DEUTSCHE NORM November 2006

DIN EN 60812

ICS 21.020; 29.020

Ersatz für
DIN 25448:1990-05
Siehe jedoch Beginn der Gültigkeit

Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (IEC 60812:2006); Deutsche Fassung EN 60812:2006

Analysis techniques for system reliability –
Procedure for failure mode and effects analysis (FMEA) (IEC 60812:2006);
German version EN 60812:2006

Techniques d'analyse de la fiabilité du système –
Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)
(CEI 60812:2006);
Version allemande EN 60812:2006

Gesamtumfang 48 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Preisgruppe 19
www.din.de
www.beuth.de

9771315

Beginn der Gültigkeit

Die von CENELEC am 2006-03-01 angenommene EN 60812 gilt als DIN-Norm ab 2006-11-01.

Daneben darf DIN 25448:1990-05 noch bis 2009-03-01 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 60812:2001-10.

Für diese Norm ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (http://www.dke.de) zuständig.

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

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem auf der IEC-Website unter „http://webstore.iec.ch“ mit den Daten zu dieser Publikation angegebenen Datum (maintenance result date) 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.

Änderungen

Gegenüber DIN 25448:1990-05 wurden folgende Änderungen vorgenommen:

a) Betrachtung von Ausfällen mit gemeinsamer Ursache;

b) Einbeziehung menschlicher Einflüsse;

c) Behandlung von Softwarefehlern;

d) Einführung des Konzeptes von Fehlzustandsart-Auswirkungen und -Kritizität;

e) Einbeziehung von in der Autoindustrie verbreitet genutzten Methoden;

f) Ergänzte normative Verweisungen und Zusammenhänge mit anderen Fehlzustandsart-Analyse-Methoden;

g) ergänzte Beispiele;

h) Behandlung von Vorteilen und Nachteilen unterschiedlicher FMEA-Methoden.

Frühere Ausgaben

DIN 25448: 1980-06, 1990-05

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN 60812

Mai 2006

ICS 03.120.01; 03.120.30; 21.020

Ersatz für HD 485 S1:1987

Deutsche Fassung

Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA)

(IEC 60812:2006)

Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)
(IEC 60812:2006)

Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)
(CEI 60812:2006)

Diese Europäische Norm wurde von CENELEC am 2006-03-01 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, Rumänien, 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

Ref. Nr. EN 60812:2006 D

Vorwort

Der Text des Schriftstücks 56/1072/FDIS, zukünftige 2. Ausgabe von IEC 60812, ausgearbeitet von dem IEC/TC 56 „Dependability“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2006-03-01 als EN 60812 angenommen.

Diese Europäische Norm ersetzt HD 485 S1:1987.

Die wesentlichen Änderungen gegenüber HD 485 S1:1987 sind folgende:

– Einführung des Konzeptes von Fehlzustandsart-Auswirkungen und -Kritizität;
– Einbeziehung von in der Autoindustrie verbreitet genutzten Methoden;
– ergänzte normative Verweisungen und Zusammenhänge mit anderen Fehlzustandsart-Analyse-Methoden;
– ergänzte Beispiele;
– Behandlung von Vorteilen und Nachteilen unterschiedlicher FMEA-Methoden.

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): 2006-12-01

– spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2009-03-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 60812:2006 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 60300-1 ANMERKUNG Harmonisiert als EN 60300-1:2003 (nicht modifiziert).

IEC 60300-2 ANMERKUNG Harmonisiert als EN 60300-2:2004 (nicht modifiziert).

IEC 61160 ANMERKUNG Harmonisiert als EN 61160:2005 (nicht modifiziert).

ISO 9000 ANMERKUNG Harmonisiert als EN ISO 9000:2000 (nicht modifiziert).

Inhalt

Seite

Vorwort 2
1 Anwendungsbereich 5
2 Normative Verweisungen 5
3 Begriffe 5
4 Überblick 6
4.1 Einleitung 6
4.2 Zweck und Ziele der Analyse 8
5 Fehlzustandsart- und -auswirkungsanalyse (FMEA) 8
5.1 Allgemeine Betrachtungen 8
5.2 Vorausgehende Arbeiten 9
5.3 Ausfallbedeutungsanalyse (FMECA) 17
5.4 Bericht über die Analyse 26
6 Weitere Betrachtungen 27
6.1 Ausfälle mit gemeinsamer Ursache 27
6.2 Menschliche Einflüsse 28
6.3 Softwarefehler 28
6.4 FMEA bezüglich der Folgen eines Systemausfalls 28
7 Anwendungen 29
7.1 Anwendung von FMEA und FMECA 29
7.2 Vorteile der FMEA 30
7.3 Grenzen und Unzulänglichkeiten der FMEA 31
7.4 Beziehungen zu anderen Verfahren 31
Anhang A (informativ) Zusammenfassung der Verfahrensschritte für FMEA und FMECA 33
A.1 Schritte zur Durchführung der Analyse 33
A.2 FMEA-Arbeitsblatt 33
Anhang B (informativ) Analysebeispiele 37
B.1 Beispiel 1 – FMEA für ein Teil einer Automobilelektronik mit Berech-nung der Risikoprioritätszahl 37
B.2 Beispiel 2 – FMEA für Teilsystem eines Motor-Generator-Satzes 40
B.3 Beispiel 3 – FMECA für einen Herstellprozess 43
Literaturhinweise 45
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen 46

Bild 1 – Zusammenhang zwischen Ausfallarten und Ausfallauswirkungen in einer Systemhierarchie 11
Bild 2 – Ablaufdiagramm für die Analyse 17
Bild 3 – Kritizitätsmatrix 21
Bild A.1 – Beispiel für das Format eines FMEA-Arbeitsblattes 36
Bild B.1 – FMEA für ein Teil der Automobilelektronik mit Berechnung der Risikoprioritätszahl 39

Seite
Bild B.2 – Diagramm der Teilsysteme eines Motor-Generator-Satzes ... 40
Bild B.3 – Diagramm der Systeme „Heizung, Lüftung und Kühlung des Gehäuses“ ... 41
Bild B.4 – FMEA für Teilsystem 20 ... 42
Bild B.5 – Teil einer Pozess-FMECA für Aluminiumstrangpressen ... 44

Tabelle 1 – Beispiel eines Satzes allgemeiner Ausfallarten ... 13
Tabelle 2 – Erläuterndes Beispiel einer Schwere-Klassifizierung für Endauswirkungen ... 16
Tabelle 3 – Risiko-/Kritizitätsmatrix ... 22
Tabelle 4 – Schwere der Ausfallart ... 23
Tabelle 5 – Auftreten der Ausfallart in Bezug auf Eintrittshäufigkeit und -wahrscheinlichkeit ... 24
Tabelle 6 – Beurteilungskriterien für die Ausfallarterkennung ... 25
Tabelle 7 – Beispiel für Ausfallauswirkungen (für einen Kfz-Anlasser) ... 26
Tabelle 8 – Beispiel für Wahrscheinlichkeiten von Ausfallauswirkungen ... 27
Tabelle B.1 – Definition und Klassifizierung der Schwere der Auswirkungen von Ausfällen auf das gesamte M-G-System ... 40

1 Anwendungsbereich

Diese Internationale Norm beschreibt Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) und die Fehlzustandsart-, -auswirkungs- und -kritizitätsanalyse (FMECA) und gibt Anleitung, wie diese Verfahren angewandt werden können, um eine Reihe von Zielen zu erreichen, indem

– die zur Durchführung einer Analyse notwendigen Verfahrensschritte bereitgestellt werden,

– geeignete Benennungen, Voraussetzungen, Maßgrößen für die Bedeutung (Kritizität) sowie Fehlzustandsarten genannt werden,

– grundlegende Prinzipien erklärt werden,

– Beispiele für die notwendigen Arbeitsblätter oder andere Tabellenformen bereitgestellt werden.

Alle für FMEA gemachten allgemeinen qualitativen Betrachtungen gelten auch für FMECA, da Letztere eine Erweiterung der FMEA ist.

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 60300-3-1:2003, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

IEC 61025, *Fault tree analysis (FTA)*

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

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1
(Betrachtungs-)Einheit
Teil, Komponente, Gerät, Subsystem, Funktionseinheit, Betriebsmittel oder System, das/die einzeln betrachtet werden kann

ANMERKUNG 1 Eine Betrachtungseinheit kann aus Hardware, Software oder beidem bestehen und kann in besonderen Fällen auch Personen einschließen.

ANMERKUNG 2 Eine Anzahl von Betrachtungseinheiten, z. B. eine Grundgesamtheit oder eine Stichprobe, kann selbst als Betrachtungseinheit aufgefasst werden.

[IEV 191-01-01]

Ein Prozess kann auch als eine Einheit definiert werden, die eine vorgegebene Funktion ausführt und für die eine Prozess-FMEA oder -FMECA durchgeführt wird. Eine Hardware-FMEA befasst sich normalerweise nicht mit Personen und ihren Wechselbeziehungen mit Hardware/Software, während eine Prozess-FMEA üblicherweise Handlungen von Personen einbezieht.

3.2
Ausfall
Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen

[IEV 191-04-01]

3.3
Fehlzustand
Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei die durch Wartung oder andere geplante Handlungen bzw. durch das Fehlen äußerer Mittel verursachte Funktionsunfähigkeit ausgeschlossen ist

ANMERKUNG 1 Ein Fehlzustand ist oft das Ergebnis eines Ausfalls der Einheit selbst, er kann aber auch ohne vorherigen Ausfall vorhanden sein.

[IEV 191-05-01]

ANMERKUNG 2 Im vorliegenden Dokument wird „Fehlzustand“ aus historischen Gründen austauschbar mit der Benennung „Ausfall“ verwendet.

3.4
Ausfallauswirkung
Folge einer Ausfallart hinsichtlich des Betriebs, der Funktion oder des Zustands einer Einheit

3.5
Ausfallart
Art und Weise, auf die eine Einheit ausfällt

3.6
Ausfall-Kritizität[N1] (Ausfallbedeutung)
Kombination der Schwere einer Auswirkung und der Häufigkeit ihres Auftretens oder anderer Eigenschaften eines Ausfalls als Maß der Notwendigkeit, sich damit zu befassen und sie zu herabzusetzen

3.7
System
Satz von in Wechselbeziehung oder Wechselwirkung stehenden Elementen

ANMERKUNG 1 Im Zusammenhang mit Zuverlässigkeit besteht ein System aus:

a) einem vorgegebenen Zweck, der durch die beabsichtigten Funktionen beschrieben ist;

b) festgelegten Betriebs- und Einsatzbedingungen [siehe IEV 191-01-12];

c) einer definierten Begrenzung.

ANMERKUNG 2 Die Struktur eines Systems ist hierarchisch.

[ISO 9000:2000]

3.8
Ausfallschwere
Bedeutung oder Einstufung der Auswirkung der Ausfallart auf den Betrieb der Einheit, die Umgebung der Einheit oder auf den Benutzer der Einheit; Schwere der Auswirkung der Ausfallart in Bezug auf die definierten Grenzen des untersuchten Systems

4 Überblick

4.1 Einleitung

Fehlzustandsart- und -auswirkungsanalyse (FMEA) ist ein systematisches Vorgehen bei der Analyse eines Systems, um mögliche Fehlzustandsarten, ihre Ursachen und ihre Auswirkungen auf das Systemverhalten zu ermitteln (Verhalten der übergeordneten Baugruppe und des gesamten Systems oder eines Prozesses). Dabei wird die Benennung System verwendet als Platzhalter für Hardware, Software (und ihre Wechselwirkung) oder für einen Prozess. Die Analyse wird erfolgreich vorzugsweise im frühen Entwicklungszyklus durchgeführt, damit die Behebung oder Entschärfung der Fehlzustandsart möglichst

---

N1) Nationale Fußnote: In DIN 25448 mit Ausfallbedeutung bezeichnet; englisch: failure criticality.

kostenwirksam ist. Mit der Analyse kann begonnen werden, sobald das System so weit festgelegt ist, dass es als Funktionsblockdiagramm dargestellt werden kann, in dem die Funktionen seiner Elemente definiert werden können.

Wichtig ist die Wahl des richtigen Zeitpunkts für eine FMEA; wenn sie früh genug im Entwicklungszyklus durchgeführt wird, dann kann die Berücksichtigung von Entwurfsänderungen zur Behebung aufgedeckter Schwächen kostengünstig sein. Daher ist es wichtig, dass die Aufgabe FMEA und die dabei durchzuführenden Arbeiten im Entwicklungsplan und -zeitplan berücksichtigt werden. FMEA ist daher ein iterativer Prozess, der den Entwurfsprozess begleitet.

FMEA kann auf unterschiedlichen Stufen der Systemzerlegung angewandt werden, von der höchsten Ebene eines Blockdiagramms bis hinunter zu den Funktionen diskreter Bauteile oder Softwarebefehle. Die FMEA ist darüber hinaus ein iterativer Prozess, der fortgeschrieben wird, sobald sich der Entwurf weiterentwickelt. Entwurfsänderungen werden die Überprüfung und Aktualisierung wesentlicher Teile der FMEA erfordern.

Eine gründliche FMEA ist das Ergebnis eines Teams, das sich aus Individuen zusammensetzt, die geeignet sind, die Schwere und die Konsequenzen unterschiedlichster möglicher Unzulänglichkeiten im Produktentwurf, die zu Ausfällen führen können, zu erkennen und zu bewerten. Vorteil der Teamarbeit ist, dass sie den Denkprozess anregt und das notwendige Fachwissen sicherstellt.

FMEA ist eine Methode zum Bestimmen der Schwere möglicher Ausfallarten und zum Bereitstellen von Eingangsinformationen für Risikoverringerungsmaßnahmen. Darüber hinaus stellt die FMEA in manchen Anwendungen einen Schätzwert für die Eintrittswahrscheinlichkeit der Ausfallarten bereit. Das wertet die Untersuchung durch Bereitstellen eines Maßes für die Wahrscheinlichkeit der Ausfallart auf.

Der FMEA-Anwendung geht eine hierarchische Zerlegung des Systems (Hardware mit Software, oder ein Prozess) in seine wichtigeren Grundbestandteile voraus. Es ist zweckmäßig, zur Illustration dieser Zerlegung einfache Blockdiagramme zu verwenden (IEC 61078). Die Analyse beginnt dann mit den Elementen der untersten Ebene. Die Auswirkung einer Ausfallart auf einer niedrigeren Ebene kann dann eine Ausfallursache für eine Ausfallart einer Einheit der nächsthöheren Ebene werden. Die Analyse schreitet von unten nach oben fort, bis die End-Auswirkung auf das System bestimmt ist. Bild 1 veranschaulicht diese Beziehung.

FMECA (Fehlzustandsart-, -auswirkungs- und -kritizitätsanalyse) ist eine Erweiterung der FMEA, die ein Mittel zur Klassifizierung der Schwere der Ausfallarten enthält, um die Einstufung der Dringlichkeit von Abhilfemaßnahmen zu ermöglichen. Dies geschieht durch Kombination des Maßes für die Schwere mit der (erwarteten) Eintrittshäufigkeit, um so eine „Kritizität“ genannte Metrik zu erzeugen.

Die FMEA-Prinzipien können auch außerhalb der konstruktiven Entwurfsarbeit angewendet werden. Das FMEA-Verfahren kann auf einen Herstellprozess oder jeden anderen Arbeitsprozess angewandt werden, wie in Krankenhäusern, medizinischen Laboratorien, Schulsystemen oder anderswo. Wenn FMEA auf einen Herstellprozess angewandt wird, ist dieses Verfahren in der Industrie bekannt als Prozess-FMEA oder PFMEA. Damit eine FMEA erfolgreich ist, müssen angemessene Ressourcen für die Teamarbeit zugestanden werden. Ein genaues Verständnis des analysierten Systems ist für eine vorläufige FMEA nicht unbedingt notwendig. Mit dem Fortschreiten des Entwurfes erfordert eine detaillierte Ausfallartanalyse gründliche Kenntnisse der Entwurfsfunktionen und ihrer Spezifikationen. Umgangreiche technische Entwurfsarbeiten erfordern üblicherweise die Einbindung von Entwurfsfachwissen aus mehreren Gebieten (z. B. Maschinenbau, Elektrotechnik, Systemtechnik, Softwaretechnik, Instandhaltungsunterstützung usw.).

FMEA behandelt üblicherweise einzelne Ausfallarten und die Auswirkung dieser Ausfallarten auf das System. Alle Ausfallarten werden als voneinander unabhängig angesehen. Das Verfahren ist daher ungeeignet für die Betrachtung abhängiger Ausfälle oder von Ausfällen, die sich aus einer Folge von Ereignissen ergeben. Um solche Situationen zu behandeln, können andere Methoden und Verfahren notwendig sein, wie etwa Markoff-Analyse (siehe IEC 61165) oder Störungsbaumanalyse (siehe IEC 61025).

Zur Bestimmung der Auswirkung eines Ausfalls müssen die auf höherer Ebene hervorgerufenen, resultierenden Ausfälle und möglicherweise auch die auf gleicher Ebene hervorgerufenen betrachtet werden. Die Analyse sollte, wo immer möglich, die Kombination von Ausfallarten oder deren Folge angeben, die Ursache einer Auswirkung auf höherer Ebene war. In diesem Fall ist zusätzliche Modellbildung erforderlich, um das Ausmaß oder die Eintrittswahrscheinlichkeit einer solchen Auswirkung abzuschätzen.

FMEA ist ein flexibles Hilfsmittel, das an besondere Industrie- oder Produkterfordernisse angepasst werden kann. Spezielle Arbeitsblätter mit besonderen Spalteneingängen können für bestimmte Anwendungen entworfen werden. Wenn Kategorien für die Schwere von Ausfallarten definiert werden, dann können sie für verschiedene Systeme oder verschiedene Systemebenen unterschiedlich definiert werden.

4.2 Zweck und Ziele der Analyse

Gründe für die Durchführung einer Fehlzustandsart- und -auswirkungsanalyse (FMEA) oder Fehlzustandsart-, -auswirkungs- und -kritizitätsanalyse (FMECA) können u. a. folgende sein:

a) Erkennen solcher Ausfälle, die unerwünschte Auswirkungen auf den Systembetrieb haben, z. B. Ausschließen oder signifikante Verschlechterung der Funktion oder Beeinträchtigung der Sicherheit des Benutzers;

b) Erfüllen vertraglicher Forderungen eines Kunden, soweit zutreffend;

c) Ermöglichen von Verbesserungen der Systemfunktionsfähigkeit oder der Sicherheit (z. B. durch Entwurfsmodifikationen oder Qualitätssicherungsmaßnahmen);

d) Ermöglichen der Verbesserung der Instandhaltbarkeit des Systems (durch Aufzeigen von Bereichen mit Risiko oder Bereichen, in denen keine Instandhaltbarkeit gegeben ist).

