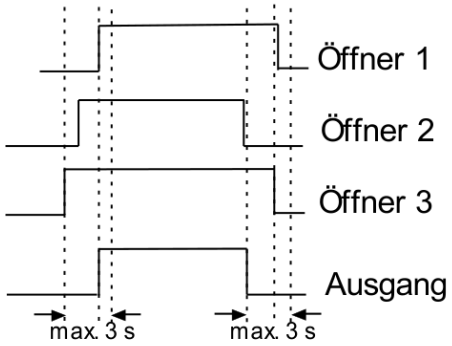
Logikfunktion	Funktionsblock	Funktion
LD E.1 **AND E.2** **AND E.3** **ST IE.X**		UND-Verknüpfung der drei Eingänge

Typ 10 – eSwitch_3oT



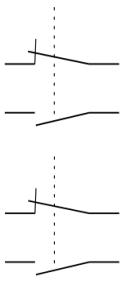
eSwitch_3oT

Ö1	Ö2	Ö3	A
0	0	0	0
1	0	0	0
0	1	0	0
1	1	0	0
1	1	1	1



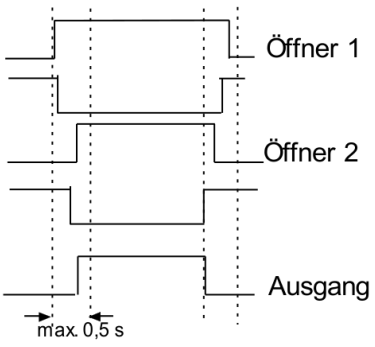
Logikfunktion	Funktionsblock	Funktion
LD E.1 **OR E.2** **OR E.3** **ST META_EN.1** **LD E.1** **AND E.2** **AND E.3** **ST METB_EN.1** **LD MET.1** **ST IE.X**	Zeitüberwachung MET1..MET4	Wie 8, jedoch mit zeitlicher Überwachung von Zustandsänderungen. Bei Signalwechsel an einem der Ö-Eingänge müssen die weiteren Eingänge innerhalb Zeit t = 3 s folgen. Falls nicht, auf Störung erkennen und A = 0

Typ 11 – eTwoHand_2o



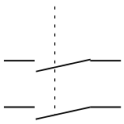
eTwoHand_2o

Ö 1	S 1	Ö 2	S 2	A
0	1	0	1	0
1	0	0	1	0
1	0	1	0	0
0	1	0	1	1



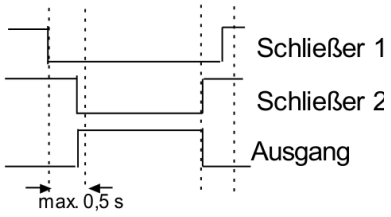
Logikfunktion	Funktionsblock	Funktion
LD NOT E.1 **OR E.2** **OR NOT E.3** **OR E.4** **ST MEZ_EN.1** **LD E.1** **AND NOT E2** **AND E3** **AND NOT E4** **ST MEZ_EN.2** **LD NOT E1** **AND E.2** **AND NOT E3** **AND E.4** **ST MEZ_EN.3** **LD MEZ.1** **ST IE.X**	Zweihandbedienung MEZ	Überwachung auf S1*S2 = inaktiv und Ö1*Ö2 = aktiv + zeitliche Überwachung dieses Zustands. D. h. erfolgt Signalwechsel eines S von 1->0 oder Ö von 0->1, dann müssen die weiteren Signale (d. h. weiterer S = 0 bzw. Ö = 1) innerhalb von 0,5 s folgen. Wenn nicht, bleibt Ausgang = 0. Keine Störungsauswertung! Keine zeitliche Überwachung bei Wechsel auf inaktiven Zustand.

Typ 12 – eTwoHand_2s



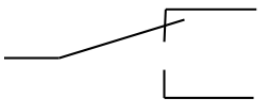
eTwoHand_2s

S1	S2	A
1	0	0
0	1	0
0	0	0
1	1	1



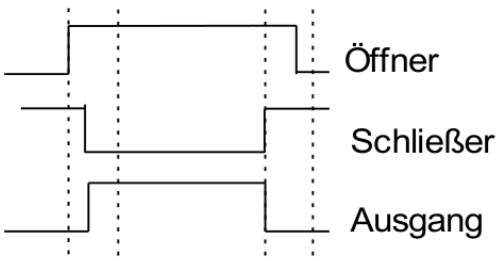
Logikfunktion	Funktionsblock	Funktion
LD E.1 **OR E.2** **ST MEZ_EN.1** **LD NOT E.1** **AND NOT E.2** **ST MEZ_EN.2** **LD E.1** **AND E.2** **ST MEZ_EN.3** **LD MEZ.1** **ST IE.X**	Zweihandbedienung MEZ	Überwachung auf S1*S2 = inaktiv + zeitliche Überwachung dieses Zustands. D. h. erfolgt Signalwechsel eines S von 1->0, dann muss das weitere Signal (d. h. weiteres S = 0) innerhalb von 0,5 s folgen. Wenn nicht, bleibt Ausgang = 0. Keine Störungsauswertung! Keine zeitliche Überwachung bei Wechsel auf inaktiven Zustand.

Typ 13 – eMode_1s1o



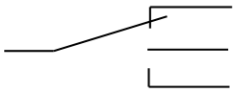
eMode_1s1o

S1	S2	A 1	A 2
1	0	1	0
0	1	0	1
0	0	0	0
1	1	0	0



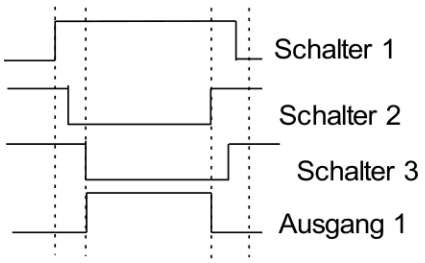
Logikfunktion	Funktionsblock	Funktion
LD E.1 **AND NOT E.2** **ST IE.X1** **LD NOT E.1** **AND E.2** **ST IE.X2**	Wahlschalter	Eindeutige Verknüpfung der zulässigen Schalterstellungen

Typ 14 – eMode_3switch



eMode_3switch

S1	S2	S3	A 1	A 2	A 3
1	0	0	1	0	0
0	1	0	0	1	0
0	0	1	0	0	1
1	1	0	0	0	0
1	0	1	0	0	0
0	1	1	0	0	0
1	1	1	0	0	0
0	0	0	0	0	0



Logikfunktion	Funktionsblock	Funktion
LD E.1 **AND NOT E.2** **AND NOT E.3** **ST IE.X1** **LDN E.1** **AND E2** **AND NOT E.3** **ST IE.X2** **LDN E.1** **AND NOT E.2** **AND E.3** **ST IE.X3**	Wahlschalter	Eindeutige Verknüpfung der zulässigen Schalterstellungen

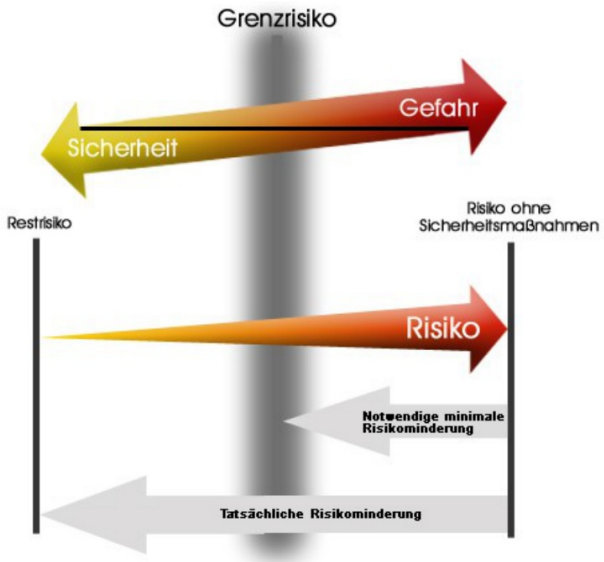
12 Hinweise für Entwurf, Programmieren, Validieren und Testen von sicherheitstechnischen Applikationen

Nachfolgende Hinweise beschreiben die Vorgehensweise für Entwurf, Programmieren, Validieren und Testen von sicherheitstechnischen Applikationen.

Die Hinweise sollen dem Anwender helfen, alle Schritte von der Risikobeurteilung bis zum Systemtest einzuordnen, leicht zu verstehen und anzuwenden. Zum besseren Verständnis der jeweiligen Punkte werden die einzelnen Schritte anhand von Beispielen näher erläutert.

12.1 Risikobetrachtung

Grundsätzlich muss der Hersteller einer Maschine die Sicherheit einer von ihm konstruierten bzw. gelieferten Maschine gewährleisten. Für die Beurteilung der Sicherheit sind die jeweils gültigen einschlägigen Richtlinien und Normen heranzuziehen. Ziel der Sicherheitsbetrachtung und der daraus abgeleiteten Maßnahmen muss eine Reduzierung der Gefährdung von Personen auf ein akzeptierbares Niveau sein.

