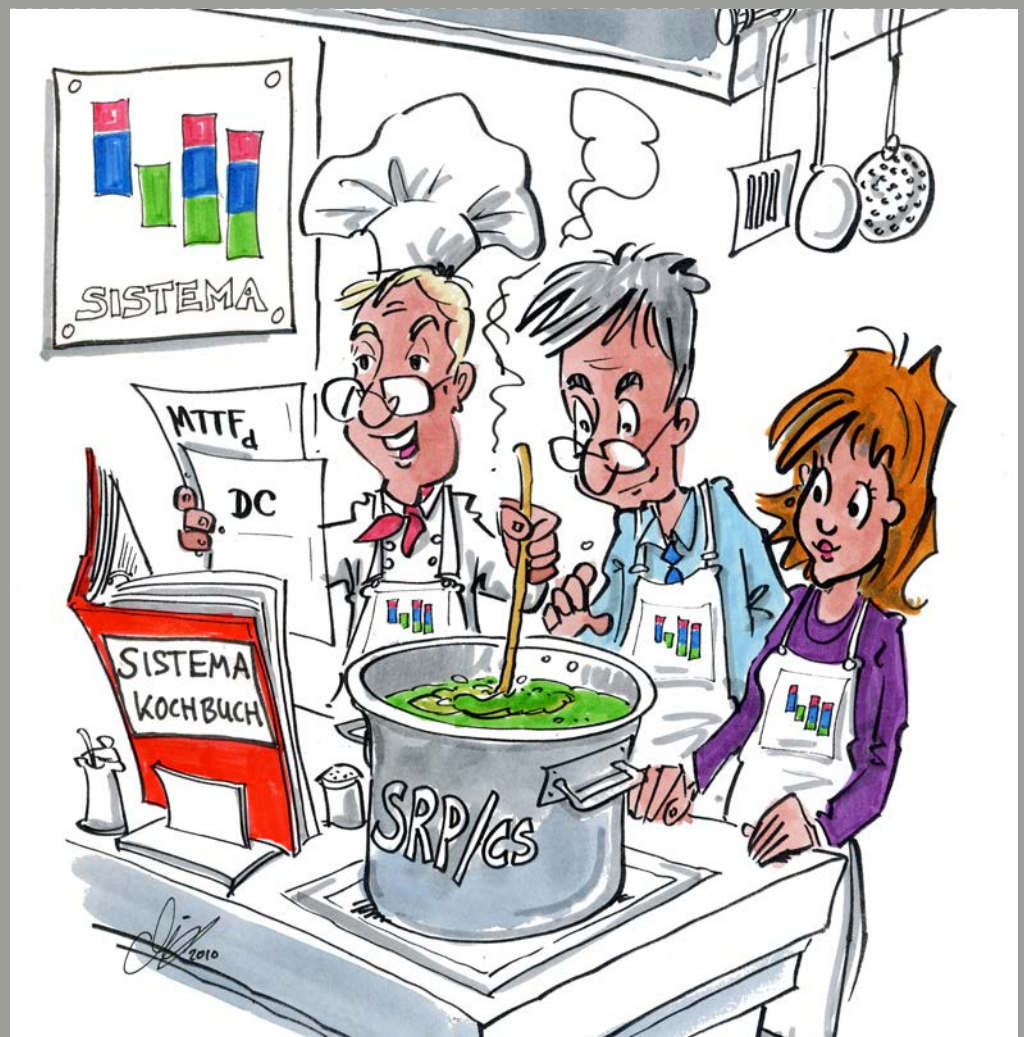


Das SISTEMA-Kochbuch 4

Wenn die vorgesehenen Architekturen
nicht passen

Version 2.0 (DE)



Verfasser: Michael Hauke, Ralf Apfeld, Michael Huelke, Thomas Bömer,
Christian Werner
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 2020 –

Inhaltsverzeichnis

Inhaltsverzeichnis	3
Einleitung	4
1 Einfehlersicherheit bei einkanaliger Struktur	5
1.1 Beschreibung.....	5
1.2 Eingabe in SISTEMA	5
1.3 Hinweise	6
2 Gekapseltes Subsystem mit parallelem Funktionskanal	7
2.1 Beschreibung.....	7
2.2 Eingabe in SISTEMA	8
2.3 Tipp.....	9
2.4 Hinweise	9
3 Mehr als zwei Funktionskanäle.....	10
3.1 Beschreibung.....	10
3.2 Eingabe in SISTEMA	10
3.3 Erster Schritt.....	11
3.4 Zweiter Schritt.....	12
3.5 Tipp.....	13
3.6 Hinweise	13
4 Testhäufigkeit in Kategorie 2	15
4.1 Beschreibung.....	15
4.2 Fall 1: Anforderungsrate zu Testrate größer als 1/100	16
4.3 Hinweise zu Fall 1	16
4.4 Fall 2: Fehlererkennung bei Anforderung der Sicherheitsfunktion	17
4.5 Hinweise zu Fall 2.....	17
5 Gebrauchsdauer größer als 20 Jahre	18
5.1 Beschreibung.....	18
5.2 Fall 1: Gebrauchsdauer von vorneherein größer als 20 Jahre spezifiziert	18
5.3 Fall 2: Nachträgliche Verlängerung der Gebrauchsdauer.....	18
5.4 Eingabe in SISTEMA	18

Einleitung


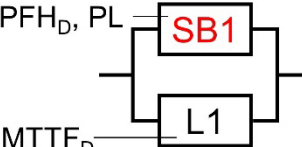
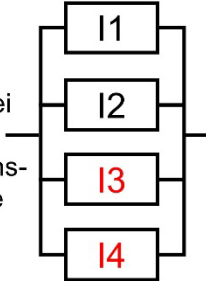
Möchte man die Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde nach der vereinfachten Methode der DIN EN ISO 13849-1 ermitteln, muss die realisierte Steuerung einer der vorgesehenen Architekturen für die Kategorien entsprechen. Ist dies nicht der Fall, kann die vereinfachte Methode nicht angewendet werden und meist ist ein aufwendigeres Verfahren, z. B. eine Markov-Modellierung, erforderlich. Manchmal reicht jedoch eine geringfügige – gedankliche – Anpassung aus, um die eigene Steuerung auf eine vorgesehene Architektur abzubilden. Im Folgenden werden einige dieser Fälle erläutert, siehe Abbildung 1. Eine SISTEMA-Datei mit zugehörigen Beispielprojekten ist im Internetangebot des Instituts für Arbeitsschutz der DGUV (IFA) unter <https://www.dguv.de/webcode/d109240> im Downloadbereich bei den SISTEMA-Kochbüchern zu finden.

