Risiko-Management in der Produktion

6

Le risque est l'onde de proue du succès! (Risiko ist die Bugwelle des Erfolgs)

F. Romeike, P. Hager, *Erfolgsfaktor Risiko-Management 4.0*,
https://doi.org/10.1007/978-3-658-29446-5_6

6.1 Risikoursachen und -wirkungen in der Produktion

In einem Industrie- und Handelsunternehmen können Risiken an jedem Punkt entlang der Wertschöpfungskette entstehen. Durch die verstärkte Globalisierung der Wertschöpfungsnetzwerke sowie die Verschlankung derartiger Netzwerke ist die Risikoexponierung vieler produzierender Unternehmen in den vergangenen Jahren angestiegen. Insbesondere durch den zunehmenden Trend zur Konzentration auf Kernkompetenzen (Verringerung von intraorganisationaler Arbeitsteilung bzw. Fertigungstiefe im Unternehmen) entwickeln sich zunehmend differenziertere Supply Chains.

Aus einer Makroperspektive kann die Wertschöpfungskette eines produzierenden Unternehmens als Prozess von vorgelagerten und nachgelagerten Prozessen – von der Rohstoffbeschaffung bis zum Service beim Endkunden – betrachtet werden (siehe Abb. 6.1). Auf die besonderen Aspekte des „Risiko-Managements in der Logistik und Supply Chain“ wird im nachfolgenden Kap. 7 eingegangen. Alle Aktivitäten, die Teil der Wertschöpfungskette sind, können mit dem Begriff *Supply Chain Management* (SCM) zusammengefasst werden.[1]

Der Wert eines Produktes oder auch einer Dienstleistung besteht nicht nur aus dem eigentlichen Produkt oder der Dienstleistung, sondern – betrachtet aus einer Mikroperspektive – aus sehr vielen unterschiedlichen Komponenten, die in den „Wertschöpfungsstufen“

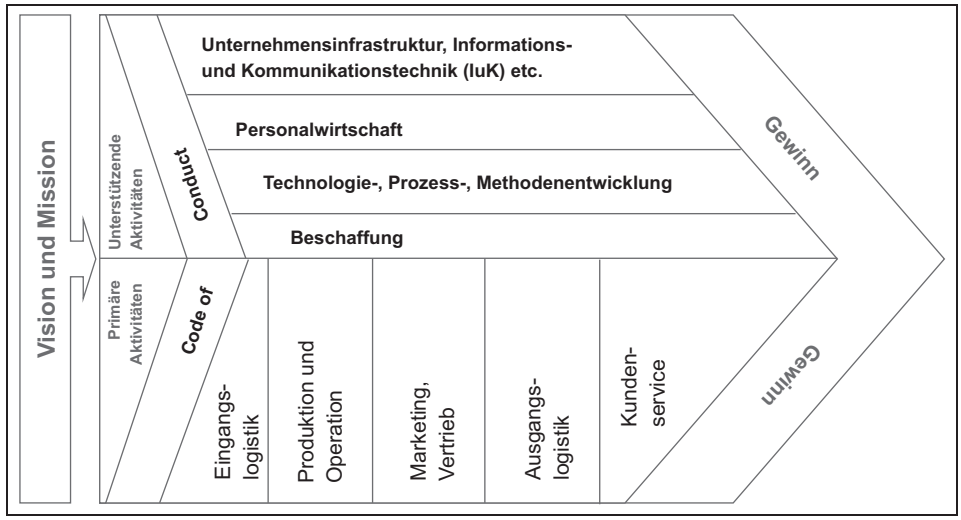


Abb. 6.1 Klassische Wertschöpfungskette in der Industrie und im Handel. (Eigene Darstellung)

[1] Vgl. Porter (1985), Sennheiser und Schnetzler (2008), Huth (2012) sowie Huth und Romeike (2016, S. 33 ff.).

[2] Die Begriffe „value chain“ und Wertschöpfungsnetzwerk bzw. Wertschöpfungskette werden im Folgenden synonym verwendet.

entstehen. In Addition stellen mehrere Wertschöpfungsstufen eine Wertschöpfungskette dar. Während sich die Wertkette (value chain)[2] ausschließlich auf die intraorganisationalen Bereiche bezieht, ist die Lieferkette (supply chain) weiter gefasst und umfasst auch externe Wertschöpfungsstufen (etwa in der Folge eines Outsourcings). In diesem Kontext spricht man auch von einem Wertschöpfungsnetzwerk.

Nachfolgend ist am Beispiel des Rohstoffs Kohle ein typisches Wertschöpfungsnetzwerk skizziert:

- Die Kohle wird in einem Bergwerk oder im Tagebau gefördert und an ein Stahlwerk verkauft.
- Das Stahlwerk verfeuert die Kohle – mit Stahlschrott – in Hochöfen. Dabei verbrennen im Stahl unerwünschte Begleitelemente wie Schwefel, Phosphor, Kohlenstoff etc. und gehen in das Rauchgas oder die Schlacke über. Der Rohstahl wird in eine Stahlgießpfanne abgegossen. Der Stahl wird dann – für das Strangguss-Verfahren in die so genannte Kokille abgegossen, bevor der Rohstahl durch Umformen oder Walzen weiterverarbeitet wird.
- Das Stahlwerk verkauft den Stahl an Automobilzulieferer, der sie in ein Karosserieteil verarbeitet, welches wiederum an einen
- Automobilhersteller verkauft und dort zu einem Auto verbaut wird.
- Das Auto wird an einen Händler verkauft und landet schließlich beim
- Verbraucher, der das Auto kauft.

An dem kleinen Beispiel erkennt man, dass die „supply chain“ ein Netzwerk von Organisationseinheiten ist, die durch Interaktion eine Leistung in Form eines Produkts oder

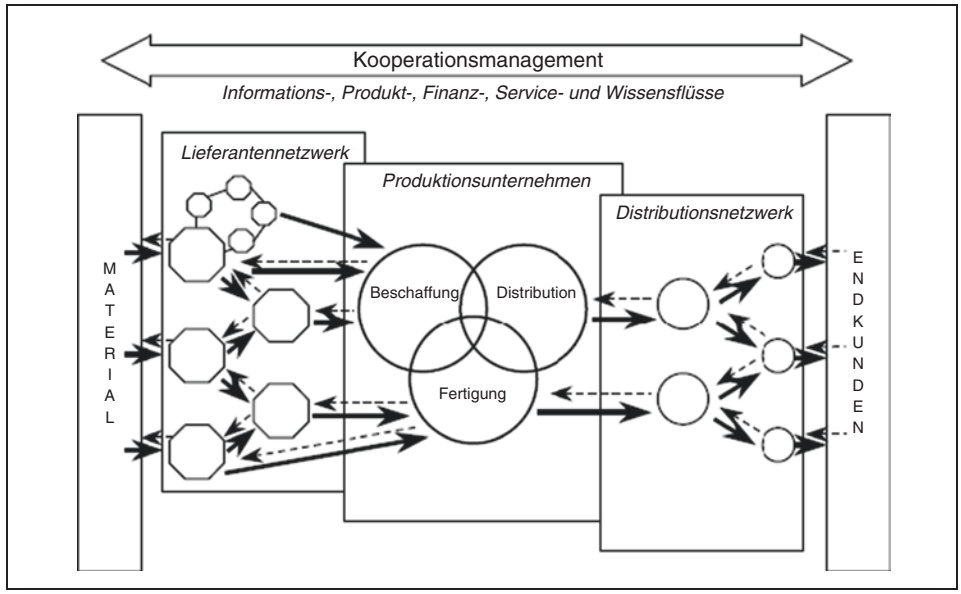


Abb. 6.2 Allgemeines Supply-Chain-Modell. (Quelle: Kersten et al. 2008)

einer Dienstleistung erbringen (vgl. Abb. 6.2). In diesem Kontext ist es unerheblich, zu welchem Unternehmen die Organisationseinheiten gehören. Im Kern der Betrachtung stehen übergreifende Prozesse, die beschreiben, wie Produkte oder Dienstleistungen erstellt werden, transportiert werden und schließlich beim Kunden ankommen. Eine Wertschöpfungskette besteht in der Regel aus Zulieferern, Produktionsstandorten, Logistikdienstleitern, Logistik- und Distributionszentren und einer Händlerorganisation sowie aus Rohstoffen, Halbfertigerzeugnissen und Fertigwaren, die zwischen den einzelnen Organisationselementen fließen. Ergänzt werden kann auch noch der Informations-, der Kapital-, Service und Wissenstransfer.[3]

Daher kann man eine derartige Wertschöpfungskette auch als ein unternehmensübergreifendes virtuelles Organisationsgebilde (= Netzwerk) betrachten, das als gesamtheitlich zu betrachtendes Leistungssystem spezifische Wirtschaftsgüter produziert.

Das oben skizzierte Beispiel könnte man daher auch noch um das Recycling des Autos ergänzen, so dass die „supply chain" sich von der Rohstoffgewinnung bis zum Recycling von Alt-Produkten erstreckt.

Das Supply Chain Management zielt in diesem Zusammenhang auf eine langfristige (strategische), mittelfristige (taktische) und kurzfristige (operative) Verbesserung von Effektivität und Effizienz industrieller Wertschöpfungsketten ab. Auch das Risiko-Management muss daher die komplette Wertschöpfungskette analysieren und potenzielle Risiken entsprechend bewerten.

Ergebnis der Verschlankung der Wertschöpfungsketten in den vergangenen Jahrzehnten – als Folge des zunehmenden globalen Wettbewerbs und der gestiegenen Anforderungen auf der Kundenseite – sind reduzierte Lagerbestände (*Just-in-time-Produktion* oder *Just-in-time-Logistik*), hoch ausgelastete Kapazitäten und optimierte Durchlaufzeiten.

So bezeichnet man als Just-in-time-Produktion (JIT) eine fertigungs- bzw. bedarfssynchrone Produktionsstrategie.[4] Hierbei wird das Ziel verfolgt, über durchgängige Material- und Informationsflüsse entlang der Wertschöpfungskette eine schnellere Auftragsbearbeitung zu ermöglichen. Ein Produkt – beispielsweise ein Auto – wird exakt zu dem Zeitpunkt produziert bzw. geliefert, zu dem es auch benötigt wird. In dem Kontext sind die einzelnen Produktionsschritte zeitlich in der Wertschöpfungskette einzuplanen.[5]

JIT kann die Effektivität der Wertschöpfungskette stark erhöhen. So sinkt beispielsweise die End-Montagezeit eines Autos in der Folge des JIT-Konzepts von ursprünglich 20 auf etwa acht Stunden beim Bau des Smart. Gleichzeitig muss der Lieferant die Vorma-

[3] Vgl. Huth und Romeike (2016) sowie Bowersox, Closs, und Cooper (2007).

[4] Vgl. Wildemann (2001), Toyota Motor Corporation (1998), Herlyn (2012) sowie Majima (1994).

