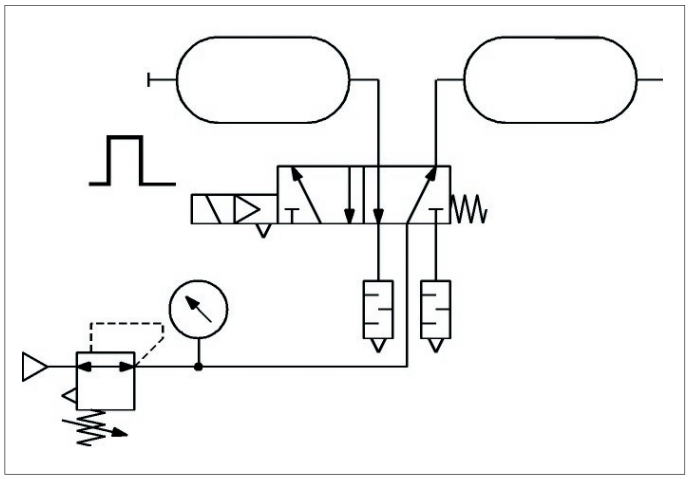
Aus Aktivität wird Vorsicht

„Sinn und Unsinn der Quantifizierung“



1: Darstellung des Schaltplans bei der Ermittlung der Lebensdauer-kennwerte

Tilmann Bork, Michael Schaefer

Dieser Artikel ist aus den Nöten der Praxis entstanden, mit neuen Anforderungen von Normen zur Sicherheit von Steuerungen zurecht zu kommen. Hierbei ist nach Auffassung der Autoren, beide haben mehr als zehn Jahre Erfahrung in Konstruktion bzw. Prüfung und Zertifizierung von Komponenten für die Sicherheit an Maschinen und Anlagen, eine sorgfältige Diskussion erforderlich. Beide versuchen in diesem Beitrag die Praxisprobleme von zwei Seiten des Tisches, einmal aus Sicht des Konstrukteurs und einmal aus Sicht einer Prüfstelle zu beleuchten.

Autoren: *Dr. T. Bork ist Mitarbeiter der FESTO AG & Co. KG in Esslingen und Dr. M. Schaefer ist Mitarbeiter beim Berufsgenossenschaftlichen Institut für Arbeitsschutz – BGIA in St. Augustin*

Dabei konnten die Autoren feststellen, dass sie speziell im Bereich Quantifizierung, also der Berechnung von Zuverlässigkeitskennwerten nicht gegenüber, sondern nebeneinander sitzen. Sie haben – zumindest diesbezüglich – die gleichen Probleme und sind teilweise entsetzt, welche Stilblüten in Bezug auf die Berechnung der sicherheitsbezogenen Zuverlässigkeit draußen z. T. durch Beratungsfirmen aber auch durch Hersteller, Prüfstellen und Sachverständige zu finden sind. Alles unter dem Motto, „mach es kompliziert, dann muss der Kunde jemanden anrufen der sich damit auskennt“. Aus Sicht der Unfallprävention werden durch die komplexen mathematischen Methoden die Ergebnisse teilweise undurchsichtig und der Wert der Berechnungen stark in Frage gestellt. Insbesondere kann die Quantifizierung von wesentlichen und notwendigen sicherheitstechnischen Merkmalen einer Steuerung ablenken, also den Blick auf das Wesentliche, wenn nicht versperren dann zumindest trüben. Solange aber bewährte sicherheitstechnische Prinzipien wie Redundanz und Diagnose nicht in Frage gestellt werden, kann Quantifizierung helfen, bestimmte – und die Autoren legen hier besonderen Wert darauf – nicht alle –Fragen zu beantworten. Dieser Artikel zeigt, wo Quantifizierung sinnvoll ist, er zeigt aber auch den Unsinn auf, den man mit Quantifizierung – unüberlegt verwendet – machen kann. Falsch eingesetzt, führt der Zahlenrausch mancher so genannter Sicherheitsexperten zu völlig unsinnigen oder auch gefährlichen Äußerungen, die ein Anwender von Komponenten leicht missverstehen kann und die bestenfalls anfänglich dem Vertrieb helfen können. Daher ist es wichtig, aus dem Gespenst Quantifizierung ein transparentes Gebilde aufzubauen, dass verstanden und nicht nur aufgegriffen wird, um dem Anwender ein Gutes Gewissen vorzugaukeln, dass er unter bestimmten Verhältnissen besser nicht haben sollte.

Lebensdauerkennwerte (unumstößliche Werte?)

Die Lebensdauerkennwerte für Komponenten werden neben anderen teilweise nicht transparenten bzw. nicht realisierbaren Methoden am seriösesten in Dauerlaufversuchen ermittelt. Dies ist im Bereich der Elektronik seit langem bekannt und wird unter besonderen Konditionen (z. B. erhöhte Temperatur zur Beschleunigung des Alterungsprozesses) auch angewendet.

Bei Lebensdauerversuchen stellen die Versuchsbedingungen eine Abstraktion und Vereinfachung der Realität dar. Um daher eine Vergleichbarkeit der Ergebnisse untereinander zu ermöglichen, ist eine Standardisierung der Versuchsbedingungen erforderlich (für die Pneumatik ist z. B. deswegen die ISO 19973 in Vorbereitung).

Die Methode der Ermittlung von Zuverlässigkeitskennwerten durch Abschätzung anhand von Ausfällen im Betrieb ist nur unter bestimmten Bedingungen möglich (z. B. mit zuverlässigkeitsorientiert geführter Schadensstatistik des Herstellers, siehe [1]). Werden nur die Ausfälle von Komponenten unterschiedlichster Hersteller in einer Anlage ohne Betrachtung der Einsatzbedingungen (Lasten, Zeiten usw.) „gezählt“, dann sind die daraus gewonnenen „Daten“ äußerst fragwürdig und für die Berechnung nicht verwendbar.

Für Dauerlaufversuche müssen
- Versuchsbedingungen und
- Abbruchbedingungen

definiert werden. Hieraus kann man schon erkennen, dass es sich um z. T. subjektive Kriterien handelt. Die Hersteller sind logischerweise bemüht, ihre Komponenten entsprechend realitätsnah zu testen und wählen die Abbruchbedingungen entsprechend ihres eigenen Qualitätsverständnisses. Dieses Vorgehen ist verständlich, kann aber bei der Betrachtung unter sicherheitstechnischem Aspekt zu unerwarteten Ergebnissen führen.

Dieser Zusammenhang lässt sich gut an einem realen Beispiel darstellen: ein Magnetventil soll einen Dauerversuch durchlaufen, um die Lebensdauerkennwerte zu ermitteln. Ein Magnetventil ist u. a. da-

zu da, einen Antriebszylinder zu steuern. Im Versuch soll nur das Ventil und nicht die Kombination Ventil-Zylinder getestet werden. Um die Randbedingungen konstant zu halten, muss daher der Zylinder durch ein anderes Bauteil (Konstanthalten der Randbedingungen) ersetzt werden. Praktischerweise greift man auf kleine Volumina zurück. Damit sieht die Versuchsschaltung wie im **Bild 1** dargestellt aus.