Angesichts dieser Gründe für die Durchführung einer FMEA können die Ziele einer FMEA (oder FMECA) Folgendes einschließen:

a) ein umfassendes Erkennen und Beurteilen aller unerwünschten Auswirkungen innerhalb der festgelegten Grenzen des analysierten Systems und die Ereignisfolgen, die durch jede erkannte Ausfallart einer Einheit auf verschiedenen Ebenen der Funktionshierarchie des Systems ausgelöst wurden, aus welchem Grund auch immer;

b) das Feststellen der Bedeutung und der Dringlichkeit für das Aufgreifen/Entschärfen (siehe Abschnitt 6) jeder Ausfallart hinsichtlich der korrekten Funktion oder Leistung des Systems und der Wirkung auf den betroffenen Prozess;

c) eine Klassifizierung der erkannten Ausfallarten entsprechend relevanter Eigenschaften; hierzu gehören Erkennbarkeit, Diagnosefähigkeit, Prüfbarkeit, Vorkehrungen für Ersatz und Betreiben (Reparatur, Instandhaltung, Logistik usw.);

d) Identifizierung von Funktionsausfällen des Systems und Abschätzung von Maßgrößen für die Ausfallschwere und Ausfallwahrscheinlichkeit;

e) Entwicklung eines Entwurfsverbesserungsplans zur Verringerung von Ausfallarten;

f) Unterstützung der Entwicklung eines wirksamen Instandhaltungsplans, um die Wahrscheinlichkeit für Ausfälle zu verringern (siehe IEC 60300-3-11).

ANMERKUNG Wenn Ausfallbedeutung (Kritizität) oder Eintrittswahrscheinlichkeit angesprochen sind, betreffen die Kommentare die FMECA-Methode.

5 Fehlzustandsart- und -auswirkungsanalyse (FMEA)

5.1 Allgemeine Betrachtungen

Traditionell gibt es große Bandbreiten in der Art, wie FMEA durchgeführt und die Ergebnisse dargestellt werden. Die Analyse wird üblicherweise so durchgeführt, dass die Ausfallarten, ihre jeweiligen Ursachen sowie unmittelbare Auswirkungen und Auswirkungen auf die Systemebene ermittelt werden. Die Ergebnisse der Analyse können in einem Arbeitsblatt dargestellt werden, das einen Kern von wesentlichen Informationen für das gesamte System enthält sowie Detailinformationen für das spezielle System. Es zeigt die Art und Weise, wie das System möglicherweise ausfallen kann, die Bauteile und ihre Ausfallarten, die den Systemausfall verursachen können, und den Grund bzw. die Gründe für das Auftreten jeder einzelnen Ausfallart.

Der Aufwand für die FMEA komplexer Produkte kann beträchtlich sein. Dieser Aufwand kann manchmal dadurch verringert werden, wenn berücksichtigt wird, dass der Entwurf einiger Unterbaugruppen oder ihrer Teile nicht gänzlich neu ist, und durch die Bestimmung von Teilen des Produktentwurfs, die eine Wiederholung oder Modifikation eines früheren Produktentwurfs sind. Eine neu erstellte FMEA sollte Informationen dieser

vorhandenen Unterbaugruppen weitestgehend nutzen. Sie muss auch auf die Notwendigkeit von abschließenden Prüfungen oder eine vollständige Analyse der neuen Eigenschaften und Einheiten hinweisen. Sobald eine ausführliche FMEA für einen Entwurf vorliegt, kann sie für nachfolgende Generationen dieses Entwurfs aktualisiert und verbessert werden, was einen bedeutend geringeren Aufwand bedeutet als eine gänzlich neue Analyse.

Wenn eine vorhandene FMEA einer früheren Produktversion verwendet wird, ist es wichtig, sich zu vergewissern, dass der übernommene Entwurf auch in der gleichen Art und unter den gleichen Beanspruchungen eingesetzt wird wie der vorangegangene. Die neuen Betriebs- und Umgebungsbeanspruchungen können eine Überprüfung der vorher durchgeführten FMEA erfordern. Abweichende Umgebungs- und Betriebsbeanspruchungen können eine gänzlich neue FMEA unter Berücksichtigung des neuen Betriebsbereichs erforderlich machen.

Der FMEA-Ablauf besteht aus den folgenden vier Hauptstufen:

a) Etablierung der wesentlichen Grundregeln für die FMEA einschließlich Planung und Terminierung, um sicherzustellen, dass Zeit und Fachwissen für die Durchführung der Analyse vorhanden sind;

b) Durchführung der FMEA unter Verwendung des geeigneten Arbeitsblattes oder anderer Hilfsmittel, wie etwa logischer Diagramme oder Störungsbaumanalysen;

c) Zusammenfassung und Berichterstattung über die Analyse, die alle Schlussfolgerungen und gegebenen Empfehlungen enthalten;

d) Fortschreiben der FMEA entsprechend dem Entwicklungsfortschritt.

5.2 Vorausgehende Arbeiten

5.2.1 Planung für die Analyse

FMEA-Tätigkeiten, Folgeaktivitäten, Verfahren, Zusammenhänge mit anderen auf die Funktionsfähigkeit gerichteten Aktivitäten, Prozesse für die Handhabung von Korrekturmaßnahmen und für deren Abschluss sowie Meilensteine sollten in den übergeordneten Programmplan aufgenommen werden.

Der Funktionsfähigkeitsprogrammplan sollte die anzuwendende FMEA-Analysemethode beschreiben. Diese Beschreibung kann eine zusammenfassende Beschreibung oder ein Verweis auf ein Originaldokument, das die Beschreibung enthält, sein.

Der Plan sollte die folgenden Punkte enthalten.

– eindeutige Definition der besonderen Ziele der Analyse und erwartete Ergebnisse;

– die Abgrenzung der vorliegenden Analyse hinsichtlich der Art, in der sich die FMEA auf bestimmte Entwurfsbestandteile konzentrieren sollte. Die Abgrenzung sollte die Reife des Entwurfs in Betracht ziehen sowie Bestandteile des Entwurfs, die als Risiko angesehen werden können, weil sie eine kritische Funktion ausführen oder weil die verwendete Technologie nicht ausgereift ist;

– Beschreibung, wie die vorliegende Analyse die Zuverlässigkeit des Gesamtprojektes absichert;

– festgelegte Maßnahmen für die Überwachung der FMEA-Überarbeitungen und die zugehörige Dokumentation. Die Überwachung der überarbeiteten Analysedokumente und -arbeitsblätter sowie der Archivierungsmethoden sollte festgelegt werden;

– Teilnahme von Entwurfsfachleuten an der Analyse derart, dass sie verfügbar sind, wenn sie benötigt werden;

– wesentliche Projektmeilensteine deutlich markiert, um sicherzustellen, dass die Analyse rechtzeitig durchgeführt wird;

– Art und Weise des Abschlusses aller im Prozess zur Entschärfung von erkannten und zu behandelnden Ausfallarten festgelegten Maßnahmen.

Der Plan sollte den Konsens aller Teilnehmer widerspiegeln und sollte von der Projektleitung freigegeben werden. Die abschließende Überprüfung der vervollständigten FMEA im Endstadium des Entwurfs eines Produktes oder seines Herstellungsprozesses (Prozess-FMEA) weist alle aufgezeichneten Maßnahmen zur Entschärfung von bedenklichen Ausfallarten und die Art und Weise ihres Abschlusses auf.

5.2.2 Systemstruktur

5.2.2.1 Information über die Systemstruktur

Die folgenden Punkte müssen in die Information über die Systemstruktur aufgenommen werden:

a) die verschiedenen Systembestandteile mit ihren Charakteristika, Leistungen, Aufgaben und Funktionen;

b) logische Verknüpfungen zwischen den Bestandteilen;

c) Redundanzniveau und Art der Redundanzen;

d) Position und Bedeutung des Systems innerhalb der gesamten Anlage (falls möglich);

e) Eingangs- und Ausgangsgrößen des Systems;

f) Änderungen in der Systemstruktur für wechselnde Betriebsarten.

Informationen über Funktionen, Charakteristika und Leistungen werden für alle betrachteten Systemebenen benötigt bis hinauf zur höchsten Ebene, damit die FMEA in geeigneter Weise alle Fehlzustandsarten ansprechen kann, die irgendeine dieser Funktionen verhindern.

5.2.2.2 Festlegen der Systembegrenzung für die Analyse

Die Systembegrenzung bildet die physikalische und funktionale Schnittstelle zwischen dem System und seiner Umgebung, einschließlich anderer Systeme, mit denen sich das betrachtete System gegenseitig beeinflusst. Die Festlegung der Systembegrenzung für die Analyse sollte der Begrenzung entsprechen, wie sie für Entwurf und Instandhaltung festgelegt ist. Das sollte für Systeme auf beliebiger Ebene gelten. Für Systeme und/oder Bestandteile außerhalb der Begrenzung sollte der Ausschluss ausdrücklich festgestellt werden.

Die Festlegung der Systembegrenzung wird eher durch den Entwurf, den beabsichtigten Verwendungszweck, die Beschaffungsquelle oder durch kommerzielle Kriterien beeinflusst als durch die Forderungen nach optimaler FMEA. Wo es jedoch möglich ist, die Begrenzungen so festzulegen, dass sie die System-FMEA und ihre Verflechtung mit anderen verwandten Untersuchungen im Programm erleichtern, ist dies vorzuziehen. Dies trifft insbesondere dann zu, wenn das System funktionsmäßig komplex ist mit vielfachen Verbindungen zwischen den Einheiten innerhalb der Begrenzung und mehreren Ausgängen, die die Begrenzung überschreiten. In solchen Fällen könnte es von Vorteil sein, eine Begrenzung für die Untersuchung eher vom funktionellen als vom Hardware- und Softwaregesichtspunkt festzulegen, um die Anzahl von Eingabe- und Ausgabeverknüpfungen zu anderen Systemen zu begrenzen. Dies würde darauf abzielen, die Anzahl der systembezogenen Ausfallauswirkungen zu reduzieren.

Es sollte sorgfältig darauf geachtet werden sicherzustellen, dass andere Systeme oder Bestandteile außerhalb der Begrenzungen des betrachteten Systems nicht vergessen werden, indem ausdrücklich festgestellt wird, dass sie von der jeweiligen Untersuchung ausgeschlossen sind.

5.2.2.3 Ebenen der Analyse

Es ist wichtig, die Gliederungsebenen in dem System, das für die Analyse verwendet wird, festzulegen. Beispielsweise können Systeme nach Funktion oder in Teilsysteme, austauschbare Einheiten oder einzelne Bauteile zergliedert werden (siehe Bild 1). Grundregeln bei der Wahl der Gliederungsebenen für die Analyse des Systems hängen von den gewünschten Ergebnissen und der vorhandenen Information über den Entwurf ab. Die folgenden Leitlinien sind hilfreich.

a) Die höchste Ebene des Systems wird vom Entwurfskonzept und den festgelegten Forderungen an das Ergebnis bestimmt.

b) Die niedrigste Ebene im System, auf der die Analyse wirkungsvoll ist, ist die Ebene, für die die Information zur Festlegung von Definition und die Beschreibung von Funktionen vorhanden sind. Die Wahl der geeigneten Systemebene wird auch durch frühere Erfahrungen beeinflusst. Eine weniger

detaillierte Analyse kann gerechtfertigt für ein System sein, das auf einem ausgereiften Entwurf mit einer guten Funktionsfähigkeits-, Instandhaltbarkeits- und Sicherheitsvorgeschichte beruht. Umgekehrt sind größere Detailtiefe und eine entsprechend niedrigere Systemebene angezeigt für alle neu entworfenen Systeme mit unbekannter Zuverlässigkeitshistorie.

c) Die spezifizierte oder angestrebte Instandhaltungs- und Instandsetzungsebene kann ein wertvoller Ratgeber bei der Festlegung niedrigerer Systemebenen sein.

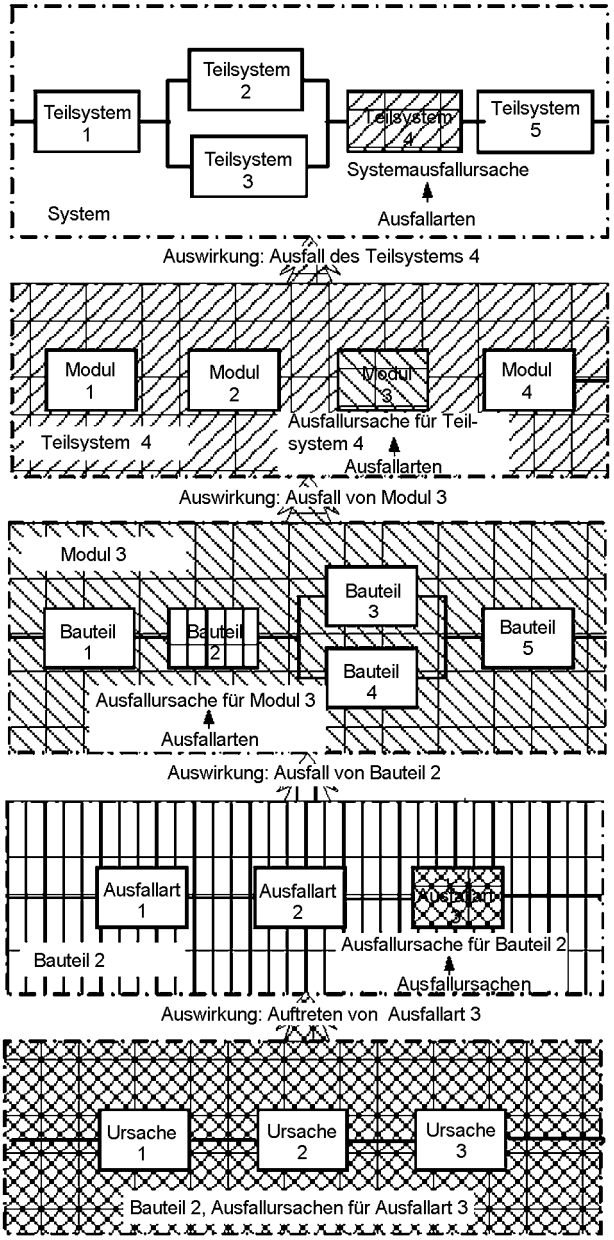

Bild 1 – Zusammenhang zwischen Ausfallarten und Ausfallauswirkungen in einer Systemhierarchie

In der FMEA hängt die Definition von Ausfallarten, Ausfallursachen und Ausfallauswirkungen von der Ebene der Analyse und von den Systemausfallkriterien ab. Mit Fortschreiten der Analyse können die auf niedrigerer Ebene festgestellten Ausfallauswirkungen auf höherer Ebene Ausfallarten bedingen. Die Ausfallarten auf niedrigerer Ebene können zu Ausfallursachen auf höherer Ebene werden und so weiter.

Wenn ein System in seine Bestandteile zergliedert worden ist, führen die Auswirkungen einer oder mehrerer Ursachen einer Ausfallart zu dieser Ausfallart, die umgekehrt eine Ursache einer Auswirkung auf höherer Ebene, eines Bauteilausfalles, ist. Der Bauteilausfall ist dann die Ursache eines Modulausfalls (Auswirkung), welcher selbst die Ursache für einen Ausfall des Teilsystems ist. Die Auswirkung einer Ursache in einer Sys-

temebene wird so eine Ursache einer anderen Auswirkung auf einer höheren Ebene. Diese Überlegungen sind in Bild 1 veranschaulicht.

5.2.2.4 Darstellung der Systemstruktur

Symbolische Darstellungen von Systemstruktur und -betrieb, insbesondere Diagramme, sind sehr hilfreich für die Analyse.

Einfache Diagramme sollten erzeugt werden, die alle wichtigen Funktionen des Systems aufzeigen. In einem Diagramm sind die Blöcke untereinander mit Linien verbunden, die die Eingangs- und Ausgangsgrößen für jede Funktion darstellen. Normalerweise muss die Art jeder Funktion und jeder Eingangsgröße genau beschrieben werden. Es kann mehrere Diagramme geben, um die verschiedenen Phasen des Systembetriebs abzudecken.

Mit Fortschreiten des Entwurfsprozesses für das System kann ein Blockdiagramm der Komponenten erzeugt werden, bestehend aus Blöcken, die die tatsächlichen Komponenten oder Bauteile darstellen. Mit diesen zusätzlichen Kenntnissen wird eine genauere Bestimmung möglicher Ausfallarten und -ursachen möglich.

Die Diagramme sollten alle Reihen- und Redundanzbeziehungen zwischen den Bestandteilen und die funktionalen Abhängigkeiten zwischen ihnen darstellen. Dies erlaubt, Funktionsausfälle durch das gesamte System zu verfolgen. Um alternative Systembetriebsarten darzustellen, kann mehr als ein Diagramm notwendig sein. Für jede Betriebsart können getrennte Diagramme notwendig sein. Als ein Minimum sollte ein Blockdiagramm mindestens enthalten:

a) eine Aufteilung des Systems in größere Teilsysteme, einschließlich der funktionalen Verknüpfungen;

b) alle geeignet bezeichneten Eingangs- und Ausgangsgrößen sowie Kennzahlen, anhand derer auf jedes Teilsystem widerspruchsfrei Bezug genommen werden kann;

c) alle Redundanzen, alternativen Signalwege und anderen technischen Eigenschaften, die Schutz gegen Systemausfälle bieten.

5.2.2.5 Systeminbetriebnahme, -betrieb, -überwachung und -instandhaltung

Der Status der verschiedenen Betriebsbedingungen des Systems sollte genau beschrieben sein, ebenso wie die Änderungen in der Konfiguration oder in der Lage des Systems und seiner Bestandteile während der verschiedenen Betriebsphasen. Die vom System verlangten Mindestleistungen sollten definiert sein, damit Erfolgs- und/oder Versagenskriterien eindeutig verstanden werden können. Spezielle Forderungen, wie die nach Verfügbarkeit oder Sicherheit, sollten hinsichtlich spezifizierter Mindestniveaus zu erreichender Leistungsmerkmale und tolerierbarer Maximalniveaus von Schaden oder Verletzung betrachtet werden. Es ist notwendig, genaue Kenntnis zu haben von

a) der Dauer jeder Funktion, die zu erfüllen das System in Anspruch genommen wird;

b) dem Zeitintervall zwischen periodischen Prüfungen;

c) der für Korrekturmaßnahmen zur Verfügung stehenden Zeit, bevor ernsthafte Folgen für das System auftreten;

d) der gesamten Anlage, der Umgebung und/oder dem Personal, einschließlich Schnittstellen und Zusammenspiel mit dem Bedienpersonal;

e) den Betriebsprozeduren während des Inbetriebsetzens und der Abschaltung des Systems und anderer Betriebsübergänge;

f) der Überwachung während der Betriebsphasen;

g) Wartung und/oder Instandsetzung;

h) den Verfahren zur Stückprüfung, sofern verwendet.

Es ist schon festgestellt worden, dass eine der Einsatzmöglichkeiten der FMEA die Unterstützung der Entwicklung von Instandhaltungsstrategien ist. Wie auch immer, wenn das Letztere vorbestimmt worden ist, sollten sowohl für Wartung als auch für Instandsetzung Informationen über Instandhaltungseinrichtungen, Geräte und Ersatzteile vorliegen.

