

	DIN IEC 60300-3-9 (VDE 0050-1)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 03.120.10; 29.020		
Einsprüche bis 2007-06-30		
<div>Entwurf</div>		
Zuverlässigkeitsmanagement – Teil 3-9: Anwendungsleitfaden – Risikobeurteilung technischer Systeme (IEC 56/1172/CD:2006)		
Dependability management – Part 3-9: Application guide – Risk analysis of technological systems (IEC 56/1172/CD:2006)		
Gestion de la sûreté de fonctionnement – Partie 3-9: Guide d'application – Analyse du risque des systèmes technologiques (CEI 56/1172/CD:2006)		
Anwendungswarnvermerk		
Dieser Norm-Entwurf 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		
<ul style="list-style-type: none">– vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden– oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.		
Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.		
Gesamtumfang 121 Seiten		
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

– Entwurf –

E DIN IEC 60300-3-9 (VDE 0050-1):2007-05

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Das internationale Dokument IEC 56/1172/CD:2006 „Dependability management – Part 3-9: Application guide – Risk analysis of technological systems“ (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 diesen Norm-Entwurf ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (<http://www.dke.de>) zuständig.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60050-191:1990 + A1: 1999 + A2: 2002	IEV Teil 191: 2005-05	–
EN 60300-2:2004	IEC 60300-2:2004	DIN EN 60300-2:2004-10	–
–	IEC 60812:2006 ^{N1}	DIN EN 60812:2006-11	–
–	IEC 61025:1990	DIN IEC 61025:1993-12	–
–	ISO/IEC Guide 51:1999 ^{N2}	DIN 820-120:2001-10	–
–	ISO/IEC Guide 73:2002	–	–
EN 61078:2006	IEC 61078:2006 ^{N3}	DIN EN 61078:2006-10	–
EN 61508 (Reihe)	IEC 61508 (Reihe)	DIN EN 61508 (VDE 0803) (Reihe)	(VDE 0803) (Reihe)

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN 820-120:2001-10, *Normungsarbeit - Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC-Guide 51:1999)*.

DIN EN 60300-2:2004-10, *Zuverlässigkeitsmanagement – Teil 2: Leitfaden zum Zuverlässigkeitsmanagement (IEC 60300-2:2004); Deutsche Fassung EN 60300-2:2004*.

DIN EN 60812:2006-11, *Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (IEC 60812:2006); Deutsche Fassung EN 60812:2006*.

DIN EN 61078:2006-10, *Techniken für die Analyse der Zuverlässigkeit – Zuverlässigkeitsblockdiagramm und Boole'sche Verfahren (IEC 61078:2006); Deutsche Fassung EN 61078:2006*.

DIN EN 61508 (VDE 0803) (Reihe), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*.

DIN IEC 61025:1993-12, *Störungsbaumanalyse; Identisch mit IEC 61025:1990*.

IEV Teil 191:2005-05, *Internationales Elektronisches Wörterbuch – Teil 191: Zuverlässigkeit und Dienstgüte*.

^{N1} Die zitierte IEC 60812:1985 wurde bereits zurückgezogen. Aktuell gültige Fassung: IEC 60812:2006.

^{N2} Der zitierte ISO/IEC-Guide 51:1990 wurde bereits zurückgezogen. Aktuell gültige Fassung: ISO/IEC Guide 51:1999.

^{N3} Die zitierte IEC 61078:1991 wurde bereits zurückgezogen. Aktuell gültige Fassung: IEC 61078:2006.

– Entwurf –

E DIN IEC 60300-3-9 (VDE 0050-1):2007-05

Zuverlässigkeitsmanagement – Teil 3-9: Anwendungsleitfaden – Risikobeurteilung technischer Systeme

Inhalt

	Seite
Einleitung.....	8
1 Anwendungsbereich	9
2 Normative Verweisungen.....	9
3 Begriffe.....	9
4 Konzeptionen zur Risikobeurteilung technischer Systeme.....	11
4.1 Zielsetzung und Nutzen einer Risikobeurteilung	11
4.2 Anwendung der Risikobeurteilung in den Lebenszyklusphasen	12
5 Vorgehensweise zur technischen Risikobeurteilung	12
5.1 Überblick	12
5.2 Planung der technischen Risikobeurteilung	13
5.3 Kommunikation und Konsultation	13
5.4 Überwachung und Überprüfung.....	14
5.5 Kontext herstellen	14
5.6 Risikobeurteilung	14
5.7 Risikobehandlung	18
6 Verfahren zur Risikobeurteilung	19
6.1 Allgemeines	19
6.2 Verfahrensauswahl	19
6.3 Risikobeurteilungsverfahren	20
Anhang A (informativ) Beurteilungsverfahren	25
A.1 Brainstorming.....	25
A.1.1 Beschreibung	25
A.1.2 Anwendung.....	25
A.1.3 Vorgehensweise	25
A.1.4 Stärken und Einschränkungen.....	26
A.2 Strukturierte und semi-strukturierte Befragungen.....	26
A.2.1 Beschreibung	26
A.2.2 Anwendung	26
A.2.3 Stärken und Einschränkungen.....	26
A.3 Delphi-Methode.....	27
A.3.1 Beschreibung	27
A.3.2 Anwendung.....	27
A.3.3 Vorgehensweise	27
A.3.4 Stärken und Einschränkungen.....	27
A.4 Prüflisten	27
A.4.1 Beschreibung	27

	Seite
A.4.2 Anwendung.....	28
A.4.3 Vorgehensweise	28
A.4.4 Stärken und Einschränkungen	28
A.5 Vorläufige Untersuchung von Gefährdungen (PHA)	28
A.5.1 Beschreibung.....	28
A.5.2 Anwendung.....	28
A.5.3 Benötigte Daten.....	28
A.5.4 Vorgehensweise	29
A.5.5 Ergebnisse.....	29
A.5.6 Stärken und Einschränkungen	29
A.6 Gefährdungs- und Betreibbarkeitsuntersuchung (HAZOP).....	29
A.6.1 Beschreibung.....	29
A.6.2 Anwendung.....	29
A.6.3 Benötigte Daten.....	30
A.6.4 Vorgehensweise	30
A.6.5 Ergebnisse.....	31
A.6.6 Stärken und Einschränkungen	31
A.6.7 Vergleiche.....	32
A.6.8 Verweise	32
A.7 Strukturiertes „Was-Wenn“-Verfahren (SWIFT)	32
A.7.1 Beschreibung.....	32
A.7.2 Anwendung.....	32
A.7.3 Benötigte Daten.....	32
A.7.4 Vorgehensweise	33
A.7.5 Ergebnisse.....	33
A.7.6 Stärken und Einschränkungen	34
A.7.7 Vergleiche.....	34
A.7.8 Verwandte Verfahren.....	34
A.8 Fehlzustandsart- und auswirkungsanalyse (FMEA) und FMECA.....	35
A.8.1 Beschreibung.....	35
A.8.2 Anwendung.....	35
A.8.3 Benötigte Daten.....	35
A.8.4 Vorgehensweise	36
A.8.5 Ergebnisse.....	36
A.8.6 Stärken und Einschränkungen	36
A.8.7 Vergleiche.....	37
A.8.8 Verweise	37
A.9 Fehlzustandsbaumanalyse (FTA).....	37
A.9.1 Beschreibung.....	37

– Entwurf –

E DIN IEC 60300-3-9 (VDE 0050-1):2007-05

	Seite
A.9.2 Anwendung	37
A.9.3 Benötigte Daten	38
A.9.4 Vorgehensweise	38
A.9.5 Ergebnisse	38
A.9.6 Stärken und Einschränkungen.....	38
A.9.7 Verweise	39
A.10 Ereignisbaumanalyse (ETA)	39
A.10.1 Beschreibung	39
A.10.2 Anwendung	39
A.10.3 Benötigte Daten	39
A.10.4 Vorgehensweise	40
A.10.5 Ergebnisse	40
A.10.6 Vergleiche und Verbindungen	40
A.10.7 Stärken und Einschränkungen.....	40
A.11 Entscheidungsbaumanalyse	41
A.11.1 Beschreibung	41
A.11.2 Anwendung	41
A.11.3 Benötigte Daten	42
A.11.4 Vorgehensweise	42
A.11.5 Ergebnisse	42
A.12 Markoffanalyse.....	42
A.12.1 Beschreibung	42
A.12.2 Anwendung	42
A.12.3 Benötigte Daten	43
A.12.4 Vorgehensweise	43
A.12.5 Ergebnisse	45
A.12.6 Stärken und Einschränkungen.....	45
A.12.7 Vergleiche	45
A.12.8 Verweise	45
A.13 Beurteilung der menschlichen Zuverlässigkeit	45
A.13.1 Beschreibung	45
A.13.2 Anwendung	46
A.13.3 Benötigte Daten	46
A.13.4 Vorgehensweise	46
A.13.5 Ergebnisse	46
A.13.6 Stärken und Einschränkungen.....	47
A.14 „Bow-Tie“-Analyse	48
A.14.1 Beschreibung	48
A.14.2 Anwendung	49

	Seite
A.14.3 Benötigte Daten.....	49
A.14.4 Vorgehensweise	49
A.14.5 Ergebnis.....	49
A.14.6 Stärken und Einschränkungen	50
A.15 Auf die Funktionsfähigkeit bezogene Instandhaltung (RCM)	50
A.15.1 Beschreibung.....	50
A.15.2 Anwendung.....	51
A.15.3 Benötigte Daten.....	51
A.15.4 Vorgehensweise	51
A.15.5 Ergebnisse.....	52
A.15.6 Verweise.....	52
A.16 Monte-Carlo-Analyse.....	52
A.16.1 Beschreibung.....	52
A.16.2 Anwendung.....	52
A.16.3 Benötigte Daten.....	52
A.16.4 Vorgehensweise	52
A.16.5 Ergebnisse.....	52
A.16.6 Stärken und Einschränkungen	52
Anhang B (informativ) Vergleich von Risikobeurteilungsverfahren	54
Anhang C (informativ) Anleitung zur Auswahl von Risikobeurteilungsverfahren	55
C.1 Zweck einer Risikobeurteilung.....	55
C.2 Risikobeurteilung beeinflussende Faktoren	55
C.3 Vorgehensweise zur Auswahl von Risikobeurteilungsverfahren.....	56
 Bild 1 – Beziehungen bei der Risikobeurteilung (vereinfachte Darstellung).....	 21
Bild 2 – Vorgehensweise zur Risikobeurteilung	22
Bild 3 – Beispiel einer Risikomatrix.....	23
Bild 4 – Typische Überlegungen bei der Auswahl der Analyseart und der Untersuchungstiefe	24
Bild A.1 – Ereignisbaum.....	41
Bild A.2 – Zustands-Übergangsdiagramm für eine Komponente mit diskretem Ausfall-/Reparaturverhalten.....	43
Bild A.3 – Zustands-Übergangsdiagramm für eine Komponente mit kontinuierlichem Ausfall-/Reparaturverhalten.....	44
Bild A.4 – Beurteilung der menschlichen Zuverlässigkeit.....	48
Bild A.5 – „Bow Tie“ – oder Fliegen-Diagramm	50
Bild C.1 – Risikobeurteilung beeinflussende Faktoren	56
 Tabelle A.1 – Beispiele möglicher HAZOP-Leitworte	 31
Tabelle C.1 – Anschauungsbeispiel für die Vorgehensweise bei der Auswahl von Risikobeurteilungsverfahren (Übersicht)	57

Einleitung

Zum technischen Risikomanagement gehören viele verschiedene Elemente, die von der erstmaligen Identifizierung und Beurteilung eines Risikos über die Bewertung seiner Vertretbarkeit und der Identifizierung potentieller Optionen zur Risikominderung bis zur Auswahl, Umsetzung und Überwachung geeigneter Steuerungs- und Minderungsmaßnahmen reichen.

Technische Risikobeurteilung, Thema dieses Teils der Normenreihe IEC 60300-3, ist ein strukturierter Vorgang, durch den sowohl die Wahrscheinlichkeit als auch das Ausmaß widriger Folgen festgestellt werden können, die sich aus einer bestimmten Tätigkeit, Anlage oder System ergeben können. Im Rahmen dieser Norm sind unter widrigen Folgen Personenschäden sowie Sach- und Umweltschäden zu verstehen.

Durch eine technische Risikobeurteilung versucht man, drei grundlegende Fragen zu beantworten:

- Was kann gefahrbringend geschehen (durch Identifizierung von Risiken)?
- Wie wahrscheinlich ist solch ein Ereignis (durch Häufigkeits- oder Wahrscheinlichkeitsanalyse)?
- Mit welchen Folgen und Schäden ist zu rechnen (durch Folgen- oder Auswirkungsanalyse)?

Diese Norm berücksichtigt den gegenwärtigen erprobten technischen Stand der Auswahl und Anwendung der Risikobeurteilungstechniken; neuartige oder gerade entstehende Verfahren, die noch keinen zufriedenstellenden fachlichen Konsensgrad erreicht haben, werden dagegen nicht berücksichtigt.

Diese Norm ist bewusst allgemein gehalten, um Anleitung für viele Industriebereiche und technisch unterschiedliche Systeme zu geben. In einzelnen Industriebereichen kann es spezifische Normen geben, in denen dort bevorzugte Verfahren und Analysen für besondere Anwendungen vorgegeben werden. Sofern diese Normen mit dieser Publikation harmonisieren, werden diese spezifischen Normen im Allgemeinen ausreichend sein.

Diese Norm stimmt mit den ISO/IEC-Grundsätzen hinsichtlich des Risikomanagements überein. Risikobezogene Begriffe und Definitionen beruhen auf relevanten ISO/IEC-Normen (Anleitungen und Begriffsnormen).

