9 Literatur

[1] Richtlinie 98/37/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen. ABl. EG Nr. L 207 (1998), S. 1; geänd. durch Richtlinie 98/79/EG - ABl. EG Nr. L 331 (1998), S. 1
http://eur-lex.europa.eu/

[2] DIN EN ISO 12100-1: Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze - Teil 1: Grundsätzliche Terminologie, Methodologie (04.04). Beuth, Berlin 2004

[3] DIN EN ISO 12100-2: Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze - Teil 2: Technische Leitsätze (04.04). Beuth, Berlin 2004

[4] DIN EN ISO 14121-1: Sicherheit von Maschinen – Risikobeurteilung – Teil 1: Leitsätze (12.07). Beuth, Berlin 2007

[5] ISO/TR 14121-2: Sicherheit von Maschinen – Risikobeurteilung – Teil 2: Praktische Anleitung und Verfahrensbeispiele (12.07). Beuth, Berlin 2007

[6] DIN EN ISO 13849-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (07.07). Beuth, Berlin 2007

[7] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (12.03). Beuth, Berlin 2003

[8] Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung). ABl. EU Nr. L 157 (2006), S. 24; mit Berichtigung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG vom 9. Juni 2006. ABl. EU Nr. L 76 (2007), S. 35
http://eur-lex.europa.eu/

[9] *Ostermann, H.-J.; von Locquenghien, D.:* Wegweiser Maschinensicherheit. Bundesanzeiger Verlagsgesellschaft, Köln 2007

[10] *Reudenbach, R.:* Sichere Maschinen in Europa – Teil 1: Europäische und nationale Rechtsgrundlagen. 8. Aufl., Verlag Technik & Information, Bochum 2007

[11] DIN EN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (03.97). Beuth, Berlin 1997

[12] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 0 bis Teil 7 (11.02 bis 10.05). Beuth, Berlin 2002 bis 2005

[13] DIN EN 62061: Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (10.05 und Berichtigung 1 06.06). Beuth, Berlin 2005

[14] *Bömer, T.:* Funktionale Sicherheit nach IEC 61508. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 219. 47. Lfg. XII/2005. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.
www.bgia-handbuchdigital.de/330219

[15] *Hauke, M.; Schaefer, M.:* Sicherheitsnorm mit neuem Konzept. O + P Ölhydraulik und Pneumatik 50 (2006) Nr. 3, S. 142-147
www.dguv.de/bgia/de/pub/grl/pdf/2006_016.pdf

[16] *Schaefer, M.; Hauke, M.:* Performance Level Calculator – PLC. 3. Aufl. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin; Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) e.V. – Fachverband Automation, Frankfurt am Main, und Verband Deutscher Maschinen- und Anlagenbau e.V. – VDMA, Frankfurt am Main 2008
www.dguv.de/bgia, Webcode d3508

[17] Summary list of titles and references of harmonised standards under Directive 98/37/EC on Machinery. Hrsg.: European Commission
http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist/machines.html

[18] *Reinert, D.:* Risikobezogene Auswahl von Steuerungen. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 320 100. 31. Lfg. I/98. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.
www.bgia-handbuchdigital.de/320100

[19] DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (04.08). Beuth, Berlin 2008

[20] DIN EN 60204-1: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen. Teil 1: Allgemeine Anforderungen (06.07). Beuth, Berlin 2007

[21] Interpretationen zu Vorschriften: Wesentliche Veränderung von Maschinen. Hrsg.: Berufsgenossenschaft der chemischen Industrie (06/2005)
www.bgchemie.de/webcom/show_article.php/_c-781/_nr-2/i.html

[22] *Apfeld, R.; Huelke, M.; Lüken, K.; Schaefer, M., et al.:* Manipulation von Schutzeinrichtungen an Maschinen. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2006
www.dguv.de/bgia, Webcode d6303

[23] Berufsgenossenschaftliche Information BGI 5048-1 und -2: Ergonomische Maschinengestaltung, Checkliste, Auswertungsbogen und Merkheft (10.2006). Carl Heymanns, Köln 2006
www.dguv.de/bgia, Webcode d3443

[24] VDI/VDE 3850 Blatt 1: Nutzergerechte Gestaltung von Bediensystemen von Maschinen (5/2000). Blatt 2: Nutzergerechte Gestaltung von Bediensystemen von Maschinen – Interaktionsgeräte für Bildschirme (11/2002). Blatt 3: Nutzergerechte Gestaltung von Bediensystemen für Maschinen – Dialoggestaltung für Touchscreens (3/2004). Beuth, Berlin

[25] *Birolini, A.:* Qualität und Zuverlässigkeit technischer Systeme: Theorie, Praxis, Management. 3. Aufl., Springer, Berlin 1991

[26] DIN EN 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (12.02). Beuth, Berlin 2002

[27] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (06.03). Beuth, Berlin 2006

[28] Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten GS-ET-26. Hrsg.: Fachausschuss Elektrotechnik, Köln 2002
www.dguv.de/bgia, Webcode d14884

[29] DIN EN 61784-3: Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen (IEC 61784-3:2007) (11.08). Beuth, Berlin 2008

[30] *Reinert, D.; Schaefer, M.:* Sichere Bussysteme für die Automation. Hüthig, Heidelberg 2001

[31] *Huckle, T.:* Kleine BUGs, große GAUs. Vortrag zum Thema „Softwarefehler und ihre Folgen“.
http://www5.in.tum.de/~huckle/bugsn.pdf

[32] DIN EN 61508-3: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:1998 und Corrigendum 1999) (12.02). Beuth, Berlin 2002

[33] DIN EN 61131-3: Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (12.03). Beuth, Berlin 2003

[34] *Schaefer, M.; Gnedina, A.; Bömer, T.; Büllesbach, K.-H.; Grigulewitsch, W.; Reuß, G.; Reinert, D.:* Programmierregeln für die Erstellung von Software für Steuerungen mit Sicherheitsaufgaben. Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Dortmund, Fb 812. Wirtschaftsverlag NW, Bremerhaven 1998 (vergriffen, auszugsweise unter:
www.dguv.de/bgia, Webcode d3250

[35] MISRA Development Guidelines for Vehicle Based Software. Hrsg.: The Motor Industry Software Reliability Association
www.misra.org.uk

[36] SN 29500: Ausfallraten – Bauelemente – Erwartungswerte. Hrsg.: Siemens AG, Center for Quality Engineering, München 1994 bis 2005

[37] DIN EN 574: Sicherheit von Maschinen – Zweihandschaltungen – Funktionelle Aspekte; Gestaltungsleitsätze (02.97). Beuth, Berlin 1997

[38] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005

[39] Norm-Entwurf DIN IEC 61508-2; VDE 0803-2:2006-07: Funktionale Sicherheit sicherheitsbezogener eletrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (07.06). Beuth, Berlin 2006

[40] *Kleinbreuer, W.; Kreutzkampf, F.; Meffert, K.; Reinert, D.:* Kategorien für sicherheitsbezogene Steuerungen nach EN 954-1. BGIA-Report 6/97. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 1997
www.dguv.de/bgia, Webcode d15190

[41] DIN EN 982: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Hydraulik (09.96). Beuth, Berlin 1996

[42] DIN EN 983: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Pneumatik (09.96). Beuth, Berlin 1996

[43] DIN EN 1037: Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf (04.96), Beuth, Berlin 1996

[44] DIN ISO 1219-1: Fluidtechnik – Graphische Symbole und Schaltpläne – Teil 1: Graphische Symbole für konventionelle und datentechnische Anwendungen (12/07). Beuth, Berlin 2007

[45] DIN ISO 1219-2: Fluidtechnik – Graphische Symbole und Schaltpläne – Teil 2: Schaltpläne (11.96). Beuth, Berlin 1996

[46] ISO 8573-1: Druckluft – Teil 1: Verunreinigungen und Reinheitsklassen (02.01). Beuth, Berlin 2001

[47] ISO 8573-1: Druckluft – Teil 1: Verunreinigungen und Reinheitsklassen; Korrektur 1 (04.02). Beuth, Berlin 2002

Anhang A:
Beispiele zur Risikobeurteilung

Beispiel 1: Schließkantensicherung

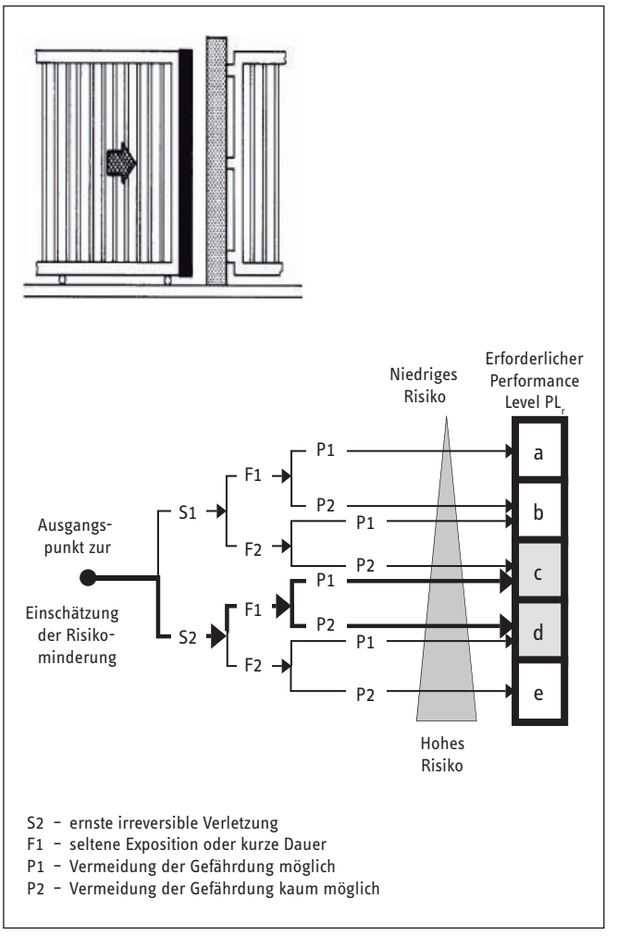
In Abbildung A.1 ist die Risikobeurteilung für die Sicherheitsfunktion

- SF1 Unterbrechung der Schließbewegung und Reversieren

einer Schließkantensicherung[1] dargestellt. Mit der Bewegung kraftbetätigter Fenster-, Tür- und Torflügel (siehe Abbildung A.1) ist in der Regel die Bildung von Quetsch- und Scherstellen verbunden. Diese Gefahrstellen bestehen im Allgemeinen nur dann, wenn sich der Flügel seinen Endstellungen nähert. Verletzungen von Personen an derartigen Gefahrstellen lassen sich z.B. durch Schließkantensicherungen vermeiden. Schließkantensicherungen, z.B. Schaltleisten, werden auf die Schließkanten der Flügel gesetzt. Bei Erkennung eines Hindernisses wird die Schließbewegung unterbrochen und eine rückläufige Bewegung eingeleitet.

Quetsch- und Scherstellen können an kraftbetätigten Fenster-, Tür- und Torflügeln Ursache für schwere, unter Umständen tödliche Verletzungen sein, sodass als Schadensausmaß S2 angenommen werden muss. Personen halten sich im Bereich der zeitlich begrenzt auftretenden Quetsch- und Scherstellen nur selten und auch nur für kurze Zeit auf (F1). Normalerweise haben gefährdete Personen die Möglichkeit, sich aus dem vom bewegten Flügel gebildeten Gefahrenbereich zu entfernen (P1), damit ergibt sich ein erforderlicher Performance Level PL_r = c. Bei Schnelllauftoren ist diese Möglichkeit eingeschränkt (P2) und es ergibt sich ein erforderlicher Performance Level PL_r = d.

Abbildung A.1:
Risikobeurteilung für die Schließkantensicherungen an kraftbetätigten Fenstern, Türen und Toren



[1] *Schließkantensicherungen fielen bisher unter die Bauproduktrichtlinie. Da die eingesetzten Schaltleisten jedoch Sicherheitsbauteile nach der Maschinenrichtlinie sind, werden auch Schließkantensicherungen nach dieser Richtlinie bewertet.*

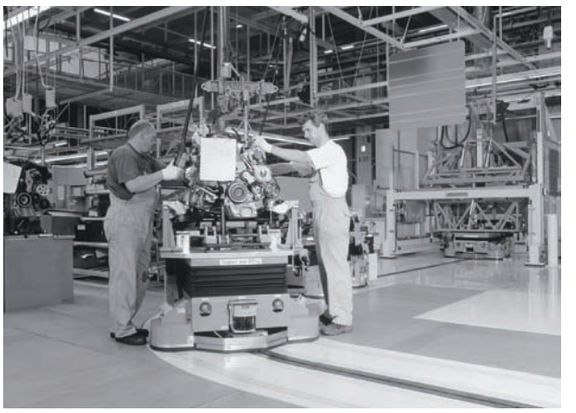
Beispiel 2: Fahrerloses Transportfahrzeug

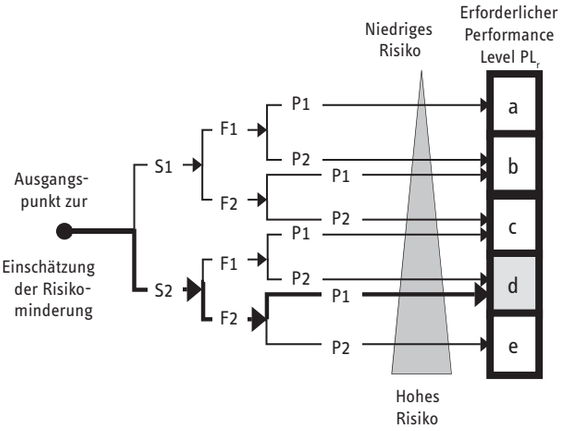
An fahrerlosen Transportfahrzeugen wird für den Auffahrschutz die Sicherheitsfunktion

- SF1 Stillsetzen des Transportfahrzeugs

eingesetzt. Da sich ein fahrerloses Transportfahrzeug unter Umständen mit tonnenschwerer Last bewegt, ist eine schwere irreversible Verletzung bei einer Kollision mit dem Fahrzeug, wenn sie bei voller Geschwindigkeit stattfindet, wahrscheinlich (S2). Die Fahrwege des Fahrzeugs sind für Personen frei zugänglich; deshalb muss mit einem relativ häufigen Aufenthalt von Personen im Gefahrenbereich gerechnet werden (F2). Da das Fahrzeug mit recht niedriger Geschwindigkeit fährt (in der Regel 3 bis 5 km/h), hat ein Fußgänger bei Herannahen eines solchen Fahrzeugs meist die Möglichkeit auszuweichen (P1). Für SF1 ergibt sich damit ein erforderlicher Performance Level PL_r = d (siehe Abbildung A.2)

Abbildung A.2:
Risikobeurteilung für den Auffahrschutz an einem fahrerlosen Flurförderzeug





S2 – ernste irreversible Verletzung
F2 – häufige Exposition oder lange Dauer
P1 – Vermeidung der Gefährdung möglich

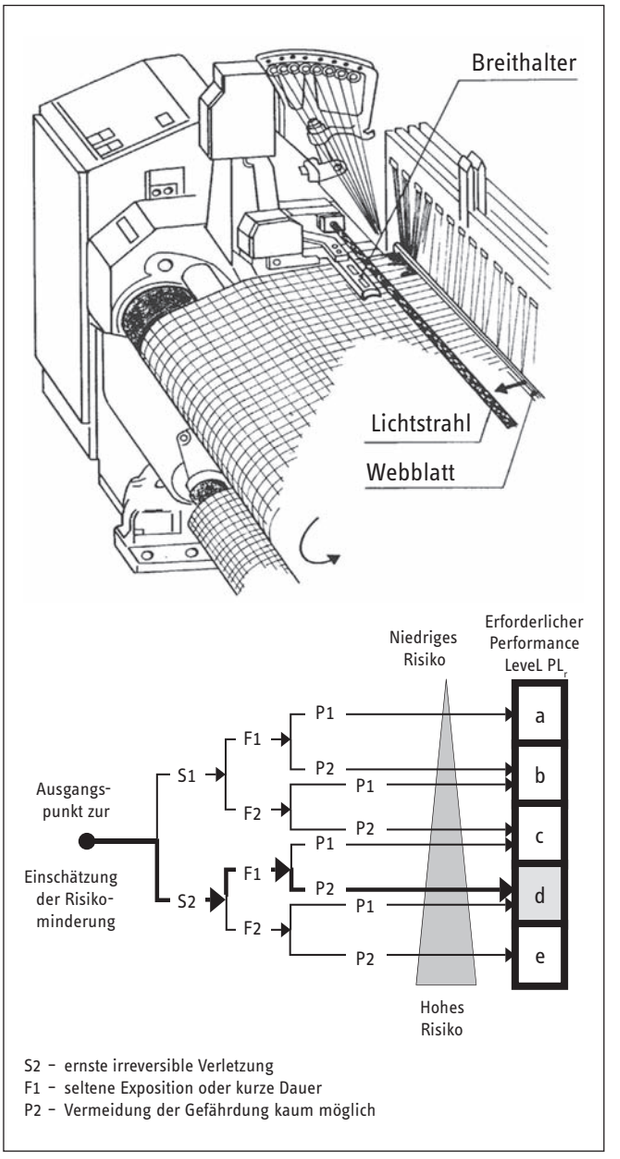
Beispiel 3: Webmaschine

Webmaschinen werden zum vollautomatischen Weben von Stoffen eingesetzt. Die wesentliche Gefährdung besteht in der Quetschung zwischen Webblatt und Breithalter. Bei Kettfadenbrüchen muss der Weber bei stehender Maschine in die Gefahrenstelle eingreifen, um die Kettfadenenden wieder zu verbinden. Zur Verhinderung des unerwarteten Anlaufs wird die Sicherheitsfunktion

- SF1 Sicher abgeschaltetes Moment

eingesetzt. Bei einem Maschinenanlauf kann der Weber Fingerquetschungen und -brüche davontragen (S2). Die Häufigkeit bzw. Dauer der Gefährdungsexposition kann mit selten bezeichnet werden (F1). Befindet sich der Weber mit den Händen bereits im Gefahrenbereich, während es zu einem unerwarteten Anlauf kommt, ist diese Bewegung so schnell, dass ein Ausweichen kaum möglich ist (P2). Damit ergibt sich für SF1 ein erforderlicher Performance Level PL_r = d (siehe Abbildung A.3).

Abbildung A.3:
Risikobeurteilung für eine Webmaschine



Beispiel 4: Rotationsdruckmaschine

In einer Rollenrotationsdruckmaschine wird eine Papierbahn durch eine Vielzahl von Zylindern geführt. Insbesondere für den Einsatz im Zeitungsdruck werden hohe Verarbeitungsgeschwindigkeiten und hohe Drehzahlen der Zylinder erreicht. Wesentliche Gefährdungen bestehen an den Einzugsstellen der gegenläufigen Zylinder. In diesem Beispiel wird eine Gefahrenstelle einer Druckmaschine betrachtet, an der zu Wartungsarbeiten manuelle Eingriffe bei reduzierten Maschinengeschwindigkeiten durchgeführt werden. Der Zugang zur Einzugsstelle wird durch eine Schutztür (Verschutzung) gesichert. Folgende Sicherheitsfunktionen sind vorgesehen:

- SF1 – Durch das Öffnen der Schutztür während des Betriebs werden die Zylinder bis zum Stillstand abgebremst.
- SF 2 – Bei geöffneter Schutztür dürfen Maschinenbewegungen nur mit begrenzten Drehzahlen erfolgen.
- SF 3 – Bei geöffneter Schutztür sind Bewegungen nur während der Betätigung eines Tipptasters möglich.

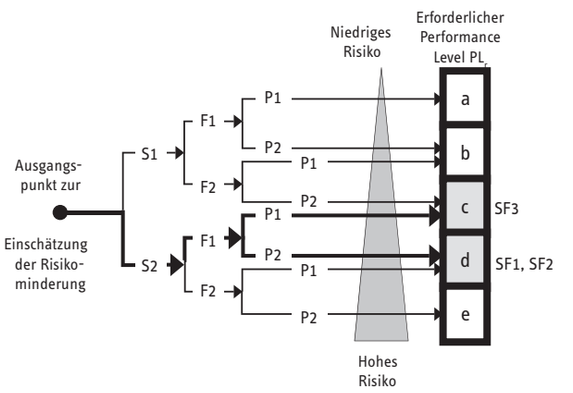
Ein Einzug zwischen die Zylinder führt zu schweren Verletzungen (S2). Da Tätigkeiten im Gefahrenbereich nur zu Wartungsarbeiten anfallen, kann die Häufigkeit bzw. Dauer der Gefährdungsexposition mit selten bezeichnet werden (F1). Die Möglichkeit, der gefahrbringenden Bewegung auszuweichen, ist bei Produktionsgeschwindigkeiten nicht gegeben (P2). Für die Sicherheitsfunktionen SF1 und SF2 ergibt sich daher ein erforderlicher Performance Level PL_r = d (siehe Abbildung A.4). Die Sicherheitsfunktion SF3 jedoch kann nur dann verwendet werden, wenn die Druckmaschine zuvor stillgesetzt (SF1) und die zulässige Zylinderdrehzahl begrenzt wurde (SF2). Damit sind die möglichen Maschinenbewegungen für den Bediener überschaubar und er kann den gefahrbringenden Bewegungen ausweichen (P1). Für SF3 ist daher ein erforderlicher Performance Level PL_r = c ausreichend (siehe Abbildung A.4). Wie man diese Sicherheitsfunktionen realisieren kann, ist in Kapitel 8 im Beispiel 24 auf Seite 160 ff. beschrieben.

Die Beispiele 1 bis 3 sind dem BGIA-Handbuch [1] entnommen, in dem sich zahlreiche weitere Anwendungen aus dem Maschinenschutz finden.

Literatur

[1] BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de

Abbildung A.4:
Risikobeurteilung an einer Rotationsdruckmaschine



S2 – ernste irreversible Verletzung
F1 – seltene Exposition oder kurze Dauer
P1 – Vermeidung der Gefährdung möglich
P2 – Vermeidung der Gefährdung kaum möglich

Anhang B:
Sicherheitsbezogenes Blockdiagramm und FMEA

Zum Nachweis von Kategorie und Performance Level (PL) nach DIN EN ISO 13849-1 muss die Struktur eines sicherheitsgerichteten Systems unter dem Aspekt der zu realisierenden Sicherheitsfunktion (ggf. mehrerer Funktionen separat) analysiert werden. Für den obligatorischen quantitativen Nachweis des PL müssen Systeminformationen auf geeignete Weise aufbereitet werden, damit die quantitative Größe *PFH* (Probability of a Dangerous Failure per Hour) oder direkt der darauf basierende PL bestimmt werden kann. Zwei wichtige Schritte auf diesem Weg sind das sicherheitsbezogene Blockdiagramm und die funktionsblockweise durchgeführte Ausfalleffektanalyse FMEA (Failure Mode and Effects Analysis).

B1 Zweck und Erstellung eines sicherheitsbezogenen Blockdiagramms

Das Ergebnis der unter sicherheitstechnischem Blickwinkel erfolgenden Analyse der Systemstruktur wird zweckmäßig in Form eines Blockdiagramms dargestellt, das man als „sicherheitsbezogenes Blockdiagramm“ bezeichnen kann. Im Diagramm soll zum Ausdruck kommen, ob die Sicherheitsfunktion ganz oder teilweise ein- oder mehrkanalig ausgeführt wird und welche Diagnosemöglichkeiten bestehen, um interne Bauelementausfälle zu erkennen. Weil unter dem hier interessierenden Aspekt der Quantifizierung von Ausfallwahrscheinlichkeiten die Diagnose ein Kompensationsmittel für Bauelementausfälle ist, wird in diesem Anhang anstelle des sonst üblichen Begriffs „Fehlererkennung“ der Ausdruck „Ausfallerkennung“ verwendet.

In der Maschinensicherheit akzeptiert man meistens, dass infolge eines Steuerungsausfalls anstelle der Ausführung der ursprünglich vorgesehenen Sicherheitsfunktion eine Ersatzreaktion erfolgt, die einen sicheren Zustand herbeiführt, z.B. die Betriebshemmung mit energielosen Ausgängen (Abschaltsystem, englisch: Shut-Down-System). Kategorie und PL sollen gemäß DIN EN ISO 13849-1 eine Aussage allein über die sicherheitstechnische Qualität machen und nicht über die Wahrscheinlichkeit des störungsfreien Betriebs, die „Verfügbarkeit“. Daher werden Signalpfade, die im Fehlerfall einen sicheren Zustand herbeiführen, genauso als vollwertig angesehen wie Funktionseinheiten, die eine unter Umständen komplizierte Sicherheitsfunktion ausführen. Ein solcher „einfacher Sicherheits-Signalpfad“ ist jedoch nur dann ein eigenständiger „Kanal“, wenn er ständig im Eingriff ist. Kann der Sicherheitspfad erst nach Aufdeckung eines Ausfalls im eigentlichen Haupt-Funktionspfad aktiv werden, so hängt sein Nutzen für die Sicherheit von der Qualität der Ausfallerkennung ab. Diese Qualität wird durch den Diagnosedeckungsgrad des Mechanismus zur Ausfallerkennung beschrieben. In solch einem Fall stellt der Sicherheitspfad in der Regel nur eine Testeinrichtung mit Abschaltweg zur Verfügung. Derartige Architekturmerkmale müssen im sicherheitsbezogenen Blockdiagramm korrekt zum Ausdruck kommen. Die unterschiedliche Darstellung einer echten Zweikanaligkeit und eines überwachten Einzelkanals ist gut zu erkennen, wenn man die Bilder 10 und 11 der Norm vergleicht.

Betrachtet werden muss auch, ob Bauelemente oder Schaltungsteile vorhanden sind, die zwar nicht die Sicherheitsfunktion oder die sicherheitsgerichtete Ersatzfunktion für den Fehlerfall ausführen, die aber bei bestimmten Bauteilausfällen die ordnungsgemäße Ausführung der Sicherheits- bzw. Ersatzfunktion durch andere Bauelemente verhindern können. Solche Schaltungsteile können notwendige Hilfsfunktionen wie z.B. die Spannungsversorgung oder Steuerungsfunktionen ohne (beabsichtigte) Sicherheitsbedeutung bereitstellen, jedoch mit einer Rückwirkung auf sicherheitsbezogene Teile. Bauelemente und Teilschaltungen müssen immer dann in einem Funktionsblock berücksichtigt werden, wenn von ihnen bei Ausfällen eine schädliche Wirkung auf die Sicherheitsfunktion, ihre Ersatzfunktion oder Diagnosefunktionen ausgehen kann. Beispielsweise muss bei Bauteilen zur Sicherstellung der elektromagnetischen Verträglichkeit (EMV) betrachtet werden, ob ihr Ausfall, z.B. ein Kondensatorkurzschluss, negative Auswirkung auf sicherheitsrelevante Schaltungen hat.

Teilschaltungen mit definierten Ein- und Ausgängen können als Funktionsblock aufgefasst werden. Um die Anzahl der benötigten Funktionsblöcke möglichst gering zu halten, können funktional in Reihe geschaltete Teilschaltungen, also Schaltungen, die nacheinander verschiedene Schritte der Signalverarbeitung ausführen, zu einem Funktionsblock zusammengefasst werden. Bei anders angeordneten Blöcken sollte die Zusammenfassung sinnigerweise nur so weit gehen, dass Redundanzen wie z.B. getrennte Abschaltpfade und die gegenseitige Diagnose von Funktionsblöcken noch zum Ausdruck kommen. Am Ende der Schaltungsanalyse muss ein Blockdiagramm stehen, das all jene Strukturen widerspiegelt, die sicherheitstechnisch bedeutsam sind:

- einfach vorhandene oder parallele Signalpfade („Kanäle“), die zur Ausführung der Sicherheitsfunktion dienen
- Signalpfade, die im Fehlerfall eine sicherheitsgerichtete Ersatzfunktion ausführen
- Schaltungen zur Ausfallerkennung (Diagnose)

Wenn Hilfsschaltungen, die für die Ausführung der Sicherheitsfunktion oder für eine andere sicherheitsgerichtete Aktion benötigt werden (z.B. Netzteile, Oszillatoren), nur einen Kanal beeinflussen können, so sollten sie dem oder den Funktionsblöcken dieses Kanals zugeordnet werden. Wirken diese Hilfsschaltungen auf mehrere Kanäle, dann bilden sie im sicherheitsbezogenen Blockdiagramm einen separaten einkanaligen Teil (Funktionsblock). Entsprechendes gilt für Schaltungen, die durch eine bestimmte Art ihres Ausfalls die Ausführung der Sicherheitsfunktion, einer anderen sicherheitsgerichteten Aktion oder der Diagnose verhindern können (z.B. Schaltungen zum Anwählen einer sicheren Betriebsart oder manche Bauelemente zur Sicherstellung der EMV).

Über Schaltpläne und Stücklisten muss der Inhalt jedes Funktionsblocks eindeutig bestimmt sein. Wegen der Art seiner Erstellung und seines speziellen Zweckes unterscheidet sich das sicherheitsbezogene Blockdiagramm im Allgemeinen von Blockdiagrammen, die anderen Zwecken dienen, z.B. solchen, die sich an einem mechanischen Aufbau von Baugruppen orientieren.

Abbildung B.1 zeigt als Beispiel das sicherheitsbezogene Blockdiagramm einer einkanaligen Maschinensteuerung in Kategorie 2 mit

- einem Mikrocontroller,
- einer Lichtschranke zur Gefahrstellenüberwachung,
- einem „Watchdog“ zur Erkennung von einigen Controller-Fehlfunktionen,
- einer geregelten Motorantriebssteuerung (Frequenzumrichter), die vom Controller angesteuert wird und
- einem Motorabschaltorgan, das vom Watchdog betätigt werden kann (Impulssperre).

Die Sicherheitsfunktion besteht im Abschalten des Motors, sobald und solange der Lichtstrahl der Lichtschranke unterbrochen wird („Sicher abgeschaltetes Moment“ bzw. „Safe Torque Off“). Der Mikrocontroller und die nachgeschaltete Antriebssteuerung führen neben der Sicherheitsfunktion noch verschiedene andere Maschinenfunktionen aus, die hier nicht betrachtet werden, weil sie keine Sicherheitsfunktionen sind. Obwohl in diesem Beispiel die Sicherheitsfunktion allein mit elektrotechnischen Mitteln realisiert wird, gelten die beschriebenen Prinzipien für das sicherheitsbezogene Blockdiagramm und die FMEA Technologie übergreifend.

Im sicherheitsbezogenen Blockdiagramm erscheinen nur Funktionsblöcke, die mit der Sicherheitsfunktion „Sicher abgeschaltetes Moment“ im Zusammenhang stehen, und keine Bedien- und Anzeigeorgane für andere Maschinenfunktionen. Eventuell kann von einigen Bauelementen dieser Schaltungsteile im Fehlerfall eine die Sicherheitsfunktion störende Rückwirkung ausgehen. Nur dann sind diese Bauelemente denjenigen Funktionsblöcken zuzurechnen, die sie zum Ausfall bringen können.

Oftmals wird das sicherheitsbezogene Blockdiagramm wie im vorgestellten Beispiel die Gestalt einer der „vorgesehenen Architekturen“ nach der Norm DIN EN ISO 13849-1, Abschnitt 6.2, (Abschnitte 6.2.1 bis 6.2.7 dieses Reports) haben. Dann kann das in Abschnitt 4.5.4 der Norm dargestellte Verfahren (ergänzt durch die Anhänge B, C, D, E, I und K) zur quantitativen Bestimmung des Performance Levels angewendet werden. Es ist aber nicht ratsam, eine andere Struktur „gewaltsam“ in die Form einer dieser Architekturen zu pressen. Möglicherweise lässt sich eine aktuell vorliegende Systemstruktur auch in Teile zerlegen, die jeweils stückweise einer vorgesehenen Architektur entsprechen. Gelingt eine solche Zerlegung nicht, so muss für das gegebene sicherheitsbezogene Blockdiagramm ein eigenes Modell zur quantitativen Bestimmung der sicherheitsbezogenen Zuverlässigkeit erstellt werden. Eine Einführung in geeignete Modellierungstechniken findet man beispielsweise in [1].