In der vorliegenden zweiten Auflage wurden im Vergleich zur ersten Fassung des SISTEMA-Kochbuchs 4 von 2012 einige Aktualisierungen vorgenommen:

- Kapitel 1 wurde angepasst: Not-Halt-Geräte werden nach der aktuellen Fassung der DIN EN ISO 13849-1 nicht mit einem Fehlerausschluss auf Subsystemebene modelliert.
- Kapitel 2 wurde nur redaktionell angepasst.
- Kapitel 3 wurde in einigen Details überarbeitet.
- Kapitel 4 wurde aktualisiert, da seit der dritten Ausgabe der DIN EN ISO 13849-1 von 2016 ein Verhältnis der Anforderungsrate der Sicherheitsfunktion zur Testrate möglich ist, das größer als 1/100 ist, aber mindestens 1/25 beträgt.
- In Kapitel 5 kam der Abschnitt „Gebrauchsdauer größer als 20 Jahre“ dazu.

Abbildung 1:

Fünf Spezialfälle, die von den vorgesehenen Architekturen (Kategorien) der Norm abweichen, aber trotzdem mit SISTEMA bewertet werden können.

<p>1. einkanalige Struktur mit $PFH_D = 0$</p>  <p>$PFH_D = 0$</p>	<p>Wenn die vorgesehenen Architekturen nicht passen</p>	<p>5. Gebrauchsdauer größer als 20 Jahre</p> <p>„$T_M > 20 \text{ Jahre}$“</p>
<p>2. gekapseltes Subsystem mit parallelem Kanal</p>  <p>PFH_D, PL</p> <p>$MTTF_D$</p>		<p>3. mehr als zwei Funktions- kanäle</p> 

1 Einfehlersicherheit bei einkanaliger Struktur

1.1 Beschreibung

In bestimmten Fällen kann ein einkanaliges Subsystem als einfehlersicher betrachtet werden. 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. Ein PFH_D -Wert von Null ist für ein Subsystem nur in Ausnahmefällen gerechtfertigt, wenn konkrete Applikationen dies zulassen. Diese Annahme gilt z. B. für Positionsschalter mit Personenschutzfunktion zur Überwachung von trennenden verriegelten Schutzeinrichtungen an Druck- und Papierverarbeitungsanlagen ohne betriebsmäßig regelmäßigen Eingriff in Gefahrstellen und maximal $PL_r d$ (vergleiche Abschnitt 5.2.11.2 in DIN EN 1010-1:2011). Die Positionsschalter müssen dazu nach EN 60947-5-1:1997 gebaut und in Übereinstimmung mit EN 60204-1:2006 installiert sein. In diesem Fall ist weder eine Angabe eines DC^1 noch die Betrachtung des CCF^2 notwendig.

In der ersten Fassung dieses SISTEMA-Kochbuchs, das auf der zweiten Ausgabe der DIN EN ISO 13849-1:2008 basierte, waren Not-Halt-Geräte als ein Beispiel für diesen Sonderfall genannt. Mit der aktuellen Normfassung von 2016 hat sich die Behandlung von Not-Halt-Geräte allerdings geändert, sodass kein Fehlerausschluss für das Not-Halt-Gerät als Subsystem mehr empfohlen wird. In Anhang D.2.5.4 des IFA Reports 2/2017 zur aktuellen Normfassung findet sich eine ausführliche Erläuterung zur Modellierung von Not-Halt-Geräten und anderen elektromechanischen Bauteilen.

Auch Bussysteme zur Übertragung sicherheitsrelevanter Informationen können physikalisch einkanalig ausgelegt sein und die Datenübertragung trotzdem einfehlersicher ausführen. Hier gibt der IFA Report 2/2017 in Abschnitt 6.2.18 ebenfalls weiterführende Hinweise.

1.2 Eingabe in SISTEMA

Die Eingabe in SISTEMA zeigt Abbildung 2. Für das Subsystem wird in der Registerkarte „PL“ (1.) der PL^3 und PFH_D^4 -Wert direkt angegeben (2.). Der PFH_D -Wert beträgt „0“ (3.). Die Angabe in der Registerkarte „Kategorie“ ist informativ und wird von SISTEMA nicht ausgewertet, aber dokumentiert.

¹ DC = Diagnostic Coverage (Diagnosedeckungsgrad)

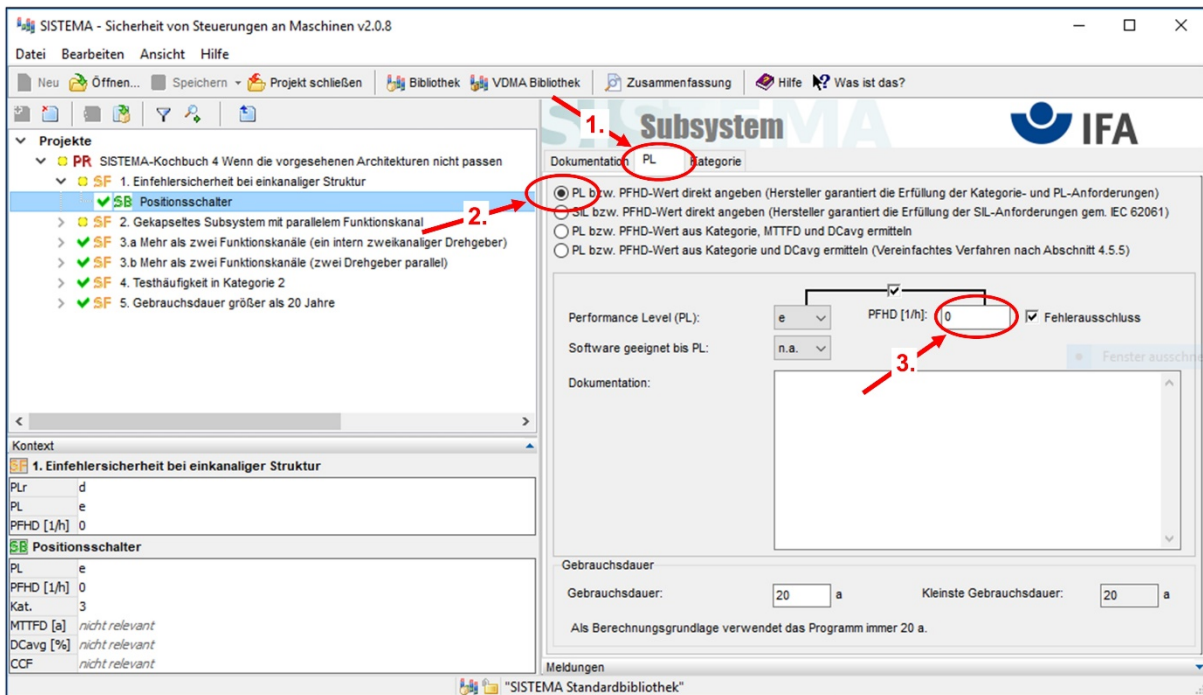
² CCF = Common Cause Failure (Ausfall aufgrund gemeinsamer Ursache)