[5] Das JIT-Konzept wurde ursprünglich vom japanischen Automobilhersteller Toyota eingeführt. Es war in den 1950er-Jahren ein Teil des Toyota Produktionssystem (TPS). Laut Taiichi Ono, dem die Idee zu JIT zugeschrieben wird, begann die Innovation in Richtung JIT im Jahr 1945, als der damalige Präsident von Toyota verlangte, dass sein Unternehmen binnen drei Jahren an Amerika Anschluss fände. Ono verfolgte daher die Strategie, dass durch die Eliminierung von Verschwendung (jap. Muda) Einsparungen erzielt werden können. Das Problem, welches er zu adressieren suchte, war die Überproduktion (mehr zu produzieren, als man unmittelbar benötigt) und die Vorratshaltung (Lagerung). Vgl. Ono (1988).

terialien und Endprodukte der jeweiligen Baugruppen vorhalten, so dass in der Folge der Hersteller seine Lagerkapazität und seine Lagerkosten verringern kann.

Auf der anderen Seite steigt in der Folge der schlanken Wertschöpfungsnetzwerke, globaler Lieferanten- und Distributionsnetzwerke auch deren Verwundbarkeit. In diesem Kontext sind nicht nur die höhere Komplexität und die kürzen Zeitfenster (siehe JIT) als Ursachen für steigende Risiken zu nennen, sondern auch der Einfluss unterschiedlicher Kulturen und Rechtssysteme. So werden bei einer JIT-Fertigung in aller Regel hohe Konventionalstrafen vereinbart, sofern der Lieferant in Lieferschwierigkeiten gerät und in der Konsequenz auch die Wertschöpfungskette des Herstellers massiv beeinflusst wird.

Die bisherigen Ausführungen verdeutlichen, dass Produktionsrisiken als Teil eines Wertschöpfungssystems oder einer Wertschöpfungskette betrachtet werden müssen. So interagieren beispielsweise logistische Risiken oder Supply-Chain-Risiken stark mit Produktionsrisiken. Die Beispiele im anschließenden Kap. 7 verdeutlichen die Verwundbarkeit der Wertschöpfungskette am Beispiel der Automobilindustrie in der Folge des Tōhoku-Erdbeben im Jahr 2011. Ein weiteres Beispiel lieferten uns im Jahr 2020 die Auswirkungen von SARS-CoV-2 / Covid-19 auf die globalen Lieferketten. So konnte beobachtete werden, dass es in der Supply Chain zu einem Dominoeffekt gekommen war. Einzelne Lieferanten oder eine „Kette an Lieferanten" gerieten in Schwierigkeit (bspw. hinsichtlich ihrer Liquidität) und die gesamte Kette verlangsamte sich bzw. brach zusammen. Diese Kettenreaktionen werden auch als „Loopback-Effekte" bezeichnet und ähneln den Nachbeben nach einem Erdbeben.

Empirische Studien zeigen auf, dass zunehmende Risiken vor allem durch die engere Zusammenarbeit in Wertschöpfungsnetzwerken, die fortschreitende Internationalisierung der „supply chains" sowie eine starke Effizienzfokussierung induziert werden. So wurden als wichtige Treiber die Globalisierung der Wertschöpfungsnetzwerke sowie der Abbau von Lagerbeständen, der Trend zu Lean Management und der anhaltende Trend zum Outsourcing identifiziert.[6]

Der Industrieversicherer Allianz Global Corporate & Specialty[7] führt regelmäßig unter mehreren Tausend Experten eine Umfrage zu den wichtigsten Risiken in produzierenden Unternehmen durch. In Abb. 6.3 sind Ergebnisse aus dem Jahr 2019 zusammengefasst.

Globale und lokale IT-Ausfälle und die Einführung strengerer Datenschutzbestimmungen rücken Cyberrisiken zunehmend in den Blickpunkt des Risiko-Managements. Laut dem Allianz Risk Barometer 2019 gehören Cybervorfälle gemeinsam mit Betriebsunterbrechungen zu den größten Geschäftsrisiken weltweit. Zwar dominiert aus Sicht deutscher Unternehmen auch weiterhin das Risiko einer Betriebsunterbrechung (48 %) knapp vor dem Risiko eines Cybervorfalls (44 %). Die Sorge vor rechtlichen Veränderungen im Wirtschaftsumfeld, zum Beispiel hervorgerufen durch Handelskriege, Zölle, Wirtschaftssanktionen, nimmt jedoch

[6] Vgl. Jüttner, U.: Supply chain risk management: Understanding the business requirements from a practitioner perspective, in: International Journal of Logistics Management, Vol 16/2005, S. 134.

[7] Vgl. www.agcs.allianz.com.

erstmals Platz drei im deutschen Ranking ein (35 %) und rangiert damit noch vor der Gefahr von Naturkatastrophen (28 %). Risiken, die von neuen Technologien wie künstlicher Intelligenz oder Autonomen Fahren ausgehen, sind ein weiterer großer Aufsteiger im deutschen Ranking und erreichen erstmals Platz 5 (20 %) gegenüber Platz 7 im Vorjahr.

In der Wirkung können viele der in Abb. 6.3 skizzierten Szenarien zu einer Betriebsunterbrechung in der Produktion führen. Denn fast alle großen Sachschäden beinhalten inzwischen das Wirkungsszenario einer Betriebsunterbrechung, das in der Regel den größten Teil des Schadens ausmacht. Auffällig ist zudem, dass Cyber- und Betriebsunterbrechungsrisiken miteinander verknüpft sind, da beispielsweise Ransomware-Angriffe oder IT-Ausfälle

Rang	Risikoursache bzw. Wirkung	Prozent	Trend
1	Betriebsunterbrechung (inkl. Supply-Chain-Unterbrechung)	48 %	↔
2	Cyber-Attacken (IT-Ausfall, Datenschutzverletzungen, Geldbußen und Straf en etc.)	44 %	↔
3	Rechtliche Veränderungen (bspw. Handelsrestriktionen und Handelskriege, Protektionismus, Zerfall Euro-Zone)	35 %	↑
4	Naturkatastrophen (bspw. Sturm, Überschwemmung, Erdbeben)	28 %	↓
5	Neue Technologien (bspw. Vernetzung Maschinen, Nanotechnologie, AI, 3D-Druck, Blockchain)	20 %	↑
6	Feuer, Explosion	19 %	↓
7	Produktrückruf, Qualitätsmängel, Serienfehler	17 %	↔
8	Marktentwicklungen (bspw. Volatilität, verstärkter Wettbewerb, M&A)	17 %	↓
9	Reputationsverlust oder Beeinträchtigung des Markenwertes	13 %	↔
10	Makroökonomische Entwicklungen (bspw. Rohstoffpreise, Deflation, Inflation)	9 %	↔

Abb. 6.3 Die 10 wichtigsten Risiken in der deutschen Industrie. (Quelle: Allianz Global Corporate & Specialty (2019). Die Zahlen repräsentieren, wie oft ein Risiko als Prozentsatz aller Antworten ausgewählt wurde. Die Zahlen addieren sich nicht zu 100 Prozent, da bis zu drei Risiken ausgewählt werden konnten. Befragt wurden insgesamt 172 Teilnehmer)

oft zu Betriebs- und Serviceunterbrechungen führen. So sind Cybervorfälle laut Allianz Risk Barometer die am meisten gefürchteten Auslöser von Betriebsunterbrechungen (50 % der Antworten), gefolgt von Feuer/Explosion (40 %) und Naturkatastrophen (38 %).

6.2 Methoden zur Analyse von Produktionsrisiken

Die Risikoquellen in einer Wertschöpfungskette können sowohl *endogener* als auch *exogener Natur* sein. Neben *Versorgungsrisiken* (exogen), *Nachfragerisiken* (exogen) und *Umfeldrisiken* (exogen) können im Workflow-Prozessrisiken (endogen und exogen) sowie Steuerungsrisiken (exogen und endogen) entstehen (Vgl. Abb. 6.4). *Umfeldrisiken* können beispielsweise durch geopolitische, politische Risiken, Naturkatastrophen oder Terrorismus entstehen. *Prozessrisiken und Steuerungsrisiken* resultieren aus den unternehmensinternen Produktions- und Logistikprozessen bzw. aus strategischen Entscheidungen des Managements.

Empirische Studien sind bei einer Analyse der wesentlichen Risikotreiber in Wertschöpfungsnetzen zu dem Ergebnis gekommen, dass vor allem Versorgungs- und Nachfragerisiken die Risikolandkarte dominieren.[8]

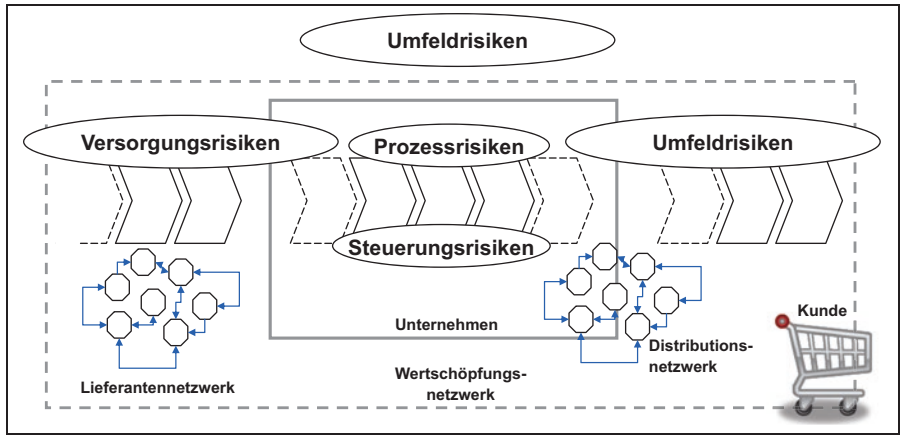


Abb. 6.4 Risikoquellen im Wertschöpfungsnetz eines Industrieunternehmens

[8] Vgl. beispielhaft Kersten und Hohrath (2008). Siehe hierzu auch das Kap. 7. Hierbei werden strategische Risiken nicht berücksichtigt.

