7 Entwerfen und Entwickeln eines Teilsystems

7.1 Allgemeines

Das Teilsystem ist in Übereinstimmung mit seiner Spezifikation der Sicherheitsanforderungen (siehe 5.2) zu entwerfen, einschließlich grundsätzlich: …

SRS → Strukturierte Anforderungen basierend auf einer Sicherheitsfunktion

Bei der Spezifikation jeder Sicherheitsfunktion sind zu betrachten:

- die Spezifikation der funktionalen Anforderungen und
- die Spezifikation der Anforderungen zur Sicherheitsintegrität.

5.2

Diese mussten in der Spezifikation der Sicherheitsanforderungen (SRS, en: safety requirement specification) bereits dokumentiert werden bzw. zur Verfügung gestellt worden sein.

5.2.2

Für ein Teilsystem heißt das, dass diese Informationen heruntergebrochen werden müssen, sodass die Gesamtheit aller Teilsysteme, die an einer Ausführung einer Sicherheitsfunktion (SCS) beteiligt sind, korrekt entworfen und entwickelt werden können.

Funktionale Beschreibung für ein Teilsystem ist das A und O

Erst danach kann quantitativ und qualitativ nachgedacht werden

Die Tabelle 5 listet aus der Praxis-Brille strukturiert und sortiert alle notwendigen Informationen auf, die als Eingangsinformationen unerlässlich sind.

Folgende sind dabei besonders hervorzuheben:

- die Bedingung(en) (z. B. Betriebsart) der Maschine;
- die Priorität derjenigen Funktionen, die gleichzeitig aktiv sein können und die in Widerspruch stehende Aktionen auslösen können;
- die erforderliche Reaktionszeit der Sicherheitsfunktion;

- die Schnittstelle(n) des SCS und des Teilsystems zu anderen Maschinenkomponenten bzw. -funktionen;
- eine Beschreibung der Betriebsumgebung;
- Tests und alle zugehörigen Einrichtungen (wie z. B. *DC*).

7.2 Entwurf der Teilsystemarchitektur

Die Architektur eines Teilsystems wird durch einen Prozess der funktionalen Zerlegung definiert, der dem Prozess der vollständigen Sicherheitsfunktion ähnlich ist, der zur Architektur des SCS führt – siehe 6.3.2: Die spezifische Teilfunktion des Teilsystems kann in Teilfunktionen der nächstniedrigeren Ordnung zerlegt werden, die dann den Elementen des Teilsystems zugeordnet werden. […]

[…] Wenn ein Teilsystementwurf eine so komplexe Komponente als Teilsystem-Element enthält, kann sie im Zusammenhang mit einem Teilsystementwurf als ein Element mit geringer Komplexität betrachtet werden, da ihre relevanten Ausfallmodi, das Verhalten bei Erkennung eines Fehlers, die Ausfallrate und andere sicherheitsrelevante Informationen bekannt sind. […]

(Sicherheits-)Teilfunktionen → Teilsysteme

6.3 Die Sicherheitsfunktion wurde bereits in Abschnitt 6 in Teilfunktionen zerlegt.

Das führt dazu, dass jedes Teilsystem hinsichtlich Teilsystem-Elemente weiter betrachtet wird: Zum Beispiel eine Schutztürüberwachung für SIL 1 bedarf nur eines einzelnen Positionsschalters. Dagegen ist für SIL 2 oder SIL 3 eine Zweikanaligkeit gefordert.

SIL 1 + SIL 2 = SIL 3
Komplexes Teilsystem-Element trifft nicht-komplexes Teilsystem-Element

7.4.1

Leistungsschütz (oder Leistungsschalter) **SIL 1**
B_{10D}
Betätigungszyklus C = 12 [1/h]
(nicht komplexes Bauteil)

$$\rightarrow \lambda_{D1} = 0{,}1 \frac{C}{B_{10D}}$$

Sicherheitsbezogener Frequenzumrichter **SIL 2**
PFH = 2E–07
(komplexer Entwurf und Prüfung nach DIN EN 61800-5-2 (**VDE 0803-2**))

$\rightarrow \lambda_{D2} \approx PFH$

SIL 3

Anmerkung 4: In diesem Dokument wird davon ausgegangen, dass der Entwurf komplexer programmierbarer elektronischer Teilsysteme oder Teilsystem-Elemente den relevanten Anforderungen der DIN EN 61508 (**VDE 0803**) entspricht und die Route 1H verwendet (siehe DIN EN 61508-2 (**VDE 0803-2**):2011-02, Abschnitt 7.4.4.2). […]

Anwendungsbereich

Komplexe programmierbare elektronische Komponenten – „Out of Scope"

Oder wie bereits im Anwendungsbereich beschrieben: „Der Entwurf komplexer programmierbarer elektronischer Teilsysteme oder Teilsystem-Elemente fällt nicht in den Anwendungsbereich dieses Dokuments. Dies fällt in den Anwendungsbereich der DIN EN 61508 (**VDE 0803**) oder damit verbundener Normen".

