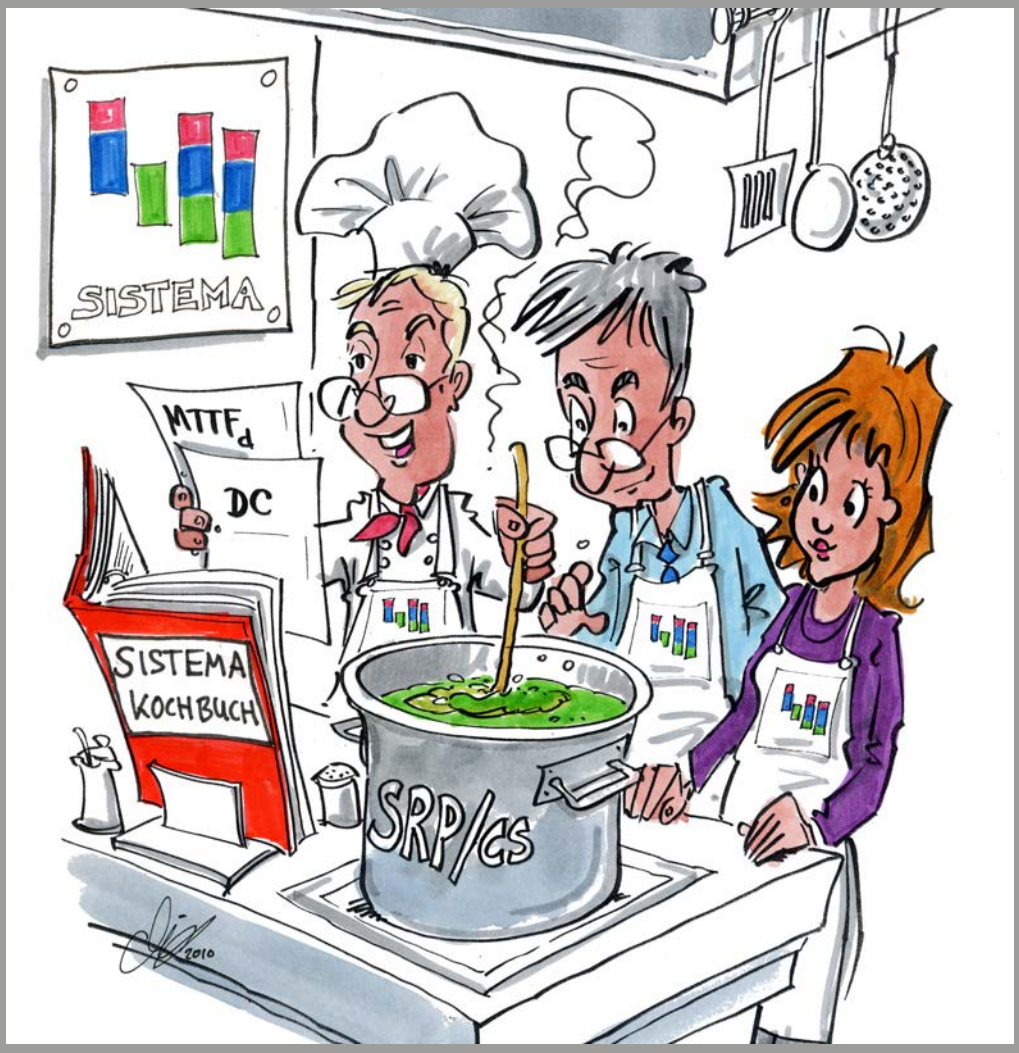
IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Das SISTEMA-Kochbuch 1

Vom Schaltbild zum Performance Level – Quantifizierung von Sicherheitsfunktionen mit SISTEMA

Version 2.0 (DE)



Verfasser: Ralf Apfeld, Michael Hauke, Michael Schaefer, Paul Rempel, Björn Ostermann, Christian Werner, Thomas Bömer, Michael Huelke
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin

Herausgeber: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Alte Heerstr. 111, 53757 Sankt Augustin
Telefon: 030 13001-0
Telefax: 030 13001-38001
Internet: www.dguv.de/ifa

– April 2020 –

Inhaltsverzeichnis

1 Einleitung

Steuerungen, die Sicherheitsfunktionen ausführen, werden eingesetzt, um Maschinen sicher zu gestalten und damit die Anforderungen der Maschinenrichtlinie 2006/42/EG zu erfüllen. Die erforderlichen Sicherheitsfunktionen werden im Rahmen der Risikobeurteilung während der Konstruktion der Maschine definiert. Anschließend können die sicherheitsbezogenen Teile von Maschinensteuerungen gemäß der Norm DIN EN ISO 13849-1 realisiert werden. Dazu ist u. a. die Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (**PFH_D**) zu berechnen, um den erreichten Performance Level (**PL**) zu bestimmen. Dieser hängt neben den systematischen Anforderungen auch von der Struktur der Steuerung (Kategorie) ab.

Als Hilfe stellt das Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) bereits seit vielen Jahren das Software-Tool SISTEMA (**Si**cherheit von **Ste**uerungen an **Ma**schinen) kostenlos zur Verfügung, das im Internet heruntergeladen werden kann, siehe www.dguv.de/ifa, Webcode d11223.

Als Grundlage für die Berechnungen muss der Maschinenkonstrukteur zunächst aus dem Schaltbild für jede Sicherheitsfunktion ein sicherheitsbezogenes Blockdiagramm erstellen, das die Ausführung der Sicherheitsfunktion in (eventuell redundant vorhandenen) Funktionskanälen und (soweit vorhanden) testenden Bauteilen darstellt.

Dieses SISTEMA-Kochbuch behandelt diesen ungewohnten Schritt der Abstraktion sowie die Folgeschritte: das Übertragen der Blöcke in SISTEMA und das Eintragen ihrer Kennwerte (siehe Abbildungen 1 und 2). Das Erstellen des sicherheitsbezogenen Blockdiagramms aus dem Schaltbild und der Funktionsbeschreibung wird in den Kapiteln 2 und 3 beschrieben, das Übertragen nach SISTEMA in Kapitel 4.

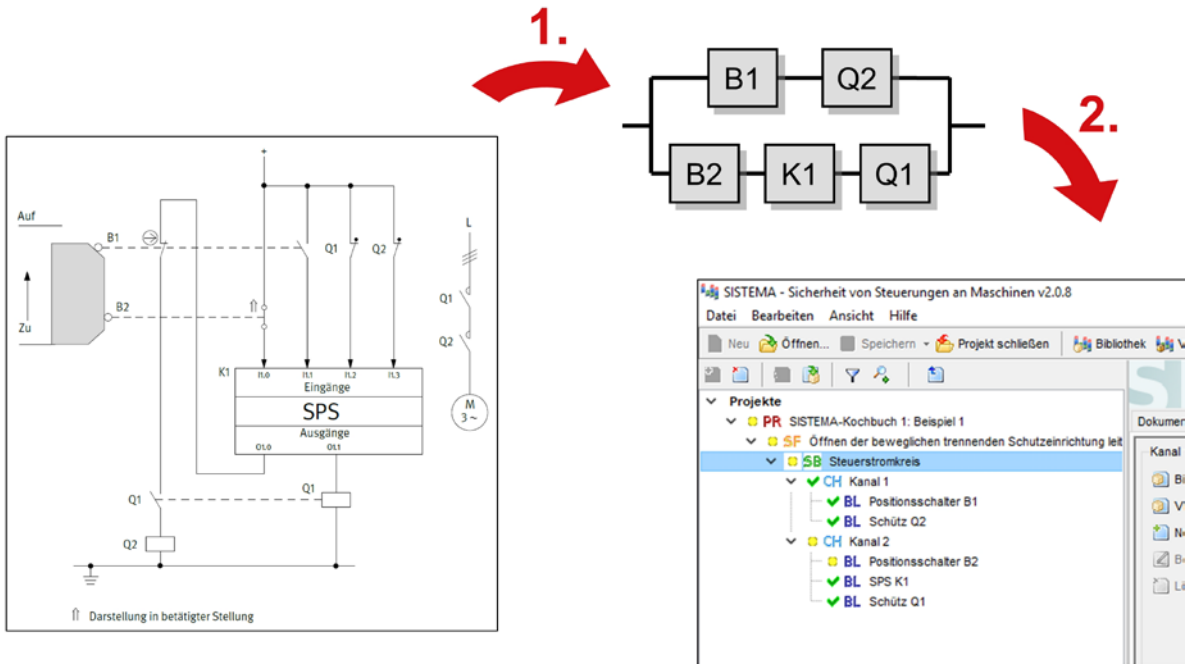


Abbildung 1: Vom Schaltbild über das sicherheitsbezogene Blockdiagramm zur Bestimmung des Performance Levels mit SISTEMA

2 Prinzipschaltbild mit Signal- und Testpfaden

2.1 Prinzipschaltbild erstellen

Für die spätere Berechnung der Ausfallwahrscheinlichkeit einer Sicherheitsfunktion ist es erforderlich zu wissen, welche Bauteile in der Sicherheitsfunktion verwendet werden und welche nicht. Eine exakte Definition der Sicherheitsfunktion ist daher unabdingbar für die nächsten Schritte (siehe Abbildung 2). Das SISTEMA-Kochbuch 6 und Kapitel 5 im IFA Report 2/2017 beschreiben detailliert, was bei der Definition von Sicherheitsfunktionen zu beachten ist (siehe www.dguv.de/ifa/13849.)

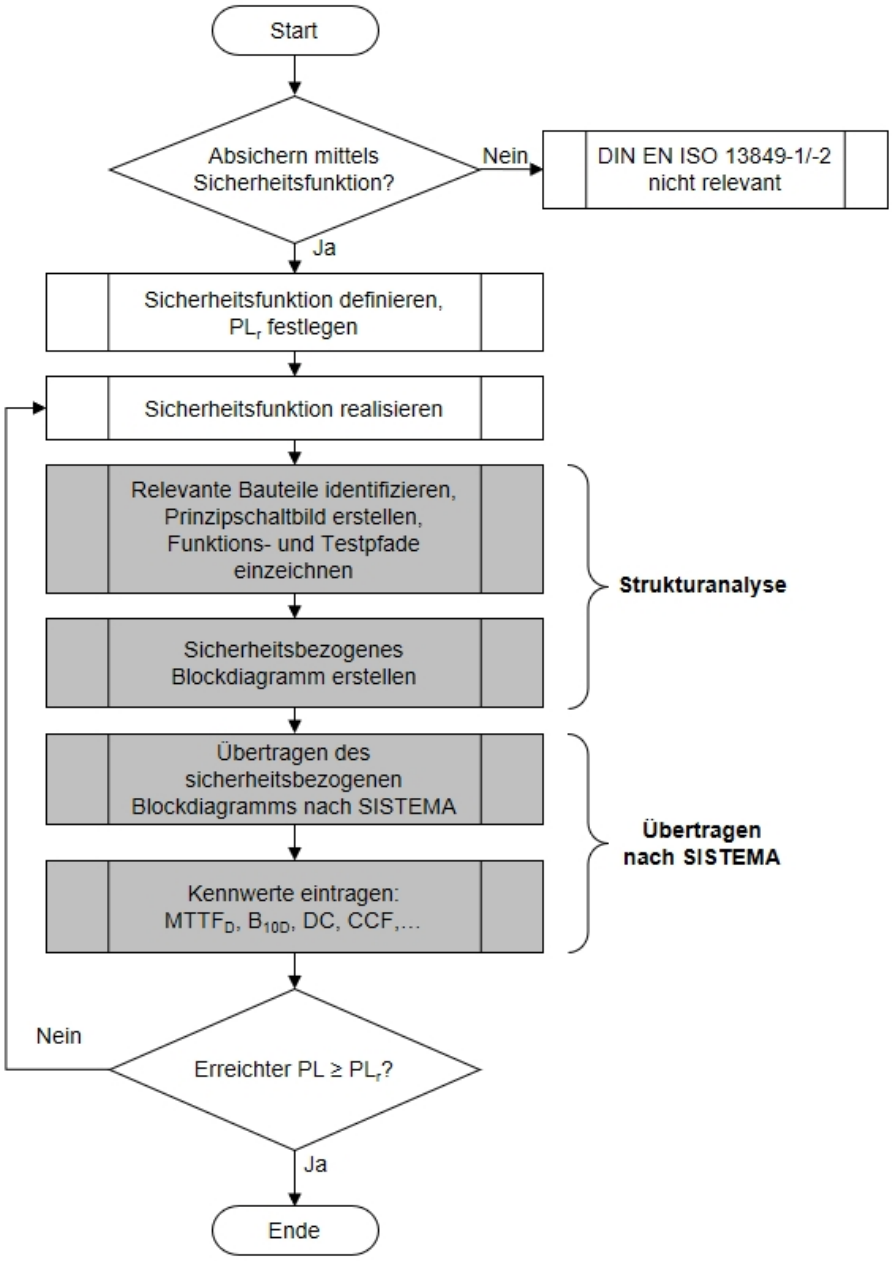


Abbildung 2: Ablaufdiagramm von der Sicherheitsfunktion zum Performance Level; die vier grau unterlegten Schritte werden in dieser Anleitung ausführlich beschrieben

Für jede Sicherheitsfunktion wird mit den relevanten Bauteilen das Prinzipschaltbild erstellt. Dazu gehören alle Bauteile, deren Ausfall die Ausführung der Sicherheitsfunktion in einem Funktionskanal (redundante Strukturen verfügen über zwei Funktionskanäle) beeinträchtigen kann. Weiterhin gehören dazu alle Testeinrichtungen, die solche gefährlichen Ausfälle erkennen oder einen sicheren Zustand einleiten. Ein Prinzipschaltbild zeigt z. B. die elektrische Verschaltung von Positionsschaltern, speicherprogrammierbaren Steuerungen (SPS) und Schützen und den Verlauf der Signalpfade vom Sensor über die Signalverarbeitung bis zum Aktor.

2.2 Signal- und Testpfade einzeichnen

Im Prinzipschaltbild werden zunächst die Signalpfade für die Ausführung der Sicherheitsfunktion markiert. Dabei hat es sich in der Praxis in vielen Fällen als hilfreich erwiesen, zunächst die Aktoren und die Sensoren zu identifizieren und dann von den Aktoren „rückwärts“ zu den Sensoren vorzugehen, um die Signalpfade vom auslösenden Ereignis zur Reaktion der Sicherheitsfunktion zu erhalten.

2.2.1 Beispiel 1: zwei Signalpfade

Im Beispiel 1 (Abbildung 3) wird eine Realisierung der Sicherheitsfunktion „Öffnen der beweglichen trennenden Schutzeinrichtung leitet die Sicherheitsfunktion STO – Sicher abgeschaltetes Moment ein“ dargestellt. Alle zusätzlichen Bauteile, die nur funktional verwendet werden und auf die Sicherheitsfunktion keinen Einfluss haben, sind bereits weggelassen.

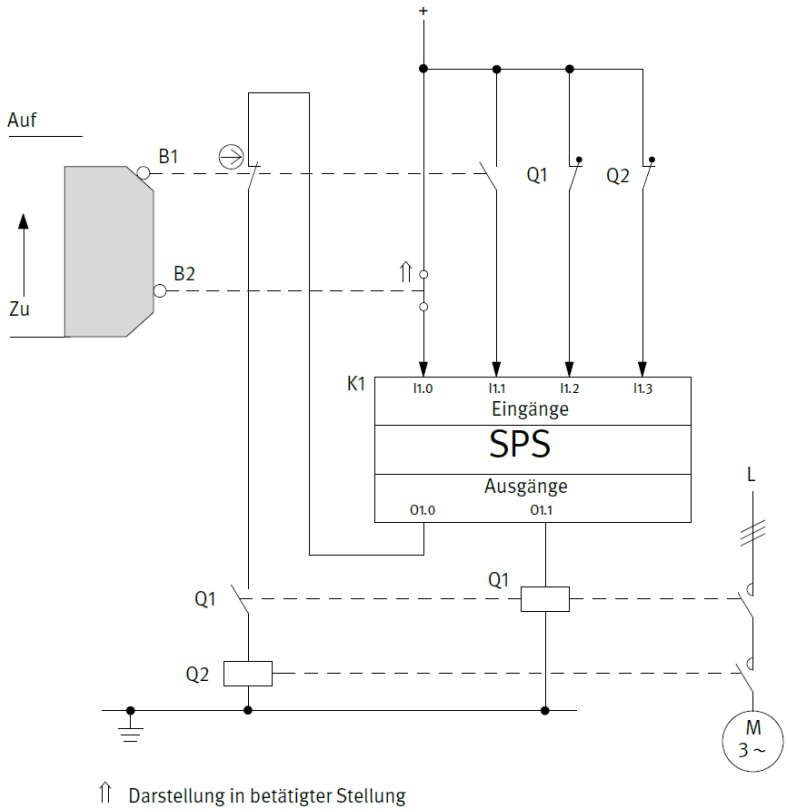


Abbildung 3:
Prinzipschaltbild mit relevanten Bauteilen (Beispiel 1); siehe auch IFA Report 2/2017, Kapitel 8.2.18

In Abbildung 3 lassen sich als Aktoren, die die Reaktion der Sicherheitsfunktion „STO – Sicher abgeschaltetes Moment“ einleiten können, die beiden Schütze Q1 und Q2 ermitteln. Der Motor M ist kein Steuerungselement und kann ohne Energie kein Moment erzeugen. Das auslösende Ereignis „Öffnen der beweglichen trennenden Schutzeinrichtung“ erfassen die Positionsschalter B1 und B2. Wird der Signalpfad wie empfohlen rückwärts verfolgt, so lässt sich im Prinzipschaltbild erkennen, dass Q1 vom Ausgang O1.1 der Standard-SPS K1 angesteuert wird, während Q2 direkt durch das Öffnen von B1 abgeschaltet wird. Zusätzlich kann Q2 auch von K1 durch Wegnahme des Ausgangs O1.0 abgeschaltet werden. Außerdem wird beim Abschalten von Q1 über einen Hilfskontakt auch Q2 mit abgeschaltet. K1 schließlich erhält Informationen über die Zustände von B1 und B2 über die Eingänge I1.0 und I1.1. Diese beiden Eingänge können zusätzlich zur Diagnose in K1 verglichen werden. Die Eingänge I1.2 und I1.3 dienen zur Rücklesung der Zustände von Q1 und Q2 und daher nicht zur Ausführung der Sicherheitsfunktion, sondern nur zur Fehlererkennung. Zusammengefasst gibt es also wie in Abbildung 4 dargestellt mehrere mögliche Signalpfade, die sich teilweise überlappen:

- B1 – K1 – Q1 sowie B2 – K1 – Q1
- B1 – K1 – Q2 sowie B2 – K1 – Q2
- B1 – K1 – Q1 – Q2 sowie B2 – K1 – Q1 – Q2
- B1 – Q2

Da die Sensoren und Aktoren bereits redundant vorliegen, scheint es sich insgesamt um eine zweikanalige Struktur zu handeln. Um dies auch nachzuweisen und im sicherheitsbezogenen Blockdiagramm darstellen zu können, müssen aus den obigen möglichen Signalpfaden zwei isoliert werden, die separat voneinander auf unterschiedliche Bauteile zurückgreifen. Die kürzeste Signalkette B1 – Q2 fällt sofort ins Auge. Ein passender zweiter Signalpfad, der die Sicherheitsfunktion unabhängig ausführen kann, darf weder B1 noch Q2 enthalten, daher ist hier nur die Kombination B2 – K1 – Q1 möglich. Neben den Signalpfaden auf der Hardware-Ebene muss natürlich auch die Software in K1 die passende Signalverarbeitung leisten. Informationen hierzu finden sich in der Funktionsbeschreibung.

