8 Schaltungsbeispiele für SRP/CS

In diesem Report wurde zunächst allgemein auf die Gestaltung sicherer Steuerungen eingegangen. Die Abschnitte 5.7, 6.5 und 7.6 illustrierten anschließend am Beispiel einer Planschneidemaschine, wie die Methoden zur Gestaltung sicherer Steuerungen umgesetzt werden können. Die Methoden zur Bestimmung des PL sind hier bzw. in DIN EN ISO 13849-1 zwar Schritt für Schritt beschrieben, einige dieser Schritte, z.B. die Ableitung des sicherheitsbezogenen Blockdiagramms aus dem Schaltplan, erfordern jedoch einige Übung. Sie lassen sich aufgrund der Vielfalt möglicher Sicherheitsfunktionen und ihrer Realisierung auch nur schwer allgemein beschreiben. Daher wird nun in diesem Kapitel die Bewertung einer Vielzahl von Schaltungsbeispielen vorgestellt, die Sicherheitsfunktionen in verschiedenen Kategorien bzw. Performance Leveln und in verschiedenen Technologien realisieren. Mit dem Begriff Steuerung sind in den Schaltungsbeispielen im Allgemeinen nur die sicherheitsbezogenen Teile von Steuerungen erfasst. Die Beispiele beschränken sich auf wesentliche Gesichtspunkte und dienen deshalb nur als Anregung für eine Realisierung. Bei deren Auswahl wurde auf ein breites Spektrum von Technologien und möglichen Anwendungen Wert gelegt. Leser des Reports zu den Kategorien für sicherheitsbezogene Steuerungen nach EN 954-1 aus dem Jahre 1997 [40] werden das eine oder andere Beispiel angereichert u.a. um die Berechnung der Ausfallwahrscheinlichkeit wiedererkennen. Die Beispiele sind eine Interpretation der Kategorien und wurden von den Autoren aufgrund langjähriger Erfahrungen mit sicherheitsbezogenen Maschinensteuerungen und Mitwirkung in nationalen und europäischen Normungsgremien zusammengestellt, um dem Konstrukteur eine wirksame Hilfestellung für eigene Entwicklungen zu geben. Da sie von verschiedenen Autoren erstellt wurden, ist naturgemäß eine Varianz, z.B. in Darstellung von Details oder in der Begründung einzelner Zahlenwerte, vorhanden. Alle „Berechnungen“ für die Schaltungsbeispiele wurden mithilfe der Software SISTEMA (siehe Anhang H) in der zum Zeitpunkt der Erstellung dieses Reportes verfügbaren Version 1.0 ausgeführt.

Die Beschreibung in den Beispielen gliedert sich jeweils nach folgendem Schema:

- Sicherheitsfunktion
- Funktionsbeschreibung
- konstruktive Merkmale
- Bemerkungen
- Berechnung der Ausfallwahrscheinlichkeit
- weiterführende Literatur

Unter „Sicherheitsfunktion“ werden neben der Bezeichnung der Sicherheitsfunktion auch die auslösenden Ereignisse und notwendigen Sicherheitsreaktionen genannt.

Unter „Funktionsbeschreibung“ werden aufbauend auf einem Prinzipschaltplan die wesentlichen sicherheitstechnischen Funktionen beschrieben. Das Verhalten im Fehlerfall wird erläutert und Maßnahmen zur Fehlererkennung werden erwähnt.

Unter „Konstruktive Merkmale“ sind die Besonderheiten im Entwurf des jeweiligen Beispieles, so auch die Anwendung bewährter Sicherheitsprinzipien oder die Verwendung bewährter Bauteile, aufgelistet.

Die Schaltbilder sind Prinzipschaltbilder, die sich ausschließlich darauf beschränken, die Sicherheitsfunktion(en) mit den hierzu notwendigen relevanten Komponenten zu zeigen. Nicht dargestellt werden zwecks besserer Übersicht solche schaltungstechnischen Maßnahmen, die in der Regel immer zusätzlich realisiert sein müssen, um z.B. den Berührungsschutz sicherzustellen, Über- und Unterspannungen bzw. Überdruck/Unterdruck zu beherrschen, Isolationsfehler, Erd- und Kurzschlüsse z.B. auf extern verlegten Leitungen aufzudecken oder die erforderliche Störfestigkeit gegen elektromagnetische Einwirkungen zu garantieren. Für die Bestimmung des sicherheitsbezogenen Blockdiagramms unwesentliche Schaltungsdetails wurden somit bewusst weggelassen. Dazu gehören in der Elektrik Schutzbeschaltungen wie Sicherungen und Dioden, z.B. als Freilaufdioden. Ebenfalls nicht aufgeführt sind Entkopplungsdioden in Schaltungen, in denen Sensorsignale z.B. redundant in mehrere Logikeinheiten eingelesen werden. Diese sollen verhindern, dass bei Redundanz im Fehlerfall ein Eingang zu einem Ausgang wird und damit den zweiten Kanal beeinflusst. Um eine Steuerung nach einer Kategorie und einem Performance Level zu realisieren, sind alle diese genannten Bauelemente unerlässlich. In den technologiebezogenen Bemerkungen zur Fluidtechnik sind weitere Beispiele aufgeführt. Selbstverständlich muss gemäß den Fehlerlisten aus DIN EN ISO 13849-2 z.B. auch der Einfluss von Leitungskurzschlüssen im Zusammenhang mit der jeweiligen Sicherheitsfunktion und abhängig von den Einsatzbedingungen berücksichtigt werden. So müssen grundsätzlich alle verwendeten Bauteile entsprechend ihrer Spezifikation geeignet ausgewählt sein, Überdimensionierung gehört zu den bewährten Sicherheitsprinzipien.

Es werden nur diejenigen konstruktiven Merkmale genannt, die für die beschriebenen Sicherheitsfunktionen wichtig sind. Meist ist dies eine „sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung“. Andere Sicherheitsfunktionen wie z.B. die „Verhinderung des unerwarteten Anlaufs“ oder eine „manuelle Rückstellungsfunktion“ sowie eine „Start-/Wiederaufnahmefunktion“ sind nicht durchgängig in allen Beispielen betrachtet. Werden manuell betätigte Einrichtungen (Taster) für die Realisierung solcher Sicherheitsfunktionen verwendet, so ist darauf zu achten, dass die Sicherheitsfunktionen gerade im

Zusammenspiel mit Elektronik durch das Loslassen (Öffnen) eines vorher betätigten Tasters realisiert werden.

Unter „Bemerkungen“, soweit für das jeweilige Beispiel vorhanden, wird insbesondere auf Besonderheiten im Hinblick auf eine mögliche Anwendung verwiesen.

Unter „Berechnung der Ausfallwahrscheinlichkeit“ wird, basierend auf dem aus dem Prinzipschaltplan abgeleiteten sicherheitsbezogenen Blockdiagramm, die rechnerische Bestimmung des PL durch die Parameter Kategorie, $MTTF_d$, DC_{avg} und CCF gezeigt. Die Festlegung der Kategorie leitet sich aus der Funktionsbeschreibung und den konstruktiven Merkmalen ab.

Die in den Berechnungen verwendeten $MTTF_d$-Werte sind als Herstellerwerte (Kennzeichnung „[H]“ für **H**ersteller), typische Werte aus Datenbanken (Kennzeichnung „[D]“ für **D**atenbank) oder als Werte aus der Norm DIN EN ISO 13849-1 ((Kennzeichnung „[N]“ für **N**orm) markiert. Die Norm sieht eine Priorisierung von Herstellerdaten vor. Für einige Komponenten, z.B. Drehgeber oder Frequenzumrichter, waren zum Zeitpunkt der Erstellung des Reports weder verlässliche Herstellerangaben noch Datenbankwerte zu erhalten. Hier wurden Hersteller gezielt angesprochen oder das „Parts Count“-Verfahren zu Hilfe genommen, um typische Beispielwerte abzuschätzen (Kennzeichnung „[G]“ für **g**eschätzt). Die $MTTF_d$-Werte in diesem Kapitel sind daher teilweise eher als Schätzwerte zu betrachten.

Die Darstellung der angenommenen Maßnahmen zur Diagnose (*DC*) und gegen Ausfälle infolge gemeinsamer Ursache (CCF) beschränkt sich auf allgemein gehaltene Angaben. Konkrete Werte hängen für beide Kriterien von Realisierung, Anwendung oder auch vom Hersteller ab. Es kann daher vorkommen, dass für ähnliche Komponenten in verschiedenen Beispielen unterschiedliche DC-Werte angenommen werden. Auch hier gilt, dass bei einer realen Umsetzung alle Annahmen hinsichtlich *DC* und CCF überprüft werden müssen und die angenommenen Werte nur unverbindlichen Beispielcharakter haben.

Der Schwerpunkt in der Darstellung liegt eher auf den Kategorien in Form der „Widerstandsfähigkeit gegen Fehler“ und den „rechnerischen“ Methoden zur Bestimmung des PL. Einige Teilschritte, z.B. Fehlerauschlüsse, grundlegende und bewährte Sicherheitsprinzipien oder Maßnahmen gegen systematische Fehler (inklusive Software), sind dagegen nur in kurzer Form erwähnt. Hierauf muss bei einer Realisierung entsprechendes Augenmerk gerichtet werden, da Fehleinschätzungen oder unzureichende Umsetzungen bei diesen Maßnahmen die Fehlertoleranz oder Ausfallwahrscheinlichkeit verschlechtern können. Als Hilfe zum Verständnis der Schaltungsbeispiele und für die praktische Umsetzung sei daher auf Kapitel 7 und Anhang C verwiesen, in denen z.B. die grundlegenden und bewährten Sicherheitsprinzipien ausführlich beschrieben sind.

Abschließend wird, soweit vorhanden, auf „Weiterführende Literatur“ verwiesen.

Für jede Technologie werden in den folgenden technologiebezogenen Abschnitten einige grundlegende Bemerkungen zum Verständnis der Beispiele und zur Umsetzung der Kategorien gegeben. Einige der Schaltungsbeispiele stellen „Steuerungen verschiedener Technologie“ dar. Diese „gemischten“ Schaltungsbeispiele sind von der Idee getragen, dass eine Sicherheitsfunktion unabhängig von der Technologie nach dem Verständnis der Norm immer über „Erfassen“, „Verarbeiten“ und „Schalten“ erfolgt.

8.1 Grundlegende technologiebezogene Bemerkungen zu den Steuerungsbeispielen

8.1.1 Elektromechanische Steuerungen

In elektromechanischen Steuerungen werden in erster Linie elektromechanische Bauteile in Form von Schaltern bzw. Befehlsgeräten (z.B. Positionsschalter, Wahlschalter, Taster) und Schaltgeräten (Steuerschütze, Relais, Leistungsschütze) eingesetzt. Diese Geräte besitzen eindeutige Schaltstellungen. Ohne Betätigung von außen oder elektrische Ansteuerung ändern sie in der Regel ihren Schaltzustand nicht. Bei bestimmungsgemäßer Verwendung und entsprechender Auswahl sind sie weitgehend unempfindlich z.B. gegenüber elektrischen und elektromagnetischen Störeinflüssen. Das unterscheidet sie zum Teil erheblich von elektronischen Betriebsmitteln. Durch geeignete Auswahl, Dimensionierung und Anordnung kann auf die Haltbarkeit und das Ausfallverhalten Einfluss genommen werden. Das gilt auch für die verwendeten Leitungen bei entsprechender Verlegung innerhalb und außerhalb der elektrischen Einbauräume.

Aus vorstehenden Gründen entsprechen die elektromechanischen Bauteile in den meisten Fällen den „grundlegenden Sicherheitsprinzipien“ und sind auch in vielen Fällen als „sicherheitstechnisch bewährte Bauteile“ zu betrachten. Diese Aussage gilt jedoch nur, wenn die Anforderungen der DIN EN 60204-1 [20] für die elektrische Ausrüstung der Maschine/Anlage berücksichtigt werden. In einigen Fällen sind auch Fehlerausschlüsse möglich, z.B. bei einem Steuerschütz in Bezug auf das Anziehen bei fehlender Steuerspannung oder das Nichtöffnen eines zwangläufig betätigten Öffners bei einem Schalter nach DIN EN 60947-5-1 [38], Anhang K.

8.1.2 Fluidtechnische Steuerungen

Bei fluidtechnischen Anlagen ist als „sicherheitsbezogener Teil der Steuerung“ insbesondere der Ventilbereich zu betrachten, und zwar die Ventile, die gefahrbringende Bewegungen oder Zustände steuern. Auch die ausgeführten fluidischen Schaltungen sind nur beispielhafte Darstellungen. Die geforderten Sicherheitsfunktionen können in der Regel auch durch andere Steuerungsverknüpfungen mit entsprechenden Ventilausführungen oder evtl. auch durch zusätzliche mechanische Lösungen wie z.B. Halteeinrichtungen oder Bremsen erreicht werden.

Bei **hydraulischen** Anlagen (siehe Abbildung 8.1) sind zusätzlich die Maßnahmen zur Druckbegrenzung im System (1V2) und zur Filtration der Druckflüssigkeit (1Z2) in diesem Zusammenhang zu sehen. Die Bauteile 1Z1, 1S1 und 1S2 in Abbildung 8.1 sind in den meisten hydraulischen Anlagen vorhanden und insbesondere für den Zustand der Druckflüssigkeit und damit für die Ventilfunktionen von großer Bedeutung. Das auf dem Flüssigkeitsbehälter angeordnete Belüftungsfilter 1Z1 verhindert, dass Schmutz von außen eindringt. Die Niveauanzeige 1S2 bewirkt die Einhaltung des Flüssigkeitsspiegels in vorgegebenen Grenzen. Die Temperaturanzeige 1S1 symbolisiert geeignete Maßnahmen zur Begrenzung des Betriebstemperaturbereiches und damit des Betriebsviskositätsbereiches der Druckflüssigkeit. Bei Bedarf müssen Einrichtungen zur Kühlung und/oder Heizung in Verbindung mit einer Temperaturregelung eingesetzt werden (siehe hierzu auch Anhang C).

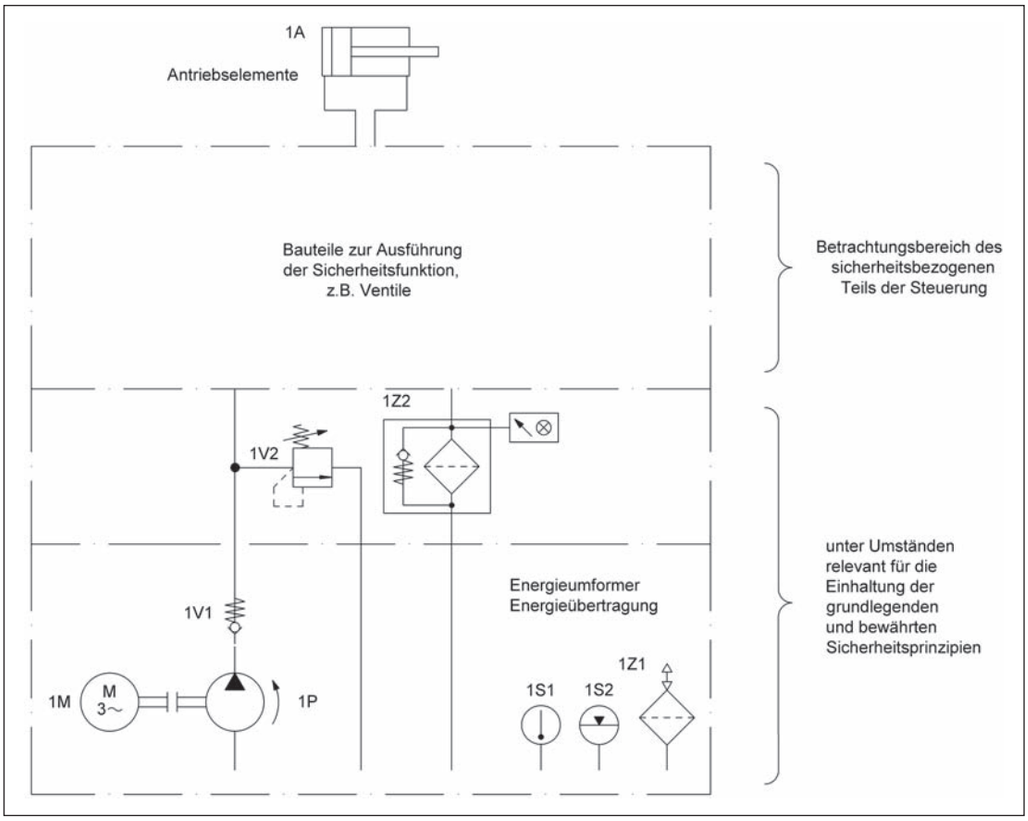


Abbildung 8.1: Anwendungsbereich der DIN EN ISO 13849 bei hydraulischen Anlagen

Die Antriebselemente sowie die Bauteile der Energieumformung und der Energieübertragung sind bei fluidtechnischen Anlagen in der Regel außerhalb des Anwendungsbereiches der Norm.

Bei **pneumatischen Anlagen** (siehe Abbildung 8.2 auf Seite 88) sind die Bauteile gegen Gefährdungen bei Energieänderungen und die sogenannte Wartungseinheit zur Aufbereitung der Druckluft in sicherheitstechnischem Zusammenhang mit dem Ventilbereich zu sehen. Um mögliche Energieänderungen sicherheitstechnisch zu beherrschen, wird häufig ein Entlüftungsventil zusammen mit einem Druckschalter eingesetzt. In den Schaltungsbeispielen dieses Kapitels sind diese Bauteile mit 0V1 (Entlüftungsventil) und mit 0S1 (Druckschalter) bezeichnet. Die Wartungseinheit 0Z (siehe Abbildung 8.2) besteht in der Regel aus einem Handabsperrventil 0V10, einem Filter mit Wasserabscheider 0Z10, wobei der Verschmutzungsgrad des Filters überwacht wird, und einem Druckregelventil 0V11 (mit ausreichend dimensionierter Sekundärentlüftung). Mit der Druckanzeige 0Z11 wird die Anforderung an die Überwachung der Anlagenparameter erfüllt.

Die in diesem Kapitel beispielhaft gezeigten fluidtechnischen Schaltungen enthalten außer dem sicherheitsbezogenen Steuerungsteil nur noch die zusätzlichen Bauteile, die zum Verständnis der fluidtechnischen Anlage notwendig sind oder einen direkten steuerungstechnischen Bezug haben. Die Gesamtheit der Anforderungen, die von fluidtechnischen Anlagen erfüllt werden müssen, ist aus [41; 42] zu entnehmen. Als weitere zutreffende Normen sind [43 bis 47] zu nennen.

Die meisten Steuerungsbeispiele sind elektrohydraulische bzw. elektropneumatische Steuerungen. Verschiedene Sicherheitsanforderungen werden bei diesen Steuerungen durch den elektrischen Steuerungsteil ausgeführt, so z.B. die Anforderungen zur Beherrschung von Energieänderungen in elektrohydraulischen Steuerungen.

Die geforderte Sicherheitsfunktion ist bei den hier aufgeführten Steuerungsbeispielen das Anhalten einer gefahrbringenden Bewegung oder die Umkehrung der Bewegungsrichtung. Die Verhinderung eines unerwarteten Anlaufs ist implizit enthalten. Die geforderte Sicherheitsfunktion kann aber auch z.B. ein definiertes Druckniveau oder ein Druckabbau sein.

Die Strukturen von fluidtechnischen Steuerungen werden in den meisten Fällen in den Kategorien 1, 3 oder 4 ausgeführt. Da die Kategorie B bereits die Einhaltung der zutreffenden Normen und der grundlegenden Sicherheitsprinzipien erfordert, unterscheiden sich fluidtechnische Steuerungen der Kategorien B und 1 im Wesentlichen nicht durch den Steuerungsaufbau, sondern nur durch die höhere sicherheitsbezogene Zuverlässigkeit der relevanten Ventile. Aus diesem Grund werden in diesem Report keine fluidtechnischen Steuerungen der Kategorie B vorgestellt.

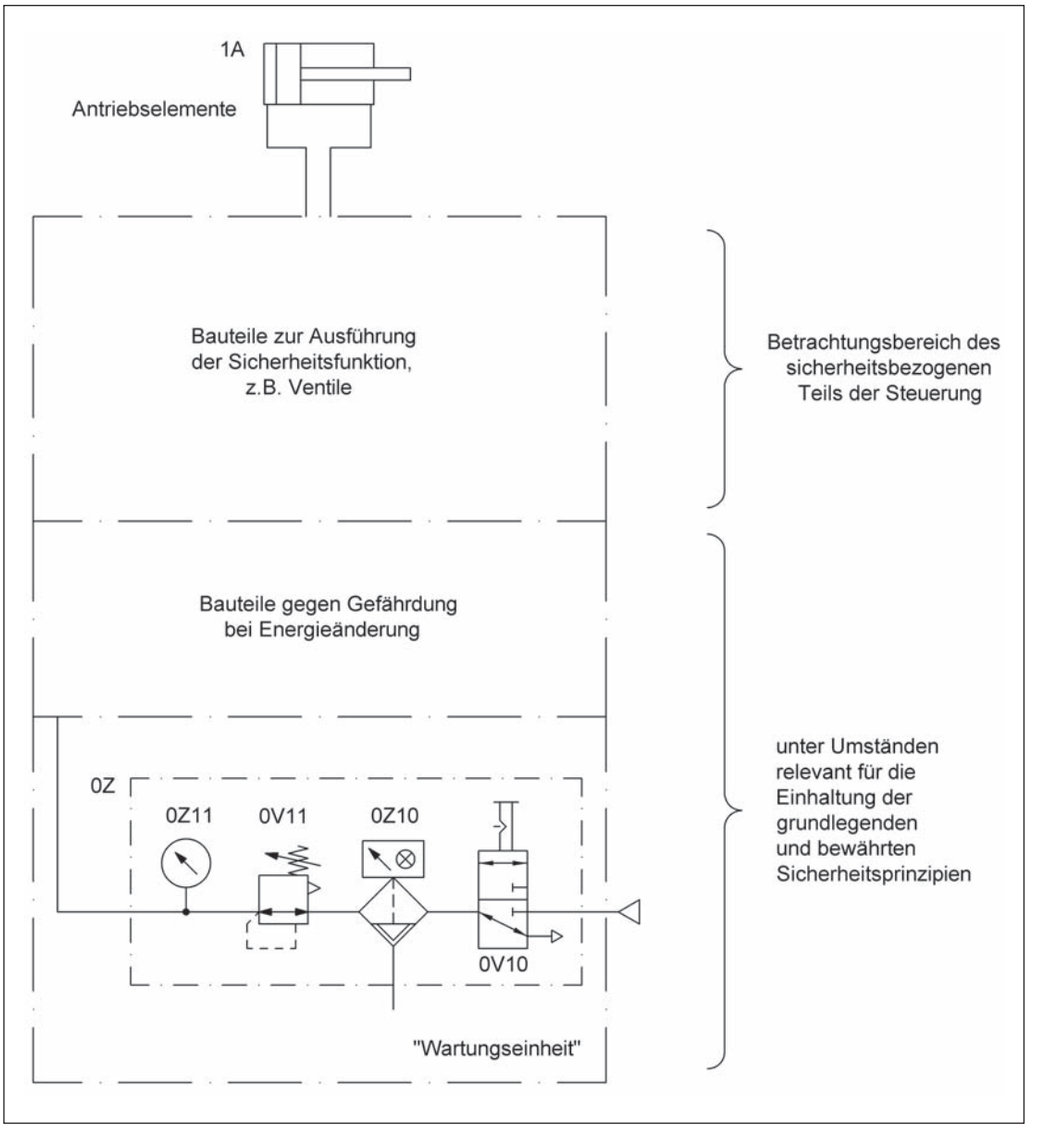


Abbildung 8.2: Anwendungsbereich der DIN EN ISO 13849 bei pneumatischen Anlagen

8.1.3 Elektronische und programmierbar elektronische Steuerungen

In der Regel sind elektronische Bauteile gegenüber äußeren Umgebungseinflüssen empfindlicher als elektromechanische Komponenten. Werden keine besonderen Maßnahmen ergriffen, können elektronische Bauelemente bei Temperaturen < 0 °C deutlich eingeschränkter eingesetzt werden als elektromechanische Bauelemente. Zusätzlich gibt es Umgebungseinflüsse, die beim Einsatz elektromechanischer Schaltelemente fast bedeutungslos, aber in Elektroniksystemen ein zentrales Problem sind: alle elektromagnetischen Störeinflüsse, die über Leitungen oder über elektromagnetische Felder in Elektroniksysteme eingekoppelt werden. Teilweise ist ein erhöhter Aufwand erforderlich, um eine für die Praxis ausreichende Störfestigkeit zu erzielen. Fehlerausschlüsse sind bei elektronischen Bauelementen kaum möglich. Dies hat zur Folge, dass grundsätzlich nicht die Konstruktion eines bestimmten Bauelementes die Sicherheit gewährleisten kann, sondern nur bestimmte Schaltungskonzepte sowie die Anwendung entsprechender Maßnahmen zur Fehlerbeherrschung.

Nach den Fehlerlisten zu elektrischen/elektronischen Komponenten und Bauteilen nach DIN EN ISO 13849-2 werden im Wesentlichen die Fehlerannahmen Kurzschluss, Unterbrechung, Veränderung eines Parameter- oder Kennwertes und sogenannte Stuck-at-Fehler unterstellt. Dies sind durchweg Fehlereffekte, die als bleibend angenommen werden. Transiente (sporadisch auftretende) Fehler wie z.B. sogenannte Soft Errors, bei denen durch hochenergetische Teilchen wie z.B. α-Teilchen eine Kondensatorumladung innerhalb eines Chips erfolgt, sind in der Regel nur schwer zu entdecken und hauptsächlich durch strukturelle Maßnahmen zu beherrschen.

Das Ausfallverhalten elektronischer Bauelemente ist häufig schwierig zu bewerten, in der Regel kann auch keine vorwiegende Ausfallart festgelegt werden. Dies soll an einem Beispiel erläutert werden: Wird ein Schütz elektrisch nicht angesteuert, d.h. wird seine Spule nicht vom Strom durchflossen, gibt es keinen Grund dafür, dass sich die Kontakte des Schützes schließen. Das bedeutet, dass ein ausgeschaltetes Relais oder Schütz sich durch einen internen Fehler nicht selbsttätig einschaltet. Anders ist das bei den meisten elektronischen Bauteilen, z.B. einem Transistor. Ist ein Transistor gesperrt, d.h., es fließt kein ausreichend hoher Basisstrom, so ist es trotzdem nicht ausgeschlossen, dass der Transistor durch einen internen Fehler plötzlich ohne

äußere Einwirkung leitfähig wird und somit unter Umständen eine gefahrbringende Bewegung einleitet. Auch dieser sicherheitstechnische Nachteil elektronischer Bauelemente muss durch ein entsprechendes Schaltungskonzept beherrscht werden. Insbesondere beim Einsatz hoch integrierter Bausteine ist es teilweise nicht mehr möglich, selbst zu Beginn der Gebrauchsdauer, d.h. zum Zeitpunkt der Inbetriebnahme, nachzuweisen, dass ein Gerät oder eine Anlage völlig fehlerfrei ist. Schon auf Bauelementebene ist ein Nachweis der Fehlerfreiheit durch die Hersteller mit 100-prozentiger Testabdeckung für komplexe integrierte Schaltkreise nicht mehr durchführbar. Ähnliches gilt für die Software programmierbarer Elektronik.

Im Gegensatz zu elektromechanischen Schaltungen haben rein elektronische Schaltungen oft den Vorteil, dass sich Zustände dynamisieren lassen. Hierdurch kann der erforderliche *DC* auch in entsprechend kurzen Zeitabständen und ohne Zustandsänderung externer Signale erreicht werden (Dynamisierung).

Zur Verhinderung von Ausfällen infolge gemeinsamer Ursache sind zwischen verschiedenen Kanälen Entkopplungsmaßnahmen erforderlich. Diese bestehen in der Regel aus galvanisch getrennten Kontakten, Widerstands- oder Diodennetzwerken, Filterschaltungen, Optokopplern und Übertragern.

Systematische Ausfälle können zum gleichzeitigen Versagen redundanter Verarbeitungskanäle führen, wenn dies nicht durch frühzeitige Berücksichtigung, insbesondere während der Entwurfs- und Integrationsphase, verhindert ist. Durch Anwendung von Prinzipien, z.B. Ruhestrom, Diversität oder Überdimensionierung, können auch elektronische Schaltungen so robust gestaltet werden, dass ein systematischer Ausfall ausreichend sicher verhindert ist. Nicht zu vernachlässigen sind Maßnahmen, die die Verarbeitungskanäle unempfindlich gegen physikalische Einflüsse machen, wie sie z.B. in einer Industrieumgebung anzutreffen sind (Temperatur, Feuchte, Staub, Vibration, Schock, korrosive Atmosphäre, elektromagnetische Beeinflussung, Spannungsausfall, Über- und Unterspannung usw.).

SRP/CS der Kategorie 1 müssen unter Verwendung bewährter Bauteile und bewährter Sicherheitsprinzipien gestaltet und gebaut werden. Da komplexe elektronische Bauteile, z.B. SPS, Mikroprozessor oder ASICs, nicht als bewährt im Sinne der Norm betrachtet werden, gibt es in diesem Report auch keine entsprechenden Beispiele von Elektronik in Kategorie 1.

Für programmierbare Elektronik wird in den Schaltungsbeispielen jeweils eine Aussage darüber getroffen, mit welcher Wirksamkeit, d.h. mit welchem Performance Level, Maßnahmen zur Fehlervermeidung bzw. Fehlerbeherrschung erforderlich sind. Weitere Ausführungen siehe Abschnitt 6.3. Werden im Rahmen einer Entwicklung ASICs eingesetzt, so sind im Entwicklungsprozess fehlervermeidende Maßnahmen erforderlich. Solche enthält zum Beispiel der Normentwurf DIN IEC 61508-2:2006 [39], der für die Entwicklung eines ASICs ein V-Modell in Anlehnung an das aus der Softwareentwicklung bekannte V-Modell vorsieht.

Erwähnenswert, weil entsprechende Fragen in der Praxis auftreten, sind folgende Punkte:

- Zwei Kanäle eines SRP/CS dürfen im Allgemeinen nicht über denselben integrierten Schaltkreis geführt werden. In Bezug auf Optokoppler bedeutet diese Anforderung z.B. die Verwendung von Optokopplern in verschiedenen Gehäusen, wenn Signale unterschiedlicher Kanäle verarbeitet werden sollen.

- Für den Einsatz programmierbarer Elektronik ist auch der Einfluss von Betriebssystemen u.Ä. zu berücksichtigen. Ein Standard-PC mit einem marktüblichen Betriebssystem eignet sich nicht für den Einsatz in einer sicherheitsrelevanten Steuerung. Die erforderliche Fehlerfreiheit (realistisch besser: Fehlerarmut) eines Betriebssystems, das nicht für sicherheitstechnische Anwendungen entwickelt wurde, wird sich in der Regel nicht mit vertretbarem Aufwand nachweisen lassen bzw. wird nicht erreichbar sein.

8.2 Schaltungsbeispiele

Tabelle 8.1 zeigt eine Übersicht der Schaltungsbeispiele 1 bis 37. Tabelle 8.2 (siehe Seite 90) nennt alphabetisch sortiert die wichtigsten in den Schaltungsbeispielen verwendeten Abkürzungen.

Tabelle 8.1:
Übersicht der Schaltungsbeispiele

Erreichter PL	Realisierte Kategorie	Technologie/Beispiel Nr.		
		Pneumatik	Hydraulik	Elektrotechnik
b	B			1
c	1	2	3	4, 5, 6, 7, 8
c	2			9
c	3			10, 24
d	2	11	12	13
d	3	14	15, 16	15, 16, 17, 18, 19, 20, 21, 22, 23, 24
e	3	25, 26	27	29, 30
e	4	31	32, 33	28, 33, 34, 35, 36, 37

Tabelle 8.2:
Übersicht der in den Schaltungsbeispielen verwendeten Abkürzungen

Abkürzung	Bedeutung
[D]	B_{10d}- oder $MTTF_d$-Werte aus Datenbanken (siehe z.B. Anhang D, Abschnitt D2.6)
[G]	Geschätzte B_{10d}- oder $MTTF_d$-Werte
[H]	B_{10d}- oder $MTTF_d$-Werte auf der Basis von Herstellerangaben
[N]	B_{10d}- oder $MTTF_d$-Werte auf der Basis von gelisteten Angaben in der Norm DIN EN ISO 13849-1 (siehe z.B. Tabelle D.2 dieses Reports)
µC	Mikrocontroller
B_{10}	Nominale Lebensdauer, die mittlere Zahl von Schaltspielen bzw. Schaltzyklen, nach der bis zu 10 % der betrachteten Einheiten ausgefallen sind
B_{10d}	Nominale Lebensdauer, die mittlere Zahl von Schaltspielen bzw. Schaltzyklen, nach der bis zu 10 % der betrachteten Einheiten gefährlich ausgefallen sind
BKK	Brems-/Kupplungskombination
BWS	Berührungslos wirkende Schutzeinrichtung
CCF	Ausfall infolge gemeinsamer Ursache (Common Cause Failure)
CPU	Mikroprozessor (Central Processing Unit)
DC	Diagnosedeckungsgrad (Diagnostic Coverage)
DC_{avg}	Durchschnittlicher Diagnosedeckungsgrad (average Diagnostic Coverage)
FIT	Ausfälle in 10^9 Bauteilstunden (Failures In Time)
FMEA	Ausfalleffektanalyse (Failure Mode and Effects Analysis)
FU	Frequenzumrichter
M	Motor
MFST	Multifunktionsstellteil
$MTTF_d$	Mittlere Zeit bis zum gefahrbringenden Ausfall (Mean Time to Dangerous Failure)
n_{op}	Mittlere Anzahl jährlicher Betätigungen (Number of Operations)
PFH	Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (Probability of a Dangerous Failure per Hour)
PL	Performance Level
PL_r	Erforderlicher Performance Level (Required PL)
RAM	Arbeitsspeicher, variabler Speicher (Random Access Memory)
ROM	Festwertspeicher, invariabler Speicher (Read-Only Memory)
SLS	Sicher begrenzte Geschwindigkeit (Safely-Limited Speed, siehe Tabelle 5.2)
SPS	Speicherprogrammierbare Steuerung
SRASW	Sicherheitsbezogene Anwender-Software (Safety-Related Application Software)
SRESW	Sicherheitsbezogene eingebettete Software (Safety-Related Embedded Software)
SRP/CS	Sicherheitsbezogener Teil einer Steuerung
SS1	Sicherer Stopp 1 (Safe Stop 1, siehe Tabelle 5.2)
SS2	Sicherer Stopp 2 (Safe Stop 2, siehe Tabelle 5.2)
STO	Sicher abgeschaltetes Moment (Safe Torque Off, siehe Tabelle 5.2)
T_{10d}	Mittlere Zeit, nach der bis zu 10 % der betrachteten Einheiten gefährlich ausgefallen sind
ZHS	Zweihandschaltung

8.2.1 Stellungsüberwachung beweglicher trennender Schutzeinrichtungen mittels Näherungsschalter – Kategorie B – PL b (Beispiel 1)

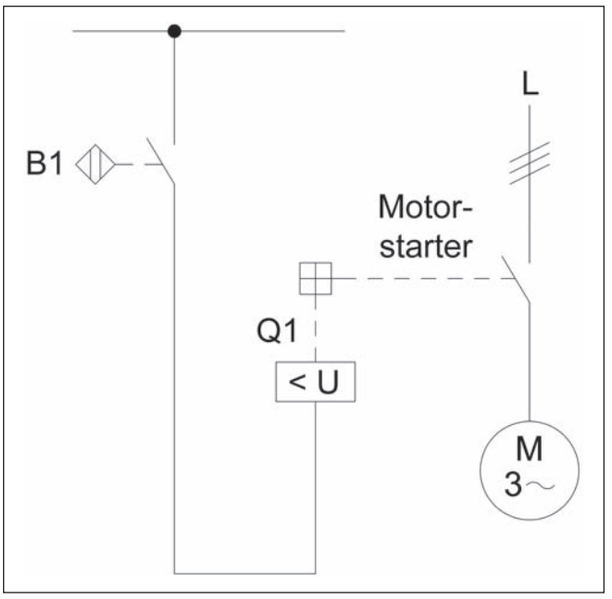


Abbildung 8.3:
Stellungsüberwachung beweglicher trennender Schutzeinrichtungen mittels Näherungsschalter

Sicherheitsfunktion

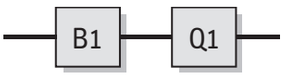
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Die Betätigung des Näherungsschalters beim Öffnen der beweglichen trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Das Öffnen der beweglichen trennenden Schutzeinrichtung (z.B. Schutzgitter) wird durch einen Näherungsschalter B1 erfasst, der auf die Unterspannungsauslösung eines Motorstarters Q1 wirkt. Durch das Abfallen von Q1 werden gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Ein Entfernen der Schutzeinrichtung wird bemerkt.
- B1 enthält keine internen Überwachungsmaßnahmen. Es sind keine weiteren Maßnahmen zur Fehlererkennung vorgesehen.

Konstruktive Merkmale

- Grundlegende Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z.B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen. Als grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip des Unterspannungsauslösers verwendet.
- Ein stabiler Aufbau der Schutzeinrichtung (Schutzgitter) zur Betätigung des Näherungsschalters ist sichergestellt.
- Die sichere Funktion kann je nach Ausführung des Näherungsschalters durch Umgehen auf eine vernünftigerweise vorhersehbare Art aufgehoben werden. Dies kann erschwert werden, z.B. durch besondere Einbaubedingungen wie verdeckter Einbau (siehe auch DIN EN 1088/A1 Anhang J).
- Die Spannungsversorgung der gesamten Maschine wird abgeschaltet (Stopp-Kategorie 0 nach DIN EN 60204-1).



Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Bei B1 handelt es sich um einen herkömmlichen Näherungsschalter an einem Schutzgitter mit $MTTF_d$ = 40 Jahren [H]. Für die Unterspannungsauslösung des Motorstarters Q1 entspricht der B_{10}-Wert näherungsweise der elektrischen Lebensdauer von 10 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10d}-Wert durch Verdoppelung des B10-Wertes. Bei täglicher Betätigung des Näherungsschalters ergibt sich mit n_{op} = 365 Zyklen/Jahr für Q1 eine $MTTF_d$ von 548 Jahren. Die Kombination von B1 und Q1 ergibt $MTTF_d$ = 37 Jahre für den Kanal. Dieser Wert wird auf den rechnerischen Maximalwert für Kategorie B, also auf 27 Jahre („mittel“) gekürzt.

- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie B nicht relevant.

- Die elektromechanische Steuerung entspricht Kategorie B mit mittlerer $MTTF_d$ (27 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}23 \cdot 10^{-6}$/Stunde. Dies entspricht PL b.

Weiterführende Literatur

- DIN EN 1088/A1: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl (07.07). Beuth, Berlin 2007

- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

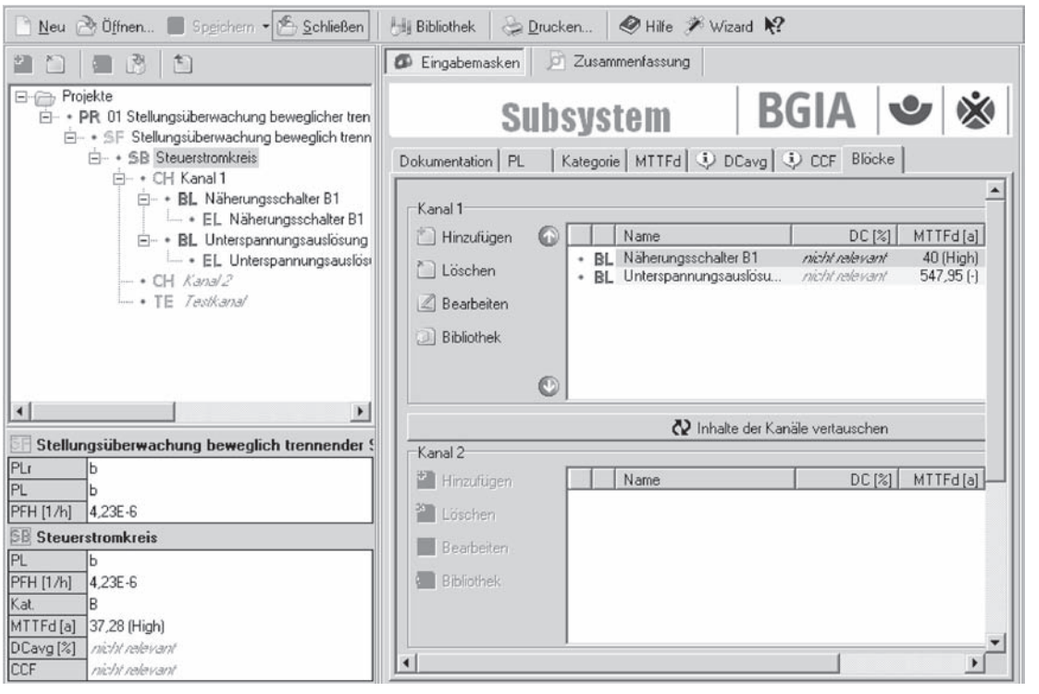


Abbildung 8.4: PL-Bestimmung mithilfe von SISTEMA

8.2.2 Pneumatisches Ventil (Subsystem) – Kategorie 1 – PL c (für PL-b-Sicherheitsfunktionen) (Beispiel 2)

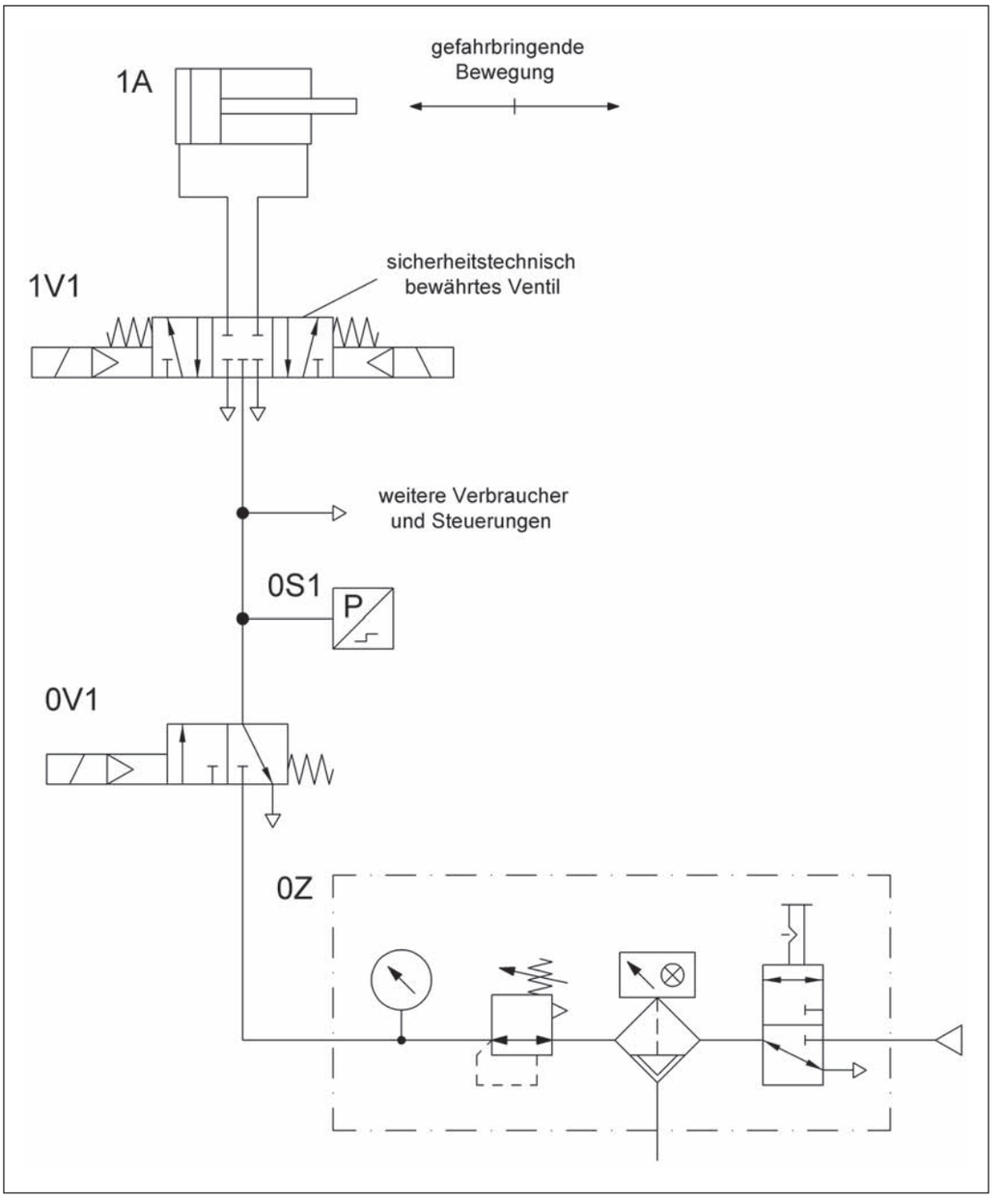


Abbildung 8.5: Pneumatisches Ventil zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch ein sicherheitstechnisch bewährtes Wegeventil 1V1 gesteuert.
- Der Ausfall des Wegeventils kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.
- Wenn durch eingesperrte Druckluft eine weitere Gefährdung auftreten kann, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V1 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung, Federzentrierung und dauerfesten Federn.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Bestätigung für das Wegeventil als sicherheitstechnisch bewährtes Bauteil (ausreichend hohe Zuverlässigkeit) erfolgt bei Bedarf durch den Hersteller/Anwender.
- Die Sicherheitsfunktion kann auch durch eine Verknüpfung von entsprechenden Ventilen erreicht werden.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für das Wegeventil 1V1 wird ein B_{10d}-Wert von 40 000 000 Schaltspielen [G] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 5 Sekunden Zykluszeit ist n_{op}=2 764 800 Zyklen/Jahr und $MTTF_d$ = 145 Jahre. Dies ist gleichzeitig der $MTTF_d$-Wert pro Kanal, der auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die pneumatische Steuerung entspricht Kategorie 1 mit hoher $MTTF_d$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für das verschleißbehaftete Wegeventil 1V1 ein Wert von 14 Jahren (T_{10d}) Betriebszeit bis zum vorgesehenen Austausch.

8.2.3 Hydraulisches Ventil (Subsystem) – Kategorie 1 – PL c (für PL-b-Sicherheitsfunktionen) (Beispiel 3)

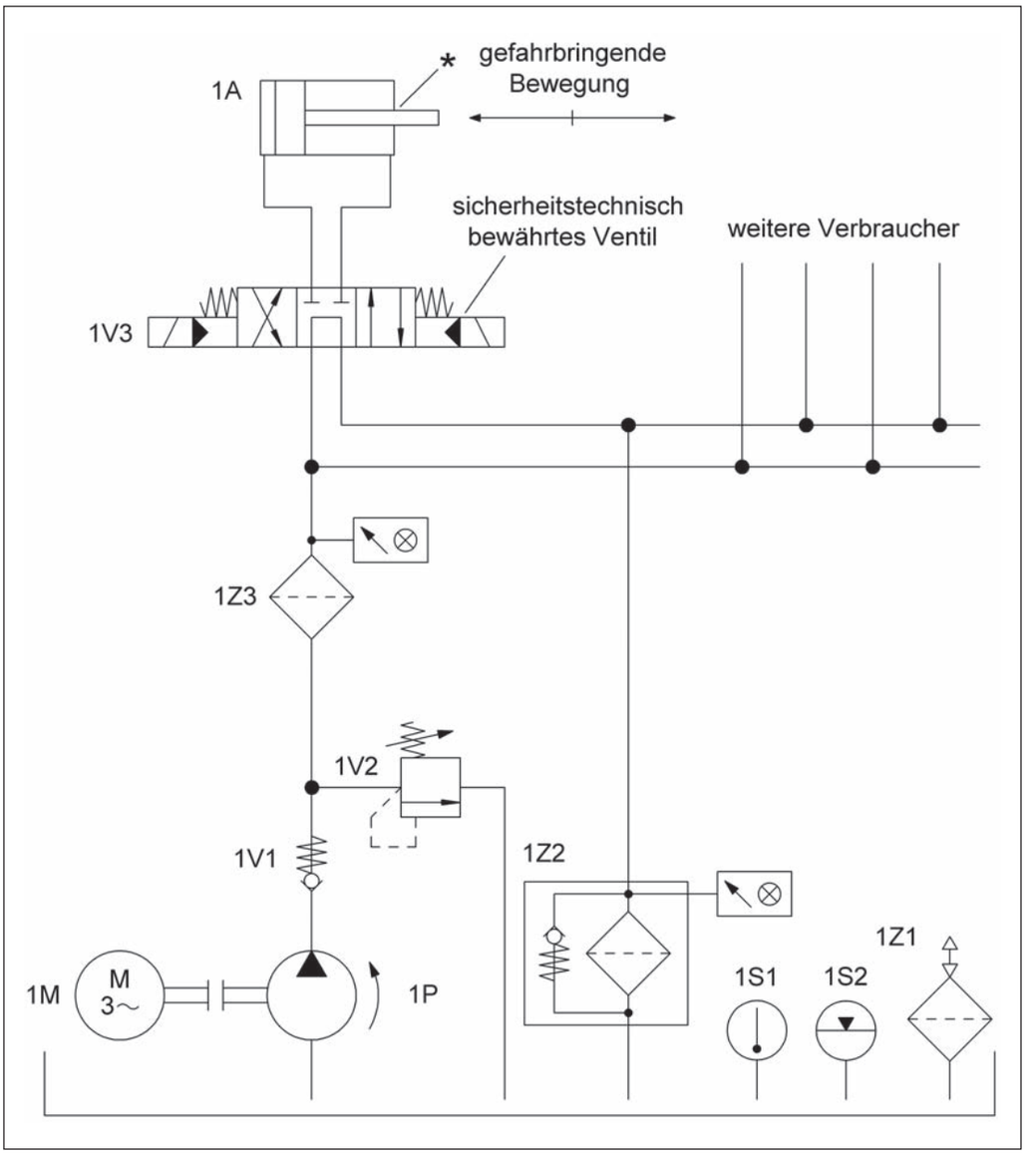


Abbildung 8.6: Hydraulisches Ventil zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- Hier ist nur der hydraulische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch ein sicherheitstechnisch bewährtes Wegeventil 1V3 gesteuert.
- Der Ausfall des Wegeventils kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V3 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung, Federzentrierung und dauerfesten Federn.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Bestätigung für das Wegeventil als sicherheitstechnisch bewährtes Bauteil erfolgt bei Bedarf durch den Hersteller/Anwender.
- Als gezielte Maßnahmen zur Erhöhung der Zuverlässigkeit des Wegeventils sind ein Druckfilter 1Z3 vor dem Wegeventil und geeignete Maßnahmen gegen Schmutzeinzug durch die Kolbenstange am Zylinder (z.B. wirksamer Abstreifer an der Kolbenstange, siehe * in Abbildung 8.6) vorgesehen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für das Wegeventil 1V3 wird eine $MTTF_d$ von 150 Jahren angenommen [N]. Dies ist gleichzeitig der $MTTF_d$-Wert pro Kanal, der auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die hydraulische Steuerung entspricht Kategorie 1 mit hoher $MTTF_d$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.

