

**DIN EN 60812**

ICS 03.120.01; 21.020; 29.020

Einsprüche bis 2015-09-03  
Vorgesehen als Ersatz für  
DIN EN 60812:2006-11**Entwurf****Fehlzustandsart- und -auswirkungsanalyse (FMEA)  
(IEC 56/1579/CD:2014)**Failure Mode and Effects analysis (FMEA)  
(IEC 56/1579/CD:2014)**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2015-07-03 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter [www.entwuerfe.din.de](http://www.entwuerfe.din.de) bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de), sofern dort wiedergegeben;
- oder als Datei per E-Mail an [dke@vde.com](mailto:dke@vde.com) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter [www.din.de/stellungnahme](http://www.din.de/stellungnahme) oder für Stellungnahmen zu Norm-Entwürfen der DKE unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 144 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

## Inhalt

|                                                                                         | Seite |
|-----------------------------------------------------------------------------------------|-------|
| Einleitung .....                                                                        | 7     |
| 1 Anwendungsbereich .....                                                               | 8     |
| 2 Normative Verweisungen .....                                                          | 8     |
| 3 Begriffe und Abkürzungen .....                                                        | 8     |
| 3.1 Begriffe .....                                                                      | 8     |
| 3.2 Abkürzungen .....                                                                   | 9     |
| 4 Überblick.....                                                                        | 10    |
| 4.1 Ziele der FMEA.....                                                                 | 10    |
| 4.2 Terminologie .....                                                                  | 10    |
| 4.2.1 Abstufung der Einheiten oder Prozesse.....                                        | 11    |
| 4.2.2 Rollen innerhalb einer FMEA .....                                                 | 11    |
| 4.2.3 Wahrscheinlichkeit eines Fehlzustandes .....                                      | 12    |
| 4.4 Struktur des Dokumentes.....                                                        | 13    |
| 5 Methodik für FMEA.....                                                                | 13    |
| 5.1 Allgemein .....                                                                     | 13    |
| 5.2 Planung des FMEA.....                                                               | 15    |
| 5.2.1 Allgemein.....                                                                    | 15    |
| 5.2.2 Bestimmen des Umfangs und der Zielsetzung der Analyse .....                       | 15    |
| 5.2.3 Ermitteln von Grenzen und Bedingungen .....                                       | 16    |
| 5.2.4 Definieren von Entscheidungskriterien für die Behandlung von Ausfallarten .....   | 17    |
| 5.2.5 Zuschneiden der FMEA um die Analyse zu planen .....                               | 17    |
| 5.2.6 Definition von Ressourcen für die Analyse .....                                   | 20    |
| 5.2.7 Zerlegen von Einheit oder Prozess in geeignete Elemente .....                     | 21    |
| 5.3 Durchführen der FMEA.....                                                           | 22    |
| 5.3.1 Allgemein.....                                                                    | 22    |
| 5.3.2 Bestimmen von Funktion und Leistungsmerkmalen von Einheit oder Prozess .....      | 22    |
| 5.3.3 Bestimmen von Ausfallarten.....                                                   | 22    |
| 5.3.4 Bestimmen von lokalen und gesamten Auswirkungen von Ausfallarten.....             | 23    |
| 5.3.5 Bestimmen von Ausfallursachen .....                                               | 24    |
| 5.3.6 Bestimmen von Aufdeckungsmethoden und existierenden Steuerungsmöglichkeiten ..... | 26    |
| 5.3.7 Bestimmung der Schwere der Auswirkung des Ausfalls auf die Einheit.....           | 27    |
| 5.3.8 Abschätzen der Wahrscheinlichkeit einer Ausfallart .....                          | 28    |
| 5.3.9 Bewerten der Kritikalität .....                                                   | 29    |
| 5.3.10 Bestimmen von Handlungen .....                                                   | 29    |
| 5.4 Dokumentieren der FMEA.....                                                         | 30    |
| 5.4.1 Allgemein.....                                                                    | 30    |
| 5.4.2 Mindestinhalt von Dokumentation .....                                             | 31    |
| 5.5 Abschließen der FMEA.....                                                           | 31    |

|                                                                                           | Seite |
|-------------------------------------------------------------------------------------------|-------|
| 6 Literaturhinweise .....                                                                 | 31    |
| Anhang A (informativ) Zuschnitt der FMEA.....                                             | 33    |
| A.1 Allgemein.....                                                                        | 33    |
| A.2 Kriterien für die Quadranten.....                                                     | 34    |
| A.2.1 „Top-down“-Analyse .....                                                            | 34    |
| A.2.2 „Bottom-up“-Analyse .....                                                           | 34    |
| A.2.3 Qualitativ und semi-quantitativ .....                                               | 34    |
| A.2.4 Quantitativ .....                                                                   | 35    |
| A.2.5 Keine Analyse notwendig.....                                                        | 35    |
| A.2.5.1 Quadrant A.....                                                                   | 35    |
| A.2.5.2 Quadrant B.....                                                                   | 35    |
| A.2.5.3 Quadrant C.....                                                                   | 36    |
| A.2.5.4 Quadrant D.....                                                                   | 36    |
| A.3 Risikoeigenschaften .....                                                             | 36    |
| A.3.1 Verwendung .....                                                                    | 36    |
| A.3.2 Reife des Designs .....                                                             | 37    |
| A.3.3 Verwendete Technologie .....                                                        | 37    |
| A.3.4 Anwendung .....                                                                     | 37    |
| A.4 Unterstützung .....                                                                   | 38    |
| A.4.1 Kontext der Nutzung von Szenarien zur Auswahl eines Quadranten.....                 | 38    |
| Anhang B (informativ) Beispiele von Inhalten des FMEA-Berichtes .....                     | 39    |
| Anhang C (informativ) Kritikalitätsbeurteilungsmethode .....                              | 40    |
| C.1 Allgemein.....                                                                        | 40    |
| C.2 Matrix-Methoden .....                                                                 | 40    |
| C.2.1 Allgemein.....                                                                      | 40    |
| C.2.2 Kategorisierung der Auswirkungen .....                                              | 40    |
| C.2.3 Wahrscheinlichkeitskategorisierung.....                                             | 41    |
| C.2.4 Kritikalitätskategorisierung .....                                                  | 41    |
| C.3 Risikoprioritätszahl .....                                                            | 42    |
| Anhang D (informativ) Beispielformen von FMEA .....                                       | 44    |
| D.1 Allgemein.....                                                                        | 44    |
| D.2 Software-FMEA.....                                                                    | 44    |
| D.3 Prozess-FMEA .....                                                                    | 44    |
| D.4 FMEA für sicherheitsrelevante Regelungssysteme .....                                  | 45    |
| D.4.1 FMEA bei der Planung einer Sicherheitsanwendung .....                               | 45    |
| D.4.2 Kritikalitätsanalyse für ein sicherheitsbezogenes Regelsystem .....                 | 45    |
| D.5 Automobil-FMEA .....                                                                  | 46    |
| D.6 FMECA innerhalb RCM.....                                                              | 46    |
| D.7 FMEA in komplexen nicht reparierbaren Systemen mit zugewiesener Ausfallfrequenz ..... | 46    |

|                                                                                                                          | Seite |
|--------------------------------------------------------------------------------------------------------------------------|-------|
| D.8 Kritikalitätsbeurteilung von komplexen reparierbaren Systemen mit zugewiesener Verfügbarkeit .....                   | 47    |
| D.9 Nichtverfügbarkeit von Kritikalitätsbeurteilungen von gewarteten Systemen .....                                      | 47    |
| Anhang E (informativ) Beispielapplikationen von Varianten von FMEA .....                                                 | 49    |
| E.1 Anwendung für Herstellungsprozesse .....                                                                             | 49    |
| E.2 Anwendung für medizinische Anwendungen .....                                                                         | 49    |
| E.3 Softwareanwendung für einen Blutzuckerrechner .....                                                                  | 50    |
| E.4 Designanwendung .....                                                                                                | 53    |
| E.4.1 Funktion der Einheit .....                                                                                         | 53    |
| E.4.2 Ausfallarten der Einheit .....                                                                                     | 53    |
| E.4.3 Ausfallauswirkungen für die Einheit .....                                                                          | 53    |
| E.5 Instandhaltungs- und Unterstützungsanwendung .....                                                                   | 54    |
| E.6 Sicherheitsbezogenes Regelungssystem .....                                                                           | 57    |
| E.7 Backend-Prozess .....                                                                                                | 60    |
| E.8 Kritikalitätsbeurteilung für ein komplexes nicht reparierbares System mit zugewiesener Fehlerfrequenzanwendung ..... | 61    |
| E.9 Reparierbares System mit zugeordneter Zuverlässigkeitsanwendung .....                                                | 62    |
| Anhang F (informativ) Automobil-FMEA .....                                                                               | 63    |
| F.1 Allgemein .....                                                                                                      | 63    |
| F.2 Design und Prozess FMEA, DFMEA und PFMEA .....                                                                       | 64    |
| F.3 Anforderungen an das Management .....                                                                                | 64    |
| F.4 Analyse .....                                                                                                        | 65    |
| F.4.1 Vorbereitung für Analyse und Analyse .....                                                                         | 65    |
| F.4.1.1 Umreißen des Anwendungsbereiches der Analyse .....                                                               | 65    |
| F.4.1.2 FMEA-Kopf und Information in Spalten der Berichtstabelle .....                                                   | 65    |
| F.4.1.3 Risikobestimmung; Ursachen- und Auswirkungsanalyse .....                                                         | 65    |
| F.5 Beispiele einer Automobil-DFMEA .....                                                                                | 68    |

## Nationales Vorwort

Das internationale Dokument IEC 56/1579/CD:2014 „Failure Mode and Effects analysis (FMEA)“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom TC 56 „Dependability“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE ([www.dke.de](http://www.dke.de)) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnichtsnummer, 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.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

## Änderungen

Gegenüber DIN EN 60812:2006-11 wurden folgende Änderungen vorgenommen:

- a) Die Norm wurde umfassend überarbeitet;
- b) in der neuen Ausgabe wird dem Zuschnitt auf die jeweilige Aufgabenstellung und unterschiedlichen Anwendungswegen wie Top-Down und Bottom-up deutlich mehr Raum gegeben;

- c) die Aufteilung in allgemeinen Teil und Anhänge, die spezielle Anwendungsfälle sowie Beispiele aus der Praxis beinhalten, erleichtert die Übersicht und gibt geeignete Hilfestellungen für den Einstieg in diese Methode.

## Fehlzustandsart- und -auswirkungsanalyse (FMEA)

### Einleitung

Diese Internationale Norm beschreibt wie eine Ausfalleffektanalyse (FMEA), welche eine systematische Methode zur Bewertung einer Betrachtungseinheit oder eines Prozesses zur Identifizierung ihrer Ausfallmöglichkeiten darstellt, durchgeführt wird. Es wird beschrieben wie die Ursachen dieser Ausfälle, die Auswirkungen auf die Leistungsfähigkeit der Betrachtungseinheit oder des Prozesses und auf deren Umgebung und Personal analysiert werden. Der Begriff „Betrachtungseinheit“ bezeichnet dabei Hardware, Software, menschliche Handlungen und die untereinander wirkenden Einflüsse.

Eine FMEA wie in dieser internationalen Norm beschrieben ist eine Methode, die individuell anpassbar ist, um den Anforderungen einer Industrie oder Organisation zu genügen.

Die FMEA kann iterativ benutzt werden und auf diese Art für die Betrachtungseinheit oder den Prozess mehrfach überarbeitet werden; eine vorläufige Analyse kann während frühen Phasen von Entwurf und Planung durchgeführt werden; eine detailliertere Analyse kann erstellt werden sobald weitere Informationen verfügbar sind. FMEA sollte die Formulierung von geeigneten Handlungen unterstützen mit deren Hilfe mögliche Ausfälle abgewendet werden können. In der Anwendung mit Rückführung der tatsächlich festgestellten Auswirkungen als geschlossener Kreis erlaubt eine FMEA die Bewertung der Wirksamkeit von risikoeduzierenden Maßnahmen.

Eine FMEA kann auf verschiedene Ebenen einer Betrachtungseinheit oder eines Prozesses angewendet werden, von höchsten Hierarchieebenen bis hinunter auf die Ebene von Einzelfunktionen oder diskreten Bauteilen, Softwarebefehlen, Individuen, Prozessen oder spezifischen Prozeduren. Eine FMEA kann die Auswirkungen einer Ausfallart auf lokaler Ebene oder auf höheren Hierarchieebenen einer Betrachtungseinheit oder eines Prozesses berücksichtigen.

Eine FMEA kann durch die Durchführung einer Kritikalitätsanalyse, welche eine Bewertung der relativen Bedeutung eines speziellen Fehlzustandes zulässt, erweitert werden. Diese FMEA wird dann als FMECA Ausfalleffekt- und Kritizitätsanalyse, bezeichnet. Die Kritikalitätsanalyse beinhaltet eine Beurteilung der Wahrscheinlichkeit einer Ausfallart und der darauf bezogenen Ausfallschwere. Eine Kritikalitätsanalyse kann eine quantitative Beurteilung der Ausfallwahrscheinlichkeit und des mit dem Verlust der Funktion verknüpften Grades der Ausfallschwere oder der Schwere der Auswirkung darstellen. Diese internationale Norm benutzt den Begriff der FMEA auch als Synonym für eine FMECA.

Diese internationale Norm gibt Hilfestellung für die Planung, die Durchführung und die Dokumentation einer FMEA durch:

- a) Beschreibung der zugrundeliegenden Prinzipien
- b) Festlegung von geeigneten Begriffen und Annahmen
- c) Bereitstellung der Abläufe die für die Durchführung der Analyse notwendig sind
- d) Bereitstellung von Beispielen der notwendigen Arbeitsblätter, Tabellen oder Datenbankstrukturen die in der Analyse benutzt werden
- e) Definition von Anwendungen der FMEA

Eine FMEA kann für die Dokumentation in einer Sicherheitsanalyse oder für regulatorische Zwecke verwendet werden, aber da diese internationale Norm eine generische Norm darstellt spricht sie nicht speziell sicherheitstechnische Aspekte an.

Die primären Anwender dieser internationalen Norm sind Personen mit der Verantwortung für diese Analysen, für die Bereitstellung der Ergebnisse der FMEA und für das Führen des FMEA-Prozesses (der Analyst, der Moderator). In zweiter Linie wird diese Norm vom Analyseteam und Betroffenen (z. B. Management, Entwickler, Kunden und Behörden) verwendet.

## 1 Anwendungsbereich

Diese Internationale Norm beschreibt wie eine Ausfalleffektanalyse (FMEA) durchgeführt wird. Eine FMEA zielt darauf ab, zu bestimmen, wie Einheiten oder Prozesse ausfallen könnten, um geeignete Handlungen zu finden, die diese potenziellen Ausfälle verhindern können. Die FMEA stellt eine systematische Methode zur Identifikation aller Ausfallarten, in Verbindung mit ihren Ursachen und Auswirkungen auf Hardware, Software, menschliche Handlungen und die untereinander wirkenden Einflüsse, dar. Der Begriff „Betrachtungseinheit“ bezeichnet dabei Hardware, Software, menschliche Handlungen und die untereinander wirkenden Einflüsse.

Um die Priorisierung von Ausfallarten zu unterstützen kann zusätzlich eine Kritikalitätsanalyse durchgeführt werden. Diese FMEA wird dann als FMECA Ausfalleffekt- und Kritizitätsanalyse, bezeichnet. Diese internationale Norm erklärt wie FMEA und deren Variante FMECA geplant, durchgeführt, dokumentiert und gepflegt werden können. Eine FMEA kann zur Dokumentation einer Sicherheitsanalyse für regulatorische und andere Zwecke verwendet werden, da dies aber eine generische Norm darstellt werden hier keine Festlegungen für diese Belange getroffen.

## 2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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).

## 3 Begriffe und Abkürzungen

### 3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 60050-192 und die folgenden Begriffe.

#### 3.1.1

**Kritikalität**<sup>NA1)</sup> (eines Fehlers oder Ausfalles)

Schwere der Auswirkung hinsichtlich der festgelegten Bewertungskriterien

Anmerkung 1 zum Begriff: Die Bewertungskriterien der Kritikalität umfassen üblicherweise die Auswirkungen der Fehlzustände oder der Ausfälle auf die Einheit selber, auf das System, in dem die Einheit ein Bestandteil ist, sowie auf die Einheiten außerhalb der Systemgrenzen.

Anmerkung 2 zum Begriff: Zur Kritikalitätsanalyse siehe Ausfalleffekt- und Kritizitätsanalyse (192-11-06).

[QUELLE: 192-03-09]

#### 3.1.2

**Ausfallursache**

Menge von Umständen, die zu einem Ausfall führt

[QUELLE: 191-03-11]

#### 3.1.3

**Ausfallauswirkung**

Konsequenz eines Ausfalls, innerhalb oder außerhalb der Grenzen der ausgefallenen Einheit

Anmerkung 1 zum Begriff: Bei einigen Analysen kann es erforderlich werden, einzelne Ausfallarten und deren Auswirkungen zu betrachten.

[QUELLE: 192-03-08]

---

<sup>NA1)</sup> Nationale Fußnote: Kritikalität wird in DIN 60812:2006 auch als Kritizität, in DIN 25448 als Ausfallbedeutung bezeichnet; englisch: criticality.

#### 3.1.4

##### **Ausfallart**

Art und Weise, wie sich ein Ausfall ereignet

Anmerkung 1 zum Begriff: Eine Ausfallart kann durch die verlorene Funktion oder durch den eingetretenen Zustandsübergang definiert werden.

[QUELLE: 192-03-17]

#### 3.1.5

##### **menschliches Fehlverhalten**

Diskrepanz zwischen der von einem Menschen ausgeführten oder unterlassenen Aktion und der beabsichtigten oder erforderlichen Aktion

BEISPIEL: Eine fehlerhafte Aktion ausführen, eine erforderliche Aktion unterlassen; Fehlberechnung; falsche Interpretation eines Wertes

[QUELLE: 192-03-14]

#### 3.1.6

##### **Wahrscheinlichkeit**

Maß wie wahrscheinlich ein Ereignis auftritt

Anmerkung 1 zum Begriff: In diesem Dokument wird der Begriff nie auf eine statistische Wahrscheinlichkeit bezogen.

Anmerkung 2 zum Begriff: Wahrscheinlichkeit kann eine Rate oder eine Wahrscheinlichkeit darstellen.

[QUELLE: 192-043-14<sup>NA2</sup>]

#### 3.1.7

##### **Redundanz (in einem System)**

Vorhandensein von mehr als einem Mittel zur Ausführung einer Funktion

#### 3.1.8

##### **Szenario**

spezifizierte äußere Bedingungen in denen die Einheits- oder Prozessfunktionen durchgeführt werden.

Anmerkung 1 zum Begriff: Äußere Bedingungen umfassen alle Faktoren außerhalb der betrachteten definierten Einheit oder der Prozessgrenzen, welche Auswirkungen auf das Verhalten der Betrachtungseinheit oder den Prozess haben können.

Anmerkung 2 zum Begriff: Physikalische Bedingungen umfassen alle Umweltfaktoren wie Temperatur, Feuchtigkeit, Beleuchtung, Schlag, Verschmutzung, Strahlung.