Praxisbeispiel: Erdbeben von Kōbe und Auswirkungen im Bereich der Produktion

So führte beispielsweise das Erdbeben von Kōbe (Hanshin-Awaji-Erdbebenkatastrophe, offizielle Bezeichnung Süd-Hyōgo-Beben), welches am 17. Januar 1995 eine Stärke von M = 7,3[9] erreichte, nicht nur zu einer Naturkatastrophe mit einer der höchsten Schadenssummen aller Zeiten in Japan, sondern vor allem auch zu massiven Schäden im Bereich der Wertschöpfungskette von diversen Computerherstellen. Die Gesamtsumme aller durch das Erdbeben verursachten Schäden wird auf etwa 100 Milliarden US-Dollar – ohne Berücksichtigung von Folgeschäden durch Produktionsunterbrechungen – geschätzt. Die Ursache für das schwere Beben liegt in der tektonischen Struktur, da vor der Ostküste Japans drei Kontinentalplatten (Eurasische Platte, philippinische Platte und Pazifische Platte) aufeinandertreffen. Durch das Erdbeben und seine Folgen starben etwa 6400 Menschen, rund 42.000 Menschen wurden verletzt. 300.000 Menschen wurden durch das Erdbeben obdachlos, viele davon erst durch die vom Beben ausgelösten mehr als 300 Brände. Es wurden etwa 210.000 Gebäude zerstört oder schwer beschädigt, davon 7500 durch Feuer.[10]

Das Epizentrum lag etwa zwanzig Kilometer südwestlich vom Stadtzentrum von Kōbe in der Straße von Akashi, das Hypozentrum lag in einer Tiefe von sechzehn Kilometern. Das Hauptbeben dauerte etwa zwanzig Sekunden und setzte achtmal soviel Energie frei wie die Hiroshima-Bombe.

Trotz der gesetzlich vorgeschriebenen erdbebensicheren Bauweise (Urban Building Law aus dem Jahr 1919) wurden sowohl Neubauten als auch ältere Gebäude beschädigt oder zerstört. Obwohl diese Gesetze im Laufe der Zeit immer wieder nach Schadenbeben in Japan modifiziert und den neuen Erkenntnissen angepasst wurde, hielten auch viele neuere Gebäude den Schwingungen und Disalokationen des Untergrunds nicht stand.[11]

[9] Die Stärke eines Erdbebens kann mit Hilfe einer Magnitudenskala gemessen werden. Die populärste Magnitudenskala ist die Richterskala, die von Charles Francis Richter und Beno Gutenberg am California Institute of Technology 1935 entwickelt und anfänglich als ML-Skala (Magnitude Local) bezeichnet wurde. Aufgrund ihrer Definition ist die Richterskala nach oben unbegrenzt, die physischen Eigenschaften der Erdkruste machen aber ein Auftreten von Erdbeben der Stärke 9,5 oder höher nahezu unmöglich, da das Gestein nicht genug Energie speichern kann und sich vor Erreichen dieser Stärke entlädt. Der angegebene Wert, die Magnitude oder Größenklasse leitet sich aus dem dekadischen Logarithmus der maximalen Amplitude (Auslenkung) im Seismogramm ab, mit der ein kurzperiodisches Standardseismometer ein Beben in einer Entfernung von 100 km zum Epizentrum aufzeichnen würde. Ein Punkt mehr auf der Skala bedeutet demnach einen etwa zehnfach höheren Ausschlag (Amplitude) im Seismogramm und die 32-fache Energiefreisetzung (logarithmischer Anstieg) im Erdbebenherd. Vgl. Seibold (1995, S. 70).

[10] Vgl. Münchener Rückversicherungs-Gesellschaft (1996, S. 8).

[11] Vgl. United Nations Centre for Regional Development (UNCRD) (1995, S. 59 ff.).

In Kobe wurde zuvor ein Sicherheits-Steuerungssystem zur Verhinderung von Überschwemmungsschäden durch gebrochene Wasserleitungen installiert. Bei einer Magnitude von M = 5 wurde automatisch die Wasserzufuhr gestoppt. Die Löschwasserversorgung sollte daher durch Tankwagen erfolgen. Durch die Zerstörung des Straßennetzes war es jedoch den Tankwagen nicht in allen Fällen möglich, die Brandherde zu erreichen. Nach einem besonders regenarmen Sommer waren die Zisternen der Stadt nicht mit Löschwasser aufgefüllt worden, so dass die Feuerwehr den meisten Bränden tatenlos zusehen musste.[12]

In der Folge des Erdbebens waren alle Transportwege zwischen zwischen Nishainomiya und Kōbe schwer beschädigt. Ebenso wurden die wesentlichen Versorgungssysteme wie Elektrizität, Wasserversorgung, Gasleitungen und Telekommunikation zum Teil stark zerstört. Dadurch wurde das urbane Leben für mehrere Tage erschwert, und auch die Aufräumarbeiten konnten nicht in vollen Umfang durchgeführt werden. So waren beispielsweise nach dem Erdbeben etwa 85 Prozent der Menschen ohne Wasserversorgung.[13]

Die Wiederherstellungszeiten der Infrastruktur gestalteten sich in Kōbe wie folgt:

- Transportwege: etwa 4 Monate
- Hafenanlage: etwa 2 bis 3 Jahre
- Telefonnetz: etwa 2 Wochen
- Stromversorgung: etwa eine Woche
- Wasserversorgung: etwa 5 Wochen
- Gasversorgung: etwa 5 Monate

Kōbe zählt zu den wirtschaftlich erfolgreichsten Zentren auf der Insel Honshū. Der bedeutende Hafen von Kōbe wickelte im Jahr 1998, gemessen am Wert, acht Prozent des gesamten japanischen Außenhandels ab und war damit nach den Häfen Yokohama und Tōkyō (je elf Prozent) der drittwichtigste Hafen. Viele Unternehmen haben in Kōbe und Umgebung ihre Niederlassungen und Produktionsstätten. Diese Agglomeration war einer der wesentlichen Gründe für das hohe Schadensausmaß. In der Folge des Erdbebens kamen die Waren- und Materialflüsse – und damit in der Konsequenz das Wertschöpfungsnetzwerk – zum Erliegen. Die Produktion des größten japanischen Automobilherstellers Toyota war aufgrund der Schäden von zwei großen Stahlproduzenten für etwa drei Wochen stark beeinträchtigt. Betriebsunterbrechungen führten fast in der kompletten globalen Computerindustrie zu Lieferengpässen und Produktionsunterbrechungen.

[12] Vgl. United Nations Centre for Regional Development (UNCRD) (1995, S. 101).

[13] Vgl. United Nations Centre for Regional Development (UNCRD) (1995, S. 75).

Zur damaligen Zeit wurden die meisten Aktiv-Matrix-Displays (Flüssigkristallbildschirme für die Laptop-Fertigung, Thin Film Transistor = TFT) in Japan und überwiegend in Kōbe produziert. So mussten die Unternehmen Fujitsu, Matsushita, Sanyo, Sharp und Display Technology ihre Produktion zeitweilig einstellen. In der Folge der globalen Vernetzung der Wertschöpfungsketten kam es auch im globalen Kontext zu wirtschaftlichen Schäden in der Folge von Betriebsunterbrechungen. Die Produktionsausfälle führten beispielsweise zu Lieferengpässen bei den US-amerikanischen Herstellern Apple und IBM Corporation.

In der Folge des Erdbebens fiel auch der japanische Nikkei 225-Börsenindex am Tag nach dem Erdbeben um über tausend Punkte (5,6 Prozent). Auch die Börsen in Hongkong und Singapur brachen um 3,6 Prozent bzw. um 3,1 Prozent ein. Dies führte indirekt zur Insolvenz der Barings Bank, da deren Mitarbeiter Nick Leeson hohe Summen in Optionen auf den Nikkei investiert hatte.[14]

Zielsetzung eines präventiv ausgerichteten Risiko-Managements ist es, potenzielle Schwachstellen sowie die Ursachen für Störungen in der Wertschöpfungskette zu identifizieren und adäquate Maßnahmen zu initiieren, um die Resilienz des gesamten Systems zu erhöhen.

Hierbei ist zu berücksichtigen, dass ein bestimmtes Risikoszenario häufig erst durch die Kombination mehrerer Ursachen auftritt. Abb. 6.5 veranschaulicht, dass ein Risikoeintritt mehrere Folgereignisse auslösen kann, wobei diese oftmals nicht nur in eine Richtung wirken, sondern es können auch Rückkopplungen auftreten. In der unternehmerischen Praxis ist nicht selten zu beobachten, dass das, was man als Wirkung bezeichnet, auf die Ursache zurückwirkt und damit selbst zur Ursache wird. Außerdem können in der Praxis so genannte *„Dominoeffekte"* eintreten, sodass einzelne als unwesentlich wahrgenommene Risikoereignisse eine Kette weiterer Risiken mit schwerwiegenden Auswirkungen auslösen können.

Derartige „Dominoeffekte" werden auch als *systemische Risiken* bezeichnet. Ein systemisches Risiko liegt vor, wenn sich ein auf ein Element eines Systems einwirkendes Ereignis aufgrund der dynamischen Wechselwirkungen zwischen den Elementen des Systems auf das System als ganzes negativ auswirken kann oder wenn sich aufgrund der Wechselwirkungen zwischen den Elementen die Auswirkungen mehrerer auf einzelne Elemente einwirkender Ereignisse so überlagern, dass sie sich auf das System als ganzes negativ auswirken können. Ihre besondere Brisanz gewinnen systemische Risiken nicht allein aus den direkten physischen Schäden, die sie verursachen. Es sind vielmehr die weitreichenden Wirkungen in zentralen gesellschaftlichen Systemen (etwa der Wirtschaft, der Finanzwelt oder der Politik), die den Umgang mit diesem Risikotyp schwierig und zugleich dringlich machen.

[14] Vgl. vertiefend Erben (2004, S. 46–50).

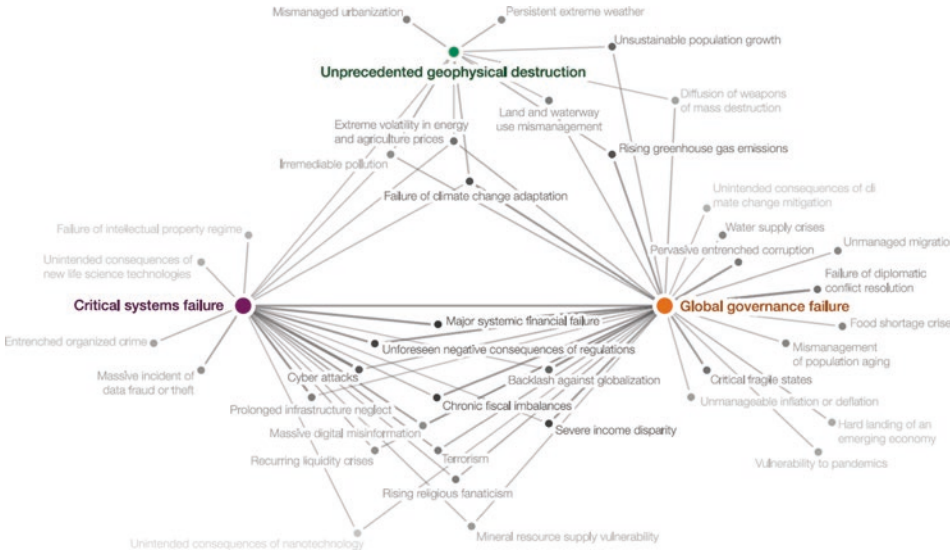


Abb. 6.5 Systemtheoretisches Risikoverständnis: Abhängigkeiten im Kontext des Tōhoku-Erdbebens 2011. (Quelle: World Economic Forum 2012, S. 31)

