

**DIN EN 60300-3-1**

ICS 03.120.10; 29.020

Ersatz für  
DIN IEC 60300-3-1:1994-02  
Siehe jedoch Beginn der  
Gültigkeit

**Zuverlässigkeitsmanagement –  
Teil 3-1: Anwendungsleitfaden –  
Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik  
(IEC 60300-3-1:2003);  
Deutsche Fassung EN 60300-3-1:2004**

Dependability management –  
Part 3-1: Application guide –  
Analysis techniques for dependability – Guide on methodology (IEC 60300-3-1:2003);  
German version EN 60300-3-1:2004

Gestion de la sûreté de fonctionnement –  
Partie 3-1: Guide d'application –  
Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique  
(CEI 60300-3-1:2003);  
Version allemande EN 60300-3-1:2004

Gesamtumfang 59 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE



## Beginn der Gültigkeit

Die von CENELEC am 2004-09-01 angenommene EN 60300-3-1 gilt als DIN-Norm ab 2005-05-01.

Daneben darf DIN IEC 60300-3-1:1994-02 noch bis 2007-09-01 angewendet werden.

## Nationales Vorwort

*Vorausgegangener Norm-Entwurf: E DIN IEC 60300-3-1:2001-12.*

Für die vorliegende Norm ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig.

Die enthaltene IEC-Publikation wurde vom TC 56 „Dependability“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zum Jahr 2007 unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

## Literaturhinweise

Meyna, A., *Zuverlässigkeitsbewertung zukunftsorientierter Technologien*, Vieweg, 1994.

Kuhlmann, A., *Einführung in die Sicherheitswissenschaft*, Verlag TÜV Rheinland, 1995.

Schneeweiss, W., *Die Fehlerbaummethode*, LiloLe, 1999.

Braband, J., *Methoden zur Sicherheitsanalyse und ihre praktische Anwendung*, Signal + Draht, Nr. 1, 2002, 9–13.

## Deutsche und englische Benennungen

Deutsch	Englisch
Analyse der Ausfallberichte und Korrekturmaßnahmen	Failure reporting analysis and corrective action (FRACAS)
Analyse der menschlichen Zuverlässigkeit	Human reliability analysis
Analyse des ungünstigsten Falls	Worst case analysis
Bayessche Zuverlässigkeitsverfahren	Bayesian reliability methods

Deutsch	Englisch
Beanspruchungsanalyse	Stress-strength analysis
Belastungsminderung und Auswahl von Teilen	Parts derating and selection
Ereignisbaumanalyse	Event tree analysis
Fehlzustandsart- und -auswirkungsanalyse (FMEA), in DIN 25448:1990-05 als „Ausfalleffektanalyse“ bezeichnet	Fault modes and effects analysis (FMEA)
Fehlzustandsart-, -auswirkungsanalyse und -kritizitätsanalyse (FMECA), in DIN 25448:1990-05 als „Ausfallbedeutungsanalyse“ bezeichnet	Fault modes, effects and criticality analysis (FMECA)
Funktionsfähigkeit	Reliability
PAAG-Verfahren (Prognose von Abweichungen, Auffinden der Ursachen, Abschätzen der Auswirkungen und Gegenmaßnahmen)  Auch „Gefährdungs- und Betreibbarkeits- untersuchung (HAZOP)“ genannt	Hazard and operability studies (HAZOP)
Kriechwegeanalyse	Sneak circuit analysis
Markoffanalyse	Markov analysis
Petri-Netz-Analyse	Petri net analysis
Fehlzustandsbaumanalyse	Fault tree analysis
Vorhersage der Ausfallrate	Failure rate prediction
Wahrheitstabelle	Truth table
Zuverlässigkeit	Dependability
Zuverlässigkeitsblockdiagrammanalyse	Reliability block diagram analysis

## Änderungen

Gegenüber DIN IEC 60300-3-1:1994-02 wurden folgende Änderungen vorgenommen:

- Zu den primären Analyseverfahren FMEA, Fehlzustandsbaum, Zuverlässigkeitsblockdiagramm, Markoff und Bauelementezählverfahren werden weitere unterstützende Verfahren neu mit aufgenommen.
- Diese Verfahren wie etwa HAZOP, Paretoanalyse, Finite Elemente, Petri-Netze, Bayessche Verfahren und Simulationsverfahren können die Zuverlässigkeitsanalysen begleitend unterstützen oder einen Mehrwert bei der Ausgestaltung der Zuverlässigkeit darstellen.

## Frühere Ausgaben

DIN IEC 60300-3-1:1994-02

– Leerseite –

**Zuverlässigkeitsmanagement  
Teil 3-1: Anwendungsleitfaden  
Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik  
(IEC 60300-3-1:2003)**

Dependability management – Part 3-1:  
Application guide  
Analysis techniques for dependability  
Guide on methodology  
(IEC 60300-3-1:2003)

Gestion de la sûreté de fonctionnement –  
Partie 3-1: Guide d'application  
Techniques d'analyse de la sûreté de  
fonctionnement  
Guide méthodologique  
(CEI 60300-3-1:2003)

Diese Europäische Norm wurde von CENELEC am 2004-09-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

**CENELEC**

Europäisches Komitee für Elektrotechnische Normung  
European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique

**Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel**

## Vorwort

Der Text der Internationalen Norm IEC 60300-3-1:2003, ausgearbeitet von dem IEC/TC 56 „Dependability“, wurde der formellen Abstimmung unterworfen und von CENELEC am 2004-09-01 als EN 60300-3-1 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2005-09-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2007-09-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

## Anerkennungsnotiz

Der Text der Internationalen Norm IEC 60300-3-1:2003 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung ist unter „Literaturhinweise“ zu der aufgelisteten Norm die nachstehende Anmerkung einzutragen:

IEC 60300-2 ANMERKUNG Harmonisiert als EN 60300-2:1996 (nicht modifiziert).

# Inhalt

	Seite
Vorwort.....	2
Einleitung .....	4
1 Anwendungsbereich .....	4
2 Normative Verweisungen .....	4
3 Begriffe .....	5
4 Grundsätzliches Verfahren zur Analyse der Zuverlässigkeit.....	6
4.1 Allgemeines Verfahren .....	6
4.2 Zuverlässigkeitsanalyseverfahren .....	7
4.3 Zuverlässigkeitszuweisungen.....	9
4.4 Zuverlässigkeitsanalyse .....	10
4.5 Analyse und Betrachtung der Instandhaltung .....	11
5 Wahl des geeigneten Analyseverfahrens.....	11
Anhang A (informativ) Kurzbeschreibung der Analyseverfahren .....	14
Literaturhinweise.....	53
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen .....	55

## Bilder

Bild 1 – Allgemeines Verfahren zur Analyse der Zuverlässigkeit .....	6
Bild A.1 – Temperaturabhängigkeit der Ausfallrate .....	16
Bild A.2 – Fehlzustandsbaum für einen Tonverstärker.....	18
Bild A.3 – Teilbaum der Fehlzustandsbaumanalyse in Bild A.2 .....	19
Bild A.4 – Ereignisbaum.....	21
Bild A.5 – Elementare Modelle .....	22
Bild A.6 – Beispiel einer Einheit.....	24
Bild A.7 – Zustands-Übergangsdiagramm.....	26
Bild A.8 – Blockdiagramm eines Multiprozessorsystems .....	28
Bild A.9 – Petri-Netz eines Multiprozessorsystems .....	29
Bild A.10 – Das Verfahren bei HAZOP-(PAAG-)Studien .....	33
Bild A.11 – Menschliches Fehlverhalten als Ereignisbaum dargestellt .....	37
Bild A.12 – Beispiel: Anwendung von Beanspruchungskriterien .....	39
Bild A.13 – Wahrheitstabelle für zwei einfache Systeme .....	40
Bild A.14 – Beispiel.....	40
Bild A.15 – Ursache-Wirkung-Diagramm.....	51

## Tabellen

Tabelle 1 – Anwendung allgemeiner Zuverlässigkeitsanalyseverfahren.....	8
Tabelle 2 – Merkmale ausgewählter Zuverlässigkeitsanalyseverfahren .....	13
Tabelle A.1 – Symbole für die Darstellung im Fehlzustandsbaum .....	19
Tabelle A.2 – Zustände der Einheit .....	25
Tabelle A.3 – Auswirkungen von Ausfällen in funktionalen und diagnostischen Teilen.....	25
Tabelle A.4 – Übergangsraten .....	26
Tabelle A.5 – Beispiel einer FMEA .....	31
Tabelle A.6 – Grundlegende Leitworte und deren allgemeine Bedeutung.....	32
Tabelle A.7 – Zusätzliche Leitworte bezüglich Zeitpunkt und Reihenfolge und Abfolge .....	32
Tabelle A.8 – Glaubwürdiges menschliches Fehlverhalten.....	36
Tabelle A.9 – Beispiel einer Wahrheitstabelle .....	41

## Einleitung

Die in diesem Teil von IEC 60300 beschriebenen Analyseverfahren werden für die Vorhersage, Bewertung und Verbesserung der Funktionsfähigkeit, Verfügbarkeit und Instandhaltbarkeit einer Einheit verwendet.

Diese Analysen werden während der Konzept- und Definitionsphase, Entwurfs- und Entwicklungsphase, Betriebs- und Instandhaltungsphase in verschiedenen Systemebenen und Analysetiefen durchgeführt, um die Zuverlässigkeit einer Einheit zu beurteilen, zu ermitteln und zu verbessern. Sie können auch dafür verwendet werden, die Ergebnisse der Analyse mit den festgelegten Anforderungen zu vergleichen.

Darüber hinaus werden sie bei der Planung der Logistik und der Instandhaltung verwendet, um die Instandhaltungshäufigkeit und den Teiletausch zu schätzen. Diese Schätzungen bestimmen häufig wichtige Kostenelemente des Lebenszyklus und sollten bei Untersuchungen der Lebenszykluskosten und bei vergleichenden Untersuchungen sorgfältig verwendet werden.

Um aussagekräftige Ergebnisse zu erhalten, sollten bei der Analyse alle zur Zuverlässigkeit eines Systems beitragenden möglichen Elemente beachtet werden: Hardware, Software, als auch menschliche Faktoren und organisatorische Aspekte.

## 1 Anwendungsbereich

Dieser Teil von IEC 60300 enthält einen allgemeinen Überblick über die üblicherweise verwendeten Verfahren zur Analyse der Zuverlässigkeit. Die jeweils übliche Methodik, deren Vor- und Nachteile, benötigte Eingabedaten und sonstige Bedingungen für die Verwendung der verschiedenen Techniken werden beschrieben.

Diese Norm ist eine Einführung in ausgewählte Verfahren und stellt die für die Auswahl der geeignetsten Analyseverfahren benötigten Informationen bereit.

## 2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*.

IEC 60300-3-2:1993, *Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field*.

IEC 60300-3-4:1996, *Dependability management – Part 3: Application guide – Section 4: Guide to the specification of dependability requirements*.

IEC 60300-3-5:2001, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*.

IEC 60300-3-10:2001, *Dependability management – Part 3-10: Application guide – Maintainability*.

IEC 60706-1:1982, *Guide on maintainability of equipment – Part 1: Sections One, Two and Three – Introduction, requirements and maintainability programme*.

IEC 60706-2:1990, *Guide on maintainability of equipment – Part 2: Section Five – Maintainability studies during the design phase*.

IEC 60812:1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*.

IEC 61078:1991, *Analysis techniques for dependability – Reliability block diagram method*.

IEC 61165:1995, *Application of Markov techniques*.

IEC 61709:1996, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*.

IEC 61882:2001, *Hazard and operability studies (HAZOP Studies) – Application guide*.

ISO 9000:2000, *Quality management systems – Fundamentals and vocabulary*.



### 3 Begriffe

Für die Anwendung dieses Teils von IEC 60300 gelten die Begriffe nach IEC 60050(191), von denen einige nachfolgend zusammen mit weiteren geltenden Begriffen angegeben sind.

#### 3.1

##### **Einheit**

Teil, Bauelement, Gerät, Teilsystem, Funktionseinheit, Betriebsmittel oder System, das/die für sich allein betrachtet werden kann

ANMERKUNG Eine Betrachtungseinheit kann aus Hardware, Software oder beidem bestehen und in besonderen Fällen auch Personen einschließen.

[IEV 191-01-01]

#### 3.2

##### **System**

Satz von in Wechselbeziehung oder Wechselwirkung stehenden Elementen

[ISO 9000:2000]

ANMERKUNG 1 Im Zusammenhang mit Zuverlässigkeit hat ein System

- a) einen festgelegten Zweck, ausgedrückt durch geforderte Funktionen, und
- b) festgelegte Betriebsbedingungen.

ANMERKUNG 2 Die Konzeption eines Systems ist hierarchisch.

#### 3.3

##### **Komponente**

in der niedrigsten Ebene der Analyse betrachtete Einheit

#### 3.4

##### **Zuweisung**

während der Entwicklung einer Einheit angewendetes Verfahren, um die für eine Einheit geforderten Leistungsmerkmale auf deren Untereinheiten nach vorgegebenen Kriterien aufzuteilen

#### 3.5

##### **Ausfall**

Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen

ANMERKUNG 1 Nach einem Ausfall befindet sich die Einheit in einem Fehlzustand.

ANMERKUNG 2 Der Ausfall ist ein Ereignis, im Unterschied zum Fehlzustand.

[IEV 191-04-01]

#### 3.6

##### **Fehlzustand;**

##### **Fehlzustandsart**

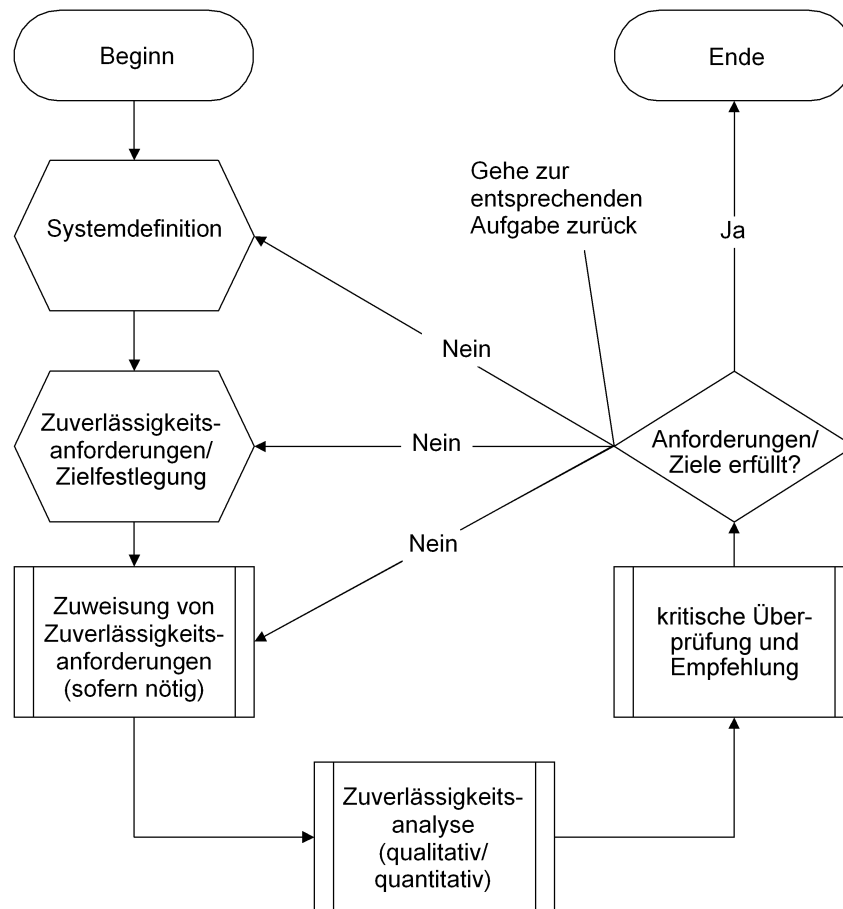
Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei durch Wartung oder andere geplante Handlungen bzw. durch das Fehlen äußerer Mittel verursachte Funktionsunfähigkeit ausgeschlossen ist

ANMERKUNG Ein Fehlzustand ist oft das Ergebnis eines Ausfalls der Einheit selbst, er kann aber auch ohne vorherigen Ausfall vorhanden sein.

[IEC 191-05-01]

## 4 Grundsätzliches Verfahren zur Analyse der Zuverlässigkeit

### 4.1 Allgemeines Verfahren



**Bild 1 – Allgemeines Verfahren zur Analyse der Zuverlässigkeit**

Ein allgemeines Verfahren zur Analyse der Zuverlässigkeit umfasst, soweit zutreffend, die nachfolgenden Aufgaben:

a) Definition des Systems

Definition des zu analysierenden Systems, seiner Betriebszustände, seiner funktionalen Beziehungen mit seiner Umgebung einschließlich der Schnittstellen und Prozesse. Im Allgemeinen ist die Systemdefinition eine aus der Systementwicklung folgende Angabe.

b) Zuverlässigkeitsanforderungen/Festlegung der Ziele

Auflistung aller Anforderungen an die Funktionsfähigkeit und Verfügbarkeit oder an Ziele, Eigenschaften und Merkmale des Systems, zusammen mit Umgebungs- und Betriebsbedingungen sowie Anforderungen an die Instandhaltung. Definition von Systemausfall, Ausfallkriterien und Ausfallbedingungen auf der Grundlage funktionaler Systemspezifikationen, erwarteter Betriebsdauer und Betriebsumgebung (Nutzungsprofil und Nutzungsdauer). IEC 60300-3-4 sollte hierfür als Anleitung verwendet werden.

c) Zuweisung der Zuverlässigkeitsanforderungen

Zuweisung von Zuverlässigkeitsanforderungen oder Zuverlässigkeitszielen des Systems an die verschiedenen Teilsysteme, wenn dies notwendig ist, in der frühen Entwicklungsphase.

d) Zuverlässigkeitsanalyse

Analyse des Systems mittels Zuverlässigkeitstechniken und zugehöriger Leistungsdaten.

1) Qualitative Analyse

- Analysiere die funktionale Systemstruktur.

- Ermittle die Fehlzustandsarten des Systems und seiner Komponenten, Ausfallmechanismen, Ursachen, Auswirkungen und Folgen von Ausfällen.
- Ermittle Abnutzungsmechanismen, die zu Ausfällen führen können.
- Analysiere Ausfall-/Fehlzustandspfade.
- Analysiere Instandhaltbarkeit hinsichtlich Zeit, Problemeingrenzungs- und Reparaturverfahren.
- Ermittle, wie zutreffend die vorgesehenen Diagnosemittel zum Erkennen von Fehlzuständen sind.
- Analysiere Möglichkeiten der Vermeidung von Fehlzuständen.
- Bestimme mögliche Instandhaltungs- und Reparaturstrategien usw.
- 2) Quantitative Analyse
  - Entwickle Zuverlässigkeitsmodelle.
  - Lege zu verwendende numerische Referenzdaten fest.
  - Führe Zuverlässigkeitsberechnungen durch.
  - Führe nach Bedarf Analysen der Kritizität und Sensitivität von Komponenten durch.

e) Bewertung und Empfehlungen

Analysiere, ob die Zuverlässigkeitsanforderungen und Ziele erfüllt sind und ob alternative Entwürfe in wirksamer und kostengünstiger Weise die Zuverlässigkeit verbessern können. Hierzu können (sofern zutreffend) die folgenden Aufgaben gehören.

- Beurteile die Verbesserung der Systemzuverlässigkeit als Ergebnis von Verbesserungen im Entwurf und in der Fertigung (z. B. Redundanz, Verringerung der Beanspruchung, Verbesserung der Instandhaltungsstrategien, Prüfsysteme, technologische Prozesse und Qualitätslenkungssystem).

ANMERKUNG 1 Die inhärenten Maßgrößen für die Zuverlässigkeit können nur durch den Entwurf verbessert werden. Falls ungenügende Werte der Maßgrößen beobachtet werden und diese einem schlechten Fertigungsprozess zuzuschreiben sind, so kann man aus betrieblicher Sicht davon sprechen, dass die beobachteten Maßgrößen für die Zuverlässigkeit durch einen verbesserten Fertigungsprozess verbessert werden können.

- Bewerte den Systementwurf, bestimme Schwachstellen und kritische Fehlzustände und Komponenten.
- Beachte Probleme mit Systemschnittstellen, Merkmale und Mechanismen für „das Ausfallen in einen sicheren Zustand“ usw.
- Entwickle alternative Wege zur Verbesserung der Zuverlässigkeit, z. B. Redundanz, Leistungsüberwachung, Erkennung von Fehlzuständen, Techniken zur Systemrekonfiguration, Instandhaltungsprozeduren, Austauschbarkeit von Komponenten, Reparaturprozeduren.
- Mache abwägende Untersuchungen zu Kosten und Komplexität von alternativen Entwürfen.
- Beurteile die Auswirkungen beherrschter Fertigungsprozesse.
- Beurteile die Ereignisse und vergleiche diese mit den Anforderungen.

ANMERKUNG 2 Das vorstehende allgemeine Verfahren fasst aus Entwicklungssicht die spezifischen Zuverlässigkeitsprogrammelemente aus IEC 60300-2 zusammen, die bei einer Zuverlässigkeitsanalyse anwendbar sind: Zuverlässigkeitsspezifikationen, Analyse der Einsatzumgebung, Funktionsfähigkeit, Instandhaltbarkeit, menschliche Einflussfaktoren, Modellierung und Simulation der Funktionsfähigkeit, Entwurfsanalyse und Beurteilung des Produkts, Ursache und Auswirkung von Ausfällen und Risikoanalyse, Vorhersage und abwägende Analysen.

## 4.2 Zuverlässigkeitsanalyseverfahren

Die in dieser Norm vorgestellten Verfahren können in zwei Hauptkategorien eingeteilt werden:

- Verfahren, die in erster Linie für die Zuverlässigkeitsanalyse eingesetzt werden;
- allgemeine technische Verfahren, welche die Zuverlässigkeitsanalysen begleitend unterstützen oder einen Mehrwert bei der Ausgestaltung der Zuverlässigkeit darstellen.

Die Anwendbarkeit der einzelnen Zuverlässigkeitsanalyseverfahren innerhalb der allgemeinen Analyseaufgabe und Analyseverfahren ist in Tabelle 1 angegeben. Tabelle 2 enthält detailliertere Merkmale. Die Verfahren werden jeweils kurz in Anhang A erläutert.

**Tabelle 1 – Anwendung allgemeiner Zuverlässigkeitsanalyseverfahren**

Analyseverfahren	Zuweisung von Zuverlässigkeitsanforderungen/Ziele	Qualitative Analyse	Quantitative Analyse	Bewertung und Empfehlungen	Anhang
Vorhersage der Ausfallrate	Anwendbar auf serielle Systeme ohne Redundanz	Möglich für Instandhaltungsstrategieanalyse	Berechnung der Ausfallraten und MTTF von elektronischen Bauelementen und Geräten	Unterstützend	A.1.1
Fehlzustandsbaum-analyse	Anwendbar, falls das Systemverhalten nicht stark von der Zeit- oder der Abfolge abhängig ist	Fehlzustandskombinationen	Berechnung der Systemzuverlässigkeit und zugehöriger Beiträge von Teilsystemen zur Systemnichtverfügbarkeit	Anwendbar	A.1.2
Ereignisbaumanalyse	Möglich	Ausfallfolgen	Berechnung der Systemausfallraten	Anwendbar	A.1.3
Zuverlässigkeitsblockdiagramm-analyse	Anwendbar auf Systeme, bei denen voneinander unabhängige Blöcke angenommen werden	Erfolgspfade	Berechnung der Systemzuverlässigkeit	Anwendbar	A.1.4
Markoffanalyse	Anwendbar	Ausfallreihenfolgen	Berechnung der Systemzuverlässigkeit	Anwendbar	A.1.5
Petri-Netz-Analyse	Anwendbar	Ausfallreihenfolgen	Liefert die Systembeschreibung für die Markoffanalyse	Anwendbar	A.1.6
Fehlzustandsart- und -auswirkungs- (und -kritizitäts-)analyse (FME(C)A)	Anwendbar auf Systeme, in denen ein unabhängiger Einzelausfall vorherrschend ist	Auswirkungen von Ausfällen	Berechnung der Systemausfallraten (und Kritizität)	Anwendbar	A.1.7
PAAG-Verfahren Gefährdungs- und Betreibbarkeitsuntersuchung (HAZOP)	Unterstützend	Ursachen und Auswirkungen von Abweichungen	Nicht anwendbar	Unterstützend	A.1.8
Analyse der menschlichen Zuverlässigkeit	Unterstützend	Auswirkung menschlicher Leistung auf den Systembetrieb	Berechnung der Wahrscheinlichkeiten menschlichen Fehlverhaltens	Unterstützend	A.1.9
Beanspruchungsanalyse	Nicht anwendbar	Brauchbar als Mittel zur Vermeidung von Fehlzuständen	Berechnung der Funktionsfähigkeit von (elektro-)mechanischen Komponenten	Unterstützend	A.1.10
Wahrheitstabelle (Strukturfunktionsanalyse)	Nicht anwendbar	Möglich	Berechnung der Systemzuverlässigkeit	Unterstützend	A.1.11
Statistische Zuverlässigkeitsverfahren	Möglich	Auswirkungen von Fehlzuständen	Quantitative Schätzung der Funktionsfähigkeit mit Unsicherheiten	Unterstützend	A.1.12
<b>ANMERKUNG</b> Die Formulierung in dieser Tabelle ist wie folgt zu verstehen. „Anwendbar“ bedeutet, dass das Verfahren allgemein anwendbar ist und für diese Aufgabe empfohlen wird (möglicherweise mit den erwähnten Einschränkungen). „Möglich“ bedeutet, dass das Verfahren für diese Aufgabe verwendet werden kann, es aber gegenüber anderen Verfahren gewisse Nachteile hat. „Unterstützend“ bedeutet, dass es für einen gewissen Teil der Aufgabe allgemein anwendbar ist, aber nicht als einziges Verfahren für die gesamte Aufgabe. „Nicht anwendbar“ bedeutet, dass es für diese Aufgabe nicht verwendet werden kann.					