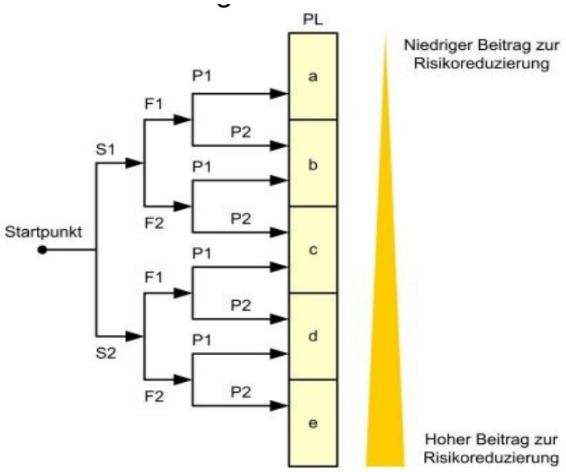


Die Analyse der Gefährdungen muss sämtliche Betriebszustände der Maschine wie Betreiben, Rüsten und Warten bzw. Aufstellen und Außerbetriebstellen sowie auch vorhersehbare Fehlanwendungen berücksichtigen.

Die hierzu erforderliche Vorgehensweise für die Risikobeurteilung und die Maßnahmen zu deren Reduzierung sind z. B. in den folgenden einschlägigen Normen enthalten:

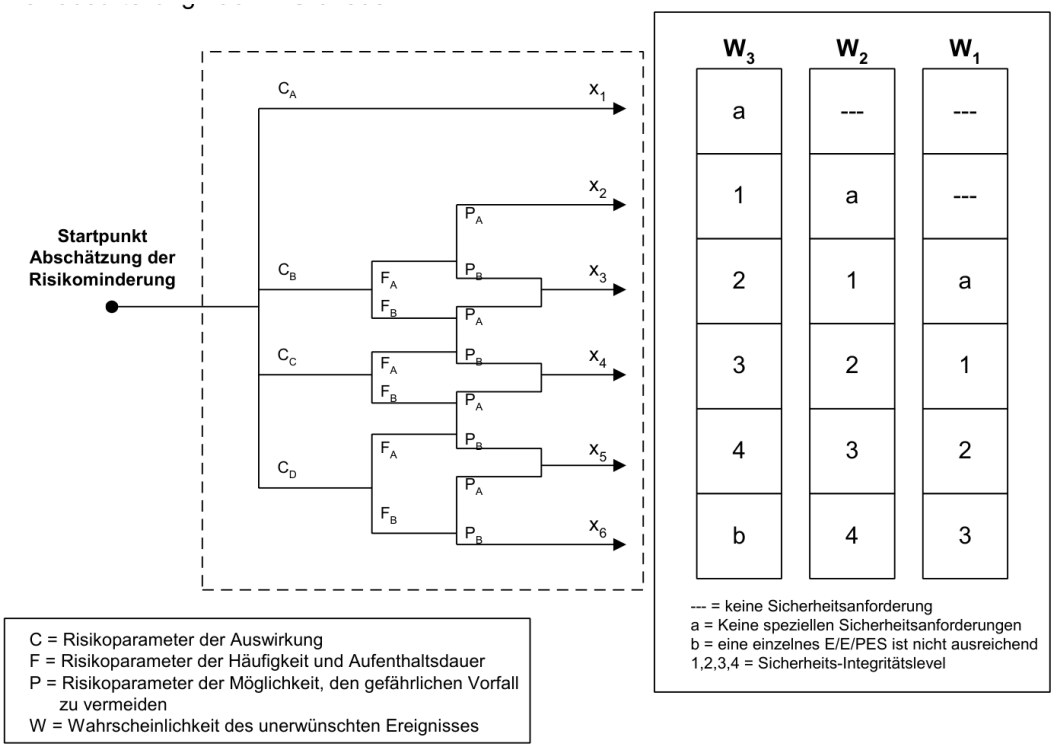
- EN ISO 13849-1 Sicherheit von Maschinen
- IEC 61508 Funktionale Sicherheit sicherheitsbezogener E/E/PE-Systeme

Risikobeurteilung nach EN ISO 13849-1



Parameter	Bedeutung
S – Schwere der Verletzung	S1 = leichte, reversible Verletzung; S2 = schwere, irreversible Verletzung
F – Häufigkeit und/oder Dauer der Gefährdungsexposition	F1 = selten, nicht zyklisch; F2 = häufig bis dauernd und/oder lange Dauer, zyklischer Betrieb
P – Möglichkeit zur Vermeidung der Gefährdung	P1 = möglich, langsame Bewegung / Beschleunigung; P2 = kaum möglich, hohe Beschleunigung im Fehlerfall

Risikobeurteilung nach IEC 61508



Die zu betrachtenden Risiken sind ebenso in einschlägigen Richtlinien und Normen enthalten bzw. sind vom Hersteller aufgrund seiner spezifischen Kenntnisse der Maschine gesondert zu betrachten.

Für innerhalb der EU in Verkehr gebrachte Maschinen sind die mindestens zu betrachtenden Risiken in der EU-Maschinenrichtlinie 2006/42/EG bzw. in der jeweils letztgültigen Fassung dieser Richtlinie spezifiziert.

Weitere Hinweise für die Risikobeurteilung und die sichere Gestaltung von Maschinen sind in den folgenden Normen enthalten:

- EN 14121 Sicherheit von Maschinen – Risikobeurteilung
- EN 12100 Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze

Maßnahmen, die zur Reduzierung identifizierter Gefährdungen angewendet werden, müssen im Niveau mindestens demjenigen der Gefährdung entsprechen. Derartige Maßnahmen und die Anforderungen hieran sind ebenso beispielhaft in den oben angeführten Richtlinien und Normen enthalten.

12.2 Erforderliche technische Unterlagen

Vom Hersteller sind verschiedene technische Unterlagen zu liefern. Deren Mindestumfang ist ebenso in den einschlägigen Richtlinien und Normen enthalten. So sind z. B. gemäß EU-Maschinenrichtlinie mindestens folgende Unterlagen zu liefern:

1. Die technischen Unterlagen umfassen:

   a) eine technische Dokumentation mit folgenden Angaben bzw. Unterlagen:
      - eine allgemeine Beschreibung der Maschine
      - eine Übersichtszeichnung der Maschine und die Schaltpläne der Steuerkreise sowie Beschreibungen und Erläuterungen, die zum Verständnis der Funktionsweise der Maschine erforderlich sind
      - vollständige Detailzeichnungen, eventuell mit Berechnungen, Versuchsergebnissen, Bescheinigungen usw., die für die Überprüfung der Übereinstimmung der Maschine mit den grundlegenden Sicherheits- und Gesundheitsschutzanforderungen erforderlich sind
      - die Unterlagen über die Risikobeurteilung, aus denen hervorgeht, welches Verfahren angewandt wurde; dies schließt ein:
        i) eine Liste der grundlegenden Sicherheits- und Gesundheitsschutzanforderungen, die für die Maschine gelten
        ii) eine Beschreibung der zur Abwendung ermittelter Gefährdungen oder zur Risikominderung ergriffenen Schutzmaßnahmen und gegebenenfalls eine Angabe der von der Maschine ausgehenden Restrisiken
      - die angewandten Normen und sonstige technische Spezifikationen unter Angabe der von diesen Normen erfassten grundlegenden Sicherheits- und Gesundheitsschutzanforderungen
      - alle technischen Berichte mit den Ergebnissen der Prüfungen, die vom Hersteller selbst oder von einer Stelle nach Wahl des Herstellers oder seines Bevollmächtigten durchgeführt wurden
      - ein Exemplar der Betriebsanleitung der Maschine
      - gegebenenfalls die Einbauerklärung für unvollständige Maschinen und die Montageanleitung für solche unvollständigen Maschinen
      - gegebenenfalls eine Kopie der EG-Konformitätserklärung für in die Maschine eingebaute andere Maschinen oder Produkte,
      - eine Kopie der EG-Konformitätserklärung

   b) bei Serienfertigung eine Aufstellung der intern getroffenen Maßnahmen zur Gewährleistung der Übereinstimmung aller gefertigten Maschinen mit den Bestimmungen dieser Richtlinie

Quelle BGIA Report 2/2008

Die Unterlagen sind dabei leicht verständlich und in der jeweiligen Landessprache abzufassen.

12.3 Erforderliche Schritte zu Entwurf, Realisierung und Prüfung

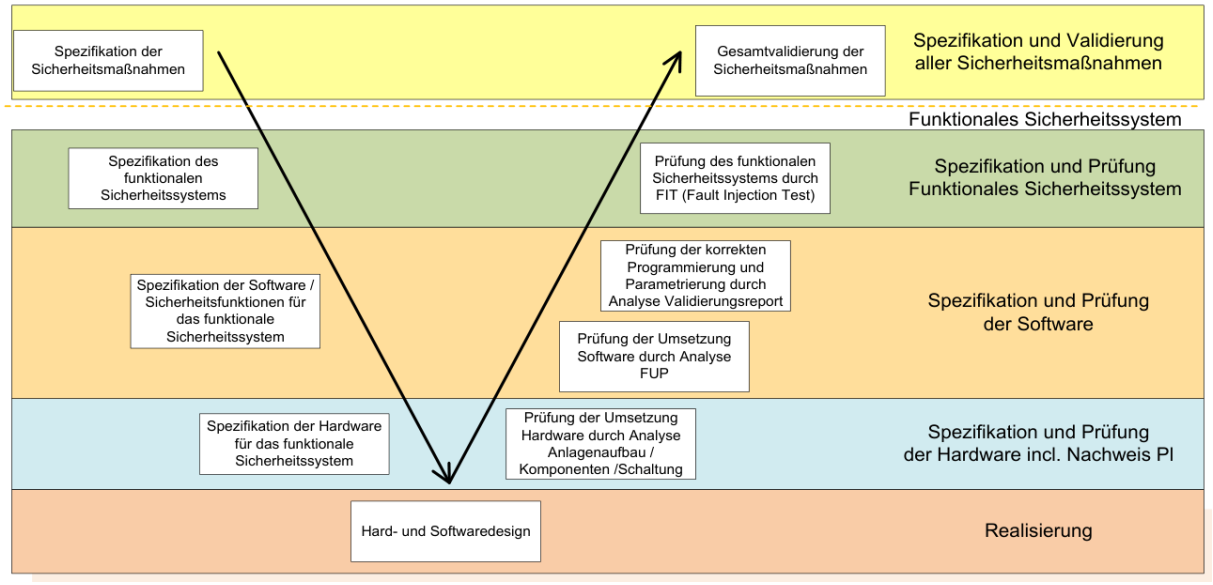
Die Realisierung von Anlagenteilen mit sicherheitstechnischer Funktion bedarf einer besonderen Sorgfalt in der Planung, Realisierung und Prüfung. Auch hierzu sind Leitlinien in den einschlägigen Normen (vgl. EN ISO 13849-2 bzw. IEC 61508) enthalten. Der Aufwand richtet sich hierbei nach der Komplexität der Aufgabenstellung für Anlagenteile mit sicherheitstechnischer Funktion.