In Abb. 6.5 sind die Abhängigkeiten und komplexen Wirkungsketten des Tōhoku-Erdbeben aus dem Jahr 2011 skizziert. Das große Seebeben vor der Sanriku-Küste der japanischen Region Tōhoku ereignete sich am 11. März 2011 und erreichte eine Magnitudenstärke von M = 9,0. Während der nördliche Teil des betroffenen Gebiets bereits mehrfach in der Historie von starken Tsunamis verwüstet wurde (vermutlich etwa 1611, 1896, 1933), gab es in der südlichen Region (Sendai) wohl nur im Jahr 869 einen ähnlich hohen Tsunami.[15] Auf der Basis diverser wissenschaftlicher Analysen historischer seismischer Flutwellen und von GPS-Messungen lässt sich eine Spannweite von Wiederkehrperioden von 440 bis 1500 Jahren für ein Großbeben der Magnitude M = 9,0 in dieser Region Japans schätzen.[16]

Die Konsequenz war, dass einige Fabrikationsstätten japanischer Automobilhersteller und Zulieferbetriebe ihren Betrieb einstellen mussten. Diese Betriebsunterbrechungen führten global zu Lieferschwierigkeiten und Produktionsunterbrechungen in der Automobilindustrie. An der japanischen Ostküste – insbesondere rund um Fukushima, wurden Mikrocontrollern bzw. Mikroprozessoren produziert. Sie werden u. a. in Geld- und Telefonkarten, Mobiltelefonen, Waschmaschinen sowie in den Steuergeräten in Kraftfahrzeugen (beispielsweise ABS, ESP, Airbag, Motorregelung) eingebaut. Betroffen waren auch Hersteller von Silizium-Wafer. Diese werden aus ein- oder polykristallinen (Halbleiter-) Rohlingen (Ingots) hergestellt und dienen in der Regel als Substrat (Grundplatte) für elektronische Bauelemente, unter anderem für integrierte Schaltkreise, mikromechanische Bauelemente oder fotoelektrische Beschichtungen. Außerdem wurden rund um Fukus-

[15] Vgl. Allmann (2012, S. 7).

[16] Vgl. Allmann (2012, S. 8).

hima Leiterplatten (Printed Circuit Boards) und Lithium-Ionen-Batterien hergestellt. Die weltweite Verknüpfung der Risiken in der Wertschöpfungskette wird bei einer Analyse der Importquellen für Wafer deutlich. Rund 60 Prozent des Weltumsatzes an Silizium-Wafern wurden im Jahr 2010 aus Japan importiert. Ebenfalls aus Japan importiert wurden 35 Prozent der Flash-Speicher. Außerdem stammte im Jahr 2010 rund 21 Prozent der Halbleiterproduktion aus Japan. Ein weiteres wichtiges Exportprodukt sind Bismaleimide-Triazine, eine Verbindungskomponente, die in Kombination mit anderen Harzbausteinen und Glasgewebe als Verstärkung dient, in denen die ausgezeichnete thermische Stabilität von Polyimid mit den guten dielektrischen Eigenschaften von Cyanatester vereint sind. Rund 90 Prozent der Bismaleimide-Triazine stammen aus Japan.

Die japanische Regierung hat die geschätzten Kosten in der Folge des Tōhoku-Erdbebens auf rund 25 Billionen Yen (220 Mrd. Euro) beziffert. Werden jedoch die Havarien der Kernkraftwerke von Fukushima-Daiichi berücksichtigt, muss der Schaden als wesentlich höher bewertet werden. Insgesamt gilt das Erdbeben als die bisher weltweit teuerste Naturkatastrophe. Außerdem kann das Tōhoku-Erdbeben als die erste Naturkatastrophe betrachtet werden, die in vielen Ländern weitab von der betroffenen Region zu nachhaltigen energiepolitischen Veränderungen (Atomausstieg in Deutschland und der Schweiz, Nichteinstieg in Italien) geführt hat.

Die beiden Ereignisse in Kōbe (1995) und Tōhoku (2011) haben vor allem vor Augen geführt, dass in einer globalisierten Weltwirtschaft sich kein Risiko mehr isoliert betrachten lässt. So kann eine Betriebsunterbrechung bei einem Zulieferer in Asien direkte und massive Rückwirkungen auf einen Dritthersteller auf der anderen Seite der Erde haben. Und auch die globalen Auswirkungen von SARS-CoV-2 / Covid-19 und der (fast) weltweite „Shut Down“ im Jahr 2020 haben vielen Unternehmen die Verwundbarkeit der Supply Chain schmerzhaft verdeutlicht.

Im Kap. 3 sind ausgewählte Methoden der Risikoidentifikation und -bewertung beschrieben worden. Im Zusammenhang mit Risiken im Kontext Produktion werden die folgenden Methoden vertiefend beschrieben:

- Szenarioanalyse/-technik,
- FMEA (Failure Mode and Effects Analysis),
- Fehlerbaumanalyse,
- Bow-Tie-Analyse,
- Key Risk Indicator (Frühwarnindikatoren),
- CIRS,
- HAZOP,
- stochastische Szenarioanalyse.

Die „stochastische“ Szenarioanalyse wird im anschließenden Kap. 7 „Risiko-Management in der Logistik und Supply Chain“ exemplarisch dargestellt. Das methodische Vorgehen lässt sich direkt auf Risiken im Bereich Produktion übertragen. Weitere Kollektionsmethoden und analytischen Methoden wurden bereits im Kap. 3 beschrieben.

6.3 Szenariotechnik/Szenarioanalyse (deterministisch)[17]

Die *Szenariotechnik* ist ursprünglich als Methode der *Zukunftsforschung*[18] entwickelt worden. Sie wurde in den 1950er-und 1960er-Jahren von Herman Kahn[19] und Mitarbeitern in den USA entwickelt und vor allem als Prognosetechnik bei nicht linearen Verläufen und unberechenbaren Ereignissen eingesetzt. Im Hinblick auf die Zukunftsforschung definiert Kahn seine Szenarien als „[…] hypothetische Folge von Ereignissen, die konstruiert werden, um die Aufmerksamkeit auf kausale Prozesse und Entscheidungspunkte zu lenken."[20] Dabei „[…] beschränkt sich die Szenario-Technik im Gegensatz zu den meisten Prognosetechniken nicht nur auf die Verarbeitung quantitativer Informationen",[21] sondern greift vor allem auch auf qualitative Daten zurück. Darauf aufbauende, komplexe Systemanalysen sollen für ein umfassendes Verständnis des Systems sorgen und alternative Zukunftsbilder hervorbringen.

Inzwischen ist die Prognosefunktion in den Hintergrund getreten und Szenarien dienen mehr als Entscheidungshilfe („Was wäre, wenn …") beispielsweise im Zusammenhang mit der Strategischen Planung. Sie basiert im Kern auf der Entwicklung und Analyse möglicher Entwicklungen der Zukunft. Die Szenariotechnik verfolgt etwa die Analyse von Extremszenarios, besonders relevanter oder typischer Szenarios (Trendszenario). Szenarios werden häufig in Form eines Szenariotrichters dargestellt (vgl. Abb. 6.6). Bezogen auf die Zukunft symbolisiert der Trichter Komplexität und Unsicherheit. Die Zukunftsbilder befinden sich folglich auf der Schnittstelle des Trichters, wohingegen die Gegenwart immer am engsten Punkt des Trichters liegt. Den Ausgangspunkt der Betrachtung bildet das Trendszenario, welches auf einer Zeitachse aufgespannt wird. Dieses Trendszenario stellt die zukünftige Entwicklung unter der Annahme stabiler Umweltentwicklungen dar (ceteris paribus).

Jenes Extremszenario, das die bestmögliche Entwicklung („best case") aufzeigt, stellt das obere Ende des Trichters dar, wohingegen der sogenannte „worst case", also die schlechteste Entwicklungsmöglichkeit, das untere Ende bildet.

---

[17] Eine ausführliche Einführung in die deterministische Szenarioanalyse enthält das Kap. 4. Hier werden auch die Vorteile und Grenzen im Detail erläutert.

[18] Die Zukunftsforschung ist eine interdisziplinär ausgerichtete wissenschaftliche Beschäftigung mit möglichen, wahrscheinlichen und wünschbaren Zukunftsentwicklungen und Gestaltungsoptionen sowie deren Voraussetzungen in Vergangenheit und Gegenwart. In der internationalen Zukunftsforschung werden hauptsächlich die Begriffe Future(s) Research und Futures Studies gebraucht. Methoden und Techniken der Zukunftsforschung umfassen unter anderem Trendanalysen und -extrapolationen, Prognoseverfahren, Modellbildungen, Szenariotechniken, Simulationsverfahren, Zukunfts- und Visionswerkstätten. Neuerdings wird versucht, die Ergebnisse der Futurologie durch sogenannte Wild Cards zu ergänzen, also unvorhersehbare Entwicklungssprünge, ausgelöst etwa durch Kriege oder die Terroranschläge vom 11. September 2001.

[19] Kahn war bei der RAND Corporation beschäftigt, einem vom amerikanischen Verteidigungsministerium gegründeten Institut für Zukunftsforschung.

[20] Vgl. Kahn und Wiener (1968, S. 6), Romeike und Spitzner (2013, S. 94 ff.), Romeike (2018a, S. 166 ff.) sowie Götze (1993, S. 36).

[21] Vgl. Meyer-Schönherr (1992, S. 31).

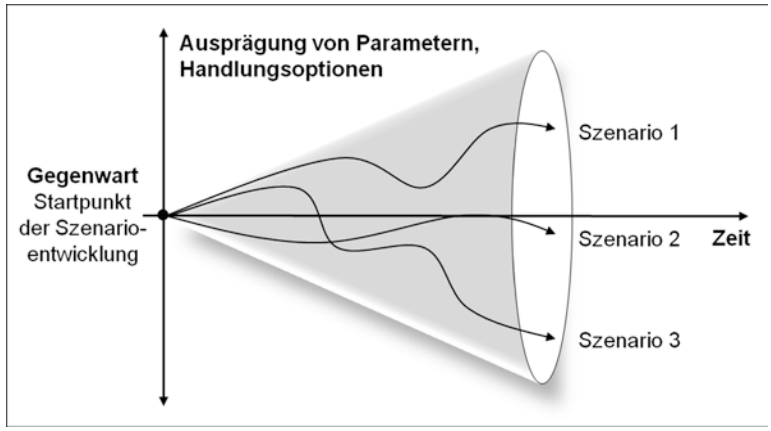


Abb. 6.6 Szenariotrichter. (Quelle: Romeike und Hager (2013, S. 254) basierend auf Linder und Spitzner (2010, S. 13))

In der Praxis ist eine enorme Vielfalt an Definitionen und Varianten der Szenariomethode anzutreffen. Daher ist eine Systematisierung der Vorgehensweise keineswegs trivial. In Kap. 4 „Strategische Chancen und Risiken" wird ein achtstufiges Vorgehen der deterministischen Szenarioanalyse im Detail beschrieben.