Zu den unterstützenden oder allgemeinen technischen Verfahren gehören (diese Liste ist nicht notwendigerweise vollständig):

- Instandhaltbarkeitsanalyse (allgemein in IEC 60300-3-10 und detailliert in IEC 60706-2 behandelt);
- Kriechwegeanalyse (siehe A.2.1);
- Analyse des ungünstigsten Falls (siehe A.2.2);

- Variationssimulations-Modellierung (siehe A.2.3);
- Verfahren für die Vorhersage der Funktionsfähigkeit von Software (siehe A.2.4);
- Analyse finiter Elemente (siehe A.2.5);
- Belastungsminderung und Auswahl von Teilen (siehe A.2.6);
- Paretoanalyse (siehe A.2.7);
- Ursache-Wirkungs-Diagramme (siehe A.2.8);
- Analyse der Ausfallberichte und Korrekturmaßnahmen (siehe A.2.9).

Es wird darauf hingewiesen, dass die Verfahren entsprechend den betreffenden IEC-Normen benannt und verstanden werden, soweit diese existieren. Die folgenden Verfahren wurden nicht als selbständige Verfahren aufgenommen, da diese entweder von primären Verfahren abgeleitet sind oder in enger Beziehung zu ihnen stehen:

- Ursache-/Folge-Analyse ist eine Kombination von Ereignisbaum- und Fehlzustandsbaumanalyse.
- Dynamische Fehlzustandsbaumanalyse ist eine Erweiterung der Fehlzustandsbaumanalyse, wobei bestimmte Ereignisse durch Markoff-Sub-Modelle ausgedrückt werden.
- Funktionale Ausfallanalyse ist eine Sonderart einer funktionalen FMEA.
- Binäre Entscheidungsdiagramme werden hauptsächlich als eine effiziente Darstellung von Fehlzustandsbäumen verwendet.

### 4.3 Zuverlässigkeitszuweisungen

Das Festlegen von Zuverlässigkeitsanforderungen an Teilsysteme ist ein wesentlicher Teil der Systementwurfsarbeit. Das Ziel dieser Arbeit ist es, die effektivste Systemarchitektur zu finden, mit der die Zuverlässigkeitsanforderungen erfüllt werden können (und somit zur Machbarkeitsstudie beizutragen). Da Zuverlässigkeit der zusammenfassende Ausdruck für Funktionsfähigkeit, Verfügbarkeit und Instandhaltbarkeit ist, muss eine Zuweisung für jedes dieser Merkmale gemacht werden. Da jedoch die Zuweisungstechniken für alle drei Merkmale gleichartig sind, wird hierfür der zusammenfassende Ausdruck Zuverlässigkeit verwendet.

In einem ersten Schritt werden die Zuverlässigkeitsanforderungen an das Gesamtsystem den Teilsystemen zugewiesen. Dabei ist die Komplexität dieser Teilsysteme in Kenntnis von Erfahrungen mit vergleichbaren Teilsystemen zu berücksichtigen. Wenn die Anforderungen vom ersten gemachten Entwurf noch nicht erfüllt werden, so müssen Zuweisung und/oder Entwurf wiederholt werden. Die Zuweisung geschieht oft auf der Grundlage von Betrachtungen der Komplexität, Kritizität, Betriebsprofil und Umweltbedingungen.

Da die Zuverlässigkeitszuweisung üblicherweise in einem frühen Stadium notwendig ist, wenn noch keine oder nur wenige Informationen verfügbar sind, sollte die Zuweisung periodisch wiederholt werden.

Die Zuweisung (auch Aufteilung genannt) der Systemzuverlässigkeit auf die Teilsysteme und Baugruppenebene ist in einem frühen Stadium während der Produktdefinitionsphase notwendig, um

- die Machbarkeit der Erfüllung der Zuverlässigkeitsanforderungen an das System zu prüfen,
- für tiefere Ebenen realistische Anforderungen an die Zuverlässigkeit des Entwurfs aufzustellen,
- klare und verifizierbare Zuverlässigkeitsanforderungen an die Unterlieferanten aufzustellen.

Bei der Durchführung der Zuverlässigkeitszuweisung müssen die folgenden Schritte gemacht werden:

- Analyse des Systems und Ermittlung der Bereiche, von denen der Entwurf bekannt ist und Angaben zu den Zuverlässigkeitsmerkmalen verfügbar oder leicht zugänglich sind.
- Zuweisung geeigneter Gewichtungen und Ermittlung deren Beitrags zu Zuverlässigkeitsanforderungen des Gesamtsystems. Die Differenz ist der Teil der Zuverlässigkeitsanforderungen, der anderen Bereichen zugewiesen werden kann.

Zuverlässigkeitszuweisung hat folgende Nutzen:

- Sie ist während der Produktentwicklung ein Weg, um die Beziehungen der Zuverlässigkeitsziele zwischen dem System und seinen Einheiten (z. B. Teilsysteme, Geräte, Komponenten) weiter zu entwickeln und zu verstehen.
- Sie behandelt Zuverlässigkeit genauso wie andere Entwurfsparameter wie Kosten und Leistungsmerkmale.

- Durch sie ergeben sich gesonderte Ziele für die Zuverlässigkeit der von Lieferanten zu liefernden Teile, wodurch wiederum Entwurf und Lieferverfahren verbessert werden.
- Sie kann zu optimaler Systemzuverlässigkeit führen, da sie solche Faktoren wie Komplexität, Kritizität und Auswirkungen der Betriebsumgebung berücksichtigt.

Andererseits sollten einige Einschränkungen zur Kenntnis genommen werden:

- Oft wird die Annahme getroffen, die Einheiten eines Systems seien voneinander unabhängig, z. B. der Ausfall einer Einheit wirke sich nicht auf die anderen aus. Da diese Annahme oft nicht stimmt, verringert diese Einschränkung die Vorzüge dieses Verfahrens.
- Zuweisung bei redundanten Systemen ist komplexer. In diesen Fällen ist es angebracht, ein iteratives Verfahren zu benutzen, um zu prüfen, ob die Zuverlässigkeitsziele für das System erreicht werden können, beispielsweise die Fehlzustandsbaumanalyse.

## 4.4 Zuverlässigkeitsanalyse

### 4.4.1 Verfahrenskategorien

Zuverlässigkeitsanalyseverfahren, die kurz im Anhang A erläutert sind, können entsprechend ihrem Hauptzweck in folgende Kategorien eingeteilt werden:

- a) Verfahren zur Vermeidung von Fehlzuständen, z. B.
  - 1) Minderbelastung und Auswahl von Teilen;
  - 2) Beanspruchungsanalyse.
- b) Verfahren zur Analyse der Systemarchitektur und Bewertung der Zuverlässigkeit (Zuweisung), z. B.
  - 1) Induktive Verfahren (behandeln hauptsächlich die Auswirkungen einzelner Fehlzustände)
    - Ereignisbaumanalyse (ETA);
    - Fehlzustandsart- und -auswirkungsanalyse (FMEA);
    - PAAG/HAZOP-Verfahren.
  - 2) Deduktive Verfahren (können Auswirkungen von Kombinationen von Fehlzuständen erklären)
    - Fehlzustandsbaumanalyse (FTA);
    - Markoffanalyse;
    - Petri-Netz-Analyse;
    - Wahrheitstabelle (Strukturfunktionsanalyse);
    - Zuverlässigkeitsblockdiagramme (RBD).
- c) Verfahren zur Schätzung der Maßgrößen für Grundereignisse, z. B.
  - Vorhersage der Ausfallrate;
  - Analyse der menschlichen Zuverlässigkeit;
  - statistische Zuverlässigkeitsverfahren;
  - Verfahren für die Vorhersage der Funktionsfähigkeit von Software.

Ob diese Verfahren mit Abfolgen von Ereignissen oder zeitabhängigen Eigenschaften arbeiten, stellt ein weiteres Unterscheidungsmerkmal dar. Wenn man dies berücksichtigt, so ergibt sich folgende zusammenfassende Einteilung:

<b>Ablauf- abhängig</b>	Ereignisbaumanalyse	Markoff, Petri, Wahrheitstabelle
<b>Ablauf- unabhängig</b>	FMEA, PAAG/HAZOP	Fehlzustandsbaumanalyse, Zuverlässigkeitsblockdiagramm

induktiv (nur ein Fehlzustand)

deduktiv (mehrfache Fehlzustände)

Diese Analyseverfahren erlauben sowohl die Beurteilung von qualitativen Merkmalen als auch die Schätzung quantitativer Merkmale, um damit das Langzeit-Betriebsverhalten vorherzusagen. Es sollte zur Kenntnis

genommen werden, dass die Gültigkeit der Ergebnisse deutlich von der Genauigkeit und Richtigkeit der Eingabedaten für die Grundereignisse abhängt.

Jedoch ist kein Zuverlässigkeitsanalyseverfahren für sich alleine ausreichend umfassend und flexibel, um alle möglichen Modellkomplexitäten zu behandeln, die erforderlich sind, um die Merkmale praktischer Systeme zu beurteilen (Hardware und Software, komplexe funktionale Strukturen, verschiedene Technologien, reparierbare und instandsetzbare Strukturen usw.). Es kann erforderlich sein, mehrere komplementäre Analyseverfahren heranzuziehen, um eine sorgfältige Behandlung von komplexen oder multi-funktionalen Systemen sicherzustellen.

In der Praxis hat sich eine gemischte Vorgehensweise mit sich gegenseitig ergänzender deduktiver und induktiver Analyse als sehr effektiv erwiesen, insbesondere um die Vollständigkeit der Analyse sicher zu stellen.

#### **4.4.2 Induktive Verfahren**

Beim induktiven Verfahren werden die Ausfallarten in der Ebene der Komponenten ermittelt. Für jede Ausfallart wird deren Auswirkung auf das Leistungsverhalten in einer betroffenen Systemebene bestimmt. Dieses induktive (von unten nach oben) Verfahren erlaubt auf sehr strenge Art, alle einzelnen Ausfallarten zu ermitteln, da es auf Teilelisten oder andere Prüflisten zurückgreifen kann. In den frühen Entwicklungsstufen kann die Analyse qualitativer Art sein und zunächst funktionale Ausfälle behandeln. Später kann dann eine quantitative Analyse unternommen werden, wenn dafür ausreichende Informationen zu den Komponenten vorhanden sind.

#### **4.4.3 Deduktive Verfahren**

Zunächst sollte das unerwünschte Einzelereignis oder die erfolgreiche Erfüllung der Systemfunktion in der höchsten interessierenden Ebene (Hauptereignis) festgelegt werden. In allen Ebenen werden hierzu beitragende Ereignisse ermittelt und analysiert.

Beim deduktiven (von oben nach unten) Vorgehen beginnt man in der höchsten interessierenden Ebene, d. h. in der Systemebene oder Teilsystemebene, um dann schrittweise tiefere Ebenen zu betrachten, um dort gegebenenfalls unerwünschtes Systemverhalten zu erkennen.

Die Analyse wird dann in der nächsttieferen Systemebene fortgesetzt, um dort solche Ausfälle und die diesen zugehörigen Ausfallarten zu finden, welche die ursprünglich identifizierte Auswirkung der Ausfallart ergeben könnten. Für jede Ausfallart in der nächsttieferen Ebene wird die Analyse wiederholt, indem die Wege und funktionalen Zusammenhänge zur nächsttieferen Ebene zurückverfolgt werden. Dieses Wechselspiel wird bis zum Erreichen der gewünschten tiefsten Ebene fortgesetzt.

Das deduktive Verfahren wird zum Beurteilen von Mehrfachausfällen einschließlich von aufeinander folgenden, sich bedingenden Ausfällen angewendet, zum Erkennen von Fehlzuständen mit gemeinsamen Ursachen oder, wenn es aufgrund der Systemkomplexität vorteilhafter ist, mit der Auflistung von Systemausfällen zu beginnen.

### **4.5 Analyse und Betrachtung der Instandhaltung**

Das Betriebsverhalten eines reparierbaren Systems wird wesentlich von seiner Instandhaltbarkeit sowie den eingesetzten Instandhaltungsstrategien beeinflusst. Die Verfügbarkeit ist die geeignete Maßgröße, um den Einfluss der Instandhaltung auf die Systemzuverlässigkeit zu bewerten, wenn die Langzeitfunktion die kritische Anwendung ist. Die Funktionsfähigkeit ist die geeignete Maßgröße, wenn eine ununterbrochene Funktion die kritische Anwendung ist.

Die Reparatur eines Systems ohne Funktionsunterbrechung ist üblicherweise nur bei redundanter Systemstruktur und zugänglichen redundanten Komponenten möglich. Wenn dem so ist, wird durch Reparatur oder Austausch die Funktionsfähigkeit und Verfügbarkeit des Systems erhöht.

Üblicherweise ist eine getrennte Analyse zur Beurteilung der Reparatur- und Instandhaltungsaspekte eines Systems erforderlich (siehe IEC 60706-1, IEC 60706-2 und IEC 60300-3-10).

## **5 Wahl des geeigneten Analyseverfahrens**

Die Wahl der Verfahren, die in ein Zuverlässigkeitsprogramm aufzunehmen sind, ist ein sehr individueller Prozess, so dass eine allgemeine Empfehlung für die Wahl eines oder mehrerer spezieller Verfahren nicht gegeben werden kann. Die Wahl geeigneter Verfahren sollte durch gemeinsames Bemühen von Zuverlässigkeits- und Systemexperten geschehen. Die Wahl sollte früh zu Beginn der Programmentwicklung geschehen und sollte auf ihre Anwendbarkeit bewertet werden.

Die Wahl kann anhand folgender Kriterien erleichtert werden:

- a) Systemkomplexität: Komplexe Systeme, z. B. mit Redundanz oder diversitären Merkmalen, erfordern üblicherweise eine tiefergehendere Analyse als einfachere Systeme.
- b) Neuartigkeit des Systems: Ein vollständig neuer Systementwurf kann eine intensivere Analyse als ein bewährter Entwurf erfordern.
- c) Qualitative oder quantitative Analyse: Ist eine quantitative Analyse notwendig?
- d) Einzel- oder Mehrfach-Fehlzustände: Wirken sich Kombinationen von Fehlzuständen aus oder können diese vernachlässigt werden?
- e) Von der Zeit oder von Abfolgen abhängiges Verhalten: Spielt das Aufeinanderfolgen von Ereignissen eine Rolle in der Analyse (z. B. fällt das System nur dann aus, wenn dem Ereignis A das Ereignis B vorangegangen ist, aber nicht umgekehrt) oder zeigt das System zeitabhängiges Verhalten (z. B. verschlechterte Betriebsarten nach Ausfall, in Phasen gestaffelte Einsätze)?
- f) Kann für abhängige Ereignisse verwendet werden: Sind die Ausfall- oder Reparaturmerkmale einer einzelnen Einheit vom Zustand des Systems abhängig?
- g) Induktive oder deduktive Analyse: Üblicherweise können induktive Verfahren in einer geradlinigen Art durchgeführt werden, wogegen deduktive Verfahren mehr Nachdenken und Kreativität erfordern und daher eher für Fehler anfällig sind.
- h) Zuweisung der Anforderungen an die Funktionsfähigkeit: Sollte das Verfahren fähig sein, Anforderungen an die Funktionsfähigkeit quantitativ aufzuteilen?
- i) Erforderlicher Ausbildungsstand: Welcher Ausbildungsgrad oder welche Erfahrung ist erforderlich, um das Verfahren sinnvoll und richtig anzuwenden?
- j) Akzeptanz und Allgemeingültigkeit: Ist das Verfahren allgemein anerkannt, z. B. von Behörden oder einem Kunden?
- k) Werkzeugunterstützung: Benötigt das Verfahren (rechnergestützte) Werkzeugunterstützung oder kann es auch von Hand durchgeführt werden?
- l) Plausibilitätsprüfungen: Kann man die Plausibilität der Ergebnisse leicht von Hand nachprüfen? Falls nicht, sind die verfügbaren Werkzeuge validiert?
- m) Verfügbarkeit von Werkzeugen: Sind Werkzeuge entweder im Hause oder im Handel verfügbar? Haben diese Werkzeuge eine gemeinsame Schnittstelle mit anderen Analysewerkzeugen, damit man Ergebnisse wiederverwenden oder exportieren kann?
- n) Normung: Gibt es eine Norm, die das Merkmal des Verfahrens und die Darstellung der Ergebnisse (z. B. Symbole) beschreibt?

In Tabelle 2 ist ein Überblick über die verschiedenen Zuverlässigkeitsanalyseverfahren mit ihren Eigenschaften und Merkmalen enthalten. Um eine vollständige Analyse eines Systems durchzuführen, kann mehr als ein Verfahren erforderlich sein.



Tabelle 2 – Merkmale ausgewählter Zuverlässigkeitsanalyseverfahren

Verfahren	Geeignet für komplexe Systeme	Geeignet für neuartige Systemauslegungen	Quantitative Analyse	Geeignet für Kombinationen von Fehlzuständen	Geeignet zur Behandlung von Abfolgeabhängigkeit	Kann für abhängige Ereignisse verwendet werden	Deduktiv oder induktiv	Geeignet für Zuverlässigkeitszuweisung	Erforderlicher Ausbildungsstand (von niedrig bis hoch)	Akzeptanz und Allgemeingültigkeit	Braucht Werkzeugunterstützung	Plausibilitätsprüfungen	Verfügbarkeit von Werkzeugen	IEC-Norm
Vorhersage der Ausfallrate	Nein	Ja	Ja	Nein	Nein	Nein	Ind.	Ja	Niedrig	Hoch	Mittel	Ja	Hoch	IEC 61709
Fehlzustandsbaumanalyse	Ja	Ja	Ja	Ja	Nein	Nein	Ded.	Ja	Mittel	Hoch	Mittel	Ja	Hoch	IEC 61025
Ereignisbaumanalyse	NE	NE	Ja	NE	Ja	Ja	Ind.	NE	Hoch	Mittel	Mittel	Ja	Mittel	–
Zuverlässigkeitsblockdiagrammanalyse	NE	NE	Ja	Ja	Nein	Nein	Ded.	Ja	Niedrig	Mittel	Mittel	Ja	Mittel	IEC 61078
Markoffanalyse	Ja	Ja	Ja	Ja	Ja	Ja	Ded.	Ja	Hoch	Mittel	Hoch	Nein	Mittel	IEC 61165
Petri-Netz-Analyse	Ja	Ja	Ja	Ja	Ja	Ja	Ded.	Ja	Hoch	Niedrig	Hoch	Nein	Niedrig	–
Fehlzustandsart- und -auswirkungsanalyse (FMEA)	NE	NE	Ja	Nein	Nein	Nein	Ind.	NE	Niedrig	Hoch	Niedrig	Ja	Hoch	IEC 60812
PAAG/HAZOP-Untersuchungen	Ja	Ja	Nein	Nein	Nein	Nein	Ind.	Nein	Niedrig	Mittel	Niedrig	Ja	Mittel	IEC 61882
Analyse der menschlichen Zuverlässigkeit	Ja	Ja	Ja	Ja	Ja	Ja	Ind.	Nein	Hoch	Hoch	Mittel	Ja	Mittel	–
Beanspruchungsanalyse	NA	NA	Ja	NA	NA	Nein	NA	Nein	Hoch	Mittel	Hoch	Ja	Mittel	–
Wahrheitstabelle	Nein	Ja	Ja	Ja	Nein	Nein	NA	Ja	Hoch	Mittel	Hoch	Nein	Niedrig	–
statistische Zuverlässigkeitsverfahren	Ja	Ja	Ja	Ja	Ja	Ja	NA	NE	Hoch	Mittel	Hoch	Nein	Niedrig	IEC 60300-3-5
<p>NE Nicht empfohlen: kann für einfache Systeme verwendet werden, als alleiniges Verfahren nicht empfohlen, ist gemeinsam mit anderen Verfahren zu benutzen.</p> <p>Ded. Deduktiv: von oben nach unten.</p> <p>Ind. Induktiv: von unten nach oben.</p> <p>NA Nicht anwendbar: Dieses Kriterium ist für dieses Verfahren nicht anwendbar.</p>														

## Anhang A (informativ)

### Kurzbeschreibung der Analyseverfahren

#### A.1 Primäre Verfahren zur Analyse der Zuverlässigkeit

##### A.1.1 Vorhersage der Ausfallrate

###### A.1.1.1 Beschreibung und Verwendung

Die Vorhersage der Ausfallrate ist ein Verfahren, das meist während der Konzeptions- und frühen Entwurfsphase angewendet wird, um die Geräte- und Systemausfallrate zu schätzen. Während der Fertigungsphase kann es auch zur Produktverbesserung eingesetzt werden.

Drei Hauptverfahren kommen zum Einsatz:

- Vorhersage der Ausfallrate bei Referenzbedingungen, auch als Bauelementezählverfahren bezeichnet;
- Vorhersage der Ausfallrate bei Betriebsbedingungen, auch als Beanspruchungsanalyse bezeichnet;
- Vorhersage der Ausfallrate durch Ähnlichkeitsanalysen.

Welches Verfahren zu wählen ist, hängt von dem zum Zeitpunkt der Durchführung der Zuverlässigkeitsvorhersage verfügbaren Wissen über das System ab sowie vom annehmbaren Näherungsgrad.

###### A.1.1.2 Vorhersage der Ausfallrate bei Referenzbedingungen und bei Betriebsbedingungen

In den beiden ersten Fällen muss der Untersuchende die Anzahl und Art der Bauelemente des Systems kennen. Auch muss der Untersuchende die Betriebsbedingungen kennen, für die die Vorhersage der Ausfallrate gemacht wird. Sind die Betriebsbedingungen gleich den Referenzbedingungen für die Bauelemente, so brauchen die Betriebsbedingungen nicht näher beachtet werden. Wenn jedoch die Ausfallrate für Betriebsbedingungen vorhergesagt werden soll, die sich von den Referenzbedingungen unterscheiden, so werden die spezifischen Anwendungsbedingungen (elektrisch, thermisch, Umwelt) für das Bauelement beachtet. Dabei werden für diesen Zweck entwickelte Modelle verwendet. Für genaue Vorhersagen wird eine verlässliche Ausfallratendatenbank benötigt. IEC 61709 gibt Empfehlungen, wie Ausfallraten bei so genannten „Referenzbedingungen“ in solchen Datenbanken angegeben werden können, sie enthält jedoch keine Ausfallraten an sich. Mehrere Ausfallraten-Handbücher wurden hierfür entwickelt, manche sind im Handel erhältlich. Berechnungen der Funktionsfähigkeit können jedoch zeitaufwendig sein. Softwarewerkzeuge zur Durchführung solcher Berechnungen sind daher im Handel erhältlich.

Die Vorhersage der Ausfallrate beruht auf folgenden Annahmen:

- Die Bauelemente sind logisch in Reihe geschaltet (d. h., jedes von ihnen ist für das System notwendig).
- Bauelementeausfallraten sind über die Zeit konstant.
- Bauelementeausfallraten sind voneinander unabhängig.

Diese Annahmen müssen im Hinblick auf das zu untersuchende System geprüft werden, da sie zu ungünstigen Schätzungen führen können, wenn in den höheren Ebenen der Baugruppen Redundanz vorhanden ist.

Durch die Annahme konstanter Ausfallraten wird der Rechenaufwand wesentlich vereinfacht, da die Gesamtausfallrate einfach gleich der Summe der Ausfallraten der einzelnen Teile ist. Dies bedeutet aber nicht notwendigerweise, dass die Gesamtausfallrate ein aussagekräftiges Merkmal für die Funktionsfähigkeit ist: Nicht alle Ausfälle werden die Systeme in gleicher Weise beeinflussen. Ausfälle in Diagnoseeinheiten als auch einige Fehlzustandsarten werden die Systemfunktionalität ggf. nicht beeinflussen. In diesen Fällen liefert die Gesamtausfallrate lediglich ein Maß für die Anzahl notwendiger korrektiver Instandhaltungsvorgänge, unabhängig davon, ob diese zu funktionalen Systemausfällen beitragen oder nicht.

