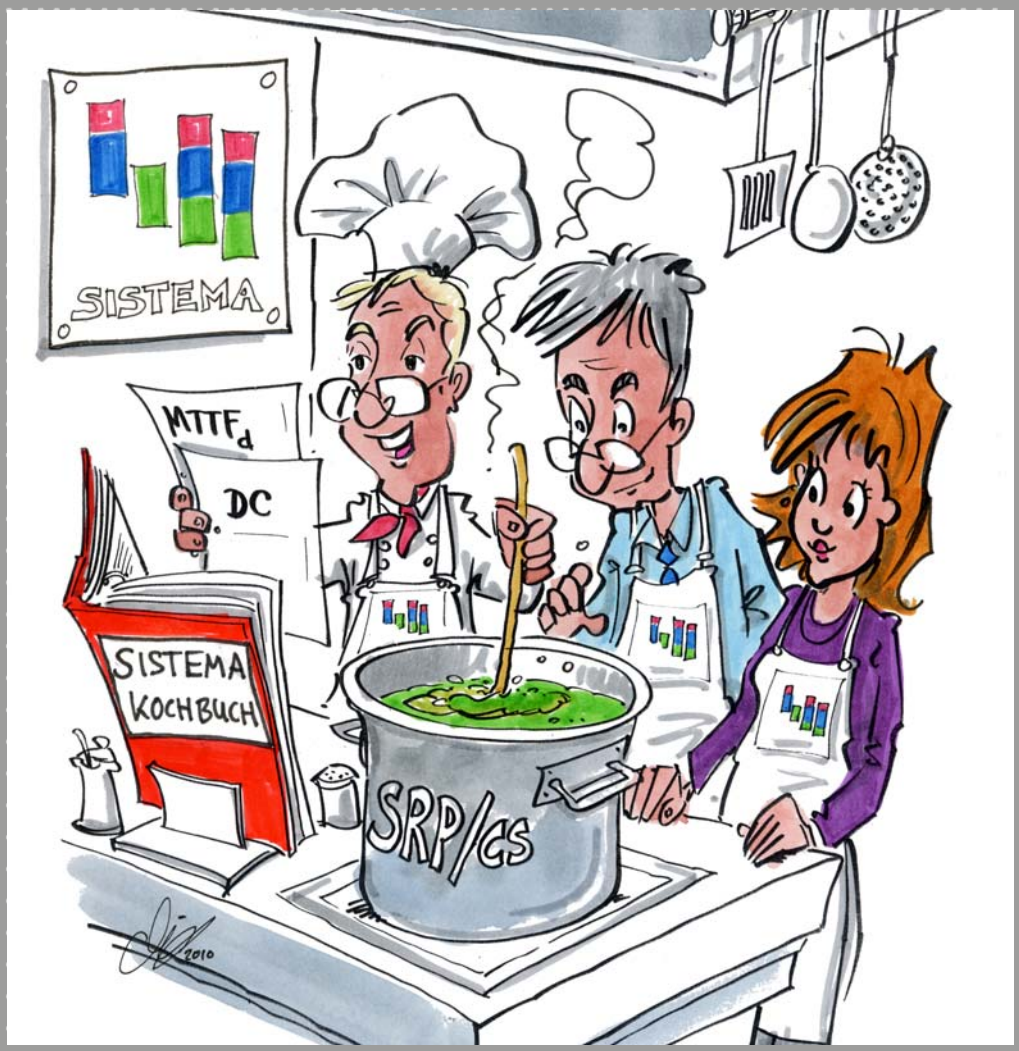
IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Das SISTEMA-Kochbuch 4

Wenn die vorgesehenen Architekturen nicht passen

Version 1.0 (DE)



Verfasser: Michael Hauke, Ralf Apfeld
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

Herausgeber: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Mittelstr. 51
10117 Berlin

