Sicherheit

Babette Fahlbruch, Markus Schöbel und Juliane Marold

2.1 Einleitung

Sicherheit in Organisationen übt einen starken Einfluss auf den wirtschaftlichen Erfolg, die gesellschaftliche Akzeptanz sowie das Wohlbefinden und die Zufriedenheit von Organisationsmitgliedern aus. In der Europäischen Union kommen jährlich über 5000 Menschen durch arbeitsbedingte Unfälle ums Leben. Neben schweren personenbedingten Konsequenzen kommt es zu hohen volkswirtschaftlichen Einbußen, diese können je nach Land zwischen 1% und 3% des Bruttosozialprodukts (OSHA, 2002) betragen.

Die Vermeidung von Unfällen ist somit ein wichtiges Ziel jeder Art von Organisation. Dies gilt sowohl für Arbeitsunfälle, bei denen das Ausmaß des Schadens in erster Linie die ausführende Person betrifft, als auch für organisationale Unfälle, die durch das Zusammentreffen fehlerhafter Einzelfaktoren entstehen und deren Schadensausmaß weit über die eigentlichen Organisationsgrenzen hinausgehen kann.

In diesem Kapitel werden ausgewählte Ansätze und Theorien der Sicherheitswissenschaft vorgestellt, die das menschliche Handeln in Systemen mit hohem Gefährdungspotenzial beschreiben. So werden zunächst unterschiedliche Perspektiven auf das Konzept Sicherheit dargestellt. Dann wird auf Theorien Bezug genommen, die sich mit dem menschlichen Beitrag zur (Un-)Sicherheit in Organisationen mit hohem Gefährdungspotenzial beschäftigen. Es folgt ein Überblick zu strategischen Steuerungsmechanismen und Implikationen des Managements von Sicherheit. Abschließend wird als Ergänzung zur Sichtweise der institutionalisierten Instrumente das Konzept der Sicherheitskultur diskutiert.

2.1.1 Begriffsbestimmung

In der alltäglichen Verwendung des Begriffs »Sicherheit« sprechen wir im Allgemeinen (in Anlehnung an ein mathematisches Verständnis) von der 100%igen Wahrscheinlichkeit des Zutreffens einer Aussage oder des (Nicht-)Eintretens eines Ereignisses. Gemäß dieser ergebnisorientierten Perspektive wird in ingenieurwissenschaftlichen Ansätzen Sicherheit als ein Zustand der voraussichtlich störungsfreien und gefahrenfreien Funktion definiert (ISO/IEC Guide 51, 1999). In diesem Zusammenhang wird Sicherheit als positiver Sollzustand mit einer weiteren Eigenschaft von Systemen gleichgesetzt, der Zuverlässigkeit. Systeme gelten als zuverlässig, wenn eine geforderte Funktion unter gegebenen Arbeitsbedingungen während einer festgelegten Zeitdauer ausfallfrei ausgeführt wird (DIN 40041, 1990). Zuverlässigkeit umfasst demzufolge drei Aspekte:

- Korrektheit (nach Vorgaben verlaufend),
- Robustheit (System kann auftretende Störungen ausgleichen) und
- Ausfallsfreiheit (definierte Sicherheit gegen einen Ausfall).

Ein Begriffsverständnis, das über die ingenieurwissenschaftliche Perspektive hinausgeht, wird in der Forschung zu Organisationen mit hohem Gefährdungspotenzial (z. B. Kernkraftwerke, Öltanker, Flugzeugträger) vorangetrieben. Sicherheit wird hier als Eigenschaft aufgefasst,

> » […] die es dem System gestattet, ohne größere Zusammenbrüche unter vorgegebenen Bedingungen und mit einem Minimum unbeabsichtigten Kontrollverlusts oder Schadens für die Organisation und die Umwelt zu funktionieren. (Fahlbruch & Wilpert, 1999, S. 56) «

Die Sicherheit ergibt sich aus fortwährenden Interaktionen von Organisationsmitgliedern, Strukturen und Regeln sowie Technologien in und außerhalb der Organisation (Gherardi, Nicolini & Odella, 1998). Nicht der störungsfreie Betrieb einzelner Systemkomponenten, beispielsweise eines einzelnen Ventils, sondern das Zusammenwirken von Faktoren wie Regelwerken, Qualifikationen der Operateure, Komponentenabhängigkeiten oder Managementsysteme sind mit einzuschließen, um eine sichere Ausführung sicherheitskritischer Prozesse in der Gesamtorganisation zu gewährleisten. Es steht bei dieser Betrachtung somit nicht mehr nur das einzelne Ergebnis im Vordergrund, sondern auch die kontinuierlich ablaufenden Prozesse, die zu diesem beitragen. Weick & Sutcliffe (2001,

S. 43) sprechen in diesem Zusammenhang von einem »dynamischen Nicht-Ereignis«.

Nach diesem Verständnis sind Zuverlässigkeit und Sicherheit unterschiedliche Qualitäten eines Systems und können unabhängig voneinander auftreten. Dies zeigt sich auch in der Diskussion um Gestaltungsaspekte von Organisationen mit hohem Gefährdungspotenzial (Sagan, 2004). Die Implementierung redundanter Komponenten (zusätzlich vorhandene funktional gleiche oder vergleichbare Ressourcen eines technischen Systems) kann die Zuverlässigkeit einer sicherheitskritischen Systemfunktion erhöhen, da bei Ausfall einer Komponente ihre Funktion durch eine redundante Komponente übernommen wird. Allerdings führt eine zunehmend redundante Systemauslegung auch zu einer erhöhten Systemkomplexität (Perrow, 1987). Diese kann neue, möglicherweise unvorhersehbare Wechselwirkungen bedingen (► Kap. 17.2). Daraus folgt, dass ein System zwar aus zuverlässigen Einzelkomponenten besteht, in der Gesamtheit aber nicht zwangsläufig als sicher einzustufen ist, da Sicherheit vornehmlich als Systemeigenschaft aufgefasst wird (Leveson, 2011).

Sicherheit entsteht kontinuierlich aus dem Zusammenwirken von intra- und extraorganisationalen Faktoren (wie z. B. den Organisationsmitgliedern, der Technologie, den Strukturen oder Regeln) und bezeichnet ein Funktionieren ohne größere Zusammenbrüche oder Schäden für die Organisation und die Umwelt, ein sog. dynamisches Nichtereignis.

2.1.2 Sicherheit in der betrieblichen Praxis

Die Förderung von Sicherheit in der betrieblichen Praxis zielt auf die Vermeidung gesundheitlicher Schädigungen der Beschäftigten ab. Sicherheit wird nach diesem Verständnis als gefahrenfreier Zustand bei der Berufsausübung definiert (Skiba, 1997). Nach dem deutschen Arbeitsschutzgesetz (ArbSchG) ist der Arbeitgeber verpflichtet, erforderliche Maßnahmen zur Herstellung sicherer Arbeitsbedingungen durchzuführen. Zudem hat er die Maßnahmen auf ihre Wirksamkeit zu überprüfen und diese gemäß sich ändernder Gegebenheiten anzupassen. Die Verhütung von Unfällen, Berufskrankheiten und arbeitsbedingten Erkrankungen hat dabei Vorrang vor Entschädigungen. Die Gesetzesvorlagen verfolgen demnach einen präventiven Weg.

Die Umsetzung von präventiven Maßnahmen kann gemäß dem TOP-Modell des Arbeitsschutzes (Skiba, 1997) erfolgen. Dieses postuliert eine Maßnahmenhierarchie, die technische (T – Vermeidung bzw. Trennung der Gefahr), organisatorische (O – zeitliche Begrenzung der Einwirkung einer Gefahr bringenden Bedingung) und persönliche Voraussetzungen (P – Bereitstellung persönlicher Schutzkleidung oder Unterweisungen) der Arbeit berücksichtigt. Das Konzept der Arbeitssicherheit erlangt in allen klassischen Industrien eine wichtige Bedeutung. Heute werden die Aufgaben im Rahmen integrierter Managementsysteme (IMS) durch eine sinnvolle Verknüpfung mit Qualitäts- und Umweltschutzaspekten verfolgt, wie z. B. im EFQM-Modell for Excellence (EFQM, 1999–2003) oder im St. Galler Konzept für ein Integriertes Qualitätsmanagement (Seghezzi, Fahrni & Herrmann, 2007).

Inwieweit eine Organisation eine umfassende bzw. systemorientierte Strategie hinsichtlich der Gewährleistung von Sicherheit verfolgen sollte, hängt in erster Linie vom Gefährdungspotenzial ihrer Produktionsprozesse ab. Systemsicherheit erhält eine unverzichtbare Bedeutung, wenn aufgrund der verwendeten Technologien bzw. Produktionsmittel ein hohes Gefährdungspotenzial entsteht, wie z. B. in sog. High-hazard-Organisationen: Kernkraftwerke, chemische Anlagen, Flugzeugträger oder Flugsicherungssysteme. Doch Organisationen, denen ein hohes Gefährdungspotenzial innewohnt, müssen nicht zwangsläufig riskant sein, im Gegenteil, das Risiko ist relativ gering. Gemäß Amalberti (2001) ist ein gefahrenträchtiges System durch ein Risiko von 10^3 gekennzeichnet. Dies bedeutet, dass das Risiko (eines »gefährdenden« Systemversagens) größer ist als ein Unfall auf 1000 Ereignisse (vergleichbar mit dem Risiko beim Bungee-Jumping). Systeme mit einem Risikograd von einem Unfall auf 1000 bis 100.000 Ereignissen (10^5) werden als regulierte Systeme bezeichnet.

Kernkraftwerke und die zivile Luftfahrt bzw. die europäische Bahn gelten als ultrasichere Systeme (»ultra safe«). Deren Risikograd liegt zwischen einem Unfall auf 100.000 bis zu unter einem Unfall auf 1.000.000 Ereignissen (10^6).