1 Anwendungsbereich

Diese internationale Norm enthält Anleitungen zur Auswahl und Anwendung systematischer und methodischer Verfahren zur Risikobeurteilung technischer Systeme und ist in allen Phasen eines Systemlebenszyklus' anwendbar. Die Anwendung bestimmter spezifischer Verfahren wird kurz vorgestellt und es wird auf andere internationale Zuverlässigkeitsnormen verwiesen, in denen die Konzeption und Anwendung von Werkzeugen ausführlicher beschrieben werden.

In Übereinstimmung mit dieser Norm durchgeführte technische Risikobeurteilung trägt zu anderen Risikomanagementtätigkeiten bei.

Diese internationale Norm ist nicht für Zertifizierung oder Konformitätsbewertungen beabsichtigt.

ANMERKUNG Diese internationale Norm enthält keine spezifischen Kriterien dafür, wie die Notwendigkeit einer Risikobeurteilung ermittelt werden kann noch legt sie ein bestimmtes Risikobeurteilungsverfahren fest, das in einer gegebenen Anwendung erforderlich ist. Sie bietet auch keine Empfehlungen zum Risikomanagement bei Risiken versicherungstechnischer, rechtlicher oder finanzieller Art an.

2 Normative Verweisungen

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

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

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

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

IEC 61025:1990, *Fault tree analysis (FTA)*

ISO/IEC Guide 51:1990, *Safety Aspects – Guidelines for their inclusion in standards*

ISO/IEC Guide 73:2002, *Risk Management - Vocabulary – Guidelines for their inclusion in standards*

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

IEC 61508: *Functional safety of programmable electronic devices*

3 Begriffe

Für die Anwendung dieses Teils der Internationalen Norm IEC 60300-3 gelten die Begriffe nach IEC 60050-191 sowie die folgenden Begriffe.

3.1

Risiko

en: risk

Kombination aus Häufigkeit oder Wahrscheinlichkeit für den Eintritt und der Folgen eines bestimmten Ereignisses

ANMERKUNG 1 Der Begriff „Risiko“ umfasst immer zwei Elemente: die Häufigkeit oder Wahrscheinlichkeit mit der ein Ereignis eintritt und die sich aus dem eingetretenen Ereignis ergebenden Folgen.

ANMERKUNG 2 Wird diese Norm auf Sicherheitsbelange angewendet, sind Risiken Gefährdung (en: hazards).

3.2

Risikoanalyse

en: risk analysis

Vorgang, bei dem in systematischer Weise anhand vorliegender Information Gefährdungen identifiziert und das Risiko für eine einzelne Person, für Personengruppen, für Sachen oder für die Umwelt eingeschätzt werden

ANMERKUNG Risikoanalyse wird gelegentlich auch als Wahrscheinlichkeitsanalyse der Sicherheit (en: probabilistic safety analysis), als Wahrscheinlichkeitsanalyse zum Risiko (en: probabilistic risk analysis), als quantitative Sicherheitsanalyse (en: quantitative safety analysis) oder als quantitative Risikoanalyse (en: quantitative risk analysis) bezeichnet.

3.3

Risikobeurteilung

en: risk assessment

gesamter Vorgang aus Risikoidentifizierung, -analyse und -bewertung

3.4

Risikosteuerung

en: risk control

Vorgang des Fällens von Entscheidungen zu Management und/oder Minderung von Risiken, zur Einführung und Umsetzung und einer wiederholten Bewertung der Wirksamkeit unter Verwendung der Ergebnisse der Risikobeurteilung

3.5

Risikoeinschätzung

en: risk estimation

Vorgang, durch den ein Maß für die zu analysierenden Risiken erhalten wird. Risikoeinschätzung besteht aus den folgenden Schritten: Häufigkeitsanalyse, Folgenanalyse und deren Zusammenführung

3.6

Risikobewertung

en: risk evaluation

Vorgang der Abwägung zur Vertretbarkeit eines Risikos auf Grundlage der Risikoanalysen und unter Einbeziehung von Faktoren wie sozioökonomischer und umweltbezogener Einflussgrößen

3.7

Risikomanagement

en: risk management

systematische Anwendung von Managementgrundsätzen, -verfahren und -praktiken zur Analyse, Bewertung und Steuerung/Bewältigung von Risiken (siehe Bild 1)

3.8

System

zusammengestellte Einheit, auf einer beliebigen Komplexitätsebene, von Personen, Verfahren, Material, Werkzeugen, Geräten, Anlagen und Software. Die Elemente dieser zusammengestellten Einheit werden gemeinsam in der Betriebs- oder Instandhaltungsumgebung benutzt, um eine gegebene Aufgabe zu erfüllen oder eine festgelegte Zielsetzung zu erreichen.

3.9

Schaden

en: harm

physische Verletzung oder Schädigung von Gesundheit oder von Sachen oder der Umwelt

3.10

Gefährdung

en: hazard

Ursprung möglicher Schäden oder einer Situation mit Schadenspotential

3.11

Gefährdungseignis

en: hazardous event

Ereignis, das einen Schaden hervorrufen kann

3.12

Identifizierung von Gefährdungen

en: hazard identification

Vorgang des Begreifens, dass eine Gefahr besteht und Beschreibung ihrer Merkmale

3.13

technisches System

System mit wissenschaftlichem oder technischem Inhalt oder Anwendung

ANMERKUNG Ein System kann Software, Hardware, Personen usw. enthalten.

4 Konzeptionen zur Risikobeurteilung technischer Systeme

4.1 Zielsetzung und Nutzen einer Risikobeurteilung

Das technische Risikomanagement soll dazu dienen, das Erreichen der Zielsetzungen durch die Beherrschung von Ungewissheiten in systematischer Weise zu ermöglichen. Zur technischen Risikobeurteilung gehört die Identifizierung, Analyse und Bewertung dieser Ungewissheiten.

Das Hauptziel der Beurteilung des Risikos eines technischen Systems ist es, die Bedrohungen zu minimieren und das Systemverhalten zu verbessern. Hierzu gehören folgende Ziele:

- Zuverlässigkeit (Verfügbarkeit und Funktionsfähigkeit) maximieren;
- mit Gefährdungen umgehen und die Sicherheit gewährleisten;
- die Instandhaltung verbessern.

Aus Sicht eines Entscheiders gehören zum hauptsächlichen Nutzen einer Risikobeurteilung:

- objektive Informationen für Entscheider liefern;
- technische Risiken identifizieren und erkennen und Vorgehensweisen zu deren Lösung ermitteln;
- systematische Ermittlung potentieller Systemausfallarten;
- Risiken quantifizieren oder deren Rangfolge ermitteln;
- mögliche Modifizierungen zur Risikominderung oder zum Erreichen besserer Zuverlässigkeitswerte beurteilen;
- die wichtigen Risiko-Faktoren und schwachen Systemzweige ermitteln;
- das System und seine Installationen besser verstehen lernen;
- die aktuellen Risiken mit den Risiken alternativer Systeme oder Technologien vergleichen;
- Risiken und Ungewissheiten ermitteln und melden;
- bei der Aufstellung von Prioritäten für die Verbesserung der Gesundheitsvorsorge und Sicherheit mithelfen;
- eine Grundlage für vorbeugende Instandhaltung und Inspektion bilden;
- nach Unfällen die Unfallgründe untersuchen und Vorkehrungen für die Vermeidung neuer Unfälle treffen;
- Alternativen, wie unterschiedliche Maßnahmen zur Risikominderung oder Technologien, auswählen;
- behördliche Vorschriften erfüllen;
- Informationen liefern, anhand derer die Vertretbarkeit von Risiken anhand vorgegebener Kriterien beurteilt werden kann.

Die Durchführung einer Risikobeurteilung macht die Anfälligkeit einer Organisation gegen die einem technischen System innewohnenden Risiken sichtbar und trägt zum Entscheidungsfindungsprozess einer Kosten/Nutzen-Beurteilung bei.

– Entwurf –

E DIN IEC 60300-3-9 (VDE 0050-1):2007-05

4.2 Anwendung der Risikobeurteilung in den Lebenszyklusphasen

Technische Risikobeurteilung kann in allen Stufen eines Lebenszyklus angewendet werden. Einige übliche Anwendungen in der Konzept- und Definitionsphase sind:

- bei der Entscheidung über eine Angebotsabgabe mitwirken und das Risiko zwischen intern und extern aufteilen;
- die wichtigsten Ursachen für das gesamte Systemrisiko ermitteln.

In der Entwicklungsphase kann (können) mithilfe der Risikobeurteilung

- sichergestellt werden, dass der Konstruktionsentwurf die Vorgaben für das Systemrisiko erfüllt;
- Eingaben in den Entwurfsprozess gemacht und die Eignung des Gesamtentwurfs bewertet werden;
- mögliche Sicherheitsvorkehrungen im Konstruktionsentwurf ermittelt und beurteilt werden;
- Information gewonnen werden, die für die Beurteilung der Annehmbarkeit der vorgeschlagenen potentiell gefährlichen Anlagen, Tätigkeiten oder Systeme verwendet werden können;
- Informationen gewonnen werden, die bei der Entwicklung von Prozeduren für normale und Notfallbedingungen behilflich sind;
- das Risiko bezüglich behördlicher Vorschriften und anderer Anforderungen bewertet werden;
- der Stand der technologischen Überalterung (Obsoleszenz) bewertet werden;
- zu Kosteneffizienzstudien beigetragen werden;
- alternative Entwurfskonzepte bewertet werden.

Während der Fertigungs- und Installationsphase kann die Risikobeurteilung

- dazu verwendet werden, das Systemverhalten zu überwachen und die gemachten Erfahrungen zu bewerten, um so das tatsächliche Systemverhalten mit den gegebenen Anforderungen vergleichen zu können;
- zu Kosteneffizienzstudien beitragen;
- Informationen zur Optimierung der Prozeduren im Normalbetrieb, für die Instandsetzung und Inspektion und Notfälle liefern.

Während der Betriebs- und Instandhaltungsphase, kann (können) mithilfe der Risikobeurteilung

- Änderungsvorschläge beurteilt werden;
- Informationen über die Hauptbeiträger zum Risiko und Einflussfaktoren aktualisiert werden;
- Informationen zur Signifikanz des Risikos betrieblicher Entscheidungen bereitgestellt werden;
- die Vorgehensweise bei der Logistikunterstützung validiert werden;
- der Status der technologischen Überalterung (Obsoleszenz) beurteilt werden;
- zu Kosteneffizienzstudien beigetragen werden;
- Schulungsbemühungen optimiert werden.

In der Entsorgungsphase ist eine Risikobeurteilung nützlich

- für die Bewertung des Risikos bezüglich der Tätigkeiten zur Beseitigung und Entsorgung des Systems und zur Sicherstellung, dass die gegebenen Anforderungen erfüllt werden können;
- um behördlichen Vorschriften zu genügen;
- um Informationen zu Entsorgungsprozeduren zu liefern.

5 Vorgehensweise zur technischen Risikobeurteilung

5.1 Überblick

Um die Wirksamkeit und die Objektivität einer Risikobeurteilung zu erhöhen und den Vergleich mit anderen Risikobeurteilungen zu erleichtern, sollte für beide Merkmale in ähnlicher Weise vorgegangen werden. Die

Risikobeurteilung sollte im Rahmen des Risikomanagements vorgenommen werden, das folgende Tätigkeiten umfasst:

- Planung der technischen Risikobeurteilung;
- Kommunikation und Konsultation:
- Überwachung und Überprüfung;
- den Kontext herstellen;
- Risikobeurteilung;
- Risikobehandlung.

Der gesamte Vorgang des Risikomanagements ist in Bild 1 dargestellt. Diese Norm behandelt vorrangig Risikobeurteilung und solche Zuverlässigkeitsverfahren, die mit diesem Aspekt des Risikomanagements zusammenhängen. Weitere Elemente des gesamten Risikomanagementvorganges müssen im Zusammenhang mit technischen Systemen ebenfalls berücksichtigt werden.

Je nach Anwendungsgebiet der Risikobeurteilung brauchen lediglich gewisse Elemente des gezeigten Vorganges berücksichtigt werden. So kann es beispielsweise in manchen Fällen nicht nötig sein, über eine Eingangsrisiko- und Folgenanalyse hinauszugehen.

Obwohl Dokumentation nicht als separater Punkt erwähnt ist, muss diese dennoch für jede Vorgangsstufe ausgearbeitet werden.

5.2 Planung der technischen Risikobeurteilung

Eine Organisation sollte Grundsätze oder Strategien entwickeln, die sicherstellen, dass die Zielsetzungen erreicht werden und eine technische Risikobeurteilung, soweit angebracht, stattfindet (siehe IEC 60300-1). Diese Grundsätze oder Strategien können für Projekte technischen Inhalts oder anderer Tätigkeiten in den Lebenszyklusphasen benötigt werden und können Folgendes festlegen:

- organisatorische Zielsetzungen für die Risikobeurteilung;
- Ausmaß und Art der hinnehmbaren technischen Risiken und Vorgaben, wie mit nicht hinnehmbaren Risiken umzugehen ist;
- bei der Risikobeurteilung zu verwendende Verfahren und Techniken;
- Rechenschaftspflicht und Verantwortlichkeiten für die Anwendung der Risikobeurteilung;
- verfügbare Ressourcen und Mittel für die Durchführung der Risikobeurteilung;
- wie über das Verhalten berichtet und wie dieses überprüft wird;
- zu erreichende Sicherheitsniveaus.

