

DIN EN 60812

ICS 21.020; 29.020

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

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

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

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

Gesamtumfang 48 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Beginn der Gültigkeit

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

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

Nationales Vorwort

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

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

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

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem auf der IEC-Website unter „<http://webstore.iec.ch>“ mit den Daten zu dieser Publikation angegebenen Datum (maintenance result date) unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

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

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

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

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

Änderungen

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

- a) Betrachtung von Ausfällen mit gemeinsamer Ursache;
- b) Einbeziehung menschlicher Einflüsse;
- c) Behandlung von Softwarefehlern;
- d) Einführung des Konzeptes von Fehlzustandsart-Auswirkungen und -Kritizität;
- e) Einbeziehung von in der Autoindustrie verbreitet genutzten Methoden;
- f) Ergänzte normative Verweisungen und Zusammenhänge mit anderen Fehlzustandsart-Analyse-Methoden;
- g) ergänzte Beispiele;
- h) Behandlung von Vorteilen und Nachteilen unterschiedlicher FMEA-Methoden.

Frühere Ausgaben

DIN 25448: 1980-06, 1990-05

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

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

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

Diese Europäische Norm wurde von CENELEC am 2006-03-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

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

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

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

CENELEC

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

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

© 2006 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 60812:2006 D

Vorwort

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

Diese Europäische Norm ersetzt HD 485 S1:1987.

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

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

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2006-12-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2009-03-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

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

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

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

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

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

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

Inhalt

	Seite
Vorwort	2
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Überblick	6
4.1 Einleitung	6
4.2 Zweck und Ziele der Analyse	8
5 Fehlzustandsart- und -auswirkungsanalyse (FMEA)	8
5.1 Allgemeine Betrachtungen	8
5.2 Vorausgehende Arbeiten	9
5.3 Ausfallbedeutungsanalyse (FMECA)	17
5.4 Bericht über die Analyse	26
6 Weitere Betrachtungen	27
6.1 Ausfälle mit gemeinsamer Ursache	27
6.2 Menschliche Einflüsse	28
6.3 Softwarefehler	28
6.4 FMEA bezüglich der Folgen eines Systemausfalls	28
7 Anwendungen	29
7.1 Anwendung von FMEA und FMECA	29
7.2 Vorteile der FMEA	30
7.3 Grenzen und Unzulänglichkeiten der FMEA	31
7.4 Beziehungen zu anderen Verfahren	31
Anhang A (informativ) Zusammenfassung der Verfahrensschritte für FMEA und FMECA	33
A.1 Schritte zur Durchführung der Analyse	33
A.2 FMEA-Arbeitsblatt	33
Anhang B (informativ) Analysebeispiele	37
B.1 Beispiel 1 – FMEA für ein Teil einer Automobilelektronik mit Berechnung der Risikoprioritätszahl	37
B.2 Beispiel 2 – FMEA für Teilsystem eines Motor-Generator-Satzes	40
B.3 Beispiel 3 – FMECA für einen Herstellprozess	43
Literaturhinweise	45
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	46
Bild 1 – Zusammenhang zwischen Ausfallarten und Ausfallauswirkungen in einer Systemhierarchie	11
Bild 2 – Ablaufdiagramm für die Analyse	17
Bild 3 – Kritizitätsmatrix	21
Bild A.1 – Beispiel für das Format eines FMEA-Arbeitsblattes	36
Bild B.1 – FMEA für ein Teil der Automobilelektronik mit Berechnung der Risikoprioritätszahl	39

	Seite
Bild B.2 – Diagramm der Teilsysteme eines Motor-Generator-Satzes.....	40
Bild B.3 – Diagramm der Systeme „Heizung, Lüftung und Kühlung des Gehäuses“	41
Bild B.4 – FMEA für Teilsystem 20	42
Bild B.5 – Teil einer Prozess-FMECA für Aluminiumstrangpressen	44
Tabelle 1 – Beispiel eines Satzes allgemeiner Ausfallarten	13
Tabelle 2 – Erläuterndes Beispiel einer Schwere-Klassifizierung für Endauswirkungen	16
Tabelle 3 – Risiko-/Kritizitätsmatrix.....	22
Tabelle 4 – Schwere der Ausfallart.....	23
Tabelle 5 – Auftreten der Ausfallart in Bezug auf Eintrittshäufigkeit und -wahrscheinlichkeit.....	24
Tabelle 6 – Beurteilungskriterien für die Ausfallarterkennung	25
Tabelle 7 – Beispiel für Ausfallauswirkungen (für einen Kfz-Anlasser)	26
Tabelle 8 – Beispiel für Wahrscheinlichkeiten von Ausfallauswirkungen	27
Tabelle B.1 – Definition und Klassifizierung der Schwere der Auswirkungen von Ausfällen auf das gesamte M-G-System.....	40

