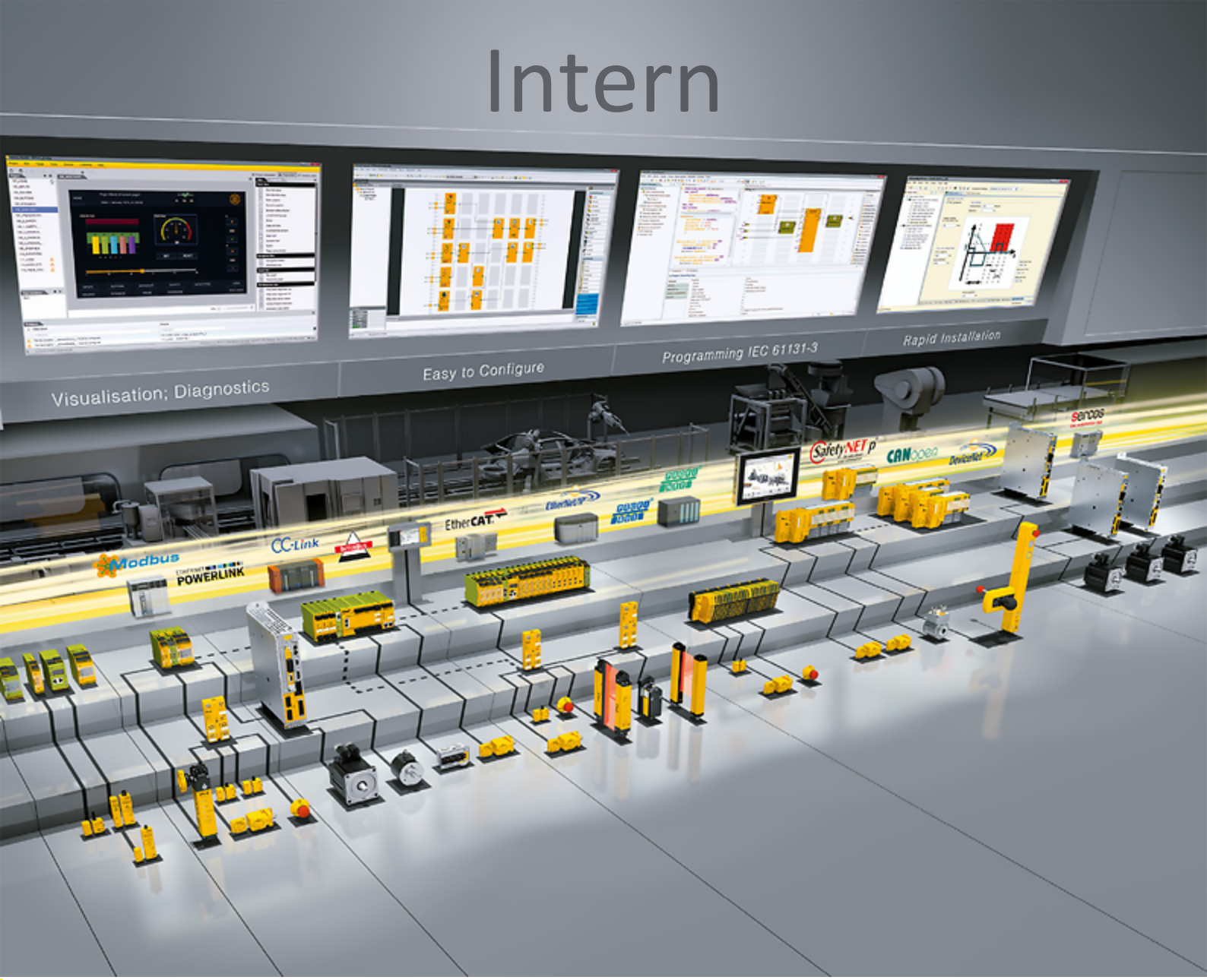
Intern



Sicherheitsmodul PMC SR6

Pilz

Handbuch-1005344-de-01

1 Vorwort

Das Sicherheitsmodul PMC SR6 erweitert Pilz Antriebsregler der Baureihe PMC SC6 oder PMC SI6 um die Sicherheitsfunktion **Safe Torque Off (STO)** (normativ in DIN EN 61800-5-2 beschrieben).

STO verhindert in einem Antriebsregler die Erzeugung eines elektrischen Drehfelds, das für den Betrieb von Synchron- oder Asynchronmotoren benötigt wird. Aufbauend auf STO sind, bei geeigneter externer Beschaltung, weitere Sicherheitsfunktionen, wie beispielsweise Safe Stop 1 (SS1-t), realisierbar.

Für die Ansteuerung von STO in einem Antriebsregler stehen unterschiedliche Schnittstellen zur Verfügung – unter anderem das klemmenbasierte Sicherheitsmodul PMC SR6.

PMC SR6 arbeitet als vollelektronische Lösung schnell und verschleißfrei. Das Sicherheitsmodul ist zudem derart konzipiert, dass regelmäßige, betriebsunterbrechende Systemtests entfallen.
Für die Praxis bedeutet dies eine gesteigerte Verfügbarkeit von Maschinen und Anlagen. Darüber hinaus entfällt die oft sehr aufwändige Planung und Dokumentation von Funktionstests.

Antriebsregler mit integriertem Sicherheitsmodul sind in sicherheitstechnisch anspruchsvollen Systemen bis SIL 3, PL e, Kategorie 4 einsetzbar. Die Übereinstimmung mit den normativen Anforderungen erfolgte durch ein externes Prüfinstitut im Rahmen einer Baumusterprüfung.

2 Benutzerinformationen

Diese Dokumentation bietet sämtliche Informationen zum bestimmungsgemäßen Einsatz des Antriebsreglers in Kombination mit dem Sicherheitsmodul PMC SR6.

2.1 Aufbewahrung und Weitergabe

Da diese Dokumentation wichtige Informationen zum sicheren und effizienten Umgang mit dem Produkt enthält, bewahren Sie diese bis zur Produktentsorgung unbedingt in unmittelbarer Nähe des Produkts und für das qualifizierte Personal jederzeit zugänglich auf.

Bei Übergabe oder Verkauf des Produkts an Dritte geben Sie diese Dokumentation ebenfalls weiter.

2.2 Beschriebenes Produkt

Diese Dokumentation ist verbindlich für:

Antriebsregler der Baureihe PMC SC6 oder PMC SI6 in Verbindung mit dem Sicherheitsmodul PMC SR6 und der Software DriveControlSuite (DS6) ab V 6.4-E und zugehöriger Firmware ab V 6.4-E.

2.3 Aktualität

Prüfen Sie, ob Ihnen mit diesem Dokument die aktuellste Version der Dokumentation vorliegt. Auf unserer Webseite stellen wir Ihnen die neuesten Dokumentversionen zu unseren Produkten zum Download zur Verfügung:
https://www.pilz.com/de-INT.

2.4 Originalsprache

Die Originalsprache dieser Dokumentation ist Deutsch; alle anderssprachigen Fassungen sind von der Originalsprache abgeleitet.

2.5 Haftungsbeschränkung

Diese Dokumentation wurde unter Berücksichtigung der geltenden Normen und Vorschriften sowie des Stands der Technik erstellt.

Für Schäden, die aufgrund einer Nichtbeachtung der Dokumentation oder aufgrund der nicht bestimmungsgemäßen Verwendung des Produkts entstehen, bestehen keine Gewährleistungs- und Haftungsansprüche. Dies gilt insbesondere für Schäden, die durch individuelle technische Veränderungen des Produkts oder dessen Projektierung und Bedienung durch nicht qualifiziertes Personal hervorgerufen wurden.

2.6 Darstellungskonventionen

Damit Sie besondere Informationen in dieser Dokumentation schnell zuordnen können, sind diese durch Orientierungshilfen in Form von Signalwörtern, Symbolen und speziellen Textauszeichnungen hervorgehoben.

2.6.1 Gebrauch von Symbolen

Sicherheitshinweise sind durch nachfolgende Symbole gekennzeichnet. Sie weisen Sie auf besondere Gefahren im Umgang mit dem Produkt hin und werden durch entsprechende Signalworte begleitet, die das Ausmaß der Gefährdung zum Ausdruck bringen. Darüber hinaus sind nützliche Tipps und Empfehlungen für einen effizienten und einwandfreien Betrieb besonders hervorgehoben.

ACHTUNG!

Achtung bedeutet, dass ein Sachschaden eintreten kann,

- wenn die genannten Vorsichtsmaßnahmen nicht getroffen werden.

VORSICHT!

Vorsicht mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann,

- wenn die genannten Vorsichtsmaßnahmen nicht getroffen werden.

WARNUNG!

Warnung mit Warndreieck bedeutet, dass erhebliche Lebensgefahr eintreten kann,

- wenn die genannten Vorsichtsmaßnahmen nicht getroffen werden.

GEFAHR!

Gefahr mit Warndreieck bedeutet, dass erhebliche Lebensgefahr eintreten wird,

- wenn die genannten Vorsichtsmaßnahmen nicht getroffen werden.

Information

Information bedeutet eine wichtige Information über das Produkt oder die Hervorhebung eines Dokumentationsteils, auf den besonders aufmerksam gemacht werden soll.

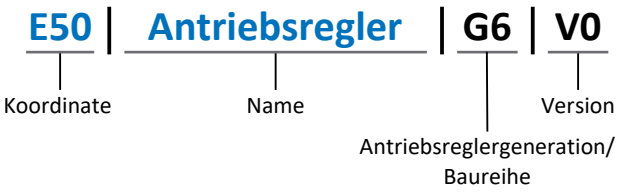
2.6.2 Auszeichnung von Textelementen

Bestimmte Elemente des Fließtexts werden wie folgt ausgezeichnet.

Wichtige Information	Wörter oder Ausdrücke mit besonderer Bedeutung
Interpolated position mode	Optional: Datei-, Produkt- oder sonstige Namen
Weiterführende Informationen	Interner Querverweis
http://www.musterlink.de	Externer Querverweis

Parameterkennung-Lesart

Eine Parameterkennung setzt sich aus nachfolgenden Elementen zusammen, wobei auch Kurzformen, d. h. die ausschließliche Angabe einer Koordinate oder die Kombination aus Koordinate und Name möglich sind.



2.6.3 Mathematik und Formeln

Zur Darstellung von mathematischen Zusammenhängen und Formeln werden die folgenden Zeichen verwendet.

-	Subtraktion
+	Addition
×	Multiplikation
÷	Division
| |	Betrag

3 Allgemeine Sicherheitshinweise

Von dem in dieser Dokumentation beschriebenen Produkt können Gefahren ausgehen, die durch die Einhaltung der beschriebenen Warn- und Sicherheitshinweise sowie der enthaltenen technischen Regeln und Vorschriften vermieden werden können.

3.1 Normen

Folgende Normen sind für das in dieser Dokumentation spezifizierte Produkt relevant:

- DIN EN ISO 13849-1:2016
- DIN EN ISO 13849-2:2013
- DIN EN 61800-5-2:2017-11
- DIN EN 61508-x:2011
- DIN EN 60204-1:2007
- DIN EN 62061:2016

Aus Gründen der besseren Lesbarkeit wird bei nachfolgenden Normverweisen auf die Angabe der jeweiligen Jahreszahl verzichtet.

3.2 Qualifiziertes Personal

Um die in dieser Dokumentation beschriebenen Aufgaben ausführen zu können, müssen die damit betrauten Personen fachlich entsprechend qualifiziert sein sowie die Risiken und Restgefahren beim Umgang mit den Produkten einschätzen können. Sämtliche Arbeiten an den Produkten sowie deren Bedienung und Entsorgung dürfen aus diesem Grund ausschließlich von fachlich qualifiziertem Personal ausgeführt werden.

Bei qualifiziertem Personal handelt es sich um Personen, die die Berechtigung zur Ausführung der genannten Tätigkeiten, entweder durch eine Ausbildung zur Fachkraft oder die Unterweisung durch Fachkräfte, erworben haben.

Darüber hinaus müssen gültige Vorschriften, gesetzliche Vorgaben, geltende Regelwerke, diese Dokumentation sowie die in dieser enthaltenen Sicherheitshinweise sorgfältig gelesen, verstanden und beachtet werden.

3.3 Bestimmungsgemäße Verwendung

Das Sicherheitsmodul PMC SR6 ist mit Pilz Antriebsreglern der Baureihe PMC SC6 oder PMC SI6 kombinierbar. Das Modul muss EMV-gerecht verdrahtet werden.

Wird ein Antriebsregler mit dem integrierten Sicherheitsmodul PMC SR6 in einer sicherheitsrelevanten Anwendung eingesetzt, muss das Sicherheitsmodul von einem Sicherheitsschaltgerät oder einer Sicherheitssteuerung angesteuert werden.

GEFAHR!

Elektrische Spannung! Lebensgefahr durch Stromschlag!

Eine aktivierte Sicherheitsfunktion STO bedeutet lediglich eine unterbrochene Drehfelderzeugung am Motor. An diesem können immer noch hohe, gefährliche Spannungen anliegen.

- Stellen Sie sicher, dass spannungsführende Teile nicht berührt werden können.
- Muss die Versorgungsspannung abgeschaltet werden, beachten Sie die Anforderungen der DIN EN 60204-1.

Nicht bestimmungsgemäße Verwendung

Das Sicherheitsmodul darf nicht außerhalb des Antriebsreglers oder der geltenden technischen Spezifikationen betrieben werden.

Information

Mit dem Sicherheitsmodul PMC SR6 ist kein Not-Aus gemäß DIN EN 60204-1 möglich!
Beachten Sie diese Norm bei der Unterscheidung von **Not-Aus** und **Not-Halt** in Verbindung mit **Safe Torque Off**.

Modifikation

Als Anwender dürfen Sie das Sicherheitsmodul PMC SR6 weder baulichen noch technischen oder elektrischen Veränderungen unterziehen.

Wartung

Das Sicherheitsmodul ist wartungsfrei.
Treffen Sie geeignete Maßnahmen, um eventuelle Fehler in der Anschlussverdrahtung ermitteln oder ausschließen zu können (siehe Kapitel Überwachung der Anschlussverdrahtung).

Produktlebensdauer

Ein Antriebsregler mit integriertem Sicherheitsmodul muss 20 Jahre nach dem Produktionsdatum außer Betrieb genommen werden. Das Produktionsdatum eines Antriebsreglers entnehmen Sie dem zugehörigen Typenschild.