Das Magnetventil wird zyklisch umgeschaltet. Als ausgefallen gilt der Prüfling, wenn eines der gewählten Abbruchkriterien erfüllt ist:

- Funktionsausfall (Nichtschalten)
- Überschreiten der Schaltdrücke (Anstieg des zum Umsteuern der Hauptstufe notwendigen Druckes)
- Leckage

Der Versuch wird gestartet und die Ventile der zu untersuchenden Stichprobe mit einer Frequenz von 3 Hz geschaltet. Das Ergebnis des Versuches: Alle Ventile fallen wegen Überschreitung der Leckagegrenzwerte aus.

Unter Versuchsbedingungen werden beispielhaft für die Prüflinge der gewählten Stichprobe die folgenden Werte ermittelt:

- charakteristische Lebensdauer $T = 120 \cdot 10^6$ Schaltspiele
- $B_{10} = 64{,}2 \cdot 10^6$ Schaltspiele
- Formparameter $b = 3{,}6$

Was liefert die Betrachtung der Versuchsergebnisse?

Die ermittelte Lebensdauer T bedeutet für den Dauerversuch, dass nach 463 Tagen reiner Versuchslaufzeit 63,2 % der Prüflinge ausgefallen sind. Hieraus ersieht man schon, welcher Aufwand für einen Hersteller entsteht, wenn er seine Produkte sorgfältig prüfen will. Daher gibt es natürlich Bestrebungen, diese extrem langen Versuchszeiten abzukürzen.

Hier muss man aber ganz klar zwischen seriösen und unseriösen Methoden trennen. Bei „forscher“ Herangehensweise könnte man einfach die Prüffrequenz oder die Temperatur (ähnlich burn-in-Test) erhöhen. Dieser Weg zeigt aber interessante Effekte. Wird z. B. die Schaltfrequenz erhöht, kann der Kolbenschieber der Hauptstufe nicht mehr seinen vollen Hub durchlaufen (ja sogar stehenbleiben). Das Ergebnis dieses „Versuches“ wird dem Ventil dann eine extrem hohe Lebensdauer bescheinigen.

Andere Änderungen bei den Versuchsbedingungen können den Dauerversuch so beeinflussen, dass plötzlich ganz andere Schadensmechanismen wirken (siehe auch [2]).

Ähnliche Auswirkungen zeigen Einsatzbedingungen, die durch extrem niedrige Anforderungsraten eine Komponente mit völlig anderen Schadensmechanismen belasten als die, die im Dauerversuch auftraten. So ist es äußerst bedenklich, wenn:

- Ventilen in Gutachten bekannter Prüfstelle ein extrem niedriger *PFD*-Wert (z. B. $PFD < 4 \cdot 10^{-7}$) testiert wird,
- diese Ventile im low demand mode (DIN EN 61 511) betrieben werden und
- die Lebensdauerkennwerte ähnlich den o.g. ermittelt werden.

Hierbei ist *PFD* ein Maß für die Ausfallwahrscheinlichkeit eines Systems, nämlich die mittlere Wahrscheinlichkeit, dass es zum Zeitpunkt einer Anforderung auf gefährliche Weise ausgefallen ist (average probability of failure on demand, DIN IEC 61 508).

Betrachtet man die Ergebnisse des gewählten Beispieles kritisch, muss man feststellen, dass die im obigen Beispiel ermittelten Lebensdauerkennwerte noch lange keine Lebensdauerkennwerte für den gefährlichen Ausfall bedeuten! Abbruchkriterien aus Sicht der Erfüllung der Sicherheitsfunktion für ein Schaltventil sind:

- selbsttätiges Schalten (z. B. durch Bruch der Plungerfeder in der Vorsteuerstufe),
- Nichtzurückschalten,
- verzögertes Zurückschalten (z. B. Auswirkung bei Anwendung der DIN EN 999).

Konsequenter Weise müssten für jeden Einsatzfall der Komponente die entsprechenden Lebensdauerkennwerte für die relevante Versagensrichtung ermittelt werden. Das ist einerseits aus wirtschaftlichen Gründen nicht vertretbar und andererseits technisch nicht immer ohne weiteres möglich (bevor die Vorsteuerstufe ausfällt versagt z. B. die Hauptsteuerstufe).

Dieses Verhalten sollte bei der Gestaltung der Produkte gezielt genutzt werden. Ein Ausfall in die sichere Richtung (ein „Nicht-mehr-Schalten“ des Ventils ist aus sicherheitstechnischer Sicht an Maschinen und Anlagen unbedenklich) ist für Produkte bei sicherheitsrelevantem Einsatz anzustreben. Wenn man nun keine Lebensdauerkennwerte für den sicherheitsrelevanten Ausfall erhält, muss man die vorhandenen Lebensdauerkennwerte auf ihre Eignung für die Anwendung nach DIN EN ISO 13849-1 beurteilen.

Die Abbruchbedingungen aus dem obigen Beispiel zeigen, dass es sich um Qualitätsmerkmale handelt. Um sicherheitsrelevant auszufallen, hätten die Prüflinge noch länger getestet werden müssen. D. h. real, die Prüflinge sind wesentlich widerstandsfähiger gegen gefährliche Ausfälle, als es die ermittelten Kennwerte suggerieren.

Aus sicherheitsrelevanter Sicht kann man also mit diesen Werten beruhigt arbeiten. Man muss nur wissen, dass diese Komponenten sich wahrscheinlich „besser“ als berechnet verhalten werden. D. h. für die praktische Anwendung: man rechnet mit „schlechten“ Werten und hat einen gewissen Sicherheitszuschlag. Wie hoch dieser ist, kann man nur abschätzen. Denn auch hier muss man bedenken, dass die Lebensdauerkennwerte anhand einer Stichprobe

endlicher Größe gewonnen wurden. Je kleiner die Stichprobe, desto größer ist der Vertrauensbereich; d. h. umso stärker streut eine Ranggröße.

Damit ist auch klar, dass man bei der Nachrechnung der *MTTF* eines Steuerungskanals bei einem dreistelligen Ergebnis die letzten beiden Stellen beruhigt runden kann. Das heißt aber auch: wer an dieser Stelle anhand von Nachkommastellen seine Entscheidungen trifft, weiß nicht was er tut.

Welche Möglichkeiten bieten sich für den Komponentenhersteller für die Kennwertermittlung? Wegen der langen Versuchsdauer ist es sinnvoll und aus sicherheitstechnischer Sicht völlig unbedenklich, wenn die Komponenten für die Versuche „zerlegt" werden. Das bedeutet, man führt die Lebensdauerversuche für die einzelnen Teilsysteme der Komponente getrennt durch z. B.:

- Lebensdauerversuch Vorsteuerventil,
- Lebensdauerversuch Hauptstufe,
- Lebensdauerversuche für Dichtungspaarungen usw.

Dieses Vorgehen spart einerseits Zeit und Kosten, bietet aber für die sicherheitstechnische Betrachtung unerwartete Vorteile. Man kommt so viel besser zu Kennwerten für die sicherheitstechnische Bewertung. Es lassen sich Fehlerausschlüsse und Ausfallrichtungen beurteilen. Liegt z. B. die Lebensdauer der Vorsteuerstufe wesentlich über der der Hauptstufe, kann u. U. ein selbsttätiges Schalten (nahezu) ausgeschlossen werden. Die Systemzuverlässigkeit (also die der vollständigen Komponenten) kann für ein Boolesches-Seriensystem dann wieder über das Produkt der Einzelzuverlässigkeiten ermittelt werden. Für den Komponentenhersteller bedeutet das aber auch, dass er seine Produkte in Richtung sicherer Ausfall optimieren kann.