Die Baureihe ESMD bietet für die Realisierung derartiger Funktionen mit Hilfe von sicherheitsgerichteten Steuer- und Überwachungsfunktionen eine effiziente Unterstützung in Form der Systemarchitektur (Architektur Kat. 4 nach EN ISO 13849-1) und vor allem auch der Programmiersprache und geprüfter Sicherheitsfunktionen an. Die Programmierung erfolgt in der nach den Sicherheitsnormen empfohlenen Form FUP (funktionsplanorientierte Programmierung). Sie entspricht weiter den Anforderungen an eine Programmiersprache mit eingeschränktem Sprachumfang (LVL), für die wesentliche Vereinfachungen in Dokumentation und Testumfang gelten.

In jedem Fall bedürfen die einzelnen Schritte einer sorgfältigen Planung und Analyse der verwendeten Methoden und Systeme. Die einzelnen Schritte sind weiter gut nachvollziehbar zu dokumentieren.

V-Modell (vereinfacht)

Die Umsetzung von sicherheitstechnischen Funktionen bedarf einer strukturierten Vorgehensweise, wie sie beispielhaft das in einschlägigen Normen empfohlene V-Modell aufzeigt. Nachfolgend ist beispielhaft die Vorgehensweise für Applikationen mit Baugruppen der Baureihe ESMD aufgezeigt.



12.3.1 Phasen des V-Modells

Benennung	Beschreibung Design-Phase	Validierungsphase
Spezifikation und Validierung aller passiven und aktiven Sicherheitsmaßnahmen	Spezifikation aller zu treffenden Sicherheitsmaßnahmen wie Abdeckungen, Abschrankungen, max. Maschinenparameter, sicherheitstechnische Funktionen etc.	Prüfung aller passiven und aktiven Sicherheitsmaßnahmen auf deren ordnungsgemäße Umsetzung und Wirksamkeit
Spezifikation der funktionalen Sicherheitssysteme	Spezifikation der aktiven Sicherheitssysteme und deren Zuordnung auf die zu reduzierenden Risiken wie z. B. reduzierte Geschw. im Einrichtbetrieb, Stop-Modus, Überwachung von Zugangsbereichen etc. Spezifikation des PLr bzw. geforderten SIL für jede einzelne Sicherheitsfunktion	Prüfung aller aktiven Sicherheitssysteme auf deren Wirksamkeit und Einhaltung der spezifizierten Parameter wie z. B. fehlerhaft erhöhte Geschwindigkeit, fehlerhafter Stopp, Ansprechen von Überwachungseinrichtungen etc. mittels praktischer Tests
Spezifikation der Software / Sicherheitsfunktionen	Spezifikation der Funktionalität der einzelnen Sicherheitsfunktionen inkl. Definition des Abschaltkreises etc. Definition der Parameter für die einzelne Sicherheitsfunktion wie z. B. max. Geschwindigkeit, Stopp-Rampen und -Kategorie etc.	Prüfung der korrekten Umsetzung der Funktionsvorgaben durch Analyse FUP-Programmierung. Validierung des Applikationsprogramms und der Parameter durch Vergleich Validierungsreport mit FUP bzw. Vorgaben für Parameter
Spezifikation der Hardware	Spezifikation des Anlagenaufbaus und der Funktionen der einzelnen Sensoren, Befehlsgeräte, Steuerungskomponenten und Aktuatoren in Bezug auf die Sicherheitsfunktionen	Prüfung der korrekten Umsetzung der Vorgaben. Ermittlung der Ausfallwahrscheinlichkeit bzw. PL mittels Analyse der Gesamtarchitektur und der Kenndaten aller beteiligten Komponenten, jeweils bezogen auf die einzelnen Sicherheitsfunktionen
Hard- und Softwaredesign	Konkrete Planung und Umsetzung des Anlagenaufbaus / Verdrahtung. Konkrete Umsetzung der Sicherheitsfunktionen durch Programmierung in FUP	nil

12.3.2 Spezifikation der Sicherheitsanforderungen (Gliederungsschema)

Auf Basis der anzuwendenden Normen, z. B. Produktnormen, sind die Sicherheitsanforderungen im Einzelnen zu analysieren.

1 Allgemeine Produkt- und Projektangaben
1.1 Produktidentifikation
1.2 Autor, Version, Datum, Dokumentenname, Dateiname
1.3 Inhaltsverzeichnis
1.4 Begriffe, Definitionen, Glossar
1.5 Versionshistorie und Änderungsvermerke
1.6 Für die Entwicklung relevante Richtlinien, Normen und technische Regeln

2 Funktionale Angaben zur Maschine, soweit sicherheitstechnisch von Bedeutung
2.1 Bestimmungsgemäße Verwendung und vernünftigerweise vorhersehbare Fehlanwendung/-bedienung
2.2 Prozessbeschreibung (Betriebsfunktionen)
2.3 Betriebsarten (z.B. Einrichtbetrieb, Automatikbetrieb, Betrieb mit lokalem Bezug oder von Teilen der Maschine)
2.4 Kenndaten, z.B. Zykluszeiten, Reaktionszeiten, Nachlaufwege
2.5 Sonstige Eigenschaften der Maschine
2.6 Sicherer Zustand der Maschine
2.7 Wechselwirkung zwischen Prozessen (siehe auch 2.2) und manuellen Aktionen (Reparatur, Einrichten, Reinigen, Fehlersuche usw.)
2.8 Handlungen im Notfall

3 Erforderliche(r) Performance Level (PL_r)
3.1 Referenz auf vorhandene Dokumentation zur Gefährdungsanalyse und Risikobeurteilung der Maschine
3.2 Ergebnisse der Risikobeurteilung für jede ermittelte Gefährdung oder Gefährdungssituation und Festlegung der zur Risikominderung jeweils erforderlichen Sicherheitsfunktion(en)

4 Sicherheitsfunktionen (Angaben gelten für jede Sicherheitsfunktion)
- Funktionsbeschreibung („Erfassen – Verarbeiten – Ausgeben") einschließlich aller funktionaler Eigenschaften (siehe auch Tabellen 5.1 und 5.2)
- Aktivierungs-/Deaktivierungsbedingungen oder -ereignisse (z.B. Betriebsarten der Maschine)
- Verhalten der Maschine beim Auslösen der Sicherheitsfunktion
- zu berücksichtigende Wiederanlaufbedingungen
- Leistungskriterien/Leistungsdaten
- Ablauf (zeitliches Verhalten) der Sicherheitsfunktion mit Reaktionszeit
- Häufigkeit der Betätigung (d.h. Anforderungsrate), Erholungszeiten nach Anforderung
- sonstige Daten
- einstellbare Parameter (soweit vorgesehen)
- Einordnung und Zuordnung von Prioritäten bei gleichzeitiger Anforderung und Bearbeitung mehrerer Sicherheitsfunktionen
- funktionales Konzept zur Trennung bzw. Unabhängigkeit/Rückwirkungsfreiheit zu Nicht-Sicherheitsfunktionen und weiteren Sicherheitsfunktionen