B2 Zweck und Eigenart einer FMEA für die Quantifizierung

Für den quantitativen Nachweis des PL muss die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (*PFH*) abgeschätzt werden. Dies kann mithilfe eines eigens für das vorliegende System erstellten Rechenmodells (z.B. Markov-Modell) geschehen. Lässt aber das sicherheitsbezogene Blockdiagramm wie im Beispiel aus Abbildung B.1 formal die Gestalt einer der „vorgesehenen Architekturen“ gemäß Abschnitt 6.2.3 bis 6.2.7 erkennen, so kann das oben erwähnte Verfahren dieser Norm zur quantitativen Bestimmung des PL angewendet werden. In beiden Fällen muss von den Funktionsblöcken des sicherheitsbezogenen Blockdiagramms jeweils die Ausfallrate in die gefährliche (sicherheitstechnisch ungünstige) Richtung bzw. ihr Kehrwert, die $MTTF_d$ (Mean Time to Dangerous Failure, mittlere Zeit bis zum Ausfall in die gefährliche Richtung), und der *DC* (Diagnostic Coverage, Diagnosedeckungsgrad) bekannt sein. Zur Ermittlung dieser Daten dient die FMEA in einer speziellen Ausprägungsart, die Bauelementausfallraten als quantitative Größen einbezieht. Darin unterscheidet sich die hier verwendete besondere Form der FMEA von den meisten anderen FMEA-Spielarten, die anderen Zwecken dienen, beispielsweise der entwicklungsbegleitenden Problemfrüherkennung und Fehlervermeidung [2].

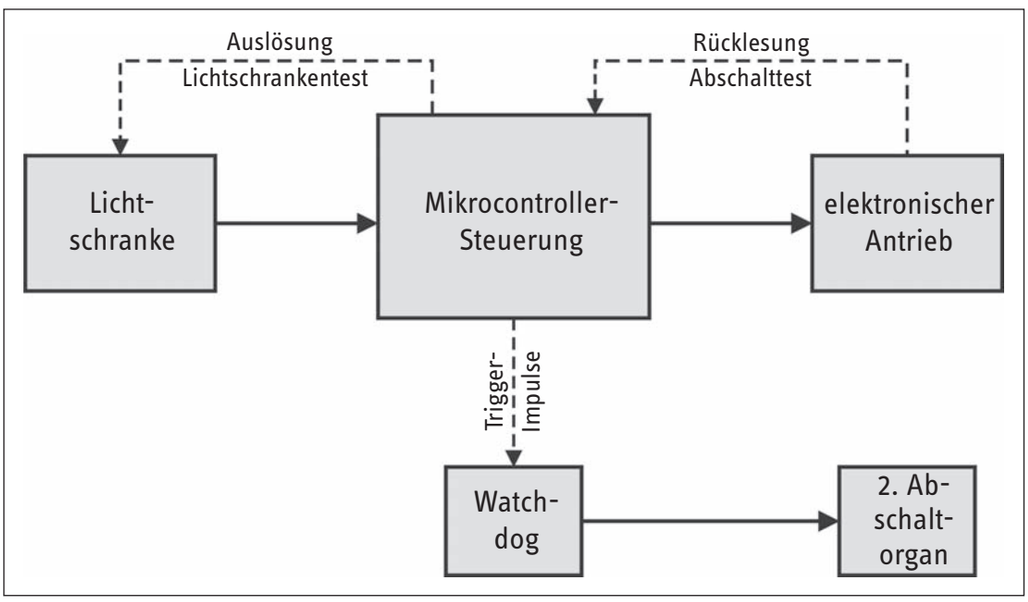


Abbildung B.1: Beispiel für das sicherheitsbezogene Blockdiagramm einer einkanaligen Maschinensteuerung in Kategorie 2

Besonderes Merkmal einer FMEA für Quantifizierungszwecke ist ihre Gliederung entsprechend den Funktionsblöcken des sicherheitsbezogenen Blockdiagramms. Im Prinzip wird für jeden dieser Funktionsblöcke eine separate FMEA durchgeführt, die nur für den jeweiligen Funktionsblock Ergebnisse liefert. Die funktionsblockbezogenen Ergebnisse werden erst nachträglich zusammengeführt, indem sie gemeinsam über ein systemspezifisches Rechenmodell oder das vereinfachte Quantifizierungsverfahren aus DIN EN ISO 13849-1 in die Ermittlung der *PFH* bzw. des PL einfließen.

B2.1 Ausführung einer FMEA für die Quantifizierung

Im Folgenden wird die prinzipielle Vorgehensweise bei einer Quantifizierungs-FMEA am Beispiel des Funktionsblocks „Lichtschranke“ aus Abbildung B.2 demonstriert. Zu diesem Zweck wurde die Schaltung bewusst einfach gehalten. Nur die gestrichelt eingerahmten Bauelemente gehören zum Funktionsblock. Die Elemente S1 und P2 sind eine Ersatzschaltung für die reale Einbindung des Funktionsblocks innerhalb des Systems nach Abbildung B.1. Solange der Fototransistor K1 Licht von der Infrarot-LED P1 empfängt, hält er den Transistor K2 gesperrt, wodurch der Transistor K3 leitet und an Anschluss X1.2 eine positive Ausgangsspannung ansteht, die mit dem Voltmeter P2 messbar ist. Wird der Lichtstrahl unterbrochen, so sperrt K1, K2 wird leitend und K3 schaltet die Ausgangspannung ab. Der Test des Funktionsblocks „Lichtschranke“, den die Mikrocontroller-Steuerung aus Abbildung B.1 programmgesteuert durchführt, kann mit dem Taster S1 und dem Voltmeter P2 simuliert werden: Die Lichtquelle P1 wird kurzzeitig ausgeschaltet und dabei wird geprüft, ob die Ausgangsspannung ordnungsgemäß auf Null Volt absinkt. Den signalverarbeitenden Elementen des Funktionsblocks „Lichtschranke“ (K1 bis K3, R2 bis R9, C1) wird dabei dasselbe Verhalten abverlangt wie bei einer „echten“ Anforderung der Sicherheitsfunktion durch Unterbrechen des Lichtstrahls. Dieser Test wird im Folgenden als „Test 1“ bezeichnet.

B2.2 Gefährliche Ausfallrichtung eines Funktionsblocks

Als erster Schritt muss die gefährliche Ausfallrichtung des Funktionsblocks bestimmt werden. Im Allgemeinen können nicht nur einzelne Bauelemente, sondern in der Folge auch ein ganzer Funktionsblock auf verschiedene Weise ausfallen. Als „gefährliche“ Ausfallrichtung eines Funktionsblocks gelten diejenigen Arten des Ausfalls, die aus sicherheitstechnischer Sicht ungünstig sind. Manche Ausfälle lassen das ganze System direkt gefährlich ausfallen, sodass es weder die ursprüngliche Sicherheitsfunktion noch eine sicherheitsgerichtete Ersatzaktion ausführen kann. Andere Ausfälle erhöhen die Wahrscheinlichkeit, dass dies geschieht, indem jetzt weniger weitere Ausfälle ausreichen, um das System gefährlich ausfallen zu lassen. Gibt es für den ausfallenden Funktionsblock keine Redundanz, also keinen zweiten Kanal, der seine Funktion ersetzen kann, und wird nicht durch Diagnose hinreichend schnell eine Aktion ausgeführt, die einen sicheren Zustand erzeugt, so führt der gefährliche Ausfall des Funktionsblocks zum gefährlichen Ausfall des Systems. Aber auch dann, wenn wegen vorhandener Redundanz oder einer schnellen Ausfallreaktion anderer Schaltungsteile keine der möglichen Ausfallarten des infrage stehenden Funktionsblocks einen gefährlichen Systemausfall verursacht, kann und muss seine „gefährliche“ Ausfallrichtung festgestellt werden. Es ist diejenige Ausfallrichtung, die dazu führt, dass der Funktionsblock seinen vorgesehenen Beitrag zu einem sicheren Systemverhalten nicht mehr leistet. Mitunter müssen auch mehrere Ausfallarten, die durch unterschiedliches, aber gleichermaßen schädliches Blockverhalten gekennzeichnet sind, berücksichtigt werden (z.B. dauerhaftes Einschalten und Schwingung am Ausgang). Es ist daher am einfachsten, die gefährliche Ausfallrichtung durch den Verlust der sicherheitstechnisch geforderten Funktion des Funktionsblocks zu beschreiben. Diagnosemöglichkeiten werden erst später berücksichtigt und bleiben bei diesem Schritt zunächst außer Acht. Beim vorliegenden Beispiel (Lichtschranke, Abbildung B.2) soll die Ausgangsspannung des Funktionsblocks auf

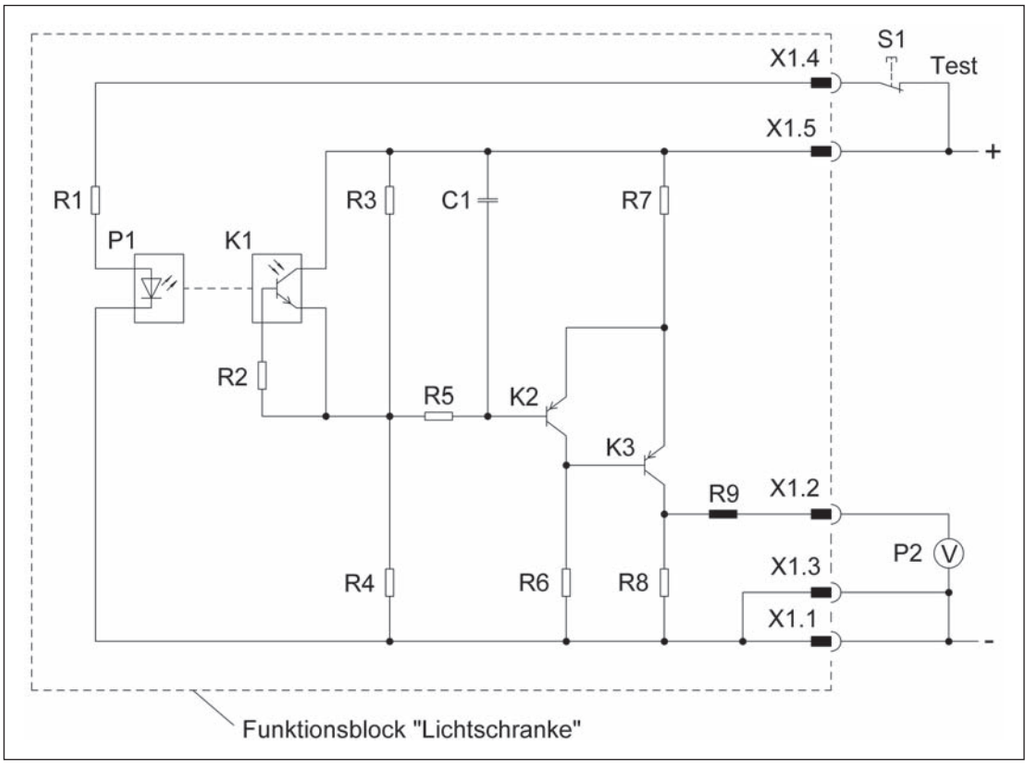


Abbildung B.2: Angenommene Schaltung (einfaches Beispiel) des Funktionsblocks „Lichtschranke“ aus dem sicherheitsbezogenen Blockdiagramm nach Abbildung B.1

Null abfallen, solange der Fototransistor K1 kein Licht von der LED P1 empfängt, denn darin besteht der Beitrag dieses Funktionsblocks zur Ausführung der Sicherheitsfunktion „Sicher abgeschaltetes Moment bei unterbrochenem Lichtstrahl“. Somit kann die gefährliche Ausfallrichtung des Funktionsblocks beschrieben werden als „Anliegen einer Ausgangsspannung größer als Null bei Nichtbeleuchtung des Fototransistors K1“.

B2.3 Bauelementausfallraten

Verschiedene Datenquellen kommen für Bauelementausfallraten infrage. Beispiele für elektronische Bauelemente sind in [3 bis 6] aufgeführt. Alle diese Quellen enthalten herstellerübergreifende Daten. Auch für mechanische, pneumatische und hydraulische Bauelemente gibt es Sammlungen von Ausfallraten. Bei einzelnen Bauelementen, die nicht in den einschlägigen Verzeichnissen gelistet sind, wird man die Ausfallrate vom Hersteller einholen müssen (z.B. bei speziellen ASICs). Viele gängige Quantifizierungstechniken, auch das vereinfachte Verfahren aus DIN EN ISO 13849-1, Abschnitt 4.5.4, gehen von der zeitlichen Konstanz der Ausfallraten aus, was eine Idealisierung darstellt. Durch entsprechende Dimensionierung und notfalls vorbeugenden Austausch kann erreicht werden, dass die Bauelemente während der Gebrauchsdauer T_M (Mission Time) noch nicht in die Verschleißphase mit stark ansteigender Ausfallrate geraten.

Als schnell verfügbare Quelle für zumeist konservativ (pessimistisch) abgeschätzte Ausfallraten bietet sich DIN EN ISO 13849-1, Anhang C, an. Hier wird insbesondere ein Weg gewiesen, auf dem für zyklisch arbeitende elektromechanische, fluidtechnische und mechanische Einzelkomponenten Ausfallraten aus den sogenannten B_{10}-Werten abgeleitet werden können (siehe Tabelle D.2 dieses Reports).

Sofern keine konservative Abschätzung der Ausfallrate vorliegt, muss bei jedem Bauelement darauf geachtet werden, dass der verwendete Wert unter den im konkreten Anwendungsfall gegebenen Einsatzbedingungen (Temperatur, Strom, Spannung, Verlustleistung ...) gilt. Auch die Eigenerwärmung ist zu berücksichtigen. Gängige Datenquellen, z.B. [3 bis 6], bieten Möglichkeiten, die unter definierten Referenzbedingungen geltenden Basisausfallraten in Werte umzurechnen, die unter davon abweichenden Bedingungen gelten. Geeignete Umrechnungsformeln, jedoch keine Basisausfallraten findet man in [7].

B2.4 Erstellung einer funktionsblockweisen FMEA für Quantifizierungszwecke

Bei der FMEA werden die Bauelemente des Funktionsblocks zunächst einzeln bewertet und daraus die Komplettbewertung des Blocks abgeleitet. Dies geschieht zweckmäßig in Form einer Tabelle, die diesen Prozess und zugleich das Ergebnis dokumentiert. Die FMEA kann mit unterschiedlichem Exaktheitsanspruch ausgeführt werden, was sich in verschieden hohem Aufwand für die Erstellung der dazugehörigen Tabellen widerspiegelt. Eine mögliche Ausführung ist beispielsweise in [8] angegeben. Verbindliche Vorschriften existieren nicht. Die in Abbildung B.3 vorgestellte Variante stellt einen Kompromiss zwischen hohem Akkuratheitsanspruch und Aufwand einerseits und allzu starker Vereinfachung andererseits dar und nimmt Rücksicht auf die Genauigkeit und die Verfügbarkeit der verwendeten Daten. Die dort verwendeten Zahlen sind angenommene Beispielwerte.

Die Bauelemente des Funktionsblocks werden zeilenweise aufgelistet und mit ihren Ausfallraten versehen. Die übliche Einheit der Ausfallrate ist „FIT“ (Failures In Time); 1 FIT = 10^{-9}/h. Als einziger Gewichtsfaktor für die Basisausfallrate erscheint hier der Temperaturfaktor. Der Verzicht auf weitere Anpassungsfaktoren ist dann gerechtfertigt, wenn die Bauelemente im Mittel elektrisch tendenziell überdimensioniert sind, was häufig der Fall ist. Ihre elektrische Belastung liegt dann überwiegend unter der Referenzbelastung, für welche die Basisausfallrate gilt, sodass die entsprechenden Anpassungsfaktoren < 1 sind. Somit bedeutet das Weglassen dieser Faktoren eine Abschätzung zur sicheren Seite und zugleich eine Arbeitsersparnis, weil die genauen elektrischen Betriebswerte für die Bauelemente nicht alle einzeln ermittelt werden müssen. Sobald jedoch bekannt ist, dass die Last bestimmter Bauelemente über der Referenzbelastung liegt, sollten die relevanten Anpassungsfaktoren berücksichtigt werden. Wenn die Basisausfallrate einzelner Bauelemente innerhalb des Funktionsblocks dominiert, was beispielsweise für Prozessoren und Leistungshalbleiter oft zutrifft, dann ist eine genaue Betrachtung und ggf. Berücksichtigung aller erforderlichen Anpassungsfaktoren für diese Bauelemente geboten.

Als nächstes wird die Gesamtausfallrate λ jedes Bauelementes in die Anteile λ_s („safe“ bzw. sichere Richtung) und λ_d („dangerous“ bzw. gefährliche Richtung) aufgeteilt, wozu u.a. die „gefährliche Ausfallrichtung“ des Funktionsblocks bekannt sein muss (s.o.). Nach der „reinen Lehre“ müsste dies in zwei Schritten geschehen: Die Gesamtausfallrate wird zuerst auf die verschiedenen Ausfallarten (z.B. Unterbrechung, Kurzschluss, Drift, Funktionsänderung) verteilt. Im zweiten Schritt werden die auf jede Ausfallart entfallenden Ausfallratenanteile λ_s oder λ_d zugewiesen, je nachdem, ob die betreffende Ausfallart den Funktionsblock in dessen sichere oder gefährliche Richtung ausfallen lässt. Das unveränderte Weiterfunktionieren wird dabei wie ein Ausfall in die sichere Richtung gewertet.

In der Praxis liegen oft keine oder nur widersprüchliche Angaben zur Ausfallartenverteilung von Bauelementen vor. Daher bietet sich der in Abbildung B.3 beschrittene pragmatische Weg an, nur zu prüfen, welcher der drei folgenden Fälle bei einem Bauelement vorliegt:

a) Alle Ausfallarten führen zum Ausfall des Funktionsblocks in dessen sichere Richtung oder haben keine Auswirkung auf sein Verhalten.

b) Es gibt mindestens eine Ausfallart, die den Funktionsblock in dessen sichere Richtung ausfallen lässt, und mindestens eine Ausfallart, die ihn in seine gefährliche Richtung ausfallen lässt.

c) Alle Ausfallarten führen zum Ausfall des Funktionsblocks in dessen gefährliche Richtung.

Im Fall a) wird die komplette Ausfallrate λ der Ausfallrate λ_s in die sichere Richtung zugewiesen (Beispiel: Infrarot-LED P1). Entsprechend wird im Fall c) die gesamte Ausfallrate λ der Ausfallrate λ_d in die gefährliche Richtung zugerechnet (Beispiel: Kondensator C1). Im Fall b) weist man die Gesamtausfallrate λ je zur Hälfte λ_s und λ_d zu (Beispiel: Transistor K2).

Abbildung B.3:

Sinnvolle Ausführungsform einer FMEA-Tabelle für den Funktionsblock „Lichtschranke“ aus Abbildung B.2

Bezeichnung des Funktionsblocks:	Lichtschranke
Gefährliche Ausfallrichtung des Funktionsblocks:	Anliegen einer Ausgangsspannung größer als Null bei Nichtbeleuchtung des Fototransistors K1
Datenquelle für Ausfallraten:	XYZ-Datenbank

Referenz-bezeich-nung	Bauelement-Art	Relev. Bauelem.-Temp. (°C)	Basis-Ausfall-Rate (FIT)	Tempe-ratur-faktor	Ausf.anteil in sichere Richtung	Ausf.anteil in gefährl. Richtung	erk.bar durch Test Nr.	*DC*	λ (FIT)	λ_s (FIT)	λ_d (FIT)	λ_{dd} (FIT)	λ_{du} (FIT)	Anm.
R1	Chip-Widerstand MS	55	0,5	1,20	1	0	–	–	0,60	0,60	0,00	0,00	0,00	
R2	Chip-Widerstand MS	50	0,5	1.15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	[1]
R3	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R4	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R5	Chip-Widerstand MS	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R6	Chip-Widerstand MS	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R7	Chip-Widerstand MS	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R8	Chip-Widerstand MS	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R9	HF-Spule SMD	50	1,8	1,12	1	0	–	–	2,02	2,02	0,00	0,00	0,00	
C1	Chip-Kond. keram.	50	1,1	1,60	0	1	1	0,5	1,76	0,00	1,76	0,88	0,88	[2]
P1	Infrarot-LED	60	2,5	2,24	1	0	–	–	5,60	5,60	0,00	0,00	0,00	
K1	Fototransistor	60	3,4	1,80	0,5	0,5	1	1	6,12	3,06	3,06	3,06	0,00	
K2	Transistor SMD	50	3,2	1,22	0,5	0,5	1	1	3,90	1,95	1,95	1,95	0,00	
K3	Transistor SMD	50	3,2	1,22	0,5	0,5	1	1	3,90	1,95	1,95	1,95	0,00	
X1	Steckverb. 5-polig	50	1,5	1,00	0,5	0,5	1	1	1,50	0,75	0,75	0,75	0,00	[3]
–	Leiterpl. mit 36 Lötst.	50	1,8	1,00	0,5	0,5	1	0,9172	1,80	0,90	0,90	0,83	0,07	[4]
								Summen:	31,23	19,71	11,52	10,57	0,95	

$MTTF_d$ (a): 9 905,9 *DC* (%): 91,72

Anmerkungen:

[1] *Bei Unterbrechung und hoher Umgebungstemperatur fließt durch K1 unter Umständen ein zu hoher Dunkelstrom.*

[2] *Bei Unterbrechung wird die Schaltung gegenüber EM-Störungen empfindlich; Erkennbarkeit nicht gesichert.*

[3] *Kurzschlüsse innerhalb von X1 können einen Ausfall in die gefährliche Richtung verursachen.*

[4] *Aufteilung dd/du wie die durchschnittliche Aufteilung von allen übrigen Elementen.*

Die vereinfachte Vorgehensweise im Fall b) ist normalerweise bei Bauelementen mit einem kleinen Beitrag zur Gesamtausfallrate des Funktionsblocks gerechtfertigt, wenn dieser viele solche Elemente enthält. Einzelne Bauelemente mit einem überdurchschnittlichen Beitrag zur Gesamtausfallrate des Funktionsblocks sind ggf. gesondert zu betrachten. Bei komplexen integrierten Schaltungen wie Prozessoren kann ebenfalls eine 50-zu-50-%-Aufteilung der Ausfallrate auf λ_s und λ_d vorgenommen werden. Dasselbe gilt für Lötstellen/Leiterplatten. Vorsicht ist geboten bei diskreten oder niedrig integrierten Bauelementen mit relativ hoher Ausfallrate. Trägt z.B. ein Schütz oder ein Leistungshalbleiter wesentlich zur Gesamtausfallrate des Funktionsblocks bei, so ist im Zweifelsfall von einem überwiegenden Ausfall in die gefährliche Richtung auszugehen. Dies gilt umso mehr, wenn es sich um die den Ausgangsstrom schaltenden Elemente von Sicherheitsausgängen handelt.

Bei Bauelementen zur Ertüchtigung der Schaltung gegenüber Störeinflüssen (z.B. elektromagnetischen Störungen oder hohe Umgebungstemperatur) ist zur Bewertung des Funktionsblockverhaltens eine Unterscheidung zwischen zwei möglichen Fällen sinnvoll. Ist das Auftreten der Störphänomene lediglich „möglich“ und dient die Schaltungsmaßnahme im Wesentlichen zur Erhöhung der Geräteverfügbarkeit unter (seltenen) ungünstigen Bedingungen, so muss bei der Beurteilung des Funktionsblockverhaltens beim Bauelementeausfall das gleichzeitige Vorliegen des „Störphänomens“ nicht angenommen werden. Sieht jedoch die vorgesehene Betriebsweise des Gerätes die gelegentliche bis ständige Präsenz der Störung vor oder legt die typische Betriebsweise dies nahe (z.B. Einbau in der Reichweite bekannter elektromagnetischer Störquellen oder heißer Einbauort), so muss die Bewertung des Bauelementausfalls die Anwesenheit der Störbeaufschlagung berücksichtigen. Das gilt auch für die Beurteilung der Ausfallerkennbarkeit bei diesen Bauelementen durch Diagnosemaßnahmen.

Der nächste Arbeitsschritt besteht in der Berücksichtigung der Diagnose. Es wird ausschließlich diejenige Diagnose berücksichtigt, die sich auf Ausfälle in die – bezogen auf den Funktionsblock – gefährliche Richtung bezieht. Daher muss nur bei solchen Bauelementen, bei denen es einen Ausfallanteil in diese gefährliche Richtung gibt, geprüft werden, ob ein Test oder ggf. mehrere Tests in der Lage sind, diese Ausfälle ganz oder teilweise zu erkennen. In entsprechenden Spalten werden der jeweils wirksame Test sowie der „bauelementbezogene" Diagnosedeckungsgrad *DC* (Diagnostic Coverage) eingetragen, der den erkennbaren Anteil der Ausfälle in die gefährliche Richtung angibt. Handelt es sich um diskrete Bauelemente wie im Beispiel aus Abbildung B.2, so kann dem gefährlichen Ausfall eines einzelnen Elementes oft einer der DC-Werte „0" für „nicht erkennbar" oder „1" für „erkennbar" zugewiesen werden. Bei komplexen integrierten Bauelementen und bei diskreten Elementen, deren Ausfall ein solches komplexes Bauelement in der Funktion beeinträchtigen kann, muss der bauelementbezogene *DC* unter Berücksichtigung sowohl der gefährlichen Ausfallart als auch des zur Verfügung stehenden Testverfahrens geschätzt werden. Eine Hilfestellung zu dieser Schätzung bietet Tabelle E.2 in der gängigen Testverfahren DC-Werte von 0 % („kein"), 60 % („niedrig"), 90 % („mittel") und 99 % („hoch") zugemessen werden. Bei der Zuweisung eines *DC* zu einem Bauelement muss auch beachtet werden, dass die Bewertung als „erkennbar" nur dann erfolgen darf, wenn das System tatsächlich in der Lage ist, die vorgesehene sicherheitsgerichtete Aktion auszuführen. So ist beispielsweise eine schaltungsinterne Ausfallerkennung nutzlos, wenn sie wegen eines bereits ausgefallenen Abschaltpfades unwirksam ist.

Im vorliegenden Beispiel brauchen die Bauelemente R1, R6 bis R9 und P1 nicht unter dem Diagnoseaspekt betrachtet zu werden, weil sie keine Ausfälle des Funktionsblocks „Lichtschranke" in dessen gefährliche Ausfallrichtung verursachen können. Ihr Ausfallanteil in die gefährliche Richtung ist jeweils 0. Der Ausfall der Elemente R2 bis R5, K1 bis K3 und X1 in die gefährliche Richtung wird von „Test 1" (in diesem Beispiel der einzige Test) vollständig erkannt, d.h., bei zu Testzwecken abgeschalteter LED P1 detektiert der Test eine Ausgangsspannung von > 0. Daher wird diesen Elementen der bauelementbezogene DC-Wert von „1" zuerkannt. Anders beim Kondensator C1, der zur Unterdrückung von regelmäßig, aber nicht ständig vorkommenden elektromagnetischen Störungen dient (Annahme bei diesem Beispiel!). Driftausfälle (begrenzte Kapazitätsänderungen) sind unkritisch, aber ein Kurzschluss führt dazu, dass der Ausgang (Anschluss X1.2) nicht abgeschaltet werden kann (gefährliche Ausfallrichtung des Funktionsblocks). Ein Kurzschluss von C1 wird durch Test 1 erkannt. Bei Unterbrechung von C1 pflanzt sich die elektromagnetische Störung über K2 und K3 bis zum Ausgang des Funktionsblocks fort. Dabei ist unklar, wie die nachfolgende Schaltung dieses hochfrequente Wechselsignal interpretiert und ob das Störphänomen auch während des Tests vorliegt. Ungünstigstenfalls verhindert die nicht unterdrückte Störung, dass das mit Störungen überlagerte Ausgangssignal bei nicht beleuchtetem Fototransistor K1 von der nachfolgenden Schaltung als Anforderung der Sicherheitsfunktion interpretiert wird (= gefährlicher Ausfall des Funktionsblocks „Lichtschranke"). Wenn die Störung zum Testzeitpunkt nicht vorliegt, kann Test 1 die Kondensatorunterbrechung nicht erkennen. Da keine verlässliche Ausfallartenverteilung für den Kondensator bekannt ist, wird (unter Vernachlässigung der unkritischen Driftausfälle) angenommen, dass Kurzschlüsse und Unterbrechungen je 50 % der Ausfälle ausmachen. Beide Ausfallarten führen zum gefährlichen Funktionsblockausfall, sicher erkennbar sind jedoch nur die Kondensatorkurzschlüsse, d.h. die (geschätzte) Hälfte aller gefährlichen Kondensatorausfälle. Somit wird der bauelementbezogene Diagnosedeckungsgrad mit 50 % bzw. 0,5 abgeschätzt. Die Leiterplatte mit den Lötstellen kann Kurzschlüsse und Unterbrechungen an verschiedenen Stellen in die Schaltung einbringen. Der in Abbildung B.3 realisierte pragmatische Ansatz zur Abschätzung des DC-Wertes für Lötstellen und Leiterplatte besteht darin, ihnen jenen mittleren DC-Wert zuzuweisen, der sich für alle übrigen Bauelemente des Funktionsblocks aus der Gleichung $DC = \Sigma \lambda_{dd} / \Sigma \lambda_d$ ergibt. So wirkt sich das Einbeziehen von Leiterplatte und Lötstellen nicht auf den DC-Wert aus, der für den kompletten Funktionsblock berechnet wird.

In jeder Tabellenzeile, d.h. für jedes Bauelement gilt:

λ = Temperaturfaktor · Basisausfallrate
(ggf. mit weiteren Korrekturfaktoren, s.o.)

λ_s = Ausfallanteil in die sichere Richtung · λ

λ_d = Ausfallanteil in die gefährliche Richtung · λ

$\lambda_{dd} = DC \cdot \lambda_d$

$\lambda_{du} = (1 - DC) \cdot \lambda_d$

Für diese λ-Werte werden in der Tabelle Spaltensummen gebildet. Aus dem Summenwert λ_d bzw. aus den Summenwerten λ_d und λ_{dd} ergeben sich die $MTTF_d$, d.h. die mittlere Zeit bis zum gefährlichen Ausfall des Funktionsblocks, sowie der *DC* des Funktionsblocks:

$MTTF_d = 1/\lambda_d$

$DC = \lambda_{dd}/\lambda_d$

Um den PL bei einer der vorgesehenen Architekturen nach Abschnitt 6.2.3 bis 6.2.7 zu bestimmen, werden als Eingangsgrößen nur die Werte von $MTTF_d$ und *DC* benötigt. Im vorliegenden Beispiel ergibt sich ein $MTTF_d$-Wert von 9 905,9 Jahren und ein *DC* von 91,72 %. Wird ein anderes Quantifizierungsverfahren angewendet, können auch Werte wie λ_{dd} bzw. λ_{du} aus der FMEA-Tabelle Verwendung finden.

B3 „Parts Count“-Verfahren

Zur Arbeits- und Zeitersparnis kann anstelle einer FMEA ein einfacheres Verfahren angewandt werden. Verzichtet man auf die detaillierte Analyse des Schaltungsverhaltens bei den verschiedenen Ausfallarten der einzelnen Bauelemente, gelangt man zum sogenannten „Parts Count“-Verfahren (vgl. Anhang D dieses Reports). Es stammt ursprünglich aus dem MIL-Handbook 217F (vgl. [6]) und wird in einer Variante in DIN EN ISO 13849-1, Anhang D.1, beschrieben. Bei gleichzeitiger Annahme verhältnismäßig „konservativer“ (hoher) Ausfallraten kann eine Anpassung der Ausfallraten an die realen Betriebsbedingungen entfallen. Zusätzlich wird häufig bei vielen Elementen von 50 % Ausfallanteil in die – bezogen auf den Funktionsblock – gefährliche Richtung ausgegangen. So entsteht aus der FMEA-Tabelle, wenn man nicht benötigte Spalten für die Gewichtung und Aufspaltung der Ausfallraten weglässt, eine einfachere Tabelle. Verglichen mit FMEA-Ergebnissen liefert das „Parts Count“-Verfahren normalerweise schlechtere (kleinere) $MTTF_d$-Werte, weil tendenzmäßig höhere Ausfallraten einfließen und auch Bauelemente berücksichtigt werden, die ausschließlich Funktionsblockausfälle in die sichere Richtung verursachen können. Wendet man das „Parts Count“-Prinzip auf das oben behandelte Beispiel (Lichtschranke) an und geht man dabei von den temperaturangepassten Ausfallraten aus Abbildung B.3 sowie bei allen Elementen von generell 50 % gefährlichen Ausfällen aus, so erhält man einen $MTTF_d$-Wert von 7 310,8 Jahren. Verglichen mit dem FMEA-Ergebnis ist dieser Wert um ca. 26 % schlechter. Die Verschlechterung ist bei diesem Beispiel allein dem Verzicht auf die Schaltungsanalyse geschuldet. Wird ein DC-Wert für den Funktionsblock benötigt, so muss – wie bei der FMEA – der bauelementbezogene *DC* für jedes Element oder, z.B. in Anlehnung an Anhang E, der *DC* des gesamten Funktionsblocks geschätzt werden.