3.4 Außerbetriebsetzung

Beachten Sie bei sicherheitsgerichteten Anwendungen die Gebrauchsdauer T_M = 20 Jahre in den sicherheitstechnischen Kennzahlen.

4 Sicherheitsmodul PMC SR6

Das Sicherheitsmodul PMC SR6 erweitert den Antriebsregler um die Sicherheitsfunktion STO (Safe Torque Off). STO verhindert – im Fehlerfall oder auf externe Anforderung hin – die Entstehung eines Drehfelds im Leistungsteil des Antriebsreglers. Das Sicherheitsmodul schaltet den Antriebsregler in den Zustand STO.

Aufbauend auf STO können, bei geeigneter externer Beschaltung, weitere Sicherheitsfunktionen, wie beispielsweise SS1-t (Safe Stop 1) realisiert werden.

Merkmale

- Zwei einpolige digitale Eingänge zur Aktivierung der Sicherheitsfunktionen:
  - Sicher abgeschaltetes Moment – STO gemäß DIN EN 61800-5-2
  - Stoppkategorie 0 gemäß DIN EN 60204-1
- STO-Abschaltzeit < 20 ms
- Verschleißfrei

Zertifizierungen nach DIN EN 61800-5-2 und DIN EN ISO 13849-1

- Safety Integrity Level (SIL) (SIL) 3
- Performance Level (PL) (PL) e
- Kategorie 4

5 Systemaufbau und Funktionsweise

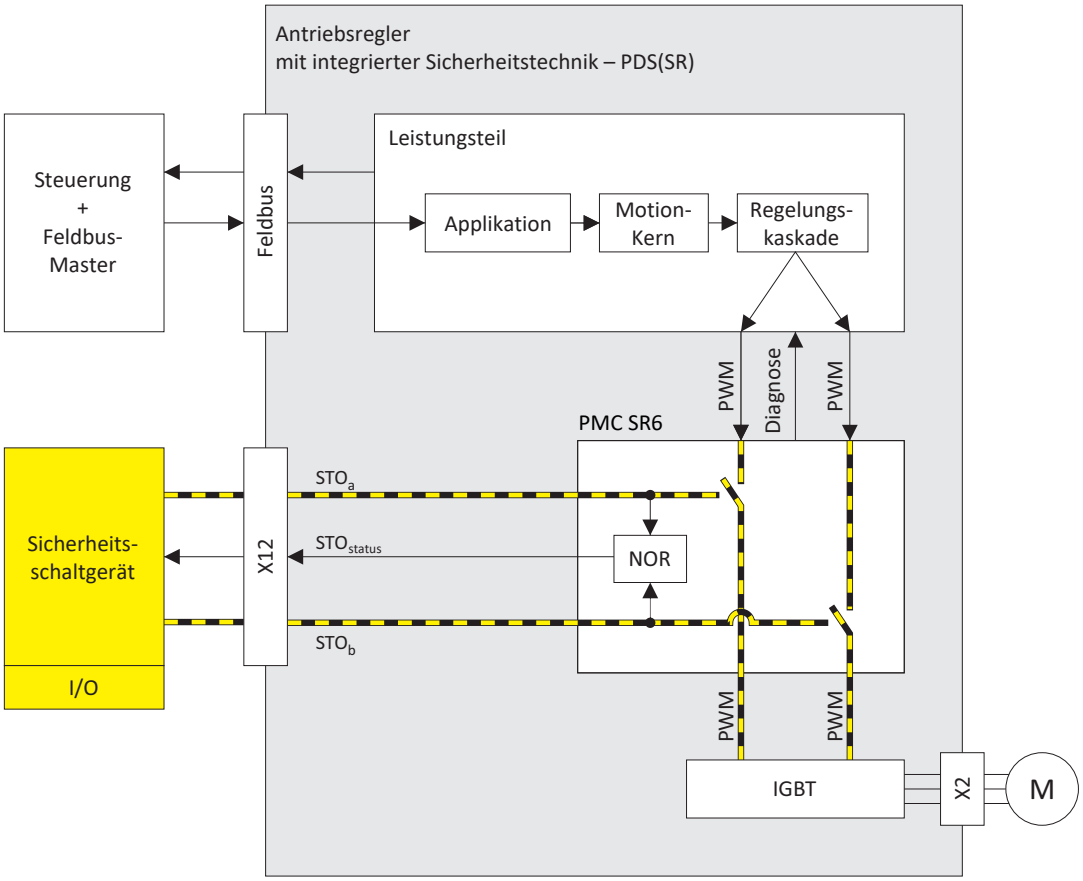


Abb. 1: Antriebsregler und Sicherheitsmodul (PDS(SR) – Systemaufbau

Funktionsweise

Das Steuerteil des Antriebsreglers generiert Pulsmuster (PWM) zur Erzeugung eines Drehfelds am IGBT-Modul des Leistungsteils. Dieses Drehfeld ist zum Betrieb von Synchron- und Asynchronmotoren notwendig.

Ist die Sicherheitsfunktion nicht aktiv, gibt das Sicherheitsmodul PMC SR6 die Drehfeldgenerierung im Leistungsteil frei; der angeschlossene Motor kann ein Drehfeld aufbauen. Ist die Sicherheitsfunktion aktiv, sperrt PMC SR6 die Drehfeldgenerierung im Leistungsteil und der Antriebsregler kann im angeschlossenen Motor kein Drehmoment erzeugen.

Die unmittelbare Abschaltung nach Not-Halt entspricht der Sicherheitsfunktion STO gemäß DIN EN 61800-5-2. In der DIN EN 60204-1 ist diese Art der Abschaltung als Stoppkategorie 0 definiert.

Ein zeitverzögertes Abschalten nach Not-Halt entspricht der Sicherheitsfunktion SS1-t gemäß DIN EN 61800-5-2. In der DIN EN 60204-1 ist diese Art der Abschaltung als Stoppkategorie 1 definiert.

WARNUNG!

Erhöhter Nachlaufweg! Restbewegung!

Das Sicherheitsmodul kann ein Versagen des funktionalen Teils des Antriebsreglers (z. B. beim gesteuerten Stillsetzen), während die Sicherheitsfunktion SS1-t ausgeführt wird, nicht verhindern. Deshalb kann SS1-t nicht angewendet werden, wenn dieses Versagen eine gefahrbringende Situation in der Endanwendung verursachen kann. Beachten Sie dies bei der Projektierung.

Bei einem Fehler im Leistungsteil des Antriebsreglers ist – trotz aktivem STO – eine statische Bestromung des Motors möglich, wobei sich die Motorwelle maximal um den Winkel 360° ÷ (p × 2) bewegen kann.

PMC SR6 – Design

Das Sicherheitsmodul PMC SR6 ist zweikanalig aufgebaut. Beide Sicherheitskanäle sind unabhängig voneinander und müssen an den zugehörigen Eingängen STO_a (Sicherheitskanal 1) und STO_b (Sicherheitskanal 2) zeitgleich angesteuert werden – entweder über potenzialfreie Kontakte direkt mit 24 V_{DC} oder alternativ über 24 V_{DC} Halbleiterausgänge mit überlagerter Testung.
Über die beiden Eingänge STO_a und STO_b wird die Drehfelderzeugung im Antriebsregler freigegeben oder gesperrt.

Überwachung der Anschlussverdrahtung

Um den Zustand der Anschlussverdrahtung und die Funktionalität der Sicherheitskanäle überprüfen zu können, stehen Statussignale zur Verfügung:

- Über Klemme X12 das Signal STO_{status}
  STO_{status} ist das Ergebnis einer NOR-Verknüpfung der beiden Eingänge STO_a und STO_b, d. h., der Ausgang STO_{status} ist immer dann 1 (High-Pegel), wenn der Eingang STO_a gleich 0 (Low-Pegel) und der Eingang STO_b gleich 0 (Low-Pegel) sind. Das Signal wird an Klemme X12 des Antriebsreglers ausgegeben.
- Über Parameter E67
  Bei Parameter E67 handelt es sich um einen Array-Parameter, der den detaillierten Zustand der beiden Sicherheitskanäle visualisiert.

Information

Werden die beiden STO-Eingänge über Ausgänge mit Testimpulsen, z. B. Interface-Typ C oder D, angesteuert, übernimmt die signalerzeugende Steuerung das Monitoring der Anschlussverdrahtung. Eventuelle Störungen werden direkt erkannt, und eine Auswertung der STO-Statussignale ist somit hinfällig.

6 Technische Daten

Die Transport-, Lager- und Betriebsbedingungen des Sicherheitsmoduls entnehmen Sie den technischen Daten des Antriebsreglers (siehe Kapitel Weiterführende Informationen).

6.1 Sicherheitsrelevante Kenngrößen

Die Tabelle beinhaltet die für die Sicherheitstechnik relevanten Kenngrößen des Moduls PMC SR6.

SIL CL	3
SIL	3
PL	e
Kategorie	4
PFH	5×10^{-9} [1/h]
Gebrauchsdauer (T_M)	20 Jahre

PMC SR6 – Sicherheitsrelevante Kenngrößen

6.2 Systemzeiten

Nachfolgendes Diagramm visualisiert die zeitlichen Relationen bei der STO-Ansteuerung und -Ausführung; die zugehörigen Werte für den Antriebsregler in Kombination mit dem Sicherheitsmodul PMC SR6 entnehmen Sie der anschließenden Tabelle.

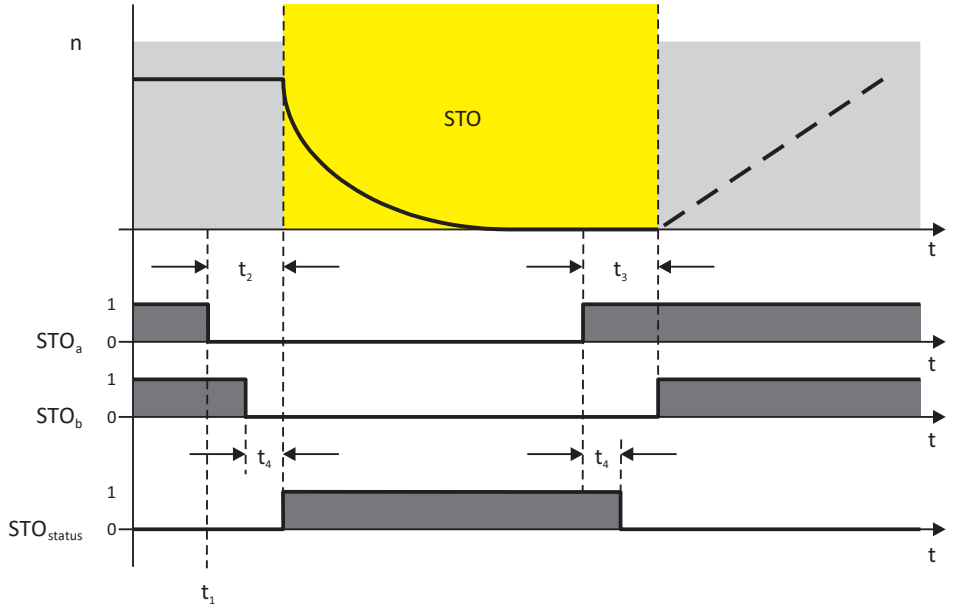


Abb. 2: STO – Zeitliche Relationen (Detaildarstellung)

t_1	STO-Auslösung
t_2	Maximale Reaktionszeit
t_3	Maximale Zeitdifferenz
t_4	Maximale Antwortzeit

Beachten Sie, dass Sie für die Berechnung einer Anwendungsfall-spezifischen Gesamtreaktionszeit die Reaktionszeiten der einzelnen Teilsysteme berücksichtigen müssen (siehe Kapitel SRP/CS: Die Verarbeitung einer typischen Sicherheitsfunktion [25]).

Maximale Reaktionszeit	20 ms
Maximale Zeitdifferenz	500 ms
Maximale Antwortzeit	20 ms

STO – Systemzeiten

6.3 Schnittstellenklassifizierung

Entsprechend der 24 V_{DC}-Schnittstellenklassifizierung des ZVEI kann das Sicherheitsmodul PMC SR6 als Informationssenke (Senke) der Interface-Typen C und D genutzt und über die Informationsquellen (Quellen) derselben Interface-Typen angesteuert werden.

Für PMC SR6 als Senke der Interface-Typen C und D gelten die in der Tabellen enthaltenen Werte[1]

	Min.	Typ.	Max.
Klasse		1	
Testimpulsdauer t_i	—	—	1000 µs
Testimpulsintervall T_i	10 ms	—	—
Eingangswiderstand R_1	300 Ω	—	—
Eingangskapazität C_1	—	—	1,5 nF
Eingangsinduktivität L_1	—	—	10 µH

PMC SR6 – Spezifische Kennzahlen zum Interface-Typ C

	Min.	Typ.	Max.
Klasse		1	
Testimpulsdauer t_i	—	—	1000 µs
Testimpulsintervall T_i	10 ms	—	—
Eingangswiderstand R_1	150 Ω	—	—
Eingangsstrom I_{1on} im EIN-Zustand	—	—	60 mA
Eingangsstrom I_{1off} im AUS-Zustand	—	—	1 mA
Eingangskapazität C_1	—	—	3 nF
Eingangsinduktivität L_1	—	—	5 µH

PMC SR6 – Spezifische Kennzahlen zum Interface-Typ D

[1] Siehe ZVEI, S. 16 und S. 19ff.

7 Anschluss

Das Sicherheitsmodul PMC SR6 wird über die Klemme X12 des Antriebsreglers angeschlossen.

Nähere Informationen zu Fehlern in der Anschlussverdrahtung, deren Ausschluss und einer STO-Funktionsprüfung entnehmen Sie dem Kapitel Überwachung der Anschlussverdrahtung [26].

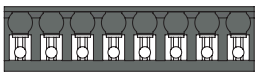
7.1 EMV-gerechter Anschluss

Beachten Sie für einen EMV-gerechten Anschluss die zugehörigen Empfehlungen in der Dokumentation des Antriebsreglers (siehe Kapitel Weiterführende Informationen [42]).