Warum? ASICs, FPGAs und Embedded Software mit einer nicht-sicherheitsbezogenen Entwicklungsumgebung machen das Ganze recht kompliziert und lässt sich nicht mehr nur auf einfache Basis Teilsystemarchitekturen reduzieren. Hier potenziert sich die Komplexität und ganz ehrlich: Wer würde selber Windows 10 neu programmieren, in der Hoffnung Kosten und Zeit zu sparen?

„Route 1H“ übrigens bedeutet, dass rechnerisch und systematisch nachgewiesen werden muss, ob ein gewünschter SIL auch erreicht wurde. „Route 2H“ erlaubt über statistische Auswertungen dieses Entwurfsszenario „abzukürzen“ – jedoch streiten die Verfasser der DIN EN 61508 (**VDE 0803**) über Sinn und Unsinn von Statistik in diesem Zusammenhang.

Die banale Erkenntnis für den pragmatischen Maschinenhersteller lautet: Funktionale Sicherheit in der heutigen Ausprägung ist herausfordernd genug und der Aufwand soll minimiert werden – ohne dabei die Schutzziele aus den Augen zu verlieren.

7.3 Anforderungen für die Auswahl und den Entwurf von Teilsystemen und Teilsystem-Elementen

7.3.1 Allgemeines

Es gibt zwei Arten von Anforderungen an Teilsysteme und Teilsystem-Elemente:

- qualitative Anforderungen: systematische Integrität; Fehlerbetrachtung(en) und Fehlerausschluss(e);
- quantitative Anforderungen: Ausfallrate und andere relevante Parameter. […]

Qualität trifft Quantität – systematische Anforderungen und Ausfallraten

6.4

Was auf SCS-Ebene, also Systemebene gilt, muss auch auf der Teilsystemebene berücksichtigt werden. Das Top-Down-Verfahren spiegelt sich in den Anforderungen des Abschnitts 7.3 wider und sind gedanklich identisch mit denen des Abschnitts 6.4 zu verstehen.

7.3.2 Systematische Integrität

7.3.2.1 Allgemeines

Die systematischen Anforderungen an die Sicherheitsintegrität eines Teilsystems werden durch Erfüllung der Anforderungen in den Abschnitten 7.3.2.2 und 7.3.2.3 erfüllt und sind für SIL 1, SIL 2 und SIL 3 gleich.

7.3.2.2 Anforderungen zur Vermeidung von systematischen Ausfällen

6.5.1

Auf Ebene des Teilsystems
Vermeiden* ist besser, als im Nachhinein versuchen zu *beherrschen

Die folgenden Maßnahmen müssen in der Praxis insbesondere angewendet werden:

- korrekte (geeignete) Auswahl und korrekte Dimensionierung, Kombination, Anordnungen, Zusammenbau und Installation von Teilsystemen, einschließlich Verkabelung;
- das Teilsystem ist gemäß DIN EN 60204-1 (**VDE 0113-1**), Abschnitt 7.2 zu „schützen".
- Beachtung der Anwendungshinweise des Komponentenherstellers, z. B. Katalogangaben, und Anwendung bewährter Betriebspraxis/-erfahrung (siehe auch DIN EN ISO 13849-2, Anhang D.1);
- Verwendung von Teilsystemen, die vergleichbare Eigenschaften haben (siehe auch DIN EN ISO 13849-2, Anhang D.1);

Und nicht zu vergessen – Augenkontakt zur Realität behalten:
Der Hardwareentwurf muss überprüft werden,

- durch Inspektion (oder Begehung);
- um etwaige Unterschiede zwischen der Spezifikation und der Implementierung (mittels dieser Überprüfungen) aufzudecken;

7.3.2.3 Anforderungen an die Beherrschung von systematischen Ausfällen

…

6.5.2

Die folgenden Maßnahmen müssen in der Praxis insbesondere angewendet werden:

- bei einer Energieabschaltung, d. h. bei Verlust der elektrischen Versorgung, muss ein sicherer Zustand der Maschine erreicht oder beibehalten werden;
- bei vorübergehender Teilsystemausfälle, z. B. ein Spannungsausfall usw. (z. B. unerwarteter Anlauf eines Motors) oder eine elektromagnetische Beeinflussung an einem einzelnen Teilsystem, dürfen nicht zu einer Gefährdungssituation führen;

- Beherrschung der Auswirkungen von Fehlern und anderer Effekte, die von einem Datenkommunikationsprozess ursächlich entstehen können (siehe DIN EN 61508-2 (**VDE 0803-2**));
- wenn an einer Schnittstelle ein gefahrbringender Fehler auftritt, muss die Fehler-Reaktion erfolgen, bevor die Gefährdung durch diesen Fehler auftreten kann. Dabei sind Schnittstellen alle Eingänge und Ausgänge der Teilsysteme und alle anderen Einheiten von Teilsystemen, die während der Integration einer Verkabelung bedürfen, z. B. die Ausgangsschaltelemente eines Lichtvorhangs oder der Ausgang eines Positionsschalters einer Schutztürüberwachung;
- PELV/SELV-Stromversorgung (siehe DIN VDE 0100-410) zwecks Beherrschens einer möglichen Überspannung.