5.2.2.6 Systemumgebung

Die Umweltbedingungen des Systems sollten spezifiziert sein, einschließlich der Umgebungsbedingungen und solcher, die von anderen Systemen in der näheren Umgebung ausgehen. Das System sollte beschrieben werden bezüglich seiner Beziehungen, Abhängigkeiten oder Verbindungen mit Hilfs- oder anderen Systemen und Mensch-Maschine-Schnittstellen.

Im Entwurfsstadium sind diese Fakten üblicherweise nicht alle bekannt und daher werden Näherungen und Annahmen notwendig sein. Mit Voranschreiten des Projektes müssen diese Daten vervollständigt und die FMEA modifiziert werden, um neue Informationen oder geänderte Annahmen oder Näherungen zu berücksichtigen. Oft wird die FMEA beim Festlegen der geforderten Bedingungen hilfreich sein.

5.2.3 Bestimmung der Ausfallarten

Ein erfolgreicher Betrieb eines gegebenen Systems hängt von der Leistung gewisser kritischer Systemelemente ab. Der Schlüssel zur Beurteilung der Systemleistung ist das Erkennen kritischer Elemente. Die Verfahren zum Erkennen von Ausfallarten, deren Ursachen und Auswirkungen können wirksam vertieft werden durch die Vorbereitung einer Liste der erwarteten Ausfallarten im Lichte folgender Punkte:

a) der Einsatz des Systems;

b) das jeweilig beteiligte Systemelement;

c) die Betriebsart;

d) die zugehörigen Festlegungen für den Betrieb;

e) die zeitlichen Einschränkungen;

f) die Beanspruchung durch die Umgebung;

g) die Beanspruchung durch den Betrieb.

Eine beispielhafte Liste allgemeiner Ausfallarten ist in Tabelle 1 enthalten.

Tabelle 1 – Beispiel eines Satzes allgemeiner Ausfallarten

1	Ausfall während des Betriebs
2	Kein Betrieb zu vorgegebener Zeit
3	Betrieb wird zu vorgegebener Zeit nicht beendet
4	Vorzeitiger Betrieb

ANMERKUNG Diese Liste ist nur ein Beispiel. Unterschiedliche Listen sind für unterschiedliche Systemarten erforderlich.

Beinahe jede Ausfallart kann einer oder mehrerer dieser Kategorien zugeteilt werden. Diese allgemeinen Ausfallartenkategorien sind jedoch für eine abschließende Analyse zu grob; folglich muss die Liste erweitert werden, um die Kategorien treffender zu beschreiben. Wenn diese in Verbindung mit Leistungsangaben zu den Eingängen und Ausgängen im Zuverlässigkeitsblockdiagramm verwendet werden, können alle potentiellen Ausfallarten erkannt und beschrieben werden. Es wird darauf hingewiesen, dass eine gegebene Ausfallart mehrere Ursachen haben kann.

Es ist wichtig, dass eine Beurteilung aller Einheiten innerhalb der Systemgrenzen auf der niedrigsten Ebene entsprechend den Zielen der Analyse durchgeführt wird, um alle potentiellen Ausfallarten zu erkennen. Untersuchungen zum Ermitteln möglicher Ausfallursachen und auch Ausfallauswirkungen auf die Funktion des Teilsystems und des Systems können danach unternommen werden.

Lieferanten von Einheiten sollten potentielle Ausfallarten zu ihren Produkten ermitteln. Um hierbei behilflich zu sein, können typische Angaben zu Ausfallarten in den folgenden Gebieten gesucht werden:

a) Für neue Einheiten kann man sich auf andere Einheiten mit ähnlicher Funktion und Struktur und auf die Ergebnisse von Prüfungen dieser Einheiten bei geeigneten Belastungsbedingungen beziehen.

b) Für neue Einheiten liefern Entwurfsziel und detaillierte Analyse der Funktionen die möglichen Ausfallarten und ihre Ursachen. Diese Methode ist gegenüber der in a) vorzuziehen, da die Belastungen und der Betrieb selbst von denen der ähnlichen Einheiten abweichen können. Ein Beispiel für diese Situation kann die Verwendung eines Signalprozessors sein, die sich von der im ähnlichen Entwurf unterscheidet.

c) Für Einheiten, die sich in Betrieb befinden, können Betriebsdaten und Ausfalldaten herangezogen werden.

d) Potentielle Ausfallarten können von für den Betrieb der Einheit typischen funktionalen und physikalischen Parametern abgeleitet werden.

Es ist wichtig, dass Ausfallarten der Einheiten nicht aus Mangel an Daten weggelassen und dass Anfangsschätzungen durch Prüfergebnisse und Fortschritte in der Entwicklung verbessert werden. Die FMEA sollte den Status solcher Schätzungen angeben.

Das Ermitteln von Ausfallarten und, wo nötig, das Festlegen von Abhilfemaßnahmen im Entwurf, vorbeugende Qualitätssicherungsmaßnahmen oder Wartungsmaßnahmen, sind von höchster Wichtigkeit. Es ist wichtiger, Ausfallarten zu ermitteln und, wenn möglich, diese durch Änderungen im Entwurf zu beseitigen, als deren Eintrittswahrscheinlichkeit zu kennen. Wenn es schwierig ist, Dringlichkeitsstufen zuzuweisen, kann eine Ausfallbedeutungsanalyse erforderlich sein.

5.2.4 Ausfallursachen

Die wahrscheinlichsten Ursachen jeder möglichen Ausfallart sollten bestimmt und beschrieben werden. Da eine Ausfallart mehr als eine Ursache haben kann, müssen die möglichen, voneinander unabhängigen Ursachen, die am wahrscheinlichsten sind, bestimmt und beschrieben werden.

Nicht immer ist die Bestimmung und Beschreibung von Ausfallursachen für alle in der Analyse bestimmten Ausfallarten notwendig. Bestimmung und Beschreibung von Ausfallursachen, ebenso wie Vorschläge für deren Beseitigung, sollten auf der Basis der Ausfallwirkungen und ihrer Schwere geschehen. Je schwerwiegender die Auswirkungen von Ausfallarten sind, desto genauer sollten die Ausfallursachen bestimmt und beschrieben werden. Sonst würde der Untersuchende unnötig viel Aufwand der Bestimmung von Ausfallursachen von Ausfallarten widmen, die keine oder sehr geringe Auswirkung auf die Funktionalität des Systems haben.

Ausfallursachen können durch die Analyse von Feldausfällen und Ausfällen in Prüfeinrichtungen ermittelt werden. Wenn der Entwurf neu und ohne Vorgänger ist, können Ausfallursachen durch das Einholen von Expertenmeinungen ermittelt werden.

Wenn die Ursachen jeder Ausfallart festgestellt sind, wird die empfohlene Maßnahme, basierend auf ihrer geschätzten Eintrittswahrscheinlichkeit und der Schwere ihrer Auswirkung, beurteilt.

5.2.5 Ausfallauswirkungen

5.2.5.1 Ausfallauswirkungsdefinition

Eine Ausfallauswirkung ist die Folge einer Ausfallart hinsichtlich des Betriebs, der Funktion oder des Zustands eines Systems (siehe Definition 3.4). Eine Ausfallauswirkung kann eine oder mehrere Ausfallarten einer oder mehrerer Einheiten zur Ursache haben.

Die Folgen jeder Ausfallart auf Betrieb, Funktion oder Zustand eines Systemelements müssen ermittelt, beurteilt und aufgezeichnet werden. Sofern zutreffend, sollten Instandhaltungsaktivitäten und Zielvorgaben für das System ebenfalls beachtet werden. Eine Ausfallauswirkung kann ebenfalls die nächsthöhere Ebene beeinflussen und sich schließlich bis zur höchsten analysierten Ebene auswirken. Daher sollten in jeder Ebene die Auswirkungen von Ausfällen auf die nächsthöhere Ebene beurteilt werden.

5.2.5.2 Örtliche Auswirkungen

Der Begriff „örtliche Auswirkungen“ bezieht sich auf die Auswirkungen der Ausfallart auf das betrachtete Systemelement. Die Folgen jedes möglichen Ausfalles auf die Ausgangsgröße der Einheit sollten beschrieben werden. Zweck der Ermittlung örtlicher Auswirkungen ist es, eine Grundlage für Beurteilungen zu schaf-

fen, falls alternative Maßnahmen bewertet oder falls Abhilfemaßnahmen entwickelt werden sollen. In manchen Fällen wird es keine örtliche Auswirkung außer der Ausfallart selbst geben.

5.2.5.3 Ausfallauswirkungen auf die Systemebene

Beim Ermitteln von Endauswirkungen wird die Wirkung eines möglichen Ausfalls auf die höchste Systemebene definiert und durch die Analyse aller dazwischen liegenden Ebenen beurteilt. Die beschriebene Endauswirkung kann das Ergebnis von Mehrfachausfällen sein. (Beispielsweise folgt aus dem Ausfall einer Sicherheitsvorrichtung nur dann eine katastrophale Endauswirkung, wenn sowohl die Sicherheitsvorrichtung ausfällt als auch die Hauptfunktion, für die die Sicherheitsvorrichtung entworfen ist, zulässige Grenzen überschreitet.) Diese aus einem Mehrfachausfall folgenden Endauswirkungen sollten in den Arbeitsblättern vermerkt werden.

5.2.6 Erkennungsmethoden

Für jede Ausfallart sollte der Untersuchende festlegen, wie der Ausfall erkannt wird, und die Art und Weise, auf die der Nutzer oder das Instandhaltungspersonal auf den Ausfall aufmerksam gemacht werden. Ausfallerkennung kann verwirklicht werden durch eine selbsttätige Einrichtung des Entwurfs (eingebautes Prüfmittel), Einrichtung einer gesonderten Erprobungsprozedur vor dem Systembetrieb oder durch Prüfung während der Instandhaltung. Sie kann bei der Inbetriebnahme des Systems oder fortlaufend während des Betriebs in festgelegten Zeitabständen durchgeführt werden. In jedem Fall sollten Ausfallerkennung und ihre Anzeige gefährliche Betriebszustände ausschließen.

Andere als die betrachteten Ausfallarten, die zu einer identischen Erscheinungsform führen, sollten untersucht und aufgelistet werden. Die Notwendigkeit der getrennten Ausfallerkennung redundanter Einheiten während des Betriebs sollte in Erwägung gezogen werden.

Bei einer Entwurfs-FMEA betrachtet die Erkennung, wie wahrscheinlich, wann und wo eine Entwurfsschwäche festgestellt werden wird (durch Bewertung, durch Analyse, durch Simulation, durch Prüfverfahren usw.). Bei einer Prozess-FMEA betrachtet die Erkennung, wie glaubhaft und wo im Prozess eine Schwäche festgestellt werden kann und mit welcher Wahrscheinlichkeit, z. B. durch die Bedienungsperson, durch statistische Prozessregelung, durch Qualitätsprüfungsverfahren oder durch spätere Schritte im Prozess.

5.2.7 Ausfallkompensierungsmaßnahmen

Die Ermittlung aller Entwurfseigenschaften auf einer gegebenen Systemebene oder andere Vorkehrungen, die die Fähigkeit haben, die Auswirkung der Ausfallart zu verhindern oder zu reduzieren, sind von äußerster Wichtigkeit. Daher sollte die FMEA das genaue Verhalten einer solchen Eigenschaft bei Vorliegen einer Ausfallart deutlich aufzeigen. Andere Vorkehrungen gegen Ausfälle, die im Rahmen der FMEA aufgezeichnet werden sollten, umfassen

a) redundante Einheiten, die einen kontinuierlichen Betrieb ermöglichen, wenn ein oder mehrere Elemente ausfallen;

b) alternative Mittel, den Betrieb aufrechtzuerhalten;

c) Überwachungs- oder Alarmvorrichtungen;

d) jedes andere Mittel, das wirksamen Betrieb ermöglicht oder Schaden begrenzt.

Während des Entwurfsprozesses können die funktionalen Bestandteile (Hardware und Software) einer Einheit wiederholt anders angeordnet oder umgestaltet werden oder, ihre Leistungsfähigkeit kann geändert werden. In jedem Stadium sollten die Bedeutung der erkannten Ausfallarten und die FMEA aktualisiert oder sogar wiederholt werden.

5.2.8 Klassifizierung der Schwere

Schwere ist eine Bewertung der Bedeutung der Auswirkung einer Ausfallart auf den Betrieb der Einheit. Die Klassifizierung der Schwereauswirkungen hängt stark von der FMEA-Anwendung ab und wird unter Berücksichtigung verschiedener Faktoren entwickelt:

– der Art des Systems in Beziehung zu möglichen, aus Ausfällen resultierenden Auswirkungen auf Benutzer oder die Umwelt;
– des funktionalen Verhaltens des Systems oder des Prozesses;
– aller durch den Kunden auferlegten vertraglichen Forderungen;
– von Sicherheitsforderungen der Regierung oder der Industrie;
– von Forderungen, die durch Gewährleistung impliziert werden.

Tabelle 2 veranschaulicht ein Beispiel eines Satzes einer qualitativen Klassifizierung der Schwere für ein Produkt für eine der FMEA-Arten.

Tabelle 2 – Erläuterndes Beispiel einer Schwere-Klassifizierung für Endauswirkungen

Klasse	Schweregrad	Auswirkungen auf Personen und Umwelt
IV	katastrophal	Eine Ausfallart, die möglicherweise zum Ausfall der Hauptfunktionen des Systems führen und daher dem System und seiner Umgebung ernsthaften Schaden zuführen und/oder zu Personenschäden führen kann.
III	kritisch	Eine Ausfallart, die möglicherweise zum Ausfall der Hauptfunktionen des Systems führen und daher dem System und seiner Umgebung ernsthaften Schaden zuführen kann, aber keine ernsthafte Gefahr für Leib und Leben darstellt.
II	geringfügig	Eine Ausfallart, die möglicherweise die Systemleistungsfunktion(en) herabsetzen kann, ohne nennenswerten Schaden für das System oder Gefahr für Leib und Leben.
I	unbedeutend	Eine Ausfallart, die möglicherweise die Systemfunktionen herabsetzen kann, aber dem System keinen Schaden zufügt und keine Gefahr für Leib und Leben darstellt.

5.2.9 Eintrittshäufigkeit oder Eintrittswahrscheinlichkeit

Die Eintrittshäufigkeit oder Eintrittswahrscheinlichkeit jeder Ausfallart sollte bestimmt werden, um die Auswirkung oder die Bedeutung der Ausfallart angemessen zu beurteilen.

Zur Bestimmung der Eintrittswahrscheinlichkeit der Ausfallart ist es sehr wichtig, neben der veröffentlichten Information bzgl. der Ausfallrate das Beanspruchungsprofil jeder Komponente (zutreffende Umgebungs-, mechanische und/oder elektrische Beanspruchungen), das zu ihrer Eintrittswahrscheinlichkeit beiträgt, zu berücksichtigen. Das gilt deswegen, weil die Ausfallraten der Komponenten und folglich die Ausfallrate der betrachteten Ausfallart in den meisten Fällen proportional mit dem Anstieg der angewandten Beanspruchungen entsprechend dem Potenzgesetz oder exponentiell ansteigen. Die Eintrittswahrscheinlichkeit der Ausfallarten kann geschätzt werden mit Hilfe von

– Daten aus der Lebensdauerprüfung der Komponenten,
– vorhandenen Ausfallratendatenbanken,
– Feldausfalldaten,
– Ausfalldaten von ähnlichen Einheiten oder Ausfalldaten für die Komponentenklasse.

Wenn die Eintrittswahrscheinlichkeit geschätzt wird, muss die FMEA sich mit dem Zeitintervall befassen, für das die Schätzungen gemacht wurden. Das ist üblicherweise die Gewährleistungsfrist oder eine vorher festgelegte Lebensdauer der Einheit oder des Produktes.

Die Anwendung von Eintrittshäufigkeit und Eintrittswahrscheinlichkeit wird bei der Beschreibung der Kritizitäts-(Bedeutungs-)analyse noch weiter erläutert.

5.2.10 Vorgehensweise bei der Analyse

Das Flussdiagramm in Bild 2 zeigt, wie die Analyse abläuft.

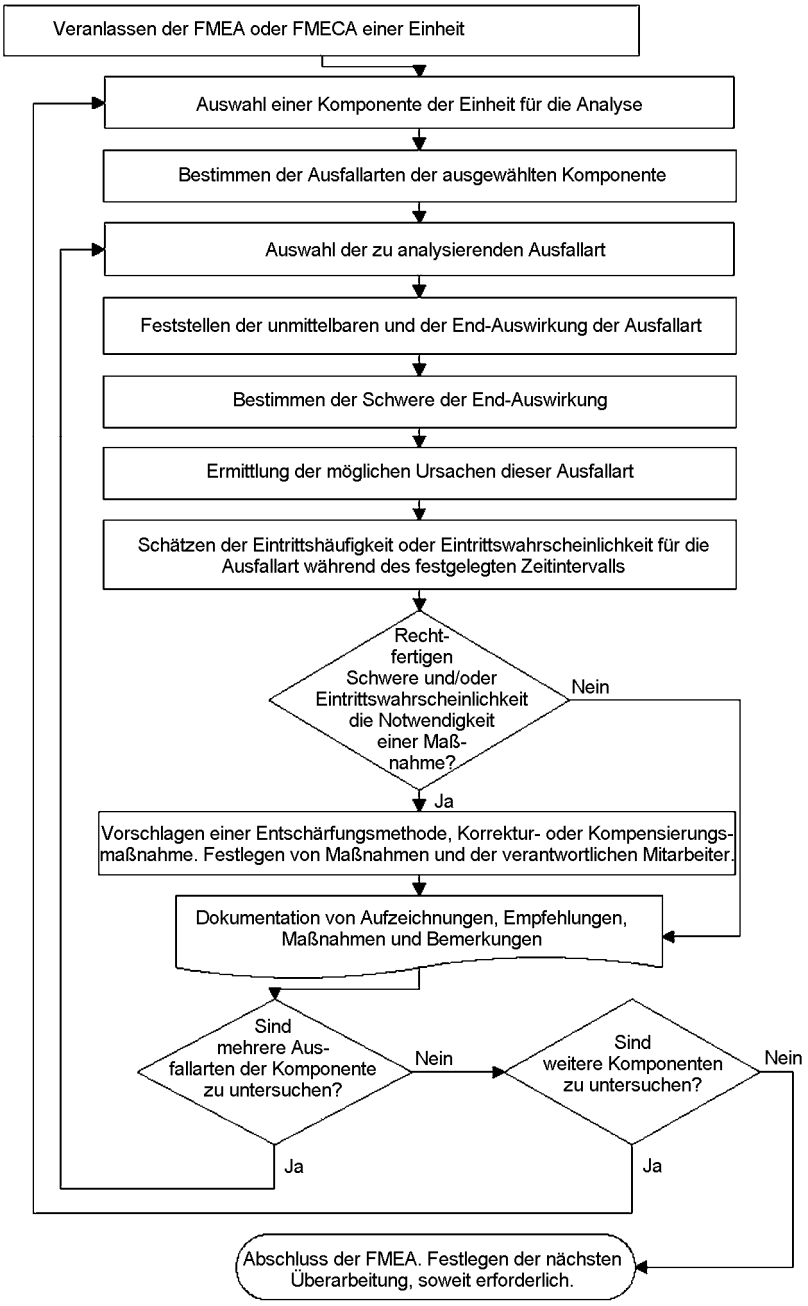

Bild 2 – Ablaufdiagramm für die Analyse

5.3 Ausfallbedeutungsanalyse (FMECA)[N2)]

5.3.1 Zweck der Analyse

Das der FMEA hinzugefügte Zeichen C kennzeichnet, dass die Fehlzustandsart- und -auswirkungsanalyse auch die Bedeutungsanalyse enthält. Die Bestimmung der Kritizität (Bedeutung) bedingt das Hinzufügen eines messbaren Merkmals für das Ausmaß einer Ausfallartauswirkung. Es gibt eine Vielzahl von Definitionen und Maßgrößen für die Kritizität, von denen die meisten ähnliche Bedeutung haben: Auswirkung oder Bedeutung einer Ausfallart, die es erfordern, diese zu behandeln und zu mildern. Einige dieser Maßgrößen werden in 5.3.2 und 5.3.4 erläutert. Zweck der Ausfallbedeutungsanalyse ist es, die relative Bedeutung jeder

---

N2) Nationale Fußnote: Für die Fehlzustandsart-, auswirkungs- und -kritizitätsanalyse, englisch „failure modes, effects and criticality analysis, FMECA“ wird in dieser deutschen Übersetzung, wo sinnvoll, der geläufigere Begriff Ausfallbedeutungsanalyse nach DIN 25448 verwendet.