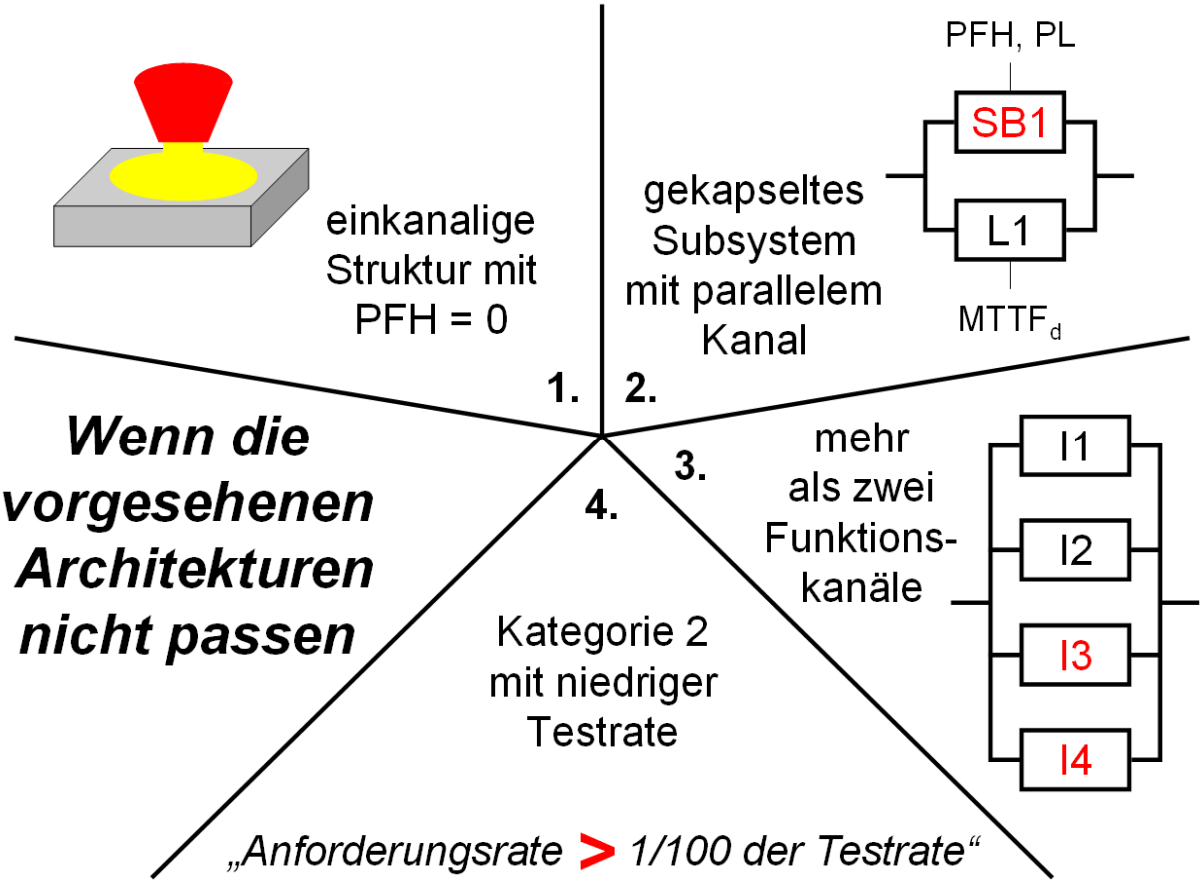
– März 2012 –

Inhaltsverzeichnis

Einleitung

Die Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde nach der vereinfachten Methode der DIN EN ISO 13849-1 zu ermitteln setzt voraus, dass die realisierte Steuerung einer der vorgesehenen Architekturen für die Kategorien entspricht. Ist dies nicht der Fall, kann die vereinfachte Methode nicht angewendet werden und meist ist ein aufwendigeres Verfahren, z. B. Markov-Modellierung, erforderlich. Manchmal reicht jedoch eine geringfügige – gedankliche – Anpassung aus, um eine Abbildung auf eine vorgesehene Architektur zu ermöglichen. Im Folgenden werden einige dieser Fälle erläutert, siehe Abbildung 1. Eine SISTEMA-Datei mit zugehörigen Beispiel-Projekten ist im Internetangebot des IFA unter www.dguv.de/ifa/13849 im Downloadbereich bei den SISTEMA-Kochbüchern zu finden.

Abbildung 1:
Vier Spezialfälle, die von den vorgesehenen Architekturen (Kategorien) der Norm abweichen, aber trotzdem mit SISTEMA bewertet werden können



1 Einfehlersicherheit bei einkanaliger Struktur

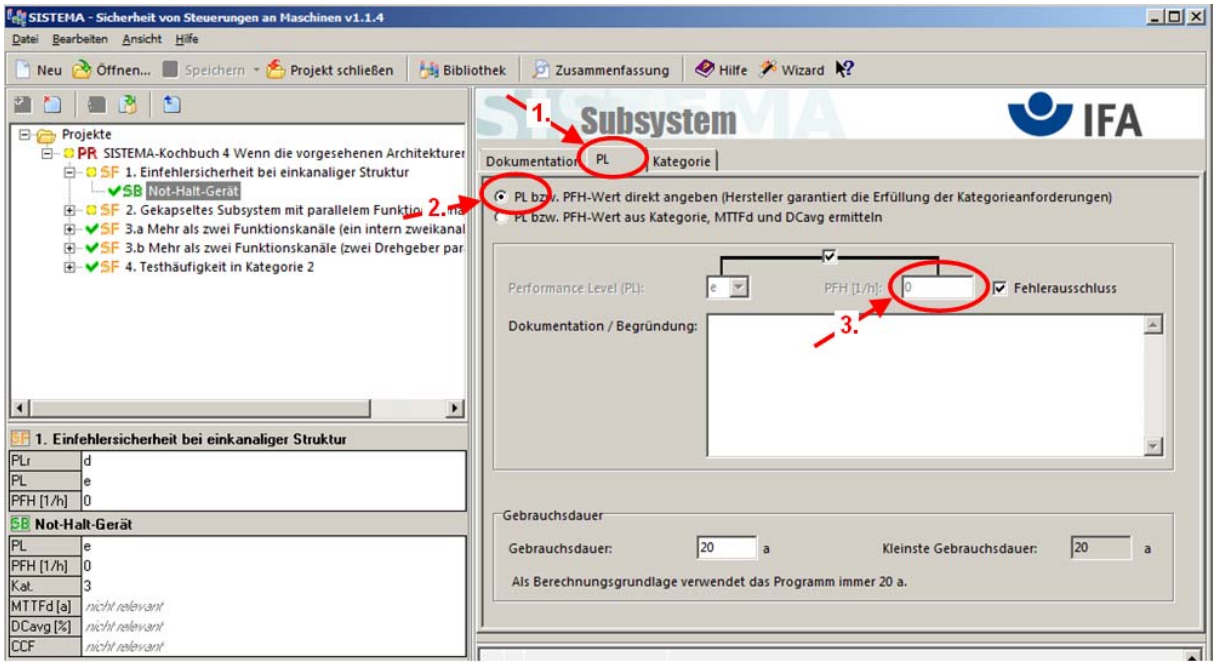
1.1 Beschreibung

In bestimmten Fällen kann ein einkanaliges Subsystem einfehlersicher sein. Dies trifft z. B. dann zu, wenn **alle** zufälligen Bauteilfehler eines Subsystems entweder zu einem Ausfall auf die sichere Seite führen oder wenn Fehlerausschlüsse angenommen werden können. Diese Annahme gilt z. B. für Not-Halt-Geräte, die nach IEC 60947-5-5 gebaut sind und nicht zu häufig betätigt werden (vgl. prEN ISO 13849-2:2010, Tabelle D.8 und BGIA-Report 2/2008, Abschnitt D2.5). In diesem Fall ist weder eine Angabe eines DC[1] noch die Betrachtung des CCF[2] notwendig.

1.2 Eingabe in SISTEMA

Die Eingabe in SISTEMA zeigt Abbildung 2. Sie erfolgt als Subsystem, bei dem in der Registerkarte „PL“ (1.) der PL[3] und PFH[4]-Wert direkt angegeben wird (2.). Der PFH-Wert beträgt „0“ (3.). Die Angabe in der Registerkarte „Kategorie“ ist informativ und wird von SISTEMA nicht ausgewertet, aber dokumentiert.

Abbildung 2:
Not-Halt-Gerät mit Fehlerausschluss und PFH = 0 als Subsystem mit Fehlerausschluss in SISTEMA