7.2 Klemme X12

Spezifikation	Elektrische Daten
STO_a	U_{1max} = 30 V_{DC} (PELV) High-Pegel = 15 – 30 V_{DC} Low-Pegel = 0 – 8 V_{DC} I_{1max} = 100 mA (typisch < 30 mA bei 24 V_{DC}) I_{max} = 4 A C_{1max} = 10 nF
STO_b	
STO_{status}	$U_2 = U_1 - (1{,}5\ \Omega * I_1)$
Versorgung STO_{status}	U_1 = +24 V_{DC}, +20 % / −25 % I_{1max} = 100 mA
GND	—

Elektrische Daten X12

Klemme	Pin	Bezeichnung	Funktion
 1|2|3|4|5|6|7|8	1	STO_a	Eingang Sicherheitskanal 1
	2		
	3	STO_b	Eingang Sicherheitskanal 2
	4		
	5	GND	Bezugspotenzial für STO_a und STO_b, intern gebrückt mit Klemme 7
	6	STO_{status}	Rückmeldesignal der Sicherheitskanäle 1 und 2 zu Diagnosezwecken
	7	GND	Bezugspotenzial für STO_a und STO_b, intern gebrückt mit Klemme 5
	8	$U_{1status}$	Versorgung STO_{status}; empfohlene Absicherung: max. 3,15 AT[2]

Anschlussbeschreibung X12

[2] Für einen UL-konformen Einsatz ist die Verwendung einer Sicherung 3,15 A (träge) Vorschrift. Die Sicherung muss nach UL 248 für DC-Spannung zugelassen sein.

Anschlussverdrahtung

Merkmal	Leitungstyp	Wert
Rastermaß	—	3,81 mm
Nennstrom bei ϑ_{amb} = 40 °C	—	CE/UL/CSA: 16 A/10 A/11 A
Max. Leiterquerschnitt	Flexibel ohne AEH	1,5 mm²
	Flexibel mit AEH ohne Kunststoffkragen	1,0 mm²
	Flexibel mit AEH mit Kunststoffkragen	1,0 mm²
	2 Leiter flexibel mit Doppel-AEH mit Kunststoffkragen	—
	AWG nach UL/CSA	16
Min. Leiterquerschnitt	Flexibel ohne AEH	0,14 mm²
	Flexibel mit AEH ohne Kunststoffkragen	0,25 mm²
	Flexibel mit AEH mit Kunststoffkragen	0,25 mm²
	2 Leiter flexibel mit Doppel-AEH mit Kunststoffkragen	—
	AWG nach UL/CSA	26
Abisolierlänge	—	10 mm
Anzugsdrehmoment	—	—

Spezifikation BCF 3,81 180 SN BK

Kabelanforderungen

Merkmal	Alle Baugrößen
Max. Kabellänge	30 m

Kabellänge [m]

Beschaltung X12

Das zweikanalige Design der PMC SR6 mit gemeinsamem Potenzialbezug unterstützt unterschiedliche Möglichkeiten der Anbindung. Diese sind abhängig davon, ob PMC SR6 kontaktbehaftet oder als Senke des Interface-Typs C oder D der Schnittstellenklassifizierung des ZVEI genutzt wird.

Nachfolgende Grafiken visualisieren die Ansteuerungsoptionen anhand entsprechender Schaltkontakte. Eine Ansteuerung über Halbleiterausgänge mit Testimpulsen ist ebenfalls zulässsig.

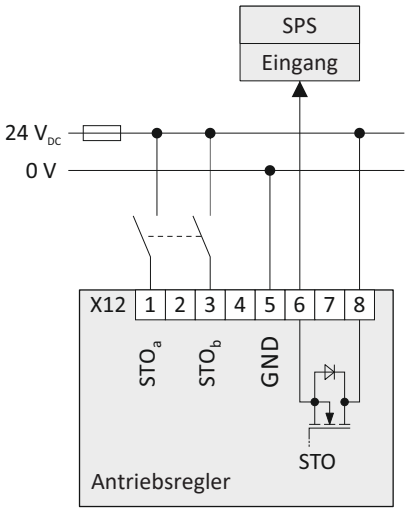


Abb. 3: Beschaltung X12 – PMC SR6 als Senke des Interface-Typs C

Die beiden Eingänge STO_a und STO_b werden über zwei getrennte Kanäle angebunden, das Bezugspotenzial GND ist fest verdrahtet.

Fehler in der Anschlussverdrahtung können bei kontaktbehafteter Schaltung nur teilweise erkannt werden. Kurzschlüsse von STO_a und STO_b gegen GND werden mithilfe der vorgeschalteten Sicherung identifiziert, gegen 24 V_{DC} bleiben sie unerkannt. Mögliche Kurz- und Querschlüsse sind lediglich durch Leitungs- oder Ausgangstests feststellbar.

Eine redundante Beschaltung gemäß Interface-Typ C deckt Kurz- und Querschlüsse in der Anschlussverdrahtung auf.

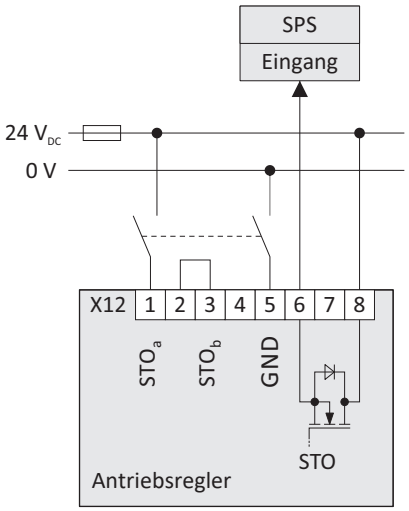


Abb. 4: Beschaltung X12 – PMC SR6 als Senke des Interface-Typs D

Die beiden Eingänge STO_a und STO_b werden gemeinsam angebunden, das Bezugspotenzial GND dient als zweiter unabhängiger Abschaltkanal.

Fehler in der Anschlussverdrahtung können bei kontaktbehafteter Ansteuerung nur teilweise erkannt werden. Mögliche Kurz- und Querschlüsse sind lediglich durch Leitungs- oder Ausgangstests feststellbar.

Eine Beschaltung gemäß Interface-Typ D deckt Kurz- und Querschlüsse in der Anschlussverdrahtung auf.

7.3 Parallelschaltung

Über den Ausgang eines Sicherheitsschaltgeräts besteht die Möglichkeit, STO an mehreren Antriebsreglern gleichzeitig zu aktivieren. In Abhängigkeit von der geforderten Sicherheitskennzahl ist eine Parallelschaltung von mehreren Antriebsreglern möglich.

WARNUNG!

Personen- und Sachschaden durch Verlust der Sicherheitsfunktion!

Bei einer Parallelschaltung können eventuelle Verdrahtungs- oder Ansteuerungsfehler zum Verlust der Sicherheitsfunktion aller Antriebsregler führen.

- Ergreifen Sie geeignete Maßnahmen, um Verdrahtungsfehler zu erkennen oder auszuschließen (siehe Kapitel Überwachung der Anschlussverdrahtung [26]).
- Beachten Sie, dass die STO_{status}-Ausgänge nicht für eine gemeinsame Auswertung in Reihe geschaltet werden können.

8 Inbetriebnahme

Wie Sie das Sicherheitsmodul PMC SR6 in Betrieb nehmen und die Sicherheitsfunktion STO aktivieren oder deaktivieren, entnehmen Sie diesem Kapitel.

Information

Bei dem Sicherheitsmodul handelt es sich um eine fest in den Antriebsregler integrierte Komponente, die weder baulich noch technisch oder elektrisch modifiziert werden darf!

Detaillierte Informationen zur Inbetriebnahme des Antriebsreglers erhalten Sie in der zugehörigen Inbetriebnahmeanleitung (siehe Kapitel Weiterführende Informationen).

8.1 Sicherheitsmodul und Antriebsregler in Betrieb nehmen

Um einen Antriebsregler mit dem integrierten Sicherheitsmodul PMC SR6 in Betrieb zu nehmen, verfahren Sie wie folgt.

1. Prüfen Sie, ob die projektierte Sicherheitstechnik den Sicherheitsanforderungen Ihres gesamten Systems genügt.
2. Verdrahten Sie die für die Sicherheitstechnik relevante Klemme X12 gemäß den in Kapitel Klemme X12 [16] enthaltenen Daten und schließen Sie eventuelle Verdrahtungsfehler aus (optional).
3. Schließen Sie den Antriebsregler an und nehmen Sie diesen in Betrieb. Detaillierte Informationen hierzu und damit verbunden zu sämtlichen relevanten Sicherheitshinweisen erhalten Sie in der zugehörigen Inbetriebnahmeanleitung.
4. Führen Sie initial einen STO-Funktionstest durch. Verfahren Sie hierzu wie in Kapitel Überwachung der Anschlussverdrahtung [26] samt zugehörigen Unterkapiteln beschrieben. Dokumentieren Sie Ihre Testergebnisse.

Information

Beachten Sie, dass die genannten Schritte auch vor jeder Wiederinbetriebnahme nach einem Tausch des Antriebsreglers und damit verbunden des Sicherheitsmoduls PMC SR6 ausgeführt und dokumentiert werden müssen!

8.2 STO aktivieren

Um die Sicherheitsfunktionen STO zu aktivieren, müssen die Ansteuersignale der Eingänge STO_a und STO_b abgeschaltet oder unterbrochen werden. Das Leistungsteil des Antriebsreglers kann nach der Reaktionszeit t_2 kein Drehfeld erzeugen, und der Motor ist drehmomentfrei (siehe auch Kapitel Systemzeiten [📖 14]).

Bevor der Antriebsregler wieder freigegeben werden kann, müssen die beiden Eingänge STO_a und STO_b für mindestens 100 ms deaktiviert werden.

GEFAHR!

Lebensgefahr durch schwerkraftbelastete Vertikalachsen oder Austrudeln des Motors!

Bei aktivierter Sicherheitsfunktion STO kann der Antriebsregler im Motor kein Drehmoment generieren. Somit sinken schwerkraftbelastete Vertikalachsen ab. Sollte sich der Motor bei einer STO-Aktivierung bewegen, trudelt er ungesteuert aus.

- Sichern Sie schwerkraftbelastete Vertikalachsen durch Bremsen oder ähnliche Maßnahmen.
- Stellen Sie sicher, dass durch das Austrudeln des Motors keine Gefahren entstehen.

8.3 STO deaktivieren

Um die Sicherheitsfunktion STO zu deaktivieren, müssen die Eingänge STO_a und STO_b innerhalb von 500 ms mit 24 V_{DC} angesteuert werden.

Ist die Sicherheitsfunktion deaktiviert, kann das Leistungsteil des Antriebsreglers am Motor das für eine aktive Bewegung notwendige Drehmoment erzeugen.

9 PMC SR6 und SS1

Das Sicherheitsmodul PMC SR6 bietet die Möglichkeit, bei geeigneter externer Beschaltung weitere Sicherheitsfunktionen, wie beispielsweise SS1-t, zu realisieren. Die Sicherheitsfunktion SS1-t nach DIN EN 61800-5-2 entspricht der Stoppkategorie 1 nach DIN EN 60204-1. Beide basieren auf STO.

Nachfolgendes Diagramm visualisiert die zeitlichen Abläufe während der Ansteuerung eines Antriebsreglers, um die Sicherheitsfunktion SS1-t zu realisieren.

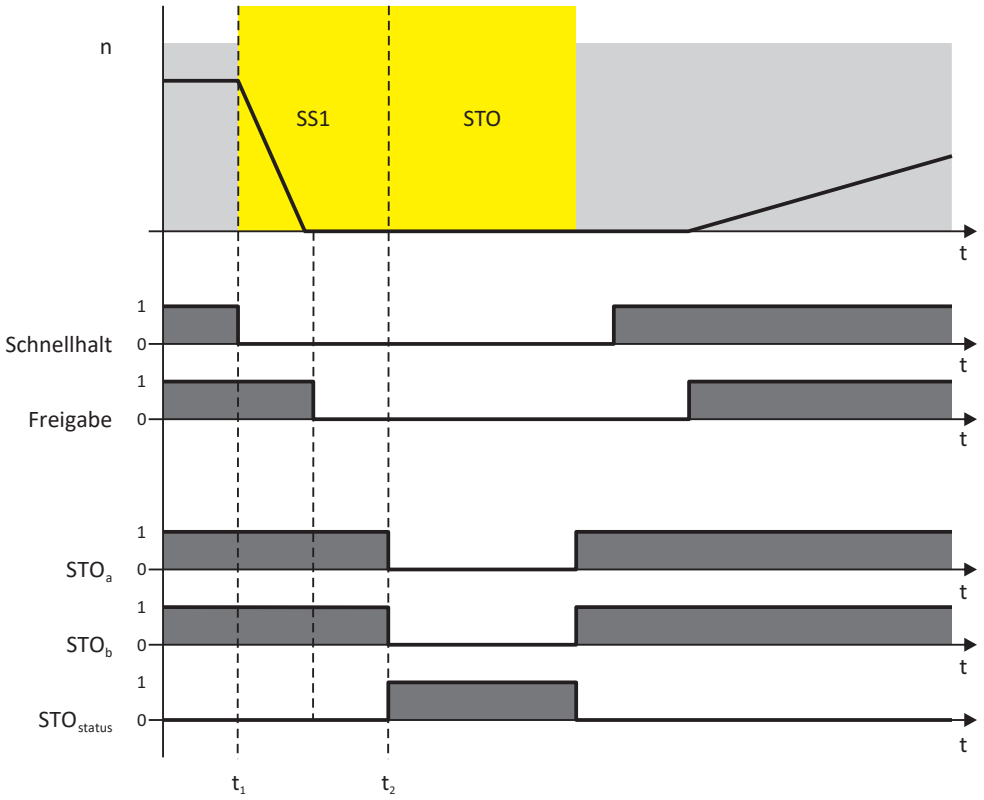


Abb. 5: PMC SR6 und SS1-t – Zeitlicher Ablauf

t_1	SS1-Auslösung
t_2	STO-Auslösung

Die Sicherheitsfunktion SS1-t besteht aus 2 Teilen:

- Teil 1: gesteuertes Stillsetzen
- Teil 2: sicheres Abschalten des Antriebsreglers (STO)

Ein Sicherheitsschaltgerät aktiviert im Antriebsregler zum Zeitpunkt t_1 z. B. über die Funktion **Schnellhalt** ein gesteuertes Stillsetzen. Nachdem die projektierte Zeit SS1-t im Sicherheitsschaltgerät abgelaufen ist, wird STO zum Zeitpunkt t_2 aktiviert. Dieser Prozess entspricht einem in DIN EN 61800-5-2 definierten **zeitgesteuerten SS1-t**.

10 Diagnose

10.1 Parameter

Folgende Anzeigeparameter sind für die Sicherheitstechnik in Kombination mit dem Sicherheitsmodul PMC SR6 von Bedeutung.

10.1.1 E53 | Soll-Sicherheitsmodul | V3

Projektiertes Sicherheitsmodul.

10.1.2 E54 | Information Sicherheitsmodul | V0

Kennzeichnende Daten des Sicherheitsmoduls.

