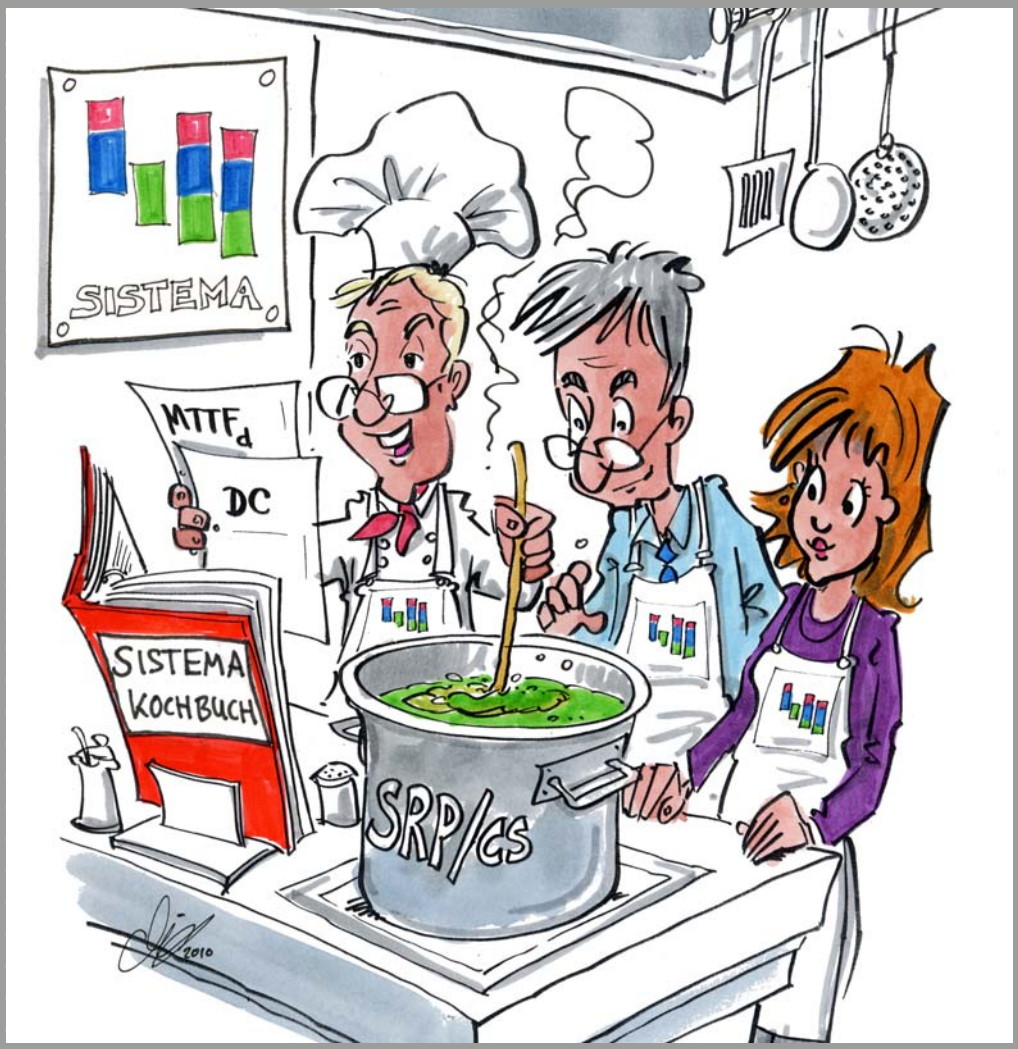
IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Das SISTEMA-Kochbuch 1

Vom Schaltbild zum Performance Level – Quantifizierung von Sicherheitsfunktionen mit SISTEMA

Version 1.0 (DE)



Verfasser: Ralf Apfeld, Michael Hauke, Michael Schaefer, Paul Rempel, Björn Ostermann
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: 02241/231-02
Telefax: 02241/231-2234
Internet: www.dguv.de/ifa

– Oktober 2010 –

Inhaltsverzeichnis

1 Einleitung

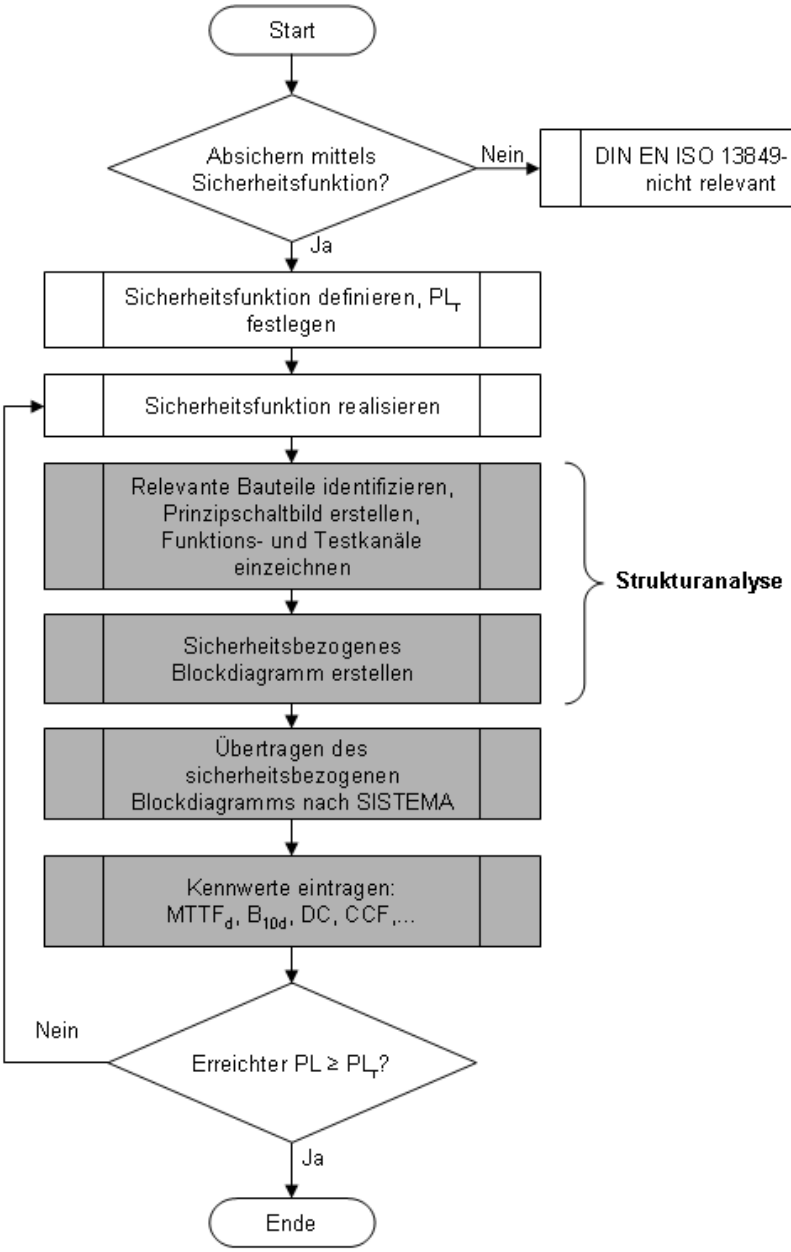
Steuerungen, die Sicherheitsfunktionen ausführen, werden eingesetzt, um Maschinen sicher zu gestalten und damit die Anforderungen der Maschinenrichtlinie 2006/42/EG zu erfüllen. Dazu definiert man bei der Risikobeurteilung während der Konstruktion der Maschine die zur Risikominderung erforderlichen Sicherheitsfunktionen und realisiert sie anschließend durch eine geeignete Steuerung. Die sicherheitsbezogenen Teile von Maschinensteuerungen können nach DIN EN ISO 13849-1 ausgeführt werden. Sie verlangt vom Maschinenkonstrukteur u. a. eine Berechnung für die Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (**PFH**), um den Performance Level (**PL**) zu bestimmen. Dieser hängt neben den systematischen Anforderungen auch von der Struktur der Steuerung (Kategorie) ab.

Als Hilfe stellt das IFA das Software-Tool SISTEMA (**Si**cherheit von **Ste**uerungen an **Ma**schinen) kostenlos zur Verfügung, das im Internet heruntergeladen werden kann unter www.dguv.de/ifa, Webcode d11223.