³ PL = Performance Level

⁴ PFH_D = Probability of a dangerous Failure per Hour (durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde)

Abbildung 2:

Positionsschalter mit Personenschutzfunktion nach Abschnitt 5.2.11.2 der DIN EN 1010-1:2011 als Subsystem mit Fehlerausschluss und $PFH_D = 0$ in SISTEMA



1.3 Hinweise

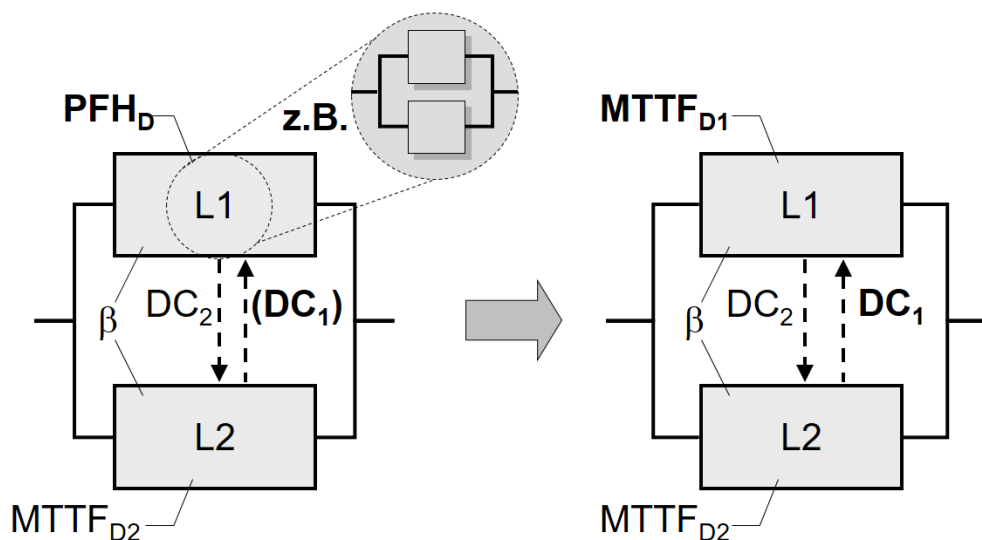
Wenn der PFH_D -Wert „0“ eingetragen wird, setzt SISTEMA aus Gründen der internen Verarbeitung das Häkchen für einen Fehlerausschluss. Ist das Subsystem mit Fehlerausschluss das einzige unterhalb der Sicherheitsfunktion, so weist SISTEMA mit einer gelben Warnmeldung darauf hin, dass die Sicherheitsfunktion 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 bieten hier die Normen DIN EN ISO 13849-1:2016 in 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 werden⁵, steht die für die Berechnung des zweikanaligen Subsystems erforderliche $MTTF_D$ ⁶ nicht zur Verfügung, sondern „nur“ PFH_D und PL (oder SIL⁷). Um trotzdem dieses Subsystem berechnen zu können, muss aus den vom Hersteller angegebenen Werten für PFH_D 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_D näherungsweise auf einen Block L1 mit $MTTF_{D1}$ und DC_1 abgebildet werden kann (siehe Abbildung 3).

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.

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 (mittlere Zeit bis zum gefährbringenden Ausfall)

⁷ SIL = Safety Integrity Level (Sicherheits-Integritätslevel)

2.2 Eingabe in SISTEMA

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

$$MTTF_{D1} = \frac{1}{PFH_D} \quad \text{und} \quad DC_1 = 0 \%$$

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:

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

Abbildung 4 zeigt die Anwendung des Ansatzes in SISTEMA. Das dargestellte Subsystem besteht aus einem Sicherheitsbaustein als gekapseltes Subsystem (mit PL d, und $PFH_D = 3,0 \cdot 10^{-7}/h$, bei Einhaltung der vom Hersteller vorgegebenen maximalen Anzahl von Schaltzyklen) im ersten Kanal und parallel dazu einem Schütz mit Spiegelkontakten im zweiten Kanal.

In Kapitel 3 findet sich ein weiteres Beispiel für die Anwendung mit $DC_1 > 0$.

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

The screenshot shows the SISTEMA software interface for 'Sicherheit von Steuerungen an Maschinen v2.0.8'. The main window displays a project tree on the left and a detailed configuration view on the right. The project tree shows a hierarchy: 'PR SISTEMA-Kochbuch 4 Wenn die vorgesehenen Architekturen nicht passen' -> 'SF 1. Einfehlersicherheit bei einkanaliger Struktur' -> 'SF 2. Gekapseltes Subsystem mit parallelem Funktionskanal' -> 'SB L1 und L2' -> 'CH Kanal 1' -> 'BL L1 Sicherheitsbaustein' and 'CH Kanal 2' -> 'BL L2 Schütz'. The context pane shows parameters for '2. Gekapseltes Subsystem mit parallelem Funktionskanal': PLr: e, PL: e, PFHD [1/h]: 9,2E-8, PL: e, Kat.: 3, MTTFD [a]: 100 (Hoch), DCavg [%]: 64,9 (Niedrig), CCF: 65 (erfüllt).

The main configuration view shows two channels. Channel 1 (Kanal 1) contains a 'BL L1 Sicherheitsbaustein' with MTTFD [a]: 380,5 (Hoch) and DC [%]: 0 (Kein). Channel 2 (Kanal 2) contains a 'BL L2 Schütz' with MTTFD [a]: 200 (Hoch) and DC [%]: 99 (Hoch). Both channels have MTTFD: 100 a and MTTFD-Bereich: Hoch. The interface also includes a menu bar, a toolbar, and a status bar.