7.3.2.4 Elektromagnetische Störfestigkeit

Bei der Auslegung des Teilsystems sind die Anforderungen von 6.6 zu berücksichtigen.

7.3.2.5 Security Aspekte

Bei der Auslegung des Teilsystems sind die Anforderungen in 6.8 zu berücksichtigen.

Kein Unterschied zu 6.6 und 6.8, daher nur ein Verweis

6.6
6.8

Was auf SCS-Ebene, also Systemebene gilt, muss auch auf der Teilsystemebene berücksichtigt werden: Manchmal reicht dazu ein einfacher Verweis in einer Norm.

7.3.3 Fehlerbetrachtung und Fehlerausschluss

7.3.3.1 Allgemeines

Alle Teilsysteme-Elemente müssen so ausgelegt sein, dass die geforderte Spezifikation der Sicherheitsanforderungen erreicht wird. Die Fähigkeit, Fehlern zu widerstehen, muss bewertet werden. Sofern nicht ausdrücklich anders angegeben, gelten die Anforderungen dieses Abschnitts 7 unabhängig von der geforderten Sicherheitsintegrität der Sicherheitsfunktion. […]

7.3.3.2 Berücksichtigung von Fehlern

…

7.3.3.3 Fehlerausschluss

Es ist nicht immer möglich, Teilsysteme zu bewerten, ohne davon auszugehen, dass bestimmte Fehler ausgeschlossen werden können. Fehlerausschluss ist ein Kompromiss zwischen technischen Sicherheitsanforderungen und der theoretischen Möglichkeit des Auftretens eines Fehlers. […]

6.4

Fehlerausschlüsse werden in der Praxis für Verdrahtung gemacht – für manche Teilsystem-Elemente kann das auch Sinn ergeben

Das Konzept der DIN EN ISO 13849-1, Komponenten in „Mechanik“ und „Elektrik“ aufzuteilen ist theoretisch korrekt – praktisch, aber sehr verwirrend.

Beispiele: Mit zwei Positionsschaltern oder zwei Leistungsschützen soll mindestens SIL 2 oder PL d erreicht werden – also jeweils eine zweikanalige Architektur mit zwei gleichartigen Kanälen. Gedanklich werden diese Komponenten nun „zerlegt“:

		„Mechanik“		„Elektrik“
Positionsschalter	=	mechanisch betätigtes Element (der Stößel und die interne Mechanik bis hin zu dem elektrischen Kontakt) B_{10D} = 10 000 000	+	zwangsöffnender (elektrischer) Kontakt Fehlerausschluss
Anmerkung: Zwar ist ein zwangsöffnender Kontakt wie ein Fehlerausschluss zu betrachten, aber die Mechanik hat trotzdem einen B_{10D}-Wert. Erkenntnis: Die Mechanik bestimmt den B_{10D}-Wert maßgeblich.				
Leistungsschütz	=	Hauptstrombahnen und elektrische Spule B_{10D} = 1 300 000	+	Spiegelkontakte Fehlerausschluss
Anmerkung: Die Spiegelkontakte werden für die Diagnose eingesetzt, und deren Versagen kann ausgeschlossen werden. Das würde einen *DC* = 100 % oder besser einer Diagnosefähigkeit von 100 % rechtfertigen – *DC* = 99 % wird aber max. angenommen. Dagegen wird der B_{10D}-Wert durch die Hauptkontakte und die damit verbundene Mechanik bestimmt. Erkenntnis: Die Mechanik bestimmt den B_{10D}-Wert maßgeblich, Spiegelkontakte können zu Diagnosezwecke verwendet werden.				

Wie hilfreich ist jetzt die gedankliche Zerlegung für den Anwender? **Gar nicht.**

Es sei denn, man ist Hersteller einer Komponente und muss seinem Kunden einen B_{10D}-Wert liefern. Zudem wird hier ein Fehlerausschluss bei Leistungs-

schützen gemacht, der die Diagnosefunktion betrifft, und bei Positionsschaltern einen internen Aufbau, der nach „außen“ überhaupt nicht sichtbar ist, weil dieser Positionsschalter bei Hersteller *X* gekauft wurde und als Blackbox zu betrachten ist. Übrigens gilt das auch für jedes Leistungsschütz: Im Grunde kann es egal sein, was da „innerlich“ verbaut wurde, solange der Hersteller mir sagt, dass es sich um ein Leistungsschütz gemäß Produktnorm handelt und ich diese überwachen kann (Anmerkung: Die Produktnorm verlangt bereits nach diesen Spiegelkontakten, und unabhängig von funktionaler Sicherheit – weil es keine „sicheren“ Leistungsschütze geben kann).

Anhang E

Extrem gefährlich und kontraproduktiv – Fehleranhäufungen wegen CCF

Der Begriff „Fehleranhäufung“ ist im ersten Augenblick schwer einzuordnen – *DC* < 100 % widerspricht dem. Wie also den Begriff verstehen?