5 Vorgaben für den SRP/CS-Entwurf
5.1 Zuweisung, durch welche SRP/CS und in welcher Technologie die Sicherheitsfunktion realisiert werden soll, vorgesehene Betriebsmittel
5.2 Auswahl der Kategorie, vorgesehene Architektur (Struktur) als sicherheitsbezogenes Blockdiagramm mit Beschreibung
5.3 Schnittstellenbeschreibung (Prozessschnittstellen, interne Schnittstellen, Bedienerschnittstellen, Bedien- und Anzeigeelemente usw.)
5.4 Einschaltverhalten, Umsetzung des erforderlichen Anlaufverhaltens und Wiederanlaufverhaltens
5.5 Leistungsdaten: Zykluszeiten, Reaktionszeiten usw.
5.6 Verhalten des SRP/CS bei Bauteilausfällen und -fehlern (Erreichen und Aufrechterhalten des sicheren Zustandes) einschließlich Zeitverhalten
5.7 Zu berücksichtigende Ausfallarten von Bauteilen, Baugruppen oder Blöcken und ggf. Begründung für Fehlerausschlüsse
5.8 Konzept zur Umsetzung der Erkennung und Beherrschung von zufälligen und systematischen Ausfällen (Selbsttests, Testschaltungen, Überwachungen, Vergleiche, Plausibilitätsprüfungen, Fehlererkennung durch den Prozess usw.)
5.9 Quantitative Aspekte
5.9.1 Zielwerte für $MTTF_d$ und DC_{avg}
5.9.2 Schalthäufigkeit verschleißbehafteter Bauteile
5.9.3 Häufigkeit von Maßnahmen zur Fehleraufdeckung
5.9.4 Gebrauchsdauer, falls abweichend von der Berechnungsgrundlage der vorgesehenen Architekturen (20 Jahre)
5.10 Betriebs- und Grenzdaten (Betriebs- und Lagertemperaturbereich, Feuchteklasse, IP-Schutzart, Schock-/Vibrations-/EMV-Störfestigkeitswerte, Versorgungsdaten mit Toleranzen usw.) (IP = International Protection, EMV = elektromagnetische Verträglichkeit)
5.11 Anzuwendende Grundnormen für die Konstruktion (zur Ausrüstung, zum Schutz gegen elektrischen Schlag/gefährliche Körperströme, zur Störfestigkeit gegen Umgebungsbedingungen usw.)
5.12 Technische und organisatorische Maßnahmen für einen gesicherten Zugriff auf sicherheitsrelevante Parameter bzw. SRP/CS-Eigenschaften (Manipulationsschutz, Zugangssicherung, Programm-/Datenschutz) und zum Schutz gegen unbefugtes Bedienen (Schlüsselschalter, Code usw.), z.B. bei Sonderbetriebsarten
5.13 Allgemeine technische Voraussetzungen und organisatorische Rahmenbedingungen für die Inbetriebnahme, Prüfung und Abnahme sowie Wartung und Instandhaltung

Quelle: Allgemeine Vorgabe, Auszug BGIA Report 2/2008 zu EN ISO 13849-1

Beispiel für einen Handhabungsautomaten

Funktionsbeschreibung: Der Handhabungsautomat dient zur automatischen Aufnahme von unterschiedlich hohen Lkw-Kabinen. Nach der Aufnahme wird die Höhe der Kabine sicher erfasst, damit im Arbeiterbereich die Kabine nicht unter eine bestimmte Höhe abgesenkt werden kann. Im Arbeiterbereich darf der Automat eine maximale Geschwindigkeit nicht überschreiten. Nachdem die Kabine fertig bearbeitet wurde, wird sie am Ende der Bearbeitungsstraße wieder abgesetzt und der Handhabungsautomat fährt über eine Rücklaufbahn wieder zum Anfang der Strecke zurück, um erneut eine Kabine aufzunehmen …

Grenzen der Maschine: Räumliche Grenzen: Im Arbeiterbereich muss genügend Raum für die Arbeiter vorhanden sein, um alle nötigen Arbeiten an der Kabine ausführen zu können ... Im Rücklauf muss genügend Raum für das leere Gehänge des Automaten vorhanden sein ...

Zeitliche Grenzen: Beschreibung der Lebensdauer, Beschreibung von Alterungsprozessen, die zur Änderung von Maschinenparametern führen können (z. B. Bremsen). Für solche Fälle müssen Überwachungsmechanismen vorgesehen werden.

Verwendungsgrenzen: Der Automat holt automatisch neue Kabinen und fährt sie durch einen Bearbeitungsbereich. Im Bearbeitungsbereich halten sich Arbeiter auf ... usw. Folgende Betriebsarten sind vorgesehen: Einrichtbetrieb, automatischer Betrieb und Servicebetrieb ... usw.

Identifizierung von Gefährdungen: Folgende mechanische Gefährdungen sind bei dem Handhabungsautomaten relevant: Gefährdung 1: Quetschen durch abfahrende Kabine / Hebebalken; Gefährdung 2: Stoßen durch fahrende Kabine / Hebebalken; Gefährdung 3: Quetschen durch zu schnelles Absenken der Kabine im Fehlerfall; Gefährdung 4: ...

Risikoanalyse: G1: Das Gewicht der Kabine und des Hebebalkens ist so hoch, dass es zu irreversiblen Quetschungen oder Todesfällen kommen kann. G2: Durch fahrende Kabinen / Hebebalken kann es zu Stößen mit irreversiblen Verletzungen kommen. G3: ...

Risikoabschätzung: Unter Berücksichtigung aller Betriebsbedingungen ist eine Risikominderung erforderlich.

Inhärent (Risiken aus dem Projekt) sichere Konstruktion: Das Bewegen der Kabine in x- und y-Richtung im Arbeiterbereich ist nicht vermeidbar. Im Bearbeitungsbereich muss die Kabine auf/ab und vorwärts bewegt werden ... Folgende Maßnahmen können ergriffen werden: Gefährdungen durch zu schnelle Bewegungen vermeiden; Gefährdungen durch zu geringe Abstände vermeiden; ...

12.3.3 Spezifikation des funktionalen Sicherheitssystems

Abgeleitet aus der allgemeinen Gefährdungs- und Risikoanalyse der Maschine sind die aktiven Schutzfunktionen zu identifizieren und zu spezifizieren.

Aktive Schutzfunktionen sind z. B. sicher reduzierte Geschwindigkeit in bestimmten Anlagenzuständen, überwachte Stopp- und Stillstandsfunktionen, Bereichsüberwachungen, Verarbeitung von Überwachungseinrichtungen wie Lichtgitter, Schaltmatten etc.

Die Sicherheitsfunktionen sind jeweils abzugrenzen und die spezifischen Anforderungen in Funktion und Sicherheitsniveau zu definieren.

12.3.3.1 Definition der Sicherheitsfunktionen

Die Definition der Sicherheitsfunktion muss

- das abzudeckende Risiko benennen,
- die genaue Funktion beschreiben,
- alle beteiligten Sensoren, Befehlsgeräte auflisten,
- alle Steuergeräte benennen,
- den angesprochenen Abschaltkreis bezeichnen.

enthalten. Die Definition soll als Grundlage für die Spezifikation des HW- und Softwaredesigns dienen.

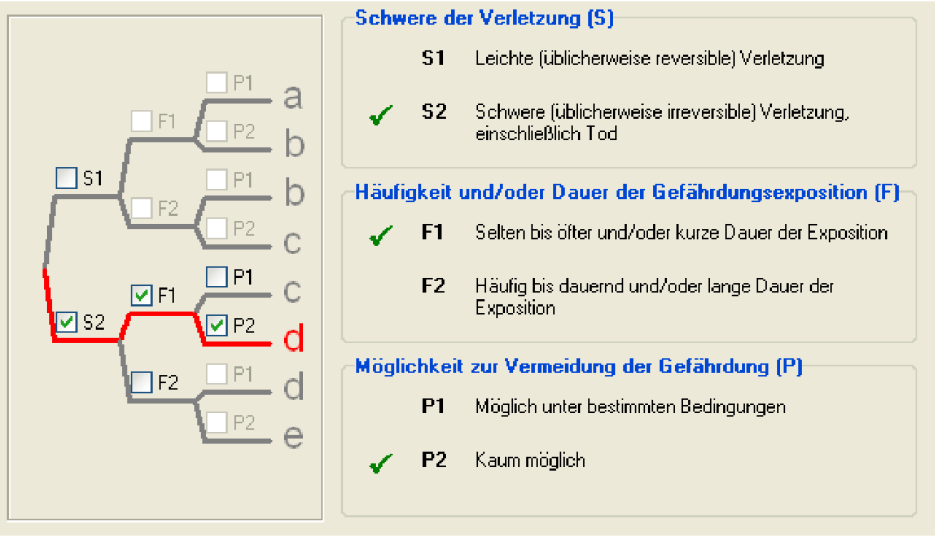
Für jede der so definierten Sicherheitsfunktionen sind die evtl. zu verwendenden Parameter wie z. B. max. Anlagengeschwindigkeit im Einrichtbetrieb etc. zu bestimmen.

Beispiele für Sicherheitsfunktionen:

- SF1: STO (sicher abgeschaltetes Moment) zum Schutz gegen sicheres Anlaufen
- SF2: Sichere Geschwindigkeiten
- SF3: Sichere Positionen
- SF4: ...

12.3.3.2 Erforderlicher Performance Level (PLr) (zusätzlich Not-Halt)

Aus den oben erkannten Sicherheitsfunktionen SF1 ... muss nun der erforderliche Performance Level bestimmt werden. Aus dem Beispiel unten ist der Entscheidungsweg ersichtlich.