- [0]: Typ
- [1]: Hardware-Version
- [2]: Produktionsnummer
- [3] – [5]: Reserviert
- [6]: Diagnose-Code

10.1.3 E67 | STO aktiv | V0

STO-Zustand des Sicherheitsmoduls:

- [0]: STO wurde durch das Eingangssignal STO_a = 0 oder STO_b = 0 ausgelöst
  - 0: Inaktiv = nicht ausgelöst
  - 1: Aktiv = ausgelöst
- [1]: STO wurde durch das Eingangssignal STO_a = 0 ausgelöst
  - 0: Inaktiv = nicht ausgelöst
  - 1: Aktiv = ausgelöst
- [2]: STO wurde durch das Eingangssignal STO_b = 0 ausgelöst
  - 0: Inaktiv = nicht ausgelöst
  - 1: Aktiv = ausgelöst

10.2 Ereignisse

Der Antriebsregler verfügt über ein System zur Selbstüberwachung, das anhand von Prüfregeln das Antriebssystem vor Schaden schützt. Bei Verletzung der Prüfregeln wird ein entsprechendes Ereignis ausgelöst. Auf manche Ereignisse wie beispielsweise das Ereignis Kurz-/Erdschluss haben Sie als Anwender keinerlei Einflussmöglichkeit. Bei anderen können Sie Einfluss auf die Auswirkungen und Reaktionen nehmen.

Mögliche Auswirkungen sind:

- Meldung: Information, die von der Steuerung ausgewertet werden kann
- Warnung: Information, die von der Steuerung ausgewertet werden kann und nach Ablauf einer definierten Zeitspanne zu einer Störung wird, sofern die Ursache nicht behoben wurde
- Störung: Sofortige Reaktion des Antriebsreglers; das Leistungsteil wird gesperrt und die Achsbewegung nicht mehr durch den Antriebsregler gesteuert oder die Achse wird durch einen Schnellhalt oder eine Notbremsung zum Stillstand gebracht

ACHTUNG!

Sachschaden durch Unterbrechung von Schnellhalt oder Notbremsung

Tritt während der Ausführung eines Schnellhalts oder einer Notbremsung eine andere Störung auf oder wird eine Sicherheitsfunktion aktiviert, wird der Schnellhalt oder die Notbremsung unterbrochen. In diesem Fall kann die Maschine durch die unkontrollierte Achsbewegung beschädigt werden.

Ereignisse, deren Ursachen sowie geeignete Maßnahmen sind nachfolgend gelistet. Ist die Fehlerursache behoben, können Sie den Fehler in der Regel direkt quittieren. Ist stattdessen ein Neustart des Antriebsreglers erforderlich, finden Sie einen entsprechenden Hinweis in den Maßnahmen.

10.2.1 Ereignis 50: Sicherheitsmodul

Der Antriebsregler geht in Störung:

- Das Leistungsteil wird gesperrt und die Achsbewegung nicht mehr durch den Antriebsregler gesteuert
- Die Bremsen werden nicht mehr durch den Antriebsregler gesteuert und fallen bei inaktivem Lüft-Override ein (F06)

Ursache		Prüfung und Maßnahme
1: Einkanalige Anforderung	Anschlussfehler	Anschluss prüfen und gegebenenfalls korrigieren; Störung ist nur quittierbar, wenn STO zuvor für mindestens 100 ms zweikanalig angefordert wurde
2: Falsches Modul	Projektiertes Sicherheitsmodul E53 stimmt nicht mit dem systemseitig erkannten E54[0] überein	Projektierung und Antriebsregler prüfen und gegebenenfalls Projektierung korrigieren oder Antriebsregler tauschen; Störung ist nicht quittierbar
16: Freigabe aktiv	STO-Anforderung bei aktivem Leistungsteil	STO nur bei inaktivem Leistungsteil anfordern
		Zeitgleich mit STO-Anforderung auch Freigabe-Aus ohne Schnellhalt anfordern (Drive Based A44)

Ereignis 50 – Ursachen und Maßnahmen

11 Mehr zur Sicherheitstechnik und PMC SR6?

Nachfolgende Kapitel fassen die wesentlichen Begriffe, Beziehungen und Maßnahmen rund um das Sicherheitsmodul PMC SR6 und die Sicherheitstechnik zusammen.

11.1 SRP/CS: Die Verarbeitung einer typischen Sicherheitsfunktion

Gehen von einer Maschine oder Anlage Gefahren aus, die durch konstruktive Maßnahmen nicht beseitigt werden können, müssen geeignete Schutzeinrichtungen und Sicherheitsfunktionen definiert und umgesetzt werden, um das Gefährdungspotenzial zu verringern.

Welche Sicherheitsfunktionen und damit verbunden Anforderungen an die Sicherheitsintegritäts- und Performance Level (SIL, PL) notwendig sind, hängt von der jeweiligen Anwendung und der möglichen Gefährdung ab. Für elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl sind Sicherheitsfunktionen in DIN EN 61800-5-2 definiert.

Die Ausführung der Sicherheitsfunktionen übernehmen in der Regel sogenannte sicherheitsbezogene Teile von Steuerungen (Safety Related Parts of Control Systems, SRP/CS).

Eine typische Sicherheitsfunktion ist eine Kombination aus sicherheitsbezogenen Teilen einer Steuerung (SRP/CS) mit folgenden Komponenten:

- Eingang (SRP/CS_a)
- Logik (SRP/CS_b)
- Ausgang (SRP/CS_c)
- Verbindungen, z. B. elektrisch oder optisch

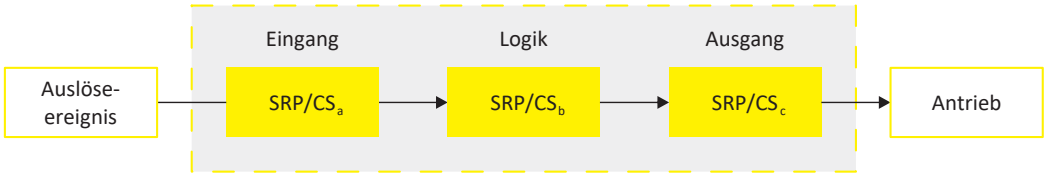


Abb. 6: SRP/CS-Komponenten zur Verarbeitung einer typischen Sicherheitsfunktion

Eingang	Sensor, z. B. Endschalter
Logik	Sicherheitssteuerung oder Sicherheitsschaltgerät
Ausgang	Aktor, z. B. Antriebsregler inkl. Sicherheitsmodul
Auslöseereignis	Öffnung einer trennenden Schutzeinrichtung oder manuelle Betätigung eines Tasters
Antrieb	Motor oder Zylinder

Erläuterung

Ein Sensor erkennt als Eingangskomponente eine die Sicherheitsfunktion auslösende Situation. Die Logikkomponente verarbeitet die erfassten Signale, der Aktor steuert schließlich als Ausgangskomponente die gefahrbringende Bewegung sicher an.
Der Antriebsregler in Kombination mit dem integrierten Sicherheitsmodul PMC SR6 ist Teil des SRP/CS-Aktors.

Ob eine Sicherheitssteuerung oder ein Sicherheitsschaltgerät als logische Komponente eines SRP/CS eingesetzt wird, hängt sowohl von deren Komplexität als auch von den benötigten SIL und PL ab.

11.2 Überwachung der Anschlussverdrahtung

Das Sicherheitsmodul PMC SR6 ist wartungsfrei, kann jedoch keine externen Verdrahtungsfehler erkennen.

WARNUNG!

Verlust der Sicherheitsfunktion und unerwartete Antriebsbewegungen durch Verdrahtungsfehler!

Das Sicherheitsmodul PMC SR6 erkennt keine Fehler in der Anschlussverdrahtung von X12!
Um diese zu identifizieren oder auszuschließen und um zu vermeiden, dass ein möglicher Fehler in der Verdrahtung oder Ansteuerung der Sicherheitsfunktion nicht zum Verlust der Sicherheit führt, ergreifen Sie eine der folgenden Maßnahmen.

- Permanente Überwachung der Anschlussverdrahtung durch ein Sicherheitsschaltgerät oder
- Fehlerausschluss für Leitungen und Verbindungen nach DIN EN 13849 oder
- Überwachung der Anschlussverdrahtung durch Plausibilisierung der Ansteuersignale von STO_a und STO_b gegen die STO-Statussignale (mittels STO-Funktionstest).

11.2.1 Überwachung durch ein Sicherheitsschaltgerät

Werden die Eingänge STO_a und STO_b durch überwachte Ausgänge angesteuert, kontrolliert das zugehörige Sicherheitsschaltgerät die Verdrahtung und die Schaltfähigkeit der Ausgänge mittels Testimpulsen.

Schalten Sie im Fehlerfall immer über den jeweils anderen STO-Eingang ab und beheben Sie den Fehler im Anschluss.

11.2.2 Fehlerausschluss für Leitungen und Verbindungen nach DIN EN 13849

Fehler in der Anschlussverdrahtung von Baugruppen und Komponenten können zum Verlust der Sicherheitsfunktionen führen. Mögliche Fehlerausschlüsse und Hinweise zu Fehlerausschlüssen liefert Tabelle D.4 der Norm DIN EN ISO 13849-2.

Betrachteter Fehler	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei beliebigen Leitern	Kurzausschlüsse zwischen Leitern, ▸ die dauerhaft fest verlegt und gegen äußere Beschädigungen geschützt sind, z. B. durch Kabelkanal, Panzerrohr, oder ▸ in unterschiedlichen Mantelleitungen, oder ▸ innerhalb eines elektrischen Einbauraums (siehe Bemerkung), oder ▸ die einzeln durch eine Erdverbindung geschützt sind	Voraussetzung ist, dass sowohl die Leitungen als auch der Einbauraum den jeweiligen Anforderungen entsprechen (siehe IEC 60204-1)
Kurzschluss zwischen einem beliebigen Leiter und einem ungeschützten leitenden Teil oder der Erde oder einer Schutzleiterverbindung	Kurzschlüsse zwischen Leiter und jedem ungeschützten leitenden Teil innerhalb eines Einbauraums (siehe Bemerkung)	
Unterbrechung eines Leiters	Nein	–

DIN EN 13849, Tabelle D.4 – Fehler und Fehlerausschlüsse – Leitungen/Kabel

11.2.3 Überwachung durch Plausibilisierung der Signale (STO-Funktionstest)

Der Zustand der Anschlussverdrahtung sowie die Funktionalität der Sicherheitskanäle kann mittels Plausibilisierung überprüft werden.

Um die Ansteuersignale der beiden Eingänge STO_a und STO_b gegen die STO-Statussignale zu plausibilisieren, führen Sie nach jedem Deaktivieren der STO-Funktion oder vor dem Aktivieren einen STO-Funktionstest durch.

In Abhängigkeit von dem jeweiligen Anwendungsgebiet, der bestimmungsgemäßen Verwendung des Sicherheitsschaltgeräts oder Maschinen- und Anlagen-spezifischen Anforderungen können kürzere Prüfzyklen notwendig sein.

Schalten Sie im Fehlerfall immer über den jeweils anderen STO-Eingang ab und beheben Sie den Fehler im Anschluss.

11.2.3.1 STO-Funktionstest

Ein STO-Funktionstest setzt voraus, dass die beiden Signale STO_a und STO_b wechselweise geschaltet und mit den daraus resultierenden STO-Statussignalen plausibilisiert werden. Im Fehlerfall muss die Sicherheitsfunktion an beiden STO-Eingängen aktiviert werden. Der Antriebsregler darf nicht mehr freigegeben werden.

STO_{status} wird direkt an Klemme X12 des Antriebsreglers zu Monitoringzwecken zur Verfügung gestellt. Wenn Sie mit einem Feldbussystem arbeiten, erhalten Sie detaillierte Statusinformationen durch die Übertragung der Parameter E67 Zustand STO, Array E67[0] – E67[2]. Diese können alternativ zu STO_{status} für die Plausibilisierung verwendet werden.

Bei Anwendungsfällen mit erhöhten Sicherheitsanforderungen wie SIL 3, PL e, muss eine Sicherheitssteuerung die Anschlussverdrahtung überprüfen. Bei Anwendungsfällen mit reduzierten Sicherheitsanforderungen, d. h. bis SIL 2, PL d, kann eine Standardsteuerung den STO-Funktionstest durchführen. Nähere Informationen zum Einsatz einer Standardsteuerung entnehmen Sie dem IFA Report 2/2016 *Sicherheitsbezogene Anwendungssoftware von Maschinen – die Matrixmethode des IFA*, siehe Kapitel 9.5 *Einsatz von Standardkomponenten für fehlerbeherrschende Maßnahmen*.

Information

Während des STO-Funktionstests wechselt der Antriebsregler in den Betriebszustand **Einschaltsperre**.

Schaltfolgen und Testergebnisse

Nachfolgende Grafik zeigt die Schaltfolgen von STO_a und STO_b sowie die erwarteten Ergebnisse. Alle hiervon abweichenden Testresultate müssen als Fehler gewertet werden. Ist dies der Fall, prüfen Sie die Verdrahtung, beheben Sie eventuelle Fehler und wiederholen Sie den STO-Funktionstest. Treten die Fehler erneut auf, nutzen Sie unsere Service-Leistungen und kontaktieren Sie unseren Support.

Information

Beachten Sie, dass die Testimpulse maximal 500 ms lang sein dürfen. Ab 500 ms wertet der Antriebsregler die Impulse als inkonsistente Anforderung und wechselt in den Betriebszustand **Störung**.

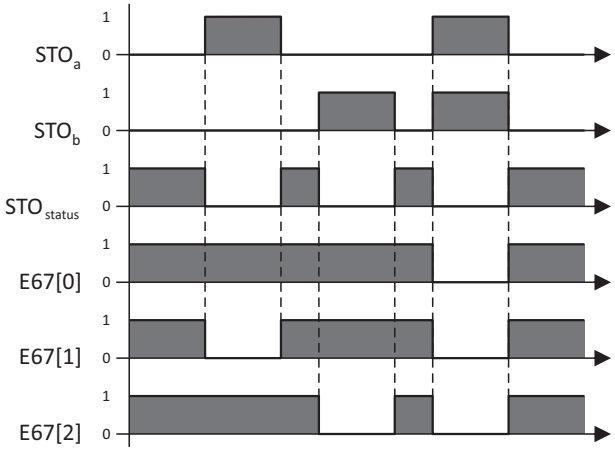


Abb. 7: Funktionstest – Schaltfolgen

STO_a, STO_b	Eingänge der beiden PMC SR6-Sicherheitskanäle
STO_{status}	STO-Statussignal an Klemme X12
E67[0]	Mindestens ein PMC SR6-Sicherheitskanal fordert eine STO-Aktivierung (STO_a = 0 V oder STO_b = 0 V)
E67[1]	STO_a fordert eine STO-Aktivierung (STO_a= 0 V)
E67[2]	STO_b fordert eine STO-Aktivierung (STO_b= 0 V)

STO-Funktionsprüfung bei parallelgeschalteten Antriebsreglern

Beachten Sie, dass STO_{status}-Ausgänge nicht zur Diagnose in Reihe geschaltet werden können.