Betrachtet man die Definition der Kategorien der DIN EN ISO 13849-1, dann wird der Unterschied zwischen Kategorie 3 und Kategorie 4 mit der Anhäufung unerkannter Fehler argumentiert. Bei Kategorie 3 dürfen diese Fehler sich anhäufen, bei Kategorie 4 nicht.

Kategorie 3 (*DC* ≥ 60 %), Systemverhalten: Die Sicherheitsfunktion bleibt beim Auftreten einzelner Fehler immer erhalten. Einige, aber nicht alle Fehler werden erkannt. *Eine Anhäufung von unerkannten Fehlern kann zum Verlust der Sicherheitsfunktion führen.*

Normentext: „… SRP/CS der Kategorie 3 müssen so gestaltet werden, dass ein einzelner Fehler in einem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt. Wenn immer in angemessener Weise durchführbar, muss ein einzelner Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden. …“

Kategorie 4 (*DC* ≥ 99 %), Systemverhalten: Wenn Fehler auftreten, bleibt die Sicherheitsfunktion immer erhalten; die Fehler werden *rechtzeitig* erkannt. *Die Erkennung von Fehleranhäufungen reduziert die Wahrscheinlichkeit des Verlustes der Sicherheitsfunktion (hoher DC).* Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern. […]“

- Normentext: „… SRP/CS der Kategorie 4 müssen so gestaltet werden, dass ein einzelner Fehler in jedem dieser sicherheitsbezogenen Teile nicht zum Verlust der Sicherheitsfunktion führt, und
- der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt wird, z. B. unmittelbar, beim Einschalten oder am Ende eines Maschinenzyklus, aber wenn diese Erkennung nicht möglich ist, dann darf die Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen. […]“

Wenn ein *DC* < 100 % ist, dann heißt das, dass es immer mindestens *x* % unerkannte Fehlergeben wird. Nur mit *DC* = 100 % kann es keine unerkannten Fehler geben und damit auch keine Fehleranhäufung. Und wie jetzt mit „Fehleranhäufung“ in der Praxis umgehen? Die Definition der Kategorie 4 ist offensichtlich nicht vereinbar mit *DC* ≥ 99 % – da es ≤ 1 % unerkannte Fehler per Definition immer existieren werden.

Die Frage muss also lauten: Wenn dies bekannt ist, worauf bezieht sich dann die Fehleranhäufung?

Ein einfaches konkretes Beispiel: Zwei Positionsschalter sollen eine Kategorie 4 Architektur bilden, weil ein *DC* = 99 % möglich ist. Sobald beide Positionsschalter gleichzeitig ausfallen, redet man von Fehleranhäufung, genauer Anhäufung unerkannter Fehler.

Würde es mit *DC* = 100 % auch eine Fehleranhäufung geben können? Ja.

Anhang E

Weil die Diagnose selbst mit *DC* = 100 % erst dann stattfinden kann, wenn die Stößel der beiden Positionsschalter gezwungen werden die zwangsöffnenden Kontakte zu betätigen, heißt: Erst wenn die Schutztüre geöffnet wird, erst dann kann festgestellt werden, ob ein Fehler vorliegt – vorher geht das leider nicht.

Dass eine Fehleranhäufung unwahrscheinlicher wird, je größer ein *DC* ist – das leuchtet einem dann auch wiederum ein.

Dass aber mit *DC* = 100 % es zu einer Fehleranhäufung kommen kann ist sehr verwirrend, aber damit erklärbar, dass die Diagnose einen Diagnose-Testintervall hat, der nicht beliebig klein ist. Und weil Diagnose selbst mit einem beliebig kleinen Diagnose-Testintervall nur zu gewissen Zeitpunkt auch Sinn macht: Die Sicherheits-SPS kann im *ms-Takt* die Eingänge der Positionsschalter überwachen, aber es kommt erst zu einem Signalwechsel, wenn die Schutztüre, z. B. stündlich durch den Bediener geöffnet wird.

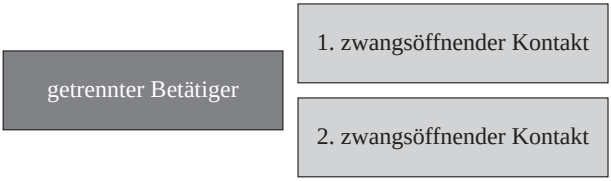
Erkenntnis für die Praxis: Fehleranhäufung immer mit CCF bewerten und somit systematisch betrachten (siehe Anhang E)

Begrenzung: Bei einigen Anwendungen wird nicht erwartet, dass alle Ausfälle mit ausreichender Sicherheit für SIL 3 ausgeschlossen werden können. Die folgende nicht erschöpfende Liste gibt einen Hinweis auf (nicht bereits entworfene und geprüfte) Teilsysteme mit einer Hardware-Fehlertoleranz von null und wo Fehlerausschlüsse auf Fehler angewendet wurden, die zu einem gefährlichen Ausfall führen könnten, bei denen ein Maximum von SIL 2 angemessen sein kann, sofern eine ausreichende Begründung gegeben wird:

- Positionsschalter mit mechanischen Aspekten mit *HFT* von 0;
- Leckage eines fluidtechnischen Ventils (wobei Leckage ein gefährlicher Fehler ist).