Bevor er mit den Berechnungen beginnen kann, muss der Maschinenkonstrukteur 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.

Das SISTEMA-Kochbuch behandelt diesen ungewohnten und schwierigen Schritt der Abstraktion (Abbildung 1) sowie den Folgeschritt, das Übertragen der Blöcke in SISTEMA und das Eintragen ihrer Kennwerte.

Abbildung 1:
Ablaufdiagramm von der Sicherheitsfunktion zum Performance Level; die vier grau unterlegten Schritte werden in dieser Anleitung ausführlich beschrieben



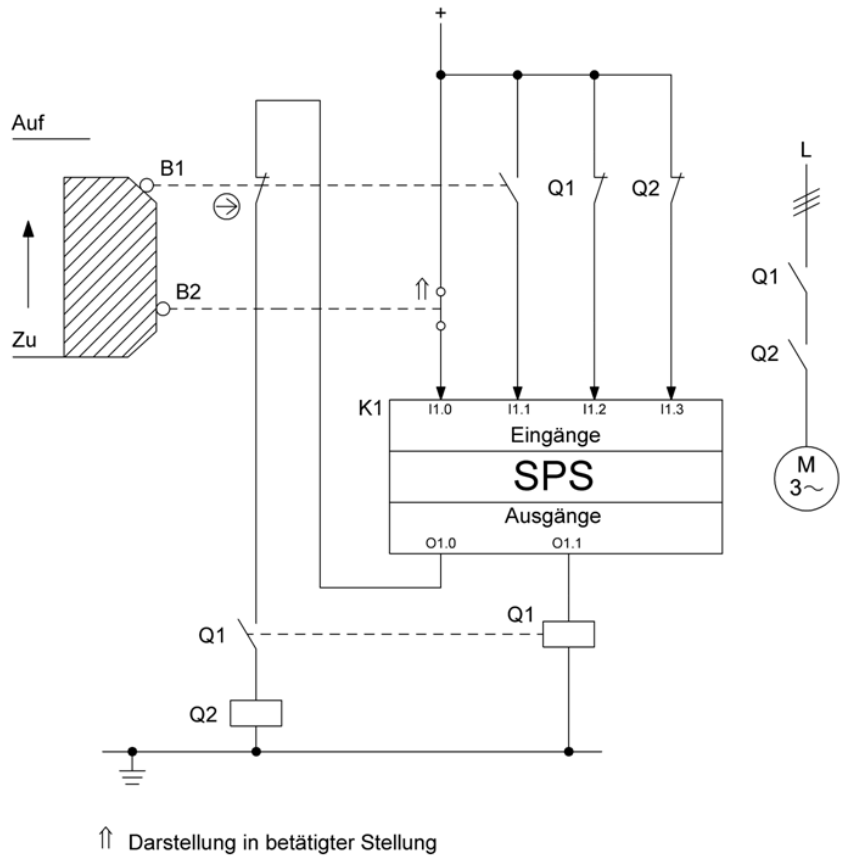
2 Prinzipschaltbild mit Funktions- und Testkanälen

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 (s. BGIA-Report 2/2008, Kapitel 5) ist daher unabdingbar für die nächsten Schritte. 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 und einen sicheren Zustand einleiten. Ein Prinzipschaltbild zeigt z. B. die elektrische Verschaltung von Positionsschaltern, Speicherprogrammierbaren Steuerungen (SPS) und Schützen und den Verlauf des Stromflusses vom Sensor über die Signalverarbeitung bis zum Aktor.

Im Beispiel 1 (Abbildung 2) 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.

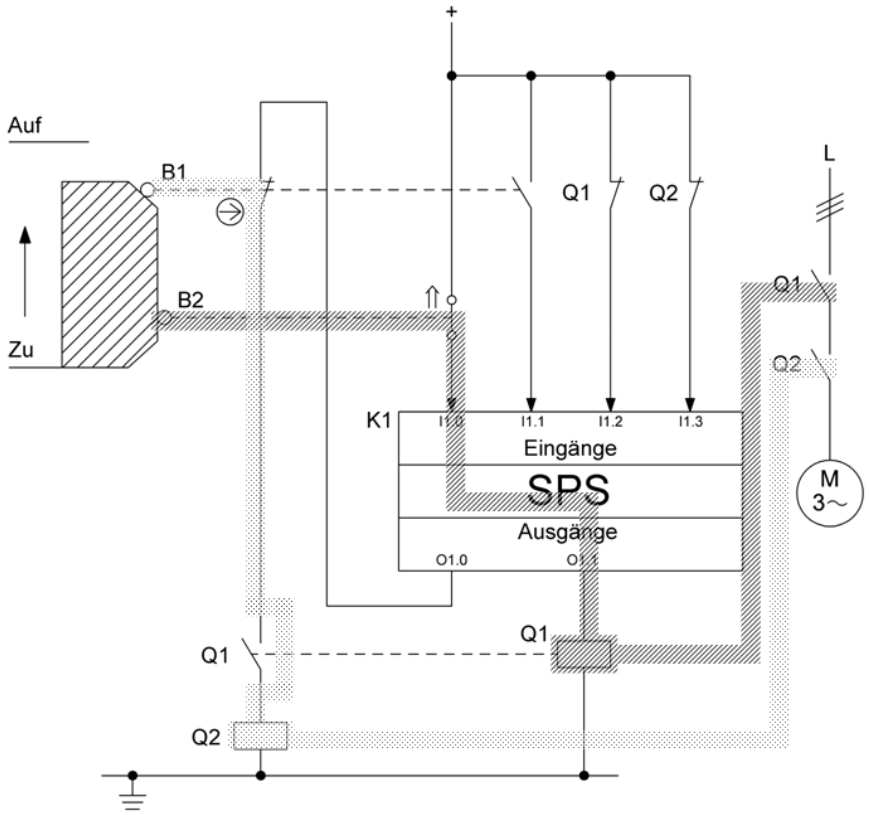
Abbildung 2:
Prinzipschaltbild mit relevanten Bauteilen (Beispiel 1); s. BGIA-Report 2/2008, Kapitel 8.2.18



2.2 Funktions- und Testkanäle einzeichnen

Im Prinzipschaltbild werden zunächst die Funktionskanäle markiert. Dabei hat es sich in der Praxis als hilfreich erwiesen, „rückwärts“ vorzugehen, also beginnend an der Aktorseite den Kanal bis zum Sensor zu verfolgen. Man erhält damit die Signalpfade vom auslösenden Ereignis zur Reaktion der Sicherheitsfunktion (Abbildung 3).

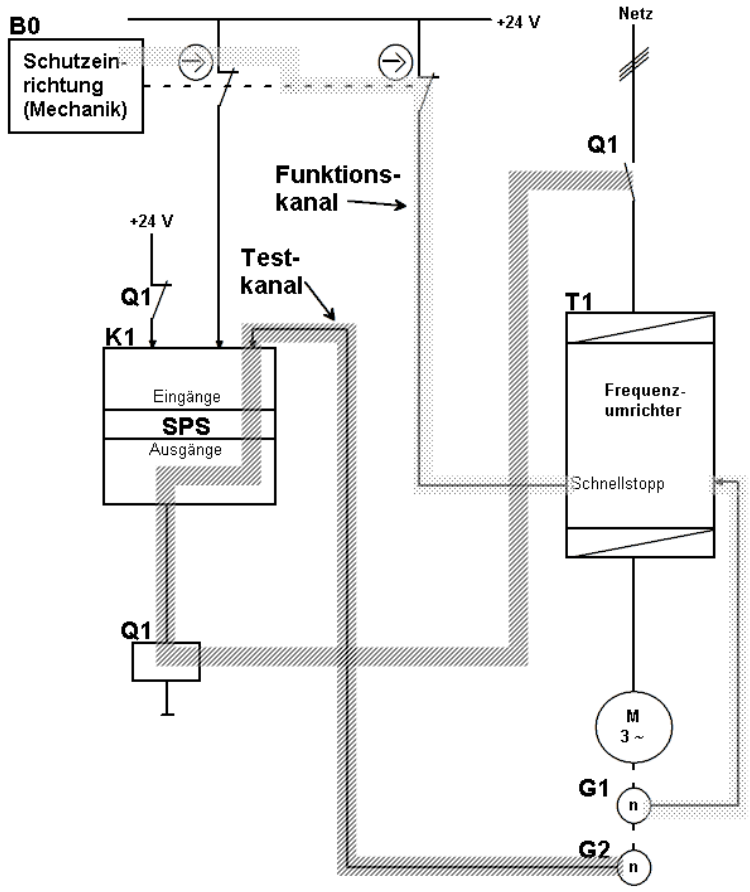
Abbildung 3:
Prinzipschaltbild mit zwei redundanten Funktionskanälen B1-Q2 und B2-K1-Q1 (Beispiel 1)