[1] DC = Diagnostic Coverage

[2] CCF = Common Cause Failure

[3] PL = Performance Level

[4] PFH = Probability of a dangerous Failure per Hour

1.3 Hinweise

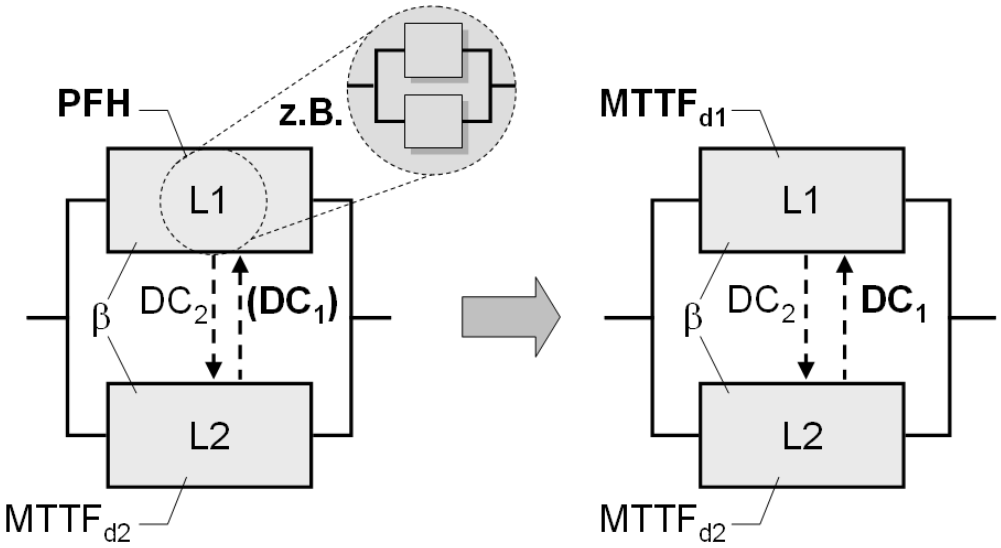
Dieses Verfahren ist möglich ab der SISTEMA-Version 1.1.2. Aus Gründen der internen Verarbeitung setzt SISTEMA dabei das Häkchen für einen Fehlerausschluss. Ist das Subsystem mit Fehlerausschluss das einzige unterhalb der Sicherheitsfunktion, so weist SISTEMA mit einer gelben Warnmeldung darauf hin, dass die Sicherheitsfunktion komplett mit Fehlerausschlüssen realisiert wird. **Für PL_r e ist ein Fehlerausschluss auf Subsystemebene in der Regel nicht zulässig.** Die Warnmeldungen sollen dazu auffordern, die hier gemachten Eingaben genau auf ihre Gültigkeit hin zu überprüfen. Mehr Informationen zu Fehlerausschlüssen gibt DIN EN ISO 13849-1:2008-12, Abschnitt 7.3 und DIN EN ISO 13849-2.

2 Gekapseltes Subsystem mit parallelem Funktionskanal

2.1 Beschreibung

Wenn in einem Kanal einer zweikanaligen Struktur gekapselte Subsysteme eingesetzt werden[5], steht die für die Berechnung des zweikanaligen Subsystems erforderliche $MTTF_d$[6] nicht zur Verfügung, sondern „nur“ PFH und PL (oder SIL[7]). Um trotzdem dieses Subsystem berechnen zu können, muss aus den vom Hersteller angegebenen Werten für PFH und PL ersatzweise die entsprechende $MTTF_d$ für einen Kanal bestimmt werden. Es stellt sich also konkret die Frage, wie das gekapselte Subsystem L1 mit bekannter PFH näherungsweise auf einen Block L1 mit $MTTF_{d1}$ und DC_1 abgebildet werden kann.

Abbildung 3:
Überführung eines gekapselten Subsystems L1 in einen Block



Bei der Überführung spielen mehrere Abhängigkeiten eine Rolle, die ein einfaches Kochrezept erschweren. Der im Folgenden vorgestellte Ansatz führt nicht immer zum Erfolg, speziell wenn Kategorie 4 erreicht werden soll. Dann bleibt nur eine detaillierte Betrachtung, z. B. durch ein von den Standardstrukturen abweichendes Markov-Modell.

2.2 Eingabe in SISTEMA

Sind keine Informationen über die wirksame Erkennung von Fehlern in L1 bekannt, dann gilt näherungsweise:

$$MTTF_{d1} = \frac{1}{PFH} \quad \text{und} \quad DC_1 = 0\ \%$$

[5] Eigentlich ist die Verwendung eines gekapselten Subsystems in Kategorie 2, 3 oder 4 in nur einem Kanal ökonomisch nicht sinnvoll. Trotzdem gibt es Fälle in der Praxis, in denen eine solche Beschaltung auftritt.

[6] $MTTF_d$ = Mean Time To dangerous Failure

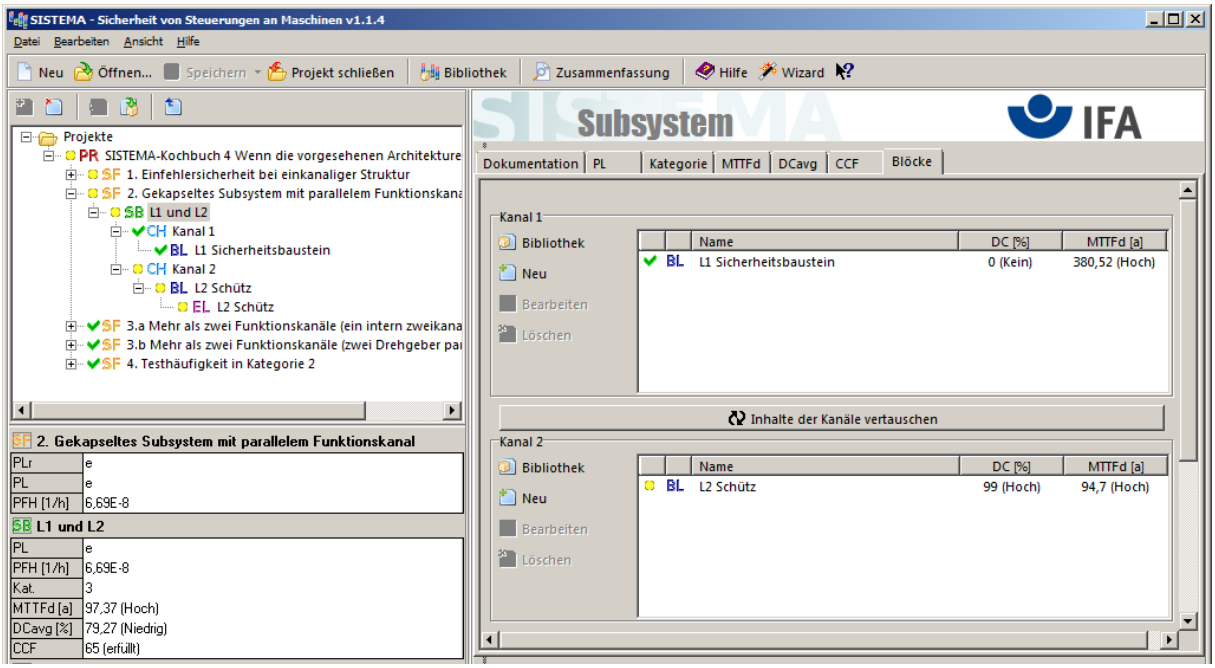
[7] SIL = Safety Integrity Level

Nur wenn von außen, z. B. durch L2, Fehler im gekapselten Subsystem L1 erkannt werden, kann ein entsprechend höherer Wert für DC_1 angesetzt werden. Dabei gilt:

$$DC_1 = \frac{\text{Ausfallrate } \textbf{von außen} \text{ erkannter gefährlicher Fehler in L1, } \textbf{die nicht durch interne Diagnosemaßnahmen in L1 erkannt werden können}}{\text{Ausfallrate aller gefährlichen Fehler in L1, } \textbf{die nicht durch interne Diagnosemaßnahmen in L1 erkannt werden können}}$$

Abbildung 4 zeigt die Anwendung des Ansatzes in SISTEMA. Das dargestellte Subsystem besteht aus einem Sicherheitsbaustein als gekapseltes Subsystem (PL d, PFH = 3,00E-7/h bei Einhaltung der vom Hersteller vorgegebenen maximalen Anzahl von Schaltzyklen) im ersten Kanal und parallel dazu einem Schütz mit Spiegelkontakten im zweiten Kanal.