Im Folgenden ist ein einfaches vierstufiges Vorgehen skizziert:[22]

Schritt 1: Aufgaben- und Problemanalyse: Im Rahmen der Aufgaben- und Problemanalyse wird der Untersuchungsgegenstand zunächst festgelegt und beschrieben. Anschließend werden die Faktoren/Deskriptoren ermittelt, die den Untersuchungsgegenstand bzw. die künftigen Szenarios dieses Feldes beschreiben und möglicherweise beeinflussen. Output dieser Phase sind eine detaillierte Aufgaben- und Problembeschreibung sowie eine Faktorenliste.

Schritt 2: Einflussanalyse: Eine gute System- und Einflussanalyse muss die wesentlichen Systemelemente (Schlüsselfaktoren) und Beziehungen erfassen. In der Einflussfaktorenanalyse[23] wird untersucht, wie sich die einzelnen Faktoren wechselseitig beeinflussen. Dies kann mit einer Vernetzungstabelle ermittelt werden. Hierbei werden die Deskriptoren einander gegenübergestellt. Im direkten Vergleich wird ermittelt, welchen Einfluss (keinen, mittlere Wirkung, hohe Wirkung) ein Faktor auf einen anderen Faktor besitzt. Anschließend können jeweils die Aktiv- und die Passivwirkungen kumuliert und die Faktoren in einer Einflussmatrix miteinander verglichen werden.

Output dieser Phase sind die Vernetzungstabelle und eine Einflussfaktorenmatrix sowie eine Übersicht über die Größe des Einflusses der einzelnen Faktoren. Mit Hilfe dessen kann man die meist sehr große Anzahl von Einflussfaktoren auf eine handhabbare Anzahl reduzieren, wenn man nur die einflussreichsten Faktoren auswählt.

[22] Im Kap. 4 ist ein achtstufiges Vorgehen skizziert.

[23] Vgl. vertiefend das Kap. 4.

Schritt 3: Trendprojektion und Ermittlung von Szenarios: Zunächst gilt es, die unterschiedlichen Entwicklungsmöglichkeiten für die einzelnen ausgewählten Faktoren zu ermitteln. Welche Ausprägungen/zukünftige Entwicklungen sind für die einzelnen Faktoren möglich/denkbar? Die unterschiedlichen Ausprägungen können generisch in einem morphologischen Kasten ermittelt werden.

Durch die mathematische Kombination der verschiedenen Faktorausprägungen entstehen mögliche Szenarios. Beispielsweise kombiniert man die erste Ausprägung des ersten Faktors mit der zweiten Ausprägung des dritten Faktors: „Politische Risiken in Drittländern" mit der Ausprägung „Single-Sourcing-Risiken" wird kombiniert mit der Ausprägung des Faktors 3 „Technologieabhängigkeit". Da aber unter Umständen nicht alle Kombinationen sinnvoll sind oder sich sogar ausschließen, oder mehrere Kombinationen aufgrund ihrer Ähnlichkeit oder Bedeutung zusammengefasst werden können, ist eine Bündelung der Alternativen und eine Beschränkung der weiteren Untersuchung auf ausgesuchte Szenarios oder Alternativenbündel sinnvoll. Diese Filterung kann mit einer paarweisen Analyse oder mit Hilfe einer Konsistenzmatrix erfolgen (vgl. hierzu Abb. 4.18 in Kap. 4). Aus den konsistenten Szenarien werden dann diejenigen ausgewählt, die im Folgenden detailliert zu untersuchen sind. Um effektiv mit den Szenarios arbeiten zu können, ist es sinnvoll, eine Anzahl von vier bis acht Szenarios auszuwählen. Üblicherweise wird man wenigstens die beiden Extremszenarios, das Trendszenario und eventuell wenige, ausgewählte Szenarios weiter betrachten. Man sollte aber darauf achten, nicht ausschließlich die beiden Extremszenarios weiter zu betrachten, sich also nicht nur auf eine schwarze oder weiße Zukunft einstellen.

Output dieser Phase sind die möglichen Ausprägungen der einzelnen Faktoren/Deskriptoren, sowie ihre Kombination/Bündelung zu verschiedenen Szenarios. Anschließend bietet sich eine Beschreibung/Ausformulierung der Szenarios an, um sie verständlicher und leichter kommunizierbar zu machen.

Schritt 4: Bewertung und Interpretation

Die ausgewählten Szenarios werden in dieser Phase weiter untersucht. Die Szenarios werden ggf. mit ihren geschätzten Eintrittshäufigkeiten bzw. Eintrittswahrscheinlichkeiten und den mit den jeweiligen Szenarios verbundenen Chancen und Risiken gegenübergestellt. Außerdem lassen sich die Szenarios bezüglich Ist-Situation (in welchem Szenario befinden wir uns) und Erwartungssituation (wohin entwickelt sich die Zukunft) bewerten. Nach dieser Betrachtung können Unternehmen Maßnahmen/Handlungsoptionen für die einzelnen Szenarios definieren, um sich für diese zu rüsten. Mit Hilfe von Szenarios kann ein Unternehmen ebenfalls seine Strategie überprüfen. Stellt es fest, dass seine aktuelle Strategie in keinem der erarbeiteten Szenarios Erfolg hat, muss eine Anpassung der Strategie stattfinden. Szenarios helfen in diesem Fall bei der zukunftsrobusten Strategiefindung.

Output dieser Phase ist Bewertung und Gegenüberstellung sowie abgeleitete Handlungsoptionen und Maßnahmen der ausgewählten Szenarios.

Beim *Einsatz der Szenariotechnik im Risiko-Management* können eine Reihe von Anforderungen definiert werden:[24]

- Sachkompetenz: Kenntnisse über Untersuchungsgegenstand und -raum,
- Vorstellungen und Kenntnisse über grundlegende ökonomische und gesellschaftliche Zusammenhänge und Prozesse,
- Methodenkompetenz,
- Fantasie und Kreativität.

Da eine einzelne Person alle Anforderungen nur in den seltensten Fällen erfüllen kann, sollte die Szenariotechnik immer nur im Rahmen von (interdisziplinär zusammengesetzten) Workshops angewendet werden. So eignet sich die Szenariotechnik ideal für die Risikoevaluierung im Rahmen von Projektteams oder Risikokomitees.

In der Unternehmenspraxis sind unterschiedliche Typen von Szenarien bekannt, deren Übergänge jedoch fließend sind.

Trendszenarien stellen die Frage, wie es weitergeht, wenn alles wie bisher weiterläuft („business as usual"). Als Ausgangsszenarien sind sie wichtig. Sie kommen Trendextrapolationen am nächsten, berücksichtigen aber auch qualitative Informationen und sind damit methodisch komplexer. Beispiel: Wie entwickelt sich die Risikolandkarte, wenn keine neuen Risiken hinzutreten und die ökonomischen Rahmenbedingungen gleichbleiben?

Alternativszenarien stellen die Frage, was wäre, wenn diese oder jene Richtung eingeschlagen würde (beispielsweise „best case" oder „worst case"). Sie geben alternative Entwicklungsmöglichkeiten an, die, wenn sie erreicht werden sollen, entsprechendes zielgerichtetes Handeln voraussetzen oder, wenn sie vermieden werden sollen, entsprechende Gegenmaßnahmen notwendig machen. Beispiel: Wie entwickelt sich die Risikolandkarte, wenn der Dollar/Euro-Wechselkurs sich um zwanzig Prozent verändert? Wie entwickelt sich die Risikolandkarte, wenn unser Hauptkunde insolvent wird?

Kontrastszenarien stellen die Frage, was zu tun ist, um ein bestimmtes Ziel zu erreichen. Beispiel: Was ist zu tun, damit unsere Risikotragfähigkeit erhalten bleibt oder Value at Risk den Betrag von fünf Millionen Euro nicht überschreitet?

In Tab. 6.1 sind die wesentlichen Stärken und Grenzen der deterministischen Szenarioanalyse zusammengefasst.

6.4 FMEA (Failure Mode and Effects Analysis)

Die Fehlermöglichkeits- und Einflussanalyse bzw. Ausfalleffektanalyse (FMEA = Failure Mode and Effects Analysis) ist eine systematische, halbquantitative Risikoanalysemethode.[25] Sie wurde ursprünglich zur Analyse von Schwachstellen und Risiken technischer

[24] Vgl. Sträter (1988, S. 429).

[25] Vgl. Romeike und Hager (2013, S. 256–257), Romeike (2018b, S. 73–77).

Tab. 6.1 Stärken und Grenzen der Szenarioanalyse. (Quelle: Romeike 2018a, S. 187–188)

Stärken	Grenzen
Eine Szenarioanalyse erlaubt den Einbezug qualitativer Aspekte und quantitativer Daten in die Analyse, sie fördert das Denken in Alternativen.	Erforderlich für den Einsatz der Szenarioanalyse ist die Fähigkeit komplex und vernetzt zu denken.
Häufig werden durch die Betrachtung aus verschiedenen Perspektiven Zusammenhänge sichtbar, die auf den ersten Blick nicht offensichtlich sind, darüber hinaus erweitert die meist interdisziplinäre Zusammenarbeit die Sichtweise des Analyseteams.	Die Qualität der Szenarien ist unter anderem abhängig von Kompetenz, Vorstellungskraft, Kreativität, Teamfähigkeit, Kommunikationsfähigkeit oder Enthusiasmus der Teilnehmer der Szenarioanalyse; hierin liegen vielfältige Möglichkeiten für ein Scheitern.
Die Szenarioanalyse kann leicht mit weiteren Methoden der Erkenntnisgewinnung kombiniert werden, beispielsweise Prognosen, Umfragen oder Delphi-Verfahren.	Die Ergebnisse der Analyse sind – je nach Stärke der subjektiven Beeinflussung durch die Teilnehmer – nicht wertfrei und daher keine gesicherten Erkenntnisse, sie sind stets angreifbar.
Die Szenarioanalyse „zwingt“ die Teilnehmer zu einem strukturierten Vorgehen bei der Analyse zukünftiger Szenarien.	Die Anwendung der Methode ist zeit- und arbeitsintensiv, damit in der Regel auch mit hohen Kosten verbunden.
Komplexität kann mit Hilfe der Einflussfaktorenanalyse sowie der Konsistenzmatrix reduziert werden.	

und militärischer Systeme und Prozesse entwickelt. Bereits im Jahr 1949 wurde sie erstmalig unter der Bezeichnung „Military Specification MIL-P-1629“ vom US-Militär entwickelt und eingesetzt. Mit der Methode solle die Zuverlässigkeit von Systemen und Ausrüstung durch eine Analyse und Darstellung der Folgen von system- und ausrüstungsbezogenen Fehlern bewertet werden. Die Fehler wurden hinsichtlich der potenziellen Auswirkungen auf Erfolg, Personal und Sicherheit der Ausrüstung unterschieden.