[…]

Es gibt ein anschauliches Beispiel aus der Praxis, das diese Begrenzung in der Norm verdeutlicht: Ein Positionsschalter mit getrenntem Betätiger und zwei elektrischen zwangsöffnenden Kontakten.



Die Mechanik ist einkanalig und die Elektrik zweikanalig. Dieses Teilsystem kann nicht SIL 3 erreichen, nur, weil eine Zweikanaligkeit auf der elektrischen Seite vorhanden ist. Der einkanalige getrennte Betätiger begrenzt hier den erreichbaren SIL, nämlich SIL 2 aufgrund des Fehlerausschlusses für den getrennten Betätiger: Das Versagen des getrennten Betätigers ist fatal und dieses Risiko möchte man SIL 3 nicht zumuten.

7.3.3.4 Funktionsprüfung zur Erkennung von Fehleranhäufungen und unentdeckten Fehlern

In einem redundanten System kann eine Anhäufung von Fehlern im Laufe der Zeit zu einem Verlust der Sicherheitsfunktion führen. In einem einkanaligen System können unerkannte Fehler ebenfalls zu einem Verlust der Sicherheitsfunktion führen.

Bei zwei Fehlern bzw. Ausfällen ist Schluss mit lustig

7.4
Anhang E
Anhang H

Eine Dreikanaligkeit ist zwar besser als eine Zweikanaligkeit, aber es bleibt die Frage nach der Sinnhaftigkeit einer solchen Lösung: Wenn die Praxis seit Erscheinen der DIN EN 954-1 gezeigt hat, dass mit zweikanaligen Architekturen das Unfallgeschehen drastisch reduziert wurde und dass die Unfälle heutzutage nicht durch das zufällige Versagen einer redundanten Lösung begründet sind, sondern durch menschliches Verhalten wie z. B. Manipulation, dann ist eine Zweikanaligkeit für hohe Risiken wie SIL 2 und SIL 3 (oder PL d bzw. PL e gemäß DIN EN ISO 13849-1) ausreichend sicher genug.

Das bedeutet also:

- selbst ein zweikanaliges Teilsystem kann grundsätzlich (theoretisch) ein versagen, wenn beide Kanäle ausfallen (Anhäufung von Fehlern/Ausfällen in beiden Kanälen);
- eine Anhäufung von Fehlern/Ausfällen für diese beiden Kanäle ist sehr unwahrscheinlich hinsichtlich des Zeitpunktes des Auftretens dieser Fehler/Ausfällen;
- wenn Diagnose verwendet wird, dann wird diese eine Fehlerreaktion für einen Kanal einleiten, bevor auch der zweite Kanal versagt;
- nur mit Ausfällen beider Kanäle aufgrund einer gemeinsamen Ursache (CCF-Betrachtung) kann nicht-elektronisches Teilsystem immer systematisch ausfallen – Mathematik hin oder her, mit oder ohne Diagnose.

Eine Funktionsprüfung kann also Abhilfe schaffen, wenn die Befürchtung besteht, dass eine Anhäufung von Fehlern bzw. Ausfällen in einem zweikanaligen Teilsystem möglich ist.

Das erklärt auch warum in der Praxis eine Architektur HFT = 0 mit DC bzw. eine Kategorie 2 im Ausgangskreis (Aktor-Seite) möglich ist.

Für ein einkanaliges Teilsystem kann der Ausfall durch eine Diagnose verhindert werden, aber nur wenn diese Diagnose auch eine Fehlerreaktion zeitnah auslösen kann – spätestens also zum Zeitpunkt der Anforderung der Sicherheitsfunktion.

7.3.4 Ausfallrate eines Teilsystem-Elements

7.3.4.1 Allgemeines

Die mathematische Ausfallwahrscheinlichkeit eines Teilsystem-Elements kann meist durch einen von drei Parametern charakterisiert werden: λ (Lambda), *MTTF* (Mean Time To Failure) oder B_{10}. […]

7.3.4.2 Beziehung der betreffenden Parameter

Für Teilsystem-Elemente werden konstante Ausfallraten (λ) angenommen. Die folgenden grundlegenden Gleichungen können verwendet werden: […]

Die wichtigsten mathematischen Beziehungen sind in den folgenden Formeln formuliert:

$$\lambda_D \left[\frac{1}{h}\right] = \frac{1}{MTTF_D \left[a\right] 8\,760 \left[\frac{h}{a}\right]}$$

$$n_{op} \left[\frac{\text{Betätigungen}}{a}\right] = \frac{d_{op} \left[\frac{d}{a}\right] \cdot h_{op} \left[\frac{h}{d}\right] \cdot 3\,600 \left[\frac{s}{h}\right]}{t_{cycle} \left[\frac{s}{\text{Betätigungen}}\right]}$$

$$\lambda_D \left[\frac{1}{h}\right] \approx \frac{0{,}1\,C \left[\frac{\text{Betätigungen}}{h}\right]}{B_{10D} \left[\text{Betätigungen}\right]} = \frac{0{,}1\,n_{op} \left[\frac{\text{Betätigungen}}{a}\right]}{B_{10D} \left[\text{Betätigungen}\right] 8\,760 \left[\frac{h}{a}\right]}$$

$$T_{10D} \left[a\right] \approx \frac{B_{10D}}{n_{op}} = 0{,}1\,MTTF_D = 0{,}1 \frac{1}{\lambda_D \left[\frac{1}{h}\right] 8\,760 \left[\frac{h}{a}\right]}$$