Abbildung 4:
SISTEMA-Screenshot eines nach dem beschriebenen Ansatz behandelten Subsystems



Kapitel 3 zeigt die Anwendung mit $DC_1 > 0$ an einem weiteren Beispiel.

2.3 Tipp

Die Bildung des Kehrwerts erledigt SISTEMA selbständig, wenn der PFH-Wert in der $MTTF_d$-Registerkarte in das Feld „Rate gefahrbringender Ausfälle“ eingegeben wird, z. B. entspricht PFH = 3,00 E-7/h einer Eingabe von 300 FIT (1 FIT = 1 E-9/h) und einem $MTTF_d$-Wert von 380,5 Jahren.

2.4 Hinweise

Bei der Berechnung von $MTTF_d$ als Kehrwert von PFH muss generell auf eine **korrekte Umrechnung der Einheiten** geachtet werden (1 Jahr = 8760 h).

Die **korrekte „zweikanalige“ Beschaltung** von L1 wird hier genauso vorausgesetzt wie die Erfüllung aller für L1 spezifizierten Randbedingungen für die angegebene PFH, z. B. hinsichtlich der Fehlererkennung.

Diese Methode gilt sowohl, wenn das gekapselte Subsystem wie in Abbildung 3 alleine einen Kanal bildet, als auch wenn mit ihm in diesem Kanal **weitere Blöcke** vorhanden sind. Dieses Vorgehen ist auch anwendbar, wenn **in beiden Kanälen** einer zweikanaligen Struktur gekapselte Subsysteme (gleiche oder unterschiedliche) eingesetzt werden. Siehe dazu auch Kapitel 3.

Alle internen Maßnahmen, die die Ausfallwahrscheinlichkeit von L1 reduzieren, wie mehrkanalige Struktur und Fehlererkennung, sind über die PFH in $MTTF_{d1}$ eingerechnet. Ein weiteres Verwenden der internen Diagnosemaßnahmen innerhalb L1 ist daher nicht mehr möglich, da diese zur Bestimmung der PFH bereits „verbraucht“ wurden. Unter diesen Umständen muss zunächst $DC_1 = 0$ angesetzt werden. Wird mit dem gesamten Subsystem, das L1 und L2 enthält, eine Kategorie 4 angestrebt, führt die Bedingung DC_{avg} mindestens 99 % (mit Toleranz[8] reichen 94 %) u. U. zum Scheitern dieses Ansatzes, sofern nicht ein ausreichender DC durch externe Testung erreicht werden kann.

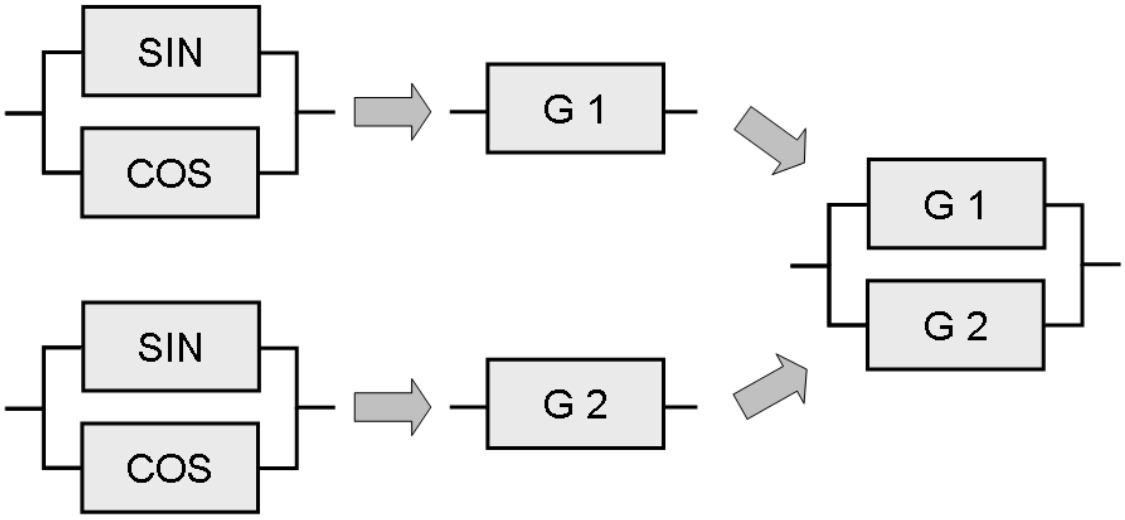
[8] unter Ausnutzung der 5-%-Toleranz nach Tabelle 6 der Norm

3 Mehr als zwei Funktionskanäle

3.1 Beschreibung

Da mit der vereinfachten Methode der DIN EN ISO 13849-1 (und damit auch mit SISTEMA) nur einkanalige und zweikanalige Strukturen berechnet werden können, muss die Anzahl vorhandener Kanäle auf zwei reduziert werden. Die einfachste Möglichkeit besteht darin, überzählige Kanäle (am besten diejenigen mit geringerer Zuverlässigkeit) einfach bei der Berechnung zu vernachlässigen. Dies ist jedoch nur dann zielführend, wenn die erreichte PFH ausreichend ist. Alternativ können zwei Kanäle in einem Zwischenschritt vorher zusammengefasst und als einzelner Block in einem Kanal dargestellt werden (siehe auch Kapitel 2). Abbildung 5 gibt hierzu einen Überblick.

Abbildung 5:
Verfahren zur Abbildung eines vierkanaligen Gebersystems auf eine zweikanalige Struktur