Eine Vorhersage der Funktionsfähigkeit eines Systems wird je nach den verfügbaren Modellen für den Ausfall der einzelnen Bauelemente entsprechende Aussagen mit annehmbarer Genauigkeit liefern. Das Gleiche gilt, wenn die Vorhersage der Ausfallrate bei Betriebsbedingungen gemacht wird.

### A.1.1.3 Vorhersage der Ausfallrate durch Gleichartigkeitsanalysen

Bei einer Gleichartigkeitsanalyse werden Betriebsdaten von in Betrieb befindlichen Geräten verwendet. Anhand dieser Daten werden neu zu entwickelnde Geräte mit Vorgängermodellen verglichen, um die Zuverlässigkeit des neuen Gerätes vorherzusagen.

Vergleiche gleichartiger Geräte können für das eigentliche Gerät, für dessen Baugruppen oder Bauelemente gemacht werden. Dabei werden dieselben Betriebsdaten benutzt, jedoch unter Verwendung unterschiedlicher Algorithmen und Rechenfaktoren für die verschiedenen Elemente. Zu den zu vergleichenden Merkmalen können gehören:

- (gemessene und spezifizierte) Betriebs- und Umweltbedingungen;
- Entwurfsmerkmale;
- Entwicklungsprozess;
- Prozess zur Sicherstellung der Zuverlässigkeit;
- Fertigungsprozess;
- Instandhaltungsprozess;
- Bauelemente und Materialien.

Für jedes vorstehende Merkmal sollte eine Reihe von Untermerkmalen verglichen werden. So können beispielsweise zu den Betriebs- und Umweltbedingungen konstante Temperatur, Feuchte, Temperaturschwankungen, elektrische Leistung, Lastzyklen, mechanische Schwingungen usw. gehören. Zu den Geräteentwurfsmerkmalen können Anzahl der Bauelemente (getrennt nach den Haupt-Bauelementefamilien), Anzahl der Baugruppen, Abmessung, Gewicht, Materialien usw. gehören.

Gleichartigkeitsanalysen sollten notwendige Algorithmen oder Berechnungsverfahren umfassen, anhand derer die Gleichartigkeit quantifiziert und Unterschiede zwischen dem neu zu entwickelnden Gerät und dem Vorgängermodell bewertet werden können.

Wenn Vorgängermodelle nicht ausreichend gleichartig oder verfügbar sind, um einen Eins-zu-Eins-Vergleich mit dem neu zu entwickelnden und zu bewertenden Gerät machen zu können, werden ersatzweise Gleichartigkeitsanalysen in der Ebene der Elemente gemacht. Gleichartigkeitsanalysen sind strukturierte Vergleiche der Elemente des neu zu entwickelnden Gerätes mit gleichartigen Elementen aus einer Reihe unterschiedlicher Vorgängermodelle, für die Zuverlässigkeitsdaten verfügbar sind.

### A.1.1.4 Vorzüge

- Zeitaufwand und Kosten für die Analyse sind sehr gering, vorausgesetzt, die Referenzdaten und Modelle sind verfügbar.
- Es sind nur wenige Ausgangsinformationen und Daten erforderlich, und diese passen daher zu der Situation in der frühen Entwurfs- und Entwicklungsphase.
- Man erhält in der frühen Entwurfs- und Entwicklungsphase grundlegende Informationen zur Zuverlässigkeit der Bauelemente.
- Es kann manuell und maschinell berechnet werden.
- Nur geringe Schulung ist notwendig.

### A.1.1.5 Einschränkungen

- Die funktionale Struktur (z. B. Redundanz in unteren Ebenen) eines Systems kann nicht berücksichtigt werden, daher sind nur einfache Strukturen für das Bauelementezählverfahren geeignet.
- Die Genauigkeit der Vorhersagen kann gering sein, insbesondere für kleine Teilsysteme und Produktionsmengen. Da veröffentlichte oder gesammelte Daten aber statistischer Natur sind, werden große Lose gebraucht.
- Die Beurteilung von Fehlzuständen und Mechanismen und deren Auswirkungen ist nicht möglich.

### A.1.1.6 Normen

Die zugehörige Norm ist IEC 61709.

### A.1.1.7 Beispiel für einen integrierten Schaltkreis (aus IEC 61709)

Für einen bipolaren RAM-Speicher wird die Ausfallrate als  $\lambda_{\text{ref}} = 10^{-7} \text{ h}^{-1}$  in einer vertrauenswürdigen Datenbank bei den folgenden Referenzbedingungen in IEC 61709 angegeben.

- Referenzumgebungstemperatur:  $\theta_{\text{amb, ref}}$  von 40 °C.
- Referenzeigenerwärmung: 20 °C.

Welchen Wert hat die Ausfallrate bei der Umgebungstemperatur  $\theta_{\text{amb}} = 70 \text{ °C}$  und gleicher Eigenerwärmung?

Schritt 1: Das Ausfallratenmodell bei Betriebsbedingungen ist nach IEC 61709 gleich  $\lambda = \lambda_{\text{ref}} \times \pi_T$ .

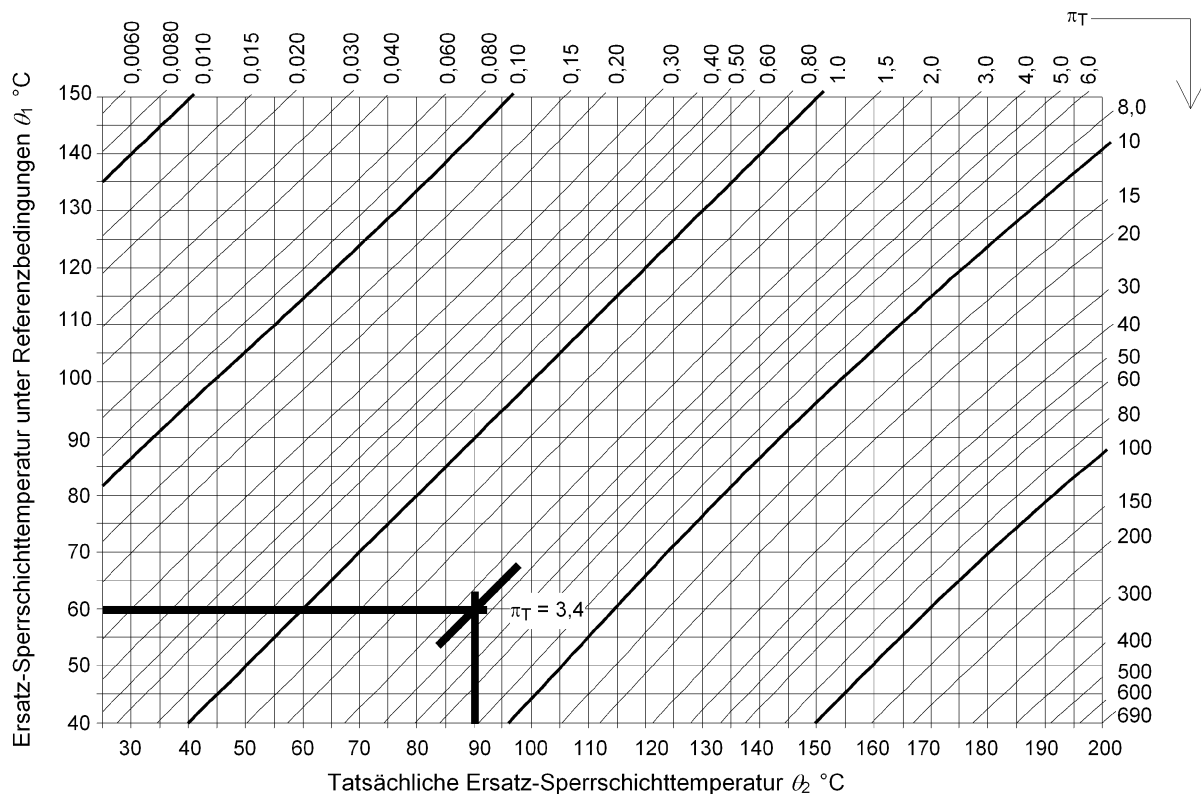
Schritt 2: Nach Bild A.1 (aus IEC 61709 entnommen) ist der Faktor für den Temperatureinfluss  $\pi_T = 3,4$

- unter Verwendung der Ersatz-Sperrschichttemperatur unter Referenzbedingungen

$$\theta_1 = \theta_{\text{amb, ref}} + \Delta T_{\text{ref}} = 40 \text{ °C} + 20 \text{ °C} = 60 \text{ °C}$$

- und der tatsächlichen Ersatz-Sperrschichttemperatur

$$\theta_2 = \theta_{\text{amb}} + \Delta T_{\text{ref}} = 70 \text{ °C} + 20 \text{ °C} = 90 \text{ °C}.$$



**Bild A.1 – Temperaturabhängigkeit der Ausfallrate**

Schritt 3: Die Ausfallrate bei  $\theta_{\text{amb}} = 70 \text{ °C}$  wird berechnet zu  $\lambda = \lambda_{\text{ref}} \times \pi_T = 10^{-7} \text{ h}^{-1} \times 3,4 = 3,4 \times 10^{-7} \text{ h}^{-1}$ .

## A.1.2 Fehlzustandsbaumanalyse

### A.1.2.1 Beschreibung und Verwendung

Die Fehlzustandsbaumanalyse (FTA) ist ein deduktives Verfahren zur Analyse der Zuverlässigkeit von Produkten. Mit ihr kann man solche Bedingungen und Faktoren erkennen und analysieren, die das Eintreten eines bestimmten, unerwünschten Ereignisses bewirken oder dazu beitragen und die die Leistung des Produktes, dessen Sicherheit, Wirtschaftlichkeit oder andere geforderte Merkmale beeinträchtigen.

Die Fehlzustandsbaumanalyse kann auch so gestaltet werden, dass mit ihr ein System-Zuverlässigkeitsvorhersagemodell gebildet werden kann und man darauf Entscheidungen über einen zu wählenden Produktentwurf basieren kann.

Wenn man sie als ein Werkzeug zum Erkennen und zur qualitativen Beurteilung von Fehlzustandsursachen verwendet, stellt die Fehlzustandsbaumanalyse ein wirksames Verfahren dar zum Erkennen und Beurteilen von Ausfallarten und Ausfallursachen von bekannten oder vermuteten Auswirkungen.

Durch die Betrachtung bekannter, unerwünschter Auswirkungen und durch das mögliche Erkennen der zugehörigen Ausfallarten und Ausfallursachen ermöglicht die Fehlzustandsbaumanalyse das rechtzeitige Mindern potentieller Ausfallarten und trägt dadurch zum Zuverlässigkeitswachstum in der Produktentwurfsphase bei.

Die Fehlzustandsbaumanalyse ist so angelegt, dass man durch sie die Hardware- und Softwarearchitektur und deren Funktionalität abbilden kann. Wenn man sie hin bis zum Grundereignis durchführt, so ergibt sich ein systematisches Verfahren zum Modellieren der Funktionsfähigkeit unter Beachtung komplexer Wechselwirkungen von Systemteilen durch das Modellieren der funktionalen Abhängigkeiten, der Ausfallabhängigkeiten, von Ereignissen, die Ausfälle ermöglichen, von Ereignissen mit gemeinsamer Ursache und durch die Abbildung von Netzen.

Damit man anhand der Fehlzustandsbaumanalyse die Systemzuverlässigkeit schätzen kann, werden z. B. Boolesche Reduktionsverfahren und Schnittmengen herangezogen. Die wichtigsten benötigten Daten sind Bauelementeausfallraten, Reparaturraten, Wahrscheinlichkeiten für das Eintreten von Fehlzustandsarten usw.

#### **A.1.2.2 Anwendung**

Die Fehlzustandsbaumanalyse kann zweifach angewendet werden: zum einen als ein Mittel zum Erkennen der Ursache eines bekannten Fehlzustandes und zum anderen zum Analysieren von Ausfallarten und zum Modellieren der Zuverlässigkeit und als Vorhersagewerkzeug.

Die Fehlzustandsbaumanalyse wird dafür verwendet, potentielle Fehlzustände, deren Arten und Ursachen und deren Beitrag zur Systemnichtverfügbarkeit im Laufe der Produktentwicklung zu untersuchen. Der Fehlzustandsbaum wird so konstruiert, dass nicht nur die Systemfunktionen, sondern auch die System-Hardware und -Software zusammen mit anderen Wechselwirkungen repräsentiert werden. Wenn Menschen Teil des Systems sind, dann kann auch menschliches Fehlverhalten in die Fehlzustandsbaumanalyse mit aufgenommen werden. Die Ereignishäufigkeiten der Ursachen von Fehlzustandsarten werden durch eine technische Analyse bestimmt. Anschließend werden darauf aufbauend der Umfang ihres Beitrages zur gesamten Funktionsunfähigkeit beurteilt und somit Abwägungen und Zuverlässigkeitswachstum ermöglicht. Dadurch wird das Modellieren der Zuverlässigkeit von gemischter Hardware, Elektronik und Mechanik sowie Software und deren Zusammenwirken ermöglicht. In dieser Anwendung wird die Fehlzustandsbaumanalyse ein leistungsfähiges Werkzeug zur Analyse der Funktionsfähigkeit.

#### **A.1.2.3 Schlüsselemente**

Die Schlüsselemente eines Fehlzustandsbaumes sind

- Gatter und Ereignisse,
- Schnittmengen.

Gatter repräsentieren die Ausgaben und Ereignisse repräsentieren die Eingaben in die Gatter. Die symbolische Darstellung einiger spezieller Gatter können in der Fachliteratur oder in der Analysesoftware unterschiedlich sein; jedoch ist die Darstellung der Basisgatter ziemlich universell.

Schnittmengen sind Gruppen von Ereignissen, die, wenn sie alle eintreffen würden, einen Systemausfall bewirken würden. Eine minimale Schnittmenge enthält die Mindestanzahl von Ereignissen, die für einen Ausfall erforderlich ist. Das Entfernen eines Ereignisses würde dazu führen, dass das System nicht mehr ausfällt.

#### **A.1.2.4 Vorzüge**

- Die FTA kann in frühen Stufen eines Entwurfs vorbereitet und später parallel zur Systementwicklung im Detail weiterentwickelt werden.
- Sie erkennt und zeichnet systematisch mittels Boolescher Algebra die logischen Fehlzustandspfade von einem speziellen Ereignis zurück zu der Primärursache auf.

- Sie erlaubt eine leichte Umwandlung von logischen Modellen in entsprechende Wahrscheinlichkeitsgrößen.

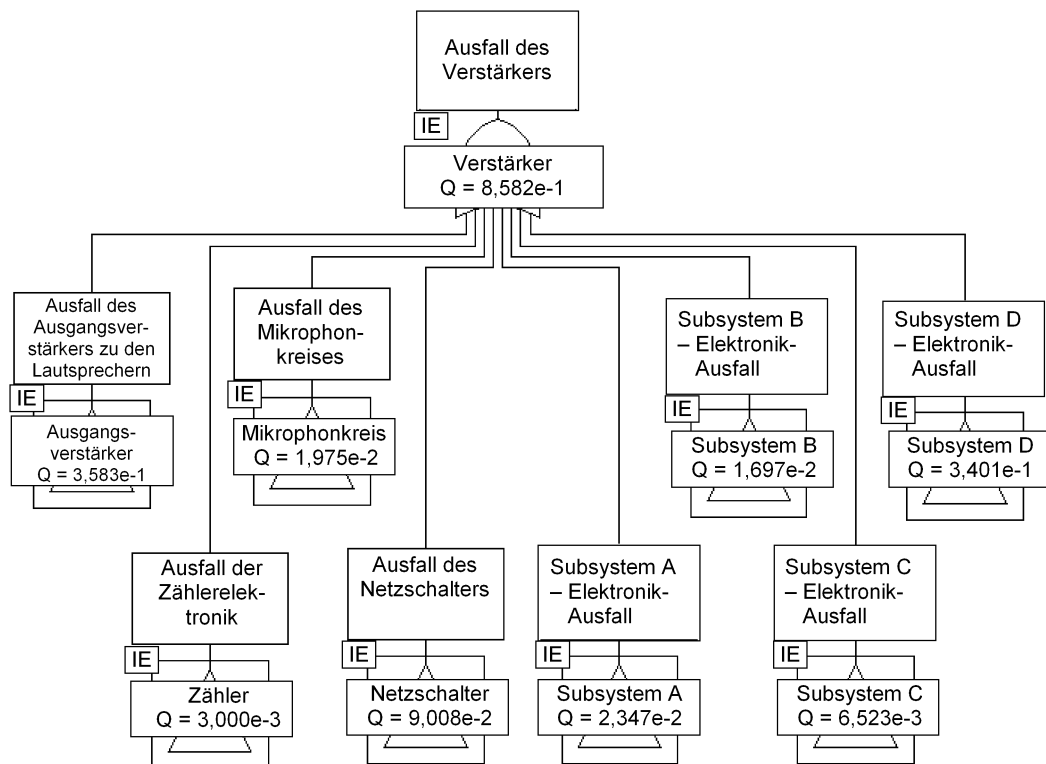
#### A.1.2.5 Einschränkungen

- Mit der Fehlzustandsbaumanalyse können Abhängigkeiten von Ereignissen, die zeit- oder abfolgeabhängig sind, nicht korrekt dargestellt werden.
- Bei Rekonfiguration oder bei zustandsabhängigem Verhalten von Systemen ist die Fehlzustandsbaumanalyse nur eingeschränkt anwendbar.

Diese Einschränkungen können kompensiert werden durch eine Kombination der Fehlzustandsbaumanalyse mit Markoff-Modellen. Dabei werden die Markoff-Modelle als Grundereignis in Fehlzustandsbäumen genommen.

#### A.1.2.6 Beispiel

Darstellung eines Fehlzustandsbaums in der höchsten Systemebene für einen Tonverstärker: Die wichtigsten Teilsysteme sind die Eingangsgatter zum Spitzengatter und dem Verstärkersystem.



**Bild A.2 – Fehlzustandsbaum für einen Tonverstärker**

Es ergab sich, dass der in Bild A.3 dargestellte Teilbaum den größten Beitrag liefert.

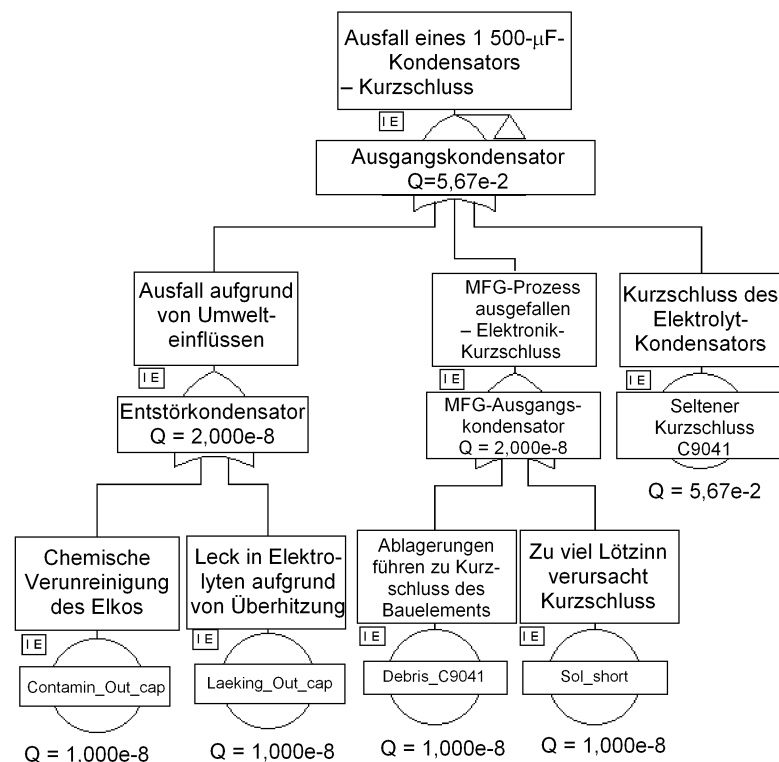


Bild A.3 – Teilbaum der Fehlzustandsbaumanalyse in Bild A.2

Die folgenden Schaltzeichen gemäß Tabelle A.1 werden zur Darstellung des Fehlzustandsbaumes verwendet.

Tabelle A.1 – Symbole für die Darstellung im Fehlzustandsbaum

FTA-Symbol	Symbolname	Beschreibung
	Hauptereignis oder Zwischenereignis	Haupt- oder Zwischenereignis, welches den Systemausfall, den Teilsystemausfall oder einen Ausfall in einer höheren Ebene als der Ebene des Grundereignisses beschreibt
	Grundereignis	Grundereignis, für das Information zur Funktionsfähigkeit vorliegt
	Nicht weiter untersuchtes Ereignis	Teil des Systems, das noch nicht weiter untersucht wurde bzw. noch definiert werden muss
	Verweisungs-gatter	Dieses Gatter zeigt an, dass dieser Teil des Systems in einem anderen Teil oder einer anderen Seite des Diagramms weiter entwickelt wird
	ODER-Gatter	Ereignis tritt ein, wenn eines der Eingangsereignisse eintritt, entweder allein oder mit anderen zusammen
	UND-Gatter	Ereignis tritt nur dann ein, wenn alle Eingangsereignisse gleichzeitig eintreten

Ziel dieser Analyse war, die wahrscheinlichste Ursache für den Ausfall des Verstärkers zu finden. Es scheint, dass der Elektrolyt-Kondensator am Verstärkerausgang zum Lautsprecher am meisten zum Ausfall des Ver-

stärkers beiträgt. Mit hoher Wahrscheinlichkeit wird ein Kurzschluss dieses Kondensators aufgrund dessen inhärenter Ausfallrate eintreten. Dies rührt daher, dass ursprünglich ein Kondensator mit niedriger Nennspannung aufgrund dessen geringerer Abmessungen gewählt worden war; damit betrug die Leistungsherabsetzung dieses Kondensators 90 %, wenn nur die Gleichspannung berücksichtigt wird. Stromwelligkeit war nur eine zusätzliche Ursache für einen Kondensatorausfall.

Beide Ursachen erhöhten um eine Größenordnung die ursprüngliche Ausfallrate dieses Kondensators, da die Kapazität dieses Elektrolyt-Kondensators (1500  $\mu$ F) selbst bei größerer Leistungsherabsetzung nicht gering ist. Der Kondensator wurde durch einen Typ mit passender Nennspannung ersetzt, und da dieser sechsmal in der Schaltung verwendet wird, hat der Austausch die Gesamtwahrscheinlichkeit für den Ausfall des Tonverstärkers für seine vorbestimmte Lebensdauer um mehr als 20 % reduziert. Das Ergebnis dieser Minderung der Ursache für diese Ausfallart ist eine Verbesserung der Systemfunktionsfähigkeit.

In diesem Fall stellt die Systemnichtverfügbarkeit  $Q$ , berechnet für die gegebene Betriebsdauer, auch die Wahrscheinlichkeit für den Ausfall des Systems  $F(t)$  dar, da die Reparaturdauer nicht berücksichtigt wurde.

Die Gatter in obigem Beispiel sind Standardzeichen, ausgenommen diejenigen, die die Teilsysteme darstellen. Dort steht das Dreieck für ein Verweisungs-gatter und bedeutet, dass die Gatter später entwickelt wurden, und das Viereck um sie herum bedeutet, dass jedes von ihnen auf einer eigenen Seite gezeigt wird.

### A.1.3 Ereignisbaumanalyse (ETA)

#### A.1.3.1 Beschreibung und Verwendung

Der Ereignisbaum behandelt eine Reihe möglicher Folgen eines Startereignisses oder eines Systemausfalls. Somit kann der Ereignisbaum sehr effizient mit einem Fehlzustandsbaum kombiniert werden. Die Wurzel eines Ereignisbaumes kann man als das Hauptereignis eines Fehlzustandsbaumes ansehen. Diese Kombination wird manchmal als Ursache-Folgen-Analyse bezeichnet, bei der die Fehlzustandsbaumanalyse zum Analysieren der Ursachen und die Ereignisbaumanalyse zum Analysieren der Folgen eines Startereignisses benutzt werden. Um die Schwere gewisser Folgen, die dem Startereignis folgen, beurteilen zu können, sollten alle möglichen Wege und Richtungen von Folgen ermittelt und deren Wahrscheinlichkeit bestimmt werden.

#### A.1.3.2 Anwendung

Die Ereignisbaumanalyse wird eingesetzt, wenn es darum geht, alle möglichen Pfade von Folgeereignissen, ihre Reihenfolge und das/die wahrscheinlichste Ergebnis/Folge des Startereignisses zu untersuchen. Nach einem Startereignis gibt es mehrere erste nachfolgende Ereignisse/Folgen, die sich ergeben können. Die Ereignishäufigkeit eines speziellen Pfades (Abfolge von Ereignissen) ist gleich dem Produkt der bedingten Wahrscheinlichkeiten aller Ereignisse in diesem Pfad.

#### A.1.3.3 Schlüsselemente

Die Schlüsselemente in der Anwendung einer Ereignisbaumanalyse sind der Auslöser (Startereignis), nachfolgende Ereignisse und Folgen.