Ausfallauswirkung als eine Hilfe für die Entscheidungsfindung zu quantifizieren, so dass mit einer Kombination aus Kritizität und Schwere Prioritäten für Aktionen zur Milderung oder Minimierung der Auswirkungen bestimmter Ausfälle gesetzt werden können.

5.3.2 Risiko (*R*) und Risikoprioritätszahl (RPN[N3)])

Eine der Methoden der quantitativen Bestimmung der Kritizität ist die Risikoprioritätszahl RPN. Risiko wird hier mit einem subjektiven Maß für die Schwere der Auswirkung und einem Schätzwert für die erwartete Eintrittswahrscheinlichkeit in einem für die Analyse angenommenen, festgelegten Zeitraum beurteilt. In einigen Fällen, in denen diese Werte nicht vorhanden sind, kann es notwendig werden, sich auf eine einfachere Form einer nicht numerischen FMEA zu beschränken.

Eine allgemeine Beziehung für eine Maßgröße für ein mögliches Risiko, *R*, in einer FMECA wird in manchen Analyseverfahren wie folgt ausgedrückt:

$$R = S \cdot P$$

Dabei ist

S die dimensionslose Größe, die für Schwere steht, d. h., ein Schätzwert dafür, wie stark die Auswirkungen eines Ausfalls das System oder den Anwender beeinflussen können.

P *die* ebenfalls dimensionslose Größe, die die Eintrittswahrscheinlichkeit bezeichnet. Wenn sie kleiner als 0,2 ist, kann sie durch die in 5.3.4 erläuterte Kritizitätszahl *C* ersetzt werden, die in manchen quantitativen FMEA-Verfahren verwendet wird, d. h., einen Schätzwert für die Wahrscheinlichkeit, dass die Ausfallwirkung eintreten wird.

Einige Anwendungen der FMEA oder FMECA unterscheiden zusätzlich den Grad der Fehlererkennung auf Systemebene. In diesen Anwendungen wird eine zusätzliche Kategorie für Fehlererkennung, *D* (ebenfalls eine dimensionslose Größe), benutzt, um eine Risikoprioritätszahl RPN wie folgt zu bilden:

$$RPN = S \cdot O \cdot D$$

Dabei ist

O die Eintrittswahrscheinlichkeit für eine Ausfallart für einen angenommenen oder festgelegten Zeitraum – selbst wenn sie als Rangzahl definiert ist, statt der tatsächlichen Eintrittswahrscheinlichkeit;

D steht für Erkennung, d. h., ein Schätzwert für die Chance, den Ausfall zu erkennen und zu beheben, bevor das System oder der Kunde betroffen werden. Diese Kenngröße wird üblicherweise ihrer Größe nach geordnet, umgekehrt zu den Rangzahlen für Schwere oder Eintrittshäufigkeit: Je höher die Erkennungszahl ist, desto unwahrscheinlicher ist ihre Erkennung. Folglich führt die geringere Erkennungswahrscheinlichkeit zu einer höheren RPN, und einer höheren Priorität für die Behandlung der Ausfallart.

Risikoprioritätszahlen können dann für die Festlegung der Reihenfolge verwendet werden, in der die Entschärfung von Ausfallarten angegangen wird. Zusätzlich zur Größe der Risikoprioritätszahl wird die Entscheidung für die Entschärfung hauptsächlich durch die Schwere der Ausfallart beeinflusst, in dem Sinne, dass, wenn es Ausfallarten mit ähnlicher oder gleicher Risikoprioritätszahl gibt, diejenigen mit hohen Werten für die Schwere zuerst anzugehen sind.

Diese Beziehungen können entweder auf einer stetigen oder einer diskreten Skala (einer endlichen Anzahl von definierten Werten) numerisch ausgewertet werden.

Die Ausfallarten werden dann entsprechend ihrer RPN geordnet und hohen RPN wird hohe Dringlichkeit zugeordnet. In einigen Anwendungen sind Auswirkungen mit einer RPN, die eine festgelegte Schwelle übersteigt, nicht akzeptabel, während in anderen Anwendungen den Schwerezahlen hohe Bedeutung beigemessen wird, unabhängig vom Wert der RPN.

N3) Nationale Fußnote: In der deutschsprachigen Fachliteratur Risikoprioritätszahl RPZ, RPZ = $B \cdot E \cdot A$, mit *B*: Schwere/Bedeutung, *E*: Entdeckungswahrscheinlichkeit, *A*: Auftretenswahrscheinlichkeit.

Manche Arten von FMECA ordnen den Werten von *S*, *O* und *D* unterschiedliche Skalen zu. Manche gehen von 1 bis 4 oder 5, andere, wie z. B. die weit verbreitet in der Automobilindustrie für die Analyse von Entwurfs- und Produktionsprozessen verwendete FMECA, die als DFMEA und PFMEA bekannt ist, verwenden Skalen für alle drei Größen von 1 bis 10.

5.3.3 Beziehung zwischen FMECA und Risikoanalyse

Kritizität kombiniert mit Schwere ist ein Maß für das Risiko, welches sich von den üblicherweise akzeptierten Maßgrößen für Risiko nur dadurch unterscheidet, dass für seine Beurteilung weniger rigoros, und somit meist weniger aufwendig, vorgegangen wird. Der Unterschied zeigt sich nicht nur in der Art, wie die Schwere einer Ausfallauswirkung vorhergesagt wird, sondern auch darin, dass sehr viel weniger komplexe Wechselwirkungen zwischen den beteiligten Faktoren in dem typischen, in der unteren Ebene beginnenden FMECA-Verfahren modelliert werden können. Auch resultiert eine FMECA üblicherweise in einer relativen Rangordnung der Beiträge zum Gesamtrisiko, während eine Risikoanalyse für Systeme mit hohem Risiko im Allgemeinen auf eine Tolerierung des Risikos abzielt. Für Systeme mit niedrigem Risiko und geringer Komplexität kann FMECA jedoch ein sehr kostengünstiges und angemessenes Verfahren sein. Sobald jedoch während einer FMECA die Wahrscheinlichkeit von Auswirkungen mit hohem Risiko erkannt wird, so ist eine wahrscheinlichkeitstheoretische Risikoanalyse (PRA) einer FMECA vorzuziehen.

Eine FMECA sollte daher nicht als einzige Grundlage zur Beurteilung dafür verwendet werden, ob das Risiko einer besonderen Auswirkung eines Systems mit hohem Risiko oder hoher Komplexität annehmbar gering ist, selbst wenn die Schätzung der Häufigkeit und der Schwere auf glaubhaften Daten basiert. Dies sollte einer wahrscheinlichkeitstheoretischen Risikoanalyse vorbehalten sein, bei der auch mehr beeinflussende Parameter (und deren Wechselwirkungen) berücksichtigt werden können, wie z. B. Einschaltzeit, Vermeidungswahrscheinlichkeit, Latenzzeit der Ausfälle, Fehlzustandserkennungsmechanismen.

Auf der Basis der Ausfallwirkungen, die in der FMEA festgestellt wurden, wird jede Auswirkung einer geeigneten Schwereklasse zugeordnet. Eine Häufigkeit für das Ereignis wird aus Ausfalldaten oder Schätzwerten des betreffenden Bauteils berechnet. Multipliziert mit der jeweiligen Einsatzzeit, ergibt die Häufigkeit eine Kennzahl für die Bedeutung (Kritizität), die dann auf einer Skala dargestellt werden kann, entweder entsprechend ihrem eigenen Wert, oder, falls die Skala die Wahrscheinlichkeiten für den Ereigniseintritt darstellt, dann wird diese Eintrittswahrscheinlichkeit auf der Skala gemessen. Die Schwereklasse und die Bedeutungs- (oder Eintrittswahrscheinlichkeits-)klasse legen zusammen für jede Auswirkung die Größe der Auswirkung fest. Zwei wichtige Ansätze zur Bewertung der Bedeutung können unterschieden werden: der Ansatz mittels Kritizitätsmatrix und das Konzept der Risikoprioritätszahlen.

5.3.4 Bestimmung von Ausfallraten für die Ausfallarten, von Wahrscheinlichkeit und von Kennzahlen für die Bedeutung (Kritizität)

Wenn Ausfallraten für die Ausfallarten ähnlicher Einheiten vorliegen, die unter Umgebungs- und Betriebsbedingungen ermittelt wurden, die ähnlich sind wie die für das untersuchte System angenommenen, dann können die Ereignishäufigkeiten für die Wirkungen direkt der FMECA hinzugefügt werden. Falls, wie es öfter der Fall ist, Ausfallraten eher für Einheiten als für Ausfallarten und für andere Umgebungs- und Betriebsbedingungen vorhanden sind, müssen die Ausfallraten der Ausfallarten berechnet werden. Im Allgemeinen gilt die folgende Beziehung:

$$\lambda_i = \lambda_j \cdot \alpha_i \cdot \beta_i$$

Dabei ist

λ_i der Schätzwert der als konstant angenommenen Ausfallrate für Ausfallart *i*,

λ_j die Ausfallrate der Komponente *j,*

α_i der Ausfallartanteil für Ausfallart *i*, d. h. die Wahrscheinlichkeit, dass die Einheit die Ausfallart *i* haben wird,

β_i die bedingte Wahrscheinlichkeit für die Ausfallwirkung unter der Annahme, dass Ausfallart *i* eingetreten ist.

Die größten Schwächen dieses Ansatzes sind die implizite Annahme der konstanten Ausfallrate und dass viele der Faktoren nur Vorhersagen oder Vermutungen nach bestem Wissen und Gewissen sind. Das ist insbesondere dann der Fall, wenn die Systemkomponenten keine zugeordnete Ausfallrate haben können, sondern nur die berechnete Ausfallwahrscheinlichkeit für die spezielle Anwendung, ihre Dauer und zugeordnete Beanspruchungen, wie etwa mechanische Komponenten und Systeme.

Umgebungs-, Belastungs- und Instandhaltungsbedingungen, die von denen abweichen, für die die Ausfallratendaten gelten, werden über Anpassungsfaktoren berücksichtigt. Hinweise zu geeigneten Werten für diese Anpassung können in Veröffentlichungen gefunden werden, die sich mit Zuverlässigkeitsangaben befassen. Besondere Sorgfalt muss aufgewendet werden, um sicherzustellen, dass die gewählten Anpassungsfaktoren zutreffend und für das spezielle System und seine Betriebsbedingungen anwendbar sind.

Bei einigen Anwendungen, wie dem quantitativen Ansatz zur Bedeutungsanalyse, wird eine Ausfallart-kritizitätskennzahl C_i (ohne Beziehung zu der allgemeinen Benennung „Kritizität“, die verschiedene Bedeutungen annehmen kann) verwendet anstelle einer Ausfallartausfallrate λ_i. Die Kritizitätskennzahl verbindet die bedingte Ausfallhäufigkeit mit der Betriebsdauer, was zu einer realistischeren Bewertung des Risikos einer Ausfallart während der vorgegebenen Lebensdauer des Produktes beitragen kann.

$$C_i = \lambda_i \cdot t_j$$

$$C_i = \lambda_j \cdot \alpha_i \cdot \beta_i \cdot t_{j,}$$

worin t_j die Betriebszeit der Komponente während der gesamten vorgegebenen für die FMECA zugrunde gelegten Zeit bezeichnet, für die die Wahrscheinlichkeit berechnet wird – die aktive Betriebszeit der Komponente.

Für die Kritizitätskennzahl von Komponenten mit *m* Ausfallarten ergibt sich dann

$$C_j = \sum_{i=1}^{m} \lambda_j \cdot \alpha_i \cdot \beta_i \cdot t_j$$

Es muss beachtet werden, dass die Kritizitätskennzahl nichts mit der Benennung „Kritizität“ selbst zu tun hat. Sie ist lediglich ein Wert, der bei manchen Arten der FMECA berechnet wird, in dem Sinne, dass sie ein relatives Maß ist für die Folge einer Ausfallart und ihrer Eintrittswahrscheinlichkeit. Hier ist die Kritizitätskennzahl eine Risikomaßzahl, jedoch nicht eine Maßzahl für die Eintrittswahrscheinlichkeit.

Für die Bestimmung von P_i, der Eintrittswahrscheinlichkeit einer Ausfallart in der Zeit t_j, aus der berechneten Kritizitätskennzahl gilt:

$$P_i = 1 - e^{-C_i}$$

Wenn die Ausfallraten der Ausfallarten und die resultierenden Kritizitätskennzahlen klein sind, dann kann für Eintrittswahrscheinlichkeiten kleiner als 0,2 (wobei die Kritizitätskennzahl gleich 0,223 sein würde) in erster Näherung gesagt werden, dass die Werte für die Kritizitätskennzahl und Ausfallwahrscheinlichkeit fast gleich sind.

Im Falle nicht konstanter Ausfallraten oder Ausfallhäufigkeiten muss die Eintrittswahrscheinlichkeit berechnet werden anstelle der Kritizitätskennzahl, deren Berechnung konstante Ausfallrate (Häufigkeit) unterstellt.

5.3.4.1 Kritizitätsmatrix

Kritizität kann in einer Kritizitätsmatrix wie in Bild 3 anschaulich dargestellt werden. Es sollte beachtet werden, dass es keine allgemeingültige Festlegung für Kritizität gibt, sondern dass Kritizität durch den Untersuchenden festgelegt und von der Projekt- oder Programmleitung akzeptiert werden muss. In unterschiedlichen Anwendungsgebieten unterscheiden sich die Festlegungen erheblich.

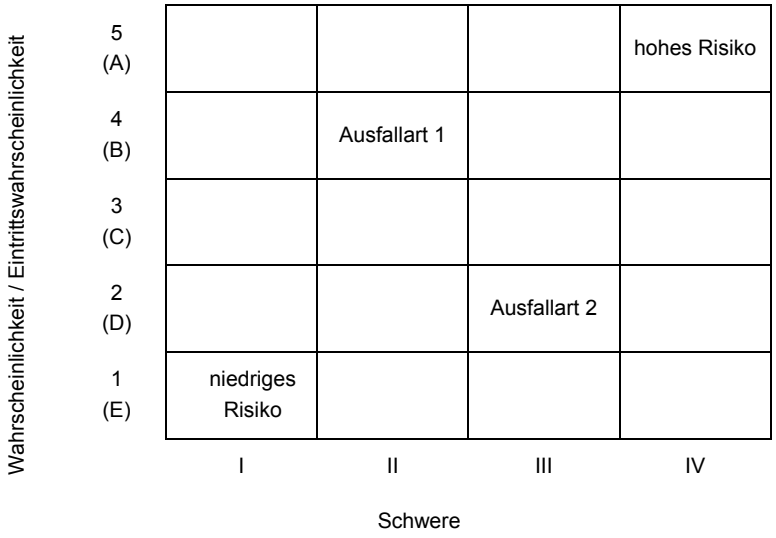

Bild 3 – Kritizitätsmatrix

In Bild 3 wird unterstellt, dass die Schwere mit aufsteigenden Zahlen zunimmt, wobei IV die größte Schwere hat (Verlust von Menschenleben und/oder Mission/Betrieb, Verletzungen). Es wird auch unterstellt, dass die Eintrittswahrscheinlichkeit auf der Y-Achse von unten nach oben zunimmt. Wenn die höchste Kategorie der Eintrittswahrscheinlichkeit einen Wert von 0,2 nicht überschreitet, dann sind Eintrittswahrscheinlichkeit und Kritizitätskennzahlen in etwa einander gleich. Eine Matrix, die man oft antrifft, hat die folgende Skala:

– Kritizitätskennzahl 1 oder E, unwahrscheinlich, Eintrittswahrscheinlichkeit: $0 \leq P_i < 0{,}001$
– Kritizitätskennzahl 2 oder D, gering, Eintrittswahrscheinlichkeit: $0{,}001 \leq P_i < 0{,}01$
– Kritizitätskennzahl 3 oder C, gelegentlich, Eintrittswahrscheinlichkeit: $0{,}01 \leq P_i < 0{,}1$
– Kritizitätskennzahl 4 oder B, wahrscheinlich, Eintrittswahrscheinlichkeit: $0{,}1 \leq P_i < 0{,}2$
– Kritizitätskennzahl 5 oder A, häufig, Eintrittswahrscheinlichkeit: $P_i \geq 0{,}2$.

Bild 3 ist nur als Beispiel gedacht. Andere Verfahren können Kritizität oder Schwere mit abweichenden Bezeichnungen und abweichenden Definitionen darstellen.

In dem in Bild 3 gegebenen Beispiel hat Ausfallart 1 eine höhere Eintrittswahrscheinlichkeit als Ausfallart 2, die umgekehrt eine höhere Schwere hat. Die Entscheidung, welche Ausfallart bei der Behandlung Vorrang hat, hängt von der Skalierung der Schwere- und Häufigkeitsklassen und den Rangreihungsprinzipien ab. Während auf einer linearen Skala Ausfallart 1 (wie üblicherweise durch die Matrix suggeriert) eine höhere Kritizitätskennzahl (oder Eintrittswahrscheinlichkeit) haben würde als Ausfallart 2, gibt es Anwendungen, in denen die Schwere absoluten Vorrang hat vor der Häufigkeit und so Ausfallart 2 zu der kritischeren Ausfallart macht. Eine andere einleuchtende Beobachtung ist, dass nur Ausfallarten, die sich auf die gleiche Systembetrachtungsebene beziehen, sinnvoll mit der Kritizitätsmatrix verglichen werden können, weil für Systeme mit niedriger Komplexität Ausfallarten auf einer niedrigeren Ebene normalerweise zu einer geringeren Häufigkeit neigen.

