

## 2 Philosophie und Modellierung des Sicherheitsmanagementsystems

Zentrale Grundlage eines Sicherheitsmanagementsystems sind systematische und konsistente Taxonomien von Fehlern und Ursachen, die – wie alle anderen Deskriptoren auch – digitalisiert werden und zur maschinellen Analyse und Vorhersage von Risiken, Maßnahmen, Kosten mit mathematischer Vorhersage verwendet werden können. Die ist im Kern der Anspruch bei der Digitalisierung des Expertenwissens von Unfalluntersuchen. Daraus erwächst als wesentliche Bedingung: Keine Interkorrelationen der Kategorien und Begriffe, da das Verfahren valide Vorhersagen eben nur dann gestattet, wenn sie ausreichend trennscharf und ein-eindeutig sind.

Vor dem Hintergrund der genannten Ziele empfehlen sich zunächst Analyse und Vergleich in Frage kommender und verfügbarer Klassifizierungssysteme, die mit Fehlern arbeiten. Solche Verfahren werden vor allem in der Luftfahrt verwendet. Hier eine kurze Zusammenfassung:

- PANDORA: Die Mehrheit der nutzbaren Begriffe kategorisiert technische Flugzeugsysteme oder Komponenten. Nur 12 der Begriffe beziehen sich auf Fehler, die 78 anderen gelten der Hardware und Defekten. Fünf Fehler beschreiben Reaktionen auf ein technisches Problem und zwei einen vermutlich vorausgegangenen Handlungsfehler („unangemessene Ansteuerung“).

Die anderen gelten z.B. Triebwerksfehlern. Hilfreich erscheint die Klassifizierung technischer Defekte durch Begriffe wie „total, teilweise, intermittierend, Strukturschaden“ usw. Diese Begriffe können auf fast alle technischen Systeme angewendet werden und erleichtern Adaptationen des SMS. PANDORA erfüllt allerdings nicht die Anforderungen an systematische Klassifizierungen von Fehlern in Systemen, in denen Menschen entscheidende Rollen spielen. Auch ist Ziel des zu

entwickelnden SMS nicht die Analysetiefe PANDORAs zu technischen Problemen, sondern von Fehlern und Ursachen, die zu Unfällen führen.

- **BRITISH CIVIL AVIATION AUTHORITY CAA:** Die CAA (1998) veröffentlicht jährliche Berichte über weltweit tödliche Unfälle in der zivilen Luftfahrt. Die zu Grunde liegende Kategorisierung gleicht denen vieler anderer ziviler und militärischer Luftfahrtbehörden, wie beispielsweise dem System FluSi DB II der deutschen Luftwaffe. Sie unterscheidet zwischen Folgen (z.B. „kontrollierter Flug ins Gelände“), kausalen Faktoren (z.B. „Desorientierung“) und beitragenden Faktoren (z.B. „fehlerhafte Sicherheitsausrüstung“).

Fehler sind hier unfallverursachende Faktoren. Die Kategorien sind breit und unscharf und fassen unterschiedliche Faktoren in einer Kategorie zusammen. So sind nur allgemeine Rückschlüsse auf Präventionsvorhaben, aber nicht auf konkrete Maßnahmen möglich. Statistische Datenanalysen können nicht vorgenommen werden, da die Informationen in Textform abgelegt werden. Diese Systeme dienen der Dokumentation und Archivierung von Einzelfällen. Solch inkonsistente Klassifizierungssysteme sind für statistische Analysen oder gar valide Risikovorhersagen unbrauchbar.

- **BRITISH AIRWAYS SAFETY INFORMATION SYSTEM:** Hauptmerkmal dieses Berichtssystems für Gefährdungen sind die Kausalketten zwischen Fehlern und Defekten einerseits sowie vorausgegangene Faktoren andererseits. Hier wurde Reasons Idee der „Psychologischen Vorläufer“ aufgegriffen, sicherlich eine gute Idee.
- **AGARD:** Eine Reihe unterschiedlicher NATO-Arbeitsgruppen vertiefte Erkenntnisse zu Human Error in unterschiedlichen militärischen Kontexten, siehe Käßler (1999), Allender et al. (2009). Besonders aktiv und weiterführend war die Mitarbeit in einer NATO Expertengruppe (NATO AGARD, 1998) und der Research Study Group 25 „Accident Investigation and Prevention in Military Crew Operations“ (Chappelow et al., unveröffentlicht). Sie erarbeiteten auf der Basis der Arbeiten und zusammen mit Reason (1990), Rasmussen (1983) und Senders & Moray (1991) zunächst eine *Human Factors* basierte Kategorisierung flugmedizinischer Daten. Die Taxonomie orientierte sich an Struktur und Verantwortlichkeit zuständiger Behörden und der

wichtigsten Aufgabe militärischer Führung, da sie Aussagen über die Haftung für Schäden trifft. Dies ist aber – wie Anfangs erläutert – nicht Ziel von Sicherheitsmanagementsystemen und weniger anspruchsvoll als die Erarbeitung einer im Analysesinne trennscharfen Kategorisierung von Fehlern und Ursachen sowie darunter liegende Mechanismen, die Unfälle zur Folge haben.

Sodann hat die hochkarätig besetzte, internationale Arbeitsgruppe RSG 25 die Taxonomie zu einem systematischen Gesamtansatz weiterentwickelt und RAFFS-Klassifizierungen um Risikosimulationen und -Vorhersagen für unterschiedliche Präventionsszenarien weiter entwickelt. Dieses System wurde als Prototyp in Unfalluntersuchungen praktisch erprobt und ins Deutsche übersetzt. Analysen von Motorradunfällen (Käppler, 2008a) und von Unfällen mit Waffen und Munition in der Bundeswehr mit diesem System zeigten die Vorteile der Analyseverfahren und der Risikosimulation. Auch diese Weiterentwicklung krankte an schlechter Bedienbarkeit und inkonsistenten Daten; kein Wunder, da ebenfalls eine ACCESS-Anwendung.

- ROYAL AIR FORCE FLIGHT SAFETY RAFFS: Parallel entwickelte Chappelow (1998) für die britische Luftwaffe die Kategorisierung von Fehlern, Unfällen und sogar Fehlerursachen weiter und testete sie praktisch mit Informationen von Flugunfällen. Seine Taxonomie umgeht wesentliche Nachteile anderer Verfahren und legt ihr Hauptaugenmerk erstmals auf psychologische, organisatorische und ergonomische Faktoren, Fehler und Ursachen. Sie legt statistisch zu verarbeitende Schlüsseltabellen zugrunde.

Alleinstellungsmerkmal dieses Ansatzes ist die umfassende Daten- und – gleichwohl einfache - Risikoanalyse auch für Fehler und Fehlerursachen. Diese werden zusätzlich einem Schätzverfahren durch Unfalluntersucher unterzogen, das der Wahrscheinlichkeit des Auftretens und der Auswirkung von Fehlern und Ursachen gilt. Ergebnisse sind Risikovorhersagen und -Simulationen. Eine Besonderheit ist die Trennung zwischen menschlichen Fehlern und technischen Defekten. Zudem wurden die vielen berücksichtigten Daten, Deskriptoren und Hintergrundvariablen nicht auf Interkorrelationen untersucht, wissenschaftliche Begleitstudien fanden nicht statt. Insgesamt war diese ACCESS-Anwendung wenig bedienerfreundlich, die Bereitstellung konsistenter Daten auf mehreren unterschiedlichen IT-Systemen sehr aufwendig.

Andere bekannte Verfahren sind nicht hinreichend dokumentiert oder veröffentlicht. Allen gemein sind weitgehend inkonsistente Fehler- und mangelnde Ursachenklassifikationen sowie überhaupt fehlende Analyse-tools oder gar Modelle. Präventionsansätze oder Risikomanagement sind, wenn überhaupt, nur rudimentär vorhanden. Dies betrifft beispielsweise die Flugunfalldatenbank FLUSI DBII der deutschen Luftwaffe, SERA der DRDC für die kanadische Air Force oder AFSID für die Israelische Air Force. Dennoch verfügen sie zum Teil über benutzungsfreundliche Oberflächen und anwendungsorientierten Workflow. Das Gesagte gilt auch für die verbreiteten Systeme „Global Event Management“ (GEMS) und das Modul „Arbeitsunfallerfassung und -Analyse“ der Unternehmenssoftware SAP.

Die Digitalisierung des Expertenwissens von Unfalluntersuchern ist damit kaum zu gewährleisten. So wurden im Sinne eines gesamthaften Sicherheitsmanagementsystems attraktive und zielführende Ideen der betrachteten Systeme in das laufende Vorhaben integriert, vor allem moderne Bedienungsfreundlichkeit, Workflow- und Internetverfügbarkeit. Neben den physikalischen Deskriptoren – oder Daten – sollen auch Einschätzungen der Wahrscheinlichkeit des Auftretens und der Wirkung von Fehlern und Ursachen erfolgen, herrscht doch nur in Ausnahmefällen Gewissheit über sie. Dazu kommen als weitere Vorteile Risikoanalysetools, Risikosimulation, Zentralarchiv, Berichtssysteme und Qualitätsmanagement.