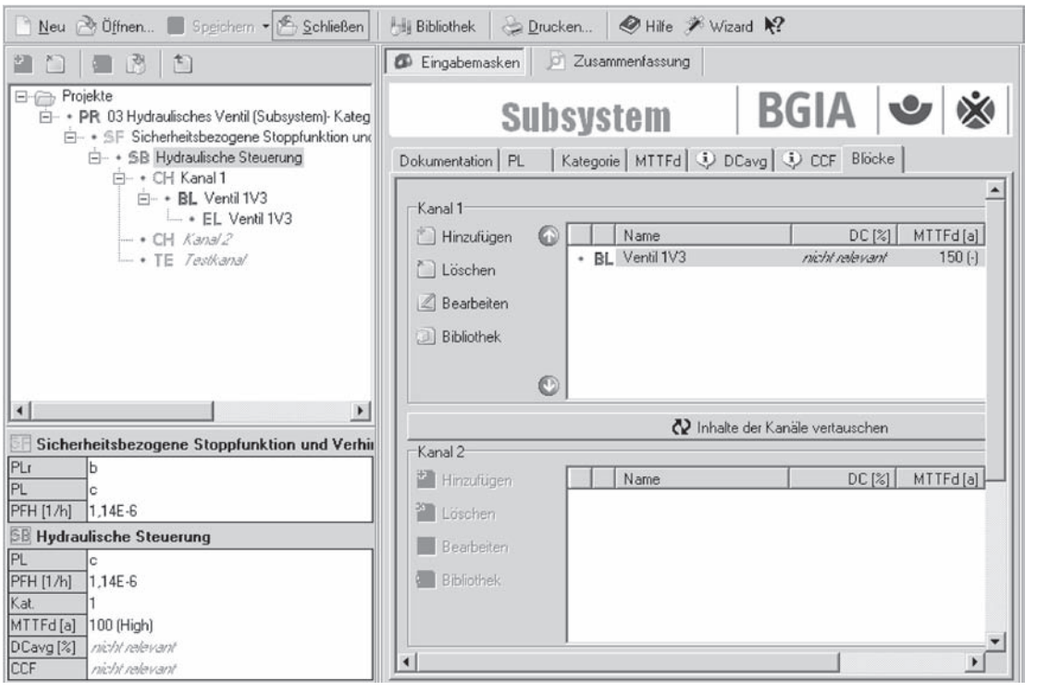


Abbildung 8.7: PL-Bestimmung mithilfe von SISTEMA

8.2.4 Stillsetzen von Holzbearbeitungsmaschinen – Kategorie 1 – PL c (Beispiel 4)

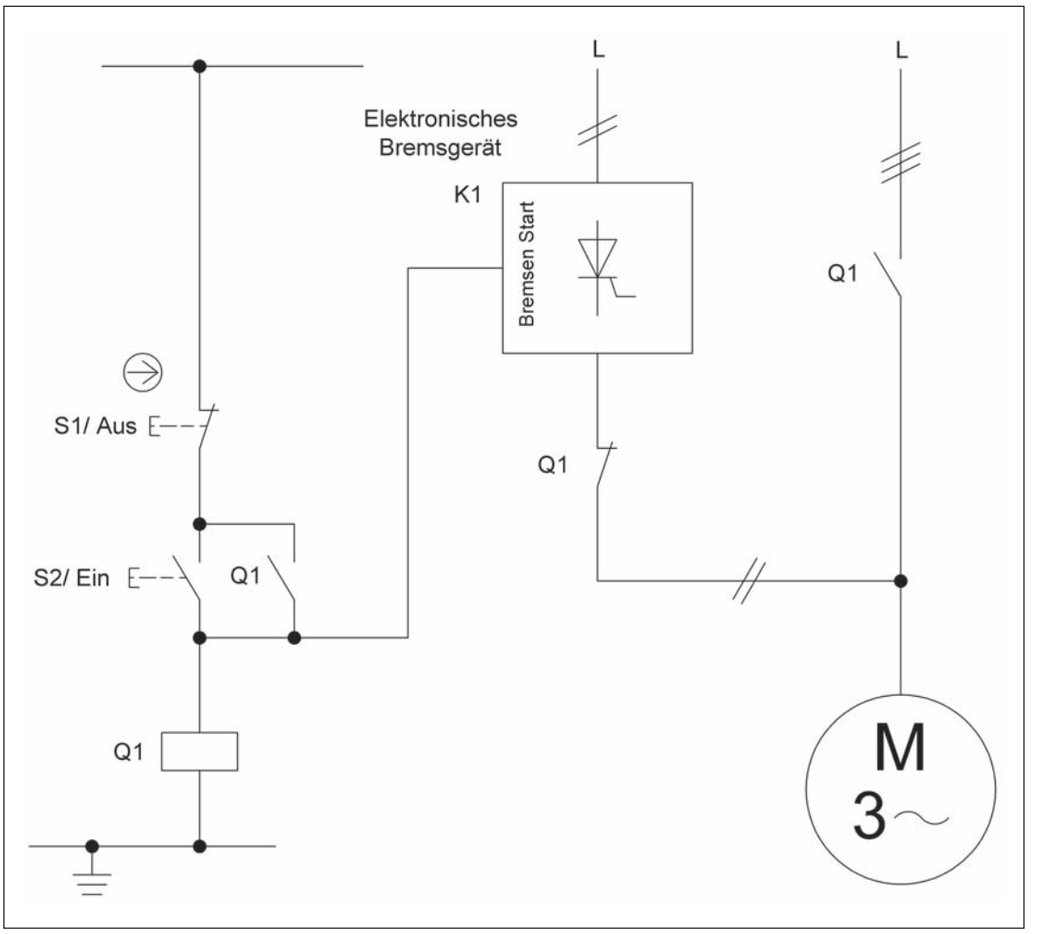


Abbildung 8.8: Kombination von elektromechanischer Befehlseinrichtung und einfachem elektronischen Bremsgerät zum Stillsetzen von Holzbearbeitungs-maschinen

Sicherheitsfunktion

- Die Betätigung des Aus-Tasters führt zu SS1 – Sicherer Stopp 1, einem gesteuerten Stillsetzen des Motors innerhalb einer maximal zulässigen Zeit.

Funktionsbeschreibung

- Mit Betätigen des Aus-Tasters S1 wird das Stillsetzen des Motors eingeleitet. Das Motorschütz Q1 fällt ab und die Bremsfunktion wird gestartet. Die Bremsung des Motors erfolgt durch einen Gleichstrom, der im Bremsgerät K1 durch eine Phasenanschnittsteuerung mit Thyristor erzeugt wird und in der Motorwicklung ein Bremsmoment erzeugt.
- Die Stillsetzzeit darf einen maximalen Wert (z.B. 10 Sekunden) nicht überschreiten. Die hierfür erforderliche Höhe des Bremsstroms kann über ein Potenziometer am Bremsgerät eingestellt werden.
- Nach Ablauf der maximalen Bremszeit wird der Thyristor nicht mehr angesteuert und der Strompfad für den Bremsstrom ist unterbrochen. Der Stillsetzvorgang entspricht einem Stopp der Kategorie 1 gemäß DIN EN 60204-1.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

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. Als grundlegendes Sicherheitsprinzip wird das Prinzip der Energietrennung (Ruhestromprinzip) angewandt. Zum Schutz gegen unerwarteten Wiederanlauf nach Wiederherstellung der Energieversorgung ist die Steuerung mit einer Selbsthaltung versehen.

- Bei S1 handelt es sich um einen Tastschalter mit zwangläufigem Betätigungsmodus gemäß DIN EN 60947-5-1, Anhang K (Zwangsöffnung). S1 wird daher als bewährtes Bauteil angesehen.

- Das Schütz Q1 ist ein bewährtes Bauteil unter Berücksichtigung der zusätzlichen Bedingungen nach Tabelle D.4 der DIN EN 13849-2.

- Das Bremsgerät K1 ist ausschließlich unter Verwendung einfacher elektronischer Bauelemente wie z.B. Transistoren, Kondensatoren, Dioden, Widerstände, Thyristoren aufgebaut, die als bewährte Bauteile angesehen werden. Die fehlerfreie Durchführung der sicherheitsrelevanten Bremsfunktion wird durch die Auswahl der Bauteile charakterisiert. Interne Maßnahmen zur Fehlererkennung sind nicht vorgesehen. Es kommen keine komplexen elektronischen Bauteile (z.B. Mikroprozessoren) zum Einsatz, die gemäß DIN EN ISO 13849-1, Abschnitt 6.2.4, nicht als gleichwertig zu bewährt betrachtet werden.

Anwendung

- Bei Holzbearbeitungsmaschinen oder ähnlichen Maschinen, bei denen das ungebremste Stillsetzen zu einem unzulässig langen Auslaufen der gefahrbringenden Werkzeugbewegungen führen würde. Die Steuerung muss so ausgeführt sein, dass mindestens PL b erreicht wird (Prüfgrundsätze Holzbearbeitungsmaschinen GS-HO-01).

Berechnung der Ausfallwahrscheinlichkeit

- Bei S1 handelt es sich um einen Tastschalter mit zwangläufigem Betätigungsmodus gemäß DIN EN 60947-5-1, Anhang K (Zwangsöffnung). Beim Einsatz eines solchen Tasters als Befehlsgerät kann ein Fehlerausschluss für das Nichtöffnen des elektrischen Kontakts inklusive der Mechanik innerhalb des Tasters erfolgen.

- $MTTF_d$: Für das Schütz Q1 wird bei nominaler Last ein B_{10d}-Wert von 2 000 000 Schaltspielen [N] angenommen. Bei 300 Arbeitstagen, 8 Arbeitsstunden und 2 Minuten Zykluszeit ist n_{op} = 72 000 Zyklen/Jahr und $MTTF_d$ = 277 Jahre. Die $MTTF_d$ für das Bremsgerät K1 wurde über die „Parts Count"-Methode ermittelt. Mit den Bauteilinformationen aus der Stückliste und den Werten aus der Datenbank SN 29500 [36] ergibt sich eine $MTTF_d$ = 518 Jahre [D]. Die Kombination von Q1 und K1 ergibt $MTTF_d$ = 180 Jahre für den Kanal, die auf 100 Jahre („hoch") gekürzt wird.

- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.

- Die elektromechanische Steuerung entspricht Kategorie 1 mit hoher $MTTF_d$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Damit ist der PL_r = b übertroffen.

Weiterführende Literatur

- Grundsätze für die Prüfung und Zertifizierung von Holzbearbeitungsmaschinen GS-HO-01. Ausg. 12/2007 www.dguv.de/bgia, Webcode d14898

8.2.5 Stellungsüberwachung beweglicher trennender Schutzeinrichtungen – Kategorie 1 – PL c (Beispiel 5)

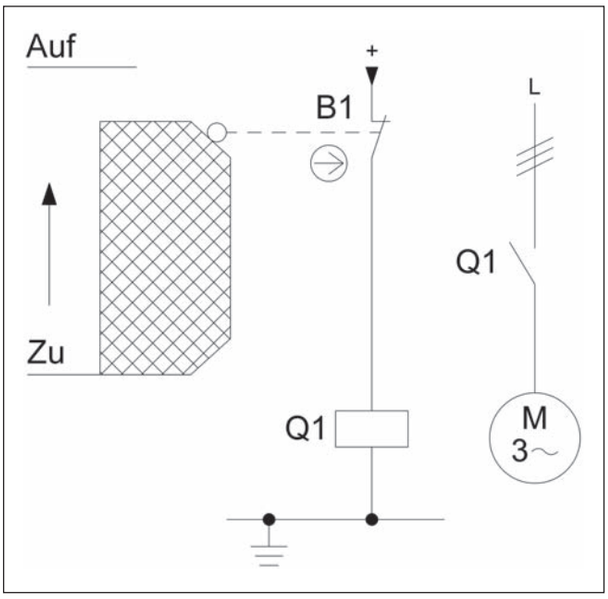


Abbildung 8.9:
Stellungsüberwachung beweglicher trennender Schutzeinrichtungen zur Verhinderung von gefahrbringenden Bewegungen (STO – Sicher abgeschaltetes Moment)

Sicherheitsfunktion

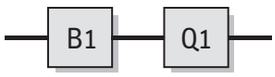
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der beweglichen trennenden Schutzeinrichtung leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Das Öffnen der beweglichen trennenden Schutzeinrichtung (z.B. Schutzgitter) wird durch einen Positionsschalter B1 mit zwangsöffnendem Kontakt erfasst, der ein Schütz Q1 ansteuert. Durch das Abfallen von Q1 werden gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.
- Ein Entfernen der Schutzeinrichtung wird nicht bemerkt.

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. Als grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip verwendet. Die Erdung des Steuerkreises ist als bewährtes Sicherheitsprinzip zu betrachten.
- Der Schalter B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K, und wird daher als bewährtes Bauteil angesehen. Der Öffnerkontakt unterbricht den Stromkreis mechanisch zwangläufig, wenn die Schutzeinrichtung sich nicht in Schutzstellung befindet.
- Das Schütz Q1 ist ein bewährtes Bauteil unter Berücksichtigung der zusätzlichen Bedingungen nach Tabelle D.4 der DIN EN 13849-2.
- Die Stellungsüberwachung erfolgt durch einen Positionsschalter. Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt. Die Betätigungselemente des Positionsschalters sind gegen Lageveränderung gesichert. Es werden nur starre mechanische Teile (keine Federelemente in Wirkrichtung der Betätigungskraft) verwendet.
- Der Betätigungshub für den Positionsschalter erfolgt nach Herstellerangabe.



Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für B1 kann ein Fehlerausschluss für den zwangsöffnenden elektrischen Kontakt erfolgen. Für den mechanischen Teil von 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 $MTTF_d$ = 285 Jahre. Für das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 300 000 Schaltspiele [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10d}-Wert durch Verdoppelung des B_{10}-Wertes. Mit dem oben angenommenen Wert für n_{op} ergibt sich für Q1 eine $MTTF_d$ von 742 Jahren. Die Kombination von B1 und Q1 ergibt für den Kanal eine $MTTF_d$ = 206 Jahre, die auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die elektromechanische Steuerung entspricht Kategorie 1 mit hoher $MTTF_d$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Damit ist der PL_r = b übertroffen.

Weiterführende Literatur

- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005

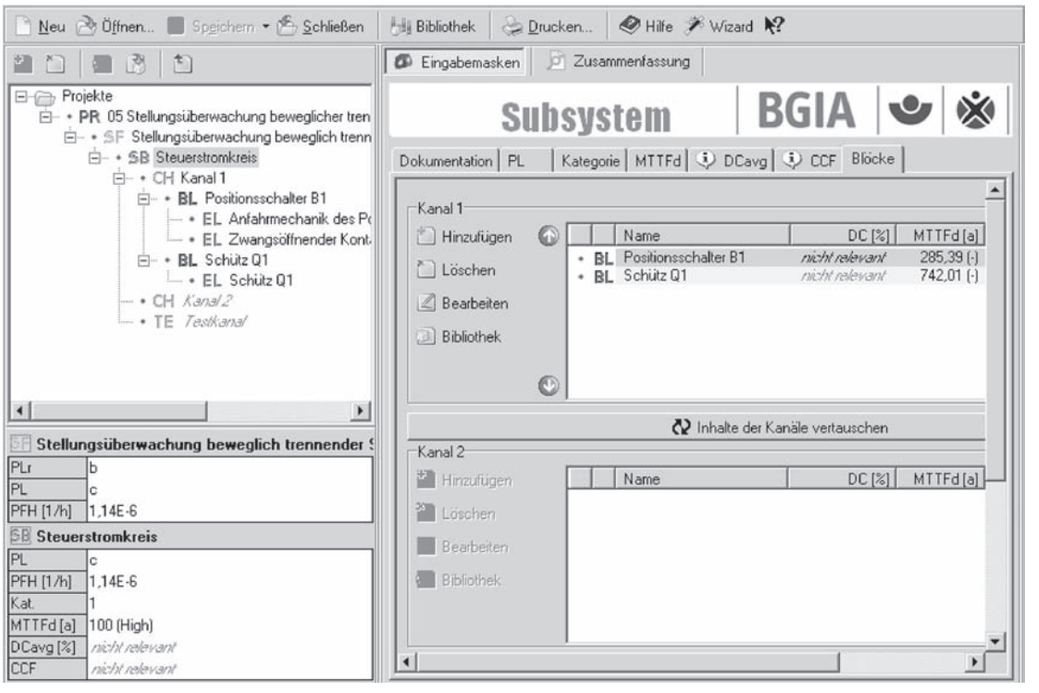


Abbildung 8.10.: PL-Bestimmung mithilfe von SISTEMA

8.2.6 Start-Stopp-Einrichtung mit Not-Halt-Gerät – Kategorie 1 – PL c (Beispiel 6)

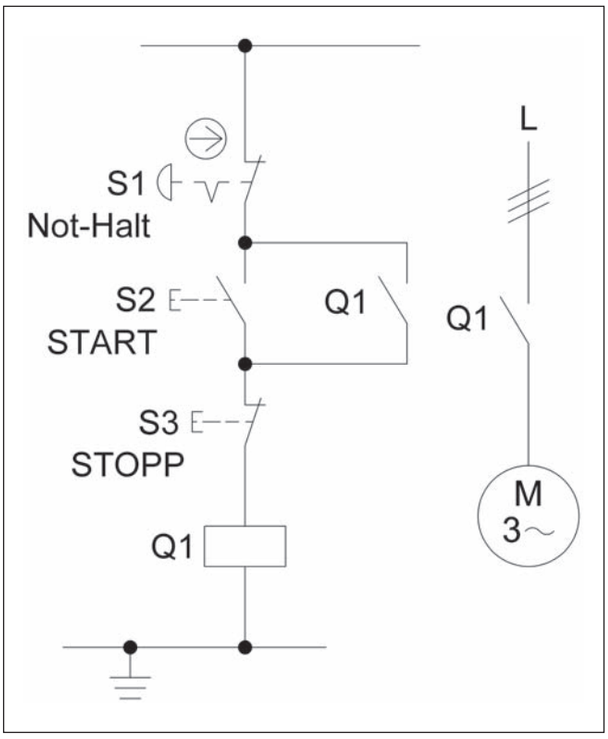


Abbildung 8.11:
Kombinierte Start-Stopp-Einrichtung mit Not-Halt-Gerät

Sicherheitsfunktion

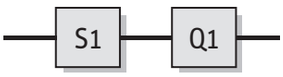
- Not-Halt-Funktion, STO – Sicher abgeschaltetes Moment durch Betätigung des Not-Halt-Gerätes

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden bei Betätigung des Not-Halt-Gerätes S1 durch Unterbrechung der Steuerspannung von Schütz Q1 abgeschaltet.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

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. Als grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip verwendet. Zusätzlich ist die Erdung des Steuerkreises als bewährtes Sicherheitsprinzip vorhanden.
- Das Not-Halt-Gerät S1 ist ein Schalter mit zwangläufigem Betätigungsmodus entsprechend EN 60947-5-1, Anhang K, und daher ein bewährtes Bauteil nach Tabelle D.4 der DIN EN ISO 13849-2.
- Die Signalverarbeitung erfolgt durch ein Schütz (Stopp-Kategorie 0 nach DIN EN 60204-1).
- Das Schütz Q1 ist ein bewährtes Bauteil unter Berücksichtigung der zusätzlichen Bedingungen nach Tabelle D.4 der DIN EN ISO 13849-2.



Bemerkung

- Die Funktion zum Stillsetzen im Notfall ergänzt als Schutzmaßnahme die Sicherheitsfunktionen zur Sicherung von Gefahrstellen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: 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 das Schütz Q1 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 300 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10d}-Wert durch Verdoppelung des B_{10}-Wertes. Werden an 365 Arbeitstagen täglich zwei Betätigungen der Start-Stopp-Einrichtung und jährlich drei Betätigungen des Not-Halt-Geräts angenommen, so ergibt sich mit n_{op} = 733 Zyklen/Jahr für Q1 eine $MTTF_d$ von 35 470 Jahren. Dies ist gleichzeitig die $MTTF_d$ für den Kanal, die auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die elektromechanische Steuerung entspricht Kategorie 1 mit hoher $MTTF_d$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Weiterführende Literatur

- DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze (03.07). Beuth, Berlin 2007
- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

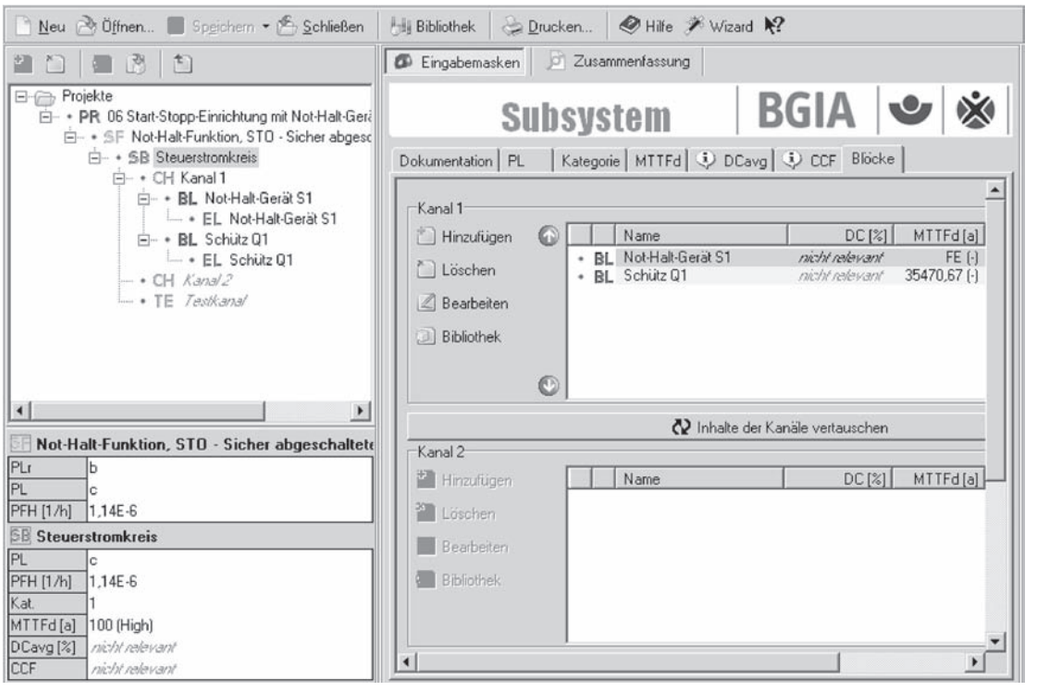


Abbildung 8.12: PL-Bestimmung mithilfe von SISTEMA

8.2.7 Unterspannungsauslösung über Not-Halt-Gerät – Kategorie 1 – PL c (Beispiel 7)

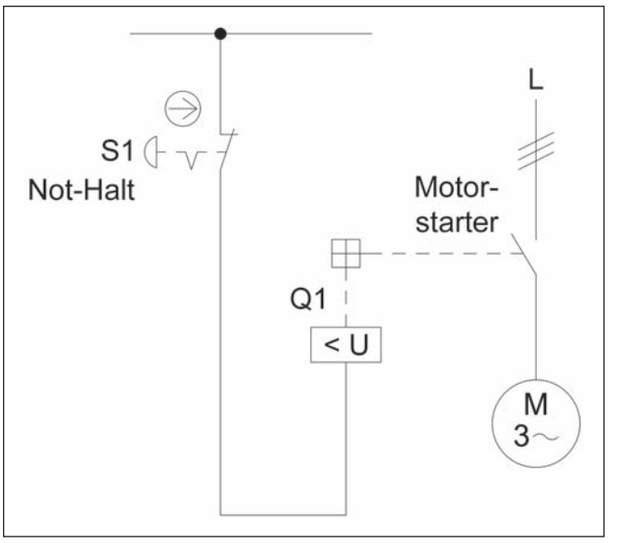


Abbildung 8.13:
Not-Halt-Gerät auf Unterspannungsauslösung der Netztrenneinrichtung (Motorstarter) wirkend

Sicherheitsfunktion

- Not-Halt-Funktion, STO – Sicher abgeschaltetes Moment durch Betätigung des Not-Halt-Gerätes, das auf die Unterspannungsauslösung eines Motorstarters, ggf. der Netztrenneinrichtung, wirkt.

Funktionsbeschreibung

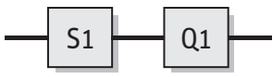
- Gefahrbringende Bewegungen oder Zustände werden bei Betätigung des Not-Halt-Gerätes S1 durch Unterspannungsauslösung der Netztrenneinrichtung – hier in Form eines Motorstarters Q1 – unterbrochen.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Es sind keine Maßnahmen zur Fehlererkennung vorgesehen.

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. Als grundlegendes Sicherheitsprinzip wird das Ruhestromprinzip des Unterspannungsauslösers verwendet.
- Das Not-Halt-Gerät S1 ist ein Schalter mit zwangläufigem Betätigungsmodus entsprechend EN 60947-5-1, Anhang K, und daher ein bewährtes Bauteil nach Tabelle D.4 der DIN EN ISO 13849-2.
- Der Motorstarter Q1 ist einem Leistungsschalter nach Tabelle D.4 der DIN EN ISO 13849-2 gleichzusetzen. Q1 kann daher als bewährtes Bauteil angesehen werden.
- Es wird die Spannungsversorgung der ganzen Maschine abgeschaltet (Stopp-Kategorie 0 nach DIN EN 60204-1).

Bemerkung

- Die Not-Halt-Funktion ergänzt als Schutzmaßnahme die Sicherheitsfunktionen zur Sicherung von Gefahrstellen.



Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: 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 die Unterspannungsauslösung des Motorstarters Q1 entspricht der B_{10}-Wert näherungsweise der elektrischen Lebensdauer von 10 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10d}-Wert durch Verdoppelung des B_{10}-Wertes. Bei jährlich drei Betätigungen des Not-Halt-Geräts ergibt sich mit n_{op} = 3 Zyklen/Jahr für Q1 eine $MTTF_d$ von 66 666 Jahren. Dies ist gleichzeitig die $MTTF_d$ für den Kanal, die auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.
- Die elektromechanische Steuerung entspricht Kategorie 1 mit hoher $MTTF_d$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

Weiterführende Literatur

- DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze (03.07). Beuth, Berlin 2007
- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

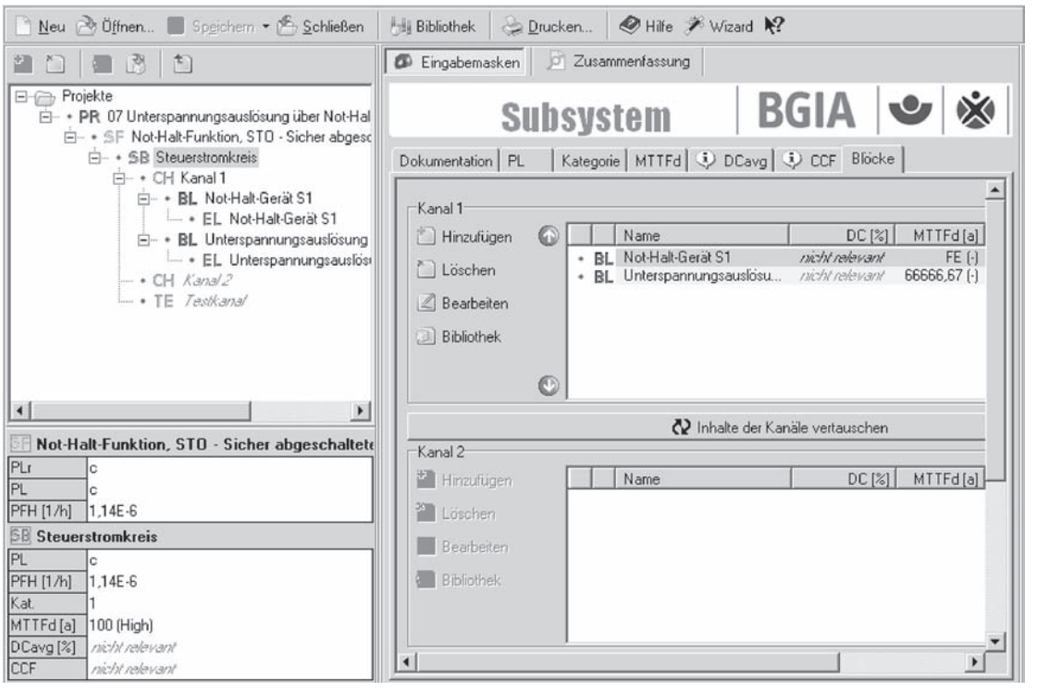


Abbildung 8.14: PL-Bestimmung mithilfe von SISTEMA

8.2.8 Stillsetzen von Holzbearbeitungsmaschinen – Kategorie 1 – PL c (Beispiel 8)

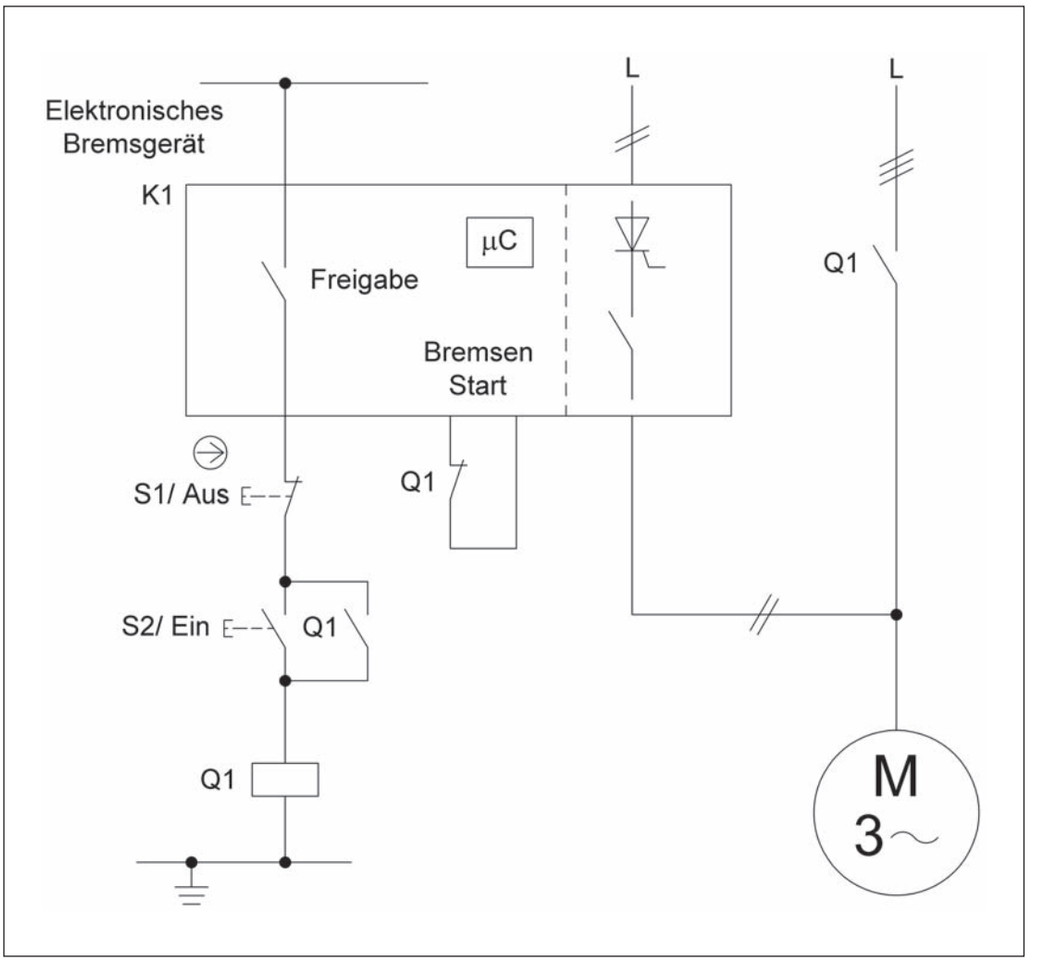


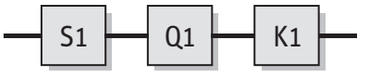
Abbildung 8.15: Kombination von elektromechanischer Befehlseinrichtung und programmierbar elektronischem Bremsgerät zum Stillsetzen von Holzbearbeitungsmaschinen

Sicherheitsfunktion

- Die Betätigung des Aus-Tasters führt zu SS1 – Sicherer Stopp 1, einem gesteuerten Stillsetzen des Motors innerhalb einer maximal zulässigen Zeit.

Funktionsbeschreibung

- Mit Betätigen des Aus-Tasters S1 wird das Stillsetzen des Motors eingeleitet. Das Motorschütz Q1 fällt ab und die Bremsfunktion wird gestartet. Die Bremsung des Motors erfolgt durch einen Gleichstrom, der im Bremsgerät K1 durch eine Phasenanschnittsteuerung mit Thyristoren erzeugt und über interne Relais auf die Motorwicklung geschaltet wird.
- Die Stillsetzzeit darf einen maximalen Wert, z.B. 10 Sekunden, nicht überschreiten. Die gewünschte Bremszeit und evtl. andere erforderliche Parameter (z.B. Bremsstrom, Schwelle für Stillstandserkennung) können am Bremsgerät eingestellt werden.
- Nach erfolgtem Stillstand bzw. nach Ablauf der maximalen Bremszeit schaltet das Bremsgerät den Bremsstrom ab und trennt den Motor wieder vom Netz. Der Stillsetzvorgang entspricht einem Stopp der Kategorie 1 gemäß DIN EN 60204-1.
- Die Sicherheitsfunktion lässt sich nicht bei allen Bauteilausfällen aufrechterhalten und hängt von der Zuverlässigkeit der Bauteile ab.
- Die fehlerfreie Durchführung der Bremsfunktion wird vom Bremsgerät K1 regelmäßig überwacht. Sollte ein Fehler festgestellt werden, z.B. eine Überschreitung der maximal zulässigen Bremszeit, wird über den Freigabekontakt im Gerät ein erneutes Starten des Motors verhindert. Maßnahmen zur Fehlererkennung in S1 oder Q1 sind nicht vorgesehen.



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. Als grundlegendes Sicherheitsprinzip wird das Prinzip der Energietrennung (Ruhestromprinzip) angewandt. Zum Schutz gegen unerwarteten Wiederanlauf nach Wiederherstellung der Energieversorgung ist die Steuerung mit einer Selbsthaltung versehen.

- Bei S1 handelt es sich um einen Tastschalter mit zwangläufigem Betätigungsmodus gemäß DIN EN 60947-5-1, Anhang K (Zwangsöffnung). S1 wird daher als bewährtes Bauteil angesehen.

- Das Schütz Q1 ist ein bewährtes Bauteil unter Berücksichtigung der zusätzlichen Bedingungen nach Tabelle D.4 der DIN EN ISO 13849-2.

- Das von einem Mikrocontroller gesteuerte Bremsgerät K1 erfüllt alle Anforderungen für Kategorie 2 und PL c. Die sicherheitsrelevanten Funktionen werden in regelmäßigen Abständen getestet. Der zeitliche Programmablauf des Mikrocontrollers wird durch einen separaten Watchdog überwacht.

Anwendung

- Bei Holzbearbeitungsmaschinen oder ähnlichen Maschinen, bei denen das ungebremste Stillsetzen zu einem unzulässig langen Auslaufen der gefahrbringenden Werkzeugbewegungen führen würde. Die Steuerung muss so ausgeführt sein, dass mindestens Performance Level b erreicht wird (Prüfgrundsätze Holzbearbeitungsmaschinen GS-HO-01).

Berechnung der Ausfallwahrscheinlichkeit

- Da das elektronische Bremsgerät K1 als handelsüblicher Baustein zum Einsatz kommt, wird dessen Ausfallwahrscheinlichkeit ($5{,}28 \cdot 10^{-7}$/Stunde [H]) am Ende der Berechnung mit SISTEMA addiert. Für den übrigen Steuerungsteil wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.

- Bei S1 handelt es sich um einen Tastschalter mit zwangläufigem Betätigungsmodus gemäß DIN EN 60947-5-1, Anhang K (Zwangsöffnung). Bei Einsatz eines solchen Tasters als Befehlsgerät kann ein Fehlerausschluss für das Nichtöffnen des elektrischen Kontakts inklusive der Mechanik innerhalb des Tasters erfolgen.

- $MTTF_d$: Für das Schütz Q1 wird bei nominaler Last ein B_{10d}-Wert von 2 000 000 Schaltspielen [N] angenommen. Bei 300 Arbeitstagen, 8 Arbeitsstunden und 2 Minuten Zykluszeit ist n_{op} = 72 000 Zyklen/Jahr und $MTTF_d$ = 277 Jahre. Dies ist gleichzeitig die $MTTF_d$ für den Kanal, die auf 100 Jahre („hoch“) gekürzt wird.

- DC_{avg} und Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache sind in Kategorie 1 nicht relevant.

- Die elektromechanische Steuerung, bestehend aus S1 und Q1, entspricht Kategorie 1 mit hoher $MTTF_d$ (100 Jahre). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $1{,}67 \cdot 10^{-6}$/Stunde. Dies entspricht PL c. Damit ist der PL_r = b übertroffen.

Weiterführende Literatur

- Grundsätze für die Prüfung und Zertifizierung von Holzbearbeitungsmaschinen GS-HO-01. Ausg. 12/2007 www.dguv.de/bgia, Webcode d14898

8.2.9 Getestete Lichtschranken – Kategorie 2 – PL c mit nachgeschaltetem Kategorie-1-Ausgangsschaltelement (Beispiel 9)

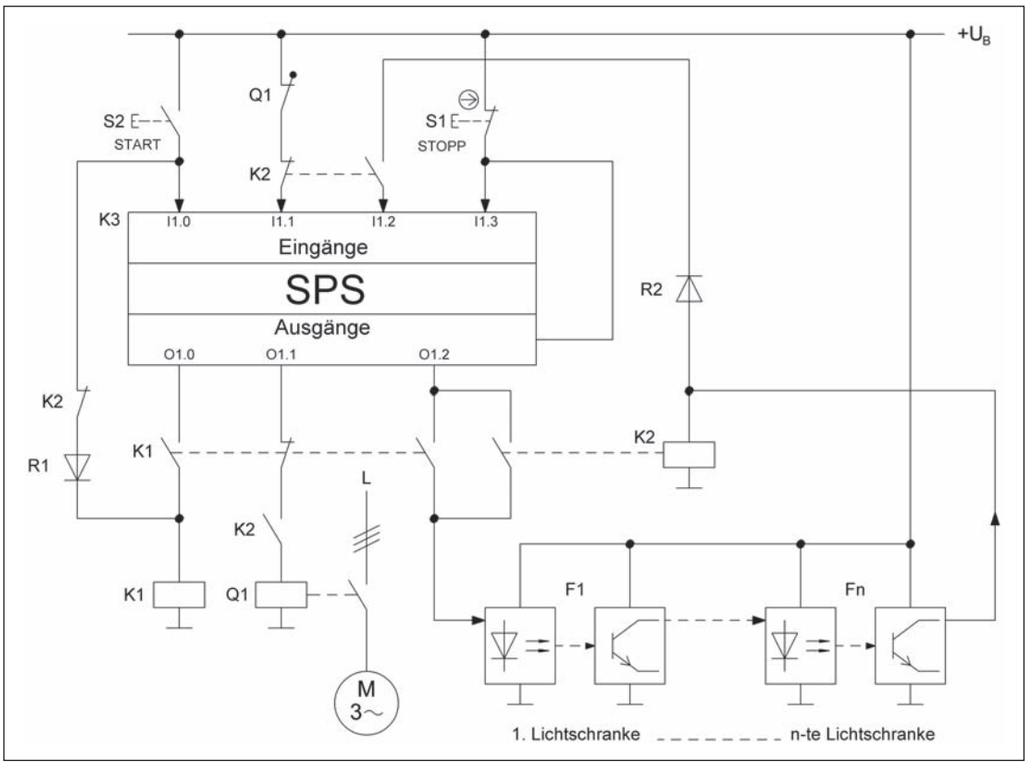


Abbildung 8.16: Testung von Lichtschranken mit einer Standard-SPS

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Bei Lichtstrahlunterbrechung wird eine gefahrbringende Bewegung stillgesetzt (STO – Sicher abgeschaltetes Moment).

Funktionsbeschreibung

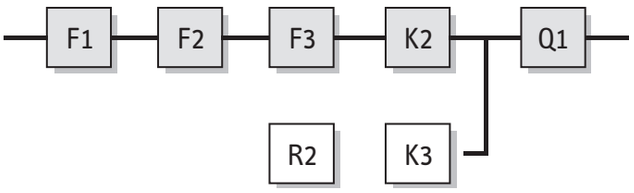
- Bei einer Lichtstrahlunterbrechung der *n* kaskadierten Lichtschranken F1 bis Fn wird sowohl kontaktbehaftet durch das Entregen des Hilfsschützes K2 als auch durch den SPS-Ausgang (O1.1) des Testkanals ein Abschaltbefehl erzeugt. Das Stillsetzen der gefahrbringenden Bewegung erfolgt dann über das Leistungsschütz Q1.

- Die Testung der Lichtschranken erfolgt vor jedem Start der gefahrbringenden Bewegung nach dem Drücken der Start-Taste S2 durch softwaregesteuertes Ausschalten der Lichtschrankensender mittels SPS-Ausgang O1.2. Die Überwachung der Empfängerreaktion (K2 fällt wieder ab) erfolgt über die SPS-Eingänge I1.1 und I1.2. Bei fehlerfreiem Verhalten gelangt K2 über O1.2 in Selbsthaltung und S2 kann zum Einleiten der gefahrbringenden Bewegung losgelassen werden. K1 wird über O1.0 entregt und über O1.1 wird das Hauptschütz Q1 angesteuert.

- Im Falle eines durch die Testung aufgedeckten Fehlers in einer Lichtschranke oder in K2 werden die Ausgänge O1.1 und O1.2 deaktiviert und es erfolgt keine weitere Ansteuerung des Hauptschützes Q1.

- Beim unterstellten globalen Versagen der SPS (Ausgang O1.0 führt Low-Potenzial, O1.1 und O1.2 führen High-Potenzial) bewirkt eine Lichtstrahlunterbrechung unabhängig von der SPS die Entregung von K2. Um diese Unabhängigkeit sicherzustellen, werden die Lichtschrankenausgänge mithilfe der Entkopplungsdiode R2 von der SPS getrennt. Im ungünstigen Fall können über das Betätigen der Start-Taste die Lichtschranken wieder mit K2 aktiviert werden und somit das Hauptschütz Q1 ansteuern. Somit wäre (nur) die Testeinrichtung ausgefallen. Ein Ausfall der Testeinrichtung wird wegen eines wahrscheinlich in diesem Zusammenhang gestörten funktionalen Prozessablaufs aufgedeckt.

- Während des Tests ist die Ansteuerung von Q1 durch K1 und O1.1 gesperrt.



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.
- Es werden spezielle Lichtschranken mit ausreichenden optischen Eigenschaften (optischer Öffnungswinkel, Fremdlichtsicherheit usw.) nach DIN CLC/TS 61496-2 verwendet.
- Mit nur zwei SPS-Eingängen und einem Relais bzw. Hilfsschütz können mehrere Lichtschranken kaskadiert und überwacht werden.
- Die Hilfsschütze K1 und K2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Das Schütz Q1 besitzt einen Spiegelkontakt entsprechend DIN EN 60947-4-1, Anhang F.
- Der Einsatz der Standardkomponenten F1 bis Fn und K3 erfolgt entsprechend den Hinweisen in Abschnitt 6.3.10.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL b (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.
- Die Start-Taste S2 muss außerhalb des Gefahrenbereiches und mit Einblick in den Gefahrenbereich bzw. in die Gefahrstelle angeordnet sein.
- Die Anzahl, Anordnung und Höhe von Lichtstrahlen muss DIN EN 999 und DIN IEC 62046 entsprechen.
- Ist bei der Absicherung von Gefahrbereichen ein „Hintertreten“ möglich, sind weitere Maßnahmen wie z.B. eine Wiederanlaufsperre erforderlich. Dazu lässt sich die Start-Taste S2 nutzen. Die SPS K3 kontrolliert dazu die Dauer des Gedrücktseins der Taste auf eine Minimal- und eine Maximalzeit. Nur wenn die Bedingungen eingehalten sind, wird von einem gültigen Start-Befehl ausgegangen.

Bemerkungen

- Das Beispiel ist für den Einsatz in Anwendungen mit seltener Anforderung der Sicherheitsfunktion vorgesehen. Damit kann die Anforderung der vorgesehenen Architektur für Kategorie 2, nämlich „Testung sehr viel häufiger als Anforderung der Sicherheitsfunktion“ (vgl. Anhang G), erfüllt werden.
- Nach dem Auslösen eines Stopps sind die Lichtschranken bis zum nächsten Start deaktiviert. Dadurch könnte z.B. ein Gefahrenbereich betreten werden, ohne dass dies schaltungstechnisch „registriert“ wird. Durch eine entsprechende Anpassung der Schaltung lässt sich das Verhalten ändern.

Berechnung der Ausfallwahrscheinlichkeit

- Bei der Berechnung der Ausfallwahrscheinlichkeit werden beispielhaft drei Lichtschranken F1 bis F3 berücksichtigt. Wird eine zweite Gefahrstelle abgesichert, so handelt es sich um eine weitere Sicherheitsfunktion, die separat berechnet wird.
- Zur Berechnung der Ausfallwahrscheinlichkeit wird das Gesamtsystem in die zwei Subsysteme „Lichtschranken“ und „Hauptschütz“ (Q1) aufgeteilt.

Für das Subsystem „Lichtschranken“ gilt:

- F1, F2, F3 und K2 stellen den funktionalen Pfad der Kategorie-2-Schaltungsstruktur dar, die SPS K3 (inklusive Entkopplungsdiode R2) stellt die Testeinrichtung dar. S2 und K1 dienen zur Aktivierung der Lichtschrankentestung und sind an der Berechnung der Ausfallwahrscheinlichkeit nicht beteiligt.

- $MTTF_d$: Für F1 bis F3 wird jeweils eine $MTTF_d$ von 100 Jahren [G] angenommen. Für K2 gilt ein B_{10d}-Wert von 20 000 000 Zyklen [N]. Mit 240 Arbeitstagen, 16 Arbeitsstunden und 180 Sekunden Zykluszeit ist n_{op}= 76 800 Zyklen/Jahr. Durch die oben beschriebene Testung verdoppelt sich dieser Wert auf n_{op}= 153 600 Zyklen/Jahr mit einer $MTTF_d$ = 1 302 Jahre für K2. Diese Werte ergeben eine $MTTF_d$ des Funktionskanals von 32 Jahren („hoch"). Für K3 wird eine $MTTF_d$ von 50 Jahren [G] angenommen. Der $MTTF_d$-Wert von 228 311 Jahren [N] für die Entkopplungsdiode R2 ist im Vergleich dazu unbedeutend.

- DC_{avg}: DC = 60 % für F1 bis F3 begründet sich durch den beschriebenen Funktionstest, DC = 99 % für K2 folgt aus der direkten Überwachung in K3 mithilfe zwangsgeführter Kontakte. Die Mittelungsformel für DC_{avg} ergibt 61,0 % („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 im Subsystem „Lichtschranken" entspricht Kategorie 2 mit hoher $MTTF_d$ pro Kanal (32,5 Jahre) und niedrigem DC_{avg} (61,0 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}85 \cdot 10^{-6}$/Stunde.

Für das Subsystem „Hauptschütz" wird angenommen:

- B_{10d} = 2 000 000 Zyklen [N] mit n_{op} = 76 800 Zyklen/Jahr. Dies führt zu einer $MTTF_d$ von 260,4 Jahren, die nach Norm auf 100 Jahre begrenzt wird. Die Struktur entspricht Kategorie 1, daher sind DC_{avg} und Ausfälle infolge gemeinsamer Ursache nicht relevant. Es ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}14 \cdot 10^{-6}$/Stunde.

- Die Addition der mittleren Wahrscheinlichkeit gefährlicher Ausfälle beider Subsysteme ergibt $3{,}0 \cdot 10^{-6}$/Stunde. Dies entspricht PL c.

- Ist abzusehen, dass die Sicherheitsfunktion häufiger als für die vorgesehene Architektur der Kategorie 2 zugrunde gelegt angefordert wird (das Verhältnis 100 : 1 wird unterschritten, d.h. häufiger als einmal in 5 Stunden), so kann dies gemäß Anhang G bis zu einem Verhältnis von 25 : 1 mit einem Zuschlag von 10 % berücksichtigt werden. Im vorliegenden Fall mit drei Lichtschranken erreicht das Subsystem „Lichtschranken" noch eine Ausfallwahrscheinlichkeit von $2{,}04 \cdot 10^{-6}$/Stunde. Die mittlere Gesamtwahrscheinlichkeit gefährlicher Ausfälle von $3{,}18 \cdot 10^{-6}$/Stunde erreicht allerdings nur noch PL b. Um PL c zu erreichen, müssten z.B. die Anzahl der Lichtschranken reduziert oder Komponenten höherer $MTTF_d$ eingesetzt werden.

