SIL Sicherheitshandbuch

Handbuch Sicherheitsrelais SCS 24VDC P2SIL3ES

Weidmüller

Hersteller
Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14-292083
www.weidmueller.com

Inhalt

1 Geltungsbereich und Standards

1.1 Geltungsbereich

Dieses Sicherheitshandbuch gilt für die SIL3-Relais der Weidmüller SAFESERIES ab dem Produktionsdatum 11/2012 für folgende Artikel:

SCS 24VDC P2SIL3ES	1319280000

Das SIL3-Relais der Baureihe
SCS 24VDC P2SIL3ES der

Weidmüller Interface GmbH & Co KG
Klingenbergstraße 26
32758 Detmold
Deutschland

ist vom

Zertifizierungsstelle der TÜV NORD CERT GmbH
Benannte Stelle 0044
Am TÜV 1
45307 Essen
Deutschland

entsprechend EN 61508 SIL3 für die Anwendungen „low demand mode“ und „high demand mode“ als „EC type-examination“ zertifiziert.

Zertifikat Registrier-Nr.:
44 207 13773715

1.2 Abkürzungen

Sicherheits-Integritätslevel (SIL, engl. Safety Integrity Level):

Vier diskrete Stufen (SIL1 bis SIL4). Je höher der SIL eines sicherheitsbezogenen Systems, umso geringer ist die Wahrscheinlichkeit, dass das System die geforderten Sicherheitsfunktionen nicht ausführen kann.

Average Probability of Failure on Demand (PFD_{avg}):

Mittlere Versagenswahrscheinlichkeit einer Sicherheitsfunktion bei niedriger Anforderung.

Probability of Failure per Hour (PFH):

Versagenswahrscheinlichkeit einer Sicherheitsfunktion bei hoher oder kontinuierlicher Anforderung.

Safe Failure Fraction (SFF):

Prozentualer Anteil sicherheitsgerichteter Ausfälle eines sicherheitsbezogenen Systems (Sicherheitsfunktion) bzw. Teilsystems.

Hardware-Fehlertoleranz (HFT, engl. Hardware Fault Tolerance):

HFT = n bedeutet, dass n+1 Fehler zu einem Verlust der Sicherheitsfunktion führen können.

Betriebsart „low demand mode“:

Betriebsart mit niedriger Anforderungsrate. Anforderungsrate an sicherheitsbezogenes System nicht mehr als einmal pro Jahr und nicht größer als die doppelte Frequenz der Wiederholungsprüfung.

Betriebsart „high demand mode“ oder „continuous mode“:

Betriebsart mit hoher oder kontinuierlicher Anforderung der Sicherheitsfunktion. Anforderungsrate an sicherheitsbezogenes System mehr als einmal pro Jahr oder größer als die doppelte Frequenz der Wiederholungsprüfung.

Gerätetyp A (einfaches Teilsystem):

Gerät, bei dem das Ausfallverhalten aller eingesetzten Bauteile und das Verhalten unter Fehlerbedingungen vollständig bekannt ist.

FMEDA (Failure Mode, Effects and Diagnostic Analysis):

Analysemethode für elektronische Schaltungen und Mechanik zur quantitativen Ermittlung von Ausfallarten und Ausfallraten.

Ausfallrate λ:

- λ_{SD} Gesamtausfallrate für sichere erkannte Ausfälle
- λ_{SU} Gesamtausfallrate für sichere unerkannte Ausfälle
- λ_{DD} Gesamtausfallrate für gefährliche erkannte Ausfälle
- λ_{DU} Gesamtausfallrate für gefährliche unerkannte Ausfälle

MTTF (Mean Time To Failure):

Mittlere Zeit bis zum Ausfall. MTTF ist eine Grundmessgröße der Zuverlässigkeit für nicht reparierbare Systeme.

Intervall für Wiederholungsprüfungen (T_{proof}):

Zeitintervall zwischen wiederkehrenden Prüfungen einer Sicherheitsfunktion zur Aufdeckung gefährlicher Ausfälle.