#### 3.1.9

##### **Prüfbarkeit**

Grad, zu dem eine Einheit geprüft werden kann

[QUELLE: 192-09-20]

### 3.2 Abkürzungen

In diesem Dokument werden folgende Abkürzungen verwendet.

|      |                                                                         |
|------|-------------------------------------------------------------------------|
| CCF  | Ausfall aufgrund gemeinsamer Ursache (en: Common Cause Failure)         |
| COTS | standardisiertes gekauftes System (en: Commercial Off The Shelf System) |
| ETA  | Ereignisbaum-Analyse (en: Event Tree Analysis)                          |
| FMEA | Ausfalleffektanalyse (en: Failure Modes and Effects Analysis)           |

---

<sup>NA2</sup> Nationale Fußnote: Der Begriff Wahrscheinlichkeit, im englischen Original likelihood, existiert im IEV-Teil 192 nicht.

|       |                                                                                              |
|-------|----------------------------------------------------------------------------------------------|
| FMECA | Ausfalleffekt- und Kritizitätsanalyse                                                        |
| FMEDA | Ausfalleffekt- und Diagnoseanalyse                                                           |
| FTA   | Fehlerbaum-Analyse (en: Fault Tree Analysis)                                                 |
| ILS   | Umfassende logistische Unterstützung (en: Integrated Logistic Support)                       |
| LORA  | (Level of Repair Analysis)                                                                   |
| MTBF  | mittlere Zeit zwischen Ausfällen (en: Mean Time Between Failure)                             |
| MTTR  | mittlere Zeit zur Wiederherstellung (en: Mean Time To Repair)                                |
| LCC   | Kosten innerhalb des Lebenszyklus (en: Life Cycle Cost)                                      |
| OEM   | Fremdprodukthersteller (en: Original Equipment Manufacturer)                                 |
| PFMEA | Prozessausfalleffektanalyse                                                                  |
| RBD   | Zuverlässigkeitsblockdiagramm (en: Reliability Block Diagram)                                |
| RCM   | Zuverlässigkeitsgetriebene Instandhaltung (en: Reliability Centered Maintenance)             |
| RPZ   | Risikoprioritätszahl (en: RPN – Risk Priority Number)                                        |
| SOD   | Schwere, Auftrittshäufigkeit und Aufdeckbarkeit (en: Severity, Occurrence and Detectability) |

## 4 Überblick

Dieser Abschnitt beschreibt die Gründe für die Durchführung einer FMEA, den Zweck und die Grenzen einer FMEA, die Begrifflichkeit, die Rollen verschiedener Personen bei der Analyse und das Verhältnis von FMEA zu anderen Zuverlässigkeitsanalysen.

### 4.1 Ziele der FMEA

Zweck der Durchführung einer FMEA für eine Einheit oder einen Prozess von Interesse ist es, alle potenziellen Ausfallarten und deren Ursachen und Auswirkungen zu identifizieren damit Ursachen analysiert und unerwünschte Auswirkungen reduziert werden können. Der Zweck der FMECA ist, danach die Kritikalität der Ausfallart zu beurteilen um Prioritäten für Handlungen festzulegen.

Die Gründe für die Durchführung eines FMEA umfassen:

- Kosteneffizientes Verbessern des Designs einer Einheit oder eines Prozesses durch Beeinflussung zu einem frühen Zeitpunkt im Entwicklungsprogramm;
- Identifizieren von Risiken dass eine Einheit oder ein Prozess definierte Anforderungen nicht erfüllen kann (Sicherheitstechnik, IT-Sicherheit, Leistungsfähigkeit, Kosten, usw.) und Etablieren von Handlungen für diese Risiken um die Zuverlässigkeit der Einheit oder des Prozesses zu verbessern [ISO 55000];
- Verringern von Betriebskosten für Einheiten oder Prozessanwendung durch Benutzung des Verständnisses für Ausfallarten, deren Auftrittsrate und den Auswirkungen, um Instandhaltung, Hilfestellung und andere Handlungen zu planen und zu priorisieren;
- Bereitstellen eines Kernprozesses innerhalb eines mit ISO 55000 konformen Asset-Management-Systems, das einen nachweisbaren Zusammenhang zwischen Funktion, Einheits- oder Prozessverhalten und dem geschaffenen oder verlorenen Wert aufweist, was ein grundlegendes Merkmal eines Asset-Management-Systems darstellt;
- Erfüllen von gesetzlichen oder geschäftlichen Verpflichtungen durch Aufbau von Rückverfolgbarkeit und Nachweis dass Risiken beherrscht und akzeptiert wurden;
- Bereitstellen der Grundlage für andere Analysen.

### 4.2 Terminologie

Zur Vereinfachung wird in dieser internationalen Norm der Begriff „Ausfalleffektanalyse“, durch FMEA abgekürzt und benutzt als allgemeiner Ausdruck für jede Anwendung und jeden Anpassungsgrad der Analyse.

#### 4.2.1 Abstufung der Einheiten oder Prozesse

Tabelle 1 bietet Beispiele für Ausdrücke, die üblicherweise mit den Hierarchieebenen für Einheiten oder Prozesse assoziiert werden.

**Tabelle 1 – Ausdrücke für Hierarchieebenen**

|          | Höchste Ebene         | Mittlere Ebene | Unterste Ebene           |
|----------|-----------------------|----------------|--------------------------|
| Hardware | System                | Modul          | Bauteil                  |
| Software | Freigegebene Software | Modul          | Ausführbare Codefunktion |
| Prozess  | Prozedur              | Aufgabe        | Schritte                 |

ANMERKUNG Die Ausdrücke in Tabelle 1 sind nicht eindeutig trennbar. Zum Beispiel kann Software in ein Hardware-system eingebunden sein, oder ein System kann menschliche Aspekte miteinbeziehen.

Um Klarheit bei der Benutzung dieser Hierarchieebenen von Einheiten oder Prozessen zu bieten werden diese Festlegungen getroffen:

f) Hardware oder Software

- wo die Ebene keine Rolle spielt (z. B. wo es keine Hierarchie gibt), dann wird der Begriff „Einheit“ benutzt.
- wo Hierarchie eine wichtige Rolle spielt, werden die Begriffe „höchste Ebene“, „mittlere Ebene“, „unterste Ebene“ benutzt.

g) Prozess

- wo die Ebene keine Rolle spielt (z. B. wo es keine Hierarchie gibt), dann wird der Begriff „Prozess“ benutzt.
- wo Hierarchie eine wichtige Rolle spielt werden die Begriffe „höchste Ebene“, „mittlere Ebene“, „unterste Ebene“ benutzt.

ANMERKUNG die Benutzung von mittlerer Ebene erlaubt die Existenz vieler Ebenen zwischen höchster und niedrigster Ebene.

#### 4.2.2 Rollen innerhalb einer FMEA

Eine FMEA benötigt Personen in verschiedenen Rollen innerhalb der Analyse. In dieser internationalen Norm werden die Folgenden Ausdrücke gebraucht um die Schlüsselpersonen innerhalb der FMEA zu beschreiben.

a) Moderator

- der Moderator sorgt dafür dass die Methodik eingehalten wird und leitet das Analyseteam an. Der Moderator muss Experte in FMEA sein und, wenn möglich, ein Verständnis für das technische Gebiet haben. Die Funktion kann von einem internen oder einem externen Spezialisten übernommen werden.

b) Analysten

- das Analyseteam besteht aus Analysten die die FMEA ausführen und an den Besprechungen zum FMEA teilnehmen. Das Team von Analysten sollte innerhalb der Gruppe relevante Kenntnisse aufweisen um alle relevanten Aspekte der Einheit oder des Prozesses abzudecken.

ANMERKUNG Andere qualifizierte Personen können Daten und Information über die Einheit oder den Prozess bereitstellen die von den Analysten für die FMEA benutzt werden. Solche Personen sind üblicherweise nicht bei jeder Teambesprechung anwesend.

c) Management

- das Management hat die Verantwortung dafür, das Problem zu definieren, den Zweck der FMEA festzulegen und die Nutzung von Hilfsmitteln zu autorisieren, die das Zuschneiden des FMEA-Pro-

zesses auf die Aufgabe unterstützen wie es vom Moderator empfohlen wird. Diese Rolle kann vom Projektleiter oder demjenigen übernommen werden der die Verantwortung für die endgültige Autorisierung der Entwicklung hat.

- d) andere Interessenvertreter
  - Interessenvertreter können Kunden (z. B. Vertragseigner), Behörden (z. B. Gesetzgeber) und Anwender (z. B. Hersteller oder Instandhaltungsfirmen) sein.

#### 4.2.3 Wahrscheinlichkeit eines Fehlzustandes

Im Bezug auf Auftreten eines Fehlzustandes wird der allgemeine Begriff „Wahrscheinlichkeit“ benutzt wo eine allgemeine Bedeutung benötigt wird. Wo ein spezifischer Begriff wie „statistische Wahrscheinlichkeit“, „Frequenz“, „Ausfallrate“, „Nichtverfügbarkeitsfunktion“ benötigt wird dann wird der spezifische Begriff benutzt.

#### 4.2.4 Kritikalität

Der Begriff „Kritikalität“ wird als allgemeiner Ausdruck für eine Einstufungsmethode verwendet. Wo Begriffe wie „Risikomatrix“ oder „RPZ“ benutzt werden, wird diese spezifische Methode besprochen.

### 4.3 Beziehung von FMEA zu anderen Zuverlässigkeitsanalysemethoden

Die Effektivität einer FMEA kann durch Kombination mit anderen Analysemethoden erhöht werden. Zum Beispiel:

- kann ein Zuverlässigkeitsblockdiagramm (RBD) oder Funktionsblockdiagramm des Systems nützlich sein um den Rahmen der FMEA zu definieren und die Entwicklung der FMEA zu unterstützen. Die Ergebnisse der FMEA können nacheinander benutzt werden um das RBD / Funktionsblockdiagramm zu überarbeiten.
- kann eine Fehlerbaumanalyse (FTA) mit einem geeigneten Ereignis auf höchster Ebene benutzt werden um die wesentlichen Teile eines komplexen Systems zu finden, die auf ihre Ausfallarten analysiert werden.
- kann, um die FMEA, die üblicherweise nur unabhängige Ausfälle betrachtet, zu ergänzen, eine detailliertere FTA benutzt werden die auch Abhängigkeiten und Redundanzen analysiert. Das Ergebnis der FMEA kann Ereignisse identifizieren die zum Ereignis auf höchster Ebene der FTA beitragen und diese Ereignisse sollten als grundlegende Ereignisse der FTA benutzt werden.
- können um schrittweise eine FMEA für ein komplexes System im Entwicklungsprozess zu entwickeln andere Zuverlässigkeitsanalysen mit der FMEA kombiniert werden. Ein FMEA auf höchster Systemebene kann beim Konzeptdesign erstellt werden in Verbindung mit RBD und FTA. Eine FMEA auf mittlerer Ebene für Module kann erstellt werden, wenn das System im Detail entwickelt wird. Eine FMEA auf niedrigster Ebene sollte ausgewählte hoch kritische Bauteile mit einbeziehen wie z. B. sicherheitskritische Bauteile, Redundanzen usw. Analysemethoden wie FTA, ETA, Markovanalyse und Petri Netze können benutzt werden um Abhängigkeit von Ausfallereignissen sowie die Reihenfolge ihres Auftretens, bedingte Wahrscheinlichkeit eines Auftretens, Redundanz, Ausschließlichkeit usw. Ausfallratenanalysen können benutzt werden um die Bezifferung der Auftretenswahrscheinlichkeit in der FMEA zu unterstützen.

ANMERKUNG Der Bezug auf andere Zuverlässigkeitsanalysenormen sind wie folgt: RBD [IEC 61078]; FTA [IEC 61025]; ETA [IEC 62505]; Markovanalyse [IEC 61165]; Petri Nets [IEC 62551]; Ausfallratenanalyse [IEC 62308].

Die Ergebnisse der FMEA geben Auskunft über kritische Aspekte eines komplexen Systemdesigns und können am Ende des Entwicklungsprozesses benutzt werden als Grundlage für:

- geplante Instandhaltungsanalyse
- Fehlerbeseitigung während der Wartung,
- Quantitative Prüfbarkeitsanalyse,
- Analyse der Prüfergebnisse,
- Analyse der logistischen Unterstützung,

- Zuverlässigkeitsanalyse,
- Verfügbarkeitsanalyse,
- Bewertung der Auswirkung von Designänderungen und
- Dokumentation zu gesetzlichen Zwecken (z. B. Sicherheit oder Typprüfung)

#### 4.4 Struktur des Dokumentes

Abschnitt 5 beschreibt die allgemeine Methodik für FMEA. Ein Flussdiagramm bietet einen Überblick über die nötigen Aktivitäten und zeigt die einzelnen Schritte die während der Planung, bei Durchführung und zur Dokumentation eines FMEA nötig sind. Anhang A bietet detaillierte Hinweise wie eine FMEA auf spezielle Anwendungen zugeschnitten wird. Anhang B bietet Beispiele zu Inhalten von typischen FMEA Reports. Anhang C beschreibt allgemeine Methoden zur Beurteilung der Kritikalität. Anhang D bietet Beispiele dafür wie die generelle FMEA-Methode für spezielle Zwecke verwendet werden kann (z. B. Software, Sicherheitstechnik, zuverlässigkeitsgetriebene Instandhaltung, Prozesse, komplexe Systeme, Nichtverfügbarkeit). Anhang E zeigt Beispiele von FMEA-Berichten für verschiedene Anwendungen (z. B. Software, Design, Einheitsfunktion, Instandhaltung und Hilfestellung). Anhang F bietet Hilfestellung für FMEA im Automobilbereich. Alle Anhänge sind informativ.

### 5 Methodik für FMEA

#### 5.1 Allgemein

Bild 1 ist ein Flussdiagramm der allgemeinen Aktivitäten die als Teil einer FMEA unternommen werden und unterscheidet zwischen Planungs-, Durchführungs- und Berichtsphase. Die Absätze in diesem Abschnitt beschreiben die Aktivitäten innerhalb jeder Phase. Allgemein entspricht die Reihenfolge in welcher die Aktivitäten präsentiert werden mit der Reihenfolge in der sie durchgeführt werden sollten. Anhang A bietet Hilfestellung zu Wegen wie der allgemeine Prozess der FMEA vom Analysten zugeschnitten werden kann um die Ziele für einen speziellen Anwendungsfall von FMEA zu erreichen.

ANMERKUNG 1 Innerhalb der Planungsphase stellt Bild 1 die Aktivitäten in ihrer Reihenfolge dar, während in der Realität die Aktivitäten auch iterativ durchgeführt werden können da die Vorbereitung für die Analyse angelegt ist um die Ziele zu erreichen.

ANMERKUNG 2 In der Durchführungsphase können die Aktivitäten auf verschiedene Weise implementiert werden wenn die betrachtete Einheit oder der betrachtete Prozess für die Analyse auf verschiedene Elemente heruntergebrochen wird. Zum Beispiel könnten alle angegebenen Aktivitäten für jede Einheit oder jeden Prozess nacheinander ausgeführt werden oder jede angegebene Aktivität wird könnte für alle Einheiten oder Prozesse komplettiert bevor die nächste Aktivität durchgeführt wird, oder eine beliebige Kombination dieser Methodik.

ANMERKUNG 3 Die Berichtsphase beinhaltet alle Aktivitäten die mit der Erstellung der Dokumentation einer FMEA zu tun haben, aber das Verstehen der Anforderungen an die Dokumentation und das Sammeln von Information für die Dokumentation sollte in Planungs- und Durchführungsphase beginnen.

Es ist üblich, Aktivitäten und Phasen der FMEA-Methode zu wiederholen wo die Analyse als Teil eines Entwicklungsprozesses durchgeführt wird oder wo die betrachteten Einheiten oder Prozesse verändert werden.

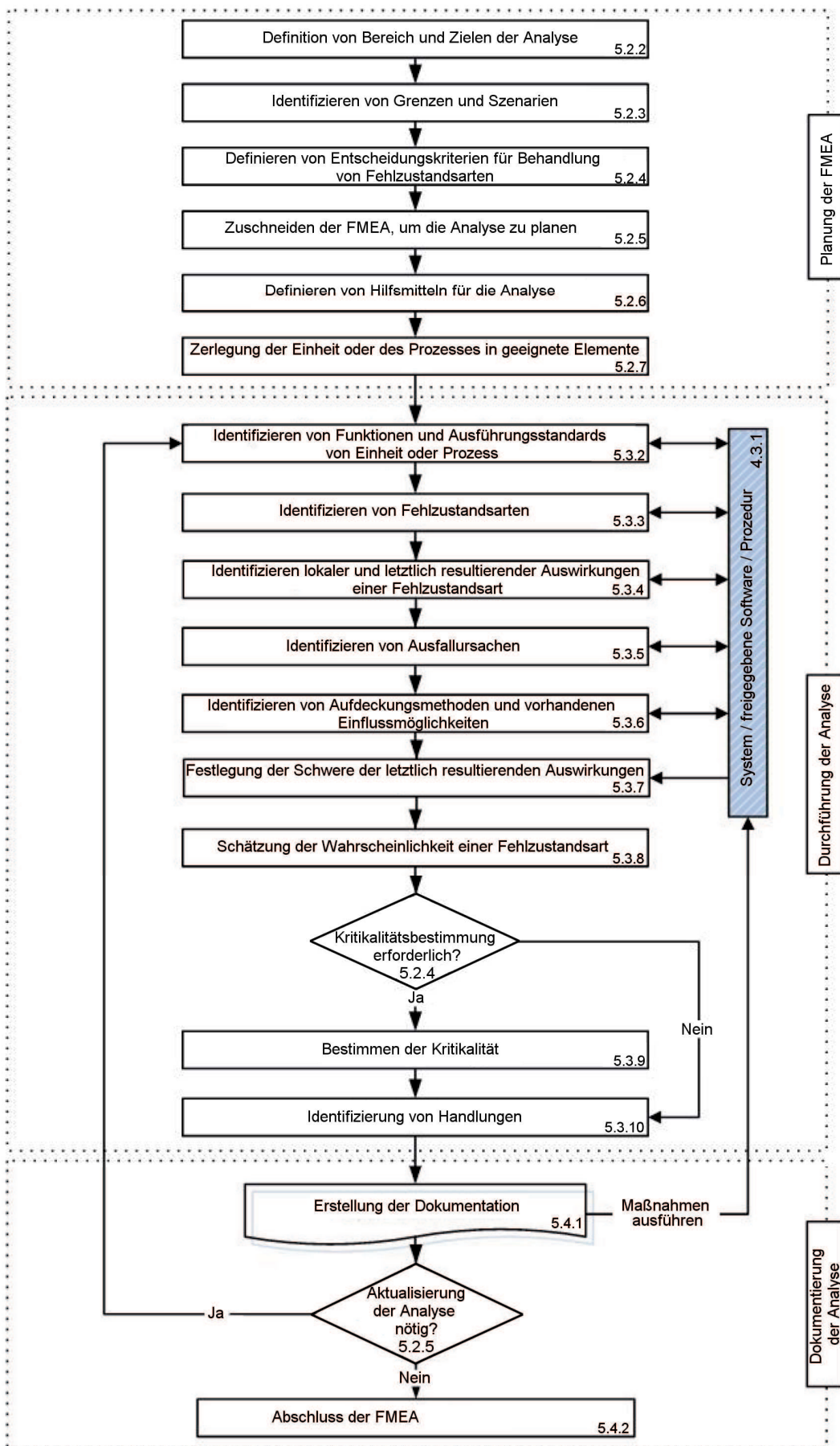


Bild 1 – Flussdiagramm der FMEA-Methode

## 5.2 Planung des FMEA

### 5.2.1 Allgemein

Die Planung des FMEA beinhaltet die Überlegung warum eine Analyse durchgeführt wird, welche Einheit oder welcher Prozess unter welchen Bedingungen analysiert werden muss und wie die Analyse möglichst effizient und effektiv durchgeführt werden kann.