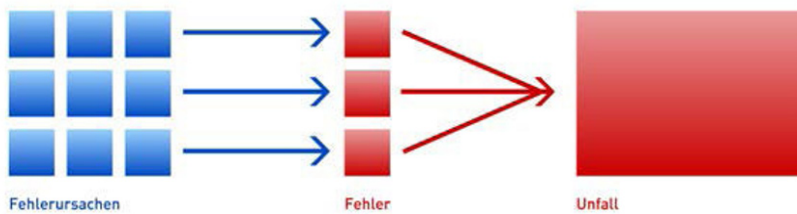
Eine weitere Idee ist, das Kriterium *Unfallfolgekosten* durch Deskriptoren, Fehler und Ursachen vorauszusagen. Die einfachen Risikomodelle von Chappelow wurden daher überarbeitet und ergänzt. Detaillierte Beschreibungen der mathematischen Modelle und Verfahren finden sich in Chappelow (1996), Käßler (2004; 2006; 2007) sowie Käßler & Dalinger (2005). Das geplante Sicherheitsmanagementsystem verknüpft all die beschriebenen Einzelelemente zu einem gesamthaften Sicherheitsmanagementsystem.

## **2.1 Drei-Ebenen-Modell der Unfallentstehung**

Es wurde bereits darauf verwiesen, dass Frieling & Sonntag (1999) im gängigen Umfeld sozio-technischer Systeme und deren technischen, organisatorischen und personalen Bedingungen der Arbeitsorganisation hinrei-

chende Kombinationen aus Fehlerursachen sehen, die zu Fehlern führen können. Wenn diese Ursachen und Bedingungen aber Fehler produzierend wirken, stellen sie die eigentlichen Unfallursachen dar. Dann muss das Hauptaugenmerk der Analyse ihnen gelten. Die viel diskutierte Fehler werden in diesem Modell des Unfallgeschehens zum Mittel, welches das Vorhandensein der Ursachen offenbart, und wirken quasi intermediär.

Im Verlaufe dieser theoretischen Überlegungen wurde ein relativ einfaches Modell der Unfallentstehung entwickelt, das Drei-Ebenen-Modell in Abb. 2.1 nach Käßler (2008). Es geht davon aus, dass multiple Fehler und Ursachen vorliegen und basiert auf den als Fehlerursachen zusammengefassten Bedingungen des sozio-technischen Umfelds. Sie haben konkrete Fehler zur Folge, welche ihrerseits Unfälle auslösen oder Gefährdungen darstellen können.



**Abb. 2.1** Vereinfachtes Drei-Ebenen-Modell der Unfallentstehung aus Käßler (2008), Käßler et al. (2008)

Dieses Modell greift die Idee auf, dass Unfälle grundsätzlich durch Fehler entstehen und hat erhebliche Konsequenzen für die Analyse. So werden beispielsweise auch technische Defekte auf vorausgegangene Fehler, z.B. bei Beschaffung, Konstruktion, Verwendung, Wartung, Organisation oder Herstellung usw. zurückgeführt.

## 2.2 Klassifizierung von Ursachen und Fehlern

Grundlage der Entwicklungen ist stets umfassendes Wissen über Vorgänge, Prozesse und beteiligte Personen und ihre Handlungen, das digitalisiert und maschinell verarbeitet werden kann und betrifft alle vorliegenden Informationen. Senders & Moray (ebda.) stellten fest, dass ohne Fehlertheorie und -klassifizierung – wie in anderen Bereichen auch – formale Analyse, Modellierung, Vorhersage und Prävention nicht möglich seien. Ohne Klassifizierung der Fehler und der Fehlerursachen könnten ih-

re Natur und Ursprünge überhaupt nicht verstanden werden, denn Verstehen basiert auf eindeutiger und umfassender Klassifikation der Phänomene, die untersucht werden und der Ziele, die verfolgt werden.

Viele weitere, auch an psychologischen Mechanismen orientierte Klassifikationen von Reason und anderen machen klar, dass sie so unterschiedlich sind wie die Systeme, in denen sie gelten. Altman (1966), modifiziert und zitiert nach Senders & Moray (1991), stellt eine Meta-Klassifizierung vor, die lediglich die Klassifizierung selbst einordnet. Sender & Moray unterscheiden beispielsweise vier Ebenen der Komplexität des Verhaltens mit unterschiedlichen Fehlerarten und Modi für jede Ebene:

1. Phänomenologisch (z.B. Unterlassung)
2. Hypothetische interne Prozesse (z.B. Befangenheit, Überlastung)
3. Neuro-psychologische Mechanismen (z.B. Aufmerksamkeit, Stress)
4. Externe Prozesse (z.B. mangelhafte Ausrüstung).

Systematische und konkret wirkende Prävention erfordert die Vorhersage eindeutiger Risiken auf der Basis von Analysen realer Daten konkreter Situationen und auf Einschätzungen von Hintergrundvariablen. Mit diesem Modell und weiteren Informationen erst werden konkrete Maßnahmen zur Prävention möglich. Die Validität der Vorhersagen ist wesentliche Forderung an die Güte der Modelle.

Diese Bemühungen werden erschwert, wenn zwischen Fehlern und Unfällen keine kausalen, sondern probabilistische Zusammenhänge bestehen und viele ähnliche Fehler und Ursachen die Wirkung der Prädiktorvariablen durch Interkorrelationen „aufblähen“. Senders & Moray schlugen deshalb *Kausalketten* aus Fehlern dieser vier Ebenen oben vor, die mit gewissen Wahrscheinlichkeiten zu Unfällen führen. In diesem – globalen – Modell führt beispielsweise in Abb. 1.1 – verkürzt betrachtet – überhöhte Geschwindigkeit zum Unfall, bei der Erstbetrachtung war es jedoch *Abkommen von der Fahrbahn*.

Allen zitierten Arbeiten gemeinsam ist, dass Auftreten und Auswirkung von Fehlern zwar vermindert, Fehler aber nicht eliminiert werden können. „Dies sei auch nicht unbedingt wünschenswert, denn Fehler, die nicht mehr auftreten, werden auch nicht mehr erwartet. Wenn sie auftreten, sind wir schlecht auf den Umgang mit ihnen vorbereitet und können kaum Folgen mindern oder ganz verhindern (Bainbridge, 1987).“

Sie hat dies elegant als „Ironien der Automatisierung“ komplexer technischer Systeme beschrieben: Schaltwarten von Kernkraftwerken, so ihr Beispiel, werden von kompetenten Experten überwacht. Bekannt ist, dass selbst hoch motivierte Operateure nicht unbegrenzt aufmerksam sein können. Im seltenen Falle des Ausfalls automatischer Überwachungssysteme müssen aber schnellstmöglich sicherheitsrelevante Entscheidungen und Handlungen erfolgen, die gar nicht oder lange nicht geübt werden konnten.

### **2.2.1 Fehlerursachen**

In den genannten Arbeiten und vielen anderen werden Bedingungen der Fehlerentstehung in der Regel genannt, aber nicht wirklich konkretisiert, klassifiziert oder gar systematisch untersucht. Sie spielen kaum eine Rolle und werden gern als „Randbedingungen“ bezeichnet oder gar mit Fehlern selbst vermengt oder verwechselt. Die geschilderte Diskussion bleibt so an Fehlern hängen und umkreist diese und das Unfallgeschehen selbst.

Aus moderner humanistischer Sicht kann mit Lessing festgestellt werden, dass das klassische Bemühen um die Vermeidung von Fehlern anhand gezielter Programme zur Erziehung, sog. Law Enforcement, tatsächlich nicht zum Ziel „mehr Sicherheit“ führt wie gewünscht. Trotz erheblicher Strafen wird nach wie vor zumal unter Zeitdruck zu schnell gefahren, oder führt Unaufmerksamkeit beim Befahren von Kreuzungen zu Unfällen aufgrund unterlassener Handlungen. All dies sind Fehler, deren Wirkungen bekannt sind und die eigentlich vermieden werden sollten und könnten.

Die Frage aus Abb. 1.1 wurde also neu gestellt. Warum kommt das Fahrzeug überhaupt von der Fahrbahn ab? Welche waren die Prozesse, die zu welchem Fehler und zu schnellem Fahren führten? So gaben die geschilderten Arbeiten Anlass zur Frage, inwieweit parallel zu den Fehlern auch die vermuteten Ursachen und Bedingungen der Fehlerentstehung systematisiert, klassifiziert, digitalisiert, untersucht und wissenschaftlich exakter Beschreibung und Analyse zugeführt werden können.

Können sie klar von den Fehlern als solchen getrennt werden? Enthalten sie wirklich neue Informationen oder sind sie nur Fehler in neuem Kleide? All diese Fragen und damit verbundenen Hypothesen können nur



mit erheblichem diagnostischem Aufwand und mit Hilfe statistischer Test- und Prüfverfahren zweifelsfrei beantwortet und verifiziert werden.

