Wenn die vorgesehenen Architekturen nicht passen

Version 1.0 (DE)
Einleitung


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


1.2 Eingabe in SISTEMA


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

SISTEMA-Kochbuch 4 (Version 1.0 DE) - 5 -
1.3 Hinweise

2 Gekapseltes Subsystem mit parallelem Funktionskanal

2.1 Beschreibung

Wenn in einem Kanal einer zweikanaligen Struktur gekapselte Subsysteme eingesetzt werden, steht die für die Berechnung des zweikanaligen Subsystems erforderliche MTTFₐ nicht zur Verfügung, sondern „nur“ PFH und PL (oder SIL). Um trotzdem dieses Subsystem berechnen zu können, muss aus den vom Hersteller angegebenen Werten für PFH und PL ersatzweise die entsprechende MTTFₐ 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 MTTFₐ₁ und DC₁ abgebildet werden kann.

Abbildung 3: Überführung eines gekapselten Subsystems L₁ in einen Block


2.2 Eingabe in SISTEMA

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

$$MTTF_{d_1} = \frac{1}{PFH} \quad \text{und} \quad DC_1 = 0 \%$$

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 MTTFₐ = Mean Time To dangerous Failure

7 SIL = Safety Integrity Level

SISTEMA-Kochbuch 4 (Version 1.0 DE)
Nur wenn von außen, z. B. durch L2, Fehler im gekapselten Subsystem L1 erkannt werden, kann ein entsprechend höherer Wert für DC\textsubscript{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 (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.

Kapitel 3 zeigt die Anwendung mit DC\textsubscript{1} > 0 an einem weiteren Beispiel.

2.3 Tipp

Die Bildung des Kehrwerts erledigt SISTEMA selbständig, wenn der PFH-Wert in der MTTF\textsubscript{d}-Registerkarte in das Feld „Rate gefahrbringerer 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\textsubscript{d}-Wert von 380,5 Jahren.

2.4 Hinweise

Bei der Berechnung von MTTF\textsubscript{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\textsubscript{a1} 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\textsubscript{1} = 0 angesetzt werden. Wird mit dem gesamten Subsystem, das L1 und L2 enthält, eine Kategorie 4 angestrebt, führt die Bedingung DC\textsubscript{avg} mindestens 99 % (mit Toleranz\textsuperscript{8} reichen 94 %) u. U. zum Scheitern dieses Ansatzes, sofern nicht ein ausreichender DC durch externe Testung erreicht werden kann.

\textsuperscript{8} unter Ausnutzung der 5-%-Toleranz nach Tabelle 6 der Norm
3 Mehr als zwei Funktionskanäle

3.1 Beschreibung


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:

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 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.
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 gefährbringender 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\(^9\).


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


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-

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


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


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

4.3 Hinweise

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


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.