Das Resultat der Planungsphase ist ein FMEA-Plan der:

- die Gründe auflistet, die Bereiche, die Analysegrenzen und die Einsatzbedingungen beschreibt;
- einen Satz von Handlungen und damit verbundene Aufgaben beschreibt aus dem die Durchführung eines FMEA auf eine spezielle Einheit (Hardware, Software oder Prozess) besteht und
- identifiziert wie Hilfsmittel den Handlungen in der FMEA zugeordnet werden.

Der FMEA-Plan kann eigenständig oder Teil eines Planes auf höherer Ebene sein wie z. B. ein Projektplan oder ein System Engineering Management Plan. Er sollte eine zugeschnittene, kosteneffiziente Anwendung des FMEA-Prozesses für eine bestimmte Anwendung darstellen. Das Zuschneiden ist ein wesentlicher Schritt um die Grenzen der Analyse festzulegen sowie einen detaillierten Satz von Handlungen oder unterstützenden Handlungen zu bestimmen, der für eine spezielle Anwendung benutzt wird.

### 5.2.2 Bestimmen des Umfangs und der Zielsetzung der Analyse

Die Bestimmung des Umfangs legt die Grundlage für den Analyseaufwand fest und untersucht die Größe, die Form und die Richtung dieses Aufwandes.

Das Resultat dieser Aktivität ist ein Dokument zum Geltungsbereich das den anfänglichen FMEA-Plan darstellt und sollte das Folgende umfassen:

- Zweckangabe, die den Grund für die Analyse bestimmt. Zum Beispiel um die Stabilität eines Designkonzeptes zu untersuchen, um Mittel zur Verbesserung eines Prozesses oder einer Prozedur zur Verringerung von Ausfällen zu finden, um Risiken zu identifizieren, um eine vertragliche Anforderung zu erfüllen, um Möglichkeiten für die Verbesserung der Zuverlässigkeit zu identifizieren, um Anforderungen für Instandhaltungs- und Unterstützungsprogramme usw. vorzuschlagen.
- Zielangabe, die die nötigen Resultate der FMEA definiert, in einer Form die es erlaubt den Erfolg der Analyse zu beurteilen. Dies kann zu einem Report wie in den Beispielen unter Anhang B und E dargestellt führen.
- Eine grobe Beschreibung der Einheit oder des Prozesses der analysiert werden soll, inklusive aller Schnittstellen zu anderen damit verbundenen Einheiten oder Prozessen. Diese Beschreibung sollte während des Planungsprozesses erweitert werden und kann Darstellungen wie Flussdiagramme oder Funktionsblockdiagramme beinhalten.
- Strategische Zuschnittanweisung, in welcher das Management die Faktoren die den Ansatz zur Analyse beeinflussen festlegt und die zum Beispiel die Notwendigkeit eines Konsens zwischen den vom Resultat betroffenen Parteien, die zeitliche Notwendigkeit von Analyseresultaten und Schnittstellen mit Meilensteinen eines Projektes, vorhandene Ressourcen, vorhandene Erfahrungen, verfügbare Information und die Ebene auf die die Analyse heruntergebrochen werden soll umfasst.

ANMERKUNG 1 Die strategische Zuschnittanweisung hat Vorrang vor technischen Zuschnittanweisungen in denen der Moderator die Methoden die in der Analyse angewendet werden sollen definiert, der Form eines resultierenden Reports, vor den Entscheidungskriterien die auf die Analyseresultate angewendet werden um die Empfehlungen zur Handlung festzulegen sowie jeder Einschränkung der potenziell verfügbaren Vermeidungshandlungen und der Begründung dieser Auswahl.

ANMERKUNG 2 Anhang A bietet Hilfestellung zum Zuschnitt der Analyse.

Das Zuschneiden hat den Zweck, auf Expertise der Organisation in strukturierter Weise zuzugreifen und die Entscheidungen und Resultate in einem formalen Zuschnittsdocument festzuschreiben. Ein vom Moderator geleitetes Seminar kann die relevanten Interessenvertreter zusammenbringen um die Bestimmung des Umfangs durchzuführen. Dieses Seminar kann virtuell oder in direktem Kontakt durchgeführt werden. Das

Seminar kann in größeren Projekten unabhängig von der Analyse oder in kleineren, in sich abgeschlossenen Analysen als erste Aktivität durchgeführt werden.

### 5.2.3 Ermitteln von Grenzen und Bedingungen

#### 5.2.3.1 Allgemein

Es ist notwendig, die Grenzen und Umgebungsbedingungen der analysierten Einheit oder des analysierten Prozesses klar festzulegen um zu erreichen dass der Umfang der Analyse von Anwendern und den Analysen verstanden wird.

Die erforderliche Information umfasst üblicherweise:

- die detaillierte physikalische und/oder funktionelle Struktur der Einheit, oder für einen Prozess der Handlungsfluss;
- die Eigenschaften, Leistungswerte, Rollen und Funktionen auf jeder Hierarchieebene;
- Eingaben und Ausgaben der Einheit oder des Prozesses;
- der Beschaffenheit der Redundanzen wo vorhanden;
- die Schnittstellen mit anderen verbundenen Einheiten oder Prozessen;
- die Umgebung in welcher die Einheit betrieben oder der Prozess unternommen wird;
- jede Änderung in der für andere Betriebsmodi nötigen Struktur der Einheit;
- organisatorische Ziele der Analyse.

#### 5.2.3.2 Festlegung von Grenzen für Einheit oder Prozess

Die Einheit oder der Prozess sollte in Bezug auf ihre Beziehungen, Abhängigkeiten und Verbindungen mit anderen Einheiten, Hilfseinheiten und Bedienerschnittstellen skizziert werden. Dies soll sicherstellen dass die Grenzen der Studie klar verstanden werden und dass wichtige Aspekte nicht aufgrund ungeeigneter Annahmen in Bezug auf den Umfang der Analyse übersehen werden.

Die Grenzen der Einheit stellen die physikalische Schnittstelle zwischen der Einheit und ihrer Umgebung dar, inklusive aller Einheiten mit denen sie interagiert. Die Grenzen der Einheit hängen vom Kontext ab und können von Faktoren wie Design oder vorgesehener Verwendung abhängen. Es kann nötig sein, Einheiten ausdrücklich außerhalb der Grenzen zu platzieren um die Größe der FMEA zu reduzieren oder weil detaillierte Kenntnisse nicht vorhanden sind (z. B. COTS).

Wo möglich sollten Grenzen definiert werden um die FMEA und ihre Integration mit anderen darauf bezogenen Studien zu erleichtern. In manchen Fällen kann es sinnvoll sein, die Grenzen aus funktionaler Sichtweise festzulegen um die Anzahl von Abhängigkeiten zu anderen Einheiten außerhalb der Analyse zu begrenzen. Das ist oft der Fall wenn die Einheit komplexe Funktionalität besitzt, mit vielfältigen Schnittstellen innerhalb der Grenzen oder nach außen.

#### 5.2.3.3 Festlegung von Betriebsbedingungen für Einheit oder Prozess

Wenn eine Analyse erstellt wird geschieht dies immer im Kontext von einem oder mehreren Szenarien für die die Ausfalleigenschaften beurteilt werden. Szenarien sollten mit Ausdrücken beschrieben werden die geeignet für die Einheit oder den Prozess sind.

**ANMERKUNG** Beispiele für Szenarien sind: „normale Operation“ oder „Speicherung“ wenn Hardware analysiert wird; oder „Nachtschicht“ oder „Notfallreaktion“ wenn ein Prozess analysiert wird.

Die Ziele der Analyse geben die Szenarien die von Interesse sind vor. Die Szenarien sollten in Bezug auf ihre Zustände und ihre Eigenschaften definiert werden, was jeden bekannten externen Faktor beinhaltet der das Ausfallverhalten der betrachteten Einheit oder des betrachteten Prozesses beeinflusst. Dies stellt sicher dass die Analyse alle Faktoren komplett umfasst die entweder Ausfälle oder Auswirkung der Ausfälle beeinflussen.

Die Festlegung der Szenarien wird normalerweise zumindest die physikalischen Umgebungsbedingungen beinhalten, außer wenn entweder über vorherige Erfahrungen oder mittels Prüfungen klar nachgewiesen werden kann dass die betrachtete Einheit oder der betrachtete Prozess nicht von diesen beeinflusst wird. Die physikalische Umgebung sollte Umweltbedingungen sowie Bedingungen anderer Aktivitäten in der Umgebung berücksichtigen da diese das Verhalten der betrachteten Einheit oder des Prozesses beeinflussen. Andere Bedingungen können Grenzen des Unternehmens wie Hierarchieebenen des Personals und physischen oder psychologischen Stress umfassen, die Auswirkungen auf einen Prozess haben können.

#### 5.2.4 Definieren von Entscheidungskriterien für die Behandlung von Ausfallarten

Die Kriterien zur Erkennung welche Ausfallarten zu Handlungen führen müssen um potenzielle Behandlung zu untersuchen, sollten vor der Durchführung der Analyse bestimmt werden. Diese Kriterien sollten die Ziele der Analyse im Bezug auf Anforderungen von Betroffenen zur Eliminierung oder Verringerung von Schäden, die sich aus den identifizierten Ausfällen ergeben, berücksichtigen.

**ANMERKUNG** In diesem Zusammenhang kann sich der Begriff „Schaden“ auf ökonomische Auswirkungen beziehen, aber auch auf immaterielle Auswirkungen wie den Verlust der geschäftlichen Reputation oder physischer oder psychologischen Schaden an Menschen.

Die Kriterien sollten eine objektive Auswahl von Ausfallarten ermöglichen, die Behandlung benötigen und solche, die sie nicht benötigen. Die Entscheidung wird üblicherweise die Schwere der Ausfallauswirkung auf Ziele und Funktion von Einheit oder Prozess berücksichtigen. Eine Methode der Auswahl ist die Anwendung einer Kritikalitätsmethode.

Details der Entscheidungskriterien sollten in den FMEA-Bericht einbezogen werden und sollten klar autorisiert werden.

##### 5.2.4.1 Identifizieren der Notwendigkeit zur Evaluierung der Kritikalität einer Ausfallart

Die Kritikalitätsanalyse ist eine Methode mit deren Hilfe, basierend auf mehreren Kriterien, jeder Ausfallart der Grad ihrer Wichtigkeit zugeordnet wird. Eine Kritikalitätsanalyse ist da nötig wo mehrere Kriterien benötigt werden um die Wichtigkeit von Ausfallarten zu gewichten oder um die Notwendigkeit der Berücksichtigung festzulegen. Diese Kriterien können umfassen:

- die Schwere der Ausfallauswirkung auf Ziele und Funktion von Einheit oder Prozess;
- die Wahrscheinlichkeit dass die Auswirkung eintritt;
- die Wahrscheinlichkeit dass die Ausfallart auftritt;
- die Möglichkeit den Ausfall zu entdecken bevor unerwünschte Auswirkungen auftreten.

Kritikalitätsanalyse muss nicht notwendig sein wenn alle identifizierten Ausfallarten Behandlung benötigen oder wenn zu wenig Information vorhanden ist um eine vernünftige Abschätzung der Kritikalitätsparameter zu erlauben. Eine Kritikalitätsanalyse kann für manche Anwendungen auch kostspielig sein oder nötig aufgrund vertraglichen oder gesetzlichen Anforderungen.

**ANMERKUNG** Anhang C beschreibt zwei übliche Methoden für Kritikalitätsanalysen.

#### 5.2.5 Zuschneiden der FMEA um die Analyse zu planen

Um kosteneffektiv zu sein, muss der FMEA-Prozess auf Beschaffenheit und Nutzungsbedingungen von Einheit oder Prozess sowie das organisatorische Umfeld in welchem die Analyse durchgeführt wird zugeschnitten sein. Die Auswahl des Zuschnitts hängt von einigen oder allen nachfolgend angegebenen Bedingungen ab die in zuvor ausgeführten Phasen der Planung identifiziert und diskutiert sein müssen wie auch in Abschnitten 5.2.2 und 5.2.3 beschrieben.

Der technische Zuschnitt der Analyse sollte die folgenden Punkte berücksichtigen:

- a) Die Ebene in der Hierarchie der Einheit oder des Prozesses auf dem die Analyse durchgeführt wird;
  - generell kann eine Einheit oder ein Prozess in eine hierarchische Struktur zerlegt werden, von einen Funktionsblockdiagramm der Einheit oder dem Flussdiagramm eines Prozesses auf der obersten

Ebene der Hierarchie bis hinunter auf Bauteile oder Prozessschritte auf der detailliertesten oder elementaren Ebene;

- die Methode der FMEA kann auf jede Hierarchieebene zwischen diesen beiden Extremen auf eine Einheit oder einen Prozess und oft auf mehrere Detaillierungsebenen angewendet werden.
- b) Ob ein „Top-down“- oder „Bottom-up“-Ansatz gewählt wird:
- die FMEA kann einem „Top-down“-Ansatz folgen der zuerst die Ziele und die Funktion der Analyse im Ganzen betrachtet und dann die dafür nötigen Beiträge untersucht;
  - alternativ kann eine „Bottom-up“-Methode angewendet werden wo Untereinheiten oder Unterprozesse auf der größten Detaillierungsebene untersucht werden um zu identifizieren wie diese ausfallen; von dort aus werden die Auswirkungen die diese Ausfälle auf höhere Ebenen der Einheit oder des Prozesses haben können abgeleitet.
- c) Der Detaillierungsgrad der FMEA:
- der geeignete Detaillierungsgrad für die Analyse hängt von Kontext und gewünschten Resultaten ab;
  - generell bietet eine größere Detailtiefe in der Hierarchieebene eine gleichwertige Detailtiefe bei Ausfallursachen und detailliertere Behandlungsstrategien, aber die Durchführung ist zeitaufwändiger;
  - eine höhere Komplexität in der Bewertung von Ausfallarten bietet mehr Information zur Priorisierung von Handlungen, ist aber komplexer und zeitaufwändiger.
- d) Die Form der Dokumentation für die Berichte:
- die im Lauf der FMEA generierte Dokumentation sollte konform zu Festlegungen innerhalb der Organisation sein und ist in den meisten Fällen eine Kombination von Datenbanken, softwarespezifischen Dokumenten und Papierberichten. Die Mittel mit denen die Rückverfolgbarkeit über diese einzelnen Medien erhalten wird sollten festgelegt werden;
  - jede Anzahl von Berichtsformaten für die FMEA ist möglich und das gewählte Format wird oft die betrachtete Information, die gemachte Beurteilung und den verfolgten Beweisprozess bestimmen;
  - da das Sammeln von Information, die Speicherung, das Halten und der Zugriff Kosten verursachen muss beachtet werden dass der Wert der Analyse gewährleistet bleibt.

ANMERKUNG Abschnitt 5.4 bietet weitere Details darüber welche Dokumentation benötigt wird.

Anhang B bietet Beispiele für Inhalte von typischen FMEA-Berichten und Anhang E zeigt Beispiele für den Stil von FMEA-Berichten für verschiedene Anwendungen. Anhang A stellt weitere Hinweise zum Zuschnitt von FMEA zur Verfügung.

#### 5.2.5.1 Bestimmen des Anwendungsbereiches und Ansatz der Analyse

Der Anwendungsbereich der Analyse sollte gewählt werden durch Definition der Breite (z. B. wie viel der Einheit oder des Prozesses und seiner Umgebung einbezogen wird) und der Tiefe (z. B. wie viele Ebenen die Analyse beinhaltet in Bezug auf den Detaillierungsgrad auf den Einheit oder Prozesses heruntergebrochen werden). Der gewählte Ansatz ist entweder „Bottom-up“ oder „Top-down“. Für eine „Bottom-up“-Analyse sollte die Analyse auf der untersten Ebene anfangen. Für eine „Top-down“-Analyse sollten die Ereignisse auf oberster Ebene identifiziert werden, daraufhin sollten die Elemente bestimmt werden die diese übergeordneten Ereignisse beeinflussen könnten. Für jedes Element und dessen Schnittstellen sollten alle relevanten Ausfallarten bestimmt und ihre Auswirkungen auf die nächste Ebene analysiert werden.

ANMERKUNG Für sicherheitsgerichtete Analysen ist die vollständige Abdeckung aller möglichen Ausfallarten wichtig. Für eine nicht sicherheitsgerichtete Analyse sollten so viele Ausfallarten wie möglich bestimmt werden bevor mit den wichtigsten und passendsten Ausfallarten fortgefahren wird.

Wenn die Auswirkungen aller Ausfallarten eines bestimmten Elementes auf die höchste Ebene bestimmt wurden, sollte die Analyse mit dem nächsten Element weitergeführt werden. Wenn Kritikalität in der Analyse adressiert werden soll dann kann diese bewertet werden sobald jeder Effekt auf der höchsten Ebene bestimmt, oder ausgeführt nachdem alle Effekte auf der höchsten Ebene bestimmt wurden.

### 5.2.5.2 Wahl der Methode zur Kritikalitätsanalyse

Die Wahl der Methode für die Kritikalitätsanalyse sollte berücksichtigen dass das Ergebnis der Kritikalitätsbewertung als Vorgabe für den Entscheidungsprozess einer Organisation dient; demnach sollten die Ziele der FMEA und der Bereich für Änderungen und/oder Handlungen verstanden sein. Die gewählte Kritikalitätsmethode sollte auch einen Schwellwert oder Rang einführen der innerhalb der Organisation eine Bedeutung hat und in geeigneter Form gegeben wird. Siehe dazu auch Abschnitt 4.2.4 und 5.2.4.1 für eine Erklärung der Kritikalität und ihres speziellen Zweckes.

Die gewählte Kritikalitätsmethode sollte exakt festlegen welche Handlung (falls spezifiziert) benötigt wird für jeden festgelegten Schwellwert oder jede Einstufung. Dies erlaubt, durchdachte Entscheidungen zu bestimmten Ausfallarten und Prioritäten zu deren Behandlung zu treffen. Kritikalitätsanalysen helfen dabei, die wichtigen Beitragsleister zu potenziellen Ausfällen und Schwachstellen in Einheiten oder Prozessen zu bestimmen.

Vor Durchführung der Analyse sollte man sich mit den betroffenen Parteien sowohl auf die Methode der Einstufung als auch auf die Auswahl einer Behandlungsmöglichkeit die in Betracht gezogen werden können einigen.