Ultrasichere Organisationen verdanken ihr geringeres Risikopotenzial bestimmten Gestaltungsmerkmalen, die sich oftmals im Design technischer Systeme widerspiegeln. So werden z. B. nach dem **Prinzip des beschränkten Versagens** (»fail safe«) schon bei der Entwicklung solcher Systeme mögliche Schadensfälle einkalkuliert, um größere Gefährdungen auszuschließen (wie das Vermeiden von Überbeanspruchungen durch Sollbruchstellen bzw. Sicherungen). Oder dem Ausfall sicherheitskritischer Funktionen wird durch mehrfache Auslegung von Systemen mit gleicher Funktion nach dem Redundanz- oder Diversitätsprinzip vorgebeugt.

Im Allgemeinen gilt das **Prinzip der tief gestaffelten Sicherheitssysteme** (»defence in depth«) als wesentliches Gestaltungsmerkmal, insbesondere in kerntechnischen Anlagen. Es wird das Ziel verfolgt, das Eintreten von sicherheitskritischen Ereignissen durch Barrieren zu verhindern (ausführlich ► Kap. 9). Beim Ausfall einzelner Komponenten wird das Schadensausmaß durch die voneinander unabhängigen Sicherheitsebenen begrenzt, um schwerwiegende Konsequenzen für die Umgebung zu verhindern, wie in einer kerntechnischen Anlage das Mehrbarrierensystem: Hüllrohre der Brennstäbe, Reaktordruckbehälter, Sicherheitsbehälter, Reaktorgebäude aus Stahlbeton. Zudem werden Barrieren auch prozedural angelegt, indem sie menschliches Verhalten im Umgang mit technischen Systemen anleiten und unterstützen (z. B. Sicherheitsanweisungen, Schulungen zur Qualifizierung des Bedienerpersonals).

Obwohl das Risiko eines Systemzusammenbruchs als relativ gering eingeschätzt wird, zeigen beispielsweise der Chemieunfall in Seveso (1976), die Reaktorkatastrophe in Tschernobyl (1986) oder die Flugzeugkollision von Überlingen (2002), dass trotz massiver technischer Sicherheitsvorkehrungen Systeme mit hohem Gefährdungspotenzial versagen. Es wird deutlich, dass eine Optimierung der Systemsicherheit nicht nur die Förderung der technischen Sicherheit umfassen sollte, sondern auch den Faktor Mensch berücksichtigen muss.

2.2 Erklärungsansätze in der Sicherheitsforschung: Warum sind Systeme (un)sicher?

Wichtige Beiträge zur Entwicklung der Sicherheitsforschung liefern die Arbeiten von Turner (1978), Perrow (1987) sowie die Arbeiten der Forschungsgruppe High Reliability (La Porte, 1996; La Porte & Consolini, 1991; Rochlin, 1993; Weick, 1987; Weick & Roberts, 1993). Die Gemeinsamkeit dieser Ansätze liegt in deren Zielstellung, die Fähigkeit von Organisationen zu beschreiben, dauerhaft zuverlässig bzw. sicher zu operieren. Zudem stellen sie die Bedeutsamkeit menschlichen Verhaltens und der organisationalen Rahmenbedingungen für die Gewährleistung der Sicherheit heraus. Während in der Theorie der fehlerhaften Informationsverarbeitung in Organisationen (Turner, 1978) und der Theorie der normalen Katastrophen (Perrow, 1987) Unzulänglichkeiten der Systemgestaltung und der Informationsnutzung deutlich gemacht werden, beschäftigen sich die Begründer der Theorie der Organisationen hoher Zuverlässigkeit (Weick & Roberts, 1993) mit wirksamen organisationalen Maßnahmen, die ein System befähigen, zuverlässig zu operieren. Im Folgenden wird auf diese Ansätze näher eingegangen.

2.2.1 Modell der fehlerhaften Informationsverarbeitung in Organisationen

Ereignen sich schwere Katastrophen, erscheinen diese zunächst als unvorhersehbar (»fundamental surprises«). Im Rahmen der nachfolgenden Analyse findet man dann aber oftmals Anzeichen dafür, dass zumindest einigen Mitgliedern der jeweiligen Organisation schon vor bzw. während der Ereignisentstehung »ereignishinweisende« Informationen vorlagen. Diesem zunächst als Paradox erscheinenden Phänomen widmet sich Turner (Turner, 1978; Turner & Pidgeon, 1997) in seiner Theorie der »man-made disasters«. Auf der Grundlage einer

systematischen Analyse von 84 Unfallberichten kam er zu dem Schluss, dass die Ursachen dieser Unfälle auf Dysfunktionalitäten von menschlichen und organisatorischen Anpassungsprozessen zurückgehen. Als Beispiel nennt er Störungen des Informationsflusses innerhalb einer Organisation bzw. fehlerhafte oder unzureichende Interpretationen und Bewertungen von vorhandenen sicherheitskritischen Informationen.

Diese Theorie der fehlerhaften Informationsverarbeitung macht auf Faktoren der Entstehung von Ereignissen aufmerksam, die mit einer deutlichen räumlich-zeitlichen Distanz zum eigentlichen Ereignisentstehungsort in einer Organisation verankert sein können. Dieser Aspekt wurde von Reason (1990, 1997) weiterentwickelt, der zwischen aktiven und latenten Fehlern unterscheidet (► Kap. 3). Ersteren kommt eine Auslösefunktion zu, während die zweiten unerkannt im System ereignisfördernd wirken. Latente Fehler oder indirekte Faktoren spiegeln organisationale Schwachstellen oder dysfunktionale Beziehungen zwischen Organisationen wider.

Zur Zeit der Entwicklung dieser Theorie stand Turners Sichtweise traditionellen Konzepten der menschlichen Fehlerforschung entgegen, die ausschließlich auf direkt ereignisauslösende Fehlhandlungen fokussieren. Einen ähnlichen Beschreibungsansatz, der insbesondere auf strukturelle Merkmale von Organisationen bei der Ereignisentstehung hinweist, wählte Perrow in seiner Arbeit mit dem provokanten Titel »Theorie der normalen Katastrophen« (1987).

2.2.2 Theorie der normalen Katastrophen (»normal accident theory«)

Auf der Basis des Unfallgutachtens von Three Mile Island (TMI, 1978) sowie der intensiven Auseinandersetzung mit vorwiegend ingenieurwissenschaftlichen Analysen der eingesetzten Untersuchungskommission entwickelte der Organisationssoziologe Perrow seinen Beschreibungsansatz. Das Hauptaugenmerk in der Analyse von Three Mile Island legte Perrow auf die Beschreibung der Mechanismen, die Systemunfälle in komplexen technischen Systemen zwangsläufig bedingen (Perrow, 1987). Nach seiner Theorie ereignen sich Systemunfälle (»normal accidents«) aufgrund unvorhergesehener Wechselwirkungen zwischen einzelnen Ausfällen. Den Schwerpunkt bei der Definition von Systemunfällen legt Perrow auf die Anzahl und Art der betroffenen Einheiten eines Systems. Die Entstehung von Unfällen wird demnach als natürliche Konsequenz eines Systems gesehen, das durch (1) viele komplexe Interaktionen und (2) enge Kopplung gekennzeichnet ist.

1. Die Eigenschaften von Interaktionen in einem System werden durch die zwei Pole **linear** und **komplex** bestimmt. Komplexe Interaktionen äußern sich in Rückkopplungsschleifen, Verzweigungen oder Sprüngen innerhalb der Prozessabläufe und führen zu für den Operateur unerwarteten Ergebnissen. Ein Wärmetauscher, der gleichzeitig als Heizvorrichtung dient, kann beim Ausfall beide Funktionen nicht mehr erfüllen. Lineare Interaktionen sind für den Operateur gut sichtbar und Teil des normalen Betriebsablaufs. Als Beispiel für lineare Interaktionen führt Perrow ein Montageband an, das beim Ausfall die Teile auflaufen lässt, aber zu keinem unvorhersehbaren Schaden führt.
2. Die zweite von Perrow identifizierte Systemeigenschaft, die Weick (1976) im Rahmen der Analyse von organisationalen Strukturen beschreibt, ist die Art der Kopplung einzelner Systemkomponenten (eng vs. lose). Eng gekoppelte Systeme (zeitlich, räumlich, funktional) zeichnen sich durch keinerlei Verzögerungen des Betriebsablaufs aus, die Abläufe sind invariabel gestaltet und das Produktionsziel kann nur mithilfe einer vorgegebenen Strategie erreicht werden. In eng gekoppelten Systemen zeigen lokale Störungen meist große Auswirkungen, da z. B. der gestörte Systemteil nicht abgeschaltet werden kann oder aufgrund der räumlichen Nähe ebenfalls zerstört wurde. Die Just-in-Time-Produktion in der Automobilindustrie erfüllt diese Kriterien. Zulieferbetriebe produzieren und liefern die Autoteile zu dem Zeitpunkt, in denen sie benötigt werden, ansonsten kommt es zur Unterbrechung des gesamten Produktionsprozesses. Eine lose

Kopplung ermöglicht bestimmten Teilen des Systems, gemäß ihrer eigenen Logik zu funktionieren. Lose gekoppelte Systeme können Störungen oder erzwungene Änderungen besser verarbeiten, ohne sich zu destabilisieren. Bei eng gekoppelten Systemen müssen Puffer, Redundanzen und Substitutionsmöglichkeiten von den Konstrukteuren vorab eingeplant werden.

Die überwiegend auf der Untersuchung des Unfalls von TMI basierenden Schlussfolgerungen zu den Versagensmechanismen überträgt Perrow auf ein sehr breites Feld technischer Systeme, angefangen von Kernkraftwerken, Petrochemie, Schifffahrt, Flugsicherung über Staudämme, Bergwerke und Gentechnologie. Deren Gemeinsamkeiten sieht er in den grundlegenden Unzulänglichkeiten der Systemgestaltung. Maßnahmen zur Förderung von Sicherheit sind in einem solchen System nur reaktiv möglich. Optimalerweise sollten Systeme schon bei der Planung im Hinblick auf die Vermeidung des Zusammentreffens dieser Eigenschaften gestaltet werden. Weitere sicherheitsfördernde Maßnahmen sieht Perrow in Faktoren wie der Systematisierung von Informationen über Fehler im System, der gleichmäßigen Verteilung und Zugänglichkeit der Informationen sowie in der Offenheit für Kritik von außen (Perrow, 1986).