Grundsätzlich ist die in diesem Anhang des Reports am Beispiel einer elektronischen Schaltung vorgestellte FMEA-Variante für Quantifizierungszwecke als Methode auf andere Technologien übertragbar. Sie kann also in formal gleicher Weise, z.B. für mechanische, hydraulische und pneumatische Systeme, angewendet werden.

Literatur

[1] *Goble, W.M.:* Control systems safety evaluation and reliability. 2nd ed. Hrsg.: Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina 1998

[2] DIN EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (11/2006). Beuth, Berlin 2006; (IEC 60812: 2006) Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

[3] SN 29500: Ausfallraten – Bauelemente – Erwartungswerte. Hrsg.: Siemens AG, Center for Quality Engineering, München 1994-2005

[4] IEC/TR 62380 (ehemals UTE C 80-810): Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment. Hrsg.: International Electrotechnical Commission (IEC), Genf 2004

[5] Telcordia SR-332, Issue 2: Reliability Prediction Procedure for Electronic Equipment. Hrsg.: Telcordia Technologies Inc., Piscataway, New Jersey

[6] 217Plus (Nachfolgeprodukt für das „MIL-Handbook 217F“) Hrsg.: Reliability Information Analysis Center (RIAC), Utica, New York, 2006

[7] DIN EN IEC 61709: Bauelemente der Elektronik, Zuverlässigkeit, Referenzbedingungen für Ausfallraten und Beanspruchungsmodelle zur Umrechnung (1/1999). Beuth, Berlin 1999

[8] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für DIN EN 61508-2 und DIN EN 61508-3; Anhang C. (6/2003). Beuth, Berlin 2003

Anhang C:
Fehlerlisten, Fehlerausschlüsse und Sicherheitsprinzipien

C1 Fehlerlisten

Die bei der Validierung von SRP/CS anzunehmenden Fehler und mögliche Fehlerausschlüsse für mechanische, pneumatische, hydraulische und elektrische Bauteile finden sich in DIN EN ISO 13849-2 [1], Anhang A bis D, in sogenannten Fehlerlisten. In einzelnen Produktnormen, z.B. DIN EN 61496-1 [2], Anhang B, oder DIN EN 60947-5-3 [3], Anhang A, sind ebenfalls Fehlerlisten (hier jeweils für elektrische Bauelemente) mit teilweise geringfügigen Abweichungen zur DIN EN ISO 13849-2 vorhanden.
Der Beitrag 340 220 [4] erläutert Hintergründe und das Zustandekommen der Fehlerlisten (Nachdruck am Ende dieses Anhangs).

C2 Fehlerausschlüsse

Ohne die Annahme von Fehlerausschlüssen sind sichere Steuerungen manchmal nicht mit vertretbarem Aufwand zu realisieren. Gründe für einen Fehlerausschluss können insbesondere die physikalische Unmöglichkeit einer bestimmten Fehlerart oder die technische Unwahrscheinlichkeit des Auftretens eines Fehlers sein sowie allgemein anerkannte technische Erfahrungen (siehe auch Abschnitt 7.3 der DIN EN ISO 13849-1). Fehlerausschlüsse sind auch für neue Komponenten oder Bauelemente grundsätzlich möglich. Jeder Fehlerausschluss muss in der technischen Dokumentation genau begründet werden. DIN EN ISO 13849-2 beschreibt für einzelne Bauelemente mögliche Fehlerausschlüsse, soweit sie als zulässig erachtet werden. Angaben in den folgenden Beispielen sind, wo erforderlich, im Sinne üblicher Praxis aktualisiert. Diese Aspekte werden bei der anstehenden Überarbeitung der Norm als Änderungsvorschläge eingebracht.

C2.1 Beispiele für Fehlerausschlüsse an Bauteilen

C2.1.1 Bauteile der Fluidtechnik

Für pneumatische und hydraulische Bauteile sind häufig vergleichbare Fehlerausschlüsse formuliert. Es sind jedoch auch fluidspezifische Fehlerausschlüsse vorhanden.

Beispiel für gemeinsame Fehlerausschlüsse an fluidischen Bauteilen:

- Wegeventile

  Die Fehlerannahme „Nichtschalten oder nicht vollständiges Schalten“ kann unter folgenden Voraussetzungen ausgeschlossen werden:

  Zwangläufige mechanische Betätigung der bewegten Bauteile, sofern die Betätigungskraft ausreichend groß ist. Bei hydraulischen Wegeventilen kann für ein Patronensitzventil spezieller Bauart (siehe Anmerkungen in DIN EN ISO 13849-2, Tabelle C.3) bezogen auf das Nichtöffnen ein Fehlerausschluss formuliert werden, wenn es mit mindestens einem weiteren Ventil den Hauptvolumenstrom des Druckmediums steuert.

C2.1.2 Elektrische Bauteile

- Optokoppler

  DIN EN ISO 13849-2, Tabelle D.20, gibt an, dass die Fehlerannahme „Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs“ unter folgenden Voraussetzungen ausgeschlossen werden: *„Das verwendete Basismaterial sollte nach IEC 60249 und die Kriech- und Luftstrecken sollten mindestens nach IEC 60664:1992, Verschmutzungsgrad 2/Einsatzklasse III bemessen sein.“*

  Hier handelt es sich offensichtlich um eine fehlerhafte Zuordnung von Anforderungen im Rahmen der Normerstellung. Daher verwendet das BGIA als notifizierte Prüfstelle in der Praxis die beiden folgenden Anforderungen für die Formulierung eines Fehlerausschlusses, die auch in IEC 61800-5-2 [5] übernommen wurden:

  - Der Optokoppler ist aufgebaut in Übereinstimmung mit Überspannungskategorie III gemäß IEC 60664-1:1992, Tabelle 1. Wird eine SELV/PELV-Spannungsversorgung verwendet, genügt Verschmutzungsgrad 2/Überspannungskategorie II.

  - Es müssen Maßnahmen vorhanden sein, die sicherstellen, dass ein interner Ausfall des Optokopplers nicht zu einer erhöhten Temperatur seines Isoliermaterials führen kann.

- Leiterplatte/bestückte Leiterplatte

  Die Fehlerannahme „Kurzschluss zwischen benachbarten Leiterbahnen/Kontaktstellen“ kann nach Norm ausgeschlossen werden, sofern folgende Voraussetzungen zutreffen:

  - Als Leiterplatte wird Basismaterial nach IEC 60249 verwendet.

  - Kriech- und Luftstrecken werden bemessen nach IEC 60664-1:1992 nach Verschmutzungsgrad 2/Überspannungskategorie III.

  - In der Praxis auch akzeptiert: Entspricht die Spannungsversorgung den Anforderungen an SELV/PELV, genügt zur Dimensionierung der Kriech- und Luftstrecken Verschmutzungsgrad 2/Überspannungskategorie II. Ein Minimalabstand von 0,1 mm darf jedoch nicht unterschritten werden.

  - Die bestückte Leiterplatte ist in einem Gehäuse eingebaut, das einen Schutz von mindestens IP54 gibt und die Leiterseite ist mit einer alterungsbeständigen Lack- oder Schutzschicht versehen, die alle Leiterbahnen abdeckt.

- In der Praxis auch akzeptiert: Die alterungsbeständige Lack- oder Schutzschicht kann aus heutiger Sicht z.B. aus einem hochwertigen Lötstopplack bestehen. Eine zusätzliche Beschichtung von Leiterplatten entsprechend IEC 60664-3 kann den zugrunde gelegten Verschmutzungsgrad und damit die erforderlichen Kriech- und Luftstrecken verringern.

- Zu dem Fehlerausschluss „Kurzschluss“ ist aus heutiger Sicht anzumerken, dass beim Einsatz bleifreier Lötprozesse und Bauteile das mögliche Entstehen nadelförmiger Zinn-Whisker berücksichtigt werden muss. Zinn-Whisker sind leitfähig, bis zu mehrere 100 µm lang und können zu einem Kurzschluss zwischen Leiterbahnen bzw. Anschlüssen führen. Daher muss das Risiko des Wachstums solcher Whisker bewertet werden. Bei zu hohem Risiko darf der Fehlerausschluss nicht erfolgen. Die Quellen [6] und [7] können bei der Bewertung hilfreich sein.

- Leitungen/Kabel

  Die Fehlerannahme „Kurzschluss zwischen zwei beliebigen Leitern“ kann unter folgenden Voraussetzungen ausgeschlossen werden: Die Leiter sind

  - dauerhaft (fest) verlegt und gegen äußere Beschädigung geschützt (z.B. durch Kabelkanal, Panzerrohr) oder

  - in unterschiedlichen Mantelleitungen verlegt oder innerhalb eines elektrischen Einbauraumes verlegt unter der Voraussetzung, dass sowohl die Leitungen als auch der Einbauraum den jeweiligen Anforderungen entsprechen, siehe EN 60204-1 oder

  - einzeln durch eine Erdverbindung geschützt.

- Elektromechanische Positionsschalter, Handschalter

  Die Fehlerannahme „Nichtöffnen von Kontakten“ kann unter folgender Voraussetzung ausgeschlossen werden:

  - Kontakte nach EN 60947-5-1: 2004, Anhang K, öffnen sich.

    Es ist anzumerken: Dieser Fehlerausschluss gilt nur für den elektrischen Teil des Schalters (es handelt sich um einen Fehlerausschluss aus der Fehlerliste zur Elektrik). Der mechanische Teil des Schalters – z.B. der an der Schutztür montierte getrennte Betätiger für einen Bauart-2-Schalter, das Anfahrlineal für einen Bauart-1-Schalter oder die Mechanik innerhalb des Schalters – muss zusätzlich betrachtet werden. Daher sind im Teil 1 der DIN EN ISO 13849 in Tabelle C.1 auch trotz dieses „elektrischen“ Fehlerausschlusses B_{10d}-Werte angegeben.

C3 Grundlegende Sicherheitsprinzipien

Grundlegende Sicherheitsprinzipien werden in den Tabellen A.1, B.1, C.1 und D.1 (einschließlich D.2) der informativen Anhänge der DIN EN ISO 13849-2 behandelt.

C3.1 Allgemein für alle Technologien

- Anwendung geeigneter Werkstoffe und Herstellungsverfahren

  Werkstoffe, Herstellungs- und Behandlungsverfahren werden unter Berücksichtigung von Einsatz und Beanspruchungen ausgewählt.

- Richtige Dimensionierung und Formgebung aller Bauteile

  Alle Bauteile werden so ausgewählt, dass sie den erwarteten Betriebsbedingungen genügen. Wichtige Kriterien sind z.B. Schaltvermögen, Schalthäufigkeit, Spannungsfestigkeit, Druckhöhe, dynamisches Druckverhalten, Volumenstrom, Temperatur und Viskosität der Druckflüssigkeit, Art und Zustand der Druckflüssigkeit bzw. der Druckluft.

- Alle Bauteile sind gegen Umgebungsbedingungen und relevante äußere Einflüsse beständig.

  Die SRP/CS sind so ausgelegt, dass sie ihre Funktionen auch unter für die Anwendung üblichen äußeren Einflüssen ausführen können. Wichtige Kriterien sind z.B. mechanische Einflüsse, klimatische Einflüsse, Dichtigkeit des Gehäuses und EMV-Störfestigkeit.

- Prinzip der Energietrennung (Ruhestromprinzip)

  Der sichere Zustand wird durch Wegnahme des Steuersignals (elektrische Spannung, Druck), also durch Energieabschaltung, erreicht. Wichtige Kriterien sind z.B. sicherer Zustand bei Energieunterbrechung oder wirksame Federrückstellung bei Ventilen in der Fluidtechnik.

- Schutz gegen unerwarteten Anlauf

  Der unerwartete Anlauf, z.B. verursacht durch gespeicherte Energie oder nach Wiederherstellung der Energieversorgung, wird vermieden.

C3.2 Beispiele für grundlegende Sicherheitsprinzipien in der Fluidtechnik

- Druckbegrenzung

  Der Anstieg des Drucks in einem System oder in Teilsystemen über ein festgelegtes Niveau hinaus wird in der Regel durch ein oder mehrere Druckbegrenzungsventile verhindert. In der Pneumatik werden dazu vorwiegend Druckregelventile mit Sekundärentlüftung eingesetzt.

- Maßnahmen zur Vermeidung von Verunreinigungen des Druckmediums

  Die für die verwendeten Bauteile erforderliche Reinheitsklasse des Druckmediums wird durch eine geeignete Einrichtung, meist ein Filter, erreicht. In der Pneumatik ist auch eine entsprechende Entwässerung erforderlich.

C3.3 Beispiele für grundlegende Sicherheitsprinzipien in der Elektrik

- Richtige Schutzleiterverbindung

  Eine Seite des Steuerstromkreises, eine Klemme jedes elektromagnetisch betätigten Geräts oder eine Klemme anderer elektrischer Geräte ist mit einem Schutzleiter verbunden. Diese Seite des Geräts wird also nicht benutzt, um z.B. die Abschaltung einer gefahrbringenden Bewegung herbeizuführen. Ein Fehler durch Masseschluss kann daher nicht dazu führen, dass ein Abschaltpfad (unbemerkt) ausfällt.

- Unterdrückung von Spannungsspitzen

  Eine Einrichtung zur Unterdrückung von Spannungsspitzen (RC-Glied, Diode, Varistor) wird parallel zur Last (nicht parallel zu den Kontakten) geschaltet.

C3.4 Beispiele für grundlegende Sicherheitsprinzipien in der Rechnertechnik/Software

DIN EN ISO 13849-2 beschreibt keine grundlegenden Sicherheitsprinzipien für den Einsatz von programmierbaren Systemen bzw. Software. Als solche können jedoch die sogenannten Basismaßnahmen für SRESW und SRASW nach den Abschnitten 4.6.2 und 4.6.3 der Norm verstanden werden (siehe hierzu auch Abschnitt 6.3). Ergänzend wirkt die Überwachung des Programmablaufs, um eine fehlerhafte Reihenfolge von Befehlen bzw. Softwaremodulen zu erkennen, die trotz aller Sorgfalt bei der Verifikation und Validierung auftreten können. Umgesetzt wird diese Maßnahme in der Regel mithilfe eines externen, zyklisch „retriggerten“ Watchdogs, der die SRP/CS bei fehlerhaftem Programmablauf in einen definierten sicheren Zustand bringen können muss.

C4 Bewährte Sicherheitsprinzipien

Die Tabellen A.2, B.2, C.2 und D.3 der informativen Anhänge der DIN EN ISO 13849-2 behandeln bewährte Sicherheitsprinzipien. Ziel der Anwendung bewährter Sicherheitsprinzipien ist es, kritische Fehler oder Ausfälle zu minimieren oder auszuschließen und so die Wahrscheinlichkeit von Fehlern oder Ausfällen, die die Sicherheitsfunktion beeinflussen, zu vermindern.

C4.1 Allgemein für alle Technologien bewährte Sicherheitsprinzipien

- Überdimensionierung/Sicherheitsfaktor

  Alle Betriebsmittel werden unter Nennwert beansprucht. Ziel ist es, die Ausfallwahrscheinlichkeit zu reduzieren.

- Zwangläufige/formschlüssige Betätigung

  Es handelt sich um eine sichere Betätigung durch starre mechanische Teile mit formschlüssigen, steifen und nicht federnden Verbindungen. Ziel ist es, eine sichere Befehlsgabe zu erreichen, z.B. beim Betätigen eines Positionsschalters das zwangläufige Öffnen auch eines verschweißten Kontaktes.

- Begrenzung elektrischer und/oder mechanischer Parameter

  Kraft-, Weg-, Zeit-, Drehzahl- oder Geschwindigkeitsbegrenzungen werden durch elektrische, mechanische oder fluidtechnische Einrichtungen auf zulässige Werte reduziert. Ziel ist die Risikominderung durch verbesserte Gefahrenabwehr.

C4.2 Beispiele für bewährte Sicherheitsprinzipien in der Fluidtechnik

- Gesicherte Position

  Das bewegliche Element eines Bauteils wird mechanisch in einer möglichen Position gehalten (Reibung allein ist nicht ausreichend). Um die Position zu verändern, ist das Aufbringen von Kraft notwendig.

- Anwendung bewährter Federn

  DIN EN ISO 13849-2 führt in Tabelle A.2 detaillierte Anforderungen zu bewährten Federn auf.

C4.3 Beispiele für bewährte Sicherheitsprinzipien in der Elektrik

- Begrenzung elektrischer Parameter

  Begrenzung von Spannung, Strom, Energie oder Frequenz zum Vermeiden eines unsicheren Zustands

- Vermeidung undefinierter Zustände

  Undefinierte Zustände im SRP/CS sind zu vermeiden. Der SRP/CS ist so zu konstruieren, dass sein Zustand während des üblichen Betriebs und unter allen zu erwartenden Betriebsbedingungen vorherbestimmt werden kann, z.B. durch Verwendung von Bauteilen mit definiertem Ansprechverhalten (Schaltschwellen, Hysterese) und mit definierter zeitlicher Abfolge.

- Trennung von Nicht-Sicherheitsfunktionen und Sicherheitsfunktionen

  Um unvorhergesehene Einflüsse auf Sicherheitsfunktionen auszuschließen, werden diese von Nicht-Sicherheitsfunktionen getrennt realisiert.

C4.4 Beispiele für bewährte Sicherheitsprinzipien in der Rechnertechnik/Software

DIN EN ISO 13849-2 beschreibt keine bewährten Sicherheitsprinzipien für den Einsatz von programmierbaren Systemen bzw. Software. Als solche können jedoch die sogenannten zusätzlichen Maßnahmen für SRESW und SRASW nach den Abschnitten 4.6.2 und 4.6.3 der Norm verstanden werden (siehe hierzu auch Abschnitt 6.3). Ein weiteres bewährtes Sicherheitsprinzip ist die Fehleraufdeckung in komplexen Bauelementen wie zum Beispiel Mikrocontrollern durch sogenannte Selbsttests. Tabelle E.1 der Norm zur Abschätzung des Diagnosedeckungsgrades listet solche Selbsttests wie zum Beispiel Speichertests oder CPU-Tests. Informationen zur Realisierung solcher Tests enthält auch ein entsprechender BGIA-Report [8]. Abhängig von der Anwendung können auch „Fehlererkennung durch den Prozess“ und „Fehlererkennung durch Vergleich zwischen Kanälen“ als bewährte Sicherheitsprinzipien gelten.

C5 Bewährte Bauteile

Bewährte Bauteile für Mechanik und Elektrik werden in den Tabellen A.3 und D.4 der informativen Anhänge der DIN EN ISO 13849-2 behandelt. Ziel der Verwendung bewährter Bauteile ist es, kritische Fehler oder Ausfälle zu minimieren oder auszuschließen und so die Wahrscheinlichkeit von Fehlern oder Ausfällen, die die Sicherheitsfunktion beeinflussen, zu vermindern. Als allgemeine Kriterien für ein bewährtes Bauteil gelten gemäß den Ausführungen zur Kategorie 1, dass das Bauteil

a) in der Vergangenheit weit verbreitet mit erfolgreichen Ergebnissen in ähnlichen Anwendungen verwendet wurde, oder

b) unter Anwendung von Prinzipien hergestellt und verifiziert wurde, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen zeigen.

Komplexe elektronische Bauteile (z.B. SPS, Mikroprozessor, ASIC) können im Sinne der Norm nicht als bewährt betrachtet werden. Die Einstufung als bewährtes Bauteil hängt auch von der Anwendung ab: In manchen Anwendungen kann ein Bauteil als bewährt gelten, wohingegen dies in anderen Anwendungen, z.B. aufgrund der Umgebungseinflüsse, ausgeschlossen werden muss.

C5.1 Beispiel für ein bewährtes Bauteil in der Mechanik

- Feder

  Eine Feder gilt als bewährtes Bauteil, wenn die Angaben zu bewährten Sicherheitsprinzipien für die Anwendung bewährter Federn in DIN EN ISO 13849-2, Tabelle A.2, eingehalten und weiterhin die technischen Festlegungen für Federstähle nach ISO 4960 [9] berücksichtigt werden.

C5.2 Beispiele für bewährte Bauteile in der Fluidtechnik

DIN EN ISO 13849-2 benennt für die Fluidtechnik keine bewährten Bauteile. Die Eigenschaft, bewährt zu sein, hängt insbesondere von der speziellen Anwendung sowie von der Einhaltung der Anforderungen zu bewährten Bauteilen der Kategorie 1 und Anforderungen aus den Normen DIN EN 982 [10] und DIN EN 983 [11] ab.

Sicherheitstechnisch bewährte Bauteile können z.B. sein:

- Wegeventile, Sperrventile und Druckventile

C5.3 Beispiele für bewährte Bauteile in der Elektrik

- Sicherung

  Eine Sicherung ist eine Überstromschutzeinrichtung, die einen Stromkreis bei zu hoher Stromstärke, z.B. infolge eines Isolationsfehlers, unterbricht (Prinzip der Energietrennung). Zu unterscheiden sind Schmelzsicherungen sowie ersatzweise Leitungsschutzschalter. Sicherungen haben sich seit Jahrzehnten als Überstromschutzeinrichtungen bewährt. Für Sicherungen existieren umfangreiche Bestimmungen [12; 13]. Versagensfälle von Sicherungen sind bei bestimmungsgemäßem Einsatz und korrekter Dimensionierung praktisch auszuschließen.

- Not-Aus-Gerät/Not-Halt-Gerät

  Zur Einleitung von Handlungen im Notfall dienen Geräte für Not-Aus und Not-Halt nach DIN EN ISO 13850 [14]. Den Geräten gemeinsam ist die Ausrüstung mit zwangsöffnenden Hilfsstromschaltern zur Energieunterbrechung nach Anhang K in DIN EN 60947-5-1 [15]. Zwei Arten von Hilfsstromschaltern mit Zwangsöffnung werden unterschieden:

  - Typ 1: Mit nur einem Schaltglied, das als zwangsöffnender Kontakt ausgeführt ist.

  - Typ 2: Mit einem oder mehreren Öffnern und möglicherweise mit einem oder mehreren Schließern und/oder einem oder mehreren Wechslern. Alle Öffnerkontakte einschließlich der Öffnerteile der Wechsler müssen zwangläufig öffnende Schaltglieder haben.

- Schalter mit zwangläufigem Betätigungsmodus (direkt öffnend)

  Diese besondere Art der Schalter wird als Tastschalter, Positionsschalter und als Wahlschalter mit Nockenbetätigung, z.B. zur Anwahl von Betriebsarten, auf dem Markt angeboten. Die Schalter haben sich seit Jahrzehnten bewährt. Ihnen zugrunde liegt das bewährte Sicherheitsprinzip des zwangläufigen Betätigungsmodus durch zwangsöffnende Kontakte. Als bewährtes Bauteil muss der Schalter den Anforderungen der DIN EN 60947-5-1, Anhang K, [15] entsprechen.

- Weitere nicht komplexe und nicht programmierbare Bauteile, deren Ausfallarten vorhersehbar sind. Beispiele sind passive Bauteile, Widerstände, Dioden, Transistoren, Thyristoren, Operationsverstärker und Spannungsregler.

Literatur

[1] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (12.03). Beuth, Berlin 2003

[2] DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (01.05). Beuth, Berlin 2005

[3] DIN EN 60947-5-3: Niederspannungsschaltgeräte – Teil 5-3: Steuergeräte und Schaltelemente – Anforderungen für Näherungsschalter mit definiertem Verhalten unter Fehlerbedingungen (PDF) (11.05). Beuth, Berlin 2005

[4] *Bömer, T.; Grigulewitsch, W.; Kühlem, W.; Meffert, K.; Reuß, G.:* Fehlerlisten für sicherheitsbezogene Bauelemente – Bei der Prüfung unterstellte Fehlerarten. Kennzahl 340 220. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 48. Lfg. V/06. Hrsg.: Berufsgenossenschaftliches Institut für Arbeitsschutz - BGIA, Sankt Augustin. Erich Schmidt, Berlin 1985 – Losebl.-Ausg. www.bgia-handbuchdigital.de/340220

[5] DIN EN 61800-5-2 (VDE 0160-105-2): Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (04.08). Beuth, Berlin 2008

[6] Test method for measuring whisker growth on tin and tin alloy surface finishes, JESD22A121.01. Hrsg.: JEDEC Solid State Technology Association, Arlington, Virginia, USA 2005 www.jedec.org/download/search/22a121-01.pdf

[7] Environmental acceptance requirements for tin whisker susceptibility of tin and tin alloy surface finishes, JESD201. Hrsg.: JEDEC Solid State Technology Association, Arlington, Virginia, USA 2006 www.jedec.org/download/search/JESD201.pdf

[8] *Mai, M.; Reuß, G.:* Selbsttests für Mikroprozessoren mit Sicherheitsaufgaben oder „Quo vadis Fehler?". BGIA-Report 7/2006. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2006 www.dguv.de/bgia, Webcode d6163

[9] ISO 4960: Kaltband aus unlegierten Stählen mit Kohlenstoffgehalten über 0,25 % (07.99). Beuth, Berlin 1999 (in Überarbeitung)

[10] DIN EN 982: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Hydraulik (09.96). Beuth, Berlin 1996

[11] DIN EN 983: Sicherheit von Maschinen – Sicherheitstechnische Anforderungen an fluidtechnische Anlagen und deren Bauteile – Pneumatik (09.96). Beuth, Berlin 1996

[12] DIN EN 60269-1: Niederspannungssicherungen – Teil 1: Allgemeine Anforderungen (11.05). Beuth, Berlin 2005

[13] DIN EN 60127-1: Geräteschutzsicherungen – Teil 1: Begriffe für Geräteschutzsicherungen und allgemeine Anforderungen an G-Sicherungseinsätze (02.07). Beuth, Berlin 2007

[14] DIN EN ISO 13850: Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze (03.07). Beuth, Berlin 2007

[15] DIN EN 60947-5-1: Niederspannungsschaltgeräte – Teil 5-1: Steuergeräte und Schaltelemente – Elektromechanische Steuergeräte (02.05). Beuth, Berlin 2005

BGIA

Sicherheitstechnisches Informations- und Arbeitsblatt

Fehlerlisten für sicherheitsbezogene Bauelemente – Bei der Prüfung unterstellte Fehlerarten –

1 Einleitung

Für technische Einrichtungen, an denen beim Versagen einer Steuerung oder Schutzeinrichtung Personen zu Schaden kommen können, gelten besondere Sicherheitsanforderungen bezüglich des Verhaltens im Fehlerfall. Beispiele hierfür sind aus technischen Regeln und Normen unterschiedlicher technischer Bereiche bekannt, zum Beispiel aus der Maschinen- und Anlagentechnik, der Verkehrs- und Transporttechnik, der Medizintechnik und der Energietechnik. Auch die Maschinenrichtlinie [1] fordert, dass Steuerungen insbesondere so konzipiert und gebaut sein müssen, dass Fehler in der Logik zu keiner gefährlichen Situation führen.

Welche Auswirkungen Fehler in sicherheitsrelevanten Steuerungen haben können, zeigt das sicherheitstechnische Informations- und Arbeitsblatt 330 250 dieses Handbuches [2].

Die in den technischen Regeln, Unfallverhütungsvorschriften und Normen formulierten Sicherheitsanforderungen hängen sehr stark von der jeweiligen Anwendung ab. Sie reichen im einfachsten Fall von organisatorischen Maßnahmen, wie regelmäßige, willensabhängige Funktionsprüfungen, über automatische Testschaltungen bis hin zu so genannten selbstüberwachten Steuerungen, bei denen sich Fehler selbsttätig bemerkbar machen. Der Begriff Fehlerbetrachtung bezeichnet die Gesamtheit der Überlegungen, die notwendig sind, um das sicherheitstechnische Verhalten einer Einrichtung im Fehlerfall zu beschreiben und auch praktisch zu überprüfen. Eine der wichtigsten Fragen im Rahmen der Fehlerbetrachtung ist, welche Fehler an Bauelementen unterstellt werden müssen. Eine solche Fehlervereinbarung ist notwendig, um dem Entwickler verbindliche Kriterien für den Entwurf seines steuerungstechnischen Sicherheitskonzepts zu liefern. Andererseits soll mit dieser Fehlervereinbarung gewährleistet werden, dass verschiedene Prüfstellen und Prüfer beim gleichen Prüfobjekt nicht zu unterschiedlichen Ergebnissen gelangen.

Welche Fehler sind nun in eine solche Fehlerliste aufzunehmen? Würde man alle theoretisch denkbaren Fehler eines Bauelementes bei der Fehlerbetrachtung unterstellen, so gäbe dies nicht nur einen extrem hohen Prüfaufwand, teilweise wäre die Prüfung überhaupt nicht mehr durchführbar. Hinweise auf unterstellte Fehler und Fehlerausschlüsse hat es in der Vergangenheit in vielen Anwendungsbereichen gegeben, z. B. in der Eisenbahnsignaltechnik. Diese Fehlerlisten waren jedoch nur bedingt auf allgemeine industrielle Anwendungen übertragbar und widersprachen sich sogar teilweise in Detailfestlegungen. In den meisten Normen und Sicherheitsregeln waren jedoch keine Aussagen enthalten, welche Fehler bei der Fehlerbetrachtung konkret zu unterstellen sind.

2 Anforderungen an eine Fehlerliste

Um für steuerungstechnische Sicherheitsprüfungen immer gleiche Voraussetzungen zu schaffen, hat das *Berufsgenossenschaftliche Institut für Arbeitsschutz – BGIA* die bei Prüfungen zugrunde gelegten Fehlerarten elektrischer, hydraulischer und pneumatischer Bauelemente zusammengestellt und in diesem Handbuch in den Jahren 1987 und 1990 veröffentlicht. Diese Zusammenstellungen für den industriellen Maschinen- und Anlagenbau wurden im Laufe der Zeit mehrfach überarbeitet und um Hinweise aus der einschlägigen Literatur und den Technischen Regeln ergänzt. Die Listen – auch schon vor ihrem Erscheinen seit vielen Jahren in der Prüfpraxis erprobt – stellen einen Kompromiss verschiedener, teilweise widersprüchlicher Anforderungen dar, die nachstehend erläutert werden:

Hoher Fehlerabdeckungsgrad

Die bei der Fehlerfallprüfung unterstellten Fehler sollten möglichst viele aller möglichen Fehler abdecken. Je höher der Fehlerabdeckungsgrad, desto geringer ist das Risiko, unter Umständen gefährliche Fehlerarten zu übersehen.

Durchführbarkeit

Je komplexer ein Bauelement, desto größer ist die Vielfalt der möglichen Fehler. So enthielt beispielsweise der Entwurf allgemeiner Richtlinien für signaltechnisch sichere Schaltungen und Einrichtungen der Elektronik allein für einen Transistor bereits 51 Fehlerarten; bei einfachen integrierten Schaltkreisen ergibt sich schon eine astronomisch hohe Zahl unterschiedlicher Fehlermöglichkeiten. Zur Durchführung der Fehlerfallprüfung müssen deshalb die theoretisch möglichen Fehlerarten eingeschränkt werden. Gleichzeitig muss gewährleistet sein, dass trotzdem ein hoher Fehlerabdeckungsgrad hinsichtlich der Fehlerauswirkung erreicht wird. Dies erreicht man zum Beispiel durch die Annahme eines worst-case-Fehlers bei einem Bauteil oder auch bei einer ganzen Baugruppe. Worst-case-Fehler bedeutet, dass an den Ausgängen des Bauelementes oder der Baugruppe der sicherheitstechnisch ungünstigste Fehler unterstellt wird.