Grundsätzlich empfiehlt es sich, Werten aus Datenbanken oder anderen Quellen, die keine Angaben zu Art der Datenerhebung machen (bzw. auch Programmen, die derartige Daten nutzen), zu misstrauen. So ist der Gedanke gar nicht so abwegig, dass die in Militär-Datenbanken angegebene Lebensdauer eines Pneumatikventils nichts anderes darstellt, als die Verweildauer der Flugabwehrrakete im Magazin (Zeit zwischen Anlieferung und Abschuss), wobei die Wahrscheinlichkeit, dass die Stichprobe den Umfang 1 hatte, nicht klein sein dürfte.

SIL-Forderungen (*SIL* ist nicht gleich *SIL* !)

In letzter Zeit ist ein sich verstärkender Trend zu beobachten, der Anlass zur Sorge sein sollte: Komponentenhersteller werden zunehmend nach einem *SIL* (Safety Integrity Level) für ihre Produkte gefragt. Diese Nachfrage dokumentiert u.a. einen gravierenden Wissensmangel bei Anwendern bzw. Anlagenprojekteuren.

Nun hat nicht jeder Komponentenhersteller (z. B. Magnetventilhersteller) den Überblick, die Ausdauer oder die Macht, um auf diesem Gebiet aufzuklären. Nur so ist es zu erklären, dass in Prospekten und Dokumentationen Ventile z. B. mit der Besonderheit: „Ausführung mit Prüf-Gutachten bis AK7/*SIL*4, «einer für alles», universelle Ausführung für alle Anwendungen" dokumentiert werden.

Dieses Vorgehen ist aus Sicht des Komponentenherstellers durchaus verständlich (er geht den Weg des geringsten Widerstandes), in der Sache aber äußerst gefährlich – wird so doch ein Halbwissen und eine falsche Herangehensweise zementiert. In letzter Konsequenz leidet die Sicherheit der projektierten Anlage – die errechnete Sicherheit gegen Versagen basiert auf falschen Annahmen. Das Problem der „*SIL*-Zulassungen" kann ein Hersteller mechanischer, elektromechanischer, hydraulischer oder pneumatischer Komponenten nicht lösen.

Es liegt einerseits einfach daran, dass auf dem Gebiet der funktionalen Sicherheit viele Dinge miteinander vermengt werden. Es lohnt sich schon, alleine über den Begriff „funktionale Sicherheit" etwas genauer nachzudenken. Funktionale Sicherheit hat noch lange nicht zwangsläufig mit Anwendersicherheit zu tun – eine Guillotine ist nämlich funktional sicher.

Andererseits werden Normen zur Anwendung gebracht, die für die betrachtete Aufgabe schlicht ungeeignet sind. So ist es äußerst ungeschickt, wenn man mit einer „Elektro"-Norm versucht, mechanische Systeme „in den Griff" zu bekommen. Erschwerend kann noch dazu kommen, dass die ins Auge gefasste Norm gar keine harmonisierte Norm (z. B. IEC 61 508) ist und damit dem Anwender die Beweislast wegen des Nichtgreifens der so genannten Vermutungswirkung aufbürdet.

Die DIN EN 61 508 bzw. IEC 61 508 deckt die „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme" ab. D. h. diese Norm generiert die Vorgaben für die Vermeidung und Beherrschung von Ausfällen in elektrischen, elektronischen und/oder programmierbaren elektronischen Geräten. Für das Gesamtsystem inklusive der risikomindernden Maßnahmen werden vier Sicherheitsstufen (*SIL*1 bis *SIL*4) unterschieden.

Der Fokus der DIN EN 61 511 ist die „Funktionale Sicherheit sicherheitstechnischer Systeme in der Prozessindustrie". Auch diese Norm greift auf die Einteilung in *SIL*-Stufen zurück. Bei einfachen Magnetventilen und ähnlichen Bauteilen handelt es sich um Komponenten. Diese Komponenten stellen aber kein System im Sinne der DIN EN 61 508 bzw. DIN EN 61 511 dar. D. h. für einfache Komponenten kann es keinen *SIL* geben.

Magnetventil · Zulassung SIL 4 nach IEC 61508	
Eingang	24 V DC · verpolsicher · Zerstörgrenze 40 V Stromaufnahme $I = \frac{U - 5{,}6\ V}{4020\ \Omega}$ (entspricht 4,5 mA bei 24 V)
Signal "0" kein Anzug	≤ 15 V
Signal "1" sicherer Anzug	> 19 V
Lebensdauer	> 2 x 10^7 Schaltspiele
Verwendung in sicherheitsgerichteten Systemen nach IEC 61508	Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktion bei einer Funktionsanforderung PFD < 2,8 x 10^{-7} für ein Konfidenzniveau von 95 %. Die Safe Failure Fraction (SFF) nach Tabelle A1 in IEC 61508-2 ist größer oder gleich 0,99. Die Ventile sind daher geeignet zur Verwendung in sicherheitsgerichteten Systemen mit einer Hardware Fault Tolerance von 1 oder 2 bis einschließlich SIL 4.

2: Angaben aus einer Dokumentation eines Pneumatikventils

Erst mit der Applikation, der Systemgestaltung und den konkreten Betriebsbedingungen ergibt sich für die verwendete Komponente ein definierter Einsatzfall. Aus diesem aktuellem Einsatzfall kann auf die Belastung und das vermutliche Ausfallverhalten der betrachteten Komponente geschlossen werden. Führt man diesen Gedanken konsequent zu Ende, bedeutet das auch, dass sich eine bestimmte Komponente in unterschiedlichen Applikationen völlig anders verhalten kann (siehe auch DIN EN ISO 13 849-2).

Ein weiterer Gesichtspunkt ist das Verhalten von Mechanikkomponenten. Mechanik verhält sich einfach anders als Elektronik: Elektronik altert mit der Zeit, Mechanik dagegen altert in der Hauptsache durch Verschleiß. Nicht genutzte Mechanik (z. B. Betrieb im low demand mode; DIN EN 61 511) kann sich noch anders verhalten (Korrosion, Kleben, Vulkanisiervorgänge, Gefügeveränderungen usw.).

Komponenten, deren Verhalten entscheidend durch mechanischen Verschleiß (Ventile, Zylinder, Lager, Relais, Schütze) gekennzeichnet ist, lassen sich nicht mit Größen beschreiben, die z. B. in der DIN EN 61 508 verwendet werden. Ganz entscheidend ist die Tatsache, dass die Ausfallrate $\lambda(t)$ nicht konstant ist.

Allerdings kann die Ausfallwahrscheinlichkeit mechanischer Komponenten ebenfalls beschrieben werden. Ein anerkanntes Verfahren ist das Verfahren nach Weibull [3].