**ANMERKUNG** Es gibt keine einzelne Methode von der gesagt werden kann dass sie für Kritikalitätsbewertung universell einsetzbar wäre; Anhang C beschreibt zwei allgemeine Methoden und Anhang D, E und F geben Beispiele aus verschiedenen Anwendungsbereichen an. Diese Methoden zur Kritikalitätsanalyse können genutzt werden wenn sie geeignet für eine spezielle Anwendung sind oder wenn sie auf die Notwendigkeiten der Organisation angepasst werden können. Hinweise zum Risikomanagement finden sich auch in IEC 31000 und IEC 31010.

Die Methode zur Kritikalitätsanalyse sollte innerhalb eines spezifischen FMEA-Projektes festgelegt werden.

**ANMERKUNG** Die Methode kann zwischen verschiedenen Projekten gewechselt werden, auch innerhalb derselben Organisation.

#### 5.2.5.2.1 Festlegen von Messskalen für die Einstufung von Ausfallarten

Wo Messskalen für die Kritikalitätsanalyse benutzt werden sollten diese so festgelegt werden dass sie aussagekräftig in Bezug auf die Einheits- oder Prozessfunktion und den Zielen der Analyse sind. Skalen können qualitativ oder quantitativ ausgeführt sein.

**ANMERKUNG** Qualitative Einstufungen dürfen mit Hilfe von strukturierten Expertenentscheidungen entweder mit numerischen oder Buchstabencodes vorgenommen werden, oder mit halbquantitativen Bezeichnungen wie „mehr als einmal pro Jahr“. Wenn solch eine Einstufung getroffen wird kann es von Vorteil sein, unterstützende Beweise aus einer Form von quantitativer Quelle zu suchen auch wenn diese ungenau erscheint.

Die Skalen für die Parameter in einer Kritikalitätsanalyse sollten eine klare und präzise Definition für jeden Schwellwert bieten der direkt auf die Analyse anwendbar ist um eine konsistente und genaue Beurteilung zuzulassen. Die Skalen sollten Kriterien benutzen die sinnvoll vom Analysten benutzt werden können.

Die Anzahl von Schwellwerten innerhalb der Bewertungsskala werden von der Anwendung abhängen, sollten aber den Bereich vom schlechtesten bis zum besten Fall abdecken.

**ANMERKUNG** Als Beispiel vom schlechtesten Fall (z. B. einer oder mehrere Tote oder dauerhafter Produktionsausfall) bis zum besten Fall (z. B. Verletzung die erste Hilfe erfordert oder geringfügige Verzögerungen in der Produktion) oder auch „kein Effekt“.

Generell werden zumindest drei oder vier Kategorien benötigt um genügend Abstufungen zwischen den Auswirkungen zu bieten. Eine große Anzahl an Kategorien kann ungeeignet sein da es übermäßigen Aufwand erfordern kann die exakte Kategorie zu identifizieren wenn resultierende Handlungen zwischen den Kategorien sich nicht wesentlich unterscheiden.

Anhang C gibt mehr Angaben zur Definition von alternativen Skalen, und Anhang D, E und F beinhalten Beispiele zur Anwendung.

### 5.2.5.3 Anpassen von Schritten und Definition von Kriterien zum Abschluss der Analyse

Die Handlungen die in der Ausführungsphase der FMEA wie in Bild 1 dargestellt aufgelistet werden sollten angepasst werden um Schritte zu zeigen die in der tatsächlichen Analyse durchgeführt werden. Allgemein sollte jeder Schritt aus Bild 1 abgeschlossen sein bevor der nächste Schritt durchgeführt wird, auch wenn Iterationsschritte gemacht werden müssen wenn ein vorhergehender Schritt nicht ausreichend gut ausgeführt worden ist. Wenn einer oder mehrere Schritte ausgelassen wurden sollten die Gründe dafür in der Zuschnittsanweisung genannt und gegenüber den betroffenen Parteien, die die Resultate der FMEA nutzen wollen begründet werden. Es sollte entschieden werden welche Kriterien anwendbar sind um den Schritt der Analyse und schlussendlich auch die FMEA abzuschließen.

Es sollte entschieden werden wer bestimmt welche Handlungen basiert auf den aufgelisteten Auswirkungen durchgeführt werden und wie der Abschluss einer potenziellen Ausfallart bestimmt wird. Diese Handlungen dürfen außerhalb der FMEA oder als Teil der Wiedervorlage zur FMEA festgelegt werden. In einigen Fällen kann entschieden werden, dass Ausfallarten mit Auswirkungen oberhalb einer bestimmten Kritikalitätszahl behandelt werden müssen.

Ein Bericht zur FMEA sollte abgegeben werden sobald alle Auswirkungen auf die höchste Ebene analysiert wurden. Sobald alle relevanten Ausfallarten analysiert wurden ist Information über Ausfallauswirkungen vorhanden, mit oder ohne Einstufung der Wichtigkeit je nachdem ob eine Kritikalitätsanalyse durchgeführt wurde. Wo keine gewichtete Liste entstanden ist sollte die komplette Information im Bericht wiedergegeben werden.

Die Form der Dokumentation der FMEA wird während der Planung der FMEA gewählt. Die Dokumentation von FMEA kann sich abhängig von den getroffenen Entscheidungen und der Komplexität der Analyse unterscheiden, was aus den Zuschnittentscheidungen und den Bedürfnissen der betroffenen Parteien resultiert.

**ANMERKUNG** In diesem Zusammenhang sind die betroffenen Parteien:

- die für das Produkt oder den Prozess verantwortliche Firma;
- die potenziellen Abnehmer und Benutzer des Systems oder des Prozesses;
- gesetzliche Behörden die eine Versicherung zur Einhaltung der gebührenden Sorgfalt fordern können;
- Personen die negativ von Ausfällen betroffen sein können.

### 5.2.6 Definition von Ressourcen für die Analyse

Beim Zuschnitt sollte die Anzahl und die Art der Ressourcen die für die Durchführung der FMEA benötigt werden bestimmt werden, wie z. B.:

- Informationsquellen wie Pläne, Zeichnungen, Spezifikationen, Zuverlässigkeitsblockdiagramme und Ausfalleigenschafts-Datenbanken, frühere FMEA über dieselbe oder ähnliche Einheiten; menschliche Ressourcen die die Fähigkeiten und technische Verantwortung (Delegierte) haben die für die gewählte Analysemethode nötig sind, und Einrichtungen wie Konferenzräume, informationelle Unterstützung und Kommunikationsmöglichkeiten wenn es um die Arbeit im Team geht.

#### 5.2.6.1 Informationsquellen

Information zu Folgendem ist üblicherweise nötig:

- die Elemente von Einheit oder der Prozess mit deren Eigenschaften, Leistungsfähigkeiten, Rollen und Funktionen;
- logische Verbindungen zwischen den Elementen;
- Redundanzen und die Eigenschaften der Redundanzen wo nötig;
- Position und Wichtigkeit von Einheit oder Prozess innerhalb deren organisatorischem Zweck (wo möglich);
- Eingangs- und Ausgangsgrößen von Einheit oder Prozess und deren Elementen;
- Schnittstellen zu anderen damit verbundenen Einheiten oder Prozessen inklusive der Umgebung in der die Einheit betrieben wird;

- jede Änderung in der Struktur der Einheit für unterschiedliche Betriebsarten.

Information die Funktionen, Eigenschaften und Leistungsfähigkeit zugeordnet ist wird für alle Ebenen von Einheit oder Prozess bis zur höchsten Ebene benötigt damit die FMEA Ausfallarten die jede der Funktionen beeinflussen können geeignet ansprechen kann.

Die Sammlung von Information wird während der gesamten FMEA weiter durchgeführt da die Analyse aufzeigt wo zusätzliche Information benötigt wird. Die Daten können von Personen mit Wissen über die Einheit oder den Prozess geliefert, müssen aber von allen Personen die an der FMEA beteiligt sind verstanden werden. Der Moderator sorgt dafür dass das Analyseteam die Daten auf Relevanz und Konsistenz überprüft. Das Verhältnis zwischen den Datenelementen wird vom Analyseteam vor und während der FMEA bestimmt. Die zugrundeliegende Information zur analysierten Einheit darf dem Analyseteam vor der ersten Besprechung als Informationspaket zur Verfügung gestellt werden und die Personen die für die FMEA verantwortlich sind sollten während der gesamten Analyse Zugang zu allen darauf bezogenen Informationen haben.

#### 5.2.6.2 Menschliche Ressourcen

Kompetentes Personal das Kenntnisse über die relevanten Aspekte der analysierten Einheit oder des analysierten Prozesses und Erfahrung mit FMEA hat ist wesentlich für die FMEA. Um beide Fähigkeiten zu bekommen ist üblicherweise ein Ansatz mit einem multidisziplinären Team erforderlich. Außerdem können zusätzliche Kenntnisse zu Produkt oder Dienst für die analysierten Einheiten nötig sein.

#### 5.2.6.3 Einrichtungen

Das Management von größeren Analysen, oft verbunden mit komplexem Design von Einheiten oder Prozessen, verlangt nach physisch vorhandenen Ressourcen um verteilte Kommunikation und Erstellung einer Analyse durch reale oder virtuelle Teams zu ermöglichen. Diese können aus dafür bestimmten Besprechungszimmern, audiovisueller Unterstützung für virtuelle Besprechungen und verteilten Informationssystemen über nationale aber auch internationale Grenzen bestehen. Solche Ressourcen sollten auf der Basis von Kosteneffizienz als auch vom Wert in Bezug auf Qualität, Nutzbarkeit (initial oder bei Wiederverwendung) sowie Produktlaufzeit gewählt werden.

ANMERKUNG Tabellen können sinnvoll sein für einfache Analysen mit wenigen Teilnehmern. Komplexe Analysen mit unterschiedlichen Informationsquellen und komplexen Anforderungen an die Berichte können eine relationsbezogene Datenbank erforderlich machen um die Vielzahl von Beziehungen zwischen Ausfallarten, Funktionen, Einheiten, Komponenten und Ausfallursachen zu verwalten.

#### 5.2.7 Zerlegen von Einheit oder Prozess in geeignete Elemente

Die Zerlegung von Einheit oder Prozess erfordert die Zerlegung in Elemente damit die FMEA handhabbar wird und um die Beziehungen zwischen einzelnen Elementen zu bestimmen. Zum Beispiel:

- Hardware-Einheiten können in kleinere, weniger komplexe Hardwaremodule zerlegt werden;
- Prozesse können in andere Prozesshandlungen, Tätigkeiten oder Schritte zerlegt werden;
- Software kann in Softwaremodule oder Prozeduren zerlegt werden; und
- Schnittstellen zwischen Elementen als auch zur Umgebung (z. B. Benutzer) können bestimmt werden.

Die Größe der Elemente darf von einer Einheit oder Prozess zur/zum anderen sowie von einer Analyse zur anderen variieren und sollte bestimmt werden um eine handhabbare Analyse zu schaffen. Für große Einheiten können die Elemente unter Beachtung der funktionalen oder hierarchischen Architektur zerlegt werden um analytisch handhabbare Ebenen zu erstellen. Ähnlich sollten Elemente des Prozesses kohärente Phasen des Prozesses darstellen. Jedes Element der Zerlegung von Einheit oder Prozess sollte definierte Einsatzanforderungen aufweisen.

Symbolische Darstellungen von Struktur und Operation der Einheit oder des Prozesses, speziell Diagramme und Flußpläne, sind für die Analyse hilfreich. Es kann mehrere Diagramme zur Darstellung der Einheit oder des Prozesses, die analysiert werden, geben.

ANMERKUNG Einfache Darstellungen wie Blockdiagramme (siehe IEC 61078) sollten generiert werden um darzustellen wie die Einheit in Teile zerlegt wird.

Alle Funktionen von Einheit oder Prozess auf niedrigster Ebene sollten bestimmt werden damit bei Durchführung der FMEA alle relevanten Ausfallarten und deren Auswirkungen für diese Elemente niedrigster Ebene bestimmt werden können.

### 5.3 Durchführen der FMEA

#### 5.3.1 Allgemein

Dieser Abschnitt beschreibt die zur Durchführung der Analyse zu verfolgenden Schritte. Diese sollten in der für „Top-down“- oder „Bottom-up“-Analysemethode beschriebenen Reihenfolge durchgeführt werden. Das Element von Einheit oder Prozess welches analysiert werden soll unterscheidet sich von Fall zu Fall.

- In einer „Top-down“-Analyse wird ein Element auf der obersten Ebene der hierarchischen Struktur (siehe Abschnitt 4.2.1) gewählt und bewertet indem die Elemente in niedrigeren Ebenen aus denen es besteht betrachtet werden.
- In einer „Bottom-up“-Analyse wird jedes Element auf der niedrigsten Ebene der Hierarchie betrachtet und seine Auswirkung auf Elemente höherer Ebene festgelegt.

ANMERKUNG 1 Für eine „Top-down“-Analyse wird jede Funktion nacheinander betrachtet. Für jede Funktion werden die Ausfallarten die diese Funktion auf höchster Ebene beeinflussen sollten bestimmt und analysiert.

ANMERKUNG 2 Für eine „Bottom-up“-Analyse werden die Auswirkungen von potenziellen Ausfallarten auf Funktion von Einheit oder Prozess, auf andere Einheiten oder Prozesse und die Auswirkungen die Ausfälle auf die Funktionen auf der höchsten Ebene haben bestimmt und analysiert.

#### 5.3.2 Bestimmen von Funktion und Leistungsmerkmalen von Einheit oder Prozess

Alle Funktionen jedes Elementes von Einheit oder Prozess sollten zusammen mit den nötigen Leistungsmerkmalen bestimmt werden die für das jeweilige Analyse-Szenario erforderlich sind. Die Funktion jedes Elementes sollte von einer Spezifikation der Funktion oder anderen verfügbaren Quellen abgeleitet werden.

ANMERKUNG Die Funktion von Einheit oder Prozess wurde zu Anfang in der Planungsphase bestimmt. Eine klare Darstellung der Funktionalität aller Elemente wird benötigt als Basis für die durchzuführende FMEA.

Das Leistungsmerkmal ist der Grad der Leistungsfähigkeit der benötigt wird um die angegebene Funktion von Einheit oder Prozess im gegebenen Szenario zu erfüllen. Dieser sollte eindeutig angegeben sein und kann quantitativ ausgedrückt werden um sicherzustellen dass die Arten in welcher die Funktion verloren werden kann klar erkannt werden können. Der gewählte Wert sollte eher den Schwellwert der Leistungsfähigkeit die nötig ist um die Funktion zu erreichen beschreiben als die Fähigkeiten von Einheit oder Prozess.

Eine einzelne Einheit oder ein einzelner Prozess kann so beschaffen sein dass sie/er mehrere Funktionen gleicher oder verschiedener Wichtigkeit für den Prozess ausführen kann.

Alle Einheiten oder Prozessfunktionen sind spezifisch für ein Szenario (z. B. ein Satz von Einsatz- und Umgebungsbedingungen); alle speziellen zusätzlichen Faktoren die auf die Art in welcher die spezifischen Einheiten betrieben werden oder Handlungen im Prozess durchgeführt werden sollten entweder gegen diese Einheit oder diesen Prozess oder als Teil der allgemeinen Aussage zum Szenario innerhalb der Analyse beschrieben werden.

#### 5.3.3 Bestimmen von Ausfallarten

Für jede Funktion eines Elementes einer Einheit oder eines Prozesses sollten die Arten in welche sie / er versagen kann seine Leistungsmerkmale zu erreichen festgelegt werden. Jede Funktion kann auf mehrere Arten versagen (z. B. seine Ausfallarten) und alle sollten aufgelistet und niedergeschrieben werden.

Abhängig von Zweck und Anwendungsbereich der Analyse kann das Folgende berücksichtigt werden um bei der Bestimmung der Ausfallarten von Einheit oder Prozess zu helfen:

- die Anwendung
- die Betriebsart
- die einschlägigen Betriebsspezifikationen
- zeitliche Beschränkungen
- Beanspruchung durch die Umgebung
- psychologischer Stress

Typische Information zu Ausfallarten kann aus Folgendem gewonnen werden:

- für neue Einheiten oder Prozesse kann Bezug auf andere Einheiten oder Prozesse genommen werden die ähnliche Funktion und Struktur haben sowie auf deren Leistungsfähigkeit unter angemessenen Bedingungen;
- für existierende Einheiten können die Ausfallarten aus vorhergehenden FMEA, aus dem Betrieb oder aus Überprüfungen bekannt sein. Die Belastung und der Betrieb selbst kann aber unterschiedlich von früherer Benutzung sein.

#### 5.3.4 Bestimmen von lokalen und gesamten Auswirkungen von Ausfallarten

Eine Ausfallauswirkung ist die Auswirkung einer Ausfallart im für die Analyse definierten Szenario. Die selbe Ausfallauswirkung kann von einer oder mehreren Ausfallarten eines oder mehrerer Elemente einer Einheit oder eines Prozesses ausgelöst werden.

Die Ausfallauswirkung wird bestimmt in Bezug auf Wissen über Einheit oder Prozess, deren Funktionen, gegenseitigen Beeinflussungen und der Position in der obersten Ebene. Die Ausfallauswirkung sollte niedergeschrieben werden mit einer Beschreibung und mit ausreichender Information um eine exakte Beurteilung der Schwere und Signifikanz der Auswirkungen zu erlauben.

Die Auswirkung die bestimmt wurde sollte die schwerste Auswirkung sein die innerhalb des Anwendungsbereiches der Analyse gemacht werden sowie unter der Bedingung dass keine Steuerung vorhanden ist mit der eine Abwendung der Auswirkungen möglich ist.

Die Auswirkung von Ausfallarten für ein Element auf derselben hierarchischen Ebene einer Einheit oder eines Prozesses wie der welcher analysiert wird sollte zusammen mit der Auswirkung auf die oberste Ebene bestimmt werden. Auswirkungen auf mittlere Ebenen könnten auch bestimmt werden wenn dies das Verständnis und die Zuordnung des Schweregrades unterstützt.

Die Bestimmung von endgültigen Auswirkungen auf die Einheit ist wichtig bei der Berücksichtigung der relativen Wichtigkeit von Ausfällen, da dies einen gemeinsamen Referenzpunkt darstellt. Das Bestimmen der lokalen Auswirkungen kann Information zur Verfügung stellen die helfen kann wenn Alternativen für Maßnahmen zur Abwendung gesucht werden. In bestimmten Fällen kann es keine lokale Ausfallauswirkung über die Ausfallart selbst hinaus geben.

Eine Auswirkung einer Ausfallart eines Elementes auf niedriger Hierarchieebene muss nicht in einem Funktionsverlust auf der nächsthöheren oder höhergelegenen Ebenen resultieren (z. B. der Auswirkung auf die Einheit). Solche Ausfälle bleiben auf lokaler Ebene mit keiner oder kleiner Auswirkung auf die nächsthöhere Ebene oder die oberste Ebene.

Zusätzlich zu Auswirkungen auf die Funktion von Einheit oder Prozess können andere Auswirkungen von Bedeutung sein; zum Beispiel in Bezug auf Sicherheit, Umwelt oder Einhaltung von Vorschriften.