Möglichkeit des Fehlereinbaus

Nach Möglichkeit sollten Fehler unterstellt werden, die in die zu prüfende Originalschaltung auch eingebaut werden können. Dies ist nicht immer möglich, denkt man beispielsweise an bestimmte interne Driftvorgänge in Halbleiter-Bauelementen oder an die Miniaturisierung elektronischer Bauelemente. Je nach Schaltungsprinzip bleibt hier unter Umständen nichts anderes übrig, als die Auswirkung solcher Fehler mit Hilfe von Analyse und Simulation zu ermitteln. In der Fluidtechnik lässt sich eine Fehlerursache häufig nicht mit vertretbarem Aufwand realistisch simulieren, z. B. eine Feststoffverschmutzung des Druckmediums. Die Auswirkungen der Fehlerursache, z. B. Hängenbleiben des bewegten Bauteils, können aber in der Regel als Fehler eingebaut werden.

Reproduzierbarkeit

Die eingebauten Fehler sollten, soweit möglich, so ausgewählt sein, dass sich ein reproduzierbares Prüfergebnis ergibt.

Wirtschaftlichkeit

Die unterstellten Fehler sollen einen rationellen Fehlereinbau erlauben. Ein Einbau der Fehler in das betrachtete Bauelement bzw. in die Originalschaltung erfordert aber immer einen deutlich höheren Zeitaufwand als eine theoretische Fehlerbetrachtung. Deshalb sollte man es bei einfach zu übersehenden Bauelementen und Schaltungen bei einer theoretischen Fehlerbetrachtung belassen.

Herstellerunabhängigkeit

Die Art der eingebauten Fehler sollte weitgehend unabhängig vom Hersteller der Bauelemente sein. Fehlerausschlüsse können aber meistens nur konstruktionsspezifisch formuliert werden und sind damit manchmal indirekt herstellerabhängig.

Realistische Fehlerausschlüsse

Ohne die Annahme konkreter Fehlerausschlüsse sind sichere Steuerungen nicht realisierbar. Diese Fehlerausschlüsse sind, abgesehen von wenigen physikalisch begründeten Einzelfällen, jeweils ein Kompromiss zwischen den sicherheitstechnischen Erfordernissen einerseits und den technischen und wirtschaftlichen Möglichkeiten andererseits. Gründe für Fehlerausschlüsse sind insbesondere

- die physikalische Unmöglichkeit einer bestimmten Fehlerart (Beispiel: starke Zunahme der Kondensatorkapazität oder Vergrößerung des Volumenstroms einer Konstantpumpe ohne Änderung der Betriebs- und Antriebsparameter)
- allgemein anerkannte, anwendungsunabhängige technische Regeln oder Erfahrungen (Beispiel: Zwangsführung bei Relais oder plötzlicher Bruch eines Ventil-Schieberkolbens in viele Einzelstücke)
- technische und wirtschaftliche Aspekte, die anwendungsabhängig und damit abhängig vom konkreten Risiko der Anwendung sind (Beispiel: Leitungsschluss bei extern verlegten Kabeln oder selbstständiges Schalten eines Ventils ohne Ansteuerung bei Anwendungen mit relativ geringem Risiko)

Die beiden erstgenannten Gründe für einen Fehlerausschluss stellen den Regelfall dar. Dennoch sind in bestimmten Anwendungen weitergehende Fehlerausschlüsse möglich. Diese zusätzlichen Fehlerausschlüsse richten sich insbesondere nach der Auftrittswahrscheinlichkeit dieser Fehler. Sie lässt sich durch konkrete Ausfallraten belegen oder von entsprechenden betrieblichen Erfahrungen ableiten.

3 Normung von Fehlerlisten

Die vormals in den sicherheitstechnischen Informations- und Arbeitsblättern 340 220 und 340 225 aufgeführten Fehlerlisten für elektri-

sche, hydraulische und pneumatische Bauelemente hat die europäische Normung mit geringen Anpassungen in die europäische/internationale Norm EN ISO 13849-2 [3] übernommen. In den Anhängen A bis D finden sich im Hinblick auf die Validierung von sicherheitsbezogenen Steuerungsteilen allgemeine Fehlerlisten zu mechanischen, pneumatischen, hydraulischen und elektrischen Bauteilen. Diese bilden heute die Grundlage für Prüfungen nach DIN EN 954-1 [4].

Auch in Produktnormen des Maschinenbereiches finden sich vereinzelt Fehlerlisten, z. B. im Anhang B der DIN EN 61496-1 [5] und in der DIN EN 60947-5-3 [6] (hier jeweils für elektrische Bauelemente); diese Listen weichen kaum von der Fehlerliste für elektrische Bauelemente in [3] ab. Teil 2 der DIN EN 61508 [7] enthält in Tabelle A.1 eine sehr knappe und allgemein gehaltene Liste von Fehlern oder Ausfällen, die während des Betriebs erkannt werden müssen oder zur Bestimmung des Anteils ungefährlicher Ausfälle zu analysieren sind. Interessant ist diese Liste in Bezug auf die einzelnen Elemente eines Rechnersystems, z. B. Hauptprozessor (CPU), Takt und Speicher.

Literatur

[1] Richtlinie 98/37/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen. ABl. EG Nr. L 207 (1998)

[2] *Börner, F.; Kreutzkampf, F.*: Unfälle und Störfälle, verursacht durch das Versagen von Steuerungen. Sicherheitstechnisches Informations- und Arbeitsblatt 330 250. In: BGIA-Handbuch 22. Lfg. VI/94. Hrsg.: Berufsgenossenschaftliches Institut für Arbeitsschutz – BGIA. Erich Schmidt, Berlin 1985 – Losebl.-Ausg.

[3] DIN EN ISO 13849-2: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung. Beuth, Berlin (Dezember 2003)

[4] DIN EN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze. Beuth, Berlin (März 1997)

[5] DIN EN 61496-1: Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen. Beuth, Berlin (Januar 2005)

[6] DIN EN 60947-5-3: Niederspannungsschaltgeräte; Teil 5-3: Steuergeräte und Schaltelemente; Anforderungen für Näherungsschalter mit definiertem Verhalten und Fehlerbedingungen (PDF). Beuth, Berlin (Februar 2000)

[7] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme. Beuth, Berlin (Dezember 2002)

Bearbeiter:

Dipl.-Ing. T. Bömer, Dipl.-Ing. W. Grigulewitsch,
Dipl.-Ing. W. Kühlem, Dr.-Ing. K. Meffert,
Dipl.-Ing. G. Reuß
Fachbereich Unfallverhütung – Produktsicherheit

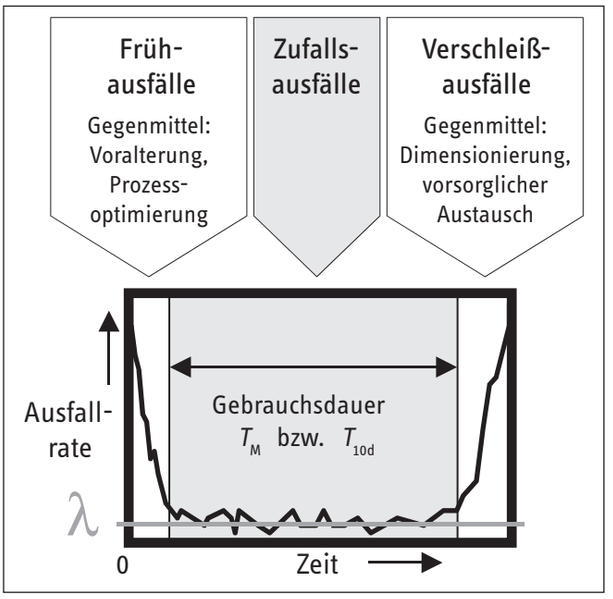
Anhang D:
Mean Time to Dangerous Failure ($MTTF_d$)

D1 Was bedeutet „$MTTF_d$“?

Die mittlere Zeit bis zum gefahrbringenden Ausfall $MTTF_d$ (Mean Time to Dangerous Failure) beschreibt die Zuverlässigkeit der in einer Steuerung verwendeten Bauteile und fließt als einer von mehreren Parametern in die Bestimmung des Performance Levels ein. In DIN EN ISO 13849-1 wird die $MTTF_d$ als „Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall“ definiert, was mehrere Aspekte betont:

- $MTTF_d$ ist eine statistische Größe, d.h. ein empirisch entstandener Wert bzw. eine Kennzahl, die nichts mit einer „garantierten Lebensdauer“, „ausfallfreien Zeit“ oder Ähnlichem zu tun hat.
- $MTTF_d$ hat die physikalische Dimension einer Zeit und wird meist in Jahren angegeben.
- Es geht nur um Ausfälle in die gefahrbringende Richtung, d.h. solche, die die Ausführung der Sicherheitsfunktion beeinträchtigen. Führen mehrere Kanäle die Sicherheitsfunktion aus (Redundanz), so spricht man auch von einem „gefahrbringenden Ausfall“, wenn nur ein einzelner Kanal betroffen ist.

Abbildung D.1:
„Badewannenkurve“ der Ausfallrate



D1.1 Badewannenkurve und konstante Ausfallrate

Eine übliche Form der Beschreibung von Bauteilzuverlässigkeiten ist die Angabe von Ausfallraten, abgekürzt λ (nur auf gefahrbringende Ausfälle bezogen entsprechend λ_d), mit der gebräuchlichen Einheit FIT (Failures In Time, d.h. Anzahl der Ausfälle in 10^9 Bauteilstunden, 1 FIT = 10^{-9}/h). Diese Ausfallrate beschreibt zu einem bestimmten Zeitpunkt die Rate, mit der funktionsfähige Bauteile gerade ausfallen. Das heißt, die Zahl der Ausfälle pro Zeit wird durch die Anzahl der zum jeweiligen Zeitpunkt noch ausfallfreien Bauteile geteilt. Das Ausfallverhalten vieler Arten von Bauteilen (speziell elektronischer Bauteile) stellt sich in Abhängigkeit von der Zeit als mehr oder weniger ausgeprägte „Badewannenkurve“ dar [1], siehe Abbildung D.1.

Am Anfang der Gebrauchsdauer fallen in der Regel verstärkt Bauteile aus. Dies sind Frühausfälle, die aber nur für kurze Zeit dominieren. Nach Überschreiten der empfehlenswerten Gebrauchsdauer steigen die Ausfälle wieder an. Im mittleren Bereich der üblichen Gebrauchsdauer ist insbesondere bei elektronischen Bauelementen oft ein plateauähnlicher Bereich konstanter Ausfallrate zu beobachten. Dieser wird durch die sogenannten Zufallsausfälle geprägt. Selbst stärker von Verschleiß als von Zufallsausfällen dominierte Bauteile, z.B. elektromechanische oder pneumatische, lassen sich oft im Rahmen ihrer Gebrauchsdauer durch die Annahme einer zur sicheren Seite hin abgeschätzten konstanten Ausfallrate beschreiben. Üblicherweise werden Frühausfälle vernachlässigt, da Komponenten mit ausgeprägten Frühausfällen den Verfügbarkeitsanforderungen an eine Maschinensteuerung nicht gerecht werden und daher im Markt nur eine geringe Rolle spielen. Geeignete Maßnahmen zur Reduktion von Frühausfällen sind Voralterung (Burn-In), Selektion und Optimierung der Herstellungsprozesse. Im Sinne der Einfachheit wird daher in DIN EN ISO 13849-1 grundsätzlich innerhalb der Gebrauchsdauer von konstanten Ausfallraten ausgegangen. Diese Annahme hat den Vorteil, dass sich damit die weitere mathematische Betrachtung stark vereinfacht und sie ist Grundlage für die hinter dem Säulendiagramm bzw. dem vereinfachten Verfahren der DIN EN ISO 13849-1 stehende Markov-Modellierung der vorgesehenen Architekturen. Aus einer konstanten Ausfallrate folgen mathematisch eine mit der Einsatzzeit exponentiell abfallende Kurve der Zuverlässigkeit und ein Erwartungswert der Zeit bis zum Ausfall ($MTTF_d$), der dem Kehrwert der Ausfallrate entspricht, d.h.

$$MTTF_d = \frac{1}{\lambda_d} \qquad (1)$$

Bei konstanter Ausfallrate ist also die Angabe der $MTTF_d$ der Angabe einer Ausfallrate gleichwertig, ist aber viel illustrativer. Während die praktische Bedeutung eines FIT-Wertes wenig anschaulich ist, vermittelt die Angabe eines zeitlichen Erwartungswertes in Jahren eher eine Vorstellung von der Bauelementgüte. Abbildung D.2 (siehe Seite 222) zeigt die statistisch zu erwartende Entwicklung des Anteils gefahrbringender Ausfälle über der Einsatzzeit für vier verschiedene $MTTF_d$-Werte. Hier lässt sich ein weiterer mathematischer Zusammenhang ablesen, nämlich dass bei Erreichen der $MTTF_d$-Marke auf der Zeitachse

im statistischen Mittel ca. 63 % aller anfänglich intakten Bauteile gefahrbringend ausgefallen sind (nicht 50 %, da zwar mehr Bauteile vor Erreichen der $MTTF_d$ ausfallen, dafür aber die dann noch intakten Bauteile mit Restlaufzeiten von teilweise dem Mehrfachen der $MTTF_d$ schwerer wiegen).

Das vereinfachte Quantifizierungsverfahren nach DIN EN ISO 13849-1 unterstellt eine übliche Gebrauchsdauer von maximal 20 Jahren für Bauteile in Sicherheitssteuerungen im Maschinenbau. Vor diesem Hintergrund und bei Kenntnis des zeitlichen Verlaufs der Ausfallrate (Abbildung D.1) wird verständlich, dass die Angabe eines $MTTF_d$-Wertes nur als illustrative Kennzeichnung für das Zuverlässigkeitsniveau innerhalb der Gebrauchsdauer verstanden werden sollte und weder eine Garantie für eine ausfallfreie Zeit vor Erreichen der $MTTF_d$ noch eine exakte Vorhersage für den Ausfallzeitpunkt eines Einzelbauteils bietet. Ist der Verschleißbereich erreicht, ändert sich das Ausfallverhalten grundlegend und kann nicht mehr sinnvoll durch eine konstante Ausfallrate beschrieben werden.

D1.2 Klasseneinteilung und Begrenzung

Die Annahme einer $MTTF_d$ für jedes sicherheitsrelevante Bauteil (wenn kein Fehlerausschluss begründet werden kann) ist Voraussetzung für die nachfolgenden Schritte, die zunächst auf Block- und dann auf Kanalebene zur sogenannten $MTTF_d$ jedes Kanals führen. Auf Kanalebene schlägt DIN EN ISO 13849-1 die Einteilung in drei typische $MTTF_d$-Klassen vor (Tabelle D.1). Diese Klassen sollen kleine Unterschiede in den errechneten $MTTF_d$-Werten nivellieren, die ohnehin innerhalb der statistischen Unsicherheit untergehen. Auch soll damit die Gleichwertigkeit mit den anderen Parametern (fünf Kategorien, vier DC-Stufen) gewahrt bleiben und die notwendige Vereinfachung für die Darstellung im Säulendiagramm erreicht werden.

Tabelle D.1:
Klasseneinteilung der $MTTF_d$ für Kanäle, die die Sicherheitsfunktion

Bezeichnung der $MTTF_d$ für jeden Kanal	Bereich der $MTTF_d$ für jeden Kanal
niedrig	3 Jahre ≤ $MTTF_d$ < 10 Jahre
mittel	10 Jahre ≤ $MTTF_d$ < 30 Jahre
hoch	30 Jahre ≤ $MTTF_d$ ≤ 100 Jahre

Gewünschte Nebeneffekte dieser Klassenbildung sind die Zurückweisung von $MTTF_d$-Werten jedes Kanals < 3 Jahre und die Beschränkung höherer $MTTF_d$-Werte jedes Kanals auf maximal 100 Jahre. Abbildung D.2 macht deutlich, dass bei einer $MTTF_d$ von drei Jahren schon nach einem Jahr fast 30 % gefahrbringende Ausfälle zu erwarten sind, was für eine Sicherheitssteuerung unakzeptabel erscheint. Am anderen Ende des Spektrums erscheint ein statistisch abgesicherter Nachweis von Zuverlässigkeiten > 100 Jahre $MTTF_d$ sehr fragwürdig. Außerdem bleibt selbst bei beliebig hohen $MTTF_d$-Zahlen eine Restwahrscheinlichkeit für einen gefahrbringenden Ausfall innerhalb der Gebrauchsdauer, der darüber hinaus auch aus anderen Gründen auftreten kann (z.B. Fehlanwendung). Daher erscheint die Absicherung hoher Performance Level alleine durch Verwendung hoch zuverlässiger Bauteile nicht angemessen. Im Säulendiagramm nach DIN EN ISO 13849-1 wird dies dadurch ausgedrückt, dass kein $MTTF_d$-Bereich über der hohen $MTTF_d$-Klasse dargestellt wird, auch wenn dies aufgrund der Wahrscheinlichkeitsrechnung möglich wäre. Die Rückstufung höherer $MTTF_d$-Werte auf den Maximalwert von 100 Jahren findet erst auf Kanalebene statt, d.h. für einzelne Bauteile können deutlich höhere $MTTF_d$-Werte in die Berechnung einfließen.

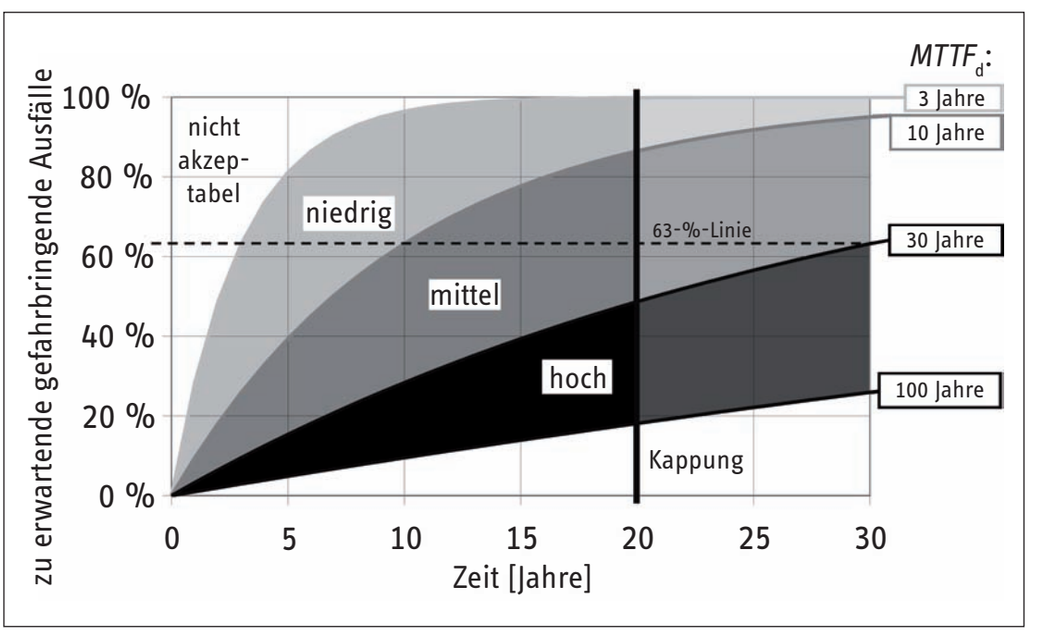


Abbildung D.2:
Illustration der $MTTF_d$

D1.3 Woher kommen die Daten?

Ein mögliches Problem für den Normanwender, besonders zum Zeitpunkt der ersten Veröffentlichung der revidierten DIN EN ISO 13849-1, sind fehlende $MTTF_d$-Angaben für Sicherheitsbauteile [2]. Grundsätzlich schlägt die Norm eine Hierarchie von Datenquellen vor, die an erster Stelle Herstellerangaben nennt, dann typische Zahlenwerte, die in der Norm selbst gelistet sind, und schließlich einen sehr konservativ abgeschätzten Ersatzwert von zehn Jahren. Da dieser Ersatzwert auf ein Bauteil bezogen ist und bei mehreren Bauteilen in einem Kanal schnell die $MTTF_d$-Untergrenze von drei Jahren erreicht wird, sind die in der Norm selbst gelisteten $MTTF_d$-Werte von besonderer Bedeutung – zumindest so lange, bis die Angabe von $MTTF_d$-Werten vonseiten der Hersteller zur Selbstverständlichkeit wird.

D2 Unterschiede der Technologien

Das Ausfallverhalten von Bauteilen hängt naturgemäß sehr stark von der eingesetzten Technologie ab, da die „Badewannencharakteristik“ und die Bedeutung von Verschleißeffekten unterschiedlich stark ausgeprägt sein können. Bei mechanischen und hydraulischen Komponenten, die von der Konstruktion und der Anwendung auf hohe Zuverlässigkeit und geringen Verschleiß optimiert werden, kann von einer sehr hohen $MTTF_d$ ausgegangen werden. Hier spielen Zufallsausfälle (der Bereich konstanter Ausfallrate) und Verschleißausfälle kaum eine Rolle. Bei den meisten elektronischen Komponenten hingegen ist das Ausfallverhalten, innerhalb der typischen Einsatzdauer vergleichsweise „billiger“ Einwegkomponenten, üblicherweise sehr gut durch eine konstante Ausfallrate beschrieben, da der Verschleißbereich nur bei verschärften Einsatzbedingungen erreicht wird. Ganz anders geartet wiederum ist das Ausfallverhalten von elektromechanischen oder pneumatischen Bauelementen: Hier kann der Verschleißbereich durchaus in der üblichen Einsatzdauer erreicht werden. Daher wird als Kenngröße üblicherweise auch die erreichbare Anzahl erfolgreicher Schaltzyklen bzw. Schaltspiele angegeben und nicht eine Lebensdauer als Zeit oder eine zeitbezogene Ausfallrate. Allen diesen technologieabhängigen Besonderheiten muss bei der Bestimmung des $MTTF_d$-Wertes Rechnung getragen werden, weshalb DIN EN ISO 13849-1 hier unterschiedliche Herangehensweisen vorschlägt.

D2.1 $MTTF_d$ mechanischer Steuerungskomponenten

Der Ansatz konstanter Ausfallrate ist für mechanische Steuerungskomponenten leider nicht sehr angemessen. Andererseits enthält fast jede Sicherheitsfunktion zumindest im Bereich der Sensoren oder Aktoren mechanische Steuerungselemente, die z.B. Bewegungen erkennen oder gefahrbringende Bewegungen stillsetzen müssen. Obwohl die Angabe einer zur sicheren Seite hin abgeschätzten $MTTF_d$ vielfach auch für diese Komponenten möglich wäre, wird hier in der Regel ein Fehlerausschluss herangezogen. Solange die Voraussetzungen für den Fehlerausschluss eingehalten und dokumentiert werden, ist dies meistens die eleganteste Methode, um die Zuverlässigkeit der mechanischen Komponenten zu berücksichtigen. Zu diesen Voraussetzungen gehört u.a. die ausreichende Widerstandsfähigkeit gegenüber den zu erwartenden Umwelteinflüssen, d.h., die Gültigkeit eines Fehlerausschlusses kann von der gewählten Applikation abhängen. Eine andere Voraussetzung ist z.B. ausreichende Überdimensionierung, die sicherstellt, dass die mechanischen Komponenten z.B. im Bereich der Dauerfestigkeit belastet werden. Falls ein Fehlerausschluss nicht möglich ist, bietet eventuell die Anwendung des weiter unten genannten Verfahrens guter ingenieurmäßiger Praxis die Möglichkeit, einen $MTTF_d$-Wert abzuschätzen.

D2.2 BGIA-Report 6/2004 „Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen“

Bei hydraulischen Anlagen ist als „sicherheitsbezogener Teil der Steuerung“ insbesondere der Ventilbereich zu betrachten. Dabei sind vor allem Ventile, die gefahrbringende Bewegungen oder Zustände steuern, für die Berechnung des Performance Levels von äußerster Wichtigkeit. Das Ausfallverhalten hydraulischer Ventile wird erfahrungsgemäß wenig von Zufallsausfällen und eher von Verschleißausfällen geprägt. Dabei handelt es sich in erster Linie um systematische Ursachen wie z.B. Überbeanspruchung, ungünstige Einsatzbedingungen oder fehlende Wartung. Um die Lebensdauer hydraulischer Ventile besser abschätzen zu können, wurde im BGIA eine Diplomarbeit zu diesem Thema initiiert, deren Ergebnisse als BGIA-Report 6/2004 „Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen“ [3] veröffentlicht wurden. Da es sich in der Regel bei Ventilen, die Steuerungsaufgaben übernehmen, um Wegeventile in Schieberbauweise handelt, wurden die $MTTF_d$-Wert für „hydraulische Bauteile“ ersatzweise an Wegeventilen in Schieberbauweise ermittelt. Die wichtigsten Ergebnisse dieser Untersuchung werden im Folgenden kurz vorgestellt.

Die Grundlage für die Abschätzung eines $MTTF_d$-Wertes bilden in erster Linie die Ausfallraten von hydraulischen Wege-Schieberventilen, die im Rahmen einer Untersuchung in den Instandhaltungsabteilungen zweier großer Hydraulikanwender ermittelt wurden (im Folgenden Anwender A bzw. B genannt). Dies erfolgte durch Auswertung von EDV-Daten (Neubeschaffungsmengen von hydraulischen Wegeventilen in Schieberbauweise und Reparaturberichten) und Mitwirkung bei Instandhaltungsarbeiten. Zusätzlich zu den Ausfalldaten der Ventile wurden die Einsatzbedingungen berücksichtigt. Somit ist die Vergleichbarkeit der bei den jeweiligen Hydraulikanwendern ermittelten $MTTF_d$-Werte gegeben. Zur Absicherung und Bestätigung dieser Daten wurden darüber hinaus durch eine Umfrage unter Ventilherstellern zusätzliche Ausfalldaten gesammelt.
Bei Anwender A wurden die Ausfallraten der Wegeventile in der Instandhaltungsabteilung der Getriebefertigung erfasst. Verfügbar waren die Daten aller ausgefallenen Wegeventile über einen Zeitraum von 38 Monaten, in dem es 143 Ausfälle von Wegeventilen gab. In den Maschinen der Getriebefertigung, größtenteils Werkzeugmaschinen, waren ungefähr 8 050 Wegeventile unterschiedlichen Alters im Einsatz. Wenn in dieser Zeitspanne eine konstante Ausfallrate unterstellt wird, lässt sich aus den Daten für Anwender A eine $MTTF_d$ von 178 Jahren als Kehrwert der Ausfallrate errechnen. Bei diesem Anwender wurden die Einsatzbedingungen an den Hydraulikanlagen weitgehend nach den Vorgaben der Hersteller eingehalten. Da es sich vorwiegend um neue Fertigungsstraßen handelte, wurde eine zustandsorientierte Instandhaltung durchgeführt.

Bei Anwender B wurden die Ausfalldaten für die Wegeventile ebenfalls in der Instandhaltungsabteilung der Getriebefertigung aufgenommen. Hier waren ungefähr 25 000 Wegeventile unterschiedlichen Alters im Einsatz. Verfügbar waren die Daten aller ausgefallenen Wegeventile in einem Zeitraum von vier Jahren (2000 bis 2003). Im Gegensatz zum Anwender A waren die Ausfalldaten für jedes Jahr einzeln abrufbar; somit war es möglich, eine $MTTF_d$ für jedes einzelne Jahr zu bestimmen. Dabei stieg die $MTTF_d$ von 195 Jahren im Jahre 2000 auf 300 im Jahre 2003. Es zeigte sich ein signifikanter Zusammenhang zwischen Ventilausfällen und Einsatz- bzw. Umgebungsbedingungen, denn Anwender B hat seine Instandhaltungsmaßnahmen und Einsatzbedingungen im Laufe der Jahre kontinuierlich verbessert. Des Weiteren wurden gegenüber Anwender A die Einsatzbedingungen durch zusätzliche Maßnahmen verbessert, z.B. Über-

wachung der Öltemperatur, größere Öltanks, meist außerhalb der Maschine untergebracht, feinere Rücklauffilter, Abzugsanlagen zur Minderung der Verunreinigungen in der Umgebungsluft. Die Untersuchung zeigte, dass die zylindrischen Führungen der Bauteile in Ventilen, z.B. Steuerschieber, in Verbindung mit Art, Qualität und Verschmutzungsgrad der eingesetzten Druckflüssigkeit sowie Auslegung, Material und Ausführung der Zentrier-/Rückstellfeder einen wesentlichen Einfluss auf die zu erwartende Lebensdauer hydraulischer Wege-Schieberventile haben. Dabei wurde ein deutlicher Zusammenhang zwischen Qualität der Einsatzbedingungen und der erreichten Lebensdauer bis zum Ausfall über einen definierten Betrachtungszeitraum festgestellt.

D2.3 $MTTF_d$ hydraulischer Steuerungskomponenten

Aufgrund der Ergebnisse der oben genannten Untersuchung wird in DIN EN ISO 13849-1 für hydraulische Bauteile unter bestimmten Voraussetzungen eine $MTTF_d$ von 150 Jahren vorgeschlagen. Zwar wurden schwerpunktmäßig Ventile in Schieberbauweise untersucht, aufgrund des ähnlichen Ausfallverhaltens lässt sich die ermittelte Lebensdauer $MTTF_d$ aber als gute Abschätzung für alle sicherheitsrelevanten hydraulischen Ventile verwenden. Voraussetzung hierfür ist allerdings die Einhaltung der in DIN EN ISO 13849-2 aufgeführten, auf hydraulische Ventile bezogenen grundlegenden und bewährten Sicherheitsprinzipien bei Konstruktion und Herstellung. Weiterhin müssen die ebenfalls in DIN EN ISO 13849-2 aufgeführten anwendungsbezogenen grundlegenden und bewährten Sicherheitsprinzipien vom Ventilhersteller genannt (Herstellervorgaben, Einsatzbedingungen) und vom Anwender eingehalten werden.

Anhang C.2, Tabelle C.1, der DIN EN ISO 13849-2 nennt die grundlegenden Sicherheitsprinzipien für hydraulische Systeme. Zu den wichtigsten Prinzipien gehört die Anwendung geeigneter Werkstoffe und Herstellungsverfahren sowie des Prinzips der Energietrennung, Druckbegrenzung, Schutz gegen unerwarteten Anlauf und ein geeigneter Temperaturbereich (weitere Erläuterungen siehe Anhang C).

Anhang C.3, Tabelle C.2, der DIN EN ISO 13849-2 listet bewährte Sicherheitsprinzipien für hydraulische Systeme auf. Die wichtigsten Prinzipien umfassen Überdimensionierung/Sicherheitsfaktoren, Begrenzung/Verringerung der Geschwindigkeit durch einen Widerstand zum Erreichen eines definierten Volumenstroms, Begrenzung/Verringerung der Kraft, einen geeigneten Bereich für die Betriebsbedingungen, Überwachung des Zustands des Druckmediums, Verwendung bewährter Federn und eine ausreichend große positive Überdeckung in Schieberventilen (weitere Erläuterungen siehe ebenfalls Anhang C).

Auch wenn DIN EN ISO 13849-1 unter diesen Voraussetzungen einen $MTTF_d$-Wert für hydraulische Ventile angibt, sollte dennoch jeder Hersteller von Ventilen für seine Bauteile möglichst eigene Ausfallzahlen ermitteln und eine eigene $MTTF_d$ angeben.