2 Gerätebeschreibung und Einsatzbereich

2.1 Besondere Produktmerkmale

- Stoppkategorie 0 nach EN 60204-1
- Anwendung bis Steuerungskategorie 4 nach EN ISO 13849-1
- Reset-Taster-Überwachung
- Ein- und zweikanalige Ansteuerung
- Querschlusserkennung
- 2 Freigabestrompfade, 1 Meldestrompfad

2.2 Allgemein

Bei diesem Sicherheitsrelais der Produktfamilie SAFESERIES handelt es sich um ein nach DIN EN 61508 / SIL 3 zertifiziertes Gerät.

Es wird zur sicherheitsgerichteten Abschaltung (DTS = de-energised to safe) von Anlagenteilen im Bereich der Prozessindustrie, wie z. B. Feuerungsanlagen (gemäß EN 746-2 und EN 50156) sowie zum Schutz von Mensch und Maschine (Not-Aus) verwendet.

2.3 Aufbau und Funktion

Zur sicherheitsgerichteten Abschaltung stehen 2 Überwachungseingänge mit Querschlusserkennung, 2 Freigabeausgänge (NO) und ein Rückmeldeausgang (NC) mit zwangsgeführten Kontakten zur Verfügung.

Der Ausgang muss extern mit maximal 5 A T abgesichert werden.

Der Baustein lässt sich wahlweise mit fallender Flanke an S33/S34 oder mit steigender Flanke an S33/S35 (Auto Start) in Betrieb nehmen. Die Reaktionszeit für das Ein- und Ausschalten an A1/A2 lässt sich durch entfernen einer Brücke an C1/C2 von > 50 ms auf < 20 ms reduzieren.

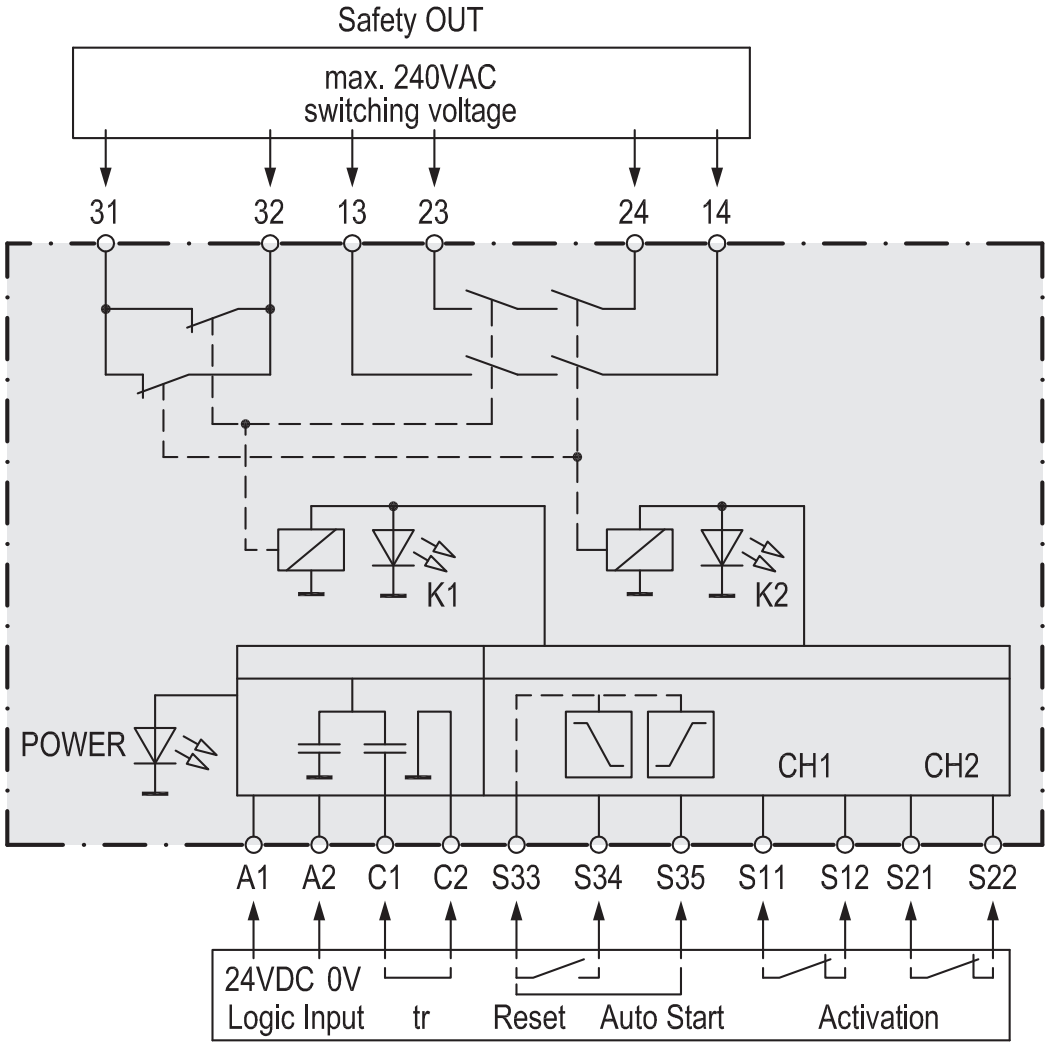
Die Ansteuerung des Sicherheitskreises erfolgt im Feld durch eine SPS mit einem 24 V Digitalausgang an A1/A2 (S11/S12 und S21/S22 gebrückt) oder mit entsprechenden Sicherheitskontakten (Schutzvorhang, Not-Aus-Taster) an S11/S12 und S21/S22 bei fester Betriebsspannung an A1/A2.