Mit diesen Überlegungen und vor dem Hintergrund von Erfahrungen aus mehr als 2000 Unfalluntersuchungen bei unterschiedlichen Arbeitstätigkeiten vor allem im Luft- und Straßenverkehr wurde eine eigene Taxonomie von Fehlern und Ursachen entwickelt und empirisch untersucht. Sie orientiert sich an den von Chappelow (1998) entwickelten und der NATO RSG 25 überarbeiteten Taxonomien und Risikomodellen.

Chappelows Dualität von Fehlern und technischen Defekten wurde jedoch in Übereinstimmung mit Dekker (2005) verworfen, siehe oben. Er plädiert ebenfalls für gesamthafte systemische Ansätze, die organisatorische, technische und personale Faktoren integrieren und verknüpfen. Eigene Analysen bestätigten dies.

Die entwickelte Taxonomie beschreibt Fehlerursachen in den acht Oberkategorien in Abb. 2.2:



**Abb. 2.2** Fehlerursachenkategorien nach Käßpler (2008), Käßpler et al. (2008)

- Fehlerursachen der *Arbeitsorganisation* bezeichnen Mängel der zielgerichteten Ordnung, Regelung und Eingliederung von Aufgaben und Tätigkeiten in Sozialgebilden, z.B. bei Gesetzen, Regeln oder Arbeitsmitteln.
- Fehlerursachen der *Kommunikation* bezeichnen Mängel von verbalen und nonverbalen Prozessen der Informationsübertragung.



- Fehlerursachen bei *Personal und Qualifikation* bezeichnen Mängel der Personalselektion, -Zuordnung und -Qualifikation; sie betreffen solche Kenntnisse und Fähigkeiten, die zur Ausübung einer bestimmten Tätigkeit befähigen.
- Fehlerursachen des *Qualitätsmanagements* bezeichnen Mängel der laufenden Überprüfung von Güte und Beschaffenheit der Arbeitsergebnisse, z.B. bei Normen, Anweisungen, Handbüchern.
- Fehlerursachen der *Einstellung* bezeichnen Beeinträchtigungen arbeitender Personen durch Neigungen oder Prädispositionen, Subjekte und Objekte in einer bestimmten Weise konsistent zu bewerten, z.B. infolge von Geltungsbedürfnis.
- Fehlerursachen der *Physiologie* bezeichnen Beeinträchtigungen arbeitender Personen durch Lebensvorgänge, wie z.B. Wachstum oder Krankheit.
- Fehlerursachen des *Verhaltens* beschreiben beobachtbare Beeinträchtigungen des Handelns und Entscheidens arbeitender Personen. Dies schließt mehr oder weniger bewusste Prozesse des Erlebens ein.
- Fehlerursachen der *Umweltbedingungen* bezeichnen anhand von physikalischen Daten beschreibbare Eigenschaften der Umwelt, die Risiken erhöhen.

Details der beobachteten Ursachen in acht Kategorien zeigt Tab. 2.1; Definitionen im Detail siehe Anhang B.

**Tab. 2.1** Fehlerursachen im Detail

Bezeichnung
<b>Arbeitsorganisation</b>
Arbeitsbelastung
Arbeitsumfang
Aufgabenstellung
Isolation
Funktional

Örtlich

Monotonie

Riskante Schicht

Schlaf- und Ruhepausen inadäquat

Teamkoordination fehlerhaft

Arbeitsplatzgestaltung

Anzeigen fehlerhaft

Ausrüstungslücke

Ausrüstungsmangel

Abrieb

Abtrennung

Bersten

Brand

Korrosion

Kurzschluss

Leck

Materialermüdung

Softwarefehler

Torsion

Überhitzung

Verschleiß

Zerstörung

Gehörschutz linear

Schutzausrüstung fehlerhaft

Verbrauchsmaterial fehlerhaft

Bedienelemente fehlerhaft

Handling fehlerhaft

Betriebsorganisation/Management fehlerhaft

**Kommunikation**

Indirekte Kommunikation

Übermittlung

Verlust

Verzögerung

Verfälschung

Nonverbale Kommunikation

Empfänger nonverbal

Fehlerhafte Dekodierung nonverbal

Keine Dekodierung nonverbal

Unvollständige Dekodierung nonverbal

Sender nonverbal

Falsche oder unklare nonverbale Information

Keine nonverbale Information

Paradoxe nonverbale Information

Verbale Kommunikation

Empfänger verbal

Fehlerhafte Dekodierung verbal

Keine Dekodierung verbal

Unvollständige Dekodierung verbal

Sender verbal

Falsche/unklare verbale Information

Keine verbale Information

Paradoxe verbale Information

Kommunikationskonzept

Hierarchisch

Partizipativ

Gewähren lassend/liberal

**Personal und Qualifikation**

Doppelfunktion

Personalmangel

Personalüberhang

Personalauswahl fehlerhaft

**Qualitätsmanagement**

Dienstaufsicht und Kontrolle fehlerhaft

Handbücher fehlerhaft

Modifikation

Nicht durchgeführt

Ohne Ankündigung

Ohne Dokumentation

Technische Regeln fehlerhaft

Vorschriften fehlerhaft

### **Einstellung**

- Extraversion
- Gewissenhaftigkeit
- Neurotizismus
  - Autoritarismus
- Offenheit
- Verträglichkeit
  - Geltungssucht

### **Physiologie**

- Ernährungseinflüsse
- Medikamentöse Einflüsse
  - Betäubungsmittel
- Physische Ermüdung
- Vorerkrankungen und Verletzungen

### **Verhalten**

- Ablenkung
  - Funk und Fernsehen
  - Gespräch
  - Navigation
  - Sprechfunk und Telefon
- Bedrohung
  - Situationsbezogen
  - Systembezogen
- Fehlgerichtete Motivation
  - Eifer
  - Emotionale Bindung
- Fixierung
- Lebensstress
- Psychische Ermüdung
- Qualifikation unzureichend
  - Allgemeinmilitärische Ausbildung unzureichend
  - Praktische Ausbildung unzureichend
  - Theoretische Ausbildung unzureichend
  - Weiterbildung unzureichend
- Unaufmerksamkeit

Unerfahrenheit  
Wissensdefizit  
    Falsches Wissen  
    Unwissen  
Zeitdruck  
Zuschauer

### **Umweltbedingungen**

Abgase und Schadstoffe  
Eingeschränkte Sicht  
Glätte  
Luftfeuchtigkeit  
Lautheit  
Sand und Staub  
Schwingung  
Temperatur  
Versalzung  
Wind und Turbulenz

---

## **2.2.2 Fehler**

Die Kategorisierung der beobachteten Fehlerarten in drei Hauptkategorien wurde nach Chappelow überarbeitet und ergänzt, siehe Abb. 2.3 und Tab. 2.2.



**Wahrnehmungsfehler**



**Kognitionsfehler**



**Handlungsfehler**

**Abb. 2.3** Fehlerkategorien nach K  ppler (2008), K  ppler et al. (2008)

- *Wahrnehmungsfehler* bezeichnen M  ngel der F  higkeit, aus sensorischen Informationen ein umfassendes und ad  quates Abbild von Eigen-

schaften der physikalischen und sozialen Umwelt abzuleiten. Deren Aggregation und Verarbeitung ist dagegen Sache der Kognition

- *Kognitionsfehler* bezeichnen die Formulierung von Plänen, die auf korrekter Wahrnehmung relevanter Informationen beruhen, den Erfordernissen von Aufgabe und Situation aber nicht gerecht werden
- *Handlungsfehler* bezeichnen die fehlerhafte Ausführung eines korrekten Handlungsplanes, beispielsweise die Verwechslung von Handlungsabfolgen oder das Abgleiten in ähnliche, aber gewohnte Routinen

Fehlerdetails in diesen drei Kategorien zeigt Tab. 2.2; Definitionen siehe Anhang A.

**Tab. 2.2** Fehler im Detail

Beschreibung
<b>Handlungsfehler</b>
Falsche Handlungsstrategie
Falsche Handlung
Handlung weggelassen
Verwechslung von Handlungsabfolgen
Fehlbedienung
Übergenaues Regeln und Steuern
Unangemessenes Koordinieren
Gewohnheitshandeln
Unorganisierte Reaktion
Langsam
Vorschnell
Ausrutschen
Stolpern und Umknicken
<b>Kognitionsfehler</b>
Nichtumsetzung von Qualitätssicherungsmaßnahmen
Unangemessenes Modell
Falsche Risikobewertung
Verletzung von Beschaffungsrichtlinien

- Verletzung von Konstruktionsregeln
- Verletzung von Produktionsrichtlinien
- Verletzung von Verwendungsvorschriften
  - Spielerischer Umgang
- Verletzung von Wartungsrichtlinien

**Wahrnehmungsfehler**

- Desorientierung
- Detektionsfehler
  - Bewegung
  - Position
- Fehlinterpretation
- Visuelle Illusion
  - Neue Information
  - Mangelhafte Information
  - Unangemessene Erwartung

---

## 2.3 Skalierungsmodell für die Hintergrundvariablen

Die klassische Dokumentation und Analyse von Unfällen basiert in erster Linie auf Daten oder sogenannten Deskriptoren. Sie beschreiben im besten Fall die Bedingungen und den Unfallhergang anhand physikalischer Daten objektiv eindeutig und nachvollziehbar. Auf dieser Basis erfolgen Unfallanalyse, Interpretation, Bewertung und Prävention.