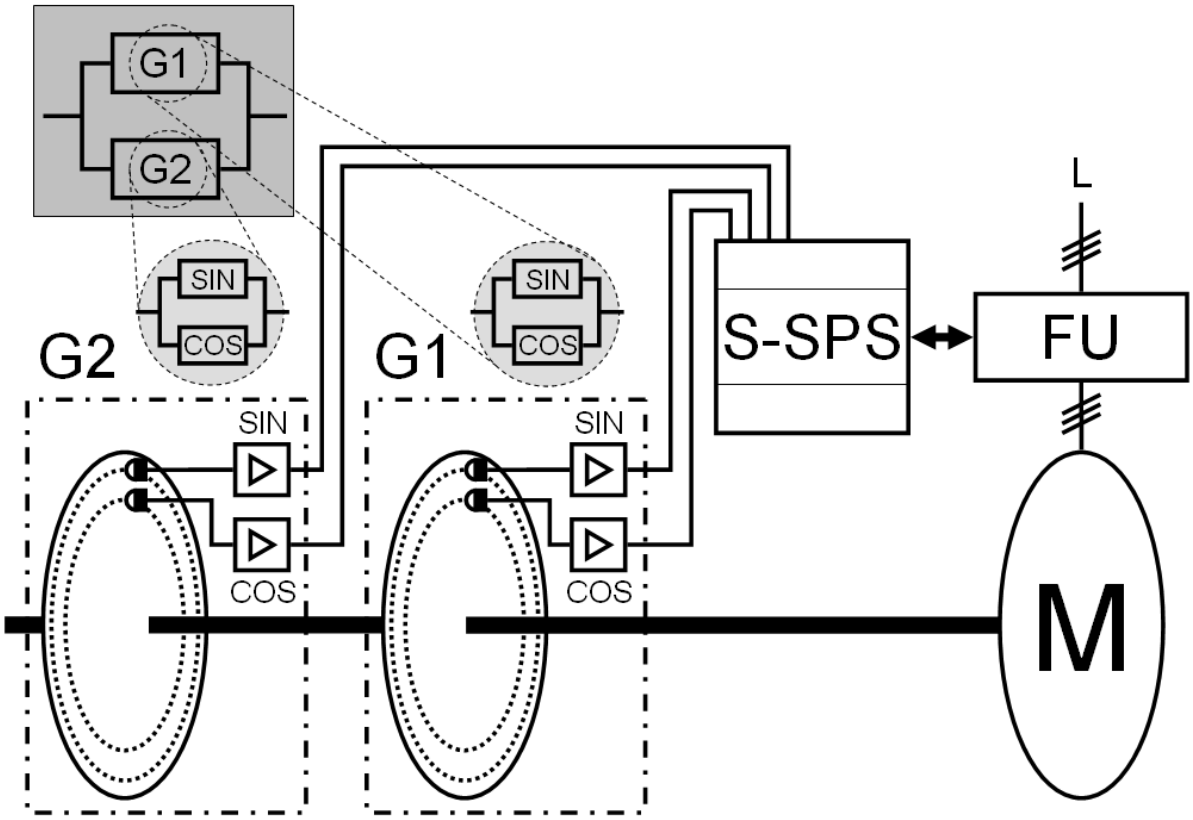


3.2 Eingabe in SISTEMA

Das Verfahren der schrittweisen Zusammenfassung wird an einem Beispiel für eine vierkanalige Struktur durchgeführt, wie in Abbildung 6 gezeigt:

Zwei identische Drehgeber G1 und G2 erfassen einen Drehwinkel α und liefern dazu jeweils sin- und cos-Ausgangssignale. Es wird unterstellt, dass diese beiden Ausgangssignale voneinander unabhängig sind und somit getrennte Kanäle darstellen (siehe Abschnitt 3.6). Die Verwendung der Mehrfachredundanz dient hier dazu, den PFH-Beitrag der Geber an der Sicherheitsfunktion zu reduzieren.

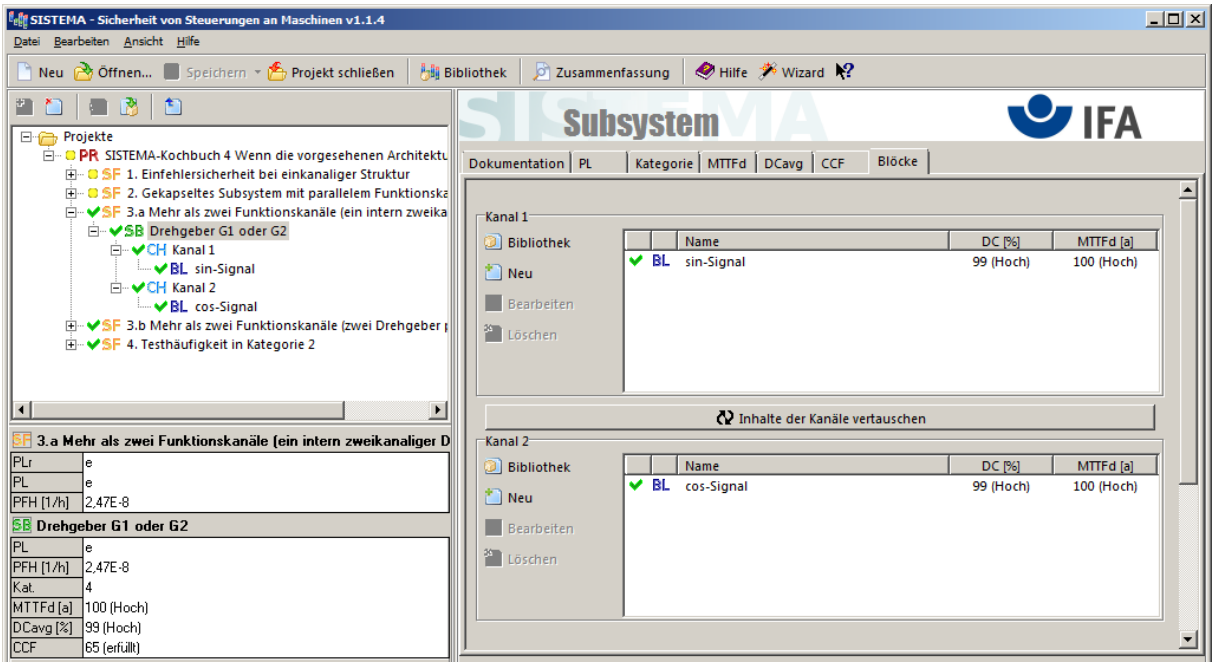
Abbildung 6:
Beispiel für eine vierkanalige Struktur zur Erfassung eines Drehwinkels α



3.3 Erster Schritt

Üblicherweise würde man die Hardware für das sin- und das cos-Signal jedes Gebers als jeweils eigenen Funktionskanal modellieren. Dies ist bei Gebern möglich, bei denen keine Bauteilfehler vorkommen können, die das sin- und das cos-Signal zueinander passend ($\sin^2\alpha + \cos^2\alpha = 1$) verfälschen (siehe Abschnitt 3.6). Um alle vier Kanäle zu berücksichtigen, wird jeder Geber G1 und G2 zunächst separat als zweikanaliges Subsystem modelliert. Die Berechnung der PFH eines Gebers erfolgt dabei auf die übliche Weise, indem die Hardware der sin- und cos-Signale jeweils einen Kanal eines Subsystems der Kategorie 3 oder 4 bilden. In diesem Beispiel wird mit Kategorie 4 und 100 Jahren $MTTF_d$ für jeden Kanal gerechnet. Als DC-Maßnahme kann z. B. die Überprüfung auf $\sin^2\alpha + \cos^2\alpha = 1$ durch die Steuerung separat für jeden Geber herangezogen werden. Dafür werden hier 99 % DC angesetzt. Die ermittelten PFH-Werte beider Geber betragen jeweils 2,47E-8/h und sind das Ergebnis des ersten Schritts (siehe Abbildung 7). Diese werden im zweiten Schritt gebraucht.