Risikobeurteilung eines technischen Systems kann ein Element eines Zuverlässigkeitsprogramms sein, wie dies in IEC 60300-2 dargestellt ist. Die Grenzen der technischen Risikobeurteilung sollten festgelegt und dokumentiert werden, um so einen technischen Risikobeurteilungsplan aufzustellen, in dem die Praxis, Mittel und Abfolge der Tätigkeiten dargelegt sind.

5.3 Kommunikation und Konsultation

Der Erfolg einer technischen Risikobeurteilung hängt von der Kommunikation und Konsultation mit Geschäftsinteressenten ab. Risikobeurteilung erfordert oft eine multidisziplinäre Vorgehensweise, da dabei Fachwissen aus den folgenden Bereichen benötigt werden kann:

- Systemanalyse;
- Anwendung statistischer Verfahren;
- technisches Fachwissen aus den Bereichen Chemie, Mechanik, Elektrotechnik, Bauwesen oder Kerntechnik;
- Fachwissen aus den Bereichen Physik, Chemie und Biologie
- medizinisches Fachwissen einschließlich Toxikologie und Epidemiologie;
- Sozialwissenschaften, einschließlich Betriebswirtschaft, Psychologie und Soziologie;
- menschliche Faktoren, einschließlich menschlicher Zuverlässigkeit;
- Umweltwissenschaften;
- Sicherheit.

5.4 Überwachung und Überprüfung

Risikobeurteilungen sollten regelmäßig überwacht und überprüft werden, um zu bewerten, ob

- die erwarteten Ergebnisse erreicht worden sind;
- die Annahmen zu hinnehmbaren Risiken richtig sind;
- die Risikobeurteilungsverfahren sauber angewendet wurden.

Eine Rechenschaftspflicht für Überwachung und Durchführung der Überprüfung sollte festgelegt werden.

5.5 Kontext herstellen

Um den Kontext einer Risikobeurteilung herzustellen, sollten folgende Schritte erfolgen:

- Beschreibung der Gründe oder Probleme, die zur Durchführung einer Risikobeurteilung geführt haben. Dazu gehört:
 - Formulieren der Zielsetzung der Risikobeurteilung aufgrund der identifizierten Hauptbedenken;
 - Die Kriterien für den Erfolg oder Ausfall des Systems festlegen. Das Hauptbedenken könnte ein unerwünschtes Ergebnis sein (z. B. Systemausfall, gefahrbringender Ausfall, Freisetzen giftiger Substanzen), oder es könnte ein potentiell gefahrbringender Zustand sein.
- Definition des zu untersuchenden Systems. Diese Definition sollte umfassen:
 - eine allgemeine Beschreibung des Systems;
 - die physikalischen und funktionalen Schnittstellen zu zugehörigen Systemen;
 - die Umweltbedingungen;
 - die Energie-, Material- und Informationsflüsse über die Schnittstellen hinweg;
 - die durch die Risikobeurteilung abgedeckten Betriebsbedingungen und ggf. relevante Einschränkungen.
- Ermittlung und Angabe der Quellen aller Einzelheiten technischer, umweltbezogener, gesetzlicher, organisatorischer und menschlicher Art, die für die Tätigkeit und das untersuchte Problem von Bedeutung sind. Insbesondere sollten auch sich auf die Sicherheit beziehende Umstände beschrieben werden;
- Offenlegen der der Beurteilung zugrunde liegenden Annahmen und Einschränkungen;
- Ermittlung und Benennung der zu treffenden Entscheidungen, der von der Studie erwarteten Ergebnisse und der Entscheidungsträger.

Zur Aufgabe der Festlegung der Grenzen der Beurteilung sollte auch das gründliche Vertrautmachen mit dem zu untersuchenden System als eine geplante Tätigkeit gehören. Ein Ziel des Vertrautmachens sollte es sein, zu bestimmen, wo und wie Fachwissen zugänglich ist und wie dies in die Beurteilung eingearbeitet werden kann.

5.6 Risikobeurteilung

5.6.1 Allgemeines

Risikobeurteilung ist der gesamte Vorgang der Risikoidentifizierung, Risikoanalyse und Risikobewertung (siehe Bild 2). Die Art und Weise wie dieser Vorgang durchgeführt wird, hängt nicht nur vom Kontext der Risikobeurteilung ab, sondern auch von den bei der Durchführung der Risikobeurteilung verwendeten Verfahren und Techniken (siehe Abschnitt 6).

5.6.2 Risikoidentifizierung

Bei technischen Systemen beziehen sich die Risiken auf gefahrbringende Ereignisse oder Situationen, die Verletzungen oder Gesundheitsschäden, Sachschäden oder Umweltschäden nach sich ziehen können. Die Quellen technischer Risiken sind System- oder Geräteausfälle oder Funktionsverlust als auch menschliche Einflüsse.

Die Verfahren der Risikoidentifizierung können in drei Hauptkategorien eingeteilt werden:

- vergleichende Verfahren; Beispiele hierfür sind Prüflisten und Nachprüfung gemachter Erfahrungen;
- grundlegende Verfahren; diese sind so strukturiert, dass sie eine Gruppe von Personen so stimulieren können, dass diese in Verbindung mit ihrem Fachwissen die Aufgabe der Risikoerkennung durch Fragen nach dem „was wenn?“ angehen;
- induktive Überlegungen wie beispielsweise Ereignisbaumlogikdiagramme.

Bei speziellen Problemen können zur noch besseren Risikoidentifizierung auch andere Verfahren verwendet werden. Einige Beispiele hierfür sind Brainstorming, Kriechwegeanalyse (en: Sneak Analysis), Delphi-Methodik und Analyse der menschlichen Zuverlässigkeit.

Unabhängig von den tatsächlich angewendeten Techniken ist es wichtig, dass in dem gesamten Vorgang der Risikoidentifizierung der Tatsache ausreichend Beachtung gewidmet wird, dass menschliche und organisatorische Fehlhandlungen bei vielen Unfällen wichtige Faktoren sind. Folglich sollten Unfallszenarien, bei denen menschliche und organisatorische Fehler eine Rolle spielen, ebenfalls mit in die Risikoidentifizierung aufgenommen werden. Diese sollte sich also nicht bloß um die „Hardware“ kümmern.

Eine Erstbewertung der Bedeutung der identifizierten und erkannten Risiken sollte auf der Grundlage einer Folgenanalyse zusammen mit einer Untersuchung über die Grundursachen durchgeführt werden. Hieraus sollten mögliche weitere Vorgehensalternativen festgelegt werden:

- Änderungen zu diesem Zeitpunkt veranlassen, um Ungewissheiten zu beseitigen oder zu mindern;
- Beurteilungsvorgang abbrechen, weil die Risiken oder deren Folgen unbedeutend sind;
- Fortsetzung der Risikoabschätzung.

Die anfänglichen Annahmen und Ergebnisse sollten dokumentiert werden (siehe 5.6.6).

5.6.3 Risikoanalyse

5.6.3.1 Allgemeines

Bei einer Risikoanalyse werden die Wahrscheinlichkeiten und Folgen identifizierter und erkannter Risikoereignisse oder Szenarien sowie das sich aus deren Kombination ergebende Risikomaß bestimmt.

Die zur Analyse des Risikos verwendeten Verfahren sind oft quantitativer, semi-quantitativer oder qualitativer Art, wobei der zur Erstellung der Schätzung erforderliche Detaillierungsgrad von der jeweiligen Anwendung abhängt. Jedoch wird eine vollständig quantitative Analyse aufgrund unzureichender Informationen über das untersuchte System oder die untersuchte Tätigkeit, fehlender Ausfalldaten, menschlicher Einflüsse usw. nicht immer möglich sein. In solchen Fällen kann eine vergleichende quantitative oder qualitative Einstufung der Risiken durch auf ihrem Arbeitsgebiet gut erfahrene Spezialisten dennoch angebracht sein. In Fällen qualitativer Einstufung sollte eine klare Erklärung zu den verwendeten Begriffen gegeben werden und die Grundlage für alle Häufigkeits- und Folgeeinstufungen sollte klar dokumentiert werden. In Fällen, in denen eine vollständige Quantifizierung durchgeführt wurde, muss dennoch beachtet werden, dass die berechneten Risikowerte nur Schätzwerte sind. Es sollte dafür gesorgt werden, dass ihnen keine mit der Genauigkeit der Grunddaten und Methoden unvereinbare Genauigkeit und Aussagekraft zugeschrieben wird.

Die Elemente des Risikoanalysevorganges sind für alle Bedrohungen gleich. Zuerst werden die möglichen Ursachen für das Risiko untersucht, um die Häufigkeit oder Wahrscheinlichkeit ihres Auftretens, ihre Dauer und auch ihre Art festzustellen. Bei der Untersuchung einer Industrieanlage kann diese Häufigkeitsanalyse eine Hauptaufgabe sein. Danach werden die Folgen des erkannten Risikos analysiert. Zu dieser Folgenanalyse gehört die Schätzung der Schwere der mit dem Risiko verbundenen Folge(n). Die Analyse kann auch die Schätzung der Wahrscheinlichkeit des Risikos, das diese Folge(n) nach sich ziehen würde, erforderlich machen. Hierfür kann eine Untersuchung nötig sein zum Ablauf der Ereignisse, um zu klären, wie der Eintritt des Ereignisses zu den Folgen führt.

Die Ungewissheiten, die im System Risiken erzeugen, sollten zusammen mit Wegen, die zu ihrer Erkennung führen, ermittelt werden. Bekannte Ungewissheiten (die vielleicht bei früheren Erfahrungen erkannt worden waren) sollten klar angegeben werden.

5.6.3.2 Schätzung der Wahrscheinlichkeit

Bei der Schätzung der Wahrscheinlichkeit werden der Eintrittswahrscheinlichkeit jedes Ereignisses Zahlenwerte zugewiesen, und es wird der Bereich möglicher Ergebnisse, der in der Stufe der Risikoidentifizierung ermittelt wurde, angegeben. Üblicherweise kommen drei Vorgehensweisen für die Schätzung der Ereigniswahrscheinlichkeit in Betracht. Bei der ersten Vorgehensweise nimmt man gemachte Erfahrungsdaten über in der Vergangenheit eingetretene Ereignisse und trifft davon ausgehend Annahmen zu der Wahrscheinlichkeit ihres zukünftigen Eintretens. Die dafür verwendeten Daten sollten sowohl für die Art des betrachteten Systems, der Anlage oder Tätigkeit relevant sein, als auch für die betrieblichen Standards der betreibenden Organisation. Sollte es in der Vergangenheit nur sehr wenige Ereignisse gegeben haben, so kann es unangebracht sein, diese Erfahrung einfach in die Zukunft zu übersetzen. Dies gilt insbesondere bei Null gezählten Ereignissen und wenn man nicht davon ausgehen kann, dass dem auch zukünftig so sein wird.

Zweitens kann man die Eintrittswahrscheinlichkeiten von Risiken mittels geeigneter Verfahren vorhersagen; hierzu eignen sich die Fehlzustandsbaumanalyse und Ereignisbaumanalyse (für Ereigniswahrscheinlichkeiten), siehe Anhang A. Sollten keine Erfahrungsdaten vorliegen oder diese unbrauchbar sein, so müssen die Ereigniswahrscheinlichkeiten durch eine Analyse des Systems und seiner zugehörigen Ausfallarten abgeleitet werden. Numerische Daten zu allen relevanten Ereignissen, einschließlich Geräteausfällen und menschlicher Fehler, die aus Betriebserfahrungen oder veröffentlichten Datenquellen stammen, werden dann kombiniert, um die Wahrscheinlichkeit von unerwünschten Ereignissen zu schätzen. Wenn man Vorhersageverfahren einsetzt, so ist es wichtig, dass bei der Analyse sorgsam darauf geachtet wird, dass es möglicherweise Ausfälle mit gemeinsamer Ursache geben kann und es daher Ausfälle von einer Reihe unterschiedlicher Teile oder Bauelemente im System aufgrund gleicher Ursache (gleichem Ereignis) geben kann. Simulationsverfahren könnten nötig werden, um Ausfallwahrscheinlichkeiten von Geräten und Bauten aufgrund von Alterung und anderen Verschleißvorgängen zu generieren, wobei die Auswirkungen von Ungewissheiten berechnet werden.

Schließlich kann man noch auf das Wissen und die Meinung von Fachleuten zurückgreifen. Es gibt eine Reihe formaler Verfahren, wie man fachliche Beurteilungen ausfindig machen und erhalten kann, und die dann dabei helfen, die geeigneten Fragen zu stellen. Fachliche Beurteilungen sollten sich aller verfügbaren und relevanten Informationen bedienen, so etwa zu früheren Erfahrungen, über Systembesonderheiten, Versuche, Entwürfe usw. Solche Verfahren sind unter anderem das Delphi-Verfahren, gepaarte Vergleiche, Einordnung in Kategorien und Beurteilung der absoluten Wahrscheinlichkeit.

Solche Verfahren können sowohl einzeln oder auch zusammen verwendet werden. Die beiden ersten Vorgehensweisen sind komplementär; jede hat dort ihre Stärken, wo die andere Einschränkungen hat. Daher sollten nach Möglichkeit immer beide eingesetzt werden. Auf diese Weise können sie als unabhängige Prüfungen des jeweils anderen Verfahrens verwendet werden und man kann somit das Vertrauen in die Ergebnisse erhöhen. Falls diese nicht eingesetzt werden können oder sie nicht ausreichen, muss möglicherweise teilweise auf die Meinung von Fachleuten zurückgegriffen werden.

