8.2.20 Sicheres Stillsetzen eines SPS-gesteuerten Antriebs – Kategorie 3 – PL d (Beispiel 20)

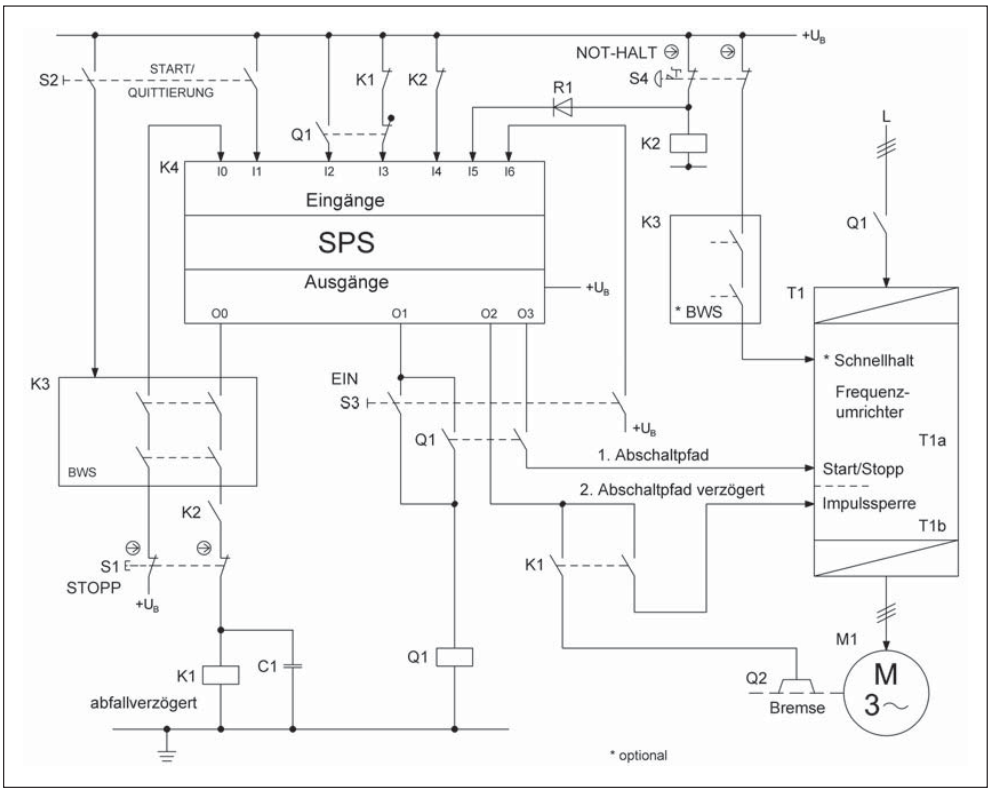


Abbildung 8.34: Sicheres Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Stopp- oder Not-Halt-Befehl oder nach dem Ansprechen einer Schutzeinrichtung (hier: BWS)

Sicherheitsfunktion

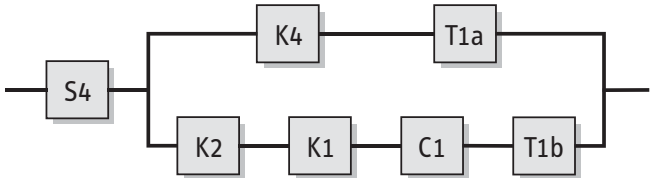
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Nach einem Stopp- oder Not-Halt-Befehl oder nach dem Ansprechen einer Schutzeinrichtung wird der Antrieb angehalten (SS1 – Sicherer Stopp 1).

Funktionsbeschreibung

- Die gefahrbringende Bewegung wird redundant unterbrochen, falls entweder die Stopp-Taste S1 oder die Schutzeinrichtung K3 (im Schaltbild als berührungslose wirkende Schutzeinrichtung (BWS) dargestellt) aktiviert wird. Das Stillsetzen des Antriebs im Notfall erfolgt nach Betätigung des Not-Halt-Gerätes S4. In allen drei Fällen wird über den Ausgang O3 der SPS K4 durch Deaktivierung des Eingangs „Start/Stopp“ (T1a) am Frequenzumrichter (FU) T1 die erste Bremszeitvorgabe realisiert. Redundant dazu wird als zweite Bremszeitvorgabe über das Entregen des Hilfsschützes K1 (abfallverzögert mithilfe des Kondensators C1) der Eingang „Impulssperre“ (T1b) an T1 deaktiviert und die Bremse Q2 fällt ein. Der erste Abschaltpfad wird also über die SPS K4 unmittelbar realisiert, wohingegen der zweite Abschaltpfad verzögert kontaktbehaftet abschaltet. Die Zeitvorgaben für O2 im SPS-Programm und für K1 sind so gewählt, dass auch unter ungünstigen Betriebsbedingungen der Stillstand der Maschinenbewegung erreicht wird.

