8.2.10 Sicheres Stillsetzen eines SPS-gesteuerten Antriebs mit Not-Halt – Kategorie 3 – PL c (Beispiel 10)

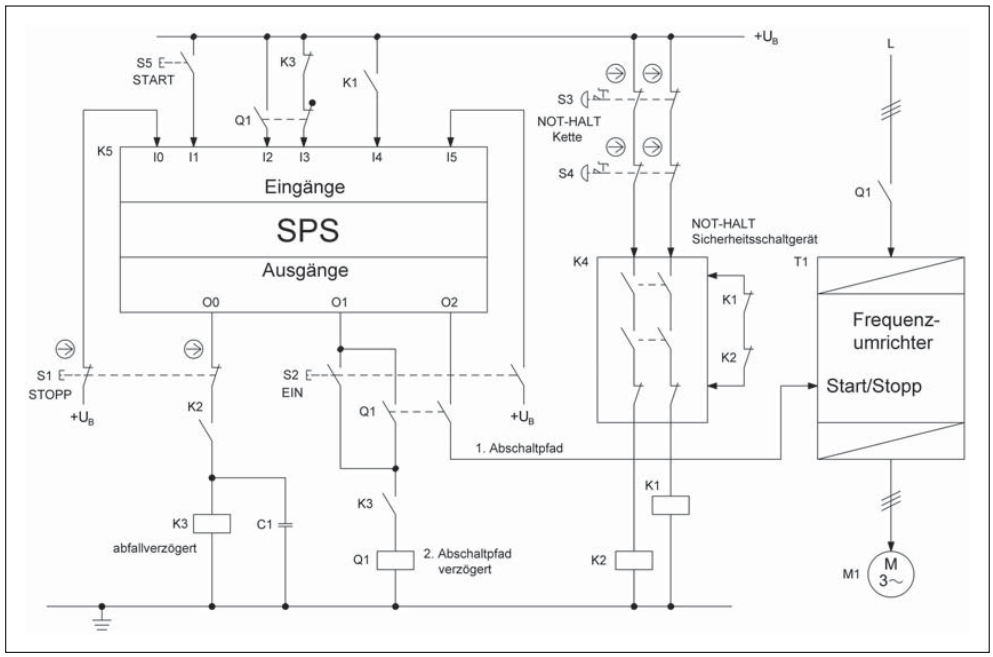


Abbildung 8.18: Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Stopp- oder Not-Halt-Befehl

Sicherheitsfunktion

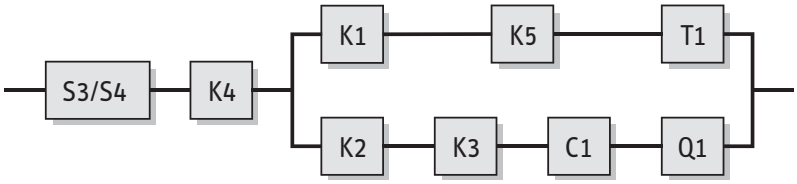
- Sicherheitsbezogene Stoppfunktion bzw. Not-Halt-Funktion: Nach einem Stopp- oder Not-Halt-Befehl wird der Antrieb angehalten (SS1 – Sicherer Stopp 1).

Funktionsbeschreibung

- Die gefahrbringende Bewegung wird redundant unterbrochen, falls entweder die Stopp-Taste S1 oder eines der Not-Halt-Geräte S3 bzw. S4 betätigt wird. Das Stillsetzen des Antriebs im Notfall erfolgt nach Betätigung von S3/S4 zuerst durch Deaktivierung des Not-Halt-Sicherheitsschaltgerätes K4 einhergehend mit dem Entregen der Hilfsschütze K1 und K2. Das Öffnen des Schließerkontaktes K1 am Eingang I4 der SPS K5 bewirkt über den SPS-Ausgang O2 die Rücknahme des Startsignals am Frequenzumrichter (FU) T1. Redundant zur Kette K1-K5-T1 startet mit dem Öffnen des Schließerkontaktes K2 vor dem abfallverzögerten Hilfsschütz K3 eine Bremszeitvorgabe, nach deren Ablauf die Ansteuerung für das Netzschütz Q1 unterbrochen wird. Die Zeitvorgabe ist so gewählt, dass unter ungünstigen Betriebsbedingungen der Stillstand der Maschinenbewegung erreicht wird, noch bevor das Netzschütz Q1 abfällt.