5.6.3.3 Folgenanalyse

Bei der Folgenanalyse geht man von den ausgewählten Ereignissen aus, nimmt hypothetisch deren Eintritt an und schätzt die sich daraus ergebenden Auswirkungen auf die Zielsetzungen.

Bei einer Folgenanalyse sollten folgende Punkte beachtet werden:

- Beachtung bereits vorhandener, die Folgen steuernde und beherrschende Vorkehrungen, zusammen mit allen sich auf Folgen auswirkenden Faktoren;
- die Folgen eines Risikos mit den ursprünglichen Zielsetzungen vergleichen;
- sowohl unmittelbar eintretende Folgen als auch solche, die erst nach einer gewissen Zeit eintreten könnten, müssen beachtet werden, sofern dies mit dem Ziel der Untersuchung in Einklang steht;
- Sekundärfolgen in benachbarten Geräten oder Systemen beachten.

Bei einer Folgenanalyse müssen je nach Geschäftsinteressen ggf. unterschiedliche Folgen beachtet werden.

5.6.3.4 Ungewissheiten

Mit der Schätzung des Risikos sind viele Ungewissheiten verbunden. Um die Risikowerte wirkungsvoll interpretieren zu können, bedarf es eines Verständnisses der Ungewissheiten und deren Gründe. Die Untersuchung der mit den Daten, Verfahren und Modellen zur Ermittlung und Schätzung des Risikos verbundenen Ungewissheiten spielt bei deren Anwendung eine bedeutende Rolle. Durch die Untersuchung der Ungewissheiten muss bestimmt werden, inwieweit die Ergebnisse der Modelle variieren oder aufgrund der kollektiven Variation der in dem Modell verwendeten Parameter und Annahmen ungenau sind. Ein mit der Untersuchung der Ungewissheiten eng zusammenhängendes Gebiet ist die Sensitivitätsanalyse.

Die Sensitivitätsanalyse beinhaltet die Bestimmung der Änderung der Ausgangsgrößen in Abhängigkeit der Änderungen der einzelnen Modellparameter. Man setzt sie einerseits ein, um diejenigen Daten zu ermitteln und zu bestimmen, die genau sein müssen, und andererseits, um solche zu bestimmen, die sich weniger auf die gesamte Genauigkeit auswirken.

Vollständigkeit und Genauigkeit der Risikoabschätzung sollten so vollständig wie möglich angegeben werden. Die Ursachen für Ungewissheiten sollten, soweit möglich, angegeben werden. Diese Angaben sollten sowohl die Ungewissheit der Daten als auch die des Modells betreffen. Parameter, auf welche die Analyse empfindlich reagiert, sollten aufgezeigt und das Maß der Empfindlichkeit sollte genannt werden.

5.6.3.5 Risikomaß

Das Maß eines Risikos sollte anhand der am besten dafür geeigneten Begriffe angegeben werden. Üblicherweise verwendete Maßgrößen sind beispielsweise:

- Zuverlässigkeitsmaßgrößen wie Funktionsfähigkeit, Verfügbarkeit und Instandhaltbarkeit;
- Beiträge zum finanziellen Gesamtengagement;
- Wahrscheinlichkeit, die zeitlichen Vorgaben einzuhalten;
- Wahrscheinlichkeit, die Hauptleistungsparameter nicht zu erreichen;
- vorhergesagte Sterblichkeitsrate oder Krankheitsziffer einzelner Personen (Individualrisiko);
- graphische Gegenüberstellungen von Häufigkeit zu Folgen gesellschaftlicher Risiken, bekannt als H-N-Kurven (en: F-N curve), wobei H (en: frequency, F) für die Häufigkeit und N für die aufsummierte Anzahl von Personen steht, die unter bestimmten Gesundheitsschädigungen leiden, oder aufsummierte Schadenssumme;
- die statistisch erwartete Verlustrate (Personenschäden, wirtschaftlicher Verlust oder Umweltschaden).

Bei der Berechnung des Risikomaßes müssen sowohl die Dauer des Ereignisses als auch die Exposition berücksichtigt werden. Bild 3 enthält ein Beispiel einer Risikomatrix, in der Wahrscheinlichkeit und Folgen in vier Risikomaße kombiniert sind.

In manchen Fällen kann man ein Risikoprofil erstellen, indem das Risikomaß als eine Wahrscheinlichkeitsverteilung eines Folgenbereichs dargestellt wird.

Die zur Berechnung der Risikomaße herangezogenen Daten sollten für die jeweilige Anwendung geeignet sein. Sofern möglich, sollten diese Daten auf den besonderen, gerade untersuchten Gegebenheiten beruhen. Sollte dies nicht möglich sein, sollten die Situation beschreibende Daten allgemeiner Art verwendet werden, ansonsten sollte man auf fachliche Beurteilungen zurückgreifen. Alle Annahmen sollten dokumentiert werden.

5.6.4 Risikobewertung

Bei der Risikobewertung werden geschätzte Risikomaße mit bekannten Risikokriterien verglichen, um so die Bedeutung des Risikos zu bestimmen und zu entscheiden, ob es vertretbar ist oder ob es behandelt werden muss. Risikokriterien sind unter anderem folgenden Quellen zu entnehmen:

- allgemein anerkannte industrielle Kriterien wie Sicherheitsniveaus;
- behördliche Vorschriften für spezielle Einrichtungen oder Anwendungen;
- aus den Zuverlässigkeitsspezifikationen stammende Kriterien;
- allgemeine Zuverlässigkeitsdatenquellen.

5.6.5 Verifizierung der Risikobeurteilung

Zur Prüfung und Bestätigung der Integrität der Analyse sollte von nicht an den Untersuchungen beteiligten Personen eine formale Bewertung und Überprüfung erfolgen. Solche Bewertungen können intern oder von externen, nicht an der Untersuchung beteiligten Organisationen durchgeführt werden.

Zur Verifizierung sollten folgende Schritte gehören:

- prüfen, ob der Zweck den vorgegebenen Zielsetzungen dienlich ist;
- alle kritischen Annahmen überprüfen und sicherstellen, dass sie angesichts der verfügbaren Informationen glaubhaft sind;
- sicherstellen, dass der Analyst geeignete Verfahren, Modelle und Daten verwendet hat;
- prüfen, ob die Analyse auch von anderen Personen als den erstmaligen Analysten wiederholt werden könnte;
- prüfen, ob die Ergebnisse der Analyse unempfindlich hinsichtlich Art und Weise der Formatierung der Daten oder Ergebnisse sind.

Sollten geeignete Betriebserfahrungen vorliegen, kann die Verifizierung direkt anhand eines Vergleichs der Analyseergebnisse mit den unmittelbaren Beobachtungen erfolgen.

5.6.6 Dokumentation

Im Bericht über die Risikobeurteilung sollten der Vorgang und die Ergebnisse der Risikobeurteilung dokumentiert werden. Die Assimilation (Einverleibung) technischer Informationen ist ein kritischer Teil des Risikobeurteilungsvorganges. Risikoschätzungen sollten in verständlichen Begriffen ausgedrückt, die Stärken und Einschränkungen der verschiedenen Risikomaße sollten erklärt werden und die Ungewissheiten der Risikoabschätzung sollten in einer für die beabsichtigte Leserschaft geeigneten Form erfolgen.

Der Umfang des Berichts hängt von den Zielsetzungen und dem Zweck der Beurteilung ab. Außer bei sehr einfachen Analysen sollte der Bericht üblicherweise die folgenden Punkte enthalten:

- Zusammenfassung;
- Schlussfolgerungen;
- Zielsetzungen und Zweck;
- Einschränkungen, Annahmen und Rechtfertigung von Hypothesen;
- Beschreibung der relevanten Systemteile;
- Beurteilungsmethodik;
- Ergebnisse der Risikoidentifizierung;
- verwendete Modelle einschließlich zugehöriger Annahmen und Validierung;
- Daten und deren Quellen;
- Ergebnisse der Risikoabschätzung;
- Sensitivitäts- und Ungewissheitsanalysen;
- Ergebnisbesprechung (einschließlich einer Besprechung der analytischen Schwierigkeiten);
- Verweise.

Falls die Risikobeurteilung zur Unterstützung eines nachhaltigen Risikomanagements benötigt wird, sollte diese Beurteilung so gestaltet und dokumentiert werden, dass sie während des Lebenszyklus' des Systems, der Anlage oder Tätigkeit gepflegt werden kann. Die Beurteilung sollte aktualisiert werden, sobald neue Informationen vorliegen oder wenn der Managementvorgang dies erfordern sollte.

5.7 Risikobehandlung

Die Art und Weise der Risikobehandlung im Kontext technischer Systeme hängt zuallererst von der Lebenszyklusphase ab, für die sie gefordert wird. In der Konzept- und Definitionsphase könnte es Optionen

zur Wahl unterschiedlicher technischer oder technologischer Vorgehensweisen geben. In der Entwicklungsphase müssen ggf. unterschiedliche Entwurfsalternativen in Erwägung gezogen werden, um auf nicht hinnehmbare Risikomaße reagieren zu können. Sobald Produkte in Betrieb genommen wurden, gehören zur Behandlung die Umsetzung von Lösungen wie neuer Konstruktionsentwurf oder Modifikation, Änderung der betrieblichen und Instandhaltungsprozeduren, verstärkte Instandhaltungstätigkeiten oder betriebliche Einschränkungen.

6 Verfahren zur Risikobeurteilung

6.1 Allgemeines

In diesem Abschnitt wird beschrieben, wie man für die Risikobeurteilung technischer Systeme geeignete Verfahren auswählen kann. In den Anhängen sind verschiedene Werkzeuge und Techniken mit Erläuterungen aufgeführt, wie diese Mittel zur Durchführung oder Unterstützung des Risikobeurteilungsvorganges eingesetzt werden können. Es kann manchmal nötig sein, mehr als ein Beurteilungsverfahren einzusetzen.

6.2 Verfahrensauswahl

Allgemein ausgedrückt sollte ein geeignetes Verfahren folgende Eigenschaften aufweisen:

- es sollte wissenschaftlich begründet und für das betrachtete System geeignet sein;
- es sollte Ergebnisse in einer Form liefern, die das Verständnis für die Art des Risikos erhöht und die aufzeigt, wie das Risiko gesteuert und beherrscht werden kann;
- es sollte von vielen Anwendern in einer nachvollziehbaren, wiederholbaren und überprüfbaren Weise einsetzbar sein.

Die Gründe für die Wahl der Verfahren sollten hinsichtlich Anwendbarkeit und Eignung angegeben werden. Wenn es hinsichtlich der Anwendbarkeit und Eignung irgendwelche Zweifel gibt, sollten alternative Verfahren angewendet und die Ergebnisse miteinander verglichen werden. Falls die Ergebnisse verschiedener Untersuchungen zusammengelegt werden, sollten die Methodiken und Ergebnisse miteinander verträglich sein.

Nachdem entschieden wurde, eine Risikobeurteilung durchzuführen und Zielsetzungen und Zweck festgelegt worden sind, sollte das oder die Beurteilungsverfahren anhand geeigneter Faktoren ausgewählt werden (siehe Bild 4). Beispiele sind:

- Systementwicklungsphase: In den frühen Entwicklungsphasen dürfen gröbere Verfahren verwendet werden; sie sollten aber verfeinert werden, sobald weitere Informationen verfügbar werden;
- Zielsetzungen der Untersuchung: Die Zielsetzungen der Risikobeurteilung wirken sich unmittelbar auf das einzusetzende Verfahren aus. Wenn beispielsweise ein Vergleich zwischen verschiedenen Optionen vorgenommen wird, so kann es erlaubt sein, ziemlich grobe Folgenmodelle für diejenigen Teile des Systems zu verwenden, die von den verschiedenen Optionen gar nicht betroffen sind;
- Art des zu untersuchenden Systems und der zu analysierenden Risiken;
- möglicher Schweregrad: Die Entscheidung darüber, wie tief die Risikobeurteilung gehen soll, sollte die anfänglich vermuteten Folgen widerspiegeln (obwohl dies ggf. später geändert werden muss, sobald erste Beurteilungen vorliegen);
- Forderungen an Personal, Fachwissen und andere Ressourcen: Ein gut durchgeführtes einfaches Verfahren wird bessere Ergebnisse liefern als ein schlecht durchgeführtes ausgeklügeltes Verfahren, vorausgesetzt, das einfache Verfahren erfüllt die Zielsetzungen und Zwecke der Beurteilung. Üblicherweise sollte der in die Beurteilung gesteckte Aufwand dem zu analysierenden potentiellen Risikoniveau entsprechen;
- Verfügbarkeit von Informationen und Daten. Einige Verfahren benötigen mehr Informationen und Daten als andere;
- Notwendigkeit zur Modifizierung/Aktualisierung der Risikobeurteilung: Die Risikobeurteilung muss möglicherweise in der Zukunft modifiziert oder aktualisiert werden; manche Verfahren sind dabei verbesserungsfähiger als andere;
- behördliche und vertragliche Forderungen.

6.3 Risikobeurteilungsverfahren

Risikobeurteilungsverfahren können auf verschiedene Weisen klassifiziert werden. Der Zweck der Kategorisierung liegt darin, die relativen Stärken und Einschränkungen der Verfahren zu begreifen. In mehreren Tabellen im Anhang A werden potentielle Verfahren zur Verdeutlichung einander gegenübergestellt.

Die erste Klassifizierung zeigt, wie das Verfahren auf jeden Schritt des Risikobeurteilungsverfahrens wie folgt angewendet wird:

- Risikoidentifizierung;
- Risikoanalyse – Wahrscheinlichkeitsermittlung: quantitativ, semi-quantitativ oder qualitativ;
- Risikoanalyse – Folgen identifizieren und ermitteln;
- Risikoanalyse – Risikoniveau;
- Risikobewertung.