Abbildung 7:
SISTEMA-Screenshot eines Gebers G1 oder G2 als zweikanaliges Subsystem



3.4 Zweiter Schritt

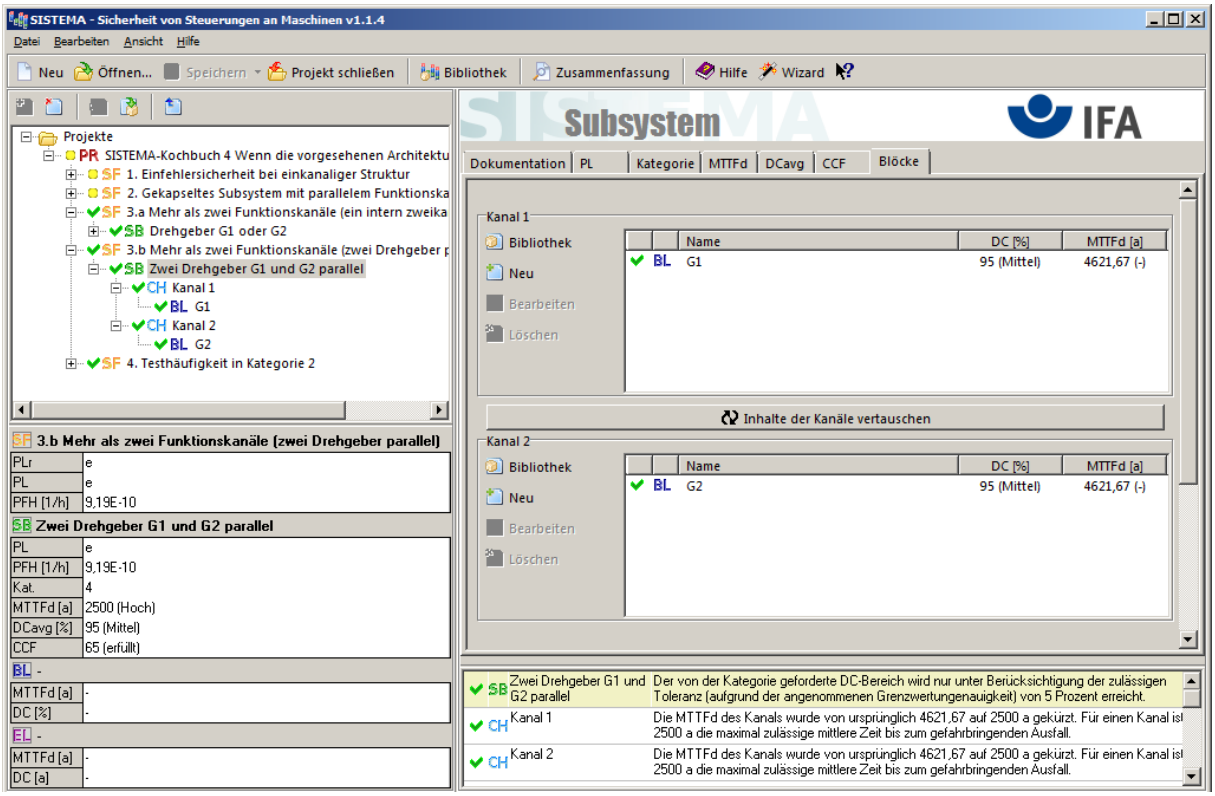
Für das Gesamtsystem aus zwei Drehgebern kann wie in Kapitel 2 dargestellt, ein neues zweikanaliges Subsystem der Kategorie 3 oder 4 angelegt werden, in dem jeder einzelne Geber als ein Block in einem Kanal abgebildet wird.

Als $MTTF_d$ der Blöcke wird der Kehrwert der PFH des einzelnen Gebers angesetzt ($MTTF_d$ = 1/PFH). Hier ergeben sich als $MTTF_d$-Werte für jeden der beiden Geber 4621,67 Jahre, das entspricht dem Kehrwert von 2,47E-8/h oder einer Eingabe als „Rate gefahrbringender Ausfälle“ von 24,7 FIT. In SISTEMA sollte dazu die Expertenoption „$MTTF_d$-Kappung für Kategorie 4 von 100 auf 2500 Jahre anheben“ aktiviert sein[9].

DC für die Blöcke wird ermittelt, indem zusätzliche „äußere“ fehlererkennende Maßnahmen bewertet werden, die gefährliche Ausfälle eines einzelnen Gebers erkennen und einen sicheren Zustand des Gesamtsystems herbeiführen. Gefährliche Ausfälle, die ggf. bereits durch die internen DC-Maßnahmen innerhalb eines einzelnen Gebers erkannt werden, bleiben dabei unberücksichtigt (siehe Abschnitt 2.4). Die DC-Anforderungen der Kategorie (mindestens „niedrig“ für Kategorie 3 und mindestens „hoch“ für Kategorie 4) müssen bei dieser Methode alleine mit dem „äußeren“ DC erfüllt werden. Als DC-Wert für den Vergleich beider Gebersignale in einer nachgeordneten Steuerung wurden hier 95 % geschätzt (siehe Abschnitt 3.6). Dies erfüllt auch die Anforderungen der im Beispiel angenommenen Kategorie 4 (siehe Abbildung 8).

[9] von Deutschland vorgeschlagen für das Amendment der Norm, vgl. Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schaefer, M.: Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) Nr. 6, S. 34-37, online unter www.dguv.de/ifa/13849

Abbildung 8:
SISTEMA-Screenshot beider Geber G1 und G2 als zweikanaliges Subsystem



3.5 Tipp

Bei Gebern für sicherheitstechnische Anwendungen gibt der Hersteller oft schon eine PFH an. Der erste Schritt erübrigt sich dann und es kann direkt mit dem zweiten Schritt begonnen werden.

3.6 Hinweise

sin-/cos-Drehgeber tasten üblicherweise eine Strichcodescheibe optisch ab und generieren dabei die gewünschte Signalform, die durch die Formgebung der lichtempfindlichen Stellen des Sensors bestimmt ist. Es schließt sich eine Aufbereitung der analogen Signale an. Prinzipiell erfolgt die Signalverarbeitung beider Kanäle teilweise innerhalb desselben Schaltkreises. Trotzdem ist die Einfehlersicherheit der Elektronik gewährleistet, da kein Bauteilfehler vorstellbar ist, der zu einer unerkennbaren Verfälschung von sin- und cos-Signal gleichzeitig führt. Es sind auch keine Bauteile zur Speicherung der Analogwerte vorhanden, sodass ein „Einfrieren“ der Ausgangssignale nicht möglich ist.

Ein Lösen der mechanischen Verbindung zwischen Antriebswelle und Geberwelle kann nicht durch $\sin^2\alpha + \cos^2\alpha = 1$ erkannt werden und liefert daher einen Beitrag zur PFH des einzelnen Gebers. Sind beide Geber unabhängig voneinander an die Antriebswelle gekoppelt, so könnte eine nachgeordnete Steuerungslogik diese gefährlichen Ausfälle aber durch einen Vergleich beider Geberinformationen mit hohem „äußerem“ DC erkennen.