Ein Rücksetzen ist nur durch Öffnen und Schließen beider Überwachungskreise oder Aus- und Einschalten der Betriebsspannung möglich.

Eine minimale Stromaufnahme von 35 mA bei 24 V DC -10 % im Eingang ist gewährleistet.

Testimpulse (t_p < 1 ms)einer SPS zur Leitungsbrucherkennung an A1/A2 führen nicht zum Ein- oder Ausschalten der Ausgangsrelaiskontakte.

2.4 Blockschaltbild



3 Hinweise zur Projektierung

3.1 Betriebsart mit niedriger Anforderungsrate nach EN 61508

Die SIL3-Relais der SAFESERIES werden in der Betriebsart mit niedriger Anforderungsrate (low demand mode) eingesetzt, wenn die Anforderungsrate an das SIL3-Relais nicht mehr als 1× pro Jahr beträgt und nicht mehr als die doppelte Frequenz der Wiederholungsprüfung ist (siehe DIN EN 61508 4, 3.5.12).
Für die Anforderungsrate und die zugehörige Kenngröße PFD gelten bei einem Prüfintervall T_{proof} von 12 Jahren die angegebenen Werte in der nachfolgenden Tabelle 2.

3.2 Betriebsart mit hoher Anforderungsrate nach EN 61508

Trifft „Betriebsart mit niedriger Anforderungsrate“ nicht zu, so ist das SIL3-Relais als sicherheitsrelevantes Teilsystem in der Betriebsart mit hoher bzw. kontinuierlicher Anforderungsrate (high demand mode oder continuous mode) einzusetzen (DIN EN 61508-4, 3.5.12). Für die Anforderungsrate und die zugehörige Kenngröße PFH gelten die angegebenen Werte in der nachfolgenden Tabelle 3.

3.3 Betriebsart mit hoher Anforderungsrate nach EN ISO 13849-1

Für die Anforderungsrate und die zugehörige Kenngröße PFH gelten die angegebenen Werte in der nachfolgenden Tabelle 4.