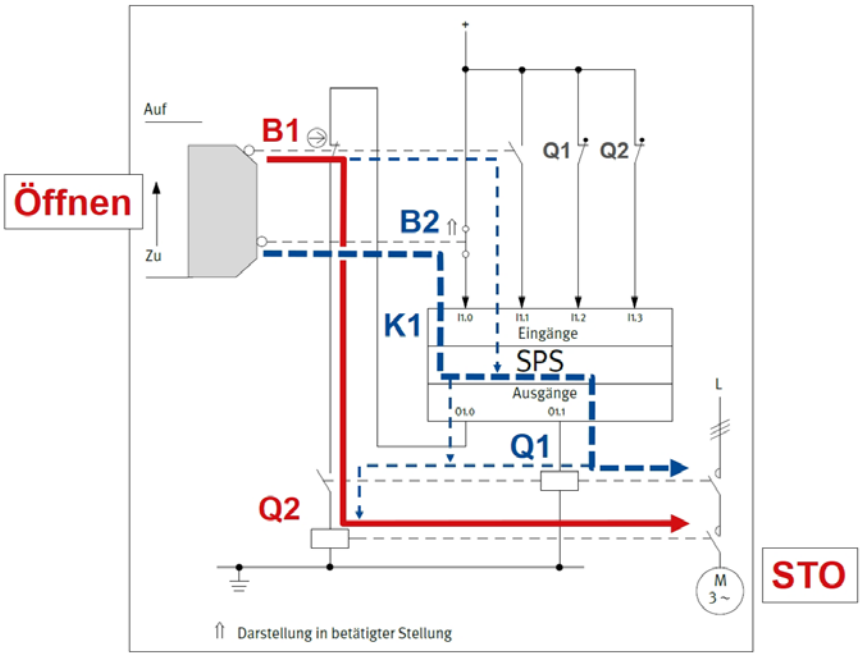


Abbildung 4:
Prinzipschaltbild mit zwei redundanten Signalpfaden B1 – Q2 und B2 – K1 – Q1

2.2.2 Beispiel 2: Signal- und Testpfad

Falls in Schaltungen ein Testkanal mit eigenständiger Abschalteinrichtung verwendet wird (Kategorie 2 nach DIN EN ISO 13849), wird im Prinzipschaltbild auch dieser Testpfad markiert. Abbildung 5 zeigt das Vorgehen an einem zweiten Beispiel. Die Sicherheitsfunktion lautet hier „Sicheres Hochhalten einer gewichtsbelasteten Vertikalachse bei Spannungsausfall“ und wird von einer Sicherheits-SPS K1 angesteuert, die die Netzspannung zweikanalig misst und so einen Spannungsausfall feststellen kann. K1 schaltet über das Schütz K2 und das Pneumatikventil 0V1 die pneumatische Versorgungsenergie weg und lässt damit die federkraftbetätigte Klemmeinrichtung Q1 einfallen.

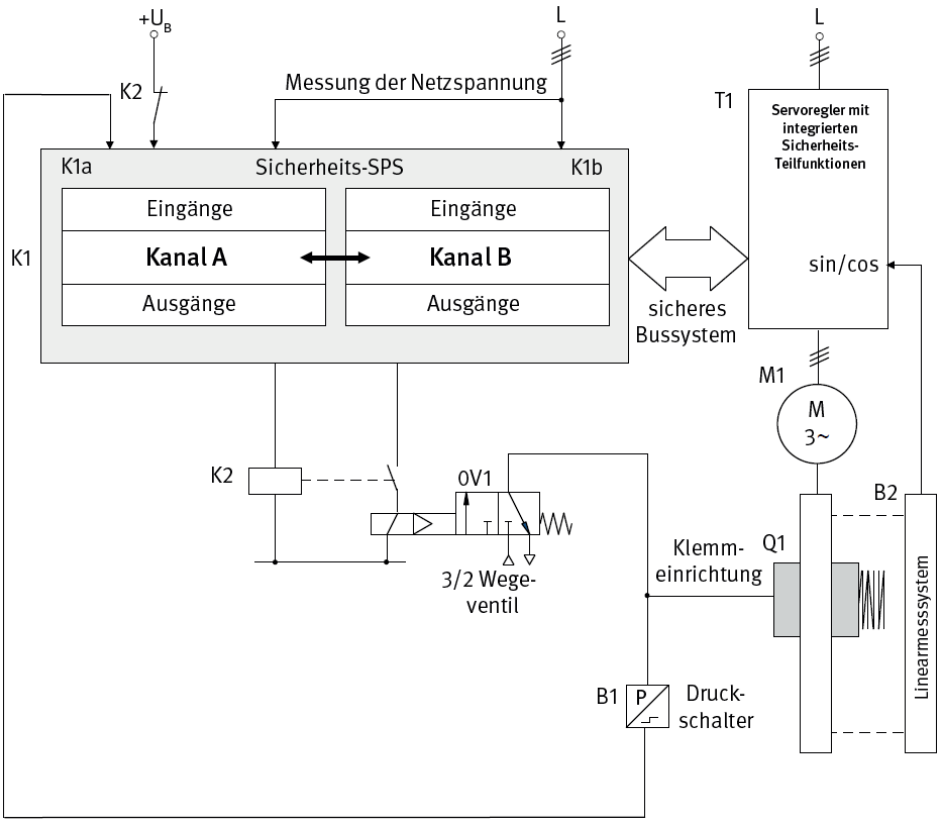


Abbildung 5:
Prinzipschaltbild mit relevanten Bauteilen; siehe IFA Report 4/2018, Anhang A, Beispiel 14

Der Signalpfad von der Detektion des Spannungsausfalls bis zum sicheren Hochhalten der Vertikalachse lässt sich hier leicht erkennen: Die Messung der Netzspannung erfolgt nur in K1, daher beginnt der Signalpfad mit K1 als Sensor. Bei Spannungsausfall ist der Motor M1 in Kombination mit dem Servoregler T1 nicht dauerhaft in der Lage, die Vertikalachse gegen die Gewichtskraft hochzuhalten. Als Aktor am Ende des Signalpfades kommt daher nur die federkraftbetätigte Klemmeinrichtung Q1 in Frage. Die Methode, den Signalpfad rückwärts von den Aktoren zu den Sensoren zu verfolgen, führt direkt auf das Pneumatikventil 0V1 und das Schütz K2 als Verbindung von K1 und Q1. Dies gilt unter der Voraussetzung, dass K1 lange genug aus einem gepufferten Netzteil versorgt wird, um den Spannungsausfall festzustellen und Q1 einfallen zu lassen. Es gibt hier also nur einen sinnvollen Signalpfad für die Ausführung der Sicherheitsfunktion, nämlich

- K1 – K2 – 0V1 – Q1

Die erforderliche Testung der Klemmeinrichtung Q1 inklusive ihrer Ansteuerung erfolgt alle acht Stunden in statischer Weise, indem die Sicherheits-SPS K1 im Stillstand die Klemmeinrichtung Q1 über K2 und 0V1 ansteuert und Q1 dann über den Servoregler T1 und den Motor M1 mit dem 1,3-fachen Lastmoment belastet. Über das Linearmesssystem B2 kontrolliert K1 dabei, dass die vorgegebene Position nicht verlassen wird. Zusätzlich erfolgt halbjährlich ein dynamischer Test unter definierten Bedingungen, bei dem K1 den Motor M1 über T1 momentenfrei schaltet, kurz danach den Bremsvorgang mit K2, 0V1 und Q1 einleitet und über B2 den ermittelten Nachlaufweg mit den zulässigen Werten vergleicht. Die Testung in den vorgegebenen Zeitabständen ist im vorliegenden Anwendungsfall ausreichend, da die Sicherheitsfunktion nur selten, nämlich bei Spannungsausfall angefordert wird. Während der statischen und dynamischen Tests können K2 über einen Rücklesekontakt direkt und OV1 über den Druckschalter B1 indirekt in K1 auf ihre korrekte Funktion überwacht werden.

Im Testpfad werden alle Komponenten gesammelt, die an den Tests beteiligt sind:

- K1 – B1 – T1 – M1 – B2

Hier fällt schon auf, dass die Sicherheits-SPS K1 eine Sonderrolle spielt, da sie sowohl im Signalpfad der Sicherheitsfunktion als auch im Testpfad vorkommt (siehe Abbildung 6). Als intern zweikanalig aufgebautes gekapseltes Subsystem gibt der Hersteller die Erfüllung der Anforderungen für Kategorie 3 und PL d an. Bei der Strukturanalyse im folgenden Kapitel wird die Rolle von K1 dann genauer betrachtet.

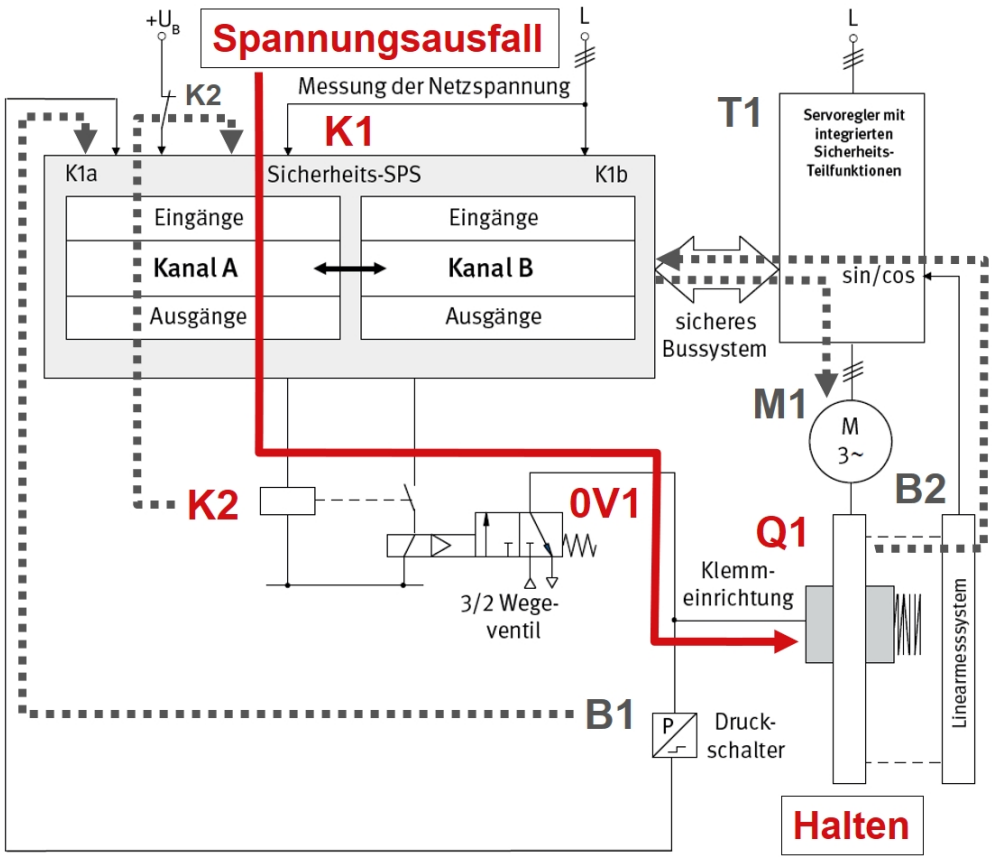


Abbildung 6: Prinzipschaltbild mit markiertem Signalpfad K1 – K2 – 0V1 – Q1 und Testpfad mit den beteiligten Komponenten K1 – B1 – T1 – M1 – B2

Im Kapitel 3 werden die hier an zwei Beispielen dargestellten Möglichkeiten, wie ein Prinzipschaltbild in ein sicherheitsbezogenes Blockdiagramm überführt werden kann, allgemein erläutert.

3 Vom Prinzipschaltbild zum sicherheitsbezogenen Blockdiagramm

Dieses Kapitel beschreibt in allgemeiner Form, wie für jede Sicherheitsfunktion eine Transformation in die Darstellung des sicherheitsbezogenen Blockdiagramms erreicht werden kann. Durch die Transformation werden die Bauteile des Prinzipschaltbilds sogenannten Subsystemen mit definierter innerer Struktur zugeordnet, mit denen in SISTEMA die Sicherheitsfunktion abgebildet wird.

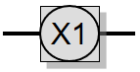
Bei der Darstellung als sicherheitsbezogenes Blockdiagramm stehen nicht mehr die physikalischen Verbindungen der Bauteile im Vordergrund, sondern die logischen Zusammenhänge (siehe Abbildung 1). Jedes Bauteil in einer Sicherheitsfunktion ist Bestandteil eines Subsystems mit einer bestimmten Struktur. Diese Strukturen werden in DIN EN ISO 13849-1 als Kategorien bezeichnet. SISTEMA stellt für jede Sicherheitsfunktion die Aneinanderreihung der Subsysteme mit ihrer jeweiligen Kategorie in einer Baumstruktur dar, die dem sicherheitsbezogenen Blockdiagramm entspricht. Die Reihenfolge der Subsysteme innerhalb einer Sicherheitsfunktion spielt für die spätere Berechnung der Ausfallwahrscheinlichkeit keine Rolle.

Anmerkung: Die in diesem Kapitel beschriebene Strukturanalyse orientiert sich an formalen Kriterien und kann die umfassende Überprüfung aller Anforderungen an die jeweilige Kategorie nicht ersetzen. Das mit Hilfe der hier beschriebenen Methode entwickelte sicherheitsbezogene Blockdiagramm liefert als Ergebnis eine Abbildung der inneren Struktur. Damit bildet es eine gute Basis für die vollständige Bestimmung und Validierung der in den Subsystemen erreichten Kategorien.

3.1 Gekapselte Subsysteme

Bauteile, für die der Hersteller bereits PL, PFH_D und Kategorie angibt (z. B. Sicherheits-SPS, Sicherheitsbaustein), stellen sogenannte gekapselte Subsysteme dar. Hier ist keine Analyse der inneren Struktur mehr notwendig und das Bauteil wird mit einem Kreis um die Bauteilbezeichnung gekennzeichnet, siehe Tabelle 1.

Tabelle 1: Gekapselte Subsysteme

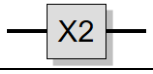
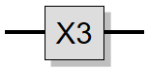
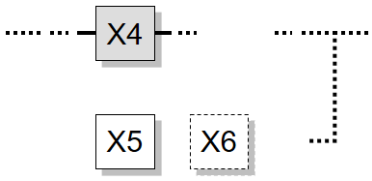
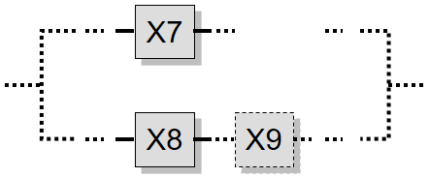
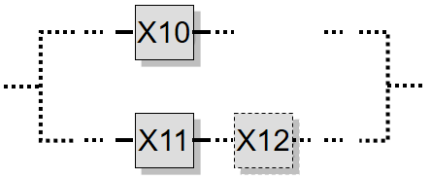
Struktur	**Kategorie nach DIN EN ISO 13849-1 und besondere Merkmale**	**Typische Darstellung im sicherheitsbezogenen Blockdiagramm**
Verschiedene interne Strukturen möglich	PL, PFH_D, Kategorie werden vom Hersteller angegeben	

Eine weitere Besonderheit stellen Bauteile dar, für die alle Ausfälle in die gefährliche Richtung ausgeschlossen werden können. Diese Blöcke können wie ein gekapseltes Subsystem behandelt werden und erfordern keine redundante Ausführung ihrer Funktion oder eine Testung (siehe auch Schritt 4 im Abschnitt 3.3 weiter unten).

3.2 Kategorien nach DIN EN ISO 13849-1

Für alle übrigen Bauteile erfolgt die Zuordnung zu einem Subsystem mit einer Kategorie nach DIN EN ISO 13849-1. Ihre charakterisierenden Merkmale und typische Darstellung zeigt Tabelle 2 in vereinfachter Form.

Tabelle 2: Merkmale und Darstellung der Kategorien

Struktur	**Kategorie nach DIN EN ISO 13849-1 und besondere Merkmale**	**Typische Darstellung im sicherheitsbezogenen Blockdiagramm**
Einkanalig	Kategorie B (Basiskategorie)	
Einkanalig	Kategorie 1 (Verwendung bewährter Bauteile)	
Einkanalig, getestet	Kategorie 2 (Bauteilfehler im Funktionskanal (X4) werden durch Fehleraufdeckung im Testkanal (X5, X6) erkannt, daraufhin wird ein sicherer Zustand eingeleitet) Anmerkung: Der Funktions- und der Testkanal können über ein oder mehrere Bauteile verfügen.	
Zweikanalig, mit Fehlererkennung	Kategorie 3 (Einfehlersicherheit durch Redundanz, Testung) Anmerkung: Jeder Kanal kann über ein oder mehrere Bauteile verfügen.	
Zweikanalig, mit Fehlererkennung	Kategorie 4 (wie Kategorie 3, zusätzlich robust gegen Anhäufung von unerkannten Fehlern) Anmerkung: Jeder Kanal kann über ein oder mehrere Bauteile verfügen.	