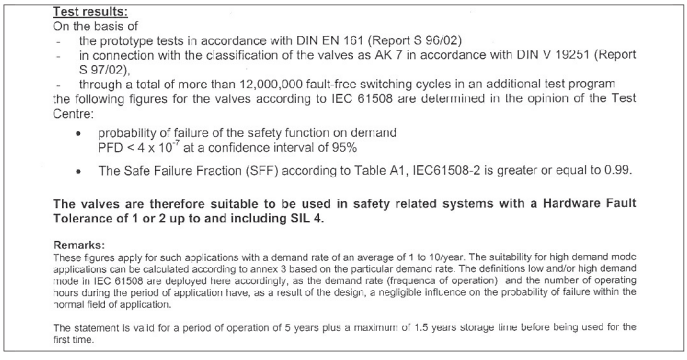
Mit den Parametern T und b der Weibull-Verteilung lässt sich die Ausfallwahrscheinlichkeit zu einem bestimmten Zeitpunkt beschreiben. Durch einfache Umrechnung kann bei bekannter angestrebter Gebrauchsdauer (mission time) T_m und bekannten Einsatzdaten auch die *MTTF* (Mean Time To Failure) für die betrachtete Komponente (z. B. Magnetventil) errechnet werden (siehe auch DIN EN ISO 13 849-1). Im Prinzip handelt es sich bei diesem Ansatz um die Bestimmung einer äquivalenten (elektrischen) Ersatzkomponente, die am Ende T_m die gleiche Ausfallwahrscheinlichkeit wie die mechanische Komponente hat.

Mit der *MTTF* als Eingangswert kann jetzt das Gesamtsystem nach DIN EN 61 508 betrachtet und ausgelegt werden. Grundsätzlich können alle Komponenten (bei bestimmungsgemäßem Gebrauch) in Systemen bis *SIL*4 eingesetzt werden. Dies gilt natürlich im Übrigen auch für die Berechnung des Performance Levels nach DIN EN ISO 13 849-1. Achtung, wenn hier vom Erreichen eines *SIL* bzw. *PL* gesprochen wird, so bezieht sich dies nur auf die Aspekte der Quantifizierung. Natürlich sind bei allen Normen noch zusätzliche deterministische Bedingungen und Maßnahmen gegen so genannte systematische Fehler, Dokumentation etc. zu erfüllen.

Kardinalfehler (Dummheit in der Statistik)

Es gibt Fehler die gemacht werden, weil

3: Angaben aus einem Zertifikat zu einem Pneumatikventil



Test results:
On the basis of
- the prototype tests in accordance with DIN EN 161 (Report S 96/02)
- in connection with the classification of the valves as AK 7 in accordance with DIN V 19251 (Report S 97/02),
- through a total of more than 12,000,000 fault-free switching cycles in an additional test program

the following figures for the valves according to IEC 61508 are determined in the opinion of the Test Centre:

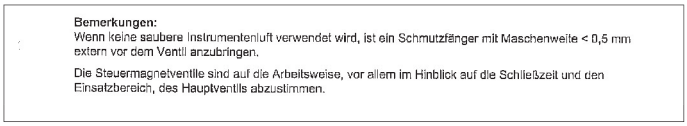
- probability of failure of the safety function on demand
  PFD < 4 x 10^{-7} at a confidence interval of 95%
- The Safe Failure Fraction (SFF) according to Table A1, IEC61508-2 is greater or equal to 0.99.

The valves are therefore suitable to be used in safety related systems with a Hardware Fault Tolerance of 1 or 2 up to and including SIL 4.

Remarks:
These figures apply for such applications with a demand rate of an average of 1 to 10/year. The suitability for high demand mode applications can be calculated according to annex 3 based on the particular demand rate. The definitions low and/or high demand mode in IEC 61508 are deployed here accordingly, as the demand rate (frequency of operation) and the number of operating hours during the period of application have, as a result of the design, a negligible influence on the probability of failure within the normal field of application.

The statement is valid for a period of operation of 5 years plus a maximum of 1.5 years storage time before being used for the first time.

4: Angaben aus einem Zertifikat zu einem Pneumatikventil



Bemerkungen:
Wenn keine saubere Instrumentenluft verwendet wird, ist ein Schmutzfänger mit Maschenweite < 0,5 mm extern vor dem Ventil anzubringen.

Die Steuermagnetventile sind auf die Arbeitsweise, vor allem im Hinblick auf die Schließzeit und den Einsatzbereich, des Hauptventils abzustimmen.

man nicht genau über die Thematik nachdenkt. Es ist eigentlich peinlich solche hier zu nennen, da sie eigentlich unmittelbar als Fehler klar werden. Die Autoren haben lange überlegt, ob sie diese hier nennen, aber Gesprächen entnehmen wir immer wieder, dass es scheinbar doch notwendig ist. Der wissende Leser mag dies verzeihen.

Fehler 1:
Ohne weitere Angaben der Quelle gibt es Kardinalfehler, die teilweise sogar von „Experten" vorgenommen werden: Es herrscht manchmal die Meinung vor, dass bei großem Stichprobenumfang von z. B. 100 Komponenten die 1 000 Schaltspiele „überleben" eine Extrapolation möglich ist, so dass man anschließend sagen kann: Wenn 100 Komponenten 1 000 Schaltspiele ertragen, dann erträgt eine Komponente 100·1 000 = 100 000 Schaltspiele. Dass dies Unsinn ist, wird sofort bei folgendem Gedankenspiel klar: Es gibt sicherlich auf der Erde 1 000 Menschen die 100 Jahre alt geworden sind. Das bedeutet aber nicht, dass ein einzelner Mensch 100 000 Jahre alt werden kann, zumindest nicht ohne zu sterben.

Fehler 2:
Eine Wahrscheinlichkeit ist ein Maß, das ohne weiteren Bezug keine Aussage macht. Die Wahrscheinlichkeit P_{tot}, dass man stirbt ist immer 1. Die Wahrscheinlichkeit, dass die Sonne irgendwann erlischt ist $P_{Sonne} = 1$. Die Wahrscheinlichkeit, dass eine Steuerung versagt, sei sie noch so gut, ist $P_{Steuerung} = 1$.

Die IEC 61 508 unterscheidet zwischen zwei Ausfallwahrscheinlichkeiten einer Steuerung. Die Wahrscheinlichkeit eines „Ausfalls bei Anforderung" der Sicherheitsfunktion *PFD* (Probability of failure on demand) und die Wahrscheinlichkeit eines „Ausfalls pro Stunde" *PFH* (probabilty of a dangerous failure per hour), in der IEC 62 061 PFH_D genannt. *PFD* darf nach Norm nur eingesetzt werden, wenn die Anforderung an die Sicherheitsfunktion nicht mehr als 1 Mal pro Jahr erfolgt. *PFH* darf immer verwendet werden. *PFD* ist eine echte Wahrscheinlichkeitsgröße [dimensionslos] während *PFH* als Rate aufgefasst werden kann (dim *PFH* = 1/h). Während man in der Mathematik unabhängige Wahrscheinlichkeiten zur Bildung einer Gesamtwahrscheinlichkeit beispielsweise multiplizieren darf, ist dies bei Raten gefährlich bzw. verboten.

Angaben in Dokumentationen (aus *SIL* 4 wird *SIL* 2)

Der eine oder andere Hersteller hat auf die Forderungen des Marktes reagiert und bietet die Komponenten mit den entsprechenden Angaben an. Es ergibt sich die Frage, was der Anwender damit anfangen kann (**Bild 2**).