3.4 Fehlerarten

Ein ungefährlicher Ausfall (safe failure) hat nicht das Potential, das sicherheitstechnische System in einen gefahrbringenden oder funktionsunfähigen Zustand zu setzen. Das SIL3-Relais geht in den definierten sicheren Zustand.

Ein gefährlicher unentdeckter Ausfall (dangerous undetected failure) hat das Potential, das sicherheitstechnische System in einen gefahrbringenden oder funktionsunfähigen Zustand zu versetzen. Das SIL3-Relais geht nicht in den definierten sicheren Zustand.

3.5 Testintervall

Das Testintervall bzw. Prüfintervall T_{proof} ist der Zeitraum, in dem Tests vollständig durchgeführt und wiederholt werden.

Innerhalb dieser Zeit werden zufällige Hardwarefehler erkannt.

Tabelle 1

Sicherheitstechnische Basiskenndaten	
Sicherheitskategorie	SIL3
Sicherheitsnorm	DIN EN 61508
Gerätetyp	A
HFT	1

Tabelle 2

Sicherheitstechnische Kenndaten „low demand mode“ nach EN 61508							
Switching cycle	**PFH**	**SFF**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SIL**
1× pro Jahr	$2{,}3 \times 10^{-12}\ h^{-1}$	99,99 %	$1{,}13 \times 10^{-1}$ FIT	$1{,}6 \times 10^{+1}$ FIT	$1{,}13 \times 10^{-1}$ FIT	$1{,}14 \times 10^{-3}$ FIT	3

FIT = $10^{-9}\ h^{-1}$ (Failure in time)

Tabelle 3

Sicherheitstechnische Kenndaten „high demand mode“ nach EN 61508							
Switching cycle	**PFH**	**SFF**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SIL**
1× pro Tag	$7{,}87 \times 10^{-10}\ h^{-1}$	99,58 %	$4{,}11 \times 10^{+1}$ FIT	$1{,}64 \times 10^{+1}$ FIT	$4{,}11 \times 10^{+1}$ FIT	$4{,}15 \times 10^{-1}$ FIT	3
10× pro Tag	$8{,}41 \times 10^{-9}\ h^{-1}$	99,51 %	$4{,}12 \times 10^{+2}$ FIT	$2{,}02 \times 10^{+1}$ FIT	$4{,}12 \times 10^{+2}$ FIT	4,17 FIT	3

FIT = $10^{-9}\ h^{-1}$ (Failure in time)

Tabelle 4

Sicherheitstechnische Kenndaten „high demand mode“ nach EN ISO 13849-1						
Switching cycle	**PFH**	**MTTFD**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
1× pro Jahr	$2{,}3 \times 10^{-12}\ h^{-1}$	2500	$1{,}13 \times 10^{-1}$ FIT	$1{,}6 \times 10^{+1}$ FIT	$1{,}13 \times 10^{-1}$ FIT	$1{,}14 \times 10^{-3}$ FIT
10× pro Tag	$8{,}41 \times 10^{-9}\ h^{-1}$	270	$4{,}12 \times 10^{+2}$ FIT	$2{,}02 \times 10^{+1}$ FIT	$4{,}12 \times 10^{+2}$ FIT	4,17 FIT

FIT = $10^{-9}\ h^{-1}$ (Failure in time)
Diagnosedeckungsgrad (DC): 99%
Hardwarekategorie: 4
Performancelevel (PL): e

4 Montage und Installation

Für das SIL3-Relais muss die Bedienungsanleitung mit der Bezeichnung / Bestellnummer

IS SCS 24VDC P2SIL3ES 1412550000

vorhanden sein.

Die darin enthaltenen Hinweise, Randbedingungen und Grenzwerte sind bei der Installation und dem Betrieb der SIL3-Relais zu berücksichtigen.