> […] Wenn der Anteil gefährlicher Ausfälle auf weniger als 0,5 (50 % gefährliche Ausfälle) geschätzt wird, ist die Lebensdauer des Bauteils auf das Doppelte von T_{10} begrenzt.
>
> Der Anteil gefährlicher Ausfälle wird auf 0,5 (50 % gefährliche Ausfälle) geschätzt, wenn keine anderen Informationen (z. B. Produktnorm) verfügbar sind. […]

Diese Aussage ist sehr wichtig, damit die Weibull-Verteilung berücksichtig wird, sodass von einer konstanten Ausfallrate λ ausgegangen werden kann.

Die Bilder 3 und 4 veranschaulichen, warum die Annahme einer konstanten Ausfallrate λ so wichtig ist.

Durch die Annäherung der Exponentialverteilung an ($\lambda \cdot t$) ergeben sich die mathematischen Herleitungen der *PFH*-Formeln im Anhang I.

Darum ist ebenfalls T_{10D} so entscheidend bei Verwendung von B_{10D}-Werten und Betätigungszyklen. Ab T_{10D} ist die Annahme eines konstanten λ hinfällig.

Zum Zeitpunkt T_{10D} muss dies Komponente getauscht werden, da danach die Ausfallrate λ sich massiv verändern wird, wie die Weibull-Verteilung mit dem Formfaktor 2 anschaulich verdeutlicht.

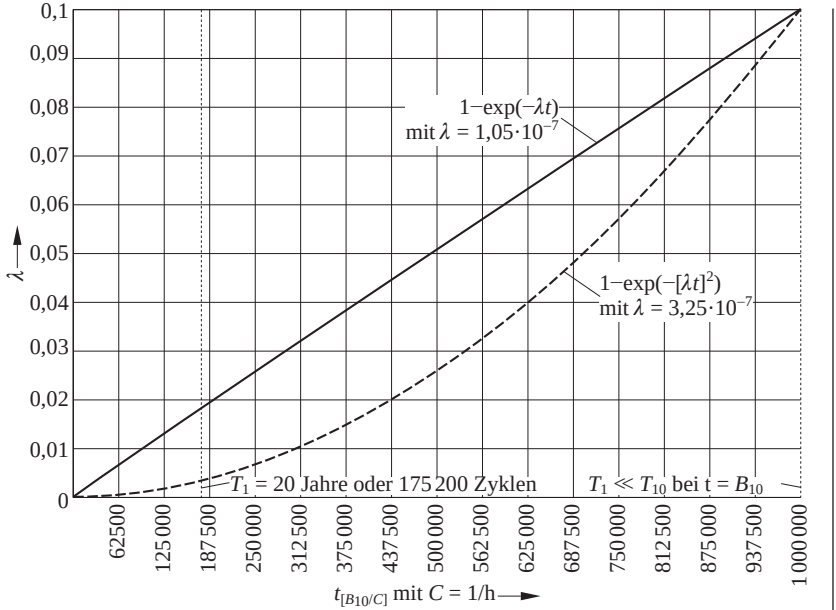


Bild 3 Weibull-Verteilung und konstante Ausfallrate λ (1)

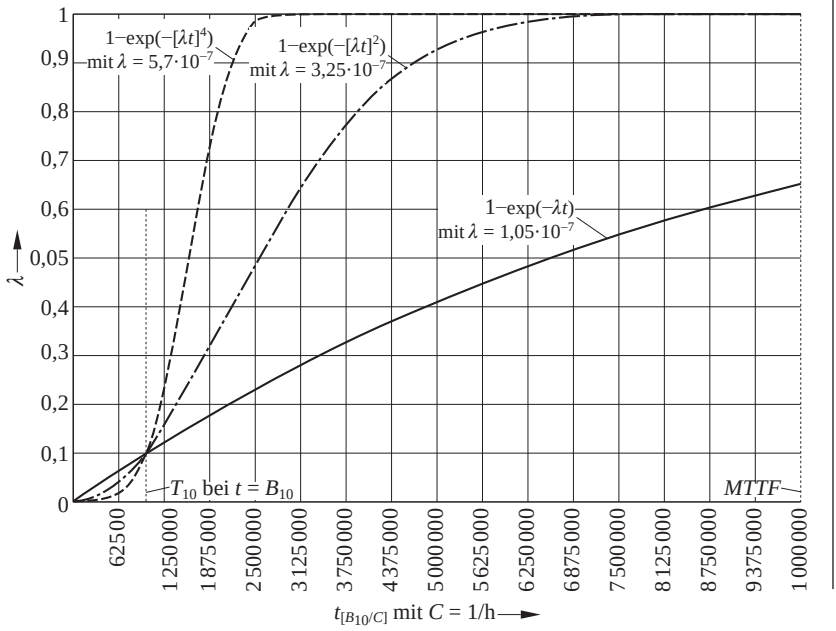


Bild 4 Weibull-Verteilung und konstante Ausfallrate λ (2)