- Steht ein Eingang „Schnellhalt“ mit besonders kurzer Geschwindigkeitsabsteuerung am FU zur Verfügung, können Not-Halt-Gerät und BWS optional – wie im Schaltbild gekennzeichnet – eingebunden werden. Diese Variante wird im Folgenden nicht weiter betrachtet.

- Bei einem einzelnen Versagen der SPS K4, der Umrichtereingänge T1a/T1b, des abfallverzögerten Hilfsschützes K1 oder des Hilfsschützes K2 wird jeweils das Stillsetzen des Antriebes sichergestellt, weil immer zwei voneinander unabhängige Abschaltpfade vorhanden sind. Das Nichtabfallen der Hilfsschütze K1 oder K2 wird wegen der vorhandenen Rückführung der zwangsgeführten Öffnerkontakte in die SPS-Eingänge I3 und I4 spätestens vor einem erneuten Ingangsetzen der Maschinenbewegung 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.
- Durch die Verwendung eines Frequenzumrichters mit sicherer Impulssperre ist der Einsatz des Leistungsschützes Q1 zum Abschalten der Versorgungsspannung nicht unbedingt erforderlich. Der Frequenzumrichter muss zum Antreiben und Bremsen geeignet sein.
- Die Hilfsschütze K1 und K2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Kontakte der Taster S1 und S4 sind zwangsöffnend ausgeführt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Standardkomponenten K4 und T1 werden entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL c (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.
- Ist die Bremse Q2 nur aus funktionalen Gründen vorhanden und somit an der Ausführung der Sicherheitsfunktion nicht beteiligt, wird sie – wie in diesem Beispiel – bei der Berechnung der Ausfallwahrscheinlichkeit nicht berücksichtigt. Diese Vorgehensweise setzt voraus, dass ein Austrudeln des Antriebs bei einem Versagen von T1a (s.u.) und somit bei alleiniger Abschaltung über die Impulssperre nicht mit einem verbleibenden inakzeptabel hohen Risiko verbunden ist. Die Beteiligung einer Bremse bei der Ausführung der Sicherheitsfunktion im Zusammenhang mit dem Einsatz eines FU ist im Beispiel Karusselltürsteuerung (Beispiel 23, siehe Seite 156 ff.) beschrieben.
- Die BWS K3 erfüllt, z.B. als Lichtgitter, die Anforderungen für Typ 4 nach DIN EN 61496-1 und DIN CLC/TS 61496-2 sowie für PL e.

Berechnung der Ausfallwahrscheinlichkeit

- Es wird die Ausfallwahrscheinlichkeit des sicheren Stillsetzens ausgelöst durch das Not-Halt-Gerät S4 bzw. durch die BWS berechnet, die auch im sicherheitsbezogenen Blockdiagramm gezeigt wird. Die Funktion „Schnellhalt“ des FU und die Möglichkeit der Abschaltung der Spannungsversorgung des FU über Q1 werden bei der Berechnung der Ausfallwahrscheinlichkeit der Sicherheitsfunktion nicht berücksichtigt.
- Der Frequenzumrichter T1 wird in die Blöcke T1a und T1b zerlegt. Im Block T1a sind die Funktionen Start und Stopp sowie deren steuerungstechnische Umsetzung enthalten. Der Block T1b beinhaltet die mit einer geringen Anzahl von Bauteilen realisierte Impulssperre.

Sicheres Stillsetzen ausgelöst durch das Not-Halt-Gerät S4:

- Für das Not-Halt-Gerät wird ein Fehlerausschluss angenommen, da die in Tabelle D.2 genannte Betätigungsanzahl nicht überschritten wird.
- $MTTF_d$: Folgende $MTTF_d$-Werte werden geschätzt: 50 Jahre für K4, 100 Jahre für T1a und 1 000 Jahre für T1b [G]. Für K1 ergibt sich bei einem B_{10d}-Wert von 400 000 Zyklen [N] und bei 240 Arbeitstagen, 8 Arbeitsstunden und 6 Minuten Zykluszeit eine n_{op} = 19 200 Zyklen/Jahr und eine $MTTF_d$ von 208 Jahren. Für K2 ergibt sich bei einem B_{10d}-Wert von 400 000 Zyklen [N] und täglichem Einschalten an 240 Arbeitstagen eine $MTTF_d$ von 16 667 Jahren. Der Kondensator C1 geht mit $MTTF_d$ = 45 662 Jahre [D] in die Berechnung ein. Diese Werte ergeben eine symmetrisierte $MTTF_d$ pro Kanal von 72 Jahren („hoch“).