1. Beispiel
Hier wird dem Anwender in der ersten Zeile suggeriert, dass ein Magnetventil erstens einen *SIL*4 haben und zweitens dafür auch noch zugelassenen sein kann. Richtig wäre die Angabe: „...das Ventil ist für den Einsatz in Systemen bis *SIL*4 geeignet..."

Die alleinige Angabe der Lebensdauer *T* „größer als" (ohne Formparameter *b*) deutet (hoffentlich nur) auf einen abgebrochenen Dauerversuch hin (und zwar bei $2 \cdot 10^7$ Schaltspielen; alle Probanden waren noch intakt). D. h. die Ventile haben einen Funktionsdauerversuch bestanden, Lebensdauerkennwerte zu Berechnung der Ausfallwahrscheinlichkeit liegen nicht vor.

Die Angabe $PFD < 2{,}8 \cdot 10^7$ (*PFD*: probability of failure on demand; neben dem Druckfehler: 10^7 statt 10^{-7}) ist für ein Magnetventil ohne Angabe des Betriebsmodus und der Einsatzdauer zwecklos (die Ausfallwahrscheinlichkeit ist eine Funktion der Schaltspiele). Nach DIN EN 62 061 ist: $PFHD = PFD/T_M$ (probability of failure in Time) für einkanalige Systeme ohne Diagnose. Dabei ist T_M die sogenannte Mission Time (max. zulässige Einsatzdauer), die nun aber von der Zahl der Schaltspiele pro Zeiteinheit abhängt.

Setzt man hier für das genannte *T* sicherheitshalber den $B10_d$-Wert ein (eine erlaubt pessimistische Betrachtung, wenn man nach Abbruch davon ausgeht, dass bei einem Stichprobenumfang von 10 das erste Ventil unmittelbar nach dem Abbruch gefährlich ausfallen könnte), dann ergäbe sich eine $MTTF_d$ bei 100 000 Schaltspielen von: $MTTF_d = 100$ Jahren ($PFDH = 1{,}17 \cdot 10^{-2}$ für einkanalige Systeme ohne Diagnose und *PL* = c bzw. *SIL* 2) gemäß DIN EN ISO EN 13 849-1. Also Vorsicht! Die Angabe von *PFD* ist nach IEC 61 508 nur erlaubt für Systeme mit maximaler Anforderung von etwa 1/Jahr. Dies ist in der Prozessindustrie durchaus denkbar, aber im Maschinenbereich praktisch nie gegeben(vergleiche auch IEC 62 061 und DIN EN ISO 13 849-1).

2. Beispiel
Angegeben werden (**Bild 3**):
- $12 \cdot 10^6$ fehlerfreie Schaltungen,
- ein $PFD < 4 \cdot 10^{-7}$.

Im Kleingedruckten folgen weitere wichtige Angaben:
- der *PFD* gilt für eine Anforderungsrate von 1 bis 10 mal pro Jahr,
- die Angaben gelten für eine Mission Time von max. fünf Jahren und
- eine maximale Lagerzeit vor Einsatz von 1,5 Jahren.

Daraus lässt sich ableiten:
- für die Ventile wurde anscheinend nur ein Funktionsdauerversuch durchgeführt,
- die Angabe des *PFD* ist auf konkrete Einsatzbedingungen bezogen,
- das Ventil kann maximal fünf Jahre eingesetzt werden (für längere Einsatzdauern kann das System nicht ausgelegt werden, weil die Daten fehlen),
- die Ventile im Ersatzteillager sind turnusmäßig zu erneuern (für den Anlagenbetreiber eine Herausforderung: Logistik, Kosten und Verantwortung).

Interessant wird es, wenn man Angaben in Prüfberichten wie in **Bild 4** findet. Analysiert man diese Angabe, dann bedeutet das:
- wird das Ventil nicht bestimmungsgemäß eingesetzt (schlechte oder sogar keine Luftaufbereitung), dann reicht auch ein Schmutzfänger aus,
- Kompressorenöle und andere schädliche flüssige Substanzen sind unbedeutend.

Gelten die Lebensdauerkennwerte (*PFD*, ausfallfreie Zeit, Mission Time) noch unter diesen Bedingungen? Ein gefährlicher Zusatz, der das Gutachten ad absurdum führt.

Von *T* und *b* zu *MTTF* (ein einfacher Ansatz)

Die *MTTF* (mean time to failure, mittlere Zeit bis zum Ausfall) ist von der Dimension eine Zeit und gilt für elektrische/elektronische Komponenten. D. h. die Elektronik altert durch die Zeit. Das bedeutet in seiner Konsequenz auch, dass es streng genommen für die *MTTF* völlig egal ist, ob die SPS in Betrieb ist oder eine „frische" SPS gleichen Herstellungsdatums aus dem Regal genommen wird (vernachlässigt man bei diesem Vergleich die schnellere Alterung durch höhere Temperaturen im Betrieb; gekühlte SPS halten wirklich ein wenig länger).

Bei der charakteristischen Lebensdauer *T* für mechanische Komponenten handelt es sich um eine dimensionslose Kenngröße für die Lastwechsel, bei der 63,2 % der Stichprobe ausgefallen sind. Zur Beschreibung der Ausfallwahrscheinlichkeit als Funktion der Zeit müssen bei Komponenten, deren wesentliches Alterungskennzeichen der mechanische Verschleiß ist, die Einsatzbedingungen (z. B. Schaltfrequenz) mit einbezogen werden. Daher ist es auch falsch, wenn z. B. für Magnetventile und ähnliche Bauteile eine *MTTF* oder eine *PFD* ohne Spezifikation der Einsatzbedingungen angegeben werden. (Ausnahme bildet hier die Hydraulik. Bei Einhaltung der spezifizierten Betriebsbedingungen ist der Verschleiß äußerst gering und Dauerversuche sind nicht praktikabel [1].) Wird bei der Nachrechnung der Sicherheitskette mit dieser *MTTF* (oder *PFD*) dann ohne Berücksichtigung der für diese Werte geltenden Einsatzbedingungen gerechnet, dann kann das Ergebnis der Rechnung schlicht nur falsch sein. Der Ansatz, beide Systeme zusammenzufügen, ist über die Ausfallwahrscheinlichkeit möglich.

Bei Annahme einer zeitlich konstanten Ausfallrate gilt für die Ausfallwahrscheinlichkeit in der Elektronik:

Klassifikation	Bereich der $MTTF_D$	Ausfallwahrscheinlichkeit F bei T_M=20 Jahre
niedrig	3 Jahre > $MTTF_D$ > 10 Jahre	99,9 % > $F_D(T_M)$ > 86,5 %
mittel	10 Jahre > $MTTF_D$ > 30 Jahre	86,5 % > $F_D(T_M)$ > 48,7 %
hoch	30 Jahre > $MTTF_D$ > 100 Jahre	48,7 % > $F_D(T_M)$ > 18,1 %

Tabelle 1: Darstellung aus DIN EN ISO 13849-1 (Tabelle 3) mit Ergänzung der $F(t)$

$$F(t) = 1 - e^{-\frac{t}{MTTF}} \quad (1)$$

Die Ausfallwahrscheinlichkeit der Mechanik errechnet sich (nach Weibull) zu:

$$F(t) = 1 - e^{-(\frac{t_{LW}}{T})^b} \quad (2)$$

Aus der Formel (2) lassen sich zwei Dinge ableiten:

- (1) kann als Sonderfall von (2) betrachtet werden
  {wenn $b = 1,$}, $\frac{t}{MTTF} = \frac{t_{LW}}{T}$
- $F(t)$ ist nur indirekt von der Zeit abhängig.