Auch wenn einige Kritiker anmerken, dass Perrow seine Schlussfolgerungen vorwiegend aus der Analyse von Unfalluntersuchungen (Hopkins, 1999) ableitet und eine Generalisierung auf ein sehr heterogenes Feld technischer Systeme anstrebt, liegt sein Verdienst v. a. in der Ausweitung des Betrachtungsspielraums und in der Einbeziehung struktureller Faktoren bei der Betrachtung von Systemsicherheit.

2.2.3 Theorie der Organisationen mit hoher Zuverlässigkeit (»high reliability theory«)

Die »high reliability theory« ging aus der intensiven Beschäftigung der interdisziplinären Forschungsgruppe in Berkeley und Michigan mit der Analyse von Organisationen mit hohem Gefährdungspotenzial hervor, denen es dennoch gelingt, weit weniger Unfälle zu produzieren als statistisch zu erwarten wären (Weick & Roberts, 1993). Die Annahmen der HR-Theorie gründen auf Felduntersuchungen, die auf Flugzeugträgern der U.S. Navy durchgeführt wurden, sowie auf der Analyse organisationaler Strukturen des Flugsicherungssystems der Federal Aviation Administration (FAA) und des Kernkraftwerks Diablo Canyon in Kalifornien/USA. Zielstellung war die Identifikation von Systemeigenschaften, die es den Organisationen ermöglichen, trotz des vorhandenen Gefährdungspotenzials (»high-hazard«) nahezu fehlerfrei und somit zuverlässig zu operieren. Die HRO-Forscher führen die Sicherheit dieser Systeme grundsätzlich auf achtsames Handeln zurück. Kennzeichen sind (► Kap. 9) eine ständige Aktualisierung der Deutung von Systemzuständen und Zusammenhängen, um frühzeitige, meist noch schwache Signale plausibel erklären und angemessene Reaktionen entwickeln zu können. Das Prinzip der Achtsamkeit (»heedfulness«) ergibt sich aus dem Zusammenspiel folgender Merkmale (Weick & Roberts, 1993):

- Toleranz gegenüber Fehlern,
- Abneigung gegen vereinfachende Interpretationen,
- Sensibilität für betriebliche Abläufe,
- Streben nach Flexibilität und
- Respekt vor fachlichem Wissen und Können.

Die Toleranz gegenüber Fehlern zeigt sich in häufig durchgeführten Analysen von Beinahe-Ereignissen oder in den Bemühungen, den Umgang mit Fehlern den Mitarbeitenden so zu vermitteln, dass ein freiwilliges Melden der Fehler gefördert wird. Das Ziel ist eine kontinuierliche Verbesserung durch die Gewährleistung eines geeigneten Erfahrungsrückflusses. Hierzu können Belohnungsstrukturen für Fehlerentdeckung und Fehlermeldung etabliert werden. Oft entstehen Fehler dadurch, dass schwache Signale übersehen wurden, die Wahrnehmung der jeweiligen Situation eingeschränkt war und dann Entscheidungen mit folgenschweren Konsequenzen getroffen wurden. Durch eine kontinuierliche Überprüfung von Sicherheitsstandards können HROs eine Sensibilität für betriebliche Abläufe entwickeln. Diese wird durch einen fortwährenden Austausch an relevanten Informationen erreicht.

Die bisher genannten Merkmale erfassen gewünschte Muster, die das Antizipieren und bewusste Wahrnehmen von unerwarteten Systemzuständen ermöglichen sollen. Kommt es innerhalb der HROs dann doch zu unvorhergesehenen Ereignissen, sind situationsabhängige flexible Wechsel zwischen Organisationsformen mit unterschiedlichem Zentralisierungs- bzw. Autonomiegrad entscheidend (► Kap. 10). Mitarbeiter und Mitarbeiterinnen können, unabhängig von ihrer Stellung in der Hierarchie, allein wichtige Entscheidungen treffen, sofern sie hierzu qualifiziert sind. Dies bedeutet, dass die Expertise der Akteure, falls notwendig, jederzeit die hierarchische Struktur aushebeln kann.

2.3 Management von Sicherheit in der Praxis

Die Gewährleistung von Sicherheit wird in Industrien mit hohem Gefährdungspotenzial v. a. als eine Managementaufgabe angesehen. Sicherheitsmanagement ist die strategische Steuerung organisationalen Handelns und kann auch als die durch die Unternehmensleitung veranlasste Institutionalisierung der sicherheitsgerichteten Aktivitäten in einer Organisation angesehen werden. Ähnlich wie beim Qualitätsmanagement sollen Faktoren mit potenziellem Einfluss identifiziert und kontrolliert werden, jedoch mit dem Ziel, die Sicherheit und Zuverlässigkeit der Organisation zu gewährleisten und zu optimieren.

2.3.1 Ansätze des Sicherheitsmanagements

Eine Unterteilung von Sicherheitsmanagementansätzen nach ihrem Schwerpunkt, der sich bei der Analyse von Stör- und Unfällen, bei Maßnahmenfindung und sicherheitsgerichteten Interventionen zeigt, nimmt Reason (1997) vor. Er unterscheidet dabei drei Sicherheitsmanagementmodelle:

- Personenmodell,
- Ingenieurmodell und
- Organisationsmodell.

Personenmodell

Das Personenmodell wird am besten durch den traditionellen Arbeitssicherheitsansatz charakterisiert. Es werden v. a. Fehler, unsichere Handlungen und Regelverletzungen fokussiert. Die Ursachen von Stör- und Unfällen werden in der Regel in psychologischen Faktoren wie mangelnde Aufmerksamkeit, unzureichende Motivation oder fehlende Fähigkeiten gesehen. Begründet ist dies in der impliziten Annahme, dass alle Mitarbeiter und Mitarbeiterinnen sich bewusst und frei zwischen sicherem und unsicherem Verhalten entscheiden können. Dementsprechend zielen Maßnahmen v. a. auf Auswahl, Training und Schulungen von Mitarbeitern. Im Grunde greift ein derart verstandenes Sicherheitsmanagement jedoch zu kurz, da sowohl Analysen als auch Interventionen hauptsächlich auf die Mitarbeiter und Mitarbeiterinnen und nicht auf die organisationalen und technischen Randbedingungen zielen.

Ingenieurmodell

Das Ingenieurmodell steht in der Tradition von Ingenieurwissenschaft, Arbeitswissenschaft und Risikomanagement (»risk control«, »loss control«). Schwachstellen werden im Rahmen dieses Modells im Design der Technologie oder der Mensch-Maschine-Schnittstelle erklärt. Sicherheit kann daher in das System »eingebaut« werden. Bei diesem Modell zielen Maßnahmen auf eine technische Verbesserung der Anlage und der Mensch-Maschine-Schnittstelle. Ausgelassen werden Aspekte wie Führung, Teamprozesse, Organisation oder Dokumente und Arbeitsunterlagen, denen im folgenden Modell besondere Beachtung geschenkt wird.

Organisationsmodell

Das Organisationsmodell kann als eine Erweiterung des Ingenieurmodells angesehen werden. Grundlage ist die Annahme, dass neben technischem Versagen und Operateursfehlern auch weitere latente Faktoren in der Organisation zu der Entstehung von Unfällen beitragen. So kann die Instandsetzung beispielsweise zu lange Prüfintervalle haben, sodass Verschleiß oder Alterung nicht rechtzeitig bemerkt werden, was zum Ausfall einer technischen Komponente führen könnte. Als ein weiteres Beispiel sei hier eine ungünstige Arbeits-

planung genannt, durch die die Wahrscheinlichkeit für das Auftreten von Operateurfehlern erhöht werden könnte. Eine kontinuierliche Kontrolle und Anpassung elementarer Systemfunktionen und -prozesse ist also erforderlich, um Sicherheit zu gewährleisten. Maßnahmen sind dementsprechend umfassend konzipiert und beziehen alle Ebenen der Organisation mit ein, da ein ausschließlicher Fokus auf Personen oder die Mensch-Maschine-Schnittstelle wichtige Einflussfaktoren auf die Sicherheit außer Acht lässt.

Für die praktische Umsetzung werden häufig Sicherheitsmanagementsysteme (SMS) eingesetzt, die in der Regel aus den Bausteinen Prozesswesen, Gefahren- und Risikomanagement, Berichtswesen und interne Auditierung bestehen. Zum Prozesswesen können Prozessidentifikation, Prozessdokumentation, Aktualisierung und Changemanagement gezählt werden. Für einen Flughafen können beispielsweise Baustellenplanung, Winterdienst auf Start- und Landebahn oder Abfertigung auf dem Vorfeld Prozesse sein, die im SMS erfasst werden. Für die Dokumentation könnten der Name des Prozesses, das Erstellungsdatum, die Dokumentennummer, das ausführende Unternehmen bzw. die Flugplatzabteilung, der Prozesseigner, am Prozess Beteiligte, existierende Vorgaben, durchgeführte Audits und vorgefallene Ereignisse festgehalten werden. Häufig werden auch Vorgaben durch Aufsichtsbehörden festgeschrieben. Zum Beispiel wurde durch die Änderung des ICAO-Abkommens über die internationale Zivilluftfahrt (International Civil Aviation Organisation) – Annex 14 die Einführung von SMS an Flugplätzen verpflichtend (ICAO, 2004).