⇑ Darstellung in betätigter Stellung

Falls in Schaltungen ein Testkanal mit eigenständiger Abschalteinrichtung verwendet wird (Kategorie 2), wird im Prinzipschaltbild auch dieser Testkanal markiert. Abbildung 4 zeigt das Beispiel einer Schutzeinrichtung an einer Walzeneinzugsstelle, deren Auslösung das Stillsetzen des Motors innerhalb 1/3 Umdrehung bewirkt. Hierbei wird der bis zum Stillsetzen benötigte Drehwinkel des Motors regelmäßig durch manuelle Betätigung der Schutzeinrichtung getestet.

Abbildung 4:
Beispiel 2 mit markiertem Funktionskanal B0 – T1 – G1 und Testkanal mit eigenständiger Abschalteinrichtung G2 – K1 – Q1



Im Kapitel 3 wird erläutert, wie ein Prinzipschaltbild in ein sicherheitsbezogenes Blockdiagramm überführt wird.

3 Vom Prinzipschaltbild zum sicherheitsbezogenen Blockdiagramm

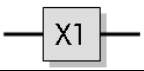
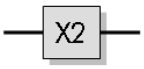
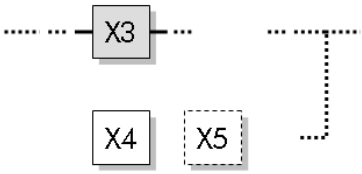
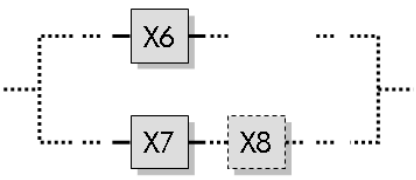
Als nächster Schritt erfolgt für jede Sicherheitsfunktion eine Transformation in die logische Darstellung des sicherheitsbezogenen Blockdiagramms. Durch die Transformation werden die Bauteile des Prinzipschaltbilds sogenannten Subsystemen zugeordnet, mit denen in SISTEMA die Sicherheitsfunktion abgebildet wird.

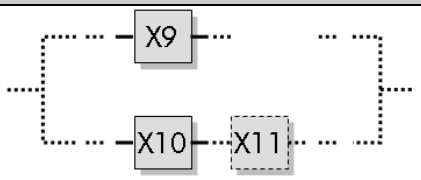
Bei der Darstellung als sicherheitsbezogenes Blockdiagramm sind nicht mehr die physikalischen Verbindungen der Bauteile relevant, sondern die logischen Zusammenhänge. Jedes Bauteil in einer Sicherheitsfunktion ist Bestandteil einer bestimmten Struktur. Diese Struktur wird in DIN EN ISO 13849-1 als Kategorie bezeichnet und in SISTEMA als Subsystem zusammengefasst. Die Aneinanderreihung der Subsysteme mit ihrer jeweiligen Kategorie stellt eine Sicherheitsfunktion als sicherheitsbezogenes Blockdiagramm dar. Die Reihenfolge der Subsysteme ist für die spätere Berechnung der Ausfallwahrscheinlichkeit beliebig.

3.1 Kategorien nach DIN EN ISO 13849-1

Die Kategorien nach DIN EN ISO 13849-1, ihre charakterisierenden Merkmale und typische Darstellung zeigt Tabelle 1.

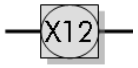
Tabelle 1: Merkmale und Darstellung der Kategorien

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 (X3) werden durch Fehleraufdeckung im Testkanal (X4, X5) erkannt, sicherer Zustand wird eingeleitet) Anmerkung: Der Funktions- und Testkanal kann über ein oder mehrere Bauteil(e) verfügen.	
Zweikanalig, mit Fehlererkennung	Kategorie 3 (Einfehlersicherheit durch Redundanz, Testung) Anmerkung: Jeder Kanal kann über ein oder mehrere Bauteil(e) verfügen.	

Struktur	Kategorie nach DIN EN ISO 13849-1 und besondere Merkmale	Typische Darstellung im sicherheitsbezogenen Blockdiagramm
Zweikanalig, mit Fehlererkennung	Kategorie 4 (wie Kategorie 3, zusätzlich robust gegen Anhäufung von zwei unerkannten Fehlern) Anmerkung: Jeder Kanal kann über ein oder mehrere Bauteil(e) verfügen.	

Eine Besonderheit stellen gekapselte Subsysteme dar. Das sind Bauteile, für die der Hersteller bereits PL, PFH und Kategorie angibt (z. B. Sicherheits-SPS, Sicherheitsbaustein), siehe Tabelle 2.

Tabelle 2: Gekapselte Subsysteme

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

Anmerkung: Alle anderen Bauteilanordnungen entsprechen nicht den vorgesehenen Architekturen der DIN EN ISO 13849-1, eine Berechnung mit SISTEMA ist nicht möglich.

3.2 Strukturanalyse und Erläuterungen

In der Strukturanalyse überträgt man die Bauteile aus dem Prinzipschaltbild in ein sicherheitsbezogenes Blockdiagramm und bestimmt die Kategorie anhand der Merkmale 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 bestehen auch quantitative Anforderungen an die Kategorien, deren Einhaltung von SISTEMA kontrolliert wird.

Das hier beschriebene Verfahren ist zugeschnitten auf die Anwendung der DIN EN ISO 13849-1 mit ihren „Vorgesehenen Architekturen“ für die Kategorien. 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 müssen andere Methoden zum Nachweis der Ausfallwahrscheinlichkeit herangezogen werden, z. B. eine Markov-Modellierung wie in DIN EN 61508-6, Anhang B, beschrieben.

Ablauf der Strukturanalyse:

Basis für die Strukturanalyse ist das Prinzipschaltbild mit den markierten Funktions- und Testkanälen. Der Ablauf ist schematisch in Anhang E dargestellt. Abbildung 5 enthält denselben Ablauf, ergänzt um die Anwendung auf die Beispiele 1 und 2 aus Kapitel 2.

Schritt 1: Bauteile eines Funktionskanals aneinanderreihen

Alle Bauteile entlang des ersten Funktionskanals (derjenige mit der geringsten Anzahl von Bauteilen) werden als Blöcke von links nach rechts (vom Sensor zum Aktor) aufgeschrieben.

Schritt 2: Ersten Block betrachten

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

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

Ein gekapseltes Subsystem ist daran zu erkennen, dass es vom Hersteller bereits durch PL (oder SIL nach IEC-Normen), PFH und eine Kategorie (innere Struktur) charakterisiert ist. Eine weitere Zerlegung der inneren Struktur des gekapselten Subsystems ist nicht erforderlich.

Anmerkung: Befindet sich ein gekapseltes Subsystem der Kategorien 3 oder 4 in beiden redundanten Funktionskanälen, verlaufen beide Funktionskanäle über dieses Subsystem.

Schritt 4: Können alle Bauteilfehler ausgeschlossen werden?