Für jeden Schritt der Risikobeurteilung ist die Anwendung des Verfahrens entweder als stark anwendbar, anwendbar oder nicht anwendbar beschrieben (siehe Anhang A.2).

Anschließend werden die Merkmale dieser Verfahren in Anhang A.3 mittels folgender Punkte beschrieben:

- Art der zur Durchführung der Risikobeurteilung erforderlichen Ressourcen hinsichtlich des Engagements des Managements, Umfang und Grad des erforderlichen Fachwissens, Daten und Kostenaufwand;
- Komplexität der Risikoumgebung;
- der wahrscheinliche Grad der Ungewissheit in der Risikobeurteilung angesichts der verfügbaren Informationen; was wird zum Erreichen der Zielsetzungen gebraucht.

Zu jedem Faktor wird angegeben, ob er als hoch, mittel oder nieder eingestuft ist.

Jedes dieser Verfahren ist im Anhang B hinsichtlich der Art der erbrachten Beurteilung weiter ausgearbeitet, zusätzlich wird zur Anwendbarkeit in gewissen Situationen angeleitet.

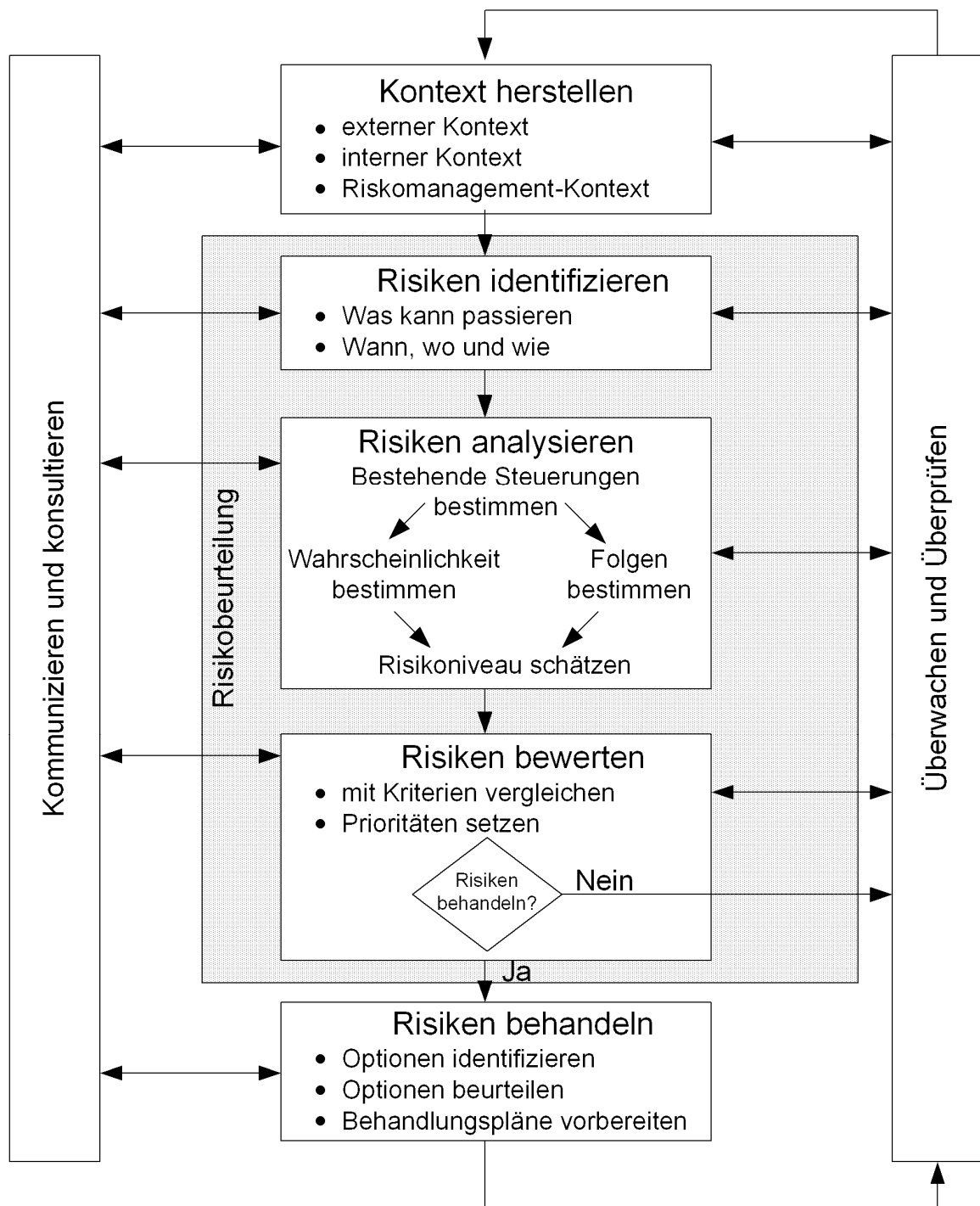


Bild 1 – Beziehungen bei der Risikobeurteilung (vereinfachte Darstellung)

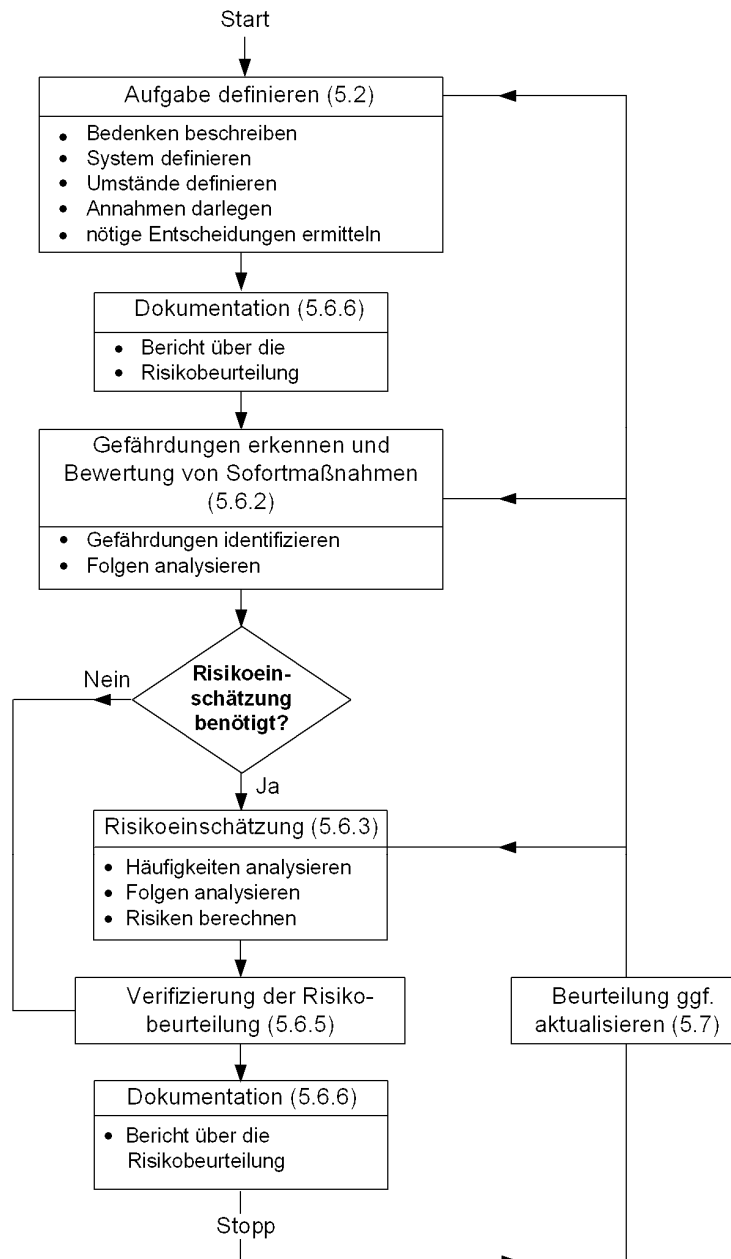


Bild 2 – Vorgehensweise zur Risikobeurteilung

Häufigkeit des Auftretens	Häufigkeitsbereich (je Jahr)	Schwere der Folgen			
		katastrophal	sehr schwer	schwer	gering
häufig	> 1	H	H	H	M
wahrscheinlich	$1 - 10^{-1}$	H	H	M	L
gelegentlich	$10^{-1} - 10^{-2}$	H	H	L	L
kaum denkbar	$10^{-2} - 10^{-4}$	H	H	L	L
unwahrscheinlich	$10^{-4} - 10^{-6}$	H	M	L	T
undenkbar	$< 10^{-6}$	M	M	T	T
ANMERKUNG Die Definition der Klassen und die Zahlenwerte in der Matrix sind nur beispielhaft.					

Bild 3 – Beispiel einer Risikomatrix

Die Risikoklassen sind dabei:

- H = Hohes Risiko
- M = Mittleres Risiko
- L = Leichtes Risiko
- T = Triviales Risiko

In diesem Beispiel sind die Klassen für die Schwere der Folgen wie folgt definiert:

- katastrophal Totalverlust der Anlage oder des Systems. Viele Todesfälle
- sehr schwer Umfangreiche Schäden an der Anlage oder am System. Einige Todesfälle
- schwer Schwere Personenschäden, schwere Krankheitsfälle, erhebliche Schäden an der Anlage oder am System
- gering leichte Personenschäden, geringfügige Krankheitsfälle oder geringe Schäden am System

– Entwurf –

E DIN IEC 60300-3-9 (VDE 0050-1):2007-05



Bild 4 – Typische Überlegungen bei der Auswahl der Analyseart und der Untersuchungstiefe

Anhang A (informativ)

Beurteilungsverfahren

A.1 Brainstorming

A.1.1 Beschreibung

Bei einem Brainstorming (Sammeln von spontanen Einfällen zur Problembewältigung) wird eine Gruppe von sachkundigen Personen dazu angeregt und ermutigt, in einer frei laufenden Konversation mögliche Ausfallarten und damit verbundene Gefährdungen, Risiken, Entscheidungskriterien und Optionen zur Steuerung und Bewältigung von Risiken zu identifizieren. Der Begriff Brainstorming wird oft sehr locker benutzt, um irgendwelche Gruppendiskussionen zu bezeichnen. Zu einem richtigen Brainstorming gehört jedoch eine besondere Technik, welche die Vorstellungskraft der Personen durch die Gedanken, Meinungen und Erklärungen der anderen Gruppenmitglieder spontan anregt.

Bei dieser Technik ist eine wirksame Sitzungsmoderation sehr wichtig, also Stimulation der Diskussion zu Beginn der Gesprächsrunde, periodische Umorientierung der Gruppe auf andere relevante Gebiete und Erfassung der sich aus der (meist lebhaften) Diskussion ergebenden Punkte.

A.1.2 Anwendung

Die Technik des Brainstormings kann sowohl in Verbindung mit den nachfolgend beschriebenen Risikobeurteilungsverfahren angewendet werden oder kann auch für sich alleine stehen als eine Technik, die zu spontanem Denken in jeder Stufe des Risikomanagementvorganges und in jeder Stufe des Lebenszyklus eines Systems ermutigt. Das Verfahren kann sowohl für Diskussionen auf höheren Ebenen verwendet werden, bei denen Punkte für spätere nähere Überprüfungen identifiziert werden oder aber in niedrigeren Ebenen zur Behandlung spezieller Probleme dienen.

Brainstorming bedarf einer starken Vorstellungskraft. Daher ist dieses Verfahren besonders dann nützlich, wenn Risiken neuer Technologien ermittelt werden sollen, für die es noch keine Erfahrungsdaten gibt und für die man neue Lösungsansätze sucht.

A.1.3 Vorgehensweise

Ein Brainstorming kann sowohl formal oder informal sein. Ein formales Brainstorming ist eher strukturiert, die Teilnehmer wurden vorbereitet und die Sitzung dient einem speziellen Zweck oder soll ein gewisses Ergebnis liefern, dabei gibt es Vorgehensweisen, die vorgebrachten Einfälle und Ideen zu bewerten. Ein informales Brainstorming ist dagegen weniger strukturiert und hat meist einen ad-hoc Charakter.

In einem formalen Prozess:

- bereitet der Moderator vor Sitzungsbeginn für den Kontext geeignete Stichworte vor, die neue Einfälle und Gedanken auslösen sollen;
- für die Sitzung werden Ziele vorgegeben und die Regeln erklärt;
- beginnt der Moderator mit einem Gedankengang und jeder Teilnehmer entwickelt anschließend eigene Ideen zu möglichst vielen Themen und Punkten. Zu diesem Zeitpunkt gibt es noch keine Diskussion darüber, ob Punkte in eine Liste aufgenommen werden sollten oder was mit gefallenem Bemerkungen und Aussagen geschehen soll, da dadurch der freie Gedankenfluss gebremst würde. Alle Gedanken und Anregungen werden akzeptiert und keine(r) wird kritisiert und die Gruppe fährt zügig fort, damit auch am Rande liegende Einfälle eine Chance haben;
- Der Moderator kann Teilnehmer auf einen neuen Gedankenweg lenken, falls eine Gedankenrichtung erschöpft ist oder wenn die Diskussion zu sehr vom Thema abweicht. Es ist dabei beabsichtigt, möglichst viele unterschiedliche Ideen zu sammeln, um diese dann später zu sichten.