Weiterführende Literatur

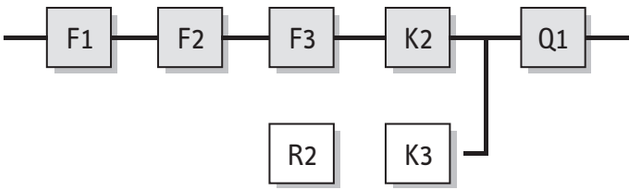
- *Grigulewitsch, W.; Reinert, D.:* Lichtschranken mit Testung. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 228. 22. Lfg. V/94. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.
www.bgia-handbuchdigital.de/330228

- 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

- DIN IEC 62046: Sicherheit von Maschinen – Anwendung von Schutzeinrichtungen zum Erkennen von Personen (Normentwurf) (08.06). Beuth, Berlin 2006

- DIN EN 999: Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (12.98). Beuth, Berlin 1998



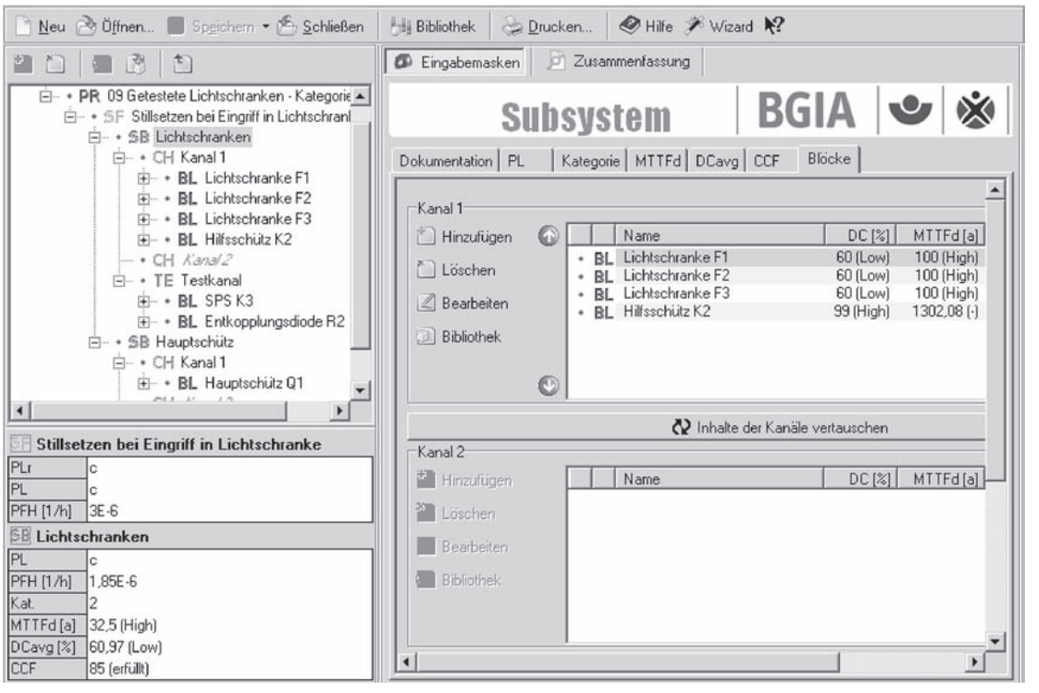


Abbildung 8.17: PL-Bestimmung mithilfe von SISTEMA

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

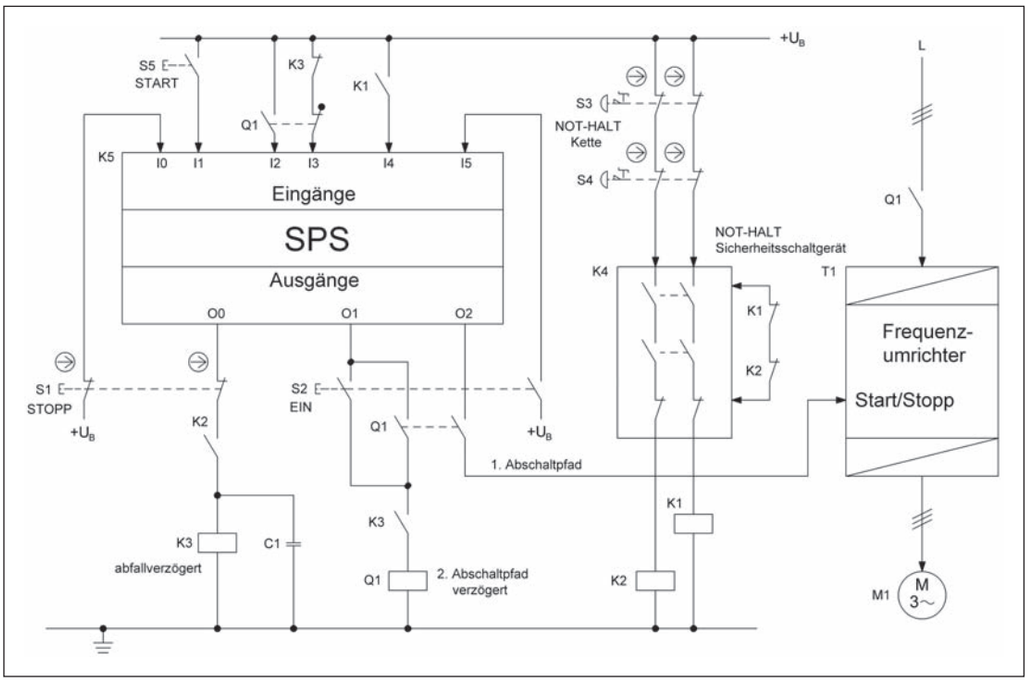


Abbildung 8.18: Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Stopp- oder Not-Halt-Befehl

Sicherheitsfunktion

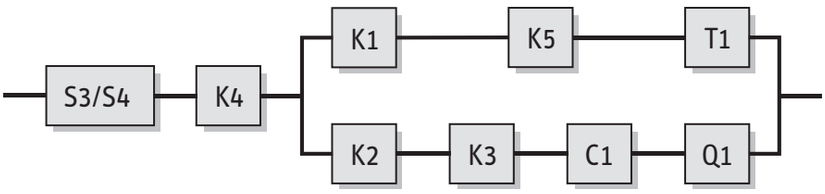
- Sicherheitsbezogene Stoppfunktion bzw. Not-Halt-Funktion: Nach einem Stopp- oder Not-Halt-Befehl wird der Antrieb angehalten (SS1 – Sicherer Stopp 1).

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

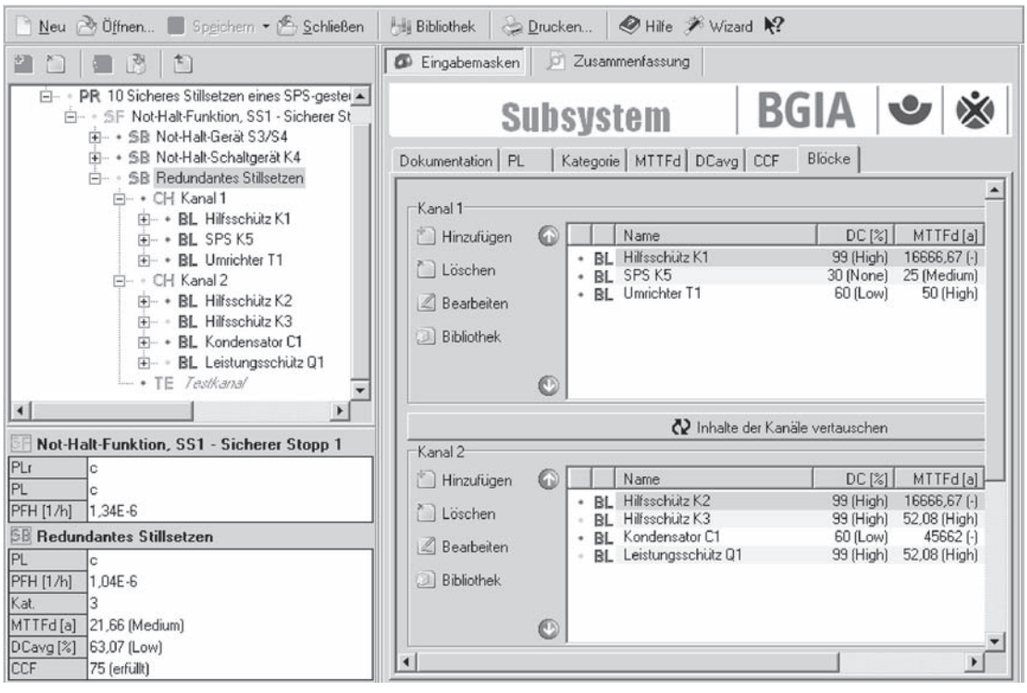


Abbildung 8.19: PL-Bestimmung mithilfe von SISTEMA

8.2.11 Getestetes pneumatisches Ventil (Subsystem) – Kategorie 2 – PL d (für PL-c-Sicherheitsfunktionen) (Beispiel 11)

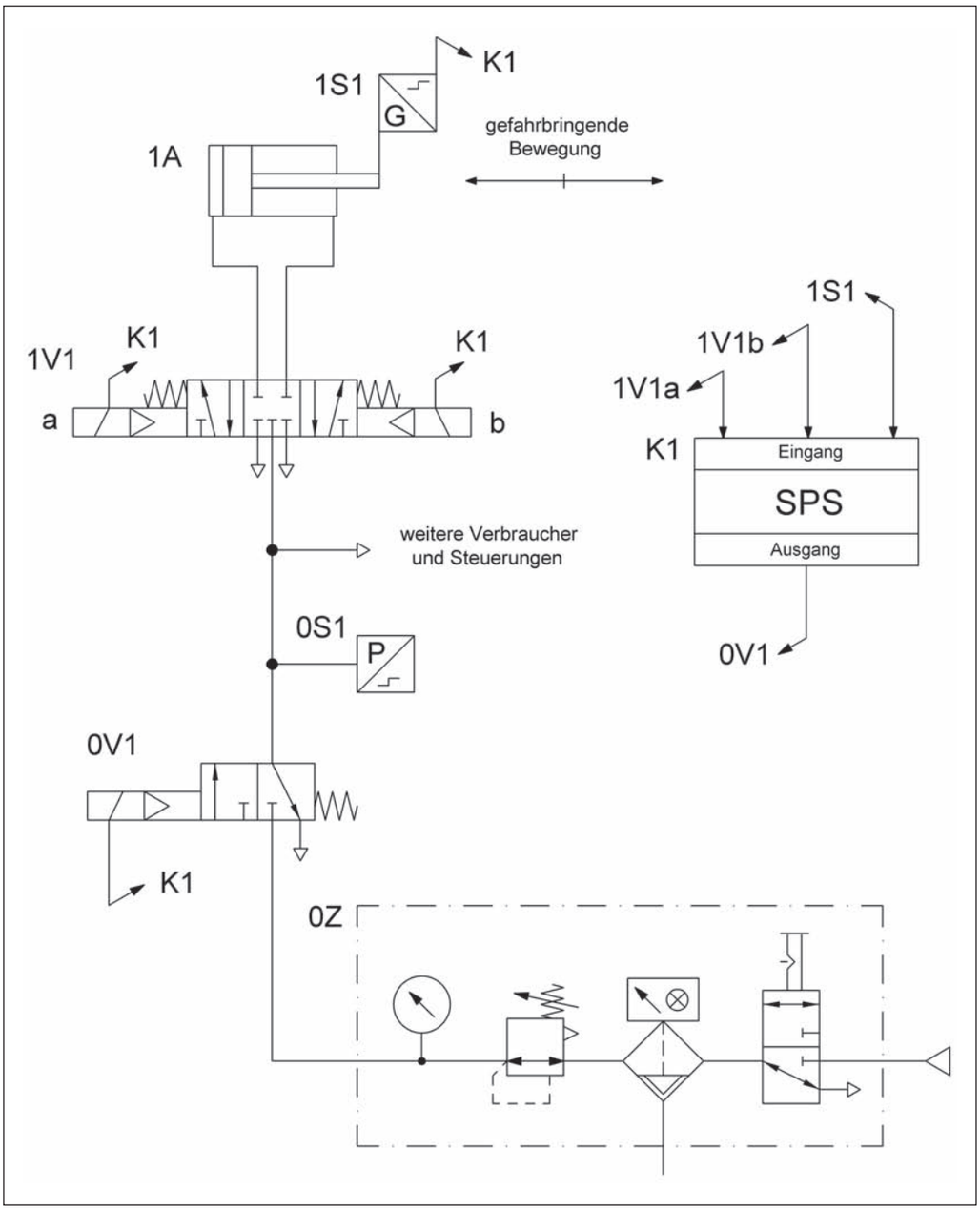
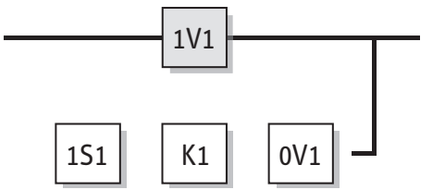


Abbildung 8.20: Pneumatisches Ventil mit elektronischer Testung zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen einer gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.



Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch ein Wegeventil 1V1 gesteuert.
- Der Ausfall des Wegeventils 1V1 zwischen den Funktionstests kann zum Verlust der Sicherheitsfunktion führen. Der Ausfall hängt von der Zuverlässigkeit des Wegeventils ab.
- Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion über die SPS K1 mithilfe eines Wegmesssystems 1S1 in geeigneten Zeitabständen und beim Anfordern der Schutzfunktion. Das Erkennen des Ausfalls von 1V1 führt zum Abschalten des Entlüftungsventils 0V1.
- Das Unterbrechen der gefahrbringenden Bewegung über das Entlüftungsventil 0V1 ergibt in der Regel einen verlängerten Nachlaufweg. Der Abstand zum Gefahrenbereich muss auf den verlängerten Nachlaufweg ausgelegt sein.
- Durch den Ausfall des Wegeventils darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zu einem Ausfall des Wegeventils führen.
- Wenn durch eingesperrte Druckluft eine weitere Gefährdung auftreten kann, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Bei 1V1 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung und Federzentrierung.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.
- Die Testung erfolgt z.B. durch Überprüfung des Weg-/Zeitverhaltens (Wegmesssystem 1S1) der gefahrbringenden Bewegungen in Verbindung mit dem Schaltzustand des Wegeventils mit Auswertung in einer SPS (K1).
- In geeigneten Zeitabständen, z.B. täglich, wird zur Verhinderung eines systematischen Ausfalls die übergeordnete Abschaltfunktion (in diesem Beispiel auf das Entlüftungsventil 0V1 wirkend) überprüft.
- Für den Einsatz in Anwendungen mit seltenem Eingriff in den Gefahrbereich vorgesehen. Damit kann die Anforderung der vorgesehenen Architektur für Kategorie 2, nämlich „Testung sehr viel häufiger als Anforderung der Sicherheitsfunktion“ (vgl. Anhang G), erfüllt werden.
- Der Einsatz der Standardkomponente K1 erfolgt entsprechend den Hinweisen in Abschnitt 6.3.10.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL b (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$ des Funktionskanals: Für das Wegeventil 1V1 wird ein B_{10d}-Wert von 20 000 000 Schaltspielen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 5 Sekunden Zykluszeit ist n_{op} = 2 764 800 Schaltspiele/Jahr und $MTTF_d$ = 72,3 Jahre. Dies ist gleichzeitig der $MTTF_d$-Wert für den Funktionskanal.

- $MTTF_d$ des Testkanals: Für das Wegmesssystem 1S1 wird ein $MTTF_d$-Wert von 150 Jahren [G] angenommen. Für die SPS K1 wird ein $MTTF_d$-Wert von 50 Jahren [G] angenommen. Für das Entlüftungsventil 0V1 gilt ein B_{10d}-Wert von 20 000 000 Zyklen [N]. Bei täglichem Einschalten an 240 Arbeitstagen ergibt sich für 0V1 ein $MTTF_d$-Wert von 833 333 Jahren. Damit beträgt die $MTTF_d$ des Testkanals 37,5 Jahre.

- DC_{avg}: DC = 60 % für 1V1 gründet sich auf den Vergleich des Weg-/Zeit-Verhaltens der gefahrbringenden Bewegung in Verbindung mit dem Schaltzustand des Wegeventils. Dies ist gleichzeitig der DC_{avg} („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 pneumatischen Steuerungselemente entspricht Kategorie 2 mit hoher $MTTF_d$ (72,3 Jahre) und niedrigem DC_{avg} (60 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}62 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile (Subsysteme) zur Vervollständigung der Sicherheitsfunktion wird sich in der Regel PL c für die komplette Sicherheitsfunktion ergeben.

- Das verschleißbehaftete Element 1V1 sollte nach jeweils ca. sieben Jahren (T_{10d}) ausgetauscht werden.

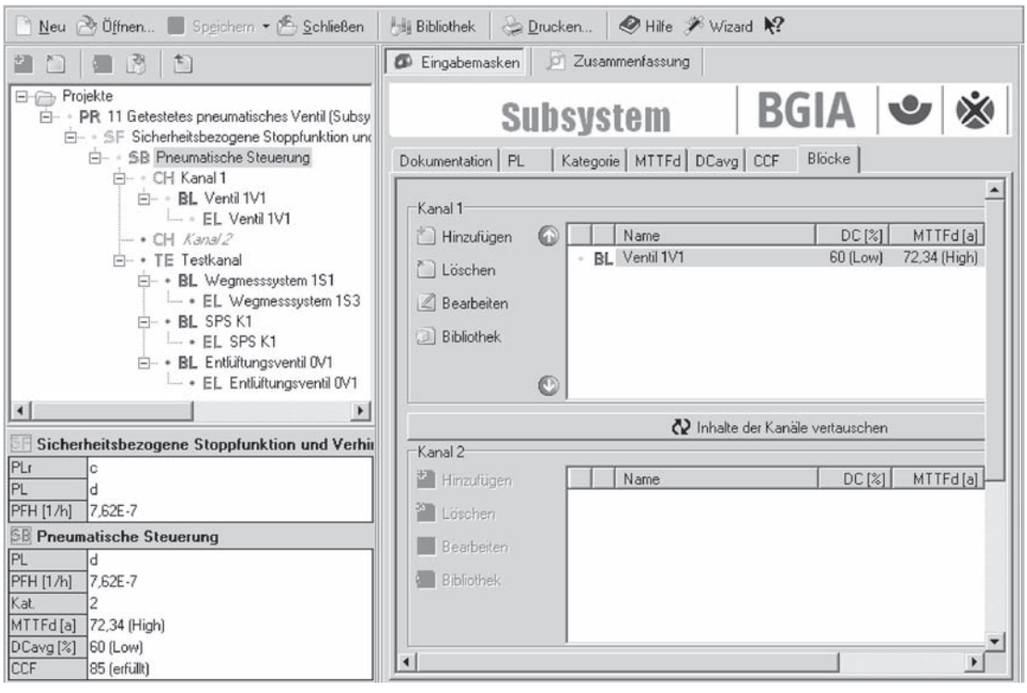


Abbildung 8.21: PL-Bestimmung mithilfe von SISTEMA

8.2.12 Getestetes hydraulisches Ventil (Subsystem) – Kategorie 2 – PL d (für PL-c-Sicherheitsfunktionen) (Beispiel 12)

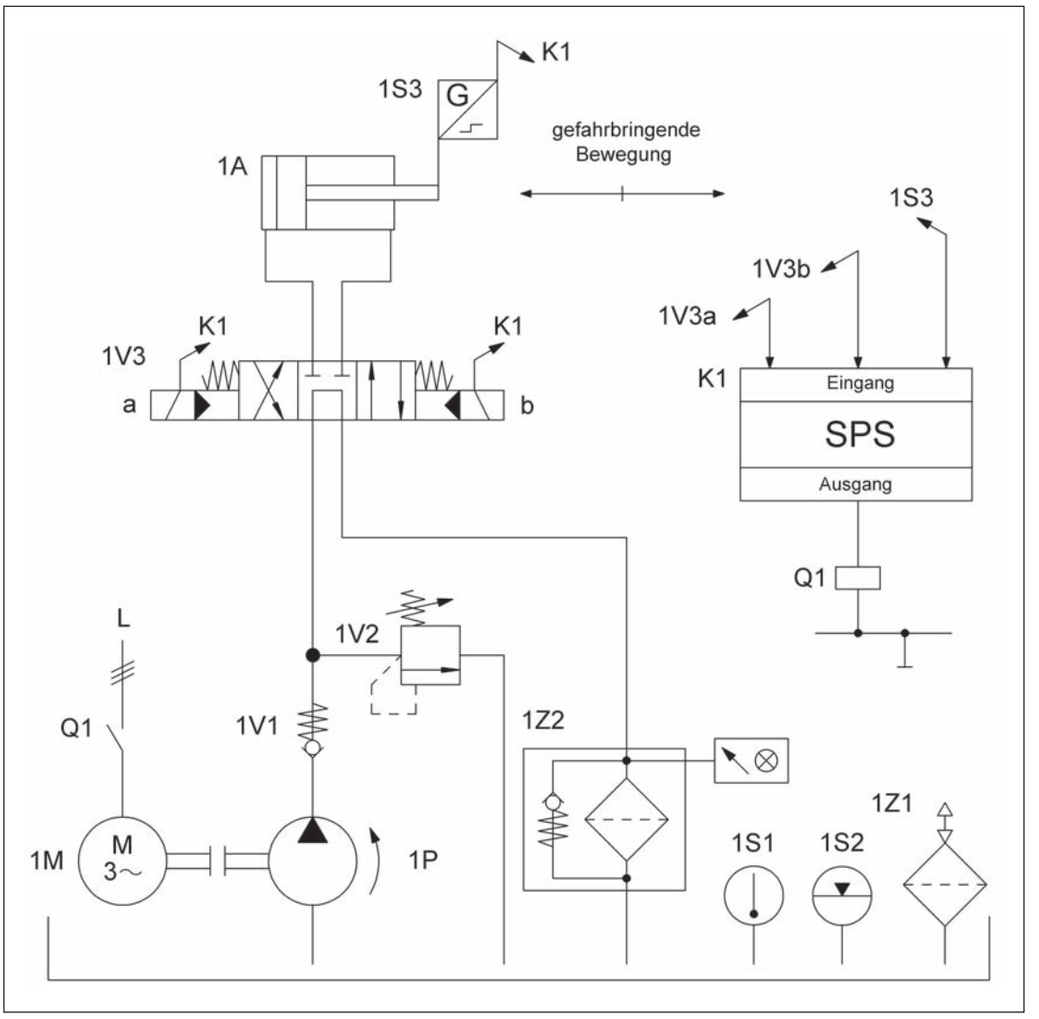


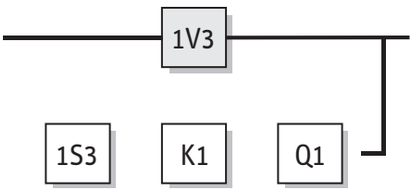
Abbildung 8.22: Hydraulisches Ventil mit elektronischer Testung zur Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen einer gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- Hier ist nur der hydraulische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere, sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch das Wegeventil 1V3 gesteuert.
- Der Ausfall des Wegeventils 1V3 zwischen den Funktionstests kann zum Verlust der Sicherheitsfunktion führen. Die Ausfallwahrscheinlichkeit hängt von der Zuverlässigkeit des Wegeventils ab.
- Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion über die SPS K1 mithilfe eines Wegmesssystems 1S3 in geeigneten Zeitabständen und beim Anfordern der Schutzfunktion. Das Erkennen des Ausfalls von 1V3 führt zum Abschalten der Hydraulikpumpe 1M bzw. 1P mittels Leistungsschütz Q1.



- Das Unterbrechen der gefahrbringenden Bewegung über die Hydraulikpumpe ergibt in der Regel einen verlängerten Nachlaufweg. Der Abstand zum Gefahrenbereich muss auf den verlängerten Nachlaufweg ausgelegt sein.

- Durch den Ausfall des Wegeventils darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zu einem Ausfall des Wegeventils führen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.

- Bei 1V3 handelt es sich um ein Wegeventil mit Sperr-Mittelstellung, ausreichender positiver Überdeckung und Federzentrierung.

- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme des Steuersignals erreicht.

- Die Testung erfolgt z.B. durch Überprüfung des Weg-/Zeitverhaltens (Wegmesssystem 1S3) der gefahrbringenden Bewegungen in Verbindung mit dem Schaltzustand des Wegeventils mit Auswertung in einer SPS (K1).

- In geeigneten Zeitabständen, z.B. täglich, wird zur Verhinderung eines systematischen Ausfalls die übergeordnete Abschaltfunktion (in diesem Beispiel auf die Hydraulikpumpe wirkend) überprüft.

- Für den Einsatz in Anwendungen mit seltenem Eingriff in den Gefahrbereich vorgesehen. Damit kann die Anforderung der vorgesehenen Architektur für Kategorie 2, nämlich „Testung sehr viel häufiger als Anforderung der Sicherheitsfunktion“ (vgl. Anhang G), erfüllt werden.

- Der Einsatz der Standardkomponente K1 erfolgt entsprechend den Hinweisen in Abschnitt 6.3.10.

- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL b (herabgestuft wegen Diversität) und den Hinweisen in Abschnitt 6.3.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$ des Funktionskanals: Für das Wegeventil 1V3 wird eine $MTTF_d$ von 150 Jahren angenommen [N]. Dies ist gleichzeitig der $MTTF_d$-Wert für den Funktionskanal, der zunächst auf 100 Jahre gekürzt wird.

- $MTTF_d$ des Testkanals: Für das Wegmesssystem 1S3 wird ein $MTTF_d$-Wert von 150 Jahren [G] angenommen. Für die SPS K1 wird ein $MTTF_d$-Wert von 50 Jahren [G] angenommen. Für das Leistungsschütz Q1 gilt ein B_{10d}-Wert von 2 000 000 Zyklen [N]. Bei täglichem Einschalten an 240 Arbeitstagen ergibt sich ein $MTTF_d$-Wert für Q1 von 83 333 Jahren. Damit beträgt die $MTTF_d$ des Testkanals 37,5 Jahre. Die $MTTF_d$ des Funktionskanals muss deshalb nach dem zugrunde liegenden Berechungsmodel auf 75,0 Jahre gekürzt werden.

- DC_{avg}: DC = 60 % für 1V3 gründet sich auf den Vergleich des Weg-/Zeitverhaltens der gefahrbringenden Bewegung in Verbindung mit dem Schaltzustand des Wegeventils. Dies ist gleichzeitig der DC_{avg} („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 2 mit hoher $MTTF_d$ (75,0 Jahre) und niedrigem DC_{avg} (60 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}31 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile (Subsysteme) zur Vervollständigung der Sicherheitsfunktion wird sich in der Regel PL c für die komplette Sicherheitsfunktion ergeben.

8.2.13 Unterlast-Erkennung für Leuchtenhänger – Kategorie 2 – PL d (Beispiel 13)

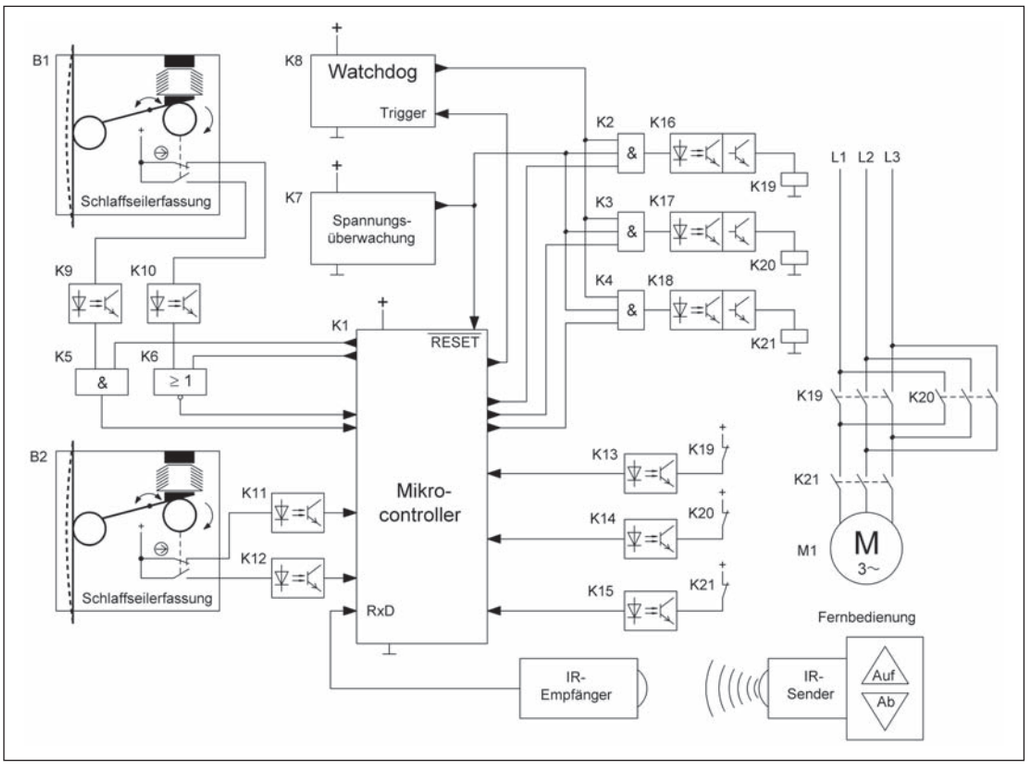


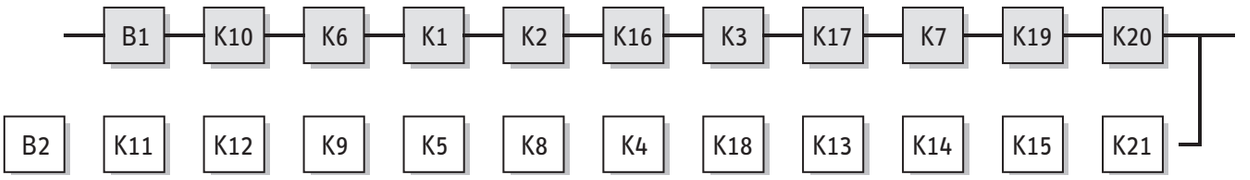
Abbildung 8.23: Kombinierte elektromechanische und programmierbare elektronische Steuerung zur Verhinderung der Unterlast von Leuchtenhängern

Sicherheitsfunktion

- Unterlast- bzw. Schlaffseilerkennung: Bei Erkennung der Unterlast eines Leuchtenhängers (schlaffes Tragmittel/Seil) wird die Abwärtsbewegung gestoppt (STO – sicher abgeschaltetes Moment).

Funktionsbeschreibung

- In der Studio- und Bühnentechnik werden zahlreiche elektromotorisch betriebene Leuchtenhänger eingesetzt. Bei der Abwärtsbewegung besteht die Gefahr, dass Unterlast (d.h., das Tragmittel wird schlaff) durch Verklemmen oder Verkanten der geführten Last oder durch Aufsetzen auf andere Gegenstände auftritt. Hierbei besteht die Gefahr, dass z.B. das Hindernis plötzlich nachgibt, die Last durchschlägt und in der Folge Personen im Gefahrenbereich gefährdet werden.
- Auf- und Abwärtsbewegungen des Leuchtenhängers können z.B. über eine Infrarot-Fernbedienung gesteuert werden. Diese Funktion wird hier nicht bewertet, sie ist aber immer sicherheitsgerichtet auszuführen.
- Um einen Absturz des Leuchtenhängers durch Reißen eines Tragmittels zu vermeiden, wird die Last von zwei Tragmitteln getragen. An jedem Tragmittel befindet sich ein Schlaffseilschalter B1 bzw. B2 mit einer Öffner-Schließer-Kombination.
- Der Mikrocontroller K1 wertet die Schaltzustände der Schlaffseilschalter B1 und B2 aus. Weiterhin steuert K1 über Logikgatter K2/K3 und optoentkoppelte Transistorverstärker K16/K17 die Hilfsschütze K19 und K20 für die Auf- bzw. Abwärtsbewegung des Leuchtenhängers an.
- Die Schaltzustände der Kontakte der Schlaffseilschalter B1 und B2 werden vom Mikrocontroller K1 ausgewertet und auf Plausibilität geprüft. Zur Testung der verwendeten Eingänge des Mikrocontrollers werden die Signale des Schlaffseilschalters B1 zwangsdynamisiert. Hierzu erzwingt der Mikrocontroller über Logikgatter K5 und K6 einen kurzzeitigen Wechsel der Signale, um festzustellen, ob die Eingänge den Signalwechsel noch übertragen können. Die Zwangsdynamisierung der Signale eines Schlaffseilschalters ist ausreichend.



- Im Mikrocontroller K1 werden Selbsttests der integrierten Einheiten wie Recheneinheit, Arbeits- und Festwertspeicher durchgeführt. Die Spannungsüberwachung K7 bemerkt Fehler in der Versorgungsspannung. Fehler im Mikrocontroller werden durch eine zeitliche Programmlaufüberwachung im Watchdog K8 erkannt. Die Bauteile K19 bis K21 zur Steuerung der Auf- bzw. Abwärtsbewegung des Leuchtenhängers werden mithilfe einer Rücklesung – entkoppelt durch Optokoppler K13 bis K15 – im Mikrocontroller überwacht. Im Falle eines erkannten Fehlers erfolgt eine übergeordnete Abschaltung über das Hilfsschütz K21 – angesteuert durch Logikgatter K4 und entkoppelt durch Optokoppler K18 – durch das fehlererkennende Bauteil. Wird der Watchdog K8 nicht rechtzeitig vom Mikrocontroller K1 retriggert, erfolgt ausgehend von K8 über alle Logikgatter K2 bis K4 ein Stillsetzen der Bewegung des Leuchtenhängers.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Die Erkennung einer Unterlast erfolgt redundant über beide Tragmittel mithilfe der beiden Schlaffseilschalter B1 und B2. Diese enthalten zwangsöffnende Positionsschalter entsprechend DIN EN 60947-5-1, Anhang K.
- Ein stabiler Aufbau der Betätigungsmechanik der Schlaffseilschalter ist sichergestellt.
- K19 bis K21 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die Programmierung der Software (SRESW) von K1 erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 6.3.

Bemerkungen

- Der Entwurf zu DIN 15560-46 fordert in Abschnitt 5.1.2 mindestens zwei Tragmittel, um den Absturz eines Leuchtenhängers und seiner Last zu verhindern.
- In geeigneten Zeitabständen sind Sichtprüfungen bzw. Wartungen der Tragmittel vorzunehmen.
- Die gezeigte Schaltungsstruktur ist in Teilen nicht explizit dazu ausgelegt, mögliche Gefährdungen durch ungewollte Bewegungen des Leuchtenhängers (unerwarteter Anlauf) zu verhindern.
- Die verwendete Schaltungsstruktur erreicht für die betrachtete Sicherheitsfunktion – wie die Berechnung der Ausfallwahrscheinlichkeit zeigt – PL d. Die Anwendung des Risikographen zur Bestimmung der erforderlichen Performance Level PL_r mit den Parametern S2, F1 und P1 führt nach DIN 15560-46, Abschnitt B.1.1.3.3, unter der Voraussetzung, dass der Betrieb mit Beaufsichtigung erfolgt und dass die Leuchtenhänger nur von Fachleuten betrieben werden, auf einen PL_r = c. Ist dies nicht der Fall, ist PL_r = d erforderlich.

Berechnung der Ausfallwahrscheinlichkeit

- Zur besseren Übersicht werden in Abbildung 8.23 Bauteile zu Blöcken zusammengefasst. K9 bis K15 beinhalten je einen Optokoppler und zwei Widerstände. K16 bis K18 beinhalten zusätzlich je einen Transistor zur Ansteuerung der nachfolgenden Hilfsschütze.

- Zur Anwendung des vereinfachten Verfahrens für die Abschätzung des erreichten PL werden die Bauteile der Schaltung wie folgt den Blöcken der vorgesehenen Architektur für Kategorie 2 zugewiesen:

  I: B1
  L: K10, K6, K1, K2, K16, K3, K17, K7
  O: K19, K20
  TE: B2, K11, K12, K9, K5, K8, K4, K18, K13, K14, K15
  OTE: K21

- $MTTF_d$: Die für die Berechnung benötigten $MTTF_d$-Werte stammen aus DIN EN ISO 13849-1 [N], SN 29500-2 und SN 29500-14 [D]. Für B1 und B2 werden folgende Kennwerte angesetzt: B_{10d} = 100 000 Zyklen [G], n_{op} = 10 Zyklen/Jahr. Für die Hilfsschütze K19 bis K21 gilt: B_{10d} = 400 000 Zyklen [N], n_{op} = 10 Zyklen/Tag an 365 Arbeitstagen. Für den Mikrocontroller K1 wird eine $MTTF_d$ von 1 141 Jahren [D] angesetzt. Für die elektronischen Bauteile werden folgende $MTTF_d$-Werte angesetzt [D]: 4 566 Jahre für Watchdog K8, 5 707 Jahre für die Optokoppler K9 bis K18, 22 831 Jahre für die Logikgatter K2 bis K6, 38 051 Jahre für die Spannungsüberwachung K7 und 45 662 Jahre für Transistoren bzw. 228 310 Jahre für Widerstände. Durch Aufsummierung der Ausfallraten aller Bauteile des funktionalen Kanals (Blöcke I, L und O) ergibt sich eine $MTTF_d$ von 288 Jahren. Diese wird gemäß den Anforderungen der Norm auf 100 Jahre beschnitten („hoch“).

- Die $MTTF_d$ des Testkanals ergibt sich durch Aufsummierung der Ausfallraten aller Bauteile der Blöcke TE und OTE. Sie beträgt 393 Jahre und ist damit größer oder gleich der Hälfte der $MTTF_d$ des funktionalen Kanals.

- DC_{avg}: DC = 60 % für B1, K10 und K6 durch Kreuzvergleich von B1 und B2 in K1 mit geringer Anforderungsrate der Sicherheitsfunktion. DC = 60 % für K1 durch zeitliche Programmlaufüberwachung und Selbsttests einfacher Wirksamkeit. DC = 99 % für K2, K3, K16, K17, K19 und K20 durch direkte Überwachung über zwangsgeführte Kontakte. Für K7 ist DC = 0 %. Die Mittelungsformel für DC_{avg} ergibt 85 % („niedrig“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung (15) und Umgebungsbedingungen (25 + 10).

- Die Kombination der Steuerungselemente entspricht Kategorie 2 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und niedrigem DC_{avg} (85 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}72 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- DIN 15560-46: Scheinwerfer für Film, Fernsehen, Bühne und Fotografie – Teil 46: Bewegliche Leuchtenhänger; Sicherheitstechnische Anforderungen und Prüfung (Normentwurf) (06.07). Beuth, Berlin 2007

- Sicherheit bei Produktionen und Veranstaltungen – Leitfaden BGI 810. Hrsg.: Verwaltungs-Berufsgenossenschaft, Hamburg 2006, http://www.vbg.de/imperia/md/content/produkte/broschueren/bgi_810_.pdf

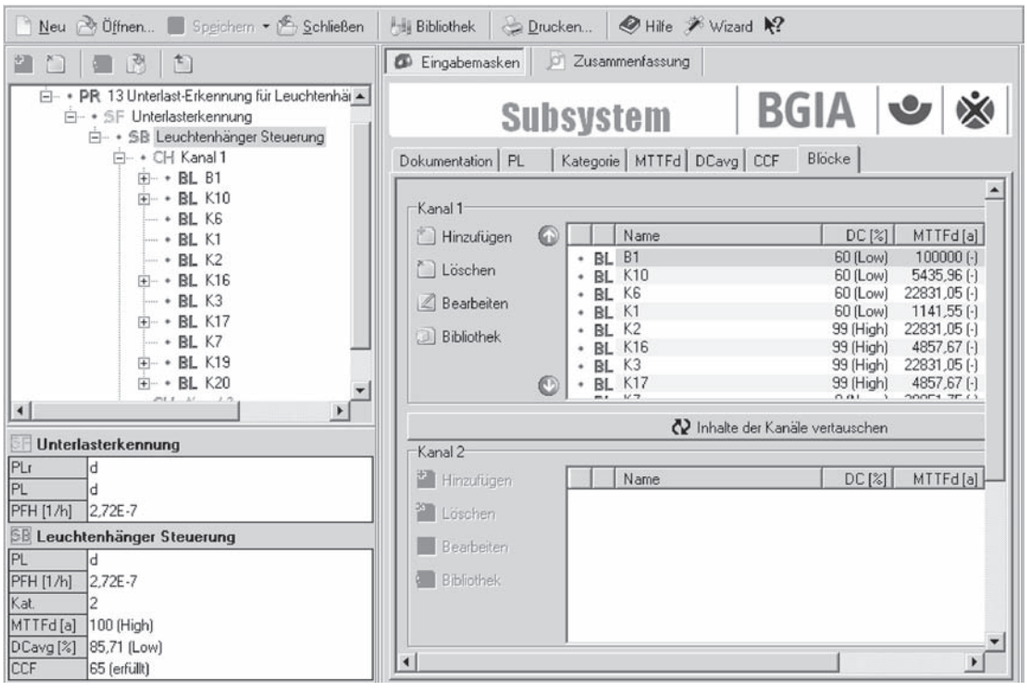


Abbildung 8.24: PL-Bestimmung mithilfe von SISTEMA

8.2.14 Pneumatische Ventilsteuerung (Subsystem) – Kategorie 3 – PL d (Beispiel 14)

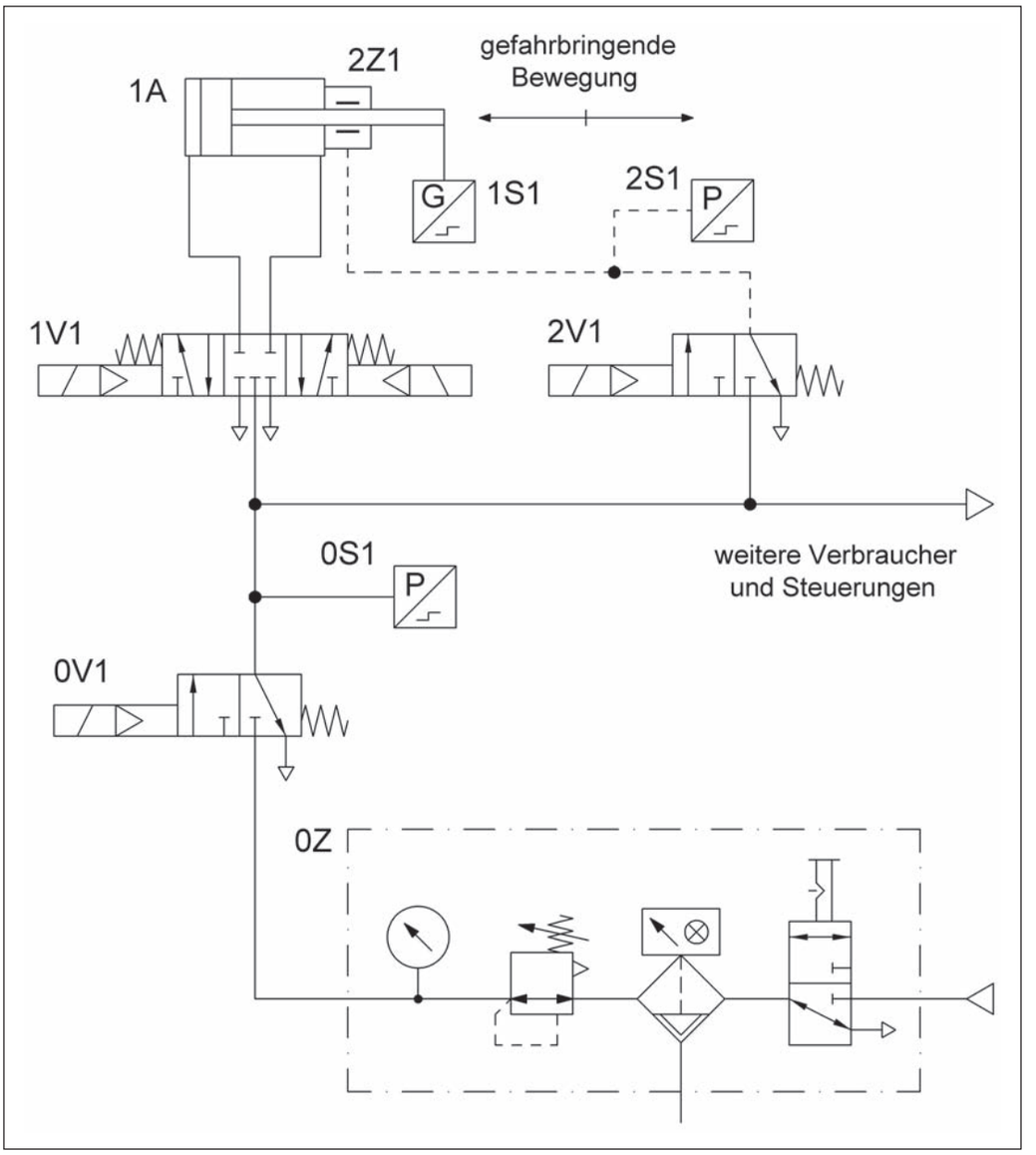


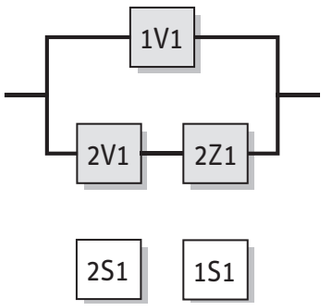
Abbildung 8.25: Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden redundant durch ein Wegeventil 1V1 und eine Bremse 2Z1 an der Kolbenstange gesteuert bzw. stillgesetzt. Die Bremse 2Z1 wird durch ein Steuerventil 2V1 angesteuert.
- Der einzelne Ausfall eines der genannten Ventile oder der Bremse führt nicht zum Verlust der Sicherheitsfunktion.
- Wegeventil und Bremse werden im Prozess zyklisch angesteuert.



- Die Funktion des Steuerventils 2V1 wird durch einen Druckschalter 2S1 überwacht. An dem nicht überwachten Ventil 1V1 und der nicht überwachten Bremse 2Z1 werden einige Fehler im Arbeitsprozess erkannt. Zusätzlich wird der Nachlaufweg (Weg-/Zeitverhalten) beim Bremsvorgang (dynamisch) oder/und bei Start der Maschine (statisch) mithilfe eines Wegmesssystems 1S1 an der Kolbenstange überwacht. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.

- Es erfolgt eine zwangsweise Testung der Sicherheitsfunktion in geeigneten Zeitabständen, z.B. mindestens alle 8 Arbeitsstunden.

- Durch den Ausfall der Bremse darf die Testfunktion nicht beeinträchtigt werden. Ein Ausfall der Testfunktion darf nicht zum Ausfall der Bremse führen.

- Kann durch eingesperrte Druckluft eine weitere Gefährdung auftreten, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.

- Das Wegeventil 1V1 hat eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung.

- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.

- Die Signalverarbeitung der Drucküberwachung 2S1 und des Wegmesssystems 1S1 erfolgt z.B. in der vorgeschalteten elektrischen Logik.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für die Wegeventile 1V1 und 2V1 werden B_{10d}-Werte von 40 000 000 Zyklen [G] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 10 Sekunden Zykluszeit ist n_{op} = 1 382 400 Zyklen/Jahr. Für 1V1 und 2V1 ergibt sich damit eine $MTTF_d$ = 289 Jahre. Für die mechanische Bremse an der Kolbenstange 2Z1 wird ein B_{10d}-Wert von 5 000 000 Schaltspielen [H] eingesetzt. Das ergibt für die mechanische Bremse $MTTF_d$ = 36 Jahre. Insgesamt ergibt sich ein symmetrisierter $MTTF_d$-Wert pro Kanal von 71 Jahren („hoch“).

- DC_{avg}: DC = 99 % für das Ventil 2V1 ergibt sich aus der Drucküberwachung des Steuersignals für die Bremse. DC = 60 % für das Ventil 1V1 aus der Fehlererkennung über den Prozess. DC = 75 % für 2Z1 folgt aus einer Anlauftestung der mechanischen Bremse. Durch Mittelung ergibt sich damit ein DC_{avg} von 75 % („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 pneumatischen Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (71 Jahre) und niedrigem DC_{avg} (75 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}21 \cdot 10^{-7}$/Stunde. Dies entspricht PL d. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.

- Die verschleißbehaftete Bremse 2Z1 sollte nach jeweils ca. drei Jahren (T_{10d}) ausgetauscht werden.

8.2.15 Schutzeinrichtung und SPS-gesteuerte Hydraulik – Kategorie 3 – PL d (Beispiel 15)

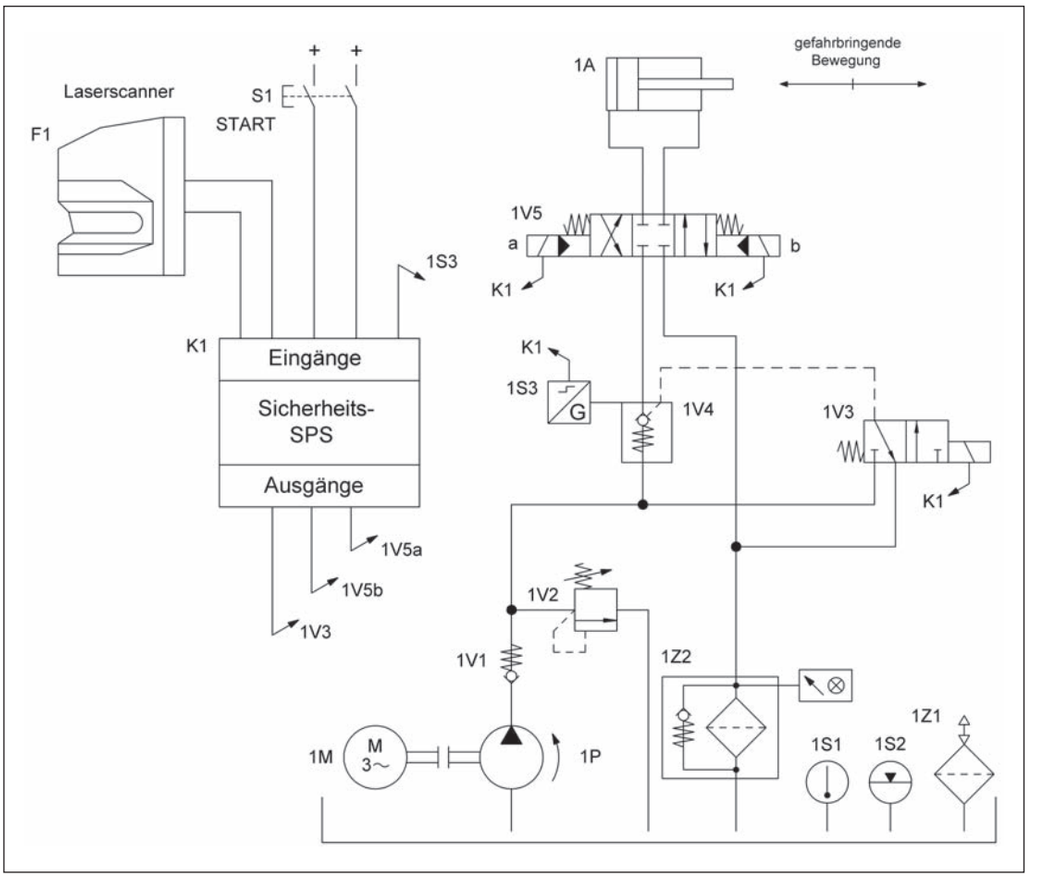


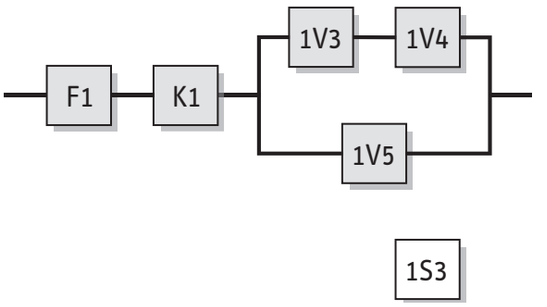
Abbildung 8.26: Schutzfeld-Überwachung durch Laserscanner mit elektrohydraulischer Abschaltung der gefahrbringenden Bewegung

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Ein Eindringen in das Schutzfeld des Laserscanners führt zu einem Stillsetzen der gefahrbringenden Bewegung.