- Das funktionsgemäße Stillsetzen des Antriebs nach einem Stopp-Befehl wird mit dem Öffnen der beiden Öffnerkontakte der Stopp-Taste S1 eingeleitet. Analog zum Stillsetzen im Notfall erfolgt zunächst die Abfrage durch die SPS K5 über Eingang I0 und die Absteuerung des FU mit dem Rücksetzen des SPS-Ausgangs O2. Redundant dazu wird das Hilfsschütz K3 – abfallverzögert mithilfe des Kondensators C1 – entregt und nach Ablauf der Bremszeitvorgabe wird die Ansteuerung für das Netzschütz Q1 unterbrochen.

- Bei einem einzelnen Versagen der SPS K5, des Umrichters T1, des Netzschützes Q1, der Hilfsschütze K1/K2 oder des abfallverzögerten Hilfsschützes K3 wird jeweils das Stillsetzen des Antriebs sichergestellt, weil immer zwei voneinander unabhängige Abschaltpfade vorhanden sind. Ein Nichtabfallen der Hilfsschütze K1 und K2 wird durch Überwachung der zwangsgeführten Öffnerkontakte innerhalb des Not-Halt-Sicherheitsschaltgerätes K4 spätestens nach dem Entriegeln des betätigten Not-Halt-Gerätes aufgedeckt. Das Nichtabfallen des Hilfsschützes K3 wird wegen der vorhandenen Rückführung des zwangsgeführten Öffnerkontaktes in den SPS-Eingang I3 spätestens vor einem erneuten Ingangsetzen der Maschinenbewegung aufgedeckt. Der Nichtabfall des Netzschützes Q1 wird über den in SPS-Eingang I3 eingelesenen Spiegelkontakt aufgedeckt.



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.
- Die Hilfsschütze K1, K2 und K3 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Kontakte der Taster S1, S3 und S4 sind zwangsöffnend ausgeführt entsprechend DIN EN 60947-5-1, Anhang K.
- Das Schütz Q1 besitzt einen Spiegelkontakt entsprechend DIN EN 60947-4-1, Anhang F.
- Die Standardkomponenten K5 und T1 werden entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL b (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.
- Die verzögerte Einleitung des Stillstands im Fehlerfall nur über den zweiten Abschaltpfad darf nicht mit einem verbleibenden inakzeptabel hohen Risiko verbunden sein.
- Der sicherheitsrelevante Steuerungsteil des Not-Halt-Sicherheitsschaltgerätes K4 erfüllt alle Anforderungen für Kategorie 3 und PL d.

Berechnung der Ausfallwahrscheinlichkeit

Es wird nur die Ausfallwahrscheinlichkeit der Not-Halt-Funktion berechnet. Für die Berechnung der sicherheitsbezogenen Stoppfunktion müssen S3/S4 und K4 durch S1 ausgetauscht sowie K1 und K2 weggelassen werden.

- Für die Not-Halt-Geräte S3/S4 wird ein Fehlerausschluss angenommen, da die in Tabelle D.2 genannte maximale Anzahl von 6 050 Schaltzyklen innerhalb der Gebrauchsdauer des Schaltgerätes nicht überschritten wird. Das Not-Halt-Sicherheitsschaltgerät K4 liegt als geprüftes Sicherheitsbauteil vor. Seine Ausfallwahrscheinlichkeit beträgt $3{,}0 \cdot 10^{-7}$/Stunde [H] und wird am Ende der Berechnung addiert. Der Wert gilt für eine maximale Anzahl von 6 050 Schaltzyklen innerhalb der Gebrauchsdauer des Schaltgerätes.

Für die Ausfallwahrscheinlichkeit der nachfolgenden zweikanaligen Struktur gilt:

- $MTTF_d$: Folgende $MTTF_d$-Werte werden geschätzt: 25 Jahre für K5 und 50 Jahre für T1 [G]. Der Kondensator C1 geht mit $MTTF_d$ = 45 662 Jahren [D] in die Berechnung ein. Für K1 und K2 ergibt sich bei einem B_{10d}-Wert von 400 000 Zyklen [N] und Schalthäufigkeit von täglichem Einschalten an 240 Arbeitstagen eine $MTTF_d$ von 16 667 Jahren. Für K3 und Q1 ergibt sich bei einem B_{10d}-Wert von 400 000 Zyklen [N] und bei 240 Arbeitstagen, 16 Arbeitsstunden und 3 Minuten Zykluszeit eine n_{op} = 76 800 Zyklen/Jahr und jeweils eine $MTTF_d$ von 52 Jahren. Diese Werte ergeben eine symmetrisierte $MTTF_d$ des Kanals von 21 Jahren („mittel“).
- DC_{avg}: Fehlererkennung durch den Prozess bei Ausfall der Ansteuerung der Bremsrampe führt auf DC = 30 % für K5. Für T1 ergibt sich DC = 60 % ebenfalls aus der Fehlererkennung durch den Prozess. K1 und K2 zeigen DC = 99 % durch in K4 integrierte Fehlererkennung und K3 DC = 99 % wegen Fehlererkennung durch K5. Für C1 gilt DC = 60 % durch Testung des Zeitglieds bei spannungsfreiem FU. Für Q1 folgt DC = 99 % durch direkte Überwachung in K5. Die Mittelungsformel für DC_{avg} ergibt 63 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (75 Punkte): Trennung (15), Diversität (20), FMEA (5) und Umgebungsbedingungen (25 + 10).

- Die zweikanalige Kombination der Steuerungselemente entspricht Kategorie 3 mit mittlerer $MTTF_d$ pro Kanal (21 Jahre) und niedrigem DC_{avg} (63 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}04 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Die Gesamtausfallwahrscheinlichkeit wird durch Addition der Wahrscheinlichkeit gefährlicher Ausfälle von K4 ermittelt und beträgt $1{,}34 \cdot 10^{-6}$/Stunde. Dies entspricht dann ebenfalls PL c.

- Die verschleißbehafteten Elemente K3 und Q1 sollten nach jeweils ca. fünf Jahren (T_{10d}) ausgetauscht werden.

Weiterführende Literatur

- *Apfeld, R.; Zilligen, H.:* Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA-Report 5/2003. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003
  www.dguv.de/bgia, Webcode d6428

- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (04.08). Beuth, Berlin 2008

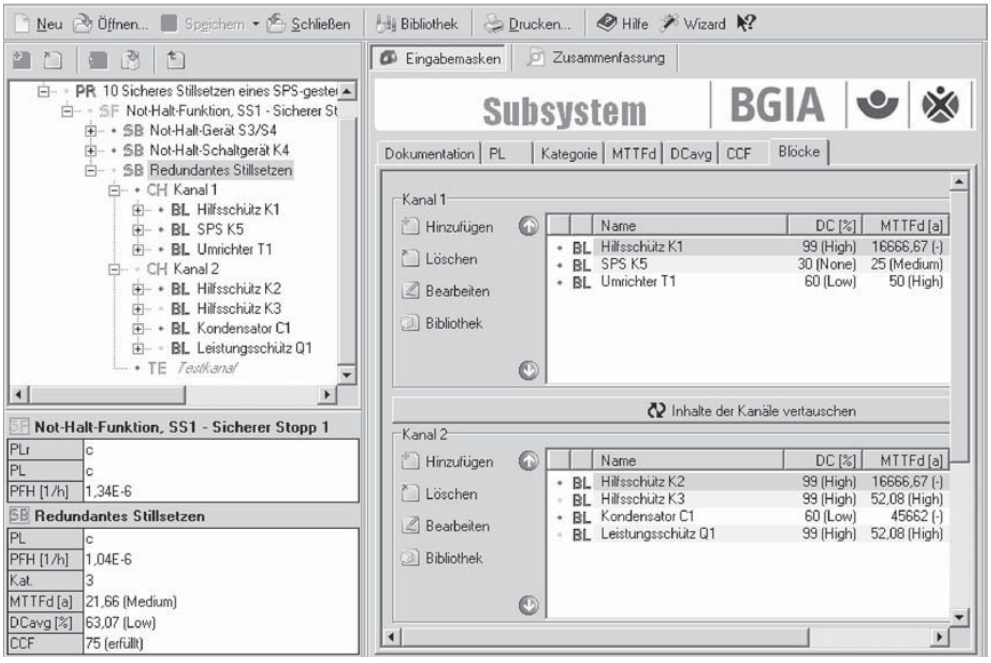


Abbildung 8.19: PL-Bestimmung mithilfe von SISTEMA