A.1.4 Stärken und Einschränkungen

Zu den Stärken eines Brainstormings gehören:

- es reizt die Vorstellungskraft an, welche neue Risiken es geben könnte und wie neuartige Lösungen aussehen könnten;
- Geschäftsinteressenten sind beteiligt und man verbessert dadurch die Kommunikation untereinander;
- es ist ziemlich schnell und leicht umzusetzen.

Zu den Einschränkungen eines Brainstormings gehören folgende Punkte:

- da es relativ unstrukturiert ist, wird es schwierig nachzuweisen, dass der Prozess umfassend war (ob beispielsweise alle potentiellen Risiken identifiziert worden sind);
- es kann sich eine besondere Gruppendynamik ergeben, wodurch Personen mit wertvollen Ideen schweigen und andere die Diskussion dominieren. Dies könnte durch ein rechnergestütztes Brainstorming in einem Chatforum überwunden werden. Ein rechnergestütztes Brainstorming kann auch anonym gestaltet werden, falls in einer offenen Diskussion der freie Gedankenfluss bei heiklen Themen gebremst werden könnte.

A.2 Strukturierte und semi-strukturierte Befragungen

A.2.1 Beschreibung

Bei einer strukturierten Befragung wird einzelnen, von einander getrennten Personen von einem Moderator ein Satz Fragen gestellt, der so vorbereitet und gestaltet ist, dass er den Befragten dazu anregt, eine Situation oder Gegebenheit aus einem anderen Blickwinkel zu sehen und so Risiken aus dieser Perspektive identifizieren hilft. Eine semi-strukturierte Befragung ist ähnlich, erlaubt aber eine freiere Konversation zur Erkundung neu auftauchender Punkte.

Zu den vorbereitenden Arbeiten dieser Fragetechnik gehört die Ausarbeitung und Gestaltung eines entsprechenden Fragenkatalogs, der den Befragten leiten soll. Fragen sollten im Ergebnis möglichst offen sein, und die Antworten müssen mit einer gewissen Flexibilität aufgenommen werden, damit die Befragung gegebenenfalls auch in andere, sich neu abzeichnende Richtungen gehen kann.

A.2.2 Anwendung

Strukturierte und semi-strukturierte Befragungen sind dann angebracht, wenn es schwierig ist, eine Gruppe von Personen zu einer Brainstorming-Sitzung zusammenzubringen oder falls ein freier Diskussionsfluss in der gegebenen Situation oder in Anbetracht der beteiligten Personen nicht opportun ist. Befragungen können in allen Projekt- oder Prozessstufen angewendet werden.

A.2.3 Stärken und Einschränkungen

Die Stärken einer strukturierten Befragung sind:

- die Zeit, die den Befragten für eine ausführliche Erörterung eines Themas zur Verfügung steht;
- die intensivere Themenerörterung, die bei einem Gespräch zwischen zwei Personen möglich wird.

Die Einschränkungen einer strukturierten Befragung sind:

- der Zeitaufwand für den Moderator, wenn er auf diese Weise mehrfache Meinungen erhalten möchte;
- die Hemmung spontaner Einfälle, die ein Merkmal des Brainstormings sind.

A.3 Delphi-Methode

A.3.1 Beschreibung

Die Delphi-Methode ist ein Verfahren, um einen verlässlichen Meinungskonsens einer Expertengruppe zu erhalten. Obwohl dieser Begriff neuerdings häufig für irgendeine Form von Brainstorming verwendet wird, ist es ein unerlässliches Merkmal der Delphi-Methode, dass Experten ihre Meinung anonym und individuell ausdrücken, dabei aber Zugang zu den von den anderen Gruppenmitgliedern geäußerten Meinungen haben, je nach Untersuchungsfortgang.

A.3.2 Anwendung

Die Delphi-Methode kann immer dann in einer Stufe des Risikomanagementprozesses oder in einer Phase eines Systemlebenszyklus' eingesetzt werden, wenn eine gemeinsame Expertensicht und Konsens gefragt ist.

A.3.3 Vorgehensweise

Einer Expertengruppe wird ein semi-strukturierter Fragebogen zur Beantwortung vorgelegt. Die Experten treffen sich nicht, so dass deren Meinungen unabhängig voneinander bleiben.

Dabei gibt es folgende Schritte:

- Bildung eines Teams um den Delphi-Prozess zu veranlassen und zu überwachen;
- Nominierung einer Expertengruppe (dabei kann es eine oder mehrere Expertengremien geben);
- einen Fragebogen entwickeln (erste Befragungsrunde)
- den Fragebogen testen
- den Fragebogen den Experten einzeln schicken
- die Informationen aus der ersten Antwortrunde werden analysiert und kombiniert und dann den Gremienmitgliedern übermittelt
- Gremienmitglieder antworten und der Prozess wird so lange wiederholt, bis Konsens erreicht wird.

A.3.4 Stärken und Einschränkungen

Zu den Stärken der Delphi-Methode gehören:

- da die Meinungen anonym bleiben, steigt die Wahrscheinlichkeit, dass auch unpopuläre Meinungen vorgebracht werden;
- alle Ansichten sind gleichgewichtig – dadurch entfällt das Problem dominierender Persönlichkeiten;
- die Teilnehmer machen sich die Ergebnisse zu eigen
- die Personen brauchen nicht an einem Ort und zur selben Zeit zusammenkommen.

Zu den Einschränkungen gehören:

- die Technik ist arbeits- und zeitaufwändig;
- die Teilnehmer müssen sich klar und deutlich in schriftlicher Form ausdrücken können.

A.4 Prüflisten

A.4.1 Beschreibung

In Prüflisten (en: check list) sind Gefährdungen, Risiken oder fehlgeschlagene Risikosteuerungen sowohl als Ergebnis früherer Risikobeurteilungen als auch als Ergebnis früherer Ausfälle aufgelistet.

A.4.2 Anwendung

Mit einer Prüfliste kann man Gefährdungen oder Risiken identifizieren oder die Wirksamkeit von Steuerungsmaßnahmen beurteilen. Prüflisten können in jeder Stufe des Lebenszyklus' eines Produkts, Prozesses oder Systems verwendet werden. Sie können als Teil eines Risikobeurteilungsverfahrens eingesetzt werden, sind jedoch dann besonders leistungsfähig, wenn man anhand solcher Listen überprüfen möchte, ob alles erfasst und bedacht wurde, nachdem man bereits phantasievollere Techniken verwendet hatte.

A.4.3 Vorgehensweise

Die Schritte sind:

- den Zweck der Maßnahme festlegen;
- eine dem Zweck entsprechende und geeignete Prüfliste mit großer Sorgfalt auswählen. Beispielsweise kann man mit standardisierten Prüflisten keine neuen Gefährdungen oder Risiken ermitteln;
- das die Prüfliste einsetzende Team oder Person nimmt sich schrittweise jedes Element des Prozesses oder des Systems vor und überprüft, ob in der Prüfliste genannte Themen für das jeweilige Element zutreffend sind.

A.4.4 Stärken und Einschränkungen

Zu den Stärken gehören:

- Prüflisten können auch von Nicht-Fachleuten verwendet werden;
- gut gestaltete Prüflisten können einen breiten Wissensbereich zu einem leicht handhabbaren Werkzeug kombinieren;
- Prüflisten können helfen, übliche Probleme nicht zu übersehen.

Zu den Einschränkungen gehören:

- durch Prüflisten wird die Vorstellungskraft zur Auffindung neuer Probleme gehemmt;
- durch Prüflisten ist man geneigt, nur auf Bekanntes zu achten und könnte daher verdeckte Probleme nicht sofort wahrnehmen;
- Prüflisten können nicht auf neue Situationen angewendet werden, für die es noch keine soliden Erfahrungen gibt, anhand derer man eine Liste erarbeiten könnte.

A.5 Vorläufige Untersuchung von Gefährdungen (PHA)

A.5.1 Beschreibung

Die vorläufige Untersuchung von Gefährdungen (auch vorläufige Sicherheitsanalyse, englisch: preliminary hazard analysis, PHA genannt) ist ein einfaches, induktives Analyseverfahren zur Identifizierung von Gefährdungen, gefahrbringenden Situationen und Ereignissen, die eine gegebene Tätigkeit, Anlage oder System schädigen können.

A.5.2 Anwendung

Eine vorläufige Untersuchung von Gefährdungen wird üblicherweise früh in der Projektentwicklung eingesetzt, wenn es noch keine Einzelheiten zum Konstruktionsentwurf oder zu den Betriebsprozeduren gibt. PHA kann auch ein Vorläufer weiterer Untersuchungen sein oder Angaben für die Spezifizierung eines Systementwurfs liefern. Bei der Analyse existierender Systeme kann es für die Priorisierung und gegebenenfalls zur weiteren Untersuchung von Gefährdungen und Risiken nützlich sein oder wenn die Umstände den Einsatz umfassenderer Verfahren verhindern.

A.5.3 Benötigte Daten

- Verständnis des beabsichtigten Zwecks des zu beurteilenden Systems;
- die zum Systementwurf vorhandenen Einzelheiten.

A.5.4 Vorgehensweise

- Eine Liste von Gefährdungen und allgemeiner gefahrbringender Situationen und Risiken wird erarbeitet, indem man folgende Merkmale erörtert und beachtet:
 - verwendete oder produzierte Materialien und deren Reaktivität;
 - eingesetzte Geräte;
 - Betriebsumgebung;
 - Auslegung (layout);
 - Schnittstellen zwischen Systemkomponenten, usw.
- es kann eine qualitative Analyse der Folgen unerwünschter Ereignisse und deren Wahrscheinlichkeit durchgeführt werden, um so Risiken zur weiteren Analyse zu identifizieren;
- PHA sollte in den Entwicklungsphasen Entwurf, Konstruktion und Prüfung aktualisiert werden, um etwaige neue Gefährdungen zu erkennen und diese nötigenfalls zu korrigieren. Die so erhaltenen Ergebnisse können auf unterschiedliche Weisen präsentiert werden, beispielsweise in Tabellen oder Bäumen.

A.5.5 Ergebnisse

- eine Liste der Gefährdungen und Risiken;
- Empfehlungen zur Annahme, zur Steuerung und Bewältigung, Entwurfsspezifikation oder Forderungen nach detaillierterer Beurteilung.

A.5.6 Stärken und Einschränkungen

Zu den Stärken einer PHA gehören, dass:

- man sie auch dann anwenden kann, wenn nur dürftige Informationen vorliegen;
- man mit ihr schon sehr früh im Systemlebenszyklus Risiken erörtern kann.

Zu den Einschränkungen einer PHA gehören:

- eine PHA liefert nur vorläufige Informationen, diese werden nicht umfassend sein und keine detaillierten Informationen zu Risiken und liefern, noch wie diese am Besten vermieden werden können.

A.6 Gefährdungs- und Betreibbarkeitsuntersuchung (HAZOP)

A.6.1 Beschreibung

Die Gefährdungs- und Betreibbarkeitsuntersuchung (en: HAZard and OPerability study, HAZOP) ist eine strukturierte und systematische Untersuchung eines geplanten oder auch bereits existierenden Produkts oder technischen Prozesses (technischen Verfahrens). Mit dieser Technik können potentielle oder existierende Sicherheits- oder Betriebsprobleme aufgefunden und bewertet werden, die ein Risiko für Personen, Gerät, Umwelt und organisatorische Ziele darstellen könnten. Von dem Untersuchungsteam wird erwartet, dass es eine Lösung anbietet, wie die identifizierte Gefährdung oder das Betriebsproblem beseitigt werden können, sofern dies möglich ist.

Grundlage des qualitativen Prozesses von HAZOP ist eine Untersuchung mittels so genannter „Leitworte“, bei der hinterfragt wird, inwieweit die Auslegungsziele bzw. die Betriebsbedingungen in jedem Entwicklungsschritt erreicht werden. Die Untersuchung wird von einem multidisziplinären Team in mehreren Sitzungen durchgeführt.

A.6.2 Anwendung

Das HAZOP-Verfahren ist ursprünglich in der Verfahrenstechnik zur Analyse chemischer Prozess-Systeme entwickelt worden und wurde später auf andere Arten von Systemen und komplexe Betriebsweisen ausgeweitet. Beispiele hierfür sind mechanische und elektronische Systeme, Verfahrenstechnik allgemein,

– Entwurf –

E DIN IEC 60300-3-9 (VDE 0050-1):2007-05

Softwaresysteme und sogar Organisationsänderungen und Gestaltung von Verträgen und deren Überprüfung.

Mit dem HAZOP-Verfahren können alle Formen von Abweichungen von der Sollfunktion aufgrund von Konstruktionsmängeln (im Konstruktionsentwurf oder den Komponenten), schlecht geplanten Prozessen und menschlichen Aktionen behandelt werden.

Das HAZOP-Verfahren wird in breiter Weise zur Überprüfung von Softwareentwürfen (en: software design review) verwendet. Bei der Anwendung auf Sicherheits-kritische Instrumentensteuerung und Rechnersysteme ist es auch unter dem Namen CHAZOP (en: Control Hazards and Operability Analysis oder Computer Hazard and Operability analysis) bekannt.

Eine HAZOP-Untersuchung findet üblicherweise in der Stufe des Detailentwurfs statt, wenn ein genaues Diagramm des beabsichtigten technischen Prozesses bereits vorliegt, aber immer noch Änderungen am Konstruktionsentwurf praktikabel sind. Eine HAZOP-Untersuchung kann auch in der Betriebsphase erfolgen, sich daraus ergebende Änderungen können dann aber teuer werden.