Die Kritizitätsmatrix (wie in Bild 3 gezeigt) kann bei qualitativen und quantitativen Betrachtungen angewendet werden, wie oben erläutert.

5.3.5 Risikoakzeptanzbeurteilung

Wenn das geforderte Endprodukt der Analyse eine Kritizitätsmatrix ist, kann diese aus den zugeordneten Werten für die Schwere und den Ereignishäufigkeiten gezeichnet werden. Risikoakzeptanz wird subjektiv definiert oder durch fachliche und finanzielle Entscheidungen gesteuert und unterscheidet sich je nach Industriesektor. Tabelle 3 gibt Beispiele für Risikoakzeptanzklassen und eine modifizierte Kritizitätsmatrix.

Tabelle 3 – Risiko-/Kritizitätsmatrix

Eintrittshäufigkeit der Ausfallwirkung	Schwereniveaus			
	1 unbedeutend	2 geringfügig	3 kritisch	4 katastrophal
5: häufig	unerwünscht	nicht akzeptabel	nicht akzeptabel	nicht akzeptabel
4: wahrscheinlich	akzeptabel	unerwünscht	nicht akzeptabel	nicht akzeptabel
3: gelegentlich	akzeptabel	unerwünscht	unerwünscht	nicht akzeptabel
2: gering	vernachlässigbar	akzeptabel	unerwünscht	unerwünscht
1: unwahrscheinlich	vernachlässigbar	vernachlässigbar	akzeptabel	akzeptabel

5.3.6 FMECA-Arten mit Rangordnungsskalen

Die in 5.3.2 beschriebenen FMECA-Arten werden in der Automobilindustrie bei der Analyse des Produktentwurfs weit verbreitet angewendet, ebenso wie für die Analyse der Produktionsprozesse für dieses Produkt.

Die Analysemethode ist die gleiche wie in allgemeiner Form für FMEA/FMECA beschrieben, mit der Ausnahme, dass die Festlegungen vorbestimmt sind in drei Tabellen für Schwere *S* (severity), Eintreten *O* (occurrence) und für die Erkennung *D* (detection).

5.3.6.1 Abweichende Bestimmung der Schwere

Tabelle 4 enthält ein Beispiel für die Einstufungen der Schwere, wie sie hauptsächlich in der Automobilindustrie verwendet werden.

Tabelle 4 – Schwere der Ausfallart

Schwere	Kriterien	Rang
keine	Keine erkennbare Auswirkung.	1
sehr gering	Passgenauigkeit und Verarbeitungsqualität / Quietsch- und Klappergeräusche erfüllen die Anforderungen nicht. Fehler wird von kritischen Kunden bemerkt (weniger als 25 %).	2
gering	Passgenauigkeit und Verarbeitungsqualität / Quietsch- und Klappergeräusche erfüllen die Anforderungen nicht. Fehler wird von 50 % der Kunden bemerkt.	3
sehr niedrig	Passgenauigkeit und Verarbeitungsqualität / Quietsch- und Klappergeräusche erfüllen die Anforderungen nicht. Fehler wird von den meisten Kunden bemerkt (mehr als 75 %).	4
niedrig	Fahrzeug/Einheit betriebsbereit, aber nur fahrfähig mit reduziertem Leistungsniveau bzgl. Komfort/Bequemlichkeit. Kunde etwas unzufrieden.	5
mittelmäßig	Fahrzeug/Einheit betriebsbereit, aber nur fahrfähig ohne Komfort/Bequemlichkeit. Kunde unzufrieden.	6
hoch	Fahrzeug/Einheit betriebsbereit, aber nur auf reduziertem Leistungsniveau. Kunde sehr unzufrieden.	7
sehr hoch	Fahrzeug/Einheit nicht betriebsbereit (Verlust der Hauptfunktion).	8
gefährlich, mit Warnung	Sehr hoher Rang für Schwere, wenn eine mögliche Ausfallart die sichere Funktion des Fahrzeugs beeinträchtigt und/oder die Nichterfüllung von behördlichen Auflagen mit Warnung nach sich zieht.	9
gefährlich, ohne Warnung	Sehr hoher Rang für Schwere, wenn eine mögliche Ausfallart die sichere Funktion des Fahrzeugs beeinträchtigt und/oder die Nichterfüllung von behördlichen Auflagen ohne Warnung nach sich zieht.	10

ANMERKUNG Aus SAE J1739.

Der Ausfallauswirkung jeder Ausfallart ist eine Rangzahl für die Schwere zugeordnet, basierend auf der Schwere der Auswirkung auf die Leistung des Gesamtsystems und die Sicherheit, angesichts der Systemanforderungen, -ziele und -beschränkungen, im Hinblick auf das Fahrzeug als System. Dies geschieht äußerst leicht im FMECA-Auswertblatt. Die Bestimmung der Schwere entsprechend Tabelle 4 ist sehr direkt für Schwerezahlen 6 und höher. Die Bestimmung der Schwere von 3 bis 5 kann subjektiv sein.

5.3.6.2 Abweichende Bestimmung des Eintretens

Tabelle 5 (auch von der Automobilindustrie entliehen) enthält Beispiele für qualitative Maße des Eintretens, die im Risikoprioritätszahlenkonzept verwendet werden können.

Tabelle 5 – Auftreten der Ausfallart in Bezug auf Eintrittshäufigkeit und -wahrscheinlichkeit

Auftreten der Ausfallart	Rang, *O*	Häufigkeit	Wahrscheinlich-keit
gering: Ausfall ist unwahrscheinlich	1	≤ 0,010 pro tausend Fahrzeuge/Einheiten	$\leq 1 \cdot 10^{-5}$
niedrig: relativ wenig Ausfälle	2	0,1 pro tausend Fahrzeuge/Einheiten	$1 \cdot 10^{-4}$
	3	0,5 pro tausend Fahrzeuge/Einheiten	$5 \cdot 10^{-4}$
mittelmäßig: gelegentliche Ausfälle	4	1 pro tausend Fahrzeuge/Einheiten	$1 \cdot 10^{-3}$
	5	2 pro tausend Fahrzeuge/Einheiten	$2 \cdot 10^{-3}$
	6	5 pro tausend Fahrzeuge/Einheiten	$5 \cdot 10^{-3}$
hoch: wiederholte Ausfälle	7	10 pro tausend Fahrzeuge/Einheiten	$1 \cdot 10^{-2}$
	8	20 pro tausend Fahrzeuge/Einheiten	$2 \cdot 10^{-2}$
sehr hoch: Ausfall ist fast unvermeidbar	9	50 pro tausend Fahrzeuge/Einheiten	$5 \cdot 10^{-2}$
	10	≥ 100 pro tausend Fahrzeuge/Einheiten	$\geq 1 \cdot 10^{-1}$

ANMERKUNG Quelle: AIAG: Potential Failure Mode and Effects Analysis, FMEA, Third Edition.

Es sollte beachtet werden, dass in Tabelle 5 die Benennung „Häufigkeit“ als eine Kennzahl für das Auftreten einer Anzahl von Möglichkeiten während einer Mission oder einer bestimmten Lebensdauer verwendet ist, die mit einem Ausfallanteil oder einer Eintrittswahrscheinlichkeit verglichen werden kann, und die zugehörigen Wahrscheinlichkeiten geben lediglich diesen Anteil wieder. Zum Beispiel würde eine Ausfallart, die mit dem Rang $O = 9$ bewertet wurde, den Ausfall eines von drei Systemen während einer vorher festgelegten Missionsdauer verursachen. Hier muss die Bestimmung der Eintrittswahrscheinlichkeit auf die interessierende Zeitspanne bezogen werden. Es ist empfehlenswert, diese Zeitspanne im Titel der Untersuchung zu nennen.

Das optimale Verfahren ist, die Eintrittswahrscheinlichkeit für die Komponenten und ihre Ausfallarten basierend auf ihren eigenen spezifischen Ausfallraten unter Berücksichtigung der angewendeten erwarteten Beanspruchungen (umgebungs- und betriebsbedingt) zu berechnen. Wenn diese Informationen nicht vorliegen, kann ein Schätzwert zugeordnet werden, aber dabei muss das Analyseteam die Bedeutung der Auftretenskennzahlen bedenken – die Anzahl des Auftretens pro tausend Fahrzeuge in der vorher für die Untersuchung festgelegten Zeit (Garantiezeit, Fahrzeuglebensdauer oder anderes); das ist die berechnete oder geschätzte Eintrittswahrscheinlichkeit dieser Ausfallart in der interessierenden Zeitspanne. Außerdem sollte beachtet werden, dass, ungleich der Schwereskala, die Auftretensskala weder linear noch logarithmisch ist. Daher sollte beachtet werden, dass, wenn die resultierende Risikoprioritätszahl RPN berechnet und beurteilt wird, diese ebenfalls nicht linear ist und mit besonderer Sorgfalt gehandhabt werden muss.

5.3.6.3 Bewertung der Ausfallerkennungswahrscheinlichkeit

Im RPN-Konzept muss die Wahrscheinlichkeit, dass ein Ausfall erkannt wird, geschätzt werden; d. h. die Wahrscheinlichkeit, dass die konstruktiven Maßnahmen/Hilfsmittel oder Verifizierungsverfahren mögliche Ausfallarten rechtzeitig erkennen, um einen Ausfall auf Systemebene zu verhindern. Für die Anwendung auf Prozesse (Prozess-FMEA bzw. PFMECA) bedeutet dies die Wahrscheinlichkeit, dass ein Satz von Prozessüberwachungsmaßnahmen, der zurzeit eingesetzt wird, in der Lage ist, einen Ausfall zu erkennen und auszusondern, bevor er dem nachfolgenden Prozess oder dem endgültigen Produktausstoß übergeben wird.

Vor allem für gewöhnliche Produkte, die in mehreren unterschiedlichen Systemen und Anwendungen eingesetzt werden können, kann es schwierig sein, die Ausfallerkennungswahrscheinlichkeit abzuschätzen.

Tabelle 6 enthält eine der Methoden zur Ausfallerkennung, wie sie in der Automobilindustrie benutzt wird.

Tabelle 6 – Beurteilungskriterien für die Ausfallarterkennung

Entdeckung	Kriterium: Erkennungswahrscheinlichkeit durch Entwurfsüberprüfung	Rang
fast sicher	Die Entwurfsüberprüfung wird eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart fast sicher erkennen.	1
sehr hoch	Sehr gute Aussichten, dass die Entwurfsüberprüfung eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart erkennen wird.	2
hoch	Gute Aussichten, dass die Entwurfsüberprüfung eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart erkennen wird.	3
mäßig hoch	Mäßig gute Aussichten, dass die Entwurfsüberprüfung eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart erkennen wird.	4
mittelmäßig	Mittelmäßige Aussichten, dass die Entwurfsüberprüfung eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart erkennen wird.	5
niedrig	Niedrige Aussichten, dass die Entwurfsüberprüfung eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart erkennen wird.	6
sehr niedrig	Sehr niedrige Aussichten, dass die Entwurfsüberprüfung eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart erkennen wird.	7
gering	Geringe Aussichten, dass die Entwurfsüberprüfung eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart erkennen wird.	8
sehr gering	Sehr geringe Aussichten, dass die Entwurfsüberprüfung eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart erkennen wird.	9
völlig ungewiss	Die Entwurfsüberprüfung wird bzw. kann eine mögliche Ursache/Mechanismus samt nachfolgender Ausfallart nicht erkennen oder es gibt keine Entwurfsüberwachung.	10

ANMERKUNG Quelle: AIAG: Potential Failure Mode and Effects Analysis, FMEA, Third Edition.

5.3.6.4 Risikobeurteilung

Dem oben beschriebenen, sehr intuitiven Ansatz muss eine Rangreihung der Dringlichkeit der durchzuführenden Maßnahmen folgen, um das beste Sicherheitsniveau für den Kunden sicherzustellen. Zum Beispiel kann eine Ausfallart mit hoher Schwereklassifizierung, geringer Auftretensrate und sehr hoher Erkennung (etwa 10, 3 und 2) eine viel niedrigere Risikoprioritätszahl (hier 60) haben als eine mit überall durchschnittlichen Werten (etwa 5 in jeder Kategorie, was zu einer Risikoprioritätszahl von 125 führt). Daher werden oft zusätzliche Verfahren festgelegt, um sicherzustellen, dass Ausfallarten mit hohem Rang für die Schwere (etwa 9 oder 10) Vorrang bekommen und zuerst gemildert werden. In diesem Fall sollte die Entscheidung von dem Ausmaß der Schwere geleitet werden und nicht so sehr von der Risikoprioritätszahl allein. In allen Fällen ist es für einen besseren Entscheidungsprozess gut, den Rang der Schwere einer Ausfallart zusammen mit der Risikoprioritätszahl zu betrachten.

Risikoprioritätszahlen werden auch bei anderen FMEA-Verfahren bestimmt, vor allem bei denen, die in erster Linie qualitativ sind.

Mit den oben angegebenen Tabellen werden Risikoprioritätszahlen berechnet und oft als Leitlinie für die Ausfallentschärfung benutzt. An die Warnhinweise in 5.3.2 muss erinnert werden und die Schwächen von Risikoprioritätszahlen müssen berücksichtigt werden.

Einige der Schwächen von Risikoprioritätszahlen (RPN) sind wie folgt:

– Lücken im Bereich: 88 % des Bereichs sind leer, nur 120 aus 1000 Zahlen werden erzeugt.
– doppelt auftretende RPN: für einige Kombinationen, bei denen unterschiedliche Faktoren zur selben RPN führen.

– Empfindlichkeit gegenüber kleinen Änderungen: Eine kleine Änderung in einem Faktor hat eine viel größere Auswirkung, wenn die anderen Faktoren größer sind, als wenn sie klein sind (Beispiel: $9 \cdot 9 \cdot 3 = 243$ und $9 \cdot 9 \cdot 4 = 324$, im Vergleich zu $3 \cdot 4 \cdot 3 = 36$ und $3 \cdot 4 \cdot 4 = 48$).
– nicht geeignete Skalierung: Die Kennzahlen in der Auftretenstabelle sind nicht proportional oder linear; d. h., das Verhältnis zwischen zwei aufeinander folgenden Einstufungen kann 2,5 oder 2 sein.
– ungeeignete Skala für RPN. Unterschiede in RPN-Werten können vernachlässigbar erscheinen, obwohl sie tatsächlich signifikant sind. Ein Beispiel dafür wäre: Die Werte $S = 6$, $O = 4$, $D = 2$ würden für RPN = 48 ergeben, während $S = 6$, $O = 5$, $D = 2$ für RPN = 60 ergeben würden. Die zweite RPN ist nicht das Doppelte der ersten, obwohl tatsächlich $O = 5$ die doppelte Eintrittswahrscheinlichkeit von $O = 4$ hat. Deshalb sollten RPN-Werte nicht linear verglichen werden.
– irreführende Schlussfolgerungen aus RPN-Vergleichen, da die Skalen Ordnungsskalen und nicht Verhältnisskalen sind.

Die Überprüfung einer RPN erfordert Vorsicht und gutes Urteilsvermögen. Ein gutes Verfahren erfordert eine sorgfältige Überprüfung der Werte für Schwere, Auftreten und Entdeckung, bevor eine Meinung gefasst wird und Korrekturmaßnahmen ergriffen werden.

5.4 Bericht über die Analyse

5.4.1 Umfang und Inhalt eines Berichtes

Der Bericht über die FMEA kann in eine umfassendere Studie eingebunden sein oder alleine stehen. In beiden Fällen sollte der Bericht eine Zusammenfassung enthalten und ein detailliertes Protokoll der Analyse sowie die Block- oder Funktionsdiagramme, die die Systemstruktur erklären. Der Bericht sollte auch eine Liste der Zeichnungen (einschließlich Ausgabestand) enthalten, auf denen die FMEA basiert.

5.4.2 Zusammenfassung der Auswirkungen

Eine Auflistung der Ausfallauswirkungen auf ein spezielles von der FMEA behandeltes System sollte vorbereitet werden. Tabelle 7 enthält typische Ausfallauswirkungen[N4)] für einen Kfz-Anlassermotor und Anlasserschaltung.

Tabelle 7 – Beispiel für Ausfallauswirkungen (für einen Kfz-Anlasser)

1	Anlassermotor versagt
2	Anlasserdrehzahl geringer als spezifiziert
3	Anlassermotorritzel rastet nicht in den Zahnkranz ein
4	Anlassermotor arbeitet vorzeitig

ANMERKUNG 1 Die Liste dient lediglich als Beispiel. Jedes untersuchte System oder Teilsystem wird seinen eigenen Satz von Ausfallauswirkungen haben.

Eine Zusammenfassung der Ausfallauswirkungen kann erforderlich sein, um die aus den aufgelisteten Ausfallauswirkungen resultierende Ausfallwahrscheinlichkeit des Systems zu bestimmen und die Dringlichkeitsstufen für Abhilfe- oder vorbeugende Maßnahmen. Die Zusammenfassung der Ausfallauswirkungen sollte auf einer Liste von Endausfallauswirkungen basieren und sollte Details der Ausfallarten der Einheiten enthalten, die zu jeder Ausfallauswirkung beitragen. Die Eintrittswahrscheinlichkeit für jede der Ausfallarten wird berechnet für die festgelegte, vorher bestimmte Zeitspanne der Nutzung der Einheit ebenso wie für das erwartete Nutzungsprofil und die Belastungen. Tabelle 8 enthält ein Beispiel für eine Zusammenfassung von Ausfallauswirkungen.

N4) Nationale Fußnote: In der deutschen Automobilindustrie mit „Fehlerfolge“ bezeichnet.

Tabelle 8 – Beispiel für Wahrscheinlichkeiten von Ausfallauswirkungen

Nummer	Auswirkung	Bezug auf beitragende Ausfallart	Eintrittswahrscheinlichkeit für Ausfallauswirkung
1	Anlassermotor versagt	1, 3, 7, 8, 9, 16, 21, 22	$8 \cdot 10^{-3}$
2	Anlasserdrehzahl geringer als spezifiziert	6, 11, 12, 19, 20	$6 \cdot 10^{-4}$
3	Anlassermotorritzel rastet nicht in den Zahnkranz ein	2, 4, 5, 10, 13	$1{,}1 \cdot 10^{-5}$
4	Anlassermotor arbeitet vorzeitig	14, 15, 17, 18	$3{,}6 \cdot 10^{-7}$

ANMERKUNG 2 Eine solche Tabelle kann auch für andere qualitative und quantitative Rangfolgen einer Einheit oder eines Systems angelegt werden.

Die Zusammenfassung sollte auch eine kurze Beschreibung der Methode der Analyse und die Ebene, bis zu der sie durchgeführt wurde, die Annahmen und die zugrunde liegenden Regeln enthalten. Zusätzlich sollte sie Auflistungen des Folgenden enthalten:

a) Ausfallarten, die schwerwiegende Auswirkungen haben;

b) Empfehlungen für Konstrukteure, Instandhaltungspersonal, Planer und Anwender;

c) Änderungen des Entwurfs, die als ein Ergebnis der FMEA bereits eingeführt worden sind;

d) Auswirkungen, die durch die eingeführten Änderungen des Entwurfs gemildert worden sind.