Funktionsbeschreibung

- Der Laserscanner F1 überwacht mit seinem Schutzfeld den Bereich, in dem die Bewegung des Zylinders 1A für den Bediener gefährlich werden kann. Das Ausgangssignal des Laserscanners wird zweikanalig in die Sicherheits-SPS K1 eingelesen. Nach jeder Schutzfeldverletzung muss eine erneute Bewegung durch die Betätigung eines in K1 ausgewerteten Start-Tasters freigegeben werden (Wiederanlaufsperre). K1 steuert mithilfe des hydraulischen Steuerungsteils die Bewegung von 1A.
- Der hydraulische Steuerungsteil ist zweikanalig aufgebaut. Der erste Kanal besteht aus dem Wegeventil 1V3, das auf das entsperrbare Rückschlagventil 1V4 wirkt. In gesperrter Stellung blockiert 1V4 Bewegungen von 1A. Der zweite Kanal besteht aus dem Richtungsventil 1V5, das in Sperr-Mittelstellung ebenfalls eine Bewegung von 1A verhindert.
- 1V5 wird zyklisch angesteuert, 1V3 und 1V4 schließen nur bei einer Verletzung des Schutzfeldes.
- Als Maßnahme zur Fehlererkennung ist an 1V4 eine direkte Stellungsüberwachung 1S3 vorgesehen, die in K1 ausgewertet wird. Fehler in 1V5 können funktionsbedingt über den Prozess erkannt werden. Die Anhäufung unentdeckter Fehler im hydraulischen Steuerungsteil kann zum Verlust der Sicherheitsfunktion führen.



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.
- Fehler in den Anschlussleitungen von F1 und K1 dürfen sich nicht gefährlich auswirken. Hierzu werden auftretende Fehler erkannt und der sichere Zustand eingeleitet. Alternativ muss ein Fehlerausschluss für Leitungskurzschlüsse nach DIN EN ISO 13849-2, Tabelle D.4, möglich sein.
- Bei dem Laserscanner F1 und der Sicherheits-SPS K1 handelt es sich um geprüfte Sicherheitsbauteile für den Einsatz in PL d, die der Kategorie 3 und den jeweiligen Produktnormen entsprechen.
- Das Wegeventil 1V5 hat eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung. 1V4 ist mit elektrischer Stellungsüberwachung ausgeführt, da 1V4 nicht zyklisch geschaltet wird.
- Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 6.3.
- Es wird davon ausgegangen, dass die Ausgänge der Sicherheits-SPS jeweils von beiden Verarbeitungskanälen der SPS angesteuert werden. Sollte dies nicht der Fall sein, werden die Ausgänge, die 1V3 und 1V4 ansteuern, von einem Kanal und der Ausgang, der 1V5 ansteuert, von dem anderen Kanal der SPS angesteuert.

Berechnung der Ausfallwahrscheinlichkeit

- Da der Laserscanner F1 und die Sicherheits-SPS K1 als käufliche Sicherheitsbauteile vorliegen, werden deren Ausfallwahrscheinlichkeiten am Ende der Berechnung addiert (F1: $3{,}0 \cdot 10^{-7}$/Stunde [G], K1: $1{,}5 \cdot 10^{-7}$/Stunde [G]). Für den hydraulischen Steuerungsteil wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.
- $MTTF_d$: Für die Ventile 1V3 bis 1V5 werden Werte von 150 Jahren [N] angenommen. Damit ergibt sich insgesamt ein symmetrisierter $MTTF_d$-Wert pro Kanal von 88 Jahren („hoch“).
- DC_{avg}: DC = 99 % für 1V4 ergibt sich durch die direkte Überwachung in K1 mithilfe der Stellungsüberwachung 1S3. Wegen der engen Kopplung von 1V3 und 1V4 wird 1V3 dadurch mit einem DC von 99 % indirekt mit überwacht. DC = 60 % für 1V5 gründet sich auf die Fehlererkennung im Prozess bei zyklischer Ansteuerung. Durch Mittelung ergibt sich damit ein DC_{avg} von 86 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (90 Punkte): Trennung (15), Diversität (20), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente im hydraulischen Teil entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (88 Jahre) und niedrigem DC_{avg} (86 %). Damit ergibt sich für die Hydraulik eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}2 \cdot 10^{-8}$/Stunde.
- Insgesamt beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $(3{,}0 + 1{,}5 + 0{,}62) \cdot 10^{-7} = 5{,}12 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- *Bömer, T.:* Hinweise zum praktischen Einsatz von Laserscannern. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 310 243. 36. Lfg. XII/99. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de/310243

8.2.16 Erdbaumaschinensteuerung mit Bussystem – Kategorie 3 – PL d (Beispiel 16)

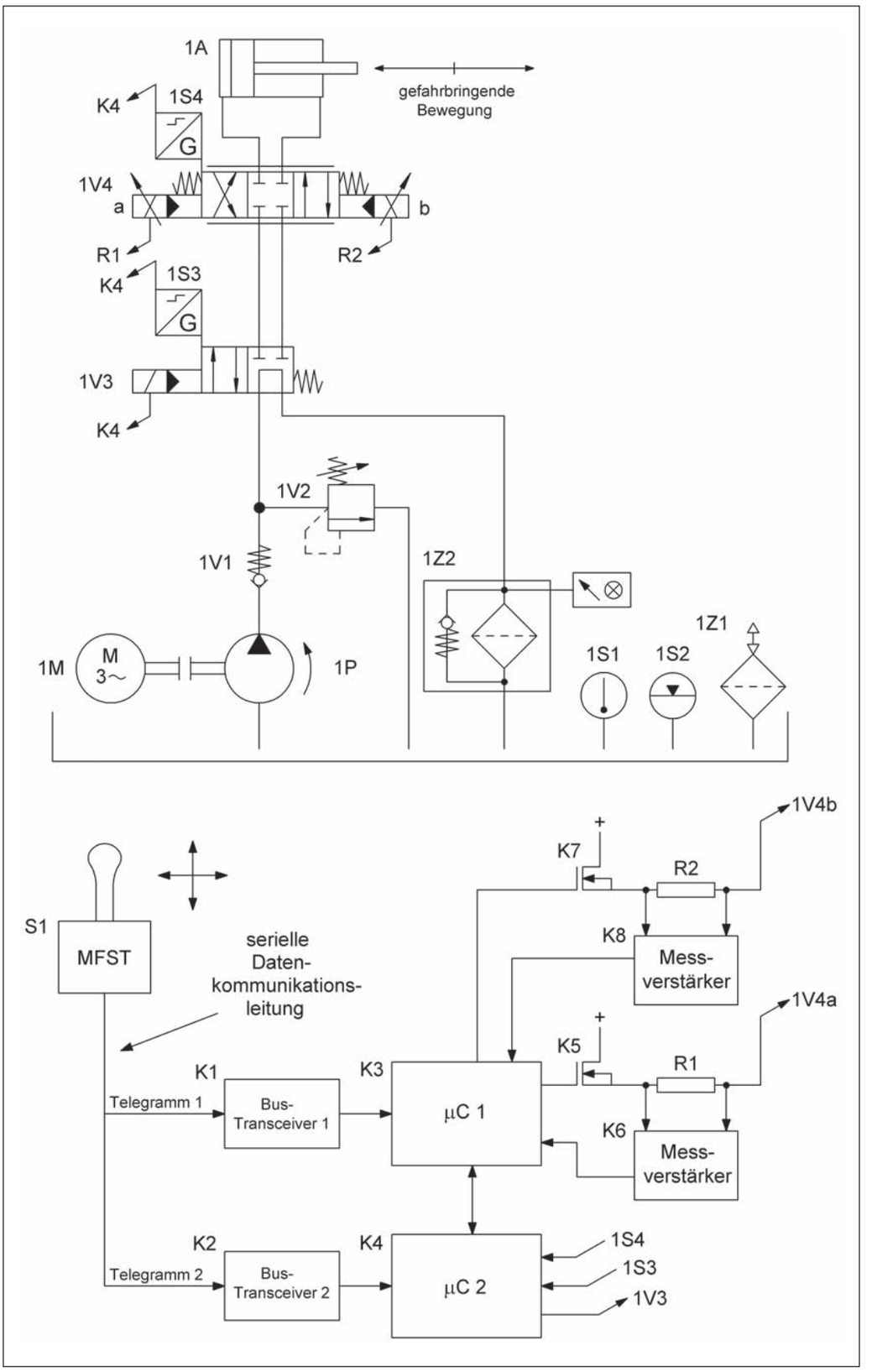
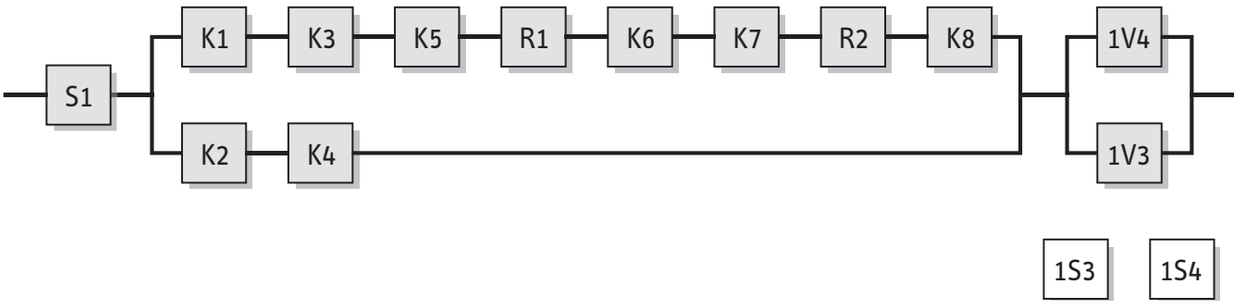


Abbildung 8.27: Ansteuerung von gefahrbringenden Bewegungen einer Erdbaumaschine



Sicherheitsfunktion

- Verhinderung des unerwarteten Anlaufs: Vermeidung unerwarteter Bewegungen der Arbeitsgeräte von Erdbaumaschinen

Funktionsbeschreibung

- Das Multifunktionsstellteil (MFST) S1 wandelt die vom Bediener ausgeführte manuelle Auslenkung des MFST in elektronische Datentelegramme um. Es sendet diese Telegramme zyklisch über eine serielle Datenkommunikationsleitung (Bussystem) zur Logiksteuerung, die Ansteuersignale für die Hydraulik zur Ausführung der vom Bediener vorgesehenen Arbeitsbewegung der Erdbaumaschine erzeugt.

- Das vom MFST S1 gesendete Telegramm 1 gelangt über den Bus-Transceiver K1 in den Mikrocontroller K3. Dieser erzeugt aus Telegramm 1 gemäß den in der Software abgelegten Algorithmen die erforderlichen analogen Signale zur Ansteuerung des Proportionalventils 1V4. Die Widerstände R1/R2 und die Messverstärker K6/K8 dienen zur Regelung der Ausgangsströme für das Proportionalventil. Der Mikrocontroller K4 erhält ein redundantes Telegramm 2 von S1 über den Bus-Transceiver K2. K4 prüft die korrekte Auslenkung des Proportionalventils 1V4 über das in 1V4 integrierte Weg-Messsystem 1S4 auf Plausibilität gegen die aus Telegramm 2 ermittelte Sollstellung. Bei erkannten Fehlern schaltet K4 übergeordnet über ein Wegeventil 1V3 den hydraulischen Druck ab und bringt das System in den sicheren Zustand.

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.

- Bei dem MFST handelt es sich um ein für den Einsatz in PL d geeignetes Sicherheitsbauteil, das der Kategorie 3 entspricht.

- Das Proportionalventil 1V4 und das Wegeventil 1V3 haben eine Sperrstellung bzw. Sperr-Mittelstellung, Federrückstellung bzw. Federzentrierung und eine ausreichend positive Überdeckung.

- Die Programmierung der Software (SRESW) von K3 und K4 erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 6.3.

- Die Datenübertragung vom MFST zur Logiksteuerung ist nach GS-ET-26 bzw. DIN EN 61784-3 abgesichert. Das verwendete Datenkommunikationsprotokoll beinhaltet redundante Telegramme und Maßnahmen, um folgende Übertragungsfehler zu erkennen: Wiederholung, Verlust, Einfügung, falsche Abfolge, Verfälschung und Verzögerung (siehe auch Abschnitt 6.2.17). Die Restfehlerrate Λ ist geringer als $1 \cdot 10^{-8}$/Stunde und trägt damit wie von den Beurteilungsgrundlagen vorgesehen weniger als 1 % zur maximal zulässigen Ausfallwahrscheinlichkeit der Sicherheitsfunktion bei. Dieser geringe Anteil ist in der Berechnung der Gesamtausfallwahrscheinlichkeit vernachlässigbar.

Bemerkung

- Eine eventuell erforderliche Notlauffunktion der Erdbaumaschine ist hier nicht dargestellt und übergeordnet zu realisieren.

Berechnung der Ausfallwahrscheinlichkeit

- Das MFST S1 liegt als handelsübliches Sicherheitsbauteil vor. Die zugehörige Ausfallwahrscheinlichkeit wird am Ende der Berechung addiert ($PFH_{MFST} = 3{,}0 \cdot 10^{-7}$/Stunde [G]). Für den übrigen Steuerungsteil wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.

- $MTTF_d$ der Logiksteuerung: Für die Bus-Transceiver K1 und K2 wird eine $MTTF_d$ von 11 415 Jahren [D] angesetzt. Für die Mikrocontroller K3 und K4 einschließlich ihrer Peripherie wird nach SN 29500-2 eine $MTTF_d$ von 878 Jahren [D] berücksichtigt. Für die restlichen Bauteile werden folgende Kenndaten angesetzt [D]: 45 662 Jahre für die Schalttransistoren K5 und K7, 228 310 Jahre für die Widerstände R1 und R2 und 1 141 Jahre für die Messverstärker K6 und K8. Die $MTTF_d$ der Kanäle beträgt damit 329 Jahre und 815 Jahre. Nach Kürzen auf 100 Jahre ergibt dies einen symmetrisierten $MTTF_d$-Wert von 100 Jahren.

- DC_{avg} der Logiksteuerung: DC = 99 % für K1 und K2 durch Kreuzvergleich der Telegramme in den Mikrokontrollern K3 und K4; DC = 60 % für K3 und K4 durch Kreuzvergleich und Selbsttests einfacher Wirksamkeit durch Software; DC = 90 % für die restlichen Bauteile durch Fehlererkennung in K4 mittels Weg-Messsystem 1S4. Die Mittelungsformel für DC_{avg} ergibt 74 % („niedrig“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung (15) und Umgebungsbedingungen (25 + 10)

- Die Logiksteuerung entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und niedrigem DC_{avg} (74 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}36 \cdot 10^{-8}$/Stunde.

- $MTTF_d$ des hydraulischen Teils der Steuerung: Für das Proportionalventil 1V4 und das Wegeventil 1V3 wird eine $MTTF_d$ von 150 Jahren [N] angesetzt. Nach Kürzen ergibt dies einen symmetrisierten $MTTF_d$-Wert von 100 Jahren.

- DC_{avg} des hydraulischen Teils der Steuerung: DC = 99 % für 1V4 und 1V3 durch direkte Überwachung der Stellung über 1S4 bzw. 1S3 in K4. Die Mittelungsformel für DC_{avg} ergibt 99 % („hoch“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), Verwendung bewährter Bauteile (5), Schutz gegen Überdruck (15) und Umgebungsbedingungen (25 + 10).

- Der hydraulische Teil der Steuerung entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde.

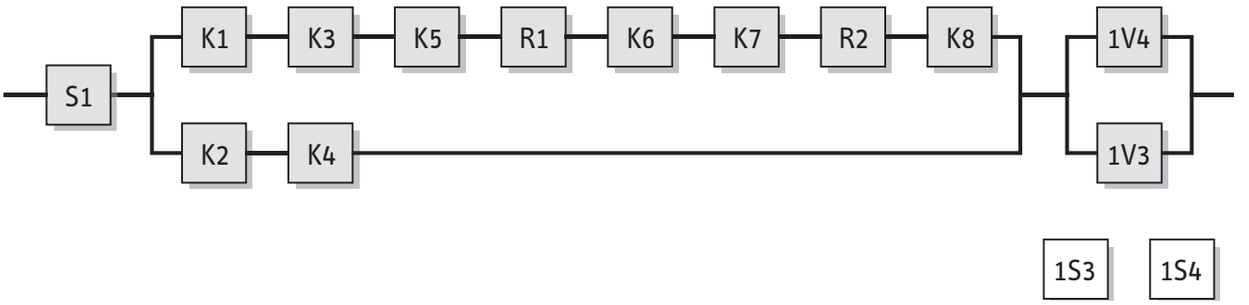
- Die mittlere Wahrscheinlichkeit gefährlicher Ausfälle der Sicherheitsfunktion ergibt sich durch Addition der Anteile des MFST, der Logiksteuerung und des hydraulischen Teils. Die Summe beträgt $3{,}98 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- ISO 15998: Earth-moving machinery – Machine control systems (MCS) using electronic components – Performance criteria and tests (Normentwurf) (11.03). Beuth, Berlin 2003

- DIN EN 61784-3: Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen (IEC 61784-3:2007) (11.08). Beuth, Berlin 2008

- Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten GS-ET-26. Hrsg.: Fachausschuss Elektrotechnik, Köln 2002
  www.dguv.de, Webcode d14884



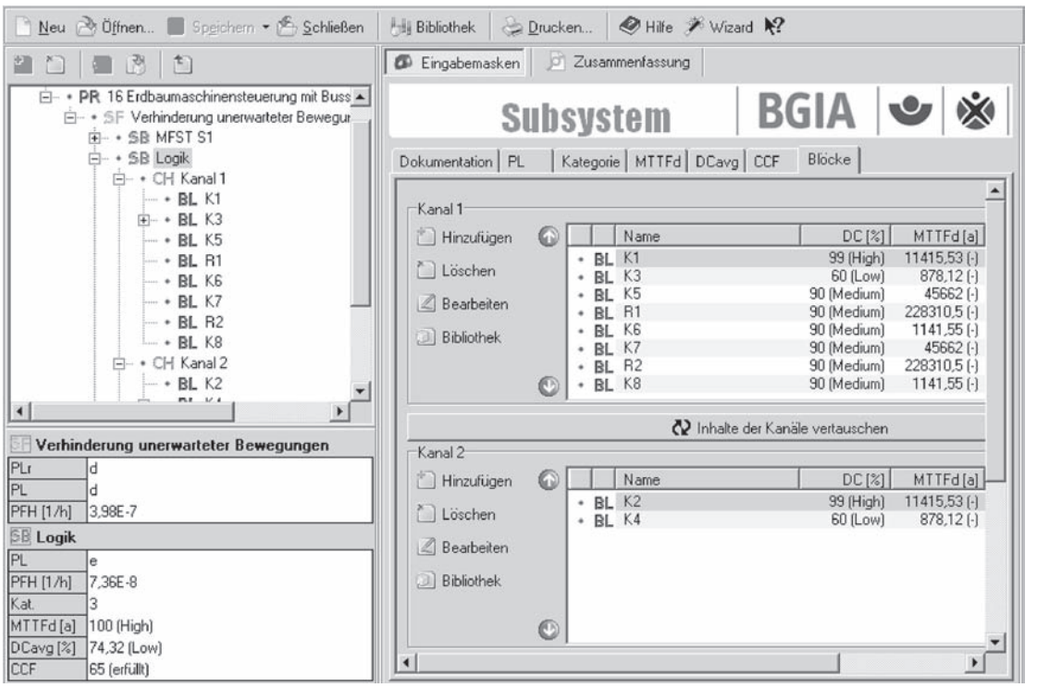


Abbildung 8.28: PL-Bestimmung mithilfe von SISTEMA

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

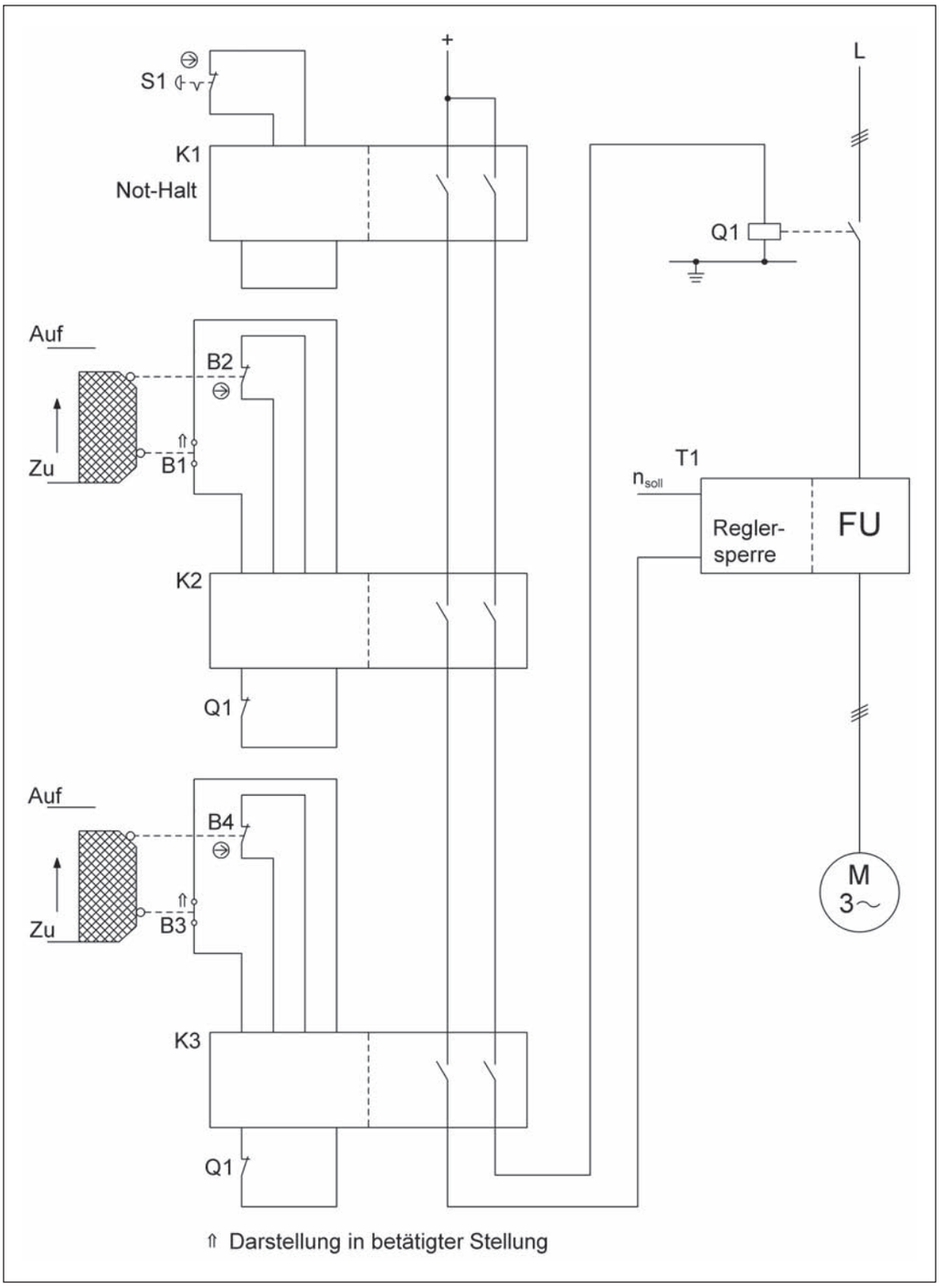
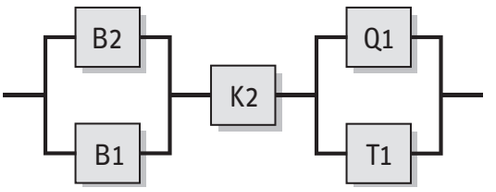


Abbildung 8.29: Kaskadierung von Schutzeinrichtungen mittels Sicherheitsbausteinen (Not-Halt-Funktion, STO)



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“).

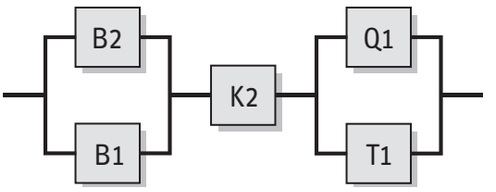
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung der Öffner-Schließer-Kombinationen in K2. Dies entspricht der DC_{avg} für das Subsystem. DC = 99 % für das Schütz Q1 ergibt sich aus der Rücklesung der Kontaktstellung in den Sicherheitsbausteinen. Für den Frequenzumrichter 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.



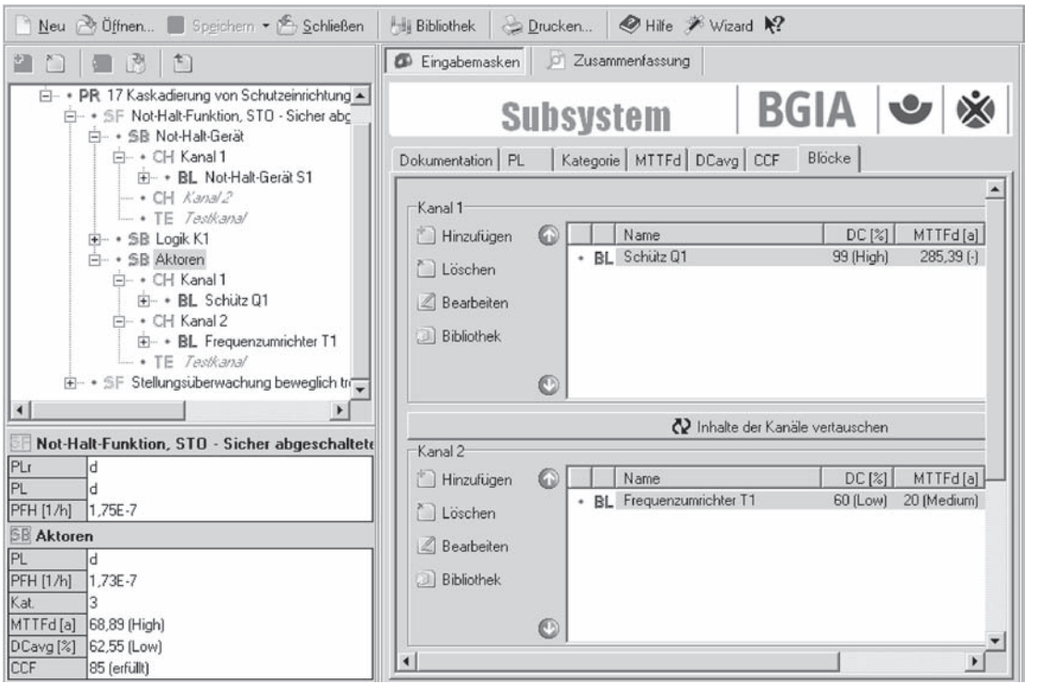


Abbildung 8.30: PL-Bestimmung mithilfe von SISTEMA

8.2.18 Stellungsüberwachung beweglicher trennender Schutzeinrichtungen – Kategorie 3 – PL d (Beispiel 18)

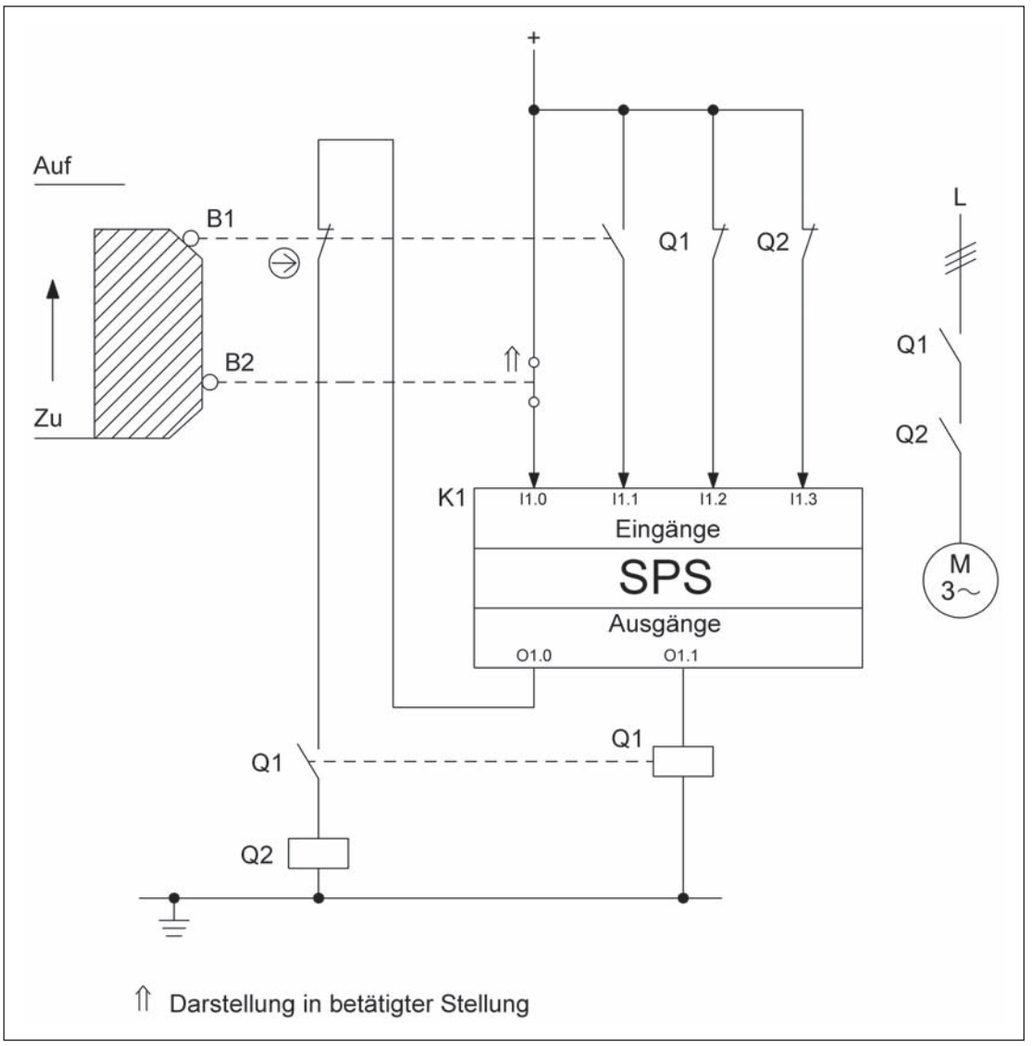


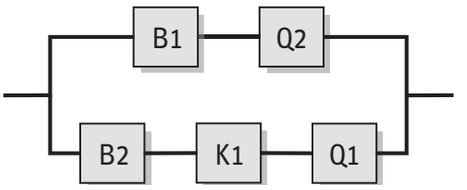
Abbildung 8.31: Redundante Stellungsüberwachung beweglicher trennender Schutzeinrichtung in diversitärer Technologie (elektromechanisch und programmierbar elektronisch)

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der beweglichen trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Das Öffnen der beweglichen trennenden Schutzeinrichtung (z.B. Schutzgitter) wird durch zwei Positionsschalter B1 und B2 in Öffner-Schließer-Kombination erfasst. Der Positionsschalter B1 mit zwangsöffnendem Kontakt steuert ein Schütz Q2 an, durch dessen Abfallen gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert werden. Der Positionsschalter B2 mit Schließerkontakt wird von einer Standard-SPS K1 eingelesen, die über die Ansteuerung eines zweiten Schützes Q1 die gleiche Abschaltreaktion bewirken kann.
- Beim Auftreten eines Bauteilausfalls bleibt die Sicherheitsfunktion erhalten.
- Die Schaltstellung von B1 wird über einen Schließerkontakt ebenfalls in die SPS K1 eingelesen und auf Plausibilität mit der Schaltstellung von B2 verglichen. Die Schaltstellung der Schütze Q1 und Q2 wird ebenfalls über zwangsgeführte Rücklesekontakte in K1 überwacht. Bauteilausfälle in B1, B2, Q1 und Q2 werden durch K1 erkannt und führen durch das Abfallen von Q1 und Q2 zur Betriebshemmung. Fehler in der SPS K1 werden nur über die Funktion erkannt (Fehlererkennung durch den Prozess).



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 Schutzeinrichtung zur Betätigung der Positionsschalter ist sichergestellt.
- B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern sind getrennt verlegt, oder es erfolgt eine geschützte Leitungsverlegung.
- Störungen im Anfahr- und Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschieden betätigten Positionsschaltern (Öffner und Schließer) erkannt.
- Q1 und Q2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die programmierbare SPS K1 erfüllt die normativen Anforderungen gemäß Abschnitt 6.3.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für den Positionsschalter B1 ist ein Fehlerausschluss für den zwangsöffnenden elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt von Positionsschalter B2 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B1 und B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 1 Stunde Zykluszeit ist für diese Komponenten n_{op}= 5 840 Zyklen/Jahr und $MTTF_d$ beträgt 1 712 Jahre für B1 bzw. 856 Jahre für B2. Für die Schütze Q1 und Q2 entspricht bei induktiver Last (AC3) der B_{10}-Wert der elektrischen Lebensdauer von 1 300 000 Schaltspielen [H]. Bei Annahme von 50 % gefahrbringenden Ausfällen ergibt sich der B_{10d}-Wert durch Verdoppelung des B_{10}-Wertes. Mit dem oben angenommenen Wert für n_{op} ergibt sich für Q1 und Q2 eine $MTTF_d$ von 4 452 Jahren. Für die SPS wird ein MTTF-Wert von 15 Jahren [H] angesetzt, aus dem sich durch Verdoppelung ein $MTTF_d$-Wert von 30 Jahren ergibt. Die Kombination von B1 und Q2 ergibt $MTTF_d$ = 1 236 Jahre für den ersten Kanal, B2, K1 und Q2 tragen zur $MTTF_d$ = 28 Jahre im zweiten Kanal bei. Insgesamt ergibt sich über beide Kanäle ein symmetrisierter $MTTF_d$-Wert pro Kanal von 70 Jahren („hoch“).
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung beider Schaltzustände in der SPS K1. DC = 99 % für die Schütze Q1 und Q2 ergibt sich aus der Rücklesung über zwangsgeführte Kontaktelemente ebenfalls in K1. Für K1 wird wegen der möglichen Fehlererkennung durch den Prozess DC = 60 % angenommen. Durch Mittelung ergibt sich damit ein DC_{avg} von 62 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_d$ (70 Jahre) und niedrigem DC_{avg} (62 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}66 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

8.2.19 Verriegelungseinrichtung mit Zuhaltung – Kategorie 3 – PL d (Beispiel 19)

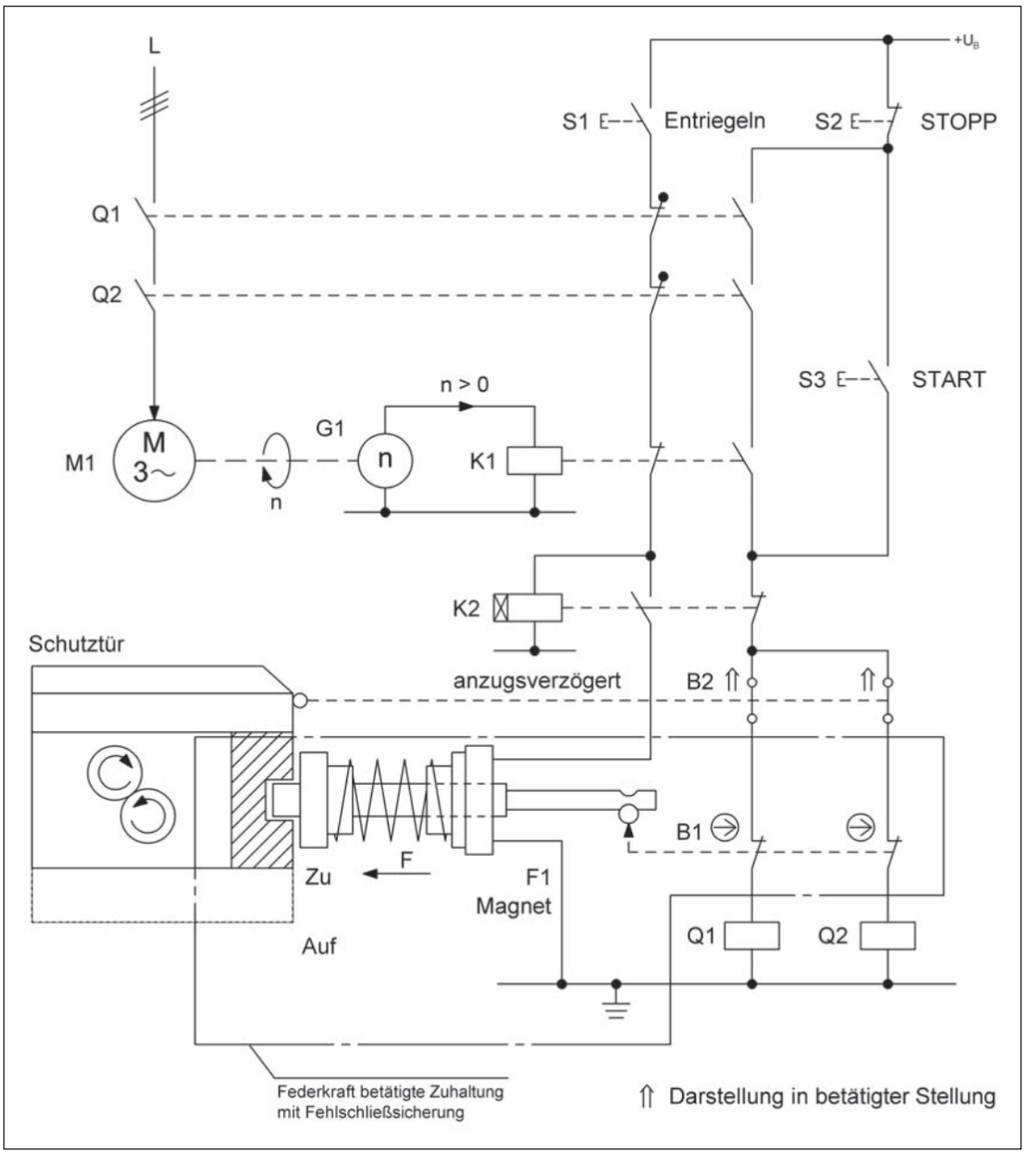


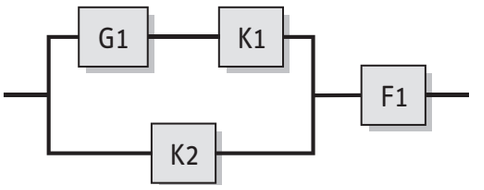
Abbildung 8.32: Zuhaltung einer Schutztür in kontaktbehafteter Technik – Kategorie 3

Sicherheitsfunktionen

- Kein Entriegeln der Zuhaltung bei Drehzahl größer Null
- Verhindern eines unerwarteten Anlaufs aus dem Stillstand bei geöffneter Schutztür

Funktionsbeschreibung

- Der Zugang zu einer gefahrbringenden Bewegung wird durch eine Schutztür mit Zuhaltung solange versperrt, bis die Bewegung zum Stillstand gekommen ist. Das Schließen der Tür erfolgt durch formschlüssiges federkraftbetätigtes Einrücken eines Sperrbolzens, der zum Öffnen elektromagnetisch gezogen wird. Die Stellung des Sperrbolzens wird über den integrierten Positionsschalter B1 überwacht, die Stellung der Schutztür zusätzlich zur Erhöhung der Manipulationssicherheit über den Positionsschalter B2. Die Verriegelungseinrichtung mit integrierter federkraftbetätigter Zuhaltung besitzt zusätzlich eine Fehlschließsicherung.



- Die gefahrbringende Bewegung kann nur bei geschlossener Schutztür und per Federkraft eingerücktem Sperrbolzen über den Starttaster S3 in Gang gesetzt werden. Der Positionsschalter B1 ist dann entlastet, Positionsschalter B2 ist betätigt. Damit sind die Öffnerkontakte von B1 geschlossen, ebenso die Schließerkontakte von B2. Ihre Reihenschaltung gibt die Ansteuerung für die Motorschütze Q1 und Q2 frei. Das sicherheitsbezogene Blockdiagramm für die Sicherheitsfunktion „Verhindern eines unerwarteten Anlaufs aus dem Stillstand bei geöffneter Schutztür“ (hier nicht dargestellt) besteht daher bei Vereinfachung zur sicheren Seite aus zwei redundanten Kanälen B1-Q1 und B2-Q2. Alternativ kann B1-Q2 und B2-Q1 gewählt werden. Ergeben sich aus diesen beiden Modellen unterschiedliche Werte der $MTTF_d$ pro Kanal, kann für die Bestimmung der Ausfallwahrscheinlichkeit der höhere $MTTF_d$-Wert verwendet werden.

- Das Öffnen der Schutztür während der gefahrbringenden Bewegung ist durch die Einbindung je eines Öffnerkontaktes (Spiegelkontaktes) der Schütze Q1, Q2 und des auf der Drehzahlinformation des Tachogenerators G1 basierenden Stillstandswächters K1 sowie des Schließerkontaktes des anzugsverzögerten Schützes K2 im Ansteuerkreis des Magneten F1 einfehlersicher verhindert.

- Ein Öffnen der Schutztür während des Austrudelns des Motors nach Betätigen des Stopptasters S2 und des Entriegelungstasters S1 ist durch die Einbindung des Öffnerkontaktes des Stillstandswächters K1 (basierend auf der Drehzahlinformation von G1) und des Schließerkontaktes des anzugsverzögerten Schützes K2 im Ansteuerkreis des Magneten F1 einfehlersicher verhindert (siehe sicherheitsbezogenes Blockdiagramm).

- Mit dem Betätigen der Entriegelungstaste S1 wird nach dem Stillstand des Motors (Q1, Q2 und K1 abgefallen) das anzugsverzögerte Schütz K2 angesteuert, der Magnet F1 aktiviert und damit der Sperrbolzen aus der Schutztür gezogen. Der Positionsschalter B1 verbleibt während der geöffneten Schutztür manipulationssicher formschlüssig zwangläufig betätigt. Ein unerwarteter Anlauf aus dem Stillstand wird auch über den Positionsschalter B2 (unbetätigt) verhindert.

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 Leitungen sind im elektrischen Einbauraum verlegt oder in getrennten Mantelleitungen ausgeführt.

- Die Hilfsschütze K1 und K2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.

- Die Schütze Q1 und Q2 besitzen Spiegelkontakte entsprechend DIN EN 60947-4-1, Anhang F.

- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt.

- Der Positionsschalter B1 ist ein zwangsöffnender Positionsschalter entsprechend DIN EN 60947-5-1, Anhang K.

- Die in der Schaltung vorgesehene Verriegelungseinrichtung (in Abbildung 8.32 gestrichelt dargestellt) enthält – in einem Gehäuse untergebracht und damit von außen nicht zugänglich – sowohl die Zuhaltung mit dem federrückgestellten Entriegelungsmagneten als auch den zur Stellungsüberwachung des Sperrbolzens und der Schutztür notwendigen Positionsschalter B1.

- Die Feder der Zuhaltung ist eine bewährte Feder nach DIN EN ISO 13849-2, Anhang A.3. Außerdem ist die Feder dauersicher nach DIN EN 13906-1. Die Kriterien nach GS-ET-19, Abschnitt 5.5.1, werden eingehalten. Der Magnet F1 zieht ohne Spannung nicht an, sodass bei gleichzeitigem Fehlerausschluss für die Fehlerannahme „Bruch des Sperrmittels“ für diese Elemente insgesamt ein Fehlerausschluss in Bezug auf gefahrbringende Fehler erfolgt.

- Die Fehlschließsicherung der Zuhaltung stellt konstruktiv sicher, dass der Sperrbolzen bei geöffneter Schutztür nicht die Sperrstellung (Zuhaltestellung) einnehmen kann.

- In Abbildung 8.32 sind nicht gezeichnet die in einer Zuhaltung zusätzlich integrierbaren Funktionen „Fluchtentriegelung“ und „Notentsperrung“ zum gewollten handbetätigten Öffnen der Schutzeinrichtung im Gefahrenfall – ohne Hilfsmittel und unabhängig vom Betriebszustand jeweils zwangläufig auf das Sperrmittel wirkend, siehe hierzu Prüfgrundsätze GS-ET-19.

- Die Standardkomponente G1 wird nach den Hinweisen in Abschnitt 6.3.10 eingesetzt.

Berechnung der Ausfallwahrscheinlichkeit

Zunächst wird die Wahrscheinlichkeit der ungewollten Aufhebung der Zuhaltung bzw. der Sicherheitsfunktion „Kein Entriegeln der Zuhaltung bei Drehzahl größer Null“ (siehe auch sicherheitsbezogenes Blockdiagramm) berechnet.

- $MTTF_d$: Für K1 und K2 gilt der B_{10d}-Wert von 400 000 Zyklen [N]. Bei 240 Arbeitstagen, 8 Arbeitsstunden und 10 Minuten Zykluszeit ist für diese Komponenten n_{op} = 11 520 Zyklen/Jahr und $MTTF_d$ = 347 Jahre. Für den elektronischen Teil der Anzugsverzögerung in K2 wird eine $MTTF_d$ von 1 000 Jahren angenommen [G], sodass K2 insgesamt eine $MTTF_d$ von 257 Jahren besitzt. Für G1 liegt keine Herstellerangabe vor, es wird eine $MTTF_d$ von 30 Jahren angenommen [G]. Diese Werte ergeben eine symmetrisierte $MTTF_d$ pro Kanal von 70 Jahren.

- DC_{avg}: Fehlerhafte Zustände von K1 oder K2 führen aufgrund der Zwangsführung der Kontakte zu einem dauerhaften Ausfall der Entriegelung der Zuhaltung oder der Motorenergie, sodass eine Fehlererkennung durch den Prozess gegeben ist und ein *DC* von 99 % angenommen wird. Eine Drift der Schaltschwelle von G1 kann durch den Prozess erkannt werden, sodass ein *DC* von 60 % angenommen wird. Für den Ausfall der Anzugsverzögerung von K2 ist keine Fehlererkennung gegeben. Dies ergibt einen DC_{avg} von 57 %, der im Toleranzbereich von „niedrig“ liegt.

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15), Verwendung bewährter Bauteile (5) und Umgebungsbedingungen (25 + 10)

- Bei gleichzeitigem Fehlerausschluss für die weiteren Elemente der Zuhaltung (siehe oben) entspricht die Kombination der Steuerungselemente Kategorie 3 mit hoher $MTTF_d$ pro Kanal (70 Jahre) und niedrigem DC_{avg} (57 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}83 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Die Berechnung der Wahrscheinlichkeit für die Sicherheitsfunktion „Verhindern eines unerwarteten Anlaufs aus dem Stillstand bei geöffneter Schutztür“ führt zu folgendem Ergebnis.

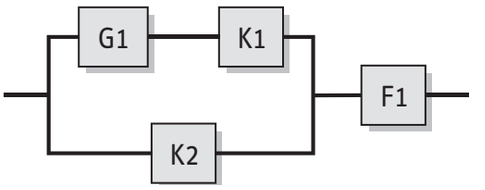
- $MTTF_d$: Für den Positionsschalter B1 wird aufgrund der Zwangsöffnung ein B_{10d}-Wert von 20 000 000 Zyklen [N] angenommen. Mit der oben angenommenen n_{op} = 11 520 Zyklen/Jahr beträgt der zugehörige $MTTF_d$-Wert 17 361 Jahre. Für den Positionsschalter B2 wird ein B_{10d}-Wert von 100 000 Zyklen [G] (siehe auch Tabelle D.2) angenommen, der zugehörige $MTTF_d$-Wert beträgt 86 Jahre. Für Q1 und Q2 gilt der B_{10d}-Wert von 400 000 Zyklen [N]. Mit der gleichen n_{op} ergibt sich jeweils eine $MTTF_d$ von 347 Jahren. Diese Werte ergeben eine symmetrisierte $MTTF_d$ pro Kanal von 85 Jahren.

- DC_{avg}: Fehlerhafte Zustände aller Elemente werden bei der angenommenen hohen Schalthäufigkeit jeweils mit einem *DC* von 99 % z.B. über Fehlererkennung durch den Prozess erkannt, was somit auch zu einem DC_{avg} von 99 % führt.

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): siehe oben

- Die Kombination der Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_d$ pro Kanal (85 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}93 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Damit ist der PL_r = d übertroffen, was bei erforderlicher zweikanaliger Ausführung der Hardware mit wenigen Bauteilen, der Verwendung von B_{10d}-Werten nach Norm, einem *DC* von „hoch“ sowie einer „moderaten“ Schalthäufigkeit nahezu immer der Fall sein wird.