- DC_{avg}: Fehlererkennung durch den Prozess führt auf *DC* = 30 % für K4, auf *DC* = 90 % für T1a und auf *DC* = 60 % für T1b. *DC* = 99 % für K1 und *DC* = 60 % für C1 folgen durch Testung des Zeitglieds bei spannungsfreiem FU. Für K2 gilt *DC* = 99 % durch Plausibilitätstest in K4 mit dem Schaltzustand von S4. Die Mittelungsformel für DC_{avg} ergibt 56,9 % (im Toleranzbereich von „niedrig“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (85 Punkte): Trennung (15), Diversität (20), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (72 Jahre) und niedrigem DC_{avg} (57 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}76 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Sicheres Stillsetzen ausgelöst durch die BWS K3:

- Die BWS K3 liegt als geprüftes Sicherheitsbauteil vor. Ihre Ausfallwahrscheinlichkeit beträgt $3{,}0 \cdot 10^{-8}$/Stunde [H] und wird am Ende der Berechnung addiert.

- Für die zweikanalige Struktur „SPS/Elektromechanik“ wird die Ausfallwahrscheinlichkeit mit den gleichen $MTTF_d$- und DC-Werten wie oben beschrieben berechnet. Das Bauteil K2 ist an der Ausführung dieser Sicherheitsfunktion jedoch nicht beteiligt. Es ergeben sich folgende Werte: $MTTF_d$ eines Kanals = 72 Jahre („hoch“) und DC_{avg} = 56,8 % (im Toleranzbereich von „niedrig“). Für Kategorie 3 ergibt dies eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}77 \cdot 10^{-7}$/Stunde. Die Gesamtausfallwahrscheinlichkeit wird durch Addition ermittelt und ergibt $2{,}07 \cdot 10^{-7}$/Stunde. Dies entspricht ebenfalls PL d.

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 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (01.05). Beuth, Berlin 2005

- DIN CLC/TS 61496-2: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 2: Besondere Anforderungen an Einrichtungen, welche nach dem aktiven opto-elektronischen Prinzip arbeiten (02.08). Beuth, Berlin 2008

- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07). International Electrotechnical Commission (IEC), Genf 2007

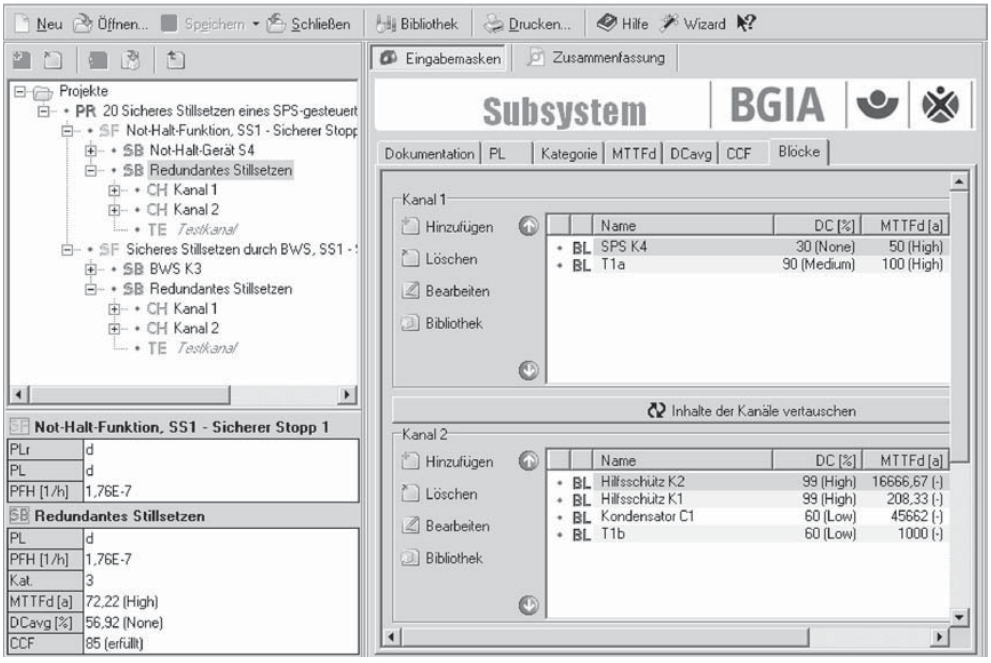


Abbildung 8.35: PL-Bestimmung mithilfe von SISTEMA