2.3 Tipp

Die Bildung des Kehrwerts erledigt SISTEMA selbständig, wenn der PFH_D -Wert in der $MTTF_D$ -Registerkarte in das Feld „Rate gefahrbringender Ausfälle“ eingegeben wird, z. B. entspricht $PFH_D = 3,0 \cdot 10^{-7}/h$ einer Eingabe von 300 FIT (1 FIT = $1,0 \cdot 10^{-9}/h$) und einem $MTTF_D$ -Wert von 380,5 Jahren.

2.4 Hinweise

Bei der Berechnung von $MTTF_D$ als Kehrwert von PFH_D ist generell auf eine **korrekte Umrechnung der Einheiten** zu achten (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_D , 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_D in $MTTF_{D1}$ eingerechnet. Ein weiteres Verwenden der internen Diagnosemaßnahmen innerhalb L1 ist daher nicht mehr möglich, da diese zur Bestimmung der PFH_D bereits „verbraucht“ wurden. Unter diesen Umständen muss zunächst $DC_1 = 0$ angesetzt werden. Dadurch zeigt SISTEMA den Warnhinweis „Bitte prüfen Sie, ob für den erforderlichen PL ein Bauteil mit einem DC von 0% im Einklang mit den Anforderungen der Kategorie 3 in Bezug auf Fehlererkennung steht.“ Dieser Hinweis kann für gekapselte Subsysteme der Kategorie 2, 3 oder 4 ignoriert werden, da diese über interne fehlererkennende Maßnahmen verfügen.

Wird mit dem gesamten Subsystem, das L1 und L2 enthält, eine Kategorie 4 angestrebt, führt die Bedingung DC_{avg} mindestens 99 % (mit Toleranz⁸ reichen 94 %) u. U. zum Scheitern dieses Ansatzes, sofern nicht ein ausreichender DC durch externe Testung von L1 erreicht werden kann.

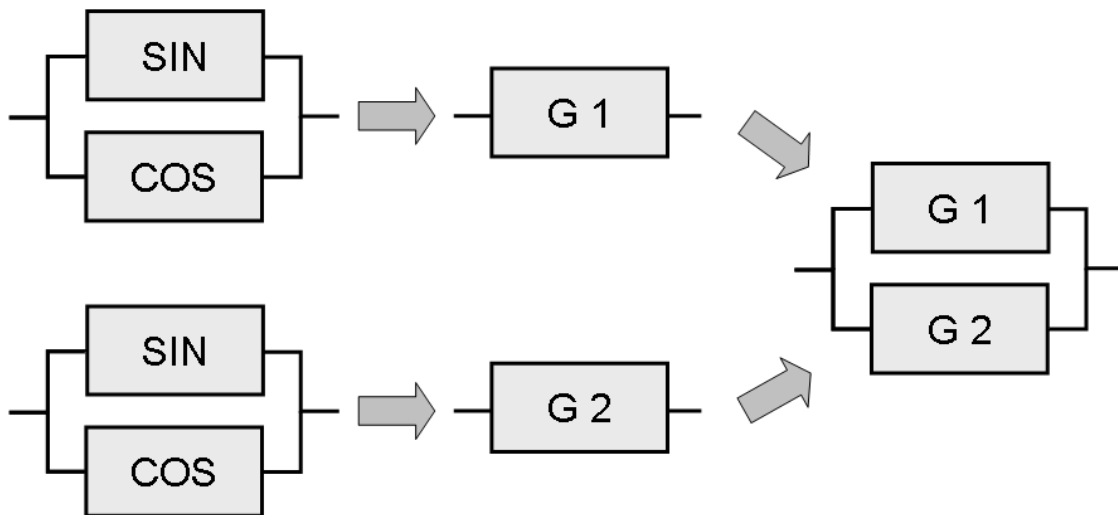
⁸ unter Ausnutzung der 5%-Toleranz nach Tabelle 5 der DIN EN ISO 13849-1

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 so berechnete PFH_D 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



Bei diesem Beispiel wird angenommen, dass die Sicherheitsfunktion allein den Betrag der Geschwindigkeit auswertet, wie z. B. die Funktion „sicher begrenzte Drehzahl“ (SLS nach DIN EN 61800-5-2)