Anmerkung: Das hier beschriebene Verfahren ist zugeschnitten auf die Anwendung der DIN EN ISO 13849-1 mit ihren „Vorgesehenen Architekturen“ für die Kategorien. In einigen Fällen kann trotz struktureller Abweichungen näherungsweise eine Abbildung auf die vorgesehenen Architekturen der Norm erreicht werden (siehe z. B. SISTEMA-Kochbuch 4: Wenn die vorgesehenen Architekturen nicht passen). Wenn – auch unter Weglassen zusätzlicher Bauteile oder Kanäle – keine Abbildung auf eine der Kategorien möglich ist, ist das vereinfachte Verfahren der Norm nicht anwendbar. Dann ist eine Berechnung mit SISTEMA nicht möglich und es müssen andere Methoden zum Nachweis der Ausfallwahrscheinlichkeit herangezogen werden, z. B. eine Markov-Modellierung wie im IFA Report 2/2017, Anhang G oder in DIN EN 61508-6, Anhang B, beschrieben.

3.3 Strukturanalyse und Erläuterungen

In der Strukturanalyse überträgt man die Bauteile aus dem Prinzipschaltbild in ein sicherheitsbezogenes Blockdiagramm und bestimmt die Subsysteme mit ihrer jeweiligen Kategorie anhand ihrer Merkmale, z. B. Redundanz, Testung und Verwendung bewährter Bauteile.

Anmerkung: In diesem Abschnitt geht es ausschließlich um die Bestimmung des strukturellen Aufbaus. Darüber hinaus bestehen zusätzliche Anforderungen an alle Kategorien, z. B. müssen Bauteile in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt, zusammengebaut und kombiniert werden, dass sie den zu erwartenden Umgebungsbedingungen standhalten können. Grundlegende Sicherheitsprinzipien müssen verwendet werden. In den Kategorien 1, 2, 3 und 4 müssen zusätzlich bewährte Sicherheitsprinzipien angewendet werden. Informationen hierzu finden sich in DIN EN ISO 13849-2. Weiterhin müssen beispielsweise in den Kategorien 2, 3 und 4 ausreichende Maßnahmen gegen Fehler gemeinsamer Ursache getroffen werden und es bestehen auch an alle Kategorien quantitative Anforderungen, deren Einhaltung von SISTEMA kontrolliert wird.

Basis für die Strukturanalyse ist das Prinzipschaltbild mit den markierten Signal- und Testpfaden. Daraus sollen sukzessive die Subsysteme mit ihren möglichen Kategorien und den Funktions- und Testkanälen abgeleitet werden. Der Ablauf ist schematisch in Abbildung 7 dargestellt. Die Anwendung dieser Anleitung auf die beiden oben in 2.2.1 und 2.2.2 eingeführten Beispiele wird im Folgenden ebenfalls beschrieben.

Tipp: Drucken Sie Abbildung 7 (siehe nächste Seite) auf einem separaten Blatt aus, um den Ablauf der Strukturanalyse bei der folgenden Beschreibung immer im Blick zu haben.

Die Strukturanalyse erfolgt entlang des kürzesten Signalpfades, der entsprechend der Anleitung in Kapitel 2 aus dem Prinzipschaltbild abgeleitet wurde. Daraus entwickelt sich der erste (oder einzige) Funktionskanal, den es in jeder der fünf Kategorie gibt. Ein zweiter Funktionskanal oder ein Testkanal wird parallel zur sukzessiven Zuordnung der Blöcke des ersten Funktionskanals mit abgeleitet. Daher wird die Strukturanalyse nur für den kürzesten Signalpfad durchgeführt und es sind keine weiteren Durchläufe für eventuell vorhandene weitere Signalpfade notwendig.

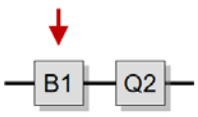
Schritt (1): Blöcke des kürzesten Signalpfades aneinanderreihen

Alle Bauteile entlang des kürzesten Signalpfades werden als Blöcke von links nach rechts (vom Sensor zum Aktor) aufgeschrieben. Es kann auch nur einen Signalpfad geben. Wenn zwei Signalpfade gleich lang sind, kann einer davon frei ausgewählt werden.

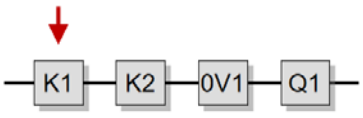
Schritt (2): Ersten Block des kürzesten Signalpfades betrachten

Nun wird nacheinander anhand der charakteristischen Merkmale der Kategorien für jeden einzelnen Block des kürzesten Signalpfades eine Zuordnung in Subsysteme der zutreffenden Kategorie vorgenommen.

In Beispiel 1 (siehe Abschnitt 2.2.1) ist B1 – Q2 der kürzeste Signalpfad. Zunächst wird der Block B1 (Positionsschalter) betrachtet.



In Beispiel 2 (siehe Abschnitt 2.2.2) ist K1 – K2 – 0V1 – Q1 der einzige (und folglich kürzeste) Signalpfad. Hier wird zunächst der Block K1 (Sicherheits-SPS) betrachtet.



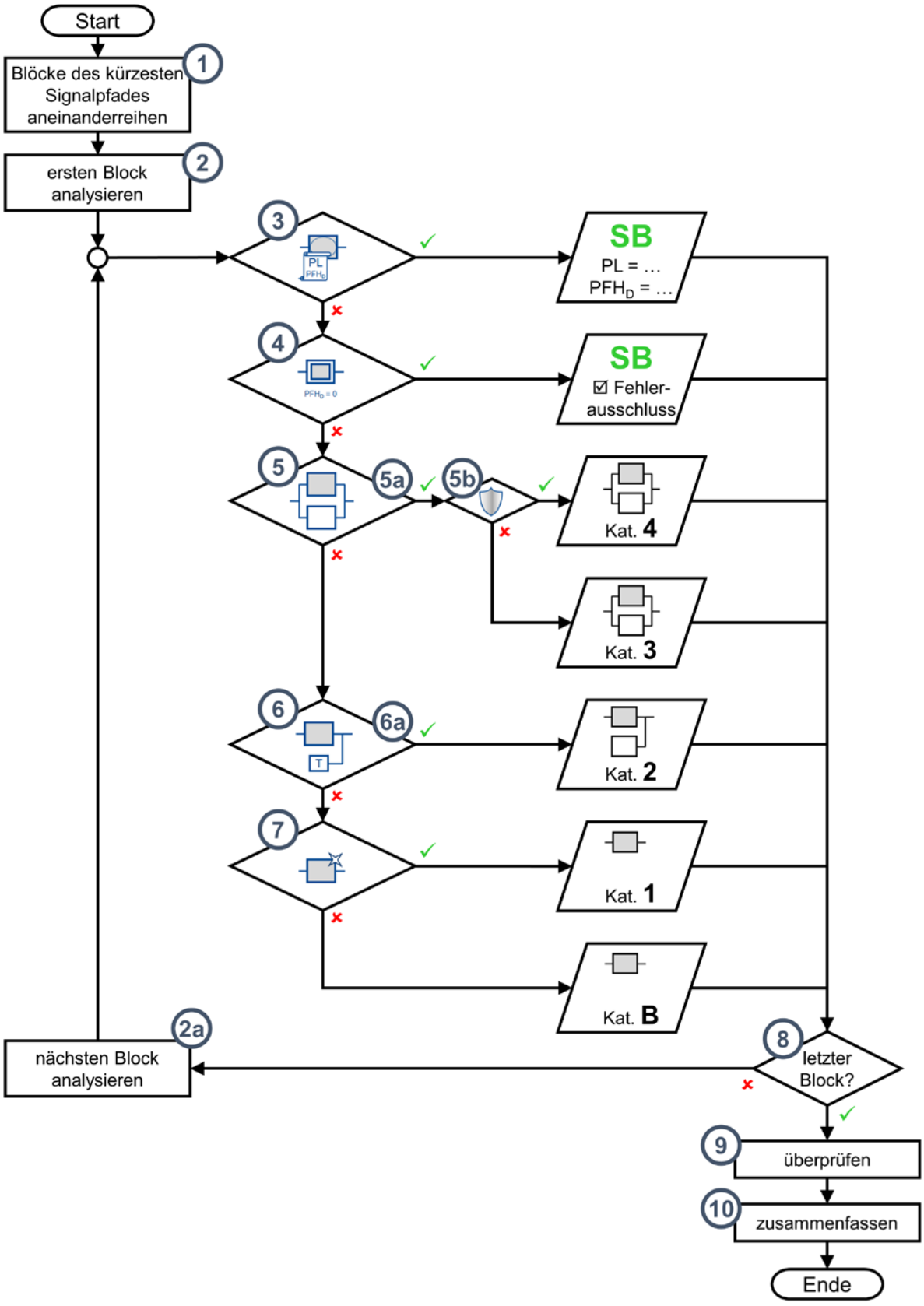


Abbildung 7: Ablaufdiagramm der Strukturanalyse in zehn Schritten

Anmerkung: In der nun beginnenden Zuordnung der einzelnen Blöcke ist es wichtig, die charakteristischen Merkmale, die in den Schritten 3 bis 7 für jeden Block abgefragt werden, genau in dieser Reihenfolge zu bearbeiten. Gekapselte Subsysteme und der Ausschluss aller Bauteilfehler sind zuerst zu identifizieren. Die Einfehlersicherheit ist vor dem Vorhandensein einer Fehlererkennung abzuklären und die Frage nach bewährten Bauteilen wird erst bei einkanaligen ungetesteten Strukturen relevant. Mit der ersten bejahten Frage der Schritte 3 bis 7 erfolgt eine Zuordnung des betrachteten Blocks zu einem Subsystem mit einer bestimmten Kategorie. Für diesen Block sind die folgenden Schritte nicht mehr relevant, es geht dann mit Schritt 8 weiter: Entweder wird der nächste Block analysiert (Schritt 2a) oder das Ende des kürzesten Signalpfades ist erreicht (mit Schritt 9 fortfahren).

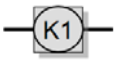
In diesem Abschnitt 3.3 wird die Strukturanalyse zunächst allgemein beschrieben und dabei mit passenden Blöcken der beiden Beispiele illustriert. In den folgenden Abschnitten 3.4 und 3.5 wird für beide Beispiele nochmal der komplette Ablauf beschrieben.

Schritt (3): Nennt der Bauteilhersteller PL, PFH_D (und Kategorie)?

Ein gekapseltes Subsystem ist daran zu erkennen, dass es vom Hersteller bereits durch PL (oder SIL nach IEC-Normen, siehe Abschnitt 4.6), PFH_D und eine Kategorie (innere Struktur) charakterisiert ist. Eine weitere Zerlegung der inneren Struktur des gekapselten Subsystems ist nicht erforderlich. Der Block wird, wie in Tabelle 1 gezeigt, im sicherheitsbezogenen Blockdiagramm durch eine Umkreisung markiert und einkanalig als separates Subsystem dargestellt. Die vom Hersteller genannte Kategorie kann darunter vermerkt werden.

Anmerkung: Werden gekapselte Subsysteme der Kategorien 3 oder 4 verwendet, so verlaufen in der Regel beide redundanten Signalpfade über dieses Subsystem.
In gekapselten Subsystemen der Kategorie 2 verlaufen in der Regel Signalpfad und Testpfad über dieses Subsystem. Der Einsatz eines gekapselten Subsystems in nur einem Signal- oder Testpfad kommt in der Praxis selten vor.

Für die Sicherheits-SPS K1 in Beispiel 2 trifft dieses Kriterium zu. Daher wird K1 als separates gekapseltes Subsystem einkanalig und mit einer Umkreisung dargestellt. Der Hersteller gibt Kategorie 3 an.



Kat. 3

$PFH_D = 0$

Schritt (4): Können alle Bauteilfehler ausgeschlossen werden?

Für das Bauteil in dem betrachteten Block werden nacheinander alle anzunehmenden Fehler betrachtet. DIN EN ISO 13849-2 enthält hierzu in den Anhängen A bis D die Fehlermodelle einer Reihe von Bauteilen verschiedener Technologien, die häufig in Maschinensteuerungen verwendet werden. Begründete Fehlerausschlüsse führen dazu, dass bestimmte Bauteilfehler nicht unterstellt werden müssen. Für jeden Fehlerfall ist zu untersuchen, ob die sicherheitstechnisch beabsichtigte Funktion des Bauteils bestehen bleibt (ungefährlicher Fehler) oder ausfällt (gefährlicher Fehler). Ein gefährlicher Fehler liegt z. B. für das Schütz Q2 in Beispiel 1 (Abbildung 3) vor, wenn die Schutztür geöffnet wird, aber Q2 nicht abfällt, weil dessen Kontakt verschweißt ist.

Falls für das Bauteil überhaupt keine gefährlichen Fehler angenommen werden müssen, ergibt sich auch kein Beitrag zur Berechnung der PFH_D der Sicherheitsfunktion. Eine Berücksichtigung im sicherheitsbezogenen Blockdiagramm darf entfallen. Trotzdem kann die

weitere Darstellung sinnvoll sein, um das Verständnis der Sicherheitsfunktion zu erleichtern. In diesem Fall wird der Block wie ein gekapseltes Subsystem behandelt (in SISTEMA wird dann später das Häkchen für „Fehlerausschluss“ gesetzt, außer der Angabe einer Kategorie B sind keine weiteren Eingaben erforderlich, siehe Abschnitt 4.5).

Anmerkung: Auch wenn dies in der Praxis selten vorkommt, kann ein Bauteil mit Fehlerausschluss auch nur in einem von zwei redundanten Funktionskanälen oder nur im Funktions- oder Testkanal einer Struktur nach Kategorie 2 verwendet werden. Um eine unnötig komplizierte Darstellung im sicherheitsbezogene Blockdiagramm zu vermeiden, kann in diesem Fall Schritt 4 ignoriert werden. Stattdessen wird das Bauteil in den Schritten 5 bis 6 als Block einem Funktions- oder Testkanal zugeordnet. In SISTEMA kann dann später für den Block in der Registerkarte „$MTTF_D$“ ein Fehlerausschluss vermerkt werden.

Schritt 5: Bleibt die Sicherheitsfunktion bei Bauteilfehlern erhalten?

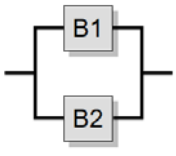
In Schritt 4 sind die für das Bauteil im betrachteten Block anzunehmenden gefährlichen Fehler betrachtet worden. Jetzt geht es um deren Auswirkungen auf die Sicherheitsfunktion. Falls im Fehlerfall des betrachteten Blocks die Sicherheitsfunktion von einem oder mehreren redundanten Bauteilen aufrechterhalten wird, gibt es offensichtlich einen zweiten Funktionskanal.

Schritt 5a: Redundante Bauteile des Blocks ergänzen

Der betrachtete Block wird dann als Teil des ersten Funktionskanals dargestellt und die redundanten Bauteile als Blöcke in einem zweiten Funktionskanal (siehe Kategorie 3 und 4 in Tabelle 2).

Anmerkung: Es kann sein, dass beide Funktionskanäle nicht symmetrisch aus den gleichen Bauteilen aufgebaut sind. Dann ist es möglich, dass die Funktion des betrachteten Blocks von mehr als einem Block im zweiten Funktionskanal ausgeführt wird. Genauso kann es vorkommen, dass bei einem erneuten Durchlauf des Schritts 5a für ein weiteres Bauteil im ersten Kanal das gleiche redundante Bauteile im zweiten Funktionskanal eingetragen wird wie bei einem vorhergehenden Durchlauf. Beides ist unproblematisch, da der sukzessive entstehende zweite Funktionskanal in den Schritten 9 und 10 nochmal bereinigt und zusammengefasst wird.

Für den Positionsschalter B1 in Beispiel 1 trifft dieses Kriterium zu, da das „Öffnen der beweglichen trennenden Schutzeinrichtung“ auch im Positionsschalter B2 erkannt werden kann. Es wird daher ein zweiter Funktionskanal angelegt, der B2 enthält.



Wenn redundante Bauteile eingetragen wurden, ist eine wichtige Grundbedingung für Kategorie 3 und 4 erfüllt: Ein einzelner Fehler in einem Bauteil des ersten oder zweiten Funktionskanals darf nicht zum Verlust der Sicherheitsfunktion führen (Einfehlersicherheit). Ausfälle aufgrund gemeinsamer Ursache werden dabei nicht als Einzelfehler betrachtet, sondern in der Norm separat bewertet.

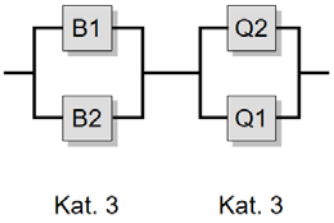
Anmerkung: Daneben erfordert Kategorie 3, dass – wann immer in angemessener Weise durchführbar – einzelne Fehler in Bauteilen der beiden Funktionskanäle erkannt werden müssen.

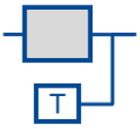
Schritt 5b: Bleibt die Sicherheitsfunktion bei Fehleranhäufung erhalten?

Für den betrachteten Block mit seinem redundanten Funktionskanal wurde bis hierhin die Einfehlersicherheit festgestellt, Kategorie 3 ist also erfüllbar. Werden aber auch die erhöhten Anforderungen an die Widerstandsfähigkeit gegen Fehleranhäufungen aus Kategorie 4 erfüllt? Hierzu muss das Verhalten beim Auftreten von unerkannten Fehlern untersucht werden. Bleibt die Sicherheitsfunktion bei Anhäufung von zwei unerkannten Fehlern erhalten, so handelt es sich um ein Kategorie-4-Subsystem. Bleibt die Sicherheitsfunktion bei einem zweiten unerkannten Fehler nicht erhalten, so liegt ein Kategorie-3-Subsystem vor. Die erreichte Kategorie wird unter den Blöcken vermerkt.

Anmerkung: In Kategorie 4 muss die Einfehlersicherheit erfüllt sein, und der einzelne Fehler in einem Bauteil des ersten oder zweiten Funktionskanals muss bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden. Wenn diese Erkennung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen. In der Praxis kann die Betrachtung einer Fehlerkombination für zwei Fehler ausreichend sein.

Der Unterschied zwischen Kategorie 3 und 4 wird in Beispiel 1 deutlich. Hier könnte die Standard-SPS K1 im Fehlerfall die Ausgänge O1.0 und O1.1 ständig ansteuern. Damit bleibt Q1 ständig angezogen. Selbst wenn die SPS diesen Fehler durch Rücklesen der Überwachungskontakte noch aufdecken könnte, wäre sie nur solange in der Lage, den sicheren Zustand herzustellen, bis durch einen zweiten Fehler z. B. die Kontakte von Q2 verschweißen. Dann läuft der Motor auch bei geöffneter Schutzeinrichtung weiter und die Sicherheitsfunktion ist ausgefallen. Kategorie 4 ist daher nicht erfüllt und es wird Kategorie 3 vermerkt.