Information

Um eine korrekte Verdrahtung von parallelgeschalteten Antriebsregler sicherzustellen, müssen Sie das STO_{status}-Signal jedes Antriebsreglers separat überprüfen.

11.3 Berechnung geeigneter Schutzmaßnahmen – Beispiele

Um die für ein System notwendigen geeigneten Schutzmaßnahmen bewerten und berechnen zu können, müssen die zugehörigen sicherheitsbezogenen Teile von Maschinensteuerungen bestimmten Anforderungen entsprechen.

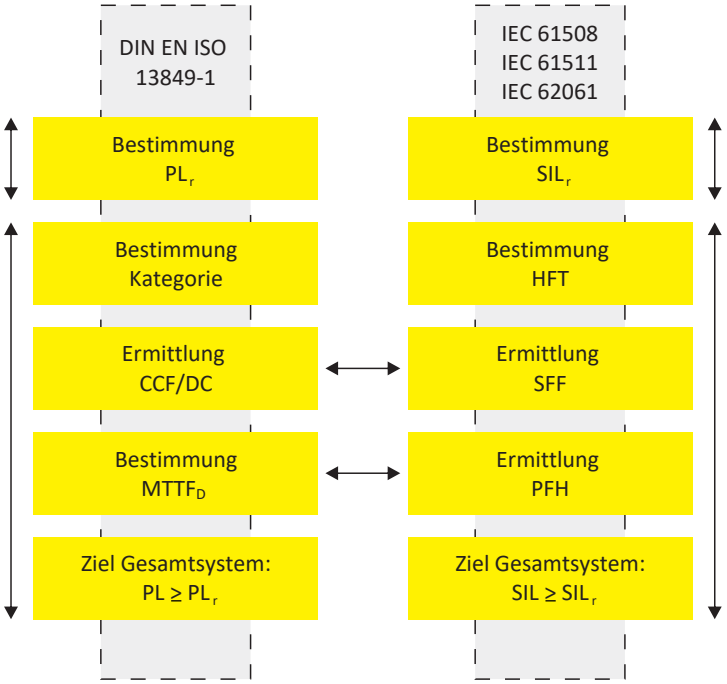


Abb. 8: Schutzmaßnahmen ermitteln und bewerten

Um den erforderlichen PL für ein System zu ermitteln, empfehlen wir, einen festen Workflow einzuhalten.
Vor den eigentlichen Berechnungen sollten alle sicherheitstechnisch relevanten Bauteile, deren Ausfall die Aktivierung der Sicherheitsfunktion beeinträchtigen könnte, in einem Prinzipschaltbild erfasst werden.

Aus dem Prinzipschaltbild lässt sich anschließend ein Blockschaltbild ableiten, das das Gesamtsystem in einzelne Subsysteme unterteilt. Für jedes Subsystem werden die sicherheitstechnisch relevanten Kennzahlen entweder den zugehörigen Herstellerangaben oder definierten Quellen entnommen. Besteht die Notwendigkeit, die Kennzahlen selbst zu berechnen, bietet beispielsweise die frei verfügbare Software SISTEMA[3] zuverlässige Hilfe.

Nachfolgende Kapitel zeigen die Realisierung der Sicherheitsfunktionen STO und SS1-t anhand exemplarischer Prinzip- und Blockschaltbilder sowie die zugehörige Berechnung der erforderlichen Sicherheitskennwerte für die Einzelsysteme und letztendlich für das Gesamtsystem.

[3] Von der DGUV kostenlos zur Verfügung gestellte Software zur Bewertung von sicherheitsbezogenen Maschinensteuerungen und zur normkonformen Berechnung von Sicherheitskennzahlen.

11.3.1 STO – Prinzip- und Blockschaltbilder erzeugen

Um die für ein System geeigneten Schutzmaßnahmen zuverlässig berechnen zu können, erzeugen Sie im ersten Schritt ein Prinzipschaltbild Ihres Systems mit sämtlichen relevanten Bauteilen. Aus diesem Prinzipschaltbild lassen sich im Anschluss sicherheitsbezogene Blockschaltbilder ableiten.

11.3.1.1 Prinzipschaltbild erzeugen

Die anschließende Grafik zeigt beispielhaft die Realisierung der Sicherheitsfunktion STO in Verbindung mit einer beweglichen, trennenden Schutzeinrichtung mit Positionsschaltern. Die Sicherheitsfunktion wird durch das Öffnen der Schutztür ausgelöst.

Das Prinzipschaltbild enthält unter anderem die Verschaltung der Positionsschalter, die Anbindung der STO-Eingänge STO_a und STO_b, ein Sicherheitsschaltgerät sowie eine Steuerung. Es verdeutlicht darüber hinaus das Zusammenspiel von Sensorik und Logik.[4]

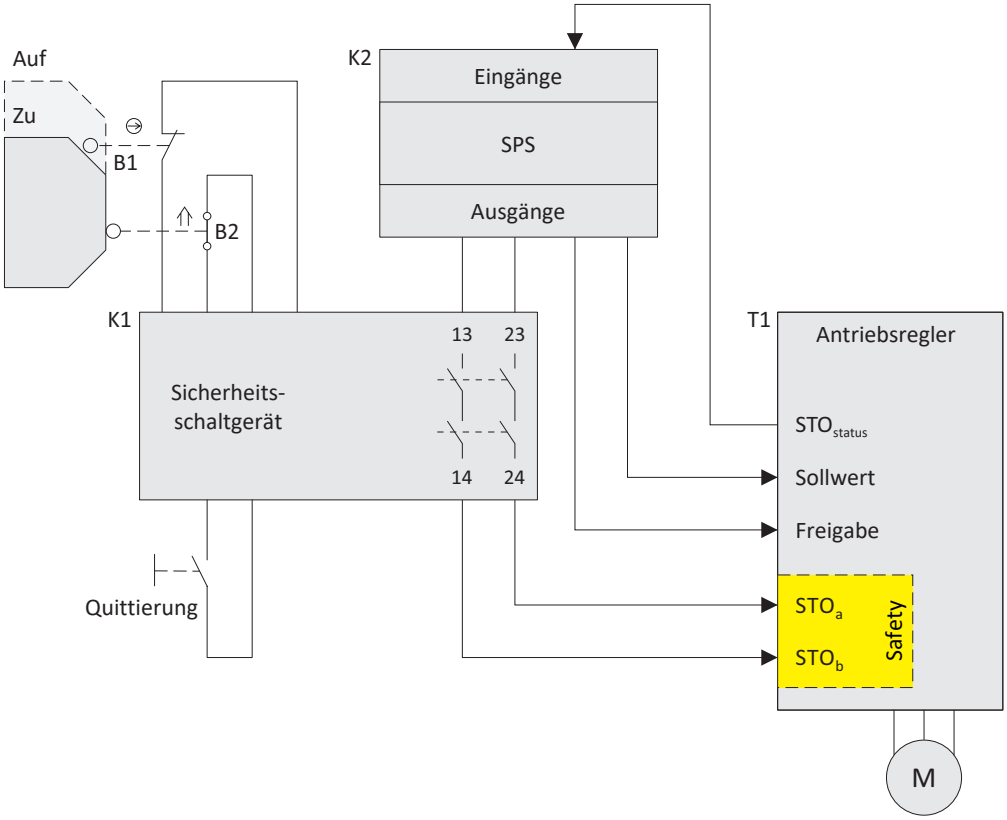


Abb. 9: STO – Prinzipschaltbild

B1, B2	Positionsschalter
K1	Sicherheitsschaltgerät
K2	Steuerung
T1	Antriebsregler mit integriertem Sicherheitsmodul PMC SR6

[4] Prinzipschaltbild und zugehörige Erläuterung sind angelehnt an IFA Report, 07 / 2013, S. 64ff.

Erläuterung

Der Antrieb wird funktional durch die SPS K2 gesteuert. Sie übermittelt dem Antriebsregler T1 Sollwerte, schaltet die beiden STO-Eingänge STO_a und STO_b und kann den Antrieb über die Freigabe starten und stoppen. Die SPS ist nicht an der Sicherheitsfunktion beteiligt.

Die Gefahrenstelle ist durch eine bewegliche trennende Schutztür abgesichert. Das Öffnen der Schutzeinrichtung wird durch die beiden Positionsschalter B1 und B2 erfasst und von dem Sicherheitsschaltgerät K1 ausgewertet. K1 schaltet die STO-Eingänge im Antriebsregler T1 – unabhängig von der SPS – ab. Im Antrieb wird dadurch die Generierung eines Drehfelds sicher verhindert.

Das Sicherheitsschaltgerät K1 deckt eventuelle Fehler in den Positionsschaltern durch einen Plausibilitätsvergleich auf. K1 selbst ist mit geeigneten Selbstüberwachungsfunktionen ausgestattet, die bei erkannten Fehlern die Freigabepfade öffnen.

Ein Fehlverhalten des Sicherheitsmoduls PMC SR6 löst die Sicherheitsfunktion STO aus und verhindert im Fehlerfall einen erneuten Start des Antriebs.

Eine fehlerhafte STO-Anschlussverdrahtung von K1, K2 und T1 kann, sofern notwendig, durch einen Plausibilitätsvergleich durch die SPS K2 erkannt werden. In diesem Fall übergibt der Antriebsregler T1 eine entsprechende STO-Statusmeldung an die SPS K2. Diese wird Teil des Sicherheitskreises.

11.3.1.2 Blockschaltbilder erzeugen

Blockschaltbilder fokussieren die konstruktiven und logischen Zusammenhänge der Bauteile des zugehörigen Prinzipschaltbilds.

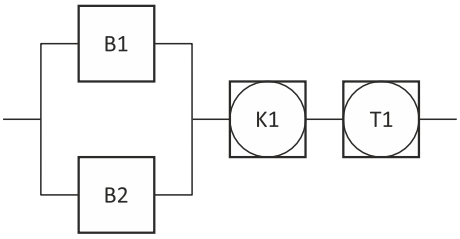


Abb. 10: Sicherheitsbezogenes Blockschaltbild

B1, B2	Positionsschalter
K1	Sicherheitsschaltgerät (gekapseltes Subsystem)
T1	Antriebsregler mit integriertem Sicherheitsmodul PMC SR6 (gekapseltes Subsystem)

Jedes Bauteil einer Sicherheitsfunktion ist Bestandteil einer bestimmten festen Struktur. Diese wird in EN ISO 13849-1 als Kategorie bezeichnet. Die Kategorien bilden die Basis für die Berechnung der resultierenden Sicherheitskennzahlen, z. B. in der Software SISTEMA. In dieser verkörpert ein Subsystem entweder eine Gruppe von Blöcken einer Kategorie oder ein Sicherheitsbauteil mit Herstellerangaben zu PL, Kategorie, PFH etc. (= gekapseltes Subsystem).

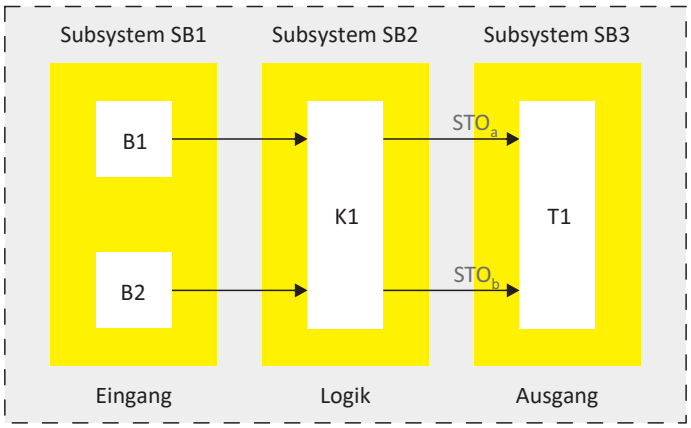


Abb. 11: Sicherheitsbezogenes Blockschaltbild mit Subsystemen

SB1 – SB3	(Gekapselte) Subsysteme 1 – 3
B1, B2	Positionsschalter
K1	Sicherheitsschaltgerät
T1	Antriebsregler mit integriertem Sicherheitsmodul PMC SR6

Die Schutzeinrichtung mit den Positionsschaltern bilden das Subsystem 1, das Sicherheitsschaltgerät Subsystem 2, der Antriebsregler samt integriertem Sicherheitsmodul PMC SR6 ist in Subsystem 3 dargestellt.

Konstruktive Merkmale

Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen an die Steuerungsstruktur der Kategorie B sind eingehalten; Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Steuerstromkreises) vorgesehen.

Quer- und Kurzschlüsse in elektrischen Anschlussleitungen sind bei der Planung entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler müssen erkannt und ein sicherer Zustand anschließend eingeleitet werden. Alternativ können die Leitungen derart verlegt werden, dass ein Fehlerausschluss für Quer- und Kurzschluss möglich ist.

Für die elektromechanischen Positionsschalter B1 und B2 muss die Anfahrmechanik bestimmungsgemäß konstruiert und angebracht sein. Betätigungselemente und Positionsschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden. Der Positionsschalter B1 ist ein bewährtes Bauteil nach DIN EN ISO 13849-2, Tabelle D.3 mit zwangsöffnendem Kontakt gemäß DIN EN 60947-5-1, Anhang K.

Das Sicherheitsschaltgerät erfüllt die Anforderungen der Kategorie 4 und PL e.

Bei T1 handelt es sich um einen Antriebsregler mit der integrierten Sicherheitsfunktion STO. Die Anforderungen der Kategorie 4 und PL e werden erfüllt.

11.3.2 SS1 – Prinzip- und Blockschaltbilder erzeugen

Um die für ein System geeigneten Schutzmaßnahmen zuverlässig berechnen zu können, erzeugen Sie im ersten Schritt ein Prinzipschaltbild Ihres Systems mit sämtlichen relevanten Bauteilen. Aus diesem Prinzipschaltbild lassen sich im Anschluss sicherheitsbezogene Blockschaltbilder ableiten.