#### A.1.3.4 Vorzüge

Der Hauptvorteil eines Ereignisbaumes ist die Möglichkeit, die Folgen eines Ereignisses zu beurteilen; dadurch ermöglicht dieses Verfahren die mögliche Minderung einer höchst wahrscheinlichen, aber nachteiligen Folge. Die Ereignisbaumanalyse wird daher vorteilhaft als Ergänzung zur Fehlzustandsbaumanalyse durchgeführt. Die Ereignisbaumanalyse kann auch als Werkzeug bei der Fehlzustandsbaumanalyse verwendet werden. Wenn man von unten in Richtung nach oben beginnt, so folgt die Analyse den möglichen Pfaden eines Ereignisses (eine Ausfallart), um die wahrscheinlichen Folgen eines Ausfalls zu bestimmen.

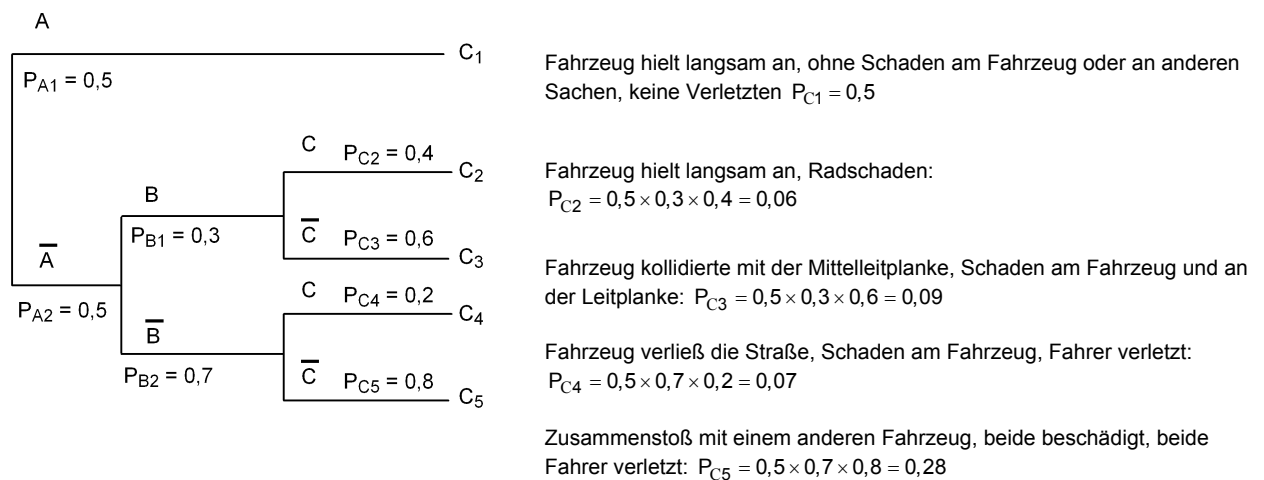
#### A.1.3.5 Einschränkungen

Hinsichtlich der korrekten Behandlung bedingter Wahrscheinlichkeiten muss besonders sorgfältig vorgegangen werden, ebenso hinsichtlich der Unabhängigkeit von Ereignissen im Baum.



### A.1.3.6 Beispiel

Ein Beispiel eines einfachen Ereignisbaumes ist im folgenden Bild A.4 enthalten. In diesem Beispiel wird das Ergebnis eines einfachen Ereignisses beurteilt; man schaut nach mehreren möglichen Folgen des Ausfalls eines Fahrzeugreifens.



#### Legende

A = Kein Sachschaden, keine Verletzten

B = Sachschaden, keine Verletzten

C = Nur Schaden am Fahrzeug, keine sonstigen Sachen beschädigt

**Bild A.4 – Ereignisbaum**

## A.1.4 Zuverlässigkeitsblockdiagrammanalyse

### A.1.4.1 Beschreibung und Verwendung

Die Zuverlässigkeitsblockdiagrammanalyse ist ein Systemanalyseverfahren. Ein Zuverlässigkeitsblockdiagramm ist die graphische Darstellung der logischen Struktur des Systems durch dessen Teilsysteme und Komponenten. Damit kann man die Erfolgspfade des Systems durch die logische Verbindung der Blöcke (Teilsysteme/Komponenten) repräsentieren.

### A.1.4.2 Anwendung

Blockdiagramme gehören zu den ersten Aufgaben, die während einer Produktdefinition erledigt werden. Sie sollten als Teil der anfänglichen Konzeptentwicklung konstruiert werden. Des Weiteren sollten sie begonnen werden, sobald das Programm definiert ist, später als Teil der Analyse der Anforderungen vervollständigt und dann fortlaufend weiter detailliert werden, je nachdem wie die Daten verfügbar werden, um auf den so gewonnenen Ergebnissen aufbauend Entscheidungen abzuwägen.

### A.1.4.3 Schlüsselemente

Um ein Zuverlässigkeitsblockdiagramm zu konstruieren, können verschiedene qualitative Analysetechniken eingesetzt werden.

- Erarbeitung der Definition der erfolgreichen Erfüllung der Systemfunktion.
- Zerlegung des Systems in für die Zuverlässigkeitsanalyse geeignete funktionale Blöcke. Einige Blöcke können dabei Teilstrukturen des Systems repräsentieren, die wiederum durch andere Zuverlässigkeitsblockdiagramme dargestellt sein können (Systemreduktion).
- Durchführung qualitativer Analysen; für die quantitative Beurteilung eines Zuverlässigkeitsblockdiagramms stehen verschiedene Verfahren zur Verfügung. Je nach Struktur (reduzierbar oder nicht reduzierbar) können zur Vorhersage der Zuverlässigkeitskenngrößen einfache Boolesche Techniken, Wahrheitstabellen sowie Pfad- und Schnittmengenanalysen eingesetzt werden; diese Kenngrößen werden aus den Basiskomponentendaten berechnet.

### A.1.4.4 Vorzüge

- Das Zuverlässigkeitsblockdiagramm wird meist direkt aus dem funktionalen Systemdiagramm konstruiert; dies hat den weiteren Vorteil, dass weniger Konstruktionsfehler begangen werden, sowie den

Vorteil des systematischen Aufzeigens von für die Systemzuverlässigkeit belangvollen funktionalen Pfaden.

- Es behandelt die meisten Arten von Systemkonfigurationen einschließlich paralleler, redundanter, in Bereitschaft befindlicher und alternativer funktionaler Pfade.
- Es erlaubt es, komplette Variationen zu analysieren und Änderungen in den Systemleistungsparametern abzuwägen.
- Es lässt (in der Anwendung mit zwei Zuständen) eine ziemlich leichte Manipulation von funktionalen (oder nicht funktionalen) Pfaden zu, woraus sich minimale logische Modelle (z. B. durch Boolesche Algebra) ergeben.
- Es erlaubt es, durch eine Empfindlichkeitsanalyse diejenigen Einheiten aufzuzeigen, die hauptsächlich zur Gesamtsystemzuverlässigkeit beitragen.
- Es erlaubt es, Modelle für die Beurteilung der Gesamtsystemzuverlässigkeit durch Angabe von Wahrscheinlichkeiten aufzustellen.
- Es resultiert in kompakten und bündigen Diagrammen für das Gesamtsystem.

#### A.1.4.5 Einschränkungen

- Mit der Zuverlässigkeitsblockdiagrammanalyse alleine kann keine spezielle Fehlzustandsanalyse gemacht werden – d. h., die Ursachen-Folge(n)-Pfade oder die Folge-Ursache(n)-Pfade werden nicht besonders hervorgehoben.
- Es erfordert ein Wahrscheinlichkeitsmodell der Leistung jedes Elementes im Diagramm.
- Mit ihm können keine ungewollten oder unbeabsichtigten Ausgaben aufgezeigt werden, außer der Untersuchende unternimmt bewusst dahingehende Schritte.
- Ist in erster Linie auf die Erfolgsanalyse ausgerichtet und kann nicht wirksam komplexe Reparatur- und Instandhaltungsstrategien oder allgemeine Verfügbarkeitsanalysen behandeln.
- Ist im Allgemeinen auf nicht-reparierbare Systeme beschränkt.

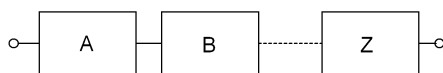
#### A.1.4.6 Normen

Die zugehörige Norm ist IEC 61078.

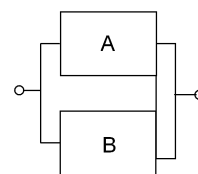
#### A.1.4.7 Beispiel

Elementare Modelle (alle Blöcke sollten voneinander unabhängig sein) sind in Bild A.5 gezeigt.

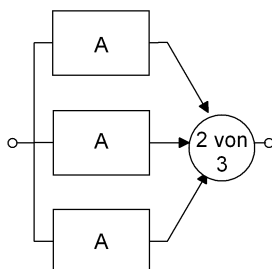
seriell (in Reihe)



parallel (aktiv)

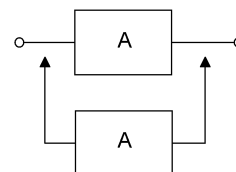


Modell m von n



in Bereitschaft

(kalte Bereitschaft)



**Bild A.5 – Elementare Modelle**

Komplexere Modelle, bei denen derselbe Block mehrfach im Diagramm erscheint, können durch

- das Theorem von der totalen Wahrscheinlichkeit,
- Boolesche Wahrheitstabellen

bewertet werden.

## **A.1.5 Markoffanalyse**

### **A.1.5.1 Beschreibung und Verwendung**

Das Markoffverfahren ist eine probabilistische Methode, mit der die statistische Abhängigkeit der Ausfall- oder Reparatüreigenschaften individueller Komponenten von dem Zustand des Systems modelliert werden kann. Mit der Modellierung nach Markoff kann man sowohl die Auswirkungen von Reihenfolge-abhängigen Komponentenausfällen und sich aufgrund von Beanspruchung oder anderer Faktoren ändernden Übergangsraten erfassen. Aus diesem Grunde ist die Markoffanalyse ein für die Beurteilung der Zuverlässigkeit von funktional komplexen Systemstrukturen und komplexen Reparatur- und Instandsetzungsstrategien passendes Verfahren.

Das Verfahren beruht auf der Theorie der Markoffschen Ketten. Für Zuverlässigkeitsanwendungen ist das zeitlich homogene Markoffmodell das übliche Referenzmodell; dies erfordert konstante Übergangsraten (Ausfall und Reparatur). Auf Kosten eines vergrößerten Zustandsraumes können auch nicht-exponentielle Übergänge mittels einer Reihe exponentieller Übergänge angenähert werden. Für dieses Verfahren sind allgemeine und effiziente numerische Lösungstechniken verfügbar, und die einzige Beschränkung seiner Anwendung ist die Größe des Zustandsraumes.

Die Darstellung des Systemverhaltens durch ein Markoffmodell erfordert die Bestimmung aller möglichen Systemzustände; diese werden vorzugsweise in Zustandsdiagrammen gezeigt. Des Weiteren müssen die (konstanten) Übergangsraten von einem Zustand in einen anderen (Komponentenausfallraten oder Reparaturraten, Ereignisraten usw.) angegeben werden. Typische Ausgaben eines Markoffmodells sind die Wahrscheinlichkeiten, dass man sich in einer gegebenen Menge von Zuständen befindet (typischerweise ist diese Wahrscheinlichkeit gleich der Maßgröße für die Verfügbarkeit).

### **A.1.5.2 Anwendung**

Das richtige Anwendungsgebiet dieser Technik ist dann gegeben, wenn die Übergangsraten (Ausfall oder Reparatur) von dem Zustand des Systems oder von der Belastung, der Beanspruchung, der Systemstruktur (z. B. in Bereitschaft), der Instandhaltungspolitik oder anderen Faktoren abhängen. Insbesondere die Systemstruktur („kalte“ oder „heiße“ Bereitschaft, Ersatzteile) und die Instandhaltungspolitik (ein oder mehrere Reparaturtrupps) verursachen Abhängigkeiten, die von anderen, weniger rechenaufwendigen Techniken nicht erfasst werden können.

Typische Anwendungen sind Zuverlässigkeitsvorhersagen.

### **A.1.5.3 Schlüsselemente**

Zu den wichtigsten Schritten bei der Anwendung des Verfahrens gehören:

- Definition des Zustandsraums des Systems;
- Zuweisung von (zeitlich unabhängigen) Übergangsraten zwischen den Zuständen;
- Festlegung der auszugebenden Maßgrößen (Zustände, die zu einem Systemausfall führen, gruppieren);
- das mathematische Modell (Übergangsratenmatrix) generieren und die Markoffmodelle mittels eines geeigneten Softwarepaketes lösen;
- Analyse der Ergebnisse.

### **A.1.5.4 Vorzüge**

Die Anwendung dieser Methodik hat folgende Vorzüge:

- Es ist ein flexibles probabilistisches Modell zur Analyse des Systemverhaltens.
- Das Verfahren kann an komplexe redundante Konfigurationen, komplexe Instandhaltungsvorgaben, komplexe Modelle zur Behandlung von Fehlzuständen (intermittierende Fehlzustände, latente Fehlzustände, Rekonfiguration) angepasst werden, und es kann Betriebsarten verminderter Leistung und Ausfälle mit gemeinsamer Ursache behandeln.

- Das Verfahren liefert probabilistische Lösungen für Module, die in andere Modelle wie z. B. Blockdiagramme und Fehlzustandsbäume eingebaut werden sollen.
- Ereignisabfolgen mit einem speziellen Muster oder Eintrittsreihenfolge können sehr genau modelliert werden.

#### A.1.5.5 Einschränkungen

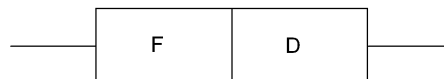
- Mit Zunahme der Anzahl der Systemkomponenten wächst die Anzahl der Zustände exponentiell und führt zu intensiver Analysearbeit.
- Für den Anwender kann es schwierig sein, das Modell zu konstruieren und zu verifizieren, und man benötigt eine spezielle Analysesoftware.
- Numerische Lösungsschritte sind nur bei konstanten Übergangsraten verfügbar.
- Besondere Maßgrößen, wie mittlere Dauer bis zum Ausfall (MTTF) und mittlere Dauer bis zur Wiederherstellung (MTTR), werden nicht unmittelbar durch die Standardlösung des Markoffmodells erhalten; um diese muss man sich gesondert bemühen.

#### A.1.5.6 Normen

Die zugehörige Norm ist IEC 61165.

#### A.1.5.7 Beispiel

Ein elektronisches Gerät (oder Einheit) enthält einen funktionalen Teil (F) und einen diagnostischen Teil (D) (siehe Bild A.6). Unter „Diagnoseeinrichtungen“ versteht man solche Teile des Systems, die Überwachungs- und Anzeigefunktionen ausführen, dies kann durch Hardware, Software, Firmware oder andere Mittel erfolgen; diese Teile sind so genannte Überwachungsteile.



**Bild A.6 – Beispiel einer Einheit**

Es gelten die folgenden Begriffe:

#### **Alarmfehler**

aufgrund eines Fehlzustandes in dem Diagnoseteil kann kein Alarm ausgelöst werden

#### **Unklarzustand (en: downstate)**

Fehlzustand einer Einheit, oder Funktionsunfähigkeit einer Einheit während der Wartung

#### **falscher Alarm**

von einer eingebauten Prüfeinrichtung oder sonstigen Überwachungsschaltkreisen angezeigter Fehlzustand, obwohl kein funktionaler Fehlzustand vorliegt

#### **Fehlzustandsart**

einer der möglichen Fehlzustände bezüglich einer geforderten Funktion einer fehlerhaften Einheit

#### **Fehlzustandserkennungsgrad**

Anteil der Fehlzustände einer Einheit, die unter gegebenen Bedingungen erkannt werden können

#### **Fehlzustandsdiagnose**

Tätigkeiten zur Fehlzustandserkennung, Fehlzustandslokalisierung und Ursachenfeststellung

#### **latenter Fehlzustand**

Fehlzustand, der noch nicht erkannt worden ist

#### **Klarzustand (en: upstate)**

Zustand, in dem die Einheit funktionsfähig ist, sofern erforderliche externe Mittel verfügbar sind

Zuverlässigkeitsmodelle bedienen sich üblicherweise Vereinfachungen: In einem Blockdiagramm hat jeder funktionale Block zwei Zustände. Der eine Zustand bedeutet betriebsfähiger Zustand (Klarzustand) und der andere bedeutet Fehlzustand (Unklarzustand). Solch ein Zwei-Zustands-Modell vereinfacht eine Zuverlässigkeitsanalyse erheblich. Aber manchmal ist es nicht geeignet, in zutreffender Weise zu beschreiben, was in der wirklichen Welt geschieht, in der jeder funktionale Block einen funktionalen Teil (F) und einen

diagnostischen Teil (D) haben muss und beide Teile ausfallen können. Die Modellierung nach Markoff erlaubt es, auch solche Fälle zu behandeln.

Die Anwendung der Markoffanalyse erfordert zuerst die Definition des Zustandsraumes des Systems. Tabelle A.2 und Tabelle A.3 zeigen die Zustände einer realen Einheit und die Auswirkungen von Ausfällen in den Zuständen F und D.

**Tabelle A.2 – Zustände der Einheit**

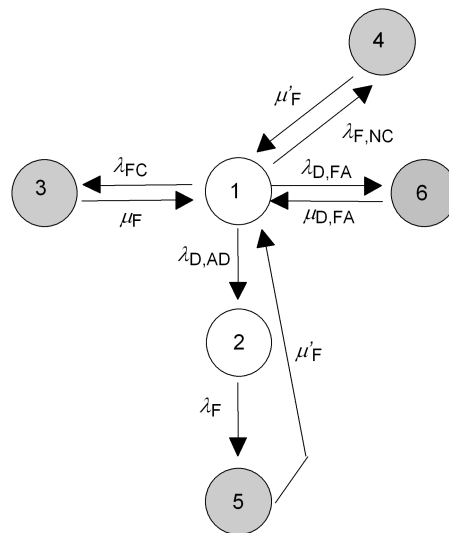
Zustand	Definition
1	Korrektter Betrieb
2	Diagnostischer Fehlzustand im Alarmfehlermodus
3	Von der Diagnoseeinrichtung erkannter funktionaler Fehlzustand
4	Von der Diagnoseeinrichtung nicht erkannter funktionaler Fehlzustand (nicht erkennbar)
5	Von der Diagnoseeinrichtung nicht erkannter funktionaler Fehlzustand, da diese in den Alarmfehlermodus ausgefallen ist
6	Diagnostischer Fehlzustand in falschem Alarmmodus

**Tabelle A.3 – Auswirkungen von Ausfällen in funktionalen und diagnostischen Teilen**

Zustand von F	Zustand von D	Zustand	Auswirkungen
In Betrieb	In Betrieb	1	Korrektter Betrieb (Zustand 1)
In Betrieb	Fehlzustand im Modus Falscher Alarm	6	Alarm ausgelöst. F ist im Klarzustand, bis das Instandhaltungspersonal eine Reparatur unternimmt. Falls F nicht redundant ist, lässt das System im Allgemeinen F so lange in Betrieb (Zustand 6), bis die Reparatur ausgeführt wird.
	Fehlzustand im Modus Alarmfehler	2	Kein Alarm ausgelöst. Der F-Teil ist im Klarzustand (Zustand 2), bis er ausfällt (Zustand 5).
Fehlzustand	In Betrieb	3	Alarm ausgelöst. Korrekte Erkennung des Fehlzustandes (Zustand 3).
Fehlzustand	Fehlzustand	5	Abfolge der Ereignisse, um in diesen Zustand zu gelangen: Diagnostischer Fehlzustand (Modus Alarmfehler), Teilsystem geht in Zustand 2. Funktionaler Fehlzustand; kein Alarm ausgelöst (Zustand 5).
Fehlzustand	Fehlt	4	Nicht erkennbarer Fehlzustand (Zustand 4)

Bild A.7 zeigt das zugehörige Übergangsratendiagramm. Es wird zugelassen, dass

- der funktionale Teil durch die Diagnoseeinrichtung nicht erfasst wird: Dies bedeutet, dass ein Ausfall im funktionalen Teil nicht erkannt werden könnte (Zustand 4),
- die Diagnoseeinrichtungen keinen Alarm auslösen, wenn sie dies nicht tun sollen (Zustand 6), oder keinen Alarm auslösen, wenn sie dies tun sollen (Zustand 2 und 5).



ANMERKUNG Weiße eingekreiste Zustände sind Klarzustände, graue unterlegte Zustände sind Unklarzustände.

**Bild A.7 – Zustands-Übergangsdiagramm**

Die (Zeit-unabhängigen) Übergangsraten zwischen den Zuständen sind in Tabelle A.4 gezeigt.

**Tabelle A.4 – Übergangsraten**

$\lambda_F$	Ausfallrate von F, dem funktionalen Teil
$\lambda_{F,C}$	Erfasste Ausfallrate von F (Ausfälle erkennbar durch Diagnoseeinrichtungen)
$\lambda_{F,NC}$	Nicht erfasste Ausfallrate von F (merke, dass $\lambda_F = \lambda_{F,C} + \lambda_{F,NC}$ )
$\lambda_{D,AD}$	Ausfallrate von D im Modus Alarmfehler
$\lambda_{D,FA}$	Ausfallrate von D im Modus falscher Alarm (merke, dass $\lambda_D = \lambda_{D,AD} + \lambda_{D,FA}$ )
$\mu_F$	Reparaturrate nach einem erfassten Fehlzustand
$\mu'_F$	Reparaturrate nach einem nicht erfassten Fehlzustand
$\mu_{D,FA}$	Reparaturrate nach einem Fehlzustand im Modus falscher Alarm

Nachdem das Zustandsdiagramm und die Übergangsraten festgelegt worden sind, kann die Verfügbarkeit mit Hilfe eines geeigneten Softwarepaketes berechnet werden. Auch ist es sehr leicht, eine parametrische Analyse durchzuführen, mit der man Variationen der Übergangsraten durchspielen kann.

## A.1.6 Petri-Netz-Analyse

### A.1.6.1 Beschreibung und Verwendung

Petri-Netze sind ein graphisches Werkzeug zur Darstellung und Analyse von komplexen logischen Wechselwirkungen zwischen den Komponenten oder Ereignissen in einem System. Typische komplexe Wechselwirkungen, die auf natürliche Weise in der Petri-Netz-Sprache enthalten sind, sind Übereinstimmung, Konflikt, Synchronisation, wechselseitiger Ausschluss und Begrenzung der Hilfsmittel.

Die statische Struktur des modellierten Systems wird durch einen Petri-Netz-Graphen dargestellt. Der Petri-Netz-Graph setzt sich aus drei einfachen Elementen zusammen:

- Plätze (üblicherweise als Kreise gezeichnet) stellen die Zustände dar, in denen das System angetroffen werden kann;
- Transitionen (üblicherweise als Balken gezeichnet) stellen die Ereignisse dar, die einen Zustand in einen anderen ändern können;
- Bögen (als Pfeile gezeichnet) verbinden Plätze mit Transitionen und Transitionen mit Plätzen und stellen die logisch zulässigen Verbindungen zwischen Zuständen und Ereignissen dar.

Ein Zustand ist in einer gegebenen Situation gültig, wenn der zugehörige Platz markiert ist, d. h., er enthält wenigstens ein Token • (gezeichnet als schwarzer Punkt). Das dynamische Verhalten des Systems wird durch die Bewegung der Token in dem Graphen dargestellt. Eine Transition ist bereit, wenn ihr Eingabepplatz wenigstens ein Token enthält. Eine bereit Transition kann schalten, und das Schalten der Transition entfernt

ein Token von jedem Eingabeplatz und legt ein Token in jeden Ausgabeplatz. Die Verteilung der Token auf die Plätze wird Markierung genannt. Von einer Anfangsmarkierung beginnend, produziert die Anwendung der Bereitschafts- und Schaltregeln alle erreichbaren Markierungen, genannt die Erreichbarkeitsmenge der Petri-Netze. Die Erreichbarkeitsmenge enthält alle Zustände, die das System von einem Ausgangszustand ausgehend erreichen kann.

In Standard-Petri-Netzen wird die Zeit nicht angegeben. Es sind jedoch viele Erweiterungen erschienen, in denen dem Petri-Netz Zeitelemente aufgestülpt wurden. Wenn jeder Transition eine (konstante) Schaltrate zugewiesen wird, kann das dynamische Verhalten der Petri-Netze mittels einer zeitlich kontinuierlichen Markoffschen Kette analysiert werden, deren Zustandsraum mit der Erreichbarkeitsmenge des zugehörigen Petri-Netzes isomorph ist.

Petri-Netze können als eine Hochsprache zur Generierung von Markoffmodellen verwendet werden. Mehrere Werkzeuge zur Zuverlässigkeitsanalyse beruhen auf dieser Methodik.

Petri-Netze sind auch eine natürliche Simulationsumgebung.

#### **A.1.6.2 Anwendung**

Die Verwendung von Petri-Netzen wird dann empfohlen, wenn komplexe logische Wechselwirkungen berücksichtigt werden sollen (Übereinstimmung, Konflikt, Synchronisation, wechselseitiger Ausschluss und Begrenzung der Hilfsmittel). Außerdem sind Petri-Netze oft eine einfachere und natürlichere Sprache zur Beschreibung eines Markoffmodells.