ANMERKUNG 1 Die Ebenen auf denen Auswirkungen niedergeschrieben werden und die Art der zu berücksichtigenden Auswirkungen hängen ab vom Zweck der Analyse über den während der Planungsphase der FMEA entschieden wurde.

ANMERKUNG 2 Die Bestimmungen der Auswirkungen des Ausfalles auf die Einheit können die Nutzung anderer Analysen wie Fehlerbaumanalysen (IEC 61025), Ereignisbaumanalysen (IEC 62502), Markov-Analysen (IEC 61165) oder Petri-Netz-Analysen (IEC 62551) erfordern.

Weil die FMEA die Auswirkungen auf die höchste Ebene Element für Element oder Funktion für Funktion bestimmt folgt dass die Auswirkungen auf die höchste Ebene die aus mehreren Ausfällen resultieren üblicherweise nicht erkannt werden.

Abhängige Auswirkungen können mit der FMEA identifiziert werden in Situationen wo ein Ausfall keine erkennbaren direkten Auswirkungen hat (z. B. wenn der Ausfall nicht aufgedeckt wird), aber in einem Ausfall auf oberster Ebene resultieren kann wenn ein zweiter ebenfalls nicht wichtiger Ausfall erfolgt.

ANMERKUNG 1 Zum Beispiel führt ein Ausfall eines Sicherheitsgerätes nur zu unerwünschten Auswirkungen wenn sowohl das Sicherheitsgerät als auch die Einheit zu deren Schutz es ausgeführt wurde ausfallen. Auswirkungen aus mehrfachen Ausfällen sollten im Analysebericht angezeigt werden.

ANMERKUNG 2 Fehlerbaumanalyse (IEC 61025) kann benutzt werden um diese Beziehungen zu verstehen.

### 5.3.5 Bestimmen von Ausfallursachen

#### 5.3.5.1 Allgemein

Ausfallursachen werden bestimmt um Entscheidungen darüber zu treffen wie Ausfallauswirkung verhindert oder gemildert werden können.

Bei der Bestimmung der Ursachen sollte der Kontext für den Gebrauch berücksichtigt werden. Ursachen die mit Hardware, Software, menschlichen Aspekten verknüpft sind sowie die Schnittstellen zwischen diesen sollten berücksichtigt werden. Wenn möglich sollten die Kausalzusammenhänge (z. B. die physischen, logischen oder psychologischen) des Ausfalles bestimmt werden.

ANMERKUNG Ursachen-Analysetechniken (IEC 62470) können beim Prozess der Ausfallursachenanalyse hilfreich sein.

Der Umfang in welchen Ausfallursachen erforscht werden sollten hängt ab von der Kosteneffizienz dieser Handlung.

ANMERKUNG Zum Beispiel mag es nicht notwendig sein, einen große Aufwand in die Analyse von Ausfallarten, die wenig Auswirkung auf die Funktionen und Ziele hat, zu investieren.

Es ist nicht immer möglich oder notwendig alle Ursachen aufzuzeichnen, aber wenn die Ausfallursache bekannt ist, ist es oft möglich, diese Ausfallart zu beheben.

ANMERKUNG Zum Beispiel kann die Änderung eines Materials Ausfallarten durch Korrosion eliminieren.

Eine Ursache kann in mehreren Ausfallarten resultieren. Die Physik der Ausfallanalyse kann die Suche nach Ursache unterstützen.

Ausfallursachen können in Ursachen die eliminiert werden können, Ursachen die reduziert werden können und Ursachen die unvermeidbar sind eingeteilt werden. Für Ursachen die nicht eliminiert werden können kann es nötig sein eine Methode zur Milderung zu nutzen um Auswirkungen der Ausfallart zu reduzieren.

#### 5.3.5.2 Ausfälle gemeinsamer Ursache

Eine FMEA sollte alle möglichen Quellen von Ausfällen gemeinsamer Ursache (Common-Cause-Fehler CCF) bei der Analyse einer Einheit oder eines Prozesses berücksichtigen wenn diese Redundanz oder mehrfache (prozedurale) Steuerungsmöglichkeiten benutzt um bei einem Ausfall die Funktion zu erhalten oder die Folgen zu mildern. Der Anwendungsbereich für solche Quellen wird durch das definierte Szenario der Studie festgelegt.

ANMERKUNG 1 CCF bedeuten, dass mehr als nur eine Einheit gleichzeitig oder innerhalb eines kurzen Zeitraumes ausfällt und damit die Auswirkung eines gleichzeitigen Ausfalles hat. CCF sind solche Fehler, die die fundamentale Annahme, dass die untersuchten Ausfallarten in der FMEA unabhängig sind, untergraben.

ANMERKUNG 2 Ein möglicher CCF kann so beschrieben werden, dass ein System betrachtet wird, in dem eine kritische Energieversorgung durch ein Backup-System geschützt wird bei dem zwei identische Versorgungen mit je 100% der nötigen Leistungsfähigkeit verwendet werden. Ein CCF der von der Umgebung ausgelöst wird könnte eine Flut sein, die einen gleichzeitigen Verlust von Primär- und Backup-System zur Folge hat, da beide im selben Raum installiert wurden oder dieselbe Anfälligkeit gegen Überflutung aufweisen. In dieser Situation muss „gleichzeitig“ nicht bedeuten dass die Ausfälle zur selben Zeit stattfinden, sondern dass sie in einer so kurzen Zeit stattfinden dass eine menschliche oder technische Handlung nicht mehr rechtzeitig ausgelöst werden kann um ein zweites oder weiteres Ereignis oder Ereignisse zu verhindern.

Wo ein CCF zwischen den bestehenden Steuerungsmöglichkeiten und der betrachteten Einheit erkannt wird, sollte der CCF in gleicher Art wie andere Ursachen als Ausfallursache berücksichtigt werden und die Begründung für die Berücksichtigung sollte in die Dokumentation aufgenommen werden.

ANMERKUNG 1 Methoden die die Bestimmung von Quellen der CCF unterstützen sind Ursache-Wirkungs-Diagramme, Bow-Tie-Diagramme und Threat-Barrier-Diagramme (IEC 62740) und können als Eingabe für den FMEA genutzt werden.

ANMERKUNG 2 Verfügbare Methoden zur Vermeidung von CCF bei Entwicklung oder Betrieb liegen außerhalb des Anwendungsbereiches dieser internationalen Norm.

### 5.3.5.3 Menschliche Aspekte

Menschen können als Element einer Einheit oder eines Prozesses der Ausfallarten aufweist angesehen werden, oder menschliches Versagen kann als Ursache des Ausfalles von Hardware, Software oder eines Elementes eines Prozesses angesehen werden.

Die Analyse des Grundes für Arten des menschlichen Versagens ist häufig komplizierter als die Ursachen von Hardware- und Softwareausfällen zu bestimmen, da es viel mehr mögliche Ausfallmechanismen gibt, jede mit verschiedenen möglichen Ursachen. Die Vernachlässigung einer Menge von psychologischen Ausfallmechanismen kann in einer zu einfachen und falschen Zuordnung von Ursachen und daraus in geeigneten Behandlungsstrategien führen.

ANMERKUNG 1 Zum Beispiel kann die Ausfallart „Handlung unterblieben“ auftreten weil eine Person ihren Platz in einer Sequenz aufgrund einer Ablenkung oder weil die Person falsche Annahmen trifft oder weil unvollständiges Wissen über die nötige Sequenz von Handlungen vorliegt. Wenn eine Handlung aufgrund von Ablenkung oder übermäßiger Routine vorliegt kann zusätzliches Training keinen Nutzen haben oder sogar kontraproduktiv sein.

ANMERKUNG 2 Die Gründe für menschliches Versagen und Faktoren die die menschliche Leistungsfähigkeit gestalten werden in IEC 62508 diskutiert. Die Taxonomie von Arten menschlichen Versagens, Mechanismen und Ursachen sowie formale Methoden die benutzt werden können um menschliches Versagen zu analysieren werden in IEC 63740 beschrieben.

Handlungen die menschliches Versagen ansprechen, versuchen, die Auftretenswahrscheinlichkeiten zu verringern, da es aber schwierig ist den Ausfall auszuschließen ist es üblich die Einheit oder den Prozess ausfalltoleranter zu gestalten.

ANMERKUNG Zum Beispiel können beim Führen eines Zuges als auch um Signale einfach sichtbar zu machen mechanische Verriegelungen bereitgestellt, um zu verhindern, dass Signale bei Gefahr passiert werden, egal was Ausfallursache war.

### 5.3.5.4 Software-Aspekte

Wenn Software in einer FMEA berücksichtigt wird, wird diese untersucht während sie in einer Hardware-Umgebung (z. B. Embedded Software oder Firmware) eingesetzt wird um die lokalen oder globalen Auswirkungen auf die Software-Ausfallarten zu beschreiben.

Beim Durchführen einer FMEA auf ein Hardware-Software-System werden Experten für Software als auch Hardware benötigt um an der Analyse zur selben Zeit teilzunehmen.

ANMERKUNG 1 Bei komplizierten Schaltungen und moderner Software können viele mögliche Ausfallarten auftreten. Beispiele können umfassen:

- Eine Auswirkung auf falsche Eingangsdaten (z. B. Null, negative Werte, außerhalb der Funktion);
- Eine Auswirkung auf falsche Ausgangsdaten (z. B. Null, negative Werte, außerhalb der Funktion);
- Störungen bei der Datenkommunikation (z. B. bei elektromagnetischen Transienten, Bitfehlerraten (BER);
- Datenkollision wegen Änderung der Ausbreitungszeit (z. B. aufgrund von Temperatur);
- übermäßige Antwortzeiten oder hängender Ausgang (z. B. eingefrorenes Display);
- Hängenbleiben in der Menüstruktur (z. B. verriegelt wegen Warten auf Antwort);
- Reset (z. B. wegen Spannungsabfall in der Versorgung, externem Reset oder Reset über den Watchdog;
- gesammelte Rückstände im Speicher;
- Änderung in gespeicherten Daten (z. B. Soft-Errors)
- Speicher nicht zurückgesetzt, nicht auf neuestem Stand oder falsch auf neuen Stand gebracht;
- Überlast (z. B. akuter Anstieg wegen exzessiver Last);
- Ausfall der Hardware (e.g. Server, Festplatten oder Router);
- „Sneak Circuit Analysis“ (see RADC-TR-82-179);
- falscher Pfad oder Position in der Menüstruktur;
- falsche Eingabe (z. B. doppeltes Drücken einer Taste oder mehrere Tasten gemeinsam gedrückt).

ANMERKUNG 2 historisch waren Bauteilausfälle Kurzschluss, Unterbruch oder Parameterdrift. Ähnlich kann jeder Pin eines Mikroprozessors als „hängt auf 0“ oder „hängt auf 1“ betrachtet werden. Diese können immer noch relevant sein, reichen aber für moderne elektronische Einheiten nicht aus.

### 5.3.6 Bestimmen von Aufdeckungsmethoden und existierenden Steuerungsmöglichkeiten

Für jede Ausfallart sollte der Analyst die Art bestimmen und niederschreiben wie:

- der Ausfall (oder der bevorstehende Ausfall) erkannt werden kann ohne dass die Ausfallauswirkung auftritt;
- die Auswirkung des Ausfalls vermindert werden kann.

Die Möglichkeiten zur Aufdeckung können physische Indikatoren oder Ergebnisse von Beobachtungen sein, die von einer Einheit oder von Überprüfungen innerhalb eines Prozesses stammen. Allgemein werden die Möglichkeiten, wie Ausfallarten während Betrieb und Nutzung aufgedeckt werden können, niedergeschrieben.

Wenn mehr als eine Ausfallart durch dieselbe Methode aufgedeckt werden kann, sollte die Beschreibung der Methode zeigen, wie Mehrdeutigkeiten aufgelöst werden können, damit eine geeignete Handlung ausgelöst wird.

In der Praxis ist die Identifikation von Aufdeckungsmethoden und Verminderungsfaktoren rekursiv, weil das Team von Analysten sowohl:

- die existierenden Eigenschaften von Einheit oder Prozess wie sie/er zum gegebenen Zeitpunkt der Analyse definiert ist; als auch
- Identifikation von Aufdeckungsmethoden und Verminderung, die für mögliche Ausfallarten benötigt werden

berücksichtigen muss.

Deshalb sollte der Analyst auch Vorschläge machen für:

- neue oder verbesserte Möglichkeiten, wie Einheit, Bedienpersonal, Nutzer und Andere den Ausfall aufdecken können, und
- das Entfernen von Aufdeckungsmöglichkeiten, die ineffektiv oder unnötig sind.

Diese Vorschläge könnten als Eingaben für den Schritt, der in 5.3.10 beschrieben ist, benutzt werden, und, wenn akzeptiert und in die Einheit oder den Prozess aufgenommen, im nächsten Update der FMEA berücksichtigt werden.

Es kann auch hilfreich sein, abhängig vom Zweck der Analyse, niederzuschreiben, wie die Ausfallart auf anderen Stufen der Analyse aufgedeckt werden kann, wie z. B.:

- im Lebenszyklus, wie zum Beispiel bei der Entwicklung, der Produktion oder während der Instandhaltung, und
- von einer anderen Einheit.

Diese Information könnte genutzt werden, um eine Behandlung auf höherer Ebene hinzuzufügen, um Teil der Designüberprüfung zu bilden, um über Entscheidungen zu Anforderungen an die Instandhaltung zu informieren oder um Prüfprozeduren zu entwickeln. Diese Vorschläge für die Behandlung sollten auf informationeller Ebene bleiben; die anderen Stufen oder höheren Ebenen sind generell außerhalb des Anwendungsbereiches der Einheit oder der Verantwortung des Analysten. Wenn nötig können diese auf der relevanten Stufe oder Ebene der FMEA behandelt werden.

#### **5.3.6.1 Aufdeckungsmethoden**

Als Teil der FMEA ist es wichtig, zu betrachten wie mögliche Ausfallereignisse oder Fehler die in einem Ausfallereignis resultieren könnten aufgedeckt werden können. Das Aufdecken von potenziellen Ausfällen erlaubt Bedienpersonal oder Nutzern, nötige Maßnahmen zu realisieren die große Auswirkungen von Ausfällen vor deren Auftreten verhindern würden.

Die Aufdeckung kann es ermöglichen den Ausfall zu verhindern oder die Folgen zu mindern.

**ANMERKUNG** In einigen Anwendungen von FMEA, speziell im Automobilbereich, hat Aufdeckung eine komplett andere Bedeutung; sie ist Teil der Bestimmung einer potenziellen Ausfallart während eines Entwicklungsprozesses. Aufdeckung heißt in diesem Fall dass Designänderungen angezeigt werden für die Minderung oder Eliminierung von Ausfallarten.

#### **5.3.6.2 Vorhandene Steuerungsmöglichkeiten**

Eigenschaften des Designs oder von anderen vorhandenen Vorrichtungen, die die Fähigkeit haben eine Auswirkung einer Ausfallart zu verhindern oder zu verringern, und ihre Handlung bei Auftreten der Ausfallart sollten klar beschrieben sein. Solche Steuerungsmöglichkeiten können folgende sein:

- redundante Einheiten die einen kontinuierlichen Betrieb zulassen wenn eine oder mehrere Einheiten ausfallen;
- alternative Betriebsmöglichkeiten;
- Überwachungs- und Alarmeinrichtungen;
- Überprüfungen um sicherzustellen dass Prozessschritte korrekt durchgeführt wurden.

#### **5.3.7 Bestimmung der Schwere der Auswirkung des Ausfalls auf die Einheit**

Die Auswirkungen eines Ausfalles können mit der Bestimmung eines Schweregrades oder Ranges angegeben werden. Dieser kann als eine einzelne Zahl oder ein einzelner Buchstabe, die, bzw. der mit einer bestimmten Auswirkung einer diskreten Ausfallart verknüpft ist, ausgedrückt werden. Schweregrade von Ausfallauswirkungen können eine einfache Alternative zu komplizierteren Kritikalitätsanalysen darstellen.

Der Schweregrad wird mit einer speziellen Ausfallart assoziiert und symbolisiert die Signifikanz seiner Auswirkung auf die höchste Ebene der Analyse oder für welche die Analyse bestimmt ist.

ANMERKUNG 1 Zum Beispiel kann die Analyse einer Einheit von einem Hersteller durchgeführt werden um den Entwickler des Produktes zu informieren, in diesem Fall würde die Schwere als Auswirkung auf die Leistungsfähigkeit des gesamten Produktes ausgedrückt. Die selbe Einheit könnte als Teil einer größeren Gruppe von Einheiten analysiert werden, in diesem Fall würde die Schwere mit den Auswirkungen auf die Leistungsfähigkeit der Gruppe verknüpft.

ANMERKUNG 2 Zum Beispiel kann ein Prozess oder eine Prozedur analysiert werden um ihre Auswirkung auf eine kleine Einheit oder Gruppe zu bewerten, oder als Teil eines größeren Prozesses oder Organisation.

Die korrekte Bestimmung der Einheit für die die Schwere belegt werden soll ist essentiell um sicherzustellen dass der wahre Einfluss bewertet wird und ein konsistentes Verständnis der Ausfallauswirkungen erlangt wird. Die Ausfallart kann auf niedrigen Ebenen der Hierarchie oft wesentlicher wirken, da Redundanz oder Verminderungseigenschaften / Handlungen noch nicht betrachtet werden.

Wenn die Schwere einer Auswirkung in einem definierten Nutzungskontext definiert wird, kann eine Anzahl von Maßnahmen bedacht werden, für die die Konsequenzen bewertet werden, wie z. B. für Sicherheitstechnik, Bereitstellung einer Dienstleistung oder finanzielle oder ökonomische Wirkung. Wenn die Auswirkungen einer speziellen Ausfallart in Bezug auf mehr als ein Kriterium bewertet werden können, dann soll nur das dominierende Kriterium für die Bestimmung des Schweregrades herangezogen werden.

ANMERKUNG Einstufungen sind keine quantitativen Werte und können daher nicht kombiniert werden um eine zusammengefasste Zahl zu ergeben, sie sind nicht den Regeln der Mathematik unterworfen.

### 5.3.8 Abschätzen der Wahrscheinlichkeit einer Ausfallart

Bei der Ausführung einer Kritikalitätsanalyse sollte die Auftretswahrscheinlichkeit jeder Ausfallart bestimmt werden.

Bei der Abschätzung der Auftretswahrscheinlichkeit einer Ausfallart ist es wichtig, die Umweltfaktoren zu berücksichtigen, die den Ausfall und seine Wahrscheinlichkeit beeinflussen. Faktoren wie mechanische oder elektrische Belastungen in Bauteilen und physischer oder psychologischer Stress für Personal das eine Prozedur ausführt, kann die Qualität der Ausführung beeinflussen.

Die Auftretswahrscheinlichkeit einer Ausfallart kann abgeschätzt werden aus:

- Daten aus Lebensdauertests an einem Bauteil oder Raten für menschliches Versagen aus Laborversuchen;
- vorhandene Datenbanken von Ausfallraten, Ausfallwahrscheinlichkeiten oder Nichtverfügbarkeit;
- Felddaten zu Ausfällen;
- Beobachtung menschlicher Leistungsfähigkeit;
- Ausfalldaten für gleiche Einheiten mit vergleichbarer Nutzung.