D2.4 $MTTF_d$ pneumatischer und elektromechanischer Steuerungskomponenten

In der Fluidtechnik sowie in der Mechanik und Elektromechanik wird die Lebensdauer bzw. die Zuverlässigkeit der Komponenten in der Regel vom Verschleißverhalten der bewegten Elemente bestimmt. Bei fluidtechnischen Komponenten wie z.B. Ventilen, die meistens komplexe Einheiten mit vielen beweglichen Elementen (z.B. Schieber, Stößel, Federn in Vorsteuerstufe und Hauptstufe) darstellen, kann die Lebensdauer auch von den betrieblichen Umgebungsbedingungen stark beeinflusst werden. Hierbei sind insbesondere zu nennen:

- Qualität und Zustand des Druckmediums (Druckluft)
- Verträglichkeit von Dichtungen mit den Schmierstoffen
- Temperatureinflüsse
- Umgebungseinflüsse wie z.B. Stäube, Gase, Flüssigkeiten

Auf eine Einhaltung der vom Hersteller der Komponenten spezifizierten Anforderungen ist unbedingt zu achten, damit die bei der Ermittlung der Steuerungskategorie zugrunde gelegten Parameter bezüglich des Ausfallverhaltens der Komponente zutreffend sind.

Sind die folgenden Merkmale erfüllt, kann der $MTTF_d$-Wert für ein einzelnes pneumatisches, elektromechanisches oder mechanisches Bauteil nach den weiter unten aufgeführten Formeln abgeschätzt werden:

- Der Hersteller des Bauteils bestätigt die Verwendung von grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003, Tabelle B.1 oder Tabelle D.1, für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).
- Der Hersteller eines Bauteils, das in einer Steuerung der Kategorie 1, 2, 3 oder 4 verwendet werden soll, bestätigt die Verwendung bewährter Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003, Tabellen B.2 oder D.2, für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).
- Der Hersteller des Bauteils legt die geeignete Anwendung und Betriebsbedingungen für den Anwender fest. Der Anwender ist über seine Verantwortung zu informieren, die grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003, Tabellen B.1 oder D.1, für die Implementierung und den Betrieb des Bauteils zu erfüllen. Für Kategorie 1, 2, 3 oder 4 ist der Anwender über seine Verantwortung zu informieren, die bewährten Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003, Tabellen B.2 oder D.2, für die Implementierung und den Betrieb des Bauteils zu erfüllen.

Die hinter den grundlegenden und bewährten Sicherheitsprinzipien stehenden konkreten Maßnahmen ähneln denjenigen, die oben für hydraulische Bauelemente ausführlicher beschrieben sind.

Der $MTTF_d$-Wert ist definiert als die mittlere Zeit bis zum gefahrbringenden Ausfall. Um diese Zeit für ein Bauteil bestimmen zu können, müssen entsprechende Lebensdauermerkmale festgelegt werden. Dies können zurückgelegte Strecken für Pneumatikzylinder, Betätigungshäufigkeiten für Ventile oder elektromechanische Bauteile sowie Lastwechsel bei mechanischen Komponenten sein. In der Regel wird die Zuverlässigkeit für pneumatische oder elektromechanische Bauteile im Labor bestimmt.

D2.4.1 Bestimmung des Lebensdauerkennwertes B_{10d}

Mit im Labor oder eventuell auch bei Felduntersuchungen ermittelten Werten kann die Ausfallhäufigkeit z.B. mithilfe der Weibull-Statistik bestimmt werden [4]. Die zweiparametrige Weibull-Verteilungsfunktion in Abbildung D.3 ist flexibler als die Exponentialverteilung, die sie als Spezialfall (b = 1) enthält. Ein Ansteigen der Ausfallrate bei Erreichen der Verschleißphase lässt sich durch b-Parameter > 1 gut beschreiben. Der T-Parameter beschreibt die charakteristische Lebensdauer, bei der 63,2 % der betrachteten Bauteile ausgefallen sind. Als Methode zur Bestimmung der Weibull-Parameter kann die „Lineare Regression XY" angewendet werden. Bei unvollständigen Daten, d.h., wenn z.B. nicht schadhafte Teile berücksichtigt werden sollen, sind auch andere Methoden anwendbar. Als Ergebnis können aus den Diagrammen die Kennwerte für die Parameter b und T abgelesen werden. Daraus lässt sich dann die nominale Lebensdauer B_{10} bestimmen, bei der 10 % der betrachteten Bauteile ausgefallen sind. Der $MTTF_d$-Wert wird mit der nominalen Lebensdauer B_{10} ermittelt. Für eine Zuverlässigkeitsanalyse mithilfe der Weibull-Statistik ist entsprechende Software auf dem Markt erhältlich. Die sicherheitstechnischen Zuverlässigkeitskennwerte für fluidtechnische und elektromechanische Komponenten sind vom Hersteller dieser Bauteile anzugeben. Für die Ermittlung der Zuverlässigkeit von pneumatischen Komponenten kann die Norm ISO 19973 „Pneumatik – Bewertung der Zuverlässigkeit von Bauteilen durch Prüfung" zugrunde gelegt werden. Diese Norm besteht zurzeit aus vier Teilen:

- Teil 1: Allgemeine Verfahren
- Teil 2: Ventile
- Teil 3: Zylinder mit Kolbenstange
- Teil 4: Druckregler

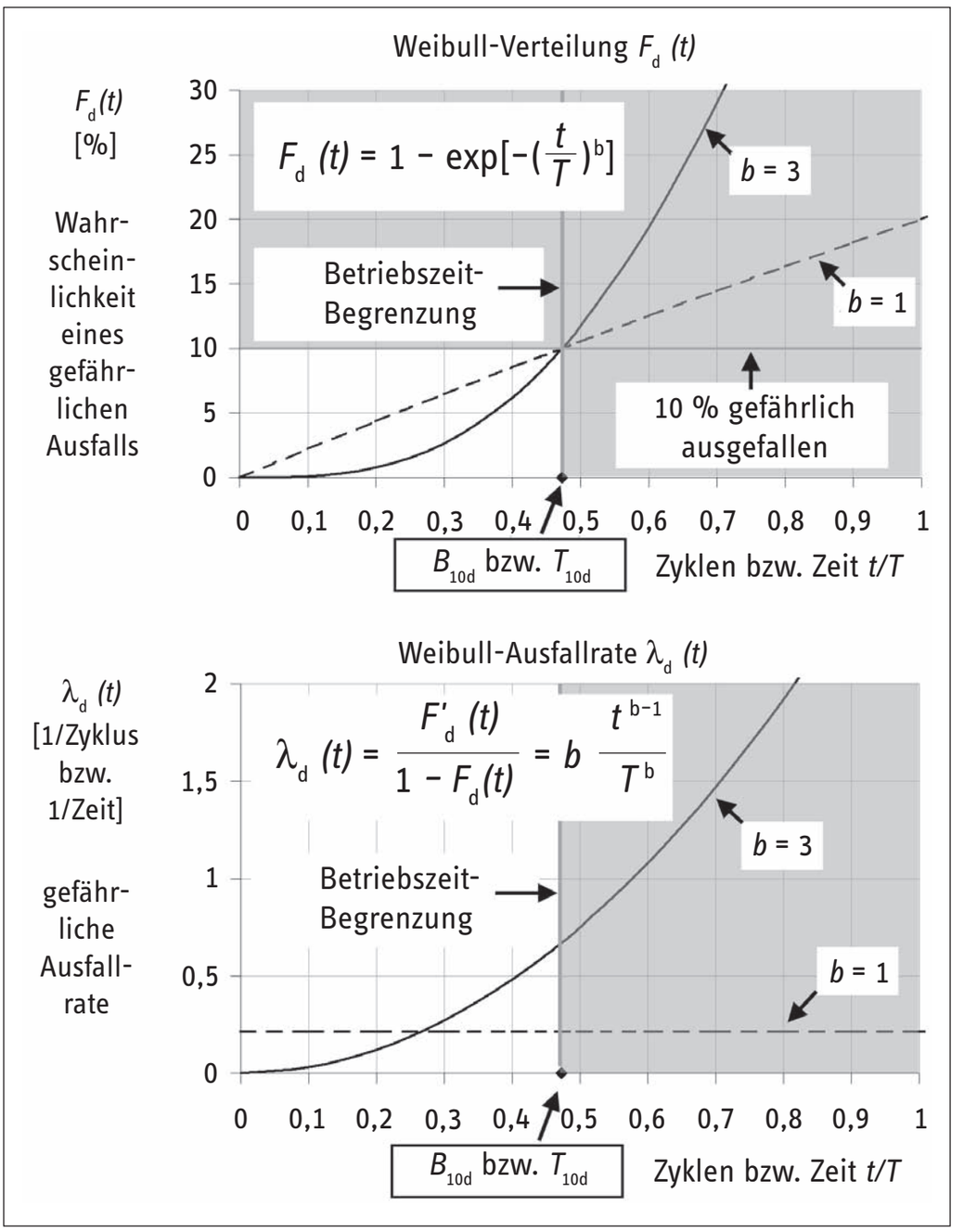


Abbildung D.3: Illustration der Umrechnung von B_{10d} in $MTTF_d$

Bei der Ermittlung der Zuverlässigkeit von Pneumatikventilen wird die Lebensdauer (B_{10}-Wert bzw. B-Wert) in Zyklen bis zum Ausfall angegeben. Die nominale Lebensdauer B_{10} (in einigen Literaturangaben auch t_{10}) ist die mittlere Zahl von Schaltspielen bzw. Schaltzyklen, nach der bis 10 % der betrachteten Menge ausgefallen sind. Da das Ausfallkriterium „Verfügbarkeit" bei Ventilen auch nicht sicherheitsrelevante Ausfälle beinhaltet (z.B. Leckage über dem definiertem Schwellwert), wurde normativ vereinbart, dass der ermittelte Wert für die nominale Lebensdauer (B_{10}) mit zwei multipliziert den B_{10d}-Wert (engl. dangerous, nominale Lebensdauer, nach der bis 10 % der Bauteile gefahrbringend ausgefallen sind) ergeben kann:

$$B_{10d} = 2 \cdot B_{10} \tag{2}$$

Der B_{10}-Wert wird in der Regel im Labor ermittelt. Dabei werden mindestens sieben Ventile von unterschiedlichen Produktionszeitpunkten einer Langzeitbelastung ausgesetzt. Die maximale Schaltfrequenz für die Langzeitbelastung wird über den Druckaufbau (Erreichen von 90 % des Prüfdruckes) und den Druckabbau (Erreichen von 10 % des Prüfdruckes) in einem angeschlossenen, nach Anschlussquerschnitten definierten Volumen ermittelt. Für eine Bewertung der Prüfergebnisse sollten mindestens fünf von sieben Ventilen ausgefallen sein.

Näherungsweise gilt, dass bei einer geringen Anzahl von Prüflingen, z.B. sieben Ventilen, der Erstausfall den B_{10}-Wert bestimmt bzw. die bis zum Zeitpunkt des Erstausfalls erreichten Zyklen ungefähr dem B_{10}-Wert entsprechen. Ist der Erstausfall gefahrbringend, entspricht diese Schaltspielzahl ungefähr dem B_{10d}-Wert.

Als gefahrbringende Ausfälle bei Pneumatikventilen sind insbesondere zu nennen:

- Nichtschalten (Hängenbleiben in der End- oder Nulllage) oder nicht vollständiges Schalten (Hängenbleiben in einer beliebigen Zwischenstellung)
- Veränderung der Schaltzeiten
- selbsttätige Veränderung der Ausgangs-Schaltstellung (ohne Eingangssignal)

Die Betrachtung der Ausfälle bezieht sich immer auf die Baueinheit, z.B. bestehend aus Hauptventil und Vorsteuerventil.

D2.4.2 Umrechnung von B_{10d} in $MTTF_d$

Da der $MTTF_d$-Wert in Jahren angegeben wird, muss der als Anzahl von Zyklen angegebene B_{10d}-Wert entsprechend umgeformt werden. Folgende Parameter sind für die Bestimmung des $MTTF_d$-Wertes notwendig

- h_{op} → mittlere Betriebszeit in Stunden (h) je Tag
- d_{op} → mittlere Betriebszeit in Tagen je Jahr
- t_{Zyklus} → mittlere Zeit zwischen dem Beginn zweier aufeinanderfolgender Zyklen des Bauteils (z.B. Schalten eines Ventils) in Sekunden (s) je Zyklus

Aus diesen Parametern kann die mittlere Anzahl jährlicher Betätigungen n_{op} (in Zyklen pro Jahr) ermittelt werden:

$$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{Zyklus}} \cdot 3\,600\ \frac{s}{h} \tag{3}$$

Setzt man den n_{op}-Wert in Gleichung (4) ein, ergibt sich die $MTTF_d$ für das betrachtete Bauteil in Jahren:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}} \tag{4}$$

Dabei wird die Betriebszeit des Bauteils auf den sogenannten T_{10d}-Wert (Zeit, bei der 10 % der betrachteten Bauteile gefährlich ausgefallen sind) begrenzt. Dieser T_{10d}-Wert kann wie folgt ermittelt werden:

$$T_{10d} = \frac{B_{10d}}{n_{op}} \tag{5}$$

Dies bedeutet, dass die betrachteten Bauteile vor Erreichen des T_{10d}-Wertes ausgewechselt werden sollten.

Die Umrechnung des B_{10d}-Wertes in einen $MTTF_d$-Wert unter Zuhilfenahme von n_{op} und der Begrenzung durch T_{10d} beruht auf einer Näherung. Das reale, von Verschleißeffekten geprägte Ausfallverhalten, das gut durch eine Weibull-Funktion beschrieben wird, wird durch eine Exponentialverteilung mit konstanter Ausfallrate (deren Kehrwert den $MTTF_d$-Wert darstellt) genähert. Dieses Verfahren wird in Abbildung D.3 illustriert. Die durchgezogene Linie stellt eine Weibull-Verteilung mit $b = 3$ dar. Die gestrichelte Linie entspricht dann einer Exponentialverteilung mit $b = 1$, welche die ursprüngliche Weibull-Verteilung im Punkt ($t = B_{10d}$; $F_d = 10$ %) schneidet. Wird der Zusammenhang $MTTF_d = 1/\lambda_d$ für Exponentialverteilungen und die Umrechnung von Zyklen in Zeiten durch n_{op} berücksichtigt, so leitet sich aus dieser Schnittbedingung die Näherungsformel für die Umrechnung von B_{10d} in $MTTF_d$ ab. Dabei wird ausgenutzt, dass die Ausfallrate vor Erreichen der Verschleißphase sehr gering ist und erst ab einem gewissen Zeitpunkt deutlich ansteigt. Dieser Zeitpunkt wird näherungsweise durch B_{10d} (in Zyklen) bzw. T_{10d} (als Zeit in Jahren) festgelegt. Indem nun die Einsatzdauer auf T_{10d} beschränkt wird, kann die leicht ansteigende Ausfallrate durch einen konstanten Wert in der Nähe von T_{10d} zur sicheren Seite hin abgeschätzt werden. In Abbildung D.3 lässt sich erkennen, dass diese Begrenzung der Einsatzdauer auf T_{10d} sehr wichtig ist: Oberhalb steigt der real zu erwartende Anteil gefährlicher Ausfälle mit der Zeit gegenüber der exponentiellen Näherung deutlich an. Auch die gewählte „Ersatz-Ausfallrate" $\lambda_d = 1/MTTF_d$ der exponentiellen Näherung entspricht ungefähr dem arithmetischen Mittelwert der real zu erwartenden Ausfallrate bis zum Zeitpunkt T_{10d}. Jenseits von T_{10d} ergeben sich jedoch durch das Eintreten in die Verschleißphase starke Abweichungen.

D2.5 Verfahren guter ingenieurmäßiger Praxis

Sind keine Herstellerangaben für die Zuverlässigkeit von Bauteilen verfügbar, schlägt die Norm als erste Alternative vor, Datenbankwerte zu verwenden. Als Unterstützung liefert sie für mechanische, hydraulische und pneumatische Komponenten sowie für häufig in der Praxis eingesetzte elektromechanische Sicherheitsbauteile „typische Werte" mit. Diese Werte sind als $MTTF_d$-Werte, B_{10d}-Werte oder Fehlerausschlüsse in Tabelle D.2 aufgeführt. Dieser B_{10d}-Wert, den der Bauteilhersteller durch Prüfung ermittelt, gibt die mittlere Anzahl von Zyklen an, bei der 10 % der Bauteile gefahrbringend ausgefallen sind. Mithilfe dieses Wertes ist es möglich, den $MTTF_d$-Wert abzuschätzen. Die Verwendung der Werte aus der Tabelle D.2 ist allerdings an verschiedene Voraussetzungen gebunden:

- Der Hersteller des Bauteils bestätigt die Verwendung von grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003 oder der entsprechenden Norm (siehe Tabelle D.2) für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).
- Der Hersteller eines Bauteils, das in einer Steuerung der Kategorie 1, 2, 3 oder 4 verwendet werden soll, bestätigt die Verwendung bewährter Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003 oder der entsprechenden Norm (siehe Tabelle D.2) für die Konstruktion des Bauteils (Bestätigung im Datenblatt des Bauteils).
- Der Hersteller des Bauteils legt die geeignete Anwendung und Betriebsbedingungen für den Anwender fest und informiert ihn über seine Verantwortung, die grundlegenden Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003 für die Implementierung und den Betrieb des Bauteils zu erfüllen.
- Der Anwender erfüllt die grundlegenden und/oder bewährten Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003 für die Implementierung und den Betrieb des Bauteils.

Tabelle D.2:
Typische Zuverlässigkeitskennwerte, die bei guter ingenieurmäßiger Praxis als erreicht angenommen werden können

	Grundlegende und bewährte Sicherheitsprinzipien nach DIN EN ISO 13849-2:2003	Andere relevante Normen	Typische Werte: $MTTF_d$ (Jahre) B_{10d} (Zyklen) bzw. Fehlerausschluss
Mechanische Bauteile	Tabellen A.1 und A.2	–	$MTTF_d$ = 150
Hydraulische Bauteile	Tabellen C.1 und C.2	EN 982	$MTTF_d$ = 150
Pneumatische Bauteile	Tabellen B.1 und B.2	EN 983	B_{10d} = 20 000 000
Relais und Hilfsschütze mit vernachlässigbarer Last	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 20 000 000
Relais und Hilfsschütze mit maximaler Last	Tabellen D.1 und D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 400 000
Näherungsschalter mit vernachlässigbarer Last	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Näherungsschalter mit maximaler Last	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 400 000
Schütze mit vernachlässigbarer Last	Tabellen D.1 und D.2	IEC 60947	B_{10d} = 20 000 000
Schütze mit nominaler Last	Tabellen D.1 und D.2	IEC 60947	B_{10d} = 2 000 000
Positionsschalter unabhängig von der Last[a)]	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Positionsschalter (mit separatem Betätiger, Zuhaltung) unabhängig von der Last[a)]	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 2 000 000
Positionsschalter und Taster[b)] bei ohmscher Last und Überdimensionierung (≤ 10 % der maximalen Last) bezogen auf die elektrischen Kontakte	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 1 000 000
Positionsschalter und Taster[b)] bei Überdimensionierung nach Tabelle D.2, DIN EN ISO 13849-2:2003, bezogen auf die elektrischen Kontakte	Tabellen D.1 und D.2	IEC 60947 EN 1088	B_{10d} = 100 000
Not-Halt-Geräte bei Einsatz unter geringer umwelttechnischer Belastung, z.B. in Laboren[a)]	Tabellen D.1 und D.2	IEC 60947 ISO 13850	Fehlerausschluss bis 100 000 Zyklen, sofern Herstellerbestätigung vorliegt
Not-Halt-Geräte bei Einsatz unter normaler umwelttechnischer Belastung, z.B an Maschinen[a)]	Tabellen D.1 und D.2	IEC 60947 ISO 13850	Fehlerausschluss bis 6 050 Zyklen
Zustimmungsschalter (3-stufig) unabhängig von der Last[a)]	Tabellen D.1 und D.2	IEC 60947	Fehlerausschluss bis 100 000 Zyklen

a) falls Fehlerausschluss für Zwangsöffnung möglich ist

b) für Schließerkontakte und für Öffnerkontakte, falls Fehlerauschluss für Zwangsöffnung nicht möglich ist

Mit der Umsetzung dieser Anforderungen soll sichergestellt werden, dass die Anwendung grundlegender und/oder bewährter Sicherheitsprinzipien von der Herstellung über die Implementierung bis zum laufenden Betrieb des Bauteils gewährleistet ist. Auch die Schnittstelle zwischen Hersteller und Anwender bzw. Betreiber der Maschine ist klar definiert: Der Hersteller muss die Berücksichtigung der Sicherheitsprinzipien bei der Konstruktion verbindlich bestätigen und alle relevanten Informationen zu Einsatz- und Betriebsbedingungen zur Verfügung stellen. Der Anwender bzw. Betreiber der Maschine seinerseits ist für die Einhaltung aller Sicherheitsprinzipien verantwortlich, die Implementierung und Betrieb des Bauteils betreffen. Unter diesen Voraussetzungen kann bei der Berechnung der $MTTF_d$ oder bei der Annahme eines Fehlerausschlusses auf die in Tabelle D.2 zitierten typischen Werte zugegriffen werden. Der oben begründete $MTTF_d$-Wert von 150 Jahren für hydraulische Steuerungskomponenten wird hier auch auf mechanische Komponenten ausgedehnt. Dieser Hilfswert kann verwendet werden, wenn zwar kein Fehlerausschluss begründet werden kann, aber der Einsatz grundlegender bzw. bewährter Sicherheitsprinzipien gewährleistet ist. Außerdem werden B_{10d}-Werte für elektromechanische Bauteile genannt, die nach dem ebenfalls oben vorgestellten Verfahren mit der durchschnittlichen Anzahl jährlicher Betätigungen n_{op} in einen $MTTF_d$-Wert umgerechnet werden können. Einen Sonderfall stellen Not-Halt-Geräte und Zustimmungsschalter dar, für die unter bestimmten Bedingungen ein Fehlerausschluss angenommen werden kann.

Alle Werte in der Tabelle beziehen sich nur auf gefahrbringende Ausfälle, was durch den Index „d“ ausgedrückt ist. Hier wurde in der Regel unterstellt, dass nur die Hälfte aller Ausfälle gefahrbringend ist. Insofern können diese Werte durchaus optimistischer aussehen als Datenblattangaben von Herstellern, die sich im Sinne der Verfügbarkeit auf alle Fehlerarten beziehen, die den Funktionsablauf beeinträchtigen können. Bei einigen elektromechanischen Bauteilen, beispielsweise Relais, Hilfsschützen und Schützen, geht die elektrische Belastung der Kontakte stark in den B_{10d}-Wert ein, was durch vielfältige Beobachtungen aus der Praxis bestätigt wird. Bei geringer elektrischer Last (typischerweise ohmscher Last), DIN EN ISO 13849-1 spricht hier von bis zu 20 % des Bemessungswertes, ergeben sich deutlich bessere Werte. Hier wurde dann die mechanische statt der elektrischen Lebensdauer unterstellt. Je nach Art (ohmsch oder induktiv) und Größe der Last können auch B_{10d}-Zwischenwerte der hier genannten Extreme abgeleitet werden. Bei den in der Tabelle aufgeführten Positionsschaltern, Zuhaltungen, Not-Halt-Geräten und Tastern, beispielsweise Zustimmungsschaltern, wird für den elektrischen Teil meist das Sicherheitsprinzip der Zwangsöffnung vorausgesetzt. Damit kann für den elektrischen Teil unabhängig von der Last von einem Fehlerausschluss ausgegangen werden und die zitierten B_{10d}-Werte begründen sich hauptsächlich durch Ausfälle in der Betätigungsmechanik. Aus dieser Sichtweise ergeben sich z.B. auch die deutlichen Unterschiede zwischen Positionsschaltern ohne bzw. mit separatem Betätiger oder Zuhaltungen. Für Schließerkontakte und Öffnerkontakte ohne zwangsöffnende Eigenschaften kann allerdings kein Fehlerausschluss herangezogen werden. Dies äußert sich in deutlich geringeren typischen B_{10d}-Werten. Da Not-Halt-Geräte und Zustimmungsschalter eine garantierte fehlerfreie Mindestbetätigungsanzahl (siehe Tabelle D.2) aufweisen müssen, kann bis zu dieser Betätigungsanzahl ein Fehlerausschluss auch für die Mechanik angenommen werden. Hierbei müssen wegen der manuellen Betätigung im Gegensatz zu Positionsschaltern auch keine Fehler in der Anfahrmechanik oder Dejustage berücksichtigt werden. Bei Not-Halt-Geräten wird zwischen geringer und normaler Beanspruchung unterschieden. Die in der Typprüfung nachzuweisende fehlerfreie Mindestbetätigungsanzahl von 6 050 Zyklen gilt dabei für normale umwelttechnische Beanspruchung. Einige Hersteller bestätigen zusätzlich 100 000 Zyklen für den Einsatz bei geringer umwelttechnischer Beanspruchung. Um den Fehlerausschluss für Zwangsöffnung für den elektrischen Teil von elektromechanischen Sicherheitsbauteilen anwenden zu können, ist es erforderlich, dass diese Komponenten zusätzlich zu den obigen Voraussetzungen die Bedingungen für „bewährte Bauteile“ erfüllen.

Naturgemäß handelt es sich bei diesen Ansätzen um starke Vereinfachungen der komplexen realen Zusammenhänge. So kann zum Beispiel insbesondere ein sehr geringer Laststrom bei seltener Betätigung zu einem Kaltverschweißen elektrischer Kontakte führen. Diese Effekte sollen aber durch die geforderte Anwendung grundlegender bzw. bewährter Sicherheitsprinzipien vermieden werden, zu denen auch die Eignung und Angepasstheit der mechanischen wie der elektrischen Bauteileigenschaften an die zu erwartende Belastung gehören.

D2.6 $MTTF_d$ elektronischer Steuerungskomponenten

Wie bereits erwähnt, ist die Angabe der Ausfallraten λ bzw. λ_d, z.B. als FIT-Werte (Failures In Time, d.h. Ausfälle in 10^9 Bauteilstunden), für elektronische Bauteile schon seit Längerem üblich. Daher ist die Chance recht hoch, über den Hersteller an Zuverlässigkeitsinformationen zu kommen. Unter Umständen müssen diese Angaben noch in $MTTF_d$-Werte umgerechnet werden, z.B. mithilfe der vereinfachenden Annahme, dass nur 50 % aller Ausfälle gefahrbringend sind. Sind trotzdem keine Herstellerangaben erhältlich, so kann eine Reihe von bekannten Datensammlungen herangezogen werden, von denen Folgende in DIN EN ISO 13849-1 beispielhaft zitiert werden:

- Siemens Standard SN 29500, Ausfallraten für Bauteile, Siemens AG (wird unregelmäßig aktualisiert) www.pruefinstitut.de
- IEC/TR 62380, Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment, identisch zu RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l’Electricité et de la Communication www.ute-fr.com
- Reliability Prediction of Electronic Equipment, MIL-HDBK-217F, Department of Défense, Washington DC, 1982; mittlerweile fortgeführt als 217Plus System Reliability Assessment Tool, Reliability Information Analysis Center, 6000 Flanagan Road, Suite 3, Utica, New York 13502-1348 (theRIAC.org)
- Reliability Prediction Procedure for Electronic Equipment, Telcordia SR-332, Issue 01, May 2001 (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06)
- EPRD, Electronic Parts Reliability Data (RAC-STD-6100), Reliability Information Analysis Center, 6000 Flanagan Road, Suite 3, Utica, New York 13502-1348 (theRIAC.org)
- NPRD-95, Nonelectronic Parts Reliability Data (RAC-STD-6200), Reliability Information Analysis Center, 6000 Flanagan Road, Suite 3, Utica, New York 13502-1348 (theRIAC.org)
- British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom (HRD5, last issue)
- Chinese Military Standard, GJB/z 299B

Neben diesen Datensammlungen gibt es auf dem Markt eine Reihe von Hilfsprogrammen, die diese oder andere Datenbanken per Software zugänglich machen. In den meisten Datenbanken sind elektronische Komponenten nach Bauteilart und weiteren Kriterien (z.B. Bauform, Material, Gehäuse) katalogisiert. Meist werden zunächst Basis-Ausfallraten für Referenzbedingungen genannt (z.B. für 40 °C Bauteil-Umgebungstemperatur und nominale Last), die für davon abweichende Beanspruchungen durch Anpassungsfaktoren auf die realen Einsatzbedingungen korrigiert werden können. In DIN EN ISO 13849-1 sind sogar für einige typische elektronische Komponenten Werte aufgelistet, die der Datensammlung SN 29500 entnommen und mit einem Sicherheitsfaktor von 10 versehen sind. Da diese Werte eher beispielhaften Charakter haben, sind sie hier nicht wiedergegeben. Der Sicherheitsfaktor 10 in Anhang C.5 der Norm soll den Worst Case abdecken, wenn ein sehr pauschaler Richtwert gesucht wird. Bei korrekter Verwendung der Datenquellen ist ein zusätzlicher Sicherheitsfaktor in der Regel nicht erforderlich. Die Anpassung an Beanspruchungen außerhalb der Referenzbedingungen wird in DIN EN ISO 13849-1 nicht explizit gefordert und sollte im Sinne der Einfachheit mit Augenmaß angewendet werden.

D3 Integration bereits zertifizierter Komponenten und Geräte

In noch seltenen, aber in Zukunft wohl häufigeren Fällen können Hersteller ihre Komponenten bereits mit der Angabe einer $MTTF_d$ im Datenblatt versehen. Ein ähnlicher Fall ergibt sich, falls für die Komponenten bereits in den Herstellerinformationen ein SIL nach DIN EN 61508 oder ein PL nach DIN EN ISO 13849-1, verbunden mit der Angabe einer „durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde“ (bzw. PFH-Wert nach DIN EN 61508), genannt wird. Falls solche Komponenten nur in einem Kanal des SRP/CS verwendet werden, kann die angegebene Ausfallwahrscheinlichkeit pro Stunde (*PFH*) als Ersatzwert für die Ausfallrate in die gefährliche Richtung betrachtet werden, wobei komponenteninterne Merkmale wie Redundanz und Eigendiagnose bereits berücksichtigt sind:

$$MTTF_d = \frac{1}{\lambda_d} \approx \frac{1}{PFH} \quad \text{(„Black-Box“-Komponenten mit PFH innerhalb eines Kanals)} \tag{6}$$

D4 „Parts Count“-Verfahren

Sind die $MTTF_d$-Werte aller sicherheitsrelevanten Komponenten bekannt, so muss hieraus zunächst die $MTTF_d$ jedes Blocks berechnet werden. Dieser Schritt lässt sich zwar per FMEA (Ausfalleffektanalyse) sehr detailliert durchführen (siehe Anhang B), allerdings müssen dazu im Idealfall die unterschiedlichen Ausfallarten jeder sicherheitsrelevanten Komponente und ihre Wirkung für den Block analysiert werden. Dieser Ansatz lohnt sich – gemessen am Aufwand – daher meist nur für Komponenten mit einer hohen Ausfallrate, d.h. einem kleinen $MTTF_d$-Wert. Als schnelle Alternative, die im Mittel auch nicht auf viel schlechtere Werte führt, bietet DIN EN ISO 13849-1 das sogenannte „Parts Count“-Verfahren an. Im Wesentlichen handelt es sich dabei um eine Summation mit drei Hauptannahmen:

- Für alle Ausfallarten einer Komponente und deren Auswirkungen auf den Block wird pauschal eine Aufteilung je zur Hälfte in ungefährliche und gefahrbringende Ausfälle angesetzt. Dies bedeutet, dass die Hälfte der Ausfallrate λ einer Komponente zur gefahrbringenden Ausfallrate λ_d des zugehörigen Blocks beiträgt. Wurde für die Komponente bereits der gefahrbringende Anteil der Ausfallrate λ_d bestimmt, so wird der gleiche Wert λ_d auch dem Block angerechnet.
- Die gefahrbringende Ausfallrate λ_d des Blocks wird dann durch Summation der λ_d-Beiträge aller N im jeweiligen Block vorhandenen sicherheitsrelevanten Komponenten gebildet (wobei sich die Beiträge identischer Komponenten einfach zusammenfassen lassen):

$$\lambda_d = \frac{1}{2}\sum_{i=1}^{N}\lambda_i \text{ bzw. } \lambda_d = \sum_{i=1}^{N}\lambda_{di} \tag{7}$$

Da DIN EN ISO 13849-1 wie oben erläutert von konstanten Ausfallraten ausgeht, lassen sich Ausfallraten λ_d einfach durch Kehrwertbildung in $MTTF_d$-Werte umrechnen. Wird dieser Zusammenhang zugrunde gelegt, so ergibt sich der $MTTF_d$-Wert eines Blocks leicht aus den $MTTF_d$-Werten der zugehörigen Komponenten. Ein Beispiel für die Anwendung des „Parts Count“-Verfahrens findet sich in Kapitel 6.