Beispiel

Die Implementierung, Funktion und Umsetzung des Sicherheitsmanagementsystems (SMS) an Flugplätzen wird durch die luftrechtliche Genehmigungsbehörde geprüft. Ein SMS gilt vom Flugplatzunternehmer als komplett umgesetzt, wenn folgende Merkmale nachweisbar eingeführt wurden:

1. Sicherheitspolitik des Unternehmens
2. Installation eines Sicherheitsmanagers
3. Zuordnung der Verantwortlichkeiten zu Prozessen
4. Einrichtung von Sicherheitsausschüssen
5. Gefahrenidentifikation und Risikomanagement
6. Berichtswesen zu sicherheitsrelevanten Vorkommnissen
7. Untersuchung sicherheitsrelevanter Vorkommnisse
8. Dokumentation
9. Auditierung
10. Changemanagement (Anpassen der Verfahren bei Änderungen)
11. Organisation von Sicherheitsunterweisungen von Mitarbeitern (eigene und Fremdfirmen)
12. Definition von Sicherheitsleitzielen
13. Fortlaufende Überwachung der Wirksamkeit des SMS
14. Notfallplanung

2.3.2 Strategien und Instrumente des Sicherheitsmanagements

Rasmussen (1991) beschreibt drei verschiedene Kontroll- oder Steuerungsstrategien für die Gewährleistung der Sicherheit, deren Angemessenheit vom Gefährdungspotenzial der Industrie und von der Geschwindigkeit der Technologieentwicklung abhängen:

- Feedforward-Steuerung,
- Feedback-Steuerung und
- Kombination aus Feedforward- und Feedback-Steuerung.

Feedforward-Steuerung kann als die vorausschauende Strategie angesehen werden, mithilfe von Risikoabschätzungen werden Interventionen geplant. Die Feedback-Steuerung bezieht sich auf das Lernen aus Betriebserfahrungen, Interventionen basieren hier auf der Analyse von Ereignissen oder Beinahe-Ereignissen.

In die Praxis umgesetzt könnte die Kombination von Feedforward- und Feedback-Steuerung in einem SMS folgendermaßen aussehen: Für die Bestandteile eines SMS »Gefahrenidentifikation« und »Risikomanagement« können Verfahren eingesetzt werden, die nach Rasmussen der Feedforward-Steuerung zuzuordnen sind. Vor allem für die Kerntechnik wurden aufgrund des hohen Gefährdungspotenzials Methoden entwickelt, um die Risiken des Systems einschätzen zu können sowie

mögliche Unfälle und Schwachstellen vorauszusehen, um durch geeignete Maßnahmen präventiv einschreiten zu können. Die meisten dieser Methoden basieren auf ingenieurwissenschaftlichen Ansätzen und modellieren Systemfunktionalitäten. In der probabilistischen Sicherheitsanalyse (PSA) werden Ansätze zur Analyse der Technologie um Verfahren ergänzt, die den menschlichen Beitrag modellieren, wie die »human reliability analysis« (HRA), um zu einer realistischen Abschätzung für das gesamte Systemverhalten zu kommen (auch ► Kap. 3). Es gibt erste Versuche, die diversen quantitativen Methoden (eine Evaluation der verschiedenen Ansätze findet man bei Kirwan, 1996 u. 1997a–d) um qualitative Aspekte zu ergänzen, mit denen beispielsweise organisationale oder kulturelle Faktoren berücksichtigt werden können (Kirwan, 1998).

Methoden zur Feedback-Steuerung sind v. a. Ereignisanalyseverfahren, die im SMS im Baustein »Berichtswesen« angesiedelt sind. Hierbei geht es um die Analyse von Ereignissen und Beinahe-Ereignissen. Den aktuellen Stand der Sicherheitsforschung stellen Modelle zur Erklärung der Entstehung von Ereignissen dar, die organisatorische und Umweltfaktoren zusätzlich zu menschlichen und technischen Ursachen abbilden. Beispiele sind das »Schweizer-Käse-Modell« von Reason (1997) oder das soziotechnische Ereignisentstehungsmodell (Fahlbruch & Wilpert, 1999). Untersuchungen von Unfällen, wie beispielsweise das Sinken der Fähre »Herald of Free Enterprise« oder der Reaktorunfall in Tschernobyl, zeigten, dass eine hoch komplexe Interaktion unterschiedlichster Faktoren, die auch außerhalb der Betreiberorganisation angesiedelt sein können, an der Entstehung der Unfälle beteiligt waren. Ereignisanalysen dienen der Aufklärung dieser Interaktion, in dem der Ereignishergang und seine Ursachen rekonstruiert werden. Damit stellen sie Ansprüche an die Analytiker, die bei der Analyse über die vorhandene Information hinaus kausale Schlüsse vornehmen müssen – ein Prozess, der nach Fahlbruch & Wilpert (1997) mit komplexem Problemlösen verglichen werden kann.

Ereignisanalysen werden mehr oder weniger systematisch durchgeführt. Oftmals unterliegen Ereignisse mit sicherheitstechnischer Bedeutung einer Meldepflicht gegenüber den zuständigen Behörden. Ziel ist es, meldepflichtige Ereignisse nach einem geordneten Verfahren mit definierten Vorgaben und einer abgestuften Dringlichkeit der Aufsichtsbehörde zur Kenntnis zu bringen. Für meldepflichtige Ereignisse gibt es je nach Industrie unterschiedliche Klassifikationssysteme, in denen beispielsweise in der Kerntechnik Systemstatus, Ablauf des Ereignisses, Ursachen, Auswirkungen, Sofortmaßnahmen, Übertragbarkeit und Vorkehrung gegen Wiederholung erfasst werden. Zumindest für Industrien mit hohem Gefährdungspotenzial existieren ferner eine Reihe unterschiedlicher Ereignisanalyseverfahren. Ereignisse werden hier als multikausale Ereignissequenzen gesehen und meistens wird von einem notwendigen Zusammenspiel direkt wirkender Faktoren oder aktiver Fehler mit indirekt wirkenden Faktoren oder latenten Fehlern ausgegangen. Ersteren kommt eine Auslösefunktion zu, während die zweiten unerkannt im System ereignisfördernd wirken. Latente Fehler oder indirekte Faktoren spiegeln organisationale Schwachstellen oder dysfunktionale Beziehungen zwischen Organisationen wider.

Neu ist die explizite Betrachtung der **Organisationsumwelt** als Einflussfaktor auf die Entstehung von Ereignissen. Kritisch anzumerken ist vor allem, dass die wenigsten Verfahren wissenschaftlich entwickelt wurden, meistens sind die Analysemethoden in der Praxis entstanden. Dementsprechend sind auch kaum Untersuchungen zu ihren Gütekriterien zu finden (Fahlbruch, 2000). Typische Verfahren für die Kerntechnik sind ASSET (Assessment of Safety Significant Event Teams – IAEA, 1991), HPES (Human Performance Enhancement System – Bishop & LaRhette, 1988), MORT (Management Oversight and Risk Tree – Johnson, 1980) und SOL (Sicherheit durch organisationales Lernen – Wilpert, Becker, Maimer, Miller, Fahlbruch, Baggen, Gans, Leiber & Szameitat, 1997; Fahlbruch & Schöbel, 2011). In der chemischen Industrie wird ebenfalls MORT angewandt, aus der Luftfahrt kann stellvertretend HERA-JANUS (Human Error in Air Traffic Management Technique – Isaac, Shorrock, Kennedy, Kirwan, Andersen & Bove, 2003) als von Eurocontrol entwickeltes Verfahren genannt werden. Im Folgenden soll als ein Beispiel das Verfahren SOL beschrieben werden, das an der TU Berlin entwickelt wurde und inzwischen das Standardver-

fahren für die vertiefte Ereignisanalyse in der deutschen Kerntechnik ist.

Beispiel

SOL – Sicherheit durch organisationales Lernen

SOL (Fahlbruch Schöbel, 2011) wird in zwei voneinander getrennten und aufeinander aufbauenden Schritten durchgeführt:

- Beschreibung der Ereignissituation und
- Identifikation beitragender Faktoren.

Erst nachdem die Situation ausreichend beschrieben wurde, soll mit dem zweiten Schritt begonnen werden. Diese klare Trennung zwischen Informationssammlung und Interpretation der Information wurde konzipiert, um eine mögliche Einschränkung durch vorschnelle Hypothesen gering zu halten. Zur Sammlung von Informationen werden dem Analytiker eine Reihe von Fragen als Anregung zur Verfügung gestellt, mit deren Hilfe geklärt werden kann, was passiert ist, aber nicht, warum es passiert ist. Die zusammengetragene Information wird in standardisierter Form auf Ereignisbausteinkarten übertragen, die Informationen über Akteure, hier Menschen und technische Komponenten, und Aktionen, hier menschliche Handlungen oder maschinelle Abläufe, sowie über Ort, Zeit und Bemerkungen enthalten. Für alle beteiligten Menschen und Maschinen bzw. technischen Komponenten werden auf diese Weise Ereignisbausteine gebildet. Pro Akteur und Aktion wird eine separate Ereignisbausteinkarte angelegt. Die Ereignisbausteine repräsentieren die einzelnen Ereignissequenzen. Sie werden dann nach Akteuren und nach der Zeit in einer Art Matrix geordnet wieder zu einem gesamten Bild zusammengesetzt.

Mit der Identifikation beitragender Faktoren wird erst begonnen, wenn eine vollständige Situationsbeschreibung erstellt wurde. Um monokausales Denken, eine abgebrochene Suche und eine Einschränkung durch vorschnelle Hypothesen sowie durch Übertragung aus Referenzsituationen zu verhindern, wird für jede Ereignisbausteinkarte einzeln nach beitragenden Faktoren gesucht. So wird für jede Ereignissequenz eine separate Analyse durchgeführt, deren Ergebnisse ebenfalls auf Karten festgehalten werden und mit denen die Ereignisdarstellung ergänzt wird. Im Laufe der Analyse entsteht so eine immer komplexer werdende Ereignisrekonstruktion. Als Hilfe für die Analytiker gibt es mögliche direkt und indirekt beitragende Faktoren wie Arbeitsbedingungen, Arbeitsplanung, Abweichung von Regeln, Qualifikation, Gruppeneinflüsse, Organisation und Management und Training, die in einer Identifikationshilfe zusammengefasst sind. Die Vorgabe dieser möglichen beitragenden Faktoren dient zum einen der Sicherung des Untersuchungsumfangs, zum anderen soll sie den Analytikern helfen, mögliche Hypothesen zu generieren.