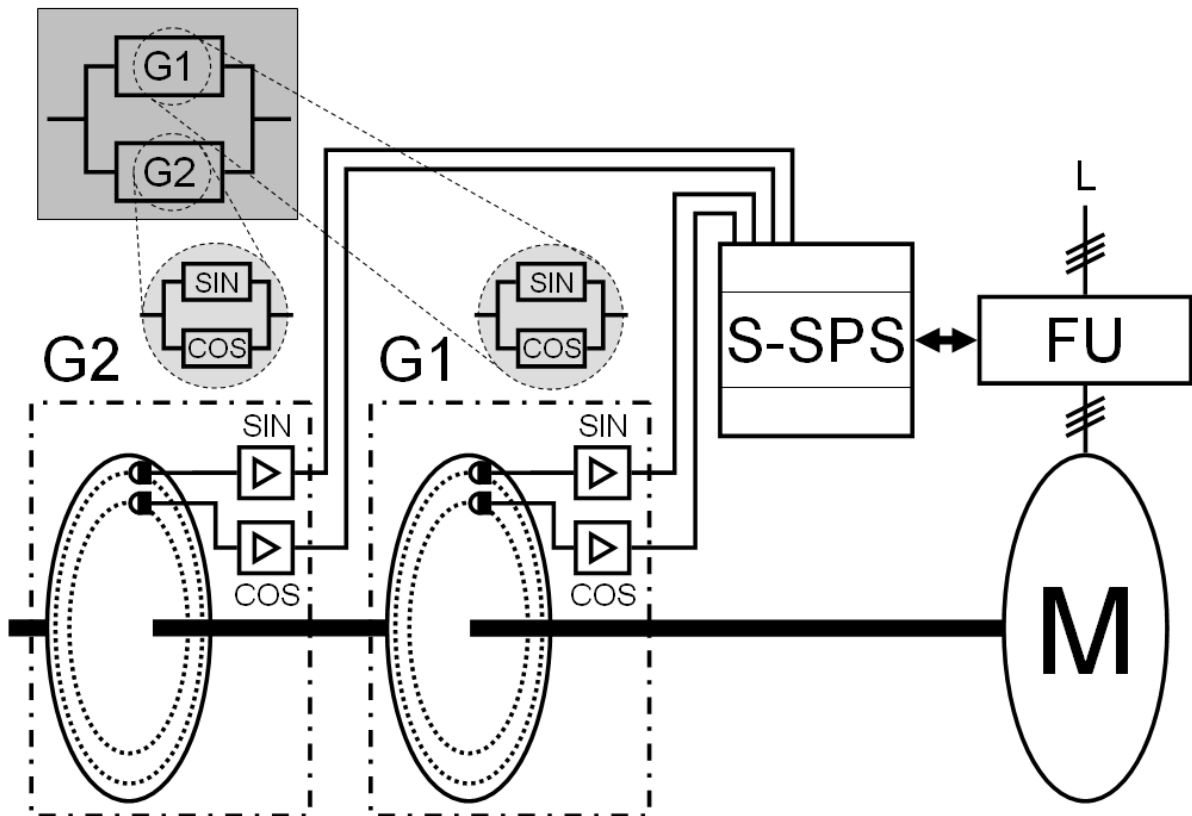
3.2 Eingabe in SISTEMA

Das Verfahren der schrittweisen Zusammenfassung lässt sich am Beispiel für eine vierkanalige Struktur nachvollziehen, wie in Abbildung 6 gezeigt:

Zwei identische Drehgeber G1 und G2 erfassen die Drehzahl derselben Welle und liefern dazu jeweils sin- und cos-Ausgangssignale⁹. 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_D -Beitrag der Geber an der Sicherheitsfunktion zu reduzieren.

⁹ Für positionsbasierte Sicherheitsfunktionen und einige andere Sicherheitsfunktionen ist ein einzelner sin/cos-Drehgeber als einkanaliges System aufzufassen, da die Information (z. B. „Bewegungsrichtung“) nur aus dem Sinus- **und** dem Cosinussignal zusammen gewonnen werden kann.

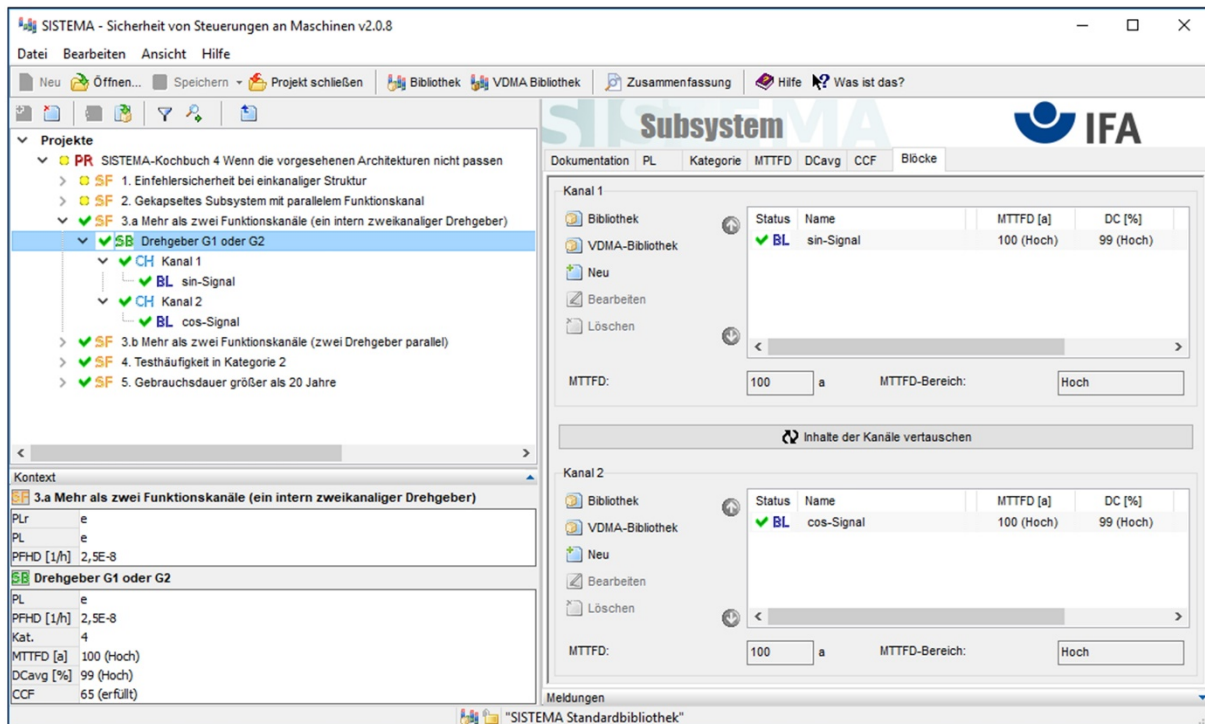
Abbildung 6:
Beispiel für eine vierkanalige Struktur zur Erfassung der Drehzahl



3.3 Erster Schritt

Bei diesem speziellen Beispiel 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_D 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_D -Werte beider Geber betragen jeweils $2,5 \cdot 10^{-8}/h$ und sind das Ergebnis des ersten Schritts (siehe Abbildung 7).