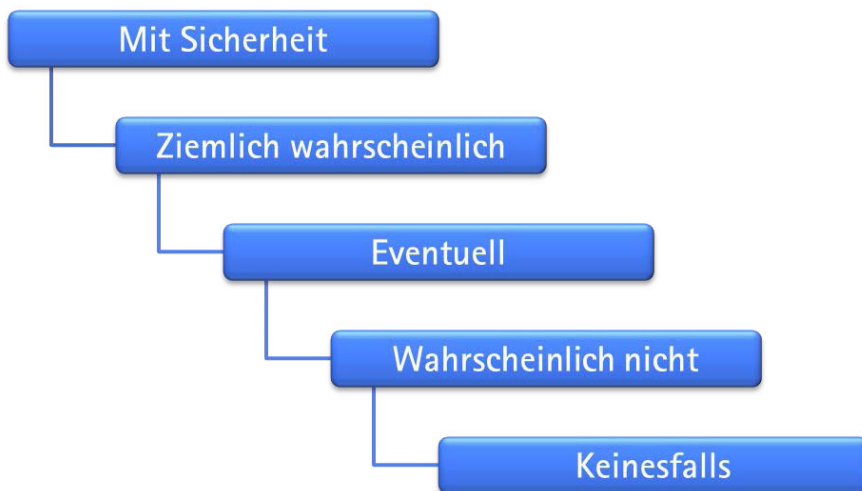
Oft sind im Rahmen von Unfalluntersuchungen aber keine exakten und eindeutigen Festlegungen möglich, stattdessen ist von Indizien, Möglichkeiten und Wahrscheinlichkeiten auszugehen. Manchmal ist nicht klar, welcher Fehler den Unfall tatsächlich ausgelöst hat. So erhöhen manche Fehler im Rahmen des Unfallgeschehens lediglich Risiken von Folgeschäden oder das Ausmaß dieser Schäden. In anderen Fällen lassen vorliegende Fakten oder Aussagen nur induktiv geführte Rückschlüsse beispielsweise auf Fehler zu, objektive Beweise können nicht geführt werden.

Diese Art der Fehleridentifikation und Einschätzung ist ein sogenanntes unscharfes System. Die Erzielung reliabler und valider Ergebnisse solcher Systeme ist möglich mit probabilistischen Verfahren, die maschinell



verarbeitbare Daten benötigen und liefern. Im vorliegenden Fall bieten sich Schätzverfahren an, mit deren Hilfe im Rahmen der Unfalluntersuchung Einschätzungen über das Vorhandensein und die Wirkungen von Variablen getroffen und dokumentiert werden. So werden auch diese „Daten“ der Analyse mit maschinellen Verfahren zugänglich. Natürlich verhält es sich ebenso mit den beobachteten oder nur vermuteten Fehlerursachen. Auch hier lassen die Beobachtungen oft nur induktives Schließen auf Ursachen zu. Dies muss in der Analyse berücksichtigt werden.

Wesentliche Folge dieser Unschärfen ist die Tatsache, dass im Rahmen der Unfallanalyse sowohl objektive Deskriptoren als auch sogenannte Hintergrundvariablen mit Skalierungen von Erwartungswerten erfasst werden. Sie müssen unterschiedlichen Analyseverfahren unterzogen werden. Analyseergebnisse sind dann insgesamt keine hundertprozentigen Wahrheiten oder Gewissheiten über Fehler oder Unfallursachen mehr, sondern mehr oder weniger hohe Wahrscheinlichkeiten. Sie bilden als *Risiken* die Grundlage des Risikomanagements, siehe Abb. 2.4.



**Abb. 2.4** Graduierungen der Wahrscheinlichkeiten des Auftretens und der Auswirkung von Fehlern und Ursachen

Die Hergangsanalyse von Unfällen oder Gefährdungen basiert natürlich auch in diesem Fall zunächst auf beobachtbaren Tatsachen, aber eben

auch auf Indizien. Deren Analyse erfolgt post factum und logisch schließend. Mit dem Skalierungsmodell der Abb. 2.4 werden folgende Aspekte des *Auftretens* und der *Auswirkung* von Fehlern und von Ursachen betrachtet:

1. Die *Wahrscheinlichkeit* des Auftretens möglicher, beobachteter, berichteter Fehler überhaupt
2. Die *Wahrscheinlichkeit* des Auftretens möglicher, beobachteter, berichteter Fehlerursachen überhaupt
3. Die *Intensität* der Auswirkung der Fehler auf die Entstehung des Unfalls und/oder bei der Verschärfung der Unfallfolgen
4. Die *Intensität* der Auswirkung der Fehlerursachen auf die Entstehung der Fehler und/oder die Verschärfung der Folgen.

Es geht bei allen vier Aspekten um die Skalierung von Wahrscheinlichkeiten. Entsprechende Fragen können lauten: „Mit welcher Wahrscheinlichkeit haben Fehler y oder Fehlerursache x den Unfall z bzw. den Fehler y verursacht?“ Bei den Antworten handelt es sich grundsätzlich um Einschätzungen. Das Auftreten oder die auslösende Wirkung von Fehlern und Fehlerursachen werden für mehr oder weniger wahrscheinlich gehalten. Da es sich im hier betrachteten Fall um Intensitäten von Wahrscheinlichkeiten handelt, wurde auf bekannte Arbeiten von Rohrmann (1978) und auf eigene Arbeiten (Käppler, 1993) zur Skalierung der Intensität zurückgegriffen.

Für die vorliegende Fragestellung wurden möglichst gleich abständige Graduierungsbegriffe mit möglichst geringer Bedeutungsstreuung aus Rohrmanns Liste extrahiert. Die ausgewählten und hier verwendeten Graduierungsbegriffe der Abb., deren Skalierungen in Prozent und die Definitionen zeigen Tab. 2.3 Graduierung des Auftretens nach Käppler (1993) und Tab. 2.4 Graduierung des Auslösens nach Käppler (1993) im Detail.

Ein Beiprodukt und weiterer Vorteil der Graduierung besteht darin, dass die Graduierungsunterschiede ganz nebenbei die genannten Fehlerketten nach Senders & Moray (1991) erzeugen, wenn z.B. Unfall auslösende Fehler höher gewichtet werden als solche, die *nur* Folgen verschärfen oder Risiken erhöhen. Analog zu Fehlern werden auch die identifizierten Fehlerursachen gewichtet und zu Ketten verarbeitet.

**Tab. 2.3** Graduierung des Auftretens nach Käßler (1993)

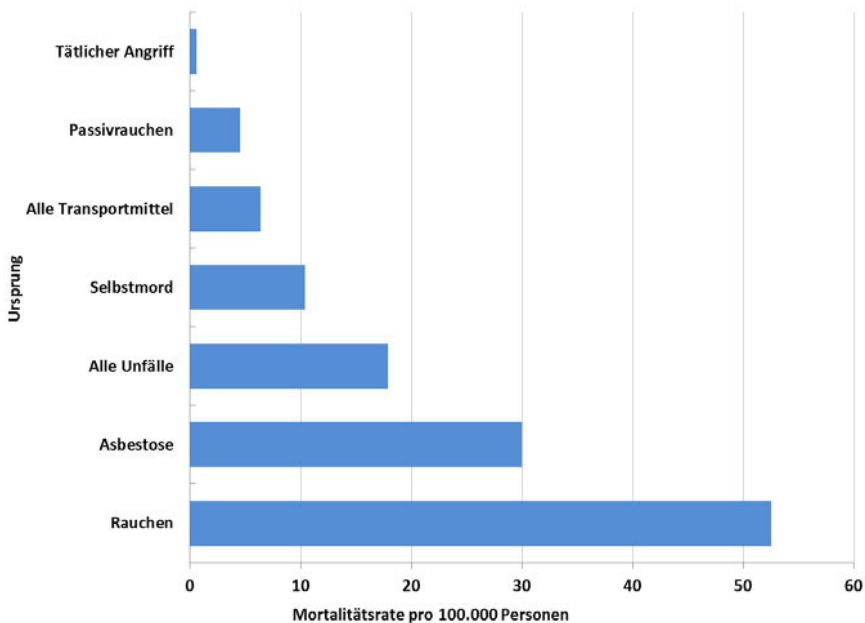
Auftreten	Graduierung	Skalierung	Definition
Fehler y/ Kausaler Faktor x ist	keinesfalls	0 %	aufgetreten. Dies ist nachweisbar.
	wahrscheinlich nicht	25%	aufgetreten. Nach menschlichem Ermessen ist dies weder glaubhaft noch nachweisbar, es bleiben jedoch geringe Zweifel.
	eventuell	50%	aufgetreten. Nach Abwägung aller Informationen kann das Auftreten angenommen werden.
	ziemlich wahrscheinlich	75%	Aufgetreten. Nach menschlichem Ermessen ist das Auftreten glaubhaft, aber nicht nachweisbar.
	mit Sicherheit	100%	Aufgetreten. Das Auftreten ist nachweisbar.