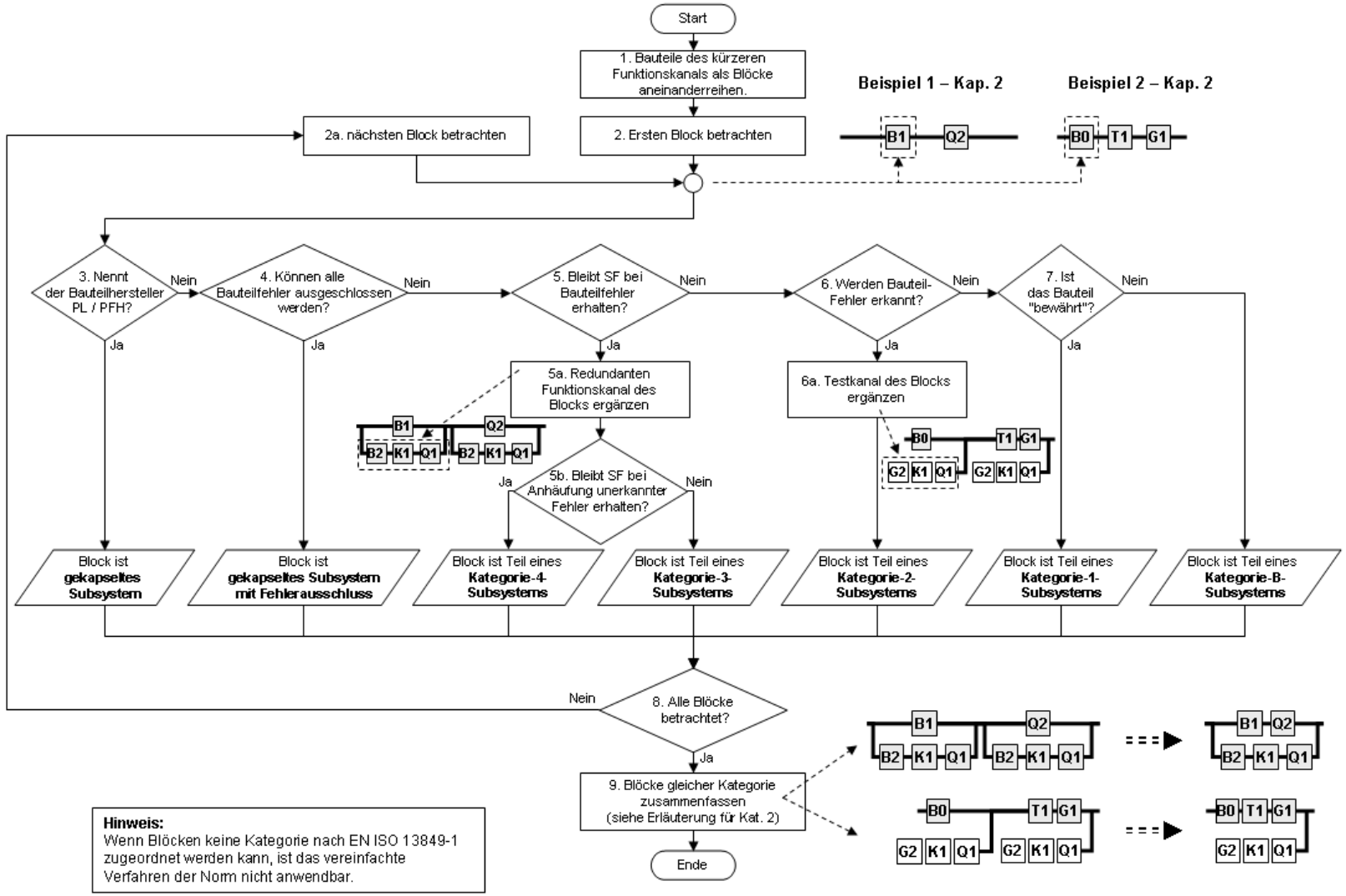
Für das Bauteil in dem betrachteten Block werden nacheinander alle anzunehmenden Fehler betrachtet. DIN EN ISO 13849-2 enthält hierzu im Anhang die Fehlermodelle einer Reihe von Bauteilen, die in Maschinensteuerungen verwendet werden. Begründete Fehlerausschlüsse führen dazu, dass bestimmte Bauteilfehler 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 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, weitere Eingaben sind nicht erforderlich).

Schritt 5: Bleibt Sicherheitsfunktion bei Bauteilfehler erhalten?

In Schritt 4 sind die für das Bauteil im betrachteten Block anzunehmenden gefährlichen Fehler bestimmt worden. Jetzt geht es um deren Auswirkungen auf die Sicherheitsfunktion.

Abbildung 5: Ablaufdiagramm der Strukturanalyse mit den Beispielen aus Kapitel 2, SF=Sicherheitsfunktion



Schritt 5a: Redundanten Funktionskanal des Blocks/der Blöcke ergänzen

Falls im Fehlerfall des betrachteten Blocks die Sicherheitsfunktion von einem oder mehreren redundanten Bauteilen aufrechterhalten wird (es gibt also einen zweiten Funktionskanal), werden diese Bauteile als Blöcke in einem zweiten Funktionskanal dargestellt (siehe Beispiel in Tabelle 1: Kategorien 3 und 4).

In Beispiel 1 (Abbildung 3) trifft dies sowohl auf B1 als auch auf Q2 zu. Beiden Blöcken wird daher der redundante Funktionskanal B2-K1-Q1 hinzugefügt.

Anmerkung: Die Bauteile des redundanten Funktionskanals werden damit mehrfach verwendet. Dies ist der schrittweisen Vorgehensweise geschuldet und soll zunächst nicht weiter stören. In Schritt 8 werden mehrfach vorhandene Blöcke wieder zusammengefasst.

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).

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 Sicherheitsfunktion bei Anhäufung unerkannter Fehler erhalten?

Für den betrachteten Block mit seinem redundanten Funktionskanal wurde bis hierhin die Einfehlersicherheit festgestellt, Kategorie 3 ist erfüllt. Werden auch die Anforderungen an 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 beim zweiten unerkannten Fehler nicht erhalten, so liegt ein Kategorie-3-Subsystem vor.

In Beispiel 1 (Abbildung 3) könnte die SPS K1 im Fehlerfall die Ausgänge O1.0 und O1.1 ständig ansteuern. Damit ist Q1 ständig angezogen. Selbst wenn die SPS diesen Fehler durch Rücklesen der Überwachungskontakte noch aufdecken könnte, wäre sie nicht in der Lage, den sicheren Zustand herzustellen. Wenn dann durch einen zweiten Fehler die Kontakte von Q2 verschweißen, läuft der Motor auch bei geöffneter Schutzeinrichtung weiter, die Sicherheitsfunktion ist ausgefallen, Kategorie 4 ist nicht erfüllt.

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 zwei unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen.

Schritt 6: Werden Bauteilfehler erkannt?

An diesem Punkt ist klar, dass keine Redundanz vorhanden ist, also weder Kategorie 3 noch Kategorie 4 vorliegt. Falls der Ausfall des Blocks von einem Testkanal erkannt und der sichere Zustand eingeleitet wird, handelt es sich um ein Kategorie-2-Subsystem.

In Beispiel 2 (Abbildung 4) erfolgt bei Auslösung von B0 ein gesteuertes Stillsetzen des Motors durch T1/G1 innerhalb 1/3 Umdrehung. Die Testung erfolgt nach Aufforderung durch K1 über eine manuelle Betätigung von B0 und eine Messung des Stillsetzwinkels durch K1/G2. Im Fehlerfall wird der sichere Zustand über Q1 hergestellt. Durch die Testung werden Fehler in B0 und T1/G1 aufgedeckt. Der Testkanal G2-K1-Q1 erkennt also Fehler in B0 und T1/G1 und stellt den sicheren Zustand her, es liegt daher Kategorie 2 vor.

Anmerkung: Angemessene Fehlererkennung wird auch für Kategorie 3 und 4 gefordert. Kategorie-2-Subsystemen fehlt jedoch ein redundanter Funktionskanal.

Schritt 6a: Testkanal des Blocks ergänzen

Die Bauteile des Testkanals, die den Ausfall des Blocks feststellen und den sicheren Zustand einleiten, werden entsprechend Tabelle 1 (Kategorie 2) als Testblöcke im sicherheitsbezogenen Blockdiagramm dargestellt.

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 (s. BGIA-Report 2/2008, Abschnitt 6.25), die jedoch bei der Strukturanalyse keine Rolle spielt.

Schritt 7: Ist das Bauteil „bewährt"?

Redundanz oder Testung konnten im Beispiel 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 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 um einen Teil eines Kategorie-B-Subsystems.

Schritt 8: Alle Blöcke betrachtet?

Sofern nach der Zuordnung des Blocks in ein Subsystem noch nicht alle Blöcke betrachtet sind, wird das Diagramm mit dem nächsten Block ab Schritt 2a erneut durchlaufen. Andernfalls geht es weiter mit Schritt 9.