Später wurde eine erweiterte Version, die FMECA (Failure Mode, Effects, and Criticality Analysis) im Jahr 1963 von der US-Bundesbehörde für Raumfahrt und Flugwissenschaft, der National Aeronautics and Space Administration (Nasa), für die Untersuchung der technischen Risiken beim Apollo-Projekt angewendet. Das Projekt brachte zum ersten und bislang einzigen Mal am 20. Juli 1969 Menschen auf den Mond. Anschließend fand die Methodik Verbreitung in der Luft- und Raumfahrt, für Produktionsprozesse in der chemischen Industrie und in der Autoindustrie – insbesondere im Bereich der Fahrzeugentwicklung und Forschung.

So wurde die FMEA in der Automobilbranche im Jahr 1977 durch Ford Motor Co. eingeführt. Im Jahr 1980 wurde die Methode als DIN-Norm 25448 veröffentlicht und vom Verband der Automobilindustrie (VDA) weiterentwickelt.

Des Weiteren wurde die FMEA nach dem Störfall im Druckwasserreaktor „Three Miles Island“ in Harrisburgh/Pennsylvania vom 28. März 1979 auch für Nuklearanlagen empfohlen. Heute empfehlen viele Standards, beispielsweise im Qualitätsmanagement, nachdrücklich den Einsatz einer FMEA-Methode. Seit einigen Jahren wird in der Automobilindustrie die Erstellung einer FMEA sogar zwingend vorgeschrieben. So ist für jedes Produkt eine FMEA nachzuweisen, die die spezifischen Risiken bewertet und abbil-

det. Bei der Analyse sind die Einsatzbedingungen des Produkts in der Nutzungsphase, insbesondere bezogen auf Sicherheitsrisiken sowie auf einen erwartungsgemäßen Fehlgebrauch, zu berücksichtigen.

Die Kernidee der modernen FMEA basiert auf dem frühzeitigen Erkennen und Vermeiden von potenziellen Fehlern und damit der Reduktion des Auftretens potenzieller Wirkungen von Risikoeintritten. Die FMEA analysiert daher präventiv bzw. antizipativ Fehler und deren Ursache. Sie folgt damit der im Risiko-Management wichtigen Unterscheidung zwischen Ursache (cause), Risiko (risk) und Wirkung (effect). Siehe hierzu vertiefend die Ausführungen zur Bow-Tie-Analyse.

Sie bewertet Risiken bezüglich Auftretens, Bedeutung und ihrer Entdeckung in der Ursachenebene. Hierbei gilt die einfache und fast triviale Logik: Je früher ein Fehler erkannt wird, desto besser. Eine Fehlerfortpflanzung über den gesamten Produktentstehungszyklus von der Forschung und Entwicklung bis zum ausgelieferten Produkt bedeutet fast immer eine Potenzierung des Aufwandes.

Aus Sicht der Automotive Action Group (AIAG) und des Verbands der Automobilindustrie e. V. (VDA)[26] unterstützt die FMEA Unternehmen bei der Erreichung der nachfolgenden Ziele:

- Verbesserung der Qualität, Zuverlässigkeit, Herstellbarkeit, Wartungsfreundlichkeit und Sicherheit von Produkten;
- Herunterbrechen und Zuordnen von Systemanforderungen auf Untersysteme und Komponenten;
- Senkung der Gewährleistungs- und Kulanzkosten;
- Nachweisbarkeit der Produkt- und Prozessrisikoanalyse im Produkthaftungsfall;
- Vermeidung von späten Änderungen während der Entwicklung;
- Fehlerfreie Produkteinführungen;
- Zielgerichtete Kommunikation bei internen und externen Kunden- und Lieferantenbeziehungen;
- Aufbau einer Wissensbasis im Unternehmen, beispielsweise Dokumentation von gewonnenen Erkenntnissen (Lessons Learned);
- Einhaltung gesetzlicher- und behördlicher Genehmigungsauflagen bei der Zulassung von Komponenten, Systemen und Fahrzeugen;
- Sicherstellen der korrekten Erfassung von hierarchischen Beziehungen, Verknüpfungen und Schnittstellen zwischen Komponenten, Systemen und Fahrzeugen.

Im Prozessschritt der Risikoidentifikation und -bewertung ermittelt die FMEA die Ursache für ein Risiko über die drei Faktoren A, B und E. Hierbei symbolisiert A (Auftreten oder auch O für „Occurrence“ beziehungsweise für „Probability“) die subjektive Wahrscheinlichkeit, dass ein gewisses Risiko auftritt, E die Entdeckungswahrscheinlichkeit (oder auch D für „Detection“) und B für die Bedeutung der Fehlerfolge/ (oder auch S für „Severity“).[27]

[26] Vgl. Automotive Action Group (AIAG) und Verband der Automobilindustrie e. V. (2017, S. 19).

[27] Vgl. Bojar (2012, S. 44) sowie Romeike und Hager (2013, S. 257).

Hierzu werden aktuell drei Matrizen (BxA = Produkt-Risiko, BxE = Verifizierungs-Risiko, AxE = Durchschlupf-Risiko) zur Analyse verwendet. Die früher oft benutzte RPZ (BxAxE) diente mehr oder weniger als Maß zur Risikobewertung, wird aber von keinem professionellen FMEA-Experten – aufgrund mangelnder Aussagekraft – mehr empfohlen.[28]

Da üblicherweise alle drei Faktoren auf den Bereich 1 bis 10 normiert werden, eignet sich das Verfahren insbesondere zur Quantifizierung von qualitativen Daten.[29] Die in der Praxis häufig noch angewendete, aber nicht mehr empfohlene RPZ entsteht durch Multiplikation der A-, B- und E-Scorewerte (RPZ = B · A · E) und kann dementsprechend Werte zwischen 1 und 1000 annehmen.

Bedingt durch dieses Vorgehen, lassen sich die Ergebnisse lediglich als grobe Einschätzung eines Risikos verstehen und bietet eine grobe Priorisierung einzelner Risiken. Eine hohe RPZ deutet demnach auf die Notwendigkeit weiterer Maßnahmen hin, während Risiken mit niedriger RPZ vernachlässigt werden können. Die multiplikative Verknüpfung der drei Faktoren muss jedoch kritisch bewertet werden: Insbesondere bei „Low-probability-high-consequence-risks“ (Extremereignissen) kann die RPZ bei extrem niedrigen P- oder W-Werten insgesamt niedrig sein und damit eine geringe Dringlichkeit suggerieren. Da die verwendeten Matrizen meistens asymmetrisch sind, wird eine Multiplikation, wie in der RPZ, oft falsche Abarbeitungs-Prioritäten liefern.

Deshalb wurde bereits im Jahr 2009 der Ampelfaktor (Farbbestimmung in den drei Matrizen) als alternative Priorisierung vorgestellt.[30] Diese Auswertung ist inzwischen in vielen Unternehmen etabliert (sowie in anerkannten Methodenbeschreibungen sowie in der Mehrzahl der am Markt angebotenen Analyse-Software umgesetzt). Inzwischen wurde der „Ampelfaktor“ zur RMR (Risk-Matrix based Ranking) weiterentwickelt.

Die Analyse der modernen FMEA erfolgt in der Regel grafisch unterstützend zu den Entwicklungstätigkeiten. Dies bringt den Beteiligten erheblich mehr Übersichtlichkeit und somit Nutzen als die früher übliche Formblattnotation.

Durch die Konsolidierung von Risiken an einzelnen Stellen eines größeren Systems, dessen Grenzen klar definiert sein müssen, erlaubt FMEA insbesondere auch die Ableitung eines Maßes für die Verlässlichkeit eines komplexen Systems. Im Kontext des Risiko-Managements ermöglicht die FMEA so, durch Analyse aller Netzwerkkomponenten, eine (grobe) Gesamtrisikobewertung für eine Infrastruktur zu erstellen.

Die FMEA ist letztendlich weniger eine Methode zur Risikoidentifikation, sondern mehr ein Mittel zu einer (möglichst) ganzheitlichen Dokumentation, Bewertung und Steuerung identifizierter Fehler beziehungsweise potenzieller Risiken sowie ein bedeutendes Medium zur Konzentration in der systematischen Kommunikation.

Ein weiterer Vorteil der Fehler-Folgen-Analyse ist die klare Formalisierung mit Hilfe von „Worksheets“ (Arbeitsblättern), die neben der Funktion, die Fehlerursache, die Fehlerwirkung, die bedrohten Objekte (targets) sowie die Risikobewertung enthalten (vgl. Abb. 6.7).

[28] Vgl. hierzu Werdich (2019).

[29] Vgl. Arvanitoyannis und Varzakas (2008).

[30] Vgl. Werdich (2012).

RiskNET®

FMEA: Formblatt

Prozess-FMEA ☐ **Produkt-FMEA** ☐

Name / Abteilung: **Prozess- / Produktname:** **Erstellt durch:** **Datum:** **Überarbeitet durch / am:**

	Fehlerort / Fehlermerkmal	Potenzielle Fehler	Fehlerfolge	Fehlerursache	Derzeitiger Zustand: Kontrollmaßnahmen	A*	B*	E*	RPZ*	Empfohlene Maßnahmen	Verant-wortlich	Verbesserter Zustand: Getroffene Maßnahmen	A*	B*	E*	RPZ*
1.	Server X200	Firmware Bug	Totalausfall	Firmware Upgrade nicht geladen	Regelmäßige Upgrades	3	10	10	300	Parallelsystem und Spiegelung	PH	Parallelsystem gestartet	1	10	10	100
2.	Lagerung	Spiel in der Lageranordnung	unexakte Funktionserfüllung	Lockern der Wellenmutter im Betrieb	Regelmäßige Kontrollen	3	8	10	240	Zusätzliche Sicherung der Wellenmutter	FR		1	8	10	80
3.		Dichtung durchlässig	frühzeitiger Lagerverschleiß	Dichtung genügt nicht den Anforderungen		2	5	10	100	Radialwellendichtring nach DIN verwenden	PH		1	5	10	50
4.	Vertrieb	Falsche Adresse	Retoursendung / Kundenverlust	Unachtsamkeit beim Kundenkontakt	Regelmäßige Stichproben im CallCenter	4	9	10	360	Bessere Schulung der CallCenter Mitarbeiter	FR	Zielgerichtete Auswahl von CallCenter Mitarbeitern	1	8	10	80
5.																
6.																
7.																
8.																
9.																
10.																