Durch Gleichsetzen von (1) und (2) lässt sich mit $t = MTTF$ eine äquivalente $MTTF$ für eine mechanische Komponente errechnen:

$$MTTF = T_m * (\frac{T}{t_{LW}})^b \quad (3)$$

Es handelt sich hier um eine Hilfsgröße, die dazu dient, die Mechanik in der Welt der IEC 61 508 und der DIN EN 62 061 fassbar zu machen.

Auslegung nach Ausfallwahrscheinlichkeit

Betrachtet man die Gleichung (3) wird schnell klar, dass bei Komponenten mit Lebensdauerwerten im Bereich von Millionen Schaltspielen beim Betrieb mit niedriger Anforderungsrate extrem große $MTTF$ errechnet werden.

So ganz falsch ist das nicht. Man vergegenwärtige sich z. B. nur die erstaunliche Funktionstüchtigkeit alter Traktoren auf den immer beliebter werdenden Oldtimerveranstaltungen – die Mechanik funktioniert; die Elektrik (wenn überhaupt jemals vorhanden) ist komplett ausgefallen.

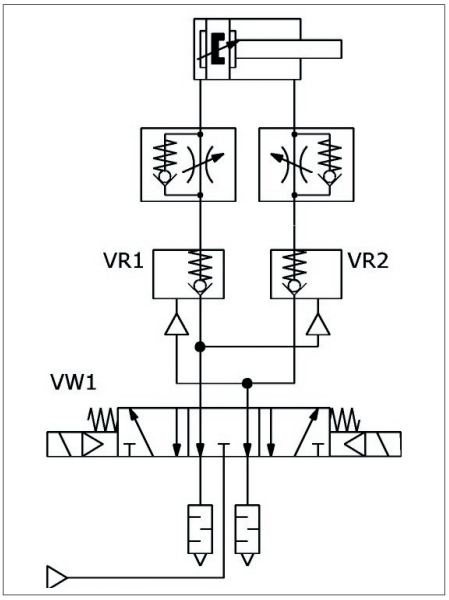
Diese Technik ist ebenfalls ein gutes Beispiel für die konsequente Anwendung teilweise verloren gegangener Ingenieurstugenden:

- dauerfeste Auslegung (der Wöhlerversuch ist seit 1856 in der Technik etabliert),
- Überdimensionierung – > Fehlerausschluss für die Mechanik,
- fehlertolerante Gestaltung („Schaufel Sand darf mit durch").

D. h. gute Konstrukteure sind es seit je gewohnt, die lebensdauerbestimmenden Bauteile entsprechend der veranschlagten Nutzungsdauer (Mission Time T_M) auszulegen.

Üblich ist z. B. die Auslegung von Wälzlagern, Wellen, Achsen Kupplungen usw. nach B_{10}-Wert. Man akzeptiert eine Ausfallwahrscheinlichkeit $F = 10$ % während T_M. In diesem Zusammenhang ist es auch interessant, diesen B_{10}-Wert mit der Klassifikation der $MTTF$ in der DIN EN ISO 13849-1 (oder auch anderen anscheinend sehr großen $MTTF$-Werten) zu vergleichen (**Bild 5**).

Aus dieser Gegenüberstellung lässt sich auch ganz gut ableiten, warum die Konstrukteure bisher immer mit einem gewissen Unverständnis auf die mächtigen Aktivitäten bei der Anwendung der IEC 61508 oder der DIN EN 62061 reagieren – ein Getriebe mit einer Ausfallwahrscheinlichkeit von 48,7 % (nach 20 Jahren) ist für einen Konstrukteur jenseits des Vorstellungsvermö-



6: Steuerkette mit wechselseitig angesteuerten Rückschlagventilen

Tabelle 2: Zusammenstellung der Lebensdauerkennwerte der Komponenten aus Bild 6

		VW1	VR1/VR2	Zylinder
Angaben aus Dokumentation	T	$68*10^6$	$55*10^6$	$14,88*10^6$
	b	1,6	1,8	5,8
mögliche Ursprungswerte	T_{min}	$67,5*10^6$	$54,5*10^6$	$14,875*10^6$
	T_{max}	$68,44*10^6$	$55,44*10^6$	$14,8844*10^6$
	b_{min}	1,55	1,75	5,75
	b_{max}	1,64	1,84	5,84

	$MTTF_D$ [Jahre] +/- 0%	$MTTF_{D1}$ [Jahre] -5%	$MTTF_{D2}$ [Jahre] +5%
VW1	147	103,3	210,5
VR1/VR2	140,5	95,4	208,4
Zylinder	25,4	8,5	79,4

Tabelle 3: Zusammenstellung der errechneten Werte für die MTTFD

gens und würde schlicht als Fehlkonstruktion eingestuft verschrottet werden. Erst wenn ein elektronisches Bauteil eine *MTTF* von 190 Jahren aufweist, besitzt es am Ende der T_m die gleiche Ausfallwahrscheinlichkeit wie das nach B_{10} ausgelegte mechanische Bauteil.

Die Tücken kleiner und großer Zahlen

Bei der Ermittlung der Ausfallwahrscheinlichkeiten steht der Anwender (Konstrukteur) vor einer nicht einfach zu lösenden Aufgabe:

- welche Lebensdauerkennwerte kann er verwenden,
- ist der bestimmungsgemäße Gebrauch für den vorgesehenen Einsatz gegeben,
- welche Annahmen kann er treffen,
- unter welchen Einsatzbedingungen wird die Anlage (bzw. das Produkt) arbeiten,
- wie oft wird die Sicherheitsfunktion angefordert?

Hat der Konstrukteur Glück, stellt ihm der Komponentenlieferant die Lebensdauerkennwerte zur Verfügung.

Für die Darstellung soll wieder das Beispiel mit den Werten: $T = 120 \cdot 10^6$ Schaltspiele, $B_{10} = 64{,}2 \cdot 10^6$ Schaltspiele und Formparameter $b = 3{,}6$ betrachtet werden.

Man kann davon ausgehen, dass alle dargestellten Zahlen durch Runden entstanden sind.

Die Angabe $T = 120 \cdot 10^6$ kann also aus einem Wert, der zwischen $119{,}5 \cdot 10^6$ und $120{,}4 \cdot 10^6$ liegt, durch Runden entstanden sein. Gleiches gilt für den Wert des Formparameters: $3{,}55 < b < 3{,}644$.

Auch die Annahmen für die voraussichtliche Schaltspielzahl beruhen auf Schätzungen. Angenommen eine Maschinenfunktion wird auf

- eine Betriebsfrequenz von 1 Hz,
- 8 h täglichen Gebrauch, 220 Tage im Jahr und
- Einsatzzeit 10 Jahre

ausgelegt. Der Fehler bei diesen Annahmen soll 5 % betragen.