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



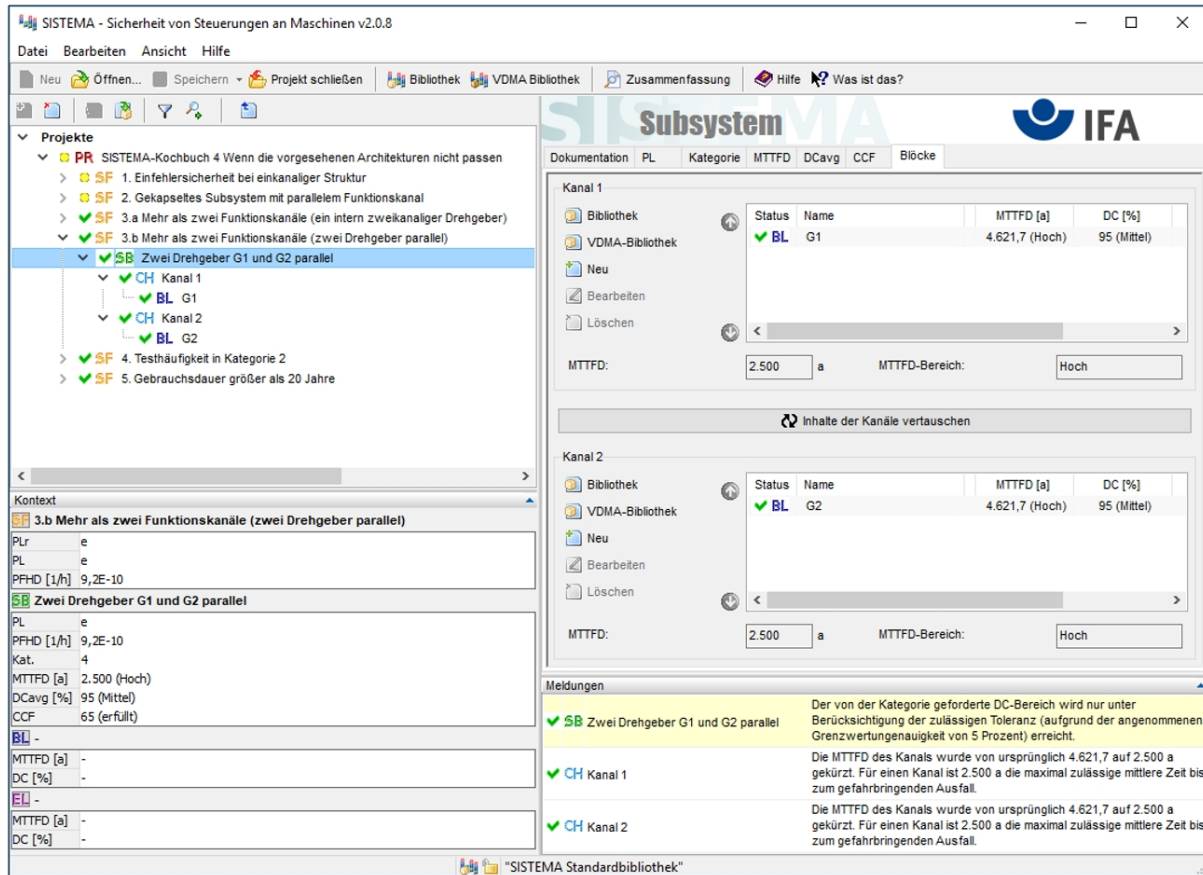
3.4 Zweiter Schritt

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_D des einzelnen Gebers angesetzt ($MTTF_D = 1/PFH_D$). Hier ergeben sich als $MTTF_D$ -Werte für jeden der beiden Geber 4621,7 Jahre, das entspricht dem Kehrwert von $2,5 \cdot 10^{-8}/h$ oder einer Eingabe als „Rate gefahrbringender Ausfälle“ von 24,7 FIT. In SISTEMA muss dazu die Expertenoption „ $MTTF_D$ -Kappung für Kategorie 4 von 2500 auf 100 Jahre absenken“ deaktiviert sein.

Der 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 % konservativ geschätzt (siehe Abschnitt 3.6). Dies erfüllt auch die Anforderungen der im Beispiel angenommenen Kategorie 4 (siehe Abbildung 8).

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_D 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 Gestaltung des Strahlenganges im Sensor bestimmt ist. Es schließt sich eine Aufbereitung der analogen Signale an. Prinzipiell erfolgt die Signalverarbeitung beider Kanäle teilweise innerhalb desselben Schaltkreises. Trotzdem kann die Einfehlersicherheit der Elektronik gewährleistet werden, 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_D 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 Geberhersteller 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 61800-5-2: 2017, Tabelle D.8.

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_D 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 mittleren Anforderungsrate der Sicherheitsfunktion zur Testrate höchstens 1/100 beträgt.

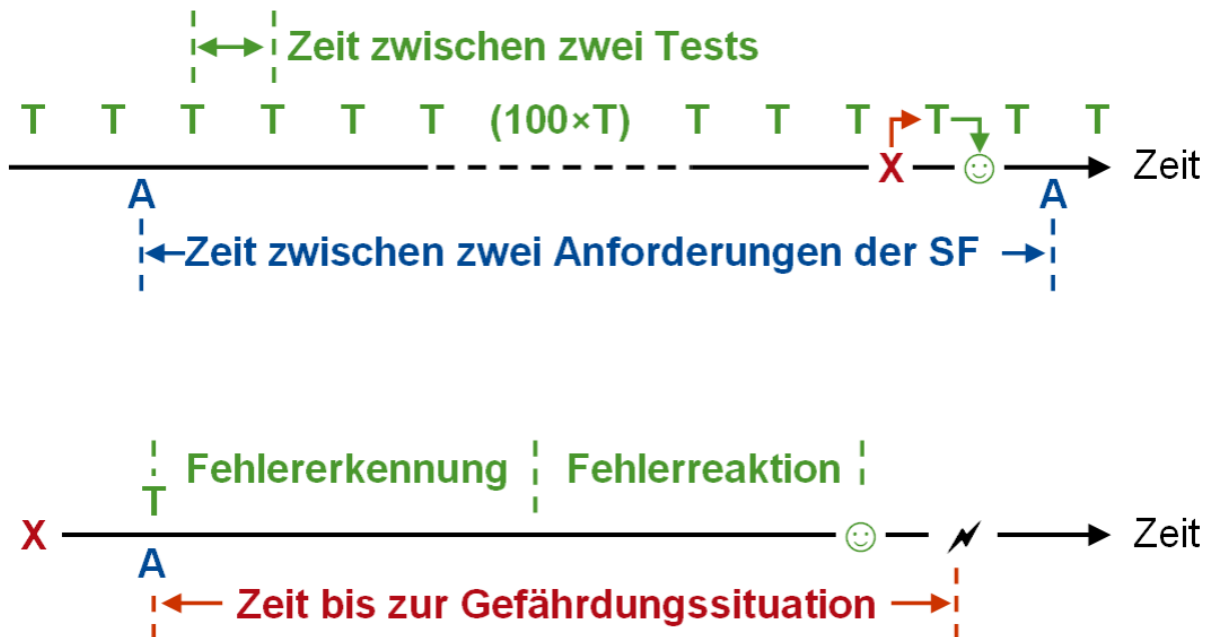
In den folgenden zwei Fällen ist seit der dritten Ausgabe der DIN EN ISO 13849-1 von 2016 eine Abweichung von dieser Regel zulässig:

- Das Verhältnis der Anforderungsrate der Sicherheitsfunktion zur Testrate ist größer als 1/100, aber höchstens 1/25. Dann kann mit einem zehnpromzentigen PFH_D-Zuschlag gerechnet werden (siehe Anmerkung 1 in Anhang K der Norm).
- 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: Anforderungsrate zu Testrate größer als 1/100

Dieser Abschnitt beschreibt den Fall, dass das Verhältnis der Anforderungsrate der Sicherheitsfunktion zur Testrate größer als 1/100 ist, aber höchstens 1/25 beträgt.