Alternativ kann für die mechanische Kopplung des Gebers an die Welle ein Fehlerausschluss angenommen werden. In diesem Fall findet die Kopplung keine Berücksichtigung im sicherheitsbezogenen Blockdiagramm. Der Fehlerausschluss erfolgt durch den Geberher-

steller bei geeigneter Konstruktion der Gebermechanik und Überdimensionierung. In Kategorie-4-Systemen ist diesem Fehlerausschluss besondere Aufmerksamkeit zu schenken. Weitere Hinweise finden sich in DIN EN IEC 61800-5-2: 2008, Tabelle D.16.

Common-Cause-Fehler im zweikanaligen Subsystem aus zwei Gebern werden wie üblich in SISTEMA automatisch durch eine eigene Registerkarte erfasst und bei der Ermittlung der PFH berücksichtigt.

4 Testhäufigkeit in Kategorie 2

4.1 Beschreibung

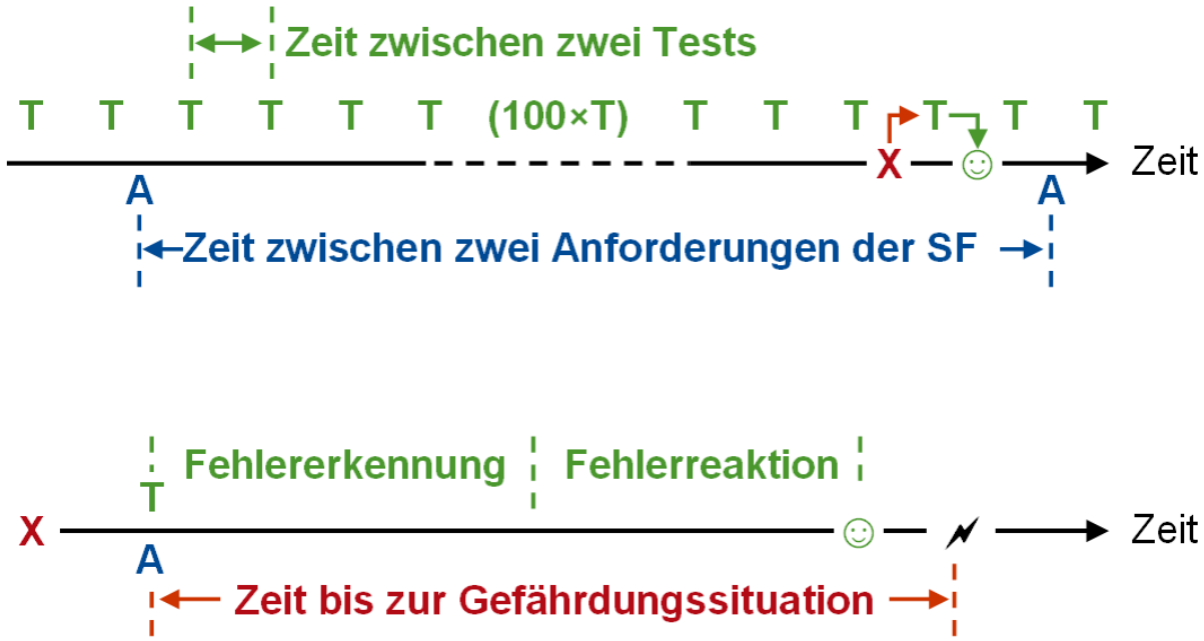
Die Zuverlässigkeit einer einkanaligen getesteten Architektur – wie sie für Kategorie 2 vorgesehen ist – hängt stark von der Testhäufigkeit ab. Wird ein Test zu selten ausgeführt, so bietet er nur trügerische Sicherheit: Mit der Länge des Testintervalls steigt die Wahrscheinlichkeit, dass auf einen gefahrbringenden Ausfall der Sicherheitsfunktion eine Anforderung der Sicherheitsfunktion folgt, bevor der nächste Test stattfindet (siehe Abbildung 9 oben). Die Testhäufigkeit konkurriert in einer einkanaligen getesteten Architektur daher mit der Häufigkeit der Anforderung der Sicherheitsfunktion. DIN EN ISO 13849-1 setzt im vereinfachten Verfahren zur Abschätzung eines PLs für Kategorie 2 voraus, dass das Verhältnis der Testrate zur mittleren Anforderungsrate der Sicherheitsfunktion mehr als 100 beträgt.

In folgenden zwei Fällen ist eine Abweichung von dieser Regel zulässig:

Fall 1 Das Verhältnis der Testrate zur Anforderungsrate der Sicherheitsfunktion ist kleiner als 100 aber mindestens 25. Dann kann mit einem PFH-Zuschlag gerechnet werden.

Fall 2 Fehlererkennung und Fehlerreaktion werden durch die Anforderung der Sicherheitsfunktion ausgelöst und erfolgen schneller als das Eintreten der Gefährdungssituation (siehe Abbildung 9 unten).

Abbildung 9: Zwei alternative Realisierungen für eine effektive Testung in Kategorie 2.
T: Testzeitpunkte, X: gefährlicher Ausfall des Funktionskanals, A: Anforderung der Sicherheitsfunktion, ☺: sicherer Zustand nach Fehlererkennung, ↯: Auftreten einer Gefährdungssituation



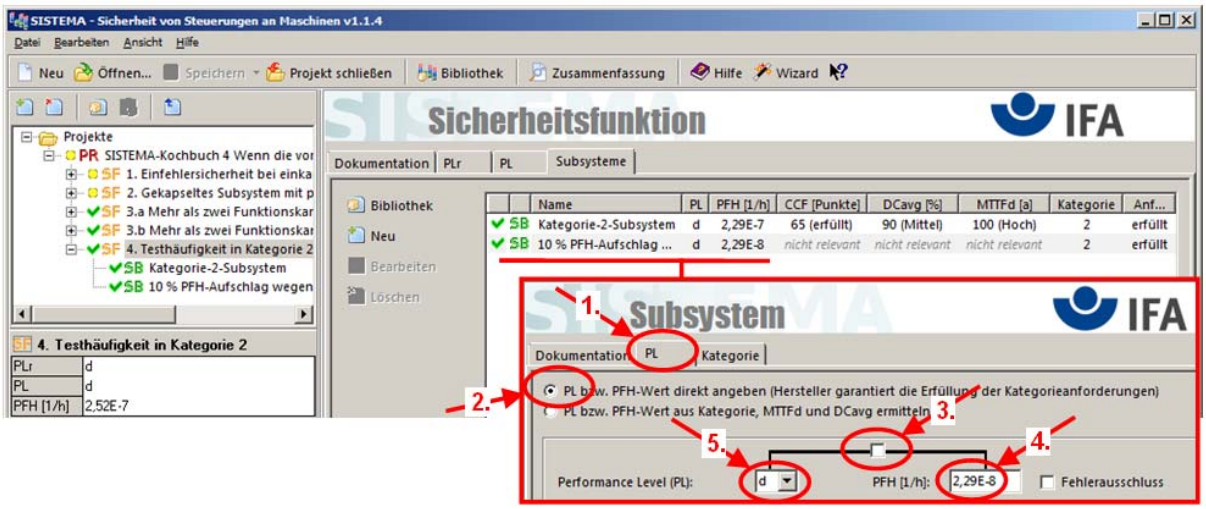
4.2 Fall 1: Verhältnis der Testrate zur Anforderungsrate der Sicherheitsfunktion ist kleiner als 100 aber mindestens 25