Es gibt ferner Verweise von den direkt beitragenden zu den indirekt beitragenden Faktoren. Diese Verweise sind in der Analyse zu überprüfen, wenn ein Faktor identifiziert wurde. Die Identifikationshilfe enthält für jeden direkt und indirekt kontribuierenden Faktor eine allgemein gehaltene Frage, wie beispielsweise »Könnte es einen Einfluss der Arbeitsbedingungen auf das Handeln gegeben haben?«, um die Bildung von Analogien anzuregen und um den Eindruck der Vollständigkeit zu vermeiden, der durch zu detaillierte Unterkategorien entstehen kann. Da SOL aber in erster Linie für das Personal in Kernkraftwerken und nicht für Human-Factors-Spezialisten konzipiert wurde, wird jede allgemeingehaltene Frage anhand von Beispielen erläutert. Die Beispiele sind nicht erschöpfend, sondern sollen vielmehr die mögliche Spannbreite der Wirkung des Faktors verdeutlichen.

Das Lernen aus Betriebserfahrung beschreibt den erfolgreichen Erfahrungsrückfluss. Nach Koornneef (2000) sind Ereignisse bzw. Beinahe-Ereignisse einerseits Lernmaterial, andererseits Auslöser für das Lernen in einer Organisation. Voraussetzung für erfolgreiches Lernen ist nach Argyris und Schön (1996), dass über ein einfaches Fehlerkorrigieren (Single-loop-Lernen) hinausgegangen wird. Beim Double-loop-Lernen werden tiefere und gemeinsame Ursachen und Schwachstellen gesucht, d. h. es wird mit einer systematischen Analyse vorgegangen. Beim Deutero-Lernen wird im Sinne eines Meta-Lernens über die Lernprozesse reflektiert. Carroll, Rudolph & Hatakenaka (2002) sehen jedoch durchaus Schwierigkeiten, besonders in hochregulierten Industrien, in denen die formale Regelbefolgung höchste Priorität besitzt. Aus Sicht der Autoren ist es für das Lernen aus Ereignissen

notwendig, dass ein nichtlineares, dynamisches, multikausales Systemverständnis existiert, und dass problemorientiertes Feedback sowie ein offener Austausch stattfinden. Schöbel & Manzey (2011) weisen zudem auf die Schwierigkeit hin, organisationale Faktoren im Rahmen von Ereignisanalysen zu identifizieren. Oftmals werden dabei motivationale Aspekte sicherheitsgerichteten Handelns unterschätzt, was vornehmlich auf die Anwendung technikorientierter Theorien des Organisierens (z. B. Vergleiche zwischen Soll- und Ist-Abläufen) im Gegensatz zur Anwendung verhaltensorientierter Theorien (z. B. Identifikation der Motive, die das sicherheitsrelevantes Verhalten anleiten) zurückzuführen ist. Dementsprechend sollten in einem SMS einerseits Methoden zur systematischen Analyse organisationaler Faktoren in Ereignissen, andererseits aber auch Feedbackschleifen für »lessons learned« implementiert sein.

2.4 Der tägliche Umgang mit Sicherheit: Konzept der Sicherheitskultur

Der Begriff »Sicherheitskultur« (auch ► Kap. 9.6.1) wurde erstmals von einer Beratergruppe der Internationalen Atomenergiebehörde (IAEA) der breiten Öffentlichkeit vorgestellt – im Zuge der Analyse des Reaktorunglücks in Tschernobyl (INSAG-1, 1986; INSAG-4, 1991). Diese Analyse führte organisationale Schwachstellen wie auch die Vielzahl an Regelverletzungen des operativen Personals auf Defizite der zum Zeitpunkt der Katastrophe vorherrschenden Sicherheitskultur zurück. Mittlerweile genießt das Konzept nicht nur in der kerntechnischen Industrie weltweite Aufmerksamkeit. Auch in anderen Ultra-safe-Branchen, wie z. B. der Raumfahrt (Leveson, Cutcher-Gershenfeld, Barrett, Brown, Carroll, Dulac, Fraile & Marais, 2004) oder der Luftfahrt (Helmreich & Merrit, 1998), wurde die Notwendigkeit erkannt, den organisationskulturellen Einfluss auf das individuelle Sicherheitshandeln der Organisationsmitglieder zu berücksichtigen. Branchenübergreifend gilt das Hauptinteresse der Entwicklung von Maßnahmen zur Optimierung von Sicherheitskultur.

In der 1991 vorgelegten Definition der IAEA wird Sicherheitskultur verstanden als

> » […] that assembly of characteristics and attitudes in organization and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance. (INSAG-4, 1991) «

Darauf aufbauend werden auf drei Ebenen Anforderungen definiert, deren Erfüllung eine »funktionierende Sicherheitskultur« ausmachen soll:

Auf der **unternehmenspolitischen Ebene** gilt es, sowohl von der Organisation selbst wie auch von politischen Aufsichtsorganen die Rahmenbedingungen zu schaffen, unter denen die Organisationsmitglieder ihre Arbeit sicherheitsgerichtet verrichten können (z. B. sicherheitspolitische Programme, ausreichende finanzielle und personelle Ressourcen, Sicherheitsmanagementsysteme).

Auf der **Ebene des Managements** werden v. a. thematisiert: die Festlegung innerbetrieblicher Verantwortlichkeiten, die regelmäßige Durchführung von Trainings- und Qualifizierungsmaßnahmen, sicherheitsförderliche Belohnungs- und Sanktionssysteme sowie die Definition und Überprüfung von Sicherheitspraktiken.

Auf der **individuellen Ebene** wird von allen Mitarbeitenden unabhängig von ihrer Position innerhalb der Organisation eine hinterfragende Grundhaltung, ein sorgfältiges und vorsichtiges Handeln und eine offene Kommunikation über sicherheitsrelevante Themen gefordert.

Die IAEA versteht Sicherheitskultur als ein ganzheitliches Phänomen, das alle Mitglieder einer Organisation (und die mit ihnen in Verbindung stehenden »interorganisationalen« Akteure) einbezieht und dessen Verhaltenswirksamkeit sich sowohl auf beobachtbaren (»characteristics«) wie auch psychologischen (»attitudes«) Merkmalen abbildet. Neuere Publikationen der IAEA erweitern diese Auffassung dahingehend, dass

- Konzepte wie »lernende Organisation« sowie konservative Entscheidungsfindung, der Aufbau einer Berichtskultur (INSAG-15, 2002) wie auch die individuellen (Sicherheits-)Werte der Organisationsmitglieder (IAEA, 2005) integriert werden und

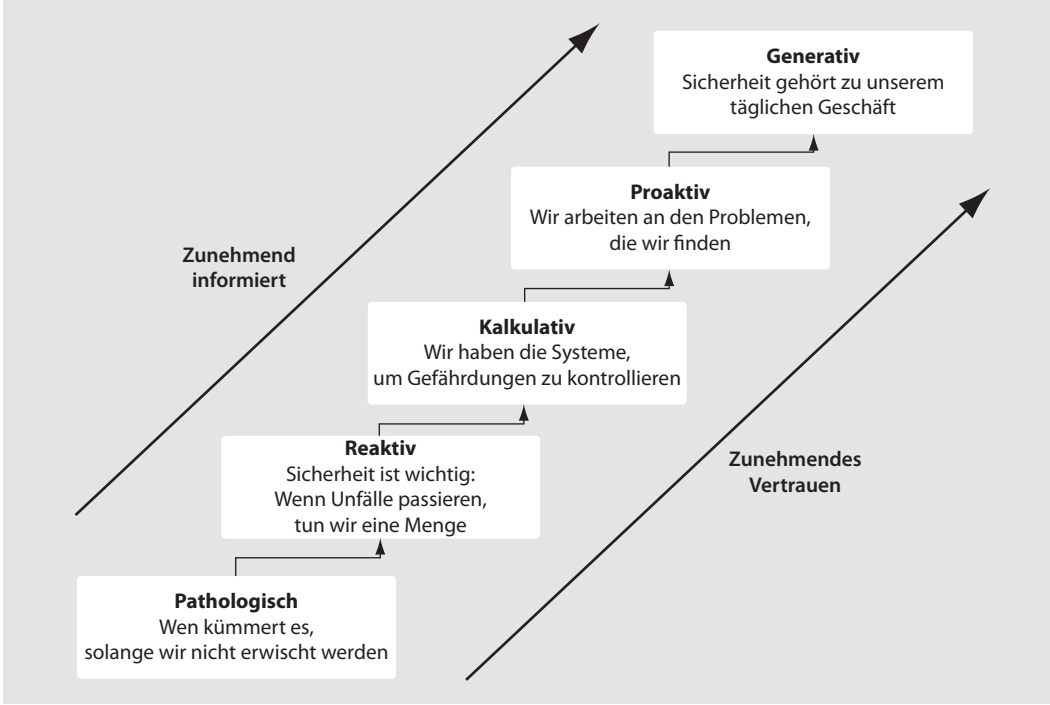

Abb. 2.1 Reifegradmodell der Sicherheitskultur. (Übersetzt nach Hudson, 2007) Reprinted from Safety Science, 45 (6), Hudson, P, Implementing a safety culture in a mojor multi-national, 697–722, Copyright (2007), with permission from Elsevier

- unterschiedliche Entwicklungsstufen von Sicherheitskultur definiert werden (IAEA, 1998).

Letzteres kennzeichnet auch die sog. Reifegradmodelle der Sicherheitskultur (z. B. Fleming & Lardner, 1999; Parker, Lawrie & Hudson, 2006; Hudson, 2007), die die jeweilige Reife einer Sicherheitskultur anhand ausgewählter Indikatoren bestimmen (Abb. 2.1).

Unklar bleibt jedoch, wie es zu unterschiedlichen Reifegraden einer Sicherheitskultur kommt bzw. wie beispielsweise das »bedrohliche« Verhalten der Mitglieder einer pathologischen Sicherheitskultur erklärt werden kann, wenn man davon ausgeht, dass diese sich nicht bewusst Gefahren und Risiken aussetzen. Basierend auf den Arbeiten zur Organisationskultur von Schein (1990) wird zunehmend ein Mehrebenenkonzept von Sicherheitskultur favorisiert (Guldenmund, 2000; Hale, 2000; Wagner, Schöbel, Klostermann & Manzey, 2010). Dieses fokussiert das Wechselspiel zwischen »nichtbeobachtbaren« und »beobachtbaren« Merkmalen einer Sicherheitskultur.