**Tab. 2.4** Graduierung des Auslösens nach Käßler (1993)

Auslösen	Graduierung	Skalierung	Definition
Fehler y/ Kausaler Faktor x ist	keinesfalls	0 %	Mitauselöser des Ereignisses /Fehlers y.  Er bleibt ohne direkte Auswirkung, könnte das Gesamtrisiko aber erhöht haben.
	wahrscheinlich nicht	25%	Mitauselöser des Ereignisses /Fehlers y.  Nach menschlichem Ermessen ist die Wirkung weder hinreichend noch nachweisbar, es bleiben jedoch geringe Zweifel.
	eventuell	50%	Mitauselöser des Ereignisses /Fehlers y neben anderen Fehlern y/Faktoren x.  Nach Abwägung aller Informationen kann die Mitwirkung und/oder eine Beteiligung an der Verschärfung der Folgen angenommen werden.
	ziemlich wahrscheinlich	75%	Auslöser des Ereignisses /Fehlers y.  Nach menschlichem Ermessen ist die Wirkung glaubhaft, aber nicht nachweisbar.
	mit Sicherheit	100%	Auslöser des Ereignisses /Fehlers y.  Die Wirkung ist hinreichend und nachweisbar.

## 2.4 Risiken bei Arbeitstätigkeiten und Risikomodell für Unfälle

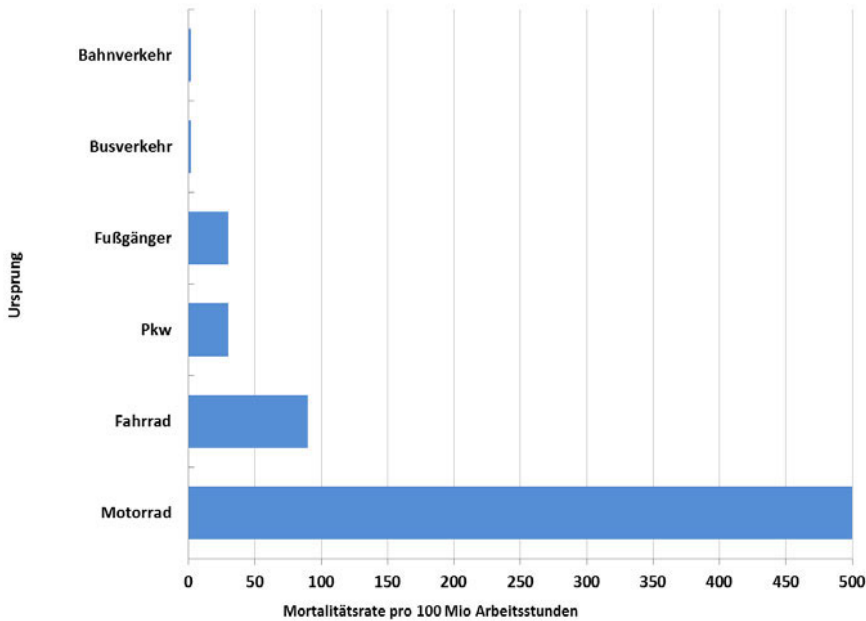
Präventionsmaßnahmen verfolgen grundsätzlich das Ziel, Risiken für Leib und Leben, Geld und Ressourcen und deren Folgen zu verhindern oder zu mindern. Zur Darstellung und Bewertung dieser Risiken werden beispielsweise Getötetenzahlen pro Jahr oder Mortalitätsraten bezogen auf 100.000 Einwohner herangezogen, siehe Abb. 2.5 mit Raten für sogenannte „Äußere Ursachen“ und „Krankheiten“ für Deutschland (DStatis, 2012). Das Risiko, durch einen tätlichen Angriff ums Leben zu kommen, betrifft demnach nur einen von 200.000 Einwohnern. Dagegen ist das Risiko, durch irgendein Transportmittel ums Leben zu kommen, 35 Mal höher. Unsere Gefahrenwahrnehmung fühlt anders.



**Abb. 2.5** Typische Mortalitätsraten vergangener Jahre pro 100.000 Einwohner pro Jahr in Deutschland (DStatis, 2012)

Deshalb hat das European Traffic Safety Council andere Berechnungsmodelle für Mortalitätsrisiken vorgeschlagen (ETSC, 1999). Sie beziehen Getötetenraten nicht auf die Anzahl von Menschen, sondern auf deren Arbeitsstunden bei unterschiedlichen Tätigkeiten, sei es Reisen oder

Fahren, Arbeit in der Bank oder im Bergbau. Eingebürgert hat sich der Bezug auf 100 Mio. Arbeitsstunden, siehe Beispiel Straßenverkehr in der EU in Abb. 2.6.



**Abb. 2.6** Typische Mortalitätsraten pro 100 Mio. Arbeitsstunden im Straßenverkehr der EU (ETSC, 1999)

Die Abb. zeigt, dass der Transport in Bus und Bahn in der EU relativ risikoarm ist, Fußgänger und Pkw-Fahrer ein 15 Mal so hohes Risiko eingehen, noch weit übertroffen vom Mortalitätsrisiko beim Fahrradfahren, das 45 Mal höher ist, ganz zu schweigen vom Mortalitätsrisiko beim Motorradfahren, das fast halb so hoch ist wie das von Soldaten in Kriegsgebieten. Sehr anschaulich wird so gezeigt, wie Risiken ganz unterschiedlicher Arbeitstätigkeiten verglichen werden können.

Des Weiteren ist klar, dass bei einem Unfall Getötete nur die „Spitze des Eisbergs“ darstellen. Die Unfallpyramide modernisiert nach Heinrich (1959) in Abb. 2.7 zeigt anschaulich, dass Mortalitätsrisiken von erheblichen Risiken durch Gefährdungen und Beinaheunfälle und von leichten und schweren Arbeitsunfällen begleitet werden. Heinrich war noch davon ausgegangen, dass ein Getöteter auf lediglich 29 Unfälle mit Leichtverletzten und auf 300 Gefährdungen ganz ohne Verletzungen entfalle. Die

Kenntnisse über und Einschätzungen von diesen Risiken haben sich in den letzten 50 Jahren jedoch entscheidend verändert. So schätzen die Berufsgenossenschaften, dass auf einen Getöteten 10 Schwerverletzte und 100 Leichtverletzte bei 1000 Gefährdungen entfallen; aus aktueller Sicht auch dies eine eher konservative Risikoschätzung. Unternehmen der privaten Luftfahrt gehen aktuell sogar davon aus, dass ein Todesrisiko von  $10^7$  Gefährdungen begleitet wird.



**Abb. 2.7** Unfallpyramide nach Heinrich (1959)

Entsprechende Aufklärung über Risiken der Arbeit und des Lebens ist ein Anspruch aufgeklärter Gesellschaften, den modernes Sicherheitsmanagement bedienen will. Erst die Kenntnis der Fehler und Ursachen mit ihren Wahrscheinlichkeiten oder Graduierungen ermöglichen Risikomanagement und entsprechende Analysen. Demzufolge wird Risikomanagement als Form der Sicherheitskultur verstanden, die Risiken als Informationsdefizite über das Erreichen von Zielen auffasst und auf die Reduktion dieser Risiken abzielt.



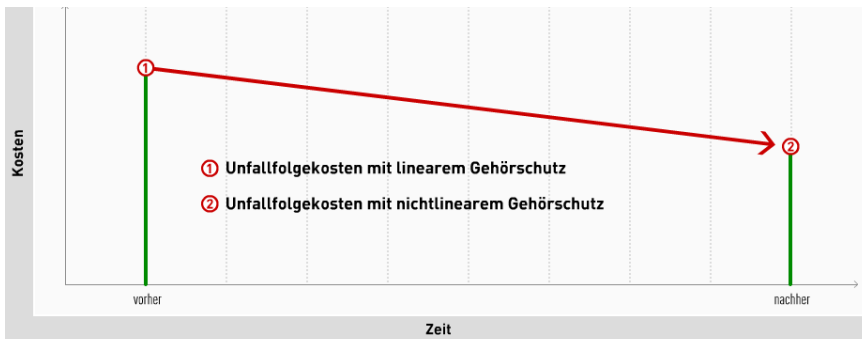
Risikomanagement vollzieht sich grundsätzlich in drei Phasen:

- Phase 1: Risikoidentifikation
- Phase 2: Risikoanalyse und -simulation
- Phase 3: Risikopolitik.

In *Phase 1* werden mit komplexen mathematischen Modellen Auftretens- und Kostenrisiken von Fehlern und Fehlerursachen anhand von Wahrscheinlichkeiten sowie echten und geschätzten Schadenkosten identifiziert und im Sicherheitsmanagementsystem errechnet.

In *Phase 2* folgt die Untersuchung des vorliegenden Ursache-Wirkungs-Komplexes mit Hilfe der Risikosimulation. In sogenannten *What-If-Simulationen* werden Annahmen über Möglichkeit und Wirkung von Präventionsmaßnahmen getroffen und Auftreten und Auswirkung einzelner Ursachen systematisch variiert. Hypothesen über das Ausbleiben von Schäden nach der Realisierung hypothetischer Präventionsmaßnahmen werden formuliert, z.B. „Wenn die Ausbildung am Gerät x verbessert wird, tritt die Ursache *Mängel der Praktischen Ausbildung* seltener auf und verhindert entsprechend viele Fehlbedienungen.“

Simulationen unterschiedlicher Präventionsszenarien zeigen die Veränderungen von Risiken und Kosten und prognostizieren Einsparpotentiale und Sicherheitsgewinne, siehe schematische Darstellung in Abb. 2.8.