Beispiel für SF1: Ergebnis PL = d (Quelle Sistema)

12.3.3.3 Beispiel – Spezifikation der Sicherheitsfunktionen in Tabellenform

Lfd.-Nr.	Sicherheitsfunktion	Ref aus GFA	PLr	Messwert / Sensor	Umsetzung in Software	Soll-Parameter	Eingang / Aktivierung	Reaktion / Ausgang
1.1	Begrenzung der max. Fahrgeschwindigkeit Fahrwerk auf Überwachung der maximalen Geschwindigkeit	2.3	e	1 × WCS Absolutencoder; 1 × Inkrementalencoder an Motor / Antriebsrad	Überwachung mittels geprüfter Sicherheitsfunktion SLS auf feste Grenzen:	550 mm/s; Fehlerdistanz überwachung: 200 mm	Ständig; Reset: Quittierungstaster	Betriebsstop; SF 1.7.1
1.2	Begrenzung der max. Fahrgeschwindigkeit Fahrwerk im Werker-Arbeitsbereich; Überwachung der maximalen Geschwindigkeit auf < 0,33 m/s	2.4	e	1 × WCS Absolutencoder; 1 × Inkrementalencoder an Motor / Antriebsrad	Überwachung mittels geprüfter Sicherheitsfunktion SLS auf feste Grenzen:	60 mm/s; Fehlerdistanz überwachung: 200 mm	Identifizierung Werker-Arbeitsbereich über Position Fahrwerk UND NICHT Einrichten; Reset: Quittierungstaster	SF 1.7.1
1.3	Begrenzung der max. Fahrgeschwindigkeit Fahrwerk im Einrichtbetrieb; Überwachung der maximalen Geschwindigkeit auf < 0,07 m/s	3.1	d	1 × WCS Absolutencoder; 1 × Inkrementalencoder an Motor / Antriebsrad	Überwachung mittels geprüfter Sicherheitsfunktion SLS auf feste Grenzen:	70 mm/s; Fehlerdistanz überwachung: 200 mm	Betriebsart Einrichten UND Taster „Sicherheit brücken“; Reset: Quittierungstaster	SF 1.7.1

Lfd.-Nr.	Sicherheitsfunktion	Ref aus GFA	PLr	Messwert / Sensor	Umsetzung in Software	Soll-Parameter	Eingang / Aktivierung	Reaktion / Ausgang
1.4	Auffahrschutz Fahrwerk; Überwachung der Abstände der Fahrwerke auf Mindestabstand mittels redundanter Laserabstandsmessung	2.5	d	2 × Laserdistanzmesseinrichtungen	Überwachung der Abstände mittels geprüfter Funktion SAC. Die analogen Messwerte Distanz werden gegenseitig auf max. Toleranz verglichen (Diagnose Analogsensor); auf Mindestwerte überwacht (Funktion SAC)	Min. Distanzwert 25 % des max. Wertes Messeinrichtung	Fahrwerk innerhalb Werker-Arbeitsbereich; Reset: Quittierungstaster	SF 1.7.1
1.6.1	Überwachung Sensorsystem Fahrwerk (* der beiden Sensoren Fahrwerk)	5.1	e	1 × WCS Absolutencoder; 1 × Inkrementalencoder an Motor / Antriebsrad	Muting der Diagnosen für beide Sensoren Fahrwerk mittels geprüfter Funktion SCA. Vor jeder Lücke wird Muting gestartet, ein falscher Geberwert dann kurzzeitig unterdrückt. In der Lücke führt ein Geberwert außerhalb 2 bis 160000 mm zum Muting		Pos 1 (7626 - 7850); Pos 2 (11030-1263); Pos 3 (75134-5338); Pos 4 (145562-145622); Pos 5 (143935-143995); Pos 6 (80000-80060)	SF 1.6.2

12.3.4 Softwarespezifikation

Die Softwarespezifikation bezieht sich auf die vorangegangene Spezifikation der Sicherheitsfunktionen. Sie kann auch ersetzt werden durch eine entsprechend ausgearbeitete Spezifikation der Sicherheitsfunktionen, sofern diese alle Vorgaben enthält (siehe Beispiel unter 12.3.3.3).

Es wird jedoch empfohlen, eine extrahierte Liste zu erstellen. Diese sollte folgende Angaben enthalten:

- Bezeichnung der Sicherheitsfunktion
- Funktionsbeschreibung
- Parameter, soweit vorhanden
- Auslösendes Ereignis / Betriebszustand
- Reaktion / Ausgang

Die Spezifikation sollte in der Detaillierung geeignet für eine spätere Validierung der Programmierung sein.

Beispiel Softwarespezifikation

Lfd.-Nr.	Sicherheitsfunktion	PLr	Messwert / Sensor	Lösung neu	Eingang / Aktivierung	Reaktion / Ausgang
1.4	Überwachung V_Seil zu V_Soll; Überwachung der Differenz zwischen Geschwindigkeit Hauptantrieb und Seiltrieb auf Maximalwert	d	Digitaler Inkrementalencoder, Tachogenerator Seilscheibe	Überwachung mittels geprüfter Funktion SLS + SAC mit Vergleich von Geschwindigkeitsbereichen / Analogwertbereichen = Vergleich zur Diagnose der Geschwindigkeitserfassung. Abschaltung 2-kanalig neu (siehe unten)	Ständig; Reset: Quittierungstaster	Betriebsstop SF 1.3.1
1.6	Rücklaufsperre; Überwachung auf Rücklauf	d	Mechanischer Endschalter 22S2; digitaler Inkrementalencoder	Überwachung mittels geprüfter Funktion Richtungsüberwachung SDI	NOT (Hilfskontakt 28K4 – Revisionsfahrt); Reset: Quittierungstaster	Betriebsstop SF 1.3.1
1.15	Stufenweise Abschaltung 3; Aktivieren der Sicherheitsbremse	e	–	Verarbeitung von SF in SafePLC	SF 1.2, SF 1.3.2, SF 1.7, SF 1.8	Setzen Sicherheitsbremse
1.8	Stillstand funktional	d	Digitaler Inkrementalencoder	Stillstandsüberwachung mittels geprüfter Funktion SOS	Reglersperre OR Betriebsbremse setzen	SF 1.15 / Sicherheitsbremse setzen
1.9	Richtungsüberwachung	e	Digitaler Inkrementalencoder	Überwachung mittels geprüfter Funktion Richtungsüberwachung SDI	28K1 = VOR, 28K2 = ZURÜCK = sichere Signale von Steuerung „Frey“	Betriebsstop SF 1.3.1

12.3.5 Hardwarespezifikation

In der Hardwarespezifikation soll der gesamte Anlagenaufbau und insbesondere die hier verwendeten Komponenten mit deren spezifischen Kenndaten beschrieben werden. Die Hardwarespezifikation dient als Grundlage für die Bestimmung des erreichten Sicherheitsniveaus auf Basis der Architektur und der Kenndaten aller an einer Sicherheitsfunktion beteiligten Geräte.

In der Hardwarespezifikation sind weiter auch die konstruktiven Maßnahmen zum Schutz gegen systematische und Common-Cause-Fehler zu benennen.

12.3.5.1 Auswahl SRP/CS und Betriebsmittel

Die Auswahl der SRP/CS (safety related parts of control system) ist geeignet für die Erzielung des angestrebten Sicherheitsniveaus für jede Sicherheitsfunktion zu treffen. In einer Gesamtübersicht des Anlagenaufbaus sind die Komponenten mit sicherheitsrelevanter Funktion zu bezeichnen und den einzelnen Sicherheitsfunktionen zuzuordnen. Für diese Komponenten sind die sicherheitstechnischen Kennzahlen zu ermitteln.

Die Kennzahlen umfassen folgende Werte:

Kennzahl	Bedeutung
MTTFd	mean time to failure, die mittlere Zeit bis zum gefahrbringenden Ausfall
DCavg	Mittlerer Diagnosedeckungsgrad
CCF	common cause failure, Ausfall aufgrund gemeinsamer Ursache

Bei einer SRP/CS sind auch die Software und systematische Fehler zu betrachten.

Grundsätzlich ist eine Analyse der an einer Sicherheitsfunktion beteiligten SRP/CS nach dem Schema Sensor / PES / Aktuator durchzuführen.



12.3.5.2 Beispiel für Vorgabe HW

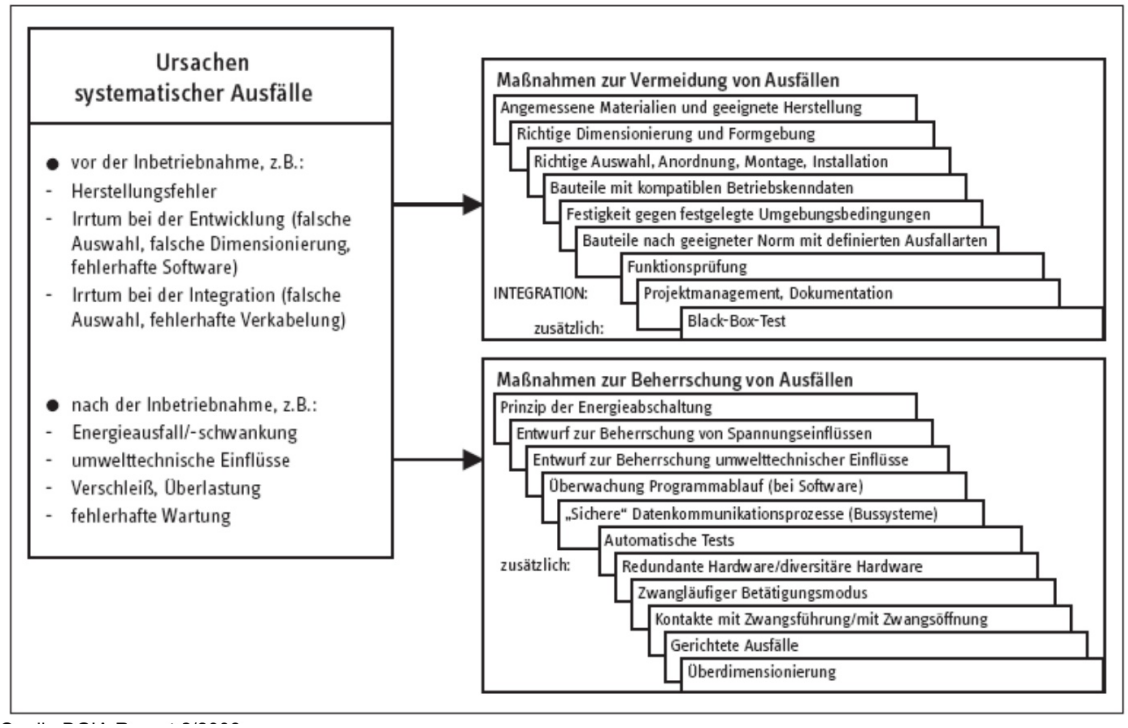
Sicherheitsfunktion: Sicher reduzierte Geschwindigkeit – SF 2.2 – Sicher überwachte limitierte Geschwindigkeit bei geöffneter Tür