Schein betrachtet die Kultur einer Organisation auf drei Ebenen, wobei Ausprägungen auf den beiden höheren Ebenen (Ebene der Artefakte bzw. des beobachtbaren Verhaltens und Ebene der bekundeten Werte) maßgeblich durch die tiefste Ebene – Ebene der Grundannahmen – beeinflusst werden. Der verhaltensbestimmende Kern einer (Organisations-)Kultur wird als ein Muster gemeinsamer Grundannahmen definiert, das eine Gruppe bzw. eine Organisation im Spannungsfeld von externer Anpassung und interner Integration erlernt hat, das sich bewährt hat, somit als bindend gilt und daher an neue Organisationsmitglieder als rationale und emotionale Leitlinie eigenen Handelns weitergegeben wird. Die Grundannahmen einer Organisationskultur sind den Organisationsmitgliedern in der Regel nicht bewusst; sie leiten ihr Handeln »wie selbstverständlich«. Auf den unmittelbaren Zusammenhang zwischen den in sozialen Gruppierungen

entstehenden Grundannahmen und sicherheitsgerichtetem Verhalten verweist Hale (2000, S. 7):

» The attitudes, beliefs, and perceptions shared by natural groups as defining norms and values, which determine how they act and react in relation to risks and risk control system. «

Auch Pidgeon (1991) in Anlehnung an Turner, Pidgeon, Blockley & Toft (1989) fasst Sicherheitskultur als sozial geteiltes Phänomen auf, d. h. als

» […] set of beliefs, norms, attitudes roles, and social and technical practices that are concerned with minimising the exposure of employees, managers, customers and members of the public to conditions considered dangerous and injurious. (S. 134) «

Das Konzept Sicherheitskultur beinhaltet sowohl beobachtbare Indikatoren wie auch psychologische Aspekte. Die Schwerpunkte der verschiedenen Modelle liegen entweder auf der Entwicklung beobachtbarer Indikatoren für Sicherheitskultur oder auf der Identifikation im Gruppenkontext entstehender verhaltenswirksamer und sozial geteilter Grundannahmen einer Sicherheitskultur. Eine gezielte Optimierung von Sicherheitskultur sollte beide Aspekte integrieren und ist in hohem Maße davon abhängig, welches Verständnis von Sicherheitskultur zugrunde gelegt wird (Baram & Schöbel, 2007).

So bedarf es psychologischer Modelle kultureller Beeinflussung, um beispielsweise Auswirkungen von Veränderungsprozessen vorhersagen und steuern zu können. Gleichzeitig benötigt man eine Vorstellung davon, was ein »wünschenswertes« sicherheitsgerichtetes Verhalten ist und welche organisationalen Rahmenbedingungen vorliegen müssten, um ein solches Verhalten zu unterstützen. Beide Aspekte einer Sicherheitskultur lassen sich allerdings nur schwer verallgemeinern; sie sollten an die spezifischen Bedingungen einer Sicherheitskultur angepasst werden. So ist durchaus vorstellbar, dass eine »starke« Teamkultur in der einen Organisation negative Effekte für die Sicherheit produziert (z. B. Verschweigen von Fehlhandlungen anderer Teammitglieder), in einer anderen Organisation jedoch positive Einflüsse hat (Teammitglieder unterstützen sich gegenseitig bei der Entdeckung von Missständen).

Des Weiteren muss bei jeglicher »sicherheitskulturellen« Intervention entschieden werden, ob auf die Veränderung des Verhaltens (z. B. durch Behavioral-Safety-Programme; s. Lardner, 2004) oder auf Veränderung von Einstellungen und Werten der Organisationsmitglieder (z. B. durch Informationsworkshops) abgezielt werden sollte, und inwieweit nichtprimäre sicherheitsrelevante Entscheidungen und Prozesse (wie z. B. die Verteilung von Ressourcen, organisationale Restrukturierungen) einbezogen werden, d. h. vordergründig eine Veränderung der Organisationskultur anzustreben ist. Daraus folgt, dass der Diagnose von Sicherheitskultur eine entscheidende Rolle zukommt, sobald sich eine Organisation mit ihrer Sicherheitskultur auseinandersetzt bzw. ihre gezielte Optimierung anstrebt.

2.4.1 Diagnose von Sicherheitskultur

Im Gegensatz zur Feedback-Steuerung von Sicherheit (beispielsweise durch Ereignisanalysen, ► Kap. 2.3.2) stellt die Diagnose der Sicherheitskultur einen Feedforward-Steuerungsmechanismus dar. Seit der Einführung des Konzeptes sind eine Vielzahl an Methoden entwickelt worden, mittels derer Optimierungspotenziale und somit Ansatzpunkte zur positiven Beeinflussung der Sicherheitskultur aufgezeigt werden. Im Bereich der kerntechnischen Industrie überwiegen Ansätze der Selbsteinschätzung der Sicherheitskultur (IAEA, 1995; VGB-Powertec, 2004; IAEA, 2005). Diese greifen zumeist auf drei unterschiedliche Verfahren zurück:

- Betriebsbegehungen,
- Dokumentenanalysen und
- Interviews.

Anhand von Betriebsbegehungen und der Analyse von Dokumenten sollen beobachtbare Merkmale einer Sicherheitskultur eingeschätzt werden. Dazu liegen Checklisten vor, die den Bewertungspro-

zess anleiten (Was soll beobachtet werden? Welche Dokumente sollen analysiert werden?) und gleichzeitig Bewertungskriterien formulieren (z. B. Housekeeping in der Anlage, Qualität von Arbeitsprozeduren und -regeln). Mit der Durchführung von Interviews werden die »tieferen« Ebenen einer Sicherheitskultur, d. h. Einstellungen und Werte der Mitarbeitenden zu Sicherheit und Zuverlässigkeit analysiert, wobei Fragenkataloge die Interviews anleiten. Zudem werden die Ergebnisse der Dokumentenanalyse und Betriebsbegehung in die Befragung integriert.

Einen weiteren Zugang zu den nichtbeobachtbaren Merkmalen einer Sicherheitskultur verspricht man sich auch durch den Einsatz von **Fragebögen.** Es wird zwar empfohlen, dass die Analyse der tieferen Ebenen einer Sicherheitskultur (Ebene der »unbewussten« Grundannahmen) dem Einsatz qualitativer Methoden vorbehalten bleiben sollte (Schein, 1990; Denison, 1996), jedoch bieten Fragebögen die Möglichkeit, Aussagen über das Sicherheitsklima einer Organisation und damit »Schnappschüsse« einer Kultur (Flin, Mearns, O'Connor & Bryden, 2000) abzuleiten. Unter Sicherheitsklima werden demnach die »offenkundigen« Merkmale einer Sicherheitskultur verstanden. Zohar (1980) beschreibt diese als »a summary of molar perceptions that employees share about their work environment« (S. 96).

Allerdings ist die Interpretation von Daten aus Klimafragebögen und damit das Schlussfolgern auf die Sicherheitskultur einer Organisation auch mit Schwierigkeiten behaftet. So gehen mittlerweile viele Konzeptionen der Sicherheitskultur davon aus, dass sich innerhalb einer Organisation unterschiedliche Subkulturen entwickeln können, deren Ausformung vom spezifischen Kontext der Arbeitstätigkeit einzelner Gruppen abhängt. Dies bedeutet für die Auswertung von Sicherheitsklimafragebögen, dass entschieden werden muss, auf welcher Ebene die erhobenen Daten sinnvoll aggregiert werden können (auf der organisationalen Ebene, der Gruppenebene, der Ebene der funktionalen Zugehörigkeit etc.), und ob hierfür die Anzahl der erhobenen Datensätze ausreicht, ohne gegen die Voraussetzung statistischer Verfahren zu verstoßen.

Weiter bleibt auch festzuhalten, dass in bisherigen Studien kaum Aussagen zur Validität der eingesetzten Fragebögen getroffen werden, d. h. inwieweit ein Zusammenhang zwischen Ausprägungen des Sicherheitsklimas bzw. der Sicherheitskultur und der tatsächlichen Sicherheit organisationalen Handelns vorliegt. Neben dem Mangel an Erklärungsmodellen bisheriger Sicherheitsklimakonzeptionen (Guldenmund, 2007; Flin, 2007) mag dies auch an der Schwierigkeit liegen, geeignete (Sicherheits-)Leistungsindikatoren zu identifizieren, da üblicherweise eingesetzte Indikatoren (Anzahl Beinahe-Unfälle, Unfallstatistiken, Verfügbarkeitsdaten, Selbstberichte) nur bedingt Rückschlüsse zulassen.

2.4.2 Positive Beeinflussung von Sicherheitskultur

Um die Sicherheit organisationalen Handelns zu gewährleisten, ist es für Organisationen unerlässlich, Informationen über potenzielle bzw. reale Gefährdungspotenziale zu generieren, zu sammeln, zu analysieren und zu verbreiten. Ultra-safe-Organisationen stehen allerdings vor der Herausforderung, dass diese Informationen im Vergleich zu anderen Industrien (z. B. in der Bauindustrie) nur schwer zugänglich sind. Ereignisse treten selten auf. Sicherheit ist »unsichtbar« in dem Sinne, dass mit dem Erreichen von Produktionszielen gleichzeitig die Sicherheit organisationalen Handelns suggeriert wird und demnach die wahrgenommene Notwendigkeit sinkt, weitere »Sicherheits«-Informationen zu suchen (Weick, 1987). An diesem Punkt sollte eine positive Beeinflussung der Sicherheitskultur ansetzen.