**Abb. 2.8** Risiko vor und nach der Einführung von Präventionsmaßnahmen nach Käppler (2008), Käppler et al. (2008)

In *Phase 3* schließlich werden zur Risikomeidung, -minderung, -teilung, -reservebildung sowie Schadenverhütung oder Kostenüberwäl-

zung endgültige Entscheidungen über risikopolitische Maßnahmen, sogenannte Präventionsmaßnahmen, getroffen und realisiert.

Grundlage des Risikomanagements sind die Risikomodelle. Mögliche Ansätze wurden im Rahmen von Forschungsarbeiten evaluiert. Beispielhafte Daten-, Risiko- und Kostenanalysen wurden durchgeführt und Ergebnisse verglichen.

Mit diesen Kenntnissen wurde das Risiko-Kostenmodell auf der Basis der Veröffentlichungen von Chappelow (1998) weiterentwickelt. Das neue Modell errechnet anhand der vorgenommenen Einschätzungen die Anteile und Wahrscheinlichkeiten aller Fehler, Ursachen und Kosten an Ereignissen und gibt diese auf 100 Prozent normiert an. Dabei ist  $E_m$  eine beliebige Menge von Ereignissen. Das können alle oder nach bestimmten Kriterien gefilterte Ereignisse sein. Weitere Definitionen sind:

$f_i$	Fehler des Typs $i$
$k(E_j)$	Gesamtkosten des Ereignisses $E_j$
$F_m$	Menge aller Fehler in $E_m$
$U_m$	Menge aller Ursachen in $E_m$
$u_i$	Ursache des Typs $i$
$g(f_i)$	Gewicht für Fehler $f_i$ in Prozent
$g(u_i)$	Gewicht für Ursache $u_i$ in Prozent.

Der Korrekturfaktor  $f$  ist definiert als 100 dividiert durch die Summe über alle Gewichte im Ereignis:

$$f = 100 / \sum g_n(f_i) \quad (1)$$

Daraus berechnet sich das normierte Gewicht der Fehler wie folgt:

$$g_n(f_i) = f \times g(f_i) \quad (2)$$

Die normierten Gewichte  $g_n(u_i)$  der Ursachen werden analog berechnet. Die Wahrscheinlichkeit  $h(f_i)$ , dass der Fehlertyp  $f_i$  in einem Ereignis auftritt, ist definiert als Anzahl des Auftretens von  $f_i$  dividiert durch die Anzahl der Ereignisse in  $E_m$ . Diese Wahrscheinlichkeit kann aufgrund der Redundanz von Fehlern größer 1 sein:

$$h(f_i) = |f_i| / |E_m| \quad (3)$$

Die normierte Wahrscheinlichkeit  $h_n(f_i)$ , dass der Fehlertyp  $f_i$  auftritt, ist definiert als Anzahl des Auftretens von  $f_i$  dividiert durch Anzahl aller Fehler. Die Wahrscheinlichkeit ist maximal 1:

$$h_n(f_i) = |f_i| / |F_m| \quad (4)$$

Die gewichtete Wahrscheinlichkeit  $p(f_i)$ , dass der Fehlertyp  $f_i$  ein Ereignis kausal bedingt, ist definiert als Summe der Gewichte von  $f_i$  dividiert durch die Anzahl der Ereignisse in  $E_m$ . Diese Wahrscheinlichkeit kann aufgrund der fehlenden Normierung der Gewichte größer 1 sein:

$$p(f_i) = \sum g(f_i) / 100 / |E_m| \quad (5)$$

Die normierte gewichtete Wahrscheinlichkeit  $p_n(f_i)$ , dass der Fehlertyp  $f_i$  ein Ereignis kausal bedingt, ist definiert als Summe der normierten Gewichte von  $f_i$  dividiert durch die Anzahl der Ereignisse in  $E_m$ . Diese Wahrscheinlichkeit ist maximal 1:

$$p_n(f_i) = \sum g_n(f_i) / 100 / |E_m| \quad (6)$$

Die Ursachenwahrscheinlichkeiten werden analog errechnet. Die von Fehler  $f_i$  in einem Ereignis  $E_j$  verursachten Kosten sind definiert als Produkt aus Gewicht des Fehlers und Gesamtkosten des Ereignisses. Es ist die Summe über alle Vorkommen des Fehlers  $f_i$  in dem Ereignis  $E_j$  zu bilden:

$$k(f_{ij}) = \sum g(f_i) / 100 \times k(E_j) \quad (7)$$

Die von Fehler  $f_i$  in einem Ereignis  $E_j$  verursachten normierten Kosten sind definiert als Produkt aus normiertem Gewicht des Fehlers und Gesamtkosten des Ereignisses. Es ist die Summe über alle Vorkommen des Fehlers  $f_i$  in dem Ereignis  $E_j$  zu bilden:

$$k_n(f_{ij}) = \sum g_n(f_i) / 100 \times k(E_j) \quad (8)$$

Die von Fehler  $f_i$  insgesamt verursachten Kosten sind definiert als Summe über alle Einzelkosten. Sie kann aufgrund der fehlenden Normierung größer als die Gesamtkosten sein:

$$k(f_i) = \sum k(f_{ij}) \quad (9)$$

Die von Fehler  $f_i$  insgesamt verursachten normierten Kosten berechnen sich analog, diese können maximal den Gesamtkosten entsprechen:

$$k_n(f_i) = \sum k_n(f_{ij}) \quad (10)$$

Die von Ursache  $u_i$  in einem Ereignis  $E_j$  verursachten Kosten sind definiert als Produkt aus Gewicht der Ursache, des Fehlers und der Gesamtkosten des Ereignisses. Es ist die Summe über alle Vorkommen der Ursache  $u_i$  in dem Ereignis  $E_j$  zu bilden:

$$K(u_{ij}) = \sum (g(u_i) / 100 \times g(f_i) / 100) \times k(E_j) \quad (11)$$

Die von Ursache  $u_i$  in einem Ereignis  $E_j$  verursachten normierten Kosten sind definiert als Produkt aus normiertem Gewicht der Ursache, des Fehlers und der Gesamtkosten des Ereignisses. Die Summe über alle Vorkommen der Ursache  $u_i$  in dem Ereignis  $E_j$  ist zu bilden:

$$k_n(u_{ij}) = \sum (g_n(u_i) / 100 \times g_n(f_i) / 100) \times k(E_j) \quad (12)$$

Die von Ursache  $u_i$  insgesamt verursachten Kosten sind definiert als Summe über alle Einzelkosten. Diese Summe kann aufgrund der fehlenden Normierung größer als die Gesamtkosten sein:

$$k(u_i) = \sum k(u_{ij}) \quad (13)$$

Analog lauten die normierten Gesamtkosten:

$$k_n(u_i) = \sum k_n(u_{ij}) \quad (14)$$

Ergebnisse dieses Risiko- und Kostenrechnungsmodells sind individuellen Fehlern und Fehlerursachen zugeordnete Einzelrisiken und Einzelkosten. Sie unterstützen und begründen Entscheidungen über effektive Präventionsmaßnahmen inhaltlich und wirtschaftlich.

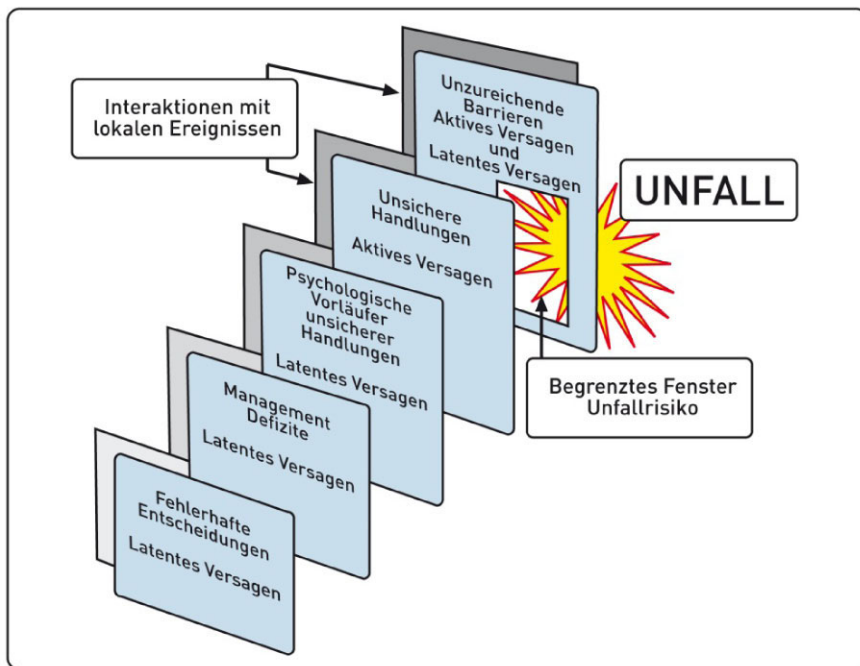
## 2.5 Unfallgeschehen und Präventionsmodell

Reason (ebda.) hatte sich mit „menschlichen“ Beiträgen am Zusammenbruch technischer Systeme beschäftigt und unterscheidet fünf Bedin-

gungsebenen der Unfallentstehung: Drei latente und zwei aktive Versagenskategorien, siehe nachfolgende Abb. 2.9:

- Fehlerhafte Entscheidungen
- Management-Defizite
- Psychologische Vorläufer (unsicherer Handlungen)
- Unsichere Handlungen
- Unzureichende Barrieren.