A* ... Auftreten

Wahrscheinlichkeit des Auftretens
(Fehler kann vorkommen)

unwahrscheinlich	= 1
sehr gering	= 2 - 3
gering	= 4 - 6
mäßig	= 7 - 8
hoch	= 9 -10

B* ... Bedeutung

Auswirkungen auf den Kunden

kaum wahrnehmbar	= 1
unbedeutender Fehler	= 2 - 3
mäßig schwerer Fehler	= 4 - 6
schwerer Fehler	= 7 - 8
äußerst schwerer Fehler	= 9 -10

E* ... Entdeckung

Wahrscheinlichkeit der Entdeckung
(vor Auslieferung an Kunden)

hoch	= 1
mäßig	= 2 - 3
gering	= 4 - 6
sehr gering	= 7 - 8
unwahrscheinlich	= 9 -10

RPZ* ... Risiko-Prioritätszahl

hoch	<= 1000
mittel	<= 250
gering	<= 125
kein	= 1

Abb. 6.7 Beispiel für ein FMEA-Arbeitsblatt. (Quelle: Romeike und Hager 2013, S. 259)

In der Praxis werden unterschiedliche Arten von FMEA unterschieden:

(1) **Design-FMEA/Konstruktions-FMEA**
Die Design- oder Konstruktions-FMEA unterstützt bei der Fehler-/Risikoeinschätzung bei der Entwicklung und Konstruktion von Produkten, um die Fertigungs- und Montageeignung möglichst präventiv und frühzeitig einzuschätzen. Die Analyse beinhaltet systematische Fehler während der Konstruktionsphase.

(2) **System-FMEA**
Hierbei liegt der Fokus vor allem auf einem einwandfreien Funktionieren der einzelnen Systemkomponenten. Bereits in einer sehr frühen Produktplanungsphase werden Überlegungen zum Gesamtrisiko, wie etwa unsichere Marktanteile, Kostenbeherrschung, Make or Buy, Sicherheit, Werbe- und Vertriebsstrategien oder Fragen der Umweltverträglichkeit gestellt. Die Analyse beinhaltet zufällige und systematische Fehler während des Betriebes.

(3) **Hardware-FMEA**
Eine Hardware-FMEA verfolgt das Ziel, Fehler beziehungsweise Risiken aus dem Bereich Hardware & Elektronik zu analysieren, zu bewerten und mit Maßnahmen abzustellen.

(4) **Software-FMEA**
Eine Software-FMEA verfolgt das Ziel, Fehler beziehungsweise Risiken im Programmcode zu analysieren, zu bewerten und mit Maßnahmen abzustellen.

(5) **Prozess-FMEA**
Hierbei liegt der Fokus vor allem bei der Analyse von einwandfreien Prozessen zur Herstellung der Bauteile und Systeme. Bevor die Einzelteile und Baugruppen in die Produktion gehen, untersucht ein Expertenteam die Realisierungsrisiken und legt fest, welche möglichen prozessbegleitenden Maßnahmen zur besseren Beherrschung notwendig werden. Entdeckt werden sollen Fehler vor der Auslieferung an den Kunden.

Im FMEA-Handbuch des Verbands der Automobilindustrie e. V.[31] sind sowohl die Design-FMEA als Prozess-FMEA wird in sechs Schritten im Detail und unterlegt mit Praxisbeispielen beschrieben (siehe hierzu exemplarisch Abb. 6.8). Außerdem wird im Handbuch die Anwendung der FMEA im Softwareentwicklungsprozess sowie für Maschinen- und Anlagenhersteller skizziert.[32]

Auf die Grenzen der FMEA weisen auch die Verbände AIAG und VDA hin.[33] So ist etwa für das richtige Verständnis und eine adäquate Interpretation der Ergebnisse das Bewusstsein wichtig, dass es sich bei der FMEA um eine qualitative bzw. semi-quantitative Analyseme-

[31] Vgl. Automotive Action Group (AIAG) und Verband der Automobilindustrie e. V. (2017).

[32] Weitere Praxisbeispiel siehe Romeike (2018b) sowie Arvanitoyannis und Varzakas (2008).

[33] Vgl. hierzu Automotive Action Group (AIAG) und Verband der Automobilindustrie e. V. (2017, S. 20 f.).

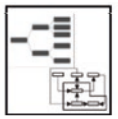
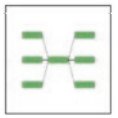
System Analysis			Failure Analysis and Risk Mitigation		
1st Step Scope Definition	2nd Step Structure Analysis	3rd Step Function Analysis	4th Step Failure Analysis	5th Step Risk Analysis	6th Step Optimization
					
Project identification	System structure for a product or elements of a process	Overview of the functionality of the product or process	Establishment of the failure chain (potential Failure Effects, Failure Modes, Failure Causes) for each product or process function (step)	Assignment of Prevention Controls (existing and/or planned) to the Failure Causes and Failure Modes	Identification of the actions necessary to reduce risks
Project plan	Visualization of the analysis scope using a structure tree or equivalent: block diagram, boundary diagram, digital model, physical parts, or process flow diagram	Visualization of product or process functions using a function tree (function net), function matrix parameter diagram or process flow diagram	Visualization of product or process failure relationships (failure nets and/or the FMEA worksheet)	Assignment of detection controls (existing and/or planned) to the Failure Causes and Failure Modes	Assignment of responsibilities and deadlines for action implementation
Analysis boundaries: What is included and excluded from the analysis	Identification of design interfaces, interactions, close clearances, or process steps	Association of requirements or characteristics to functions and functions to system or process elements	Creation of failure structures by linking the failures in the failure chain	Rating of Severity, Occurrence and Detection for each failure chain	Implementation and documentation of actions taken
Identification of baseline FMEA with lessons learned		Cascade of customer (external and internal) functions with associated requirements	Identification of product noise factors or process sources of variation (4M) using a fishbone diagram, parameter diagram, or failure network Collaboration between customer and supplier (Failure Effects)	Collaboration between customer and supplier (Severity) Evaluation of Priority Matrix Results (PMR)	Confirmation of the effectiveness of the implemented actions Assessment of risk after actions taken Continuous Improvement of the product and process
Basis for the Structure Analysis step	Basis for the Function Analysis step	Basis for the Failure Analysis step	Basis for the record of failures in the FMEA form and the Risk Analysis step	Basis for the product or process Optimization step	Basis for refinement of the product and/or process requirements and prevention / detection controls

Abb. 6.8 Die Durchführung der Design-FMEA in sechs Schritten. (Quelle: Automotive Action Group (AIAG) und Verband der Automobilindustrie e. V. (VDA) 2017, S. 37)

thode handelt. Außerdem zeigt sie die Abhängigkeiten von den Fehlerursachen auf, die stets als Einzelfehler betrachtet werden. Für quantitative Analysen und Mehrfachfehler bietet die Werkzeugkiste des Risikomanagers ergänzende Methoden (beispielsweise die FMEDA, Failure Modes, Effects and Diagnostic Coverage Analysis oder Methoden aus dem Bereich der stochastischen Szenarioanalyse beziehungsweise quantitativer Simulationsmethoden). Diese quantitativen Methoden ermöglichen beispielsweise die Analyse potenzieller Einzelfehler, Mehrfachfehler sowie latente Fehler auf der Grundlage quantitativer Metriken.

Für die Anwendung in der Praxis ist es außerdem wichtig, dass die FMEA möglicher Fehler sowie angemessene Maßnahmen eindeutig beschreibt. So weisen die Verbände AIAG und VDA darauf hin, dass technisch präzise Formulierungen zu verwenden sind, die es einem Experten erlauben, Fehler zu erkennen und deren mögliche Folgen abzuschätzen. Dehnbare oder gar emotional besetzte Begriffe (gefährlich, untragbar, unverantwortlich, usw.) sind unbedingt zu vermeiden. Außerdem dürfen potenzielle Fehler nicht verharmlost werden, auch wenn eine mögliche Wirkung zu einem Stressszenario führen könnte (siehe hierzu der Diesel- oder Abgasskandal, der im September 2015 öffentlich bekanntgemacht wurde. Die Volkswagen AG hatte eine illegale Abschalteinrichtung in der Motorsteuerung ihrer Diesel-Fahrzeuge verwendet. Die US-amerikanischen Abgasnormen wurden nur in einem speziellen Prüfstandsmodus erreicht, im Normalbetrieb wurde dagegen ein Großteil der Abgasreinigungsanlage weitgehend abgeschaltet.).

In Tab. 6.2 sind die wesentlichen Stärken und Grenzen der FMEA zusammengefasst.

Tab. 6.2 Stärken und Grenzen der FMEA. (Quelle: Romeike 2018a, S. 85)

Stärken	Schwächen
Das System wird vollumfassend betrachtet und schrittweise in kleinste Komponenten zerlegt.	Die Multiplikation der ordinal skalierten Merkmale B, A und E ist streng mathematisch nicht definiert. Daher ist die (klassische) RPZ eher kritisch zu bewerten.
FMEA wird in diversen ISO-Regelwerken beschrieben und ist beispielsweise in der Automobilindustrie zwingend vorgeschrieben.	Viele Risiken (vor allem schwankungsorientierte) können nicht mit Hilfe B, A und E bewertet werden. Bei einer Multiplikation von Eintrittswahrscheinlichkeit und Schadensausmaß wird eine Binomialverteilung der Risiken unterstellt.
Ein wesentlicher Vorteil der Ausfalleffektanalyse ist die klare Formalisierung mit Hilfe von „Worksheets“ (Arbeitsblättern).	Es ist nicht sichergestellt, dass ähnlichen Risiken eine identische RPZ zugeordnet wird.
	Zeit- und Ressourcenverbreich hoch.
	Großer Datenbedarf und Systemkenntnisse erforderlich (Spezialisten-Know-how).
	Interdependenzen zwischen den einzelnen Komponenten des Gesamtsystems können (in der originären FMEA) nicht analysiert werden.
	Bei einer nur schwach ausgeprägten Fehler-/Risikokultur sind Manipulationen bei der qualitativen Bewertung sehr einfach möglich.

Die FMEA zielt darauf ab, Fehler von vornherein zu vermeiden, statt sie nachträglich zu entdecken und zu korrigieren, da dies in der Regel immer mit höheren Kosten verbunden ist. Um optimale Ergebnisse zu erzielen, sollte die FMEA bereits vor der Einführung eines potenziell fehlerträchtigen Produkts oder Prozesses vorgenommen werden.

Aufgrund der aufgezeigten Schwächen der FMEA befindet sich die Methode zurzeit massiv im Wandel (unter anderem auch durch die Arbeiten der Verbände AIAG und VDA). Durch eine Ergänzung anderer Methoden beziehungsweise eine Erweiterung etwa im Bereich der Bewertung, könnte die FMEA in der Zukunft eine größere Rolle in einem universellen Analysemodell spielen.

Bei der Bewertung der Möglichkeiten und Grenzen der FMEA sollte man sich vor allem ins Bewusstsein rufen, für welchen Zweck die FMEA ursprünglich entwickelt wurde. Die Ursprünge liegen im Bereich der Analyse von Fehlern in der Design- bzw. Entwicklungsphase neuer Produkte oder Prozesse. Mit der Analyse komplexer Systeme (etwa im Bereich eines Produktionsprozesses oder einer Supply Chain) ist die FMEA überfordert und bietet hier keinen bzw. einen nur geringen Nutzen.