A.6.3 Benötigte Daten

Die für eine HAZOP-Untersuchung benötigten Daten sind im Wesentlichen aktuelle Informationen über das zu überprüfende System bzw. den technischen Prozess und die Spezifikationen für die von der Konstruktion geforderte Sollfunktion und Leistung. Zu den benötigten Daten gehören: Zeichnungen, Spezifikationsblätter, Flussdiagramme, Diagramme zur Prozess-Steuerung und Logik, Übersichtszeichnungen, Betriebs- und Instandhaltungs- und Notfallprozeduren.

A.6.4 Vorgehensweise

Bei einer HAZOP-Untersuchung nimmt man die Unterlagen (Konstruktionsunterlagen und Spezifikationen) des (der) zu untersuchenden Prozesses, Prozedur bzw. Systems und überprüft und bewertet jedes Teil dahingehend, welche Abweichungen von der Sollfunktion eintreten können, die potentiellen Ursachen hierfür und die wahrscheinlichen Folgen einer Abweichung. Dies erreicht man durch eine systematische Untersuchung, wie jedes Teil des Systems, Prozesses oder der Prozedur auf Änderungen der Schlüsselparameter reagiert, dafür verwendet man geeignete Leitworte. Leitworte können für ein gegebenes System, Prozess oder Prozedur maßgeschneidert werden, oder man nimmt allgemeine Worte, die für alle Abweichungsarten zutreffend sind. Tabelle A.1 enthält Beispiele üblicher Leitworte.

Zu den üblichen Schritten einer HAZOP-Untersuchung gehören:

- Verantwortlichkeit festlegen. Eine Person benennen, welche die nötige Verantwortlichkeit und Zuständigkeit besitzt, die HAZOP-Untersuchung zu führen. Sie muss sich später darum kümmern, dass gegebenenfalls zu ergreifende Maßnahmen auch umgesetzt werden;
- Zweck und Ziel der Untersuchung festlegen;
- Schlüsselemente oder Leitworte für die Untersuchung erarbeiten;
- Ein HAZOP-Untersuchungsteam benennen. Dieses Team ist üblicherweise multidisziplinär zusammengesetzt, darin sollten Fachleute aus Entwicklung und Betrieb mitwirken, die geeignetes Fachwissen haben, um die Wirkung von Abweichungen von der Sollfunktion bewerten zu können. Darüber hinaus wird empfohlen, dass dem Team auch Personen angehören, die nicht direkt an der Entwicklung des zu bewertenden Systems, Prozesses oder Prozedur beteiligt sind;
- benötigte Dokumentation zusammen tragen;
- in einem Workshop mit dem Untersuchungsteam
 - System, Prozess oder Prozedur in kleinere Elemente oder Subsysteme oder Prozesse aufgliedern und so die Bewertung handhabbar machen;
 - für jedes Subsystem oder Prozess oder Element sich über die jeweilige Sollfunktion einigen und dann auf jede Einheit in diesem Subsystem oder Element die Leitworte nach einander anwenden und so mögliche Abweichungen mit unerwünschten Ergebnissen ermitteln;

- falls ein unerwünschtes Ergebnis identifiziert wurde, sich über dessen Ursache und Folgen in jedem Einzelfall einigen und vorschlagen, wie diese behandelt werden könnten, damit sie erst gar nicht eintreten, oder falls dennoch, wie die daraus resultierenden Folgen abgemindert werden könnten;
- die Diskussion dokumentieren und spezielle Aktionen zur Behandlung der identifizierten Risiken vereinbaren.

Tabelle A.1 – Beispiele möglicher HAZOP-Leitworte

Leitwort	Bedeutung
kein (nicht/kein/keine)	kein Teil der Sollfunktion wird erreicht oder die beabsichtigte Bedingung ist nicht gegeben
mehr (höher)	quantitative Zunahme der Ausgabe (Leistung) oder der Betriebsbedingungen
weniger (niedriger)	quantitative Abnahme
sowohl als auch	quantitative Zunahme (z. B. mehr Material)
teilweise	quantitative Abnahme (z. B. nur eine oder zwei Komponenten in einem Gemenge)
Umkehrung	entgegen gesetzter Ablauf (z. B. Rücklauf)
anders als	die Sollfunktion wird überhaupt nicht erreicht, es geschieht etwas vollkommen anderes (es fließt beispielsweise das falsche Material)
Kompatibilität	Material, Umwelt
Die Leitworte werden auf folgende Parameter angewendet:	
	physikalische Eigenschaften eines Materials oder Prozesses
	physikalische Bedingungen wie Temperatur, Geschwindigkeit
	Sollfunktion einer Komponente eines Systems oder eines Konstruktionsentwurfs (z. B. Informationsübertragung)
	betriebliche Gesichtspunkte

A.6.5 Ergebnisse

Die Sitzungen des HAZOP-Teams werden protokolliert, im Sitzungsbericht ist jeder überprüfte Punkt bzw. Thema zu nennen. Im Bericht ist folgendes anzugeben: das verwendete Leitwort, die Abweichung(en), mögliche Ursachen, Maßnahmen zur Behandlung der identifizierten Probleme und die dafür verantwortliche Person.

Für jede nicht behebbare Abweichung muss das entsprechende Risiko beurteilt werden.

A.6.6 Stärken und Einschränkungen

Zu den Stärken einer HAZOP-Untersuchung gehören:

- systematische und umfassende Vorgehensweise zur Untersuchung eines Systems, Prozesses oder einer Prozedur;
- multidisziplinäres Team, Teammitglieder haben zum einen wirkliche Betriebserfahrung, andere werden gegebenenfalls Abhilfemaßnahmen ausführen müssen;
- es werden Lösungen erarbeitet und Maßnahmen zur Risikobehandlung vorgeschlagen;
- kann auf viele und verschiedenartige System, Prozesse oder Prozeduren angewendet werden;
- ermöglicht explizit die Erörterung der Folgen und Auswirkungen menschlicher Fehlhandlungen;
- ergibt eine schriftliche Aufzeichnung des Prozesses, dieser Bericht kann dazu verwendet werden, die Dringlichkeit zu demonstrieren.

– Entwurf –

E DIN IEC 60300-3-9 (VDE 0050-1):2007-05

Zu den Einschränkungen einer HAZOP-Untersuchung gehören:

- kann sehr zeitaufwändig und daher teuer sein;
- benötigt einen sehr großen Dokumentationsaufwand oder umfangreiche Spezifikationen zu System, Prozess oder Prozedur;
- auf Grund der benötigten umfangreichen Dokumentation findet die HAZOP-Untersuchung üblicherweise erst zu einem sehr späten Entwicklungszeitpunkt statt (wenn Daten zum Detailentwurf vorliegen), dann sind vorgeschlagene größere Modifizierungen meist zu teuer und nicht haltbar;
- das Team könnte sich zu sehr darauf konzentrieren, Lösungen zu finden anstelle sich zu fragen „warum tun wir dies“;
- die Diskussion könnte sich zu sehr um Konstruktionsdetails drehen und darüber eine breitere Sichtweise verlieren;
- sie ist auf den/die dem Team vorgegebenen vorläufigen Konstruktionsentwurf, Sollfunktion und Untersuchungszweck und -ziel beschränkt;
- die Vorgehensweise fordert den Entwicklern angesichts ihres Fachwissens viel ab, diese könnten sich damit schwer tun, mit genügender Objektivität Probleme in ihren eigenen Entwürfen zu suchen.

A.6.7 Vergleiche

Die HAZOP-Untersuchung ähnelt einer Fehlzustandsart- und –auswirkungsanalyse (FMEA) dahingehend, dass man mit ihr Ausfallarten eines Prozesses oder Gerätes und auslösende Ursachen und Folgen identifizieren kann. HAZOP unterscheidet sich insofern von einer FMEA, dass das Team unerwünschte Ergebnisse sowie Abweichungen von der Sollfunktion her betrachtet und von dort aus rückwärts bis zu möglichen Ursachen und Ausfallarten arbeitet, wogegen eine FMEA mit der Identifizierung von Ausfallarten beginnt.

A.6.8 Verweise

IEC 61882 „Hazard and Operability studies (HAZOP studies) – Application guide“

A.7 Strukturiertes „Was-Wenn“-Verfahren (SWIFT)

A.7.1 Beschreibung

Das strukturierte „Was-Wenn“-Verfahren (en: structured What-If, SWIFT) ist ursprünglich als eine wirksamere Alternative zu HAZOP entwickelt worden. Es ist ein systematisches, Team-basiertes Verfahren, bei dem der Moderator in einem Workshop bestimmte Stichwörter oder Sätze einsetzt, durch die die Teilnehmer zur Identifizierung von Risiken und Gefährdungen stimuliert werden sollen. Der Moderator und das Team verwenden standardisierte Fragesätze der Art „Was-Wenn“ in Kombination mit dem Stichwort und untersuchen auf diese Weise, wie sich Abweichungen im Betrieb und im Verhalten auf ein System, ein Anlagenteil, eine Organisation oder Prozedur auswirken. SWIFT wird eher in höheren Systemebenen und mit geringerem Tiefgang als HAZOP eingesetzt.

A.7.2 Anwendung

SWIFT wurde ursprünglich für die Untersuchung der von chemischen und petrochemischen Anlagen möglicherweise ausgehenden Gefährdungen entworfen, jetzt wird das Verfahren in breiter Weise auf Systeme, Anlagenteile, Prozeduren und allgemein auf Organisationen angewendet. Es wird insbesondere eingesetzt, um die Folgen von Änderungen und dabei veränderten oder neu erzeugten Risiken zu untersuchen.

A.7.3 Benötigte Daten

System, Prozedur, Anlagenteile und Änderung müssen sorgfältig vor Untersuchungsbeginn festgelegt werden. Sowohl der externe und der interne Kontext werden vom Moderator durch Interviews und durch das Studium von Dokumenten, Plänen und Zeichnungen hergestellt. Üblicherweise wird die zu untersuchende

Einheit, Situation oder das System zur leichteren Analyse in Knoten oder Schlüsselemente aufgespalten. Dabei dringt die Untersuchung höchst selten in die bei HAZOP geforderte Tiefe vor.

Eine weitere wichtige Voraussetzung ist, dass im Untersuchungsteam geeignetes Fachwissen und Erfahrung präsent sind, das Team sollte daher entsprechend sorgfältig zusammengestellt werden. Alle Geschäftsinteressenten sollten vertreten sein sowie möglichst solche Personen, die Erfahrungen mit ähnlichen Einheiten, Systemen, Änderungen oder Situationen haben. Üblicherweise sind Teams mit vier bis zwanzig Mitgliedern am wirkungsvollsten.

A.7.4 Vorgehensweise

Im Allgemeinen wird wie folgt vorgegangen.

- Vor Untersuchungsbeginn bereitet der Moderator eine passende Liste mit Stichworten oder Sätzen vor, diese Liste kann aus einer dafür üblichen Zusammenstellung abgeleitet werden oder extra dafür geschaffen werden und sollte eine umfassende Überprüfung und Bewertung der Gefährdungen und Risiken erlauben.
- Im Workshop diskutiert und einigt man sich auf den externen und internen Kontext mit der Einheit, dem System, der Änderung oder der Situation und auf den Zweck der Untersuchung.
- Der Moderator befragt die Teilnehmer nach:
 - bekannten Risiken und Gefährdungen;
 - früheren Erfahrungen und Vorfällen;
 - bekannten und existierenden Steuerungs- und Sicherungsvorkehrungen;
 - behördlichen Vorgaben und Einschränkungen.
- Die Diskussion wird durch einen „Was-Wenn“-Satz und einem Stichwort oder Thema angereizt. Die anzuwendenden „Was-Wenn“-Sätze sollten folgendermaßen oder in ähnlicher Weise beginnen: „Was wenn...“, „Was würde geschehen, falls...“, „Könnte jemand oder etwas ...“, „Hat jemand jemals oder hat irgendwas...“. Dadurch soll das Untersuchungsteam stimuliert werden, potentielle Szenarien, deren Ursachen und Folgen und Wirkungen zu erforschen.
- Die Risiken werden zusammengefasst, und das Team erörtert bereits vorhandene Überwachungs- und Steuerungsmaßnahmen.
- Die Beschreibung der Risiken, ihre Ursachen, Folgen, und die erwarteten Überwachungs- und Steuerungsmaßnahmen werden vom Team bestätigt und aufgezeichnet.
- Das Team erörtert, ob die Überwachungs- und Steuerungsmaßnahmen geeignet und wirksam sind und einigt sich über eine Aussage zur Wirksamkeit der Überwachungs- und Steuerungsmaßnahmen. Sollten diese nicht zufrieden stellend sein, bespricht das Team weitere Behandlungsmaßnahmen, und es werden andere mögliche Überwachungs- und Steuerungsmaßnahmen festgelegt.
- Während diesen Diskussionen werden weitere „Was-Wenn“ Fragen gestellt, und der Vorgang wird wiederholt, um weitere Risiken zu identifizieren.
- Der Moderator begleitet mittels der Stichwortliste die Diskussion und schlägt dem Team zusätzliche Themen und Szenarien zur Diskussion vor.
- Üblicherweise ordnet man mit Hilfe eines qualitativen oder semi-qualitativen Risikoanalyseverfahrens die beschlossenen Maßnahmen nach deren Priorität. Bei der Risikoanalyse werden üblicherweise die bereits vorhandenen Überwachungs- und Steuerungsmaßnahmen und deren Wirksamkeit berücksichtigt.

A.7.5 Ergebnisse

Man erhält ein Risiken- und Gefährdungsregister mit nach der Wichtigkeit geordneten Maßnahmen oder Aufgaben. Diese Aufgaben können dann Grundlage für einen Behandlungsplan sein.

