8.2.17 Kaskadierung von Schutzeinrichtungen mittels Sicherheitsbausteinen – Kategorie 3 – PL d (Beispiel 17)

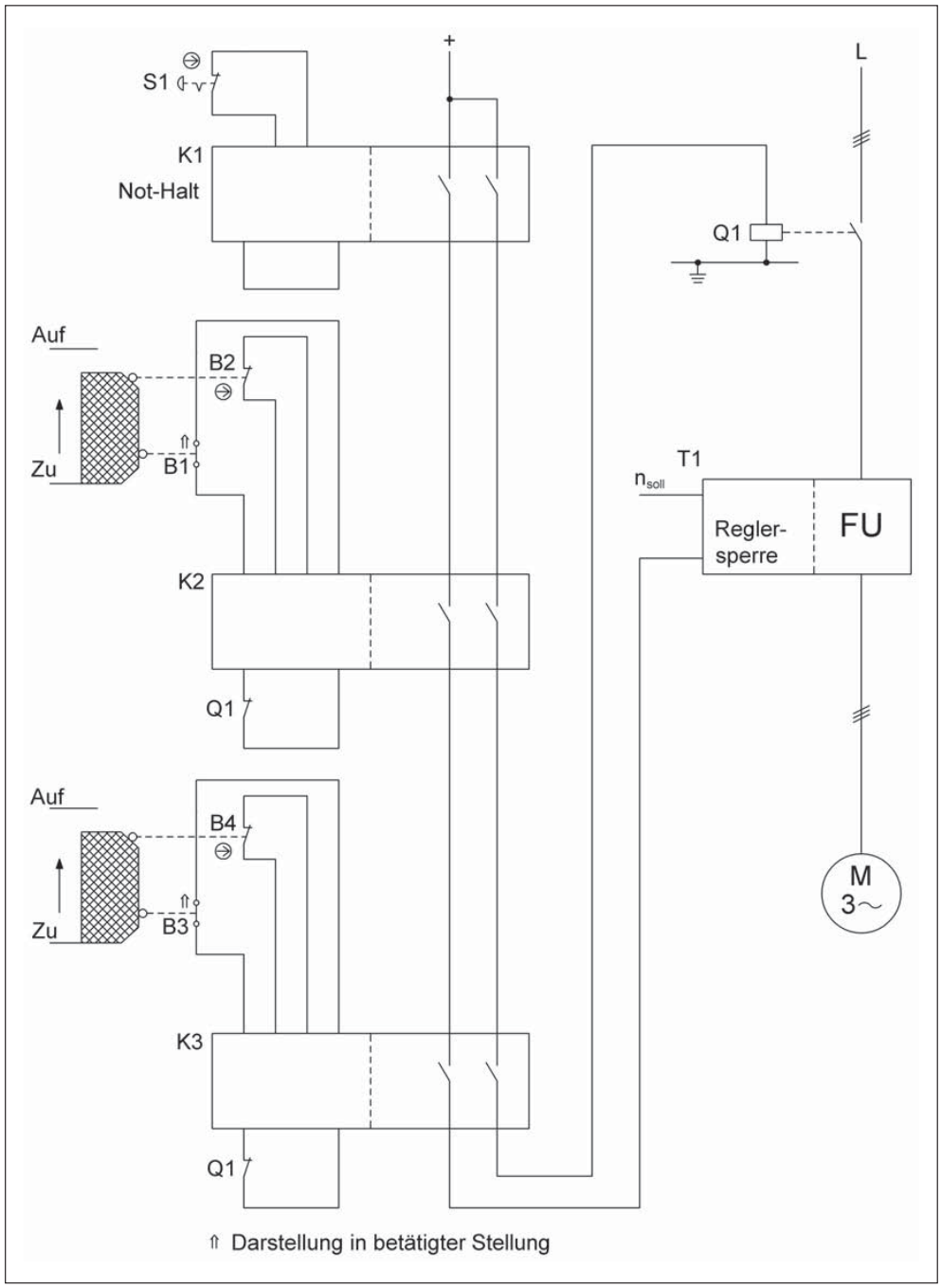
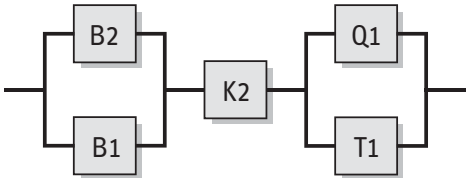


Abbildung 8.29: Kaskadierung von Schutzeinrichtungen mittels Sicherheitsbausteinen (Not-Halt-Funktion, STO)