D5 Reihenschaltung von Blöcken in einem Kanal und $MTTF_d$-Begrenzung

Liegen $MTTF_d$-Werte bzw. Ausfallraten λ_d für jeden Block vor, lässt sich durch Summation der Ausfallraten aller an einem Kanal beteiligten Blöcke ebenfalls gemäß Gl. (7) die $MTTF_d$ für jeden Kanal berechnen. Dabei wird unterstellt, dass der gefährliche Ausfall eines beliebigen Blocks in der Kette der Blöcke, die einen Kanal darstellt, auch als gefährlicher Ausfall des Kanals zu werten ist. Da unter Umständen aber durch nachgeordnete Blöcke ein gefährlicher Ausfall von davor angeordneten Blöcken bemerkt werden kann, bildet diese Annahme eine Abschätzung zur sicheren Seite. In dieser Phase der $MTTF_d$-Bestimmung greift die Kappungsregel der DIN EN ISO 13849-1: Jeder $MTTF_d$-Wert eines Kanals, der rechnerisch > 100 Jahre ist, wird regelgemäß auf den Höchstwert von 100 Jahren reduziert. Durch diese Regel wird die Überbewertung der Bauteilzuverlässigkeiten gegenüber den anderen für den PL relevanten Größen wie Architektur, Tests und Ausfälle infolge gemeinsamer Ursache vermieden.

D6 Symmetrisierung bei mehreren Kanälen

Sobald zwei Kanäle in einer Steuerung vorhanden sind (dies ist in der Regel bei Kategorie 3 und 4 der Fall), stellt sich die Frage, welcher der $MTTF_d$-Werte für jeden Kanal bei der Bestimmung des PL mithilfe des Säulendiagramms verwendet werden soll. Auch für diese Frage hält DIN EN ISO 13849-1 eine einfache Formel als Antwort bereit:

$$MTTF_d = \frac{2}{3}\left(MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right) \tag{8}$$

Die mittlere $MTTF_d$ pro Kanal ergibt sich also durch eine Mittelungsformel aus den $MTTF_d$-Werten beider redundanter Kanäle C1 und C2 (diese Formel lässt sich mathematisch herleiten, indem der $MTTF_d$-Wert für ein zweikanaliges System ohne Diagnose, aber mit bekannten $MTTF_d$-Werten beider Kanäle – $MTTF_{dC1}$ und $MTTF_{dC2}$ – gesucht wird [5]). Damit ist die sukzessive Zusammenfassung der $MTTF_d$-Werte aller an der Steuerung beteiligten Komponenten abgeschlossen. Das Ergebnis ist ein Kennwert für die typische Zuverlässigkeit der in der Steuerung vorhandenen Komponenten ohne Berücksichtigung von Redundanz, Diagnose oder CCF. Während $MTTF_d$ bereits für jeden beteiligten Kanal auf 100 Jahre begrenzt wird, ist die Einteilung der $MTTF_d$-Werte in eine der drei Klassen „niedrig", „mittel" oder „hoch" erst nach der Symmetrisierung sinnvoll. Der symmetrisierte Wert geht als ein Parameter neben der Kategorie, dem durchschnittlichen Diagnosedeckungsgrad und den Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache in die numerische Bestimmung des PL ein. Daneben wird je nach zu erreichender Kategorie ein minimaler $MTTF_d$-Wert von drei Jahren (für Kategorie B, 2 und 3) oder 30 Jahren (für Kategorie 1 und 4) benötigt.

Literatur

[1] *Birolini, A.:* Qualität und Zuverlässigkeit technischer Systeme: Theorie, Praxis, Management. 3. Aufl. Springer, Berlin 1991

[2] *Bork, T.; Schaefer, M.:* Aus Aktivität wird Vorsicht – Sinn und Unsinn der Quantifizierung. O + P Ölhydraulik und Pneumatik 51 (2007) Nr. 3, S. 78-85
http://www.dguv.de/bgia/de/pub/grl/pdf/2007_016.pdf

[3] *Schuster, U.:* Untersuchung des Alterungsprozesses von hydraulischen Ventilen. BGIA-Report 6/04. Hrsg.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2004
www.dguv.de/bgia, Webcode d6362

[4] *Weibull, W.:* A statistical distribution function of wide applicability. J. Appl. Mech. 18 (1951), S. 292-297

[5] *Goble, W.M.:* Control systems safety evaluation and reliability. 2nd ed. Hrsg.: Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina 1998

Anhang E:
Bestimmung des Diagnosedeckungsgrades *(DC)*

Der Diagnosedeckungsgrad *DC* (Diagnostic Coverage) ist ein Maß für die Wirksamkeit der Selbsttest- und Überwachungsmaßnahmen in einer Steuerung. Er kann sich auf Bauelemente, Blöcke oder die ganze Steuerung (DC_{avg}) beziehen. Die genaue Definition des *DC* beruht auf einer Einteilung von Ausfällen in drei Gruppen (siehe Abbildung E.1):

- Ungefährliche Ausfälle s (safe): Diese führen automatisch dazu, dass ein sicherer Zustand eingenommen wird, aus dem heraus keine Gefährdungen entstehen (Beispiel: Offenbleiben eines Schützes oder Geschlossenbleiben eines Ventils mit der Folge eines Stillstands potenziell gefahrbringender Bewegungen).

- Erkennbare gefahrbringende Ausfälle dd (dangerous detectable): Diese potenziell gefahrbringenden Ausfälle werden durch Test- oder Überwachungsmaßnahmen erkannt und in einen sicheren Zustand überführt (Beispiel: Geschlossenbleiben eines Schützes oder Offenbleiben eines Ventils, das durch einen Rücklesekontakt oder eine Stellungsüberwachung erkannt und sicher abgefangen wird).

- Unerkennbar gefahrbringende Ausfälle du (dangerous undetectable): Diese potenziell gefahrbringenden Ausfälle werden nicht erkannt (Beispiel: unbemerktes Geschlossenbleiben eines Schützes oder Offenbleiben eines Ventils, wodurch bei einer Anforderung eines sicher abgeschalteten Moments kein Stillsetzen einer gefahrbringenden Bewegung erfolgt).

Bei mehrkanaligen Systemen wird die Bezeichnung „gefahrbringender Ausfall“ im Hinblick auf einen einzelnen Kanal verwendet, obwohl damit noch kein gefahrbringender Systemausfall gegeben sein muss. „dd“ und „du“ lassen sich zur Gruppe der gefahrbringenden Ausfälle d (dangerous) zusammenfassen. Auch die ungefährlichen Ausfälle können erkennbar oder unerkennbar sein, was aber unerheblich ist, da in beiden Fällen der sichere Zustand eingenommen wird.

Der Diagnosedeckungsgrad bestimmt sich durch den Anteil der erkennbaren gefahrbringenden Ausfälle (dd) an allen gefahrbringenden Ausfällen (d) und wird meist als Prozentzahl notiert. Zu seiner Berechnung, z.B. im Zusammenhang mit einer FMEA (Ausfalleffektanalyse, siehe Anhang B), werden die aufsummierten Ausfallraten λ_{dd} und λ_{d} der Betrachtungseinheit zueinander ins Verhältnis gesetzt. Hier zeigt sich, dass der *DC* eine Kenngröße ist, die der getesteten Einheit (z.B. Block) zugeordnet wird und nicht der Testeinrichtung, welche die Tests durchführt. Um die DC-Bestimmung zu vereinfachen, geht DIN EN ISO 13849-1 einen anderen Weg und schlägt für typische Diagnosemaßnahmen DC-Eckwerte vor, von deren Erreichung ausgegangen werden kann. Auf diese Weise wird eine mühsame FMEA durch eine tabellarische Bewertung der umgesetzten Diagnosemaßnahmen ersetzt. Dies ist in ähnlicher Weise oft gängige und ökonomisch sinnvolle Praxis von Prüfstellen.

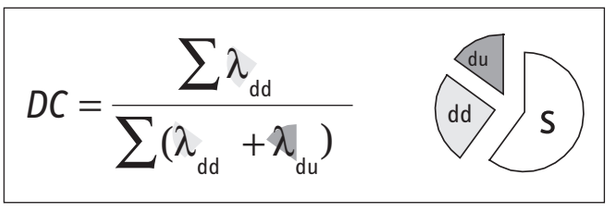
Da der Anteil der unerkennbar gefahrbringenden Ausfälle (also 1 – *DC*) die für die Ausfallwahrscheinlichkeit relevante Größe zur Bewertung der realisierten Test- und Überwachungsmaßnahmen ist, erklärt sich die Wahl der Eckwerte (60, 90 und 99 %), mit deren Hilfe vier DC-Qualitätsstufen gebildet werden (Tabelle E.1).

Tabelle E.1:
Die vier Stufen des Diagnosedeckungsgrades im vereinfachten Ansatz der DIN EN ISO 13849-1

DC (Diagnosedeckungsgrad)	
Bezeichnung	Bereich
kein	DC < 60 %
niedrig	60 % ≤ DC < 90 %
mittel	90 % ≤ DC < 99 %
hoch	99 % ≤ DC

Es muss grundsätzlich unterschieden werden zwischen dem *DC* eines einzelnen Tests für eine bestimmte Komponente bzw. einen Block und dem durchschnittlichen Diagnosedeckungsgrad DC_{avg} (average) für die gesamte betrachtete Steuerung. Die Gruppenbildung mithilfe der Eckwerte wird dabei sowohl zur Qualifizierung der einzelnen Tests herangezogen als auch bei der Benennung von DC_{avg}. Da der DC_{avg} eine der Eingangsgrößen für die vereinfachte Quantifizierung der Ausfallwahrscheinlichkeit mithilfe des Säulendiagramms ist, wird der berechnete DC_{avg}-Wert auf einen der vier Eckwerte (0 %, 60 %, 90 % und 99 %) in Einklang mit Tabelle E.1 abgerundet bzw. in eine der vier DC-Klassen (kein, niedrig, mittel und hoch) eingeordnet. Ein DC_{avg}-Wert von 80 % wird im vereinfachten Ansatz daher auf einen Wert von 60 % herabgestuft (anders als im BGIA-Software-Assistenten SISTEMA, der in der Grundeinstellung mit DC_{avg}-Zwischenwerten rechnet, siehe Anhang H). Im Folgenden wird zunächst auf den *DC* einzelner Tests und danach auf die Berechnung von DC_{avg} eingegangen.

Abbildung E.1:
Illustration des Diagnosedeckungsgrades



In Tabelle E.2 sind typische Test- und Überwachungsmaßnahmen bezogen auf Komponenten bzw. Blöcke und ihre DC-Bewertung nach DIN EN ISO 13849-1 dargestellt. Je nach Funktion (I, L, O bzw. Eingabe, Logik, Ausgabe), Kategorie und Technologie sind unterschiedliche Maßnahmen üblich. Ihre Bewertung kann je nach Ausführung oder äußeren Umständen schwanken, z.B. je nach Anwendung, in der die Steuerung betrieben wird. Die indirekte Überwachung durch Wegaufnehmer oder Entschalter an den Aktoren statt an den Steuerungselementen lässt je nach Anwendung z.B. keinen Rückschluss zu, ob jeder von zwei

Tabelle E.2:
DC-Eckwerte für typische Test- und Überwachungsmaßnahmen auf Komponenten- bzw. Blockebene nach DIN EN ISO 13849-1

Maßnahme	hauptsächlich relevant für			*DC* [%]	Maßnahmen-Beschreibung
	I	L	O		
Zyklische Testung/Dynamisierung	X			90	Periodische Generierung eines Signalwechsels mit Überwachung des Ergebnisses
Plausibilität/Rücklesung/(Kreuz-)Vergleich					Der erreichte DC-Wert ist abhängig von der Häufigkeit eines Signalwechsels in der Anwendung.
● ohne Dynamisierung	X		X	0-99	
● mit Dynamisierung, ohne hochwertige Fehlererkennung	X		X	90	
● mit Dynamisierung, mit hochwertiger Fehlererkennung	X		X	99	
Indirekte Überwachung	X	X	X	90-99	Der erreichte DC-Wert ist abhängig von der Anwendung.
Direkte Überwachung	X	X	X	99	
Fehlererkennung durch den Prozess	X	X	X	0-99[1]	Der erreichte DC-Wert ist abhängig von der Anwendung, diese Maßnahme alleine ist nicht ausreichend, um PL e [2] zu erreichen.
Überwachung von Eigenschaften	X			60	
Programmlaufüberwachung					zeitliche Überwachung
● einfache zeitliche		X		60	
● zeitlich und logisch		X		90	
Selbsttests bei Anlauf		X	(X)	90	zur Erkennung verborgener Fehler, *DC* abhängig von der Testausführung
Testung der Überwachungseinrichtung		X		90	Testung der Reaktionsmöglichkeit der Überwachungseinrichtung durch den Hauptkanal nach Anlauf oder wann immer die Sicherheitsfunktion angefordert wird oder wann immer ein externes Signal dies durch eine Eingangseinrichtung anfordert

redundanten Steuerungskanälen die Sicherheitsfunktion noch unabhängig ausführen kann. Generell wird bei der Bewertung nicht unterschieden zwischen automatischen (z.B. regelmäßig ablaufenden Programmroutinen) oder willensabhängigen Tests (z.B. manuell durch den Bediener in regelmäßigen Abständen eingeleitete Tests). Auch welche Einheit einen Test durchführt, ist unerheblich, z.B. bei Selbsttests. Wichtig ist aber, dass ein Test nur dann überhaupt wirksam ist, wenn nach Erkennung eines gefahrbringenden Ausfalls auch der sichere Zustand eingenommen wird. Wird z.B. das Verschweißen eines Hauptschützes erkannt, aber ohne eine Möglichkeit zur rechtzeitigen Stillsetzung einer gefahrbringenden Bewegung, so ist die Erkennung nutzlos und mit einem *DC* von 0 % zu bewerten.

<table>
<tr><th colspan="5">typische Realisierung in verschiedenen Technologien</th></tr>
<tr><th>Mechanik</th><th>Pneumatik</th><th>Hydraulik</th><th>Elektrik</th><th>(Programmierbare) Elektronik</th></tr>
<tr><td colspan="5">siehe Maßnahmenbeschreibung</td></tr>
<tr><td rowspan="2"></td><td colspan="4">manuelle Initiierung der Prüffunktion</td></tr>
<tr><td colspan="2" rowspan="2">Positionserfassung des Ventilschiebers,
Höhe des DC abhängig von der
konkreten Ausführung</td><td colspan="2">Vergleich von Eingängen oder Ausgängen ohne Kurzschlusserkennung</td></tr>
<tr><td>Kreuzvergleich von Eingängen oder Ausgängen mit Kurzschlusserkennung und Erkennung statischer Fehler, z.B. mithilfe von Sicherheitsbausteinen</td><td>Kreuzvergleich von Signalen und Zwischenwerten mit Kurzschlusserkennung, Erkennung statischer Fehler und zeitliche und logische Programmlaufüberwachung; dynamischer Kreuzvergleich unabhängig gewonnener Stellungs- oder Geschwindigkeitsinformationen</td></tr>
<tr><td>Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen</td><td colspan="2">Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen;
Ventilüberwachung durch Druckschalter</td><td colspan="2">Wegaufnehmer oder Endschalter an den Aktoren statt an den Steuerungselementen</td></tr>
<tr><td>Stellungsüberwachung direkt am überwachten Steuerungselement</td><td colspan="2">Stellungsüberwachung direkt am Ventilschieber über den gesamten Hub</td><td>Stellungsüberwachung durch zwangsgeführte Rücklesekontakte (antivalente Öffnerkontakte)</td><td>Signalüberwachung durch Rücklesung z.B. mittels Optokopplern</td></tr>
<tr><td colspan="5">Versagen der Prozessregelung, die sich durch Fehlfunktion, Beschädigung von Werkstück oder Maschinenteilen,
Prozessunterbrechung oder -verzögerung funktional bemerkbar macht, ohne sofort eine Gefährdung darzustellen</td></tr>
<tr><td colspan="3">Überwachung von Antwortzeiten, Signalstärke analoger Signale</td><td colspan="2">Überwachung von Antwortzeiten, Signalstärke analoger Signale
(z.B. Widerstand, Kapazität)</td></tr>
<tr><td colspan="3">nicht relevant

nicht relevant</td><td>Zeitglied als Watchdog, mit Triggersignalen im Programm der Logik

durch einen Watchdog, wobei die Testeinrichtung Plausibilitätstests des Verhaltens der Logik durchführt</td></tr>
<tr><td></td><td></td><td></td><td>Erkennung z.B. verschweißter Kontakte durch Ansteuerung und Rücklesung</td><td>Erkennung verborgener Fehler in Programm- und Datenspeicher, Eingangs-/Ausgangsanschlüssen, Schnittstellen</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Testung der Reaktionsmöglichkeit des Watchdogs</td></tr>
</table>

Tabelle E.2:
(Fortsetzung)

Maßnahme	hauptsächlich relevant für			DC [%]	Maßnahmen-Beschreibung
	I	L	O		
Dynamische Prinzipien		X		99	alle Bauteile der Logik erfordern eine Zustandsänderung EIN-AUS-EIN, wenn die Sicherheitsfunktion angefordert wird
Speicher- und CPU-Tests					
● Invarianter Speicher: Signatur einfacher Wortbreite (8 Bit)		X		90	
● Invarianter Speicher: Signatur doppelter Wortbreite (16 Bit)		X		99	
● Varianter Speicher: RAM-Test durch Verwendung redundanter Daten, z.B. Flags, Merker, Konstanten, Timer, und Kreuzvergleich dieser Daten		X		60	
● Varianter Speicher: Test der Lesbarkeit und der Beschreibbarkeit der verwendeten Speicherzellen		X		60	
● Varianter Speicher: RAM Überwachung mit modifiziertem Hammingcode oder RAM Selbsttest (z.B. „Galpat“ oder „Abraham“)		X		99	
● Verarbeitungseinheit: Selbsttest durch Software		X		60-90	
● Verarbeitungseinheit: Kodierte Verarbeitung		X		90-99	
Redundanter Abschaltpfad					
● ohne Überwachung des Aktors			X	0	
● mit Überwachung eines der Aktoren entweder durch die Logik oder durch eine Testeinrichtung			X	90	
● mit Überwachung der Aktoren durch die Logik und Testeinrichtung			X	99	

[1] *Zum Beispiel zu ermitteln über eine FMEA durch Bildung des Quotienten der erkannten gefahrbringenden Ausfälle zu allen gefahrbringenden Ausfällen*

[2] *PL e erfordert in der Regel zwei Kanäle. Daher sollte mindestens der komplemantäre Block des redundanten Kanals eine andere DC-Maßnahme umsetzen, deren DC mindestens so groß sein sollte wie der angenommene DC durch den Prozess.*

typische Realisierung in verschiedenen Technologien				
Mechanik	Pneumatik	Hydraulik	Elektrik	(Programmierbare) Elektronik
	Verriegelungsschaltungen in Pneumatik		Verriegelungsschaltungen in Relaistechnik	
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung
	nicht relevant			siehe Maßnahmenbeschreibung

Zu den in Tabelle E.2 genannten Test- und Überwachungsmaßnahmen gilt als zusätzliche Anforderung Folgendes: Wird „mittel“ oder „hoch“ als *DC* für die Logik gefordert, muss mindestens je eine Maßnahme für varianten Speicher, invarianten Speicher und Verarbeitungseinheit mit mindestens je 60 % gewählt werden. Es können auch andere Maßnahmen als die in Tabelle E.2 genannten verwendet werden.

Weitere Informationen zur DC-Bestimmung für typische Testmaßnahmen finden sich z.B. in den Tabellen A.2 bis A.15 der DIN EN 61508-2 [1]. Dort sind die Eckwerte von 60, 90 und 99 % als maximaler durch die jeweilige Maßnahme zu erreichender *DC* notiert. Bei geeigneter uneingeschränkter Umsetzung der genannten Maßnahmen kann dieser Höchstwert aber in der Regel zur Abschätzung herangezogen werden.

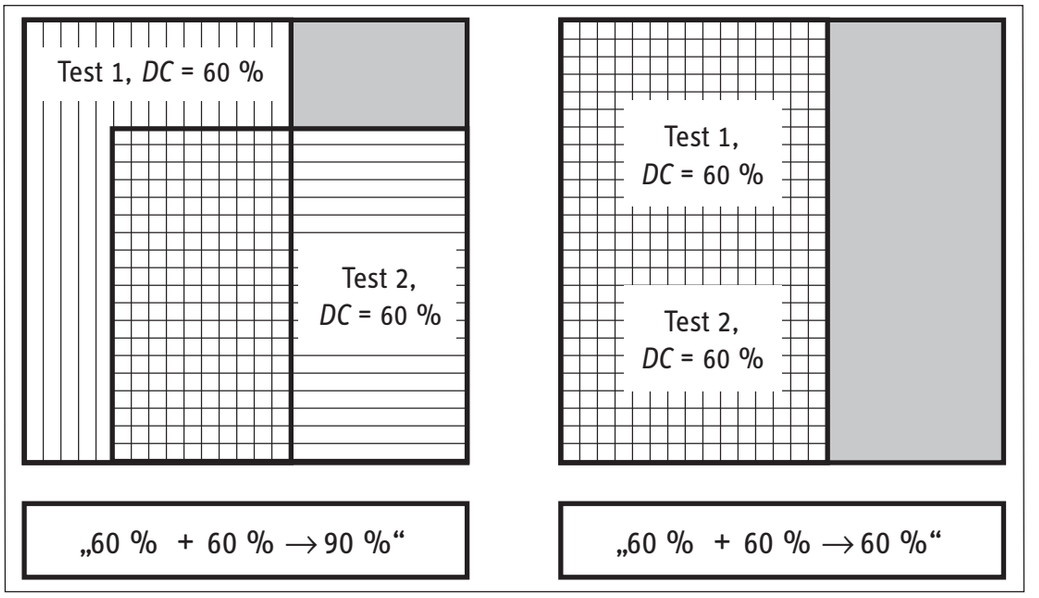


Abbildung E.2: Wirken auf einen Block mehrere Tests, so kann deren Überlappung zu einem höheren Gesamt-DC führen (links) oder auch nicht (rechts); die schraffierten Flächen repräsentieren den Anteil der erkannten gefahrbringenden Ausfälle; die quadratische Gesamtfläche repräsentiert alle gefahrbringenden Ausfälle (100 %)

Nach der Bestimmung des *DC* für einzelne Testmaßnahmen und vor der Berechnung des DC_{avg} muss der DC-Wert pro Block ermittelt werden. Meist wirkt eine einzelne Testmaßnahme auf einen gesamten Block (z.B. Kreuzvergleich): Dann kann der Einzelwert einfach für den Block übernommen werden. Es sind aber weitere Konstellationen möglich:

- Wird ein Block durch mehrere Einzelmaßnahmen überwacht (siehe Abbildung E.2), so ist der Block-DC mindestens so gut wie der beste Einzel-DC. Bei gegenseitiger Ergänzung ist sogar ein höherer Block-DC möglich, dessen Bestimmung erfordert aber dann eine Analyse der durch jeden Test abgedeckten Ausfälle, ähnlich einer FMEA.
- Ein Block besteht aus mehreren Einheiten, von denen jede durch andere Maßnahmen getestet wird, z.B. programmierbare Elektronik mit separaten Tests für Speicher und Verarbeitungseinheit (siehe Abbildung E.3). Dann ist der Block-DC mindestens so gut wie der schlechteste Einzel-DC (ist dieser 0 %, d.h., gibt es Einheiten, die gar nicht getestet werden, so wäre nach dieser groben Abschätzung auch der Block-DC 0 %). Ein besserer und genauerer Wert für den Block-DC lässt sich durch Gewichtung der Einzel-DC mit der zugehörigen Ausfallrate λ_d (=1/$MTTF_d$) erreichen. Die gewichtete Mittelungsformel entspricht dabei Gl. (1) für DC_{avg}. Je nach Genauigkeit gipfelt eine solche Analyse allerdings ebenfalls in einer FMEA.

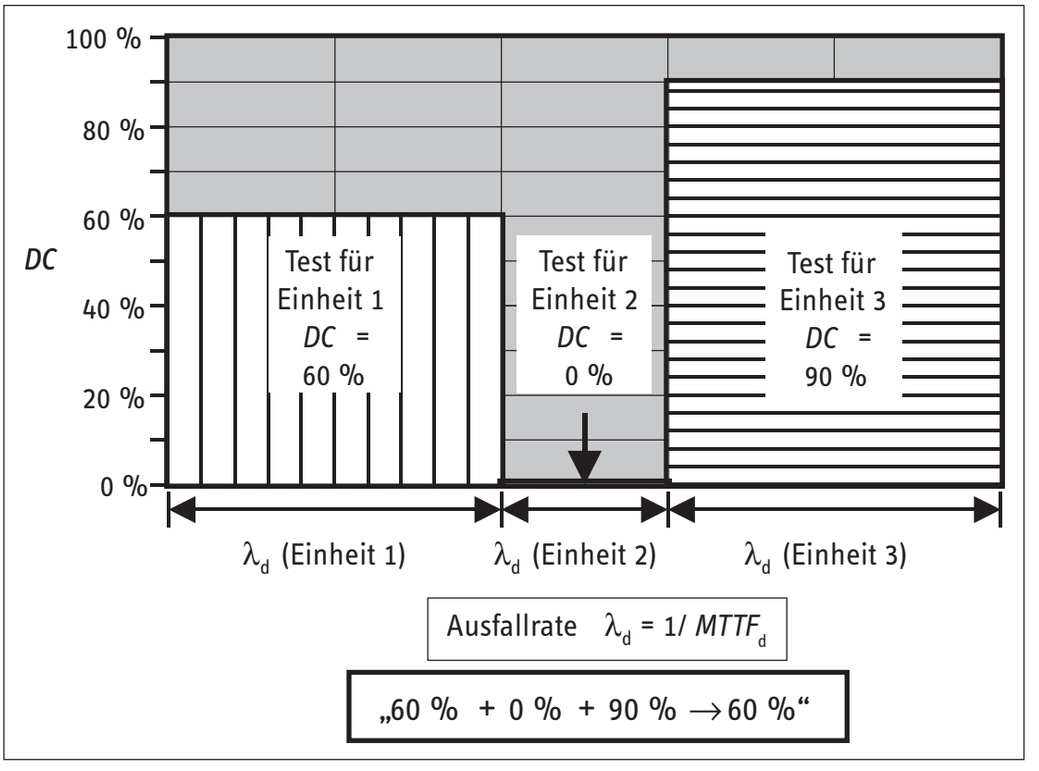


Abbildung E.3: Bei der DC-Mittelung für mehrere Einheiten eines Blocks führt die Gewichtung der Einzel-DC 60 %, 0 % und 90 % mit λ_d auf einen anderen Wert (60 %) als z.B. das ungewichtete arithmetische Mittel (50 %)

Der durchschnittliche *DC* für die gesamte betrachtete Steuerung wird mit DC_{avg} bezeichnet und errechnet sich aus den DC-Werten aller ihrer Blöcke. Im Gegensatz zur $MTTF_d$ pro Kanal wird nicht zwischen den Steuerungskanälen unterschieden, sondern direkt ein Gesamtwert ermittelt. Die Mittelungsformel gewichtet die Einzel-DCs mit der zugehörigen Ausfallrate λ_d (= $1/MTTF_d$) jedes Blocks. Dies gewährleistet, dass Blöcke mit einer hohen Ausfallrate, d.h. geringen $MTTF_d$, stärker berücksichtigt werden als Blöcke, deren gefahrbringender Ausfall vergleichsweise unwahrscheinlich ist. Die Mittelungsformel lautet:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}} \quad (1)$$

Die Summation läuft über alle relevanten Blöcke mit folgender Festlegung:

- Für Blöcke ohne *DC* wird eine *DC* = 0 % eingesetzt. Diese tragen damit nur zum Nenner des Bruchs bei.
- Für Blöcke mit Fehlerausschluss bezüglich der gefahrbringenden Ausfallrichtung (verschwindender Ausfallrate λ_d bzw. unendlich hoher $MTTF_d$) wird der entsprechende Summand im Zähler und im Nenner weggelassen.
- Alle Blöcke, die Sicherheitsfunktionen in den verschiedenen Steuerungskanälen ausführen, werden berücksichtigt. Blöcke, die nur allein der Testung dienen, werden nicht berücksichtigt. Für Kategorie-2-Strukturen bedeutet dies, dass Blöcke des Überwachungskanals („TE“ und „OTE“) nicht mitgezählt werden. In Kategorie 3 und 4 wird der Mittelwert direkt über beide Kanäle hinweg gebildet, eine gesonderte Symmetrisierung wie bei der $MTTF_d$ pro Kanal entfällt.

Für eine detaillierte Analyse des Einflusses der Tests auf die Ausfallwahrscheinlichkeit des Gesamtsystems sind neben dem *DC* weitere Größen zu berücksichtigen. Dazu zählt neben der Testrate z.B. die Ausfallrate der Testeinrichtung selbst. In mehrkanaligen Systemen hat allerdings die Häufigkeit eines Tests nur geringe Auswirkungen, da die dabei relevanten Zeiten in aller Regel sehr viel kleiner sind als die $MTTF_d$-Werte der Kanäle. Bevor also die Beeinträchtigung eines Tests für das System relevant wird, müssen erst mehrere Kanäle ausfallen, was sehr unwahrscheinlich ist, solange die Testzyklen sehr viel kleiner bleiben als die $MTTF_d$ eines Kanals. Grundsätzlich anders sieht dies in Kategorie-2-Strukturen aus. Der Ausfall der Testeinrichtung macht hier aus einem einkanalig getesteten System ein einkanalig ungetestetes System, das beim nächsten Ausfall die Sicherheitsfunktion nicht mehr ausführen kann. Daher gelten für die vereinfachte Beurteilung der Ausfallwahrscheinlichkeit von Kategorie-2-Systemen neben Anforderungen zum *DC* weitere Voraussetzungen:

- Alle Testraten sollten mindestens 100-mal größer sein als die Anforderungsrate der Sicherheitsfunktion. Damit soll gewährleistet werden, dass ein Ausfall von einem Test bemerkt werden kann, bevor eine Anforderung der Sicherheitsfunktion nicht bedient werden kann (siehe auch Anhang G).
- Die $MTTF_d$ der testenden Einheit (TE) sollte mindestens halb so groß sein wie die $MTTF_d$ der zu testenden Einheit (L). Durch diese Annahme wird sichergestellt, dass die Ausfallwahrscheinlichkeit der Testeinrichtung nicht unangemessen hoch ist.

Lässt sich der Funktionskanal nicht auf die Blöcke I, L und O (bzw. der Testkanal auf die Blöcke TE und OTE) abbilden, kann die obige Bedingung so interpretiert werden, dass die $MTTF_d$ des gesamten Testkanals mindestens halb so groß sein soll wie die $MTTF_d$ des Funktionskanals. Ist diese Bedingung verletzt (auch nach Begrenzung der $MTTF_d$ des Funktionskanals auf 100 Jahre), so ist es natürlich zulässig, die Ausfallwahrscheinlichkeit mit einer $MTTF_d$ des Funktionskanals zu berechnen, die rechnerisch auf die doppelte $MTTF_d$ des realisierten Testkanals reduziert wird.

Literatur

[1] DIN EN 61508-2: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (12.02). Beuth, Berlin 2002

Anhang F:
Ausfälle infolge gemeinsamer Ursache (CCF)

Der Begriff des Ausfalls infolge gemeinsamer Ursache CCF (Common Cause Failure) beschreibt die Tatsache, dass in einem redundanten System oder einem einkanaligen System mit externer Testeinrichtung durch eine Ursache mehrere Kanäle außer Kraft gesetzt werden können. Die gewünschte Einfehlersicherheit einer redundanten Struktur wird damit unterlaufen. Deshalb ist es sehr wichtig, diese Fehlerquelle möglichst auszuschalten. Die CCF-Auslöser können physikalischer Natur sein, z.B. Übertemperatur oder starke elektromagnetische Störungen, oder systematischer Art, z.B. fehlerhaftes Schaltungsdesign oder Programmierfehler bei identischer Software in beiden Kanälen.