ANMERKUNG Es existieren Datenbanken von Ausfallarten für allgemein benutzte Bauteile von Ausrüstung (z. B. MIL STD 338B, IEC 62308), für menschliches Versagen (z. B. HSE 2009 Human reliability assessment methods, IEC 62508) und für die Beurteilung von Ausfällen ähnlicher Einheiten (z. B. IEC 61709).

Wenn die Wahrscheinlichkeit eines Auftretens abgeschätzt wird, dann muss die FMEA auf den Zeitraum, für den die Abschätzung gilt, eingehen. Diese Periode wird von den Zielen der FMEA abhängen. Beispiele von üblicherweise genutzten Zeitperioden sind:

- der Garantiezeitraum;
- die angenommene Lebensdauer der Einheit;
- die spezifische Nutzungsdauer der Einheit;
- die Dauer einer Schicht.

### 5.3.9 Bewerten der Kritikalität

Wo eine Kritikalitätsanalyse benötigt wird sollte die Methode zur Festlegung der Kritikalitätszahl jeder Ausfallart benutzt werden auf die man sich in der Planungsphase für die FMEA (siehe Abschnitt 5.2.5.2) geeinigt hat.

Die Kritikalitätsanalyse kann entweder als Teil der Analyse jeder Ausfallart oder nach der Bestimmung aller Ausfallarten erfolgen. Das Resultat der Kritikalitätsbewertung ist eine Liste aller Ausfallarten, mit Einstufung wo erforderlich, die bestimmt welche davon Maßnahmen erfordern. Die Auswahl geeigneter Maßnahmen wird in 5.3.10 diskutiert.

### 5.3.10 Bestimmen von Handlungen

#### 5.3.10.1 Allgemein

Der abschließende Schritt in der Aktivität zur „Durchführung der Analyse“ ist es, die potenziellen Maßnahmen zu jedem potenziellen Ausfall der in der Ausfallanalyse bestimmt wurde zu bestimmen, zu bewerten und zu dokumentieren.

Die Maßnahmen können die Auftrittswahrscheinlichkeit, die Auswirkung oder die Kombination aus Beiden beeinflussen. Die Gründe für die Empfehlung oder Ablehnung jeder einzelnen potenziellen Maßnahme wird basiert auf den Entscheidungskriterien, die in Abschnitt 5.2.4 beschrieben wurden und sollten dokumentiert werden.

Die Bestimmung von Handlungen und ihrer Dokumentation ist abhängig von der Art der FMEA:

- für grundlegende FMEA wird eine Liste von Maßnahmen, die direkt offensichtlich sind, dokumentiert, aber die Auswahl der endgültigen Lösung ist das Thema für weitere Analyse und Verhandlung außerhalb der FMEA;
- für eine FMEA die eine Kritikalitätsanalyse beinhaltet wird das Ergebnis genauso sein wie für die grundlegende FMEA mit zusätzlicher Angabe der Priorität.

Bei der Festlegung der Maßnahmen muss auch wenn eine vollständige Quantifizierung durchgeführt wurde eine Unsicherheit berücksichtigt werden, da die Kritikalitätszahl nur Abschätzungen darstellen. Es sollte Sorge dafür getragen werden, dass Abschätzungen nicht ein Grad von Exaktheit und Präzision unterstellt wird der nicht vereinbar mit den Daten und der verwendeten Methoden ist.

Maßnahmen die manchmal als „kompensierende Vorrichtungen“ aus vorhergehenden FMEA bekannt sind bestehen aus drei Kategorien:

- Designhandlungen, die ausgeführt werden um Steuerungsausfälle zu verhindern;
- Handlungen des Bedienpersonals, die zur Abmilderung der Ausfallauswirkung vorgesehen sind;
- Instandhaltungsmaßnahmen, die zur Reduzierung der Auftrittswahrscheinlichkeit von Ausfällen vorgesehen sind.

#### 5.3.10.2 Designmaßnahmen

Designbezogene Maßnahmen zur Risikoreduzierung beinhalten die Änderung von Eigenschaften des Designs von Einheit oder Prozess, die:

- die Ausfallart komplett eliminieren;
- die Wahrscheinlichkeit des Auftretens einer Ausfallart verringern;
- die Ausfallauswirkungen eliminieren oder reduzieren.

ANMERKUNG Beispiele von Designhandlungen beinhalten:

- automatische Aktivierung oder Deaktivierung von Einheiten um die Entstehung oder Verbreitung von Ausfallauswirkungen zu verhindern;
- Aktivierung von redundanten, Backup- oder Standby-Möglichkeiten;

- Vorsehen von Warnungen vor bevorstehenden Ausfällen an das Bedienpersonal wo eine Eingriffshandlung durchführbar ist;
- Änderung von Schritten eines Prozesses um Ausfallwahrscheinlichkeit zu reduzieren.

Und Designhandlungen können erreicht werden durch die Einführung von Designeigenschaften wie:

- entweder vollständig oder teilweise redundante Einheiten, die einen dauerhaften und sicheren Betrieb zulassen;
- Sicherheits- oder Entlastungseinheiten die einen kontinuierlichen Betrieb zulassen oder Schaden begrenzen;
- alternative Betriebszustände, wie Backup- oder Standby-Einheiten oder -Systeme;
- Sensoren und Überwachungssysteme, wie Alarmer um Bedienpersonal über potenzielle oder aufgetretene Ausfallbedingungen zu informieren;
- ergonomisches Design, wie verbesserte Computerschnittstellen oder Arbeitssysteme.

### 5.3.10.3 Instandhaltungsmaßnahmen für Einheiten

Instandhaltungsprogramme sollten auf strukturierte Art aus der FMEA entwickelt werden. Der Wert eines Instandhaltungsprogramms sollte auf ein klar definiertes Risiko bezogen sein.

ANMERKUNG Ein gründlicher Prozess für die Entwicklung solcher Programme ist „Auf die Funktionsfähigkeit bezogene Instandhaltung“ (IEC 60300-3-11)

### 5.3.10.4 Bedienhandlungen

Bedienpersonal kann einschreiten um die Auswirkung eines identifizierten potenziellen oder aufgetretenen Ausfalles umzukehren oder zu mildern.

ANMERKUNG 1 Beispiele von Handlungen für Einheiten beinhalten Isolierung, Lastreduktion, Umlenkung, Aktivierung von Unterdrückungsfunktionen und Alarmer.

ANMERKUNG 2 Beispiele von Handlungen für Prozesse beinhalten Prüfungen und Anpassungen die während einer Prozedur vorgenommen werden.

ANMERKUNG 3 Betriebsumgebungen sind eine Schlüsselfunktion der Design-Konfiguration und sollten so behandelt werden, siehe ISO 10007.

## 5.4 Dokumentieren der FMEA

### 5.4.1 Allgemein

Dokumentieren der FMEA ist nötig um:

- die Entscheidungen zu rechtfertigen, die zur Nutzung einer FMEA und wie deren Ergebnisse verwendet werden, geführt haben;
- den Zuschnitt der FMEA zu beschreiben und den Grund für die Auswahl der Kritikalitätsmetrik, Anwendungsbereich, Abteilung usw.;
- die Betroffenen zu identifizieren, die an der FMEA beteiligt waren;
- die Information zu beschreiben, die während der FMEA verfügbar war und um eine überprüfbare Verknüpfung zu den Quellen zur Verfügung zu stellen;
- die Ereignisse im Verlauf der FMEA zu beschreiben;
- die Ergebnisse der FMEA und wie deren Information benutzt wird zu beschreiben;
- die Empfehlungen für weitere Handlungen oder Analysen festzulegen;
- die Mängel in der FMEA zu identifizieren auf die mit Änderungen an den FMEA-Aktivitäten in der Zukunft eingegangen werden kann;
- die Rückverfolgbarkeit der Dokumentation als wesentlicher Teil des Audit-Prozesses zu gewährleisten;

- eine Eingabe für andere Aktivitäten zu bilden oder als FMEA-Bericht alleine zu stehen.

Da eine FMEA iterativ vorgenommen wird, entsteht die Dokumentation fortschreitend während der Handlungen in der FMEA. Eine neue Revision der FMEA-Dokumentation sollte herausgegeben werden wenn die Information überarbeitet wurde. Die FMEA sollte überarbeitet werden zu Zeiten, die angemessen für die Anwendung sind. Dies kann bei Meilensteinen im Projekt der Fall sein.

ANMERKUNG Zum Beispiel, wenn die Arbeit am Design fortschreitet, oder wenn Handlungen zur Verminderung von Auswirkungen implementiert wurden, wenn Einheiten oder Prozesse entwickelt und in einem betrieblichen Kontext eingesetzt werden.

Die FMEA-Dokumentation sollte einer Versionskontrolle unterliegen.

#### 5.4.2 Mindestinhalt von Dokumentation

Als Minimum sollte die Dokumentation enthalten:

- eine Beschreibung des analysierten Systems zusammen mit einem Block-, Funktions- oder Flussdiagramm, das die Struktur umschreibt,
- eine klare Beschreibung von Anwendungsbereich und Grenzen, die jede spezielle Ausnahme aus dem Anwendungsbereich aufzeigt,
- Kriterien die inakzeptable Auswirkungen oder Risiken festlegen und wann Behandlung erforderlich wird,
- über das analysierte System getroffene Annahmen,
- die verfolgte Methodik einschließlich einer Liste der beteiligten Personen mit deren Kenntnissen,
- eine Beschreibung der Methode, die für die Kritikalitätsanalyse benutzt wurde, sollte in ausreichender Detailtiefe beschrieben sein um ein unabhängiges Audit von angewendeten Einstufungen und Bewertungen zu ermöglichen,
- Datenquellen und andere Materialien (einschließlich Status des Anliegens) auf welchen die FMEA basiert ist,
- eine Liste von Quellen die verwendet wurden um die Analyse zu unterstützen,
- eine Zusammenfassung der Entdeckungen, einschließlich Ausfallarten die in schwerwiegenden Auswirkungen resultieren, deren Auswirkungen und Ursachen. Ausfallarten und Auswirkungen sollten ohne Referenz auf andere Dokumente, die nicht Teil des Reports sind, angegeben werden,
- empfohlene Handlungen, soweit diese erzeugt wurden;

ANMERKUNG Die Dokumentation der FMEA könnte nur eine kurze Aussage zu den nötigen korrektiven Handlungen enthalten. Diese Handlungen müssen in einen Aktionsplan überführt werden, der aufzeigt, wer verantwortlich für die Handlungen ist und wie und wann diese umgesetzt werden. Die Kritikalitätsanalyse bietet eine Vorgabe um im Aktionsplan Prioritäten zu setzen, aber Kosten und Vorteile der Handlungen werden auch mit berücksichtigt. In einigen Fällen könnte keine Handlung erfolgen auch wenn eine Handlung während der FMEA identifiziert wurde. Der Grund für das Unterlassen der Umsetzung einer Empfehlung sollte niedergeschrieben werden und die potenziellen Auswirkungen sollten beobachtet und überprüft werden wenn erforderlich.

- Designänderungen die als Resultat der FMEA schon umgesetzt wurden und jede nicht erfolgte Handlung, und
- Arbeitsblätter die als Anhang zum Bericht eingebracht werden können, oder die Referenz auf ihre Stelle, wenn diese zu umfangreich sind und eine Datenbank benutzt wird.

#### 5.5 Abschließen der FMEA

Alle Ausfallarten und Kausalzusammenhänge die während der Analyse identifiziert wurden sollten bewertet und formell abgeschlossen sein.

### 6 Literaturhinweise

- [1] AIAG, *Potential Failure Mode and Effects Analysis*, Third Edition, 2001

- [2] 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.
- [3] HSE 2009, *Human Reliability Assessment Methods*
- [4] IEC 60050(192): 2014, *International Electrotechnical Vocabulary (IEV) – Chapter 192: Dependability and quality of service*
- [5] IEC 60300-1, *Dependability management – Part 1: Dependability management systems*
- [6] IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management*
- [7] IEC 60300-3-1:2003, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*
- [8] IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*
- [9] IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*
- [10] IEC 61025, *Fault Tree Analysis*
- [11] IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*
- [12] IEC 61160, *Formal design review*
- [13] IEC 61165, *Application of Markov techniques*
- [14] IEC 61709, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*
- [15] IEC 62308, *Equipment reliability – Reliability assessment methods*
- [16] IEC 62502, *Analysis techniques for dependability – Event tree analysis (ETA)*
- [17] IEC 62551, *Analysis techniques for dependability – Petri net techniques*
- [18] IEC 62308, *Equipment reliability – Reliability assessment methods*
- [19] IEC 62508, *Guidance on human aspects of dependability*
- [20] ISO 31000, *Risk Management*
- [21] ISO/IEC 31010, *Risk management – Risk assessment techniques*
- [22] ISO 9000:2000, *Quality management systems – Fundamentals and vocabulary*
- [23] 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.
- [24] Lars E. Lyberg et al [ed], *Survey Measurement and Process Quality*, Wiley & Sons, Inc. 1997
- [25] MIL-STD 338B, *Electronic Reliability Design Handbook*
- [26] 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*
- [27] SAE ARP5580:2001, *Failure Modes, Effects, and Criticality Analysis Procedures*

## Anhang A (informativ)

### Zuschnitt der FMEA

#### A.1 Allgemein

Moderne Einheiten und Prozesse sind so komplex, dass es oft nicht möglich ist die traditionelle Methode des FMEA zu nutzen die alle Komponenten und deren einzelne Ausfallarten nacheinander analysiert (z. B. „Bottom-up“-Analyse). Deshalb gibt es oft die Notwendigkeit, den Anwendungsbereich der FMEA auf einen Teil des Designs zu reduzieren (z. B. einige Bauteile, einige Prozeduren), oder die kritischen Funktionen zu analysieren um die kritischen Bauteile oder Prozeduren und deren Ausfallarten zu finden. (z. B. „Top-down“-Analyse).

In jeder Anwendung muss nicht ein einzelner Ansatz für alle analysierten Einheiten oder Prozesse anwendbar sein; deshalb wird mit dem folgenden Vier-Quadranten-Diagramm in Bild A.1 – Umgebungsquadrantendiagramm – Hilfestellung zur Wahl des am besten passenden Ansatzes für einen bestimmten Anwender und deren spezielle Nutzungsumgebung angeboten.

Jedes FMEA-Projekt kann aus einer Mischung von Analyse Kandidaten mit unterschiedlichem Nutzungsrisiko, Ausgereiftheit des Designs, angewandeter Technologie, Anwendung, Verantwortung für die schlussendliche Leistungsfähigkeit und Gewinnpotenzial bestehen. Es wird erwartet dass jeder Analyse Kandidat unter eine der Quadrantenmethoden oder den Defaultwert „keine Analyse erforderlich“ fällt.

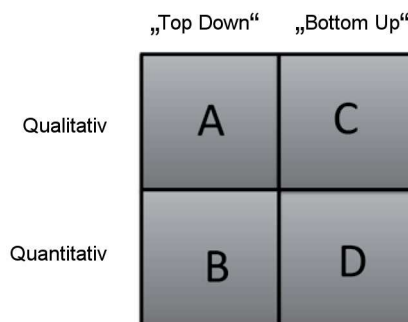


**Bild A.1 – Umgebungsquadrantendiagramm**

In Bild A.1 ist jeder Quadrant eine mögliche Option um den Ansatz einer FMEA zu bilden, dieser wird gewählt in Bezug auf die Nutzung und das inhärente Risiko eines bestimmten Analyse Kandidaten. Solch ein Kandidat kann sich auf jeder Ebene in der Hierarchie von Einheit oder Prozess befinden und die Nutzungsumgebung kann als Szenario beschrieben werden. Dieser Ansatz nimmt die Anforderung für einen Lieferplan vorweg, der die gewählte Methode aus der Liste der möglichen Kandidaten optimiert. Solch ein Plan kann eine Leistung sein, um den Nutzen der resultierenden Maßnahmen aufzuzeigen.

Der Quadrant ist so aufgebaut, dass er die zwei möglichen Ansätze um die Analyse zu entwickeln („Top-Down“ oder „Bottom-up“) mit den zwei möglichen Ansätzen um Risiko oder Auswirkung zu identifizieren, kombiniert. Es ist nicht nötig, die identifizierten Ausfälle in der Analyse einzustufen, aber es ist unüblich die Auswirkungen eines Ausfalles nicht zumindest einen Grad von Wichtigkeit zuzuordnen.

Die auf jedes Segment des Quadranten bezogenen Kriterien werden in den nächsten Absätzen behandelt.

## A.2 Kriterien für die Quadranten

### A.2.1 „Top-down“-Analyse

Der Begriff „Top-down“ bezieht sich auf das Konzept, dass eine Analyse so fortschreitet, dass die Funktionen oder Ziele der ganzen Einheit oder des ganzen Prozesses bestimmt werden, um danach die einzelnen Elemente zu untersuchen, damit die Ausfälle gefunden werden, welche den Verlust der Funktion oder die Abweichung von Zielen verursachen können.

Deshalb wird eine „Top-down“-Analyse meistens als funktionale Analyse realisiert, die dazu bestimmt ist den Aufwand auf die wichtigsten Anforderungen oder Funktionen zu fokussieren. Da dieser Ansatz die Betonung von spezifischen Interessenfeldern berücksichtigt wird er oft als kosteneffizient angesehen.

Die Durchführung einer solchen Analyse erlaubt eine Bewertung des Verlustes einer Funktion auf der Systemebene, schränkt aber die Ergebnisse auf eine Untersuchung, wie vorgegebene Ereignisse auftreten können, ein statt zu versuchen alle Ereignisse, die auftreten könnten zu bewerten. Deshalb wird dieser Ansatz verwendet, wenn spezielle Auswirkungen von Interesse sind und nur die Gründe einer Untersuchung bedürfen.

Dieser Ansatz benötigt eine Beurteilung, um den Punkt im Analysefluss zu finden, an dem die Weiterführung auf niedrigeren Ebenen wenig oder keine sinnvolle Information liefert, die wichtig für das Erreichen des Analysezieles wäre.

### A.2.2 „Bottom-up“-Analyse

Der Begriff „Bottom-up“ bezieht sich auf den Analyseprozess bei dem die Einheiten oder Schritte auf der Ebene des höchsten Detaillierungsgrades von System oder Prozess untersucht werden, um herauszufinden, wie diese ausfallen können und daraus auf die Auswirkungen zu schließen die diese Ausfälle auf höheren Ebenen in System oder Prozess haben.

Dieser Ansatz wird meist auf Hardwaresysteme bezogen bei denen das kleinste individuelle Bauteil des Systems analysiert wird und daraus auf die Auswirkungen von deren Ausfällen auf spezifischen höheren Systemebenen geschlossen wird.

Zur Durchführung dieser Art von Analyse ist keine Kenntnis der funktionalen Anforderungen auf Systemebene nötig weil der Verlust der Funktion auf Systemebene sich aus der Fortpflanzung der Ausfallauswirkung der Bauteile durch die Systemstruktur ergibt. Aus diesem Grund wird diese Methode meist bei neuen Designs benutzt wenn die Spanne von Auswirkungen auf höherer Ebene oder Systemebene nicht bekannt ist. Der Ansatz ist deshalb sehr geeignet für die Bestimmung aller möglichen Systemauswirkungen wenn eine komplett neue Zusammensetzung von Bauteilen oder existierenden Einheiten in eine neue Umgebung oder Anwendung eingebracht wird.