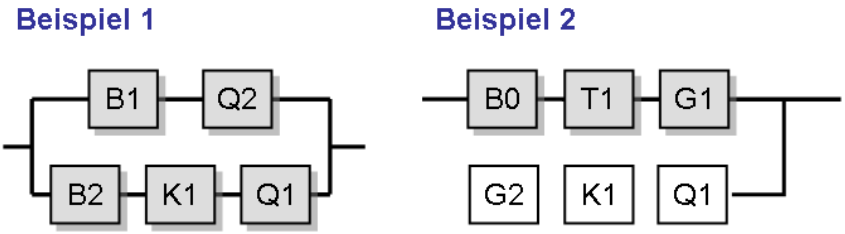
Schritt 9: Blöcke gleicher Kategorie zusammenfassen

Subsysteme derselben Kategorie können vereinigt werden, indem die Bauteile gleicher Kanäle zusammengefasst werden (s. BGIA-Report 2/2008, Abbildung 6.14). Jedes Bauteil kommt innerhalb eines Kanals nur genau einmal vor, Dubletten können entfernt werden. Selbstverständlich darf dasselbe Bauteil auch nicht gleichzeitig in zwei redundanten Funktionskanälen verwendet werden. Bei Kategorie 2 können nur die Bauteile in einem Funktionskanal zusammengefasst werden, die über denselben Testkanal verfügen.

Da SISTEMA innerhalb der Subsysteme $MTTF_d$-Werte jedes Kanals begrenzt (Kappung), kann sich durch die Zusammenfassung rechnerisch eine geringere Wahrscheinlichkeit für einen gefährlichen Ausfall pro Stunde ergeben. Die kleinere Ausfallwahrscheinlichkeit (PFH) ist ein Vorteil. Nachteilig ist jedoch, dass durch die zusammengefasste Darstellung die logische Abfolge der Signalverarbeitung oft schwerer zu erkennen ist.

Für die Beispiele aus Kapitel 2 ergeben sich die sicherheitsbezogenen Blockdiagramme in Abbildung 5a:

Abbildung 5a: Ergebnis der Strukturanalyse für die Beispiele aus Kapitel 2



Mit dem sicherheitsbezogenen Blockdiagramm liegt nun die logische Darstellung der Sicherheitsfunktion vor. Im nächsten Kapitel erfolgt die Berechnung der Ausfallwahrscheinlichkeit (**PFH**) mithilfe von SISTEMA.

4 Übertragung nach SISTEMA

Das Software-Tool SISTEMA verwendet mehrere Hierarchieebenen (Abbildung 6). Die einzelnen Ebenen erklärt Tabelle 3.

Abbildung 6: Hierarchieebenen in SISTEMA

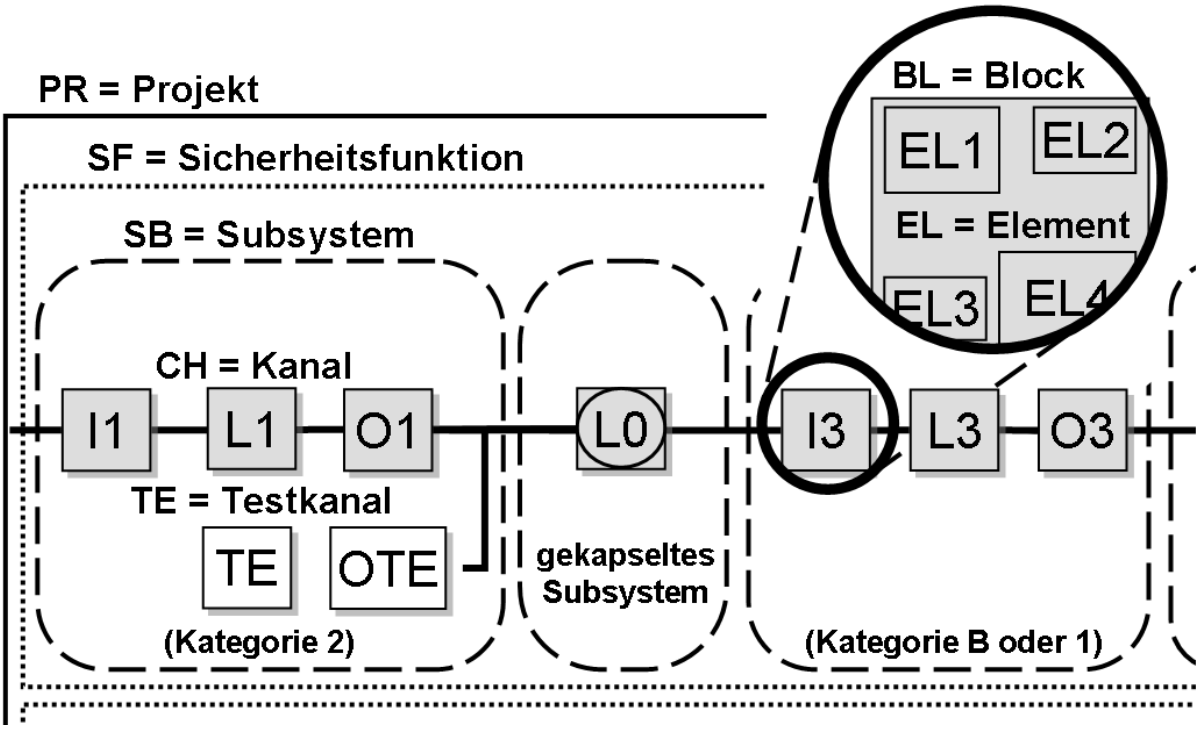
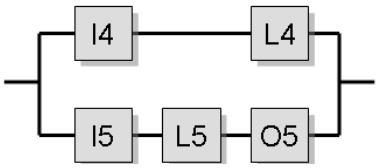
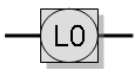
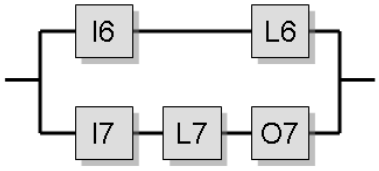
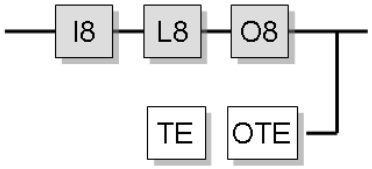
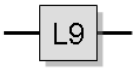


Tabelle 3: Beschreibung der Hierarchieebenen in SISTEMA

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 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
Element	Ein Block beinhaltet ein oder mehrere Elemente. Nur für Elemente kann ein B_{10d}-Wert (siehe Anhang B) eingegeben werden.	Schütze, Positionsschalter, elektromechanische Bauteile, alle Bauteile mit einem B_{10d}-Herstellerwert

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 7). Nach dem Anlegen eines neuen Projektes mit „Neu“ (1.) kann im Maskenfeld „Projektname“ (3.) eine Bezeichnung eingegeben werden, die dann auch im Navigationsfenster hinter dem Kürzel **PR** erscheint (2.).

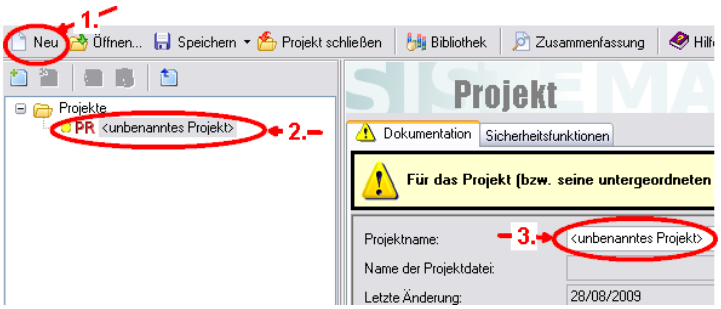


Abbildung 7

4.2 Sicherheitsfunktionen anlegen

In der Registerkarte „Sicherheitsfunktion“ (2.) werden durch „Neu“ (3.) die erforderlichen Sicherheitsfunktionen angelegt (Abbildung 8). Der „Name der Sicherheitsfunktion“ erscheint auch im Navigationsfenster hinter dem Kürzel **SF** (siehe Abbildung 9; 1.).