Demnach führen fehlerhafte Strategieentscheidungen, Managementfehler oder psychologische Bedingungen zu so genanntem „latentem Versagen“. Daraus können unsichere Handlungen folgen. Deren latentes Risiko führt dann zum Unfall, wenn unzureichend präventive Barrieren entsprechende *Fenster* vorfinden, siehe Abb. 2.9.



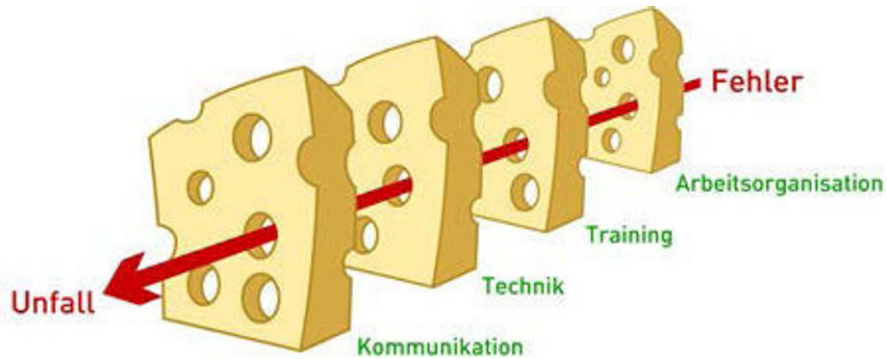
**Abb. 2.9** Latentes Versagen und Unfallentstehung (Reason, 1990)

Darauf bauten Frieling & Sonntag (1999) auf und forderten ein Arbeitssystem, „in dem Fehler als Erkenntnisquelle und nicht als personelles

Problem angesehen werden“. Fehler seien Folgen ergonomischer und organisatorischer Fehlgestaltungen des Arbeitssystems sowie fehlender personeller Leistungsvoraussetzungen. Ihnen liege im gängigen Umfeld technischer, organisatorischer und personaler Bedingungen zum Beispiel der Arbeitsorganisation eine hinreichende Kombination latenter Fehlerbedingungen zu Grunde. Auch sie beziehen sich ähnlich Reason (1990) oder Senders & Moray (1991) auf die Arbeits- und Managementebenen laut INSAG (1991).

Die Bedingungen auf der Arbeits- und der Managementebene haben unter weiteren Randbedingungen unsichere Handlungen und aktives Versagen mit konkreten Fehlern zur Folge. Fehler verursachen dann Unfälle, wenn unzureichende Barrieren entsprechende Risiken nicht verhindern oder minimieren, weil keine oder unzureichende Prävention stattfindet. Latentes Versagen ließe sich durch Maßnahmen auf der Strategie- und der Managementebene verhindern, siehe Abb. 2.9. Solche Barrieren seien humane Arbeitssystemgestaltung, ergonomische Arbeitsbedingungen oder effiziente und lernförderliche Organisationsstrukturen (Frieling & Algedri, 2001).

Teil der Risikopolitik ist die Qualitätssicherung als fortlaufende Überprüfung von Kosten und Nutzen von Maßnahmen als Teil des umfassenden Sicherheitsmanagementsystems. Sicherheitsmanagement versteht Präventionsmaßnahmen als sogenannte technische, personale oder organisatorische Barrieren, die verhindern, dass aus Fehlern Unfälle überhaupt entstehen oder deren Folgen zumindest mindern. Reason (1990) versinnbildlichte verbleibende Risiken durch die Löcher in Schweizer Käse. Abb. 2.10 zeigt eine sehr *löchrige* Präventionssituation, wenn in diesem Fall überhaupt von Prävention gesprochen werden kann.

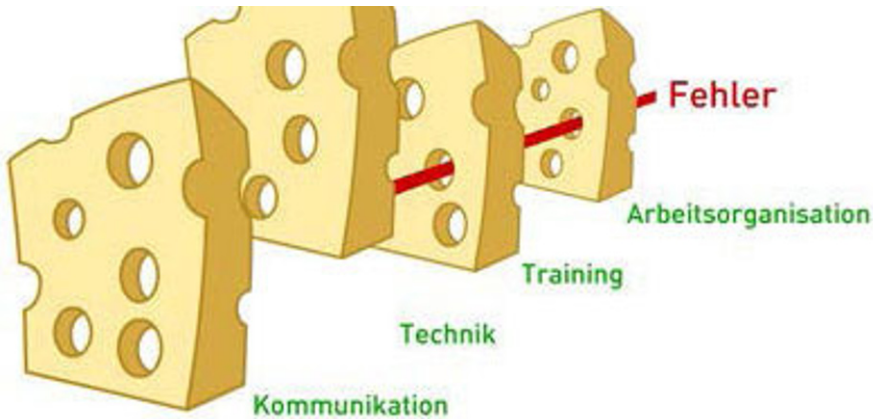


**Abb. 2.10** Präventionsmaßnahmen als Barrieren (nach Reason, 1990)

Effizientes Sicherheitsmanagement nach Reason verknüpft nun Einzelmaßnahmen so miteinander, dass zumindest die technische Barriere in Abb. 2.11 den Unfall verhindert; beispielsweise kann ABS die Folgen von Bremsen auf nasser Fahrbahn in der Kurve mindern.

Reasons Modell geht von tatsächlichen Unfällen aus, deren Daten und Hergänge analysiert wurden. So können nächste Unfälle derselben Art, also bekannte, erwartete Ereignisse, verhindert werden. Proaktive Sicherheitskultur geht darüber hinaus, will sie doch auch unbekannte, aber erwartete und schließlich gänzlich unbekannte und unerwartete Ereignisse verhindern bzw. deren Folgen mindern. Sicherheitsmanagementsysteme wie auch Ariadne SMS gehen einen Schritt in Richtung Prävention unbekannter, aber erwarteter Ereignisse. Dies leistet Sicherheitsmanagement auf der Basis umfassender Datenlage unter Einbezug der Hintergrundvariablen.





**Abb. 2.11** Wirksame Prävention (nach Reason, 1990)

Hier erscheinen verstärkte Bemühungen um Analysen von Gefährdungen und Zwischenfällen angezeigt, wie sie für den Luftverkehr im Safety Management Manual (2012) zur quantitativen Bewertung von Risiken und deren Abwehrmaßnahmen verpflichtend gefordert werden. Entsprechende Fehlermeldesysteme wurden in der Luftfahrt denn auch verpflichtend eingeführt. Entsprechende Bemühungen im Straßenverkehr oder anderen Bereichen befinden sich bestenfalls in den Anfängen und sollten forciert werden.

Noch weiter geht die Bewegung *Resilience Engineering*. Der Begriff *Resilienz* lässt sich aktuell nicht eindeutig und fachgebietsübergreifend definieren, siehe Diskussion in Longstaff, Koslowski & Geoghegan (2013). Im gegenständlichen Kontext bedeutet Resilienz oft Elastizität bzw. die Fähigkeit, in den Ausgangszustand zurückzuspringen, während im abstrakten Zusammenhang meist eine unscharfe Kombination aus Resistenz und Rekonvaleszenz gemeint ist.

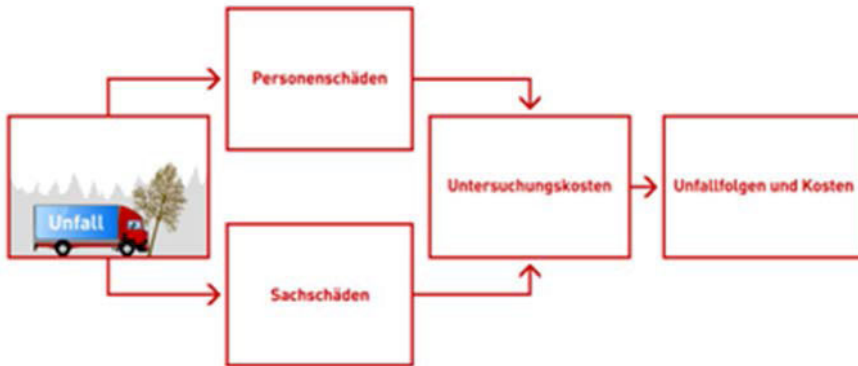
Zur Dokumentation von Resilienz gibt es unterschiedliche Ansätze, ein Beispiel ist die Zeit, die ein System benötigt, um in einen funktionsfähigen Zustand zurückzukehren. Andere wiederum verstehen Resilienz als Gegenteil der Brüchigkeit/Zerbrechlichkeit eines Systems, die wiederum durch die Multiplikation der Konstrukte Komplexität und Ungewissheit definiert wird.