6 Weitere Betrachtungen

6.1 Ausfälle mit gemeinsamer Ursache

In einer Zuverlässigkeitsanalyse reicht es nicht aus, nur zufällige und voneinander unabhängige Ausfälle zu betrachten. Einige Ausfälle mit gemeinsamer Ursache (englisch „common cause failures“ (CCF)) können auftreten, die eine Minderung der Systemleistung oder seinen Ausfall bewirken durch gleichzeitige Mängel in mehreren Systemkomponenten aufgrund einer einzigen Quelle, wie beispielsweise Entwurfsfehler (ungeeignete Unterlastung von Komponenten), Umgebungsbelastungen (Blitzschlag) oder menschliches Fehlverhalten.

Ausfälle mit gemeinsamer Ursache (CCF) sind solche Ausfälle, welche die grundlegende Annahme zunichte machen, dass die in der FMEA betrachteten Ausfallarten voneinander unabhängig sind. Die CCF veranlassen mehr als eine Einheit gleichzeitig auszufallen oder innerhalb einer hinreichend kurzen Zeitspanne, wobei sie die Auswirkung eines gleichzeitigen Ausfall haben.

Üblicherweise gehören zu den Ursachen von CCF:

– Entwurf: Software, Dimensionierung;

– Herstellung: chargenbezogene Fabrikationsfehler;

– Umgebung: elektrische Interferenz, Temperaturzyklen, Vibration;

– menschliche Einflüsse: fehlerhafte Bedienung oder Instandhaltungsaktionen.

Die FMEA muss deswegen mögliche Quellen von CCF berücksichtigen, wenn ein System analysiert wird, das Redundanzen verwendet, um die Funktion aufrechtzuerhalten, oder mehrfache Einheiten, um die Folgen im Falle eines Ausfalls zu mildern.

Ein CCF ist das Ergebnis eines Ereignisses, welches aufgrund logischer Abhängigkeiten ein Zusammentreffen von Ausfallzuständen in zwei oder mehr Komponenten verursacht (davon ausgenommen sind durch einen Primärausfall verursachte Sekundärausfälle). Ausfälle mit gemeinsamer Ursache können identische Bauteile sein mit denselben Ausfallarten und Schwächen, die in verschiedenen Baugruppen eines Systems verwendet werden – möglicherweise redundant, wo Redundanz wertlos ist.

Ausfälle mit gemeinsamer Ursache können durch eine FMEA qualitativ analysiert werden, aber die Fähigkeit der FMEA, diese vollständig zu analysieren, ist ziemlich begrenzt. Dennoch ist FMEA ein Verfahren, alle Ausfallarten und die zugehörigen Ursachen sukzessiv zu untersuchen und zusätzlich alle wiederkehrenden Prüfungen, vorbeugenden Instandhaltungsmaßnahmen usw. festzulegen. Sie ermöglicht eine Untersuchung aller der Ursachen, die mögliche Ausfälle mit gemeinsamer Ursache hervorrufen können.

Eine Kombination verschiedener Methoden ist nützlich, um Ausfälle mit gemeinsamer Ursache zu verhindern oder ihre Auswirkungen zu mildern (Systemmodellierung, physikalische Analyse von Komponenten): funktionale Vielfalt (bei der redundante Zweige oder Teile des Systems, die die gleiche Funktion ausführen, nicht identisch sind und unterschiedliche Ausfallarten haben), physikalische Trennung, um umgebungsbedingte oder elektromagnetische Beanspruchungen, die solche Ausfälle verursachen können, auszuschalten, oder Prüfungen usw. Die Untersuchung vorbeugender Maßnahmen gegen CCF wird üblicherweise nicht zum Aufgabenbereich der FMEA gerechnet. Dennoch müssen diese Maßnahmen in die Spalte mit den Bemerkungen aufgenommen werden, um zum Verständnis der ganzen FMEA beizutragen.

6.2 Menschliche Einflüsse

Manche Systeme müssen entwickelt werden, um menschliches Fehlverhalten zu verhindern oder seine Auswirkungen zu mildern. Beispiele dafür sind mechanische Verriegelungen bei Eisenbahnsignalen und Kennwörter bei Rechnereinsatz und Datenabfragen. Wo solche Vorkehrungen in einem System vorhanden sind, wird die Auswirkung eines Ausfalls von der Fehlerart abhängen. Manche Arten menschlichen Fehlverhaltens sollten für ein ansonsten fehlzustandfreies System ebenfalls beachtet werden, um die Wirksamkeit der Vorkehrungen zu prüfen. Selbst wenn unvollständig, kann eine teilweise Auflistung dieser Ausfallarten vorteilhaft sein für das Erkennen von Mängeln in Entwurf und Verfahren; das Erkennen aller möglichen Formen menschlichen Fehlverhaltens ist wahrscheinlich unmöglich.

Viele Ausfälle mit gemeinsamer Ursache haben mit menschlichem Fehlverhalten zu tun. Beispielsweise kann eine fehlerhafte Instandhaltung ähnlicher Einheiten die Redundanz vernichten. Um dies zu vermeiden, werden in redundanten Elementen oft unterschiedliche Materialien eingesetzt.

6.3 Softwarefehler

Eine FMEA über die Hardware eines komplexen Systems kann Rückwirkungen auf die Software im System haben. Daher können Entscheidungen über Auswirkungen, Kritizität und bedingte Wahrscheinlichkeiten, die aus der FMEA folgen, von den Softwareelementen und deren Art, Abfolge und zeitlicher Reihenfolge abhängen. Wenn dies der Fall ist, müssen die gegenseitigen Beziehungen zwischen Hardware und Software eindeutig festgelegt werden, da jede spätere Änderung oder Verbesserung der Software die FMEA und die daraus abgeleiteten Einschätzungen modifizieren kann. Die Bewilligung der Softwareentwicklung und -änderung kann von einer Überarbeitung der FMEA und der zugehörigen Einschätzungen abhängig gemacht werden, z. B. könnte die Softwarelogik verändert werden, um die Sicherheit auf Kosten der Funktionsfähigkeit während des Betriebs zu verbessern.

Fehlfunktionen aufgrund von Softwarefehlern oder -unzulänglichkeiten werden Auswirkungen haben, deren Tragweite sowohl vom Hardware- als auch vom Softwareentwurf bestimmt wird. Die Vermutung (en: postulation) solcher Fehler oder Unzulänglichkeiten und die Analyse ihrer Auswirkungen sind nur in begrenztem Umfang möglich. Die Auswirkungen möglicher Softwarefehler auf zugehörige Hardware kann abgeschätzt werden und die Bereitstellung von Sicherungssystemen entweder in der Software oder der Hardware wird oft durch solch eine Analyse angeregt.

6.4 FMEA bezüglich der Folgen eines Systemausfalls

Eine System-FMEA kann ohne Bezug auf eine bestimmte Anwendung durchgeführt werden und könnte anschließend für Projektanwendungen angepasst werden. Dies gilt für relativ kleine Baugruppen, die man als gewöhnliche Baugruppen ansehen könnte (beispielsweise ein elektronischer Verstärker, ein Elektromotor, ein mechanisches Ventil).

Es ist jedoch üblicher, eine projektspezifische FMEA zu erarbeiten und dabei auf die besonderen Folgen eines Systemausfalls zu achten. Es könnte erforderlich sein, die Auswirkungen von Ausfällen auf das System entsprechend den Folgen dieser Ausfälle zu kategorisieren. Beispiele hierfür sind: Ausfall zur sicheren Seite,

instand zu setzender Ausfall, nicht instand zu setzender Ausfall, eingeschränkte Erfüllung der Aufgabe, Aufgabe nicht erfüllt, Auswirkungen auf Personen, Gruppen oder die Gesellschaft allgemein.

Die Notwendigkeit, eine FMEA auf die letztendlichen Folgen eines Systemausfalls zu beziehen, wird von dem Projekt und der Beziehung zwischen der FMEA und anderen Analyseformen abhängen, wie z. B. Störungsbäumen, Markoff-Graphen, Petri-Netzen usw.

7 Anwendungen

7.1 Anwendung von FMEA und FMECA

FMEA ist ein Verfahren, das in erster Linie auf die Untersuchung von Material- und Geräteausfällen abgestimmt ist und das auf Klassen von Systemen unterschiedlicher Technologien (elektrisch, mechanisch, hydraulisch usw.) sowie auf Kombinationen von Technologien angewendet werden kann, oder es kann für bestimmte Geräte, Systeme oder Projekte als Ganzes zugeschnitten sein.

FMEA sollte auch die Betrachtung von Software und menschlichem Verhalten einschließen, wenn diese für die Zuverlässigkeit des Systems von Bedeutung sind. Eine FMEA kann eine Untersuchung für allgemeinen Gebrauch sein, um unterschiedliche Prozesse (medizinische, labortechnische, Herstellungs-, Entwicklungs-, Ausbildungsprozesse usw.) zu untersuchen, wobei sie üblicherweise als Prozess-FMEA oder PFMEA bezeichnet wird. Wenn eine Prozess-FMEA durchgeführt wird, wird dies immer im Hinblick auf das letztendliche Ziel oder den Prozesszielbereich getan, und sie betrachtet jeden Schritt innerhalb dieses Prozesses als Möglichkeit, ein unerwünschtes Ergebnis bei den folgenden Prozessschritten oder dem letztendlichen Prozessziel hervorzubringen.

7.1.1 Anwendung in einem Projekt

Der Anwender sollte bestimmen, wie und für welche Zwecke er eine FMEA innerhalb seiner eigenen technischen Disziplin nutzt. Sie kann für sich alleine oder zur Ergänzung und Unterstützung anderer Zuverlässigkeitsanalyseverfahren genutzt werden. Die Forderungen nach einer FMEA entstammen der Notwendigkeit, das Verhalten der Hardware und ihre Auswirkungen auf den Betrieb des Systems oder Gerätes zu verstehen. Die Notwendigkeit für eine FMEA kann von Projekt zu Projekt stark variieren.

FMEA unterstützt das Entwurfsüberprüfungskonzept und sollte während des System- und Teilsystementwurfs so zeitig wie möglich zum Einsatz kommen. FMEA ist auf alle Ebenen des Systementwurfs anwendbar; sie ist jedoch am besten für untere Ebenen, in denen viele Einheiten beteiligt sind, und/oder bei funktionaler Komplexität geeignet. Es ist unerlässlich, dass die die FMEA durchführenden Mitarbeiter besonders ausgebildet sind und dass sie eng mit Systemingenieuren und Entwicklern zusammenarbeiten können. Die FMEA sollte mit Projektfortschritt und bei Entwurfsänderungen aktualisiert werden. Am Ende des Projektes wird die FMEA zur Prüfung des Entwurfs verwendet und sie kann für den Nachweis der Konformität eines Systementwurfs mit geforderten Normen, Vorschriften und Anwenderforderungen erforderlich sein.

Informationen aus einer FMEA können die Dringlichkeit aufzeigen für statistische Prozessregelung, Stichproben- und Inspektionsprüfungen während Fertigung und Installation und für Qualifikation, Zulassung, Annahmeprüfungen und Inbetriebnahmeprüfungen. FMEA liefert wesentliche Informationen für Diagnose- und Instandhaltungsverfahren zur Aufnahme in Handbücher.

Bei der Entscheidung über das Ausmaß einer FMEA und wie diese auf eine Einheit oder einen Entwurf angewendet werden sollte, ist es wichtig, die besonderen Zwecke zu beachten, für die die Ergebnisse der FMEA benötigt werden, die zeitliche Abstimmung mit anderen Tätigkeiten und die Bedeutung der Festlegung eines bestimmten Grades der Kenntnis und Beherrschung unerwünschter Ausfallarten und -auswirkungen. Dies führt zur Planung der FMEA in qualitativer Beziehung auf festgelegten Ebenen (System, Teilsystem, Komponente, Einheit), um dem iterativen Entwurfs- und Entwicklungsprozess zu entsprechen.

Um die Wirksamkeit einer FMEA sicherzustellen, sollte diese im Zuverlässigkeitsprogramm fest verankert werden, zusammen mit der Zeit, dem Personalaufwand und anderen Mitteln, die benötigt werden, um sie wirkungsvoll zu machen. Es ist entscheidend, dass die FMEA nicht abgekürzt wird, um Zeit und Geld zu sparen. Wenn Zeit und Geld knapp sind, sollte die FMEA auf die Teile des Entwurfs konzentriert werden, die

neu sind oder auf eine neue Art verwendet werden. FMEA kann in wirtschaftlicher Weise auf Gebiete ausgerichtet werden, die durch andere Analyseverfahren als kritisch ermittelt wurden.

7.1.2 Anwendung auf einen Prozess

Wenn sie für einen Prozess durchgeführt wird, verlangt die PFMEA folgendes:

a) eine klare Festlegung des Prozesszieles. Wenn ein Prozess komplex ist, kann das Prozessziel zerlegt werden in das umfassende Ziel (oder das Produkt des Prozesses), das Ziel (oder ein Produkt eines Satzes von Prozesssequenzen oder -schritten) und das Produkt eines einzelnen Prozessschrittes;

b) Verstehen der einzelnen Prozessschritte;

c) Verstehen möglicher Schwachstellen in jedem Prozessschritt;

d) Verstehen der Auswirkungen, die jede einzelne Schwachstelle (möglicher Ausfall) auf das Prozessprodukt haben kann;

e) Verstehen der möglichen Ursachen jeder Schwachstelle oder jedes möglichen Prozessausfall/ -fehlzustands.

Wenn ein Prozess mehr als ein Produkt hervorbringt, dann kann er mit dem speziellen Produkt im Sinn untersucht werden; d. h., PFMEA ist ein Verfahren für einzelne Produkte. Der Prozess kann auch bezüglich seiner Schritte und möglicher unerwünschter Ergebnisse daraus untersucht werden, was zu einer verallgemeinerten PFMEA für den Prozess führen würde, ohne Berücksichtigung der Typen individueller Produkte.

7.2 Vorteile der FMEA

Einige detaillierte Anwendungen und Vorteile der FMEA sind nachfolgend aufgeführt:

a) Vermeiden von teuren Modifikationen durch frühzeitiges Erkennen von Schwächen im Entwurf;

b) Erkennen von solchen Ausfällen, die, wenn sie allein oder in Kombination auftreten, unannehmbare oder bedeutende Auswirkungen haben, und Bestimmen derjenigen Ausfallarten, die den erwarteten oder geforderten Betrieb ernstlich beeinträchtigen können;

ANMERKUNG 1 Solche Auswirkungen können Sekundärausfälle einschließen.

c) Erkennen der Notwendigkeit für Entwurfsmethoden zur Zuverlässigkeitsverbesserung (Redundanz, Betriebsbeanspruchungen, Ausfall zur sicheren Seite, Bauteileauswahl und -unterlastung usw.);

d) Erstellen des Logikmodells, das für die Bewertung der Wahrscheinlichkeit oder der Eintrittsrate anomaler Betriebsbedingungen des Systems in Vorbereitung einer Ausfallbedeutungsanalyse erforderlich ist;

e) Offenlegen von sicherheits- und hinsichtlich der Produkthaftung problematischen Gebieten oder von Nicht-Übereinstimmung mit behördlichen Anforderungen;

ANMERKUNG 2 Für die Sicherheit werden häufig getrennte Studien gefordert, aber eine Überschneidung ist unvermeidlich und daher ist eine Zusammenarbeit höchst ratsam.

f) Sicherstellen, dass das Entwicklungsprüfprogramm potentielle Ausfallarten entdecken kann;

g) Hinweisen auf die entscheidenden Gebiete, auf die sich Qualitätslenkung, Prüfung und Überwachung des Fertigungsprozesses konzentrieren sollen;

h) dazu beitragen, dass verschiedene Aspekte der allgemeinen Wartungsstrategie einschließlich Ablaufplan festgelegt werden;

i) Fördern oder Unterstützen der Festlegung von Prüfkriterien, Prüfplänen und Diagnoseverfahren, beispielsweise: Leistungsprüfung, Zuverlässigkeitsprüfung;

j) Unterstützen des Entwurfs von Abläufen zur Isolation von Fehlzuständen, der Planung für alternative Betriebsarten und der Planung von Umgestaltungen;

k) den Entwicklern ein Verständnis für diejenigen Faktoren vermitteln, die die Zuverlässigkeit des Systems beeinflussen;

l) Bereitstellen eines Abschlussdokumentes, aus dem hervorgeht, dass dafür gesorgt wurde (und bis zu welchem Maße), dass der Entwurf die Spezifikation im Einsatz erfüllen wird. (Dies ist insbesondere für den Fall der Produkthaftung bedeutend.)

7.3 Grenzen und Unzulänglichkeiten der FMEA

FMEA ist äußerst effizient, wenn sie zur Analyse von Elementen angewendet wird, die den Ausfall des gesamten Systems oder einer Hauptfunktion des Systems verursachen. Bei komplexen Systemen mit Mehrfach-Funktionen, an denen unterschiedliche Systemkomponenten beteiligt sind, kann FMEA jedoch schwierig und mühsam sein. Der Grund hierfür liegt in der Menge der zu berücksichtigenden detaillierten Informationen über das System. Diese Schwierigkeit kann noch dadurch verstärkt werden, dass es mehrere mögliche Betriebsarten gibt, als auch durch die Berücksichtigung von Reparatur- und Instandhaltungsvorschriften.

FMEA kann ein arbeitsaufwendiges und ineffizientes Verfahren sein, wenn es nicht mit Verstand angewendet wird. Der anschließende Verwendungszweck der Ergebnisse sollte festgelegt und FMEA sollte nicht wahllos in Anforderungsspezifikationen aufgenommen werden.

Komplikationen, Missverständnisse und Fehler können auftauchen, wenn die FMEA versucht, mehrere Ebenen in einer hierarchischen Struktur zu umfassen, und der Systementwurf Redundanz enthält.

Nicht alle Beziehungen zwischen einzelnen oder Gruppen von Ausfallarten oder Ursachen von Ausfallarten können tatsächlich in einer FMEA dargestellt werden, da die wesentliche Voraussetzung der Analyse die Unabhängigkeit der Ausfallarten ist. Diese Unzulänglichkeit tritt noch deutlicher hervor angesichts von Hardware-/Softwarewechselwirkungen, bei denen die Voraussetzung der Unabhängigkeit nicht erfüllt ist. Dieselbe Art von Schwierigkeiten kann angetroffen werden, wenn Wechselwirkungen zwischen Mensch und Hardware einbezogen und ihre gegenseitigen Abhängigkeiten modelliert werden. Die Annahme von Unabhängigkeit kann eine Ausfallart, die drastische Folgen haben kann, verschleiern, wenn sie das Ergebnis einer anderen Ausfallart ist, solange jede von ihnen alleine eine geringe Eintrittswahrscheinlichkeit hat. Die Zusammenhangsszenarien werden weit besser modelliert, wenn die Ausfallartanalyse zusammen mit dem FTA-Verfahren angewendet wird (IEC 60300-3-1, Ed. 2).