11.3.2.1 Prinzipschaltbild erzeugen

Die anschließende Grafik zeigt beispielhaft die Umsetzung der Sicherheitsfunktion SS1-t in Verbindung mit einer beweglichen, trennenden Schutzeinrichtung mit Positionsschaltern. Die Sicherheitsfunktion wird durch das Öffnen der Schutztür ausgelöst.

Das Prinzipschaltbild enthält unter anderem die Verschaltung der Positionsschalter, die Anbindung der STO-Eingänge STO_a und STO_b, ein Sicherheitsschaltgerät mit abschaltverzögerten Kontakten sowie eine Steuerung. Es verdeutlicht darüber hinaus das Zusammenspiel von Sensorik und Logik.

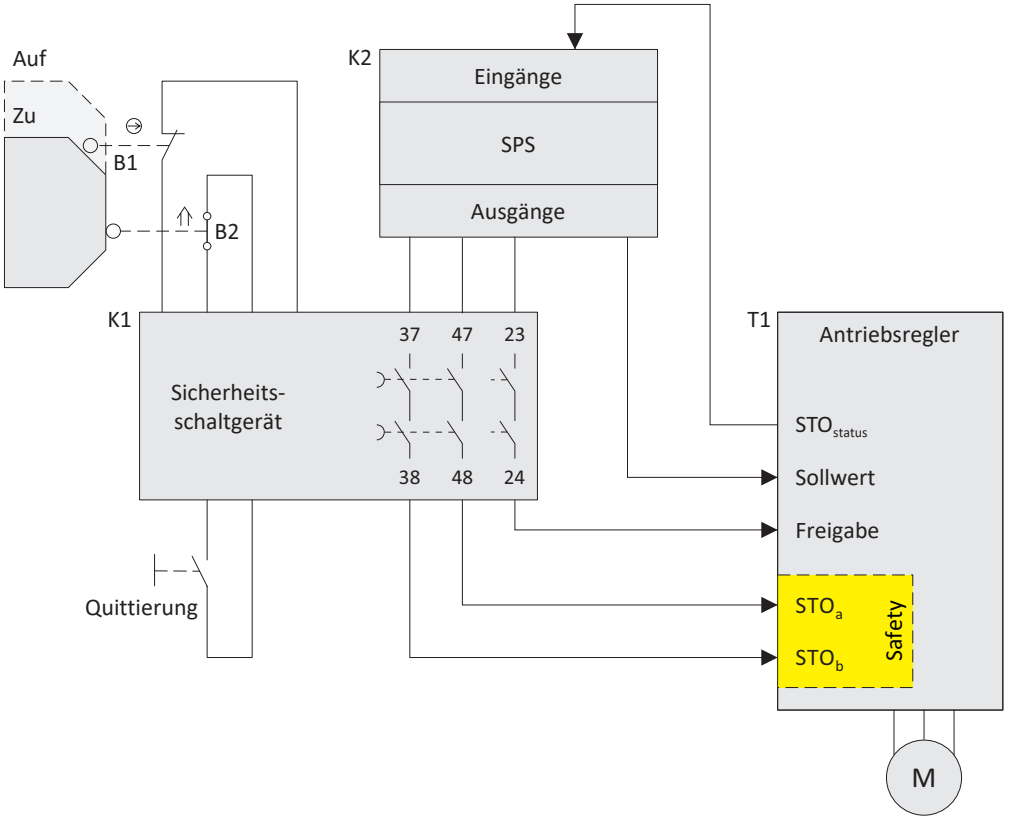


Abb. 12: SS1 – Prinzipschaltbild

B1, B2	Positionsschalter
K1	Sicherheitsschaltgerät
K2	Steuerung
T1	Antriebsregler mit integriertem Sicherheitsmodul PMC SR6

Erläuterung

Der Antrieb wird funktional durch die SPS K2 gesteuert. Sie übermittelt dem Antriebsregler T1 Sollwerte, schaltet die beiden STO-Eingänge STO_a und STO_b und kann den Antrieb über die Freigabe starten und stoppen. Die SPS ist nicht an der Sicherheitsfunktion beteiligt.

Die Gefahrenstelle ist durch eine bewegliche trennende Schutztür abgesichert. Das Öffnen der Schutzeinrichtung wird durch die beiden Positionsschalter B1 und B2 erfasst und von dem Sicherheitsschaltgerät K1 ausgewertet.

Über die abschaltverzögerten Freigabepfade des Sicherheitsschaltgeräts K1 werden die STO-Eingänge, nach Ablauf einer definierten Verzögerungszeit und unabhängig von der SPS abgeschaltet. Entweder Antriebsregler oder SPS können während dieser verzögerten STO-Abschaltung den Antrieb gesteuert stillsetzen. Löst, wie in diesem Beispiel, der Antriebsregler das gesteuerte Stillsetzen aus, besteht die Möglichkeit, die Funktion **Schnellhalt bei Freigabe-Aus** zu aktivieren und zu parametrieren.

Das Sicherheitsschaltgerät K1 deckt eventuelle Fehler in den Positionsschaltern durch einen Plausibilitätsvergleich auf. K1 ist mit geeigneten Selbstberwachungsfunktionen ausgestattet, die bei erkannten Fehlern die Freigabepfade öffnen.

Ein Fehlverhalten des Sicherheitsmoduls PMC SR6 löst die Sicherheitsfunktion STO aus und verhindert im Fehlerfall einen erneuten Start des Antriebs.

Eine fehlerhafte STO-Anschlussverdrahtung von K1, K2 und T1 kann, sofern notwendig, durch einen Plausibilitätsvergleich durch die SPS K2 erkannt werden. In diesem Fall übergibt der Antriebsregler T1 eine entsprechende STO-Statusmeldung an die SPS K2. Diese wird Teil des Sicherheitskreises.

11.3.2.2 Blockschaltbilder erzeugen

Blockschaltbilder fokussieren die konstruktiven und logischen Zusammenhänge der Bauteile des zugehörigen Prinzipschaltbilds.

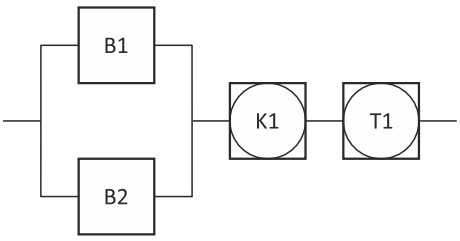


Abb. 13: Sicherheitsbezogenes Blockschaltbild

B1, B2	Positionsschalter
K1	Sicherheitsschaltgerät (gekapseltes Subsystem)
T1	Antriebsregler mit integriertem Sicherheitsmodul PMC SR6 (gekapseltes Subsystem)

Jedes Bauteil einer Sicherheitsfunktion ist Bestandteil einer bestimmten festen Struktur. Diese wird in EN ISO 13849-1 als Kategorie bezeichnet. Die Kategorien bilden die Basis für die Berechnung der resultierenden Sicherheitskennzahlen, z. B. in der Software SISTEMA. In dieser verkörpert ein Subsystem entweder eine Gruppe von Blöcken einer Kategorie oder ein Sicherheitsbauteil mit Herstellerangaben zu PL, Kategorie, PFH etc. (= gekapseltes Subsystem).

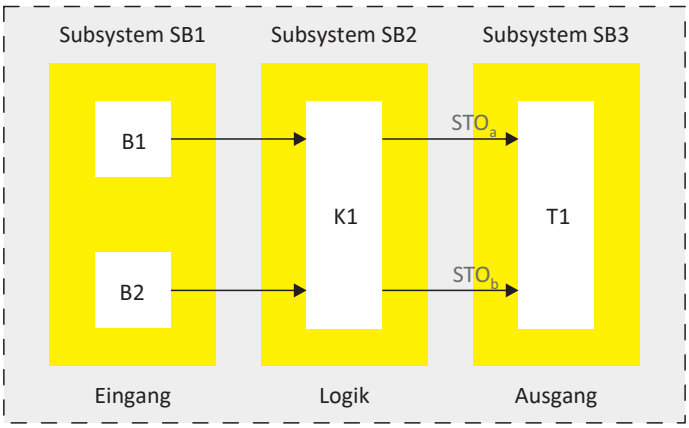


Abb. 14: Sicherheitsbezogenes Blockschaltbild mit Subsystemen

SB1 – SB3	(Gekapselte) Subsysteme 1 – 3
B1, B2	Positionsschalter
K1	Sicherheitsschaltgerät
T1	Antriebsregler mit integriertem Sicherheitsmodul PMC SR6

Die Schutzeinrichtung mit den Positionsschaltern bilden das Subsystem 1, das Sicherheitsschaltgerät Subsystem 2, der Antriebsregler samt integriertem Sicherheitsmodul PMC SR6 ist in Subsystem 3 dargestellt.

Konstruktive Merkmale

Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen an die Steuerungsstruktur der Kategorie B sind eingehalten; Schutzbeschaltungen (z. B. Kontaktabsicherung, Erdung des Steuerstromkreises) vorgesehen.

Quer- und Kurzschlüsse in elektrischen Anschlussleitungen sind bei der Planung entsprechend DIN EN ISO 13849-2, Tabelle D.4 zu berücksichtigen. Auftretende Fehler müssen erkannt und ein sicherer Zustand anschließend eingeleitet werden. Alternativ können die Leitungen derart verlegt werden, dass ein Fehlerausschluss für Quer- und Kurzschluss möglich ist.

Für die elektromechanischen Positionsschalter B1 und B2 muss die Anfahrmechanik bestimmungsgemäß konstruiert und angebracht sein. Betätigungselemente und Positionsschalter sind gegen Lageveränderung zu sichern. Es dürfen nur starre mechanische Teile (keine Federelemente) verwendet werden. Der Positionsschalter B1 ist ein bewährtes Bauteil nach DIN EN ISO 13849-2, Tabelle D.3 mit zwangsöffnendem Kontakt gemäß DIN EN 60947-5-1, Anhang K.

Das Sicherheitsschaltgerät erfüllt die Anforderungen der Kategorie 4 und PL e.

Bei T1 handelt es sich um einen Antriebsregler mit der integrierten Sicherheitsfunktion STO. Die Anforderungen der Kategorie 4 und PL e werden erfüllt.

11.3.3 Sicherheitskennwerte ermitteln

Um die Sicherheitskennwerte des Gesamtsystems zu ermitteln, müssen die Kennwerte der einzelnen Subsysteme recherchiert, berechnet und bewertet werden. Da die Subsysteme in beiden Beispielen (STO und SS1) nahezu identisch sind, gelten die nachfolgenden Kapitel sowohl für STO als auch für SS1.

11.3.3.1 Subsystem SB1

In Subsystem SB1 sind die beiden Positionsschalter B1 und B2 enthalten. Die mechanischen Schalter des Typs PSEN me4 der Pilz GmbH und Co. KG dienen in diesem Fall als konkretes Beispiel.

Durchschnittlicher Diagnosedeckungsgrad – DC_{avg}

- DC_{avg} Subsystem SB1: 99 %
- B1 und B2 werden hinsichtlich Plausibilität, Quer- und Kurzschlüsse über das Sicherheitsschaltgerät K1 überwacht.

Quelle: DIN EN ISO 13849-1, Anhang E, Tabelle E.1

Ausfall infolge gemeinsamer Ursache – CCF

Folgende Maßnahmen werden getroffen, um die Anforderungen zur Vermeidung von Fehlern gemeinsamer Ursache zu erfüllen. Für jede Maßnahmenkategorie wird eine bestimmte Anzahl von Punkten vergeben. Der maximale Wert für CCF liegt bei 100 Punkten. Ab 65 Punkten gelten sämtliche CCF-Anforderungen als erfüllt.

- Trennung der Verdrahtung: 15 Punkte in Kategorie "Trennung/Abtrennung"
- Verwendung von NC- und NO-Kontakten: 20 Punkte in Kategorie "Diversität"
- Schutz gegen Überspannung und Verwendung bewährter Bauteile: 20 Punkte in Kategorie "Entwurf/Anwendung/Erfahrung"
- FMEA des Beschaltungsbeispiels: 5 Punkte in Kategorie "Beurteilung/Analyse"
- Positionsschalter werden gemäß der Herstellerspezifikation gesetzt: 10 Punkte in Kategorie "Umgebung"
- -> CCF Subsystem SB1: 70 Gesamtpunkte

Quelle: DIN EN ISO 13849-1, Anhang F, Tabelle F.1

Nominelle Lebensdauer – B_{10D}

Für den Positionsschalter mit Zwangsöffnung B1 ist ein Fehlerausschluss für den elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt von B2 wird der B_{10D}-Wert von 2.000.000 Zyklen angenommen. Das gilt auch für den mechanischen Teil von B1 und B2.

- $B1_{(NC)}$
  Ausschluss gefährlicher Bauteilfehler für den elektrischen Kontakt möglich
  B_{10D} (mechanisch): 2.000.000 Zyklen
- $B2_{(NO)}$
  B_{10D} (mechanisch): 2.000.000 Zyklen
- $B2_{(NO)}$
  B_{10D} (elektrisch): 2.000.000 Zyklen

Quelle: Pilz GmbH und Co. KG

Information

Sind vom Hersteller keine Kennzahlen verfügbar, können Sie die Kennzahlen der Tabelle C.1 im Anhang C der DIN EN ISO 13849-1 entnehmen.

Schalthäufigkeit – n_{op}

Bei 365 Arbeitstagen pro Jahr, 16 Arbeitsstunden pro Tag und einer Zykluszeit von 5 Minuten bedeutet dies für B1 und B2 ein jeweiliger Schaltzyklus von n_{op} = 70.080 Zyklen/Jahr.

Quelle: DIN EN ISO 13849-1, Anhang C, Tabelle C.1, Berechnung: SISTEMA

Mittlere Betriebsdauer bis zum gefährlichen Ausfall – $MTTF_D$

- B1
  $MTTF_D$: 285 Jahre
- B2
  $MTTF_D$: 143 Jahre

Berechnung: SISTEMA

Wahrscheinlichkeit eines gefährlichen Ausfalls – PFH_D

B1 und B2
PFH_D: 2,47 × 10^{-8}

Berechnung: SISTEMA

11.3.3.2 Subsystem SB2

Bei Subsystem SB2 handelt es sich um ein gekapseltes Subsystem, d. h. um ein Sicherheitsbauteil, bei dem PL, PFH und Kategorie bereits durch den Hersteller vorgegeben sind.

Subsystem SB2 beinhaltet das Sicherheitsschaltgerät K1. Das Gerät des Typs PNOZ S5 der Pilz GmbH und Co. KG dient hier als konkretes Beispiel.