### A.2.3 Qualitativ und semi-quantitativ

Bei Durchführung einer Analyse wird die Schwere einer aufgestellten Ausfallauswirkung normalerweise gewichtet um die Ausfallursachen zu finden, die für die weitere Handlung oder Untersuchung priorisiert werden sollten. Die Einteilung wird oft erreicht durch die Zuweisung eines einfachen Wortes oder eines Satzes um den Schweregrad anzuzeigen, wie z. B. „geringfügig“, „schwerwiegend“ oder „katastrophal“. Die Wahrscheinlichkeit des Auftretens eines Ausfalles kann auch gänzlich qualitativ mit Worten wie „häufig“, „gelegentlich“ oder „unwahrscheinlich“ ausgedrückt werden.

Es ist nicht nötig, die exakte Bedeutung jeder Abstufung in einem komplett qualitativen Ansatz zu bestimmen, wo eine präzise Interpretation nicht nötig ist weil generell verstandene Bedeutungen ausreichend für den Zweck sind. Jede Form von mathematischer Kalkulation ist mit solchen Bewertungen außerdem unmöglich.

Dieser Ansatz wird oft zu einem semi-quantitativen Ansatz weiterentwickelt in dem eine spezifische messbare oder beobachtbare Eigenschaft mit jeder Stufe verknüpft wird. Zum Beispiel: ein Schweregrad „schwerwiegend“ kann mit der Auswirkung eines physischen Schadens mit Krankenhausaufenthalt verknüpft werden, oder eine Wahrscheinlichkeitseinstufung von „häufig“ kann mit einer Auswirkung verknüpft werden die min-

destens einmal im Monat erfolgt. In diesem Fall sieht es so aus als ob eine Kalkulation mit den Werten möglich wäre: aber dies ist nicht der Fall, da die Zuordnung allgemein auf breite Gruppierungen von Resultaten oder Auftreten basiert. Dieser Ansatz hat den Vorteil gegenüber rein qualitativen Einstufungen dass durch die Bereitstellung klarer Richtlinien zu der Bedeutung der Bezeichnungen ein höherer Konsistenzgrad erreicht wird

Der qualitative Ansatz hat seine Vorteile, wo die Einstufung von Ausfällen benötigt wird, aber detaillierte Information nicht verfügbar ist oder weil System oder Prozess ungenügend beschrieben sind um quantitative Daten zu verwenden.

#### **A.2.4 Quantitativ**

Ein quantitativer Ansatz zur Analyse bezieht sich allgemein nur auf Bewertung der Wahrscheinlichkeit eines Ausfalles mit der Nutzung von empirischen Daten. Er kann angewendet werden wenn Felderfahrung, Prüfdaten oder Vorhersagen verfügbar sind, die die Zuweisung einer Ausfallrate oder statistischen Wahrscheinlichkeit erlauben. Er kann für Schweregrade herangezogen werden wenn die betrachteten Auswirkungen so sind, dass Quantifizierung möglich und geeignet ist.

Ein quantitativer Ansatz wird generell benutzt, wenn betrachtete Einheiten eine gut bekannte Einsatzhistorie in der betrachteten Anwendung aufweisen.

#### **A.2.5 Keine Analyse notwendig**

Bei der Bestimmung von Einheiten oder Prozessen oder deren Grenzen für die Analyse sollte die Möglichkeit betrachtet werden, dass für einige Einheiten oder Prozesse keinen FMEA in irgendeiner Form benötigt wird; speziell wenn kein klar bestimmbarer Nutzen aus der Durchführung der Analyse ersichtlich ist. Die Option keinen FMEA jedweder Form durchzuführen zeigt das Unvermögen der Entwicklungsverantwortlichen, Nutzen aus FMEA zu ziehen.

Die FMEA gewinnt ihren geschäftlichen Wert als Erstes durch Beeinflussung des Designs und als Zweites durch die Bereitstellung von Information für die Entwicklung von kosteneffizienter präventiver oder korrigierender Instandhaltungsgrundsätze. Wenn die Resultate der Analyse das Design eines Entwurfs nicht beeinflussen können, wie z. B. bei COTS-Betriebsmitteln die verbreitet vertrieben werden oder das Instandhaltungsprogramm beeinflussen ist ein FMEA nicht gerechtfertigt.

In vielen Fällen können COTS-Systeme oder -Systemelemente von spezialisierten Ausrüstern nur als „Black Box“ behandelt werden, die nicht zufriedenstellend analysiert werden können.

Die Quadranten in Bild A.1 sind mit A, B, C und D bezeichnet und repräsentieren Methoden zum Erreichen der Analyseziele auf kosteneffizienteste Art durch Kombination von möglichen Strukturierungsansätzen und Risikobewertungsmethoden. Die folgenden Absätze bieten generelle Anleitung zur Zuordnung von Entwürfen zu Quadranten basiert auf die Eigenschaften der Risiken.

##### **A.2.5.1 Quadrant A**

Dieser Quadrant stellt eine qualitative „Top-Down“-Analyse dar, die üblicherweise in der frühen Phase einer Entwicklung eines Systems durchgeführt wird. Der Ansatz ermutigt zu einer kosteneffizienten Beurteilung, da er dem Analysten erlaubt aufzuhören, wenn eine Ebene erreicht wird auf der keine weitere Zerlegung möglich ist oder wenn das Wissen über Ausfallarten aus anderen Gründen nicht verfügbar ist.

Eine mögliche Anwendung ist eine kostengünstige Prüfung der Vertrauenswürdigkeit, dass ein definiertes Reglement zur OEM-Unterstützung für ein reifes Produkt den erwarteten Ausfallarten aus dem Design Rechnung trägt. Dies kann erreicht werden durch eine „Top-Down“-Analyse, die die Rückverfolgbarkeit zwischen definierten Instandhaltungsaufgaben und den Ausfallarten, die sie verringern oder verhindern, aufzeigt.

##### **A.2.5.2 Quadrant B**

Dieser Quadrant stellt die Anwendung eines „Top-Down“-Strukturierungsansatzes, jedoch mit einer quantitativen Bewertung, dar. Diese Kombination wird generell auf existierende, komplexe und oft gealterte Betriebs-

vermögen angewendet, bei denen quantitative Leistungswerte leicht verfügbar sind. Diese Anwendungsart wird benutzt wo:

- eine wesentliche Veränderung eines Systems die Integration von neuer Ausrüstung während der Entwicklung erfordert und ein kompletter Datensatz für andere Analysen erforderlich ist, z. B. RAM;
- Durchführung einer zuverlässigkeitsorientierten Instandhaltung oder gleichwertiger, risikobasierter Techniken um vorhandene Instandhaltungs- und Logistikpraktiken zu rechtfertigen und / oder zu verbessern.

Dieser Ansatz ermutigt den Analysten wieder, auf eine vertragliche Ebene hinunter zu gehen, die den Zweck der Analyse darstellt, z. B. auf COTS-Ebene.

#### **A.2.5.3      Quadrant C**

Dieser Quadrant stellt die Anwendung von qualitativer Beurteilung dar, beginnend auf der niedrigsten Ebene von Teilen aus denen das System besteht. Solche Analysen werden generell vereinbar bei der Entwicklung von neuen Systemen, bei denen die Architektur bekannt und die Handlung auf die Identifikation von Designverbesserungsmöglichkeiten durch Einstufung von Arten und Auswirkungen ausgerichtet ist.

Analysen dieser Art sind langatmig und kostspielig und generell nur da zu rechtfertigen, wo es um große Produktionsmengen eines speziellen Systems oder von Ausrüstung geht die einen Ertrag aus der investierten Anstrengung wahrscheinlich machen.

#### **A.2.5.4      Quadrant D**

Dieser Quadrant stellt eine quantitative Beurteilung dar, die auf der niedrigsten Ebene der Einheits- oder Prozesshierarchie beginnt. Solche Analysen werden oft bei der Komplettierung eines Entwicklungsvorganges benötigt um die Erfüllung der Design-Spezifikation zu demonstrieren und detailliertes Material zur Verfügung zu stellen, das von anderen Analysten wie für Sicherheitstechnik oder Logistikunterstützung verwendet wird. Eine Analyse dieser Art ist langatmig und generell nur gerechtfertigt wo große Produktionsmengen oder schwere Risiken eines speziellen Systems oder Ausrüstung einen Profit aus der investierten Anstrengung wahrscheinlich machen.

### **A.3      Risikoeigenschaften**

Die folgenden Abschnitte diskutieren die Themen, die berücksichtigt werden müssen, wenn der kosten-effizienteste Quadrant gewählt wird. Der Zweck ist, diese Information zu nutzen um zuerst zu bewerten, ob eine FMEA unternommen werden sollte und, wenn ja, zu bewerten, welche Sorte von Analyse bezogen auf „Top-Down“ oder „Bottom-up“ und qualitativ oder quantitativ verwendet werden soll.

Eine gute FMEA kann signifikante Kosten verursachen. Die einzubeziehenden geschäftlichen Ziele für die Analyse müssen deshalb klar und der Wert eingeschätzt sein.

Die Entscheidung darüber, ob eine FMEA durchgeführt wird, und, wenn ja, die Entscheidung über den gewählten Quadranten, können von rechtlichen oder vertraglichen Anforderungen oder der potenziellen Notwendigkeit eine effektive gesetzliche Verteidigung sicherzustellen beeinflusst werden.

#### **A.3.1      Verwendung**

Schlüsselfaktoren für die Auswahl einer FMEA sind:

- wurde die Einheit schon zuvor von der Organisation verwendet?
- sind Daten aus der Verwendung verfügbar die den Zweck der Analyse befriedigen?
- spiegeln die Betriebskonfiguration und der Kontext genau die bestimmungsgemäße Nutzung des analysierten Entwurfs wider?

Der zu analysierende Entwurf mag in vorhandenen Umgebungen betrieben und auf potenzielle Verbesserungen analysiert werden oder mag Daten aus ähnlichen Betriebsanwendungen nutzen, wenn der Entwurf zum ersten Mal gekauft wird. Diese unterschiedlichen Situationen geben den Grad der Unsicherheit bezüglich den

in der Analyse genutzten Ausfalls- und Zuverlässigkeitsdaten wider. Neue Ausrüstung betreffende Daten sollten überprüft werden um die Annahme von Ähnlichkeiten zu bestätigen. Bei analysierten Entwürfen in Massenproduktion, commercial-off-the-shelf (COTS)-Einheiten, die von verschiedenen Kunden und potenziell über viele Industrien genutzt werden, kann es sein, dass keine FMEA-Daten vom OEMs verfügbar sind. In diesen Fällen hat eine FMEA geringen Wert, mit Ausnahme dass sie ein Mittel ist um einiges Vertrauen in das vom OEM bereitgestellte Instandhaltungsprogramm zu gewinnen. In diesem Fall wird das COTS als „Black Box“ betrachtet und muss die niedrigste Ebene (Bauteil) der Analyse in der FMEA darstellen.

### A.3.2 Reife des Designs

Reife bezieht sich sowohl auf Projektreife (Fortschritt des Projektes über den Lebenszyklus) als auch auf Reife des Designs.

In der Konzeptphase, wenn die höchste Architekturebene reift, bieten funktionale „Top-Down“-Ansätze die Möglichkeit, Ausfallarten auf höchster Ebene zu identifizieren, die die Auswahl dieser Architektur unterstützen. Während das Design über das Konzept zum detaillierten Design reift verschiebt sich der Schwerpunkt bei der Wahl aus existierenden Design oder Produkten in Richtung eines „Bottom-up“-Ansatzes. Der Ausgangspunkt für eine solche „Bottom-up“-Analyse hängt üblicherweise davon ab, dass der Ausgangspunkt durch eine funktionale „Top-down“-Analyse ausgewählt wurde.

Das Design kommerzieller Systeme oder Systemelemente auf dem Markt entwickeln sich oft über die Zeit, oft über Jahrzehnte, durch fortschreitende Wellen von Veränderungen und Entwicklung, die die Zuverlässigkeit verbessern. Solche reifen Designs haben zum Beispiel keine formale FMEA verfügbar, weil sie sich vor der allgemeinen Akzeptanz des Wertes von FMEA oder ohne Nutzung eines auf FMEA beruhenden Verbesserungsprozesses entwickelt haben.

Solche reifen Designs haben oft bekannte Zuverlässigkeitskennwerte und bereitgestellte Instandhaltungsprogramme die diese Leistungsfähigkeit bieten. Die Durchführung einer detaillierten FMEA könnte keinen oder kleinen Einfluss auf entweder Design oder Instandhaltungsprogramm haben.

Unreife Designs werden oft charakterisiert von kürzlichen Innovationen in Architektur oder der Anwendung von neuartigen Materialien und Teilen um verbesserte Fähigkeiten und / oder Kosteneffizienz zu erreichen. Von OEMs sollte erwartet werden dass sie formale FMEA verfügbar haben zur Einbindung in das Gesamtsystem oder das Programm des Endproduktes. Die fehlende Verfügbarkeit einer FMEA für solche Designs könnte ein Grund sein um zusätzliche Handlungen vorzunehmen um eine benötigte Leistungsfähigkeit sicherzustellen. Unreife Designs könnten unter Benutzung von reifen oder unreifen Komponenten gemacht worden sein. Die wird die Ausdehnung der FMEA beeinflussen.

### A.3.3 Verwendete Technologie

Neue Technologien oder neuartige Anwendungen von existierender Technologie werden oft von signifikantem Risiko bezüglich der Leistungsfähigkeit begleitet. Die Beurteilung und Beherrschung solcher technologiebezogenen Risiken kann durch formale FMEA belegt werden, wenn möglich in sowohl „Top-down“ als auch „Bottom-up“-Form, während das Projekt von Konzept nach kompletierter Ingenieurentwicklung von Systemelementen oder detailliertem Design im Fall von Systemen voranschreitet. Detaillierte „Bottom-up“-FMEA dürfen semi-quantitativ oder quantitativ sein.

Reife Technologien sind ähnlich in ihrer Beschaffenheit zu reifen Designs. Langzeitentwicklungen können den Entwicklungspfad unklar werden lassen und es kann an Vollständigkeit von Funktionsbeschreibungen für System und Systemelemente mangeln. Eine nützliche Prüfung für die Notwendigkeit einer FMEA wird die Möglichkeit, das Design zu beeinflussen, die möglichen Fähigkeiten zu beurteilen und die Instandhaltung und damit verbundene integrierte Notwendigkeiten für Unterstützung zu überprüfen, sein.

### A.3.4 Anwendung

Der Grad und die Beschaffenheit des Risikos das mit der Anwendung des Entwurfes einer Einheit verbunden ist wäre eine Schlüsselbetrachtung in der Wahl der Methode der FMEA. Sicherheitskritische Systeme können demonstrierbare Beweise erfordern, dass sie entweder entwickelt oder ausgewählt wurden in einer Weise die transparent das Risiko eines Ausfalles aufzeigt, analysiert, bewertet und behandelt.

Der gewählte Quadrant muss Rückverfolgbarkeit der Risikobehandlung unterstützen, verbunden mit dem Nachweis dass die benutzte Methode für den Kontext geeignet ist.

## A.4 Unterstützung

Die praktische Anwendung des Quadrantenansatzes wird unten für diejenigen beschrieben, die Unterstützung für die Auswahl und Begründung zu den angewendeten unterschiedlichen Ansätzen innerhalb eines Projektes suchen.

### A.4.1 Kontext der Nutzung von Szenarien zur Auswahl eines Quadranten

Tabelle A.1 soll Beispiele zur Auswahl geeigneter Quadranten für Umstände, die in jeder der oben angegebenen Betrachtungen und derjenigen die in Abschnitt 5.2.5 diskutiert wurden zur Verfügung stellen.

**Tabelle A.1 – Beispiele von Szenarien zur Auswahl von Quadranten**

|   | Lebensphase          | Designreife / Technologie       | Designquelle              | Anwendung          | Designverantwortlichkeit      | Mehrwert-Potenzial        | Quadrant        |
|---|----------------------|---------------------------------|---------------------------|--------------------|-------------------------------|---------------------------|-----------------|
| 1 | Detailliertes Design | Reif und gut verstanden         | Vielfach verwendetes COTS | Bestehendes Design | Kein Designverantwortlicher   | Nicht anwendbar           | Nicht anwendbar |
| 2 | Detailliertes Design | Neues Design & neue Technologie | Speziell angefertigt      | Neues Design       | Designverantwortlicher        | Hoch (Risikominderung)    | D               |
| 3 | Detailliertes Design | Reif & etwas neue Technologie   | Vielfach verwendetes COTS | Bestehendes Design | System-Designverantwortlicher | Hoch (ILS)                | B               |
| 4 | Konzept              | Neues Design und gut verstanden | N/A                       | Neues Design       | System-Designverantwortlicher | Hoch (Leistungsfähigkeit) | A               |
| 5 | Vorläufiges Design   | Neues Design & neue Technologie | Speziell angefertigt      | Neues Design       | Designverantwortlicher        | Hoch (Leistungsfähigkeit) | C               |
| 6 | Detailliertes Design | Neues Design & neue Technologie | Speziell angefertigt      | Neues Design       | Designverantwortlicher        | Hoch (Leistungsfähigkeit) | D               |

## Anhang B (informativ)

### Beispiele von Inhalten des FMEA-Berichtes

Der FMEA-Bericht sollte das Ziel der Analyse und des zugeschnittenen Resultates widerspiegeln. Es gibt kein allgemeingültiges Berichtsformat. Der Bericht muss nicht notwendigerweise in irgendeinem Format dargestellt sein, wie es in den Beispielen in Anhängen D, E und F gegeben ist.

Der Bericht sollte alle analysierten Einheiten oder Prozesse auflisten, die potenziellen Ausfallarten und deren übergeordnete Auswirkung sowie mögliche Einstufung von Auswirkungen bezüglich Kritikalität, sofern eine Kritikalitätsanalyse durchgeführt wurde.

Es existieren kommerzielle Softwarepakete die Berichte zu Resultaten einer FMEA erstellen.

Wenn ein datenbankbasiertes Informationssystem vorhanden ist, dann kann die FMEA eine Datei sein, die die folgenden Datenbanken verknüpft:

- Die Liste der Vorgaben;
- Die Stückliste (Materialliste);
- Die Liste der für Bauteile und Produkte der Firma relevanten Ausfallarten;
- Die Liste der Handlungen (Handlungsdatenbank).

Bild B.1 zeigt wie ein datenbankbasiertes Informationssystem strukturiert sein könnte. Ein Vorteil dieser Datenbankmethode ist, dass Informationen nicht mehrfach eingegeben werden und dass es einfacher ist die FMEA auf neuestem Stand zu halten während das Projekt voranschreitet und Änderungen auftreten.