#### **A.1.6.3 Schlüsselemente**

Das Schlüsselement der Petri-Netz-Analyse ist eine Beschreibung der Systemstruktur und ihres dynamischen Verhaltens mittels einfacher Elemente (Plätze, Transitionen, Bögen und Token) der Petri-Netz-Sprache; dieser Schritt erfordert den Einsatz von Ad-hoc-Software-Werkzeugen:

- a) Strukturelle qualitative Analyse;
- b) Quantitative Analyse: Falls den Transitionen im Petri-Netz konstante Schaltraten zugewiesen sind, kann die quantitative Analyse durch die numerische Lösung des entsprechenden Markoffmodells erfolgen, andernfalls bleibt als brauchbare Technik nur Simulation übrig.

#### **A.1.6.4 Vorzüge**

Petri-Netze sind geeignet zur Darstellung von komplexen Wechselwirkungen von Hardware- oder Software-Modulen, die nicht durch andere Techniken leicht modellierbar sind.

Petri-Netze sind ein gangbarer Weg zur Generierung von Markoffmodellen. Gewöhnlich erfordert die Beschreibung eines Systems durch ein Petri-Netz sehr viel weniger Elemente als bei einer entsprechenden Markoff-Darstellung.

Das Markoffmodell wird automatisch aus der Petri-Netz-Darstellung heraus generiert; dabei bleibt die Komplexität des analytischen Lösungsverfahrens dem Modellierer verborgen, der lediglich in der Ebene des Petri-Netzes eingreift.

Zusätzlich ermöglichen Petri-Netze eine qualitative Strukturanalyse, die lediglich auf den Eigenschaften des Graphen beruht. Diese Strukturanalyse ist im Allgemeinen weniger aufwendig als das Markoffmodell und liefert Informationen, die für die Validierung der Folgerichtigkeit des Modells nützlich sind.

#### **A.1.6.5 Einschränkungen**

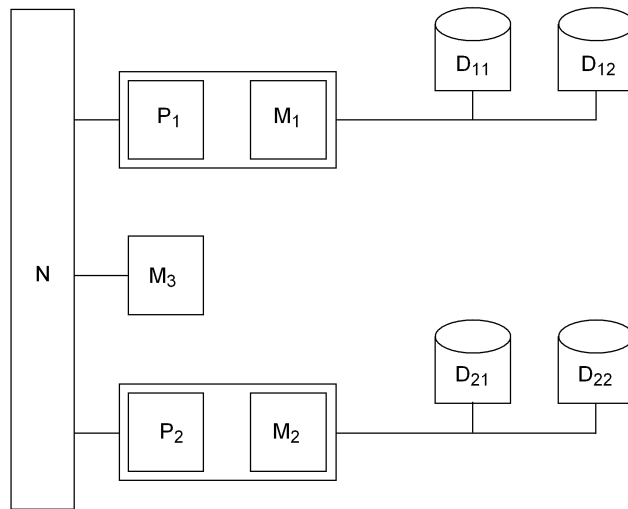
Da die quantitative Analyse auf der Generierung und Lösung des entsprechenden Markoffmodells beruht, werden auch die meisten für die Markoffanalyse geltenden Einschränkungen geteilt.

Die Methodik der Petri-Netze erfordert den Einsatz von Software-Werkzeugen (mehrere Werkzeuge sind verfügbar, die von akademischen und industriellen Stellen entwickelt wurden).

#### **A.1.6.6 Beispiel**

Ein Fehlzustand-tolerantes Multiprozessor-System, siehe Bild A.8, enthält zwei unabhängige Teilsysteme  $S_1$  und  $S_2$  mit einem gemeinsam benutzten Speicher  $M_3$ .

Jedes Teilsystem  $S_i$  ( $i = 1; 2$ ) setzt sich zusammen aus einem Prozessor  $P_i$ , einem lokalen Speicher  $M_i$  und zwei replizierten Plattenspeichereinheiten  $D_{i1}$  und  $D_{i2}$ . Die beiden Teilsysteme sind über einen Bus N mit dem gemeinsam benutzten Speicher verbunden.



**Bild A.8 – Blockdiagramm eines Multiprozessorsystems**

In Bild A.9 ist eine Darstellung des Multiprozessorsystems nach Bild A.8 mittels eines verallgemeinerten stochastischen Petri-Netzes dargestellt.

Plätze, deren Namen den Suffix *.dn* tragen, modellieren Komponenten in dem Zustand nicht-betriebsfähig.

Ein Token im Platz *S.dn* modelliert einen Totalausfall des Systems.

Transitionen, deren Namen den Suffix *.f* tragen, modellieren den Ausfall einer Komponente.

Die Anfangsmarkierung des Netzes stellt das Multiprozessorsystem mit allen Komponenten als betriebsfähig dar.



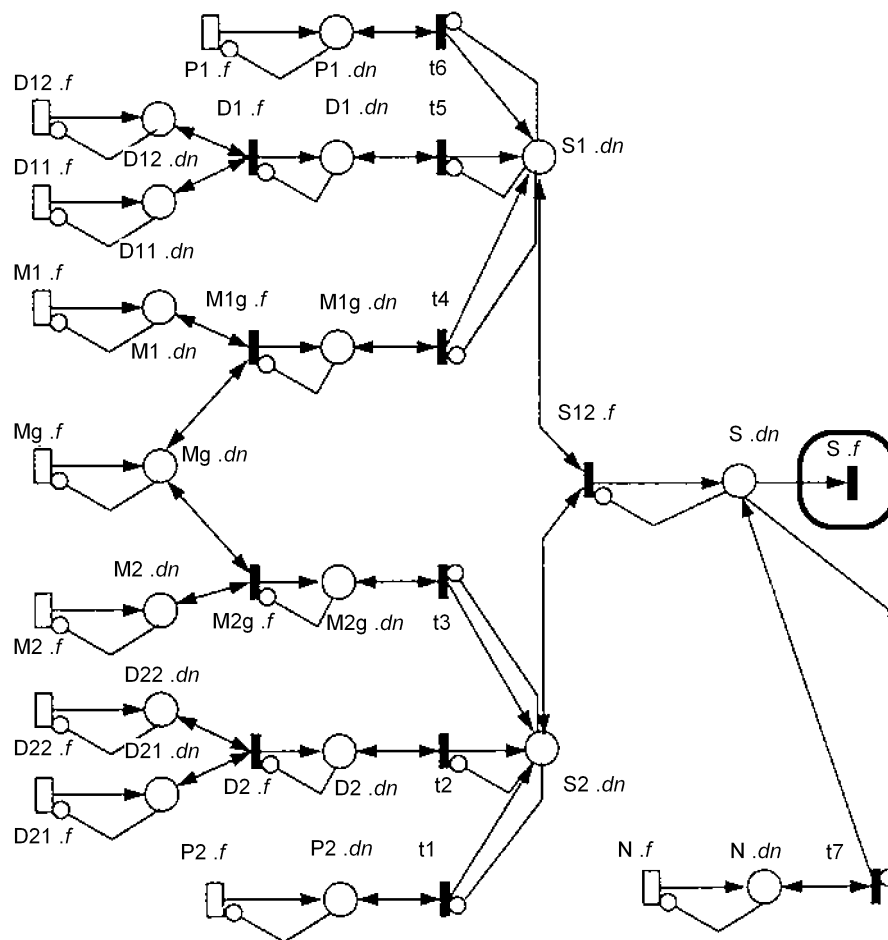


Bild A.9 – Petri-Netz eines Multiprozessorsystems

### A.1.7 Fehlzustandsart- und -auswirkungsanalyse

#### A.1.7.1 Beschreibung und Verwendung

Fehlzustandsart- und -auswirkungsanalyse (FMEA) ist ein induktives, in der unteren Ebene beginnendes qualitatives Verfahren zur Analyse der Zuverlässigkeit. Es ist besonders ausgerichtet auf Untersuchung von Werkstoff-, Komponenten- und Geräteausfällen und deren Auswirkungen auf die funktional nächsthöchste Systemebene. Schrittweises Vorgehen (Feststellen von einzelnen Ausfallarten und Beurteilung ihrer Auswirkungen auf die nächsthöchste Systemebene) führt schließlich zum Erkennen aller einzelnen Ausfallarten des Systems. Die FMEA eignet sich für die Analyse von Systemen unterschiedlicher Technologien (elektrisch, mechanisch, hydraulisch, softwaregesteuert usw.) mit einfachen funktionalen Strukturen. Durch eine Ausfallbedeutungsanalyse (FMECA) wird die FMEA durch das Quantifizieren von Ausfallauswirkungen, d. h. die Angabe von Ereignishäufigkeiten und der Schwere von Auswirkungen, ausgeweitet. Die Schwere von Auswirkungen wird durch Zuordnung zu einer festgelegten Skale bewertet.

#### A.1.7.2 Anwendung

FMEA oder FMECA werden gewöhnlich dann durchgeführt, wenn in einem Programm früh während der Produkt- oder Prozessentwicklung ein gewisses Risiko erwartet wird. Folgende Faktoren können betrachtet werden: neue Technologie, neue Prozesse, neue Entwürfe oder Änderungen in der Umgebung, Belastung oder gesetzliche Regulierung. FMEA oder FMECA können auf Komponenten oder Systeme angewendet werden, aus denen Produkte, Prozesse oder Geräte für die Fertigung bestehen. Auch können sie auf Software-Systeme angewendet werden.

#### A.1.7.3 Schlüsselemente

Die FMEA- oder FMECA-Analyse läuft gewöhnlich in folgenden Schritten ab:

- Ermitteln, wie sich die Systemkomponenten verhalten sollen;

- Ermitteln von potentiellen Ausfallarten, Ausfallauswirkungen und Ursachen;
- Ermitteln von Risiko-behafteten Ausfallarten und Ausfallauswirkungen;
- Ermitteln von Empfehlungen, wie das Risiko beseitigt oder verringert werden kann;
- Folgemaßnahmen zum Abschließen der empfohlenen Aktionen.

#### **A.1.7.4 Vorzüge**

- Das Verfahren ermittelt systematisch die Beziehungen zwischen Ursache und Auswirkung.
- Es gibt einen Anfangshinweis, welche Ausfallarten vielleicht kritisch sein könnten, besonders zu einzelnen Ausfällen, die sich weiter ausbreiten könnten.
- Es führt zu aus besonderen Ursachen oder auslösenden Ereignissen sich ergebenden Erkenntnissen, von denen man annimmt, dass sie wichtig sein könnten.
- Es gibt einen Rahmen zur Ermittlung von Maßnahmen zur Minderung des Risikos.
- Es ist hilfreich in der Voranalyse von neuen, noch nicht erprobten Systemen oder Prozessen.

#### **A.1.7.5 Einschränkungen**

- Die gewonnenen Daten können umfangreich sein, selbst bei verhältnismäßig einfachen Systemen.
- Das Verfahren kann kompliziert und schlecht beherrschbar werden, falls es keine ziemlich direkte (oder geradlinige) Beziehung zwischen Ursache und Auswirkung gibt.
- Es können zeitliche Abfolgen, Wiederherstellungsprozesse, Umgebungsbedingungen, Gesichtspunkte der Instandhaltung usw. nicht einfach behandelt werden.
- Die Betonung der Kritizität von Ausfallarten wird durch beteiligte und gegeneinander gerichtete Faktoren erschwert.

#### **A.1.7.6 Normen**

Die zugehörige Norm ist IEC 60812.

#### **A.1.7.7 Beispiel**

Ein Beispiel für eine Fehlzustandsart- und -auswirkungsanalyse ist in Tabelle A.5 enthalten.

Tabelle A.5 – Beispiel einer FMEA

Unterebene: Blatt-Nr.: Betriebsart:					Entworfen von: Einheit: Ausgabe:				Erarbeitet von: Angenommen von: Datum:			
Einheit Ref.	Funktionsbeschreibung der Einheit	Ausfallcode	Ausfallart	Mögliche Ausfallursachen	Symptom erkannt durch	Lokale Auswirkung	Auswirkung auf die Ausgabe der Einheit	Vorkehrungen zur Ausfallvermeidung	Schwere-Klasse	Ausfallrate	Datenquelle	Empfehlungen und ergriffene Maßnahmen
1.1.1	Stator des (Elektro-) Motors	1111	Unterbrechung (elektrisch)	Wicklungsbruch	ruckelt bei niedrigen Umdrehungen	geringe Leistung	abgeschaltet	Einphasen-temperatur-schutzschalter	4			
		1112	Unterbrechung (elektrisch)	Anschluss unterbrochen	ruckelt bei niedrigen Umdrehungen	geringe Leistung	abgeschaltet	Einphasen-temperatur-schutzschalter	3			
		1113	Isolationsdurchbruch	anhaltend hohe Temperatur, Fertigungsfehler	Schutzsystem	Überlastung	keine Leistung	jährliche Inspektion des Temperaturschalters	4			
		1114	Thermistor ist unterbrochen	Anschluss wegen Alterung unterbrochen	Schutzsystem	keine	keine Leistung	Ersatzteil montiert	3			Ersatzteil vorhalten, das zum Gehäuseäußeren durchverbunden wird
		1115	Thermistor hat Kurzschluss	Schutzsystem	Schutzsystem	reduzierter Abschaltbereich	bei hoher Last keine Leistung	Ersatztemperaturschalter montiert	3			Ersatzteil vorhalten, das zum Gehäuseäußeren durchverbunden wird
1.1.2	Motorkühl-system	1121	nicht ausreichende Kühlung	niedriger Differentialdruck blockiert	hohe Statortemperatur vom Thermistor erkannt	Wicklung zu heiß	Motor zu heiß	Stator-temperatur-schalter	2			
		1122	Undichtheit zur Außenluft hin	Leitungsverbindung	Motortemperatur	Motor-kühlung nicht ausreichend	Motor zu heiß	Temperaturschalter alle 2 Stunden prüfen	2			
		1123	Undichtheit von der Außenluft her	Leitungsverbindung	geringe Leistung	Luft im System	keine	alle 2 Stunden prüfen	2			
1.1.3	Motorlager	1131	Dichtring nach außen undicht	Lagerabnutzungs-ausfall	niedriger Stand in der Schmierölwanne	Schmieröl-verlust	keine, solange Undichtheit nicht groß	täglich prüfen	3			

## A.1.8 Gefährdungs- und Betreibbarkeitsuntersuchung (HAZOP/ PAAG<sup>N1)</sup>)

### A.1.8.1 Beschreibung und Verwendung

Das HAZOP-(PAAG-)Verfahren ist eine systematische Vorgehensweise zum Auffinden nicht offensichtlicher Gefahrenquellen und wird von einem Team durchgeführt. Das Verfahren behandelt das Ermitteln möglicher Abweichungen vom bestimmungsgemäßen Betrieb eines Systems, das Auffinden der möglichen Ursachen und das Abschätzen der Auswirkungen.

Grundlage des Verfahrens ist eine Untersuchung mittels so genannter „Leitworte“, bei der systematisch und konsequent Abweichungen von der Sollfunktion hinterfragt werden. Die Sollfunktion ist das gewünschte oder spezifizierte Verhalten eines Systems, seiner Elemente und Merkmale. Um die Untersuchung zu erleichtern, wird ein System in Funktionseinheiten zergliedert und für jede einzelne Funktionseinheit in überschaubarer und abgeschlossener Weise die Sollfunktion festgelegt. Die Sollfunktion für einen speziellen Teil des Systems wird mittels Elementen formuliert, die die wesentlichen Merkmale der Funktionseinheit samt ihrer Untergliederungen vermitteln. Elemente können sein: einzelne Schritte oder Stufen eines Prozesses, einzelne Signale und Geräteeinheiten in einem Lenkungssystem, Geräte oder Komponenten in einem Prozess, elektronische Systeme usw.

Das Ermitteln der Abweichungen von der Sollfunktion geschieht in einem Frageprozess, bei dem vorgegebene „Leitworte“ angewendet werden. Durch die „Leitworte“ soll das Team zu kreativem Denken stimuliert und eine Diskussion angestoßen werden, um eine möglichst umfassende Untersuchung zu erreichen. Leitworte und deren Bedeutung sind in den Tabellen A.6 und A.7 enthalten.

**Tabelle A.6 – Grundlegende Leitworte und deren allgemeine Bedeutung**

Leitwort	Bedeutung
Nein (nicht)	Verneinung der gesamten Sollfunktion
Mehr	quantitative Zunahme
Weniger	quantitative Abnahme
Sowohl als auch	qualitative Zunahme
Teilweise	qualitative Abnahme
Umkehrung	entgegengesetzter Ablauf/Zustand
Anders als	vollständiger Austausch

**Tabelle A.7 – Zusätzliche Leitworte bezüglich Zeitpunkt und Reihenfolge und Abfolge**

Leitwort	Bedeutung
Früher	vor dem Zeitpunkt
Später	nach dem Zeitpunkt
Vorher	vor der Reihe/Folge
Nachher	nach der Reihe/Folge

### A.1.8.2 Anwendung

Die Anwendung des HAZOP-Verfahrens erfolgt zweckmäßigerweise in der Schluss-Phase der Planung zur Untersuchung der Betriebsbedingungen und bei Änderungen bestehender Verfahren. Der beste Zeitpunkt der Durchführung einer HAZOP-Studie ist unmittelbar vor Abschluss der Entwicklungsarbeiten.

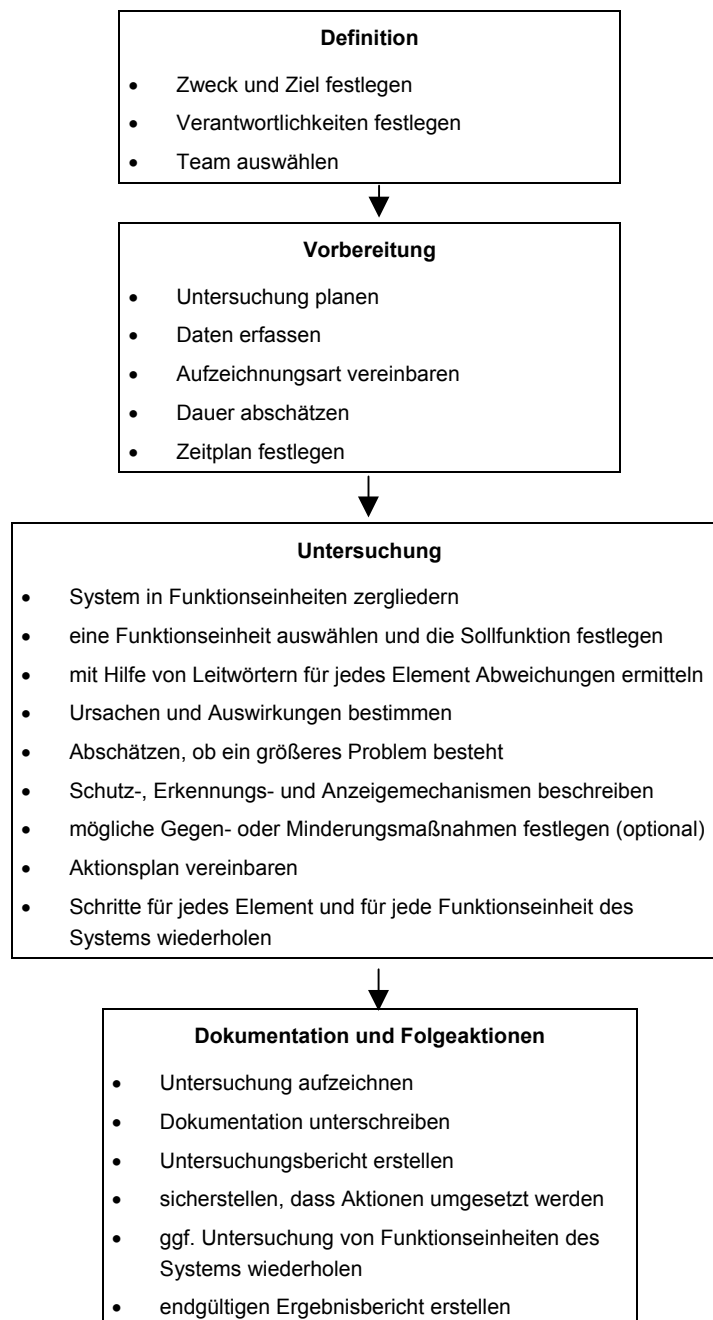
### A.1.8.3 Schlüsselemente

- Die Untersuchung ist ein kreativer Prozess.

<sup>N1)</sup> HAZOP steht für die englischen Begriffe Hazard and Operability. PAAG steht für Prognose von Abweichungen, Auffinden der Ursachen, Abschätzen der Auswirkungen und Gegenmaßnahmen.

- Während der Untersuchung wird systematisch eine Reihe von Leitworten angewendet, um mögliche Abweichungen von der Sollfunktion zu erkennen. Diese Abweichungen sollen bei den Teammitgliedern Überlegungen auslösen, wie die Abweichung entstehen und welche Auswirkungen sie haben könnten.
- Die Untersuchung wird unter der Anleitung eines ausgebildeten und erfahrenen Untersuchungsleiters durchgeführt. Dieser muss eine umfassende Betrachtung des untersuchten Systems gewährleisten und dabei logisches und analytisches Denken einsetzen.
- Für die Untersuchung benötigt man Fachleute aus verschiedenen Fachbereichen mit entsprechender Erfahrung und Fähigkeiten, Intuition und gutem Urteilsvermögen.
- Die Untersuchung sollte mittels positivem Denken und in freier Diskussion durchgeführt werden. Wenn ein Problem erkannt wird, wird es zur anschließenden Bewertung und Lösung protokolliert.
- Die Lösung erkannter Probleme ist nicht primäres Ziel der HAZOP-Studie; wenn diese jedoch gefunden werden, sollten sie dokumentiert werden, damit sie den Entwicklungsverantwortlichen zur Lösungsfindung zur Verfügung stehen.

HAZOP-Studien bestehen aus vier grundlegenden aufeinander folgenden Schritten, wie in Bild A.10 gezeigt.



**Bild A.10 – Das Verfahren bei HAZOP-(PAAG-)Studien**

#### A.1.8.4 Vorzüge

- Das Wissen und die unterschiedlichen Fähigkeiten einer Gruppe von Fachleuten, von denen jeder mit einem unterschiedlichen Aspekt des untersuchten Systems vertraut ist, wird zusammengetragen.
- In wirksamer Weise werden sowohl Ursachen als auch Auswirkungen von Abweichungen in verschiedenen Systemebenen gefunden.
- Es können Prozesse bewertet werden, die z. B. mittels eines Flussdiagramms beschrieben werden.
- Das bei der Untersuchung gesammelte Wissen ist bei der Bestimmung geeigneter Gegenmaßnahmen von großer Hilfe.

#### A.1.8.5 Einschränkungen

Das HAZOP-Verfahren hat sich in mehreren unterschiedlichen Industriebereichen als äußerst wirksam erwiesen. Man sollte sich jedoch bei einer möglichen Anwendung über Einschränkungen im Klaren sein.

- Bei dem HAZOP-Verfahren werden Funktionseinheiten eines Systems einzeln untersucht und die Auswirkungen von Abweichungen jeder Funktionseinheit beschrieben. Es kann jedoch sein, dass eine Abweichung zu einer Wechselwirkung einer ganzen Reihe von Funktionseinheiten des Systems führt. In solchen Fällen kann es erforderlich sein, die Gefährdung eingehender mit Hilfe von Techniken wie etwa Fehlzustandsbaum und Ereignisbaum zu untersuchen.
- Wie bei allen Verfahren zur Erkennung von Gefahren oder Problemen mit der Betreibbarkeit kann es keine Sicherheit dafür geben, dass durch das HAZOP-Verfahren alle Gefahren oder Probleme mit der Betreibbarkeit erkannt werden. Die Untersuchung eines komplexen Systems sollte deshalb nicht nur von einer HAZOP-Untersuchung abhängen. Sie sollte in Verbindung mit anderen angemessenen Techniken, wie z. B. Fehlzustandsbaumanalyse, angewendet werden.
- Viele Systeme sind hoch vernetzt, und eine Auswirkung an der einen Stelle hat möglicherweise Ursachen anderswo. Eine Maßnahme könnte begrenzt richtig sein, im Zusammenspiel jedoch die eigentliche Ursache nicht beheben und somit zu Folgeunfällen führen.
- Der Erfolg einer HAZOP-Untersuchung hängt stark von den Fähigkeiten und der Erfahrung des Untersuchungsleiters und vom Wissen, der Erfahrung und der Interaktion zwischen den Teammitgliedern ab.
- In einem ungünstigen Fall betrachtet das HAZOP-Verfahren nur Funktionseinheiten, deren Elemente und Merkmale, die in der Darstellung der Funktion erscheinen. Tätigkeiten und Geschehen, die nicht in dieser Darstellung erscheinen, werden nicht behandelt.

#### A.1.8.6 Normen

Die zugehörige Norm ist IEC 61882.