- Das verschleißbehaftete Element B2 sollte nach jeweils ca. 8 Jahren (T_{10d}) ausgetauscht werden.



Weiterführende Literatur

- *Reudenbach, R.:* Maßnahmen gegen das Umgehen von Verriegelungseinrichtungen an Schutztüren. die BG 2003 Nr. 7, S. 275-281
  www.diebg.info/download/reudenbach.pdf
- *Lüken, K., et al.*: Manipulation von Schutzeinrichtungen an Maschinen. HVBG-Report. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2006
  www.dguv.de/bgia, Webcode d6303
- GS-ET-19: Grundsätze für die Prüfung und Zertifizierung von Verriegelungseinrichtungen mit elektromagnetischen Zuhaltungen (4/04)
  www.dguv.de, Webcode d14884
- BGI 575: Merkblatt für die Auswahl und Anbringung elektromechanischer Verriegelungseinrichtungen für Sicherheitsfunktionen. Carl Heymanns, Köln 2003
- DIN EN 1088: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl (02.96). Beuth, Berlin 1996
- DIN EN 1088/A1: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl (07.07). Beuth, Berlin 2007
- DIN EN 13906-1: Zylindrische Schraubenfedern aus runden Drähten und Stäben – Berechnung und Konstruktion – Teil 1: Druckfedern (07.02). Beuth, Berlin 2002

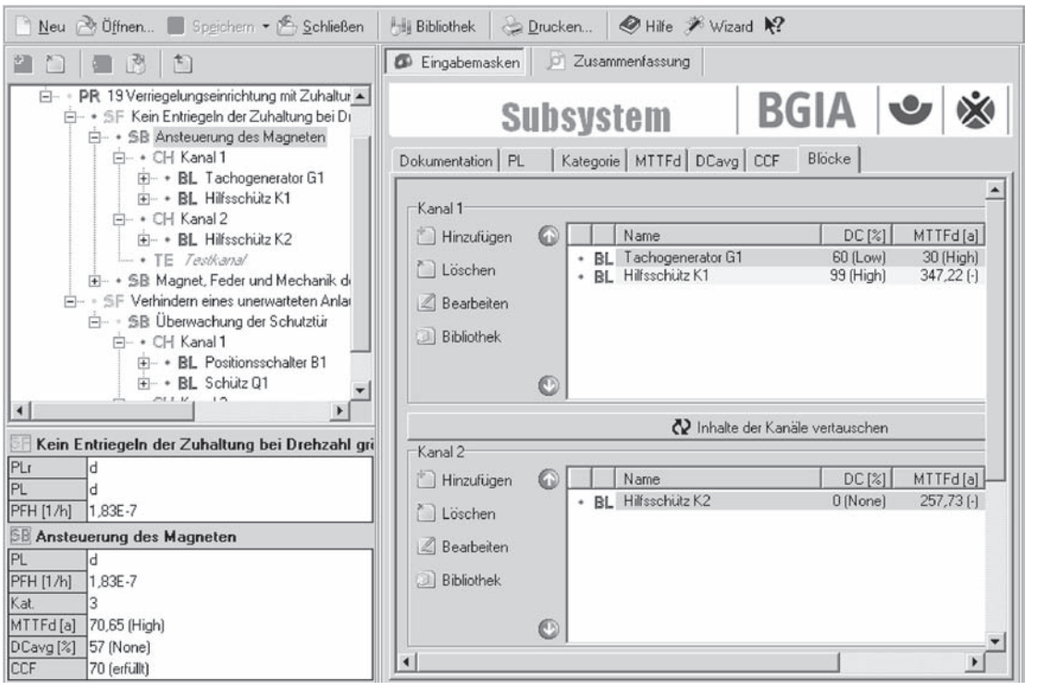


Abbildung 8.33: PL-Bestimmung mithilfe von SISTEMA

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

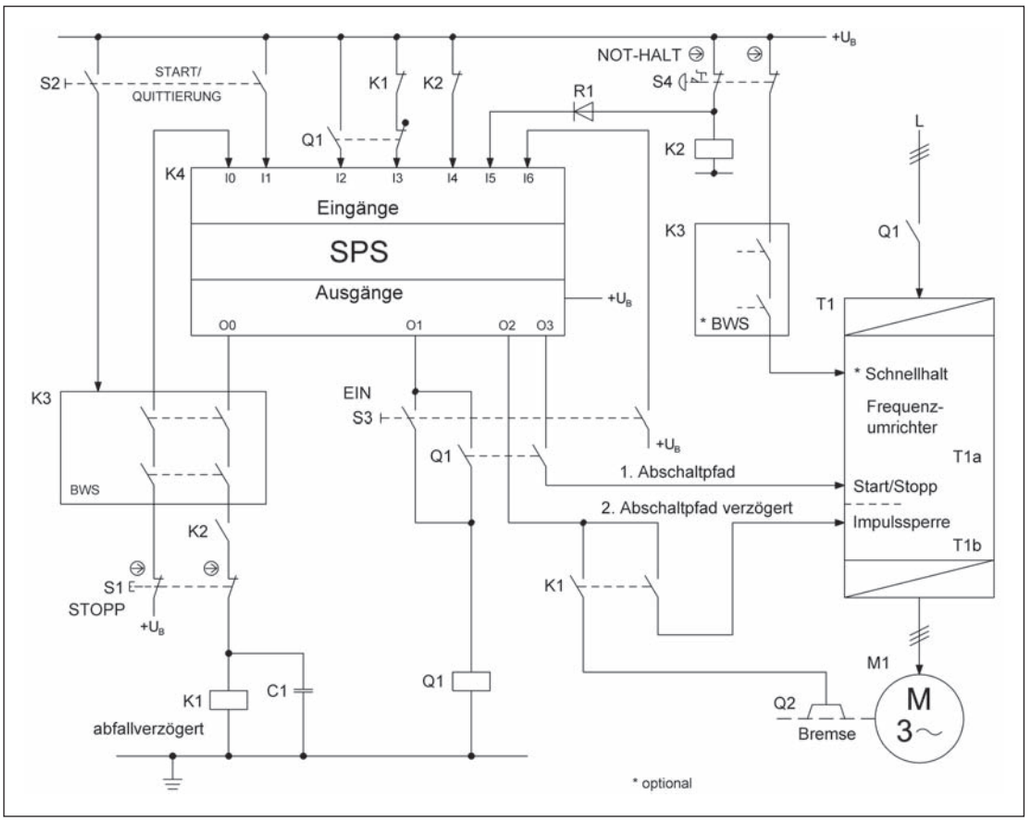


Abbildung 8.34: Sicheres Stillsetzen eines SPS-gesteuerten Frequenzumrichter-Antriebs nach einem Stopp- oder Not-Halt-Befehl oder nach dem Ansprechen einer Schutzeinrichtung (hier: BWS)

Sicherheitsfunktion

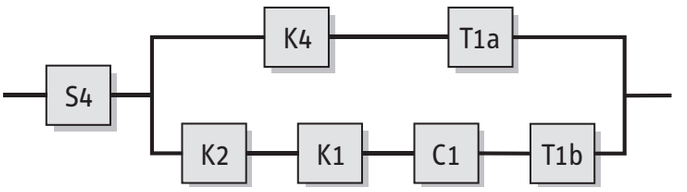
- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Nach einem Stopp- oder Not-Halt-Befehl oder nach dem Ansprechen einer Schutzeinrichtung wird der Antrieb angehalten (SS1 – Sicherer Stopp 1).

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

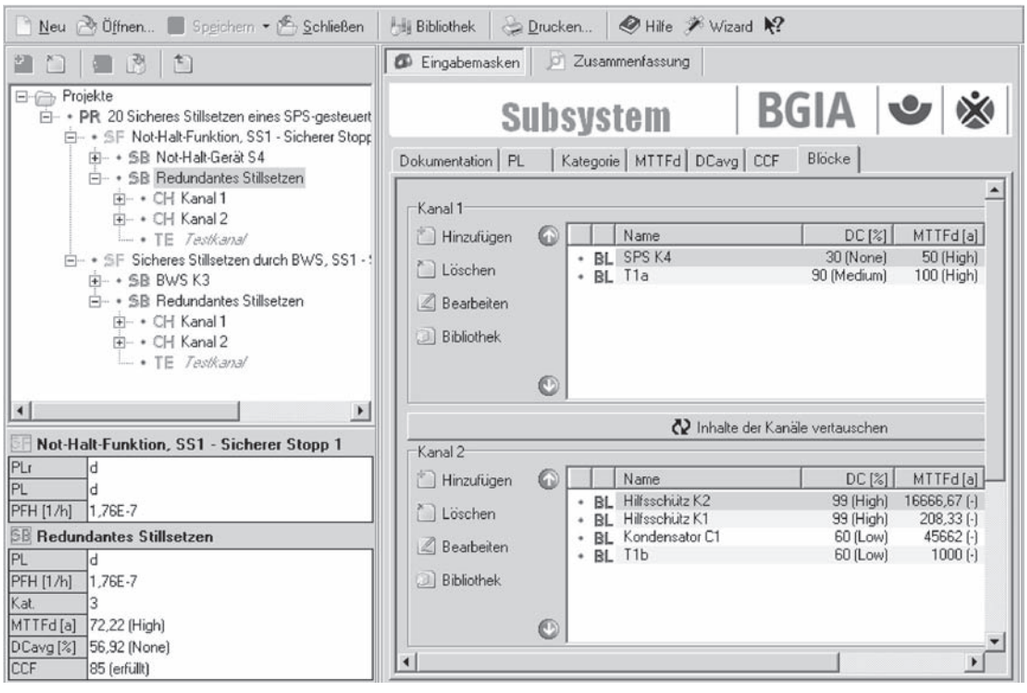


Abbildung 8.35:
PL-Bestimmung mithilfe von SISTEMA

8.2.21 Sicher begrenzte Geschwindigkeit für Tippbetrieb – Kategorie 3 – PL d (Beispiel 21)

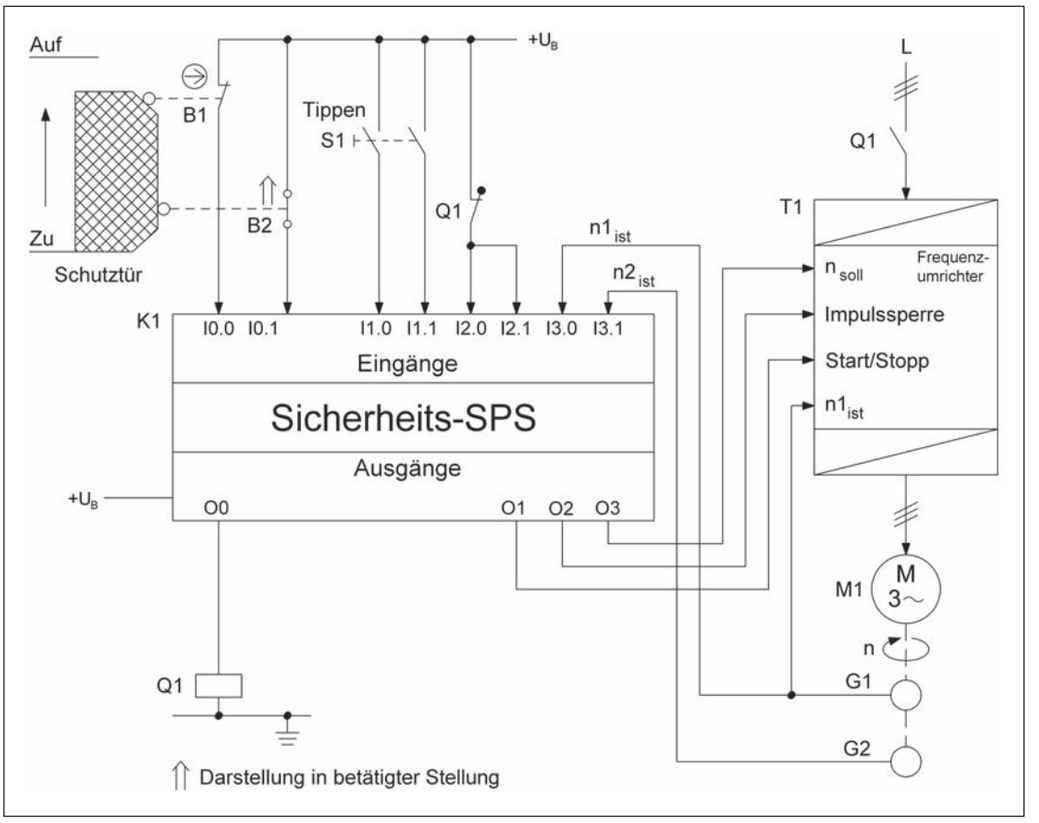


Abbildung 8.36: Tippbetrieb mit sicher begrenzter Geschwindigkeit bei geöffneter Schutztür, mit Soll-/Ist-Vergleich und Drehzahl-Grenzwertvorgabe innerhalb einer Sicherheits-SPS

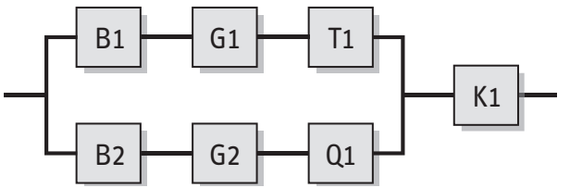
Sicherheitsfunktion

- Sicher begrenzte Geschwindigkeit (SLS): Bei geöffneter Schutztür wird das Überschreiten einer zulässigen Drehzahl im Tipp-Betrieb verhindert.

Funktionsbeschreibung

- Eine gefahrbringende Bewegung wird bei geöffneter Schutztür sicher verhindert oder unterbrochen. Das Öffnen der Schutztür wird über zwei Positionsschalter B1 und B2 in Öffner-Schließer-Kombination erfasst. Bei betätigtem Taster S1 wird mithilfe der Sicherheits-SPS K1 eine sicher begrenzte Geschwindigkeit am Frequenzumrichter T1 eingestellt. Beide Verarbeitungskanäle innerhalb der SPS erhalten jeweils über ihre Anwendersoftware voneinander unabhängige Soll-Grenzwert-Vorgaben. Die Überwachung der Ist-Drehzahl der begrenzten Geschwindigkeit an den Eingängen I3.0 und I3.1 von K1 erfolgt über zwei separate Tachogeneratoren G1 und G2. Jeder Kanal der SPS führt unabhängig den Soll-/Ist-Vergleich durch. Schlägt die über T1 geregelte Reduzierung der Drehzahl auf den begrenzten Wert fehl, so kann K1 über Sperrung des Start-/Stopp-Signals und der Impulssperre am Umrichter einen Stillstand einleiten. Zusätzlich kann über ein Netzschütz Q1 die Energieversorgung zu T1 getrennt werden.

- Über eine intern in der Sicherheits-SPS K1 vorhandene Schnittstelle werden sicherheitsrelevante Daten ausgetauscht, z.B. zwecks Fehlererkennung durch Zustandsvergleich der beiden Verarbeitungskanäle. Versagt ein Verarbeitungskanal, so erfolgt die Abwärtssteuerung des Umrichters T1 sowie des Netzschützes Q1 jeweils durch den anderen noch funktionierenden Verarbeitungskanal. Ein Versagen des Umrichters, das z.B. zum unerwarteten Anlaufen, zum Weiterlaufen oder zu einer Erhöhung der Drehzahl führen kann, wird über die getrennte Erfassung der Drehzahlen durch die Tachogeneratoren G1 und G2 in beiden Verarbeitungskanälen erkannt. Das Nichtabfallen des Netzschützes Q1 wird über den in beide Verarbeitungskanäle geführten Öffnerkontakt (Eingänge I2.0 und I2.1 von K1) bemerkt und führt sowohl zur Sperrung des Start/Stopp-Signals als auch der Impulssperre am Umrichter durch beide Verarbeitungskanäle.



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 Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt.
- Der Positionsschalter B1 ist zwangsöffnend entsprechend DIN EN 60947-5-1, Anhang K, ausgeführt. Der Positionsschalter B2 entspricht ebenfalls DIN EN 60947-5-1.
- Das Schütz Q1 besitzt einen Spiegelkontakt entsprechend DIN EN 60947-4-1, Anhang F.
- Die Anschlussleitungen der Positionsschalter sind entweder getrennt oder gegen mechanische Beschädigung geschützt verlegt.
- Für die Sicherheitsfunktion „Sicher begrenzte Geschwindigkeit“ wird ein Fehlerausschluss für den Fehler Geberwellenbruch (G1/G2) angenommen. Einzelheiten zur Möglichkeit eines Fehlerausschlusses gibt z.B. IEC 61800-5-2, Tabelle D.16.
- Die Standardkomponenten G1 und G2 (soweit für die Drehgeber zutreffend) und T1 werden entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.
- Das Sicherheitsbauteil K1 erfüllt alle Anforderungen für Kategorie 3 und PL d. Die Programmierung der Software (SRASW) erfolgt entsprechend den Anforderungen für PL d und den Hinweisen in Abschnitt 6.3.
- Es wird davon ausgegangen, dass die Ausgänge der Sicherheits-SPS jeweils von beiden Verarbeitungskanälen der SPS angesteuert werden (Ausnahme O3).

Bemerkungen

- Nach DIN EN 1010-1 genügt bei Maschinen ohne betriebsmäßig regelmäßigen Eingriff in Gefahrstellen auch der Einsatz eines zwangsöffnenden Positionsschalters nach DIN EN 60947-5-1, Anhang K, je trennender verriegelter Schutzeinrichtung. Für den Fehlerausschluss in diesem Zusammenhang ist die Installation des Schalters nach DIN EN 60204-1 Bedingung.
- Für die vollständige Realisierung des Tippbetriebs ist zusätzlich die Sicherheitsfunktion „Kein unerwarteter Anlauf im Tippbetrieb“ zu betrachten.

Berechnung der Ausfallwahrscheinlichkeit

- Der SRP/CS wird in die beiden Subsysteme Sensor/Aktor und SPS unterteilt. Für das Teilsystem SPS wird eine geprüfte, für PL d taugliche Sicherheits-SPS eingesetzt, deren Ausfallwahrscheinlichkeit $1{,}5 \cdot 10^{-7}$/Stunde [G] am Ende der Berechnung für das Subsystem Sensor/Aktor addiert wird. Zur Aufstellung des Blockdiagramms siehe auch Abbildung 6.14 und entsprechende Hinweise im zugehörigen Text. Nachfolgend wird die Ausfallwahrscheinlichkeit für das Teilsystem Sensor/Aktor berechnet.
- $MTTF_d$: Bei 240 Arbeitstagen, 8 Arbeitsstunden und einer Stunde Zykluszeit beträgt n_{op} = 1 920 Zyklen/Jahr. Für den Positionsschalter B1 wird aufgrund der Zwangsöffnung ein B_{10d}-Wert von 20 000 000 Zyklen [N] angenommen, der zugehörige $MTTF_d$-Wert beträgt 104 116 Jahre. Für B2 wird aufgrund des definierten Steuerstroms (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend) ein B_{10d}-Wert von 1 000 000 Zyklen [G] angenommen (siehe auch Tabelle D.2) und damit eine $MTTF_d$ = 5 208 Jahre. Das Schütz Q1 mit B_{10d}-Wert von 400 000 Zyklen schaltet betriebsmäßig nur einmal täglich, entsprechend n_{op} = 240 Zyklen/Jahr und $MTTF_d$ = 16 667 Jahre. Folgende Werte werden geschätzt: Für T1 $MTTF_d$ = 100 Jahre und für G1/G2 $MTTF_d$ = 50 Jahre [G]. Diese Werte ergeben eine symmetrisierte $MTTF_d$ pro Kanal von 41 Jahren („hoch“).

- DC_{avg}: Für die verwendeten Komponenten wird jeweils ein *DC* = 99 % angenommen. Dieser basiert für die Positionsschalter und die Tachogeneratoren auf einem Kreuzvergleich von Eingangssignalen in K1. Für den Umrichter T1 erfolgt eine Fehlererkennung durch den Prozess, für das Netzschütz Q1 erfolgt eine direkte Überwachung über die SPS. Diese Werte ergeben einen DC_{avg} von 99 % („hoch“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Das Subsystem Sensor/Aktor entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (41 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}56 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Der PL_r = d wird übertroffen, was bei erforderlicher zweikanaliger Ausführung der Hardware mit wenigen Bauteilen und der Verwendung von B_{10d}-Werten nach Norm, einem *DC* von „hoch“ sowie einer „moderaten“ Schalthäufigkeit nahezu immer der Fall sein wird.

- Die Gesamtausfallwahrscheinlichkeit wird durch Addition der Wahrscheinlichkeit gefährlicher Ausfälle von K1 ($1{,}5 \cdot 10^{-7}$/Stunde) ermittelt und beträgt $2{,}16 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- *Grigulewitsch, W.; Reinert, D.:* Schaltungsbeispiele mit programmierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. Kennzahl 330 227. 27. Lfg. I/95. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.
www.bgia-handbuchdigital.de/330227

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

- DIN EN 1010-1: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 1: Allgemeine Anforderungen (03.05). Beuth, Berlin 2005

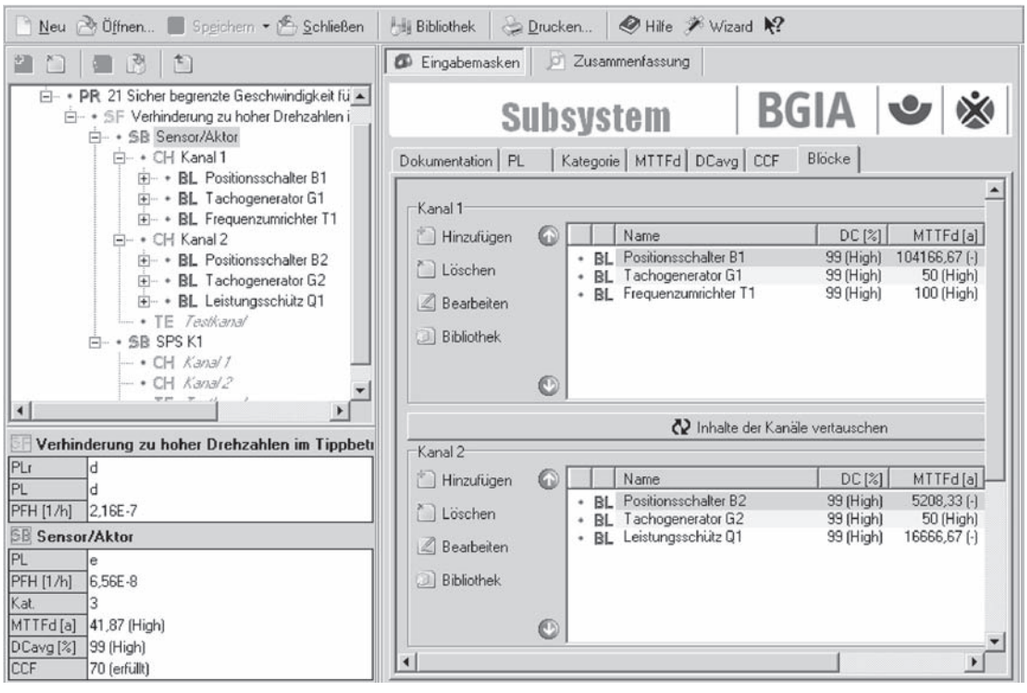


Abbildung 8.37: PL-Bestimmung mithilfe von SISTEMA

8.2.22 Muting einer Schutzeinrichtung – Kategorie 3 – PL d (Beispiel 22)

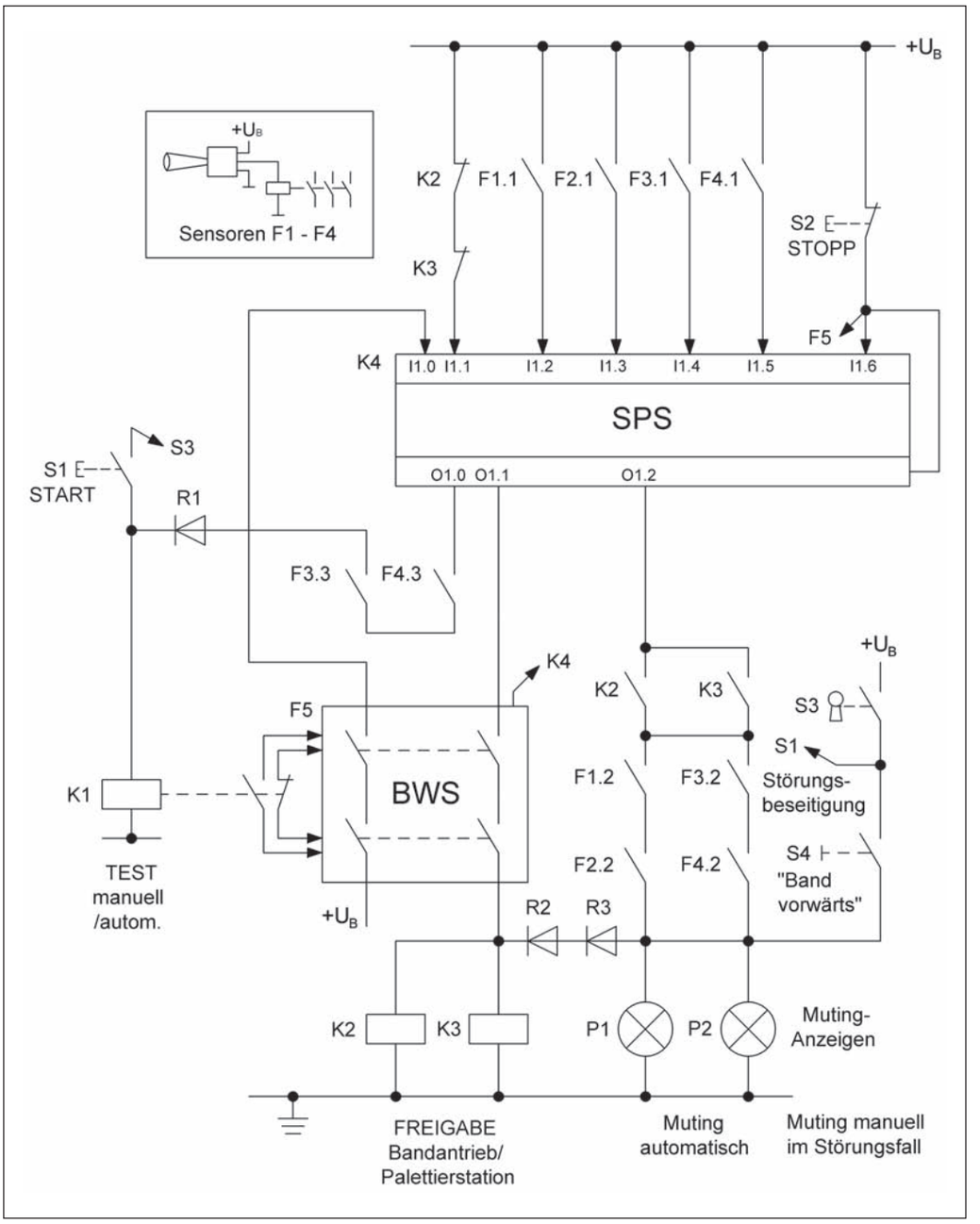
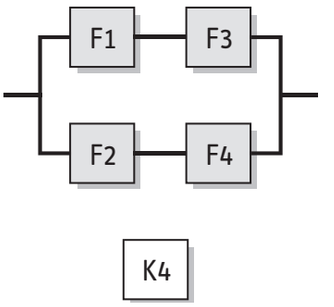


Abbildung 8.38: Überbrückung einer Schutzeinrichtung am Auslauf einer SPS-gesteuerten Palettieranlage

Sicherheitsfunktion

- Mutingfunktion: Zeitlich begrenzte, prozessabhängige Überbrückung einer Schutzeinrichtung. Weitere Sicherheitsfunktionen wie zum Beispiel die Absicherung des Zugangs zur Palettieranlage oder die Anlauf-/Wiederanlaufsperre sind im Folgenden nicht detailliert behandelt.



Funktionsbeschreibung

- Der Zugang am Auslauf der Palettieranlage wird durch eine dreistrahlige Lichtschranke (BWS) F5 des Typs 4 nach DIN EN 61496 abgesichert. Diese enthält die zusätzlichen Funktionen Anlaufsperre und Wiederanlaufsperre, die mithilfe von zwei antivalenten Eingängen realisiert sind. Das Aufheben der Anlaufsperre der Lichtschranke ist an den Startbefehl des Bandantriebs bzw. an das Einschalten der Palettierstation gekoppelt und wird ausgelöst durch den Anzug und nachfolgenden Abfall des Hilfsschützes K1 entsprechend dem Betätigen und Loslassen des Starttasters S1. Voraussetzung für einen gültigen Startbefehl ist das Abgefallensein der Hilfsschütze K2 und K3 (abgefragt über Eingang I1.1) und die Aufhebung der Anlaufsperre (abgefragt über Eingang I1.0). Als Folge wird Ausgang O1.1 gesetzt.

- Zur Steuerung des Überbrückungsvorgangs sind vier Infrarot-Lichttaster F1 bis F4 (zur Anordnung siehe auch Abbildung 8.39) eingebunden. Über die Eingänge I1.2 bis I1.5 überwacht die SPS die Betätigungsabfolge der vier Infrarot-Lichttaster über deren Kontakte F1.1 bis F4.1 unter Berücksichtigung von zwei hinterlegten Zeitvorgaben. Die Überbrückungsfunktion ist allein im Ausgangsstromkreis der SPS (Ausgang O1.2) realisiert, unabhängig vom Ausgangsstromkreis der Lichtschranke F5. Die in Reihe geschalteten Überbrückungskontakte F1.2 und F2.2 sowie F3.2 und F4.2 sind jeweils über die Dioden R2 und R3 mit der über die Hilfsschütze K2 und K3 realisierten „Freigabe“ durch ODER-Verknüpfung verbunden.

- R2 und R3 bewirken die korrekte Anzeige der Mutingfunktion und trennen den aktivierten Freigabeausgang von den Mutinganzeigen P1/P2 bei nicht aktiver Überbrückungsfunktion. Fehler in R2 oder R3 können nicht zu einem ungewollten Muting (d.h. gefährlichem Ausfall der Mutingfunktion) führen.

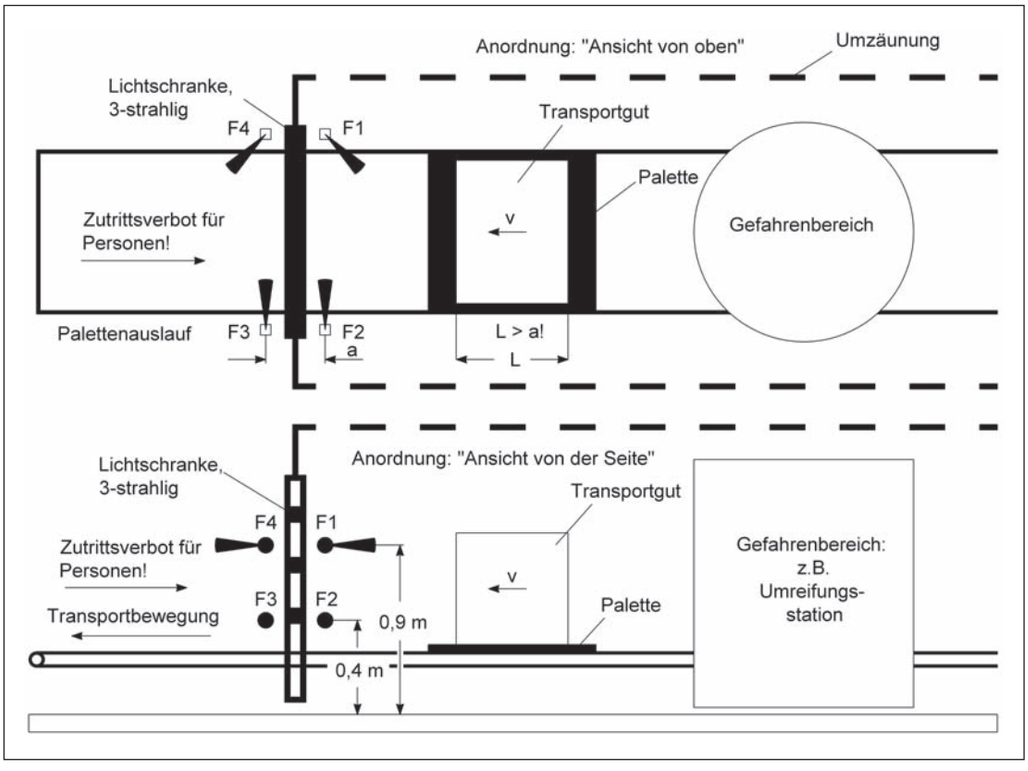


Abbildung 8.39: Automatisch gesteuerte Palettierstation – Prinzip der Absicherung des Palettenauslaufs mit Lichtschranke und Anordnung der Überbrückungssensoren F1 bis F4

- Bei Spannungsausfall mit anschließender Wiederkehr oder bei unterbrochener Lichtschranke F5 und nicht aktiver Überbrückungsfunktion werden die Hilfsschütze K2 und K3 entregt. Die jetzt nicht vorhandene Selbsthaltung verhindert deren Wiederanzug bei einem Wiederschließen der Überbrückungsstromkreise. Ein erneutes Ingangsetzen der Anlage kann nur über das Aufheben der Wiederanlaufsperre, d.h. durch willentliche Betätigung und Entlastung des Starttasters S1 erfolgen.

- Für das bestimmungsgemäße Ingangsetzen bzw. Wiederingangsetzen, z.B. nach einer Störung der Anlage, muss der Schlüsselschalter S3 betätigt werden. Mithilfe des Totmann-Tasters S4 kann eine Palette vom Bediener im Störfall aus dem Detektionsbereich der Lichtschranke und der Überbrückungssensoren herausgefahren werden.

  Für einen störungsfreien Ablauf des Palettentransportes durch die Auslassöffnung hindurch müssen zwei Zeitvorgaben im SPS-Programm auf die Geschwindigkeit der Transportbewegung abgestimmt werden:

  - Die Zeitvorgabe T1 bestimmt die maximale Zeitspanne, innerhalb derer – nach Aktivierung des Sensors F1 – die Aktivierung des Sensors F2 und damit das Einleiten der Überbrückungsfunktion durch das Transportgut zu erfolgen hat.

  - Die Zeitvorgabe T2 wird mit dem Wiederfreiwerden des Sensors F2 gestartet. Sie muss so gewählt werden, dass K1 bei wieder frei gewordenem Schutzfeld der Lichtschranken erregt und wieder entregt wird, noch bevor Sensor F3 durch das Transportgut deaktiviert wird und damit die Überbrückungsfunktion beenden wird.

- Das Nichtabfallen der Schütze K2 und K3 wird wegen der vorhandenen Rückführung der zwangsgeführten Öffnerkontakte in den SPS-Eingang I1.1 spätestens vor einem erneuten Ingangsetzen des Bandantriebs bzw. der Palettieranlage aufgedeckt. Ein Versagen von K1 wird mit dem nächsten Auslass einer Palette aufgedeckt.

- Ein selbsttätiger unbeabsichtigter Anlauf des Bandantriebs bzw. der Palettieranlage bei einem Energieausfall mit anschließender Wiederkehr oder bei einem Versagen der Standard-SPS wird durch die Funktion der Anlauf- bzw. Wiederanlaufsperre verhindert. Die SPS kann die Wiederanlaufsperre nur direkt, nachdem die Palette die Lichtschranke passiert hat, also bei noch aktivierten Sensoren F3 und F4, aufheben.

- Das Versagen einzelner Überbrückungssensoren wird vom Programm der SPS entweder unmittelbar aufgedeckt (wegen Überwachung auf korrekten Ablauf von Aktivierung und Deaktivierung) oder macht sich während des Palettendurchlaufs betriebshemmend bemerkbar.

- Ein Versagen des Totmann-Tasters S4, der nur zur Störbeseitigung verwendet wird (Muting manuell), unterliegt einer unmittelbaren Erkennung durch den Benutzer.

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 bis K3 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.

- Die Zuleitungen zur Lichtschranke F5 und zum Totmann-Taster S4 sind so verlegt, dass Kurzschlüsse einzelner Leitungen untereinander (auch zur Versorgungsspannung) ausgeschlossen werden können.

- Die Befehlsgeber S1 bis S4 sind außerhalb des Gefahrenbereichs und mit Einblick in den Gefahrenbereich angeordnet.

- Der Überbrückungszustand wird gut erkennbar für den Bediener am Zugang zum Gefahrenbereich von zwei Leuchtmeldern angezeigt.

- Die Standardkomponenten F1 bis F4 werden, soweit zutreffend, entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.

Bemerkungen

- Beispiel für die Ermöglichung einer automatischen Materialabfuhr bei der Absicherung der Zugänge von Palettierern und Depalettierern, Umsetzstationen, Umreifungs- oder Umwickelungsmaschinen. Das gleiche Prinzip lässt sich für Zugänge mit Materialzufuhr verwenden.

- Nach DIN EN 415-4 kann vorausgesetzt werden, dass ein unbemerkter Zutritt von Personen durch Einlauf- bzw. Auslauföffnungen ausreichend sicher verhindert ist, wenn u.a. folgende Anforderungen eingehalten sind:

  - Verwendung einer zwei- bis dreistrahligen Lichtschranke unter Beachtung erforderlicher Montagehöhen (bei offenem Zugang bzw. vorhandener Leerpalette im Zugang) oder

– bei überbrückter Schutzfunktion der Lichtschranke durch die beladene Palette mit seitlichen Öffnungsweiten < 0,2 m sowie einsetzender Überbrückung durch die Palettenladung erst unmittelbar vor dem Unterbrechen der Lichtstrahlen (ohne größere zeitliche und geometrische Lücken)

Berechnung der Ausfallwahrscheinlichkeit

Für die Ausgangsrelais der Überbrückungssensoren F1 bis F4 wird in der folgenden Berechnung ein DC von 0 % angenommen, da die zum Muting verwendeten Kontakte keiner automatischen Fehlererkennung unterliegen. Aus diesem Grunde ist eine manuelle periodische Überprüfung vorgesehen, die sich mit einfachen Mitteln realisieren lässt.

- $MTTF_d$: Für den Sensorteil der Mutingsensoren F1 bis F4 wird jeweils eine $MTTF_d$ von 100 Jahren [G] angenommen. Für die Ausgangsrelais von F1 bis F4 gilt ein B_{10d}-Wert von 2 000 000 Zyklen [N]. Bei 300 Arbeitstagen, 16 Arbeitsstunden und 200 Sekunden Zykluszeit ist für diese Elemente n_{op} = 86 400 Zyklen/Jahr und $MTTF_d$ = 231 Jahre. Die $MTTF_d$ des Kanals ergibt sich zu 35 Jahren („hoch“).

- DC_{avg}: DC = 90 % für den Sensorteil der Mutingsensoren F1 bis F4 wird durch die SPS-Überwachung erreicht. Der DC für die Ausgangsrelais wird zur sicheren Seite mit 0 % abgeschätzt. Der daraus ermittelte DC_{avg}-Wert beträgt 63 % („niedrig“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_d$ pro Kanal (35 Jahre) und niedrigem DC_{avg} (63 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}16 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.

Weiterführende Literatur

- *Grigulewitsch, W.:* Speicherprogrammierbare Steuerung (SPS) zum zeitlich begrenzten, prozessabhängigen Aufheben einer Sicherheitsfunktion – Schaltungsbeispiel. Kennzahl 330 231. 36. Lfg. XII/99. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de/330231

- *Kreutzkampf, F.; Hertel, W.:* Zeitbegrenztes Aufheben von Sicherheitsfunktionen. Kennzahl 330 214. 19. Lfg. X/92. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de/330214

- DIN EN 415-4: Sicherheit von Verpackungsmaschinen – Teil 4: Palettierer und Depalettierer (08.97) und Berichtigung 1 (03.03), Beuth, Berlin 1997 und 2003

- 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

- DIN IEC 62046: Sicherheit von Maschinen – Anwendung von Schutzeinrichtungen zum Erkennen von Personen (Normentwurf) (08.06). Beuth, Berlin 2006

- DIN EN 999: Sicherheit von Maschinen – Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (12.98). Beuth, Berlin 1998

8.2.23 Karusselltürsteuerung – Kategorie 3 – PL d (Beispiel 23)

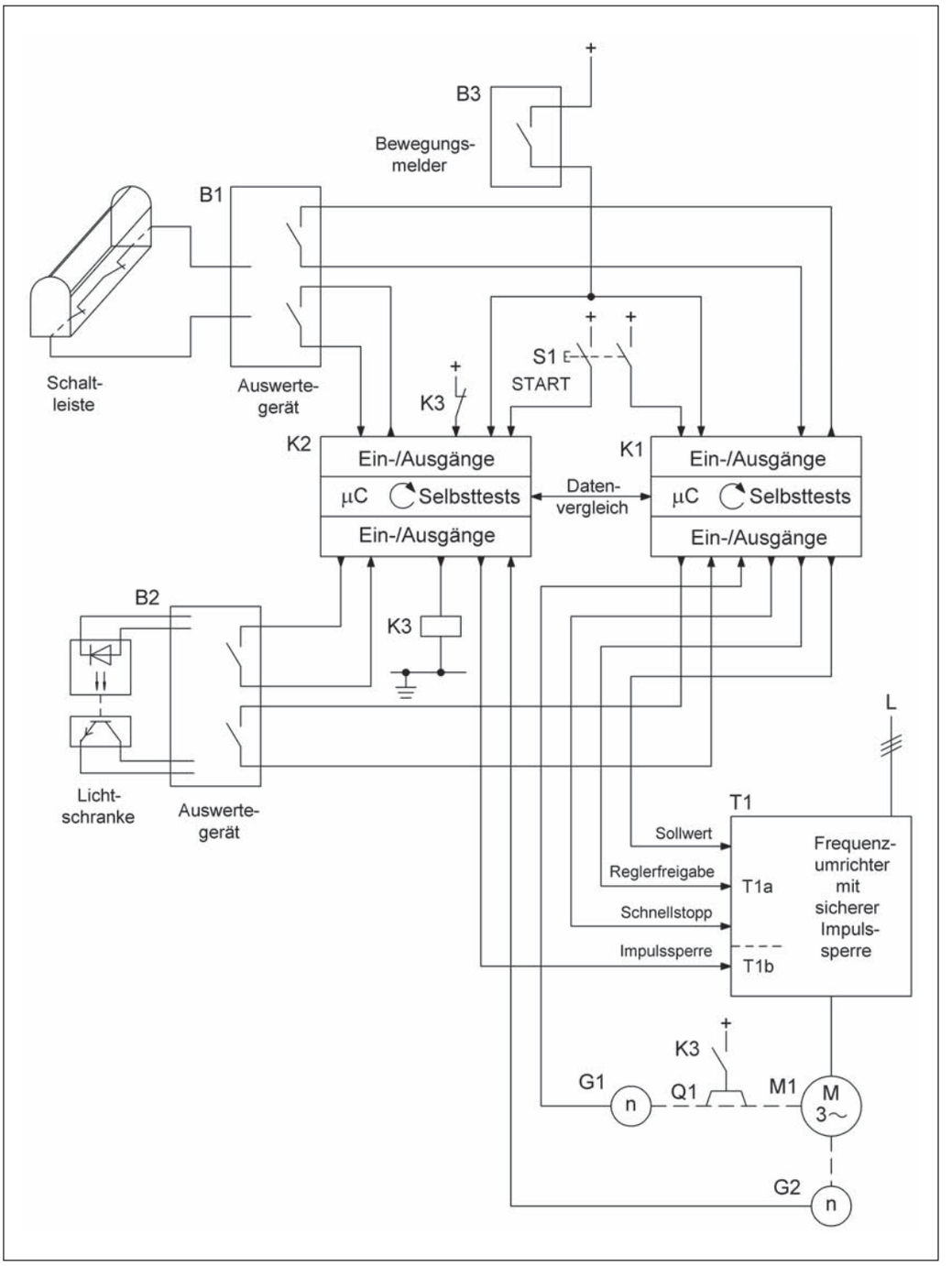
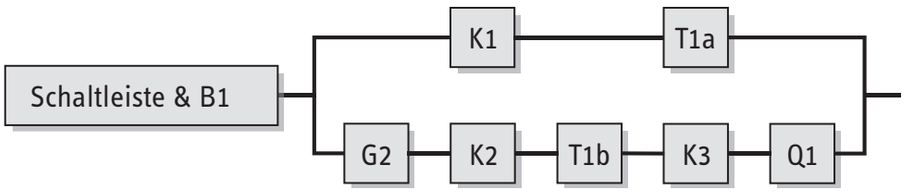


Abbildung 8.40: Karusselltürsteuerung mit Mikrocontrollern

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Bei Betätigung der Schaltleiste wird die Drehbewegung der Karusselltür stillgesetzt (SS1 – Sicherer Stopp 1).
- Sicher begrenzte Geschwindigkeit (SLS): Bei Detektion einer Person oder eines Gegenstandes durch die Lichtschranke wird die Geschwindigkeit der Karusselltür reduziert und sicher begrenzt.



Funktionsbeschreibung

- Die Drehbewegung der Karusselltür wird erstmals nach dem Einschalten der Steuerung durch den Taster S1 eingeleitet. Im Normalbetrieb erfolgt die Anforderung zur Drehung über den an der Tür befindlichen Bewegungsmelder B3. Der Frequenzumrichter T1 wird gemeinsam durch die beiden Mikrocontroller K1 und K2 angesteuert. Jeder Mikrocontroller (µC) beinhaltet einen Mikroprozessor (CPU) als Recheneinheit sowie Arbeits- (RAM) und Festwertspeicher (ROM). K1 steuert die Funktionen der Sollwertvorgabe, Reglerfreigabe sowie des Schnellstopps. Durch K2 wird die Impulssperre angesteuert und die Haltebremse Q1 kann mithilfe des Hilfsschützes K3 gelöst werden. Die Drehgeber G1 und G2 übermitteln die Motordrehzahl an K1 bzw. K2.

- Fehler in der Schaltleiste bzw. der Lichtschranke werden in den zugehörigen Auswertegeräten B1 und B2 erkannt werden. Dies gilt auch für Fehler in B1 und B2, die durch interne Überwachung erkannt werden. Fehler in den Komponenten der Mikrocontroller werden über durchgeführte Selbsttests bzw. durch Datenvergleich erkannt. Die korrekte Funktion des Frequenzumrichters T1 wird mithilfe der Drehgeber G1 und G2 in K1 bzw. K2 überwacht. Aufgedeckte Fehler führen, gesteuert über K1 und/oder K2, zur Stillsetzung der Türdrehbewegung durch T1 und/oder Q1. Zur Befreiung eingeschlossener Personen können die Türflügel von Hand geklappt werden.

- Durch redundante Verarbeitungskanäle führt ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktionen. Die Kombination unerkannter Fehler kann zum Verlust der Sicherheitsfunktionen führen.

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 Schaltleiste dient der Absicherung von Quetsch-, Scher- und Einzugsstellen. Sie ist über B1 mit der Steuerung verbunden. Das Teilsystem aus Sensor und Auswertegerät erfüllt die Anforderungen nach DIN EN 1760-2 in Kategorie 3 und nach DIN EN ISO 13849-1 für PL d. Fehler im Signalgeber der Schaltleiste bzw. in den Zuleitungen müssen ausgeschlossen oder über das Auswertegerät erkannt werden können (es können Schaltleisten, die nach dem Öffner- oder Schließer-Prinzip arbeiten, verwendet werden). Nach Entlastung einer zuvor betätigten Schaltleiste erfolgt ein automatischer zeitverzögerter Wiederanlauf der Drehbewegung. Die Schaltleiste verfügt über einen hinreichenden Verformungsweg und einen ausreichenden Wirkbereich.

- Die Lichtschranke dient der voreilenden, berührungslos wirkenden Absicherung von Gefahrstellen. Sie erfüllt zusammen mit B2 mindestens die Anforderungen für Typ 2 nach DIN EN 61496-1 und DIN CLC/TS 61496-2 sowie nach DIN EN ISO 13849-1 für PL d. Die nach der Detektion einer Person oder eines Gegenstandes durch die Lichtschranke eingenommene reduzierte, sicher begrenzte Geschwindigkeit wird nach einer voreingestellten Zeit wieder auf Normaldrehgeschwindigkeit erhöht. Die Zuleitungen zu Sender und Empfänger sind getrennt oder geschützt verlegt.

- Während des ersten Anlaufs der Türdrehbewegung werden Einschalttests durchgeführt. Dabei werden unter anderem die Blöcke der Mikrocontroller (Mikroprozessor, Arbeits- und Festwertspeicher) getestet, Ein- und Ausgangstests durchgeführt sowie die Ansteuerung des Motors über den Frequenzumrichter überprüft (u.a. Test der Reglerfreigabe, der Schnellstoppfunktionalität sowie der Impulssperre). Ebenfalls findet ein Bremsentest statt, bei dem der Frequenzumrichter gegen die eingefallene Haltebremse arbeiten muss.

- Im Rahmen des Datenvergleichs zwischen den beiden Controllern erfolgt der Austausch von Sollwerten und Zwischenergebnissen unter Einbeziehung der zyklisch durchgeführten Selbsttests.

- Durch die Verwendung eines Frequenzumrichters mit sicherer Impulssperre ist der Einsatz eines Schützes zum Abschalten der Versorgungsspannung nicht mehr erforderlich. Der Frequenzumrichter ist zum Antreiben und Bremsen geeignet.

- K3 besitzt zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Die Schaltstellung des Öffnerkontaktes wird vom Mikrocontroller K2 zur Fehleraufdeckung überwacht.

- Bei dem Beispiel wird davon ausgegangen, dass zur Bremsung der Karusselltür die Regelung über den Frequenzumrichter T1 hinreichend ist. Nach Erreichen des Stillstandes wird die Impulssperre aktiviert und die Reglerfreigabe weggenommen zur Vermeidung des unerwarteten Anlaufes. Bremszeit und Bremsweg werden von der Steuerung überwacht. Die Bremse Q1 ist im Fehlerfall erforderlich, damit es nach einem Fehler, wenn z.B. T1 die spezifizierte Funktion nicht mehr ausführen kann, zu keiner Gefährdung durch eine ungewollte Bewegung kommen kann. Q1 arbeitet nach dem Ruhestromprinzip.