Vor Inbetriebnahme bzw. nach jeder Änderung der Verdrahtung ist die bestimmungsgemäße Funktion des SIL3-Relais zu überprüfen, siehe Kapitel 5.1 „Überprüfung der Funktion“.

Das Gerät darf nur mit einer externen Sicherung betrieben werden.

Im Falle eines Kurzschlusses ist sicherzustellen, dass die Ursache beseitigt wird und nach dem Austausch der Sicherung ein Funktionstest erfolgt.

5 Wiederkehrende Prüfungen

Es liegt in der Verantwortung des Betreibers, die Art der Überprüfung und die Zeitabstande zu wählen. Die Testintervalle werden u. a. bei der Berechnung jedes einzelnen Sicherheitskreises einer Anlage (PFD-Werte) bestimmt.

Die Prüfung ist so durchzuführen, das die einwandfreie Funktion der Sicherheitsfunktion im Zusammenwirken aller Komponenten nachgewiesen wird.

5.1 Überprüfung der Funktion

Die Überprüfung der Funktion erfolgt in 3 Schritten, gemäß der unten stehenden Tabellen.

5.1.1 Funktionstest „Reset“

Eingangsspannung: 24 V DC

Verbindung: S33/S34

Reset	Überwachung		Signalisierung		Ausgang		Rück-meldung
S33/S34	S11/S12	S21/S22	LED K1	LED K2	13/14	23/24	31/32
0→1→0	offen	offen	AUS	AUS	offen	offen	geschlossen
0→1→0	geschlossen	offen	AUS	AUS	offen	offen	geschlossen
0→1→0	offen	geschlossen	AUS	AUS	offen	offen	geschlossen
0→1→0	geschlossen	geschlossen	AN	AN	geschlossen	geschlossen	offen

5.1.2 Funktionstest „Auto Start“

Eingangsspannung: 24 V DC

Verbindung: S33/S35

Steuer-eingang	Überwachung		Signalisierung		Ausgang		Rück-meldung
A1/A2	S11/S12	S21/S22	LED K1	LED K2	13/14	23/24	31/32
0→1	offen	offen	AUS	AUS	offen	offen	geschlossen
0→1	geschlossen	offen	AUS	AUS	offen	offen	geschlossen
0→1	offen	geschlossen	AUS	AUS	offen	offen	geschlossen
0→1	geschlossen	geschlossen	AN	AN	geschlossen	geschlossen	offen

5.1.3 Funktionstest „Überwachung“

Eingangsspannung: 24 V DC

Verbindung: S33/S35

Testschritt	Überwachung		Signalisierung		Ausgang		Rück-meldung
	S11/S12	S21/S22	LED K1	LED K2	13/14	23/24	31/32
1.	geschlossen	geschlossen	AN	AN	geschlossen	geschlossen	offen
2.	offen	geschlossen	AUS	AN	offen	offen	geschlossen
3.	geschlossen	geschlossen	AUS	AN	offen	offen	geschlossen
4.	geschlossen	offen	AUS	AUS	offen	offen	geschlossen
5.	geschlossen	geschlossen	AN	AN	geschlossen	geschlossen	offen
6.	offen	offen	AUS	AUS	offen	offen	geschlossen

6 Sicherheitstechnische Kenngrößen

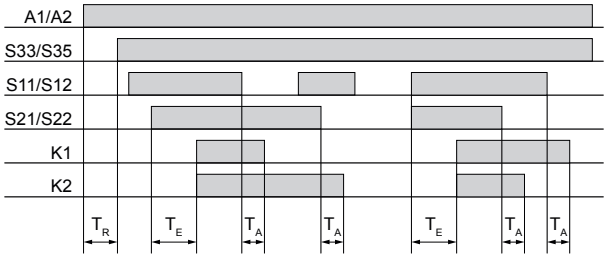
6.1 Annahmen

- Die max. zulässige Umgebungstemperatur im Betrieb beträgt 55 °C
- Die Umweltbedingungen entsprechen einer durchschnittlichen industriellen Umgebung
- Die Spezifikationen im Datenblatt und in der Bedienungsanleitung dürfen nicht überschritten werden.