1 Anwendungsbereich

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

- die zur Durchführung einer Analyse notwendigen Verfahrensschritte bereitgestellt werden,
- geeignete Benennungen, Voraussetzungen, Maßgrößen für die Bedeutung (Kritizität) sowie Fehlzustandsarten genannt werden,
- grundlegende Prinzipien erklärt werden,
- Beispiele für die notwendigen Arbeitsblätter oder andere Tabellenformen bereitgestellt werden.

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

2 Normative Verweisungen

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

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

IEC 61025, *Fault tree analysis (FTA)*

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

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

(Betrachtungs-)Einheit

Teil, Komponente, Gerät, Subsystem, Funktionseinheit, Betriebsmittel oder System, das/die einzeln betrachtet werden kann

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

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

[IEV 191-01-01]

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

3.2

Ausfall

Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen

[IEV 191-04-01]

3.3

Fehlzustand

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

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

[IEV 191-05-01]

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

3.4

Ausfallauswirkung

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

3.5

Ausfallart

Art und Weise, auf die eine Einheit ausfällt

3.6

Ausfall-Kritizität^{N1)} (Ausfallbedeutung)

Kombination der Schwere einer Auswirkung und der Häufigkeit ihres Auftretens oder anderer Eigenschaften eines Ausfalls als Maß der Notwendigkeit, sich damit zu befassen und sie zu herabzusetzen

3.7

System

Satz von in Wechselbeziehung oder Wechselwirkung stehenden Elementen

ANMERKUNG 1 Im Zusammenhang mit Zuverlässigkeit besteht ein System aus:

- a) einem vorgegebenen Zweck, der durch die beabsichtigten Funktionen beschrieben ist;
- b) festgelegten Betriebs- und Einsatzbedingungen [siehe IEV 191-01-12];
- c) einer definierten Begrenzung.

ANMERKUNG 2 Die Struktur eines Systems ist hierarchisch.

[ISO 9000:2000]

3.8

Ausfallsschwere

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

4 Überblick

4.1 Einleitung

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

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

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

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

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

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

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

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

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

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

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

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

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

4.2 Zweck und Ziele der Analyse

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

- a) Erkennen solcher Ausfälle, die unerwünschte Auswirkungen auf den Systembetrieb haben, z. B. Ausschließen oder signifikante Verschlechterung der Funktion oder Beeinträchtigung der Sicherheit des Benutzers;
- b) Erfüllen vertraglicher Forderungen eines Kunden, soweit zutreffend;
- c) Ermöglichen von Verbesserungen der Systemfunktionsfähigkeit oder der Sicherheit (z. B. durch Entwurfsmodifikationen oder Qualitätssicherungsmaßnahmen);
- d) Ermöglichen der Verbesserung der Instandhaltbarkeit des Systems (durch Aufzeigen von Bereichen mit Risiko oder Bereichen, in denen keine Instandhaltbarkeit gegeben ist).

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

- a) ein umfassendes Erkennen und Beurteilen aller unerwünschten Auswirkungen innerhalb der festgelegten Grenzen des analysierten Systems und die Ereignisfolgen, die durch jede erkannte Ausfallart einer Einheit auf verschiedenen Ebenen der Funktionshierarchie des Systems ausgelöst wurden, aus welchem Grund auch immer;
- b) das Feststellen der Bedeutung und der Dringlichkeit für das Aufgreifen/Entschärfen (siehe Abschnitt 6) jeder Ausfallart hinsichtlich der korrekten Funktion oder Leistung des Systems und der Wirkung auf den betroffenen Prozess;
- c) eine Klassifizierung der erkannten Ausfallarten entsprechend relevanter Eigenschaften; hierzu gehören Erkennbarkeit, Diagnosefähigkeit, Prüfbarkeit, Vorkehrungen für Ersatz und Betreiben (Reparatur, Instandhaltung, Logistik usw.);
- d) Identifizierung von Funktionsausfällen des Systems und Abschätzung von Maßgrößen für die Ausfallschwere und Ausfallwahrscheinlichkeit;
- e) Entwicklung eines Entwurfsverbesserungsplans zur Verringerung von Ausfallarten;
- f) Unterstützung der Entwicklung eines wirksamen Instandhaltungsplans, um die Wahrscheinlichkeit für Ausfälle zu verringern (siehe IEC 60300-3-11).