Typ	Benennung	Funktion	Bezeichn.	Kenndaten	Anmerkung
Sensor	Sensor 1	Türzuhaltung – Überwachung der Zugangstür	A 3.1	Architektur 4; B10d 100000 (Quelle: Datenblatt); DC 99 % (Quelle: Inst.Handb. ESMD)	
	Sensor 2.1	Inkrementalencoder – Motor-Feedback SIN/COS	G 1.1	Architektur 4; MTTFd 30 Jahre (Quelle: Allg. Vorgabe); DC 99 % (Quelle: Inst.Handb. ESMD)	Kat. 4 in Verbindung m. Ausw. ESMD
PES	Sicherheits-SPS	Zentrale Sicherheits-SPS für Steuerung und Auswertung von sicherheitsrelevanten Funktionen	A 4.1	PFH 1,4 E-8 1/h (Quelle: Datenblatt ESMD)	
Aktuator	STO	Safe Torque Off an Umrichter	A 5.1	Architektur 4; MTTFd 150 Jahre (Quelle: Datenblatt Umrichter); DC 99 % (Quelle: Inst.Handb. ESMD)	Kat. 4 in Verbindung m. 2. Kanal
	Netzschütz	Schütz in Netzleitung des Umrichters	K 5.1	Architektur 4; B10d 20 E6 (Quelle: Datenblatt Schütz); DC 99 % (Quelle: Inst.Handb. ESMD)	Kat. 4 in Verbindung m. 2. Kanal

12.3.5.3 Betrachtung von systematischen Ausfällen

Innerhalb der HW-Spezifikation sind weiter auch systematische Ausfälle zu betrachten.

Beispiel zu Maßnahmen gegen systematische Ausfälle: Energieabfall während des Betriebs. Ist hier eine Gefährdung gegeben, muss ein Energieabfall wie ein Betriebszustand betrachtet werden. Die SRP/CS muss diesen Zustand beherrschen, so dass der sichere Zustand erhalten bleibt.



Maßnahmen gegen systematische Ausfälle nach Anhang G DIN EN ISO 13849-1 (Quelle BGIA Report 2/2008)

Fehlerausschlüsse: Werden für bestimmte Geräte oder Anlagenkomponenten Fehlerausschlüsse getroffen, so sind diese im Einzelnen zu benennen und zu spezifizieren. Fehlerausschlüsse können z. B. mech. Wellenbruch, Klebenbleiben von Schaltkontakten, Kurzschlüsse in Kabeln und Leitungen usw. sein.

Die Zulässigkeit der Fehlerausschlüsse soll begründet werden, z. B. durch Referenzierung auf zulässige Fehlerausschlüsse nach einschlägigen Normen (z. B. EN ISO 13849-1). Sind für diese Fehlerausschlüsse gesonderte Maßnahmen erforderlich, so sind diese zu benennen.

Beispiele für Fehlerausschlüsse und zugeordnete Maßnahmen:

- Formschlüssige Verbindung bei mech. Wellenverbindungen
- Dimensionierung auf Basis ausreichender theoretischer Grundlagen bei Bruch von Komponenten der Sicherheitskette
- Zwangsführung in Verbindung mit Zwangstrennung bei Klebenbleiben von Schaltkontakten
- Geschützte Verlegung innerhalb der Schaltanlage bei Kurzschlüssen in Kabeln und Leitungen sowie Verlegung von Kabeln in Kabelschächten

12.3.6 Hard- und Softwaredesign

Die Umsetzung der Vorgaben aus den HW- und SW-Spezifikationen erfolgt im eigentlichen Anlagendesign.

Die Vorgaben für die zu verwendenden Komponenten und deren Verschaltung aus der HW-Spezifikation sind ebenso einzuhalten wie die Vorgaben für die Fehlerausschlüsse. Beides ist mit geeigneten Mitteln sicherzustellen und zu dokumentieren.

In der Software sind ebenso die Vorgaben aus der SW-Spezifikation zu beachten und komplett umzusetzen.

Weiter sind hier die übergeordneten Vorgaben an die SW von sicherheitstechnischer Programmierung zu beachten. Dies sind u. a.:

- Aufbau des Programms modular und klar strukturiert
- Zuordnung von Funktionen zu den Sicherheitsfunktionen
- Verständliche Darstellung der Funktionen durch: eindeutige Bezeichnungen, verständliche Kommentierungen
- Weitestgehende Verwendung von geprüften Funktionen / Funktionsbausteinen
- Defensive Programmierung

12.3.7 Prüfung des HW-Designs

Nach Abschluss der Planung ist das HW-Design auf die Einhaltung der Vorgaben aus der HW-Spezifikation zu prüfen.

Weiter ist die Einhaltung des spezifizierten Sicherheitsniveaus für jede einzelne Sicherheitsfunktion durch geeignete Analyse zu prüfen. Die Analyseverfahren sind in den einschlägigen Normen beschrieben (z. B. EN ISO 13849-1).

Analyse Schaltplan: Anhand des Schaltplans und der Stückliste ist die Einhaltung der Vorgaben in sicherheitstechnischer Hinsicht zu überprüfen. Insbesondere ist zu prüfen:

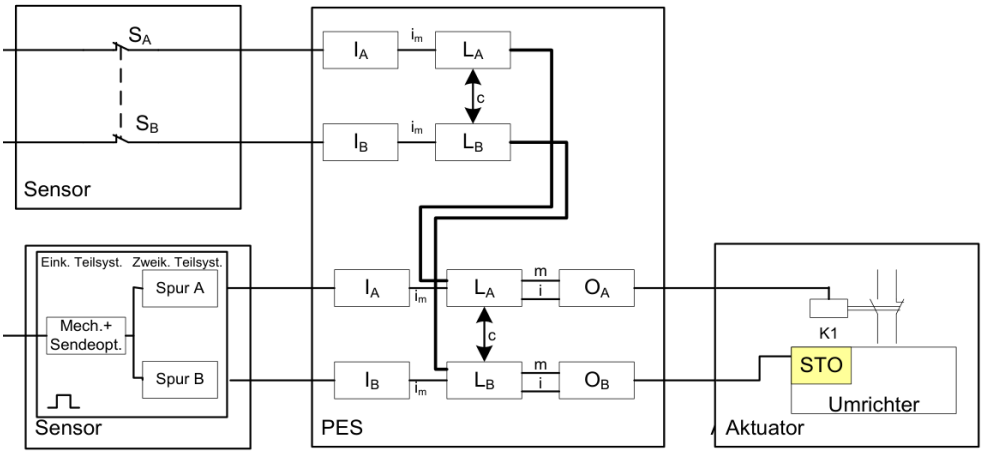
- die korrekte Verschaltung der Komponenten gemäß Vorgabe,
- der zweikanalige Aufbau, soweit vorgegeben,
- die Rückwirkungsfreiheit von parallelen, redundanten Kanälen,
- die Verwendung der Komponenten gemäß Vorgabe.
- Die Prüfung soll durch nachvollziehbare Analyse erfolgen.

Iterative Überprüfung des erreichten Sicherheitsniveaus: Das erreichte Sicherheitsniveau ist anhand des Schaltungsaufbaus (= Architektur einkanalig / zweikanalig / mit oder ohne Diagnose), der Gerätekenndaten (Angaben Hersteller oder einschlägige Quellen) und des Diagnosedeckungsgrads (Angabe Hersteller PES oder allgemeine Quellen) zu ermitteln. Die einschlägigen Verfahren sind der zugrunde gelegten Sicherheitsnorm zu entnehmen.