7 Funktionsdiagramme

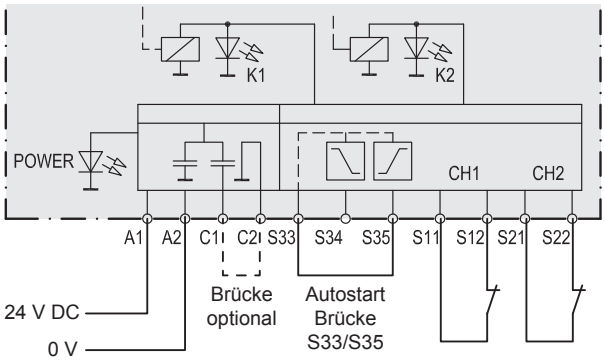
7.1 Automatischer Start

Der Reset-Eingang S33 wird mit S35 verbunden. An A1/A2 liegt die Versorgungsspannung an. Das Gerät startet mit steigender Flanke des Signals an den Sicherheitseingängen S11/S12 und S21/S22.



T_E = 30 ms (Einschaltzeit K1 und K2)
T_A = 15 ms (Ausschaltzeit K1 und K2)

T_R = typ. 50 ms (Reaktionszeit mit Brücke C1/C2)
T_R = typ. 20 ms (Reaktionszeit ohne Brücke C1/C2)

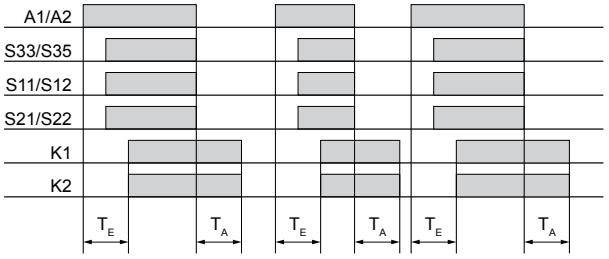


Achtung

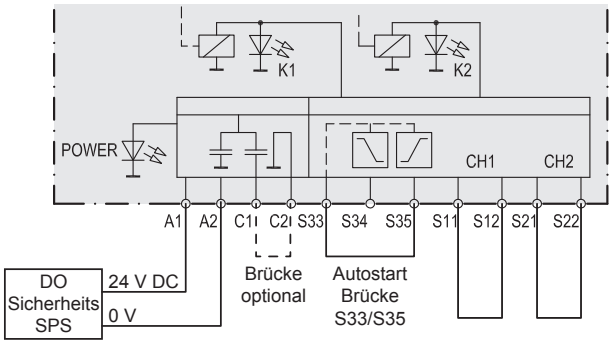
Es muss sichergestellt werden, dass es nicht zu einem unerwarteten Anlauf nach Unterbrechung der Versorgungsspannung kommt.

7.2 Start über A1/A2

Der Reset-Eingang S33 wird mit S35 verbunden. Die Sicherheitseingänge S11/S12 und S12/S22 werden überbrückt. Nach Anlegen der Versorgungsspannung an A1/A2 werden die Freigabestrompfade geschlossen.



T_E = 55 ms (Einschaltzeit K1 und K2 mit Brücke C1/C2)
T_A = 55 ms (Ausschaltzeit K1 und K2 mit Brücke C1/C2)