### A.1.9 Analyse der menschlichen Zuverlässigkeit

#### A.1.9.1 Beschreibung und Verwendung

Die Analyse der menschlichen Zuverlässigkeit ist eine Teilaufgabe der allgemeineren Analyse menschlicher Einflussfaktoren. Unter menschlichen Einflussfaktoren versteht man üblicherweise die Zuweisung von Funktionen, Aufgaben und Mitteln an Menschen und Maschinen sowie die Abschätzung der menschlichen Zuverlässigkeit. Die Analyse der menschlichen Einflussfaktoren ist keine Disziplin an sich; sie ist vielmehr eine Tätigkeit, die die Anwendung von verschiedenen Disziplinen in einem Problemgebiet bedingt, auf dem Menschen und Maschinen zuverlässig arbeiten sollten. Sie umfasst die Disziplinen Psychologie, Physiologie, Soziologie, Medizin und Technik.

Ein besonderer Zweck einer Analyse der menschlichen Einflussfaktoren ist es, solche Faktoren abzuschätzen und zu bewerten, die auf die menschliche Zuverlässigkeit beim Betreiben eines Systems einwirken können; dies wird oft mit Analyse der menschlichen Zuverlässigkeit bezeichnet. Zuverlässiges menschliches Verhalten ist für den Erfolg von Mensch-Maschine-Systemen erforderlich und wird durch viele Faktoren beeinflusst. Diese Faktoren können interner Art sein, wie Stress, emotionaler Zustand, Ausbildung, Motivation und Erfahrung, oder externer Art, wie Arbeitszeiten, Umgebung, Maßnahmen von Vorgesetzten, Prozeduren und Schnittstellen zu den Geräten.

#### A.1.9.2 Anwendung

Die wirkungsvollste Berücksichtigung der menschlichen Einflussfaktoren ist die aktive Berücksichtigung in allen Phasen der Systementwicklung vom Entwurf bis zu Schulung, Betrieb und Entsorgung. Dieses reicht von umfassenden Systembetrachtungen (einschließlich Betriebsführung) bis zu Handlungen eines einzelnen Individuums in der untersten betrieblichen Ebene.

Grundsätzlich stellt jede von einem Menschen durchgeführte Aufgabe eine Gelegenheit für ein menschliches Fehlverhalten dar; d. h., jede dieser Aufgaben sollte zuverlässig ausgeführt werden. Nach dem Feststellen dieser Aufgaben wird jede analysiert, um fehlerträchtige Situationen zu erkennen, die dazu führen könnten, dass der Betreiber versagt. Dies könnte man mit einer Art FMEA für menschliche Aufgaben vergleichen.

Häufig bewertet man diese Aufgaben dadurch, dass man Ereignisbäume für jede einzelne Aufgabe aufstellt. Durch den Ereignisbaum wird die Information über die Analyse der Aufgaben vermittelt und ein Schema zur quantitativen Bewertung der Kombination der Versagensfälle festgelegt.

#### **A.1.9.3 Schlüsselemente**

Die folgende Liste enthält typische Elemente einer Analyse der menschlichen Zuverlässigkeit:

- Beschreibung des Personals, der Arbeitsumgebung und der auszuführenden Arbeiten;
- Analyse der Mensch-Maschine-Schnittstellen;
- Analyse der beabsichtigten Bedienerfunktionen;
- Analyse möglichen menschlichen Fehlverhaltens bei beabsichtigten Bedienerfunktionen;
- Dokumentation der Ergebnisse.

#### **A.1.9.4 Vorzüge**

Die Analyse von Pannen und Unfällen hat gezeigt, dass zuverlässige menschliche Leistung ein Schlüsselfaktor für die Zuverlässigkeit von Mensch-Maschine-Systemen ist. Wenn menschliche Einflussfaktoren missachtet werden, können die Zuverlässigkeitsvorhersagen für ein System ganz und gar irreführend sein. Die Analyse der menschlichen Zuverlässigkeit trägt zur Brauchbarkeit des Produktes bei.

#### **A.1.9.5 Einschränkungen**

Die Analyse der menschlichen Zuverlässigkeit als Teil eines Systems erfordert eingehende Kenntnisse menschlicher Leistungsparameter.

Insbesondere wenn keine schadensgeschichtlichen Daten verfügbar sind, muss sich die quantitative Analyse möglicherweise auf subjektive Schätzungen der Wahrscheinlichkeiten menschlichen Fehlverhaltens verlassen.

Menschliche Einflussfaktoren werden häufig nicht als Teil der Zuverlässigkeitsarbeiten angesehen, und es kann manchmal schwer sein, die Projektleitung davon zu überzeugen, eine Analyse der menschlichen Zuverlässigkeit zu veranlassen.

#### **A.1.9.6 Beispiel**

In einer Anwendung soll der Schlüssel zur Inbetriebnahme des Systems, in diesem Beispiel ein Zug, durch eine elektronische Smart Card ersetzt werden (die Gründe hierfür sind für dieses Beispiel unerheblich). Diese Lösung ist in mehreren Variationen von Bargeldautomaten her bekannt. Die (relative) Wirkung dieser Änderung auf die Verfügbarkeit des Systems (hinsichtlich der früheren Lösung) soll geschätzt werden.

Schritt 1: Man betrachte einen Zugführer in einer Eisenbahn-spezifischen Arbeitsumgebung und seine Wechselwirkung mit dem System bei der Inbetriebnahme des Zuges. Um sich zu authentisieren, muss er seine Smart Card und die persönliche Geheimzahl (PIN) eingeben.

Schritt 2: Die Schnittstelle ist von Bargeldautomaten her gut bekannt. Sie besteht aus einem Kartenleser, einer Anzeige und einem Zahlenfeld zur Eingabe der persönlichen Geheimzahl.

Schritt 3: Aufgabe 1 ist es die, Smart Card einzuschieben. Aufgabe 2 ist es, die persönliche Geheimzahl einzugeben.

Schritt 4: Glaubwürdiges menschliches Fehlverhalten ist in Tabelle A.8 aufgeführt (Liste ist nicht notwendigerweise erschöpfend).

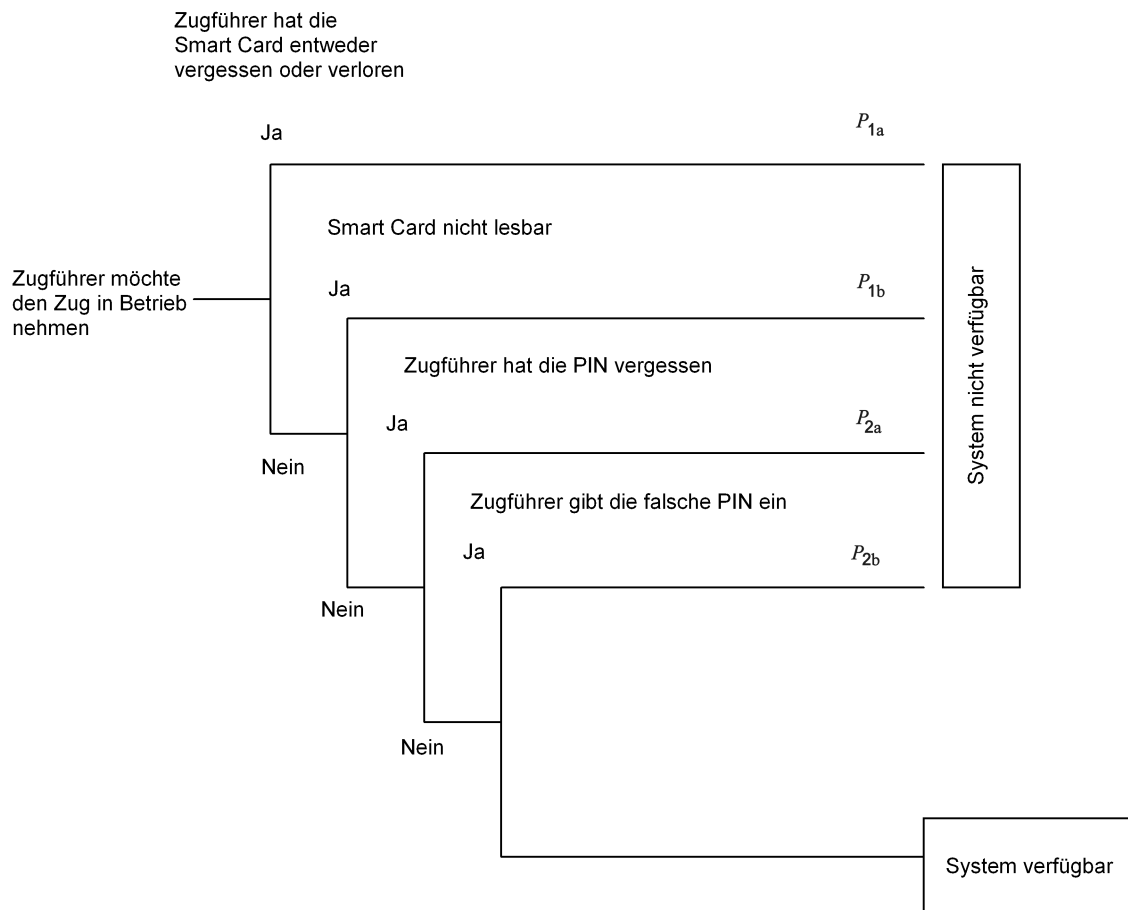
Tabelle A.8 – Glaubwürdiges menschliches Fehlverhalten

Aufgabe	Menschliches Fehlverhalten	Ursache	Maßnahmen
a)	1) Der Zugführer hat die Smart Card entweder vergessen oder verloren.	i) Ungeeignete Aufbewahrung der Karte	Bereitstellung einer geeigneten Aufbewahrung oder einer Schutzhülle für die Karte, die von dem Zugführer angenommen wird.
		ii) Unaufmerksamkeit	Prüfungen einführen, die sicherstellen, dass dies keine betrieblichen Auswirkungen hat (etwa zu Beginn der Schicht). Für diesen Fall Joker-Karten bereitstellen.
	2) Die Smart Card befindet sich in einem Zustand, der sie für das System unlesbar macht.	i) Ungeeignete Aufbewahrung der Karte	wie vorstehend
		ii) Ungeeignete Handhabung	Schulung zur Handhabung von Smart Cards. Regelmäßige Prüfungen. Kontaktlose Smart Cards als eine alternative Lösung, unter Beachtung des Kosten/Nutzen-Verhältnisses erwägen.
b)	1) Der Zugführer hat die PIN vergessen.	Vergesslichkeit	Schulung. Eine alternative Lösung könnte sein, dass der Zugführer die PIN selbst wählen darf (eine Zahl, an die er sich leichter erinnern kann), anstelle einer ihm vom System zugewiesenen PIN.
	2) Der Zugführer gibt eine falsche PIN ein.	Tippfehler usw.	Wenigstens eine Wiederholung zulassen. Die Zahlentastatur ergonomisch gestalten, um Tippfehler zu vermeiden (z. B. sollten die Tasten nicht zu klein und leicht lesbar sein, nach Drücken einer Taste ein Quittungssignal (Piepser) geben usw.).

Diese Information kann auch durch einen Ereignisbaum (siehe Bild A.11) dargestellt werden.

Der Ereignisbaum kann durch Zuweisung von Wahrscheinlichkeiten zu jedem Zweig quantifiziert werden. Jedoch kann es selbst bei diesem kurzen Beispiel eine aufwendige Arbeit sein, genaue Daten und Modelle zu bekommen. Manche Daten könnten zwar bei Geldautomatenanwendungen erfasst werden, aber es ist zu beachten, dass die hier angetroffene Arbeitsumgebung davon vollständig verschieden ist. In diesem Beispiel ist die Nichtverfügbarkeit lediglich die Summe aller in dem Ereignisbaum genannten Wahrscheinlichkeiten. Zur Illustrierung dieses Beispiels werden (hypothetische) Zahlenwerte genannt.





Parameter	Wert	Bemerkung
$P_{1a}$	$10^{-4}$	Zugführer sind bekanntermaßen sorgfältig und geschult, Smart Cards wie Schlüssel zu behandeln; geeignete Aufbewahrung ist gewährleistet, Prüfungen werden durchgeführt.
$P_{1b}$	$10^{-4}$	Geeignete Schutzhülle für Smart Cards.
$P_{2a}$	$10^{-4}$	Zugführer dürfen ihre PIN wählen, sie kennen die Folgen, z. B. Verspätungen.
$P_{2b}$	$10^{-2}$	Ergonomisch gestaltete Zahlentastatur, aber Tippfehler können immer passieren.

**Bild A.11 – Menschliches Fehlverhalten als Ereignisbaum dargestellt**

Das Ergebnis liefert eine schlechte Nichtverfügbarkeit, etwa 0,01 je Fahrt, dies ist nicht annehmbar. Als Abhilfemaßnahme wird es dem Zugführer erlaubt, nach einer Fehleingabe in einem zweiten Versuch die PIN nochmals einzugeben. Die Wahrscheinlichkeit eines zweimaligen Versagens ist in diesem Beispiel  $P_{2b} \times P_{2b} = 10^{-4}$ ; dieses ergibt somit eine geschätzte gesamte Nichtverfügbarkeit von 0,0004 je Fahrt (vier von 10 000 Zügen werden verspätet sein), dies erscheint annehmbar. Wenn man noch mehr Versuche zuließe, könnte man die Nichtverfügbarkeit auf 0,0003 verringern, aber dies könnte aus Sicherheitsgesichtspunkten nicht annehmbar sein.

## A.1.10 Beanspruchungsanalyse

### A.1.10.1 Beschreibung und Verwendung

Die Beanspruchungsanalyse (Analyse der Belastung und Widerstandsfähigkeit) ist ein Verfahren, mit dem die Fähigkeit eines Bauelementes oder einer Einheit bestimmt werden kann, elektrischen, mechanischen, umgebungsbedingten oder anderen Belastungen, die eine Ursache für deren Ausfall sein könnten, zu widerstehen. Mit dieser Analyse können die physikalischen Wirkungen der Belastungen eines Bauelementes als auch die mechanischen oder physikalischen Eigenschaften des Bauelementes selbst bestimmt werden. Die Wahrscheinlichkeit eines Bauelementeausfalls ist direkt proportional zu den einwirkenden Belastungen. Das

jeweilige Verhältnis von Belastung zur Widerstandsfähigkeit des Bauelementes bestimmt die Zuverlässigkeit des Bauelementes.

#### A.1.10.2 Anwendung

Die Beanspruchungsanalyse wird hauptsächlich zur Bestimmung der Zuverlässigkeit oder der entsprechenden Ausfallraten von mechanischen Bauelementen verwendet. Sie wird darüber hinaus für die Physik von Ausfällen verwendet, um die Häufigkeit des Auftretens einer besonderen Ausfallart aufgrund einer besonderen Ursache in einem Bauelement zu bestimmen.

Die strukturelle Bauelementzuverlässigkeit, die Fähigkeit elektrischen oder anderen Beanspruchungen zu widerstehen, hängt von der Widerstandsfähigkeit oder Belastungsfähigkeit des Bauelementes ab. Überlebensfähigkeit ist das Wahrscheinlichkeitsmaß für die Erfüllung der erwarteten Eigenschaften des Bauelementes. Die Bestimmung dieser Belastungsfähigkeit birgt eine Unsicherheit in sich. Daher modelliert man diese Fähigkeit als eine Zufallsvariable, im Gegensatz zur tatsächlich anliegenden Belastung, die aus demselben Grund der Unsicherheit ebenfalls als eine weitere Zufallsvariable modelliert wird. Die Überlappung dieser Zufallsvariablen, als Verteilung dargestellt, steht für das Wahrscheinlichkeitsmaß, dass die Belastung die Widerstandsfähigkeit übersteigt. Anders ausgedrückt heißt dies, dass der Überlappungsbereich der entsprechenden Wahrscheinlichkeitsdichtefunktion die Wahrscheinlichkeit für das Eintreten eines Ausfalls darstellt.

Die Beurteilung der Belastung gegenüber der Widerstandsfähigkeit und die daraus resultierende Teilezuverlässigkeit beruht auf der Beurteilung der zweitrangigen Momente Mittelwert und Varianz der erwarteten Zufallsvariablen von Belastung und Widerstandsfähigkeit. Diese Beurteilung wird oft auf eine Belastungsvariable im Vergleich mit der Widerstandsfähigkeit des Bauelementes vereinfacht.

Allgemein ausgedrückt müssen Widerstandsfähigkeit und Belastung entweder durch die Leistungsfunktion oder die Zustandsfunktion dargestellt werden, welche für eine Vielzahl von Auslegungsvariablen, einschließlich Fähigkeiten und Belastungen, stehen. Ein positiver Wert dieser Funktion steht für einen sicheren Zustand, ein negativer Wert für den Ausfallzustand.

#### A.1.10.3 Schlüsselemente

Zu den Schlüsselementen gehört die detaillierte Kenntnis der Materialien und des Aufbaus des Bauelementes sowie anderer interessierender Eigenschaften sowie eine saubere Modellierung der erwarteten Belastung.

#### A.1.10.4 Vorzüge

Durch eine Beanspruchungsanalyse kann man eine genaue Darstellung der Zuverlässigkeit eines Bauelementes als Funktion der erwarteten Ausfallmechanismen erhalten. Die Analyse berücksichtigt Variationen der Auslegung als auch der erwarteten anliegenden Belastungen sowie beider Wechselwirkung. In diesem Sinne liefert dieses Verfahren eine realistischere Sicht der Auswirkungen multipler Beanspruchungen; sie stellt die Physik der Bauelementeausfälle gut dar, da viele Faktoren – Umwelt- und Mechanik – einschließlich deren Wechselwirkungen betrachtet werden können.

#### A.1.10.5 Einschränkungen

Bei Mehrfachbelastungen und insbesondere wenn es zwischen zwei oder mehr anliegenden Belastungen Wechselwirkungen oder Korrelationen gibt, kann die für die Lösung des Problems erforderliche Mathematik sehr aufwendig werden und den Einsatz von rechnergestützten professionellen mathematischen Werkzeugen notwendig machen. Ein weiterer Nachteil ist die möglicherweise falsche Annahme zur Verteilung einer oder mehrerer Zufallsvariablen, welche ihrerseits zu fehlerhaften Schlussfolgerungen führen kann.

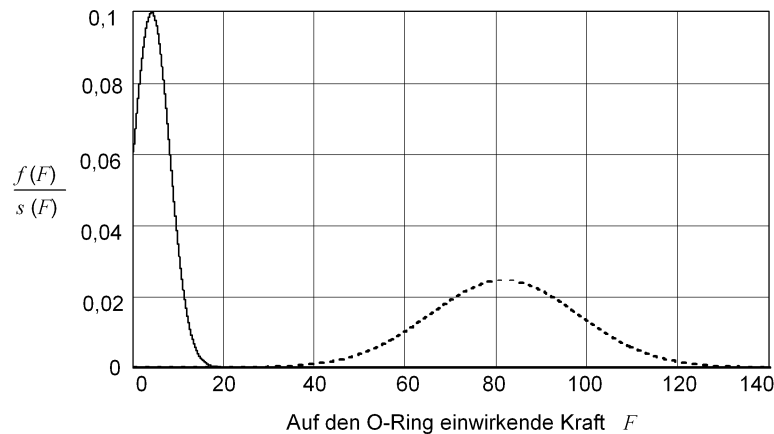
#### A.1.10.6 Beispiel

Ein einfaches Beispiel für Beanspruchungskriterien ist die anliegende Kraft auf einen Dichtungsring (O-Ring), und das zugehörige Ausfallkriterium ist Undichtigkeit. Um die Häufigkeit des Auftretens dieses Ausfalls zu berechnen, wurde die mittlere Kraft  $F_0$  berechnet, die notwendig ist, um das Leck hervorzurufen. Diese Berechnung beruht auf den inneren und äußeren Abmessungen des O-Rings, seiner Geometrie und Materialeigenschaften – dies wird als Widerstandsfähigkeit verstanden. Es wird angenommen, dass sowohl die Widerstandsfähigkeit als auch die anliegende Kraft  $F$  normal verteilt sind und die entsprechenden

Standardabweichungen gleich einem Zehntel der entsprechenden Mittelwerte sind. Die Ausfallwahrscheinlichkeit wird berechnet zu:

$$P_F = \Phi \left[ \frac{F - F_0}{\sqrt{\sigma_F^2 + \sigma_{F_0}^2}} \right] = 1,9 \times 10^{-6}$$

Bild A.12 stellt das Beispiel dar.



**Bild A.12 – Beispiel: Anwendung von Beanspruchungskriterien**

## A.1.11 Wahrheitstabelle

### A.1.11.1 Beschreibung und Verwendung

Die mathematischen Qualitäten des Wahrheitstabellenverfahrens – auch Strukturfunktionsanalyse genannt – werden auf gewissen Gebieten, insbesondere in der Elektrotechnik und Elektronik, in großem Maße geschätzt. Das Verfahren besteht darin, alle möglichen Zustandskombinationen (in Betrieb, ausgefallen) der verschiedenen Elemente, aus denen ein System besteht, aufzulisten und deren Auswirkungen zu untersuchen.

### A.1.11.2 Anwendung

Die ersten Schritte in der Anwendung dieses Verfahrens sind denen einer Ausfallbedeutungsanalyse (FMECA) ähnlich. Nachdem das System in eine handhabbare Größe aufgespalten wurde, sollten die Ausfallarten der Komponenten sowie deren Ausfallzustände aufgelistet werden. Üblicherweise ist jede Komponente durch den Zustand „in Betrieb“ bzw. „ausgefallen“ gekennzeichnet. Ein Zustandsvektor wird definiert als die Kombination von Komponenten-Zuständen, wobei jede Komponente entweder durch ihren Zustand „in Betrieb“ bzw. „ausgefallen“ dargestellt wird.

Die Wahrheitstabelle wird durch das Analysieren der Auswirkungen aller Zustandsvektoren der Komponenten erarbeitet. Alle Ausfälle des Systems werden auf diese Weise ermittelt. Die Ergebnisse werden dann in einer so genannten „Wahrheitstabelle“ zusammengefasst; dabei bezeichnet man mit „0“ den Zustand „in Betrieb“ und mit „1“ den Zustand „ausgefallen“. Bei der Untersuchung jedes Zustandsvektors sollte auch eine Ausfall- (bzw. Fehlzustands-)Analyse unternommen werden, damit man mögliche Ausfälle mit gemeinsamer Ursache erkennen kann.

Die Wahrscheinlichkeit des Zustandes „System ausgefallen“ ergibt sich aus der Summe aller einzelner Eintrittswahrscheinlichkeiten derjenigen Zustandsvektoren, die in einen Systemausfall münden. Sofern die Komponenten voneinander unabhängig sind, ist dieses Aufsummieren erlaubt, da die Zustandsvektoren dann disjunkt sind. In Bild A.13 ist eine Wahrheitstabelle für zwei einfache Systeme gezeigt.


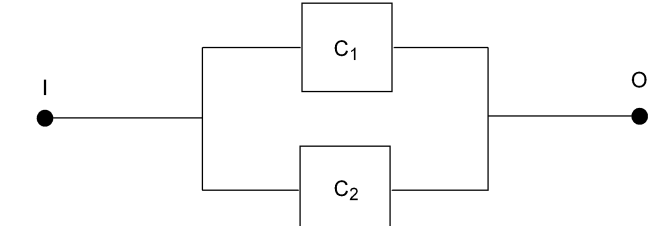
System	Wahrheitstabelle		
	C <sub>1</sub>	C <sub>2</sub>	O
	0	0	0
	0	1	1
	1	0	1
	1	1	1
	C <sub>1</sub>	C <sub>2</sub>	O
	0	0	0
	0	1	0
	1	0	0
	1	1	1

Bild A.13 – Wahrheitstabelle für zwei einfache Systeme

Das Wahrheitstabellenverfahren bedingt die Untersuchung aller möglichen Kombinationen der Zustände „in Betrieb“ und „ausgefallen“ aller einzelnen Elemente. Es ist somit theoretisch das strikteste bis jetzt jemals erdachte Verfahren. Um die belangvollen Kombinationen zu erhalten, kann die Wahrheitstabelle mittels Boolescher Verfahren reduziert werden. Die Anwendung dieses Verfahrens auf komplexe Systeme kann schwierig werden, da die Anzahl der Zustände schnell sehr groß werden und somit schwierig zu handhaben sein kann.

#### A.1.11.3 Normen

Das Verfahren ist in Abschnitt 8 von IEC 61078 behandelt.

#### A.1.11.4 Beispiel

Eine Systemauslegung besteht aus einem Hauptsignalpfad (K) und einem alternativen Pfad (E). Der alternative Pfad stellt keine funktionale Redundanz dar, sondern ist funktionsbeteiligt. Der Schalter (U) liegt nicht im Signalpfad. Es ist die Verfügbarkeit des Systems zu bestimmen.