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

5 Fehlzustandsart- und -auswirkungsanalyse (FMEA)

5.1 Allgemeine Betrachtungen

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

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

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

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

Der FMEA-Ablauf besteht aus den folgenden vier Hauptstufen:

- a) Etablierung der wesentlichen Grundregeln für die FMEA einschließlich Planung und Terminierung, um sicherzustellen, dass Zeit und Fachwissen für die Durchführung der Analyse vorhanden sind;
- b) Durchführung der FMEA unter Verwendung des geeigneten Arbeitsblattes oder anderer Hilfsmittel, wie etwa logischer Diagramme oder Störungsbaumanalysen;
- c) Zusammenfassung und Berichterstattung über die Analyse, die alle Schlussfolgerungen und gegebenen Empfehlungen enthalten;
- d) Fortschreiben der FMEA entsprechend dem Entwicklungsfortschritt.

5.2 Vorausgehende Arbeiten

5.2.1 Planung für die Analyse

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

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

Der Plan sollte die folgenden Punkte enthalten.

- eindeutige Definition der besonderen Ziele der Analyse und erwartete Ergebnisse;
- die Abgrenzung der vorliegenden Analyse hinsichtlich der Art, in der sich die FMEA auf bestimmte Entwurfsbestandteile konzentrieren sollte. Die Abgrenzung sollte die Reife des Entwurfs in Betracht ziehen sowie Bestandteile des Entwurfs, die als Risiko angesehen werden können, weil sie eine kritische Funktion ausführen oder weil die verwendete Technologie nicht ausgereift ist;
- Beschreibung, wie die vorliegende Analyse die Zuverlässigkeit des Gesamtprojektes absichert;
- festgelegte Maßnahmen für die Überwachung der FMEA-Überarbeitungen und die zugehörige Dokumentation. Die Überwachung der überarbeiteten Analysedokumente und -arbeitsblätter sowie der Archivierungsmethoden sollte festgelegt werden;
- Teilnahme von Entwurfsfachleuten an der Analyse derart, dass sie verfügbar sind, wenn sie benötigt werden;
- wesentliche Projektmeilensteine deutlich markiert, um sicherzustellen, dass die Analyse rechtzeitig durchgeführt wird;
- Art und Weise des Abschlusses aller im Prozess zur Entschärfung von erkannten und zu behandelnden Ausfallarten festgelegten Maßnahmen.

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

5.2.2 Systemstruktur

5.2.2.1 Information über die Systemstruktur

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

- a) die verschiedenen Systembestandteile mit ihren Charakteristika, Leistungen, Aufgaben und Funktionen;
- b) logische Verknüpfungen zwischen den Bestandteilen;
- c) Redundanzniveau und Art der Redundanzen;
- d) Position und Bedeutung des Systems innerhalb der gesamten Anlage (falls möglich);
- e) Eingangs- und Ausgangsgrößen des Systems;
- f) Änderungen in der Systemstruktur für wechselnde Betriebsarten.

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

5.2.2.2 Festlegen der Systembegrenzung für die Analyse

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

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

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

5.2.2.3 Ebenen der Analyse

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

- a) Die höchste Ebene des Systems wird vom Entwurfskonzept und den festgelegten Forderungen an das Ergebnis bestimmt.
- b) Die niedrigste Ebene im System, auf der die Analyse wirkungsvoll ist, ist die Ebene, für die die Information zur Festlegung von Definition und die Beschreibung von Funktionen vorhanden sind. Die Wahl der geeigneten Systemebene wird auch durch frühere Erfahrungen beeinflusst. Eine weniger