Performance Level – PL, Kategorie

- PL = e
- Kategorie = 4

Quelle: Pilz GmbH und Co. KG

Wahrscheinlichkeit eines gefährlichen Ausfalls – PFH_D

- Unverzögerte Kontakte (STO)
  PFH_D = 2,31 × 10^{-9} [1/h]
- Abschaltverzögernde Kontakte (SS1)
  PFH_D = 2,34 × 10^{-9} [1/h]

Quelle: Pilz GmbH und Co. KG

11.3.3.3 Subsystem SB3

Bei Subsystem SB3 handelt es sich ebenfalls um ein gekapseltes Subsystem, bei dem die sicherheitsrelevanten Daten durch den Hersteller benannt werden.

Subsystem SB3 beinhaltet den Antriebsregler T1 der Baureihe PMC SC6 oder PMC SI6 inklusive Sicherheitsmodul PMC SR6.

Performance Level – PL und Kategorie

- PL = e
- Kategorie = 4

Quelle: Pilz GmbH & Co. KG

Wahrscheinlichkeit eines gefährlichen Ausfalls – PFH_D

$PFH_D = 5 \times 10^{-9}$ [1/h]

Quelle: Pilz GmbH & Co. KG

11.3.3.4 Verdrahtung der Subsysteme

Das Sicherheitsschaltgerät K1 ist derart konfiguriert und beschaltet, dass dieses die beiden Positionsschalter B1 und B2 und deren Verdrahtung auf Plausibilität, Quer- und Kurzschlüsse überwacht. Für die Verdrahtung zwischen Sicherheitsschaltgerät K1 und Antriebsregler T1 wird aufgrund der Montage dieser Bauteile innerhalb eines elektrischen Einbauraums ein Fehlerausschluss gemäß DIN EN ISO 13849-2, Anhang D, Tabelle D 5.2 angenommen.

11.3.3.5 Sicherheitskennwerte des Gesamtsystems

Nachfolgende Tabelle beinhaltet die ermittelten Sicherheitskennwerte der einzelnen Subsysteme sowie die daraus resultierende Wahrscheinlichkeit eines Gesamtausfalls.

Subsystem	Wertequelle	Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]
SB1 – Eingang	Berechnung SISTEMA	$PFH_D = 2{,}47 \times 10^{-8}$
SB2 – Logik	Herstellerangaben	$PFH_D = 2{,}31 \times 10^{-9}$ (STO) $PFH_D = 2{,}34 \times 10^{-9}$ (SS1)
SB3 – Ausgang	Herstellerangaben	$PFH_D = 5{,}0 \times 10^{-9}$
Gesamtsystem	Berechnung SISTEMA	$PFH_D = 3{,}2 \times 10^{-8}$

PFH_D – Subsysteme und Gesamtsystem

Die Ermittlung und Berechnung der Wahrscheinlichkeit gefährlicher Ausfälle pro Stunde für die Beispielsysteme mit den Sicherheitsfunktionen STO und SS1 ergibt einen Wert von $3{,}2 \times 10^{-8}$ [1/h], was einem jeweiligen System-PL e und einem SIL 3 in hoher, kontinuierlicher Betriebsart entspricht (siehe nachfolgende Tabelle).

Performance Level	Wahrscheinlichkeit eines gefährlichen Ausfalls [1/h]	Safety Integrity Level
a	$\geq 10^{-5}$ bis $< 10^{-4}$	Keine Entsprechung
b	$\geq 3 \times 10^{-6}$ bis $< 10^{-5}$	1
c	$\geq 10^{-6}$ bis $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ bis $< 10^{-6}$	2
e	$\geq 10^{-8}$ bis $< 10^{-7}$	3

PL, PFH_D, SIL – Gesamtsystem

Bei der Ermittlung des Performance Levels müssen zusätzlich zu den Anforderungen an die Ausfallwahrscheinlichkeit strukturelle Anforderungen berücksichtigt werden.

Die Subsysteme SB1 – SB3 erfüllen hinsichtlich Steuerungsstrukturen die Mindestanforderungen der Kategorie 4-Systeme:

- DC_{avg}: Hoch
- CCF: Anforderung erfüllt
- $MTTF_D$: Hoch

11.4 PMC SR6 gemäß Schnittstellenklassifizierung (ZVEI)

Der Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) publizierte 2016 ein Positionspapier (siehe Kapitel Weiterführende Informationen), das die Klassifizierung binärer 24 V_{DC}-Schnittstellen im Bereich Funktionale Sicherheit thematisiert.

Das Positionspapier definiert fachspezifische Begriffe, arbeitet die kennzeichnenden Merkmale der einzelnen Schnittstellentypen (Interface-Typen) mit dynamischen Testimpulsen heraus und beschreibt herstellerspezifische Produktinformationen und technische Daten für die untersuchten Interface-Typen.

Aufgrund einer in diesem Positionspapier dargelegten Klassifizierung kann das Sicherheitsmodul PMC SR6 als Informationssenke (Senke) der Interface-Typen C und D genutzt und über die Informationsquellen (Quellen) derselben Interface-Typen angesteuert werden.
Senken und Quellen der Interface-Typen C und D werden dem Zeitverhalten der Testimpulse entsprechend in Klassen unterteilt, wobei eine höhere Klasse kürzere Testimpulse bedeutet. Bei der Kombination von Senke und Quelle ist zu beachten, dass eine gewählte Quelle mindestens der gleichen Klasse angehört wie die gewählte Senke.

Interface-Typ C

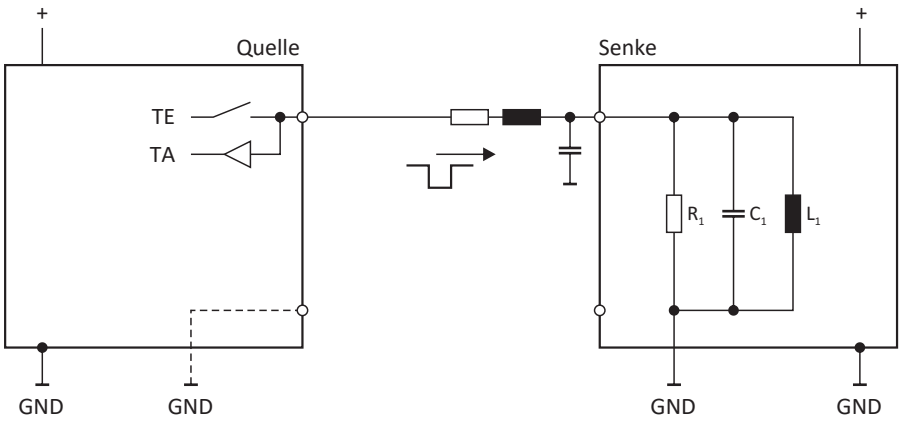


Abb. 15: Schnittstellenklassifizierung – Interface-Typ C

TE	Testimpulserzeugung
TA	Testimpulsauswertung
GND	Bezugspotenzial
R_1	Eingangswiderstand
C_1	Eingangskapazität
L_1	Eingangsinduktivität

Interface-Typ C[5] wird häufig als OSSD-Ausgang eingesetzt – beispielsweise für Sicherheitsausgänge bei Lichtgittern und Näherungsschaltern (mit definiertem Verhalten unter Fehlerbedingungen gemäß EN 60947-5-3). Die zugehörigen Geräte überprüfen als Quelle mit Testimpulsen die Funktion ihrer Ausgänge; die entsprechende Senke, z. B. Sicherheitsmodul PMC SR6, darf per Definition nicht auf diese Testimpulse reagieren.

[5] Siehe ZVEI, S. 13ff.

Interface-Typ D

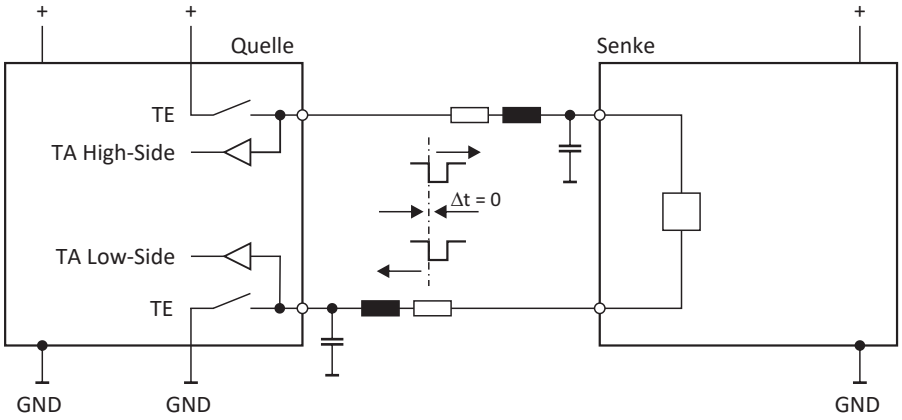


Abb. 16: Schnittstellenklassifizierung – Interface-Typ D

TE	Testimpulserzeugung
TA	Testimpulsauswertung
TA High-Side	Testimpulsauswertung High-Side-Schalter
TA Low-Side	Testimpulsauswertung Low-Side-Schalter
GND	Bezugspotenzial
Δt_i	Zeitspanne

Interface-Typ D[6] wird entweder zum sicheren Schalten von Aktoren (Schütze, Motoren, Ventile) oder zum vollständigen Freischalten der Betriebsspannung von elektrischen/elektronischen Baugruppen und Geräten verwendet. Der Unterschied zum reinen pulsschaltenden Ausgang des Interface-Typs C liegt vor allem in der Schaltung und dem Testen der Rückleitung.

Eventuelle Rückleitungsfehler wie Kurzschlüsse können gegen 0 V detektiert werden. Spannungsverschleppungen durch einen gemeinsamen, schwebenden 0 V-Anschlusspunkt werden durch diese Anschlussart vermieden.

Darüber hinaus besteht die Möglichkeit, über zwei Leitungen zweikanalig abzuschalten. Ein einzelner Kurzschluss auf einen der Leiter führt somit nicht zu einem unzulässigen Schalten des Aktors. Die Quelle gibt hierzu Testimpulse an die Senke aus, die wiederum von der Quelle ausgewertet werden. Die Testimpulse werden von der Senke weder verfälscht noch verzögert.

Die Senke, z. B. Sicherheitsmodul PMC SR6, kann induktive, kapazitive und ohmsche Anteile besitzen. Bei der Quelle handelt es sich typischerweise um eine Sicherheitssteuerung oder ein Sicherheitsschaltgerät mit bipolarem Ausgang.

[6] Siehe ZVEI, S. 17ff.

12 Anhang

12.1 Weiterführende Informationen

Die in nachfolgender Tabelle gelisteten Dokumentationen liefern weitere relevante Informationen zum Antriebsregler.

Aktuelle Dokumentversionen finden Sie unter https://www.pilz.com/de-INT.

Gerät/Software	Dokumentation	Inhalte	ID
Antriebsregler PMC SC6	Handbuch	Systemaufbau, technische Daten, Projektierung, Lagerung, Einbau, Anschluss, Inbetriebnahme, Betrieb, Service, Diagnose	1005343
Antriebsregler PMC SC6	Inbetriebnahmeanleitung	Systemaufbau, technische Daten, Lagerung, Einbau, Anschluss, Inbetriebnahme	1005357
Anreihtechnik mit PMC SI6 und PMC PS6	Handbuch	Systemaufbau, technische Daten, Projektierung, Lagerung, Einbau, Anschluss, Inbetriebnahme, Betrieb, Service, Diagnose	1005342
Anreihtechnik mit PMC SI6 und PMC PS6	Inbetriebnahmeanleitung	Systemaufbau, technische Daten, Lagerung, Einbau, Anschluss, Inbetriebnahme	1005356

Zusätzliche Informationen und Quellen, die als Grundlage für diese Dokumentation dienen oder aus denen zitiert wird:

Deutsche Gesetzliche Unfallversicherung, 2013. *Sichere Antriebssteuerungen mit Frequenzumrichtern* [online]. *IFA Report 7 / 2013*.
Sankt Augustin: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
[Zugriff am 01.08.2016]. Verfügbar unter
http://www.dguv.de/ifa/publikationen/reports-download/reports-2013/ifa-report-7-2013/index.jsp

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), 2010. *Das SISTEMA-Kochbuch 1. Vom Schaltbild zum Performance Level – Quantifizierung von Sicherheitsfunktionen mit SISTEMA* [online]. *Version 1.0 (DE) / 2010*.
Sankt Augustin: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
[Zugriff am 01.08.2016]. Verfügbar unter
http://www.dguv.de/medien/ifa/de/pra/softwa/sistema/kochbuch/sistema_kochbuch1_de.pdf

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA). *SISTEMA 1.1.9* [Software]. *Bewertung von sicherheitsbezogenen Maschinensteuerungen nach DIN EN ISO 13849.*
Sankt Augustin: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
[Zugriff am 01.08.2016]. Verfügbar unter
http://www.dguv.de/ifa/praxishilfen/praxishilfen-maschinenschutz/software-sistema/alle-sistema-versionen/index.jsp

Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI). *Klassifizierung binärer 24-V-Schnittstellen mit Testung im Bereich der Funktionalen Sicherheit* [online]. Edition 2.0, *November 2016*.
Frankfurt am Main: ZVEI – Zentralverband Elektrotechnik- und Elektroindustrie e. V. (Fachverband Automation)
[Zugriff am 17.11.2016]. Verfügbar unter
https://www.zvei.org/presse-medien/publikationen/zvei-positionspapier-klassifizierung-binaerer-24-v-schnittstellen-mit-testung-im-bereich-der-funktionalen-sicherheit/

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), 2016. *Sicherheitsbezogene Anwendungssoftware von Maschinen – die Matrixmethode des IFA* [online]. *IFA Reportt 2/ 2016*.
Sankt Augustin: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
[Zugriff am 14.02.2020]. Verfügbar unter
https://www.dguv.de/ifa/publikationen/reports-download/reports-2016/ifa-report-2-2016/index.jsp