Schritt 6: Werden Bauteilfehler ausreichend gut erkannt?

In diesem Zweig der Strukturanalyse ist klar, dass für den betrachteten Block keine Redundanz vorhanden ist, also weder Kategorie 3 noch Kategorie 4 vorliegt. Falls der Ausfall des Blocks von einem Testkanal rechtzeitig erkannt und der sichere Zustand eingeleitet wird, handelt es sich um ein Kategorie-2-Subsystem.

Anmerkung: Angemessene Fehlererkennung wird auch für Kategorie 3 und 4 gefordert. Kategorie-2-Subsystemen fehlt im Unterschied dazu jedoch ein redundanter Funktionskanal, der vorher in Schritt 5 abgefragt wird.

In Beispiel 2 wird diese Frage für die auf K1 folgenden Bauteile im Signalpfad relevant. Das Schütz K2, das Ventil 0V1 und die Klemmeinrichtung Q1 haben keine redundanten Partner, die bei Energieausfall die Vertikalachse hochhalten können. Fehler in K2 werden durch die Rücklesung in K1 bei den oben beschriebenen statischen und dynamischen Tests mit hohem Diagnosedeckungsgrad erkannt. Fehler in 0V1 werden über den Druckschalter B1 in K1 erkannt. Eine fehlerhafte Klemmeinrichtung Q1 wird ebenfalls durch K1 erkannt, die dazu auf T1, M1 und B2 zurückgreift: Dabei werden zusätzlich Fehler in K2 und OV1 indirekt mit erkennt.

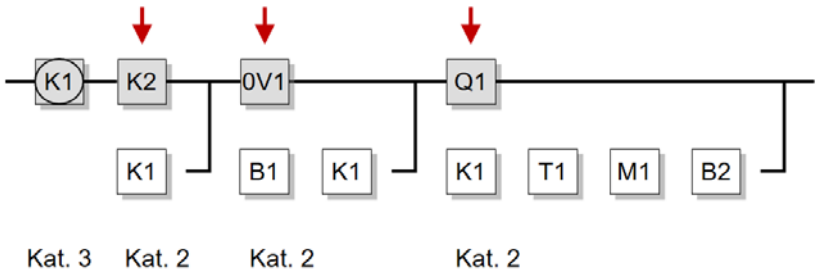
Schritt 6a: Testkanal des Blocks ergänzen

Der betrachtete Block im kürzesten Signalpfad wird als Teil des Funktionskanals dargestellt. Die Bauteile des Testkanals, die den Ausfall des Blocks feststellen und den sicheren Zustand einleiten, werden entsprechend Tabelle 2 (Kategorie 2) als Testblöcke im sicherheitsbezogenen Blockdiagramm dargestellt. Darunter kann Kategorie 2 vermerkt werden.

In Beispiel 2 kann unter K2 im Funktionskanal K1 im Testkanal eingetragen werden.

Unter 0V1 werden B1 und K1 im Testkanal notiert.

Unter Q1 werden K1, T1, M1 und B2 im Testkanal eingetragen.



Anmerkung: Wenn Bauteile im Testkanal eingetragen wurden, ist eine wichtige Grundbedingung für Kategorie 2 erfüllt: Die Sicherheitsfunktion muss in geeigneten Zeitabständen getestet werden. Dadurch wird der Verlust der Sicherheitsfunktion erkannt und ein sicherer Zustand durch eine unabhängige Abschalteinrichtung eingeleitet. Eine weitere wichtige Anforderung der Kategorie 2 betrifft die Testhäufigkeit (siehe IFA Report 2/2017, Abschnitt 6.2.5 und 6.2.14) Werden diese oder andere Anforderungen der Kategorie 2 nicht erfüllt, dann ist die Testung nicht ausreichend wirksam, um als Kategorie 2 dargestellt zu werden.

Schritt 7: Ist das Bauteil „bewährt"?

Redundanz oder ausreichend wirksame Testung konnten bis zu diesem Zweig im Flussdiagramm nicht festgestellt werden. Es kommen also nur noch Kategorie 1 oder Kategorie B infrage. Falls es sich bei dem Bauteil im betrachteten Block um ein „bewährtes“ Bauteil nach DIN EN ISO 13849 handelt, wird der Block als Teil des Funktionskanals eines Kategorie-1-Subsystems dargestellt. Eine Liste von bewährten Bauteilen ist in der DIN EN ISO 13849-2 zu finden. Andernfalls handelt es sich bei dem Block bestenfalls um einen Teil des Funktionskanals eines Kategorie-B-Subsystems (siehe auch die einleitende Anmerkung zu Beginn von Abschnitt 3.3).

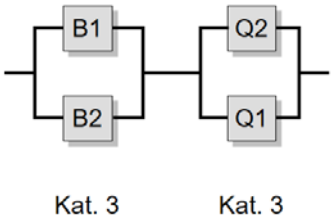
Anmerkung: Wurde der Block bereits vorher in den Schritten 3 bis 6 einem gekapselten Subsystem oder einer Kategorie 4, 3 oder 2 zugeordnet, dann ist die „Bewährtheit“ für die Strukturanalyse nicht relevant.

Blöcke der Kategorie B oder 1 werden im sicherheitsbezogenen Blockdiagramm, wie in Tabelle 2 gezeigt, einkanalig dargestellt. Die mögliche Kategorie (B oder 1) wird darunter vermerkt.

Schritt 8 und 2a: Sind alle Blöcke des kürzesten Signalpfades betrachtet?

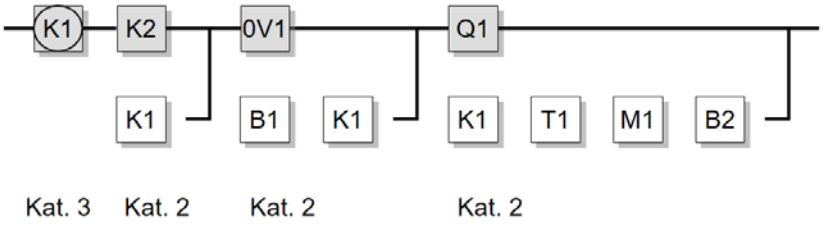
Nach der Zuordnung des ersten Blocks im kürzesten Signalpfad wird das Diagramm mit dem nächsten Block über die Schritte 8 und 2a erneut durchlaufen. So werden nach und nach alle Blöcke des kürzesten Signalpfades abgearbeitet. Danach geht es weiter mit Schritt 9.

In Beispiel 1 werden nach Block B1 die Schritte 2a bis 8 mit dem nächsten Block des kürzesten Signalpfades, also Q2 durchlaufen. Hier ergibt sich derselbe Weg durch das Flussdiagramm, da auf Q1 die Kriterien in den Schritten 3 und 4 ebenfalls nicht zutreffen, aber die Frage nach der Redundanz in Schritt 5 auch bejaht werden kann. Das sicher abgeschaltete Moment (STO) kann neben Q1 auch durch Q2 erwirkt werden. Schritt 5b führt ebenfalls auf Kategorie 3. Nach dem zweiten Durchlauf bis Schritt 8 sind alle Blöcke des kürzesten Signalpfades betrachtet und es kann mit Schritt 9 fortgefahren werden. Das sicherheitsbezogene Blockdiagramm sieht zu diesem Zeitpunkt so (oder ähnlich) aus:



Wurde hier schon erkannt, dass der zweite Funktionskanal unvollständig ist, dann ist K1 im zweiten Funktionskanal bereits ergänzt. Sonst wird das in Schritt 9 vollzogen.

In Beispiel 2 werden nach Block K1 die Schritte 2a bis 8 mit den nächsten Blöcken des Signalpfades, also K2, 0V1 und Q1 sukzessive durchlaufen. Während K1 bereits in Schritt 3 als gekapseltes Subsystem identifiziert wurde, erfolgt für K2, 0V1 und Q1 erst im Schritt 6 eine Zuordnung zum Funktionskanal eines Kategorie-2-Subsystems. Die zugehörigen Blöcke des Testkanals werden dann jeweils im Schritt 6a ergänzt. Das sicherheitsbezogene Blockdiagramm sieht zu diesem Zeitpunkt so aus:

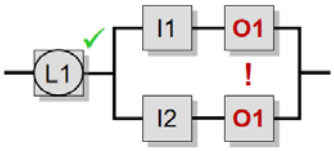


Hier fällt auf, dass einige Blöcke mehrfach auftauchen. Diese können in Schritt 10 zusammengefasst werden.

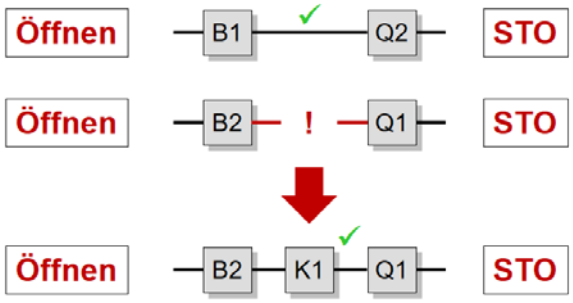
Schritt (9): Ermitteltes sicherheitsbezogenes Blockdiagramm überprüfen

Anhand mehrerer Kriterien kann das bisher nach formalen Gesichtspunkten entwickelte sicherheitsbezogene Blockdiagramm auf Vollständigkeit und Korrektheit überprüft werden:

- Um die mit der Einfehlersicherheit verbundene Unabhängigkeit der Kanäle in Kategorie 3 und 4 nicht zu unterlaufen, darf dasselbe Bauteil nicht gleichzeitig in zwei redundanten Funktionskanälen auftauchen. In ähnlicher Weise gilt für Kategorie 2, dass dasselbe Bauteil nicht gleichzeitig im Funktions- und Testkanal erscheinen darf.
  Gekapselte Subsysteme oder Bauteile mit Fehlerausschluss spielen dabei eine Sonderrolle: hier dürfen zwei Signalpfade oder der Signal- und der Testpfad über dasselbe Bauteil führen. Im sicherheitsbezogenen Blockdiagramm werden gekapselte Subsysteme oder Bauteile mit Fehlerausschluss daher auch einkanalig dargestellt.



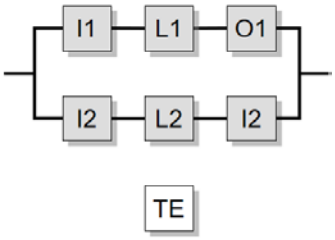
- Außerdem ist es wichtig zu prüfen, dass jeder ermittelte Funktionskanal in Kategorie 3 und 4 für sich separat die Sicherheitsfunktion ausführen kann. Dazu ist es hilfreich, sich den jeweils anderen Kanal wegzudenken (oder sich vorzustellen, dass dort alle Bauteile gefährlich ausgefallen sind) und dann gedanklich zu überprüfen, ob die Sicherheitsfunktion im verbliebenen Funktionskanal trotzdem noch ausgeführt wird. Fällt bei dieser Überprüfung auf, dass Blöcke im redundanten Signalpfad fehlen, wie in Beispiel 1 der Block K1 als Verbindung der Blöcke B2 und Q1, dann müssen diese ergänzt werden.



- Für ermittelte Testkanäle ist zu prüfen, ob alle Bauteile des Testpfads lückenlos enthalten sind. Dazu gehören alle Bauteile von der Fehlererkennung (TE – Testeinrichtung) bis zum Einleiten des sicheren Zustands im Fehlerfall (OTE – Ausgang der Testeinrichtung). Dazu kann dem zugehörigen Funktionskanal gedanklich ebenfalls ein gefährlicher Komplettausfall unterstellt werden. Der Testkanal muss dann in der Lage bleiben, den sicheren Zustand herzustellen. Fehlende Bauteile im Testkanal sind zu ergänzen.

- Jedes Bauteil im Prinzipschaltbild der betrachteten Sicherheitsfunktion sollte jetzt einen Platz im sicherheitsbezogenen Blockdiagramm zugewiesen bekommen haben. Bleiben Bauteile übrig, sollte deren Rolle nun geklärt werden. Es kann sich beispielsweise um Bauteile handeln, die partiell eine Mehrfehlersicherheit (Dreifach-Redundanz) oder Mehrfachtestung realisieren. Da die Norm maximal zwei Funktionskanäle vorsieht, bildet SISTEMA auch maximal zwei Funktionskanäle ab. Hier kann die günstigste Kombination ausgewählt werden, weitere Funktionskanäle bleiben unberücksichtigt. Bauteile zur Mehrfachtestung können optional in den Testkanal aufgenommen werden, z. B. wenn dadurch ein höherer Diagnosedeckungsgrad realisiert werden kann.

In Kategorie 3 und 4 können Bauteile außerhalb der beiden Funktionskanäle, die nur der Testung dienen, zur Information in einer dritten Zeile notiert werden (wie in einigen Schaltungsbeispielen aus Kapitel 8 des IFA Report 2/2017 umgesetzt). In die Berechnung der Ausfallwahrscheinlichkeit fließen diese Bauteile aber nicht direkt ein, daher werden sie in SISTEMA auch nicht mit eingegeben.



- Alle Kategorieanforderungen, deren Erfüllung nicht direkt anhand der Strukturanalyse entschieden werden können, sind zu überprüfen. Beispielsweise kann eine nicht ausreichende Testhäufigkeit in einem System mit Funktions- und Testkanal dazu führen, dass dieses nicht als Kategorie-2-Subsystem dargestellt werden kann. Auch die Basisbedingungen der Kategorie B, wie die Verwendung grundlegender Sicherheitsprinzipien, sind hier nochmal zu verifizieren, da diese ja für alle Kategorien verbindlich sind. Bei der Überprüfung dieser Bedingungen hilft SISTEMA mit entsprechenden Hinweisen und Checklisten, nachdem dort alle Daten eingegeben sind (siehe Abbildung 19). Wird die Kategorie, wie sie in der Strukturanalyse ermittelt wurde, aus den hier beschriebenen Gründen nicht erreicht, so muss die im sicherheitsbezogenen Blockdiagramm dargestellte Kategorie entsprechend herabgestuft werden oder die Steuerung nachgebessert werden.

An diesem Punkt der Strukturanalyse sollte bereits ein korrektes sicherheitsbezogenes Blockdiagramm entstanden sein, dass in vielen Fällen aber noch vereinfacht werden kann (siehe Schritt 10).

Schritt (10): Blöcke und Subsysteme zusammenfassen

Im letzten Schritt der Strukturanalyse können noch einige Vereinfachungen am sicherheitsbezogene Blockdiagramm durchgeführt werden. Diese Bereinigung betrifft Bauteile, die in verschiedenen Subsystemen mehrfach auftreten, und die Zusammenfassung mehrerer Subsysteme gleicher Kategorie. Das aus dem hardwarebasierten Prinzipschaltbild entwickelte sicherheitsbezogene Blockdiagramm stellt die logische Struktur der Sicherheitsfunktion in den Vordergrund. Die lineare Verkettung der Subsysteme symbolisiert die Eigenschaft, dass der Ausfall jedes Subsystems zum Verlust der Sicherheitsfunktion führt. Redundante Funktionskanäle zeigen die Toleranz gegenüber gefährlichen Ausfällen, die nur einen Kanal betreffen. Testkanäle sollen gefährliche Ausfälle im Funktionskanal erkennen und beherrschen, bevor die Sicherheitsfunktion angefordert wird. Aus diesen Eigenschaften des sicherheitsbezogenen Blockdiagramms ergeben sich folgende zulässige Vereinfachungen:

- Die Reihenfolge der Subsysteme im sicherheitsbezogenen Blockdiagramm ist grundsätzlich nicht relevant und folglich vertauschbar.

- Mehrere Bauteile der Kategorie B können in einem Subsystem der Kategorie B zusammengefasst werden.
- Mehrere Bauteile der Kategorie 1 können in einem Subsystem der Kategorie 1 zusammengefasst werden.

- Mehrere Subsysteme der Kategorie 2 können in einem Subsystem der Kategorie 2 zusammengefasst werden. Dabei werden alle Bauteile aus Funktionskanälen in einem gemeinsamen Funktionskanal gesammelt und alle Bauteile aus Testkanälen in einem gemeinsamen Testkanal (siehe Abbildung 10 und IFA Report 2/2017, Beispiel 13 in Abschnitt 8.2.13). Doppelte Blöcke im gleichen Kanal, die durch die Zusammenfassung entstehen, müssen nur einmal genannt werden.
  Hier könnte der unwahrscheinliche Fall auftreten, dass nach der Zusammenfassung ein Bauteil sowohl im neuen Funktionskanal als auch im neuen Testkanal vorkommt, was dem ersten unter Schritt 9 genannten Kriterium widerspräche. Um zu beurteilen, ob die Zusammenfassung in diesem Fall zulässig ist und die Anforderungen der Kategorie 2 eingehalten sind, ist die Rolle dieses Bauteils im Fehlerfall nochmal genau zu analysieren: Der gefährliche Ausfall dieses Bauteils darf nicht dazu führen, dass die Ausführung der Sicherheitsfunktion und die Fehlererkennung gleichzeitig ausfallen. Mit anderen Worten: Mit den verbliebenden funktionierenden Bauteilen im Funktions- und Testkanal muss der sichere Zustand noch eingeleitet werden können.
- Mehrere Subsysteme der Kategorie 3 können in einem Subsystem der Kategorie 3 zusammengefasst werden. Dabei erfolgt die Zusammenfassung kanalweise (siehe Abbildung 8). Die Zugehörigkeit zum neuen gemeinsamen ersten oder zweiten Funktionskanal richtet sich nach dem Verlauf der Signalpfade. Die unter Schritt 9 genannten Kriterien zur Überprüfung des sicherheitsbezogenen Blockdiagramms müssen auch nach der Zusammenfassung erfüllt bleiben. Doppelte Blöcke im gleichen Kanal, die durch die Zusammenfassung entstehen, müssen nur einmal genannt werden.