- Programmierung der Software (SRESW) in K1 und K2 entsprechend den Anforderungen für PL d nach Abschnitt 6.3

- Die Standardkomponenten G1, G2 (soweit für die Drehgeber zutreffend) und T1 werden entsprechend den Hinweisen in Abschnitt 6.3.10 eingesetzt.

- Für die Sicherheitsfunktion „Sicher begrenzte Geschwindigkeit“ wird ein Fehlerausschluss für den Fehler Geberwellenbruch (G1/G2) angenommen. Einzelheiten zur Möglichkeit eines Fehlerausschlusses siehe z.B. IEC 61800-5-2, Tabelle D.16

Bemerkungen

- Das Schaltungsbeispiel ist einsetzbar zur Realisierung der Sicherheitsfunktionen „Sicherheitsbezogene Stoppfunktion“ und „Sicher begrenzte Geschwindigkeit“ in einer Steuerung für drei- und vierflügelige Karusselltüren mit Break-Out-Funktion (Türflügel können im Notfall von Hand geklappt werden) für den Einsatz im öffentlichen und gewerblichen Bereich.

- Eine regelmäßige manuelle Überprüfung der Schaltleiste ist erforderlich. Zum einen muss die Funktionsfähigkeit überprüft werden und zum anderen ist eine optische Begutachtung der Schaltleiste notwendig, um Beschädigungen frühzeitig erkennen zu können.

Berechnung der Ausfallwahrscheinlichkeiten

- Der Frequenzumrichter T1 wird für die Berechnung der Ausfallwahrscheinlichkeiten in die Blöcke T1a und T1b zerlegt. Im Block T1a sind die Funktionen Sollwertvorgabe, Reglerfreigabe und Schnellstopp sowie deren steuerungstechnische Umsetzung enthalten. Der Block T1b beinhaltet die mit einer geringen Anzahl von Bauteilen realisierte sichere Impulssperre.

Die detaillierte Berechnung der Ausfallwahrscheinlichkeit wird für die Sicherheitsfunktion „Sicherheitsbezogene Stoppfunktion (SS1)“, die auch im Blockdiagramm dargestellt ist, durchgeführt:

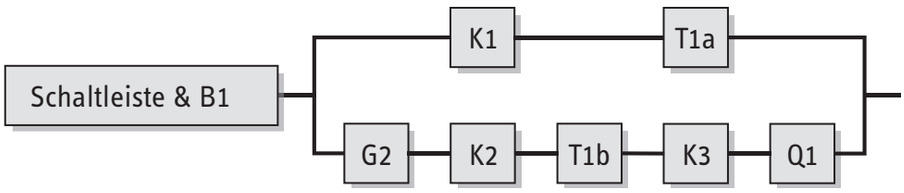
- Da die Schaltleiste mit zugehörigem Auswertegerät B1 als käufliches Sicherheitsbauteil vorliegt, wird deren Ausfallwahrscheinlichkeit am Ende der Berechnung addiert ($3{,}00 \cdot 10^{-7}$/Stunde [G]).

- $MTTF_d$: Die sicherheitsrelevanten Bauteile von K1 und K2 einschließlich ihrer Peripherie werden nach Anwendung des „Parts Count“-Verfahrens mit einem Wert von 878 Jahren [G] berücksichtigt. Für G2 fließt ein Wert von 75 Jahren [G] in die Berechnung ein. Für T1a wird ein Wert von 100 Jahren [G] und für T1b ein Wert von 1 000 Jahren [G] angesetzt. Für K3 wird ein B_{10d}-Wert von 400 000 Zyklen [N] angesetzt. Bei einer Betätigung pro Tag ergeben sich n_{op} = 365 Zyklen/Jahr und eine $MTTF_d$ = 10 959 Jahre. Q1 wird mit einer $MTTF_d$ von 50 Jahren [G] berücksichtigt. Die Haltebremse Q1 ist nur im Fehlerfall erforderlich und unterliegt keinem betriebsmäßigen Verschleiß. Insgesamt ergibt sich ein symmetrisierter $MTTF_d$-Wert pro Kanal von 64,3 Jahren („hoch“).

- DC_{avg}: Für K1 und K2 ergibt sich aufgrund der Auswahl geeigneter Testmaßnahmen ein *DC* von 60 %. Interne Selbsttests der Komponenten der Mikrocontroller werden durchgeführt. Für den Block T1a wird ein *DC* von 90 % angesetzt, da eine Fehleraufdeckung über den Prozess erfolgt. G2 wird mit einem *DC* von 90 % bemessen, die Fehleraufdeckung erfolgt auch hier durch den Prozess und den Vergleich mit G1 über K1 und K2. K3 wird mit einem *DC* = 99 % bemessen aufgrund der direkten Überwachung eines zurückgelesenen zwangsgeführten Kontaktes. Aufgrund des durchgeführten statischen Einschalttestes wird für T1b ein *DC* = 60 % und für Q1 ein *DC* = 30 % angesetzt. Durch Mittelung ergibt sich damit ein DC_{avg} von 62 % („niedrig“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Die Kombination der Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_d$ (64,3 Jahre) und niedrigem DC_{avg} (62 %). Für die Kombination der Komponenten K1 und T1a im ersten Kanal sowie G2, K2, T1b, K3 und Q1 im zweiten Kanal ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $1{,}94 \cdot 10^{-7}$/Stunde. Zuzüglich der Sensoreinheit, bestehend aus Schaltleiste und Auswertegerät B1, beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle der Steuerung für diese Sicherheitsfunktion insgesamt $4{,}94 \cdot 10^{-7}$/Stunde. Dies entspricht PL d.



Berechnung der Ausfallwahrscheinlichkeit für die Sicherheitsfunktion „Sicher begrenzte Geschwindigkeit (SLS)“:

- Für diese Berechnung muss zusätzlich G1 im ersten Kanal berücksichtigt werden. Dafür wird eine $MTTF_d$ von 75 Jahren [G] angesetzt. Der *DC* von 99 % ergibt sich aufgrund der Fehleraufdeckung durch den Prozess sowie den Vergleich mit G2 über K2 und K1. Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache wurden analog zur ersten Beispielberechnung gewählt. Mit 34,9 Jahren $MTTF_d$ und 70 % DC_{avg} ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}46 \cdot 10^{-7}$/Stunde. Nach Hinzufügen der Sensoreinheit, hier bestehend aus Lichtschranke und Auswertegerät B2 mit einem Wert von $2{,}00 \cdot 10^{-7}$/Stunde [G], beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle der Steuerung für diese Sicherheitsfunktion insgesamt $6{,}46 \cdot 10^{-7}$/Stunde. Dies entspricht ebenfalls PL d.

Weiterführende Literatur

- DIN EN 1760-2: Sicherheit von Maschinen – Druckempfindliche Schutzeinrichtungen – Teil 2: Allgemeine Leitsätze für die Gestaltung und Prüfung von Schaltleisten und Schaltstangen (07.01). Beuth, Berlin 2001
- DIN 18650-1: Schlösser und Baubeschläge – Automatische Türsysteme (12.05). Beuth, Berlin 2005
- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005
- 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
- DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebe mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (07.07). Beuth, Berlin 2007

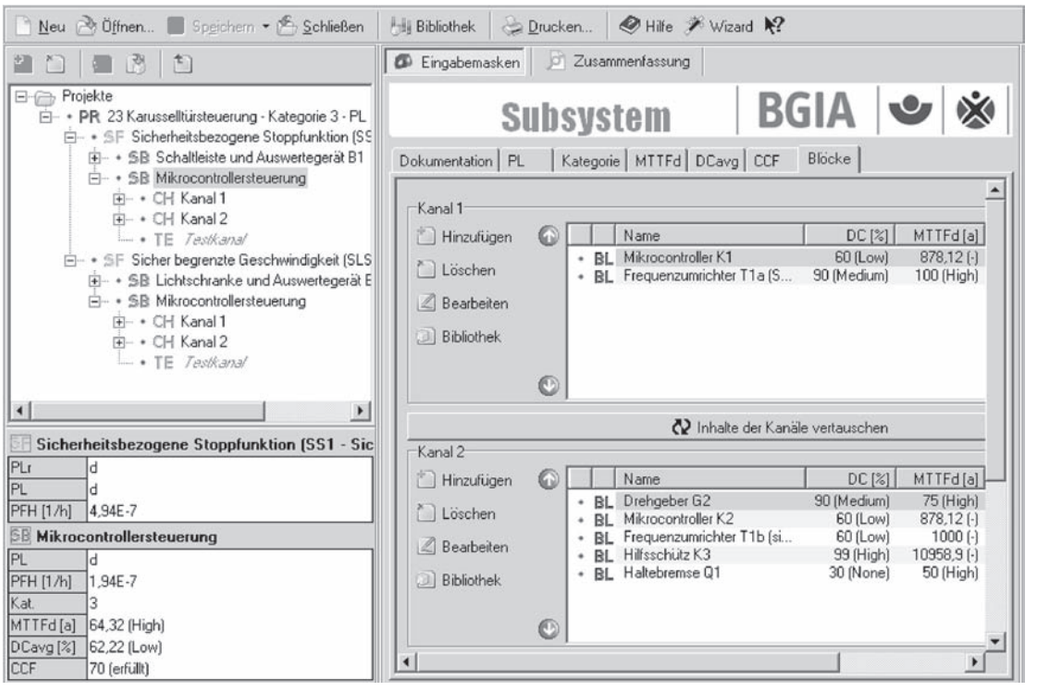
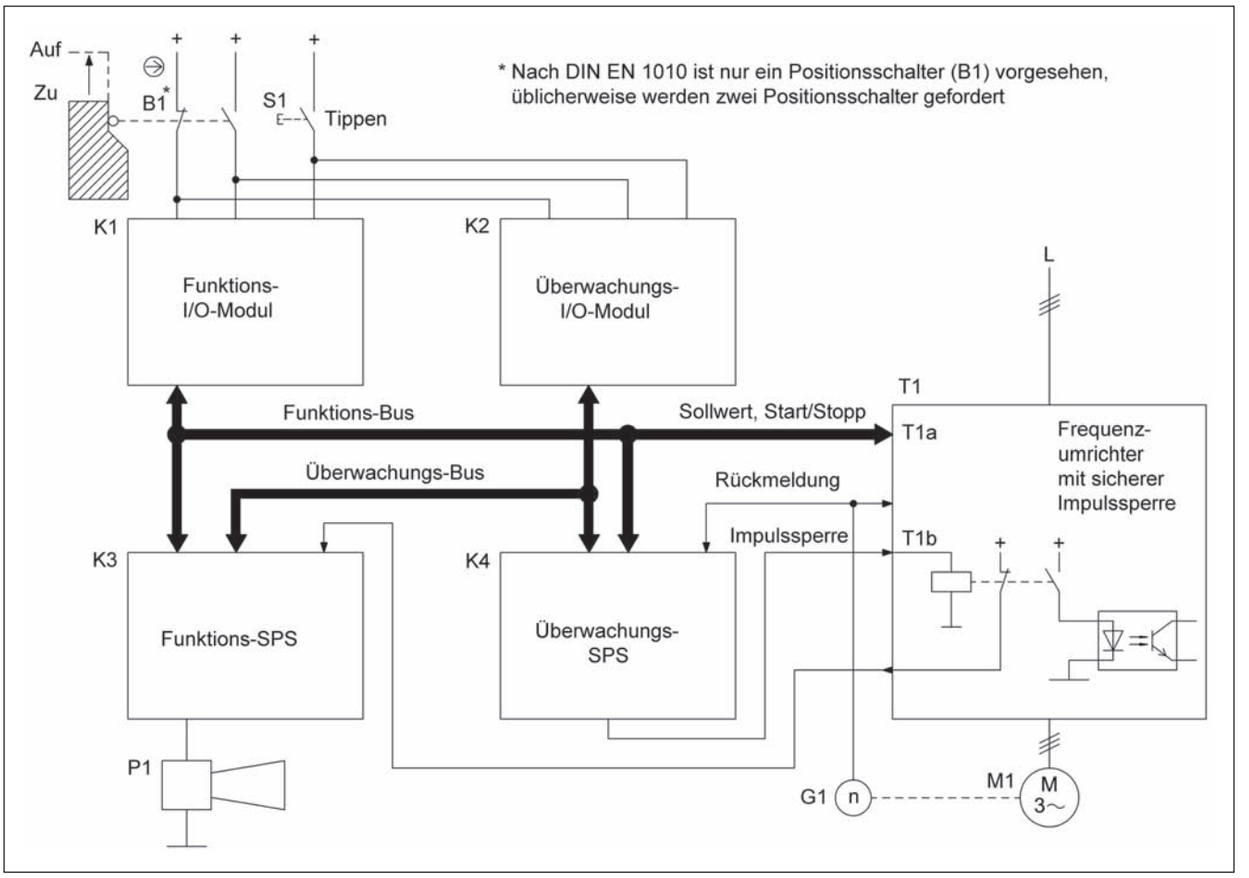


Abbildung 8.41: PL-Bestimmung mithilfe von SISTEMA

8.2.24 Tippbetrieb mit sicher begrenzter Geschwindigkeit an einer Druckmaschine – Kategorie 3 – PL d bzw. c (Beispiel 24)

Abbildung 8.42:
Tippbetrieb mit sicher begrenzter Geschwindigkeit an einer Druckmaschine durch eine zweikanalige Rechnersteuerung

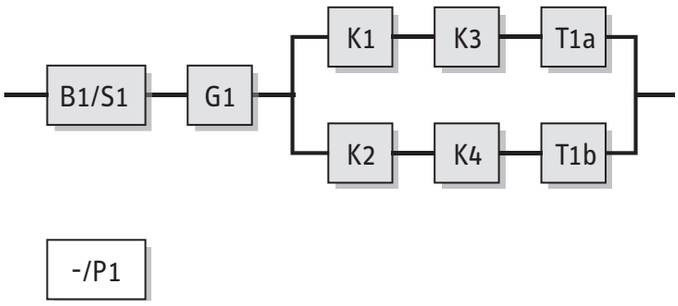


Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Beim Öffnen der Schutztür soll der Antrieb anhalten (SS1 – Sicherer Stopp 1).
- Sicher begrenzte Geschwindigkeit (SLS): Bei geöffneter Schutztür dürfen Maschinenbewegungen nur mit begrenzten Drehzahlen erfolgen.
- Tippbetrieb: Bei geöffneter Schutztür sind Bewegungen nur während der Betätigung eines Tipptasters möglich.

Funktionsbeschreibung

- Das dezentrale I/O-Modul K1 erfasst die Zustände des Positionsschalters mit Personenschutzfunktion B1 und des Tipptasters S1 und stellt diese auf dem Funktionsbus als Information zur Verfügung. Diese Information wird durch die Funktions-SPS K3 ausgewertet und führt zur Ansteuerung des Frequenzumrichters T1 (Funktionsmäßige Ansteuerung T1a) über den Funktionsbus. Redundant zu K1 und K3 arbeiten das I/O-Modul K2 und die Überwachungs-SPS K4, die über einen eigenen Überwachungsbus kommunizieren. K4 kann durch Anwahl der sicheren Impulssperre von T1 eine ungesteuerte Stillsetzung (Austrudeln) herbeiführen (Sicherheitsabschaltung T1b).
- Bei geöffnetem B1 ist nur ein Tippbetrieb über S1 mit sicher begrenzter Geschwindigkeit erlaubt.



- Entsprechend DIN EN 1010-1 ist ein einziger Positionsschalter B1 ausreichend. Die meisten Fehler in S1 werden durch eine akustische Anlaufwarnung mittels P1 und Zwangsdynamisierung aufgedeckt und beherrscht: Nach erstmaliger Betätigung von S1 erfolgt eine akustische Warnung (P1), erst nach Loslassen und erneutem Betätigen das verzögerte Anlaufen des Antriebs.

- Fehler in K1 und K2 werden durch Zustandsvergleich in K4 erkannt. K4 überwacht auch K3 durch Mithören der Eingangs- und Ausgangsinformationen. Ein Teil der Fehler in K3 werden zusätzlich durch Fehler im Prozess offenbart. In K4 finden Selbsttests (z.B. zeitliche Programmlaufüberwachung durch internen Watchdog) statt, außerdem benutzt K3 K4 zur regelmäßigen Anwahl der Impulssperre und überwacht deren Rückmeldung durch den zwangsgeführten Öffnerkontakt des Impulssperrerelais von T1.

- Der Frequenzumrichter T1 bildet mit dem Sin/Cos-Geber G1 ein Regelsystem, in dem Fehler durch den hochsynchronen Produktionsprozess offenbart werden (Fehldruck, Papierriss). G1 wird zur Überwachung der sicher begrenzten Geschwindigkeit zusätzlich in K4 zurückgelesen und auf Plausibilität der Sin/Cos-Information ($Sin^2 + Cos^2 = 1$) sowie Übereinstimmung mit dem Sollwert für T1 überwacht.

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.

- Der Öffner von B1 entspricht DIN EN 60947-5-1, Anhang K. Maßnahmen zur Verhinderung der Lageänderung und der vernünftigerweise vorhersehbaren Manipulation sind realisiert (siehe DIN EN 1088 mit Anhang A1). Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung des Positionsschalters ist sichergestellt.

- Trotz Anlaufwarnung und Zwangsdynamisierung kann S1 während des Tippbetriebs hängen bleiben. Daher muss in Reichweite des Bedieners zusätzlich ein Not-Halt-Gerät installiert sein.

- Für die Anschlussleitungen von S1 müssen die Bedingungen eines Fehlerausschlusses für Leitungskurzschlüsse nach DIN EN ISO 13849-2, Tabelle D.4, eingehalten werden. Fehler in den Anschlussleitungen von B1 werden durch eine Antivalenzüberwachung des Öffner- und Schließerkontaktes in K1 und K2 erkannt.

- Die programmierbaren Komponenten K1 bis K4 erfüllen die normativen Anforderungen gemäß Abschnitt 6.3.

- G1 liefert redundante Positionsinformationen (z.B. Sin/Cos-Geber) und ist in den Regelkreis eingebunden (Gewinnung der Kommutierung).

- T1 besitzt eine sichere Impulssperre (T1b), deren erfolgreiche Anwahl durch einen zwangsgeführten Öffnerkontakt zurückgelesen wird.

- Der Einsatz der Standardkomponenten G1 und T1 erfolgt entsprechend den Hinweisen aus Abschnitt 6.3.10.

- Der Einsatz der Bussysteme (Funktionsbus, Überwachungsbus) erfolgt entsprechend den Hinweisen aus Abschnitt 6.2.17.

Bemerkungen

- Anwendung z.B. zur Absicherung von Einzugsstellen an Rotationsdruckmaschinen. Die Anwendung der DIN EN 1010-1 erfordert für nicht zyklischen Eingriff in den Gefahrenbereich, d.h. weniger als einen Eingriff pro Stunde, nur einen Positionsschalter für die Stellungsüberwachung der trennenden Schutzeinrichtung. Das Kriterium der Fehlertoleranz für Kategorie 3 erfordert für vergleichbare Maschinensteuerungen üblicherweise die Verwendung von zwei Positionsschaltern (z.B. ein Öffner, ein Schließer).

- Für den Tippbetrieb unter der Voraussetzung bereits gewährleisteter sicher begrenzter Geschwindigkeit kann unter bestimmten Bedingungen von der Möglichkeit zur Vermeidung der Gefährdung ausgegangen werden.

Berechnung der Ausfallwahrscheinlichkeit

- Die Sensorebene B1, S1 und G1 liegt außerhalb der redundanten Logik- und Aktorebene und wird daher separat betrachtet.

- Für B1 kann ein Fehlerausschluss für den zwangsöffnenden Kontakt erfolgen. Für den mechanischen Teil wird ein B_{10d}-Wert von 20 000 000 Zyklen [N] angenommen. Bei wöchentlich 10-facher Betätigung ist n_{op} = 520 Zyklen/Jahr und $MTTF_d$ = 384 615 Jahre. Dies entspricht rechnerisch einer mittleren Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}97 \cdot 10^{-10}$/Stunde. Um den Besonderheiten der DIN EN 1010-1 Rechnung zu tragen, wird dieser Wert auf den oberen Eckwert $1{,}00 \cdot 10^{-7}$/Stunde für PL d zurückgestuft, statt wie üblich die $MTTF_d$ für einen Kanal auf 100 Jahre zu begrenzen.

- S1 besitzt einen B_{10d}-Wert von 100 000 Zyklen [H]. Bei wöchentlich 10-facher Betätigung ist n_{op} = 520 Zyklen/Jahr und $MTTF_d$ = 1 923 Jahre. Wegen Zwangsdynamisierung und Anlaufwarnung wird ein *DC* von mindestens 60 % angenommen (ein Hängenbleiben nach wiederholtem Tippen wird aber nicht erkannt). S1 erreicht damit durch die Einbindung in eine Kategorie-2-Struktur eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}28 \cdot 10^{-7}$/Stunde.

- G1 ist durch Auswertung der Sin/Cos-Signale und Nutzung im Regelkreis (Verwendung für die Kommutierung) gemäß Kategorie 3 eingebunden. Mit 30 Jahren $MTTF_d$ pro Kanal [G] und 90 % *DC* durch Plausibilitätsprüfung und Fehlererkennung im Prozess ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}65 \cdot 10^{-7}$/Stunde.

- $MTTF_d$: Es werden 100 Jahre [G] für K1 und K2, 50 Jahre [G] für K4 und 30 Jahre [G] für K3 in Rechnung gestellt. Außerdem werden 30 Jahre [G] für T1a und 1 000 Jahre [G] für T1b angesetzt. Damit ergibt sich insgesamt ein symmetrisierter $MTTF_d$-Wert pro Kanal von 24 Jahren („mittel“).

- DC_{avg}: *DC* = 99 % für K1 und K2 ergibt sich durch den direkten Vergleich der bereitgestellten Zustandsinformationen in K4. *DC* = 99 % für K3 gründet sich auf der parallelen Verarbeitung aller sicherheitsrelevanter Informationen in K4 und den dortigen direkten Vergleich mit den von K3 gebildeten Zwischenergebnissen und Ausgangssignalen. Die in K4 umgesetzten Selbsttests plus partielle Überwachung durch die von K3 zurückgelesene Impulssperre führen für K4 auf einen *DC* von 60 %. *DC* = 99 % für T1a basiert auf dem Soll-/Ist-Wert-Vergleich der Achsposition in K4. Für T1b ergibt sich bei Annahme eines Fehlerausschlusses für den internen Optokoppler durch Rücklesung der Impulssperrenanwahl ein *DC* von 60 %. Durch Mittelung ergibt sich damit ein DC_{avg} von 91 % („mittel“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

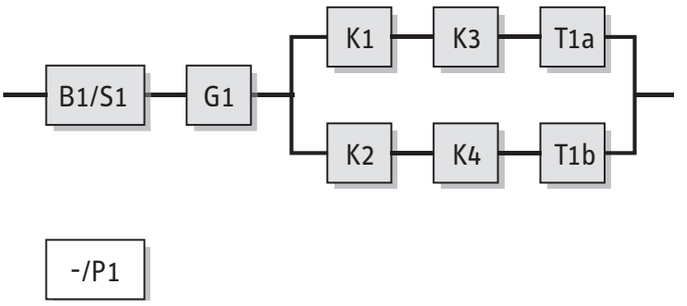
- Die Kombination von K1 bis K4 und T1 entspricht Kategorie 3 mit mittlerer $MTTF_d$ pro Kanal (24 Jahre) und mittlerem DC_{avg} (91 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $3{,}33 \cdot 10^{-7}$/Stunde. Für die sicherheitsbezogene Stoppfunktion und die sicher begrenzte Geschwindigkeit ist dazu der Wert von B1 und G1 zu addieren. So ergibt sich mit $(1{,}00 + 2{,}65 + 3{,}33) \cdot 10^{-7}$/Stunde = $6{,}98 \cdot 10^{-7}$/Stunde ein PL d. Für den Tippbetrieb muss der Wert von S1 und G1 hinzugefügt werden, womit sich ein Wert von $(5{,}28 + 2{,}65 + 3{,}33) \cdot 10^{-7}$/Stunde = $1{,}13 \cdot 10^{-6}$/Stunde errechnet. Dies entspricht PL c.

Weiterführende Literatur

- DIN EN 1010-1: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 1: Gemeinsame Anforderungen (03.05). Beuth, Berlin 2005

- Sicherheitsgerechtes Konstruieren von Druck- und Papierverarbeitungsmaschinen. Elektrische Ausrüstung und Steuerungen. Hrsg.: Berufsgenossenschaft Druck und Papierverarbeitung, Wiesbaden 2004
http://www.bgdp.de/pages/service/download/medien/220-2.pdf

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



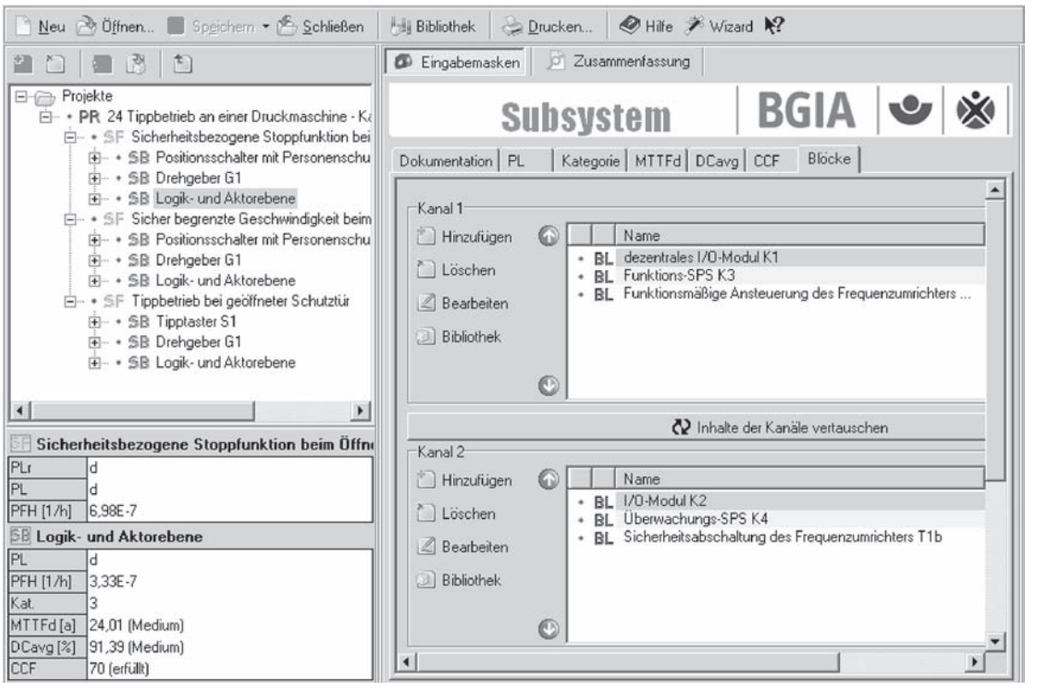


Abbildung 8.43: PL-Bestimmung mithilfe von SISTEMA

8.2.25 Pneumatische Ventilsteuerung (Subsystem) – Kategorie 3 – PL e (für PL-d-Sicherheitsfunktionen) (Beispiel 25)

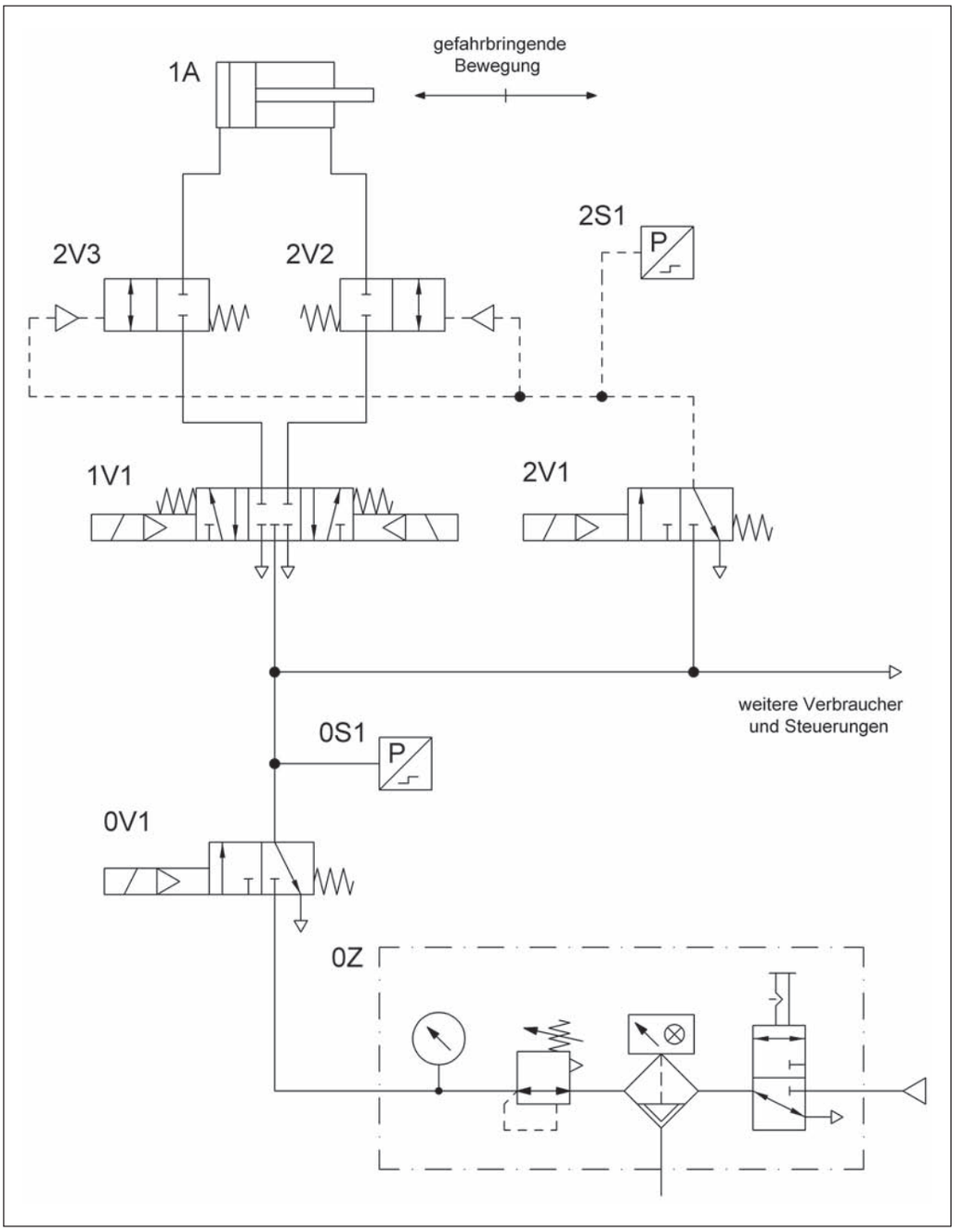
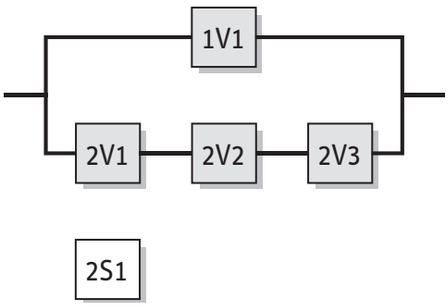


Abbildung 8.44: Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.



Funktionsbeschreibung

- Gefahrbringende Bewegungen werden redundant durch Wegeventile gesteuert. Ein Stillsetzen kann entweder durch das Wegeventil 1V1 oder durch die Wegeventile 2V2 und 2V3 erfolgen. Letztere werden durch das Steuerventil 2V1 angesteuert.
- Der alleinige Ausfall eines der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- Alle Wegeventile werden zyklisch im Prozess angesteuert.
- Die Funktion des Steuerventils 2V1 wird durch einen Druckschalter 2S1 überwacht. An den nicht überwachten Ventilen werden einige Fehler im Arbeitsprozess erkannt. Die Ventile 2V2 und 2V3 sollten eine Stellungsüberwachung aufweisen oder – da diese noch nicht Stand der Technik ist – es muss eine regelmäßige Überprüfung der Funktion durchgeführt werden. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.
- Kann durch eingesperrte Druckluft eine weitere Gefährdung auftreten, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Das Wegeventil 1V1 hat eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung.
- Die Sperrventile 2V2 und 2V3 sind möglichst im Zylinder eingeschraubt und vorgesteuert über das Ventil 2V1.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Die Signalverarbeitung der Drucküberwachung 2S1 erfolgt z.B. in einer einkanaligen SPS.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für die Ventile 1V1 und 2V1 werden B_{10d}-Werte von 40 000 000 Zyklen [G] angenommen. Für die Ventile 2V2 und 2V3 werden B_{10d}-Werte von 60 000 000 Zyklen [G] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 10 Sekunden Zykluszeit ist n_{op} = 1 382 400 Zyklen/Jahr. Damit beträgt die $MTTF_d$ für 1V1 und 2V1 289 Jahre und für 2V2 und 2V3 434 Jahre. Nach Kürzen beider Kanäle auf 100 Jahre ergibt sich ein symmetrisierter $MTTF_d$-Wert pro Kanal von 100 Jahren („hoch“).
- DC_{avg}: DC = 99 % für 2V1 ergibt sich aus der Drucküberwachung des Steuersignals für die Sperrventile. DC = 60 % für 1V1 ergibt sich aus der Fehlererkennung über den Prozess und DC = 60 % für 2V2 bzw. 2V3 aus der regelmäßigen Überprüfung der Funktion. Durch Mittelung ergibt sich damit ein DC_{avg} von 71 % („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 pneumatischen Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_d$ (100 Jahre) und niedrigem DC_{avg} (71 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $7{,}86 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.

8.2.26 Pneumatische Ventilsteuerung – Kategorie 3 – PL e (Beispiel 26)

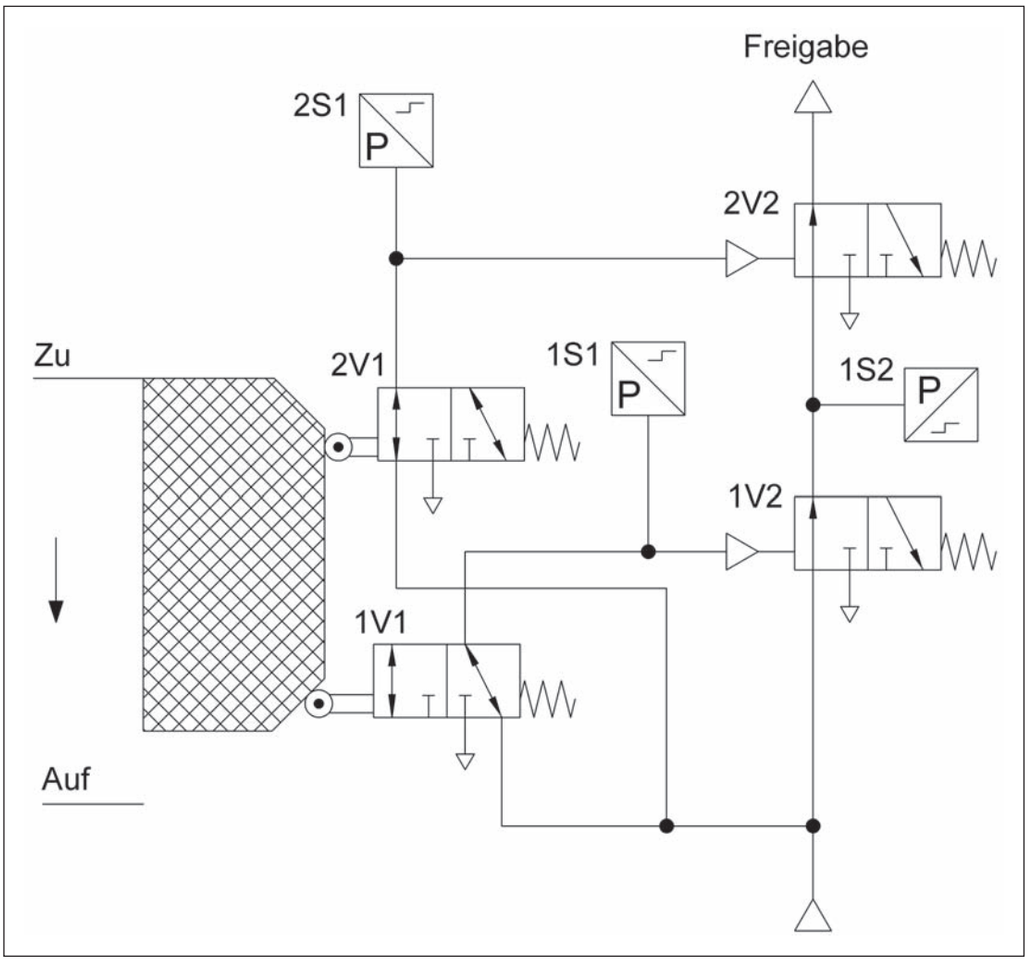


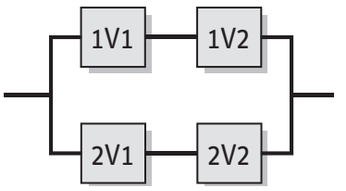
Abbildung 8.45: Redundante pneumatische Steuerung zur Verriegelung beweglicher trennender Schutzeinrichtungen

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Beim Öffnen der beweglichen trennenden Schutzeinrichtung erfolgt eine Energietrennung und Druckentlastung in der pneumatischen Steuerung.

Funktionsbeschreibung

- Die Verriegelung der beweglichen trennenden Schutzeinrichtung erfolgt durch zwei „pneumatische Positionsschalter“ (1V1 und 2V1). Diese geben jeweils einen Steuerbefehl an die Wegeventile 1V2 und 2V2.
- Pneumatische Energiezufuhr findet nur bei geschlossener Schutzeinrichtung statt.
- Der Ausfall eines „pneumatischen Positionsschalters“ oder Wegeventils führt nicht zum Verlust der Sicherheitsfunktion.
- Eine Fehlererkennung der Ventile 2V1 und 1V2 erfolgt über die Druckschalter 1S1, 2S1 und 1S2. Die entsprechenden Signale können in einer SPS verarbeitet werden. Bei einer Fehlererkennung kann z.B. die Energie abgeschaltet werden. Für das Ventil 2V2 ist keine Fehlererkennung vorhanden. Die Funktion dieses Ventils sollte regelmäßig überprüft werden. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.
- Kann durch eingesperrte Druckluft eine weitere Gefährdung auftreten, sind weitere Maßnahmen erforderlich.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- 1V1 ist ein pneumatischer Positionsschalter mit zwangläufiger Betätigung durch die bewegliche trennende Schutzeinrichtung, entsprechend DIN EN 1088.
- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung der Positionsschalter ist sichergestellt.
- Die sicherheitsgerichtete Schaltstellung der Wegeventile 1V2 und 2V2 wird durch Wegnahme der Steuersignale erreicht.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für Ventil 1V1 wird ein Fehlerausschluss angenommen, da eine zwangläufige Betätigung durch die beweglich trennende Schutzeinrichtung gegeben ist und da das Ventil als Positionsschalter mit Personenschutzfunktion ausgelegt ist (in Anlehnung an DIN EN 60947-5-1). Für die Ventile 2V1, 1V2 und 2V2 werden $B10_d$-Werte von 20 000 000 Zyklen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitstunden und 30 Sekunden Zykluszeit ist n_{op} = 460 800 Zyklen/Jahr und $MTTF_d$ = 434 Jahre. Nach Kürzen beider Kanäle auf 100 Jahre ergibt sich ein symmetrisierter $MTTF_d$-Wert pro Kanal von 100 Jahren („hoch“).
- DC_{avg}: DC = 99 % für die Wegeventile 2V1 und 1V2 ergibt sich aus der Fehlererkennung über die Druckschalter. Für das Wegeventil 2V2 wird ein DC = 0 % angenommen (Abschätzung zur sicheren Seite). Durch Mittelung ergibt sich damit ein DC_{avg} von 66 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_d$ (100 Jahre) und niedrigem DC_{avg} (66 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $8{,}95 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

Weiterführende Literatur

- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005

8.2.27 Hydraulische Ventilsteuerung (Subsystem) – Kategorie 3 – PL e (für PL-d-Sicherheitsfunktionen) (Beispiel 27)

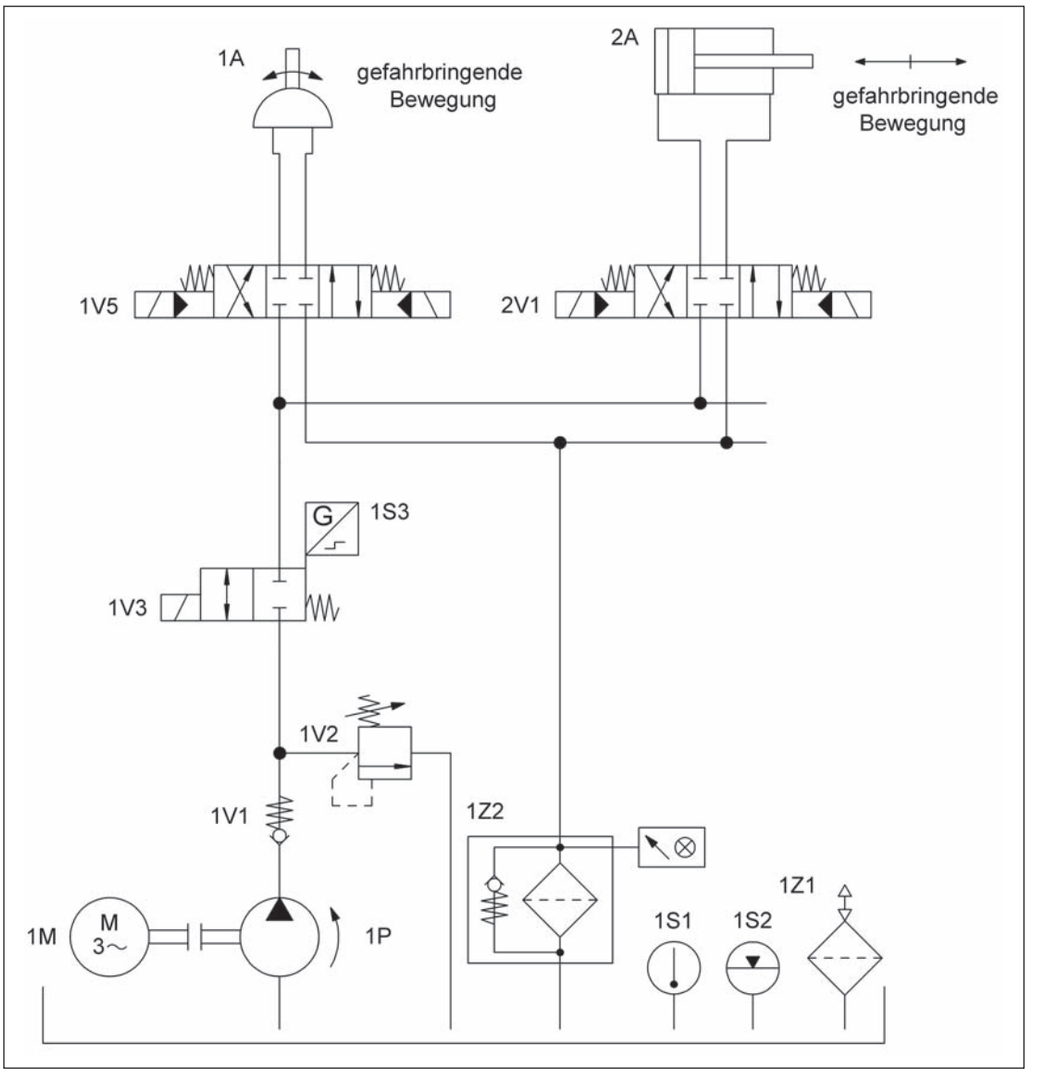


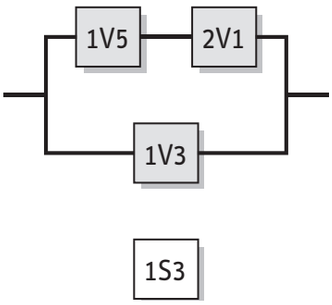
Abbildung 8.46: Getestete hydraulische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- Hier ist nur der hydraulische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch zwei Aktoren 1A und 2A in demselben Gefahrenbereich ausgeführt. Ein Stillsetzen beider Bewegungen kann entweder durch die beiden Wegeventile 1V5 und 2V1 oder übergeordnet durch das Wegeventil 1V3 erfolgen.
- Der alleinige Ausfall eines der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- 1V5 und 2V1 werden zyklisch im Prozess angesteuert, 1V3 schließt nur bei Anforderung der Sicherheitsfunktion, jedoch mindestens einmal pro Schicht.



- Eine technische Maßnahme zur Fehlererkennung ist nur an 1V3 vorgesehen (Stellungsüberwachung 1S3). An den nicht überwachten Ventilen werden einige Fehler im Arbeitsprozess erkannt. Die Anhäufung unentdeckter Fehler kann zum Verlust der Sicherheitsfunktion führen.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Die Wegeventile 1V5 und 2V1 haben eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung und Federzentrierung. 1V3 ist mit elektrischer Stellungsüberwachung ausgeführt, da 1V3 nicht zyklisch geschaltet wird.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals (elektrisch bzw. hydraulisch) erreicht.
- Die Signalverarbeitung der elektrischen Stellungsüberwachung erfolgt z.B. in einer einkanaligen SPS.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für die Wegeventile 1V3, 1V5 und 2V1 wird eine $MTTF_d$ von 150 Jahren angenommen [N]. Nach Kürzen des zweiten Kanals (1V3) auf 100 Jahre ergibt sich ein symmetrisierter $MTTF_d$-Wert von 88 Jahren („hoch“).
- DC_{avg}: DC = 99 % für 1V3 beruht auf der direkten Überwachung des Schaltzustandes durch 1S3. DC = 60 % für die Wegeventile 1V5 bzw. 2V1 beruht auf der indirekten Überwachung durch den Prozess. Durch Mittelung ergibt sich damit ein DC_{avg} von 73 % („niedrig“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der hydraulischen Steuerungselemente entspricht Kategorie 3 mit hoher $MTTF_d$ (88 Jahre) und niedrigem DC_{avg} (73 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $9{,}35 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.

8.2.28 Stellungsüberwachung beweglicher trennender Schutzeinrichtungen – Kategorie 4 – PL e (Beispiel 28)

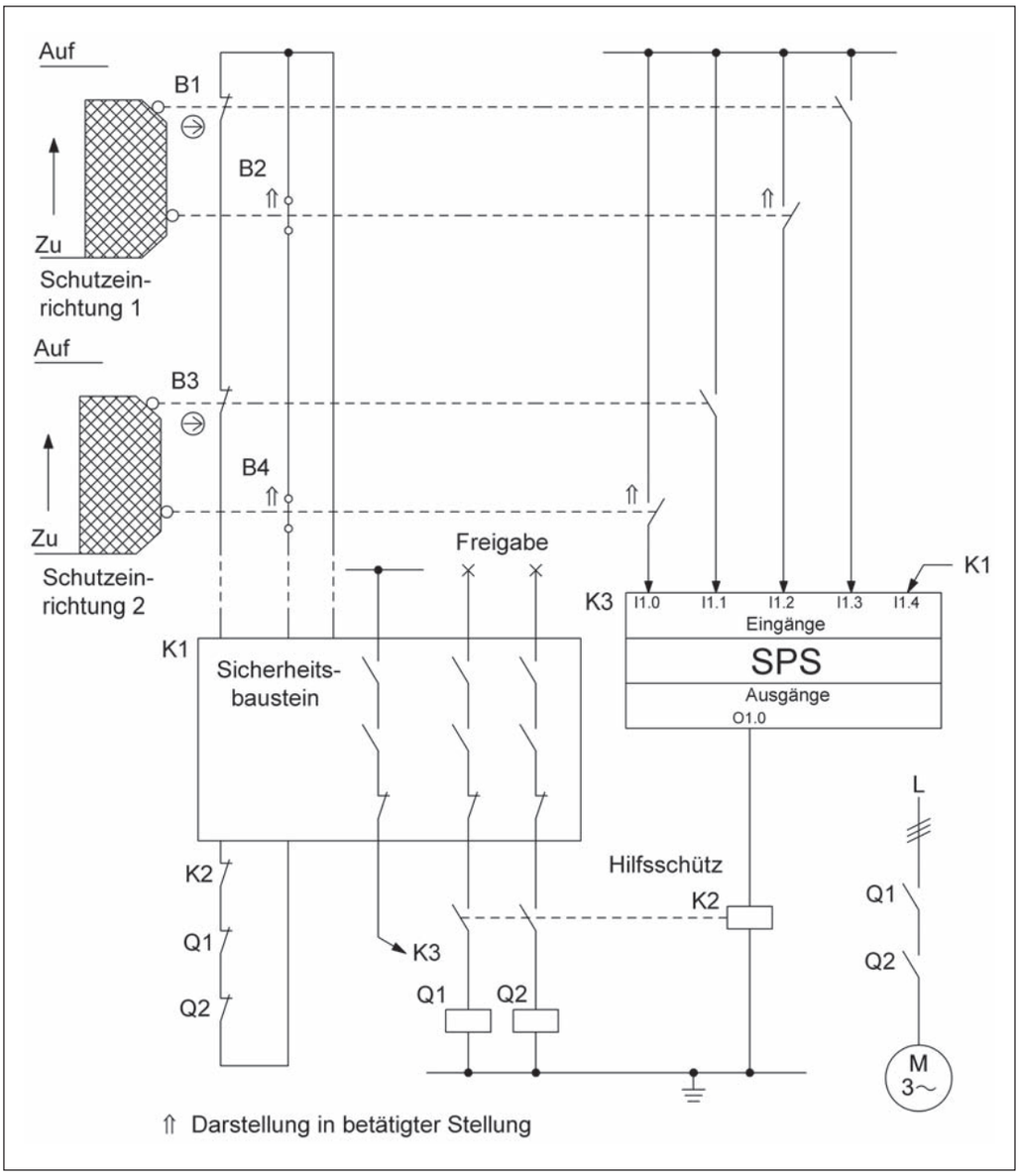


Abbildung 8.47: Stellungsüberwachung beweglicher trennender Schutzeinrichtungen zur Verhinderung von gefahrbringenden Bewegungen

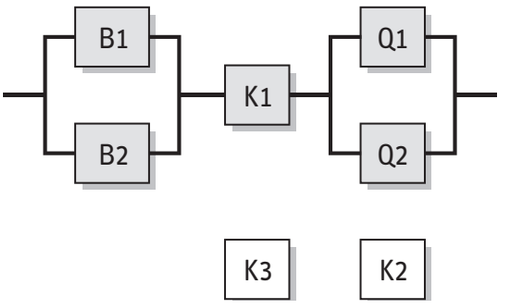
Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen einer beweglichen trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt mit zwei beweglichen trennenden Schutzeinrichtungen (Schutzgittern). Das Öffnen jedes Schutzgitters wird durch zwei Positionsschalter B1/B2 bzw. B3/B4 in Öffner-Schließer-Kombination erfasst und in einem zentralen Sicherheitsbaustein K1 ausgewertet. Dieser steuert zwei Schütze Q1 und Q2 an, durch deren Abfallen gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert werden.