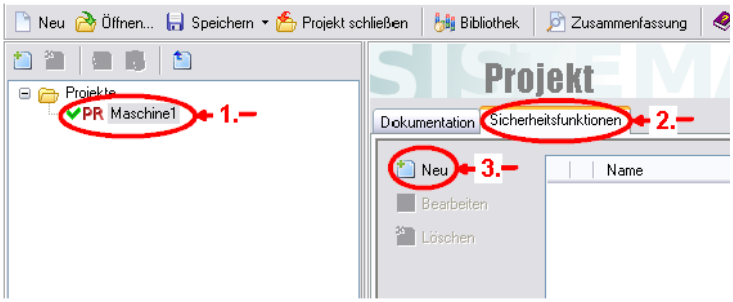


Abbildung 8

4.3 PL_r festlegen

Der erforderliche Performance Level PL_r wird individuell für jede Sicherheitsfunktion (1.) festgelegt (Abbildung 9). Dazu benutzt man unter „Sicherheitsfunktion – PLr“ (2.) den Risikografen (3.) oder gibt den PL_r direkt ein, z. B. wenn eine Vorgabe durch eine maschinenspezifische Norm vorliegt.

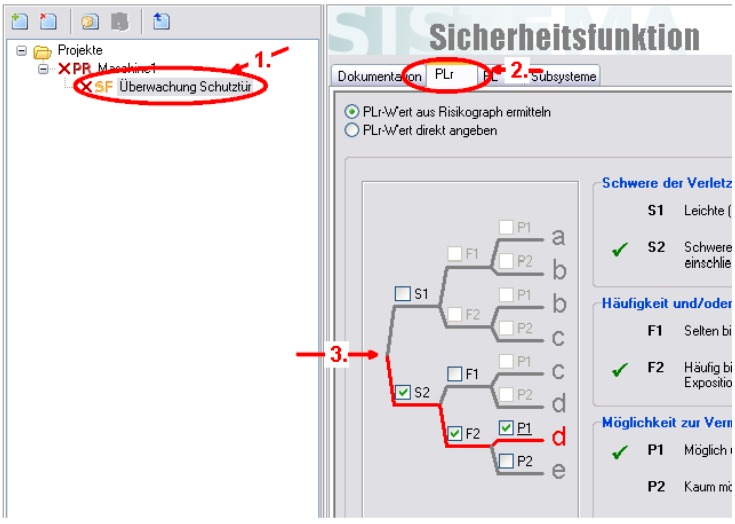


Abbildung 9

4.4 Subsysteme hinzufügen

Die im sicherheitsbezogenem Blockdiagramm ermittelten Subsysteme werden angelegt. Ein Subsystem wird unter der Sicherheitsfunktion (1.) in der Registerkarte „Subsysteme“ (2.) durch „Neu“ (3.) hinzugefügt (Abbildung 10).

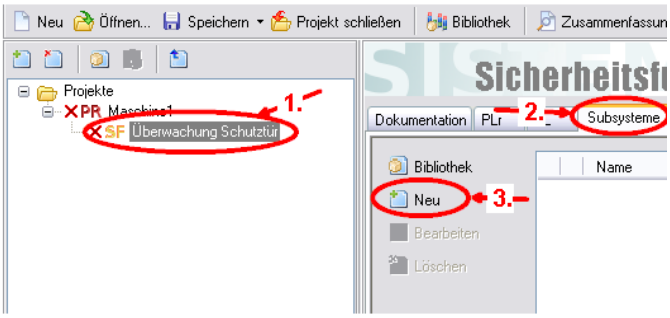


Abbildung 10

4.5 Gekapselte Subsysteme

Für gekapselte Subsysteme liegen Herstellerangaben zu PL, PFH und Kategorie vor. Die Eingabe (4.) erfolgt direkt unter dem Subsystem (1.) in der Registerkarte „PL“ (2.) nach Auswahl von „PL bzw. PFH-Wert direkt angeben“ (3.) (Abbildung 11). Die Kategorie kann in der nächsten Registerkarte „Kategorie“ eingegeben werden. Da PL und PFH für dieses Subsystem vorliegen, ist die Kategorieangabe für die Berechnung der PFH der gesamten Sicherheitsfunktion nicht erforderlich.

Anmerkung: Falls das Häkchen gesetzt ist (4.), erfolgt eine wechselseitige Berechnung von PL und PFH mit Mittelwerten.

Fehlerausschluss:

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

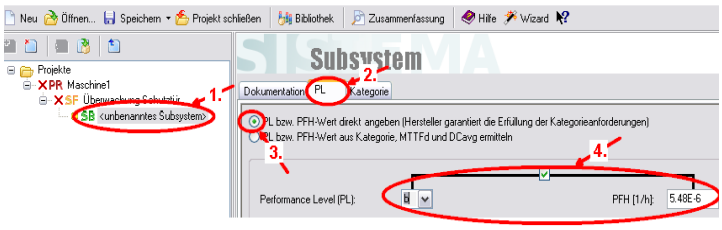


Abbildung 11

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

Im Subsystem (1.) erfolgt unter „PL“ (2.) die Auswahl von „PL bzw. PFH aus Kategorie, $MTTF_d$ und DC_{avg} ermitteln“ (3.) (Abbildung 12).

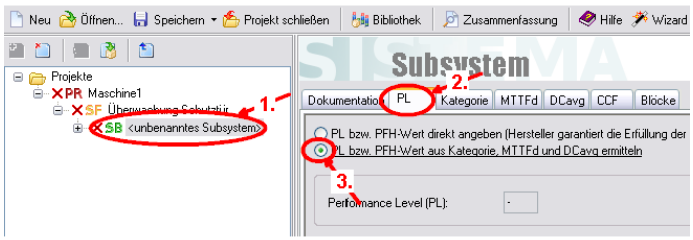


Abbildung 12

Danach werden:

a) im Subsystem (1.) unter „Kategorie“ (2.) (Abbildung 13) die jeweilige Kategorie ausgewählt und die „Anforderungen der Kategorie“ beurteilt.

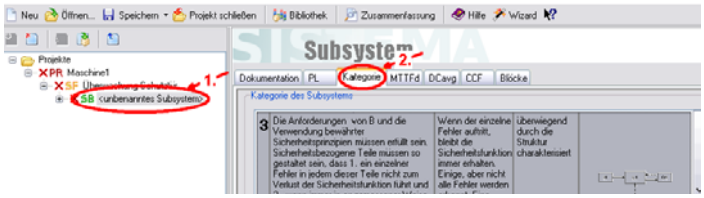


Abbildung 13

b) im Subsystem (1.) unter „$MTTF_d$“ (2.) der $MTTF_d$-Wert direkt angegeben oder die Auswahl „$MTTF_d$-Wert aus Blöcken ermitteln“ getroffen (3.) (Abbildung 14).

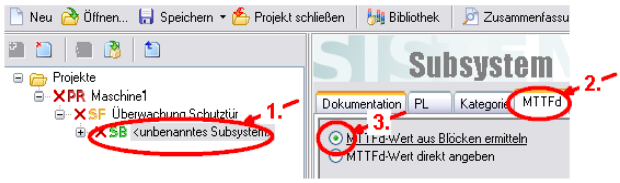


Abbildung 14

c) im Subsystem (1.) unter „DC_{avg}“ (2.) der DC_{avg}-Wert direkt angegeben oder die Auswahl „DC_{avg}-Wert aus Blöcken ermitteln“ getroffen (3.) (Abbildung 15).

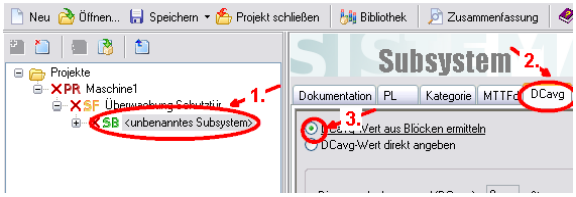


Abbildung 15

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 16). Es müssen mindestens 65 Punkte erreicht werden. Die erreichte Punktzahl kann direkt eingegeben oder über eine Maßnahmen-Bibliothek zusammengestellt werden (3. und 4.).