Reason (1998) greift die Notwendigkeit der aktiven Suche und Verbreitung sicherheitsrelevanter Informationen in seinem Konzept der informierten Kultur (»informed culture«, auch ► Kap. 9) auf. Hierunter versteht er eine Kultur, in der die Organisationsmitglieder Gefährdungspotenziale bewusst wahrnehmen, verstehen und respektieren. Sicherheitsmanagementsysteme stellen die notwendigen formalen Strukturen zur Verfügung, gleichzeitig bedarf es einer Organisationskultur, die zur Nut-

zung dieser Strukturen motiviert. Reason nennt dafür zwei Voraussetzungen:

Zunächst bedarf es einer **»reporting culture«:** Die Organisationsmitglieder sollten bereit sein, eigene Fehlhandlungen sowie Beobachtungen zu abweichendem Systemverhalten zu kommunizieren. Dies erfordert ein Meldesystem mit förderlichen Merkmalen wie z. B. Vertraulichkeit, einfacher Zugang, schnelle Rückmeldung (van der Schaaf & Kanse, 2004). Primär sollte jedoch das Vertrauen der Organisationsmitglieder in die Ziele und die zu erwartenden Gewinne eines (»freiwilligen«) Meldesystems gestärkt werden (Schöbel, 2009). Voraussetzung dafür ist eine sog. gerechte Kultur **(»just culture«):** In der Organisation muss Klarheit darüber herrschen, wie mit Schuldzuweisungen und Bestrafungen umgegangen wird. Das Spektrum, wie Organisationen heutzutage solche Aspekte handhaben, reicht von der Null-Toleranz gegenüber Fehlern bis hin zur **»no-blame culture«.** Ziel einer just culture sollte jedoch sein, dass die Organisationsmitglieder genau wissen, wo die Linie gezogen wird zwischen inakzeptablem Verhalten, das einer Disziplinierung bedarf, und sonstigem Fehlverhalten, dessen Bestrafung weder angemessen noch hilfreich für eine Entdeckung von sicherheitskritischen Systemdysfunktionalitäten ist.

Ein potenzielles Kriterium dafür, wie bei Ereignissen mit menschlicher Beteiligung vorgegangen werden soll, bietet der Substitutionstest. In einer möglichen Variante dieses Tests werden die Kollegen eines in ein Ereignis verwickelten Mitarbeiters gefragt, ob sie unter den gegebenen Umständen ähnlich gehandelt hätten. Wird die Frage bejaht, sollte man davon ausgehen, dass eine Bestrafung des Mitarbeiters keinen Sinn ergibt und eher mit negativen Effekten hinsichtlich der Etablierung einer informierten Kultur verbunden wäre – in Form von wahrgenommener Ungerechtigkeit und daraus resultierendem Misstrauen gegenüber dem Management. Im Hinblick auf die Umsetzung einer just culture sollte jedoch auch darauf hingewiesen werden, dass jegliche Interventionen die Privatsphäre und die Grundrechte von Arbeitnehmern und Arbeitnehmerinnen zu achten haben.

Die positive Beeinflussung der Sicherheitskultur in Richtung einer informierten Kultur sollte sicherstellen, dass die hier bislang aufgezählten Aspekte nicht nur auf der Ebene einzelner Subkulturen umgesetzt werden, sondern zu Merkmalen der »dominanten« Organisationskultur werden. Dies bedeutet, dass das Top-Management sich den Zielen und der Vision einer informierten Kultur verpflichtet fühlt und somit bereit ist, bestehende Grundannahmen zu hinterfragen und aufzugeben. Ein kritischer Aspekt dabei ist die Bereitschaft, auch das sicherheitsrelevante Verhalten von Mitarbeitern auf höheren Führungsebenen zu thematisieren bzw. zu verändern (► Kap. 10).

2.5 Zusammenfassung und Ausblick

Dieses Kapitel beschreibt die Gewährleistung von Sicherheit im organisationalen Kontext. Über eine ergebnisorientierte Sichtweise hinaus wird Sicherheit als Systemmerkmal betrachtet, das sich aus Interaktionsprozessen intra- und extraorganisationaler Einzelfaktoren kontinuierlich generiert. Die strategische und sicherheitsgerichtete Steuerung der Vielzahl organisationaler Prozesse wird durch Sicherheitsmanagementsysteme vollzogen. Diese ermöglichen einer Organisation sowohl die Feedforward- (z. B. durch probabilistische Sicherheitsanalysen) wie auch Feedback-Steuerung (z. B. durch Ereignisanalysen) von Gefährdungspotenzialen. Neben diesen institutionalisierten Instrumenten sind die Bedeutung und das Ausmaß eines organisationskulturellen Einflusses auf das Sicherheitshandeln der Organisationsmitglieder unumstritten. Eine Sicherheitskultur wird als ganzheitliches Phänomen beschrieben, dessen Verhaltenswirksamkeit sich sowohl auf beobachtbaren Indikatoren wie auch psychologischen Merkmalen abbildet. Während Sicherheitsmanagementsysteme die »beobachtbaren« Strukturen zur Verfügung stellen, bedarf es gleichzeitig einer Sicherheitskultur, die zur Nutzung dieser Strukturen motiviert.

Eine Weiterentwicklung dieser systemischen Sichtweise auf die Sicherheit stellt der Ansatz zur Resilienzforschung (Hale & Heijer, 2006; Hollnagel, Woods & Leveson, 2006; auch ► Kap. 3) dar. Dem Resilienzansatz liegt das Drift-to-danger-Modell von Rasmussen (1997) zugrunde, das davon ausgeht, dass sich das Verhalten der Mitarbeitenden in

Organisationen mit hohem Gefährdungspotenzial innerhalb definierter Grenzen (»safety margins«) bewegt. Entscheidungen und Handlungen der Organisationsmitglieder werden grundsätzlich durch das Streben nach maximalem Produktionsoutput bei minimalem individuellen Aufwand geprägt. Resilienz ist die Fähigkeit von Organisationen und ihrer Mitglieder, Übertretungen dieser Grenzen (z. B. durch Abweichungen von Sicherheitsregeln) und die daraus folgenden Konsequenzen frühzeitig zu antizipieren und deren Einfluss auf die Gesamtleistung eines Systems abzuschätzen.

Schwerpunkte aktueller Entwicklungen sind Methoden zur Erfassung und Beobachtung von Resilienz, entsprechende Unterstützungssysteme bezüglich sicherheitsrelevanter Entscheidungsprozesse, Visualisierungstechniken zur Antizipation möglicher Auswirkungen getroffener Entscheidungen und damit verbundener Veränderungen im System.

Resiliente Organisationen schenken »unerwarteten« bzw. nicht vorab definierten Systemzuständen erhöhte Aufmerksamkeit und entwickeln angemessene Abwehrstrategien (Hollnagel, Woods & Leveson, 2006). Resilienz erinnert somit stark an die Konzeption der Achtsamkeit, bezieht sich darüber hinaus aber auch auf die Fähigkeit, nach aufgetretenen Störungen einen reibungslosen Betrieb zu garantieren, in dem Ausgleichsmechanismen vorhanden sind und auch angewendet werden. Demnach müssen Organisationen heutzutage Strategien entwickeln, die sowohl auf die Beherrschung »vorhersehbarer« Störfälle als auch auf den Umgang mit und die Bewältigung von unerwarteten Situationen abzielen.

Literatur

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Safety Science, 37,* 109–126.

Argyris, C. & Schön, D. (1996). *Organizational learning II: Theory, method, and practice.* Reading MA: Addison-Wesley.

Baram, M. & Schöbel, M. (2007). Safety culture and behavioral change at the workplace (Editorial). *Safety Science, 45 (6),* 631–636.

Bishop, J. & LaRhette, R. (1988). Managing human performance – INPO's human performance evaluation. System. *Human-Error-Avoidance-Techniques Conferences Proceedings.* Warrendale, Pennsylvania: Society of Automotive Engineers, Inc. (SAE), Publications No. P-204, 79–85.

Carroll, J. S., Rudolph, J. W. & Hatakenaka, S. (2002). *Organizational learning from experience in high-hazard industries: Problem investigation as off-line reflective practice.* MIT Sloan School of Management: Working Paper 4359–02.

Denison, D. R. (1996). What is the difference between organizational culture and organizational climate? A native's point of view on a decade of paradigm wars. *Academy of Management Review*, *21*, 619–654.

DIN 40041. (1990-12). *Zuverlässigkeit; Begriffe*. Berlin: Beuth-Verlag.

EFQM (2003). *Die Grundkonzepte der Excellence*. [Online] http://www.luzern.phz.ch/fileadmin/media/luzern.phz.ch/qualitaetsmanagement/plu_efqm_grundkonzepte_2003.pdf [23.06.2011].

Fahlbruch, B. & Schöbel, M. (2011). SOL – Safety through organizational learning: A method for event analysis, *Safety Science*, 49 (1), 27-31.

Fahlbruch, B. (2000). *Vom Unfall zu den Ursachen – Empirische Bewertung von Analyseverfahren*. Berlin: Mensch & Buch.

Fahlbruch, B. & Wilpert, B. (1997). Event analysis as problem solving process. In A. R. Hale, B. Wilpert & M. Freitag (Eds.), *After the event: from accident to organisational learning* (pp. 113–130). Oxford: Elsevier.

Fahlbruch, B. & Wilpert, B. (1999). System safety – an emerging field for I/O psychologie. In C. L. Cooper & I. T. Robertson (Hrsg.), *International Review of Industrial and Organizational Psychology* (Bd. 14, S. 55–93). Chichester: Wiley.

Fleming, M. & Lardner, R. (1999). *The development of a draft safety culture maturity model*. Suffolk: HSE Books.

Flin, R. (2007). Measuring safety culture in healthcare. A case for accurate diagnosis. *Safety Science, 45 (6),* 653–667.

Flin, R., Mearns, K., O'Connor, P. & Bryden, R. (2000). Measuring safety climate: Identifying the common features. *Safety Science*, *34 (1–3),* 177–192.

Gherardi, S., Nicolini, D. & Odella, F. (1998). What do you mean by safety? Conflicting perspectives on accident causation and safety management in a construction firm. *Journal of Contingencies and Crisis Management*, *6 (4),* 202–213.

Guldenmund, F. W. (2000). The nature of safety culture: A review of theory and research. *Safety Science*, *34 (1–3),* 215–257.

Guldenmund, F. (2007). The use of questionnaires in safety culture research: An evaluation. *Safety Science, 45 (6),* 723–740.