Zu dem ursprünglichen Kategorie-2-Subsystem mit nicht optimalem Ratenverhältnis wird ein zweites Subsystem hinzugefügt, dessen PFH-Wert den PFH-Aufschlag gegenüber dem Verhältnis von 100 widerspiegelt. Der direkt einzugebende PFH-Wert beträgt 10 % des PFH-Wertes des ersten Kategorie-2-Subsystems (siehe Abschnitt 4.3).

Im ersten Subsystem muss dazu in der Registerkarte „Kategorie“ die Kategorie 2 ausgewählt werden und unter „Anforderungen der Kategorie“ die Bedingung „Die Anforderungsrate der Sicherheitsfunktion ist kleiner oder gleich einem Hundertstel der Testrate“ trotzdem als erfüllt markiert werden. Im Dokumentationsfeld zum Subsystem sollte auf den besonderen Sachverhalt und die Zusammengehörigkeit der beiden Subsysteme hingewiesen werden.

Abbildung 10 zeigt das Beispiel eines Kategorie-2-Subsystems mit $MTTF_d$ = 100 Jahre, DC = 90 % und Verhältnis der Testrate zur Anforderungsrate der Sicherheitsfunktion von 25. SISTEMA berechnet einen PFH-Wert von 2,29E-7/h (PL d) unter der Voraussetzung eines Verhältnisses der Raten von 100. Gemäß obiger Anleitung wird der PFH-Aufschlag als 0,1 x 2,29E-7/h = 2,29E-8/h ermittelt. Für das zusätzliche Subsystem müssen in der Registerkarte „PL“ (1.) der PL und der PFH-Wert direkt angegeben werden (2.). Die PL-Eingabe wird dazu vom PFH-Wert entkoppelt (3.), ein PFH-Wert von 2,29E-8/h eingetragen (4.) und als PL ebenfalls d eingegeben (5.). Für das zusätzliche Subsystem kann auch Kategorie 2 eingetragen werden.

Abbildung 10:
Beispiel eines Kategorie-2-Subsystems mit Verhältnis der Testrate zur Anforderungsrate der Sicherheitsfunktion von 25:1



4.3 Hinweise

Durch Markov-Modellierung kann die Erhöhung der Ausfallwahrscheinlichkeit in Abhängigkeit vom Verhältnis der Testrate zur Anforderungsrate berechnet werden. Bei einem Verhältnis von mindestens 25 beträgt der unter den ungünstigsten Bedingungen gültige maximale relative PFH-Aufschlag ca. 10 %. Der relative Aufschlag bezieht sich auf den mit SISTEMA ermittelbaren PFH-Wert des Kategorie-2-Subsystems mit optimalem Verhältnis der Testrate zur Anforderungsrate von 100 oder größer.

4.4 Fall 2: Fehlererkennung und Fehlerreaktion werden durch die Anforderung der Sicherheitsfunktion ausgelöst und erfolgen schneller als das Eintreten der Gefährdungssituation

In SISTEMA kann in der Registerkarte „Kategorie“ eines Kategorie-2-Subsystems unter „Anforderungen der Kategorie“ die Bedingung „Die Anforderungsrate der Sicherheitsfunktion ist kleiner oder gleich einem Hundertstel der Testrate“ auch dann als erfüllt markiert werden, wenn die Testwirksamkeit auf diesem alternativen Wege sichergestellt wird. Die Begründung dafür sollte im Dokumentationsfeld zum Subsystem aufgeführt werden, z. B. „Die Anforderungen für Kategorie 2 an die Testhäufigkeit werden erfüllt, da Tests und Anforderungen der Sicherheitsfunktion so synchronisiert sind, dass die Testung bei der Anforderung der Sicherheitsfunktion stattfindet, und die Testung so schnell ausgeführt wird, dass der sichere Zustand erreicht wird, bevor es zu einer Gefährdung kommt (siehe SISTEMA-Kochbuch 4 „Wenn die vorgesehenen Architekturen nicht passen“, Kapitel 4)“.

4.5 Hinweise

Abbildung 9 auf Seite 15 illustriert, dass eine Kategorie-2-Struktur auch dann effektiv ist, wenn die Testung gleichzeitig mit der Anforderung der Sicherheitsfunktion und z. B. damit verbundenen Signalwechseln erfolgt. Der sichere Zustand kann allerdings nur erreicht werden, wenn die Fehlererkennung (z. B. Auswertung der Sensorsignale in der Logik) sowie die sichere Fehlerreaktion (z. B. Signalweitergabe der Logik an die Aktoren und Stillsetzen einer gefahrbringenden Bewegung) schneller erfolgen, als die tatsächliche Gefährdungssituation eintritt. Diese Zeitspanne wird z. B. durch ausreichende Sicherheitsabstände zwischen fester oder berührungslos wirkender Schutzeinrichtung und der Gefahrenstelle bestimmt. Die alternative Möglichkeit, eine effektive Testung zu realisieren, ist auch im BGIA-Report 2/2008, Abschnitt 6.2.14, dritter Aufzählungspunkt und in Abschnitt 6.3.2 der IEC 62061 beschrieben. Sie ist zudem aktuell für das Amendment der DIN EN ISO 13849-1 vorgeschlagen. Passende Schaltungsbeispiele sind im BGIA-Report 2/2008, Abschnitt 8.2.11 und 8.2.12 dargestellt: Das Versagen eines einkanaligen Abschaltventils wird bei der Anforderung der Sicherheitsfunktion erkannt und ein alternatives Stillsetzen der gefahrbringenden Bewegung durch das Abschalten des Entlüftungsventils oder der Hydraulikpumpe eingeleitet. Die größeren Nachlaufwege gehen dabei in die Fehlerreaktionszeit ein. Die Zeitspanne bis zum Eintritt der Gefährdungssituation muss daher entsprechend lang sein.

Muss eine Sicherheitsfunktion kontinuierlich ausgeführt werden, so kann die Testrate gar nicht hoch genug sein. In diesem Fall ist eine Realisierung von Kategorie 2 nur auf diesem alternativen Wege möglich, indem Fehlererkennung und Fehlerreaktion immer rechtzeitig vor dem Entstehen einer Gefährdung erfolgen.