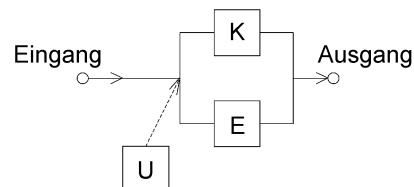


Bild A.14 – Beispiel

Es ergibt sich die folgende Wahrheitstabelle, dabei steht „0“ für den Zustand „in Betrieb“ und „1“ für den Zustand „ausgefallen“:

Tabelle A.9 – Beispiel einer Wahrheitstabelle

Zu- stand	K	E	U	$P(S \mid A_i)$	$P(A_i)$	$P(S \mid A_i) \times P(A_i)$
$A_1$	0	0	0	1	$a_K \times a_E \times a_U$	$1 \times a_K \times a_E \times a_U$
$A_2$	0	1	0	1	$a_K \times (1 - a_E) \times a_U$	$1 \times a_K \times (1 - a_E) \times a_U$
$A_3$	1	0	0	1	$(1 - a_K) \times a_E \times a_U$	$1 \times (1 - a_K) \times a_E \times a_U$
$A_4$	1	1	0	0	$(1 - a_K) \times (1 - a_E) \times a_U$	0
$A_5$	0	0	1	1	$a_K \times a_E \times (1 - a_U)$	$1 \times a_K \times a_E \times (1 - a_U)$
$A_6$	0	1	1	1	$a_K \times (1 - a_E) \times (1 - a_U)$	$1 \times a_K \times (1 - a_E) \times (1 - a_U)$
$A_7$	1	0	1	0,5	$(1 - a_K) \times a_E \times (1 - a_U)$	$0,5 \times (1 - a_K) \times a_E \times (1 - a_U)$
$A_8$	1	1	1	0	$(1 - a_K) \times (1 - a_E) \times (1 - a_U)$	0
ANMERKUNG Im Zustand $A_7$ hängt die Funktion des Systems davon ab, ob der Schalter sich in Position (K) oder (E) befindet. Man nimmt daher an, dass sich das System mit der Wahrscheinlichkeit 0,5 in diesem Zustand befindet.						

Falls die Zufallsereignisse  $A_1, \dots, A_n$  sich gegenseitig paarweise ausschließen, berechnet sich die Wahrscheinlichkeit  $P_S$  wie folgt

$$P_S = \sum_{i=1}^n P(S \mid A_i) \times P(A_i)$$

wobei

$P(S \mid A_i)$  die Wahrscheinlichkeit ist, dass das System im Zustand  $A_1$  betrieben wird,

$P(A_i)$  Wahrscheinlichkeit, dass das System im Zustand  $A_1$  ist.

Setzt man Verfügbarkeiten  $a$  anstelle der Wahrscheinlichkeiten  $P$ , dann erhält man:

$$P_S = a_S = [a_K \times a_E \times a_U] + [a_K \times (1 - a_E) \times a_U] + [(1 - a_K) \times a_E \times a_U] + [a_K \times a_E \times (1 - a_U)] + [a_K \times (1 - a_E) \times (1 - a_U)] + [0,5 \times (1 - a_K) \times a_E \times (1 - a_U)]$$

Dies führt zu

$$a_S = a_K + 0,5 \times (1 - a_K) \times a_E \times (1 - a_U).$$

## A.1.12 Statistische Zuverlässigkeitsverfahren

### A.1.12.1 Beschreibung und Verwendung

Zuverlässigkeit ist ein Gesichtspunkt technischer Unsicherheit, den man als Wahrscheinlichkeit quantifizieren kann. Die Notwendigkeit, Unsicherheit bei Zuverlässigkeitsanalysen zu messen und zu beherrschen, bedingt den Einsatz statistischer Verfahren.

Statistische Verfahren werden zur Quantifizierung der Zuverlässigkeit aus einer Reihe von Gründen verwendet. Hierzu gehören unter anderem:

- die Zuverlässigkeit von Produkten schätzen und vorhersagen;
- Merkmale von Materialien während einer Gewährleistungsdauer oder während der Lebensdauer eines Produktes bewerten;
- Gewährleistungskosten vorhersagen;
- die Auswirkung einer vorgeschlagenen Entwicklungsänderung bewerten;
- bewerten, ob Kundenanforderungen und behördliche Vorschriften eingehalten worden sind;
- das Produkt im Einsatz beobachten, um Angaben zu Ausfallursachen und für Maßnahmen zur Verbesserung der Funktionsfähigkeit von Produkten zu gewinnen;

- Vergleich von Bauelementen von zwei oder mehreren verschiedenen Herstellern, von Materialien, von Fertigungsperioden, der Betriebsumgebung usw.

Bevor statistische Verfahren angewendet werden können, müssen zunächst Daten erfasst werden. Die Art der zu erfassenden Daten hängt von dem zu lösenden Problem und der durchzuführenden Analyseart ab. Für Zuverlässigkeitsanalysen benötigte und angewandte Daten zielen darauf ab, das Verhalten von einem Risiko ausgesetzten Einheiten (z. B. in einer Betriebsumgebung) zu erfassen. Die Art der Daten variiert je nach Art der zu untersuchenden Einheit. So sind beispielsweise die Grunddaten für nur einmal zu verwendende Einheiten die Anzahl der Versuche und der erfolgreichen Einsätze. Die Grunddaten für nicht-reparierbare Einheiten sind die Dauern bis zum Eintritt eines Ereignisses der einem Risiko ausgesetzten Population; für reparierbare Einheiten sind die Grunddaten die akkumulierten Dauern bis zum Ereignis während der gesamten Lebensdauer der Einheiten. Üblicherweise fallen nicht alle einem Risiko ausgesetzten Einheiten während der Beobachtungsperiode aus. Daher werden die Dauern bis zum Ausfallereignis nur für diejenigen Einheiten aufgezeichnet, die ausfallen, und die Laufdauern der Einheiten, die nicht ausfallen, werden aufgezeichnet. Diese Auswahlverfahren (en: censoring structures) können sehr komplex sein und hängen von den Zielen der Zuverlässigkeitsstudie und der interessierenden Einheit ab.

Zusätzlich zu den Grunddaten können Angaben zu Faktoren erfasst werden, die die Zuverlässigkeit beeinflussen und die in statistische Analysen zur Messung der Auswirkung auf das Leistungsverhalten einfließen.

IEC 60300-3-2 leitet zur Erfassung von Zuverlässigkeitsdaten aus dem Betrieb an.

IEC 60300-3-5 leitet zu Zuverlässigkeits-Prüfbedingungen und Grundsätzen statistischer Tests an.

Klassische statistische Verfahren verwenden nur quantitative Daten zu Ereignissen wie vorstehend beschrieben. Es kann jedoch sein, dass Zuverlässigkeits-Daten aus vergangenen Erfahrungen oder Prüfungen begrenzt sind, dass es aber dennoch notwendig ist, gewisse statistische Maßgrößen zur Zuverlässigkeit zu haben. Aus diesem Grunde können beurteilende Daten gesammelt und mit quantitativen Daten kombiniert werden, um damit Schätzungen der Zuverlässigkeit mittels Bayesscher Verfahren zu erzeugen.

Mit Bayesschen Verfahren ist es möglich, die Zuverlässigkeit anhand von aus verschiedenen Quellen kombinierten Daten zu schätzen. Man setzt zuerst ein Zuverlässigkeitsmodell auf und benützt die vorhandenen Daten, um eine a-priori-Verteilung zu formulieren. Diese a-priori-Verteilung ist eine Wahrscheinlichkeitsverteilung, welche die Ungewissheit der Modellparameter oder der Zuverlässigkeit widerspiegelt, ehe mit der Erfassung von Erkenntnissen über die Zuverlässigkeit begonnen wird. Die a-priori-Verteilung sollte alle verfügbaren Daten erfassen, wie zum Beispiel historische Daten über die Betriebszuverlässigkeit von Einheiten, Daten über die Fähigkeiten von Fertigungsprozessen und Daten über die beobachtete Wirksamkeit von Prüfungen. Die Daten können subjektive technische Beurteilungen sein. Das Zusammenfassen aller Daten in einer einzigen a-priori-Verteilung kann eine sehr anspruchsvolle Aufgabe sein.

Bayessche Verfahren schaffen einen Rahmen, innerhalb dessen Zuverlässigkeitsschätzungen entsprechend dem Eingang neuer Daten aktualisiert werden können. Die a-priori-Verteilung wird mit dem ursprünglichen Zuverlässigkeitsmodell kombiniert, um dadurch eine a-posteriori-Verteilung zu erzeugen, anhand derer man eine aktualisierte Zuverlässigkeitsschätzung erhält. Zum Beispiel möchte man eine anfängliche Zuverlässigkeitsschätzung im Laufe der Entwicklung aktualisieren, nachdem neue Prüfdaten vorliegen. Die Ungewissheit der Schätzungen kann dahingehend quantifiziert werden, dass man obere und untere Grenzwerte für die Zuverlässigkeitskenngrößen angeben kann.

Mit Bayesschen Verfahren kann man Daten aus unterschiedlichen Geräteebenen, zum Beispiel Modul- und Bauelementebene, kombinieren.

#### **A.1.12.2 Anwendung**

Die verwendeten Zuverlässigkeitsmodelle variieren entsprechend der Anwendung, z. B. Verteilung der Lebensdauer wie Exponentialverteilung und Weibull-Verteilung, stochastische Prozesse wie das Exponentialmodell, Zuverlässigkeitswachstumsmodelle, Abnutzungsmodelle, Instandhaltungsmodelle und viele andere.

Jede Modellart kann mittels klassischer oder Bayesscher Verfahren geschätzt werden. Beide liefern unter Angabe eines Unsicherheitsbandes eine Schätzung der Zuverlässigkeit.

#### **A.1.12.3 Schlüsselemente**

Klassische statistische Zuverlässigkeitsverfahren setzen sich aus folgenden Schritten zusammen:

- Ermittlung und Festlegung des für das anstehende Problem zu verwendenden Zuverlässigkeitsmodells;
- Ermittlung der Daten, die man zur Beschreibung der Parameter des Zuverlässigkeitsmodells benötigt;

- Erfassung zugehöriger Ereignisdaten;
- Schätzung des statistischen Modells mittels klassischer Verfahren;
- Gewinnung zugehöriger Zuverlässigkeitsschätzungen aus dem Modell;
- Wiederholung vorstehender Schritte, falls die Zuverlässigkeitsschätzung aktualisiert werden muss.

Bayessche Zuverlässigkeitsverfahren laufen im Allgemeinen in folgenden Schritten ab:

- Ermittlung und Festlegung des für das anstehende Problem zu verwendenden Zuverlässigkeitsmodells;
- Ermittlung der Daten, die man zur Beschreibung der Parameter des Zuverlässigkeitsmodells benötigt;
- Kombination subjektiver Beurteilung in der zugehörigen a-priori-Verteilung;
- Kombination der a-priori-Verteilung mit dem Modell, um die a-posteriori-Verteilung zu erzeugen;
- Gewinnung zugehöriger Zuverlässigkeitsschätzungen aus der a-posteriori-Verteilung;
- Wiederholung vorstehender Schritte, falls die Zuverlässigkeitsschätzung aktualisiert werden muss.

#### **A.1.12.4 Vorzüge**

Allen statistischen Verfahren sind folgende Vorzüge gemeinsam:

- Daten können aus einer Vielzahl von Quellen kombiniert werden;
- die Zuverlässigkeit kann, mit einer gewissen Unsicherheit, geschätzt werden;
- Zuverlässigkeitsschätzungen können aktualisiert werden, sobald mehr Daten vorliegen.

Zusätzlich haben Bayessche Verfahren folgende Vorzüge:

- subjektive Entwicklungs-Daten können mit historischen Ausfalldaten kombiniert werden;
- selbst wenn zunächst nur wenige Ereignisse beobachtet worden sind, können schon früh Zuverlässigkeitsschätzungen erbracht werden.

#### **A.1.12.5 Einschränkungen**

Allen statistischen Verfahren sind folgende Schwierigkeiten gemeinsam:

- die Festlegung eines geeigneten funktionalen Modells, das als Grundlage für Entscheidungen brauchbar ist;
- die Strukturierung von Ereignisdaten zur Verwendung in der Analyse.

Zusätzlich zeichnen sich Bayessche Verfahren durch folgende Schwierigkeiten aus:

- die technische Beurteilung kann schwierig zu erhalten sein;
- das Erstellen einer a-priori-Verteilung kann eine schwierige Aufgabe sein;
- das Berechnen der aktualisierten Zuverlässigkeitskenngrößen (a-posteriori-Verteilung) erfolgt ggf. nicht geradeaus.

## **A.2 Ausgewählte unterstützende Verfahren**

### **A.2.1 Kriechwegeanalyse**

#### **A.2.1.1 Beschreibung und Verwendung**

Kriechwegeanalyse (en: sneak circuit analysis, SCA) ist eine rechnergestützte Vorgehensweise, um Kriechwege zu finden. Unter einem Kriechweg versteht man einen latenten Pfad, der eine ungewollte Funktion verursacht oder der eine gewollte Funktion verhindert, ohne dass Teile ausfallen. Der Pfad kann aus Drähten, Teilen, Software-Schnittstellen und Energiequellen bestehen. Es gibt im Zusammenhang mit Kriechwegen sechs Arten latenter Ausfall-Bedingungen:

- Kriech-Kennzeichnungen;
- Kriech-Indikatoren;
- Zeichnungsfehler;
- Kriechpfade;
- zeitliche Abhängigkeiten;
- Bedenken zum Entwurf.

### A.2.1.2 Anwendung

Kriechwegeanalyse wird zum Aufdecken latenter Wege- oder Schaltkreisverhältnisse verwendet, die zu einer nicht geplanten Betriebsart führen. Kriechwegeanalyse ist verbreitet in der Luft- und Raumfahrttechnik und wird in der atomaren Kraftwerkstechnik eingesetzt.

### A.2.1.3 Schlüsselemente

Kriechwegeanalyse besteht aus folgenden Schritten:

- Untersuchung von Schaltkreisen (oder Funktionen);
- Suche nach unbeabsichtigten Pfaden.

### A.2.1.4 Vorzüge

Kriechwegeanalyse verringert Entwicklungsfehler und menschliches Fehlverhalten in dem System.

### A.2.1.5 Einschränkungen

- Nur wenige Fachleute können Kriechwege mit spezieller Software analysieren.
- Großrechenanlagen sind erforderlich.

## A.2.2 Analyse des ungünstigsten Falls

### A.2.2.1 Beschreibung und Verwendung

Die Analyse des ungünstigsten Falls (en: worst case analysis, WCA) ist eine nicht-statistische Vorgehensweise, mit der man bestätigen und bestimmen kann, ob die Leistung des Systems innerhalb der Spezifikation bei allen Kombinationen gegebener Grenzwerte der Systemparameter liegen kann oder nicht.

### A.2.2.2 Anwendung

Die Analyse des ungünstigsten Falls wird allgemein bei einem aus mehreren Komponenten bestehenden System während der Entwurfs- und Entwicklungsphase eingesetzt. Man kann beispielsweise jeden Mechanismus, Schaltkreis oder jedes Netzwerk als das System betrachten. Die Leistungskenngrößen der Komponenten, wie z. B. die Systemparameter, können die Leistungseigenschaften des Systems beeinflussen. Sie werden mit mathematischen Ausdrücken oder logischen Funktionen kombiniert.

### A.2.2.3 Schlüsselemente

Die Analyse des ungünstigsten Falls läuft im Allgemeinen in folgenden Schritten ab:

- das zu betrachtende System und seine Komponenten festlegen;
- die mathematische oder logische Funktion zur Erklärung der objektiven Systemleistung mit ihren Parametern ermitteln, die die Komponentenleistung beschreiben;
- die Grenzwerte der Systemparameter ermitteln;
- die Leistungseigenschaften des Systems für alle Kombinationen gegebener Grenzwerte der Systemparameter analysieren;
- die Ergebnisse mit den vorgegebenen Spezifikationen der Systemleistung verifizieren;
- Maßnahmen zur Umgestaltung der Systemkonfiguration festlegen und empfehlen;
- sicherstellen, dass empfohlene Maßnahmen abgeschlossen werden;
- den analytischen Prozess und abschließende Ergebnisse dokumentieren.

### A.2.2.4 Vorzüge

- Der Entwickler kann zuversichtlich sein, dass das System hinsichtlich der Drift von Komponenteneigenschaften eine hohe Zuverlässigkeit hat, vorausgesetzt, alle Analyseergebnisse liegen innerhalb der Spezifikationen.
- Es sind keine komplexen mathematischen Bearbeitungen erforderlich.
- Analyseergebnisse sind genau.

### A.2.2.5 Einschränkungen

- Alle mathematischen und logischen Beziehungen zwischen Parametern müssen bekannt sein.
- Um vernünftige Analyseergebnisse zu erhalten, müssen alle Systemkomponenten betrachtet werden.
- Die Analyseergebnisse stellen keine optimalen Werte dar.



### A.2.3 Variationssimulations-Modellierung

#### A.2.3.1 Beschreibung und Verwendung

Unter dem Begriff Variationssimulations-Modellierung werden statistische Vorgehensweisen zusammengefasst, mit denen man ermitteln und bestätigen kann, ob die Systemleistung bei allen Kombinationen gegebener Grenzwerte der Systemparameter innerhalb der Spezifikation bleiben kann. Es gibt zwei typische statistische Verfahren: das Momentverfahren und das Monte-Carlo-Verfahren. Das Momentverfahren für die variable Größe Systemleistung beruht auf der linearen Näherung einer Funktion der Entwurfparameter der Nennwerte in der Taylor-Serie. Das Monte-Carlo-Verfahren beruht auf der Simulation mittels statistischer Verfahren, bei denen jeder Entwurfparameter zufällig aus der gegebenen Wahrscheinlichkeitsverteilung ausgewählt wird.

#### A.2.3.2 Anwendung

Variationssimulations-Modellierung wird allgemein hauptsächlich während der Entwurfs- und Entwicklungsphase für ein aus verschiedenen Komponenten zusammengesetztes System, gemeinsam mit einer Analyse des ungünstigsten Falls, eingesetzt. Man kann beispielsweise jeden Mechanismus, Schaltkreis oder Netzwerk als das System betrachten. Die Leistungskenngrößen der Komponenten sowie auch die Entwurfparameter des Systems können die Leistungseigenschaften des Systems beeinflussen. Die Monte-Carlo-Simulation wird häufig während des rechnergestützten Entwurfsvorganges (CAD) ausgeführt.

#### A.2.3.3 Schlüsselemente

Variationssimulations-Modellierung läuft im Allgemeinen in folgenden Schritten ab.

- a) Beiden Verfahren gemeinsame Schritte:
  - das zu betrachtende System und seine Komponenten festlegen;
  - Leistungsfunktion des Systems ermitteln, ausgedrückt durch alle Leistungs- oder Entwurfparameter der Komponenten;
  - Grenzwerte der Systemparameter ermitteln.
- b) Momentverfahren:
  - lineare Näherung der Leistungsfunktion des Systems in der Taylor-Serie erarbeiten;
  - Nennwert und Varianz der Entwurfparameter ermitteln;
  - aus den Entwurfparametern Nennwert und Varianz der Systemleistung berechnen und ermitteln.
- c) Monte-Carlo-Simulation:
  - Wahrscheinlichkeitsverteilung eines jeden Entwurfparameters ermitteln;
  - die Generierung von Zufallsvariablen für Entwurfparameter festlegen, beruhend auf der durch den Rechner gegebenen Wahrscheinlichkeitsverteilung;
  - durch Simulation die Wahrscheinlichkeitsverteilung der Systemleistung ermitteln, mit Mittelwert und Varianz.
- d) Beiden Verfahren gemeinsame Schritte:
  - die Ergebnisse mit den vorgeschriebenen Spezifikationen der Systemleistung verifizieren;
  - Maßnahmen zur Umgestaltung der Systemkonfiguration festlegen und empfehlen;
  - sicherstellen, dass empfohlene Maßnahmen abgeschlossen werden;
  - den analytischen Prozess und abschließende Ergebnisse dokumentieren.

#### A.2.3.4 Vorzüge

- a) Momentverfahren:
  - der Entwickler kann zuversichtlich sein, dass das System hinsichtlich der Drift von Komponenteneigenschaften eine festgelegte Zuverlässigkeit hat, falls alle Analyseergebnisse innerhalb der Spezifikationen liegen;
  - Analyseergebnisse stellen eine genauere Intervallschätzung als bei einer Analyse des ungünstigsten Falls (WCA) dar.

b) Monte-Carlo-Simulation:

- der Entwickler kann zuversichtlich sein, dass das System hinsichtlich der Drift von Komponenteneigenschaften eine festgelegte Zuverlässigkeit hat, falls alle Analyseergebnisse innerhalb der Spezifikationen liegen;
- passend für rechnergestützten Entwurf;
- beliebige Wahrscheinlichkeitsverteilung kann simuliert werden;
- simulierte Ergebnisse liegen meist nahe dem Optimum;
- es sind keine komplexen mathematischen Bearbeitungen notwendig.

### A.2.3.5 Einschränkungen

a) Momentverfahren:

- es werden mathematische Modelle benötigt, die differenzieren können;
- um vernünftige Analyseergebnisse zu erhalten, müssen alle Systemkomponenten betrachtet werden;
- komplexe mathematischen Bearbeitungen sind notwendig;
- es wird angenommen, dass die Wahrscheinlichkeitsverteilung die Normalverteilung ist.

b) Monte-Carlo-Simulation:

- es werden mathematische Modelle für die Simulation benötigt;
- um vernünftige Analyseergebnisse zu erhalten, müssen alle Systemkomponenten betrachtet werden;
- eine große Anzahl von Systemrepliken werden simuliert.

## A.2.4 Verfahren für die Vorhersage der Funktionsfähigkeit von Software

### A.2.4.1 Beschreibung und Verwendung

Der Zweck dieses Verfahrens ist es, die Funktionsfähigkeit von Software mit statistischen Verfahren vorherzusagen. Das Problem dabei ist, dass Software im Prinzip nicht ausfällt. Die Software kann jedoch bei gegebener fester Eingabe deterministisch korrekte oder fehlerhafte Ergebnisse produzieren. In dem zugrunde liegenden Modell nimmt man daher nicht an, dass die Software zufällig agiert, sondern dass die Systemkonfiguration und das Betriebsprofil (z. B. Eingabedaten) als eine Zufallsumgebung angesehen werden können.

### A.2.4.2 Anwendung

Die Vorhersage der Funktionsfähigkeit von Software kann während der Phase des Testens der Software angewendet werden als ein Mittel zum Entscheiden, ob das Testen beendet werden soll (für den Fall, dass ein Annahmekriterium gesetzt wurde) oder zum Vorhersagen der Funktionsfähigkeit im Betrieb. Üblicherweise werden die Daten in Gruppen zusammengefasst, z. B. als Anzahl der Ausfälle je kumulierter Ausführungsdauer, da es sehr schwer ist, echte Angaben zu den Zeitintervallen zwischen dem Auftreten von Ausfällen zu erhalten.

Bei den meisten Anwendungen nimmt man an, dass Versagen der Software als ein nicht-homogener Poisson-Prozess beschrieben werden kann. Man geht somit davon aus, dass die Zeitintervalle zwischen dem Auftreten von Software-bedingten Ausfällen statistisch voneinander unabhängig und exponentiell verteilt sind, dass aber die Ausfalldichte über der Zeit variiert. Man nimmt allgemein eine abnehmende Ausfalldichte an; in den Modellen geht man also davon aus, dass einmal gefundene Fehler anschließend erfolgreich entfernt wurden, ohne dabei neue Bugs einzuführen. Das Hauptziel bei der Vorhersage der Funktionsfähigkeit von Software ist die Bestimmung der Form der Ausfalldichtefunktion und die Schätzung ihrer Parameter anhand der beobachteten Ausfalldaten. Nachdem die Ausfalldichtefunktion bestimmt wurde, kann man mehrere Maßgrößen für die Funktionsfähigkeit ableiten. Hierzu gehören:

- kumulierte Anzahl von Ausfällen;
- Anzahl noch verbleibender Ausfälle;
- Dauer bis zum nächsten Ausfall;

- verbleibende Testdauer (bis zur Annahme);
- maximale Anzahl von Ausfällen (bezogen auf die Lebensdauer).

Andere Vorgehensweisen berücksichtigen die Softwarearchitektur als funktionale Module und modellieren zuerst deren Wechselwirkung und Ausführungsverhalten, z. B. durch Markoffsche Prozesse. In einem zweiten Schritt werden Daten erfasst und untersucht und hinsichtlich der Module bewertet.

#### **A.2.4.3 Schlüsselemente**

- Man lege relevante Maßgrößen für die Funktionsfähigkeit und Ziele fest.
- Man lege das für die Softwarefunktionsfähigkeit zu verwendende Modell fest.
- Man erfasse und untersuche die Ausfalldaten.
- Man validiere das Modell.
- Man sage aus den Daten hergeleitete Maßgrößen für die Funktionsfähigkeit vorher.

#### **A.2.4.4 Vorzüge**

- Softwareeinflüsse können in Vorhersagen für die Funktionsfähigkeit aufgenommen werden.
- Für das Testende können objektive Kriterien festgelegt und kontrolliert werden.