- Alle Positionsschalter werden zur Fehlererkennung durch einen zweiten Kontakt in eine handelsübliche SPS K3 eingelesen, die hauptsächlich der Funktionssteuerung dient. Über ein Hilfsschütz K2 kann diese im Fehlerfall unabhängig von K1 die Schütze Q1 und Q2 abschalten. Fehler in K2, Q1 und Q2 werden durch den Sicherheitsbaustein K1 erkannt. Einige wenige Fehler werden nicht erkannt (z.B. Nichtunterbrechung der Kontakte in B2 und B4).



- Beim Auftreten eines Bauteilausfalls bleibt die Sicherheitsfunktion erhalten. Die meisten Bauteilausfälle werden erkannt und führen zur Betriebshemmung. Eine Anhäufung von unerkannten Fehlern führt nicht zum Verlust der Sicherheitsfunktion.

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.
- B1 und B3 sind Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern sind getrennt oder geschützt verlegt.
- Störungen im Anfahr- und Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschieden betätigten Positionsschaltern (Öffner-Schließer-Kombination) erkannt.
- Es können mehrere Schutzeinrichtungen hintereinander geschaltet werden (Kaskadierung).
- Der Sicherheitsbaustein K1 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Die Schütze K2, Q1, Q2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.
- Die programmierbare SPS K1 erfüllt die normativen Anforderungen gemäß Abschnitt 6.3.

Berechnung der Ausfallwahrscheinlichkeit

- Die Schaltung lässt sich in drei Subsysteme aufteilen, wie im sicherheitsbezogenen Blockdiagramm gezeigt. Die Ausfallwahrscheinlichkeit des Sicherheitsbausteins K1 wird am Ende der Berechung addiert ($2{,}31 \cdot 10^{-9}$/Stunde [H], geeignet für PL e). Für die übrigen Subsysteme wird die Ausfallwahrscheinlichkeit im Folgenden berechnet. Da jede Schutztür Bestandteil einer eigenen Sicherheitsfunktion ist, wird hier stellvertretend die Berechnung für die Schutzeinrichtung 1 gezeigt.
- $MTTF_d$: Für den Positionsschalter B1 ist ein Fehlerausschluss für den zwangsöffnenden elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt des Positionsschalters B2 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B1 und B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden pro Tag und 1 Stunde Zykluszeit ist für diese Komponenten n_{op}= 5 840 Zyklen/Jahr und $MTTF_d$ beträgt 1 712 Jahre für B1 bzw. 856 Jahre für B2. Für die Schütze Q1 und Q2 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. Mit dem oben angenommenen Wert für n_{op} folgt für Q1 und Q2 eine $MTTF_d$ von 3 424 Jahren pro Kanal. Insgesamt ergibt sich in beiden Subsystemen ein symmetrisierter $MTTF_d$-Wert pro Kanal von 100 Jahren („hoch“).
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung der Öffner-Schließer-Kombinationen in der SPS K3. DC = 99 % für die Schütze Q1 und Q2 ergibt sich aus der Überwachung bei jedem Einschalten von K1. Die genannten DC-Werte entsprechen dem DC_{avg} für das jeweilige Subsystem.
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in den Subsystemen B1/B2 und Q1/Q2 (70 Punkte): Trennung (15), bewährte Bauteile (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Subsysteme B1/B2 und Q1/Q2 entsprechen jeweils Kategorie 4 mit hoher $MTTF_d$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von jeweils $2{,}47 \cdot 10^{-8}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $5{,}16 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

8.2.29 Kaskadierung von Not-Halt-Geräten mittels Sicherheitsbaustein – Kategorie 3 – PL e (Beispiel 29)

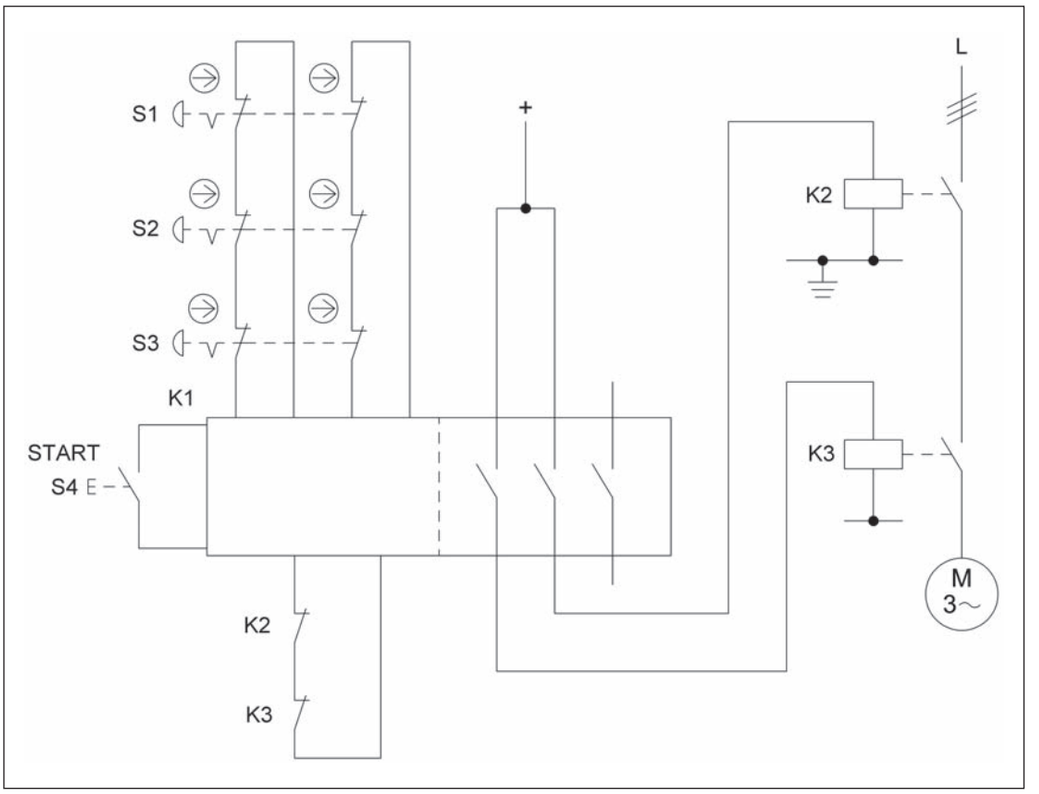


Abbildung 8.48: Kaskadierung von Not-Halt-Geräten mittels Sicherheitsbaustein (Not-Halt-Funktion, STO)

Sicherheitsfunktion

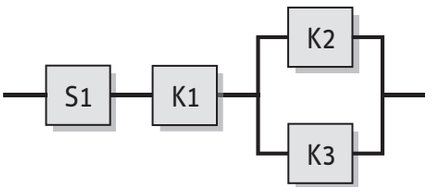
- Not-Halt-Funktion, STO durch Betätigung eines Not-Halt-Gerätes

Funktionsbeschreibung

- Gefahrbringende Bewegungen oder Zustände werden durch Betätigung eines Not-Halt-Gerätes unterbrochen bzw. verhindert. Entsprechend Beispiel 3 in Abschnitt 5.3.2 löst jedes Not-Halt-Gerät eine eigene Sicherheitsfunktion aus. Stellvertretend wird im Folgenden nur S1 betrachtet. Die Auswertung von S1 erfolgt in einem Sicherheitsbaustein K1, der zwei redundante Hilfsschütze K2 und K3 ansteuert.
- Die Not-Halt-Geräte werden zur Fehlererkennung redundant in den Sicherheitsbaustein K1 eingelesen. Dieser verfügt außerdem über interne Testmaßnahmen. Die Hilfsschütze K2 und K3 werden mithilfe zwangsgeführter Rücklesekontakte ebenfalls in K1 überwacht. Ein Schalten von K2 und K3 erfolgt bei jedem Startbefehl durch den Schalter S4, ca. zweimal pro Monat. Eine Fehlerhäufung von mehr als zwei Fehlern zwischen zwei aufeinander folgenden Betätigungszeitpunkten kann zum Verlust der Sicherheitsfunktion führen.
- Es wird nicht unterstellt, dass mehr als ein Not-Halt-Gerät gleichzeitig gedrückt wird.

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.
- Bei den Not-Halt-Geräten S1, S2, S3 handelt es sich um Schaltgeräte mit zwangsöffnenden Kontakten entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Schaltgeräten sind geschützt verlegt.



- Der Sicherheitsbaustein K1 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- K2 und K3 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.

Bemerkung

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

Berechnung der Ausfallwahrscheinlichkeit

- Bei S1, S2, S3 handelt es sich um handelsübliche Not-Halt-Geräte nach DIN EN ISO 13850. Es erfolgt jeweils ein Fehlerausschluss für den zwangsöffnenden Kontakt und die Mechanik, sofern die in Tabelle D.2 dieses Reports angegebene Anzahl der Betätigungen nicht überschritten wird.
- Die Ausfallwahrscheinlichkeit des fertigen Sicherheitsbausteins K1 wird am Ende der Berechung addiert ($2{,}31 \cdot 10^{-9}$/Stunde [H], geeignet für PL e). Für das Subsystem K2/K3 wird die Ausfallwahrscheinlichkeit im Folgenden berechnet.
- $MTTF_d$: Für die Hilfsschütze K2 und K3 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. Bei jährlich drei Anforderungen der Not-Halt-Funktion und 24 Startbefehlen ist n_{op}= 27 Zyklen/Jahr und $MTTF_d$ beträgt 740 740 Jahre. Dies ist gleichzeitig die symmetrisierte $MTTF_d$ für den Kanal, die auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg}: DC = 90 % für K2 und K3 beruht auf der Testung durch den Sicherheitsbaustein K1. Dies ist gleichzeitig DC_{avg} („mittel“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), bewährte Bauteile (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Das Subsystem K2/K3 entspricht Kategorie 3 mit hoher $MTTF_d$ (100 Jahre) und mittlerem DC_{avg} (90 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}29 \cdot 10^{-8}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $4{,}52 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Damit ist der PL_r = d übertroffen.

8.2.30 Schützüberwachungsbaustein – Kategorie 3 – PL e (Beispiel 30)

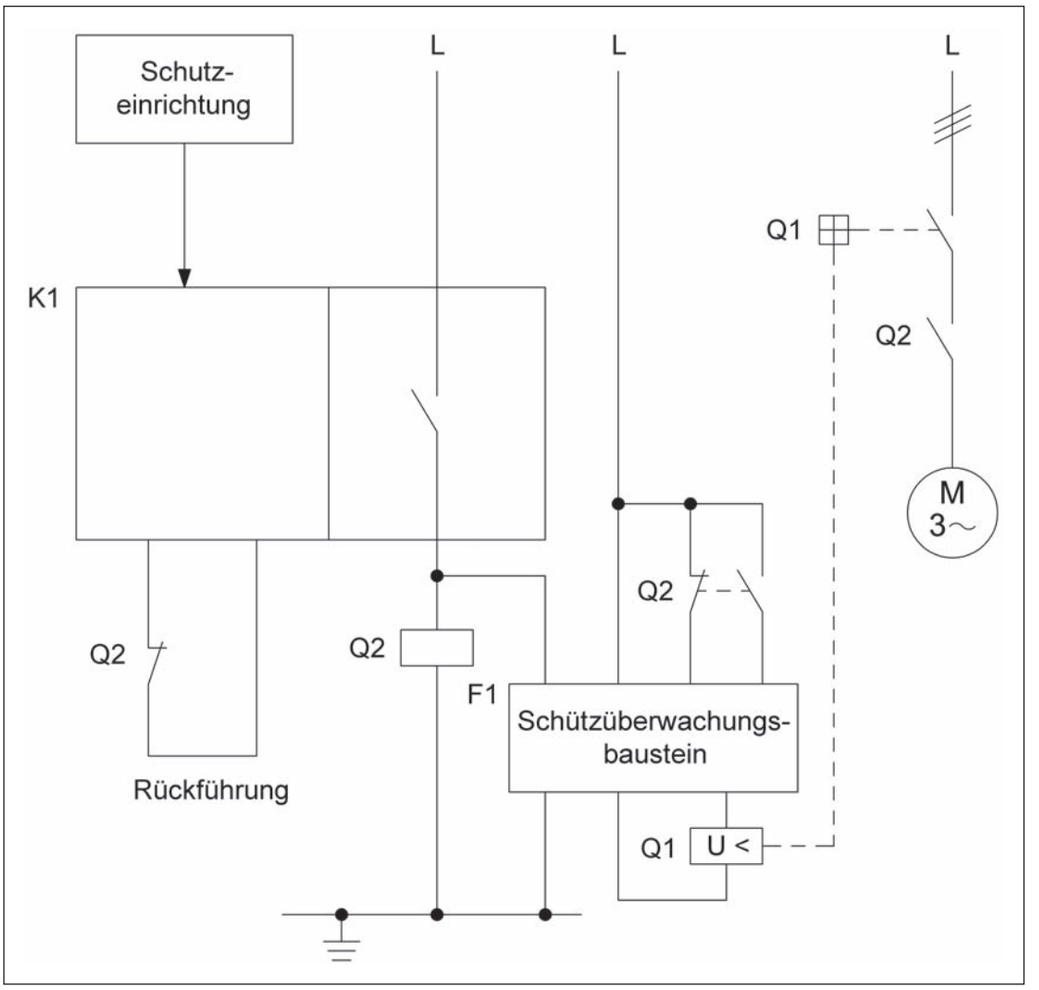


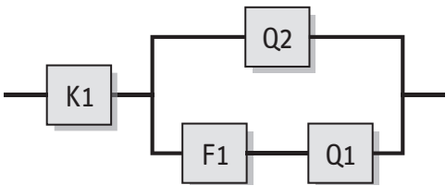
Abbildung 8.49: Einleitung des STO – Sicher abgeschaltetes Moment mittels Sicherheitsbaustein und Schützüberwachungsbaustein

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der beweglichen trennenden Schutzeinrichtung leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt mit einer Schutzeinrichtung, deren Öffnen durch einen Sicherheitsbaustein K1 detektiert wird. Dieser steuert ein Leistungsschütz Q2 und eine Kombination aus einem Schützüberwachungsbaustein F1 und einer Unterspannungsauslösung Q1 an. Das Abfallen von Q2 unterbricht gefahrbringende Bewegungen bzw. verhindert gefahrbringende Zustände. Der Schützüberwachungsbaustein F1 hat die Funktion, die Hauptkontakte von Leistungsschütz Q2 auf Verschweißen zu überwachen. Fällt Q2 nicht ab, löst F1 den vorgeordneten Leistungsschalter oder Motorstarter Q1 über dessen Unterspannungsauslösung aus. Dieser schaltet dann den Motor ab.
- Bei Auftreten eines Bauteilausfalls bleibt die Sicherheitsfunktion erhalten.
- Eine Fehlerhäufung zwischen zwei aufeinander folgenden Betätigungen kann zum Verlust der Sicherheitsfunktion führen.



Konstruktive Merkmale

- Der Leistungsschalter Q1 wird über eine manuell zu implementierende Testfunktion regelmäßig geprüft. Die Zeit zwischen den Tests sollte ein Hundertstel der $MTTF_d$ von Q1 nicht überschreiten und könnte z.B. bei Maschinenwartung erfolgen. Das Schütz Q2 wird durch den Schützüberwachungsbaustein ständig getestet. Ein Verlust der Sicherheitsfunktion zwischen den Tests – wie es bei Kategorie 2 möglich ist – kann nicht vorkommen. Die Einfehlersicherheit ist damit gewährleistet und die Anforderungen der Kategorie 3 sind erfüllt.

- 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.

- Aus Vereinfachungsgründen wurde bei der Darstellung auf Details zur Schutzeinrichtung verzichtet.

- Die Schutzeinrichtung wirkt auf einen Sicherheitsbaustein K1, der alle Anforderungen für Kategorie 3 oder 4 und PL e erfüllt.

- Das Schütz Q2 besitzt Spiegelkontakte entsprechend DIN EN 60947-4-1, Anhang F, und ist in die Rückführung des Sicherheitsbausteins K1 zur Fehlerdetektion des Schützes eingebunden.

- Die Fehlerbetrachtung für Q2 (mit Spiegelkontakten) und für das interne Relais des Schützüberwachungsbausteins F1 erfolgt wie bei zwangsgeführten Kontakten.

Bemerkung

- Die Reaktionszeit durch den Schützüberwachungsbaustein F1 hinsichtlich des Abfalls von Q1 ist zu berücksichtigen.

Berechnung der Ausfallwahrscheinlichkeit

- Die Sicherheitsfunktion lässt eine Aufteilung in zwei Subsysteme zu. Das Subsystem aus Schutzeinrichtung und Sicherheitsbaustein K1 wird in diesem Beispiel nicht berücksichtigt.

- $MTTF_d$: Für den Schützüberwachungsbaustein F1 beträgt die $MTTF_d$ 125 Jahre bei maximaler n_{op} = 350 400 Zyklen/Jahr [H]. Bei induktiver Last (AC3) ergibt sich für Q1 ein B_{10d}-Wert von 10 000 Schaltspielen und für Q2 ein B_{10d}-Wert von 1 300 000 Schaltspielen. Bei einer angenommenen täglichen Betätigung an 365 Arbeitstagen ist für Q1 n_{op}= 365 Zyklen/Jahr und $MTTF_d$ beträgt 274 Jahre. Bei 365 Arbeitstagen, 16 Arbeitsstunden und 1 Minute Zykluszeit ist für Q2 n_{op}= 350 400 Zyklen/Jahr und die $MTTF_d$ beträgt 37 Jahre. Für den aus F1 und Q1 bestehenden Kanal folgt eine $MTTF_d$ von 85 Jahren. Insgesamt ergibt sich ein symmetrisierter $MTTF_d$-Wert pro Kanal von 64 Jahren („hoch“).

- DC_{avg}: DC = 99 % für Q2 beruht auf der Testung über den Schützüberwachungsbaustein F1. DC = 99 % für F1 wird durch Fehler erkennende Maßnahmen innerhalb des Schützüberwachungsbausteins realisiert. Der Leistungsschalter wird über die zu implementierende manuelle Prüffunktion getestet, woraus sich DC = 90 % ableitet. Für F1 wird eine DC = 99 % angesetzt. Durch Mittelung ergibt sich damit ein DC_{avg} von 98 % („mittel“).

- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Das Subsystem, bestehend aus Q1, Q2 und F1, entspricht Kategorie 3 mit hoher $MTTF_d$ (64 Jahre) und mittlerem DC_{avg} (98 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}45 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen des Subsystems, bestehend aus Schutzeinrichtung und Sicherheitsbaustein K1, wird der PL unter Umständen geringer.

- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für das verschleißbehaftete Element Q2 ein T_{10d}-Wert von 3,7 Jahren für den vorgesehenen Austausch.

8.2.31 Pneumatische Ventilsteuerung (Subsystem) – Kategorie 4 – PL e (Beispiel 31)

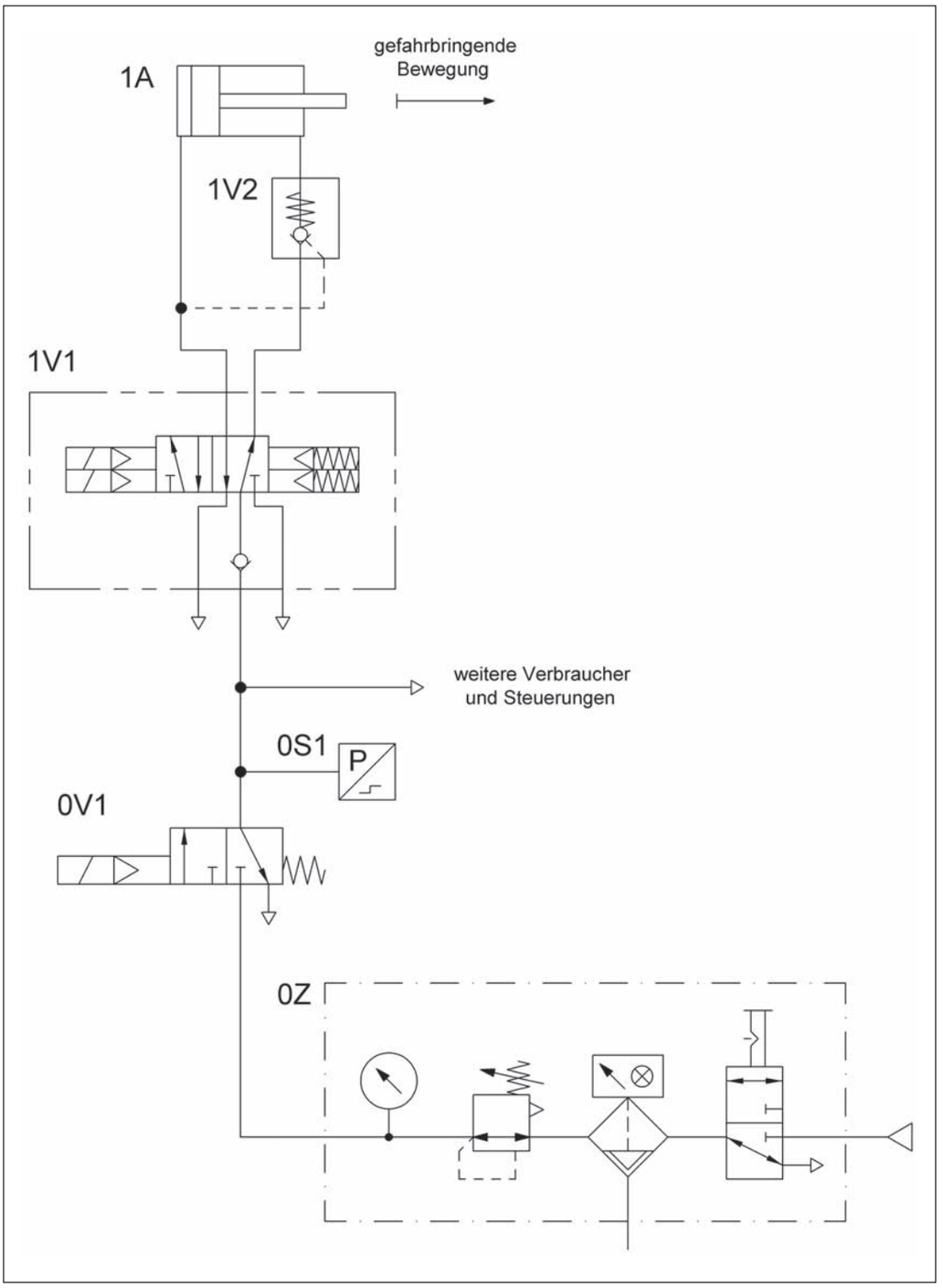
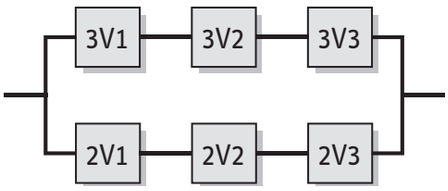


Abbildung 8.50: Getestete pneumatische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Funktion: Reversieren der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- Hier ist nur der pneumatische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.



Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch eine selbstüberwachte Ventilkombination 1V1 gesteuert, in Verbindung mit einem entsperrbaren Rückschlagventil 1V2 (bei Ausfall der Druckluft und äußeren Kräften von Bedeutung).
- Ein Bauteilausfall innerhalb der Ventilkombination führt nicht zum Verlust der Sicherheitsfunktion.
- Beide in 1V1 enthaltenen Vorsteuerventile der Ventilkombination werden getrennt angesteuert. Nach Wegnahme mindestens eines Steuersignals erfolgt immer eine Reversierung der Bewegung.
- Der einzelne Fehler innerhalb der Ventilkombination führt zu einer Selbsthemmung im sicheren Zustand und wird daher im Arbeitsprozess erkannt; ein Einleiten der nächsten gefahrbringenden Bewegung wird verhindert.
- Die Ventilkombination 1V1 kann auch durch mehrere Ventile mit einer entsprechenden Verknüpfung und einer entsprechenden Stellungsabfrage der Schaltstellungen aufgebaut werden.
- Kann durch eingesperrte Druckluft eine weitere Gefährdung auftreten, sind weitere Maßnahmen erforderlich.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- 1V1 ist eine selbstüberwachte Ventilkombination mit mechanisch getrennten integrierten Vorsteuerventilen und pneumatisch/mechanisch realisierter Fehlererkennung mit integriertem Rückschlagventil in der P-Leitung.
- Die sicherheitsgerichtete Schaltstellung wird durch Wegnahme der Steuersignale erreicht.
- Das entsperrbare Rückschlagventil 1V2 ist möglichst im Zylinder eingeschraubt.
- Die Fehlererkennung innerhalb der Ventilkombination erfüllt entsprechende Anforderungen an den Fehlerfall.

Berechnung der Ausfallwahrscheinlichkeit

Die Ventilkombination1V1 besteht aus zwei Ventilkanälen mit jeweils drei verbundenen Ventilen. Diese sind im Blockschaltbild bezeichnet mit 2V1, 2V2 und 2V3 sowie 3V1, 3V2 und 3V3.

- $MTTF_d$: Für jedes der Ventile der Ventilkombination 1V1 wird ein B_{10d}-Wert von 20 000 000 Zyklen [N] angenommen. Bei 240 Arbeitstagen, 16 Arbeitsstunden und 10 Sekunden Zykluszeit ist n_{op} = 1 382 400 Zyklen/Jahr und $MTTF_d$ = 144 Jahre. Dies ergibt einen $MTTF_d$-Wert pro Kanal von 48 Jahren („hoch“).
- DC_{avg}: DC = 99 % für 1V1 ergibt sich über eine Zwangsführung der beiden Ventilkanäle bei gleichzeitigem internen Kreuzvergleich des Steuerdruckes(Steuerdrucküberwachung). Damit ergibt sich ein DC_{avg} von ebenfalls 99 % („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der pneumatischen Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_d$ (48 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}60 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL unter Umständen geringer.
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für die verschleißbehaftete Ventilkombination 1V1 ein Wert von 14 Jahren (T_{10d}) für den vorgesehenen Austausch.

8.2.32 Hydraulische Ventilsteuerung (Subsystem) – Kategorie 4 – PL e (Beispiel 32)

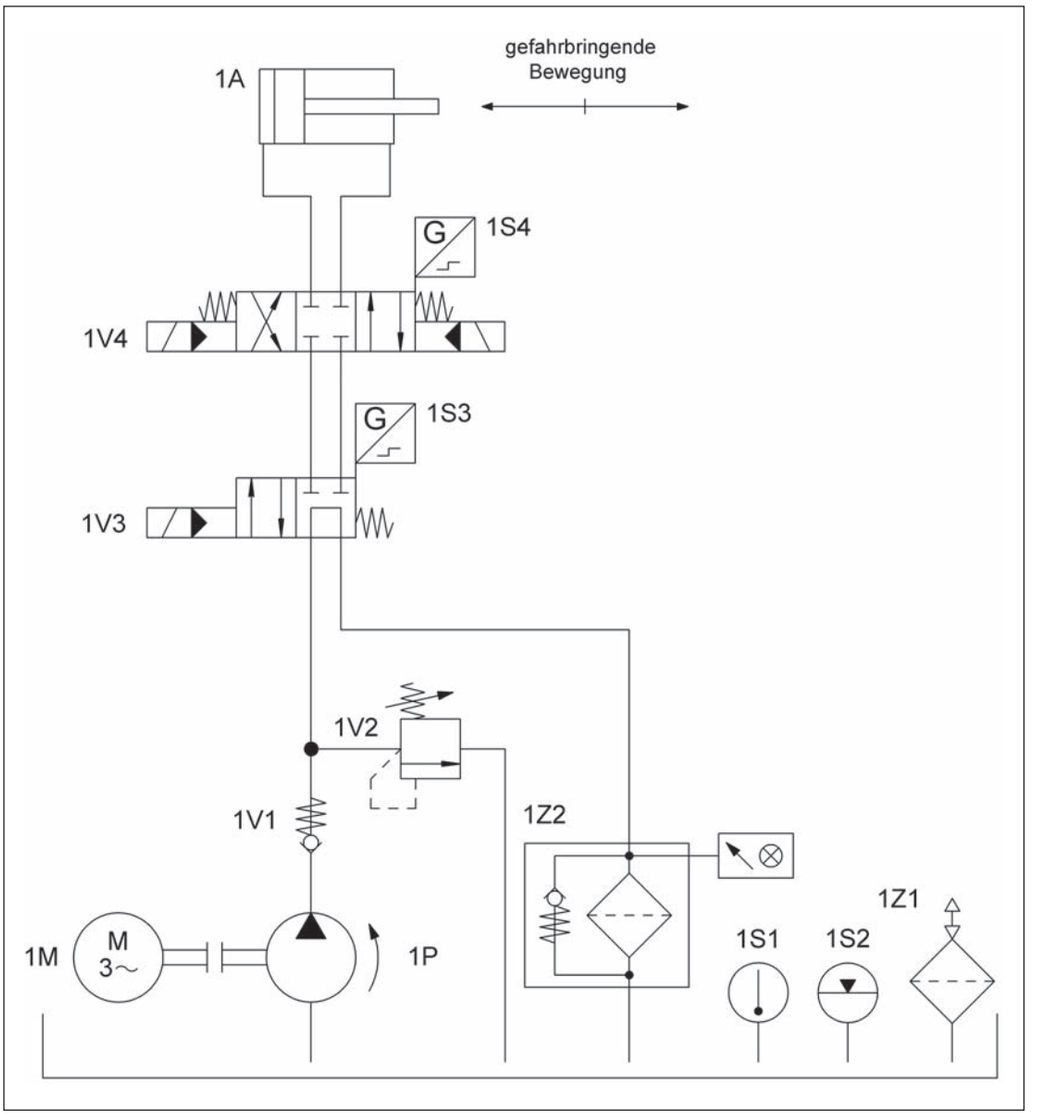


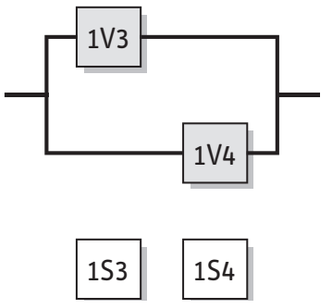
Abbildung 8.51: Getestete hydraulische Ventile zur redundanten Steuerung von gefahrbringenden Bewegungen

Sicherheitsfunktionen

- Sicherheitsbezogene Stoppfunktion: Stillsetzen der gefahrbringenden Bewegung und Verhinderung des ungewollten Anlaufs aus der Ruhelage
- Hier ist nur der hydraulische Steuerungsteil als Subsystem gezeigt. Für die komplette Sicherheitsfunktion sind weitere sicherheitsbezogene Steuerungsteile (z.B. Schutzeinrichtungen und elektrische Logik) als Subsysteme hinzuzufügen.

Funktionsbeschreibung

- Gefahrbringende Bewegungen werden durch zwei Wegeventile (1V3 und 1V4) gesteuert.
- Der einzelne Ausfall eines der genannten Ventile führt nicht zum Verlust der Sicherheitsfunktion.
- Beide Wegeventile werden zyklisch angesteuert.
- An beiden Wegeventilen ist jeweils eine direkte Stellungsüberwachung (1S3 und 1S4) vorgesehen. Der Ausfall jedes der beiden Wegeventile wird erkannt; nach einem Fehler wird das Einleiten der nächsten gefahrbringenden Bewegung verhindert.



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten.
- Die Wegeventile 1V3 und 1V4 haben eine Sperr-Mittelstellung mit ausreichender positiver Überdeckung, Federzentrierung bzw. -rückstellung sowie eine elektrische Stellungsüberwachung.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.
- Die Signalverarbeitung der elektrischen Stellungsüberwachung erfüllt entsprechende Anforderungen zur Beherrschung von Ausfällen.

Berechnung der Ausfallwahrscheinlichkeit

- $MTTF_d$: Für die Wegeventile 1V3 und 1V4 wird eine $MTTF_d$ von 150 Jahren angenommen [N]. Dies ist gleichzeitig der $MTTF_d$-Wert pro Kanal, der auf 100 Jahre („hoch“) gekürzt wird.
- DC_{avg}: DC = 99 % für die Wegeventile 1V3 und 1V4 beruht auf der direkten Überwachung der Schaltzustände. Durch Mittelung ergibt sich damit ein DC_{avg} von ebenfalls 99 % („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der hydraulischen Steuerungselemente entspricht Kategorie 4 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. Dies entspricht PL e. Nach Hinzufügen weiterer sicherheitsbezogener Steuerungsteile als Subsysteme zur Vervollständigung der Sicherheitsfunktion wird der PL in der Regel geringer.

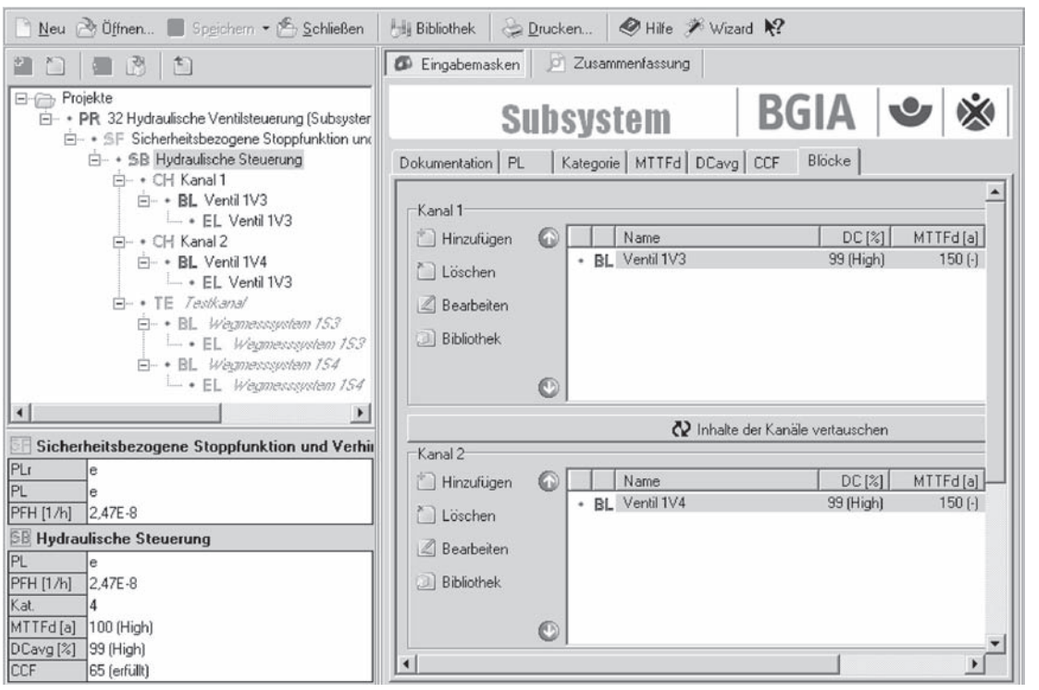


Abbildung 8.52: PL-Bestimmung mithilfe von SISTEMA

8.2.33 Elektrohydraulische Pressensteuerung – Kategorie 4 – PL e (Beispiel 33)

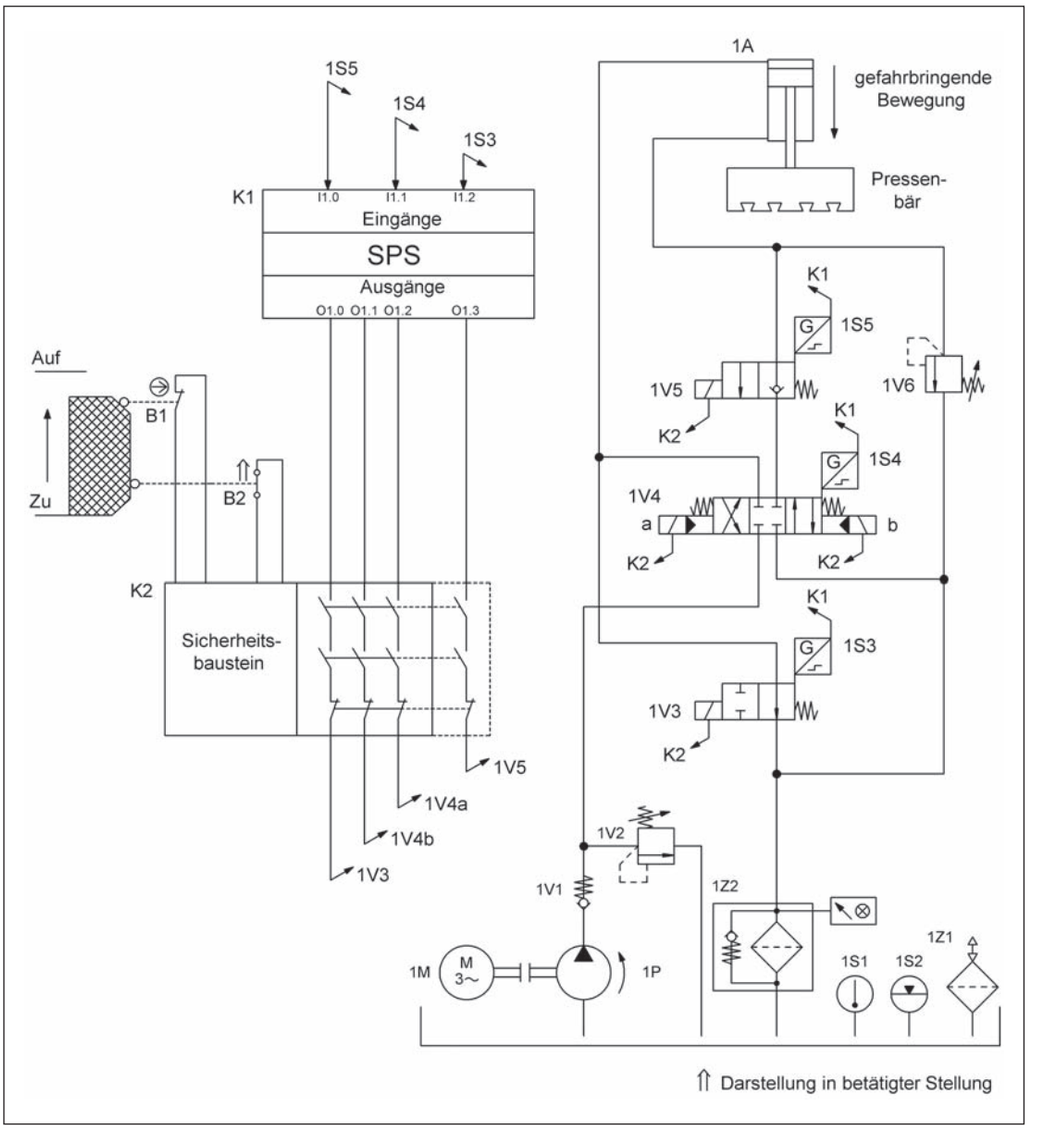


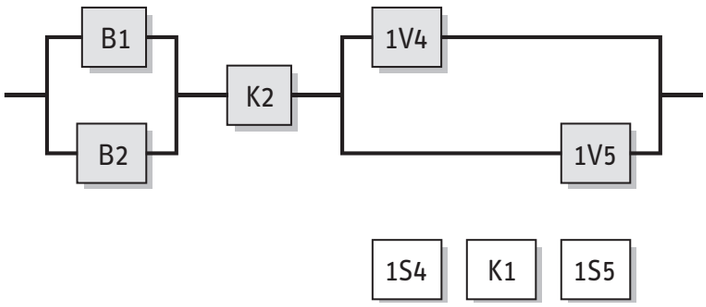
Abbildung 8.53: Pressensteuerung, elektrische Überwachung einer beweglichen trennenden Schutzeinrichtung mit hydraulischem Stillsetzen der gefahrbringenden Bewegung

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Stillsetzen der gefahrbringenden Bewegung

Funktionsbeschreibung

- Der Gefahrenbereich ist mittels einer beweglichen trennenden Schutzeinrichtung gesichert, deren Stellung von zwei Positionsschaltern B1 und B2 in Öffner-Schließer-Kombination erfasst wird. Die Signale werden in einen handelsüblichen Sicherheitsbaustein K2 eingelesen, der in den Freigabepfad der elektrischen Vorsteuerung K1 (herkömmliche SPS) für die hydraulischen Aktoren eingeschleift ist. Gefahrbringende Bewegungen oder Zustände werden aktorseitig durch drei Wegeventile (1V3, 1V4 und 1V5) gesteuert. Voraussetzung dafür ist ein Fehlerausschluss für das Druckbegrenzungsventil 1V6. Wenn z.B. die Feder bricht, wird die Abwärtsbewegung des Oberwerkzeugs nicht gestoppt. Die sicherheitsbezogene Stoppfunktion wird mittels der Ventile 1V4 und 1V5 realisiert. Das Ventil 1V3 wird z.B. für die Sicherheitsfunktion „Verhinderung eines unerwarteten Anlauf aus der Ruhelage“ benötigt. Diese und weitere Sicherheitsfunktionen werden hier jedoch nicht behandelt.



- Bei Anforderung der Sicherheitsfunktion werden beide Ventile durch K2 stromlos geschaltet und gehen aufgrund der vorhandenen Rückstellfedern in die Sperr-Mittelstellung (1V4) bzw. in die Sperr-Stellung (1V5). Dabei wird der Ölrückfluss von der Kolbenunterseite des Zylinders zum Tank durch die beiden Ventile gleichzeitig unterbrochen. Bei Ventil 1V5 handelt es sich um ein Sitzventil, das aufgrund seiner Konstruktion den Volumenstrom leckagefrei absperrt. Ventil 1V4, das auch die Bewegungsrichtung des Zylinders steuert, ist ein Wegeventil in Schieberbauweise, das auch in der Sperr-Mittelstellung eine gewisse Leckage aufweist.
- Der Ausfall eines Ventils führt nicht zum Verlust der Sicherheitsfunktion. Beide Ventile werden zyklisch angesteuert.
- An beiden Ventilen ist jeweils eine Stellungsabfrage 1S4 bzw. 1S5 zur Fehlererkennung vorgesehen. Der Ausfall jedes der beiden Ventile wird in der herkömmlichen SPS K1 erkannt, die nach einem Fehler das Einleiten der nächsten gefahrbringenden Bewegung verhindert.
- Ein einzelner Fehler in einer sicherheitstechnischen Komponente führt nicht zum Verlust der Sicherheitsfunktion. Darüber hinaus werden einzelne Fehler bei oder vor der nächsten Anforderung erkannt. Eine Anhäufung von unerkannten Fehlern führt nicht zum Verlust der Sicherheitsfunktion.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B werden eingehalten. Schutzbeschaltungen (z.B. Kontaktabsicherung) wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.
- Ein stabiler Aufbau der Schutzeinrichtung zur Betätigung der Positionsschalter ist sichergestellt.
- Der Schalter B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Der handelsübliche Sicherheitsbaustein K2 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Die Zuleitungen zu den Positionsschaltern sind getrennt oder geschützt verlegt.
- Für K1 wird eine handelsübliche SPS ohne Sicherheitsfunktionen verwendet.
- Die Ventile 1V4 und 1V5 haben eine Sperr-Mittelstellung bzw. Sperr-Stellung mit ausreichender positiver Überdeckung, Federzentrierung bzw. -rückstellung und sind stellungsüberwacht.
- Die sicherheitsgerichtete Schaltstellung wird jeweils durch Wegnahme des Steuersignals erreicht.

Berechnung der Ausfallwahrscheinlichkeit

- K2 wird als Subsystem mit einer Ausfallwahrscheinlichkeit von $2{,}31 \cdot 10^{-9}$/Stunde [H] betrachtet. Der übrige Steuerungsteil wird getrennt nach Elektromechanik und Hydraulik zu zwei Subsystemen der Kategorie 4 zusammengefasst, deren Ausfallwahrscheinlichkeit im Folgenden berechnet wird.
- $MTTF_d$: Für den Positionsschalter mit Zwangsöffnung B1 ist ein Fehlerausschluss für den elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt von Positionsschalter B2 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B1 und B2 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 die $MTTF_d$ beträgt 285 Jahre für B1 bzw. 142 Jahre für B2. Für die Ventile 1V4 und 1V5 wird jeweils eine $MTTF_d$ von 150 Jahren [N] angenommen. Daraus ergibt sich ein gekürzter $MTTF_d$-Wert pro Kanal von 100 Jahren („hoch“) für beide Subsysteme.

- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung beider Schaltzustände in K2. Der DC von 99 % für beide Ventile beruht auf der direkten Überwachung der Schaltzustände durch die SPS K1. Dies ergibt einen DC_{avg} von 99 % („hoch“) für beide Subsysteme.
- Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (75 Punkte) für beide Subsysteme: Trennung (15), bewährte Bauteile (5), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Der elektromechanische und der hydraulische Teil der Steuerung entsprechen Kategorie 4 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich jeweils eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde. Für die komplette Sicherheitsfunktion ergibt sich durch Addition inklusive K2 eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $5{,}16 \cdot 10^{-8}$ pro Stunde. Dies entspricht PL e.

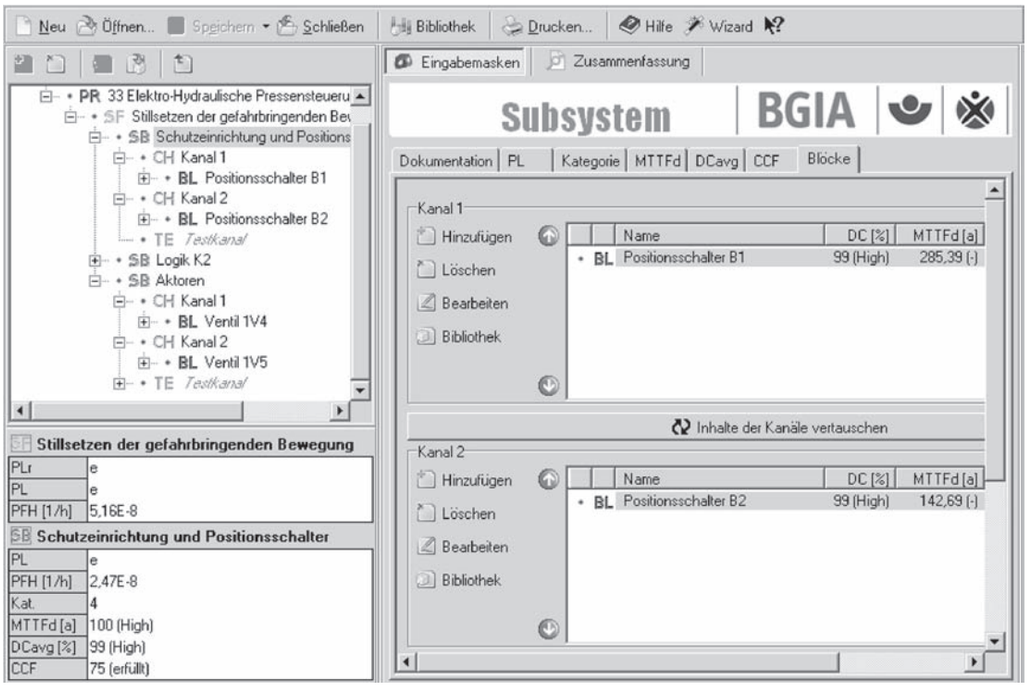


Abbildung 8.54: PL-Bestimmung mithilfe von SISTEMA

8.2.34 Stellungsüberwachung beweglicher trennender Schutzeinrichtungen – Kategorie 4 – PL e (Beispiel 34)

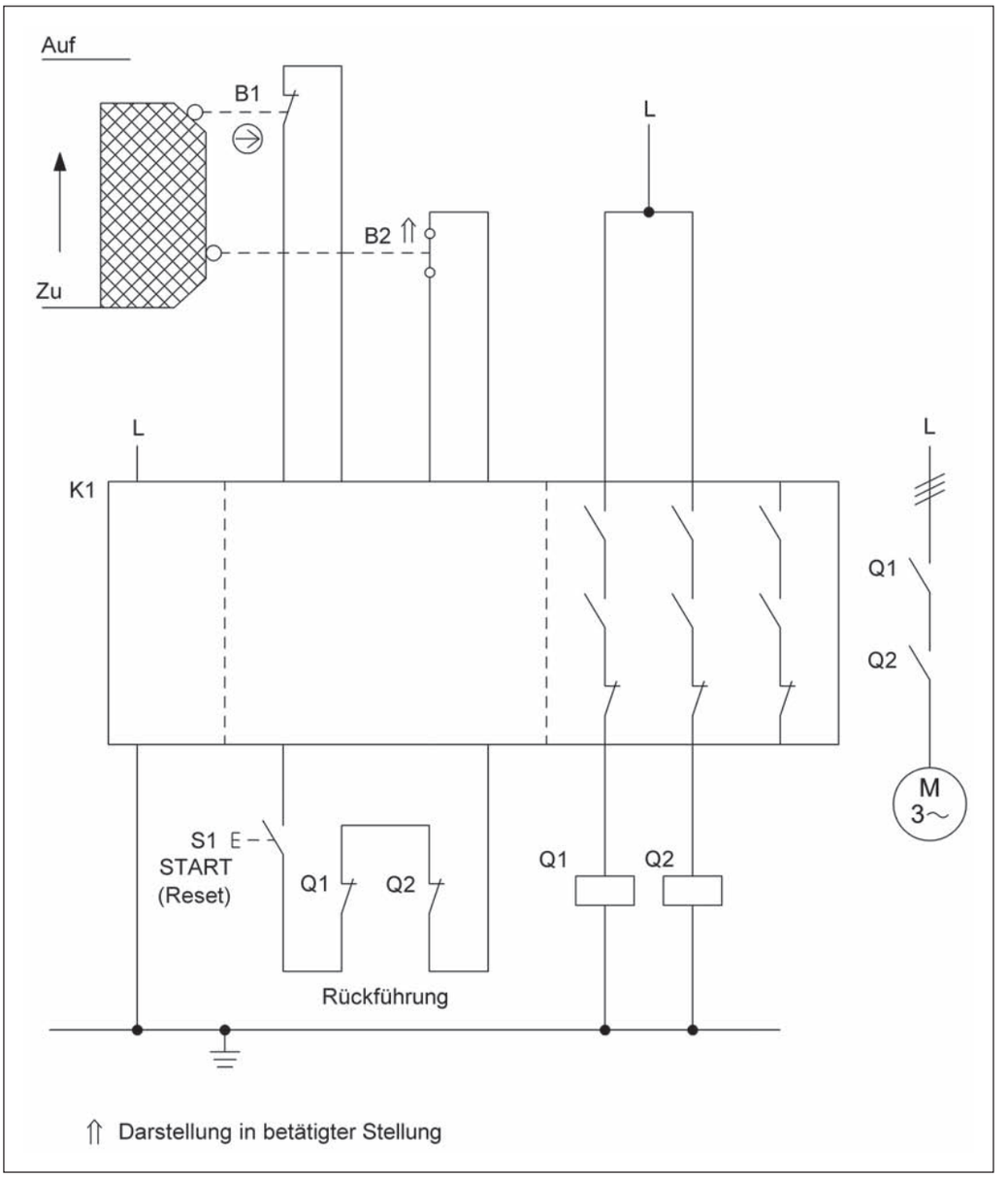


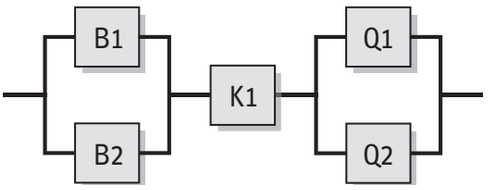
Abbildung 8.55: Stellungsüberwachung beweglicher trennender Schutzeinrichtung mittels Sicherheitsbaustein

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Das Öffnen der beweglichen trennenden Schutzeinrichtung (Schutzgitter) leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein.