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

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

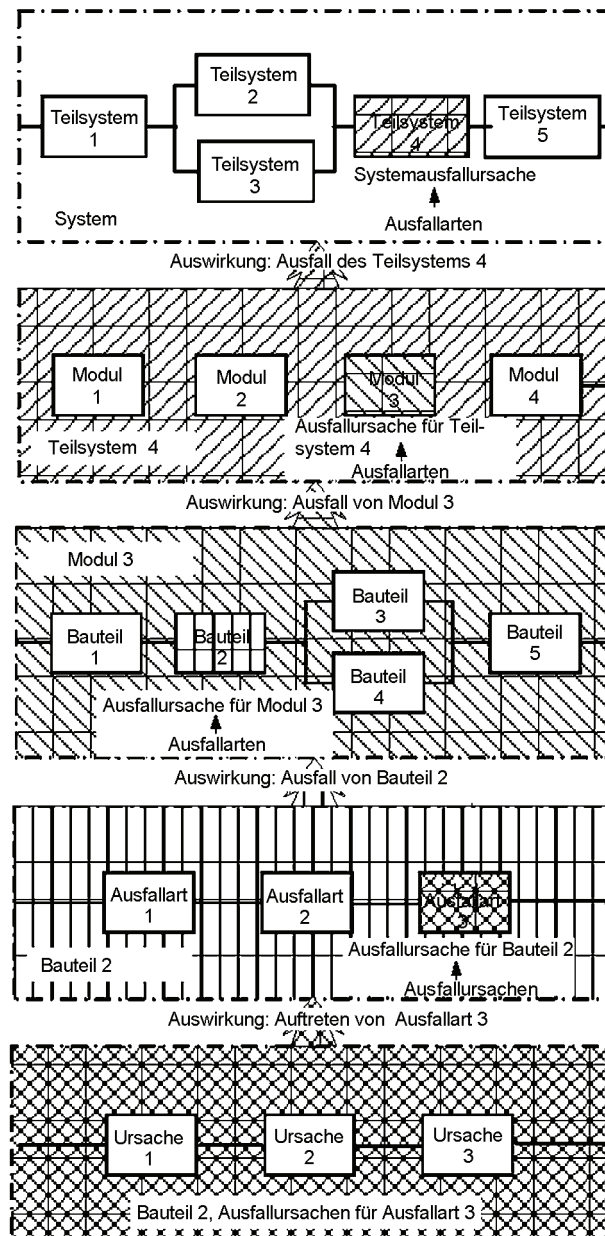


Bild 1 – Zusammenhang zwischen Ausfallarten und Ausfallauswirkungen in einer Systemhierarchie

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

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

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

5.2.2.4 Darstellung der Systemstruktur

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

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

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

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

- a) eine Aufteilung des Systems in größere Teilsysteme, einschließlich der funktionalen Verknüpfungen;
- b) alle geeignet bezeichneten Eingangs- und Ausgangsgrößen sowie Kennzahlen, anhand derer auf jedes Teilsystem widerspruchsfrei Bezug genommen werden kann;
- c) alle Redundanzen, alternativen Signalwege und anderen technischen Eigenschaften, die Schutz gegen Systemausfälle bieten.

5.2.2.5 Systeminbetriebnahme, -betrieb, -überwachung und -instandhaltung

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

- a) der Dauer jeder Funktion, die zu erfüllen das System in Anspruch genommen wird;
- b) dem Zeitintervall zwischen periodischen Prüfungen;
- c) der für Korrekturmaßnahmen zur Verfügung stehenden Zeit, bevor ernsthafte Folgen für das System auftreten;
- d) der gesamten Anlage, der Umgebung und/oder dem Personal, einschließlich Schnittstellen und Zusammenspiel mit dem Bedienpersonal;
- e) den Betriebsprozeduren während des Inbetriebsetzens und der Abschaltung des Systems und anderer Betriebsübergänge;
- f) der Überwachung während der Betriebsphasen;
- g) Wartung und/oder Instandsetzung;
- h) den Verfahren zur Stückprüfung, sofern verwendet.

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

5.2.2.6 Systemumgebung

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

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

5.2.3 Bestimmung der Ausfallarten

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

- a) der Einsatz des Systems;
- b) das jeweilig beteiligte Systemelement;
- c) die Betriebsart;
- d) die zugehörigen Festlegungen für den Betrieb;
- e) die zeitlichen Einschränkungen;
- f) die Beanspruchung durch die Umgebung;
- g) die Beanspruchung durch den Betrieb.

Eine beispielhafte Liste allgemeiner Ausfallarten ist in Tabelle 1 enthalten.

Tabelle 1 – Beispiel eines Satzes allgemeiner Ausfallarten

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

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

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

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

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

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