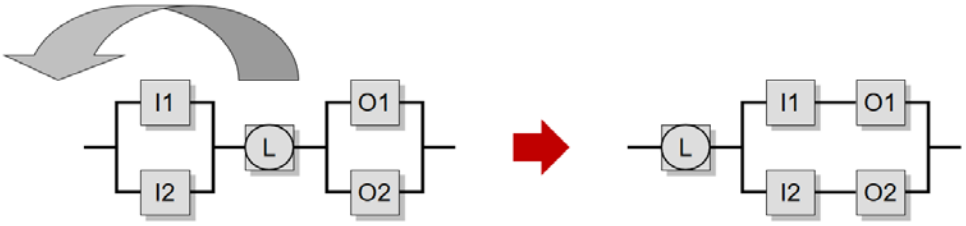
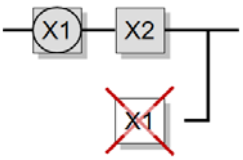
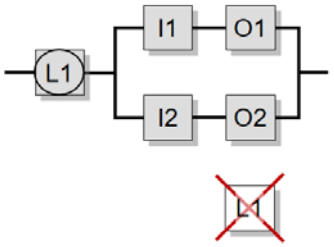


Abbildung 8: Kanalweise Zusammenfassung zweier Subsysteme der Kategorie 3

- Mehrere Subsysteme der Kategorie 4 können in einem Subsystem der Kategorie 4 zusammengefasst werden. Dabei gelten die gleichen Regeln wie für Kategorie 3 genannt.
- Es kann vorkommen, dass ein gekapseltes Subsystem oder ein Bauteil eines Subsystems der Kategorie B oder 1 zusätzlich im Testkanal eines weiteren Subsystems der Kategorie 2 zur gleichen Sicherheitsfunktion erscheint. Im oben beschriebenen Beispiel 2 trifft dies auf die Sicherheits-SPS K1 zu, die bei Spannungsausfall das Einfallen der Klemmeinrichtung einleitet und zusätzlich die statischen und dynamischen Tests der Klemmeinrichtung durchführt und darauf reagiert. Da beim gefährlichen Ausfall eines solchen Bauteils nicht unterschieden wird, welche Funktion ausfällt, wird hier der schlimmste Fall unterstellt, d. h. die Sicherheitsfunktion wird nicht mehr ausgeführt. Ein partieller Ausfall nur der Testfunktion wird nicht berücksichtigt. Da die Ausfallwahrscheinlichkeit des Bauteils schon als gekapseltes Subsystems eingeht, ist eine zusätzliche Berücksichtigung im Testkanal eines weiteren Subsystems nicht erforderlich. Das Bauteil (X1 im Bild rechts) kann in diesem Fall aus dem Testkanal gestrichen werden. In seltenen Fällen kann es dadurch dazu kommen, dass ein Subsystem der Kategorie 2 im Testkanal gar keinen Block mehr enthält.



- In ähnlicher Weise kann (wie L1 im Bild rechts) ein Bauteil als gekapseltes Subsystem und zusätzlich informativ als nur testendes Bauteil in Subsystemen der Kategorie 3 oder 4 zur gleichen Sicherheitsfunktion erscheinen. Dann braucht wie im vorgenannten Punkt seine untergeordnete Rolle als testendes Bauteil im sicherheitsbezogenen Blockdiagramm nicht dargestellt zu werden.



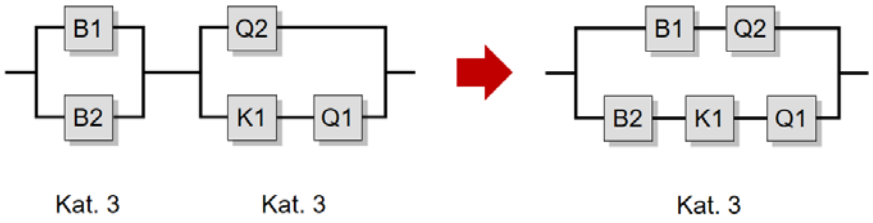
  In ähnlicher Weise kann verfahren werden, wenn L1 im Bild oben kein gekapseltes Subsystem, sondern ein Bauteil eines Subsystems der Kategorie B oder 1 zur gleichen Sicherheitsfunktion wäre. Dieser Fall ist in der Praxis aber kaum relevant.

Die hier beschriebenen Vereinfachungen sind oft vorteilhaft, aber nicht zwingend erforderlich. Da SISTEMA innerhalb der Subsysteme die $MTTF_D$-Werte jedes Kanals begrenzt (Kappung), kann sich durch die Zusammenfassung von Subsystemen gleicher Kategorie rechnerisch eine geringere Wahrscheinlichkeit für einen gefährlichen Ausfall pro Stunde ergeben. Diese kleinere Ausfallwahrscheinlichkeit (PFH_D) ist ein Vorteil. Durch die zusammengefasste Darstellung ist die physikalische Abfolge der Signalverarbeitung aber oft schwerer zu erkennen. Im Zweifelsfall kann mit SISTEMA eine vergleichende Berechnung der verschiedenen Darstellungen durchgeführt werden, um die günstigste Kombination zu ermitteln. Grundsätzlich bilden aber alle Möglichkeiten das Prinzipschaltbild korrekt ab.

3.4 Strukturanalyse für Beispiel 1

In Beispiel 1 besteht der kürzeste Signalpfad aus dem Positionsschalter B1 und dem Schütz Q2. Die Strukturanalyse für B1 zeigt, dass weder ein gekapseltes Subsystem vorliegt, noch alle Bauteilfehler ausgeschlossen werden können. Mit dem zweiten Positionsschalter B2 liegt aber ein zu B1 redundantes Bauteil vor, dass die Kriterien für Kategorie 3 (aber nicht für Kategorie 4) erfüllt. Damit ist für B1 und B2 mit Schritt 5b die Zuordnung erfolgt und die Strukturanalyse kann mit Q2 fortgesetzt werden. Sie führt auf dem gleichen Pfad durch das Flussdiagramm auf ein Kategorie-3-Subsystem aus den beiden Schützen Q2 und Q1. Spätestens in Schritt 9 wird dann K1 als fehlendes Glied im zweiten Funktionskanal zwischen B2 und Q1 identifiziert. In Schritt 10 können dann die beiden Subsysteme der Kategorie 3 wie in Abbildung 9 dargestellt zusammengefasst werden.

Abbildung 9: Letzter Schritt und Ergebnis der Strukturanalyse für Beispiel 1



3.5 Strukturanalyse für Beispiel 2

In Beispiel 2 beginnt die Strukturanalyse mit der Sicherheits-SPS K1, die direkt in Schritt 3 als gekapseltes Subsystem identifiziert werden kann. Für die folgenden Blöcke des Funktionskanals, K2, 0V1 und Q1, wird das Flussdiagramm anschließend auf einem anderen Pfad durchlaufen. Für alle drei trifft erst das Kriterium aus Schritt 6 (Bauteilfehler werden ausreichend gut erkannt) zu, so dass eine Zuordnung zu Kategorie-2-Subsystemen erfolgt und die jeweiligen Testkanäle hinzugefügt werden. In Schritt 10 können dann die drei Subsysteme der Kategorie 2 wie in Abbildung 10 dargestellt kanalweise zusammengefasst werden. K1 braucht dabei im zusammengefassten Testkanal nur einmal aufgeführt zu werden. In einem weiteren Vereinfachungsschritt wird K1 ganz aus dem Testkanal gelöscht, da K1 bereits als gekapseltes Subsystem in derselben Sicherheitsfunktion auftaucht. Zur besseren Erkennbarkeit kann das gekapselte Subsystem K1 anschließend ans Ende gestellt werden.

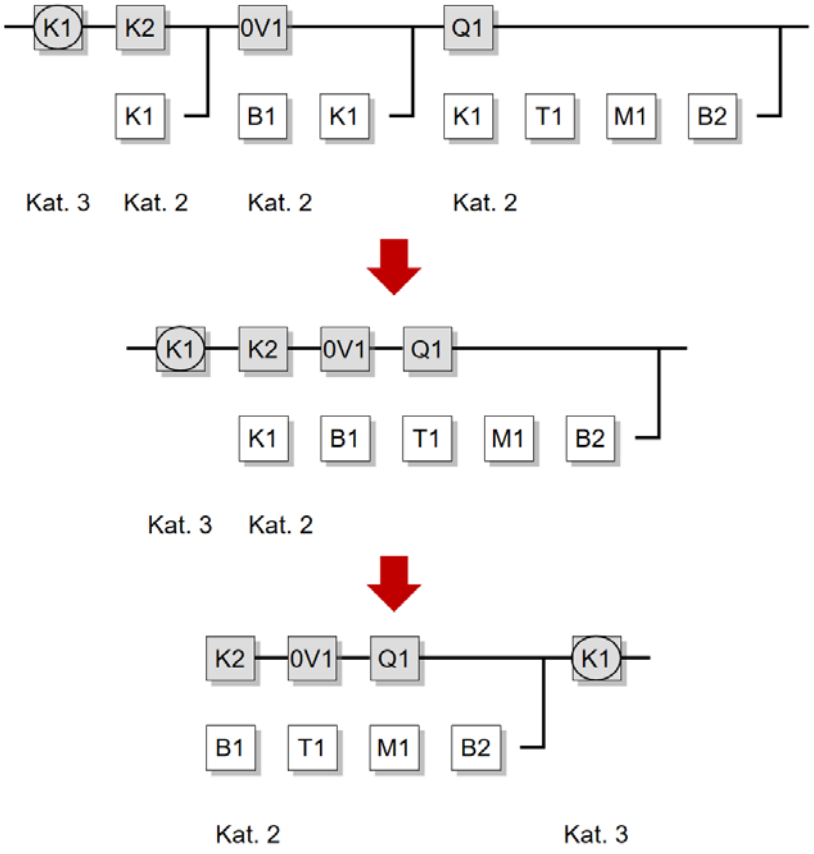


Abbildung 10: Vereinfachung des sicherheitsbezogenen Blockdiagramms und Ergebnis der Strukturanalyse für Beispiel 2 aus Kapitel 2

Mit dem sicherheitsbezogenen Blockdiagramm liegt nun die logische Darstellung der Sicherheitsfunktion vor. Das nächste Kapitel beschreibt die Übertragung nach SISTEMA und die darauf basierende Berechnung der Ausfallwahrscheinlichkeit (**PFH_D**).

4 Übertragung nach SISTEMA

Das Software-Tool SISTEMA verwendet mehrere Hierarchieebenen (Abbildung 11). Die einzelnen Ebenen erklärt Tabelle 3.

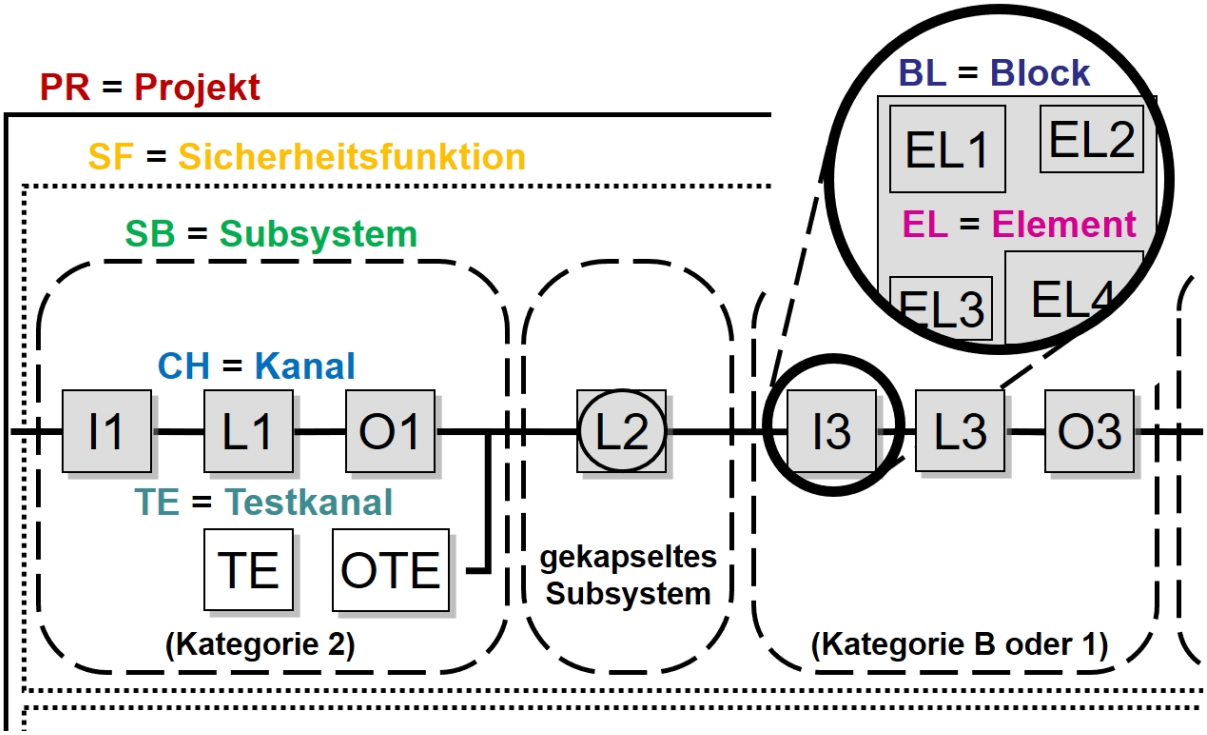
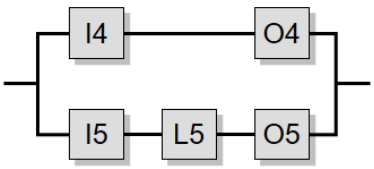
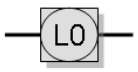
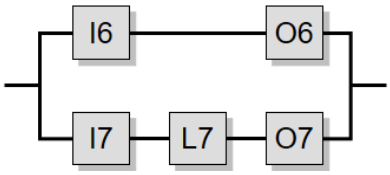
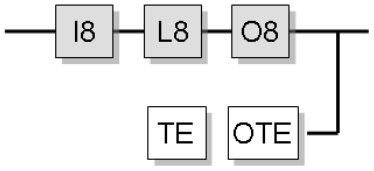
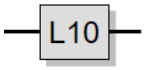


Abbildung 11: Hierarchieebenen in SISTEMA

Tabelle 3: Beschreibung der Hierarchieebenen in SISTEMA

Name	Beschreibung	Beispiele
Projekt	Zusammenfassung von Sicherheits-funktionen, z. B. an einer (Teil-) Maschine oder Gefahrenstelle	Arbeitsraumtür an Drehmaschine XY
Sicherheits-funktion	Sicherheitsgerichtete Reaktion auf ein auslösendes Ereignis	Sicherer Betriebshalt bei Öffnen einer Schutztür
Subsystem	a) Gruppe von Blöcken in einer festen Struktur (Kategorie) b) Sicherheitsbauteil mit Herstellerangabe von PL, PFH_D und Kategorie (gekapseltes Subsystem)	a) Kategorie-3-Subsystem  b) Sicherheits-SPS 

Name	Beschreibung	Beispiele
Kanal	Serienschaltung von Blöcken, SISTEMA legt je nach gewählter Kategorie einen oder zwei Funktionskanäle an.	Funktionskanal 1  Funktionskanal 2
Testkanal	Serienschaltung von Blöcken zur Testfunktion, SISTEMA legt nur in Kategorie 2 einen Testkanal an.	Funktionskanal 1  Testkanal
Block	Bauteil im Funktions- oder Testkanal.	 Standard-SPS, Ventil, Schütz, Schalter
Element	Ein Block beinhaltet ein oder mehrere Elemente. Bei sehr vielen Bauteilen in einem Kanal können diese durch Blöcke, die Elemente enthalten, übersichtlicher dargestellt werden.	 Elektronische Bauteile (IC, Widerstände, Halbleiter)

Im Folgenden werden alle erforderlichen Schritte zur Erstellung eines SISTEMA-Projekts und zur Berechnung erläutert. Die Eingaben zur Dokumentation haben keinen Einfluss auf die Berechnung; hierauf wird nicht eingegangen.

Anmerkung: Es empfiehlt sich, die Reihenfolge der Eingaben so zu wählen, dass die Registerkarten im Arbeitsbereich von links nach rechts und die Hierarchieebenen (Baumansicht im Navigationsfenster) von oben nach unten abgearbeitet werden.

4.1 Projekt anlegen

In einem Projekt können alle Sicherheitsfunktionen einer (Teil-)Maschine zusammengefasst werden (Abbildung 12). Nach dem Anlegen eines neuen Projektes mit „Neu“ (1.) erscheint im Navigationsfenster hinter dem Kürzel **PR** ein neues Projekt (2.), für das im Eingabefeld „Projektname“ (3.) eine Bezeichnung eingegeben werden kann.

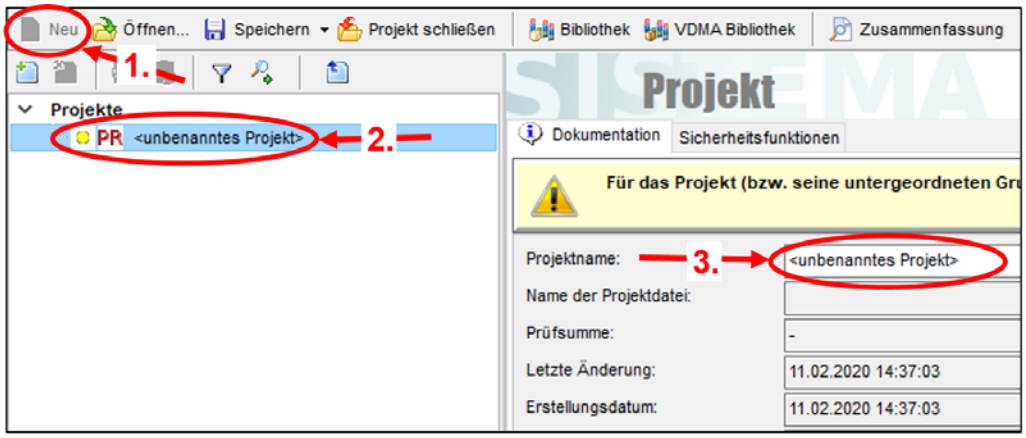


Abbildung 12: Projekt anlegen

4.2 Sicherheitsfunktionen anlegen

In der Registerkarte „Sicherheitsfunktion“ (2.) des Projekts (1.) werden durch die Schaltfläche „Neu“ (3.) die erforderlichen Sicherheitsfunktionen angelegt (Abbildung 13). Der „Name der Sicherheitsfunktion“ erscheint auch im Navigationsfenster hinter dem Kürzel **SF** (siehe Abbildung 14).