#### **A.2.4.5 Einschränkungen**

- Das Erfassen von Daten zur Funktionsfähigkeit von Software kann schwierig sein. Die Ergebnisse sind nur so gut wie die erfassten Daten.
- Es gibt mehrere Vorgehensweisen, aber weder für die Vorgehensweise noch für die Ausfalldichtefunktion sind bis jetzt Normen erschienen. Es besteht die Versuchung, das Modell so zu wählen, dass die Daten gut dazu passen, anstelle das Modell a priori festzulegen.
- Die theoretische Begründung für den nicht-homogenen Poisson-Prozess ist im Vergleich mit der Vorhersage der Funktionsfähigkeit von Hardware viel schwächer.

### **A.2.5 Analyse finiter Elemente**

#### **A.2.5.1 Beschreibung und Verwendung**

Analyse finiter Elemente ist ein rechnergestütztes numerisches Verfahren zum Analysieren von an physischen Einheiten anliegenden Belastungen; diese können mechanischer, thermischer, elektromagnetischer, strömungstechnischer Art oder Kombinationen davon sein. Das zu lösende Problem ist üblicherweise für klassische Verfahren zu komplex.

Dieses Verfahren unterscheidet sich aus Sicht der Behandlung einer Einheit grundlegend von klassischen Verfahren. Durch die infinitesimalen differentiellen Elemente, die in Kalkulus-, Differential- und partiellen Differentialgleichungen verwendet werden, wird eine Einheit als ein Kontinuum betrachtet. Bei der Analyse finiter Elemente wird die Einheit in einfache, miteinander in Beziehung stehende Bausteine, so genannte Elemente, unterteilt. Elemente sind gekennzeichnet durch Formfunktionen. Zusammen bilden sie ein geometrisches Modell der Einheit. Elemente sind an Knoten miteinander verbunden. Information wird von Element zu Element nur in der Ebene gemeinsamer Knoten weitergegeben. Um Kontinuität innerhalb von Elementen und über Elementgrenzen hinaus sicherzustellen, wird interpoliert. Somit können Auswirkungen an beliebigen Punkten der Einheit als Knotenverschiebungen ausgedrückt werden.

#### **A.2.5.2 Anwendung**

Analyse finiter Elemente ist ein wirksames Verfahren zur Vorhersage des Verhaltens und der Ausfallarten komplexer Strukturen. Man kann es zur Analyse vielfältiger technischer Probleme verwenden, wie etwa mechanische Belastungsanalysen, Schwingungen, Strömungsmechanik, Wärmeübertragung, elektromagnetische Felder und mehr.

#### **A.2.5.3 Schlüsselemente (Schritte)**

- Man wähle den geeignetsten Typ finiter Elemente zur Modellierung der Einheit.
- Man unterteile die Einheit in Elemente und lege die Eigenschaften der Elemente fest.
- Man stelle in einer Matrixdarstellung die Wechselwirkungen zwischen den Freiheitsgraden der Knoten zusammen.
- Man lege Grenzbedingungen fest und Belastungen an.

- Man löse den Satz algebraischer Gleichungen für die Matrix, um die Knotenverschiebungen zu berechnen.
- Man berechne die interessierenden physikalischen Parameter, z. B. Beanspruchung, Schwingungsarten.

#### **A.2.5.4 Vorzüge**

- Es können sowohl elastische als auch nicht elastische Effekte analysiert werden.
- Es können sowohl statische als auch dynamische Analysen durchgeführt werden.
- Es können Einheiten mit unregelmäßigen Formen, multiplen Grenzbedingungen und Belastungen als auch verschiedene Materialien analysiert werden.
- Es können Entwürfe optimiert werden.
- Die Funktionsfähigkeit kann bewertet und validiert werden.

#### **A.2.5.5 Einschränkungen**

- Erfordert einen hohen Grad speziellen Fachwissens.
- Ergebnisse können leicht falsch interpretiert oder umgesetzt werden.

### **A.2.6 Belastungsminderung und Auswahl von Teilen**

#### **A.2.6.1 Beschreibung und Verwendung**

Teile werden ausgewählt im Hinblick auf die zwei Kriterien Zuverlässigkeit und Fähigkeit der Teile, bei Verwendung in einem Produkt der erwarteten Beanspruchung durch Umgebung und Betrieb zu widerstehen. Bei der Auswahl der Teile ist sowohl die geforderte Zuverlässigkeit des Teils zu beachten als auch seine mechanische und elektrische Belastung unter Berücksichtigung der Beschreibung der Umgebung, in der die Teile ausfallfrei betrieben werden sollen.

Jeder elektronische (aktiv oder passiv) oder mechanische Bauelementtyp muss dahingehend beurteilt werden, ob seine spezifizierte thermische (Temperatur-)Belastung, Konstruktion sowie weitere spezifische Merkmale (mechanische oder andere) für die Einsatzumgebung geeignet sind. Diese Aufgabe kann man in folgenden Schritten bewerkstelligen:

- a) Beurteilung des Temperaturprofils eines Produktes (innerhalb des Gehäuses). Wenn dieses Profil nicht erarbeitet wurde, muss mit dem Entwicklungsteam darüber gesprochen werden, welche ungünstigste Temperatur zu erwarten sein wird.
- b) Bewertung anderer Angaben und Forderungen zur Umgebung des Produktes (klimatisch und dynamisch).
- c) Vergleich der Erkenntnisse aus den Schritten a) und b) mit den Bauelementespezifikationen und Bestimmung, ob jeder Bauelementtyp in der Lage sein wird, den thermischen und anderen Umgebungsbedingungen zu genügen.

Die Teile sollten so gewählt werden, dass deren annehmbare Zuverlässigkeit sichergestellt wird. Jedes Teil hat eine gewisse Ausfallwahrscheinlichkeit, die abhängt von seinem Einsatz, seiner Konstruktion und seiner Komplexität. Das Produkt (Baugruppe), in dem das Teil betrieben werden soll, hat seine eigenen Zuverlässigkeitsanforderungen. Aus diesem Grund müssen die Schlüsselteile einer Baugruppe bzw. Produktes, also diejenigen Teile, die für den Betrieb des Produktes unverzichtbar sind, so gewählt werden, dass diese eine annehmbare Überlebenswahrscheinlichkeit haben.

Belastungsminderung eines Teils bedeutet, dass man es geringeren betrieblichen und umgebungsbedingten Beanspruchungen aussetzt, mit dem Ziel, seine Ausfallwahrscheinlichkeit innerhalb der geforderten Betriebsdauer zu verringern.

Wenn man den Nennwert für die Widerstandsfähigkeit des Bauelementes mit der erwarteten Beanspruchung vergleicht, ist es wichtig, zwischen beiden einen gewissen Abstand zu lassen. Dieser kann auf der Grundlage der kumulativen Beanspruchung oder Ermüdungsbeanspruchung und der Widerstandsfähigkeit des Bauelementes oder aufgrund anderer technischer Analyseverfahren berechnet werden. Dieser Abstand ermöglicht das Erreichen der gewünschten Teilezuverlässigkeit hinsichtlich besonderer Fehlzustandsarten und deren jeweiligen Ursachen.

#### **A.2.6.2 Anwendung**

Die Auswahl von Teilen mit dem Ziel der Übereinstimmung mit den erwarteten Umgebungen und der Zuverlässigkeit muss auf alle Produktzuverlässigkeitsaufgaben angewendet werden. Belastungsminderung von

Teilen muss ein integraler Bestandteil der Entwicklungstätigkeiten sein, da Teile mit nicht sorgfältig geminderter Belastung Ursache für ein unzuverlässiges Produkt sein können.

### A.2.6.3 Schlüsselemente

Die Schlüsselemente für diesen Prozess sind:

- Angaben zur betrieblichen Umgebung der Teile und der Lagerbedingungen;
- Angaben zur Zuverlässigkeit der Teile in der Umgebung, für die das Produkt entwickelt werden muss;
- Leitfäden zur Belastungsminderung, ausgearbeitet im Hinblick auf die Produktzuverlässigkeit und unter Berücksichtigung erprobter Entwicklungsregeln.

### A.2.6.4 Vorzüge

Die Vorteile von Regeln für die Wahl von Teilen und deren Belastungsminderung sind das Erreichen der gewünschten Zuverlässigkeit.

### A.2.6.5 Einschränkungen

Die einzige Einschränkung dieser Verfahrensweise ist der Fall, dass es keine Angaben zur Teilezuverlässigkeit in den zugänglichen Datenbanken oder seitens des Bauelementeherstellers gibt. In diesem Fall sind Einschränkungen bei der Minderung der Belastung von Teilen gegeben, falls die Leitfäden zur Belastungsminderung sich auf die Zuverlässigkeit erstrecken. Falls die Leitfäden zur Belastungsminderung ohne Blick auf die Zuverlässigkeit befolgt werden, kann die Belastungsminderung zu weitgehend sein.

## A.2.7 Paretoanalyse

### A.2.7.1 Beschreibung und Verwendung

Die Paretoanalyse, auf der Grundlage des von dem italienischen Wirtschaftsfachmannes Vilfredo Pareto entwickelten Paretoprinzips, ist eines der sieben grundlegenden Werkzeuge der Qualitätslenkung (Strichlisten, Pareto-Diagramme, Ishikawa-Diagramme, Flussdiagramme, Histogramme, Korrelationsdiagramme und Kontrolldiagramme). Diese Werkzeuge, obwohl für die Zwecke der Qualitätslenkung entwickelt und dort breit verwendet, können auch für die Zuverlässigkeitstechnik nutzbringend angewendet werden. Das Paretoprinzip besagt, dass eine kleine Teilmenge der Probleme (die „entscheidenden paar“), die die gemeinsame Ausgabe beeinträchtigen, dazu tendieren, viel häufiger aufzutreten als der Rest (die „nützlichen vielen“). Dieses Prinzip kann man auch so beschreiben, dass „80 % der Fehler aus 20 % der Ursachen entstehen“.

Der Zweck der Paretoanalyse ist es, die Bemühungen auf Probleme mit dem höchsten Potenzial für Verbesserungen zu lenken und dabei zu helfen, Mittel mit Priorität dort einzusetzen, wo sie am wirksamsten sind.

Das Pareto-Diagramm ist eines der am meisten verwendeten Verbesserungswerkzeuge. Es zeigt die relative Bedeutung des Problems in einer einfachen, schnell interpretierbaren visuellen Form. Es hilft zu vermeiden, das „Problem zu verschieben“ durch eine Lösung, die einige Ursachen beseitigt, aber andere verschlimmert. Es kann die Auswirkung einer Entwurfsänderung auf die Produktleistung durch gewollte Variationen messen:

- Hauptursache für Zusammenbrüche: in diesem Fall wird die schlankeste Säule in Untermengen zu einem verbundenen Pareto-Diagramm aufgespalten;
- vor und nach der Analyse: in diesem Fall werden die neuen Pareto-Säulen Seite an Seite mit dem ursprünglichen Pareto gezeichnet und zeigen dadurch die Auswirkung einer Änderung;
- Änderung der Datenquelle: in diesem Fall werden Daten zu demselben Problem, aber aus unterschiedlichen Quellen (Systeme/Geräte, Ort, Kunde usw.) erfasst und in Seite-an-Seite-Pareto-Diagrammen gezeigt;
- Änderungsmessung: in diesem Fall werden dieselben Kategorien verwendet, aber unterschiedlich gemessen (z. B. Kosten und Häufigkeit).

### A.2.7.2 Anwendung

Eine Paretoanalyse kann während aller Phasen (Konzept- und Definitionsphase, Entwurfs- und Entwicklungsphase, Fertigungsphase, Einbauphase, Betriebs- und Instandhaltungsphase) eines Zuverlässigkeitsprogramms angewendet werden.

### A.2.7.3 Schlüsselemente

Um Paretoanalyseverfahren wirksam durchzuführen, müssen folgende Betrachtungen angestellt werden:

- entscheiden, über welches Problem man mehr wissen möchte (z. B. Ausfälle und damit verbundene Ursachen);
- Ursachen oder Probleme auswählen, die überwacht, verglichen und nach Klassen (anhand vorhandener Daten, Brainstorming, Fachwissen) geordnet werden sollen;
- die bedeutungsvollste Maßeinheit wählen, z. B. Häufigkeit oder Kosten;
- den Zeitabschnitt für die Untersuchung wählen;
- die zu analysierenden Daten zusammenfassen und die Einheiten der Größe nach auflisten, beginnend mit der größten;
- die Summe aller Einheiten und den jeweiligen prozentualen Anteil jeder Einheit an der Summe berechnen;
- das Säulendiagramm mit den Kategorien auf der horizontalen Achse und den Häufigkeiten (oder Kosten) auf der vertikalen Achse zeichnen;
- falls angebracht, eine Hüllkurve einzeichnen;
- das Diagramm mit passenden Bezeichnungen versehen;
- Ergebnisse interpretieren.

### A.2.7.4 Vorzüge

- Der Anwender erhält eine wirkungsvolle graphische Darstellung des analysierten Problems.
- Es ist ein sehr einfaches Verfahren und erfordert nicht viel Zeit und Aufwand.
- Es kann zur Entscheidungsfindung in technischen als auch nicht-technischen Gebieten verwendet werden.

### A.2.7.5 Einschränkungen

- Das Pareto-Diagramm ist lediglich ein Werkzeug zur Darstellung von Daten in einer nützlichen Weise. Die Untersuchung zur Ursache eines Problems muss von Fachleuten mit dafür geeigneten Verfahren gemacht werden.
- Erfahrung und gesunder Menschenverstand müssen verwendet werden; manche Kundenbeschwerden verdienen möglicherweise mehr Aufmerksamkeit als viele andere Beschwerden, dies hängt davon ab, wer der Kunde und was die Beschwerde ist.

## A.2.8 Ursache-Wirkung-Diagramm

### A.2.8.1 Beschreibung und Verwendung

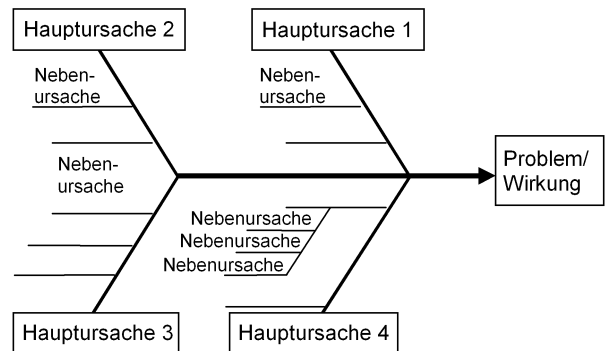
Das Ursache-Wirkung-Diagramm wird auch das Ishikawa-Diagramm (nach seinem Entwickler, dem Japaner Kaoru Ishikawa) oder das Fischgrätendiagramm (aufgrund seiner Form) genannt. Es veranschaulicht in einer bildlichen Darstellung mögliche Ursachen von Problemen oder von Faktoren, die zum Erreichen des Erfolgs benötigt werden oder die zum Ausfall führen, und hilft bei deren Ermittlung und Organisation.

Es ist ein wirksames Werkzeug, mit dem man leicht die Beziehungen zwischen Faktoren sehen kann, und es unterstützt die Untersuchung von Prozessen, Situationen und die Planung.

Ursache-Wirkung-Diagramme werden typischerweise mittels Brainstorming-Verfahren erarbeitet. Im Ergebnis werden sie oft von Hand auf Papier gezeichnet. Es gibt jedoch Software-Pakete, mit denen das Diagramm professionell dargestellt werden kann.

- 1) Problem beschreiben
- 2) Ermitteln der Hauptursachen
- 3) Ermitteln der Nebenursachen
- 4) Ermitteln der wahrscheinlichsten Nebenursachen

ANMERKUNG Im Schritt b) wird oft die 4-M-Methode verwendet: Mensch, Maschine, Methoden und Material. Andere Hauptursachen können auch verwendet werden, z. B. Prozessabläufe.



**Bild A.15 – Ursache-Wirkung-Diagramm**

#### A.2.8.2 Anwendung

Ursache-Wirkung-Diagramm wird für vorläufige Analysen während der Entwurfsphase und Analyse von im Betrieb aufgetretenen Problemen verwendet.

#### A.2.8.3 Schlüsselemente

- Die Wirkungen müssen von allen verstanden werden.
- Die genannten Ursachen müssen für das Problem von Belang sein.
- Eine angemessene Anzahl von Nebenursachen hilft, die Baumstruktur übersichtlich zu halten.
- Wirkliche Ursachen müssen durch vorhandene Daten und Fakten untermauert werden.
- Wenn Substrukturen zu komplex werden oder zu einfach bleiben, könnte dies ein Hinweis dafür sein, dass die Struktur zur besseren Beurteilung optimiert werden kann.

#### A.2.8.4 Vorzüge

- Ermutigt und unterstützt die Arbeit von interdisziplinären Teams.
- Liefert eine visuelle Darstellung von Ursachen und deren Zusammenfassung.
- Ergebnisse können als Eingabe für FMEA oder Fehlzustandsbaumanalysen benützt werden.

#### A.2.8.5 Einschränkungen

- Keine quantitativen Analysen;
- Wahl der richtigen Ursachen und Nebenursachen hängt von der Erfahrung des Teams ab;
- multiple Konsequenzen werden nicht erfasst.

### A.2.9 Analyse der Ausfallberichte und Korrekturmaßnahmen

#### A.2.9.1 Beschreibung und Verwendung

Analyse der Ausfallberichte und Korrekturmaßnahmen (en: Failure Reporting Analysis and Corrective Action, FRACAS) ist ein geschlossenes System zum fristgerechten Ermitteln, Beurteilen und Korrigieren von Problemen aufgrund von Ausfällen. Ausfälle, die während Prüfungen und Beurteilungen auftreten, werden dokumentiert. Daten werden in verschiedenen Ebenen erfasst. Das System wird dazu verwendet, Teileprobleme, Entwurfsfehler, schlechte Ausführung und Prozessschwächen zu verfolgen, diese zu analysieren und festzustellen, damit diese dann korrigiert werden können. Die Entwicklung von Korrekturmaßnahmen folgt auf die Feststellung der eigentlichen Ursache des Ausfalls. Die Wirksamkeit von Korrekturmaßnahmen wird vor der Umsetzung verifiziert.

#### A.2.9.2 Anwendung

FRACAS sollte eingeführt sein, sobald Hardware und Software verfügbar sind. Alle mit Prüfung und Beurteilung befassten Personen sind für das Dokumentieren von Ausfällen verantwortlich. Ausfälle werden so weit als möglich verifiziert und lokalisiert.

Ein Bewertungsteam analysiert die Daten, um die Signifikanz von Problemen zu bestimmen, es bestimmt, welche Probleme Korrekturmaßnahmen erfordern, und stellt sicher, dass diese sauber gelöst werden. Alle Disziplinen, die möglicherweise durch die Probleme berührt sein könnten, sind in dem Team vertreten.

Ausfallanalysen werden bis zur notwendigen Ebene durchgeführt, um Korrekturmaßnahmen für die Beseitigung der Probleme auszuarbeiten. Die Verifizierung der Wirksamkeit der Korrekturmaßnahmen beinhaltet die Feststellung seitens des Teams, dass die Wiederkehr der Ausfälle verhindert ist.

#### **A.2.9.3 Schlüsselemente**

- Ein auf das gerade entwickelte System und den Entwicklungsprozess zugeschnittenes Berichtsformat,
- eine für das Dokumentieren aller auf die Analyse bezogenen Tätigkeiten und für das Lösen von Problemen geeignete Datenbasis,
- ein multidisziplinäres Bewertungsteam,
- ein Mechanismus für das Verfolgen von Problemlösungen.

#### **A.2.9.4 Vorzüge**

- Das Verfahren kann Daten verwenden, die bei sehr unterschiedlichen Betriebs- und Umweltbedingungen erfasst wurden.
- Es kann für Entwurf und Entwicklung, Fertigung und Instandhaltung verwendet werden.
- Es kann ein wichtiger Beitrag für Zuverlässigkeitswachstum sein.
- Es kann Daten aus früheren Projekten verwenden und für zukünftige Projekte Daten bereitstellen.

#### **A.2.9.5 Einschränkungen**

- Es verhindert lediglich das wiederholte Auftreten von Problemen.
- Es hängt davon ab, wie Ausfälle aus Prüfungen, Beurteilungen und Instandhaltung berichtet werden.
- Es ist oft umständlich, Daten für numerische Schätzungen zu kombinieren.



## Literaturhinweise

Diese Literaturhinweise sind als Ausgangspunkt für weiteres Lesen gedacht. Absichtlich wird lediglich eine repräsentative Quelle angegeben.

IEC 60300-2:1995, *Dependability management – Part 2: Dependability programme elements and tasks*.

ANMERKUNG Harmonisiert als EN 60300-2:1996 (nicht modifiziert).

### Vorhersage der Ausfallrate

BAJENESCU, T.I., BAZU, M.I., *Reliability of Electronic Components*, Springer, 1999.

### Fehlzustandsbaumanalyse

ROBERTS, et al. (1981), „*Fault Tree Handbook*“, US Nuclear Regulatory Commission, Washington, D.C., USA, 1981.

### Ereignisbaumanalyse

ANG, A.H-S., TANG, W.H., *Probability Concepts in Engineering Planning and Design; Volume II Decision, Risk, and Reliability*, 1990.

### Zuverlässigkeits-Blockdiagramme

SAE JA1000-1, *Reliability Program Standard Implementation Guide*; Issued 1999-03.

### Markoffanalyse

STEWART, W.J., *Introduction to the Numerical Solution of Markov Chains*, Princeton University Press, 1994.

### Petri-Netz-Analyse

SCHNEEWEISS, W., *Petri Nets for Reliability Modelling*, LiLoLe, Hagen, 1999.

### FMEA

SAE ARP5580, „*Failure mode, effects and criticality analysis*“.

SAE J1739, *Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) Reference Manual*.

### HAZOP

REDMILL, F., CHUDLEIGH, M., CATMUR, J., *HAZOP and Software HAZOP*, Wiley, 1999.

### Analyse der menschlichen Zuverlässigkeit

Dhillon, B.S., *Human Reliability with Human Factors*, Pergamon Press, 1988.

### Beanspruchungsanalyse

Shu-Ho Dai, Ming-O Wang, *Reliability Analysis in Engineering Applications*, van Nostrand Reinhold, New York, 1992.

### Wahrheitstabelle

VILLEMEUR, A., *Reliability, Availability, Maintainability and Safety Assessment*, vol. 1 and vol. 2, John Wiley & Sons, 1992.

### Statistische Zuverlässigkeitsverfahren

MEEKER, W.Q., ESCOBAR, L.A., *Statistical methods for reliability data*, John Wiley, 1998.

### Kriechwegeanalyse

GODOY, S.G., ENGELS, G.J., *Sneak Analysis and Software Sneak Analysis*, J. Aircraft Vol. 15, No. 8, 1978.

### Analyse des ungünstigsten Falls

IRESON, W.G., COOMBS, C.F.Jr., MOSS, R.Y., *Handbook of Reliability Engineering and Management*, McGraw-Hill 1996.

**Variationssimulations-Modellierung**

LAW, A.M., KELTON, W.D., *Simulation modelling and analysis*, McGraw-Hill, 1991.

**Verfahren für die Vorhersage der Funktionsfähigkeit von Software**

LYU, M.R. (Ed.), *Handbook of Software Reliability Engineering*, IEEE Computer Society Press, 1995.

**Analyse finiter Elemente**

ADAMS, A., ASKENAZI, M.V., *Building Better Products With Finite Element Analysis*, Thomson Learning, 1998.

**Belastungsminderung und Auswahl von Teilen**

FUQUA, N.B., *Reliability Engineering for Electronic design*, Dekker, 1986.

**Paretoanalyse**

SAE JA-1, *Reliability Program Standard Implementation Guide*, Warrendale, PA, 1999.

**Ursache-Wirkung-Diagramme**

KUNE, H., *Statistical Methods for Quality Improvement*, AOTS, 1985.

**FRACAS**

MIL-HDBK-2155, *Failure Reporting, Analysis and Corrective Action System (FRACAS)*, 1995.

---

## Anhang ZA (normativ)

### Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ANMERKUNG Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod), dann gilt die entsprechende EN oder das HD.

Publikation	Jahr	Titel	EN/HD	Jahr
IEC 60050-191	1990	International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service	–	–
IEC 60300-3-2	1993	Dependability management – Part 3: Application guide – Section 2: Collection of dependability data from the field	–	–
IEC 60300-3-4	1996	Part 3: Application guide – Section 4: Guide to the specification of dependability requirements	–	–
IEC 60300-3-5	2001	Part 3-5: Application guide – Reliability test conditions and statistical test principles	–	–
IEC 60300-3-10	2001	Part 3-10: Application guide – Maintainability	–	–
IEC 60706-1	1982	Guide on maintainability of equipment – Part 1 – Sections 1, 2 and 3: Introduction, requirements and maintainability programme	–	–
IEC 60706-2	1990	Part 2 – Section 5: Maintainability studies during the design phase	–	–
IEC 60812	1985	Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)	HD 485 S1	1987
IEC 61078	1991	Analysis techniques for dependability – Reliability block diagram method	EN 61078	1993
IEC 61165	1995	Application of Markov techniques	–	–
IEC 61709	1996	Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion	EN 61709	1998
IEC 61882	2001	Hazard and operability studies (HAZOP studies) – Application guide	–	–
ISO 9000	2000	Quality management systems – Fundamentals and vocabulary	EN ISO 9000	2000