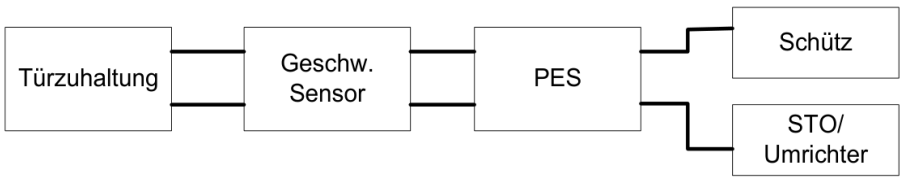
Beispielhaft ist eine Berechnung nach EN ISO 13849-1 dargestellt:

Sicherheitsfunktion: Sicher reduzierte Geschwindigkeit bei geöffneter Zugangstür

Aufbauschema:



Sicherheitstechnisches Aufbauschema:



Berechnung nach EN ISO 13849-1:

Kanal A – Abschaltung über Netzschütz:

Komponente	$MTTF_d$ [Jahre]	DC
Türschutz-schalter[1]	B_{10d} = 100000 n_{op} = 30/AT = 9270/Jahr (309 AT/Jahr)	DC_{Switch} = 99%

$$MTTF_d = \frac{B_{10d}}{0{,}1 * n_{op}} = 107{,}87 \text{ Jahre}$$

SIN/COS-Encoder	$MTTF_d$ = 30 Jahre	$DC_{Encoder}$ = 99%
PES[2]	$\lambda_d = 1884{,}21$ fit	DC_{PES} = 94,5%

$$MTTF_d = \frac{10^9}{365 \cdot 24 \cdot \lambda_d} = 60{,}59 \text{ Jahre}$$

Netzschütz[3]	$B_{10d} = 1{,}3 \cdot 10^6$	$DC_{Contactor}$ = 60%

N_{op} = 20/AT = 6180/Jahr (309 AT/Jahr)

$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = 2103{,}56 \text{ Jahre}$$

$$MTTF_d^A = \frac{1}{\frac{1}{MTTF_d^{Switch}} + \frac{1}{MTTF_d^{Encoder}} + \frac{1}{MTTF_d^{PES}} + \frac{1}{MTTF_d^{Contactor}}} = 16{,}78 \text{ Jahre}$$

1 Wert für MTTFd aus EN ISO 13849-1, Tabelle C.1 · 2 Wert aus firmeninterner HW-FMEA · 3 Wert für MTTFd aus EN ISO 13849-1, Tabelle C.1; Annahme „worst case“ durch „Schütz mit nominaler Last“

Kanal B – Abschaltung über STO/Umrichter:

Komponente	$MTTF_D$ [Jahre]	DC
Türschutz-schalter	B_{10d} = 100000 n_{op} = 30/AT = 9270/Jahr (309 AT/Jahr) $MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = 107{,}87$ Jahre	DC_{Switch} = 99%
SIN/COS-Encoder	$MTTF_d$ = 30 Jahre	$DC_{Encoder}$ = 99%
PES	$\lambda_d = 1884{,}21$ fit $MTTF_d = \frac{10^9}{365 \cdot 24 \cdot \lambda_d} = 60{,}59$ Jahre	DC_{PES} = 94,5%
STO/Umrichter [4]	$MTTF_d$ = 150 Jahre	DC_{STO} = 90%

$$MTTF_d^B = \frac{1}{\frac{1}{MTTF_d^{Switch}} + \frac{1}{MTTF_d^{Encoder}} + \frac{1}{MTTF_d^{PES}} + \frac{1}{MTTF_d^{STO}}} = 15{,}20 \text{ Jahre}$$

Resultierender PL für beide Kanäle:

Symmetrisierung beider Kanäle:	$MTTF_d = \frac{2}{3}\left[MTTF_d^A + MTTF_d^B - \frac{1}{\frac{1}{MTTF_d^A} + \frac{1}{MTTF_d^B}}\right] = 16{,}00$ Jahre
DC Mittelwert	$DC_{avg} = \frac{\sum_i \frac{DC_i}{MTTF_i}}{\sum_i \frac{1}{MTTF_i}} = 97{,}2\ \%$
PL	$MTTF_d$ = 16,00 Jahre (mittel) DC_{avg} = 97,4 % (mittel) PL =“d“ (aus EN ISO 13849-1, Tabellen 5, 6 und 7) Bestimmend für den PL ist in diesem Fall der $MTTF_d$-Wert des Sin/Cos-Encoders. Soll ein höheres Sicherheitsniveau erzielt werden, ist ein entsprechend höher qualitativer Schalter zu verwenden.

Anmerkung: Die hier verwendeten charakteristischen Werte der einzelnen Komponenten wurden beispielhaft gewählt und müssen für Nutzeranwendungen entsprechend angepasst werden. · 4 Wert für MTTFd aus EN ISO 13849-1, Tabelle C.1

Hinweis Eine Ermittlung des PL ist u. a. auch mit dem Programmtool „Sistema“ der BGIA möglich.

12.3.8 Verifikation Software (Programm) und Parameter

Die Verifikation findet in zwei Schritten statt:

– Überprüfung des FUP in Bezug auf die spezifizierte Funktionalität

– Überprüfung des FUP gegen das AWL-Listing des Validierungsreports bzw. der vorgegebenen Parameter gegen die im Validierungsreport gelisteten

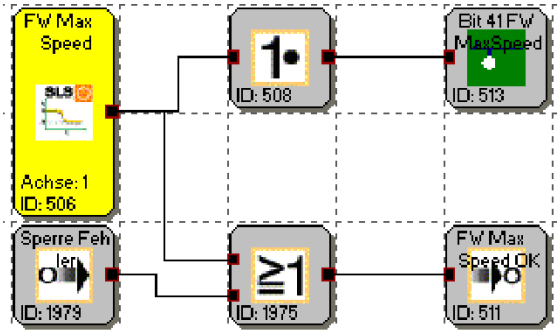
12.3.8.1 Überprüfung FUP

Zur Überprüfung ist der tatsächlich programmierte FUP gegen die Vorgaben der Spezifikation zu vergleichen.

Hinweis Der Vergleich ist umso effizienter, je deutlicher die Programmierung in Bezug auf die Sicherheitsfunktionen strukturiert wurde.

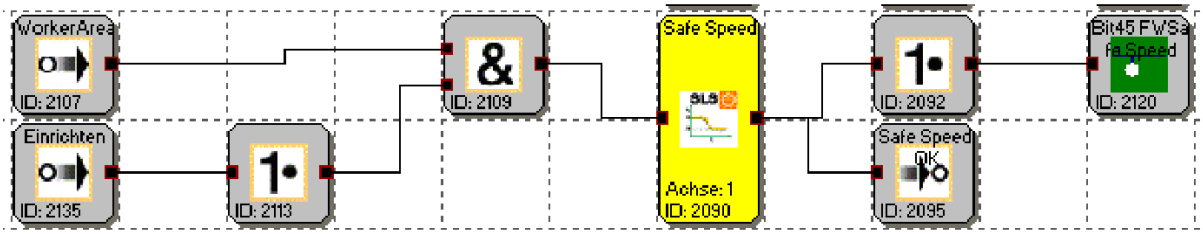
Beispiel – Sicherheitsfunktion: 1.1 Begrenzung der max. Fahrgeschwindigkeit Fahrwerk auf 1,1 VMax; Überwachung der maximalen Geschwindigkeit auf < 1,1 VMax

FW Max Speed OK (ID 548) (wird gebrückt durch Lücke vorhanden): FW Max Speed ist dauerhaft aktiviert und spricht dann an, wenn eine Geschwindigkeit von 550 mm/s überschritten wird.



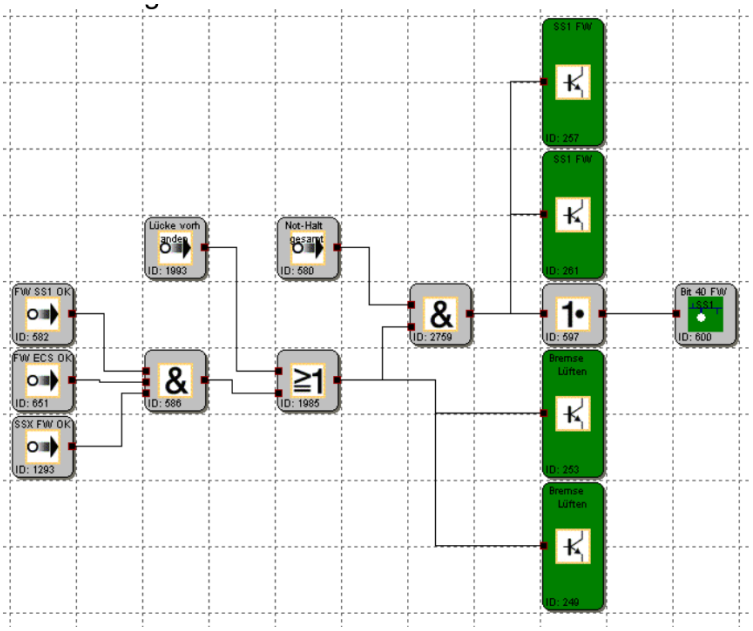
Sicherheitsfunktion: Begrenzung der max. Fahrgeschwindigkeit Fahrwerk im Werker-Arbeitsbereich; Überwachung der maximalen Geschwindigkeit auf < 0,33 m/s

Safe Speed OK (ID 2124) (wird gebrückt durch Lücke vorhanden): Safe Speed OK spricht an, wenn in der Workerarea und bei keinem Einrichten die sichere Geschwindigkeit SLS (ID 2090) überschritten wird.



Parameter SLS Safe Speed: 60 mm/s, keine weiteren Parameter

Sicherheitsfunktion: Abschaltung Fahrwerk; Abschaltung Fahrantrieb und Deaktivieren Bremsen; Abschaltungen am Fahrwerk



Das Fahrwerk wird über zwei Ausgänge abgeschaltet (EAA1.5 ID 257 und 1.6 ID 261).

Die Bremsen werden über zwei Ausgänge gelüftet (EAA1.3 ID 253 und 1.4 ID 249).

Es erfolgt eine Meldung an die SPS über Bit 40 (ID 600).

Bei Not-Halt wird die Abschaltung sofort ausgeführt.