Sicherheitsfunktionen

- Not-Halt-Funktion, STO – Sicher abgeschaltetes Moment durch Betätigung des Not-Halt-Gerätes
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der beweglichen trennenden Schutzeinrichtung leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden bei Betätigung des Not-Halt-Geräts S1 über den Sicherheitsbaustein K1 redundant durch Unterbrechung der Steuerspannung von Schütz Q1 und Anwahl der Reglersperre des Frequenzumrichters T1 abgeschaltet. Zusätzlich erfolgt die Sicherung einer Gefahrenstelle mit zwei beweglichen trennenden Schutzeinrichtungen (z.B. jeweils für Beladung und Entnahme). Das Öffnen eines Schutzgitters wird durch zwei Positionsschalter B1/B2 in Öffner-Schließer-Kombination erfasst und in einem zentralen Sicherheitsbaustein K2 ausgewertet. Dieser kann in gleicher Weise wie K1 gefahrbringende Bewegungen oder Zustände unterbrechen bzw. verhindern. Die Überwachung des zweiten Schutzgitters erfolgt in der gleichen Weise mit den zwei Positionsschaltern B3/B4 und einem Sicherheitsbaustein K3, der ebenfalls auf Q1 und T1 wirkt.
- Bei Auftreten eines Bauteilausfalls bleibt die Sicherheitsfunktion erhalten.
- Die meisten Bauteilausfälle werden erkannt und führen zur Betriebshemmung. Beide Positionsschalter an einem Schutzgitter werden im zugehörigen Sicherheitsbaustein, der auch über interne Diagnosemaßnahmen verfügt, auf Plausibilität überwacht. Fehler im Schütz Q1 werden über zwangsgeführte Kontakte und deren Rücklesung in K2 und K3 erkannt. Eine zusätzliche Rücklesung in K1 ist nicht erforderlich, da die Not-Halt-Funktion viel seltener angefordert wird. Ein Teil der Fehler in T1 werden durch den Prozess erkannt. Einige wenige Fehler werden von der Steuerung nicht erkannt.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z.B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtungen zur Betätigung der Positionsschalter ist sichergestellt.
- Das Not-Halt-Gerät S1 entspricht DIN EN ISO 13850, B2 und B4 sind Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern B1 bis B4 sind getrennt oder geschützt verlegt.
- Das Schütz Q1 besitzt zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Sicherheitsbausteine K1, K2 und K3 erfüllen alle Anforderungen für Kategorie 4 und PL d.
- Der Frequenzumrichter T1 verfügt über keine integrierte Sicherheitsfunktion.

Bemerkungen

- Die Not-Halt-Funktion ist eine ergänzende Schutzmaßnahme nach DIN EN ISO 12100-2:2004.

Berechnung der Ausfallwahrscheinlichkeit

- Die Schaltung lässt sich in drei Sicherheitsfunktionen und jeweils drei Subsysteme aufteilen. Das sicherheitsbezogene Blockdiagramm zeigt die sicherheitsbezogene Stoppfunktion beispielhaft für eine Schutzeinrichtung, da zu einem Zeitpunkt immer nur eine Schutzeinrichtung geöffnet wird. Für die zweite Schutzeinrichtung gilt die gleiche Sicherheitsfunktion und eine identische Berechnung der Ausfallwahrscheinlichkeit. Bei der Not-Halt-Funktion treten das Not-Halt-Gerät S1 und der Sicherheitsbaustein K1 an die Stelle der ersten beiden Subsysteme. Die Ausfallwahrscheinlichkeit der fertigen Sicherheitsbausteine K1, K2 und K3 wird am Ende der Berechnung addiert ($2{,}31 \cdot 10^{-9}$/Stunde [H], geeignet für PL e). Für die übrigen Subsysteme wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.

- Bei S1 handelt es sich um ein handelsübliches Not-Halt-Gerät nach DIN EN ISO 13850. Es erfolgt ein Fehlerausschluss für den zwangsöffnenden Kontakt und die Mechanik, sofern die in Tabelle D.2 dieses Reports angegebene Anzahl der Betätigungen nicht überschritten wird. Für n_{op} wird von drei Betätigungen im Jahr ausgegangen. Hinsichtlich der Gesamtschaltungen von Q1 und dem Frequenzumrichter wird dieser Wert bei der weiteren Berechnung für beide Sicherheitsfunktionen vernachlässigt.