Im Subsystem müssen dazu in der Registerkarte „Kategorie“ die Kategorie 2 ausgewählt und unter „Anforderungen der Kategorie“ die Bedingung „Die Anforderungen an die Testhäufigkeit sind erfüllt“ markiert werden. Zusätzlich wird die Bedingung „Reduzierte Testhäufigkeit (1/25)“ ausgewählt. SISTEMA berücksichtigt dadurch den zehnpromzentigen PFH_D-Zuschlag automatisch in der Berechnung.

Abbildung 10 zeigt das Beispiel eines Kategorie-2-Subsystems mit MTTFD_D = 100 Jahre, DC = 90 % und Verhältnis der Anforderungsrate der Sicherheitsfunktion zur Testrate von 1/25. SISTEMA berechnet einen PFH_D-Wert von $2,5 \cdot 10^{-7}/h$ (PL d). Bei einem Verhältnis der Raten von 1/100 ergäbe sich ein PFH_D-Wert ohne Zuschlag in Höhe von $2,3 \cdot 10^{-7}/h$.

Abbildung 10:

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

The screenshot shows the SISTEMA software interface for configuring a subsystem. The main window is titled "Subsystem" and includes the IFA logo. The "Kategorie" tab is selected, showing a table of requirements for Category 2. The "Anforderungen der Kategorie" section has several checkboxes checked, including "Reduzierte Testhäufigkeit (1/25)" and "Die Anforderungen an die Testhäufigkeit sind erfüllt". The "Kontext" panel on the left displays the calculated PFH_D value of 2,5E-7.

Anforderungen der Kategorie	Status
Reduzierte Testhäufigkeit (1/25)	<input checked="" type="checkbox"/>
Übereinstimmung mit zutreffenden Normen, um zu erwartenden Einflüssen standzuhalten.	<input checked="" type="checkbox"/>
Grundlegende Sicherheitsprinzipien werden angewendet.	<input checked="" type="checkbox"/>
Bewährte Sicherheitsprinzipien werden angewendet.	<input checked="" type="checkbox"/>
Die Anforderungen an die Testhäufigkeit sind erfüllt.	<input checked="" type="checkbox"/>
MTTFD ist mindestens Niedrig oder Mittel oder Hoch. [100 (Hoch)].	<input checked="" type="checkbox"/>
DCavg ist mindestens Niedrig oder Mittel. [90 (Mittel)].	<input checked="" type="checkbox"/>
Die MTTFD des Testkanals ist größer oder gleich der Hälfte der MTTFD des getesteten Systems.	<input checked="" type="checkbox"/>
Der erreichte Punktestand der CCF-Bewertung beträgt mindestens 65. [65 (erfüllt)].	<input checked="" type="checkbox"/>

Kontext

4. Testhäufigkeit in Kategorie 2

PLr d

PL d

PFHD [1/h] 2,5E-7

Kategorie-2-Subsystem

PL d

PFHD [1/h] 2,5E-7

Kat. z

MTTFD [a] 100 (Hoch)

DCavg [%] 90 (Mittel)

CCF 65 (erfüllt)

Meldungen

SB Kategorie-2-Subsystem Die reduzierte Testhäufigkeit (Anforderungsrate \leq 1/25 der Testrate) ist aktiv. Der PFHD Wert wird mit dem Faktor 1,1 multipliziert als Abschätzung zur sicheren Seite.

4.3 Hinweise zu Fall 1

Durch Markov-Modellierung kann die Erhöhung der Ausfallwahrscheinlichkeit in Abhängigkeit vom Verhältnis der Anforderungsrate zur Testrate berechnet werden. Bei einem Verhältnis von höchstens 1/25 beträgt der unter den ungünstigsten Bedingungen gültige maximale relative PFH_D-Aufschlag ca. 10 %. Der relative Aufschlag bezieht sich auf den mit SISTEMA ermittelbaren PFH_D-Wert des Kategorie-2-Subsystems mit optimalem Verhältnis der Anforderungsrate zur Testrate von 1/100 oder kleiner.

4.4 Fall 2: Fehlererkennung bei Anforderung der Sicherheitsfunktion

Dieser Abschnitt beschreibt den Fall, dass die Fehlererkennung und Fehlerreaktion durch die Anforderung der Sicherheitsfunktion ausgelöst werden und beide zusammen schneller erfolgen als das Eintreten der Gefährdungssituation.

In SISTEMA kann in der Registerkarte „Kategorie“ eines Kategorie-2-Subsystems unter „Anforderungen der Kategorie“ die Bedingung „Die Anforderungen an die Testhäufigkeit sind erfüllt“ auch dann 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 zu Fall 2

Abbildung 9 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 in Abschnitt 4.5.4 der DIN EN ISO 13849-1:2016 genannt. Passende Schaltungsbeispiele sind im IFA Report 2/2017, 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, 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.

5 Gebrauchsdauer größer als 20 Jahre

5.1 Beschreibung

Soll die Gebrauchsdauer eines SRP/CS 20 Jahre überschreiten, so verlieren die nach dem vereinfachten Verfahren (Anhang K der Norm) ermittelten PFH_D -Werte für Kategorie 2, 3 und 4 ihre Grundlage. Unter Umständen kann diese Situation mit wenigen Nachbesserungen trotzdem im Rahmen des vereinfachten Verfahrens behandelt werden. Es ist aber nicht sinnvoll, die Gebrauchsdauer über 30 Jahre hinaus zu verlängern. Dabei sind zwei Fälle zu unterscheiden.

5.2 Fall 1: Gebrauchsdauer von vornherein größer als 20 Jahre spezifiziert

Im ersten Fall ist das SRP/CS von vornherein für eine Gebrauchsdauer größer als 20 Jahre spezifiziert. Dann kann der Einfluss der höheren Gebrauchsdauer aus den Markov-Modellen, die Anhang K der Norm zugrunde liegen, zur sicheren Seite hin folgendermaßen abgeschätzt werden: Pro fünf Jahre längere Gebrauchsdauer als 20 Jahre wird bei den Kategorien 2, 3 und 4 ein prozentualer PFH_D -Zuschlag von 15 % eingerechnet (Kategorie B oder 1 erfordern keine PFH_D -Anpassung). Das vereinfachte Verfahren und SISTEMA sind also trotzdem nutzbar. Voraussetzung sind konstante Ausfallraten unabhängig von der Gebrauchsdauer. Für Verschleißbauteile bedeutet dies, dass diese nach Ablauf der zulässigen Betriebszeit T_{10D} jeweils vorsorglich ausgetauscht oder für die spezifiziertere höhere Gebrauchsdauer T_M ausgelegt werden müssen ($T_{10D} \geq T_M$).