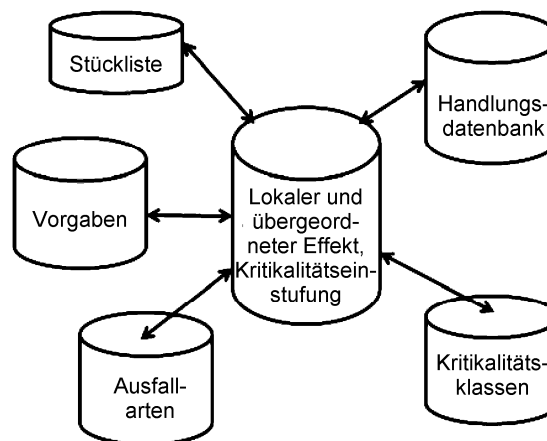


**Bild B.1 – Ein FMEA-Bericht basiert auf Verknüpfungen zwischen Datenbanken**

## Anhang C (informativ)

### Kritikalitätsbeurteilungsmethode

#### C.1 Allgemein

Für spezifische Industrien und Anwendungen wurde eine große Vielfalt von Kritikalitätsbeurteilungsmethoden entwickelt. Die folgenden Abschnitte beschreiben zwei allgemeine Ansätze, die die grundlegenden Prinzipien hinter den in der Industrie gebräuchlichen Methoden zusammenfassen.

#### C.2 Matrix-Methoden

##### C.2.1 Allgemein

Die Analysemethode der Kritikalitätsmatrix ist eine Risikobewertungsmethode, die qualitative oder semi-quantitative Einstufungen benutzt. Eine Anzahl diskreter Kategorien wird sowohl mit Wahrscheinlichkeit als auch Schweregraden verbunden die dann in eine Matrix wie in Bild C.1 gezeigt übertragen werden. Den Zellen in der Matrix wird dann ein Kritikalitätsgrad zugeordnet, der benutzt wird um die durchzuführenden Handlungen zu beurteilen und über die Festlegung der Handlungen zu informieren.

##### C.2.2 Kategorisierung der Auswirkungen

Die Arten von Auswirkungen und deren Schwere sollte in Begriffen definiert werden, die relevant für die betrachtete Einheit oder den betrachteten Prozess sind und die in eine ausreichende Anzahl von Kategorien unterteilt sind, um zu ermöglichen, dass in die komplette Bandbreite von Auswirkungen eingestuft und geeignet separiert wird. Dies wird im Detail in Abschnitt 5.2.5.2 beschrieben.

Die Auswahl der Beschreibungen der Skalenwerte und ihre Bedeutungen sollten, unter Beachtung der Art und Weise in welcher sie benutzt werden sollen, sorgfältig bedacht werden. Wo eine Expertenmeinung genutzt werden soll, sollte Sorgfalt angewendet werden in die Wahl von verbalen Beschreibungen oder Skalenwerten oder Buchstaben, da diese in sich die während der Analyse getroffene Auswahl beeinflussen kann. Es existieren akademische Studien welche dieses Thema erörtern [15].

Die Schwere der Auswirkung wird üblicherweise in zumindest vier Abstufungen von maximal glaubwürdiger Auswirkung bis zur kleinsten Auswirkung von Interesse eingestuft.

ANMERKUNG Zum Beispiel:

Kategorie 1: „Katastrophal“ (z. B. Ausfall der zum Tod von Personal führt);

Kategorie 2: „Schwerwiegend“ (z. B. Ausfall der zu einer Einweisung ins Krankenhaus führt);

Kategorie 3: „Geringfügig“ (z. B. Ausfall der zu Verletzungen die im Krankenhaus behandelt werden müssen führt);

Kategorie 4: „Unbedeutend“ (z. B. Ausfall der zu einer Verletzung führt die nicht mehr als erste Hilfe erfordert).

Für einige Analysen können mehr Abstufungen nötig sein um zwischen bedeutungsvollen Abstufungen von Auswirkungen unterscheiden zu können, jedoch sind weniger als diese selten erforderlich, da die Beschreibungen zu allgemein für eine praktische Nutzung werden.

Die Benutzung von numerischen Kategorien hat keine mathematische Bedeutung, ebenso wie die Reihenfolge in der sie zugeteilt werden. Ein sinnvolles Einteilungssystem kann in der Organisation schon bestehen und sollte bei der Anwendung berücksichtigt werden.

### C.2.3 Wahrscheinlichkeitskategorisierung

Die Wahrscheinlichkeit jeder Ausfallart wird in Bänder entsprechend der Wahrscheinlichkeit, Frequenz oder andere Wahrscheinlichkeitsmaße eingeteilt. Die Definition jeden Bandes und der Anzahl benötigter Bänder ist abhängig von der analysierten Einheit und deren Nutzungskontext.

Die Beschreibung der Wahrscheinlichkeitsbänder kann verwendbare Zuverlässigkeitsdaten oder andere Daten, Expertenurteile des Entwicklungsteams oder andere Methoden nutzen. Welcher Ansatz auch benutzt wird, es ist wesentlich dass er konstant verfolgt wird damit die relative Frequenz der Ausfallarten präzise eingeschätzt wird und kompatibel mit verfügbaren Daten ist.

Die Anzahl von Bändern und die Bedeutung jeden Bandes sollte entsprechend den Bedürfnissen der Organisation und des Bereiches von Ausfallwahrscheinlichkeiten festgelegt werden, die im Kontext der Anwendung der FMEA erwartet werden. Allgemein sollte eine numerische Erklärung der Beschreibung der Bänder, die relevant sind für den Bereich von Wahrscheinlichkeiten, die in der gegebenen Anwendung erwartet werden, betrachtet werden.

**ANMERKUNG** Zum Beispiel kann bei hochverfügbaren Hardwaresystemen die Kategorie „häufig“ für die Ausfallart eines Elementes gleich einem Fehler in mehreren Jahren sein während bei einem weniger zuverlässigen System ein „häufig“ auftretender Ausfall eines Elementes mehrmals im Jahr auftreten kann.

### C.2.4 Kritikalitätskategorisierung

Kritikalitätskategorien werden in Hinsicht auf eine Kombination von Schwere- und Wahrscheinlichkeitskategorien festgelegt. Die einfachste und allgemeinste Art die Kombination von Schwere und Wahrscheinlichkeit anzugeben ist in Form einer Matrix. Bild C.1 zeigt ein Beispiel einer Matrix.

Zu jeder Kritikalitätszahl werden Handlungsebenen verknüpft; siehe Abschnitt 5.2.5.2. Die Abstimmung von Kritikalitätskategorien auf jede Zelle in der Kritikalitätsmatrix sollten als Teil des Festlegungsprozesses unternommen werden.

Es ist unverzichtbar die Bedeutung jeder Kritikalitätszahl und die Handlungen, die mit ihnen verbunden sind, zu diskutieren und mit den betroffenen Parteien vor der Analyse abzustimmen. Das gibt ein klares und eindeutiges Verständnis wie Ausfallarten behandelt werden sollten und der potenziellen geschäftlichen Auswirkungen dieser Entscheidungen. Eine Unterlassung stellt den Wert der Analyse in Frage und kann durch überflüssige Aktivitäten oder das Unvermögen, Ausfälle angemessen zu behandeln, wesentlich Zeit und Kosten verursachen.

Die Kritikalität einer Ausfallart wird normalerweise in mindestens drei Stufen ausgedrückt, um eine sinnvolle Einteilung zu erlauben. Die Anzahl benötigter Stufen wird von Anforderungen der Organisation und der Anwendung der Analyse bestimmt.

**ANMERKUNG** Ein Beispiel einer Kritikalität in vier Ebenen wäre:

1. „Inakzeptabel“
2. „Unerwünscht“
3. „Akzeptabel“
4. „Unbedeutend“

Wie bei Schwere- und Wahrscheinlichkeitseinstufungen hat die numerische Klassifizierung der Kritikalitätszahlen keine Bedeutung und die Beschaffenheit der bestimmten Kritikalitätskategorie sollte angemessen für die Anwendung sein. Ähnlich sollte die Reihenfolge in der die Wahrscheinlichkeitskategorien und Schweregrade dargestellt werden können in einer Form sein, die innerhalb der Organisation direkt verstanden werden können.

**ANMERKUNG** Zum Beispiel könnte die Schwereskala wie in Bild C1 gezeigt auf ansteigende Schwere von links nach rechts umgekehrt werden, so dass ansteigendes Risiko von unten links nach oben rechts steht.

In der Beispielmatrix in Bild C1 steigt das Risiko das mit jeder Kritikalitätskategorie verbunden wird von unten rechts in der Matrix nach oben links an. Allerdings hängen die vorgenommenen Handlungen für jede Ausfallart nur von der Kritikalitätseinstufung und nicht von der „Zelle“ der Matrix ab. Deshalb muss eine ausreichende Zahl von Kategorien festgelegt werden um eine klare Unterscheidung zwischen benötigten Handlungen zu erlauben. Es sollte angemerkt werden, dass, obwohl Begriffe wie „Akzeptabel“ benutzt werden können, nicht impliziert werden kann, dass keine weitere Handlung benötigt wird.

| Auswirkung         |   | Katastrophal | Schwerwiegend | Marginal | Unbedeutend |
|--------------------|---|--------------|---------------|----------|-------------|
| Wahrscheinlichkeit |   | 1            | 2             | 3        | 4           |
| Häufig             | A | X            | X             | 1        | 2           |
| Wahrscheinlich     | B | X            | X             | 1        | 2           |
| Gelegentlich       | C | X            | X             | 1        | 2           |
| Unwahrscheinlich   | D | X            | 1             | 1        | 2           |
| Unbedeutend        | E | 1            | 2             | 2        | 3           |

**Bild C.1 – Beispiel einer Kritikalitätsmatrix**

**ANMERKUNG** Dies ist nur ein Beispiel der Struktur einer Matrix und sollte nicht als eine festgelegte Form angesehen werden. Die tatsächliche Form wird von Zweck und Kontext der Anwendung abhängen. Andere Beispiele werden in Anhang D, E und F gezeigt.

### C.3 Risikoprioritätszahl

Die auf Risikoprioritätszahl (RPZ) basierten Methoden werden allgemein als von drei Parametern abgeleitet angesehen: Schwere, Auftretensfrequenz und Aufdeckungsmöglichkeit, was für manche Anwendungen dazu führt, dass von der SOD-Methode gesprochen wird.

Die RPZ wird üblicherweise für jede identifizierte Ausfallart berechnet und ist ein Produkt der drei Kategorien von Schwere, Auftretensfrequenz und Aufdeckungsmöglichkeit.

$$R = S \times O \times D$$

Die Skala für die RPZ hängt von den Skalen der drei Parameter ab, wobei diese Werte fast immer ordinale Bewertungsskalen von 1 bis 10 benutzen, was eine kombinierte RPZ-Skala von 1 – 1 000 entstehen lässt.

Die Schweregrade für S, O und D werden über Tabellen bestimmt, in denen jede Einstufungen mit einem beschreibenden Satz verknüpft wird, der den Analysten in der Wahl des Ranges unterstützt. Es ist wesentlich, dass die Skalen gleichmäßig angewendet werden, damit die Parameter exakt und konsistent eingeschätzt werden.

Der Wert für die Wahrscheinlichkeit eines Auftretens wird allgemein je nach verfügbarer Information unter Nutzung anwendbarer Zuverlässigkeitsdaten, Expertenurteilen oder anderen Methoden gewählt. Die Einstufung wird allgemein auf Urteile basiert, da die Analyse häufig durchgeführt wird bevor berechnete oder getestete Werte vorhanden sind. Die Einstufung beginnt üblicherweise bei „kein Ausfall“ (1) und endet mit „hohe Wahrscheinlichkeit eines Ausfalles“ (10); allerdings hängt sie von analysierter Einheit oder analysiertem Prozess und deren Betriebsumgebung ab.

Die Aufdeckungsmöglichkeitszahl D kann die Leichtigkeit darstellen mit der eine Ausfallart während des Betriebs auftreten kann, bevor ein wesentlicher Fehlereffekt auftritt.

Es sollte angemerkt werden dass eine RPZ-Bewertung subjektiv ist, da sie ein Produkt aus drei Zahlen ist, die normalerweise selbst subjektiv sind.

Der Vergleich der RPZ-Werte vor und nach Änderungen in einem Design, der Betriebsumgebung oder der Möglichkeiten zur Aufdeckung kann genutzt werden, um eine qualitative Indikation der erreichten Verbesserung zu liefern.

Obwohl die RPZ-Methode einfach und intuitiv ist sollte bedacht werden, dass wegen der ordinalen Skalen die Ergebnisse nicht die relative Wichtigkeit der Ausfallarten anzeigt, nur dass eine größer oder kleiner als die andere ist. Die Anordnung der Ränge wird auch beeinflusst davon wie die Skalen aufgesetzt wurden. Die selbe RPZ kann oft mit mehreren Kombinationen von zusammengesetzten Werten erreicht werden und die relative Wichtigkeit dieser Zusammensetzungen beachtlich variieren. Dies kann die Möglichkeit, aus dem Vergleich der RPZ-Werte eine Bedeutung abzuleiten, wesentlich beeinflussen.

Wenn Schlüsse aus einem RPN-Wert oder aus dem Vergleich der Werte gezogen werden sollte Folgendes in Erwägung gezogen werden:

- a) Die RPZ-Skala ist nicht kontinuierlich. Zum Beispiel bleibt mit Skalen von 1 bis 10 88% des Wertebereiches leer, und nur 120 von 1 000 Zahlen werden generiert da RPZ-Werte doppelt vorkommen.
- b) Relative Beziehungen zwischen Werten haben keine Bedeutung. Dies ist das Ergebnis daraus dass die Skalen ordinal sind. Deshalb könnten die Unterschiede in RPZ-Werten vernachlässigbar erscheinen aber signifikant sein. Zum Beispiel können die Werte  $S = 6$ ,  $O = 4$  und  $D = 2$  eine RPZ von 48 ergeben, während  $S = 6$ ,  $O = 5$  und  $D = 2$  einen Wert von 60 ergeben. Der zweite Wert ist nicht nur leicht höher, während  $O = 5$  eine 5 mal höhere Auftrettsfrequenz als bei  $O = 4$  bedeuten kann.
- c) Ähnlich kann die RPZ empfindlich auf kleine Änderungen in Parametern sein. Eine kleine Änderung in einem Faktor hat eine offenbar viel größere Auswirkung wenn die anderen Faktoren groß sind gegenüber wenn diese Werte klein sind. (Beispiel:  $9 \times 9 \times 3 = 243$  und  $9 \times 9 \times 4 = 324$  gegenüber  $3 \times 4 \times 4 = 36$  und  $3 \times 4 \times 4 = 48$ ).

Deshalb benötigt ein Review einer RPZ Vorsicht und gutes Urteilsvermögen. Eine gute Ausführung würde ein sorgsames Review der Werte für Schwere, Auftrettsfrequenz und Aufdeckungsmöglichkeit bevor eine Meinung geformt und korrektive Maßnahmen getroffen werden. Außerdem gibt es Wege um die zuvor beschriebenen Mängel der RPZ-Methode zu umgehen (siehe z. B. [15]).

ANMERKUNG Anhang F bietet spezifische Hilfestellung zur Erstellung einer Kritikalitätsanalyse für die Automobilindustrie.

## Anhang D (informativ)

### Beispielvarianten von FMEA

#### D.1 Allgemein

Während der allgemeine Teil dieser Norm die generischen Eigenschaften der FMEA-Methode beschreibt, existieren einige Varianten die ermöglichen auf spezielle Arten von untersuchter Einheit oder Prozess konkreter einzugehen. Des Weiteren gibt es Anpassungen der allgemeinen FMEA-Methode die auf die Bedürfnisse von bestimmten Industrien oder Organisationen passen, oder die bestimmte Zwecke der Analyse unterstützen.

In diesem informativen Anhang werden mehrere Varianten von generischen FMEA-Methoden beschrieben. Diese können bestimmte Anforderungen bezüglich der Kritikalitätsbeurteilung haben (z. B. Sicherheitstechnik und Automobilindustrie-FMEA), oder Kompatibilität mit spezifischen Normen sicherstellen (z. B. FMECA innerhalb einer RCM). In Betracht gezogen wird auch die Nutzung von FMEA für komplexe Systeme wo Risiko über Module und Komponenten verteilt ist.

#### D.2 Software-FMEA

Ein Software-FMEA unterscheidet sich von Hardware-FMEA weil Software nicht greifbar ist. Um Software zu analysieren, müssen ihre Funktion und das Fehlen der Funktion bewertet werden. Deshalb muss der Software-FMEA die Software betrachten, wie sie in der relevanten Hardware funktioniert.

Wie die Hardware wird die Software in verschiedene Ebenen zerlegt, z. B. Softwaremodule und Softwarekomponenten. Für jede analytische Instanz muss die Analyse die Eingänge, die Verarbeitung und den Ausgang betrachten. Die Verarbeitung hängt ab von Startbedingungen am Eingang (z. B. Position in einer Menüstruktur, Inhalt von Registern und Speicher, RAM-Speicher als auch ROM-Speicher). Fehler können in Eingängen (z. B. ungültige oder beschädigte Daten), in Startbedingungen (z. B. falsche Position im Menü, falsche oder beschädigte Inhalte von Speicher, falsche Verarbeitung (z. B. in Algorithmen) oder in Ausgängen (beschädigter Ausgang oder ungültige Daten) auftreten. Siehe auch Abschnitt 5.3.5.4 für Beispiele von möglichen Fehlern in Software. Schließlich kann der Softwareausgang Probleme verursachen bei Interaktion mit der Hardware, z. B. bei Timing-Problemen. Deshalb müssen Analysten, die die zu analysierende Software kennen als auch Analysten, die die Hardware kennen gemeinsam an der FMEA teilnehmen.

#### D.3 Prozess-FMEA

FMEA können auch auf Prozesse und Prozeduren angewendet werden. Die FMEA-Methode ist die Gleiche wie für Hardware- oder Software-Einheiten. Allgemein ist der Ausgangspunkt für die Analyse das Prozess-Flussdiagramm, die Arbeitsschrittstruktur oder Aufgabenanalyse. Der Prozess wird zerlegt in Elemente, die die Schritte des Prozesses darstellen. Der Grad der Zerlegung wird gewählt, damit sie auf die Anwendung passt. Die Funktion jedes Schrittes oder das benötigte Ergebnis wird ausreichend konkret definiert mit einer Beschreibung der Funktion aus der der Grad der Leistungsfähigkeit, die einen Ausfall darstellt ersichtlich ist. Wie bei FMEA für Hardware- oder Software-Einheiten, werden die Arten, in welcher die Prozessfunktion nicht erreicht werden könnte, als Ausfallarten in der Prozess-FMEA aufgelistet. Ausfallauswirkungen, Mechanismen und mögliche Ausfallgründe werden ebenfalls definiert. Ausfallmechanismen und Gründe umfassen beide, menschliches Versagen und Hardware-Fehler. Kritikalitätsanalysen können genau wie in der allgemeinen Anleitung zu FMEA beschrieben angewendet werden.

Prozess-FMEA wurden zuerst auf Herstellungsprozesse angewendet, wird heute aber auf weiteren Gebieten angewandt, z. B. wird sie verbreitet für die Analyse von medizinischen Prozeduren in Pflegediensten eingesetzt.