Die entsprechenden Werte in Gleichung (2) eingesetzt, ergeben einmal eine Ausfallwahrscheinlichkeit von $F(10\,y) = 4{,}5$ % und einmal $F(10\,y) = 19$ %. Dagegen geht der „exakt berechnete" Wert von $F(10\,y) = 9{,}5$ % in die weitere Berechnung der Zuverlässigkeit des Gesamtsystems ein.

Durch Einsetzen der entsprechenden Werte in Gleichung (3) erhält man für die *MTTF* einmal einen Wert von 49,9 Jahren und einmal einen Wert von 208,2 Jahren. Die Abweichung zum oberen Wert beträgt jetzt bereits 208,8 % (bzw. nur 47,9 %, siehe dazu auch [4]).

Diese Abweichungen sind an sich noch nicht als besonders groß einzuschätzen. Wesentlich kritischer wird es, wenn ein System an den Grenzen betrieben wird:

- nahe der Charakteristischen Lebensdauer T oder
- im Bereich mit extrem geringer Ausfallwahrscheinlichkeit.

Der Betrieb nahe T ist ein typischer Fall für nicht bestimmungsgemäßen Gebrauch – bei der einen Anwendung funktioniert das System ohne Probleme und bei einer anderen Anwendung häufen sich (hoffentlich nur) die Reklamationen. Ursache können kleine Änderungen der Randbedingungen sein.

Wird die betrachtete Anlage statt 220 Tage im Jahr volle 365 Tage gefahren, steigt die Ausfallwahrscheinlichkeit von 9,5 % bereits auf 46,3 %. Bei derartigen Abweichungen von den projektierten Einsatzdaten werden erfahrungsgemäß auch wichtige Wartungsarbeiten während des Betriebs entfallen. Angenommen, durch schlechte (keine) Wartung der Druckluftaufbereitung steigt der Verschleiß – die Lebensdauer fällt auf $T_{red} = 80{*}10^6$ und der Formparameter steigt auf $b_{Ver} = 4{,}5$. Im Ergebnis steigt die Ausfallwahrscheinlichkeit des Ventils von vorher 9,5 % auf 96,7 %. Aus sicherheitstechnischer Sicht eine Katastrophe.

Aus diesem Beispiel ist schon zu ersehen, wie wichtig die Einhaltung der der Nachrechnung zugrunde liegenden, Betriebsbedingungen ist. Der Betrieb mit geringer Ausfallwahrscheinlichkeit trifft für Komponenten in Sicherheits-Steuerketten zu (so wird man z. B. immer bestrebt sein, die Funktion des Airbags im Auto nicht anfordern zu müssen).

Angenommen, das Ventil mit den Kennwerten aus dem Beispiel soll für die Sicherheitsfunktion eingesetzt werden. Die Sicherheitsfunktion wird einmal pro Tag angefordert (werden an dieser Stelle z. B. für Not-Aus größere Anforderungsraten eingesetzt, sollte man sich mit der Gestaltung der Funktion intensiv auseinandersetzen – womöglich wurden wesentliche Dinge der DIN EN ISO 12100 nicht beachtet).

Versucht man für diesen Anwendungsfall die *MTTF* über die Ausfallwahrscheinlichkeit $F(t)$ auszurechnen, liefert die Tabellenkalkulation die Fehlermeldung #DIV/0!.

Der Grund ist:

- der Term $(t/T)^b$ ist extrem klein,
- $F(t)$ wird damit zu 0,
- der Term $\ln(1\text{-}F)$ der Gleichung $MTTF = -t/\ln(1\text{-}F)$ ergibt 0 und
- die Division durch 0 ist nicht erlaubt.

Vertraut man nicht blind der Allmacht der Tabellenkalkulation und macht sich die Mühe, die Formel entsprechend Gleichung (3) in der Tabellenkalkulation zu definieren, dann erhält man $MTTF = 1{,}128 \cdot 10^{18}$ Jahre. Das ist das 10^8 -fache Alter des Universums nach neuesten Messungen der Entfernung der Hintergrundstrahlung des Hubble-Weltraumteleskops (Hubble-Volumen: 46 Milliarden Lichtjahre)!

Noch extremer werden die Werte beim Betrieb mit niedriger Anforderungsrate: z. B. Anforderung der Funktion kleiner gleich einmal im Jahr (DIN EN 61511). Im konkreten Fall hieße das, das Ventil schaltet während der Einsatzdauer 20 mal. Wobei man davon ruhig ausgehen sollte, dass das Ventil in der Inbetriebnahmephase einige Schaltspiele mehr absolviert haben dürfte. Bei diesen Einsatzfällen muss generell überlegt werden, ob die ermittelten Lebensdauerkennwerte für die Berechnung geeignet sind. Komponenten, die für dermaßen hohe Schaltspiele entwickelt sind, haben ihr Anwendungsgebiet in der klassischen Automatisierungstechnik (Schaltfrequenzen im Bereich von einigen Hz bis zu 1/Tag). Komponenten, deren Dasein im Wesentlichen durch „Nichtstun" gekennzeichnet ist, werden ganz anderen Alterungs- und Verschleißmechanismen unterworfen sein:

- Alterung der Elastomere,
- Kollaps des tribologischen Systems,
- elektrochemische Korrosion,
- Kriech- und Setzvorgänge.

Genaue Rechnung mit ungenauem Ergebnis

Im Folgenden sollen die Auswirkungen der vorher beschriebenen Effekte an Beispielen kompletter Steuerketten gezeigt werden.

Zur Beschreibung der Ausfallwahrscheinlichkeit der Steuerkette soll deren $MTTF_D$ (nach DIN EN ISO 13849-1) ermittelt werden.

Für die Betriebsbedingungen sollen die folgenden Werte gelten:

- $T_M = 10$ Jahre
- $h_{op} = 8$ Stunden/Tag

	$MTTF_D$ [Jahre]	$MTTF_{Dmin}$ [Jahre]	$MTTFD_{max}$ [Jahre]
VW1	147	42,5	1382,6
VR1/VR2	140,5	39,9	1382,6
Zylinder	25,4	6,4	398,5

Tabelle 4: Werte aus Tabelle 3 unter Berück-sichtigung des Ver-trauensbereiches 90% für eine Stichprobe n = 10

- d_{op} = 220 Tage/Jahr
- t_{cycle} = 5s.

Die Abweichung der realen Einsatzdaten soll wieder ± 5 % betragen.

In **Bild 6** ist eine relativ einfache und sehr oft verwendete Steuerkette dargestellt. VW1 steuert die gefährliche Bewegung. Die Rückschlagventile VR1 und VR2 sperren den Zylinder ab. Für die Bauteile sollen die in **Tabelle 2** aufgeführten Werte gelten. Die Anzahl der Schaltzyklen errechnen sich nach [DIN EN ISO 13849-1] AnnexC zu:

$$t_{LW} = \frac{h_{op} * d_{op} * 3600}{t_{cycle}} * \left[\frac{s}{h}\right] \quad (4)$$

Durch Einsetzen in Gleichung (3) wird die jeweilige $MTTF_D$ berechnet.