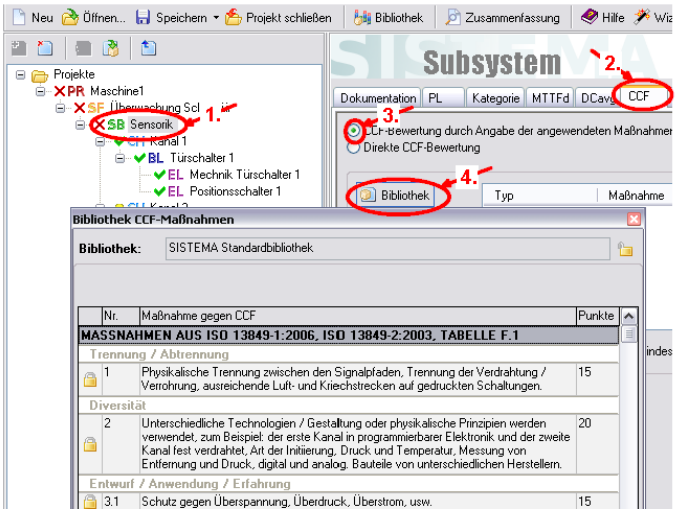


Abbildung 16

4.6.1 Blöcke eingeben

Nachdem die Subsysteme gebildet wurden, ist eine weitere Spezifizierung vorzunehmen (Ausnahme: 4.5 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. Falls eine weitere Gliederung der Blöcke nicht erforderlich ist, kann direkt mit Schritt 4.6.3 fortgefahren werden. Falls eine weitere Gliederung eines Blocks in Elemente erfolgen soll (immer erforderlich bei Bauteilen mit Angabe von B_{10d}), sind folgende Einstellungen erforderlich:

a) im Block (1.) unter „$MTTF_d$“ (2.) die Auswahl „$MTTF_d$-Wert aus Elementen ermitteln“ (3.) (Abbildung 17) treffen.

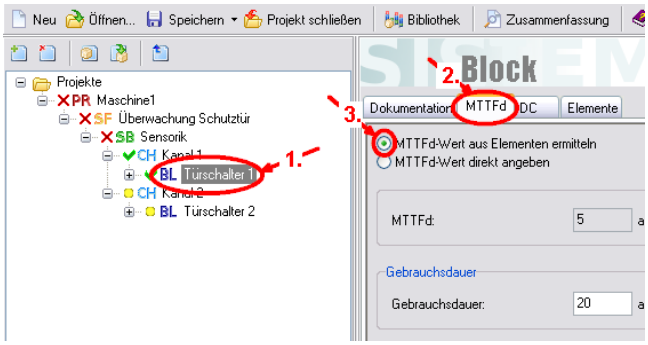


Abbildung 17

b) im Block (1.) unter „DC“ (2.) die Auswahl „DC-Wert aus Elementen ermitteln“ (3.) (Abbildung 18) treffen.

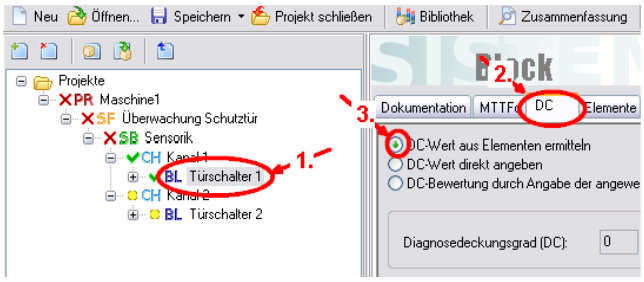


Abbildung 18

4.6.2 Elemente eingeben

Falls ein Block in Elemente **EL** unterteilt werden soll, sind im Block (1.) unter „Elemente“ (2.) durch „Neu“ (3.) Elemente anzulegen (Abbildung 19).

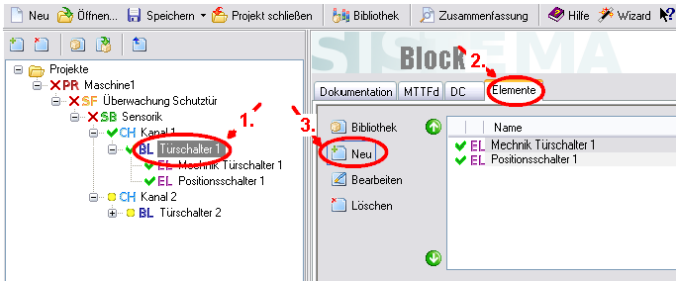


Abbildung 19

Auf Elementebene (1.) muss z. B. zur Ermittlung der $MTTF_d$ (2.) von elektromechanischen und pneumatischen Komponenten eine Berechnung unter Berücksichtigung des B_{10d}-Wertes und der Anzahl der Betätigungen n_{op} erfolgen (Abbildung 20). Man wählt „$MTTF_d$-Wert über B_{10d}-Wert ermitteln“ (3.) und „n_{op} berechnen“ (4.), um die erforderlichen Werte einzugeben (5.).

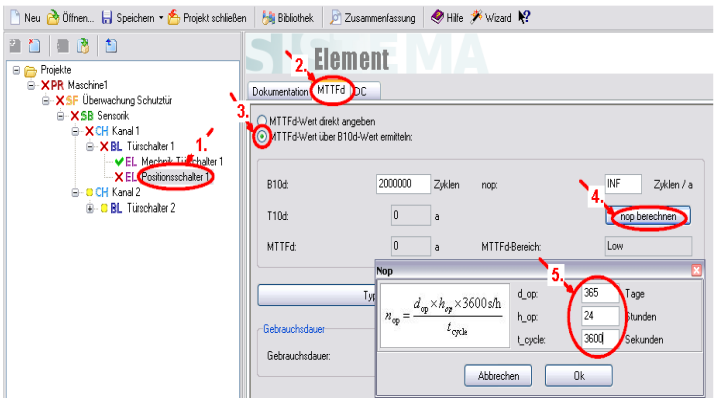


Abbildung 20

4.6.3 Sicherheitsrelevante Daten eingeben

Zu den für die Berechnung der PFH erforderlichen sicherheitsrelevanten Daten gehören die jeweilige Bauteilgüte ($MTTF_d$, B_{10d}), die Anzahl der Betätigungen von elektromechanischen und pneumatischen Bauteilen (n_{op}) und der Diagnosedeckungsgrad (DC).

4.6.3.1 $MTTF_d/B_{10d}$

Die Eingabe erfolgt auf Block- bzw. Elementebene (1.) in der Registerkarte „$MTTF_d$“ (2.) (Abbildung 21).

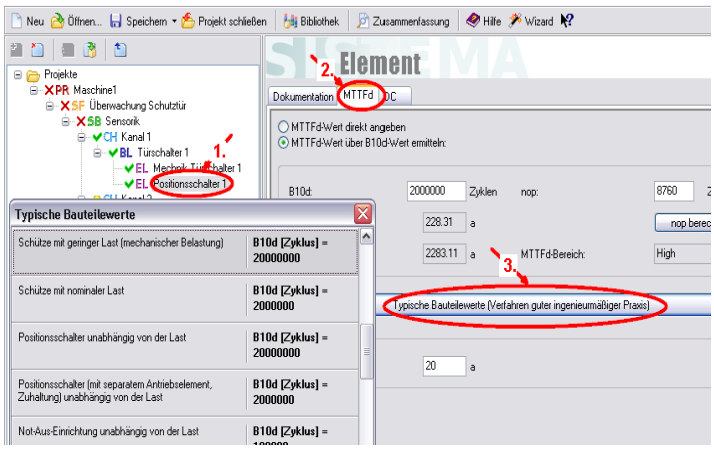


Abbildung 21

Die sicherheitsrelevanten Parameter der Bauteile können ermittelt werden:

a) aus Herstellerangaben,
b) aus etablierten Datensammlungen (Quellen siehe DIN EN ISO 13849-1, Anhang D) oder
c) aus DIN EN ISO 13849-1, Anhang C; hinterlegt in SISTEMA unter „Typische Bauteilwerte“ (3.).

Wenn alle gefährlichen Bauteilfehler ausgeschlossen werden können, kann bei Anwahl von „MTTFd direkt eingeben“ auch ein Fehlerausschluss gewählt werden.