Es ist daher empfehlenswert, eine FMEA auf lediglich zwei Ebenen in der hierarchischen Struktur zu beschränken. Zum Beispiel ist es eine ziemlich überschaubare Aufgabe, die Ausfallarten von Einheiten zu ermitteln und deren Auswirkungen auf die Baugruppe zu bestimmen. Diese Auswirkungen werden dann die Ausfallarten in der nächsthöheren Ebene, z. B. den Modulen, und so weiter. Dennoch werden FMEA über mehrere Ebenen oft erfolgreich durchgeführt.

Eine weitere Schwäche der FMEA liegt in ihrer Unfähigkeit, ein Maß für die Zuverlässigkeit des Gesamtsystems zu liefern, und aus demselben Grund ist sie nicht in der Lage, Maßnahmen für Entwurfsverbesserungen und Kompromissstudien zu liefern.

7.4 Beziehungen zu anderen Verfahren

Eine FMEA (oder FMECA) kann für sich alleine durchgeführt werden. Als ein systematisches, induktives Analyseverfahren wird FMEA meistens als Ergänzung zu anderen Vorgehensweisen verwendet, insbesondere zu deduktiven Verfahren, wie z. B. FTA. In der Entwurfsphase ist es oft schwierig zu entscheiden, ob die induktive oder die deduktive Vorgehensweise überwiegt, da beide in Gedanken- und Analyse-Prozessen kombiniert sind. Wenn in industriellen Anlagen und Systemen risikobehaftete Ebenen erkannt werden, wird die deduktive Vorgehensweise bevorzugt, aber dennoch ist FMEA ein nützliches Hilfsmittel für den Entwurf. Sie sollte jedoch durch andere Verfahren ergänzt werden. Dies gilt insbesondere dann, wenn Probleme erkannt und Lösungen in Situationen gefunden werden müssen, in denen Mehrfachausfälle und sequentielle Auswirkungen zu untersuchen sind. Welches Verfahren zuerst angewandt wird, hängt vom Projektprogramm ab.

Während der frühen Entwurfsphasen, in denen zunächst nur Funktionen, allgemeine Systemstruktur und Teilsysteme festgelegt worden sind, kann erfolgreiches Verhalten des Systems durch ein Zuverlässigkeitsblockdiagramm oder durch den Ausfallpfad in einem Störungsbaum graphisch beschrieben werden. Dennoch sollte zur Unterstützung beim Zeichnen dieser Diagramme zur Beschreibung des Systemverhaltens ein induktiver FMEA-Prozess auf die Teilsysteme angewendet werden, ehe diese entworfen werden. Unter diesen Umständen kann die FMEA-Vorgehensweise kein umfassendes Verfahren sein, sondern ist eher ein gedanklicher Prozess, der nicht gleich in einer strengen Tabellenform ausgedrückt wird. Beim Analysieren eines komplexen Systems mit mehreren Funktionen, vielen Einheiten und Beziehungen zwischen diesen Einheiten, erweist sich die FMEA im Allgemeinen als notwendig, aber nicht als hinreichend.

Die Störungsbaumanalyse (FTA) ist ein ergänzendes deduktives Verfahren für die Analyse von Ausfallarten und ihrer entsprechenden Ursachen. Es macht in unteren Ebenen die Ursachen eines in einer hohen Ebene unterstellten Ausfalls ausfindig. Obwohl die logische Analyse lediglich für eine qualitative Analyse von Fehlzustandssequenzen verwendet werden kann, und manchmal auch so verwendet wird, so ist sie doch ein Vorläufer für die Schätzung der Häufigkeit des unterstellten Ausfalls in einer hohen Ebene. FTA eignet sich dafür, die gegenseitigen Abhängigkeiten verschiedener Ausfallarten zu modellieren, wobei diese Wechselwirkung zu einem Ergebnis beträchtlichen Ausmaßes und möglicherweise beträchtlicher Schwere führen kann. Das ist besonders wichtig, wo das Auftreten einer Ausfallart als Erstes das Auftreten einer anderen mit hoher Wahrscheinlichkeit und großer Schwere nach sich ziehen würde. Ein solches Szenario könnte mit einer FMEA nicht erfolgreich modelliert werden, bei der jede Ausfallart als unabhängig und individuell angesehen wird. Eine der Unzulänglichkeiten einer FMEA ist ihr Unvermögen, Wechselwirkung und die Dynamik des Auftretens von Ausfallarten in einem System zu betrachten.

FTA konzentriert sich auf die Logik von gleichzeitigen (oder sequentiellen) und alternativen Ereignissen, die unerwünschte Folgen verursachen. Sie kann ein wahrheitsgetreues Modell des analysierten Systems ergeben, ebenso wie einen Schätzwert für seine Funktionsfähigkeit (oder Ausfallwahrscheinlichkeit), und kann auch die Auswirkungen von Entwurfsverbesserungen und von Ausfallartentschärfung auf die Funktionsfähigkeit des Gesamtsystems beurteilen, was vorteilhaft sein kann. Das Format der FMEA kann mehr beschreibend sein. Beide Verfahren haben ihre Verwendung in einer umfassenden Analyse für Sicherheit und Zuverlässigkeit in einem komplexen System. Wenn jedoch das System hauptsächlich auf einer seriellen Logik beruht mit wenig Redundanzen und wenig Funktionen, dann ist FTA ein unnötig komplizierter Weg zur Darstellung der Logik und zum Erkennen der Ausfallarten. In solchen Fällen sind FMEA und Zuverlässigkeitsblockdiagramme angebracht. In anderen Fällen, in denen FTA bevorzugt wird, muss die FTA dennoch um Beschreibungen der Ausfallarten und Auswirkungen angereichert werden.

Die wesentlichen Überlegungen zur Wahl des Analyseverfahrens sollten auf den besonderen Anforderungen des Projektes, nicht nur im Hinblick auf die technischen Forderungen, sondern auch hinsichtlich Zeit, Kosten, Effizienz und Verwendung der Ergebnisse, beruhen. Im Folgenden finden sich einige allgemeine Leitlinien.

a) FMEA ist angebracht, wenn ein umfassendes Wissen über die Ausfalleigenschaften einer Einheit gefordert wird.

b) FMEA ist eher für kleine Systeme, Module und Baugruppen geeignet.

c) FMEA ist ein wesentliches Hilfsmittel während der Forschungs-, Entwurfs- und Entwicklungsphase, wenn nicht akzeptable Auswirkungen von Ausfällen erkannt und Lösungen gefunden werden müssen.

d) FMEA kann für neuerungsträchtige Einheiten notwendig sein, deren Ausfalleigenschaften noch nicht aus früheren Betriebserfahrungen bekannt sind.

e) FMEA ist üblicherweise besser geeignet für Einheiten mit einer großen Zahl zu betrachtender Komponenten, die vorwiegend eine serielle Ausfalllogik haben.

f) FTA ist allgemein eher geeignet für die Analyse mehrfacher Ausfallarten und von Abhängigkeiten mit komplexer Ausfalllogik und Redundanz. FTA kann auf den höheren Ebenen der Systemstruktur frühzeitig im Entwurfsstadium verwendet werden und kann hilfreich sein beim Erkennen, ob eine eingehende FMEA in den unteren Ebenen während des detaillierten Entwurfs notwendig ist.

Anhang A
(informativ)

Zusammenfassung der Verfahrensschritte für FMEA und FMECA

A.1 Schritte zur Durchführung der Analyse

Folgende Verfahrensschritte müssen für eine Analyse ausgeführt werden:

a) Entscheiden, ob eine FMEA oder FMECA erforderlich ist,
b) Festlegen der Systemgrenzen für die Analyse,
c) Verstehen der Forderungen an das System und seine Funktion,
d) Festlegen der Kriterien für Ausfall und Erfolg,
e) Ermitteln und Aufzeichnen der Ausfallarten für jede Einheit sowie deren Ausfallauswirkung,
f) Zusammenfassen jeder Ausfallauswirkung,
g) Berichten der Ergebnisse.

Für eine FMECA müssen folgende zusätzliche Schritte ausgeführt werden:

h) Festlegen der Schwereklassen für das System,
i) Ermitteln der Schwere der Ausfallart der Einheit,
j) Ermitteln der Häufigkeit von Ausfallart und -auswirkungen der Einheit,
k) Ermitteln von Ausfallarthäufigkeiten,
l) Zeichnen der Kritizitätsmatrix für die Ausfallarten der Einheit,
m) Zusammenfassen der Bedeutung der Ausfallauswirkung anhand der Kritizitätsmatrix,
n) Zeichnen der Kritizitätsmatrix für die Systemausfallauswirkungen,
o) Berichten der Ergebnisse aus allen Analyseebenen.

ANMERKUNG Quantifizierung der Häufigkeiten von Ausfallart und -auswirkung kann in einer FMEA geschehen, indem die Schritte h), i) und j) am Ende der FMEA ausgeführt werden.

A.2 FMEA-Arbeitsblatt

A.2.1 Umfang eines Arbeitsblattes

Das FMEA-Arbeitsblatt enthält die Einzelheiten der Untersuchung in tabellarischer Art. Wenngleich die allgemeine FMEA-Vorgehensweise eine Richtschnur ist, kann der Entwurf eines bestimmten Arbeitsblattes angepasst werden, um den Anwendungs- und Projektforderungen zu entsprechen.

Bild A.1 ist ein Beispiel für die Ausführung eines FMEA-Arbeitsblattes.

A.2.2 Kopf des Arbeitsblattes

Der Kopfteil des Formblattes enthält die folgenden Informationen:

– das System als Ziel-Einheit bezeichnet die Einheit, für die die Endauswirkungen ermittelt werden sollen. Diese Bezeichnung sollte im Einklang stehen mit der in Blockdiagrammen, Schaltbildern und anderen Darstellungen verwendeten Terminologie;
– die für die Analyse unterstellte Betriebsart;
– Einheit bezieht sich auf die Einheit (Modul, Baugruppe oder Bauteil), die in diesem Arbeitsblatt untersucht wird;

– Überarbeitungsebene, Datum und Name des Bearbeiters, der den FMEA-Aufwand abstimmt, sowie die Namen der Kernteammitarbeiter bilden weitere Informationen für die Dokumentenlenkung.

A.2.3 Spalteneingänge des Arbeitsblattes

Die Spalten für „Bezeichnung der Einheit“ und „Funktionsbeschreibung der Einheit“ sollen den Gegenstand der Untersuchung festlegen. Die Kennzeichnung sollte zum Blockdiagramm und zu anderen unterstützenden Dokumenten passen. Eine kurze Beschreibung der Einheit und seiner Funktion wird eingetragen.

Die Art und Weise, in der die Einheit ausfallen kann, wird unter „Ausfallart“ eingetragen. Unterabschnitt 5.2.3 enthält Leitlinien für die Ermittlung möglicher Ausfallarten. Das Eintragen eines eindeutigen Identifizierungsmerkmals („Ausfallart-Code“) für jede einzelne Ausfallart wird die Zusammenfassung der Ergebnisse der Untersuchung erleichtern.

Die wahrscheinlichsten Ursachen für die Ausfallart werden unter „Mögliche Ausfallursachen“ aufgelistet.

Eine knappe Beschreibung der Auswirkungen der Ausfallart auf die untersuchte Einheit wird unter „lokale Auswirkung“ eingetragen. Ähnliche Informationen werden in die Spalte „Auswirkungen auf die Ziel-Einheit“ eingetragen, um auf die Auswirkungen der Ausfallart auf die Ziel-Einheit hinzuweisen. Für manche FMEA-Analysen ist es wünschenswert, die Ausfallauswirkung auf eine dazwischen liegende Ebene zu beurteilen. In diesem Fall wird die Auswirkung auf „Nächsthöhere Ebene“ in eine zusätzliche Spalte eingetragen. Die Ermittlung von Ausfallartauswirkungen wird in 5.2.5 eingehender behandelt.

Eine kurze Beschreibung, wie die Ausfallart erkannt wird, wird unter „Erkennungsmethode“ angedeutet. Die Erkennung kann automatisch erfolgen durch ein in den Entwurf eingebautes Prüfmittel (en: built-in-test, BIT) oder kann diagnostische Verfahren seitens des Betriebs- oder Instandhaltungspersonals erfordern. Es ist wichtig, die Erkennungsmethode festzuhalten, damit der Bearbeiter sicher sein kann, dass Abhilfemaßnahmen getroffen werden.

Eigenschaften des Entwurfs, die eine besondere Ausfallart entschärfen, wie z. B. Redundanz, müssen unter „Vorkehrungen zur Ausfallvermeidung“ festgehalten werden. Kompensierung durch spezielle Instandhaltungs- oder Betreibermaßnahmen sollten hier ebenfalls eingetragen werden.

Die „Schwereklasse“ kennzeichnet das von den FMEA-Bearbeitern festgelegte Schwereniveau.

„Eintrittshäufigkeit“ kennzeichnet die Eintrittsrate der jeweiligen Ausfallart. Die Häufigkeitsskala wird angepasst, um der Anwendung zu genügen (z. B. Ausfälle pro Millionen Stunden, Ausfälle pro zurückgelegter Entfernung, d. h. 1000 km, usw.)

Die Spalte „Bemerkungen“ enthält die Beobachtungen und Empfehlungen der Bearbeiter, wie in 5.3.4 beschrieben.

A.2.4 Bemerkungen im Arbeitsblatt

Der letzte Spalteneingang im Arbeitsblatt sollte alle sachdienlichen Hinweise zur Erläuterung anderer Spalten geben. Mögliche zukünftige Maßnahmen, wie etwa Empfehlungen für Entwurfsverbesserungen, können festgehalten und dann in dem Bericht näher ausgeführt werden. Diese Spalte kann auch das Folgende enthalten:

a) jedwede ungewöhnlichen Bedingungen;

b) Auswirkungen des Ausfalls redundanter Einheiten;

c) Kenntlichmachung besonders kritischer Entwurfseigenschaften;

d) beliebige Bemerkungen zur Verstärkung des Eintrags;

e) Verweis auf andere Spalten für anschließende Ausfallanalyse;

f) wichtige Forderungen an die Instandhaltung;

g) dominierende Ausfallursachen;

h) vorherrschende Ausfallwirkungen;

i) getroffene Entscheidungen, z. B. bei Bewertungen des Entwurfs.

FMEA

Ziel-Einheit: Betriebsdauer:			Einheit: Ausgabestand:					Bearbeiter: Datum:			
Bezeichnung der Einheit	Funktionsbeschreibung der Einheit	Ausfallart	Ausfallart-Code	Mögliche Ausfallursachen	Lokale Auswirkung	Auswirkung auf die Ziel-Einheit	Erkennungsmethode	Vorkehrungen zur Ausfallvermeidung	Schwereklasse	Häufigkeit oder Eintrittswahrscheinlichkeit	Bemerkungen

Bild A.1 – Beispiel für das Format eines FMEA-Arbeitsblattes

Anhang B
(informativ)

Analysebeispiele

B.1 Beispiel 1 – FMEA[N5)] für ein Teil einer Automobilelektronik mit Berech-nung der Risikoprioritätszahl

In Bild B.1 wird ein kleiner Teil einer umfangreichen FMECA für ein Produkt der Automobiltechnik dargestellt. Die untersuchte Anordnung ist die Stromversorgung und lediglich ihre Verbindungen zum Batteriekabel.

Die Verbindung zum Batteriekabel[N6)] enthält eine Diode D1 und einen Kondensator C9, die den Pluspol der Batterie mit der Erde verbinden. Die Diode ist in Sperrrichtung eingebaut, so dass, falls der Minuspol der Batterie mit der Einheit verbunden wird, die negative Spannung einen Kurzschluss zur Erde verursachen und so die Einheit vor Schaden bewahren würde. Der Kondensator dient als Entstörfilter. Falls eines dieser Teile einen Kurzschluss haben sollte, würde es die Batterie auch kurzschließen, was zur Entleerung der Fahrzeugbatterie führen könnte. Solch ein Ausfall tritt natürlich ohne vorherige Warnung auf, und ein so genannter „Liegenbleiber“ (en: „walk home“ failure) wird in der Automobilindustrie als gefährlich eingestuft. Daher ist bei beiden Bauelementen die Schwere (en: severity) für die Ausfallart „Kurzschluss“ mit 10 eingestuft. Die Auftretenswahrscheinlichkeiten wurden aus den Bauelementeausfallraten unter Beachtung der jeweiligen Beanspruchungen während der Fahrzeuglebensdauer berechnet und dann an die *O*-Skala (en: probability of occurrence) der Fahrzeug-FMEA angepasst. Der Rang für die Erkennung ist sehr niedrig, da das Kurzschließen irgendeines der beiden Bauelemente im Test sofort auffallen würde – Einheit nicht betriebsbereit.

Eine Unterbrechung irgendeines der oben genannten Bauelemente würde an der Einheit keinen Schaden verursachen, außer wenn die Diode unterbricht, denn dann gäbe es keinen Batterieschutz bei Verpolung, während es bei unterbrochenem Kondensator keine Entstörfilterung gäbe – also mögliche Störung für andere Geräte im Fahrzeug.

Zwischen der Batterie und der Schaltung der Einheit ist eine Spule L1 eingebaut, in erster Linie zum Filtern. Wenn die Spule unterbricht, wäre die Einheit nicht betriebsbereit, da die Batterie abgetrennt würde. Die Einheit wäre nicht betriebsbereit, so dass die Warnanzeige nicht leuchten würde. Spulen haben eine sehr geringe Ausfallrate, so dass der Rang für das Auftreten 2 ist.

Der Widerstand R91 führt die Batteriespannung zu den Schalttransistoren; wenn er durch Unterbrechung ausfällt, würde dies die Einheit außer Funktion setzen, was auch Rang 9 bei der Schwere hat. Da Transistoren eine sehr niedrige Ausfallrate haben, ist der Rang für das Auftreten 2. Der Rang für die Entdeckung ist 1, da die Einheit nicht betriebsbereit wäre.

N5) Nationale Fußnote: Offensichtlich handelt es sich um eine FMECA.

N6) Nationale Fußnote: Im Original: „The battery line has a diode …“, vgl. dazu Bild B.1, Spalten 2 und 3.