Ein üblicher Ansatz zur Quantifizierung der „CCF-Anfälligkeit" einer Steuerung ist das sogenannte Beta-Faktor-Modell. Dabei wird davon ausgegangen, dass mit einem bestimmten Anteil der gefährlichen Ausfälle in einem Kanal infolge derselben Ursache auch gefährliche Ausfälle im zweiten Kanal einhergehen. Dieser Sachverhalt ist in Abbildung F.1 dargestellt: Die gefährlichen Ausfallraten beider Kanäle (symbolisch dargestellt als Ellipsenflächen) besitzen eine schraffiert dargestellte CCF-Überlappung. Der Proportionalitätsfaktor zwischen der CCF-Rate und der gefährlichen Ausfallrate des einzelnen Kanals λ_d wird üblicherweise mit β bezeichnet (Common Cause Faktor oder auch Beta-Faktor).

Die exakte Berechnung des Beta-Faktors für eine konkrete Steuerung ist nahezu unmöglich, besonders da dies im Vorfeld vor der eigentlichen Konstruktion geschehen soll. DIN EN 61508-6 [1] bedient sich dazu eines Punkteschemas, um β-Werte zwischen 0,5 und 10 % zu ermitteln. In einer langen Liste aus nach verschiedenen Ursachen sortierten Maßnahmen werden Punkte vergeben, die in der Summe nach Anwendung einiger Regeln zu einem β-Schätzwert führen. DIN EN ISO 13849-1 greift diese Methode auf – sowohl vereinfacht als auch für den Maschinenschutz angepasst. Die Vereinfachung wurde auf der Basis von technischen Maßnahmen vorgenommen, die von Experten als besonders hilfreich zur CCF-Vermeidung angesehen wurden. Es handelt sich allerdings um einen Kompromiss, der nicht wissenschaftlich, aber empirisch begründet werden kann:

- Die Liste der CCF-Gegenmaßnahmen wurde auf die im Maschinenschutz relevanten und hauptsächlich technischen Lösungen konzentriert.
- Statt mehrerer möglicher β-Werte wurde ein einziger Zielwert von höchstens 2 % ausgewählt, der nur entweder erreicht oder verfehlt werden kann. Die vereinfachte Methode zur Bestimmung des Performance Levels nach DIN EN ISO 13849-1 basiert auf der Annahme eines Beta-Faktors von 2 %.

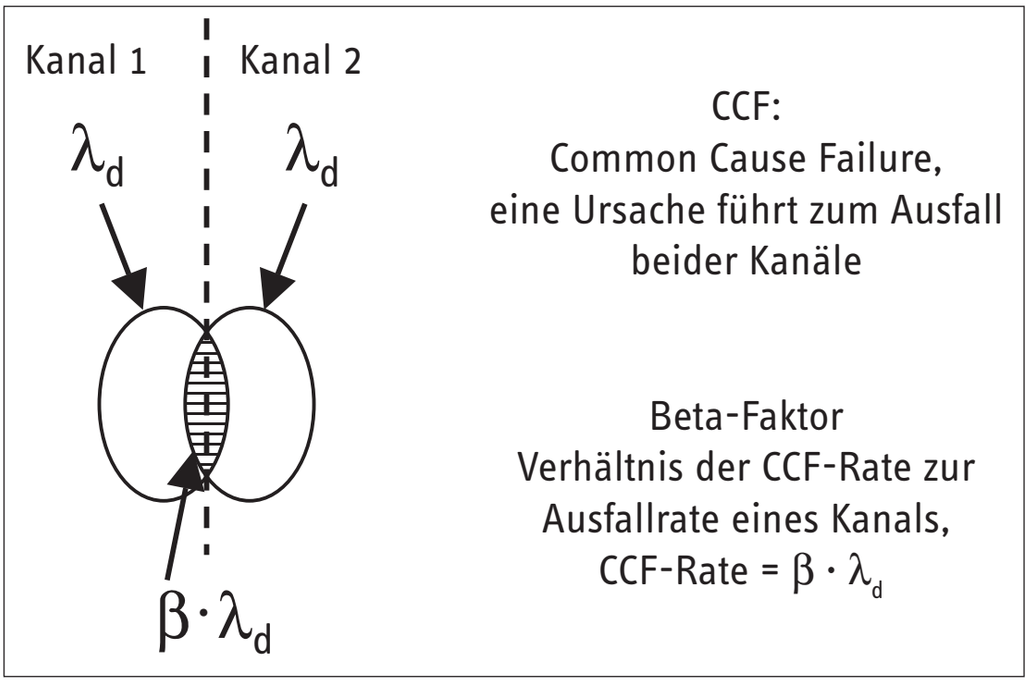


Abbildung F.1: Illustration des Ausfalls infolge gemeinsamer Ursache (CCF) anhand des Beta-Faktor-Modells

- Die Rechenregeln für das Punkteschema wurden auf zwei Schritte zusammengefasst: Jede Maßnahme kann nur voll erfüllt (volle Punktzahl) oder nicht erfüllt sein (Punktzahl Null), anteilige Punktzahlen für unvollständig erfüllte Maßnahmen werden nicht angerechnet. Wenn Maßnahmen (z.B. Diversität, Verwendung bewährter Bauteile) nur in einzelnen SRP/CS als Subsysteme komplett erfüllt werden, können subsystemweise unterschiedliche Maßnahmenbündel gegen CCF wirken. Die Mindestpunktzahl von 65 Punkten muss für die Kategorien 2, 3 und 4 erfüllt werden, um die vereinfachte Methode zur Bestimmung des Performance Levels anwenden zu können. Maximal können 100 Punkte erreicht werden.

Bei der Bewertung der Maßnahmen ist Folgendes zu beachten:

- Die Maßnahmen sind mit besonderem Schwerpunkt auf ihre Wirksamkeit gegen CCF zu bewerten. Beispielsweise fordern die Produktnormen ohnehin Unempfindlichkeit gegenüber Umwelteinflüssen und elektromagnetischen Störungen. Darüber hinaus ist zu beurteilen, ob diese Einwirkungen als Ursachen für gemeinsame Fehler wirksam minimiert wurden.

- Je nach Steuerungstechnologie unterscheiden sich die physikalischen Gegenmaßnahmen, z.B. sind unter Umwelteinflüssen bei elektrischen Steuerungen elektromagnetische Störungen eher relevant, während es bei fluidischen Steuerungen eher Verunreinigungen des Mediums sind. Gegenmaßnahmen sind daher angepasst auf die verwendete Technologie zu bewerten.

- Einen Sonderfall stellt die getestete Struktur von Kategorie-2-Systemen dar. Hier betrifft CCF den gemeinsamen Ausfall des Sicherheits- und des Testkanals. Ein gemeinsamer Ausfall führt dazu, dass der Strukturvorteil durch CCF zunichte gemacht wird. Die Bewertung der Maßnahmen ist dazu sinngemäß auf die Besonderheiten der Kategorie-2-Struktur anzupassen.

- Für eine Maßnahme gegen Ausfälle infolge gemeinsamer Ursache, die aufgrund der inhärenten Eigenschaften der Steuerung nicht auftreten können, darf die volle Punktzahl angerechnet werden.

Die Maßnahmen gegen gemeinsame Ausfälle und die assoziierten Punktzahlen aus DIN EN ISO 13849-1 im Einzelnen sind Folgende:

- Trennung (15 Punkte): Physikalische Trennung zwischen den Signalpfaden, z.B. getrennte Verdrahtung/Verrohrung oder ausreichende Luft- und Kriechstrecken auf gedruckten Schaltungen

- Diversität (20 Punkte): In beiden Steuerungskanälen werden unterschiedliche Technologien/Gestaltung oder physikalische Prinzipien verwendet. Beispiele dafür sind:

  - ein Kanal aus programmierbarer Elektronik aufgebaut, der andere fest verdrahtet

  - Art der Initiierung, z.B. Druck und Temperatur

  - Messung von Entfernung und Druck

  - digital und analog

  - Bauteile von unterschiedlichen Herstellern

- Entwurf/Anwendung/Erfahrung: Schutz gegen Überspannung, Überdruck, Überstrom usw. (15 Punkte) und Verwendung bewährter Bauteile (5 Punkte)

- Beurteilung/Analyse (5 Punkte): Wurden die Ergebnisse einer Ausfalleffektanalyse berücksichtigt, um Ausfälle infolge gemeinsamer Ursache in der Entwicklung zu vermeiden?

- Kompetenz/Ausbildung (5 Punkte): Wurden Konstrukteure/Monteure geschult, um die Gründe und Auswirkungen von Ausfällen infolge gemeinsamer Ursache zu erkennen?

- Umgebungsbedingungen hinsichtlich Schutz vor Verunreinigung und elektromagnetischer Beeinflussung gegen CCF in Übereinstimmung mit den angemessenen Normen (25 Punkte):

  - Fluidische Systeme: Filtrierung des Druckmediums, Verhinderung von Schmutzeintrag, Entwässerung von Druckluft, z.B. in Übereinstimmung mit den Anforderungen des Herstellers für die Reinheit des Druckmediums

  - Elektrische Systeme: Wurde das System hinsichtlich elektromagnetischer Immunität gegen CCF geprüft, z.B. wie in zutreffenden Normen festgelegt?

  Bei kombinierten fluidischen und elektrischen Systemen sollten beide Aspekte berücksichtigt werden.

- Umgebungsbedingungen hinsichtlich anderer Einflüsse (10 Punkte): Wurden alle Anforderungen der Unempfindlichkeit gegenüber allen relevanten Umgebungsbedingungen wie Temperatur, Schock, Vibration, Feuchtigkeit (z.B. wie in den relevanten Normen festgelegt) berücksichtigt?

Literatur

[1] DIN EN 61508-6: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (06.03). Beuth, Berlin 2003

Anhang G:
Was steckt hinter dem Säulendiagramm in Bild 5 der DIN EN ISO 13849-1?

Anders als die Vorgänger-Norm DIN EN 954-1 [1] sieht DIN EN ISO 13849-1 zusätzlich zur Kategorieprüfung den Nachweis eines Performance Levels (PL) vor. Numerisch leitet sich der Performance Level gemäß Tabelle 6.1 dieses Reports aus der durchschnittlichen Wahrscheinlichkeit eines gefährlichen Ausfalls des Systems je Stunde ab, die auch als *PFH* (Probability of a Dangerous Failure per Hour) bezeichnet wird. Diese Größe muss aus der Systemstruktur, den Bauelementausfallraten, dem Diagnosedeckungsgrad der automatischen Tests, der Gebrauchsdauer des Systems und, bei entsprechender Systemstruktur, der Empfindlichkeit des Systems gegenüber Ausfällen infolge gemeinsamer Ursache CCF (Common Cause Failures) ermittelt werden.

Zu diesem Zweck dienen Rechenmodelle, die das Zusammenwirken der genannten Faktoren berücksichtigen und als Ergebnis die *PFH* liefern (Mittelwert während der Gebrauchsdauer). Eigentlich müsste vom Anwender der Norm für jedes zu untersuchende System ein maßgeschneidertes Modell erstellt werden. Für einige gebräuchliche Strukturvarianten, die sogenannten „vorgesehenen Architekturen" aus DIN EN ISO 13849-1, Abschnitt 6.2 (vgl. Abschnitte 6.2.1 bis 6.2.7 dieses Reports), wurden im BGIA Markov-Modelle entwickelt, deren numerische Ergebnisse als sogenanntes „Säulendiagramm" in der Norm in Abschnitt 4.5.4, Bild 5 (Abbildung 6.10 bzw. G.3 dieses Reports), zusammengetragen sind. Dadurch kann auf die Entwicklung eines eigenen Rechenmodells und eine komplexe Berechnung verzichtet werden, falls das System im Wesentlichen die Gestalt einer der vorgesehenen Architekturen hat oder es sich in Teilsysteme von solcher Gestalt zerlegen lässt (vgl. hierzu Abschnitt 6.3 und Anhang H der DIN EN ISO 13849-1 oder Abschnitt 6.4 dieses Reports). Eine grundlegende Einführung in die Technik der Markov-Modellierung findet man z.B. in [2].

Um ein übersichtliches Diagramm zu erhalten, mussten einige Einschränkungen und Vereinfachungen vorgenommen werden. Zum einen begrenzt die Norm die Anzahl der vorgesehenen Architekturen und damit die Anzahl der notwendigen Modelle. Zum anderen wurde die Vielzahl der Eingangsparameter durch sinnvolle Bündelung verringert. Hierzu wurden die Größen $MTTF_d$ und DC_{avg} eingeführt, die jeweils mehrere Eingangsparameter zusammenfassen.

Die im Diagramm verwendete $MTTF_d$ hat die Bedeutung einer mittleren Zeit bis zum Ausfall jedes Kanals in dessen gefahrbringende Ausfallrichtung (Mean Time to Dangerous Failure). Die $MTTF_d$-Werte mehrerer Funktionsblöcke werden dabei zu einer einzigen Kanal-$MTTF_d$ zusammengefasst (Kapitel 6 und Anhang D). Allen $MTTF_d$-Werten liegt die Annahme konstanter Bauelement-Ausfallraten λ_d zugrunde, wodurch die Beziehung $MTTF_d = 1/\lambda_d$ gilt. Bei Zweikanaligkeit mit unterschiedlicher Kanal-$MTTF_d$ wird mit einer gemittelten Ersatz-$MTTF_d$ gearbeitet. Hingegen gibt der Wert DC_{avg} den gewichteten Mittelwert des Diagnosedeckungsgrades für das gesamte System an, der für die Zuordnung zu einer der vier DC_{avg}-Stufen (vgl. Tabelle 6.4) benutzt wird.

Die Sinnhaftigkeit und Zulässigkeit dieser Zusammenfassungen innerhalb der geforderten Quantifizierungsgenauigkeit wurden durch umfangreiche Testrechnungen nachgewiesen. Das gilt auch für das in Abschnitt 4.5.4 der Norm zugelassene Verhältnis der $MTTF_d$-Werte von Test- und Funktionskanal bei der Kategorie-2-Architektur: Die $MTTF_d$ der Testeinrichtung muss mindestens den halben Wert der $MTTF_d$ für die getestete Logik aufweisen. Bei redundanzbehafteten Strukturen wurde schließlich vorausgesetzt, dass Ausfälle gemeinsamer Ursache auf ein angemessenes Niveau reduziert sind: Nur maximal 2 % der gefährlichen Ausfälle dürfen eine gemeinsame Ursache haben. Dies ist vom Anwender der Norm mit einem einfachen Schätzverfahren (Anhang F) jeweils zu belegen.

Die Markov-Modelle, die dem Säulendiagramm aus DIN EN ISO 13849-1 (bzw. Abbildung G.3 dieses Reports) zugrunde liegen, berücksichtigen den Betrieb der Systeme unter Randbedingungen, die für den Maschinenbereich realistisch sind. Sie gehen davon aus, dass die Systeme

- mindestens einer Anforderung der Sicherheitsfunktion pro Jahr ausgesetzt sind,
- sich bei selbsttätiger Erkennung eines internen Fehlers in den sicheren Zustand „Betriebshemmung" versetzen und dann i.d.R. kurz darauf (spätestens nach einigen Stunden) manuell abgeschaltet werden,
- nach Eintritt der Betriebshemmung oder nach einem Unfall bzw. erkanntem gefährlichen Versagen repariert oder ersetzt und wieder in Betrieb genommen werden.

Unter diesen Randbedingungen stellt die quantitative Zielgröße der Modellierung, die *PFH*, die durchschnittliche Anzahl der ausfallbedingt nicht bedienten Anforderungen der Sicherheitsfunktion pro Stunde dar. Bei ständig vorliegender Anforderung (Continuous Mode of Operation) gibt sie die Anzahl der gefährlichen Systemausfälle pro Stunde an (Ausnahme: Kategorie 2, deren *PFH* nur für zeitdiskrete Anforderungen berechnet wurde). Da die so ermittelte *PFH* allein Zufallsausfälle berücksichtigt, nicht jedoch systematische Ausfälle und andere negative Effekte, ist sie als theoretische Leistungskenngröße anzusehen, welche die sicherheitstechnische Güte eines Designs bewertet, aber keine Aussagen etwa zur Unfallhäufigkeit gestattet. Diese *PFH* ist die mathematische Größe, die auf der vertikalen Achse des Säulendiagramms aufgetragen ist (vgl. Abbildung G.3 dieses Anhangs).

Trotz der prinzipiellen Berücksichtigung von Anforderungen der Sicherheitsfunktion und der Reparatur wirken sich die absoluten Größen von Anforderungsrate und Reparaturrate (Kehrwert der mittleren Reparaturzeit) nur in vernachlässigbar kleinem Maß auf die so verstandene *PFH* aus. Lediglich bei der für Kategorie 2 vorgesehenen Architektur muss gefordert werden, dass die Testung sehr viel häufiger erfolgt als die Anforderung der Sicherheitsfunktion (vgl. DIN EN ISO 13849-1, Abschnitt 4.5.4; Ausnahme: Testintervall und die Zeit für die sicherheitsgerichtete Reaktion sind zusammen kürzer als die spezifizierte Systemreaktionszeit). Die Norm schlägt dazu eine mindestens 100-mal größere Testrate im Vergleich zur Anforderungsrate vor. Aber selbst bis hinunter zu einem Verhältnis von 25 : 1 erhöht sich die *PFH* lediglich um ca. 10 %. Aus ähnlichem Grund gelten die per Diagramm ermittelten PFH-Werte – mit der Einschränkung bei der Kategorie-2-Architektur – für beliebige Anforderungsraten und beliebige (mittlere) Reparaturzeiten. (Bei weniger als einer Anforderung pro Jahr liefert das Säulendiagramm eine Abschätzung zur sicheren Seite.)

Die Säulen für Kategorie B und 1 in Abbildung G.3 wurden mithilfe eines Modells berechnet, das die Anforderung der Sicherheitsfunktion und die Reparatur berücksichtigt. Die PFH-Werte bei diesen Kategorien lassen sich aber auch sehr gut durch die einfache Beziehung $PFH \approx \lambda_d = 1/MTTF_d$ annähern. Dies bedeutet nichts anderes, als dass die *PFH* des einkanaligen ungetesteten Systems (*DC* = 0) praktisch dessen Ausfallrate in die gefährliche Richtung entspricht.

Für die anderen Kategorien ist jedoch eine aufwendigere Rechenmethode erforderlich. Die prinzipielle Modellierungsweise wird im Folgenden beispielhaft an der „vorgesehenen Architektur“ für Kategorie 2 erläutert. Diese Struktur ist in Abbildung G.1 nochmals dargestellt. Es gibt fünf Funktionsblöcke, von denen die Blöcke I (Input), L (Logic) und O (Output) die eigentliche Sicherheitsfunktion in logischer Reihenschaltung ausführen. Der Block L testet die Blöcke I, O und sich selbst im Zusammenspiel mit dem Funktionsblock TE (Test Equipment). Der Funktionsblock OTE (Output of TE) kann bei Ausfall des Hauptkanals I-L-O einen sicheren Zustand herbeiführen. Die nicht direkt funktionsnotwendigen zusätzlichen Funktionsblöcke TE und OTE stellen somit eine Art Ersatzkanal für den Fehlerfall zur Verfügung, der jedoch – anders als ein „echter“ zweiter Kanal – nur bei erkannten Ausfällen im Hauptkanal wirken kann.

Aus dem sicherheitsbezogenen Blockdiagramm in Abbildung G.1 kann der Zustandsgraph in Abbildung G.2 abgeleitet werden. Dazu werden zunächst alle $2^5 = 32$ Ausfallkombinationen der fünf Funktionsblöcke gebildet. Der Zustand ohne Ausfall ist der oben abgebildete OK-Zustand. Darunter folgt eine Reihe von Zuständen mit nur einem ausgefallenen Funktionsblock, dann eine Reihe mit zwei ausgefallenen Blöcken usw. Die Zustandsbezeichnung benennt jeweils die ausgefallenen Funktionsblöcke mit einem nachgestellten „D“ für „Dangerous“, das den Ausfall des Blocks in dessen „gefährliche“ (= sicherheitstechnisch ungünstige) Ausfallrichtung symbolisiert. Durch Ausfälle von Funktionsblöcken, abgebildet durch Pfeile, werden Folgezustände erreicht. Zustände, in denen das System die Sicherheitsfunktion nicht mehr ausführen kann, sind grau dargestellt. Wo immer eine Erkennung des Ausfalls möglich ist und als Folge sicherheitsgerichtet reagiert werden kann, gibt es einen Übergang in den links dargestellten Zustand „Betriebshemmung“. Von den 32 Ausfallkombinationen sind zur Modellvereinfachung diejenigen zusammengefasst, in denen das System in gefährlicher Richtung und (für sich selbst) unerkennbar ausgefallen ist. Dieser Sammelzustand mit der Bezeichnung „System DU“ (Dangerous Undetectable) ist rechts dargestellt. Er kann aus verschiedenen Zuständen durch den Ausfall von Funktionsblöcken erreicht werden. In Abbildung G.2 ist unten der Zustand „Gefährliche Situation/Schaden“ zu sehen. In ihn gelangt das System nur aus gefährlichen (grau dargestellten) Vorzuständen und zwar immer dann, wenn die Sicherheitsfunktion angefordert wird. Wie der Zustand „Betriebshemmung“ so wird auch dieser Zustand durch Reparatur in Richtung OK-Zustand verlassen. Zusätzliche Übergangspfeile, z.B. von „OK“ nach „System DU“, ergeben sich durch gleichzeitige Ausfälle mehrerer Funktionsblöcke infolge einer gemeinsamen Ursache (Common Cause Failures, CCF). Es wird angenommen, dass bei 2 % der Ausfälle eines der Funktionsblöcke L und TE in gefährliche Richtung aufgrund derselben Ursache auch der jeweils andere Block gefährlich ausfällt. Dasselbe wird auch von den Funktionsblöcken O und OTE angenommen.

Allen Pfeilen sind Übergangsraten zugeordnet, deren Größe sich aus den jeweiligen Übergangsprozessen (Ausfällen, Tests, Anforderungen, Reparaturen) ergibt. Auch bewirkt die Berücksichtigung von Common Cause Failures (CCF) an verschiedenen Stellen eine Änderung der ursprünglichen Übergangsrate. Bei der Berechnung des Säulendiagramms wird der ungünstige Fall angenommen, dass die im System eingesetzte Testeinrichtung selbst nicht getestet wird. Darum wird einigen Übergängen in Abbildung G.2 die Rate Null zugewiesen. Systeme, die ihre Testeinrichtung testen, sind dadurch zur sicheren Seite abgeschätzt. Zur vereinfachten Berechnung nach der Markov-Methode wird angenommen, dass alle Übergangsprozesse durch exponentialverteilte Zustandsverweildauern gekennzeichnet sind, obwohl dies streng genommen nur für die Zufallsausfälle mit konstanter Rate gilt. Separate Betrachtungen rechtfertigen diese Vereinfachung.

Man geht davon aus, dass sich das System zu Beginn der Gebrauchszeit mit der Wahrscheinlichkeit 1 im OK-Zustand befindet und die Wahrscheinlichkeit aller anderen möglichen Systemzustände 0 beträgt. Während der angenommenen Gebrauchsdauer von 20 Jahren ändern sich alle Zustandswahrscheinlichkeiten allmählich: Ausgehend vom OK-Zustand verteilen sie sich entlang den Übergangspfeilen um. Die Summe der Zustandswahrscheinlichkeiten bleibt konstant Eins. Dabei ergibt sich auch ein zeitabhängiger Zufluss in den Zustand „Gefährliche Situation/Schaden“, dessen zeitlicher Mittelwert während der 20-jährigen Gebrauchsdauer die *PFH* darstellt, d.h. die durchschnittliche Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Systems je Stunde.

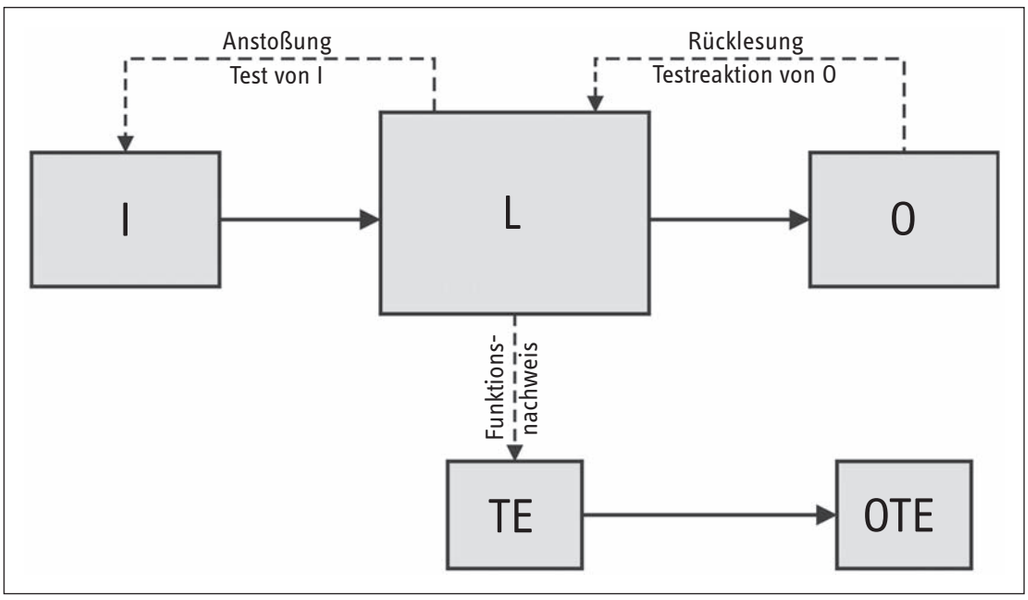
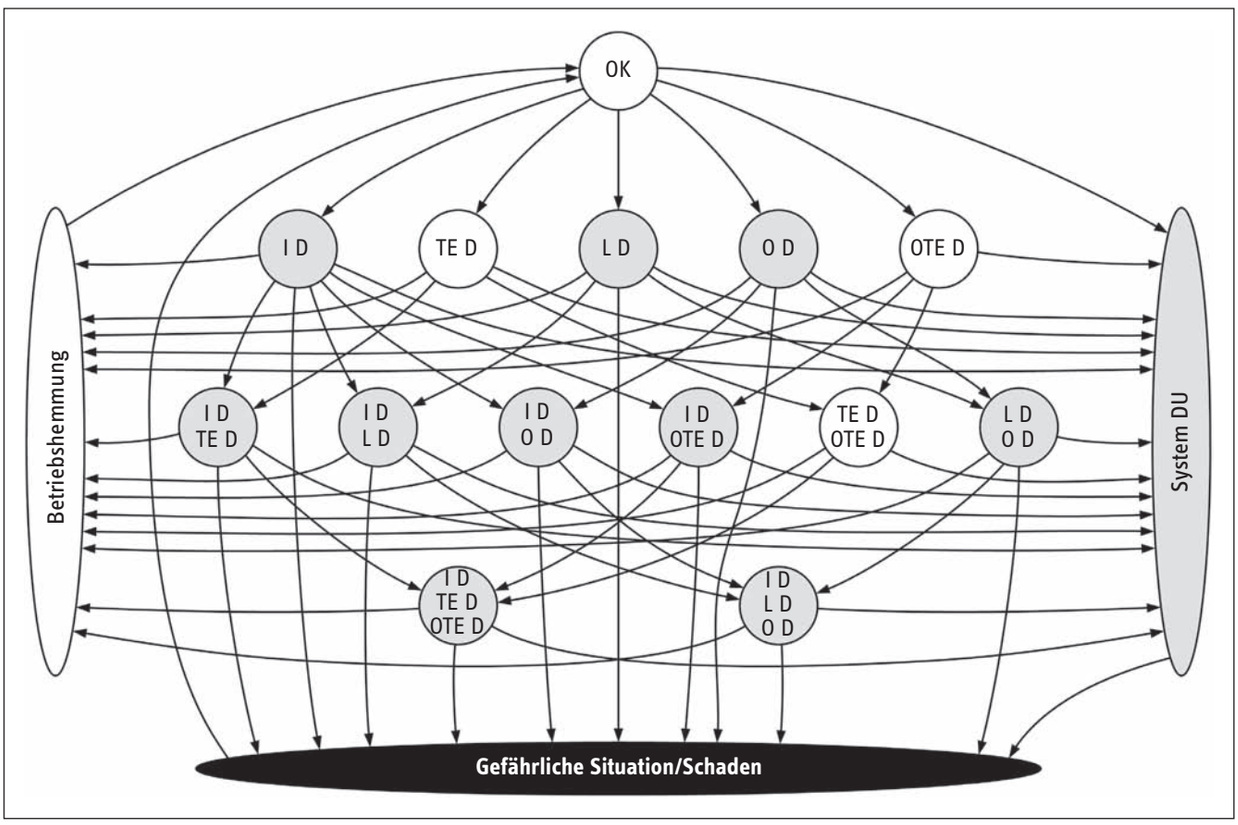


Abbildung G.1:
Vorgesehene Architektur für Kategorie 2 nach DIN EN ISO 13849-1, Abschnitt 6.2.5

Abbildung G.2:
Zustandsgraph des Markov-Modells zur vorgesehenen Architektur für Kategorie 2 für die Ermittlung der PFH



Diese *PFH* ist auf der vertikalen Achse des Säulendiagramms für die verschiedenen „vorgesehenen Architekturen“ nach Abschnitt 6.2 der Norm (vgl. Abschnitte 6.2.3 bis 6.2.7 dieses Reports) aufgetragen, wobei die Kategorien 2 und 3 noch nach dem durchschnittlichen Diagnosedeckungsgrad (DC_{avg}) unterteilt wurden. Die Säulen entstehen, indem für eine Kombination aus Architektur (bzw. dem zugeordneten Markov-Modell) und DC_{avg} die $MTTF_d$, d.h. die mittlere Zeit bis zum Ausfall des (bzw. eines) Funktionskanals in dessen gefährliche Richtung, variiert wird. So könnten beispielsweise mit dem Markov-Modell in Abbildung G.2 die beiden Säulen für die vorgesehene Kategorie-2-Architektur berechnet werden. (Tatsächlich wurde aus rechentechnischen Gründen ein hiervon abweichendes äquivalentes Ersatzmodell benutzt, das hier nicht dargestellt wird, weil sein Zusammenhang mit dem Blockbild von Abbildung G.1 weniger leicht einsichtig ist. Das Ersatzmodell liefert praktisch identische Ergebnisse.) Die übrigen Säulen basieren auf weiteren Markov-Modellen, die für die entsprechenden vorgesehenen Architekturen ebenfalls nach den oben beschriebenen Prinzipien entwickelt wurden.

Gemäß Tabelle 6.1 wurden den PFH-Intervallen auf der logarithmisch geteilten PFH-Skala die Performance Levels a bis e zugewiesen. Dies ist in Abbildung G.3 gezeigt, in der Bild 5 der Norm DIN EN ISO 13849-1 um eine zusätzliche PFH-Skala ergänzt wurde.

Eine Besonderheit gibt es beim PFH-Intervall von 10^{-6}/h bis 10^{-5}/h. Es ist auf die beiden benachbarten Performance Levels b und c abgebildet. Durch die mittige Teilung der logarithmischen Skala liegt die Grenze zwischen Performance Level b und Performance Level c beim geometrischen Mittelwert von 10^{-6}/h und 10^{-5}/h, d.h. bei $\sqrt{10 \cdot 10^{-6}}\text{/h} \approx 3 \cdot 10^{-6}$/h. Die Zuordnung von PFH-Intervallen und Performance Level deckt sich im Wesentlichen mit Tabelle 6.1 und DIN EN 61508-5, Abbildung D.2, siehe [3; 4].