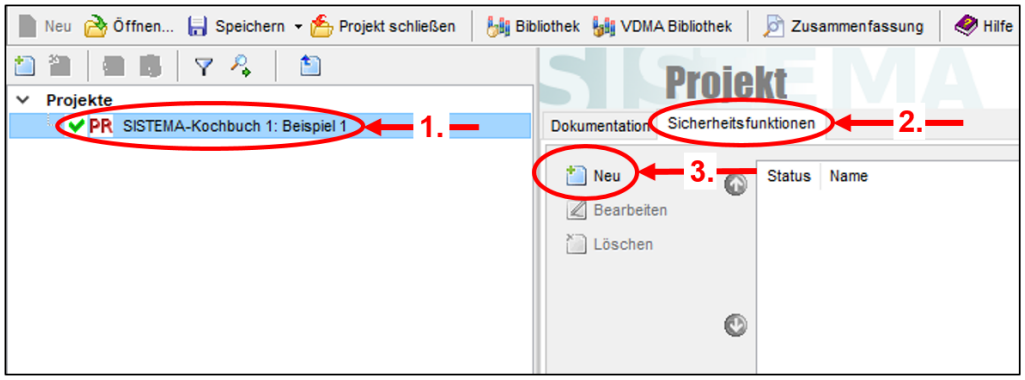


Abbildung 13: Sicherheitsfunktionen anlegen

4.3 PL_r festlegen

Der erforderliche Performance Level PL_r wird individuell für jede Sicherheitsfunktion (1.) festgelegt (Abbildung 14). Dazu benutzt man in der Registerkarte „PL_r“ (2.) den Risikographen (3.) oder gibt den PL_r direkt ein, z. B. wenn eine Vorgabe durch eine maschinenspezifische Norm vorliegt.

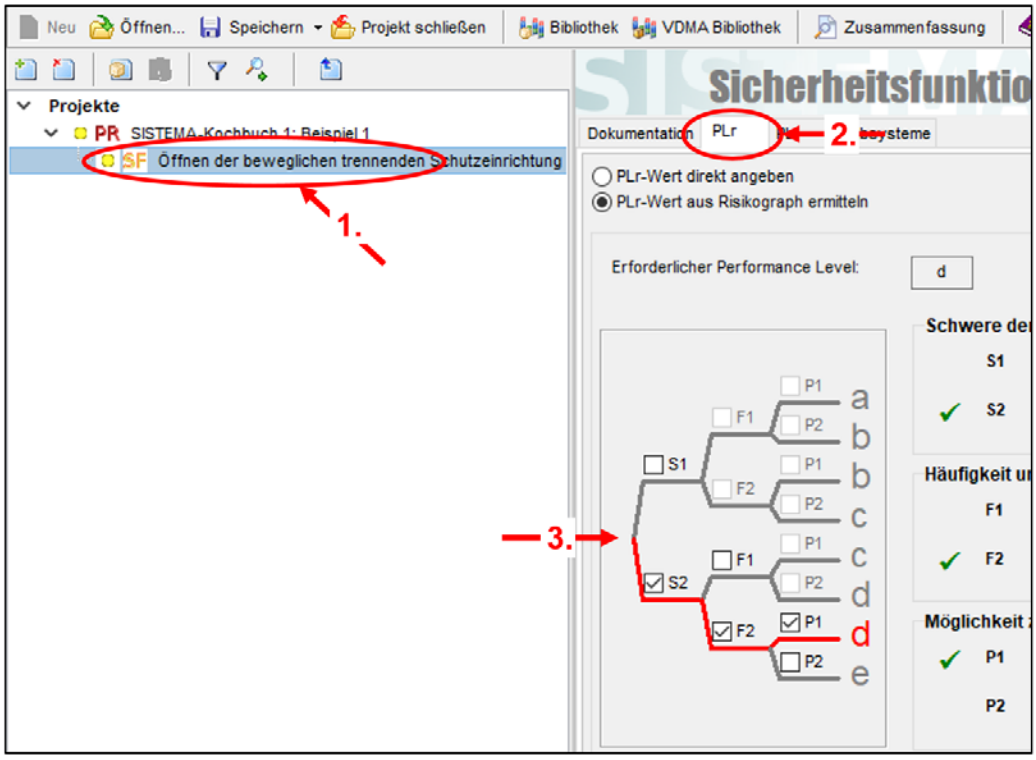


Abbildung 14: PL_r festlegen

4.4 Subsysteme hinzufügen

Die im sicherheitsbezogenem Blockdiagramm ermittelten Subsysteme werden angelegt, indem sie unter der Sicherheitsfunktion (1.) in der Registerkarte „Subsysteme“ (2.) durch „Neu“ (3.) hinzugefügt (Abbildung 15) werden.

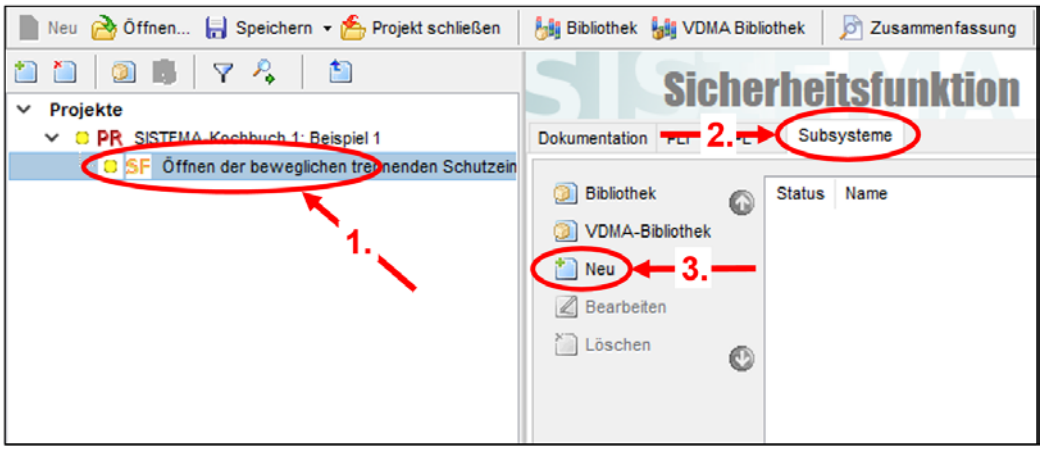


Abbildung 15: Subsysteme hinzufügen

4.5 Gekapselte Subsysteme mit PL, PFH_D und Kategorie

Für gekapselte Subsysteme liegen meist Herstellerangaben zu PL, PFH_D und Kategorie vor. Die PL- und PFH_D-Werte werden in dem Subsystem (1.) in der Registerkarte „PL“ (2.) nach Auswahl von „PL bzw. PFH_D-Wert direkt angeben“ (3.) in mehreren Eingabefeldern (4.) eingetragen (Abbildung 16).

Anmerkung: Falls das Häkchen gesetzt ist (4.), erfolgt eine wechselseitige Berechnung von PL und PFH_D (z. B. PFH_D-Wert in der Mitte des zugehörigen logarithmisch skalierten Wertebereichs für den angegebenen PL).

Fehlerausschluss: Bei gekapselten Subsystemen, bei denen alle gefährlichen Bauteilfehler ausgeschlossen werden, wird das Häkchen „Fehlerausschluss“ gesetzt (5.) (➔ PFH_D=0).

Wenn für dieses Subsystem Anwendungssoftware notwendig ist (z.B. ein SPS-Programm für eine Sicherheits-SPS), kann deren Qualität als PL dieser Software in der Auswahlliste (6.) dokumentiert werden. Abschließend muss noch die Gebrauchsdauer des Subsystems (Herstellerangabe) angeben werden (7.).

Die Kategorie kann in der nächsten Registerkarte „Kategorie“ (8.) eingegeben werden. Da PL und PFH_D für dieses Subsystem vorliegen, ist die Kategorieangabe für die Berechnung der PFH_D der gesamten Sicherheitsfunktion zwar nicht erforderlich, die Kategorie muss aber gemäß Abschnitt 11 der Norm dokumentiert werden.

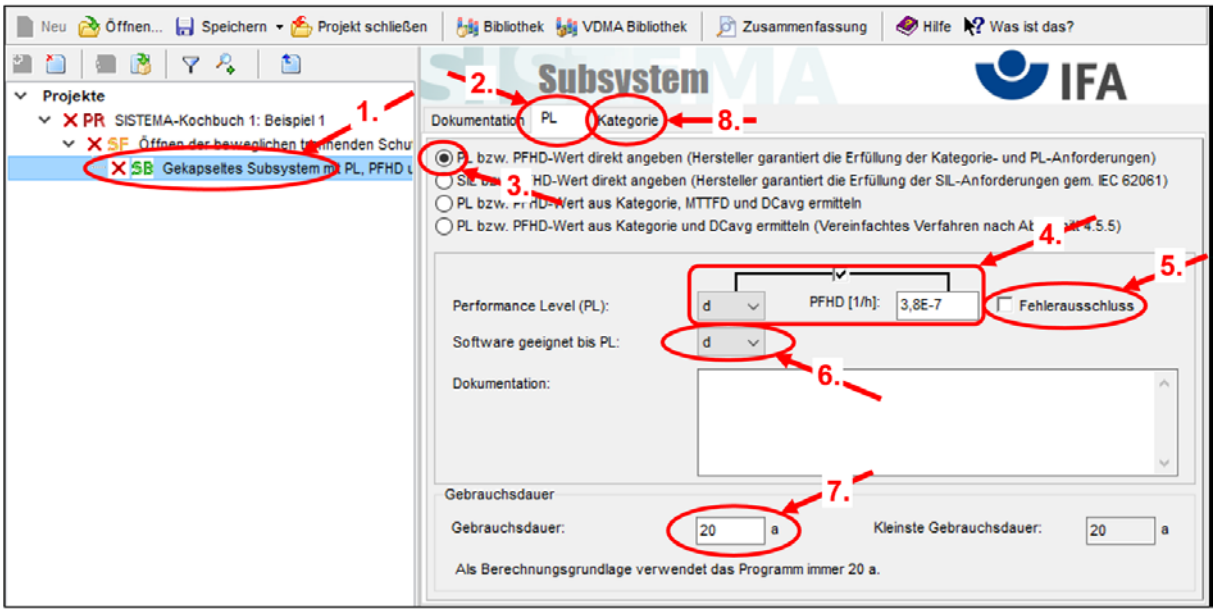


Abbildung 16: Gekapselte Subsysteme mit PL, PFH_D und Kategorie

4.6 Gekapselte Subsysteme mit SIL und PFH_D

Alternativ können für gekapselte Subsysteme (1.) auch Herstelleranagaben zu SIL und PFH_D gemäß IEC 62061 vorliegen und in SISTEMA eingetragen werden (Abbildung 17). Dazu muss in der Registerkarte „PL“ (2.) die zweite Option (3.) ausgewählt werden. Aus der Eingabe von SIL und PFH_D-Wert (4.) wird ein entsprechender PL abgeleitet. Die weiteren Eingaben werden entsprechend Abschnitt 4.5 vorgenommen. Die Angabe einer Kategorie entfällt allerdings.

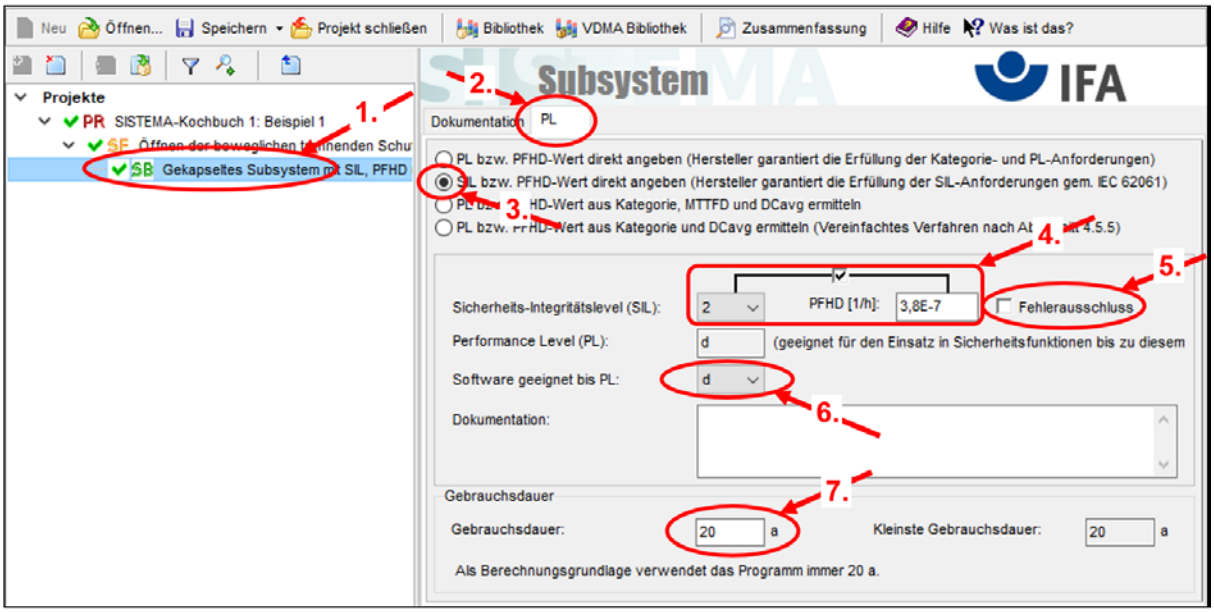


Abbildung 17: Gekapselte Subsysteme mit SIL und PFH_D

4.7 Subsysteme als Gruppe von Blöcken in einer festen Struktur (Kategorie)

Im Subsystem (1.) erfolgt unter „PL“ (2.) die Auswahl von „PL bzw. PFH_D-Wert aus Kategorie, $MTTF_D$ und DC_{avg} ermitteln“ (3.) (Abbildung 18).

Mit dem Anklicken in der Liste (4.) wird bestätigt, dass diese Aspekte bei der Abschätzung des PL berücksichtigt wurden. Wenn für das Subsystem keine Anwendungssoftware erforderlich ist, bleibt in der Auswahlliste (5.) der Eintrag „n.a.“ stehen, ansonsten wäre hier der PL für diese Software einzutragen.

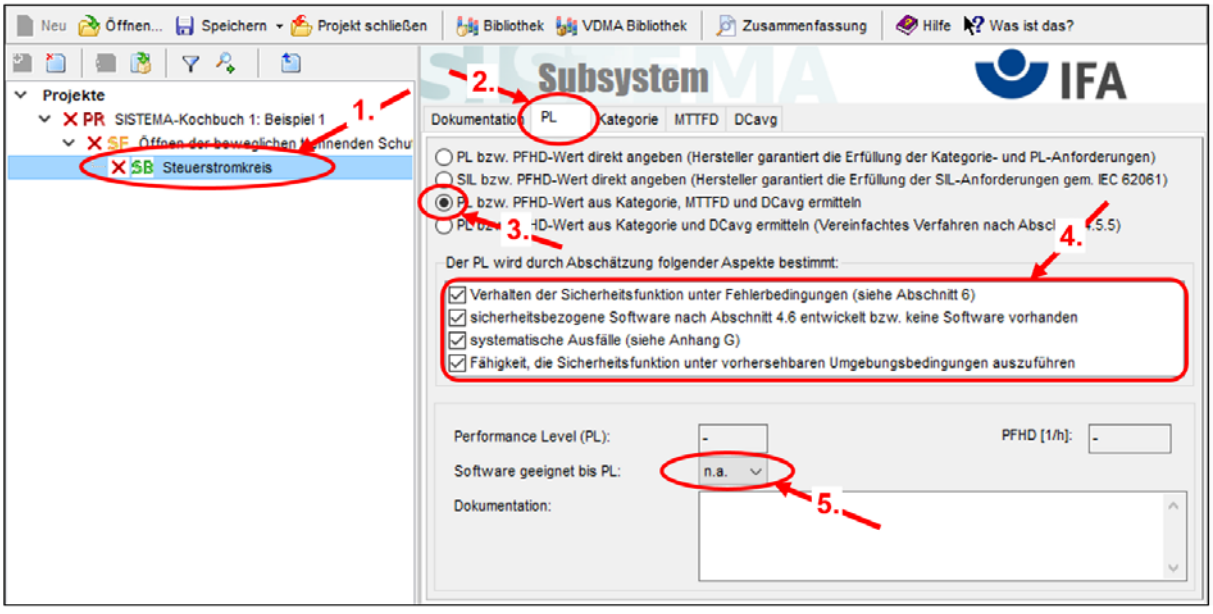


Abbildung 18: Subsysteme als Gruppe von Blöcken definieren

Danach werden:

a) im Subsystem (1.) unter „Kategorie“ (2.) (Abbildung 19) die jeweilige Kategorie (3.) ausgewählt und die Erfüllung der „Anforderungen der Kategorie“ (4.) durch Anklicken bestätigt. Die letzten drei Anforderungen werden von SISTEMA überprüft.

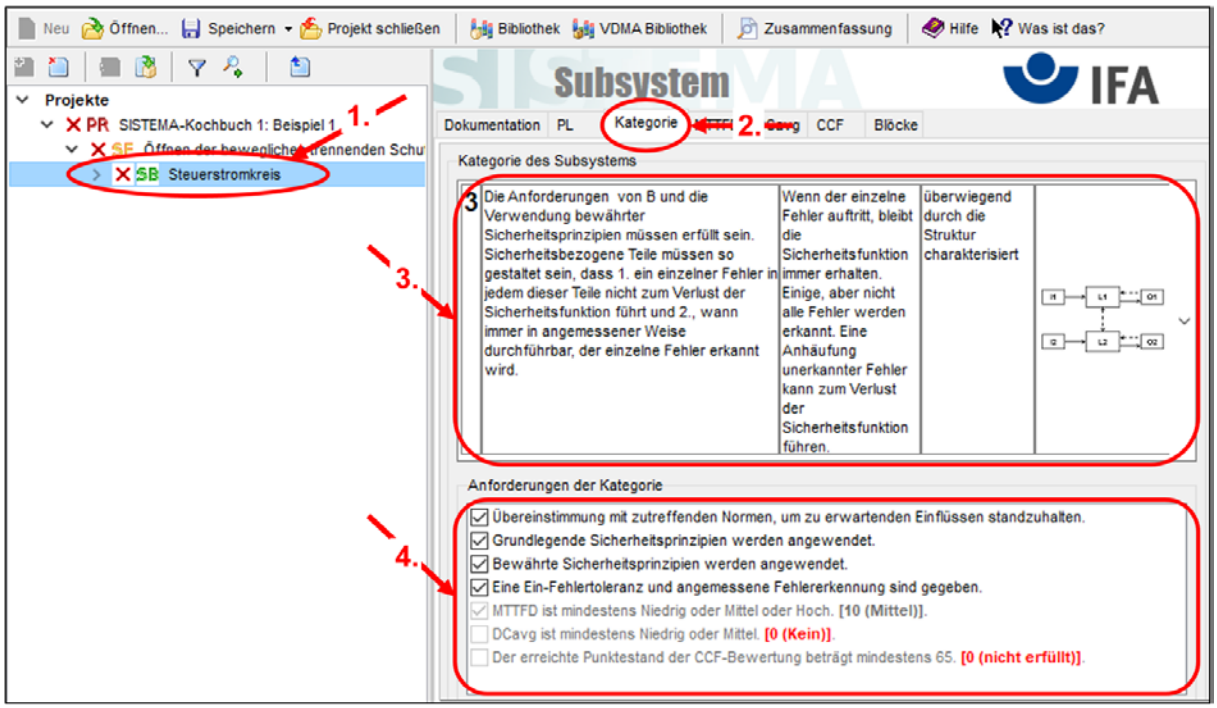


Abbildung 19: Auswahl der Kategorie

b) im Subsystem (1.) unter „$MTTF_D$“ (2.) ist die Auswahl „$MTTF_D$-Wert aus Blöcken ermitteln“ voreingestellt (3.) und wird typischerweise nicht verändert (Abbildung 20). In Sonderfällen könnte hier die Auswahl „$MTTF_D$-Wert direkt angeben“ getroffen werden. Dazu muss die entsprechende Option in den Experteneinstellungen aktiviert werden.