7.4 Strukturelle Einschränkungen eines Teilsystems

7.4.1 Allgemeines

Im Zusammenhang mit der Sicherheitsintegrität der Hardware wird der höchste Sicherheitsintegritätslevel, der für ein SCS beansprucht werden kann, durch die Hardware-Fehlertoleranz (*HFT*) und den Anteil sicherer Ausfälle (*SFF*) der Teilsysteme, die diese Sicherheitsfunktion ausführen, begrenzt. Tabelle 6 gibt den höchsten Sicherheitsintegritätslevel an, der für ein SCS beansprucht werden kann, die ein Teilsystem verwendet, wobei die Hardware-Fehlertoleranz und der Anteil sicherer Ausfälle dieses Teilsystems berücksichtigt werden. Die in Tabelle 6 angegebenen strukturellen Einschränkungen sind auf jedes gemäß Abschnitt 7 entworfenes Teilsystem anzuwenden. In Bezug auf diese strukturellen Einschränkungen: […]

$$\lambda_{gesamt} = \lambda_S + \lambda_D$$

$$\lambda_{gesamt} = \{\lambda_{SU} + \lambda_{SD}\} + \{\lambda_{DU} + \lambda_{DD}\}$$

$$\lambda_{gesamt} = \{(1-DC)\,\lambda_S + DC\,\lambda_S\} + \{(1-DC)\,\lambda_D + DC\,\lambda_D\}$$

mit

λ_S sicherheitsgerichtete Ausfallrate des Teilsystem-Elements (en: Safe),

λ_{SU} unerkannte sicherheitsgerichtete Ausfallrate des Teilsystem-Elements (en: Safe Undetected),

λ_{SD} erkannte sicherheitsgerichtete Ausfallrate des Teilsystem-Elements (en: Safe Detected),

λ_D gefahrbringende Ausfallrate des Teilsystem-Elements (en: Dangerous),

λ_{DU} unerkannte gefahrbringende Ausfallrate des Teilsystem-Elements (en: Dangerous Undetected),

λ_{DD} erkannte sicherheitsgerichtete Ausfallrate des Teilsystem-Elements (en: Dangerous Undetected),

DC Diagnosedeckungsrad des Teilsystem-Elements (en: Diagnostic Coverage)

Merke: *SFF* ist vereinfacht eine Funktion von *DC* jeder Ausfallrate λ (λ_S gibt es nicht und wird mit $\lambda_S \approx 0$ (1/h) angenommen)

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} \cong \frac{\sum \lambda_{DD}}{\sum \lambda_D}$$

Bei einer einkanaligen Architektur ergibt sich

$$SFF = \frac{\lambda_{DD1}}{\lambda_{D1}} = \frac{DC_1\ \lambda_{D1}}{\lambda_{D1}} = DC_1$$

Typischerweise sind die *DC*-Werte in beiden Kanälen gleich.

Bei einer zweikanaligen Architektur ergibt sich

$$SFF = \frac{\lambda_{DD1} + \lambda_{DD2}}{\lambda_{D1} + \lambda_{D2}} = \frac{DC_1\ \lambda_{D1} + DC_2\ \lambda_{D2}}{\lambda_{D1} + \lambda_{D2}} = DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}}}$$

Typischerweise sind die *DC*-Werte in beiden Kanälen gleich.

7.4.1 […] Wenn zwei oder mehr vorgefertigte Teilsysteme zu einem redundanten Teilsystem kombiniert werden, können die strukturellen Einschränkungen des kombinierten Teilsystems bestimmt werden. Dazu kann das Teilsystem mit dem höchsten SIL gemäß den strukturellen Einschränkungen genommen und in Tabelle 6 in der Spalte *HFT* 0 nach dem entsprechenden SIL gesucht werden. Dadurch wird der geltende *SFF*-Bereich wiederhergestellt. Der SIL des kombinierten Teilsystems ist durch Erhöhung des *HFT* um eins im gleichen *SFF*-Bereich gemäß DIN EN 61508-2 (**VDE 0803-2**):2011-02, 7.4.4.2.4, abzuleiten. […]

Komplexes Teilsystem-Element trifft nicht-komplexes Teilsystem-Element SIL 2 und SIL 1 = SIL 3

Übrigens: Dies ist in der ISO 13849-1 so ohne Weiteres öffentlich und offenkundig nicht beschrieben. Ein SRP/CS ist alles und nichts, aber die Kategorien geben per Definition nicht die Möglichkeiten, die die *SFF*-Tabelle 6 bietet. Hier unterscheiden sich beide Normen grundlegend.