Hubwerk – Sicherheitsfunktion: Not-Aus-Taster Eingänge und Abschaltausgänge; Not-Aus Kopfsteuerung

Zweikanaliger Not-Aus mit Pulsüberwachung. Wird an der übergeordneten Steuerung ein Not-Aus ausgelöst, kann dieser Not-Aus mit Zustimmung „Sicherheit brücken" überbrückt werden. Not-Aus-Taster Kopfsteuerung: Not-Aus-Kontakte vom Not-Aus-Relais mit Pulsen von der Baugruppe.

12.3.8.2 Validieren FUP gegen AWL und Parameter mittels Validierungsreport

Die im FUP erfolgte Programmierung ist jeweils mit dem AWL-Listing des Validierungsreports zu vergleichen.

Beispiel AWL-Listing im Validierungsreport (Validierungsreport – PLC Programm)

Index	Befehl	Operand	validiert
1	**S1**	**SLI_EN.1**	
2	**S1**	**SLI_EN.2**	
3	**S1**	**SLI_EN.3**	
4	**S1**	**SCA_EN.1**	
5	**S1**	**SCA_EN.2**	
6	**S1**	**SCA_EN.3**	
7	**S1**	**SLS_EN.2**	
8	**S1**	**SCA_EN.4**	
9	**S1**	**SLS_EN.3**	
10	**S1**	**SLS_EN.4**	
11	**S1**	**SLI_EN.5**	
12	**SQH**		
13	**LD**	**E0.1**	
14	**ST**	**MX.2**	
15	**SQC**		
16	**SQH**		
17	**LD**	**E0.3**	
18	**AND**	**E0.4**	
19	**ST**	**MX.3**	
20	**SQC**		

Es wird eine schrittweise Prüfung empfohlen. Die Prüfung ist umso effizienter, je strukturierter die Programmierung im FUP ausgeführt wurde.

Nach Prüfung des Programms sind die Parameter gegen die Vorgaben in der Spezifikation durch Vergleich zu prüfen.

Beispiel SLS: Validierungsreport – Safe Limited Speed (SLS)

Index	Parameter	Wert		validiert
SLS - 0	Gewählte Achse:	1		
	Geschwindigkeitsschwelle:	2	0	
SLS - 1	Gewählte Achse:	1		
	Geschwindigkeitsschwelle:	500	0	
SLS - 2	Gewählte Achse:	1		
	Geschwindigkeitsschwelle:	2	0	
	Beschleunigungsschwelle:	2	0	
SLS - 3	Gewählte Achse:	1		
	Geschwindigkeitsschwelle:	2	0	
	Zugeordnete SSX Rampe:	0		

Beispiel Geberkonfiguration: Validierungsreport – Achskonfiguration / Sensorinterface – Achse 1

Allgemeine Parameter	Wert	
Messstrecke:	500	0
Typ: Rotatorisch	Nein	
Positionsverarbeitung:	Aktiv	
Maximalgeschwindigkeit:	2000	0
Inkrementale Abschaltung:	10000	0
Abschaltung Geschwindigkeit:	100	0

Sensoren	0	0
Typ:	SSI-Standard	SSI-Standard
Format:	Binär	Binär
Drehrichtung:	Steigend	Steigend
Versorgungsspannung:	0	0
Auflösung:	1024 Schritte/1000mm	64 Schritte/1000mm
Offset:	0 Schritte	0 Schritte

- Allgemeine Parameter korrekt konfiguriert
- Parameter Sensor 1 korrekt
- Parameter Sensor 2 korrekt

12.3.9 Durchführung der Systemtests / FIT (fault injection test)

Für den FIT muss der Hersteller eine vollständige Liste von zu testenden Funktionen erstellen. Diese Liste umfasst die definierten Sicherheitsfunktionen sowie Fehlertests zur Überprüfung der richtigen Reaktion der SRP/CS auf diese Fehler.

Beispiele Testliste:

No	Setup	Test	Resultat
1 Test SLS für max. Geschw. Einrichtbetrieb	Aktivieren Einrichtbetrieb; Fahrt mit max. erlaubter Geschwindigkeit	Diagnose der tatsächlichen Geschwindigkeit versus SLS-Grenze; Manipulation der Einrichtgeschwindigkeit über erlaubte reduzierte Geschwindigkeit	
2 Test SSX für Stop-Kategorie 2	Fahrt mit max. Geschwindigkeit; Betätigen Not-Aus	Diagnose der SSX-Rampe gegen die tatsächliche Verzögerungsrampe; Einstellen einer unzulässig schwachen Verzögerung; Verfahren der Achse nach erreichtem Stillstand durch Manipulation des Antriebs	
3 Test der 2-kanaligen Türüberwachung	Betriebsmodus Einrichtbetrieb anwählen	Diagnose der inaktiven Überwachung bei geschlossener Tür (durch Diagnosefunktion FUP); Diagnose der aktiven Überwachung bei offener Tür (durch Diagnosefunktion FUP); Abklemmen eines Kanals und Öffnen der Tür; Querschluss zwischen beiden Eingängen erzeugen	

Anhang A Einstufung der Schaltertypen

Hinweis Die einzelnen Schalter der folgenden Eingangselemente können den digitalen Eingängen DI1 bis DI8 jeweils frei wählbar zugeordnet werden.

Zustimmtaster

Schaltertyp	Bemerkung	Einstufung PL nach EN ISO 13849-1	Einstufung SIL nach IEC 61508
1 Öffner	Zustimmschalter einfach	PL d	SIL 2
1 Schließer	Zustimmschalter einfach	PL d	SIL 2
2 Öffner	Zustimmschalter erhöhte Anforderung	PL e	SIL 3
2 Öffner Zeitüberwachung	Zustimmschalter überwacht	PL e	SIL 3

Not-Aus

Schaltertyp	Bemerkung	Einstufung Kategorie	Einstufung SIL
1 Öffner	Not-Aus einfach	PL d 1)	SIL 2
2 Öffner	Not-Aus erhöhte Anforderung	PL e	SIL 3
2 Öffner Zeitüberwachung	Not-Aus überwacht	PL e	SIL 3

1) Fehlerausschlüsse und Randbedingungen nach EN 13849-2 sind zu beachten!

Tür-Überwachung

Schaltertyp	Bemerkung	Einstufung Kategorie	Einstufung SIL
2 Öffner	Türüberwachung erhöhte Anforderung	PL e	SIL 3
2 Öffner Zeitüberwachung	Türüberwachung überwacht	PL e	SIL 3
1 Schließer + 1 Öffner	Türüberwachung erhöhte Anforderung	PL e	SIL 3
1 Schließer + 1 Öffner zeitüberwacht	Türüberwachung überwacht		SIL 3
2 Schließer + 2 Öffner	Türüberwachung erhöhte Anforderung	PL e	SIL 3
2 Schließer + 2 Öffner zeitüberwacht	Türüberwachung überwacht	PL e	SIL 3
3 Öffner	Türüberwachung erhöhte Anforderung	PL e	SIL 3
3 Öffner zeitüberwacht	Türüberwachung überwacht	PL e	SIL 3

Zweihandtaster

Schaltertyp	Bemerkung	Einstufung Kategorie	Einstufung SIL
2 Wechsler	Zweihandtaster erhöhte Anforderung	Typ III C PL e	SIL3
2 Schließer	Zweihandtaster überwacht	Typ III A PL e	SIL1

Hinweis: Bei diesen Eingangselementen findet eine feste Pulszuordnung statt, die vom Anwender nicht beeinflusst werden kann!

Lichtvorhang

Schaltertyp	Bemerkung	Einstufung Kategorie	Einstufung SIL
2 Öffner	Lichtvorhang erhöhte Anforderung	PL e	SIL 3
2 Öffner Zeitüberwachung	Lichtvorhang überwacht	PL e	SIL 3
1 Schließer + 1 Öffner	Lichtvorhang erhöhte Anforderung	PL e	SIL 3
1 Schließer + 1 Öffner zeitüberwacht	Lichtvorhang überwacht	PL e	SIL 3

Betriebsartenwahlschalter

Schaltertyp	Bemerkung	Einstufung Kategorie	Einstufung SIL
2 Stellungen	Betriebsartwahlschalter überwacht	PL e	SIL 3
3 Stellungen	Betriebsartwahlschalter überwacht	PL e	SIL 3

Sicherheitshinweis Beim Zustandswechsel des Schalters ist durch das zu erstellende Programm der Programmiersoftware sicherzustellen, dass die Ausgänge der Baugruppe deaktiviert werden (Hinweis: Norm 60204-Teil 1-Abschnitt 9.2.3).

Sensor

Schaltertyp	Bemerkung	Einstufung Kategorie	Einstufung SIL
1 Öffner	Sensoreingang einfach	PL d	SIL 2
1 Schließer	Sensoreingang einfach	PL d	SIL 2
2 Öffner	Sensoreingang erhöhte Anforderung	PL e	SIL 3
2 Öffner Zeitüberwachung	Sensoreingang überwacht	PL e	SIL 3
1 Schließer + 1 Öffner	Sensoreingang erhöhte Anforderung	PL e	SIL 3
1 Schließer + 1 Öffner zeitüberwacht	Sensoreingang überwacht	PL e	SIL 3

Start- / Resetelement

Schaltertyp	Bemerkung	Einstufung Kategorie	Einstufung SIL
1 Schließer	Alarm-Reset einfach (Auswertung Flanke)	–	–
1 Schließer	Logik-Reset einfach	PL d	SIL 2
1 Schließer	Startüberwachung einfach (Sonderfunktion)	–	–

Hinweis: Der Alarm-Reset-Eingang kann mit 24-V-Dauerspannung betrieben werden und ist flankengesteuert.