In Anhang K der Norm ist der Inhalt von Abbildung G.3 in Form von Tabelle K.1 numerisch wiedergegeben. Mithilfe von Tabelle K.1 kann der Performance Level präziser ermittelt werden als mit der Abbildung, was insbesondere dann nützlich ist, wenn PFH-Beiträge von mehreren kaskadierten Teilsystemen aufsummiert werden müssen. Hingegen bietet das Säulendiagramm vor allem eine schnelle Übersicht über die PL-Tauglichkeit verschiedener technischer Lösungswege und kann somit bei deren Vorauswahl helfen. Die Informationen aus Tabelle K.1 der Norm sind auch in einem sogenannten „Performance Level Calculator“ (PLC) enthalten, einer handlichen Drehscheibe aus Karton zur PL-Bestimmung, die u.a. beim BGIA erhältlich ist [5].

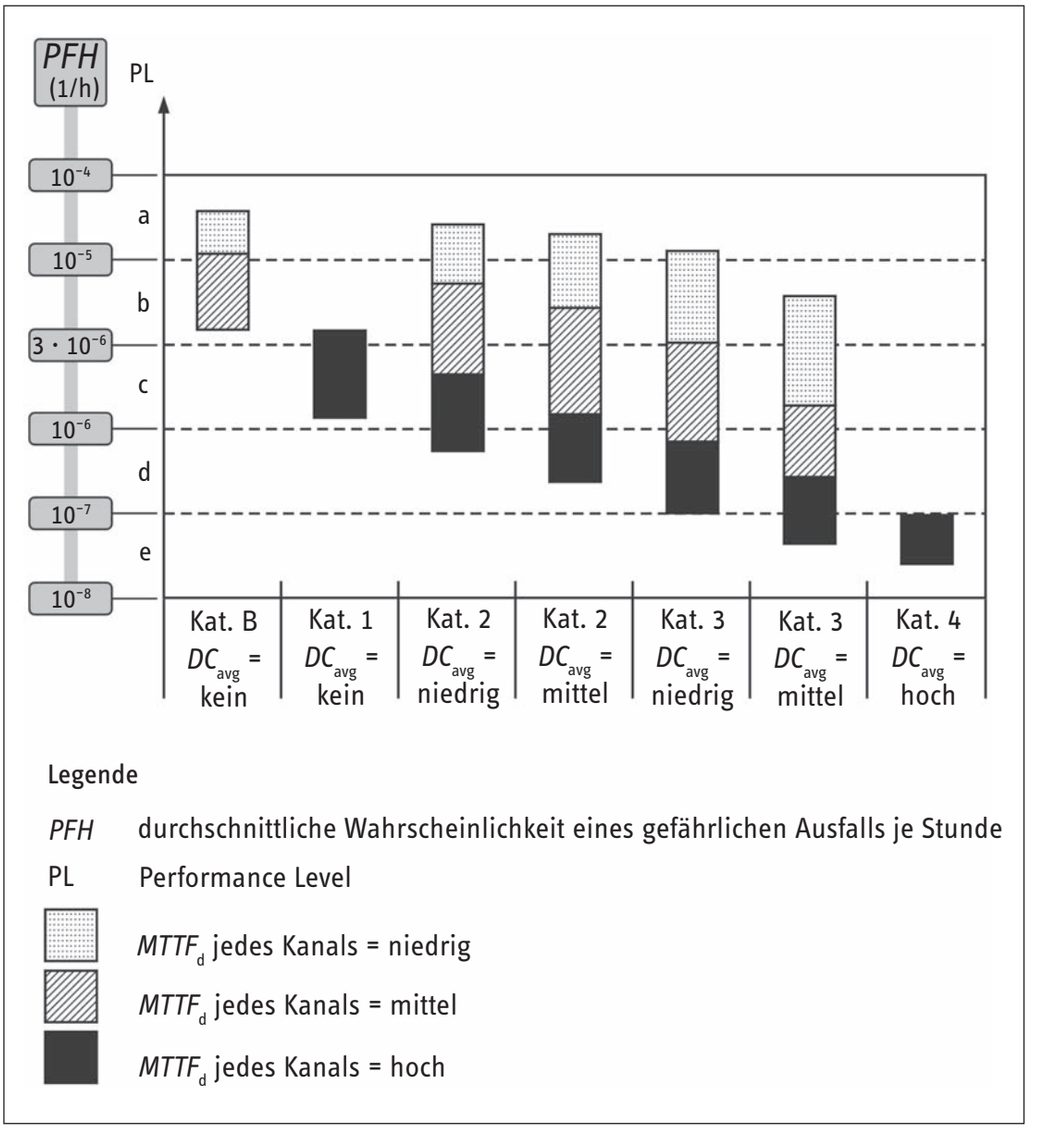


Abbildung G.3: PFH und Performance Level in Abhängigkeit von Kategorie, DC und $MTTF_d$

Mitunter kommt es vor, dass der für ein System ermittelte DC_{avg}-Wert nur geringfügig unterhalb einer der Schwellen „niedrig“ (60 %), „mittel“ (90 %) oder „hoch“ (99 %) liegt. Wird dann das vereinfachte Quantifizierungsverfahren aus DIN EN ISO 13849-1 angewendet, muss rein formal jeweils mit der nächst kleineren DC_{avg}-Stufe, also mit „kein“, „niedrig“ bzw. „mittel“ weitergearbeitet werden. Diese Vorgehensweise schätzt das System zur sicheren Seite ab. Wegen der wenigen Stufen der DC_{avg}-Skala kann jedoch manchmal eine nur kleine Systemänderung, die den Wert DC_{avg} eine der Schwellen gerade unterschreiten lässt, zu einer deutlich schlechteren Bewertung des Systems führen. Dies kann sogar passieren, wenn in einem Kanal hochwertig getestete Bauelemente (hoher *DC*) durch bessere Bauelemente (mit höherer $MTTF_d$) ersetzt werden (vgl. DC_{avg}-Formel z.B. in Abschnitt 6.2.14). Die kleine Verbesserung der Kanal-$MTTF_d$ wird dann durch die formal vollzogene Herabstufung von DC_{avg} auf den nächst kleineren Wert überkompensiert, wodurch die ermittelte *PFH* schlechter (größer) wird. Dieser paradox erscheinende Effekt ist eine Folge der Grobstufigkeit der DC_{avg}-Skala, also letztlich eine Konsequenz der Einfachheit von Bild 5 (bzw. Tabelle K.1) der Norm, vgl. Abbildung G.3 dieses Reports.

Der beschriebene Effekt kann verhindert oder gemildert werden, indem anstelle von Abbildung G.3 eine Grafik mit feinerer Abstufung der DC_{avg}-Werte benutzt wird (Abbildung G.4). Mit Rücksicht auf die begrenzte Genauigkeit von DC_{avg}-Werten (vgl. DIN EN ISO 13849-1, Tabelle 6, Anmerkung 2) wurden für alle Kategorien auch die minimal möglichen DC_{avg}-Werte berücksichtigt. Zur PFH-Bestimmung bietet sich der BGIA-Softwareassistent „SISTEMA“ an (siehe Anhang H). Er interpoliert sogar zwischen den in Abbildung G.4 gezeigten Säulen. Generell kann dadurch eine starke Herabstufung von DC_{avg} vermieden und oft ein genauerer und zugleich besserer PFH-Wert ermittelt werden.

Literatur

[1] DIN EN 954-1: Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (03.1997). Beuth, Berlin 1997

[2] *Goble, W.M.:* Control systems safety evaluation and reliability. 2nd ed. Hrsg.: Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina 1998

[3] DIN EN 61508-1: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 und Corrigendum 1999) (11.02). Beuth, Berlin 2002

[4] DIN EN 61508-5: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:1998 und Corrigendum 1999) (11.02). Beuth, Berlin 2002

[5] *Schaefer, M.; Hauke, M.:* Performance Level Calculator – PLC. 3. Aufl. Hrsg.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin; Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) e.V. – Fachverband Automation, Frankfurt am Main, und Verband Deutscher Maschinen- und Anlagenbau e.V. – VDMA, Frankfurt am Main im März 2008
www.dguv.de/bgia, Webcode d3508

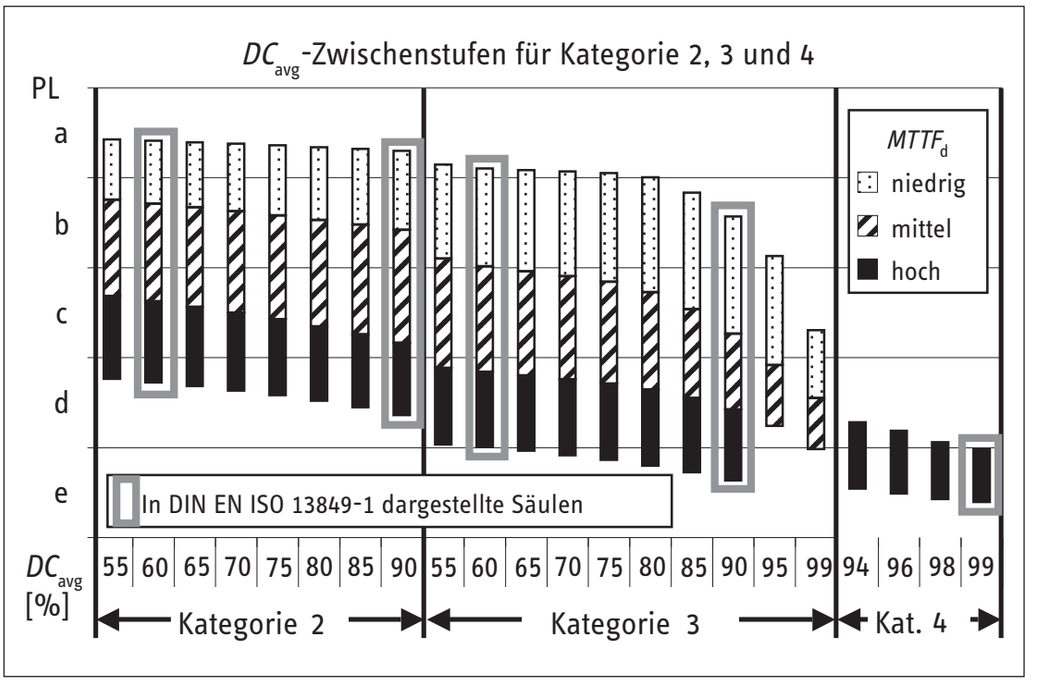


Abbildung G.4: Performance Level bei feinstufigerer Auflösung der DC_{avg}-Skala (Erweiterung von Bild 5 aus DIN EN ISO 13849-1)

Anhang H:
SISTEMA – Der Softwareassistent zur Bewertung von SRP/CS

H1 Was kann SISTEMA?

Mit dem Software-Assistenten SISTEMA (**Si**cherheit von **Ste**uerungen an **Ma**schinen) steht Entwicklern und Prüfern von sicherheitsbezogenen Maschinensteuerungen eine umfassende Hilfestellung bei der Bewertung der Sicherheit im Rahmen der DIN EN ISO 13849-1 zur Verfügung. Das Windows-Tool bietet dem Nutzer die Möglichkeit, die Struktur der sicherheitsbezogenen Steuerungsteile auf der Basis der sogenannten vorgesehenen Architekturen nachzubilden und erlaubt schließlich eine automatisierte Berechnung der Zuverlässigkeitswerte auf verschiedenen Detailebenen einschließlich des erreichten Performance Levels (PL).

Über Eingabemasken werden relevante Parameter wie Risikoparameter zur Bestimmung des erforderlichen Performance Levels (PL_r), Kategorie des SRP/CS, Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) bei mehrkanaligen Systemen, mittlere Bauteilgüte ($MTTF_d$) und die mittlere Testqualität (DC_{avg}) von Bauelementen bzw. Blöcken Schritt für Schritt erfasst. Nachdem die geforderten Daten in SISTEMA eingetragen wurden, sind die berechneten Ergebnisse sogleich sichtbar. Praktisch für den Benutzer: Jede Parameteränderung wird in ihrer Auswirkung auf das Gesamtsystem über die Programmoberfläche direkt angezeigt. Das umständliche Nachschlagen in Tabellen und Ausrechnen von Formeln (Bestimmung der $MTTF_d$ nach dem „Parts Count"-Verfahren, Symmetrisierung der $MTTF_d$ für jeden Kanal, Abschätzung des DC_{avg}, Ermittlung von *PFH* und PL etc.) wird durch die Software übernommen und entfällt daher weitestgehend. Dies ermöglicht es dem Benutzer, Parameterwerte zu variieren, um so die Auswirkungen von Änderungen zu beurteilen, ohne dabei großen Aufwand zu treiben. Die Resultate können schließlich in einem Übersichtsdokument ausgedruckt werden.

H2 Wie wird SISTEMA verwendet?

SISTEMA verarbeitet sogenannte Grundelemente aus insgesamt sechs Hierarchiestufen: das Projekt (PR), die Sicherheitsfunktion (SF), das Subsystem (SB), der Kanal (CH)/Testkanal (TE), der Block (BL) und das Element (EL). Deren Zusammenhang ist im Folgenden kurz dargestellt (Abbildung H.1).

Der Benutzer eröffnet zunächst ein Projekt und kann darin die Maschine bzw. die Gefahrenstelle, die weiter betrachtet werden soll, definieren. Dem Projekt werden schließlich alle erforderlichen Sicherheitsfunktionen zugewiesen. Diese können durch den Benutzer festgelegt und dokumentiert sowie mit einem PL_r belegt werden. Der tatsächlich erreichte PL des parametrierten SRP/CS wird automatisch aus den Subsystemen ermittelt, die – in Serie geschaltet – die Sicherheitsfunktion ausführen. Den Subsystemen liegt jeweils – in Abhängigkeit von der gewählten Kategorie – eine sogenannte vorgesehene Architektur aus der Norm zugrunde. Aus der Architektur bestimmt sich unter anderem, ob die Steuerung einkanalig, einkanalig getestet oder redundant ausgelegt ist und ob bei der Auswertung ein spezieller Testkanal zu berücksichtigen ist. Jeder Kanal kann sich wiederum in beliebig viele Blöcke unterteilen, für die der Benutzer entweder direkt einen $MTTF_d$-Wert und einen DC-Wert einträgt, oder aber auf der niedrigsten Hierarchieebene die Werte für die einzelnen Elemente einträgt, aus denen sich der Block zusammensetzt.

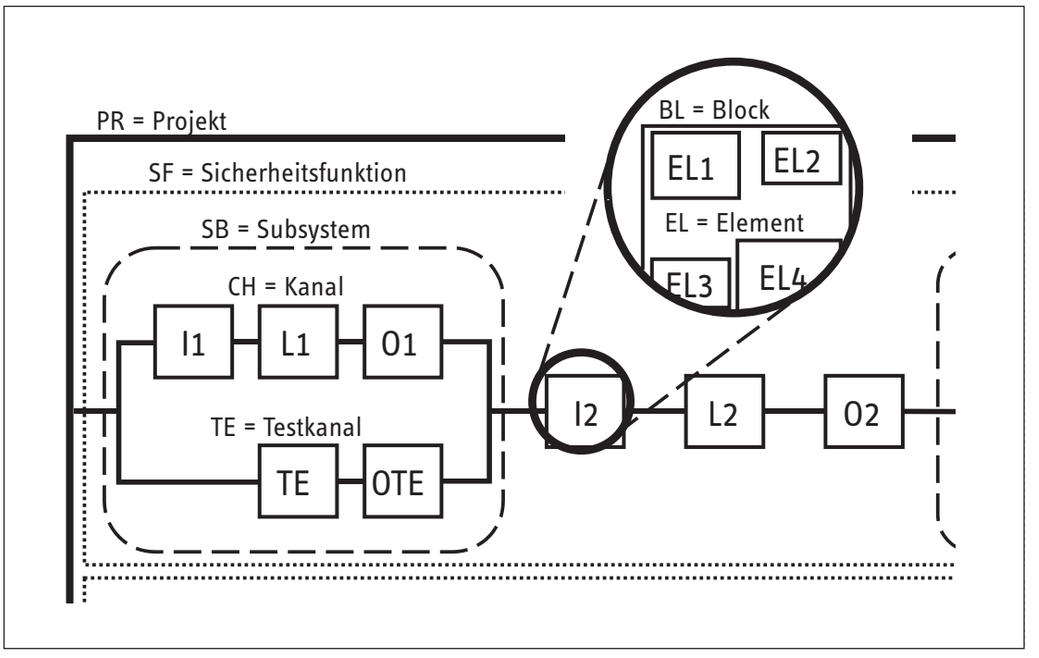


Abbildung H.1: In SISTEMA betrachtete Hierarchieebenen

Komfortable Bibliotheksfunktionen runden den Leistungsumfang von SISTEMA ab. Die mitgelieferten Bibliotheken enthalten einige Standardelemente; Blöcke und komplette Subsysteme lassen sich jedoch durch den Benutzer beliebig erweitern. Optional können weitere Bibliotheksmodule nachinstalliert werden, falls diese von Herstellern für ihre Komponenten verfügbar sind.

H3 Die Benutzerschnittstelle von SISTEMA

Die Programmoberfläche von SISTEMA gliedert sich in vier Bereiche (siehe Abbildung H.2). Den größten Anteil der Fläche nimmt der Arbeitsbereich in der Mitte ein. Er enthält je nach aktiver Sicht eine editierbare Eingabemaske oder einen Abschnitt aus dem Übersichtsdokument. Der Inhalt der jeweiligen Sicht ist durch das ausgewählte Grundelement aus der weiter oben genannten Hierarchie bestimmt und wird über die Selektion in einer Baumansicht auf der linken Seite festgelegt. Jede Verzweigung in der Baumansicht steht für ein Grundelement. Über den Baum lassen sich auch Grundelemente auf den verschiedenen Ebenen neu erzeugen, entfernen, verschieben oder kopieren. Die Details des angewählten Grundelements werden in der Editieransicht über die Eingabemaske eingetragen. Jede Eingabemaske ist selbst über Register in verschiedene Bereiche untergliedert. Die jeweils letzte Registerkarte enthält eine Tabelle, die alle untergeordneten Verzweigungen zusammenfasst und die wichtigsten Informationen auflistet. Hat der Benutzer beispielsweise einen Block in der Baumansicht markiert, so zeigt diese Tabelle alle darin enthaltenen Elemente mit ihren $MTTF_d$- und DC-Werten an.

Ferner enthält die Baumansicht zu jedem Grundelement eine Statusinformation durch eine farbliche Markierung in Form eines Punktes neben der Verzweigung. Rot zeigt an, dass eine Bedingung der Norm nicht erfüllt ist, ein Grenzwert überschritten ist oder eine allgemeine Inkonsistenz vorliegt, durch die ein erforderlicher Wert nicht berechnet werden kann. In diesem Fall wird eine Warnung ausgegeben. Gelb bedeutet, dass ein unkritischer Hinweis vorliegt (z.B. wenn ein Grundelement noch unbenannt ist). Alle anderen Grundelemente werden grün gekennzeichnet. Eine farbige Kennzeichnung vererbt sich immer auch auf die übergeordneten Verzweigungen, wobei rot die höchste und grün die niedrigste Priorität hat. Alle Warnungen und Hinweise zu dem aktiven Grundelement werden im Meldungsfenster unterhalb des Arbeitsbereiches aufgeführt.

Der Bereich unterhalb der Baumansicht zeigt die wichtigsten Kontextinformationen des ausgewählten Grundelementes an. Diese bestehen aus PL, *PFH*, $MTTF_d$, DC_{avg} und CCF des übergeordneten Subsystems sowie PL_r, PL und *PFH* der übergeordneten Sicherheitsfunktion (das gilt natürlich nur für Grundelemente, die in tieferen Hierarchieebenen liegen). So sieht der Benutzer laufend, wie sich seine Änderungen in den angezeigten Parametern bemerkbar machen.

Neben ihrer Flexibilität zeichnet sich die Programmoberfläche von SISTEMA durch eine komfortable und intuitive Bedienbarkeit aus. Kontextspezifische Hilfetexte auf der rechten Seite sollen den Einstieg erleichtern. Zusätzliche Unterstützung bietet der mit der Anwendung ausgelieferte Wizard – ein Assistent, der den Einsteiger Schritt für Schritt bei der virtuellen Nachbildung seiner Steuerung begleitet und ihm einen schnellen Zugang gewährleistet.

H4 Wo ist SISTEMA zu erhalten?

Die Software SISTEMA wird auf den Internetseiten des BGIA zum Download bereitgestellt. Zunächst wird SISTEMA nur in deutscher Sprache erhältlich sein, Versionen für weitere Sprachen werden folgen. Das Tool wird im Übrigen nach Registrierung als Freeware zur kostenlosen Benutzung angeboten. Aktuelle Informationen sowie den Link zum Download erhalten Sie unter der Internetadresse www.dguv.de/bgia über den Webcode 2447262.

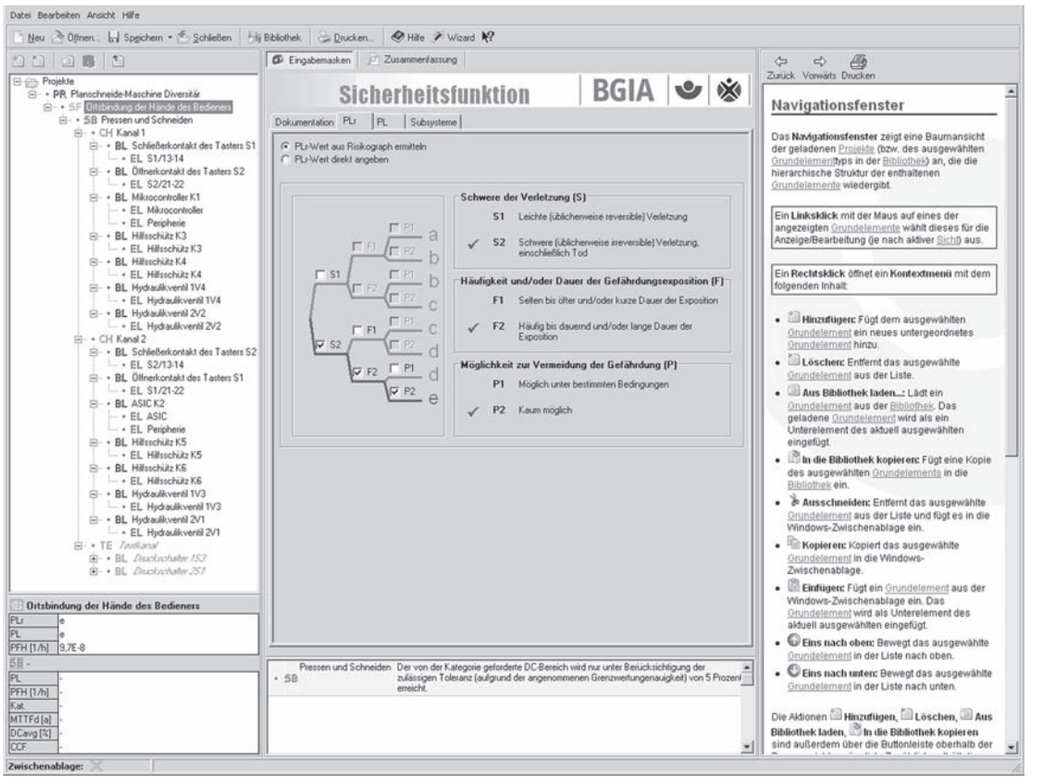


Abbildung H.2: Programmoberfläche von SISTEMA

Anhang I:
Positionspapier des VDMA

VDMA-Positionspapier

Funktionale Sicherheit: Sicherheitsbezogene Teile von Steuerungen nach EN ISO 13849-1

1. Einleitung

Der VDMA (Verband Deutscher Maschinen- und Anlagenbau) ist der größte europäische Verband der Investitionsgüterindustrie. Er ist Interessenvertreter, Dienstleister und Ansprechpartner für rund 3.000 deutsche und europäische Unternehmen des Maschinen- und Anlagenbaus. In Deutschland beschäftigt der Maschinen- und Anlagenbau rund 865.000 Menschen, mit einem Umsatz von € 151 Milliarden und einem Exportanteil von rund 75%. VDMA-Mitgliedsunternehmen sind global aktiv und haben allein in der EU insgesamt 1.649 Tochterunternehmen gegründet, wovon 327 produzierende Tätigkeiten ausführen. Das hohe technische Niveau der mehr als 20.000 unterschiedlichen Produkte der Investitionsgüterindustrie begründet ihren weltweiten Ruf als „Innovationsbranche".

2. Situation: Funktionale Sicherheit

Nach einer Übergangszeit von 3 Jahren wird Ende 2009 die über viele Jahre im Maschinen- und Anlagenbau verwendete Norm EN 954-1:1996 "*Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen – Teil 1*" durch die im November letzten Jahres erschienene EN ISO 13849-1:2006-11 (ISO 13849-1:2006-11) ersetzt werden. Dies wird für den Anwender einen Betrachtungswechsel weg von der Deterministik[1], hin zur Probabilistik[2] mit sich bringen und bei nicht wenigen Anwendern im Maschinen- und Anlagenbau aber auch bei Komponentenlieferanten Fragen zur praktischen Umsetzung nach sich ziehen.
Ebenso wie die EN ISO 13849-1 bemüht sich die bereits Ende 2005 abgeschlossene Norm EN 62061 "*Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme*" (IEC 62061:2005) um die Vormachtstellung auf diesem Themengebiet. Die EN 62061 gilt als ein sektorspezifischer Ableger der aus 8 Teilen bestehenden IEC Horizontalnorm EN 61508:2001 "Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme" mit Ausrichtung auf den Maschinenbau.

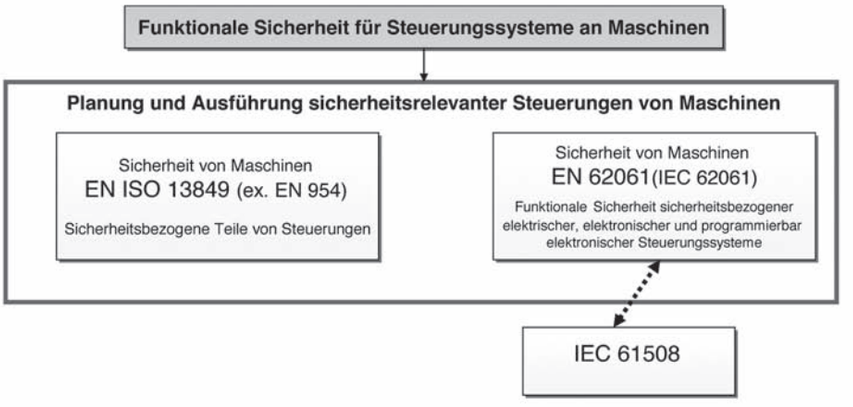
[1] Vorbestimmtheit, kausaler Zusammenhang
[2] Wahrscheinlichkeit, nicht streng kausal zusammenhängend

Während sich die IEC-Normen sehr stark auf das Thema Probabilistik mit Hilfe wahrscheinlichkeits-theoretischer Mathematik und Modellierung konzentrieren, wurde bei der Erarbeitung der ISO Norm 13849-1, ausgehend von der deterministisch orientierten EN 954-1, ein für den Anwender überschaubarer und begrenzter Anteil an probabilistischen Elementen zu den bekannten Elementen der EN 954-1 hinzugefügt, um Aufwand und Nutzen in einem ausgewogenen Verhältnis zu halten, und auch um den Bedürfnissen des mittelständischen Maschinen- und Steuerungsbauers zu entsprechen. Damit wird dem Willen der EG-Kommission entsprochen, dass Normen, die gesetzliche Anforderungen konkretisieren, von klein- und mittelständischen Unternehmen in der Praxis angewendet werden können.
In Bezug auf die Entwicklung sicherheitsbezogener Embedded-Software (Firmware, Systemsoftware) ab dem höchsten Anforderungslevel verweist auch die EN ISO 13849-1 auf die entsprechenden Teile der Normenreihe EN 61508.

3. Ausblick

Die EN ISO 13849-1 wird nach einem Übergangszeitraum von 3 Jahren nach Veröffentlichung die EN 954-1 zum 30.11.2009 ablösen. Mit dem im Mai 2007 neu erschienenen Amtsblatt zur Maschinenrichtlinie ist die EN ISO 13849-1 als harmonisierte Norm unter der EG-Maschinenrichtlinie gelistet und löst damit bei Anwendung die Vermutungswirkung zur Einhaltung der Richtlinie aus.
Die EN 62061:1995 ist bereits seit August 2006 als harmonisierte Norm unter der EG-Maschinenrichtlinie gelistet.
Bereits im Vorfeld der Fertigstellung der Normen, wurde in gemeinsamen Sitzungen beider verantwortlichen Normungskomitees der Versuch unternommen, mit einer gemeinsamen Tabelle in der Einleitung eine Empfehlung hinsichtlich der bevorzugten Anwendung beider Normen zu geben.
Nach der Fertigstellung der ISO 13849-1 im November 2006 haben sich beide Normungskomitees dahingehend geeinigt, einen gemeinsamen Anhang für beide Normen zu erstellen, der das Verständnis und die Anwendung der beiden Standards erleichtern soll.
Als weiterer Schritt ist geplant, in naher Zukunft beide Normen zu einer gemeinsamen Norm oder einer mehrteiligen Norm verschmelzen zu lassen, die das Thema "Funktionale Sicherheit für Steuerungssysteme an Maschinen" abdeckt.

4. Normen im Blickfeld



5. Fazit

Der VDMA begrüßt die Bemühungen der verantwortlichen Normungskomitees und erwartet, dass die beiderseits angestrebten Zielvorstellungen erfolgreich umgesetzt werden, die für eine verbesserte Kohärenz der Normen und für mehr Transparenz für die Anwender sorgen.

Der VDMA vertritt die folgende Auffassung:

- Als praktikabler Weg, um das für die Anwendung erforderliche Schutzniveau zu bestimmen, erweist sich in den meisten Anwendungsfällen des Maschinen- und Anlagenbaus die Ermittlung des Performance Levels (PL) nach der EN ISO 13849-1. Die EN 62061 ist insbesondere für klein- und mittelständische Unternehmen im Maschinen- und Anlagenbau, die eine Vielzahl von Projekten im Sondermaschinenbau bearbeiten und Einzelfertigung von Maschinen realisieren, zu komplex und zu umfangreich.

- Um die Auswahl von Komponenten sowie die Integration von Maschinen in Anlagen und Netzwerkumgebungen, die nach dem SIL (Safety Integrity Level) der EN 62061 klassifiziert wurden, zu ermöglichen, ist eine klare, verbindliche und leicht verständliche Zuordnungstabelle zwischen PL und SIL notwendig.

- Zur Unterstützung der Anwender und deren Konstrukteure sind Hilfsmittel , die den Umgang mit der Norm erleichtern, bereits zu Beginn der Übergangsphase zur Verfügung zu stellen, um Erfahrungswerte und Erkenntnisse zu sammeln. Die entsprechenden Bemühungen des BGIA (Berufsgenossenschaftliches Institut für Arbeitsschutz), in Kürze einen Leitfaden mit Musterberechnungen zu gängigen Konstruktionen und eine Software zur Verfügung zu stellen, mit deren Hilfe man die "Sicherheitsbezogenen Teile von Steuerungen" rechnerisch auf Basis der EN ISO 13849-1 ermitteln kann, werden vom VDMA begrüßt und entsprechend unterstützt.

- Da die probabilistische Betrachtungsweise der neuen Normenansätze auf geeigneten Zuverlässigkeitskennwerten von Bauteilen aufbaut, ist es wichtig, dass diese Werte zumindest für die Standardkomponenten in zentralen und zugänglichen Bibliotheken zur Verfügung stehen. Im Hinblick auf eine praxistaugliche Lösung unterstützt der VDMA ein konzertiertes Vorgehen der Hersteller entsprechender Bauteile.

Kontakt:
Dieter Gödicke
Telefon: +49 69 66 03-14 92
E-Mail: dieter.goedicke@vdma.org

Frankfurt, 30.05.2007 - DG

Anhang J:
Stichwortverzeichnis

Eine Übersicht der in den Schaltungsbeispielen verwendeten Abkürzungen findet sich in Tabelle 8.2 auf Seite 90.

Seite

C

D

E

F

Seite

F (Fortsetzung)

G

H

I

K

L

Seite

L (Fortsetzung)

M

N

O

P

Seite

P (Fortsetzung)

Q

R

S

T