- $MTTF_d$: Für den Positionsschalter B2 mit zwangsöffendem Kontakt ist ein Fehlerausschluss für den elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt des Positionsschalters B1 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B2 und B1 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 10 Minuten Zykluszeit ist für diese Komponenten n_{op}= 35 040 Zyklen/Jahr und $MTTF_d$ beträgt 285 Jahre für B2 bzw. 142 Jahre für B1. Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 000 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10d}-Wert durch Verdoppelung des B_{10}-Wertes. Da Q1 an beiden sicherheitsbezogenen Stoppfunktionen beteiligt ist, folgt mit dem Doppelten des oben angenommenen Wertes für n_{op} eine $MTTF_d$ von 285 Jahren. Für den Frequenzumrichter T1 beträgt die $MTTF_d$ 20 Jahre [H]. Insgesamt ergibt sich im Subsystem Q1/T1 ein symmetrisierter $MTTF_d$-Wert pro Kanal von 68 Jahren („hoch“).

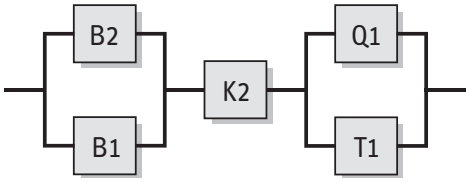
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung der Öffner-Schließer-Kombinationen in K2. Dies entspricht der DC_{avg} für das Subsystem. DC = 99 % für das Schütz Q1 ergibt sich aus der Rücklesung der Kontaktstellung in den Sicherheitsbausteinen. Für den Frequenzumrichter T1 folgt DC = 60 % aus der Fehlererkennung durch den Prozess. Durch Mittelung ergibt sich damit für das Subsystem Q1/T1 ein DC_{avg} von 62 % („niedrig“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in den Subsystemen B2/B1 bzw. Q1/T2 (70 bzw. 85 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10), in B2/B1 bewährte Bauteile (5), in Q1/T1 Diversität (20)

- Das Subsystem B1/B2 entspricht Kategorie 3 mit hoher $MTTF_d$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde. Das Subsystem Q1/T1 entspricht Kategorie 3 mit hoher $MTTF_d$ (68 Jahre) und niedrigem DC_{avg} (62 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}73 \cdot 10^{-7}$/Stunde.

- Für die sicherheitsbezogene Stoppfunktion ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}00 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

- Für Not-Halt-Funktion ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}75 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.



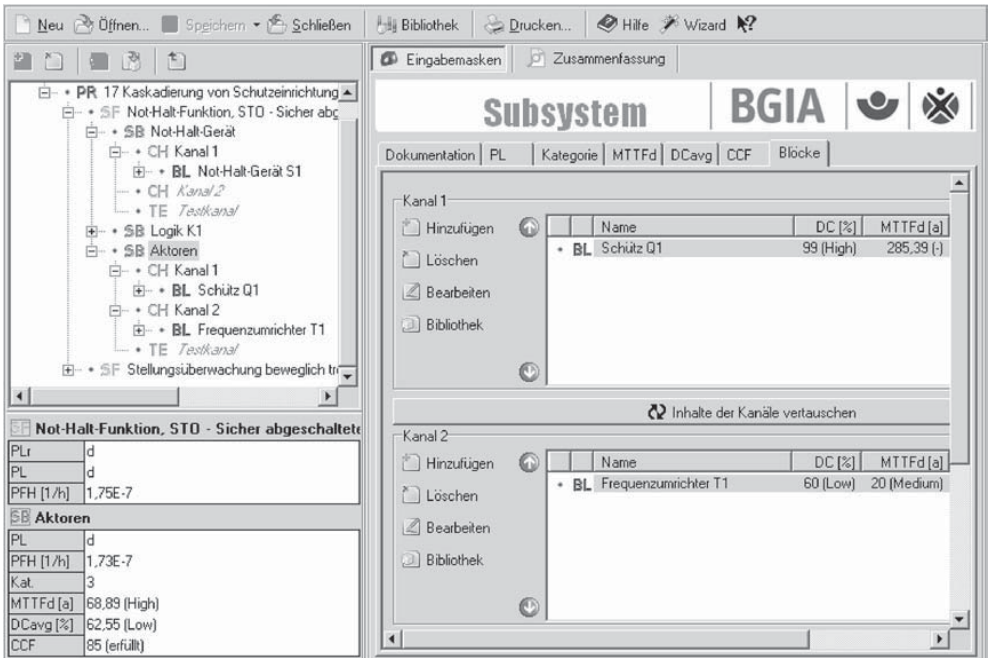


Abbildung 8.30: PL-Bestimmung mithilfe von SISTEMA