4.6.3.2 DC

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. Bei Auswahl von „DC-Bewertung durch Angabe der angewendeten Maßnahme“ kann über „Bibliothek“ (3.) 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 man innerhalb dieser Spanne einen konkreten Wert auswählen (Abbildung 22).

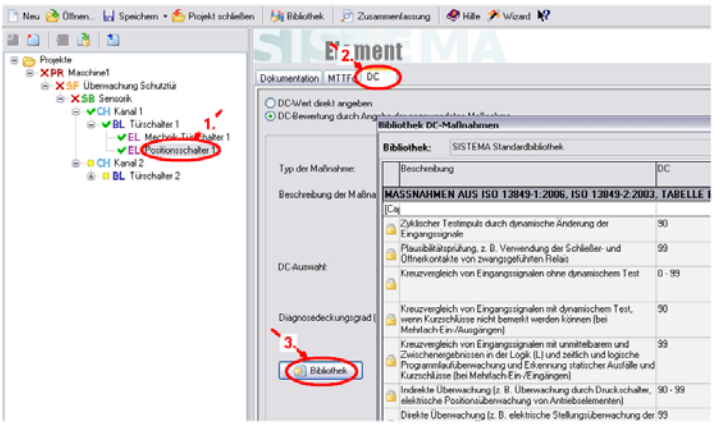


Abbildung 22

4.7 Ziel erreicht?

Im Hinweisfenster (Mitte, unten) ist zu prüfen, ob Fehlermeldungen mit einem roten Kreuz vorliegen. Falls dies nicht der Fall ist, ließ sich die PFH berechnen (Abbildung 23).

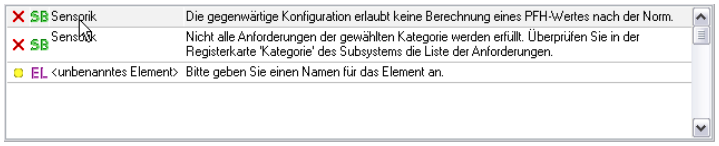


Abbildung 23

Das Ergebnis der Berechnung wird für die ausgewählte Sicherheitsfunktion und die jeweiligen Subsysteme, Blöcke und Elemente links unten angezeigt (Abbildung 24). 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.

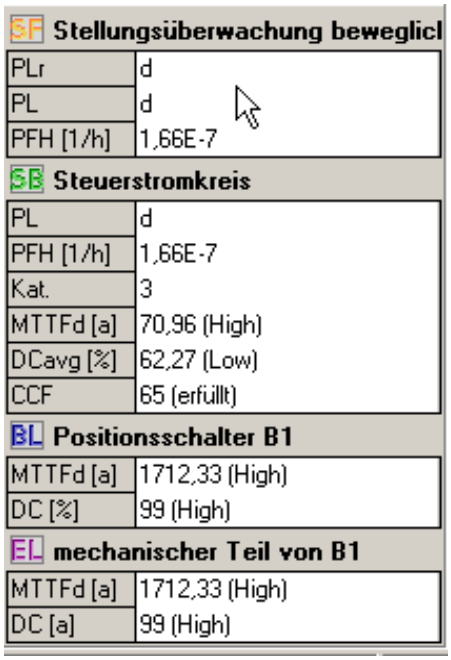


Abbildung 24

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, das die technische (hardwarenahe) Verknüpfung der sicherheitsbezogenen Teile der Steuerung zeigt
Sicherheitsbezogenes Blockdiagramm	Darstellung der logischen Verknüpfung der Bauteile, aus der die Funktions- und Testkanäle 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 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.
Funktionssignal	Signal, das die Anforderung der Sicherheitsfunktion entlang eines Funktionskanals vom Sensor zum Aktor weiterreicht und dort z. B. zur Abschaltung führt
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 dem Signalpfad, auf dem 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	Leitungsunterbrechungen führen zum sicheren Zustand.

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	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)

Anhang C: Beispielformular für eigene Anwendungen

Definition der Sicherheitsfunktion:

Auslösendes Ereignis:

Reaktion:

Sicherer Zustand:

Prinzipschaltbild mit eingetragenen Funktions- und Testkanälen:
als Anlage

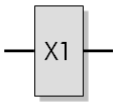
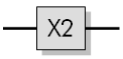
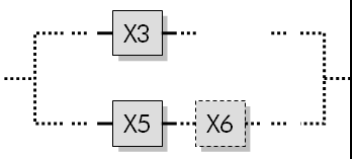
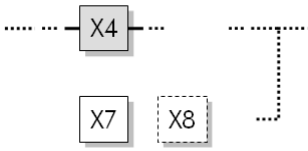
Sicherheitsbezogenes Blockdiagramm des ersten Funktionskanals, ggf. ergänzt um Bauteile im zweiten Funktionskanal oder im Testkanal:

Endgültiges Sicherheitsbezogenes Blockdiagramm, ggf. nach Zusammenfassung von Subsystemen gleicher Kategorie:

Anhang D: Tabellenschema

Das Tabellenschema ist eine alternative Methode zur Strukturanalyse nach Abbildung 5. Alle im Prinzipschaltbild dargestellten Bauteile werden entsprechend der in Abschnitt 3 beschriebenen Systematik in eine Tabelle eingetragen. Tabelle 4 zeigt die möglichen Kombinationen und die daraus abgeleitete Struktur (mögliche Kategorie) und Darstellung im Sicherheitsbezogenen Blockdiagramm, Tabelle 5 ist für das Beispiel aus Abschnitt 3 ausgefüllt und Tabelle 6 bietet ein leeres Formblatt für eigene Beispiele.

Tabelle 4: Formalisiertes Tabellenschema zur Strukturanalyse nach Abschnitt 3 (die in Abschnitt 3 genannten Schritte sind rot eingetragen)

Bauteile im ersten Funktionskanal	(1) X1 (2)	X2(2a)	X3 (2a)	X4 (2a)
Bauteilhersteller nennt Kategorie (3)?	Ja			
Redundante(s) Bauteil(e) (4)			X5 (, X6) (4a)	
Bauteil(e) im Testkanal (Fehlererkennung und Abschaltung) (5)				X7 (, X8) (5a)
Mögliche Kategorie	B bis 4 gekapseltes Subsystem	B oder 1 (6)	3 oder 4 (4b)	2
Blockdarstellung				

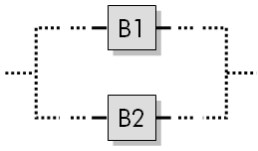
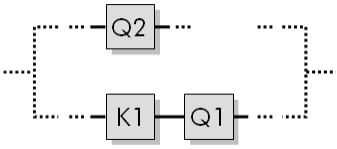
Bei der Strukturanalyse kann es hilfreich sein, sich die Schritte 3, 4 und 5 folgendermaßen zu versinnbildlichen: Was passiert, wenn mit einem „Prüfhammer“ auf das Bauteil geschlagen, also ein Bauteilfehler provoziert wird?

(3) Bleibt aufgrund der inneren Struktur die (Sicherheits-)Funktion erhalten?

(4) Bleibt aufgrund einer redundanten Ausführung der SF über andere Bauteile die SF erhalten?

(5) Wird der Bauteilfehler rechtzeitig erkannt und ein sicherer Zustand eingeleitet?

Tabelle 5: Für das Beispiel aus Abschnitt 3 ausgefüllte Tabelle

Bauteile im ersten Funktionskanal	B1	Q2
Bauteilhersteller nennt Kategorie?		
Redundante(s) Bauteil(e)	B2	K1, Q1
Bauteil(e) im Testkanal (Fehlererkennung und Abschaltung)		
Mögliche Kategorie	3 oder 4	3 oder 4
Blockdarstellung		

zusammengefasstes Blockdiagramm: (8)

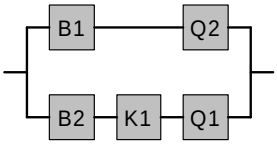


Tabelle 6: Formblatt für eigene Beispiele

Bauteile im ersten Funktionskanal								
Bauteilhersteller nennt Kategorie (3)?								
Redundante(s) Bauteil(e) (4)								
Bauteil(e) im Test-kanal (Fehlererken-nung und Abschal-tung) (5)								
Mögliche Kategorie								
Blockdarstellung								

Anhang E: Ablaufdiagramm der Strukturanalyse (ohne Beispiel)