Hale, A. R. (2000). Editorial: Culture's confusion. *Safety Science, 34,* 1–14.

Hale, A. & Heijer, T. (2006). Defining resilience. In E. Hollnagel, D. D. Woods & N. Leveson (Eds.), *Resilience engineering: concepts and precepts* (pp. 35–41). Burlington, VT: Ashgate.

Helmreich, R. L. & Merritt A. C. (1998). *Culture at work: National, organisational and professional influences*. Aldershot, UK: Ashgate.

Hollnagel, E., Woods, D. D. & Leveson, N. (2006). *Resilience engineering: concepts and precepts*. Burlington, VT: Ashgate.

Hopkins, A. (1999). The limits of normal accident theory. *Safety Science, 32 (2–3),* 93–102.

Hudson, P. (2007). Implementing a safety culture in a major multi-national. *Safety Science, 45 (6),* 697–722.

IAEA (1991). *ASSET Guidelines revised 1991 edition. Reference material prepared by the IAEA for assessment of safety significant event teams* (IAEA-TECDOC-632). Vienna: International Atomic Energy Agency.

IAEA (1995). *ASCOT-Guidelines. Guidelines for reviews by the assessment of safety culture in organizations teams*. Vienna: International Atomic Energy Agency.

IAEA (1998). *Developing safety culture in nuclear activities: Practical suggestions to assist progress*. IAEA Safety Report Series Nr. 11. Vienna: International Atomic Energy Agency.

IAEA (2005). *SCART Guidelines. Guidelines for safety culture assessment review teams*. Unpublished report. Vienna: International Atomic Energy Agency.

ICAO (2004). ICAO-Annex 14, Volume I, »Aerodrome design and operations«. 4th Edition, July 2004.

INSAG-1 (1986). Summary *Report on the Post-Accident Review Meeting on the Chernobyl accident*. Vienna: International Atomic Energy Agency.

INSAG-4 (International Nuclear Safety Advisory Group) (1991). *Safety Culture.* Vienna: International Atomic Energy Agency.

INSAG-15 (International Nuclear Safety Advisory Group) (2002). *Key practical issues in strengthening safety culture*. Vienna: International Atomic Energy Agency.

ISO/IEC Guide 51 (1999). *Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen*. Berlin: Beuth Verlag.

Isaac, A., Shorrock, S. T., Kennedy, R., Kirwan, B., Andersen, H. & Bove, T. (2003). *The human error in ATM technique (HERA-JANUS)* (HRS/HSP-002-REP-03). Brussels: Eurocontrol.

Johnson, W. (1980). *MORT Safety Assurance Systems*. New York: Marcel Dekker.

Kirwan, B. (1996). The validation of three human reliability quantification techniques – THERP, HEART and JHEDI: Part 1 – technique descriptions and validation issues. *Applied Ergonomics*, *27 (6),* 359–373.

Kirwan, B. (1997a). The development of a nuclear chemical plant human reliability management approach: HRMS and JHEDI. *Relibility Engineering and System Safety*, *56,* 107–133.

Kirwan, B. (1997b). The validation of three human reliability quantification techniques – THERP, HEART and JHEDI: Part III – Practical aspects of the usage of the techniques. *Applied Ergonomics*, *28 (1),* 27–39.

Kirwan, B. (1997c). Validation of human reliability assessment techniques: Part 1 – Validation issues. *Safety Science*, *27 (1),* 25–41.

Kirwan, B. (1997d). Validation of human reliability assessment techniques: Part 2 – Validation results. *Safety Science*, *27 (1),* 43–75.

Kirwan, B. (1998). Safety management assessment and task analysis – a missing link. In A. Hale & M. Baram (Eds.), *Safety management: The challenge of change* (pp. 67–92). Amsterdam: Elsevier.

Koornneef, F. (2000). *Organised learning from small-scale incidents*. Delft: Delft University Press.

La Porte, T. R. (1996). High reliability organizations: Unlikely, demanding and at risk. *Journal of Contingencies and Crisis Management, 4 (2),* 60–71.

La Porte, T. R. & Consolini, P. M. (1991). Working in practice but not in theory: theoretical challenges of high-reliability organizations. *Journal of Public Administration Research and Theory, 1,* 19–47.

Lardner, R. (2004). *Mismatches between safety culture Improvement and behaviour-based safety*. Paper presented at the 23th NetWork-Meeting on Safety Culture and Behavioral Change, Blankensee, Germany.

Leveson, N. (2011). Applying systems thinking to analyze and learn from events. *Safety Science*, 49 (1), 55-64.

Leveson, N., Cutcher-Gershenfeld, J., Barrett, B., Brown, A., Carroll, J., Dulac, N., Fraile, L. & Marais, K. (2004). *Effectively addressing NASA's organizational and safety culture: Insights from system safety and engineering systems.* Paper presented at MIT ESD Symposium, March 2004.

OSHA (2002). Arbeitsunfälle verhindern. *Magazin der Europäischen Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz, 4,* 1–33.

Parker, D., Lawrie, M. & Hudson, P. (2006). A framework of understanding the development of organisational safety culture. *Safety Science, 44 (6),* 551–562.

Perrow, C. (1986). Lernen wir etwas aus den jüngsten Katastrophen? *Soziale Welt, 37*, 390–401.

Perrow, C. (1987). *Normale Katastrophen. Die unvermeidbaren Risiken der Großtechnik*. Frankfurt u. a.: Campus-Verlag.

Pidgeon, N. F. (1991). Safety culture and risk management in organizations. *Journal of Cross-Cultural Psychology,* Vol. 22, pp. 129–140.

Rasmussen, J. (1991). *Safety control: Some basic distinctions and research issues in high hazard low risk operation.* Paper preseted at the NeTWork workshop on Risk Management, Bad Homburg, May 1991.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science, 27 (2–3),* 183–213.

Reason, J. (1990). *Human error.* Cambridge: Cambridge University Press.

Reason, J. (1997). *Managing the risks of organizational accidents.* Aldershot: Ashgate.

Reason, J. T. (1998). Achieving a safe culture: theory and practice. *Work and Stress, 12 (3),* 293–306.

Rochlin, G. I. (1993). Defining »High reliability« organizations in practice: A taxonomic prologue. In K. H. Roberts (Ed.), *New challenges to understanding organizations* (pp. 11–32). New York, Toronto: Macmillan.

Sagan, S. D. (2004) Learning from normal accidents. *Organization and Environment, 17 (1),* 15–19.

Schaaf, T. W. van der & Kanse, L. (2004). Biases in incident reporting databases: An empirical study in the chemical process industry. *Safety Science*, *42 (1),* 57–67.

Schein, E. H. (1990). Organizational culture. *American Psychologist, 45 (2),* 109–119.

Schöbel, M. & Manzey, D. (2011). Subjective Theories of Organizing and Learning from Events, *Safety Science*, 49 (1), 47-54.

Schöbel, M. (2009). Trust in high reliability organizations. *Social Science Information*, 48(2), 315-333.

Seghezzi, H. D., Fahrni, F. & Herrmann, F. (2007). *Integriertes Qualitätsmanagement. Der St. Galler Ansatz.* (3., vollst. überarbeitete Aufl.). München: Carl Hanser.

Skiba, R. (1997). *Taschenbuch Arbeitssicherheit* (9., neubearb. Aufl.). Bielefeld: Schmidt.

Turner, B. A. (1978). *Man-made disasters*. London: Wykeham Publ.

Turner, B. A. & Pidgeon, N. F. (1997). *Man-made disasters* (2. ed.). Boston [u. a.]: Butterworth-Heinemann.

Turner, B. A., Pidgeon, N., Blockley, D. & Toft, B. (1989) *Safety culture: its importance in future risk management.* Position paper for the Second World Bank Workshop on safety control and risk management, Karlstad, Sweden.

VGB-Powertec (2002). *Sicherheitskultur in deutschen Kernkraftwerken – Konzept zur Bewertung und Trendverfolgung.* [Unveröffentliches Manuskript].

Wagner, R., Schöbel, M., Klostermann, A. & Manzey, D. (2010). Sikumeth: Ein Multi-Methoden-Verfahren zur Erhebung von Sicherheitskultur in Kernkraftwerken. In R. Trimpop, G. Gericke & J. Lau (Hrsg.), *Psychologie der Arbeitssicherheit und Gesundheit: Sicher bei der Arbeit und unterwegs -wirksame Ansätze und neue Wege*, 16. Workshop 2010 (pp. 375-378). Kröning: Asanger Verlag.

Weick, K. E. (1976). Educational organisations as loosely coupled systems. *Administrative Science Quarterly, 21,* 1–19.

Weick, K. E. (1987). Organizational culture as a source of high-reliability. *California Management Review*, *29 (2),* 112–127.

Weick, K. E. & Roberts, K. H. (1993). Collective mind in organizations – Heedful interrelating on flight decks. *Administrative Science Quarterly, 38 (3),* 357–381.

Weick, K. E. & Sutcliffe, K. M. (2001). Das unerwartete Managen: Wie Unternehmen aus Extremsituationen lernen. Stuttgart: Klett-Cotta.

Wilpert, B., Becker, G., Maimer, H., Miller, R., Fahlbruch, B., Baggen, R., Gans, A., Leiber, I. & Szameitat, S. (1997). *Umsetzung und Erprobung von Vorschlägen zur Einbeziehung von Human Factors (HF) bei der Meldung und Ursachenanalyse in Kernkraftwerken.* [Endbericht SR 2039/8, Bericht der Technischen Universität Berlin und des TÜV Rheinland e. V. im Auftrag des Bundesministers für Umwelt, Naturschutz und Reaktorsicherheit im Rahmen des Vorhabens SR 2039/8].

Zohar, D. (1980). Safety climate in industrial organizations: Theoretical and applied implications. *Journal of Applied Psychology, 65 (1),* 96–102.

http://www.springer.com/978-3-642-19885-4

Human Factors
Psychologie sicheren Handelns in Risikobranchen
Badke-Schaub, P.; Hofinger, G.; Lauche, K. (Hrsg.)
2012, XIII, 365 S., Hardcover
ISBN: 978-3-642-19885-4