Anteil sicherer Ausfälle	Fehlertoleranz der Hardware (*HFT*) (siehe Anmerkung 1)		
	0	**1**	**2**
< 60 %	nicht erlaubt (Ausnahme, siehe Anmerkung 3)	SIL 1	SIL 2
60 % … < 90 %	SIL 1	SIL 2	SIL 3
90 % … < 99 %	**SIL 2**	**SIL 3**	SIL 3 (siehe Anmerkung 2)
≥ 99 %	SIL 3	SIL 3 (siehe Anmerkung 2)	SIL 3 (siehe Anmerkung 2)

Anmerkung 1: Eine Fehlertoleranz der Hardware von *N* bedeutet, dass *N* + 1 Fehler zu einem Verlust der Sicherheitsfunktion führen können.
Anmerkung 2: Ein SIL-4-Anspruch wird in diesem Dokument nicht berücksichtigt. Für SIL 4 siehe DIN EN 61508-1 (**VDE 0803-1**).
Anmerkung 3: Siehe 7.4.3.2, wo Teilsysteme, die einen Anteil sicherer Ausfälle von weniger als 60 % und eine Hardware-Fehlertoleranz von null aufweisen, bei denen bewährte Bauteile verwendet werden, in Betracht gezogen werden können, um SIL 1 zu erreichen; oder für Teilsysteme, bei denen Fehlerausschlüsse auf Fehler angewendet wurden, die zu einem gefährlichen Ausfall führen könnten.
Anmerkung 4: In DIN EN 62061 (**VDE 0113-50**):2016-05 wurde der maximale SIL, der beansprucht werde konnte, als SILCL bezeichnet.
Anmerkung 5: Siehe 7.3.3.3 zur Begrenzung des SIL bei der Anwendung von Fehlerausschlüssen.
Anmerkung 6: Für *HFT* 0 bei *SFF* 99 % ist dies nur möglich, wenn eine ununterbrochene Überwachung der korrekten Funktion des Elements erfolgt. Typischerweise wird dazu elektronische Technologie erforderlich sein.

Tabelle 6 Strukturelle Einschränkungen für ein Teilsystem: max. SIL die für ein SCS mit dem Teilsystem beansprucht werden kann

***HFT* = Anzahl Kanäle ohne Berücksichtigung einer Diagnosefunktion (Fehlerreaktion)**

Wenn für einen Kanal eine Diagnose bereitgestellt wird, z. B. durch ein anderes Teilsystem, dann wird dieser Kanal nur dann nicht versagen, wenn die Diagnose rettend eingreift.

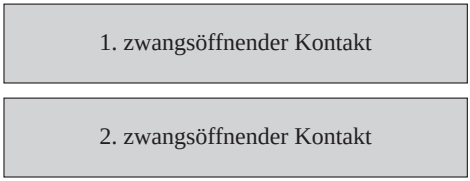
HFT = 0 bedeutet Einkanaligkeit
(Kategorie 1 und Kategorie 2 gemäß DIN EN ISO 13849-1)

ein zwangsöffnender Kontakt

Ohne eine Diagnose zum Erkennen des Ausfalls des einzelnen Teilsystem-Elements kommt es garantiert zum Ausfall des gesamten Teilsystems. Das bedeutet, dass die Fehlertoleranz nicht gut ist – nämlich gleich 0.

Ein Fehler führt zum Totalausfall des Teilsystems, und somit zum Verlust der entsprechenden Sicherheitsfunktion.

HFT = 1 bedeutet Zweikanaligkeit
(Kategorie 3 und Kategorie 4 gemäß DIN EN ISO 13849-1)



Sobald aber zwei Teilsystem-Elemente jeweils einen Kanal bilden – somit zusammen zwei unabhängige Kanäle, dann führt der Ausfall eines Kanals nicht zum Ausfall des Teilsystems – die Fehlertoleranz ist daher gleich 1.

Ein Fehler führt nicht zum Totalausfall des Teilsystems, und somit nicht zum Verlust der entsprechenden Sicherheitsfunktion.

Höchstens SIL 1 mit einem Anteil sicherer Ausfälle (*SFF*) von weniger als 60 % (λ_S gibt es nicht und wird mit $\lambda_S \approx 0$ (1/h) angenommen)

Gemeint ist eine einkanalige Architektur –
Kategorie 1 gemäß DIN EN ISO 13849-1.

Ein einkanaliges Teilsystem hat ohne Diagnose einen *SFF* ≈ 0. Nur bewährte Bauteile sind erlaubt wie in der Kategorie 1 gemäß DIN EN 13849-1. Eine einkanalige elektronische Lösung ohne Diagnose ist somit verboten.

Ein solche ungetestete elektronische Lösung ist in der DIN EN ISO 13849-1 nur mit einem erreichbaren PL b erlaubt.

Da PL b aber „anderen Maßnahmen“ in DIN EN 62061 (**VDE 0113-50**) bedeutet, ist die Einschränkung pauschal auf die Verwendung von bewährten Bauteilen plausibel und sinnvoll.

Anhang A