Einheit/Funktion			Mögliche Ausfallart	Mögliche Ausfallauswirkung(en)		Schwere	Klasse	Mögliche Ausfallursache(n)/ -mechanismen	Genaue Ursache(n)/ Mechanismen des Ausfalls	Auftreten	Derzeitige Entwurfsüberwachung, Vorbeugung	Derzeitige Entwurfsüberwachung, Entdeckung	Entdecken	RPN	Empfohlene Maßnahmen	Verantwortung und geplantes Abschlussdatum	Ergebnis der Maßnahmen				
Teilsystem	Baugruppe	Komponente		Lokale Auswirkung	Endauswirkung												ergriffene Maßnahmen	Schwere	Auftreten	Entdecken	RPN
Stromversorgung																					
	V1																				
		D1	Kurzschluss	Batteriepluspol hat Kurzschluss zur Erde	Batterie entleert sich – Liegenbleiber	10		Fehler innerhalb der Komponente	Elektrischer Durchschlag im Isoliermaterial	3	Wahl besserer Qualität u. Auslegung	Bewertung und Zuverl. validierungsprüfung	1	30							
		D1	Unterbrechung	kein Verpolungsschutz	nicht zu bemerken	2		Fehler innerhalb der Komponente	Riss in der Bondverbindung oder Bruch/Riss des Halbleiters	3	Wahl besserer Qualität u. Auslegung	Bewertung und Zuverl. validierungsprüfung	2	12							
		C9	Kurzschluss	Batteriepluspol hat Kurzschluss zur Erde	Batterie entleert sich – Liegenbleiber	10		Fehler innerhalb der Komponente	Dielektrischer Durchschlag oder Riss	3	Wahl besserer Qualität u. Auslegung	Bewertung und Zuverl. validierungsprüfung	1	30							
		C9	Unterbrechung	Keine Entstörfilterung	Betrieb der Einheit außerhalb der Spezifikation	2		Fehler innerhalb der Komponente	Unterbrechung, Leck, Fehlstelle oder Riss im Dielektrikum	2	Wahl besserer Qualität u. Auslegung	Bewertung und Zuverl. validierungsprüfung	1	4							
		L1	Unterbrechung	Keine V1 –	Einheit nicht betriebsbereit, keine Warnanzeige	9		Fehler innerhalb der Komponente	Elektrischer Durchschlag im Isoliermaterial	2	Wahl besserer Qualität u. Auslegung	Bewertung und Zuverl. validierungsprüfung	1	18							
		R91	Unterbrechung	Schaltkreis der	Einheit nicht	9		Fehler innerhalb der	Riss in der Bondver-	2	Wahl besserer Qualität	Bewertung und Zuverl.	1	18							

Einheit/Funktion			Mögliche Ausfallart	Mögliche Ausfallauswirkung(en)		Schwere	Klasse	Mögliche Ausfall-ursache(n)/ -mechanismen	Genaue Ursache(n)/ Mechanis-men des Ausfalls	Auftreten	Derzeitige Entwurfs-über-wachung, Vorbeugung	Derzeitige Entwurfs-über-wachung, Entdeckung	Entdecken	RPN	Empfoh-lene Maß-nahmen	Verant-wortung und geplantes Abschluss-datum	Ergebnis der Maßnahmen				
Teilsystem	Bau-gruppe	Kompo-nente		Lokale Auswir-kung	End-auswir-kung												ergriffene Maß-nahmen	Schwere	Auftreten	Entdecken	RPN
				Einheit span-nungslos	betriebs-bereit, keine Warn-anzeige			Komponente	bindung oder im Material		u. Auslegung	validierungs-prüfung									

Bild B.1 – FMEA[N7)] für ein Teil der Automobilelektronik mit Berechnung der Risikoprioritätszahl

N7) Nationale Fußnote: Hier muss „FMECA“ stehen, siehe B.1 - 1. Satz.

B.2 Beispiel 2 – FMEA für Teilsystem eines Motor-Generator-Satzes

Dieses Beispiel zeigt die Anwendung der FMEA-Technik auf ein Motor-Generator(M-G)-System. Das Ziel der Untersuchung war auf dieses System beschränkt und betraf weder die Ausfallauswirkungen auf irgendwelche vom M-G-Satz mit der elektrischen Energie versorgten Verbraucher noch andere externe Auswirkungen von Ausfällen. Damit sind die Grenzen der Analyse festgelegt. Das nur teilweise gezeigte Beispiel veranschaulicht, wie das System in Form eines hierarchischen Diagramms[N8)] dargestellt war. Eine zu Anfang gemachte Unterteilung legte fünf Teilsysteme fest (siehe Bild B.2), und eines davon, das Teilsystem Heizung, Lüftung und Kühlung des Gehäuses, wird über dazwischen liegende Ebenen der hierarchischen Struktur bis zur Komponentenebene entwickelt, auf der mit der FMEA zu beginnen entschieden wurde (siehe Bild B.3). Die Diagramme zeigen auch das verwendete Nummerierungssystem, das als Querbezug in den FMEA-Arbeitsblättern benutzt wurde.

Ein Beispiel eines Arbeitsblattes, das im Allgemeinen mit dem in dieser Norm empfohlenen Format übereinstimmt, ist für eines der Teil-Teilsysteme des M-G-Satzes (siehe Bild B.4) gezeigt.

Eine wesentliche Voraussetzung für solch eine FMEA ist die Definition und Klassifizierung der Schwere der Auswirkung von Ausfällen auf das gesamte M-G-System. Für die spezielle Anwendung dieses Beispielsystems wurden sie so festgelegt, wie in Tabelle B.1 angegeben.

Tabelle B.1 – Definition und Klassifizierung der Schwere der Auswirkungen von Ausfällen auf das gesamte M-G-System

Grad	Schwere	Beschreibung
5	katastrophal	Ausfall der Stromerzeugung für den Rest der Mission
4	kritisch	Leistung des Systems für den Rest der Mission eingeschränkt
3	bedeutend	keine Stromerzeugung aufgrund erzwungener Abschaltung, bis die Reparatur erfolgt ist
2	geringfügig	Leistung des Systems vorübergehend bis zu günstigem Reparaturzeitpunkt eingeschränkt
1	vernachlässigbar	keine oder nur vernachlässigbare Einschränkung der Stromerzeugungs-fähigkeit

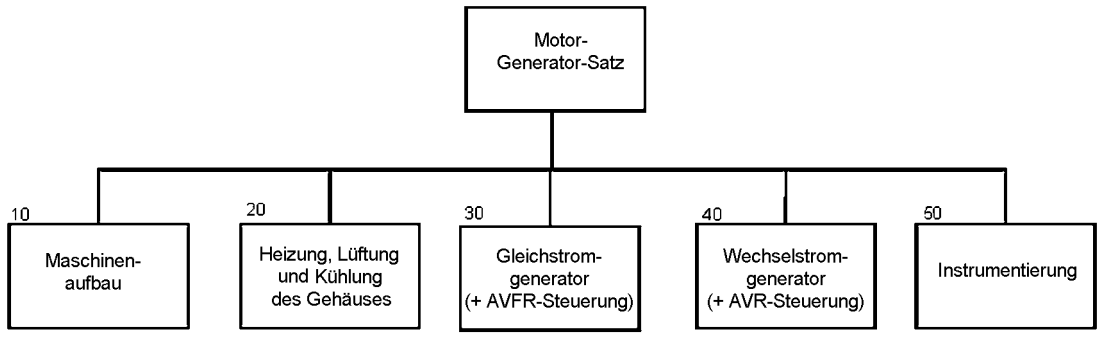

Bild B.2 – Diagramm der Teilsysteme eines Motor-Generator-Satzes

N8) Nationale Fußnote: In der englischen Fassung „hierarchisches Blockdiagramm“ genannt.

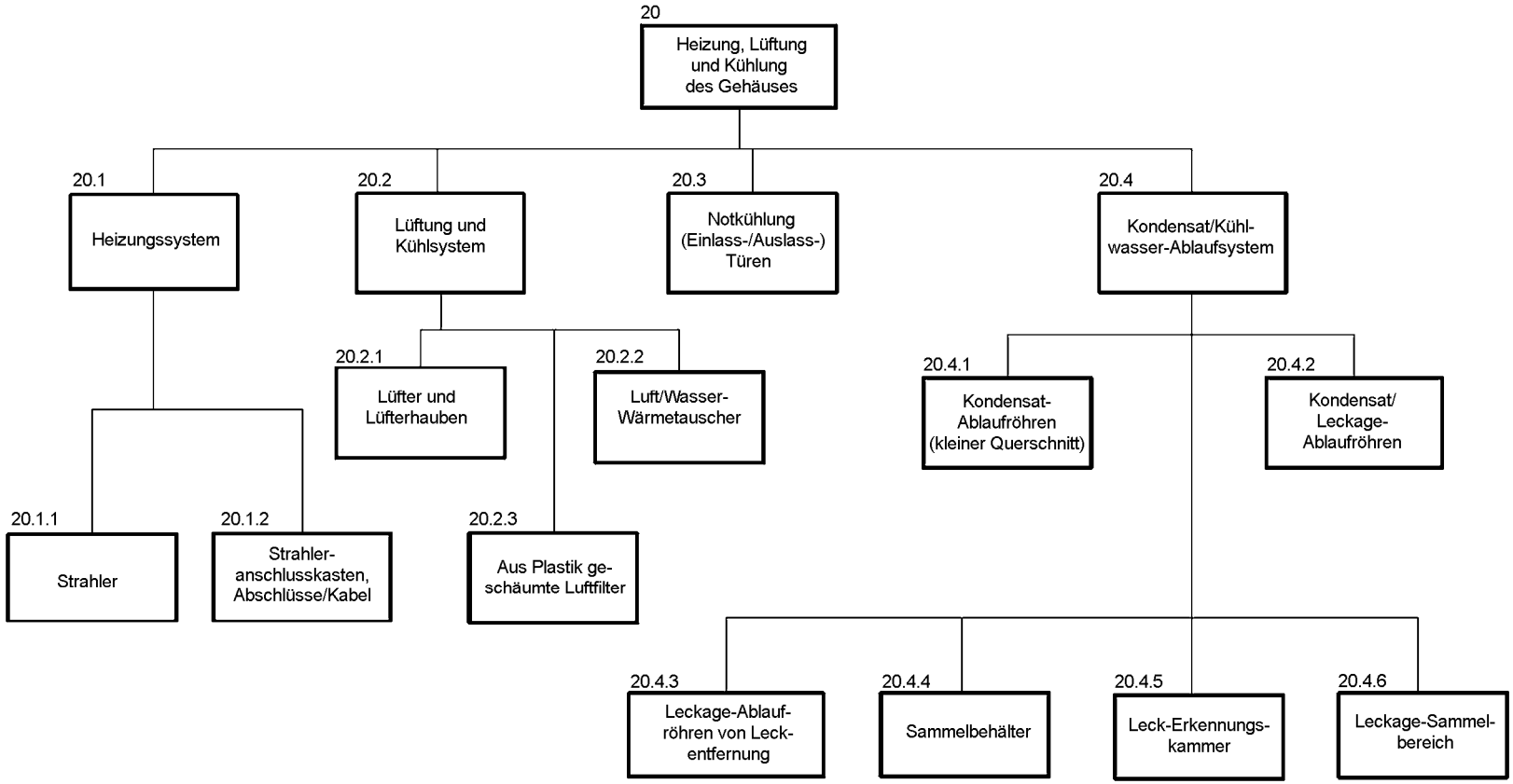

Bild B.3 – Diagramm der Systeme „Heizung, Lüftung und Kühlung des Gehäuses“

Teilsystem – 20 „Heizung, Lüftung und Kühlung des Gehäuses“													
Ref.	**Komponente**	**Funktion**	**Ausfallart**	**Ausfallaus-wirkung**	**Erkennung durch bzw. Symptom**	**Redundanz-vorkeh-rungen**	**Ausfallrate (je Ausfallart und Schwereklasse) (10^{-6}/h)**					**Bemerkungen**
							1	2	3	4	5	
20.1	Heizsystem (12 aus – 6 aus an jedem Ende) (nur verwendet, wenn Maschine nicht betriebs-bereit)	Alle										ANMERKUNG Die Maschine kann überhitzen, wenn die Strahler nicht automatisch abgeschaltet werden, wenn die Maschine läuft.
20.1.1	Strahler	Gehäuse heizen	a) elektrisch unter-brochen, Strahler ausgebrannt b) Kurzschluss oder Erdschluss durch Isolationsbruch	reduzierte Heiz-leistung Heizleistung ist null – Konden-sation möglich	a) Temperatur-anzeige < 5° über Umgebung b) Versorgungs-strom, Schmelz-sicherung oder Sicherungsauto-mat überwacht	Alle parallel, keine Versor-gungsredun-danz				1,2 0,3		 Ein Erdschluss sollte das System nicht zum Aus-fallen bringen.
20.1.2	Strahleranschluss-kasten, Abschlüsse/Kabel	Anschluss zur Versor-gung der Strahler	a) elektrisch unter-brochener Abschluss oder Kabel kann einen, drei, sechs oder alle Strahler zum Ausfall bringen b) Kurzschluss der Abschlüsse (Ketten-reaktion)	keine oder reduzierte Heizleistung – Kondensation Heizleistung ist null – Konden-sation	Temp. < 5° über Umgebung Versorgung überwacht					0,5 vernach-lässigbar		
						Summe				2,0		

Bild B.4 – FMEA für Teilsystem 20

B.3 Beispiel 3 – FMECA für einen Herstellprozess

Mit einer Fertigungs- oder Prozess-FMECA werden die bei der Fertigung einer Einheit beteiligten Prozesse betrachtet, was schiefgehen könnte, welche Schutzvorkehrungen gegen Ausfall bestehen, wie oft dies sich ereignen könnte und wie es durch eine Änderung des Entwurfs der Einheit oder des Prozesses beseitigt werden könnte. Das Ziel ist, die Aufmerksamkeit auf mögliche (oder bekannte) Probleme beim Aufrechterhalten oder Erreichen der geforderten Qualität des Ausstoßes zu konzentrieren. Bei der Montage komplexer Güter, wie etwa Kraftfahrzeugen, sind die Montagefirmen gut beraten, darauf zu bestehen, dass die Zulieferer ihrer Komponenten solche Analysen durchführen; die Hersteller der Komponenten haben jedoch üblicherweise den größten Nutzen davon. Die Durchführung der Prozess-FMECA zwingt zu einer Neu-Untersuchung eingefahrener Fertigungsmethodik und führt meistens zu Kostenverbesserungen.

Die Ausführung ist grundsätzlich ähnlich zu der einer Produkt-FMECA, aber einige Änderungen werden durch leicht unterschiedliche Forderungen (siehe Bild B.5) erzwungen. Das Maß für die Kritizität ist eine Maßnahmenprioritätszahl APN (en: Action Priority Number), die im Wesentlichen der weiter oben diskutierten Risikoprioritätszahl RPN entspricht. Die Prozess-FMECA untersucht, wie Fehler und fehlerhafte Teile entstehen und den Kunden erreichen können oder wie sie durch Qualitätslenkungsverfahren gefunden werden können. Sie untersucht nicht, wie das Produkt im Einsatz aufgrund von Abnutzung oder falschem Betreiben ausfallen kann. Es gibt eine unvermeidbare geringe Überlappung, da einige Fehler die Haltbarkeit der Komponenten im Einsatz beeinträchtigen, andere dagegen unmittelbar zu Ausfällen oder zu Frühausfällen führen.

								Bestehende Bedingungen						Geänderte Bedingungen			
Ref.	**Prozess**	**Ausfallart**	**Aus wirkung auf**	**Mögliche Aus-wirkung**	**V**	**Mögliche Ursache**	**Bestehende Über wachungen**	**Occ**	**Sev**	**Det**	**APN**	**Empfohlene Maßnahme**	**Durchg eführte Maß-nahme**	**Occ**	**Sev**	**Det**	**APN**
01-01-01	Einführen	Falsche Größe oder verbogene Schulter-winkel	i)a	Einführen ohne Last auf Pressform, reduzierte Produktivität		Schlechte Fertigung oder schlechte Qualitätslenkung	Hersteller- und Annahme-Stichproben-pläne	1	9	9	81	Bewertung der Stichprobenpläne; Aussortieren fehlerhafter Rohlinge; Schulung der Maschinenführer					
02			i)b	Einführung falsch aus-gerichtet													
03			i)a	Falsche Dicke des Einfüh-rungsrands													
04			iv)b	Reduzierte Leistung													
05			iv)c	Reduzierte Lebensdauer													
01-02-01	Einführen	Schlechte schnelle Nickel-plattierung	ii)a	Korrosion; Rückweisung bei der Ober-flächen-behandlung			Sichtprüfung während der Ausführung des Annahme-Stichproben-plans	5	6	1	30	Anweisungen zur Sichtprüfung auf korrekte Plattierung in die Stichprobenprü-fung aufnehmen					
01-03-01	Einführen	Unpas-sende Ausrich-tung	i)a	Schlechter Metallfluss; falsche Wand-stärke. Schrott		Schlechte Ferti-gung oder schlechte Qua-litätslenkung	Sichtprüfung während der Ausführung der Annahme-Stichproben-prüfung	2	8	6	96	Anweisungen zur Sichtprüfung auf korrekte Plattie-rung in die Stich-probenprüfung aufnehmen					
02			ii)a	Dünne Wände während des Pressens er-kannt													
				Schrott													
03			iv)a	Reduzierte Lebensdauer													

Auswirkungscode:
Auswirkung auf den Pressprozess
Auswirkung auf den Oberflächenbehandlungsprozess
Auswirkung auf den Montageprozess
Auswirkung auf den Endanwender

Kritizitätscode:
Occ = Eintrittswahrscheinlichkeit × 10
Sev = Schwere der Auswirkung auf Skala von 1–10
Det = Wahrscheinlichkeit nicht erkannt vor Eintreffen beim Kunden × 10
APN = Maßnahmenprioritätszahl = Occ × Sev × Det

Bild B.5 – Teil einer Pozess-FMECA für Aluminiumstrangpressen

Literaturhinweise

[1] BS 5760-5:1991, *Reliability of systems equipment and components – Part 5: Guide to failure modes, effects and criticality analysis (FMEA and FMECA).*

[2] SAE J1739:2000, *Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery.*

[3] SAE ARP5580:2001, *Failure Modes, Effects, and Criticality Analysis Procedures.*

[4] AIAG, *Potential Failure Mode and Effects Analysis, Third Edition, 2001.*

[5] M. Krasich, *Fault Tree Analysis for Failure Modes Identification and Product Reliability Improvement,* Tutorial presented at the Reliability and Maintainability Symposium; Tutorial Proceedings of 2002, 2003, and 2005.

[6] J. Bowles, *An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis*, technical paper presented at the Reliability and Maintainability Symposium, 2003.

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

[8] IEC 60300-1, *Dependability management – Part 1: Dependability management systems.*

ANMERKUNG Harmonisiert als EN 60300-1:2003 (nicht modifiziert).

[9] IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management.*

ANMERKUNG Harmonisiert als EN 60300-2:2004 (nicht modifiziert).

[10] IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems.*

[11] IEC 61160, *Formal design review.*

ANMERKUNG Harmonisiert als EN 61160:2005 (nicht modifiziert).

[12] IEC 61165, *Application of Markov techniques.*

[13] IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance.*

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

ANMERKUNG Harmonisiert als EN ISO 9000:2000 (nicht modifiziert).

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 Wenn internationale Publikationen durch gemeinsame Abänderungen geändert wurden, durch (mod.) angegeben, gelten die entsprechenden EN/HD.

Publikation	Jahr	Titel	EN/HD	Jahr
IEC 60300-3-1	2003	Dependability management Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology	EN 60300-3-1	2004
IEC 61025	–[1)]	Fault tree analysis (FTA)	HD 617 S1	1992[2)]
IEC 61078	–[1)]	Analysis techniques for dependability – Reliability block diagram and Boolean methods	EN 61078	2006[2)]

1) Undatierte Verweisung.

2) Zum Zeitpunkt der Veröffentlichung dieser Norm gültige Ausgabe.