12.2 Formelzeichen

Formel-zeichen	Einheit	Erklärung
B_{10D}	–	Anzahl der Zyklen, bis 10 % der Komponenten gefährlich ausgefallen sind
C_1	F	Eingangskapazität
C_{1max}	F	Maximale Eingangskapazität
DC	%	Diagnosedeckungsgrad
DC_{avg}	%	Durchschnittlicher Diagnosedeckungsgrad
Δt	s	Zeitspanne
I_{max}	A	Maximalstrom
I_{1max}	A	Maximaler Eingangsstrom
I_{1off}	A	Eingangsstrom im AUS-Zustand
I_{1on}	A	Eingangsstrom im EIN-Zustand
L_1	H	Eingangsinduktivität
MTTF	Jahr, a	Mittlere Zeit bis zum Ausfall
$MTTF_D$	Jahr, a	Mittlere Zeit bis zum gefahrbringenden Ausfall
n_{op}	1/a	Mittlere Anzahl jährlicher Betätigungen (Schalthäufigkeit)
p	–	Polpaarzahl
PFH_D	1/h	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde
R_1	Ω	Eingangswiderstand
T_i	ms	Testimpulsintervall
t_i	µs	Testimpulsdauer
T_M	Jahr, a	Gebrauchsdauer
U_1	V	Eingangsspannung
U_{1max}	V	Maximale Eingangsspannung
U_2	V	Ausgangsspannung

12.3 Abkürzungen

Abkürzung	Bedeutung
AWG	American Wire Gauge
CCF	Common Cause Failure (dt.: Ausfall aufgrund gemeinsamer Ursache)
EMV	Elektromagnetische Verträglichkeit
FMEA	Failure Modes and Effects Analysis (dt.: Ausfallarten und Effektanalyse)
HFT	Hardware Fault Tolerance (dt.: Hardware-Fehlertoleranz)
OSSD	Output Signal Switching Device (dt.: Ausgang mit überlagerten Testimpulsen)
PDS(SR)	Power Drive System(Safety Related) (dt.: Leistungsantriebssystem mit integrierter Sicherheitsfunktion)
PELV	Protective Extra Low Voltage (dt.: Schutzkleinspannung)
PFH, PFH_D	Probability of a (dangerous) Failure per Hour (dt.: Wahrscheinlichkeit eines (gefahrbringenden) Ausfalls pro Stunde)
PL	Performance Level (dt.: Leistungsgrad)
PWM	Pulsweitenmodulation
SFF	Safe Failure Fraction (dt.: Anteil sicherer Ausfälle)
SIL	Safety Integrity Level (dt.: Sicherheits-Integritätslevel)
SIL CL	Safety Inegrity Level Claim Limit (dt.: Anspruchsgrenze des Integritätslevels Sicherheit)
SRECS	Safety Related Electrical Control System (dt.: sicherheitsbezogenes elektr. Steuerungssystem einer Maschine)
SRP/CS	Safety Related Part of a Control System (dt.: sicherheitsbezogenes Teil einer Steuerung)
SS1	Safe Stop 1 (dt.: sicherer Stopp 1)
SS1-t	Save Stop 1-time (dt.: sicherer Stopp 1, zeitgesteuert)
STO	Safe Torque Off (dt.: sicher abgeschaltetes Moment)
TA	Testimpulsauswertung
TE	Testimpulserzeugung
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie

Average Diagnostic Coverage (DC_{avg})

Gemäß DIN EN ISO 13849-1: Durchschnittlicher Diagnosedeckungsgrad. Maß für die Wirksamkeit der Diagnose, die bestimmt werden kann als Verhältnis der Ausfallrate der bemerkten gefährlichen Ausfälle und Ausfallrate der gesamten gefährlichen Ausfälle. Es kann für das gesamte System oder Teile eines sicherheitsbezogenen Systems gelten.

B_{10D}-Wert

Gemäß DIN EN ISO 13849-1: Anzahl der Zyklen, bis 10 % der Komponenten gefährlich ausgefallen sind (für pneumatische und elektromechanische Komponenten).

Common Cause Failure (CCF)

Ausfall aufgrund gemeinsamer Ursache. Gemäß DIN EN 61800-5-2: Ausfall, der das Ergebnis eines oder mehrerer Ereignisse ist, die gleichzeitige Ausfälle von zwei oder mehreren getrennten Kanälen in einem mehrkanaligen System verursachen und zu einem Ausfall der Sicherheitsfunktion führen.

Gebrauchsdauer (T_M)

Gemäß DIN EN 61800-5-2: Festgelegte kumulierte Betriebsdauer des PDS(SR) während seiner Gesamtlebensdauer.

Informationsquelle (Quelle)

Gemäß Zentralverband Elektrotechnik- und Elektronikindustrie: Sender einer Information an die Informationssenke. Die Quelle verfügt über einen Ausgang, der mit dem Eingang der Senke verbunden wird. Eine Quelle kann gleichzeitig die Anforderungen unterschiedlicher Interface-Typen erfüllen. Der Begriff Informationsquelle bezieht sich auf die Erzeugung einer Information, nicht auf die Erzeugung zugehöriger Testimpulse.

Informationssenke (Senke)

Gemäß Zentralverband Elektrotechnik- und Elektronikindustrie: Empfänger einer Information von einer Informationsquelle. Die Informationssenke verfügt über einen Eingang, der mit dem Ausgang der Quelle verbunden wird. Eine Senke kann gleichzeitig die Anforderungen unterschiedlicher Interface-Typen erfüllen. Der Begriff Senke bezieht sich auf die Auswertung einer Information, nicht auf die Auswertung zugehöriger Testimpulse.

Insulated Gate Bipolar Transistor (IGBT)

Bipolartransistor mit isolierter Gate-Elektrode. Vierschicht-Habeiterbauelement, das über ein Gate gesteuert wird und die Vorteile von Bipolar- und Feldeffekttransistor vereinigt. Ein IGBT wird hauptsächlich in der Leistungselektronik eingesetzt.

Interface-Typ

Gemäß Zentralverband Elektrotechnik- und Elektronikindustrie: Standardisierte Schnittstelle zwischen Sendern ("Informationsquellen") und Empfängern ("Informationssenken") von Signalen mit Festlegungen über die Erzeugung aus Auswertung von zugehörigen Testimpulsen.

Kategorie

Gemäß DIN EN ISO 13849-1: Einstufung der sicherheitsbezogenen Teile einer Steuerung bezüglich ihres Widerstands gegen Fehler und ihres nachfolgenden Verhaltens bei einem Fehler. Eine Kategorie wird erreicht durch die Struktur und die Anordnung der Teile, deren Fehlererkennung und/oder ihre Zuverlässigkeit. Mögliche Kategoriebezeichnungen, d. h. Einstufungen sind B, 1, 2, 3, 4.

Klasse

Gemäß Zentralverband Elektrotechnik- und Elektronikindustrie: Menge von Informationsquellen und -senken mit kompatiblen technischen Daten bezüglich der Testimpulse innerhalb eines Interface-Typs.

Mean Time to dangerous Failure ($MTTF_D$)

Gemäß DIN EN ISO 13849-1: Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall von Systemen oder Baugruppen. Statistische Kenngröße, die durch Versuche und Erfahrungswerte ermittelt wird. Gibt keine garantierte Lebensdauer oder garantiert ausfallfreie Zeit an.

NOR-Verknüpfung

NICHT-ODER-Verknüpfung. Werden binäre Signalzustände (0 oder 1) von Variablen über eine Funktion miteinander verbunden, handelt es sich um Verknüpfungen. Mit der Negation NICHT sowie den Operatoren UND und ODER sind sämtliche Verknüpfungsvarianten realisierbar. Bei einer NOR-Verknüpfung wird das Ergebnis einer ODER-Verknüpfung umgedreht, d. h., die Ausgangsvariable hat nur dann das Signal 1, wenn alle Eingangsvariablen ein Signal 0 liefern.

OSSD-Ausgang

Ausgang mit integrierten Testimpulsen. Die zugehörigen Geräte überprüfen während des Betriebs mit kurzen Testimpulsen die Funktion dieses Ausgangstyps.

Performance Level (PL)

Gemäß DIN EN 13849-1: Maß für die Zuverlässigkeit einer Sicherheitsfunktion oder eines Bauteils. Der Performance Level wird auf einer Skala von a – e (geringster – höchster PL) bemessen. Je höher der PL, desto sicherer und zuverlässiger ist die betrachtete Funktion. Der PL kann einem bestimmten SIL zugeordnet werden. Ein umgekehrter Rückschluss von einem SIL zu einem PL ist nicht möglich.

Power Drive System(Safety Related) (PDS(SR))

Gemäß DIN EN 61800-5-2: Elektrisches Leistungsantriebssystem mit integrierter Sicherheitsfunktion und einstellbarer Drehzahl, das für den Einsatz in sicherheitsbezogenen Anwendungen geeignet ist.

Probabilitiy of a dangerous Failure per Hour (PFH_D)

Gemäß DIN EN 61508/DIN EN 62061: Durchschnittliche Wahrscheinlichkeit eines gefährlichen Geräteausfalls pro Stunde. Zusammen mit PFH eine der wesentlichen Berechnungsgrundlagen für die Zuverlässigkeit der Sicherheitsfunktion von Geräten, dem SIL.

Probabilitiy of a Failure per Hour (PFH)

Gemäß DIN EN 61508/DIN EN 62061: Durchschnittliche Wahrscheinlichkeit eines Geräteausfalls pro Stunde. PFH ist zusammen mit PFH_D eine der wesentlichen Berechnungsgrundlagen für die Zuverlässigkeit der Sicherheitsfunktion von Geräten, dem SIL.

Safe Stop 1 (SS1)

Gemäß DIN EN 61800-5-2: Verfahren zum Stillsetzen eines PDS(SR). Bei der Sicherheitsfunktion SS1 führt das PDS(SR) eine der folgenden Funktionen aus:
a) Auslösen und Steuern der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der STO-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt (SS1-d), oder
b) Auslösen und Überwachen der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der STO-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt (SS1-r), oder
c) Auslösen der Motorverzögerung und Auslösen der STO-Funktion nach einer anwendungsspezifischen Zeitverzögerung (SS1-t). SS1(-t) entspricht in diesem Fall dem zeitgesteuerten Stillsetzen nach IEC 60204-1, Stoppkategorie 1(-t).

Safe Torque Off (STO)

Gemäß DIN EN 61800-5-2: Verfahren zum Stillsetzen eines PDS(SR). Bei der Sicherheitsfunktion STO wird dem Motor keine Energie zugeführt, die eine Drehung (oder bei einem Linearmotor eine Bewegung) verursachen kann. Das PDS(SR) liefert keine Energie an den Motor, die eine Drehmoment (oder bei einem Linearmotor eine Kraft) erzeugen kann. STO ist die grundlegendste antriebsintegrierte Sicherheitsfunktion. Sie entspricht dem ungesteuerten Stillsetzen nach DIN EN 60204-1, Stoppkategorie 0.

Safety Integrity Level (SIL)

Gemäß DIN EN 61800-5-2: Ausfallwahrscheinlichkeit einer Sicherheitsfunktion. SIL ist in die Stufen 1 – 4 (geringster – höchster Level) eingeteilt. Durch SIL werden Systeme oder Teilsysteme auf ihre Zuverlässigkeit von Sicherheitsfunktionen exakt beurteilt. Je höher der SIL, desto sicherer und zuverlässiger ist die betrachtete Funktion.

Safety Integrity Level Claim Limit (SIL CL)

Maximaler SIL, der beansprucht werden kann – bezogen auf strukturelle Einschränkungen und systematische Sicherheitsintegrität eines SRECS-Teilsystems. Ein SIL CL wird durch die Hardware-Fehlertoleranz (HFT) und den Anteil sicherer Ausfälle der Teilsysteme (SFF) bestimmt.

Safety Related Part of a Control System (SRP/CS)

Gemäß DIN EN ISO 13849-1: Sicherheitsbezogenes Teil einer Steuerung, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt.

Schalthäufigkeit (n_{op})

Gemäß DIN EN 13849-1: Mittlere Anzahl jährlicher Betätigungen.

STO-Abschaltzeit

Zeitspanne ab dem Aktivieren der Sicherheitsfunktion bis hin zum sicheren Abschalten des Leistungsteils des Antriebsreglers.

STO-Antwortzeit

Zeit zwischen dem Aktivieren oder Deaktivieren der Sicherheitsfunktion STO und der Rückmeldung in den STO-Statussignalen.

STO-Reaktionszeit

Zeit zwischen dem Aktivieren der Sicherheitsfunktion STO (Flanke von 1 auf 0) und dem Sperren des Pulsmusters am Leistungsteil.

Testimpuls

Gemäß Zentralverband Elektrotechnik- und Elektronikindustrie: Zeitlich begrenzte Änderung eines Signalspannungspegels zur Überprüfung der Funktionstüchtigkeit des Ausgangs oder Geräts oder zur Überprüfung der Übertragungsstrecke.

Testimpulsauswertung (TA)

Gemäß Zentralverband Elektrotechnik- und Elektronikindustrie: Schaltungsteil, der die für eine Diagnose erforderlichen Testimpulse sicherheitstechnisch auswertet.

Testimpulserzeugung (TE)

Gemäß Zentralverband Elektrotechnik- und Elektronikindustrie: Schaltungsteil, der die für eine Diagnose erforderlichen Testimpulse erzeugt.

Intern

Support

Technische Unterstützung von Pilz erhalten Sie rund um die Uhr.

Amerika
Brasilien
+55 11 97569-2804
Kanada
+1 888-315-PILZ (315-7459)
Mexiko
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asien
China
+86 21 60880878-216
Japan
+81 45 471-2281
Südkorea
+82 31 450 0680

Australien
+61 3 95600621

Europa
Belgien, Luxemburg
+32 9 3217575
Deutschland
+49 711 3409-444
Frankreich
+33 3 88104000
Großbritannien
+44 1536 462203
Irland
+353 21 4804983
Italien, Malta
+39 0362 1826711
Niederlande
+31 347 320477
Österreich
+43 1 7986263-0
Schweiz
+41 62 88979-30
Skandinavien
+45 74436332
Spanien
+34 938497433
Türkei
+90 216 5775552

Unsere internationale Hotline erreichen Sie unter:
+49 711 3409-444
support@pilz.com

Haben Sie Fragen zur Maschinensicherheit?
Pilz antwortet auf www.wissen-maschinensicherheit.de

Pilz entwickelt umweltfreundliche Produkte unter Verwendung ökologischer Werkstoffe und energiesparender Techniken. In ökologisch gestalteten Gebäuden wird umweltbewusst und energiesparend produziert und gearbeitet. So bietet Pilz Ihnen Nachhaltigkeit mit der Sicherheit, energieeffiziente Produkte und umweltfreundliche Lösungen zu erhalten.

Energy saving by Pilz

BLUECOMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Deutschland
Tel.: +49 711 3409-0
Fax: +49 711 3409-133
info@pilz.com
www.pilz.com

1005344-de-01, 06/2020 Printed in Germany