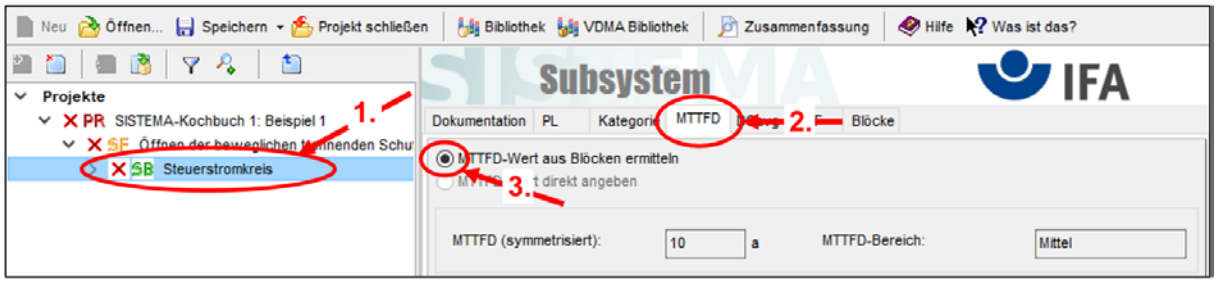


Abbildung 20: $MTTF_D$-Wert aus Blöcken ermitteln

c) im Subsystem (1.) unter „DC_{avg}“ (2.) ist die Auswahl „DC_{avg}-Wert aus Blöcken ermitteln“ voreingestellt (3.) und wird typischerweise nicht verändert (Abbildung 21). In Sonderfällen könnte hier die Auswahl „DC_{avg}-Wert direkt angeben“ getroffen werden. Dazu muss die entsprechende Option in den Experteneinstellungen aktiviert werden.

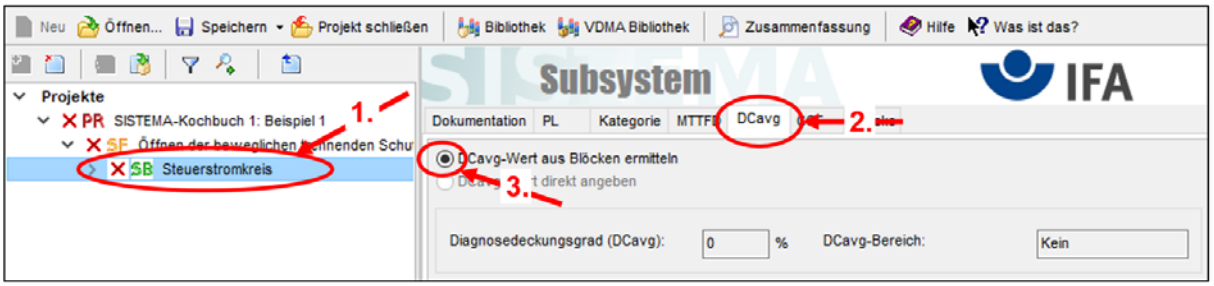


Abbildung 21: DC_{avg}-Wert aus Blöcken ermitteln

d) Für jedes zweikanalige Subsystem sind Fehler zu berücksichtigen, bei denen beide Kanäle durch dieselbe Ursache ausfallen (CCF). Davon sind die Kategorien 2 (Funktionskanal und Testkanal) sowie 3 und 4 (jeweils zwei Funktionskanäle) betroffen.

Die Eingabe erfolgt im Subsystem (1.) unter „CCF“ (2.) durch Auswahl der zu treffenden Maßnahmen (Abbildung 22). Es müssen mindestens 65 Punkte erreicht werden. Die erreichte Punktzahl kann über eine Maßnahmen-Bibliothek zusammengestellt (3.) oder direkt eingegeben werden. In der Bibliothek (4.) sind die zutreffenden Maßnahmen auszuwählen (5.) und in die Liste der Registerkarte „CCF“ zu laden (6.).

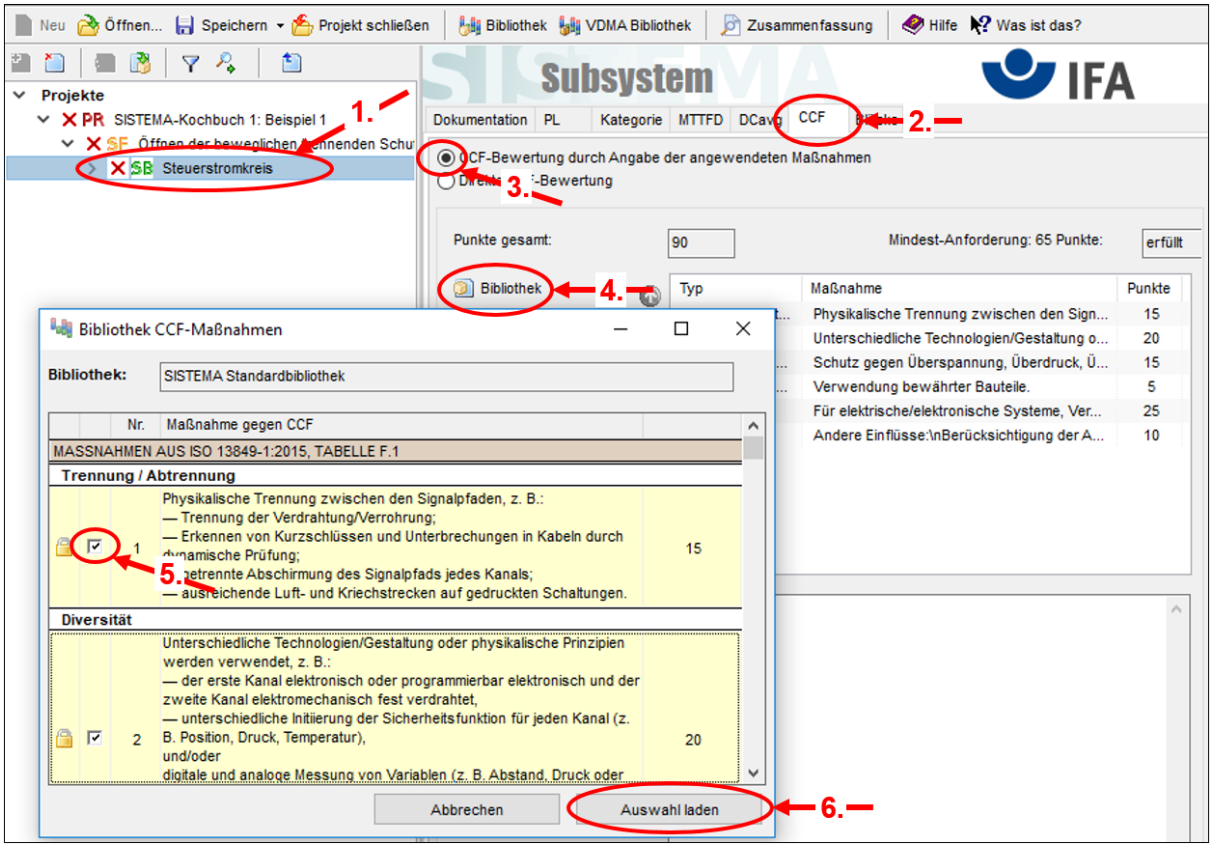


Abbildung 22: CCF bewerten

4.7.1 Blöcke eingeben

Nachdem die Subsysteme gebildet wurden, ist eine weitere Spezifizierung vorzunehmen (Ausnahme: Abschnitte 4.5 und 4.6 „Gekapselte Subsysteme“). SISTEMA hat durch die Auswahl der Kategorie eines Subsystems die relevanten Kanäle (**CH**) gebildet. Unter „Kanal“ werden die Blöcke **BL** hinzugefügt, die den einzelnen Bauteilen eines Kanals entsprechen. Diese Blöcke können neu definiert werden (Schaltfläche „Neu“) oder aus Bibliotheken geladen werden.

Typischerweise ist eine weitere Gliederung der Blöcke nicht erforderlich ist, d. h. es können alle Bauteile als Blöcke eingetragen werden. **Dann geht es direkt mit Schritt 4.7.3 weiter.** Falls doch eine weitere Gliederung eines Blocks in Elemente erfolgen soll (nur bei sehr vielen Bauteilen sinnvoll), sind folgende Einstellungen erforderlich:

a) im Block (1.) unter „$MTTF_D$“ (2.) die Auswahl „$MTTF_D$-Wert aus Elementen ermitteln“ (3.) (Abbildung 23) treffen. Im Feld (4.) wird der aus den untergeordneten Elementen ermittelte $MTTF_D$-Wert dargestellt.

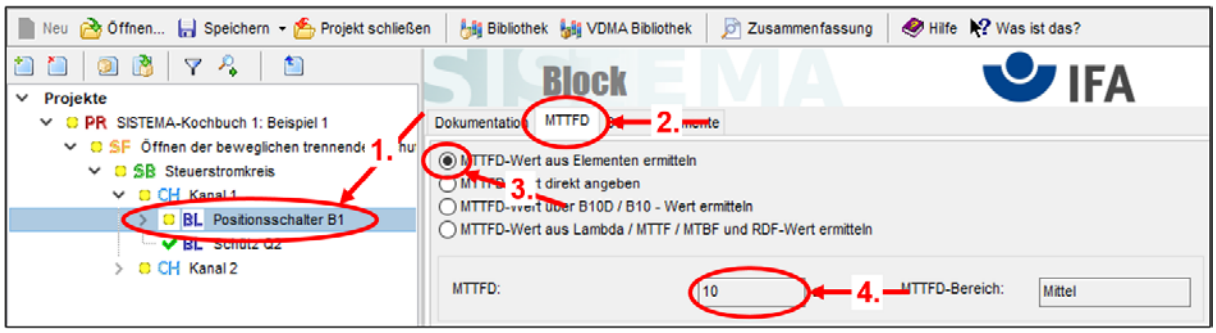


Abbildung 23: $MTTF_D$-Wert aus Elementen ermitteln

b) im Block (1.) unter „DC“ (2.) die Auswahl „DC-Wert aus Elementen ermitteln“ (3.) (Abbildung 24) treffen. Im Feld (4.) wird der aus den untergeordneten Elementen ermittelte DC-Wert dargestellt.

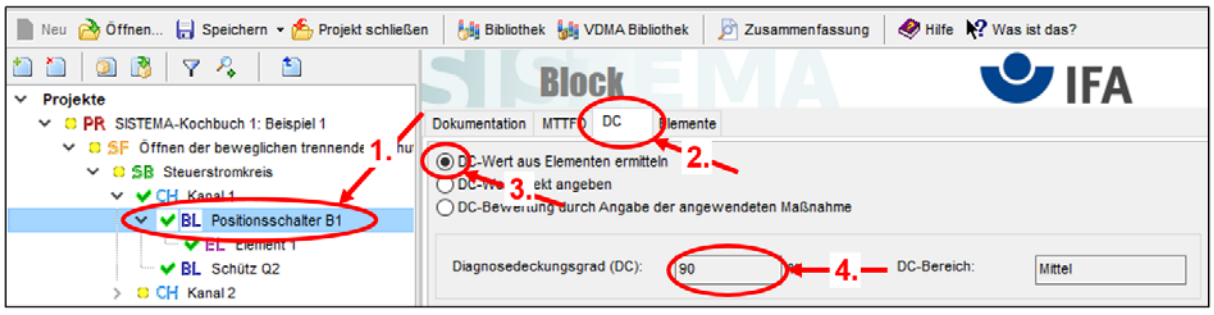


Abbildung 24: DC-Wert aus Elementen ermitteln

4.7.2 Elemente eingeben

Falls ein Block in Elemente **EL** unterteilt werden soll, sind im Block (1.) unter „Elemente“ (2.) durch „Neu“ (3.) Elemente anzulegen (Abbildung 25). Alternativ können auch hier neue Elemente aus den Bibliotheken geladen werden.

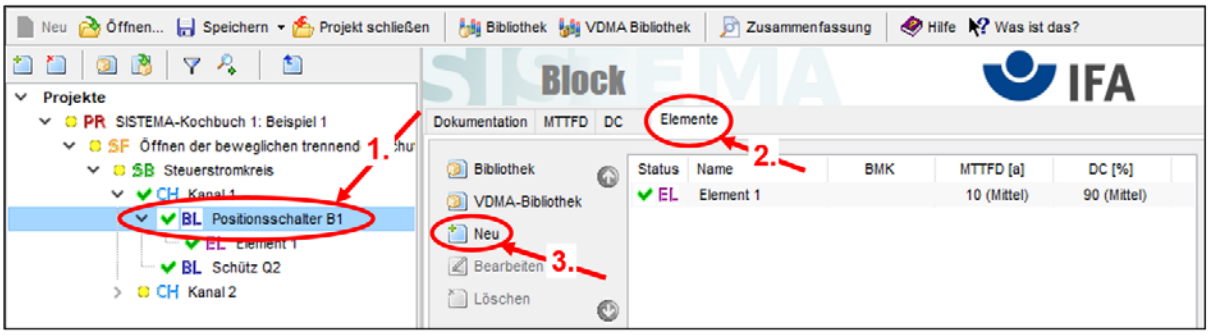


Abbildung 25: Elemente eingeben

Auf Elementebene (1.) können in den Registerkarten „$MTTF_D$“ (2.) und „DC“ (3.) die Daten zum Element eingegeben werden (Abbildung 26). Diese Registerkarten entsprechen denen eines Blocks und werden im folgenden Schritt 4.7.3 beschrieben.

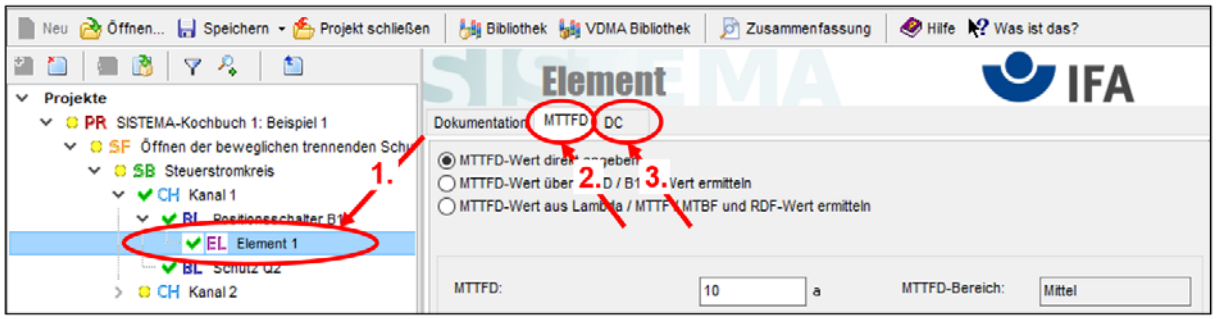


Abbildung 26: MTTFD und DC im Element eintragen

4.7.3 Sicherheitsrelevante Daten eingeben

Zu den für die Berechnung der PFH_D erforderlichen sicherheitsrelevanten Daten gehören die jeweilige Bauteilgüte ($MTTF_D$, B_{10D} u.a.), die Anzahl der Betätigungen von verschleißbehafteten elektromechanischen und pneumatischen Bauteilen (n_{op}) und der Diagnosedeckungsgrad (DC). Die sicherheitsrelevanten Parameter der Bauteile können ermittelt werden:

a) aus Herstellerangaben,

b) aus etablierten Datensammlungen (Quellen siehe DIN EN ISO 13849-1, Literaturhinweise – Datenbanken) oder

c) aus DIN EN ISO 13849-1, Anhang C; hinterlegt in SISTEMA unter „Typische Bauteilwerte“ (Abbildung 27, (5.)).

4.7.3.1 $MTTF_D$ bzw. λ_D direkt eingeben

Wenn für ein Bauteil $MTTF_D$-Werte vorliegen, erfolgt die Eingabe auf Block- bzw. Elementebene (1.) in der Registerkarte „$MTTF_D$“ (2.) mit der Auswahl „$MTTF_D$-Wert direkt eingeben“ (3.) im Eingabefeld „$MTTF_D$“(4.) (Abbildung 27). Anstelle des $MTTF_D$-Wertes kann in dem Eingabefeld darunter die Ausfallrate λ_D in der Einheit FIT eingetragen und umgerechnet werden.

Wenn alle gefährlichen Bauteilfehler ausgeschlossen werden können, kann bei Auswahl von „$MTTF_D$ direkt eingeben“ auch ein Fehlerausschluss gewählt werden (6).