Funktionsbeschreibung

- Die Sicherung einer Gefahrenstelle erfolgt mit einer beweglichen trennenden Schutzeinrichtung (Schutzgitter). Das Öffnen des Schutzgitters wird durch zwei Positionsschalter B1/B2 in Öffner-Schließer-Kombination erfasst und in einem zentralen Sicherheitsbaustein K1 ausgewertet. Dieser steuert zwei Schütze Q1 und Q2 an, durch deren Abfallen gefahrbringende Bewegungen oder Zustände unterbrochen bzw. verhindert werden.
- Die Positionsschalter werden zur Fehlererkennung in K1 auf Plausibilität überwacht. Fehler in Q1 und Q2 werden durch eine Anlauftestung in K1 erkannt. Ein Start-Befehl ist nur erfolgreich, wenn Q1 und Q2 vorher abgefallen waren. Es ist keine Anlauftestung durch Öffnen und Schließen der Schutzeinrichtung erforderlich.



- Die Sicherheitsfunktion ist auch erfüllt, wenn ein Bauteilausfall auftritt. Fehler werden während des Betriebs oder beim Betätigen (Öffnen und Schließen) der Schutzeinrichtung durch Abfall von Q1, Q2 und Betriebshemmung erkannt.
- Eine Fehlerhäufung von mehr als zwei Fehlern zwischen zwei aufeinander folgenden Betätigungszeitpunkten kann zum Verlust der Sicherheitsfunktion führen.

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.
- Der Schalter B1 ist ein Positionsschalter mit zwangsöffnendem Kontakt entsprechend DIN EN 60947-5-1, Anhang K.
- Die Zuleitungen zu den Positionsschaltern B1 und B2 sind getrennt oder geschützt verlegt.
- Der Sicherheitsbaustein K1 erfüllt alle Anforderungen für Kategorie 4 und PL e.
- Die Schütze K2, Q1, Q2 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.

Bemerkung

- Kategorie 4 wird nur eingehalten, wenn nicht mehrere mechanische Positionsschalter verschiedener Schutzeinrichtungen hintereinander geschaltet werden (keine Kaskadierung), da sonst keine Fehlererkennung in den Schaltern möglich ist.

Berechnung der Ausfallwahrscheinlichkeit

- Die Schaltung lässt sich in drei Subsysteme aufteilen, wie im sicherheitsbezogenen Blockdiagramm gezeigt. Die Ausfallwahrscheinlichkeit des handelsüblichen Sicherheitsbausteins K1 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.
- $MTTF_d$: Für den Positionsschalter mit Zwangsöffnung B1 ist ein Fehlerausschluss für den elektrischen Kontakt möglich. Für den elektrischen Schließerkontakt des Positionsschalters B2 beträgt B_{10d} = 1 000 000 Schaltspiele [H]. Für den mechanischen Teil von B1 und B2 wird ein B_{10d}-Wert von 1 000 000 Zyklen [H] angegeben. Bei 365 Arbeitstagen, 16 Arbeitsstunden und 1 Stunde Zykluszeit ist für diese Komponenten n_{op}= 5 840 Zyklen/Jahr und $MTTF_d$ beträgt 1 712 Jahre für B1 bzw. 856 Jahre für B2. Für die Schütze Q1 und Q2 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. Mit dem oben angenommenen Wert für n_{op} folgt für Q1 und Q2 eine $MTTF_d$ von 3 424 Jahren pro Kanal. Insgesamt ergibt sich in beiden Subsystemen ein symmetrisierter $MTTF_d$-Wert pro Kanal von 100 Jahren („hoch“).
- DC_{avg}: DC = 99 % für B1 und B2 beruht auf der Plausibilitätsüberwachung der Öffner-Schließer-Kombinationen in K1. DC = 99 % für die Schütze Q1 und Q2 ergibt sich aus der regelmäßigen Überwachung durch K1 beim Start. Die genannten DC-Werte entsprechen dem DC_{avg} für das jeweilige Subsystem.
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in den Subsystemen B1/B2 und Q1/Q2 (70 Punkte): Trennung (15), bewährte Bauteile (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Subsysteme B1/B2 und Q1/Q2 entsprechen jeweils Kategorie 4 mit hoher $MTTF_d$ (100 Jahre) und hohem DC_{avg} (99 %). Damit ergibt sich jeweils eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde. Nach Hinzufügen des Subsystems K1 beträgt die mittlere Wahrscheinlichkeit gefährlicher Ausfälle $5{,}16 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

8.2.35 Zweihandschaltung – Kategorie 4 – PL e (Beispiel 35)

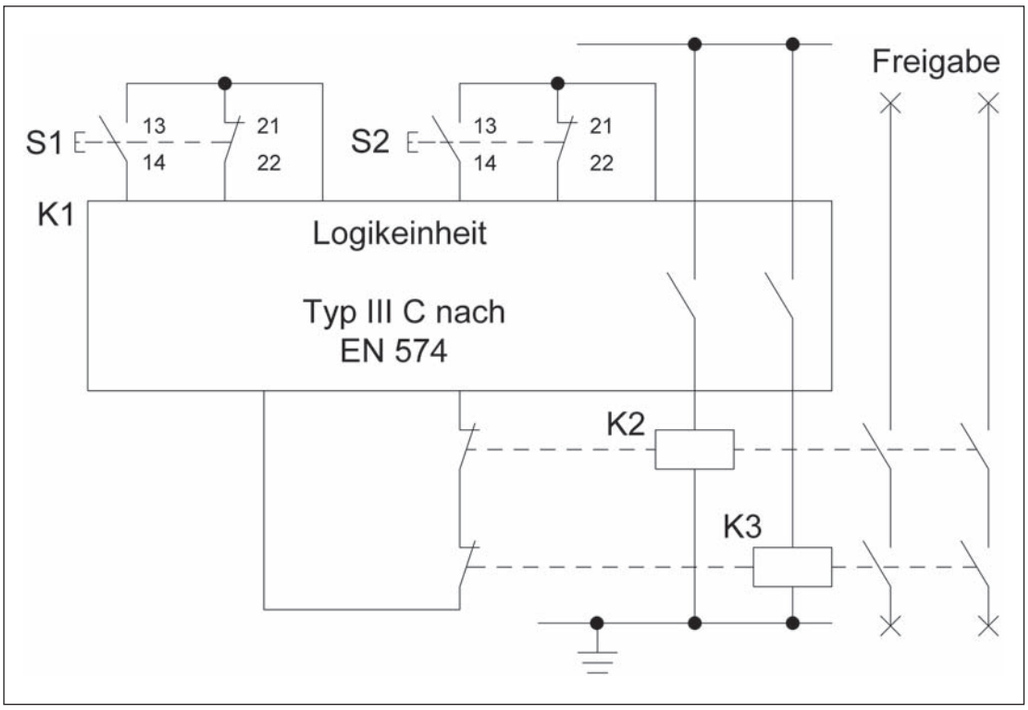


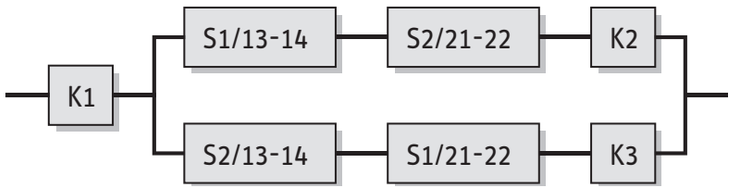
Abbildung 8.56: Zweihandschaltung, Signalverarbeitung durch eine Logikeinheit mit nachgeschalteten Hilfsschützen

Sicherheitsfunktion

- Ortsbindung der Hände des Bedieners außerhalb des Gefährdungsbereiches während einer gefahrbringenden Bewegung: Beim Loslassen mindestens eines der beiden Taster S1/S2 wird die Freigabe aufgehoben und solange blockiert, bis beide Taster entlastet und erneut synchron betätigt werden.

Funktionsbeschreibung

- Die Logikeinheit K1 überwacht die Betätigung der Stellteile (Taster) S1 und S2. Nur wenn beide aus dem entlasteten Zustand synchron (d.h. innerhalb einer festgelegten Zeitvorgabe) betätigt werden, ziehen die Hilfsschütze K2 und K3 an und die Freigabe erfolgt. Beim Loslassen mindestens eines der Taster S1/S2 heben K2/K3 die Freigabe auf.
- Durch K2 und K3 erfolgt eine Kontaktvervielfachung/Lastanpassung. Die eigentliche Verhinderung der gefahrbringenden Bewegung, z.B. durch Trennung der elektrischen oder hydraulischen Energie, ist anwendungsabhängig und hier nicht dargestellt.
- Störungen im Betätigungsmechanismus werden durch Verwendung von zwei prinzipverschiedenen Kontakten (Öffner-Schließer-Kombination) in S1/S2 weitestgehend erkannt. Hinsichtlich mechanischer Fehler kann für diese Anwendung ein Fehlerausschluss bzgl. des Nichtöffnens des Öffnerkontakts erfolgen, wenn die Taster DIN EN 60947-5-1 entsprechen.
- Fehler in S1/S2 und in K2/K3 (mit Öffnerkontakten im Rückführkreis) werden in K1 erkannt und führen zum dauerhaften Abschalten über K2 und K3. Alle Einzelfehler werden bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt.
- Eine häufige Betätigung der elektromechanischen Elemente sorgt für eine ausreichend hohe Testrate (Dynamisierung).



Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen (z.B. Kontaktabsicherung) wie in Abschnitt 8.1 beschrieben sind vorgesehen.
- Die Stellteile S1 und S2 der Zweihandschaltung entsprechen DIN EN 60947-5-1.
- Fehler in den Anschlussleitungen von S1 und S2 werden in der Logikeinheit erkannt. Wäre dies nicht möglich, so müssten die Bedingungen für einen Fehlerausschluss für Leitungskurzschlüsse nach DIN EN ISO 13849-2, Tabelle D.4, eingehalten werden. Wegen der geringen Ströme werden Taster mit Goldauflage empfohlen.
- Zum Anbau der Taster und zu Maßnahmen zur Vermeidung von versehentlicher Betätigung und von Umgehen siehe DIN EN 574, Abschnitt 8. Der Abstand zum Gefährdungsbereich muss ausreichend groß sein.
- Die Logikeinheit K1 entspricht Typ III C gemäß DIN EN 574 mit Selbstüberwachung und Erkennung interner Fehler. K1 ist ein geprüftes Sicherheitsbauteil für den Einsatz in Kategorie 4 und PL e.
- K2 und K3 besitzen zur Rücklesung zwangsgeführte Öffnerkontakte.

Bemerkung

- Anwendung z.B. an mechanischen Pressen (DIN EN 692)

Berechnung der Ausfallwahrscheinlichkeit

- K1 wird als Subsystem mit einer Ausfallwahrscheinlichkeit von $2{,}47 \cdot 10^{-8}$/Stunde [G] betrachtet. Der übrige Steuerungsteil wird zu einem Subsystem der Kategorie 4 zusammengefasst, dessen Ausfallwahrscheinlichkeit im Folgenden berechnet wird.
- Da S1 und S2 unabhängig voneinander beim Loslassen eine Abschaltung auslösen müssen, sind sie logisch in Reihe geschaltet. Dazu wurde je ein Schließerkontakt 13-14 und ein Öffnerkontakt 21-22 einem Steuerungskanal zugeordnet. Das sicherheitsgerichtete Blockdiagramm unterscheidet sich hier deutlich vom funktionalen Schaltplan. Wenn Zuverlässigkeitsdaten nur für die Taster insgesamt (Betätigungsmechanik plus Öffner- **und** Schließerkontakt) verfügbar sind, können die Ausfallwerte der Taster als Abschätzung zur sicheren Seite für die Ausfallwerte der Kontakte (plus Betätigungsmechanik) herangezogen werden.
- $MTTF_d$: Für S1 und S2 werden wegen des durch K1 erzeugten definierten Steuerstroms (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend) B_{10d}-Werte von je 20 000 000 Schaltspielen [H] angenommen. Da K2 und K3 ebenfalls Steuerströme schalten, gelten für K2 und K3 B_{10d}-Werte von je 20 000 000 Zyklen [N]. Bei 240 Arbeitstagen, 8 Arbeitsstunden und 20 Sekunden Zykluszeit ist für diese Komponenten n_{op} = 345 600 Zyklen/Jahr und $MTTF_d$ = 579 Jahre. Bei höheren Anforderungen (längere Arbeitszeit oder kürzere Zykluszeit) sind unter Umständen für K2/K3 höhere, durch den Hersteller abgesicherte B_{10d}-Werte erforderlich. Insgesamt ergibt sich ein $MTTF_d$-Wert pro Kanal von 193 Jahren, gekürzt auf 100 Jahre („hoch“).
- DC_{avg}: DC = 99 % für S1 und S2 ergibt sich durch die direkte Überwachung mithilfe der Öffner-Schließer-Kombinationen in K1. DC = 99 % für K2 und K3 gründet sich auf dem Rücklesen der zwangsgeführten Öffnerkontakte im Rückführkreis von K1. Die hohe Betätigungsdynamik in der Anwendung führt zu einer effektiven Testung. Durch Mittelung ergibt sich damit ein DC_{avg} von 99 % („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (70 Punkte): Trennung (15), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)
- Die Kombination der Steuerungselemente entspricht Kategorie 4 mit hoher $MTTF_d$ pro Kanal (100 Jahre) und hohem DC_{avg} (99 %). Für die Kombination von S1, S2, K2 und K3 ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $2{,}47 \cdot 10^{-8}$/Stunde. Wird ein Wert von $2{,}47 \cdot 10^{-8}$/Stunde [G] für K1 hinzuaddiert, so ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $4{,}94 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Unter Umständen ist zur Komplettierung der Sicherheitsfunktion zusätzlich die Ausfallwahrscheinlichkeit nachgeordneter Leistungselemente zu addieren.

Weiterführende Literatur

- DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte – Gestaltungsleitsätze (02.97). Beuth, Berlin 1997
- Recommendation for Use. Hrsg.: Vertikalgruppe 11 (VG 11) im europäischen Erfahrungsaustausch notifizierter Prüfstellen europa.eu.int/comm/enterprise/mechan_equipment/machinery/vertical_rfu.pdf. CNB/M/11.033/R/E Rev 05, S. 252, April 2006

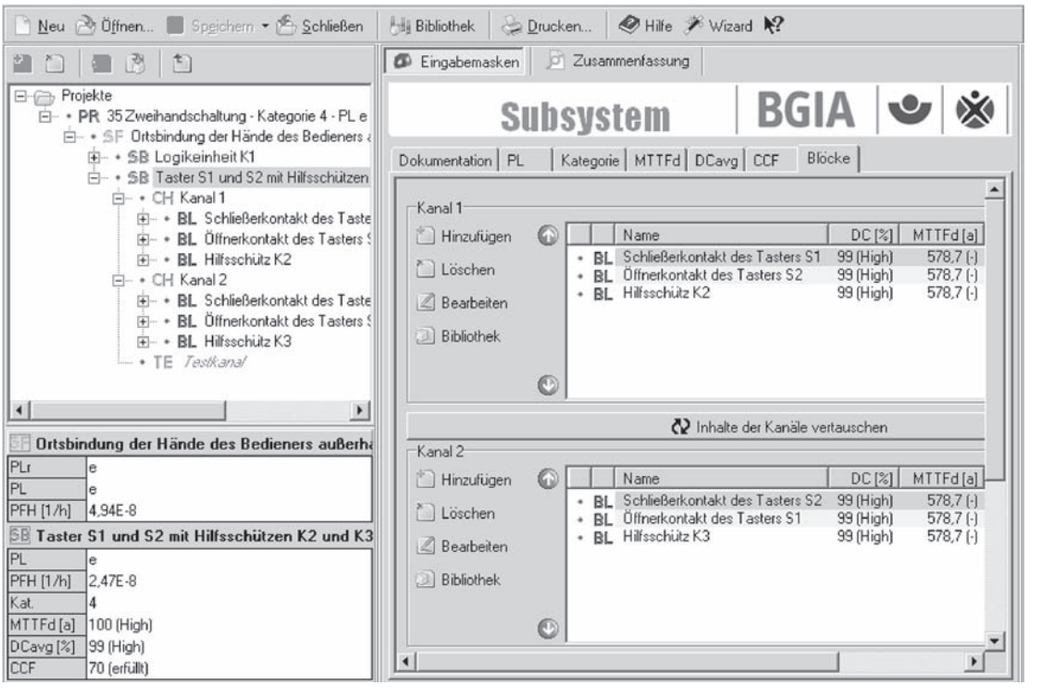


Abbildung 8.57: PL-Bestimmung mithilfe von SISTEMA

8.2.36 Verarbeitung von Signalen einer Lichtschranke – Kategorie 4 – PL e (Beispiel 36)

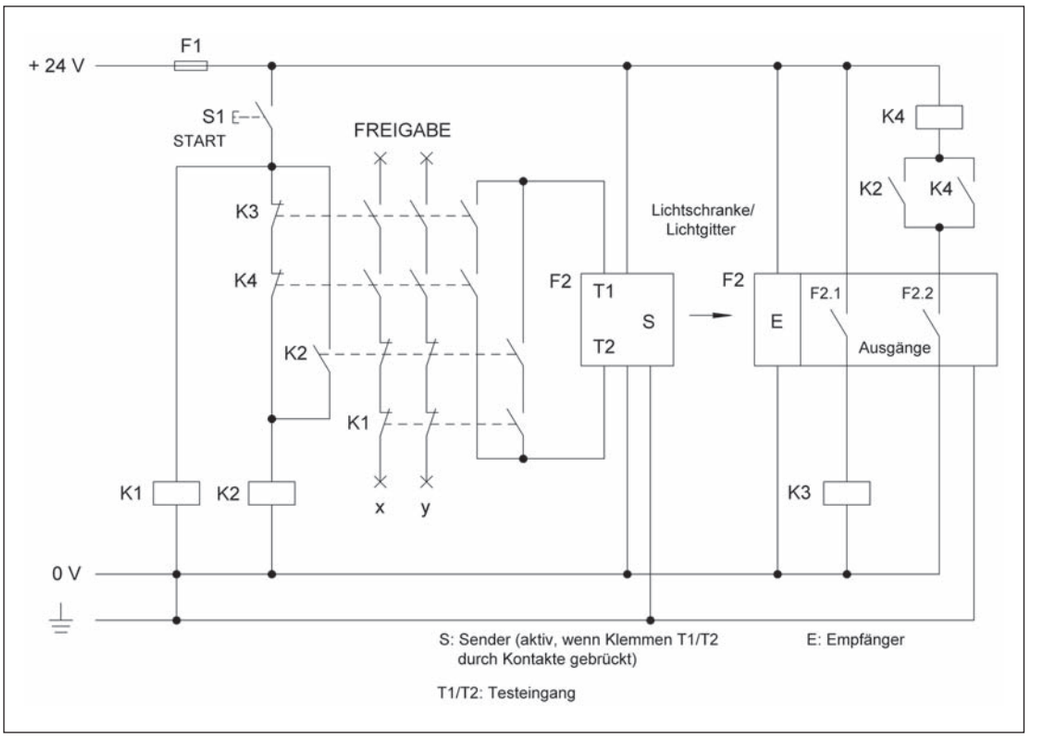


Abbildung 8.58: Elektromechanische Einbindung von sicherheitsrelevanten Signalen in die Maschinensteuerung am Beispiel einer Lichtschranke bzw. eines Lichtgitters

Sicherheitsfunktion

- Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine Schutzeinrichtung: Bleibende Stillsetzung einer gefahrbringenden Bewegung bei Zutritt zu einem Gefahrenbereich oder bei Eingriff in eine Gefahrenstelle sowie Anlauf- und Wiederanlaufsperre

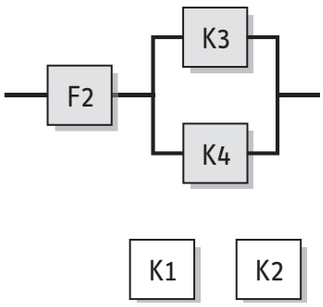
Funktionsbeschreibung

- Der Zutritt zu einem Gefahrenbereich oder Eingriff in eine Gefahrenstelle wird durch die Lichtschranke F2 detektiert. Die sicherheitsrelevanten Ausgangssignale der Lichtschranke (Schließer F2.1 und F2.2) entregen die in versetzter Spulenanordnung an die Spannungsversorgung angeschlossenen Hilfsschütze K3 und K4, die die Freigabesignale x und y sperren.

- Zur Aktivierung des Lichtschrankensenders werden bei betätigter Starttaste S1 die Testeingänge T1 und T2 zunächst über die dann angezogenen Hilfsschütze K1und K2 miteinander verbunden. K2 kann nur bei zunächst abgefallenen Hilfsschützen K3/K4 zum Anzug mit Selbsthaltung kommen. Bei geschlossener Lichtstrecke erfolgt dann auch der Anzug von K3 und K4. K4 gelangt nur über den Schließerkontakt von K2 zum Anzug mit Selbsthaltung. Mit dem Anzug von K3 und K4 ist bei noch betätigter Starttaste auch die Aktivierung des Lichtschrankensenders mit Selbsthaltung erfolgt, sodass die Starttaste losgelassen werden kann und mit dem Abfallen von K1 und K2 auch die Freigabepfade x und y geschlossen sind. Die Funktion der Anlaufsperre/Wiederanlaufsperre verhindert ein gültiges Freigabesignal nach einer Lichtstrahlunterbrechung oder nach einem Spannungsausfall mit darauf folgender Spannungswiederkehr so lange, bis nach einer erneuten Betätigung der Starttaste K3 und K4 wieder zum Anzug gelangen.

- Je ein Schließer von K3 und K4 ist sowohl in beiden Freigabepfaden als auch im Eingangskreis zur Aktivierung des Lichtschrankensenders (Testeingänge T1/T2) eingebunden. Mit dem Verbinden der Testeingänge erfolgt intern im Gerät eine Anlauftestung, z.B. durch eine definierte kurzzeitige Austastung des Lichtstrahls, die auf der Empfangsseite erwartungsgemäß nur innerhalb eines engen Zeitfensters als gültig bewertet wird. Bei erfolgreichem Anlauftest werden die Lichtschrankenausgänge frei geschaltet, im Störungs- bzw. Fehlerfall oder bei unterbrochener Lichtstrecke jedoch gesperrt.

- Fehler in den anderen Komponenten der Schaltung (Hilfsschütze, Ausgangskontakte der Lichtschranke, Starttaste), die in Kombination zum Verlust einer Sicherheitsfunktion führen könnten, werden nach einer Lichtstrahlunterbrechung während der Anlauf- bzw. Wiederanlauftestung aufgedeckt und verhindern eine erneute Freigabe.



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 bis K4 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L. Die Anzugsspannung der Hilfsschütze K3 und K4 muss größer als der halbe Wert der Spannungsversorgung gewählt werden, damit sich ein gleichzeitiger Anzug von K3 und K4 im Falle eines Kurzschlusses im Kabel (Reihenschaltung führt zur Spannungsaufteilung über den Schützspulen) auch in Kombination mit anderen Fehlern nicht gefahrbringend auswirken kann.
- Die Ausgangssignale der Lichtschranke F2 werden vom elektrischen Einbauraum des Empfängers gemeinsam in einem Kabel zusammen mit den Versorgungsleitungen zum elektrischen Einbauraum der Maschinensteuerung geführt. Durch Anwendung des Ruhestromprinzips und des Prinzips der versetzten Spulen (K3, K4) im geerdeten Steuerstromkreis werden alle im Kabel auftretenden Unterbrechungen, Erdschlüsse und Querschlüsse im aktivierten Zustand der Lichtschranke unmittelbar bemerkt (u.a. durch Ansprechen der Sicherung F1). Ein Kurzschluss, der die Überbrückung eines einzelnen Ausgangs bewirkt, wird spätestens nach dem Unterbrechen des Lichtstrahls der Lichtschranke beim erneuten Betätigen der Starttaste aufgedeckt. Daher ist gemeinsame Führung der Ausgangssignale innerhalb eines Kabels zulässig.
- Die Lichtschranke entspricht dem Typ 4 gemäß DIN EN 61496-1 und DIN CLC/TS 61496-2 sowie PL e.

Bemerkungen

- Wird die Schaltung in Anwendungen eingesetzt, bei denen die Lichtschranke sehr selten schaltet, so muss die Möglichkeit des Verlustes der Sicherheitsfunktion durch Fehlerhäufung (zwei einzeln unbemerkte Fehler) betrachtet werden. Periodische Prüfungen können einem solchen Verlust entgegenwirken.
- Angaben des Herstellers zur maximalen Schalthäufigkeit der Lichtschranke sind zu berücksichtigen.

Berechnung der Ausfallwahrscheinlichkeit

Es wird die Ausfallwahrscheinlichkeit der sicherheitsbezogenen Stoppfunktion, die auch im sicherheitsbezogenen Blockdiagramm dargestellt ist, berechnet. Werden die Kontakte der Freigabepfade x und y steuerungstechnisch weiterverarbeitet, so müssen diese zusätzlichen Steuerungsteile, z.B. Leistungsschütze, bei der Berechnung der Ausfallwahrscheinlichkeit berücksichtigt werden.

- Die Lichtschranke F2 liegt als handelsübliches Sicherheitsbauteil vor. Die Ausfallwahrscheinlichkeit $3{,}0 \cdot 10^{-8}$/Stunde [G] wird am Ende der Berechnung addiert.
- $MTTF_d$: Für K3 und K4 gilt wegen der unbekannten Lasten B_{10d} = 400 000 Zyklen [N]. Bei 220 Arbeitstagen, 8 Betriebsstunden/Tag und 120 Sekunden Zykluszeit beträgt n_{op} = 52 800 Schaltspiele/Jahr und damit die $MTTF_d$ 75 Jahre. Dies ist gleichzeitig die $MTTF_d$ pro Kanal („hoch“).
- DC_{avg}: DC = 99 % für K3 bis K4 ergibt sich aus der Einbindung der zwangsgeführten Öffnerkontakte in die Ansteuerung von K2. Dies entspricht gleichzeitig DC_{avg} („hoch“).
- Ausreichende Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (75 Punkte): Trennung (15), bewährte Bauteile (5), FMEA (5), Schutz gegen Überspannung usw. (15) und Umgebungsbedingungen (25 + 10)

- Das Subsystem K3/K4 entspricht Kategorie 4 mit hoher $MTTF_d$ pro Kanal (75 Jahre) und hohem DC_{avg} (99 %). Dies ergibt eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $3{,}37 \cdot 10^{-8}$/Stunde. Die Gesamtausfallwahrscheinlichkeit wird durch Addition der Wahrscheinlichkeit gefährlicher Ausfälle von F2 ($3{,}0 \cdot 10^{-8}$/Stunde) ermittelt und beträgt $6{,}37 \cdot 10^{-8}$/Stunde. Dies entspricht PL e. Unter Umständen ist zur Komplettierung der Sicherheitsfunktion zusätzlich die Ausfallwahrscheinlichkeit nachgeordneter Leistungselemente zu addieren.

- Die verschleißbehafteten Elemente K3 und K4 sollten nach jeweils ca. sieben Jahren (T_{10d}) ausgetauscht werden.

Weiterführende Literatur

- DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen (IEC 60204-1:2005, modifiziert). Abschnitt 9.4.3: „Schutz gegen fehlerhaften Betrieb durch Erdschlüsse, Spannungsunterbrechungen und Verlust der elektrischen Durchgängigkeit“. Beuth, Berlin 2007

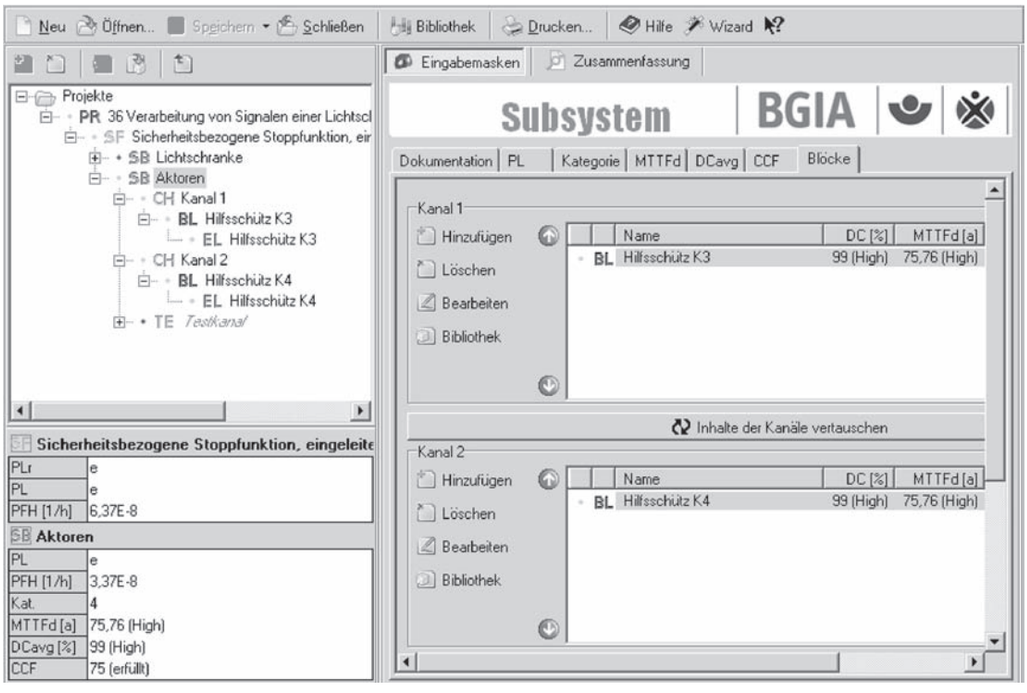


Abbildung 8.59: PL-Bestimmung mithilfe von SISTEMA

8.2.37 Planschneidemaschine mit programmierbar elektronischer Logiksteuerung – Kategorie 4 – PL e (Beispiel 37)

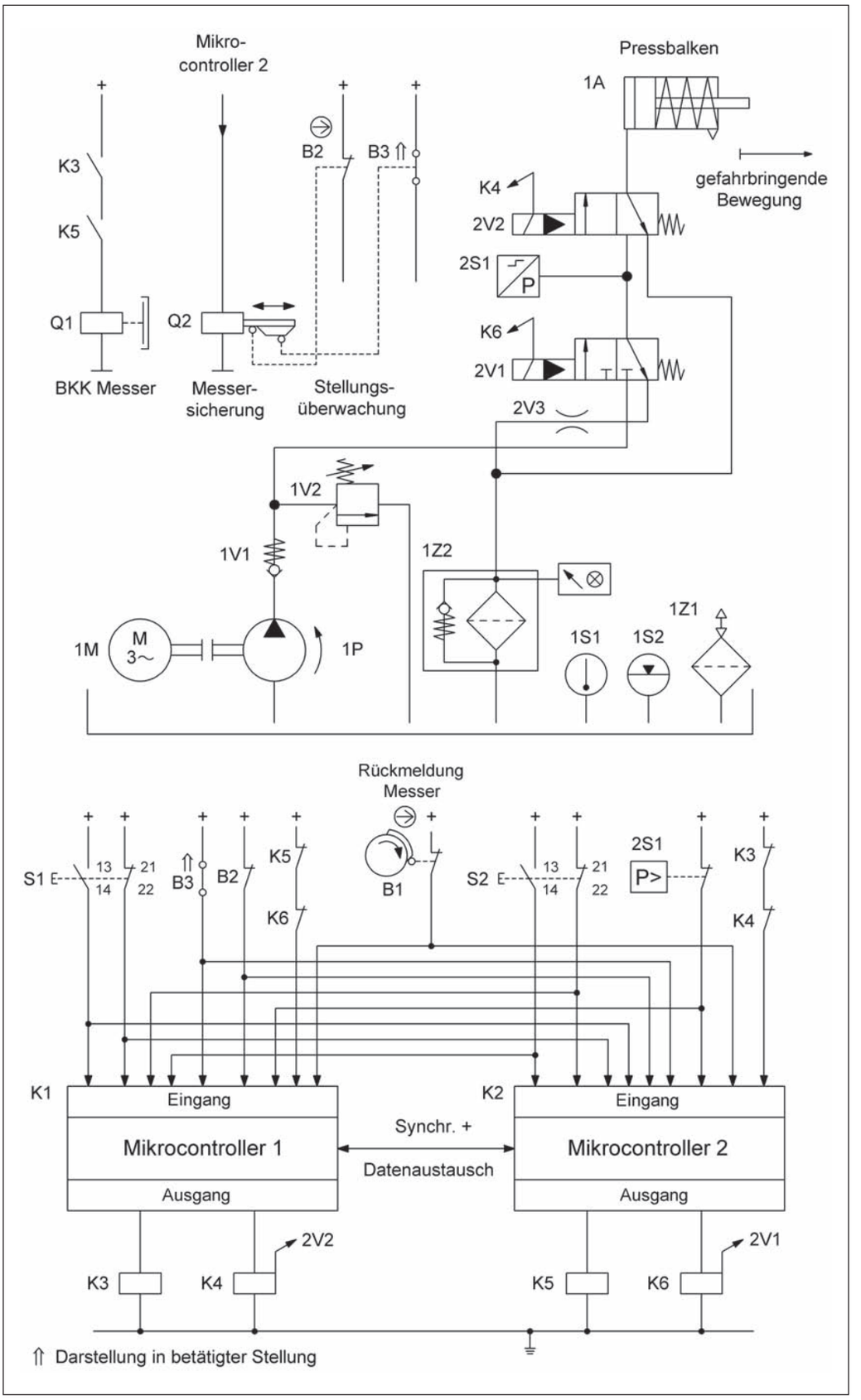
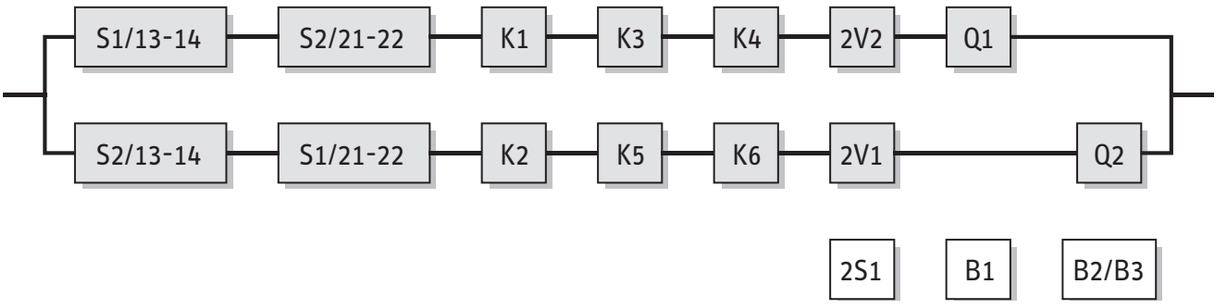


Abbildung 8.60: Ansteuerung eines elektrischen Messerantriebs und eines hydraulischen Pressbalkens



Sicherheitsfunktion

- Ortsbindung der Hände eines einzelnen Bedieners außerhalb des Gefährdungsbereiches während der Press- und Schneidbewegung: Beim Loslassen mindestens eines der beiden Taster S1/S2 wird die Freigabe aufgehoben und so lange blockiert, bis beide Taster entlastet und erneut synchron betätigt werden.

Funktionsbeschreibung

- Die Betätigung der Zweihandschaltung (ZHS) S1 und S2 startet die gefahrbringenden Bewegungen (Bearbeitungszyklus) des Pressbalkens (Hydraulik) 1A und des Messers (Elektromechanik). Wird während eines Zyklus auch nur ein Taster S1 oder S2 losgelassen, oder erfolgt ein Signalwechsel in der Peripherie der Maschine (z.B. Lichtgitter, im Schaltbild nicht dargestellt) nicht wie durch die Steuerung erwartet, stoppt der Zyklus und die Maschine verbleibt in diesem sicheren Zustand. Das Messer und der Pressbalken stellen wegen ihrer unmittelbaren räumlichen Nähe zueinander eine gemeinsame Gefahrstelle dar, die Gefährdung wiederholt sich zyklisch. Nicht explizit dargestellt ist der Antrieb des Messers durch einen Exzenterantrieb, dessen Energie aus einer kontinuierlich laufenden Schwungmasse entnommen wird. Der Pressbalken wird linear durch eine Hydraulik angetrieben, deren Pumpe an den Antrieb der Schwungmasse gebunden ist.

- Mit Drücken der Taster S1/S2 (ZHS) werden die Signalwechsel beiden Mikrocontrollern K1 und K2 zugeführt. Erfüllen diese Signale die Anforderungen an die Gleichzeitigkeit nach Norm (DIN EN 574, Typ III C) und erfüllen alle peripheren Signale eine Startbedingung, setzen K1 und K2 die Ausgänge für eine gültige Schnittanforderung. Über die Hilfsschütze K3 bis K6 kontrolliert jeder Mikrocontroller beide gefahrbringenden Bewegungen. Über zwei hydraulische Ventile 2V1 und 2V2 kann die Schließbewegung des Pressbalkens 1A unterbunden werden. Die Ansteuerung der Brems-/Kupplungskombination (BKK) Q1 kann über K3 und K5 unterbunden werden. Eine geeignet dimensionierte mechanische Konstruktion einer Messersicherung Q2 muss zusätzlich zyklisch von K2 freigegeben werden. Bei erkannten Fehlern in Q1 kann damit spätestens im Folgezyklus der Messerdurchlauf verhindert werden.

- Fehler in den Schaltern S1/S2 oder in den Hilfsschützen K3 bis K6 mit zwangsgeführten Rücklesekontakten werden durch einen Kreuzvergleich in den Mikrocontrollern erkannt. Die Funktion von 2V1/2V2 wird mithilfe des Druckschalters 2S1 überwacht. Da die Mikrocontroller während des Betriebs im Hintergrund zusätzlich Selbsttests ausführen, können hier interne Fehler und Fehler in der Peripherie rechtzeitig erkannt werden.

- Alle Maschinenzustände werden durch beide Mikrocontroller überwacht und gesteuert. Durch den zyklischen Ablauf eines Schnittes werden alle Systemzustände ebenfalls zyklisch durchlaufen und untereinander verglichen. Fehler und Abweichungen von definierten Zwischenzuständen führen spätestens nach einem durchlaufenen Zyklus zum Stopp der Maschine. Dieses Verfahren ist im Schaltbild durch „Rückmeldung Messer“ B1 und „Stellungsüberwachung“ B2/B3 der Messersicherung Q2 angedeutet.

- Die Überwachung eines Verschleißes der Bremse erfolgt mithilfe von Positionsschalter B1. Schon bei minimal erhöhtem Nachlauf wird B1 angefahren und ein weiterer Schnitt steuerungstechnisch verhindert.

Konstruktive Merkmale

- Grundlegende und bewährte Sicherheitsprinzipien sowie die Anforderungen der Kategorie B sind eingehalten. Schutzbeschaltungen wie in den ersten Abschnitten von Kapitel 8 beschrieben sind vorgesehen.

- Die Stellteile S1 und S2 der Zweihandschaltung entsprechen DIN EN 60947-5-1.

- B1 und B2 sind zwangsöffnende Positionsschalter entsprechend DIN EN 60947-5-1, Anhang K.

- K3 bis K6 besitzen zwangsgeführte Kontaktelemente entsprechend DIN EN 60947-5-1, Anhang L.

- Die Anschlussleitungen der Positionsschalter sind entweder getrennt oder gegen mechanische Beschädigung geschützt verlegt.

- Die Software der homogen redundanten Rechnerstruktur entspricht den Anforderungen der DIN EN 61508-3, Abschnitt 7, für SIL 3.

- Für den Fehler „vollständiges Versagen der Brems-/Kupplungskombination“, d.h. Nicht-Auskuppeln bei zurückgezogener Schnittfreigabe nach ausgelöstem Schnitt, erfolgt ein Fehlerausschluss. Dieser begründet sich in langjähriger Erfahrung und den konstruktiven Merkmalen der Brems-/Kupplungs-Kombination mit der Möglichkeit, einen Bremsenverschleiß frühzeitig zu bemerken.

- Die Bauteile B1 und B2/B3 werden benötigt, um die in DIN EN 1010-3 geforderten Maßnahmen zu Messerstillstand und Messernachlauf umzusetzen.

Berechnung der Ausfallwahrscheinlichkeit

- Die vorgesehene Architektur für Kategorie 4 für die Ansteuerung des Messerantriebs und des Pressbalkens wird wie beschrieben durch zwei unabhängige Kanäle realisiert. Da die Kanäle nahezu identisch aufgebaut sind und mit gleichen Zahlenwerten berechnet werden, ist eine Symmetrisierung nicht erforderlich. Zur Vereinfachung wird die Ansteuerung von Q1 nur einkanalig angenommen. Die berechnete Ausfallwahrscheinlichkeit ist daher in der Realität geringfügig kleiner.

- Da S1 und S2 unabhängig voneinander beim Loslassen eine Abschaltung auslösen müssen, sind sie logisch in Reihe geschaltet. Dazu wurde je ein Schließerkontakt 13-14 und ein Öffnerkontakt 21-22 einem Steuerungskanal zugeordnet. Das sicherheitsgerichtete Blockdiagramm unterscheidet sich hier deutlich vom funktionalen Schaltplan. Als Abschätzung zur sicheren Seite wird der B_{10d}-Wert für jeden einzelnen Schaltkontakt verwendet.

- $MTTF_d$: Bei 240 Arbeitstagen, 8 Arbeitsstunden und 60 Sekunden Zykluszeit beträgt n_{op} = 115 200 Schaltspiele/Jahr. Für S1 und S2 werden wegen des definierten Steuerstroms (niedrige Last, mechanische Lebensdauer der Kontakte ist bestimmend) B_{10d}-Werte von je 2 000 000 Schaltspielen [H] angenommen und damit eine $MTTF_d$ = 173 Jahre. Für die Mikrocontroller einschließlich ihrer Peripherie wird nach SN 29500-2 eine $MTTF_d$ von 878 Jahren [D] angegeben. Für die Hilfsschütze K3 bis K6 gilt bei geringer Last B_{10d} = 20 000 000 Schaltspiele [N] und damit $MTTF_d$ = 1 736 Jahre. Für die Brems-/Kupplungskombination Q1 wird der $MTTF_d$ -Wert von 607 Jahre aus B_{10d} = 7 000 000 Zyklen [G] errechnet. Der gleiche Wert wird für die Messersicherung Q2 im zweiten Kanal angenommen. Die Werte für die beiden Wegeventile 2V1 und 2V2 betragen 150 Jahre [N]. Diese Werte ergeben eine $MTTF_d$ eines Kanals von 45,2 Jahren („hoch“).

- DC_{avg}: DC = 99 % für S1/S2 basiert auf dem Kreuzvergleich von Eingangssignalen ohne dynamischen Test mit häufigem Signalwechsel. DC = 90 % für K1/K2 folgt aus Selbsttests durch Software und dynamischem Kreuzvergleich von Daten mit zeitlicher Erwartungshaltung. DC = 99 % für K3 bis K6 ergibt sich durch Plausibilitätsprüfung über zwangsgeführte Kontakte. Für 2V1/2V2 ist die DC = 99 % wegen indirekter und direkter Überwachung durch elektrische Drucküberwachung bei häufigem Signalwechsel. Ein Verschleiß der Kupplung führt zu einem geänderten Schnittverhalten. Dieses Verhalten wird messtechnisch erfasst und daher für Q1 ein DC = 99 % angenommen. Ein Ausfall von Q2 wird infolge der zyklischen Betätigung und den Überwachungselementen B1 und B3 sofort bemerkt. Damit wird ein DC = 99 % begründet. Diese Werte ergeben einen DC_{avg} von 98,5 % (im Toleranzbereich von „hoch“).

- Ausreichende Maßnahmen gegen Fehler gemeinsamer Ursache (65 Punkte): Trennung (15), Schutz gegen Überspannung usw. (15) und Umgebung (25 + 10)

- Für Kategorie 4 ergibt sich eine mittlere Wahrscheinlichkeit gefährlicher Ausfälle von $6{,}47 \cdot 10^{-8}$/Stunde. Dies entspricht PL e.

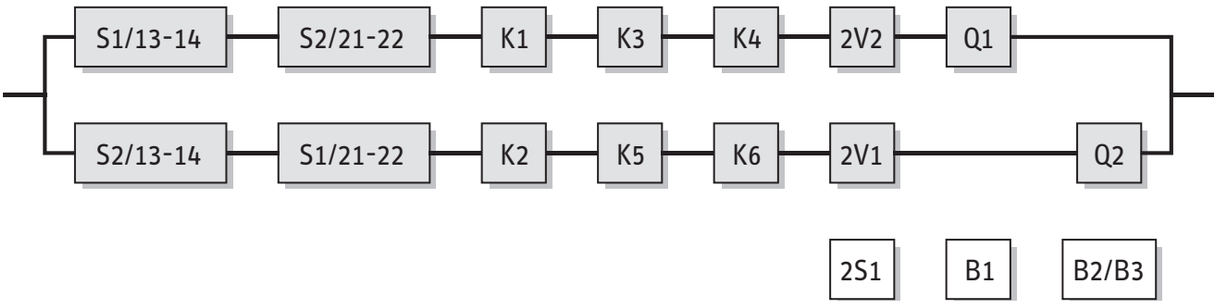
- Unter Berücksichtigung der oben aufgeführten Abschätzung zur sicheren Seite ergibt sich für die verschleißbehafteten Elemente S1 und S2 ein Wert von über 17 Jahren (T_{10d}) für den vorgesehenen Austausch.

Weiterführende Literatur

- DIN EN 1010-3: Sicherheit von Maschinen – Sicherheitsanforderungen an Konstruktion und Bau von Druck- und Papierverarbeitungsmaschinen – Teil 3: Schneidemaschinen (12.02). Beuth, Berlin 2002

- DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte; Gestaltungsleitsätze (02.97). Beuth, Berlin 1997

- DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005



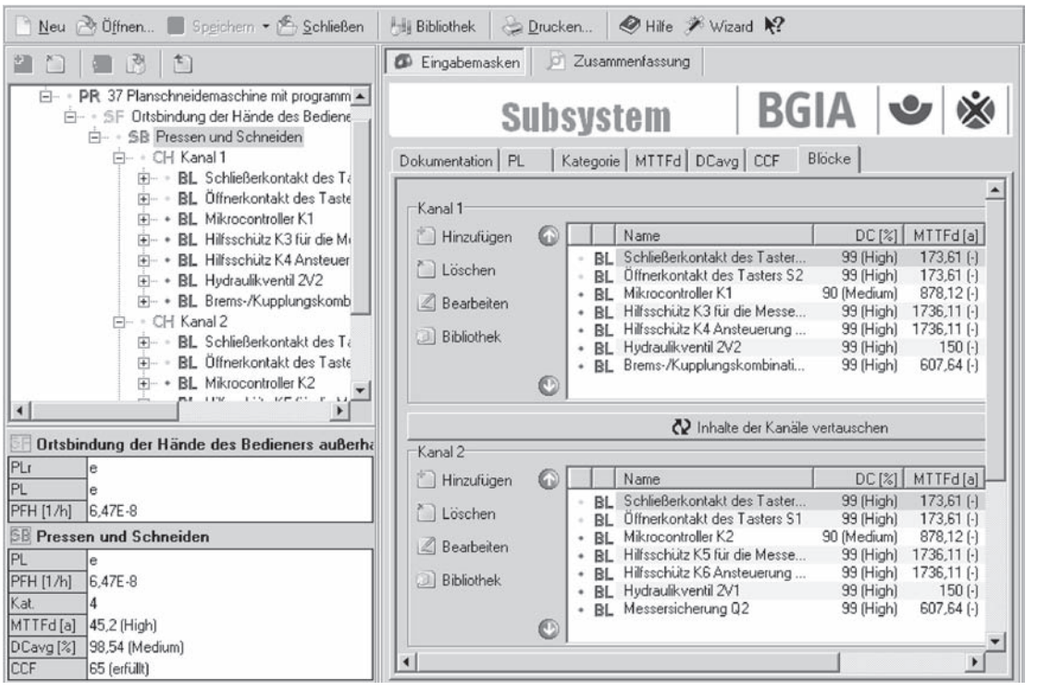


Abbildung 8.61:
PL-Bestimmung mithilfe von SISTEMA