A.7.6 Stärken und Einschränkungen

Zu den Stärken von SWIFT gehören:

- Es kann in breitem Maße auf alle Arten von technischen Anlagen, Systemen, Situationen oder Umständen, Organisation oder Tätigkeit angewendet werden;
- es bedarf seitens des Teams nur geringer Vorbereitung;
- es ist relativ schnell, und die größten Gefährdungen und Risiken werden in der Workshop-Sitzung offensichtlich;
- die Untersuchung ist System-orientiert und ermöglicht es den Teilnehmern zu erkennen, wie das System auf Abweichungen reagiert, und es werden so nicht nur die Folgen von Komponenten- und Bauelementeausfällen untersucht;
- mit ihm kann man Gelegenheiten zur Verbesserung von technischen Prozessen und Systemen ermitteln; allgemein eignet es sich, um Maßnahmen zu ermitteln, die sich wahrscheinlich positiv auf die Folgen auswirken;
- Beteiligung solcher Personen, die für vorhandene Überwachungs- und Steuerungsmaßnahmen zuständig und für weitere Maßnahmen zur Risikobehandlung verantwortlich sind, wodurch deren Verantwortlichkeit gestärkt wird;
- man erhält ein Risiken- und Gefährdungsregister und einen Plan zur Behandlung von Risiken- und Gefährdungen mit nur geringem Zusatzaufwand;
- obwohl oft eine qualitative oder semi-qualitative Risikoklassifizierung zur Risikoanalyse und Priorisierung der sich ergebenden Maßnahmen verwendet wird, kann man mit SWIFT Risiken und Gefährdungen identifizieren, die dann Eingang in eine quantitative Untersuchung finden.

Zu den Einschränkungen von SWIFT gehören:

- Es bedarf eines erfahrenen und fähigen Moderators;
- der Workshop muss sorgfältig vorbereitet werden, sonst könnte die Zeit der Teilnehmer vergeudet werden;
- falls das Workshopteam keine ausreichend breite Erfahrungsgrundlage hat, oder falls das Stichwortsystem nicht umfassend genug ist, könnten manche Risiken und Gefährdungen nicht identifiziert werden;
- da das Verfahren hauptsächlich höhere Ebenen betrachtet, könnten komplexe, einzelne oder miteinander verbundene Ursachen nicht offen gelegt werden.

A.7.7 Vergleiche

Wie die meisten deduktiven Verfahren zur Risikoidentifizierung kann man mit dem SWIFT-Verfahren die bedeutendsten Risiken und Gefährdungen schnell ermitteln.

SWIFT kann häufig zur groben Identifizierung von Subsystemen und Komponenten eingesetzt werden, die dann später tiefer gehend mittels anderer Verfahren wie HAZOP, FTA oder FMECA analysiert werden.

A.7.8 Verwandte Verfahren

Brainstorming und normale „Was-Wenn“-Techniken gehen ähnlich vor. Jedoch erreicht man durch das Stichwortsystem, dass die Risikoidentifizierung umfassend ist. Auf Prüflisten basierende Verfahren sind ähnlich, aber bei SWIFT sieht und benützt üblicherweise lediglich der Moderator die Stichwortliste, so dass die Diskussion durch diese Liste nicht eingeschränkt wird.

A.8 Fehlzustandsart- und auswirkungsanalyse (FMEA) und FMECA

A.8.1 Beschreibung

Fehlzustandsart- und -auswirkungsanalyse (FMEA) und die Ausfallbedeutungsanalyse (FMECA) (en: Failure Modes and Effects and Criticality Analysis, FMECA)^{N4} sind Verfahren zur Ermittlung der Art und Weise, in der Komponenten oder Systeme ausfallen können und somit nicht mehr ihre Sollfunktion erbringen.

Mit einer FMEA kann Folgendes ermittelt und identifiziert werden:

- alle potentiellen Ausfallarten der verschiedenen Systemteile;
- die Auswirkung, die diese Ausfälle auf das System haben können;
- Ausfallursachen;
- wie man solche Ausfälle vermeiden oder die Ausfallauswirkung für das System vermindern kann.

Die Ausfallbedeutungsanalyse (FMECA) erweitert eine FMEA dahingehend, dass jede ermittelte Ausfallart gemäß der Bedeutung des kombinierten Einflusses auf die Eintrittswahrscheinlichkeit und auf die Schwere ihrer Folgen eingestuft wird. Diese Analyse ist üblicherweise qualitativer oder semi-quantitativer Art, sie kann jedoch bei Verwendung aktueller Ausfallraten quantifiziert werden.

A.8.2 Anwendung

Eine FMEA bzw. FMECA kann während der Entwicklung, Fertigung oder in der Betriebsphase eines Systems angewendet werden; sich aus der Analyse ergebende Änderungen sind üblicherweise in der Entwicklungsstufe leichter umzusetzen.

Eine FMEA bzw. FMECA kann zu Folgendem verwendet werden:

- bei der Auswahl von Entwurfsalternativen für höhere Zuverlässigkeit assistieren;
- sicherstellen, dass alle Ausfallarten und deren Auswirkung auf einen erfolgreichen Betrieb berücksichtigt worden sind;
- potentielle Ausfälle auflisten und die Schwere ihrer Auswirkung identifizieren;
- eine Grundlage für die Prüfplanung und Instandhaltung liefern;
- eine Grundlage für quantitative Zuverlässigkeitsanalysen liefern.

Sie wird meist auf Fehlzustände in Komponenten physikalischer Systeme angewendet, kann jedoch auch zur Ermittlung menschlicher Versagensarten und deren Auswirkungen benützt werden.

Die FMEA und FMECA können auch Eingaben für andere Analysetechniken liefern, wie beispielsweise für qualitative oder quantitative Fehlzustandsbaumanalysen.

A.8.3 Benötigte Daten

Für eine FMEA benötigt man ausreichend detaillierte Informationen über die Komponenten (bzw. Bauelemente) eines Systems, damit man in sinnvoller Weise analysieren kann, auf welche Art und Weise jede Komponente ausfallen kann. Hierzu gehören unter anderem:

- Zeichnungsunterlagen des untersuchten Systems und seiner Komponenten;
- Zeichnungsunterlagen oder Informationen über die Komponenten des untersuchten Systems;
- Einzelheiten zum Prozess und zu Umweltparametern, die sich auf den Betrieb auswirken könnten;
- Betreiberschnittstellen;

^{N4} Für die Fehlzustandsart-, auswirkungs- und -kritizitätsanalyse, englisch "Failure Modes and Effects and Criticality Analysis, FMECA" wird in dieser deutschen Übersetzung, wo sinnvoll, der geläufigere Begriff "Ausfallbedeutungsanalyse" nach DIN 25448 verwendet.

E DIN IEC 60300-3-9 (VDE 0050-1):2007-05

- Verständnis für die Ergebnisse bestimmter Ausfälle;
- Erfahrungsberichte über Ausfälle einschließlich eventuell vorhandener Daten.

A.8.4 Vorgehensweise

Die Schritte zur Durchführung einer FMEA sind:

- Zweck und Zielsetzung der Untersuchung festlegen;
- das Untersuchungsteam zusammenstellen;
- das einer FMECA zu unterziehende System verstehen lernen;
- das System in seine Komponenten oder Schritte aufteilen;
- für jede aufgelistete Komponente oder jeden Schritt Folgendes ermitteln:
 - Wie kann jedes Teil denkbarerweise ausfallen?
 - Welche Mechanismen könnten diese Ausfallart bewirken?
 - Was wären die Folgen, falls diese Ausfälle eintreten würden?
 - Geht der Ausfall in eine sichere oder unsichere Richtung?
 - Wie wird der Ausfall erkannt? Welche Vorkehrungen sieht der Konstruktionsentwurf vor, um diesen Ausfall zu kompensieren?
- bei einer FMECA klassifiziert das Untersuchungsteam anschließend jede der identifizierten Ausfallarten entsprechend des kombinierten Einflusses der Schwere der Folgen und der Eintrittswahrscheinlichkeit;
- Abhilfemaßnahmen festlegen und umsetzen, durch die das Eintreten der bedeutenderen Ausfallarten minimiert wird.
- einen Bericht zusammenstellen, der Folgendes enthält: Einzelheiten des untersuchten Systems, wie die Analyse durchgeführt wurde, während der Analyse gemachte Annahmen, Datenquellen und die Ergebnisse, gegebenenfalls einschließlich der ausgefüllten Arbeitsblätter und Kritizitätsmatrizen. Gegebenenfalls Empfehlungen für weitere Analysen, Änderungen des Konstruktionsentwurfs oder in Prüfpläne aufzunehmende Merkmale, usw.
- Neubeurteilung des Systems in einer weiteren FMEA-Runde, nachdem die Maßnahmen vollzogen wurden.

A.8.5 Ergebnisse

Das Hauptergebnis einer FMEA ist eine Liste der Ausfallarten und Auswirkungen für jede Komponente oder jedes Bauelement; dabei kann die Ausfallwahrscheinlichkeit mit angegeben werden. Weiterhin erhält man Angaben zu den Ausfallursachen und den Auswirkungen auf das Gesamtsystem.

Das Ergebnis einer FMECA enthält zusätzlich eine qualitative Risikoanalyse und daraus resultierend die kritische Bedeutung einer Ausfallart.

A.8.6 Stärken und Einschränkungen

Die Stärken einer FMEA bzw. FMECA sind:

- Ausfallarten der Komponenten oder Bauelemente, deren Ursachen und Auswirkungen auf das System werden ermittelt, und alles wird in einer leicht lesbaren Form dargestellt;
- teure Gerätemodifikationen während des Betriebs werden durch frühzeitige Problemerkennung während des Entwurfsprozesses vermieden;
- Ermittlung von sich nicht weiter auswirkender Ausfallarten und Notwendigkeit für Redundanz oder Sicherheitssystemen;
- für die Prüfprogramme in der Entwicklungsphase werden wichtige zu prüfende Merkmale genannt;
- bei der Festlegung der Instandhaltungsstrategie assistieren.

Die Einschränkungen einer FMEA bzw. FMECA sind:

- man kann mit diesen Analysen lediglich Einzelausfälle identifizieren, aber keine Ausfallkombinationen; Ausfälle die aus multiplen gleichzeitigen Fehlzuständen resultieren, werden durch diese Technik nicht erkannt;
- falls die Untersuchungen nicht angemessen gelenkt und fokussiert werden, können diese zeitaufwändig und teuer werden;
- bei komplexen, mehrlagigen Systemen können die Untersuchungen schwierig und mühsam sein;
- sie sind zur Quantifizierung der Systemzuverlässigkeit nicht geeignet.

A.8.7 Vergleiche

FMEA kann mit HAZOP dahingehend verglichen werden, dass es ein Verfahren zur Identifizierung von Risiken auf der Grundlage einer eingehenden Betrachtung einzelner Komponenten des Systems ist. Bei einer FMEA werden jedoch die Ausfallmechanismen einer Komponente oder eines Bauelementes betrachtet, wogegen HAZOP bemüht ist, herauszufinden warum die Sollfunktion nicht erreicht werden kann.

FMEA und FMECA können qualitative oder quantitative Informationen und Daten für weitere Analyseverfahren wie beispielsweise Fehlzustandsbaumanalyse bereitstellen.

A.8.8 Verweise

IEC 60812 „Procedures for failure mode and effect analysis (FMEA)“

A.9 Fehlzustandsbaumanalyse (FTA)

A.9.1 Beschreibung

Die Fehlzustandsbaumanalyse (en: Fault Tree Analysis, FTA) ist ein Verfahren zur Identifizierung und Analyse von Faktoren, die zu einem unerwünschten Ereignis beitragen können, dieses wird mit Hauptereignis bezeichnet. Ursächliche Faktoren werden in deduktiver Weise identifiziert, logisch angeordnet und graphisch durch ein Baumdiagramm dargestellt; die ursächlichen Faktoren und deren Logikverbindung zum Hauptereignis werden so erkennbar. In Fehlzustandsbäumen häufig benutzte Symbole und graphische Zeichen sind in IEC 61025 enthalten.

Die identifizierten und im Baum dargestellten Faktoren können Ereignisse sein, die im Zusammenhang mit Bauelementeausfällen, menschlichem Fehlverhalten oder sonstigen sachbezogenen Ereignissen stehen, die zum unerwünschten Ereignis führen.^{N5}

A.9.2 Anwendung

Ein Fehlzustandsbaum dient entweder in qualitativer Weise zur Identifizierung möglicher Ursachen eines Ausfalls bzw. der dorthin führenden Pfade oder andererseits in quantitativer Weise zur Berechnung der Wahrscheinlichkeit für den Eintritt des Hauptereignisses, sofern die Wahrscheinlichkeiten der auslösenden Ursachenereignisse bekannt sind.

Die Fehlzustandsbaumanalyse kann in der Entwicklungsphase eines Systems zum Auffinden potentieller Ausfallursachen verwendet werden, so dass anschließend zwischen gegebenenfalls vorhandenen Entwurfsoptionen ausgewählt werden kann. FTA kann in der Betriebsphase verwendet werden, um herauszufinden, wie sich schwere Ausfälle ereignen können und welche relative Bedeutung die zum Hauptereignis führenden Pfade haben. Auch im Nachhinein kann man mit einer Fehlzustandsbaumanalyse untersuchen, wie es zu einem Ausfall kommen konnte, indem man in einem Baumdiagramm darstellt, wie verschieden Ereignisse zusammentrafen und den Ausfall verursachten.

^{N5} Die Hinweise in 56/1172/CD zu Bild A.2 und Tabelle A.3 an dieser Stelle wurden hier weggelassen, da bezüglich FTA kein Bild A.2 und auch keine Tabelle A.3 eingefügt wurden.