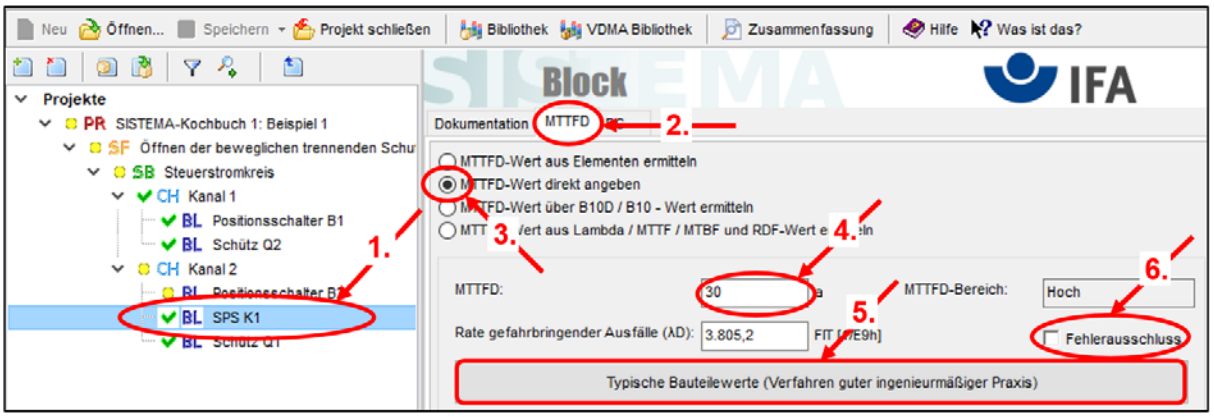


Abbildung 27: $MTTF_D$ bzw. λ_D direkt im Block eingeben

4.7.3.2 $MTTF_D$ über B_{10D}- oder B_{10}-Wert ermitteln

Wenn für ein Bauteil B_{10D}- oder B_{10}-Werte vorliegen, erfolgt die Eingabe auf Block- bzw. Elementebene (1.) in der Registerkarte „$MTTF_D$“ (2.) mit der Auswahl „$MTTF_D$-Wert über B_{10D}- / B_{10}-Wert ermitteln“ (3.) (Abbildung 28). Im Auswahlfeld (4.) wird der entsprechende Parameter ausgewählt und der Wert in Eingabefeld (5.) eingetragen. Unter „Typische Bauteilwerte“ (6.) können die in der DIN EN ISO 13849-1, Anhang C hinterlegten Werte ausgewählt werden.

Anhand der Verwendung des verschleißbehafteten Bauteils in der konkreten Steuerungsapplikation muss die Anzahl seiner Betätigungen (n_{op}) abgeschätzt und eingetragen werden (7.). Dabei kann der integrierte „n_{op}-Rechner“ (8.) helfen.

Bei Auswahl von „B_{10}“ kann der gefahrbringende Parameteranteil genauer spezifiziert werden. Im dann eingeblendeten Eingabefeld „RDF“ wird dazu der prozentuale Anteil gefahrbringender Ausfälle zu allen Ausfällen eingetragen – soweit dieser bekannt ist oder abgeschätzt werden kann.

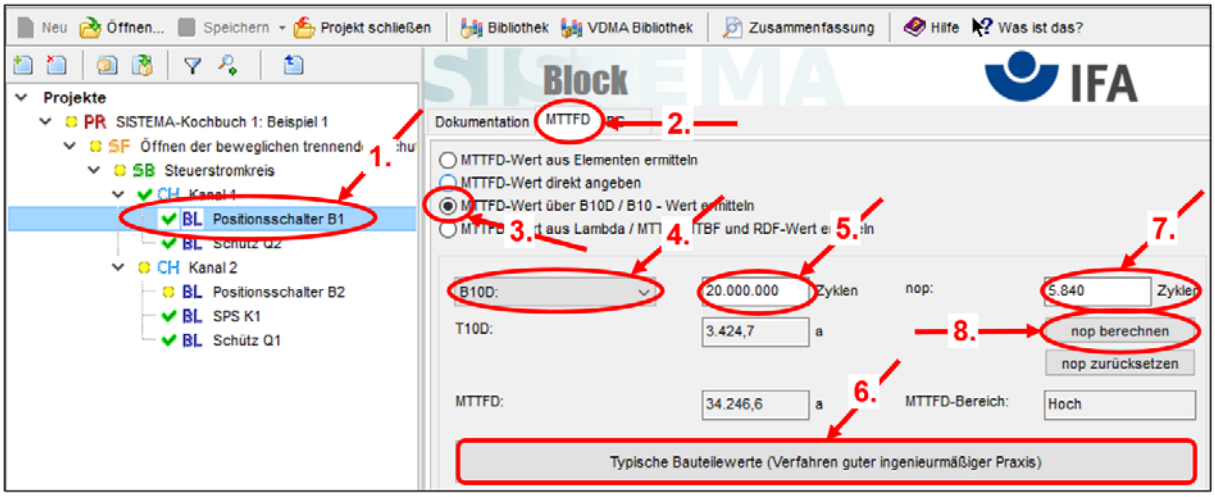


Abbildung 28: $MTTF_D$ des Blocks über B_{10D}- oder B_{10}-Wert ermitteln

4.7.3.3 $MTTF_D$ über MTTF-, MTBF- oder λ-Werte ermitteln

Wenn für ein Bauteil MTTF-, MTBF- oder λ-Werte vorliegen, erfolgt die Eingabe auf Block- bzw. Elementebene (1.) in der Registerkarte „$MTTF_D$“ (2.) mit der Auswahl „$MTTF_D$-Wert aus

Lambda / MTTF / MTBF und RDF-Wert ermitteln“ (3.) (Abbildung 29). Im Auswahlfeld (4.) wird der entsprechende Parameter ausgewählt und der Wert in Eingabefeld (5.) eingetragen.

Um die gefahrbringenden Parameteranteile genauer zu spezifizieren, kann im Eingabefeld „RDF“ (6.) der prozentuale Anteil gefahrbringender Ausfälle zu allen Ausfällen eingetragen werden – soweit dieser bekannt ist oder abgeschätzt werden kann.

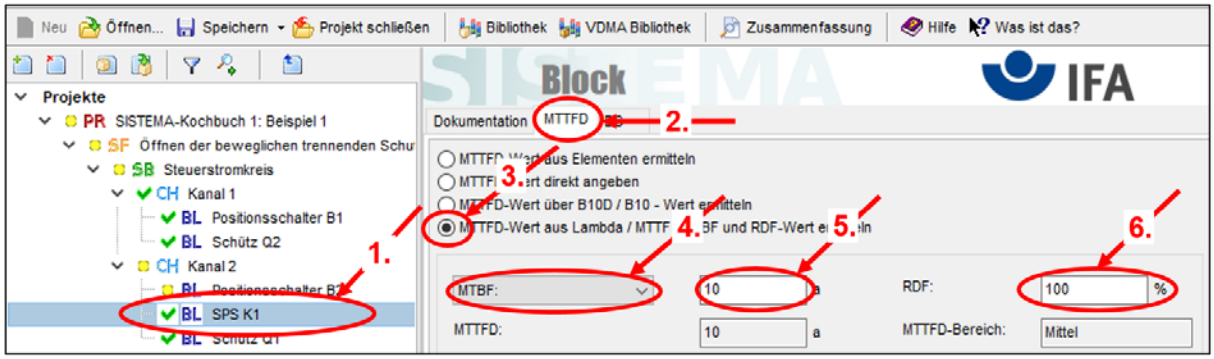


Abbildung 29: $MTTF_D$ des Blocks über MTTF-, MTBF- oder λ-Werte ermitteln

4.7.3.4 DC ermitteln

Ab Kategorie 2 sind Fehler erkennende Maßnahmen für die Bauteile erforderlich. Im Block oder Element (1.) wird für jedes Bauteil in der Registerkarte „DC“ (2.) eine Prozentzahl eingegeben, um den Abdeckungsgrad der Fehlererkennung zu beschreiben (Abbildung 30).

Bei Auswahl von „DC-Bewertung durch Angabe der angewendeten Maßnahme“ (3.) kann über „Bibliothek“ (4.) auf die DC-Tabellen aus DIN EN ISO 13849-1, Anhang E zugegriffen werden. Die Werte können direkt übernommen oder zur Orientierung herangezogen werden. Schlägt die Norm eine Spanne möglicher DC-Werte vor, kann innerhalb dieser Spanne ein begründbarer, konkreter Wert eintragen werden (5.).

Alternativ kann bei Auswahl von „DC-Wert direkt angeben“ ebenfalls ein begründbarer, konkreter Wert eintragen werden.

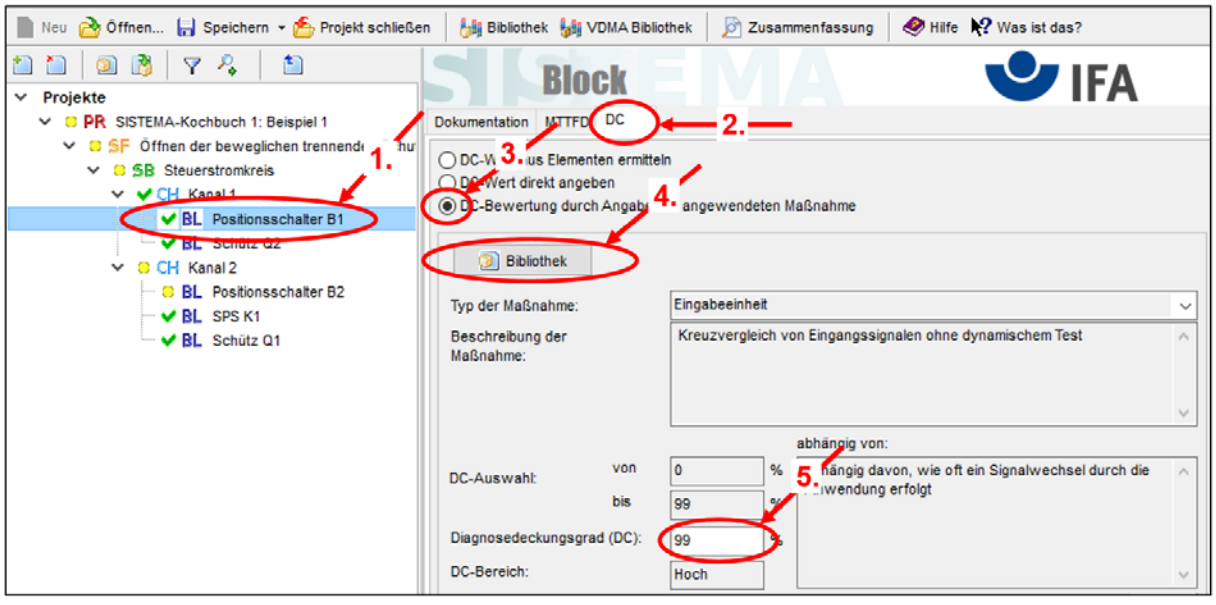


Abbildung 30: DC des Blocks ermitteln

4.8 Ziel erreicht?

Im Hinweisfenster (rechts, unten) ist zu prüfen, ob Fehlermeldungen mit einem roten Kreuz vorliegen, wie z. B. in Abbildung 31. Falls dies nicht der Fall ist, lässt sich die PFH_D berechnen.

Abbildung 31: Hinweisfenster

Das Ergebnis der Berechnung wird für die ausgewählte Sicherheitsfunktion und die jeweiligen Subsysteme, Blöcke und eventuell Elemente im Kontextfenster (links, unten) angezeigt (Abbildung 32). Der (erreichte) PL der Sicherheitsfunktion muss mindestens dem (erforderlichen) PL_r entsprechen. Ist der erreichte PL ungenügend, sind Bauteile mit einer höheren $MTTF_D$ oder einem höheren B_{10D}-Wert einzusetzen, die Fehlererkennung (DC) zu verbessern oder es sind gegebenenfalls Subsysteme anderer Kategorien zu realisieren.

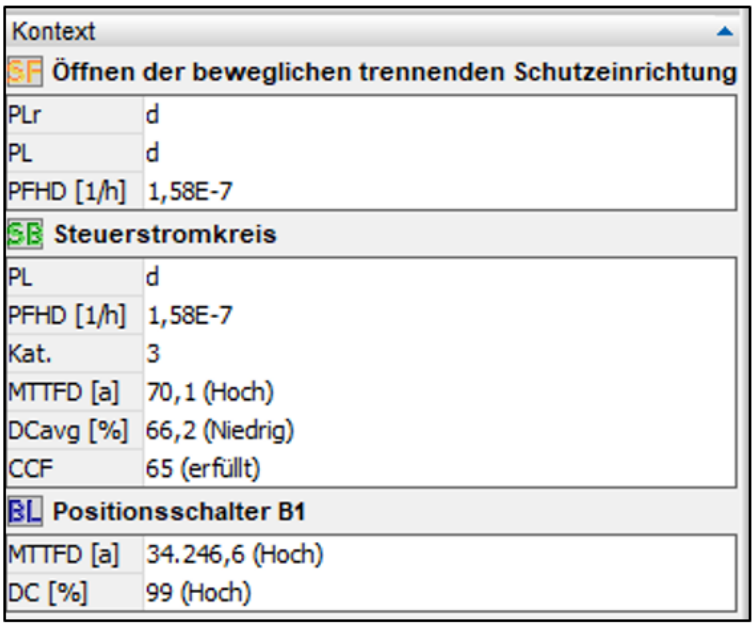


Abbildung 32: Kontextfenster

Anhang A: Begriffe und Abkürzungen

Definition grundlegender Begriffe, die in ähnlicher Weise auch in Anhang B der DIN EN ISO 13849-1 aufgeführt sind:

Begriffe	Definition
Sicherheitsfunktion (SF)	Sicherheitsgerichtete Reaktion auf ein auslösendes Ereignis (Anforderung der Sicherheitsfunktion). In redundanten Systemen wird die Sicherheitsfunktion mehrfach unabhängig ausgeführt. Der PL beschreibt die Zuverlässigkeit der Ausführung.
Prinzipschaltbild	Auszug aus dem Schaltplan oder Funktionsschaltbild, der die technische (hardwarenahe) Verknüpfung der sicherheitsbezogenen Teile der Steuerung zeigt
Sicherheitsbezogenes Blockdiagramm	Darstellung der logischen Verknüpfung der Bauteile, aus der die Subsysteme mit Funktions- und Testkanälen ersichtlich sind
Bauteile	Sicherheitsrelevante Hardwareeinheiten, Teile der Steuerung
Subsystem (SB)	Größte Einheit von Bauteilen, die die Sicherheitsfunktion ganz oder abschnittsweise ausführt. Ein Subsystem besitzt eine durchgängige Struktur und wird durch eine Kategorie beschrieben.
Gekapseltes Subsystem	Sicherheitsbauteil, für das der Hersteller bereits PL, PFH_D und Kategorie angibt. Die interne Struktur muss daher nicht weiter berücksichtigt werden.
Funktionskanal	Hardwareeinheiten in Serienschaltung, Kette von Bauteilen, die vom Sensor bis zum Aktor die gesamte Sicherheitsfunktion ausführen. In redundanten Subsystemen gibt es (mindestens) zwei unabhängige Funktionskanäle.
Signalpfad	Entlang eines Signalpfades wird die Anforderung der Sicherheitsfunktion vom Sensor zum Aktor weitergereicht und führt dort z. B. zur Abschaltung.
Redundanter Funktionsblock	Hardwareeinheit in Parallelschaltung, Bauteil in einem Abschnitt eines redundanten Funktionskanals, Teil eines Funktionskanals in Subsystemen der Kategorie 3 oder 4
Nicht redundanter Funktionsblock	Bauteil in einem Abschnitt eines nicht redundanten Funktionskanals, Teil eines Funktionskanals in Subsystemen der Kategorien B, 1 oder 2
Testkanal	Kette von Bauteilen, die ein Abschaltsignal „Testung“ übermittelt (nicht zu verwechseln mit der Schnittstelle, auf der Testsignale zwischen dem testenden und dem zu testenden Block ausgetauscht werden, um einen gefährlichen Ausfall zu erkennen)
Abschaltsignal Testung	Übermittelt das Ergebnis eines Tests, der einen gefährlichen Ausfall eines Funktionsblocks erkannt hat, von einem Testblock an einen „weiter hinten liegenden“ Funktionsblock oder zusätzlichen Abschaltblock, sodass die Sicherheitsfunktion erfolgreich abgeschlossen wird oder ein sicherer Zustand eingeleitet wird
Testblock	Hardwareeinheit zur Diagnose: Bauteil, das einen oder mehrere Funktionsblöcke testet und ein Abschaltsignal „Testung“ generiert, wenn es dort einen gefährlichen Ausfall erkannt hat, oder übermittelnder oder abschaltender Block im Testkanal
Ruhestromprinzip	Entwurfsprinzip für sichere Steuerungen, bei dem der energielose Zustand, z. B. bei Leitungsunterbrechungen, zum sicheren Zustand führt.

Anhang B: Abkürzungen aus DIN EN ISO 13849-1

Abkürzung	Erklärung	Einheit	englische (deutsche) Bezeichnung
SRP/CS	Sicherheitsbezogenes Steuerungsteil	-	**S**afety-**R**elated **P**art of a **C**ontrol **S**ystem (Sicherheitsbezogenes Teil einer Steuerung)
$MTTF_D$	Bauteilgüte	Jahr, a	**M**ean **T**ime **T**o **d**angerous **F**ailure (Mittlere Zeit bis zum gefahrbringenden Ausfall)
DC	Testgüte (Block, Element)	%	**D**iagnostic **C**overage (Diagnosedeckungsgrad)
DC_{avg}	Testgüte (Subsystem)	%	**Av**era**g**e **D**iagnostic **C**overage (Durchschnittlicher Diagnosedeckungsgrad)
CCF	Gemeinsamer Ausfall von redundanten Kanälen	-	**C**ommon **C**ause **F**ailure (Ausfall infolge gemeinsamer Ursache)
PFH_D	Ausfall-wahrscheinlichkeit	1/h	**P**robability of a dangerous **F**ailure per **H**our (Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde)
PL	Istwert der Funktionalen Sicherheit	-	**P**erformance **L**evel (Performance Level, es gibt keine deutsche Übersetzung)
PL_r	Sollwert der Funktionalen Sicherheit	-	**R**equired **P**erformance **L**evel (Erforderlicher Performance Level)
Cat.	Kategorie	-	**Cat**egory (Kategorie)
T_M	Gebrauchsdauer	Jahr, a	**M**ission **T**ime (Gebrauchsdauer)
B_{10D}	Bauteilgüte (bei Verschleiß)	Zyklen	Number of cycles until **10**% of the components fail **d**angerously (Mittlere Anzahl von Zyklen bis 10 % der Bauteile gefährlich ausfallen)
T_{10D}	Zulässige Betriebszeit (bei Verschleiß)	Jahr, a	Mean **T**ime until **10**% of the components fail **d**angerously (Mittlere Zeit, bis 10 % der Bauteile gefährlich ausfallen)
n_{op}	Schalthäufigkeit	Zyklen/a	**n**umber of **op**erations (Mittlere Anzahl jährlicher Betätigungen)
RDF	Anteil der gefährlichen Ausfälle an der Gesamtheit der Ausfälle	-	**R**atio of **D**angerous **F**ailure (Anteil der gefährlichen Ausfälle)