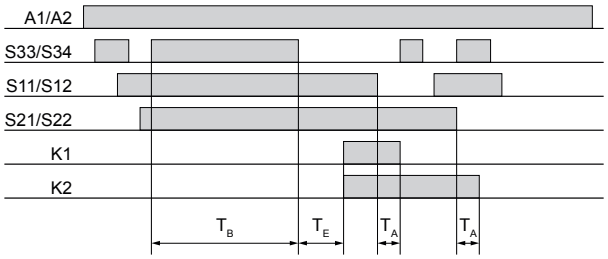


Achtung

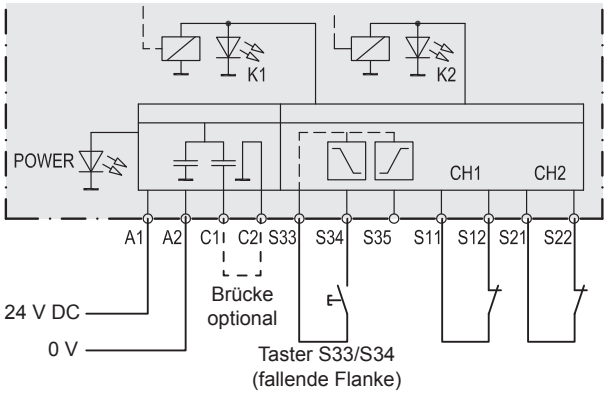
Es muss sichergestellt werden, dass es nicht zu einem unerwarteten Anlauf nach Unterbrechung der Versorgungsspannung kommt.

7.3 Manueller Start – Triggerung auf fallende Flanke

Mittels eines Tasters wird bei geschlossenen Sicherheitseingängen der Reset-Eingang S34 geöffnet (Triggerung bei fallender Flanke)

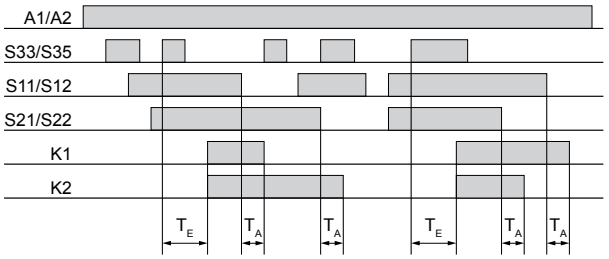


T_B = 100 ms (Bereitschaftszeit)
T_E = 30 ms (Einschaltzeit K1 und K2)
T_A = 15 ms (Ausschaltzeit K1 und K2)

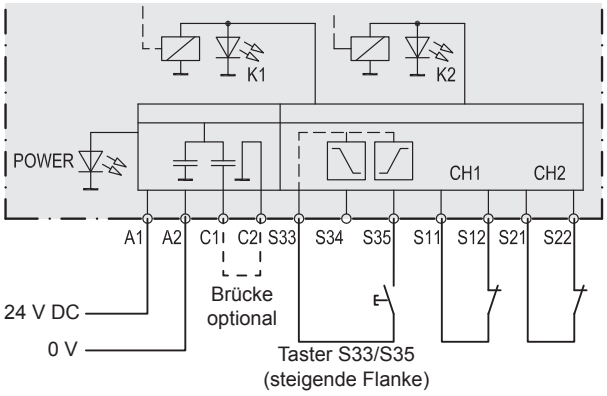


7.4 Manueller Start – Triggerung auf steigende Flanke

Mittels eines Tasters wird bei geschlossenen Sicherheitseingängen der Reset-Eingang S35 geschlossen (Triggerung bei steigender Flanke)



T_E = 30 ms (Einschaltzeit K1 und K2)
T_A = 15 ms (Ausschaltzeit K1 und K2)



8 Betriebsarten / Hinweise

- Ein- oder zweikanalige Ansteuerung
  - Bei einkanaliger Ansteuerung erfolgt keine Querschlusserkennung.

- Wiederanlaufsperre
  - Nach Öffnen und Schließen der Sicherheitseingänge erfolgt kein erneuter Anlauf.
    Der Wiederanlauf kann nur nach Betätigung des Reset-Tasters erreicht werden.
    Für die Wiederanlaufsperre sind wie bei der Betriebsart „Manueller Start”, die Reset-Eingänge mit Taster anzusteuern.

www.weidmueller.com

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14-292083
www.weidmueller.com

1438120000/03/03-2023