5.3 Fall 2: Nachträgliche Verlängerung der Gebrauchsdauer

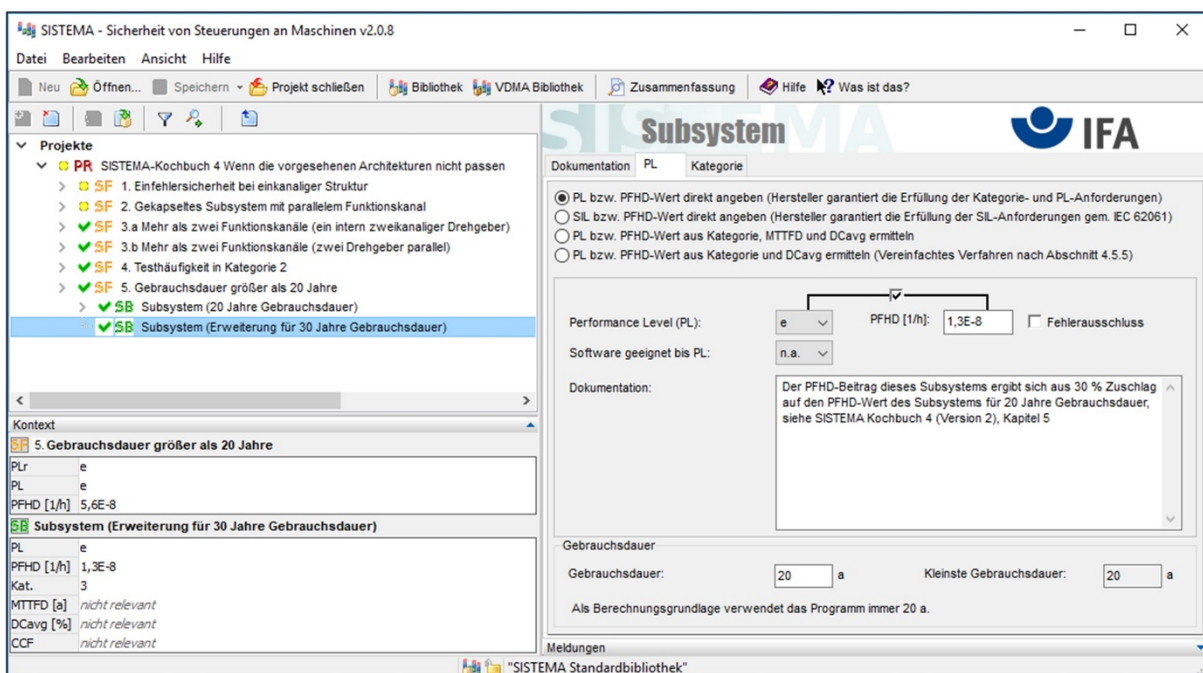
Im zweiten Fall war das SRP/CS ausgelegt für 20 Jahre Gebrauchsdauer, soll aber nun darüber hinaus weiterverwendet werden. Dann kann die aus der Markov-Modellierung zu erwartende PFH_D -Verschlechterung mit einem wie im ersten Fall beschriebenen Zuschlag abgeschätzt werden. Kritisch wird es bei enthaltenen Verschleißbauteilen oder sich durch Alterung verschlechternden Bauteilen, zu denen typischerweise „chemische“ Bauteile (z. B. „nasse“ Elektrolytkondensatoren, Batterien, elektrochemische Sensoren), mechanische Bauteile (z. B. Bremsen, Kupplungen), elektromechanische Bauteile (z. B. Schalter, Relais, Schütze), fluidtechnische Bauteile (z. B. Ventile) und manche optischen Bauteile (z. B. Optokoppler) gehören. Hier kann der Betreiber der Maschine in der Regel nicht selbst beurteilen, ob alle enthaltenen Bauteile auch für eine verlängerte Gebrauchsdauer ausgelegt sind oder welche Maßnahmen, z. B. vorsorglicher Austausch einzelner Bauteile, Proof-Test usw., in diesem Fall durchzuführen sind. Eine Verlängerung der Gebrauchsdauer – bei o. g. PFH_D -Zuschlag – kann dann nur erfolgen, wenn Herstellerangaben darüber vorliegen, was bei einer Verlängerung der Gebrauchsdauer zu tun ist, und wenn diese Maßnahmen vom Betreiber umgesetzt werden.

5.4 Eingabe in SISTEMA

In SISTEMA kann ein erforderlicher fünfzehnprozentiger PFH_D -Zuschlag pro fünf Jahre Verlängerung der Gebrauchsdauer folgendermaßen umgesetzt werden: Der PFH_D -Wert des

Subsystems, dessen Gebrauchsdauer mehr als 20 Jahre betragen soll, wird wie üblich auf Basis von Kategorie, $MTTF_D$ und DC_{avg} ¹⁰ durch SISTEMA berechnet. Dabei wird als Gebrauchsdauer 20 Jahre angegeben. Anschließend wird in demselben Projekt ein zweites Subsystem angelegt, dessen PL und PFH_D -Wert direkt angegeben werden, wie in Abbildung 11 dargestellt. Hier wird der händisch ermittelte PFH_D -Zuschlag nach dem oben beschriebenen Ansatz als PFH_D -Wert eingetragen und als Gebrauchsdauer ebenfalls 20 Jahre gewählt. Der Haken für die Verbindung zwischen PFH_D und PL sollte dabei gesetzt bleiben. Unter dem Reiter „Kategorie“ kann die gleiche Kategorie angegeben werden wie bei dem ursprünglichen Subsystem. Auf die erhöhte Gebrauchsdauer kann in beiden Subsystemen in den Dokumentationsfeldern im Reiter PL hingewiesen werden.

Abbildung 11:
SISTEMA-Screenshot zur Gebrauchsdauer von 30 Jahren



¹⁰ DC_{avg} = average Diagnostic Coverage (durchschnittlicher Diagnosedeckungsgrad)