Resilienz entstand aus der Kritik an Reasons Ansatz, er fördere eine reaktive Sicherheitskultur und wisse ungekannten Unfällen nicht vorzubeugen (Sheridan, 2008). Laut dieser Kritik bedarf die Entwicklung einer generativen Sicherheitskultur der Annahme, dass menschliches Versagen nicht vollständig verhindert und im Organisations- oder Designprozess nicht jedes Risiko antizipiert werden kann. Reason selbst suggeriert zudem, Prävention nicht allein anhand Analysen größerer Unfälle zu betreiben, sondern auch kleinere Pannen und Beinaheunfälle als Informationsquellen zu nutzen, da diese wesentlich häufiger aufträten.

Kritiker bemängeln zudem, dass erfolgreichen Arbeitsabläufen zu wenig Beachtung geschenkt werde, was eher zur Bestrafung falschen Verhaltens als zur Förderung sicheren Verhaltens führe (Hollnagel, 2011). Zudem sei Reasons Modell eine moderne Neuauflage unzähliger Zero-Risk-Models und lege den Fokus auf das vollständige Beseitigen von Risiken und nicht auf das Minimieren derselben; siehe Morgenstern (1910) und Diskussion in Kapitel 6 „Anmerkungen zu Sicherheitsmanagement und Resilienz“.

## **2.6 Kostenmodell für Unfälle**

Eine hier vorgenommene und schon erwähnte Neuerung ist die Ökonomisierung des Unfallgeschehens durch Kostenmodellierung mit den Kategorien Personenschäden, Sachschäden und Untersuchungskosten, siehe Abb. 2.12.



**Abb. 2.12** Struktur des Kostenmodells nach Käßler (2008), Käßler et al. (2008)

Die Unfallfolgekosten sind das Kriterium der Risikovorhersage und Basis der Prävention. In einem umfassenden Kostenmodell werden Personenschäden, Sachschäden und Untersuchungskosten in ca. 30 Kostenstellen erfasst.

*Personenschäden* enthalten Kosten für:

- Bergung
- Transport
- Untersuchung
- Vorstationär
- Stationär
- Nachstationär
- Todesfall
- Dienstausschuss
- Ersatz
- Gemeinkosten.

*Sachschäden* enthalten Kosten für:

- Bergung
- Transport
- Prüfung
- Reparatur
- Neubeschaffung

- Gemeinkosten.

*Untersuchungskosten* errechnen sich aus:

- Externe Kosten
- Reisekosten
- Personalkosten
- Analysekosten
- Gemeinkosten.

Dieses Modell wurde analog zu Baum & Höhnscheid (1999) und Baum et al. (2001) entwickelt, die volkswirtschaftliche Kosten von Personen- und Sachschäden im Straßenverkehr simulieren. Die Bundesanstalt für Straßenwesen lässt mit diesem Modell zyklisch z.B. von Höhnscheid & Straube (2006), Baum, Kranz & Westerkamp (2010) oder Kranz & Straube (2011) entsprechende Pauschalen für Volkswirtschaftliche Schäden durch Straßenverkehrsunfälle errechnen. In 2011 wurden beispielsweise für Personenschadenskosten im Jahr 2009 folgende Summen ermittelt, siehe Kranz & Straube (2011) und Tab. 2.5.

**Tab. 2.5** Kostensätze je verunglückte Person bzw. je Unfall in 2009

Kostensätze Personenschäden	Euro
Getötete	996.412
Schwerverletzte	110.571
Leichtverletzte	4.416
Kostensätze Sachschäden	Euro
Unfall mit Getöteten	40.108
Unfall mit Schwerverletzten	19.215
Unfall mit Leichtverletzten	13.036
Schwerwiegender Unfall nur Sachschaden	19.365
Übriger Sachschadenunfall	5.643

Aufgrund fehlender Zahlen der Bundeswehr dazu verwendet das vorliegende Modell für Getötete bei Unfällen mit Waffen und Munition usw. die Pauschalen der Tab. 2.5, siehe oben. Alle anderen Kosten werden tatsächlich erfasst oder von den Unfalluntersuchern in den Kategorien laut Abb. 2.12 oben geschätzt.

Dieses Kostenrechnungsmodell schätzt konservativ, da es weder Schmerzensgelder noch Aufwände für Rehabilitation, Renten oder Entschädigungen enthält. Diese Kosten sind innerhalb der BW nicht verfügbar oder aus datenschutzrechtlichen Gründen nicht zugänglich. Zudem untersucht die BW ihre Unfälle in Eigenregie. Lediglich in Rechnung gestellte Fremdkosten werden als Untersuchungskosten aufgenommen, nicht aber eigene Personalkosten.

## 2.7 Selbstlernende Modelle: Bayessche und Semantische Netze im Rahmen des Unfallgeschehens

Die Digitalisierung des Expertenwissens der Unfalluntersucher verfolgt das Ziel, weitgehend maschineller Analyse. Solche Verfahren wurden analysiert und erprobt. Hier erschienen besonders Verfahren des maschinellen Lernens mit Semantischen und Bayesschen Netzen angezeigt, um

langfristig vor allem die Fehler- und Ursachensuche zu unterstützen oder gar zu ersetzen.

Zunächst werden die Abhängigkeitsstrukturen zwischen Zufallsvariablen nach Borgelt & Kruse (2002) mit Bayesschen Netzen untersucht. Sie definieren aus mathematischer Sicht eine gemeinsame Verteilung der Daten auf allen Variablen des Gegenstandsbereiches und stellen damit ein konsistentes, probabilistisches Modell zur Verfügung. Die Modelle können auf unterschiedlichste Art ausgewertet werden, z.B. diagnostisch zum Rückschluss von Beobachtungen auf mögliche Ursachen - wie beispielsweise in der Medizin - oder auch prognostisch zur probabilistischen Vorhersage des Eintretens zukünftiger Ereignisse, wie beispielsweise den voraussichtlichen Strombedarf in Kraftwerken.

Analysen mit Bayesschen und Semantischen Netzen werden genutzt, um Vorhersagen zu machen und Zusammenhänge der Daten untereinander, Interkorrelationen, offen zu legen. Netze können sowohl maschinell aus Daten gelernt als auch durch Experten erstellt werden. Es ist auch möglich, beide Vorgehensweisen zu kombinieren: Ein maschinell gelerntes Netz kann von Experten modifiziert werden. Es kann vervollständigt werden, indem es durch die nicht im Datensatz enthaltene latente Variablen ergänzt wird.

Um die Möglichkeiten der Bayesschen Netze nutzen zu können, muss die Anzahl der Daten groß sein. Zum Untersuchungszeitpunkt standen ca. 1200 Datensätze zur Verfügung. Mit anwachsendem Datenbestand werden die Ergebnisse der Netze reliabler.

Es war geplant, mit Hilfe maschinellen Lernens mit Bayesschen Netzen das Sicherheitsmanagement mittel- bis langfristig um multivariate Dimensionen ergänzen. Allerdings zeigte sich, dass Entwicklung und Test äußerst zeit- und personalaufwendig waren und mittelfristig nicht aus Projektmitteln finanziert werden konnten. Zudem entsprachen die Ergebnisse auch infolge geringen Datenbestandes nicht den Erwartungen und waren wenig zielführend. Die Arbeiten mit Bayesschen Netzen wurden daher eingestellt.

Dennoch blieben moderne multivariate Verfahren zur Unterstützung der Analysen angezeigt. Recherchen zu unaufwendigeren Verfahren maschinellen Lernens zeigten, dass für die Unterstützung der Sachbearbeiter

bei der Fehler- und Ursachensuche Semantische Netze geeigneter sind, siehe Anhang E „Evaluation der Daten- und Modellqualität“.

Dieses Verfahren wird heute zur Unterstützung der Unfalluntersucher bei der Fehler- und Ursachensuche eingesetzt. Die Semantik generiert mehrere Fehler und Ursachen pro Ereignis und stellt sie den Unfalluntersuchern als zur Annahme oder Ablehnung zur Verfügung. So lernt das Netz Zusammenhänge genauer vorherzusagen.

Überprüfungen der Vorhersagequalität erfolgten anhand Korrelation der durch die Sachbearbeiter ohne Unterstützung ausgesuchten Fehler und Ursachen mit den durch das semantische Netz vorhergesagten. Die Korrelation betrug nach einer Anlernphase bereits nahezu 80 Prozent und stieg mit anwachsendem Datenbestand weiter. So kann bereits heute der Arbeitsaufwand erheblich reduziert werden.

Dies ist ein erster Schritt in Richtung Automatisierung der gesamten Fehler- und Ursachenidentifikation des Sicherheitsmanagementsystems.



Smart Safety Management mit Ariadne SMS

Käppler, W.D.; Pressler, R.K.; Siebel, M.; Specht, D.

2014, XVII, 308 S. 150 Abb., Hardcover

ISBN: 978-3-642-55250-2