Die Kombination der Extremwerte:

- maximale Belastung (+ 5 % bei Einsatzdaten) mit niedrigen Lebensdauerkennwerten {Index $_{min}$} und
- minimale Belastung (- 5 % bei Einsatzdaten) mit hohen Lebensdauerkennwerten {Index $_{max}$} ergibt für die Komponenten der Steuerkette die in **Tabelle 3** dargestellten Werte.

Die $MTTF_D$ der gesamten Steuerkette kann mit dem „Parts Count" Verfahren [DIN EN ISO 13849-1], Anhang D berechnet werden:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d,i}} = \sum_{j=1}^{\bar{N}} \frac{n_j}{MTTF_{d,j}} \quad (5)$$

Durch Einsetzen der Ergebnisse aus Tabelle 3 erhält man $MTTF_D$ = 16,55 Jahre (es wurden hier nur die Pneumatikkomponenten berücksichtigt; mit Eingängen, SPS usw. läge der Wert entsprechend niedriger).

Setzt man dagegen die Extremwerte ein, dann ergibt sich

$MTTF_{Dmin}$ = 6,7 Jahre und

$MTTF_{Dmax}$ = 37,1 Jahre.

Durch Vergleich mit Tabelle 3 aus [DIN EN ISO 13849-1] können die Werte wie folgt klassifiziert werden:

- eine $MTTF_D$ von 16,55 Jahren ist als mittel,
- eine $MTTF_D$ von 6,7 Jahre ist als niedrig und
- eine $MTTF_D$ von 37,1 Jahren ist als hoch einzustufen.

Interessant wird es, die mit diesen Werten erreichbaren Kategorien zu betrachten.

Dazu hilft ein Blick in das **Bild 5** aus [DIN EN ISO 13 849-1]. Geht man von einem mittleren DC_{avg} (durchschnittlicher Diagnosedeckungsgrad) aus, ist:

- mit einer mittleren $MTTF_D$ maximal ein *PL* = d bzw. eine Kategorie 3,
- mit einer niedrigen $MTTF_D$ maximal ein *PL* = c bzw. eine Kategorie 3,
- mit einer hohen $MTTF_D$ ein *PL* = e bzw. eine Kategorie 3 erreichbar.

Hieraus ist ersichtlich, dass schon mit kleinen Rundungsfehlern und leichten Abweichungen in den Betriebsbedingungen der Bereich von 3 *PL*'s überstrichen werden kann.

In der Realität bedeutet das: man hat u. U. trotz korrekter Rechnung (mit den erhaltenen Angaben vom Hersteller) für das System ungeeignete Komponenten ausgewählt.

Wie man weiß, streuen die Lebensdauerkennwerte. Die Angaben in den Unterlagen stellen oft den Median dar. Berücksichtigt man die Streuung, ergeben sich (nach [2]) für einen Vertrauensbereich 90 % (nur 5 % der Komponenten liegen mit ihren Lebensdauerkennwerten niedriger) und eine Stichprobengröße 10 die in **Tabelle 4** dargestellten Werte.

Mit (5) ergibt sich jetzt eine $MTTF_D$ für die gesamte Kette:

- $MTTF_{Dmin}$ = 4,4 Jahre und
- $MTTF_{Dmax}$ = 213 Jahre.

Da es sich um eine einkanalige Struktur handelt, kann man (bei korrekter Verwendung des unteren Wertes) mit einer $MTTF_D$ von 4,4 Jahren maximal den *PL* = a erreichen. Ohne Berücksichtigung der aufgeführten Abweichungen würde man dieser Kette einen *PL* = c testieren.

Schlussfolgerungen (Aus Aktivität wird Vorsicht)

Die oben gezeigten Beispiele und Warnungen sollen nun nicht dazu aufrufen, die Quantifizierung zu vernachlässigen, sondern zur Vorsicht raten. Zum einen ist für den Anwender wichtig, dass er die von Herstellern angegebenen Zahlen hinterfragt und deren Entstehung versteht. Zum anderen sollte der Anwender allein aus angegebenen Zahlen nicht notwendigerweise auf die Sicherheit eines Produktes schließen. Die Abweichungen zeigen, dass das Berechnen allein unter zu Hilfenahme von Mittelwerten durchaus kritisch zu betrachten ist. So kann beispielsweise ein Konstruktionsfehler, nicht durch Quantifizierung aufgedeckt werden. Auch sind immer die Einsatzbedingungen einer Komponente an der Anwendung zu spiegeln. Auch sind immer die Auswirkungen der Einsatz- und Umgebungsbedingungen auf die Komponente zu beachten und zu beurteilen. Quantifizierung kann – wenn überhaupt – nur Anhaltspunkte liefern, wie sich ein Produkt unter idealen Bedingungen verhält. Umgebungsbedingungen wie Lastkollektive, Schock, Vibration, Klima haben einen großen Einfluss auf die tatsächliche Lebensdauer eines Produktes. Bei höheren Risiken sollte in jedem Falle überprüft werden, ob einkanalige Systeme, die „schön" gerechnet werden, wirklich unter allen Aspekten den Ansprüchen genügen. Hier sollte zur Beherrschung von Fehlern Redundanz, Diversität und/oder gute Diagnose nicht generell aufgrund „guter" Zahlen verworfen werden. Insbesondere sind die in DIN EN ISO 13849-2 beschriebenen „grundlegenden" und „bewährten Sicherheitsprinzipien" einzuhalten, um auch Rechtssicherheit für das in Verkehr gebrachte Produkt zu erhalten. Letztendlich sollte jedoch immer das Prinzip GSM zur Anwendung kommen (GSM = gesunder Menschenverstand).

Verwendete Formelzeichen

T_M	mission time, Gebrauchsdauer, Dimension [Jahre]
h_{op}	tägliche Betriebsstunden, Dimension [Stunden/Tag]
d_{op}	jährliche Betriebstage, Dimension [Tage/Jahr]
t_{cycle}	Zykluszeit, Dimension [s]
T	charakteristische Lebensdauer, Dimension [Lastwechsel]
b	Formparameter der Weibull-Verteilung, Dimension [dimensionslos]
t_{LW}	Anzahl der Lastwechsel während T_m, Dimension [Lastwechsel]
B_{10}	Anzahl der Lastwechsel, die zu einer Ausfallwahrscheinlichkeit von 10 % führen
$F(t)$	Ausfallwahrscheinlichkeit als Funktion der Zeit [dimensionslos]
$MTTF_D$..	mean time to dangerous failure [Jahre]
PFD	Probability of failure on demand [dimensionslos]
PFH	probabilty of failure per hour [1/h]

Quellen:

Katalogangaben diverser Hersteller (liegen den Autoren vor und werden als schlechte Beispiele besser nicht genannt)

Gutachten von Prüfstellen (liegen den Autoren vor und werden als schlechte Beispiele besser nicht genannt)

[1] Schuster, U., Untersuchung des Alterungsprozesses von hydraulischen Ventilen BIA-Report 6/2004. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2004. ISBN: 3-88383-672-9

[2] B. Bertsche/G. Lechner, „Zuverlässigkeit im Maschinenbau, Springer-Verlag 1999

[3] W. Weibull: „A statistical distribution function of wide applicability." J. Appl. Mech. 18:292–297, 1951.

[4] W. Krämer, „So lügt man mit Statistik", Campus Verlag 1994