6.5 Fehlerbaumanalyse (Fault Tree Analysis)

Mit Beginn der 1960er-Jahre wurden Techniken zur systematischen Analyse sicherheitskritischer Systeme entwickelt. Dazu gehören neben der Hazard and Operability Analysis (HAZOP) und der FMEA auch die *Fehlerbaumanalyse* (*fault tree analysis*, FTA). Sie wurde im Jahr 1961 in den Bell Telephone Laboratories entwickelt.[34]

So wurde beispielsweise in der Planungsphase des Apollo-Programms, bei dem zum ersten und bislang einzigen Mal Menschen auf den Mond gebracht wurde, die Frage gestellt, mit welcher Wahrscheinlichkeit Astronauten erfolgreich auf den Mond geschickt und sicher zur Erde gebracht werden können. Es wurde eine quantitative Risiko- oder Zuverlässigkeitsberechnung durchgeführt, und das Ergebnis war eine unannehmbar niedrige Wahrscheinlichkeit für den Erfolg der Mission. Die Ergebnisse entmutigte die NASA von weiteren quantitativen Risiko- oder Zuverlässigkeitsanalysen. Daher hat im Jahr 1963 die NASA die eher qualitativ ausgerichtete „Failure Mode and Effects Analysis“ (FMEA) für das Apollo-Projekt entwickelt und andere qualitative Methoden zur Bewertung der Systemsicherheit eingesetzt.[35]

Erst nach dem katastrophalen Unfall des Space Shuttles Challenger am 28. Januar 1986 hat die NASA die Bedeutung einer probabilistischen Risikobewertung (PRA) und einer quantitativen Risikoanalyse mit Hilfe einer Fehlerbaumanalyse erkannt. Bei der Katastrophe explodierte bereits 73 Sekunden nach dem Start die Raumfähre, in der Folge kamen alle sieben Besatzungsmitglieder ums Leben. Der Auslöser für die Explosion waren ein oder mehrere Dichtungsringe (O-Ringe) in einer der seitlichen Feststoffraketen (Booster). Durch ungewöhnlich tiefe Temperaturen in der Nacht vor und am Morgen des Starts büßte

[34] Vgl. Romeike (2018a, S. 81 ff.).

[35] Vgl. Romeike (2018b) und Romeike (2019c).

der Kunststoff der Dichtungsringe seine Elastizität ein, was durch die extremen Druck- und Hitzebelastungen nach der Zündung zunächst zu einem Verschleiß der O-Ringe und schließlich zum teilweisen Ausströmen des Verbrennungsgases führte (Blowby). Dies führte schließlich zur Explosion der Challenger und führte zur vorübergehenden Einstellung des Shuttle-Programms der NASA. Aus Sicht der Risikoanalyse ist erwähnenswert, dass bereits am Abend vor dem Start der Raumfähre, ein Ingenieur von Morton Thiokol, der Herstellerfirma der Feststoffraketen, wegen der Kälte vor dem Start, auf die potenziellen Risiken hingewiesen hatte.

Ein berühmtes Mitglied der Untersuchungskommission der Challenger-Katastrophe war der Physiker und Nobelpreisträger Richard P. Feynman, der detaillierte Erkenntnisse der Ursachen und Versäumnisse in einem Buch zusammengefasst hat.[36]

In der Folge des Challenger-Unfalls gilt die Fehlerbaumanalyse heute als eine der wichtigsten Techniken der Systemzuverlässigkeit und Sicherheitsanalyse in der Raumfahrt und in anderen Branchen.

Als internationaler Standard IEC 61025 (EN 61025) ist das Verfahren unter dem Begriff Fehlerzustandsbaumanalyse von der International Electrotechnical Commission beschrieben. In Deutschland ist die Fehlerbaumanalyse Inhalt der nationalen DIN 25424.[37]

Die Fehlerbaumanalyse basiert auf der booleschen Algebra[38] und dient dazu, die Wahrscheinlichkeit eines Ausfalls einer Anlage oder Gesamtsystems zu bestimmen. Die Fehlerbaumanalyse verfolgt das Ziel, durch die Analyse der logischen Verknüpfungen potenzielle Teilsystemausfälle auf allen kritischen Pfaden zu ermitteln, die zu einem Ausfall des Gesamtsystems führen können.

Die Fehlerbaumanalyse nimmt daher als Ausgangspunkt – im Gegensatz zur FMEA – nicht eine einzelne Systemkomponente, sondern das potenziell gestörte Gesamtsystem. Sie gehört zu den „Top-down"-Analyseformen (vgl. Abb. 6.9). In einem ersten Schritt wird daher das Gesamtsystem detailliert und exakt beschrieben. Darauf aufbauend wird analysiert, welche primären Störungen eine Störung des Gesamtsystems verursachen oder dazu beitragen können. Der nächste Schritt gliedert die sekundären Störungsursachen weiter auf, bis schließlich keine weitere Differenzierung der Störungen mehr möglich oder sinnvoll ist. Der Fehlerbaum stellt damit alle Basisergebnisse dar, die zu einem interessierenden Top-Ereignis führen können.

In der einfachsten Form besteht er aus den folgenden Elementen: Entscheidungsknoten (E), die Entscheidungen kennzeichnen, Zufallsknoten, die den Eintritt eines zufälligen Ereignisses darstellen sowie aus Ergebnisknoten (R), die das Ergebnis von Entscheidungen oder Ereignissen darstellen. Zwischen diesen Elementen befinden sich Verbindungslinien

[36] Vgl. Feynman (1996).

[37] Fehlerbaumanalyse, Teil 1: Methode und Bildzeichen, Teil 2: Handrechenverfahren zur Auswertung eines Fehlerbaumes.

[38] Die boolesche Algebra ist eine spezielle algebraische Struktur, die die Eigenschaften der logischen Operatoren UND ($\wedge$), ODER ($\vee$), NICHT ($\neg$) sowie die Eigenschaften der mengentheoretischen Verknüpfungen Durchschnitt ($\sqcap$), Vereinigung ($\sqcup$ oder *), Komplement ($\circ$) verallgemeinert.

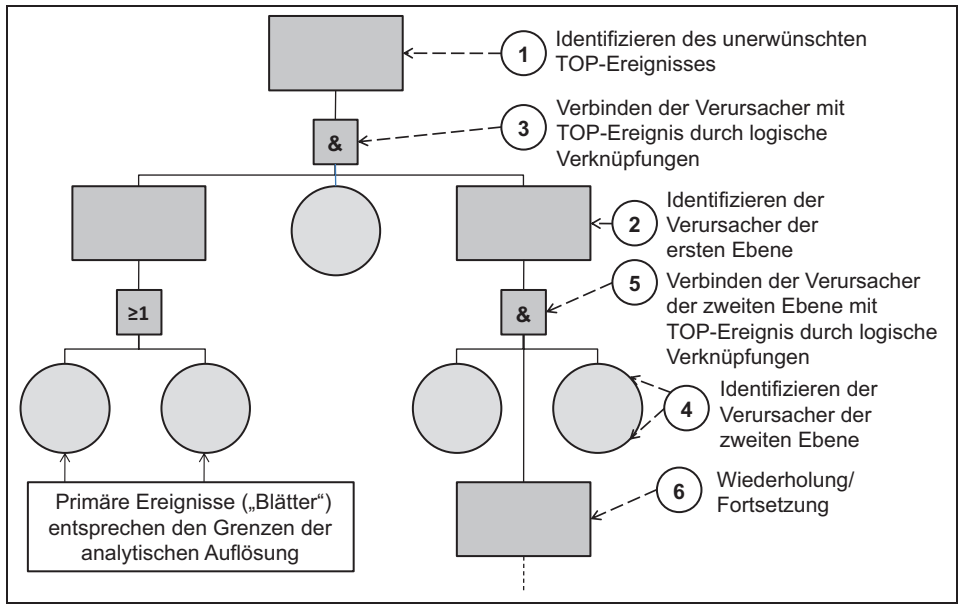


Abb. 6.9 Vorgehensweise zur Konstruktion eines Fehlerbaumes (Vgl. Romeike 2018a, S. 82)

Komplexe Fehlerereignisse werden mittels logischer Verknüpfung (booleschen Algebra; auch als boolescher Verband bezeichnet) weiter in einfachere Ereignisse aufgeteilt. Verknüpfungen lassen sich grundlegend in zwei Kategorien einteilen: in Oder-Verknüpfungen, bei denen der Fehler auftritt, falls eines der Ereignisse auftritt, sowie in Und-Verknüpfungen, bei denen der Fehler nur auftritt, falls alle Ereignisse auftreten. Ein Block-Gatter führt zwischen einem Ereignis und der entsprechenden Ursache eine Nebenbedingung ein.

Die Nebenbedingung muss zusätzlich zur Ursache vorhanden sein, damit die Wirkung eintritt. Die Bedingung beschreibt Ereignisse, die keine Fehler oder Defekte sind und im Normalbetrieb auftreten. Um einen großen Fehlerbaum anschaulich zu präsentieren, können ganze Unterbäume durch ein Transfer-Symbol markiert und separat analysiert werden. Die im Fehlerbaum definierten Ursachen sind Zwischenereignisse, die weiter untersucht werden, bis ein gewünschter Detaillierungsgrad erreicht wird. Ursachen, die nicht weiter untersucht werden, sind Blätter im Fehlerbaum. Blätter sind entweder Basisereignisse des Systems oder Ereignisse, die für die Analyse (noch) nicht detailliert genug beschrieben wurden (nicht untersuchte Ereignisse).

In Abb. 6.9 ist ein Beispiel für einen Fehlerbaum dargestellt. In Abb. 6.10 sind die grundlegenden Symbole im Zusammenhang mit der Fehlerbaumanalyse skizziert.

Eine wesentliche Eigenschaft der Ereignisse in einem Fehlerbaum ist, dass sie unerwünscht sind. Sie beschreiben Fehlerzustände, Störungen oder Ausfälle. Nach Erstellung des Fehlerbaums wird bei der quantitativen Fehlerbaumanalyse jedem Basisereignis eine bestimmte Eintrittswahrscheinlichkeit für den Ausfall zugewiesen.

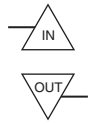
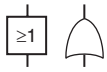
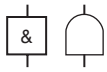
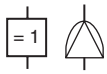
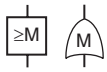
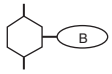
Symbol(e)	Name	Bedeutung
	Top/Zwischen-ereignis	Ein Ereignis, das aus der Interaktion mehrerer Ereignisse durch eine logische Verknüpfung resultiert, u.a. das *unerwünschten Ereignis* (Top Event) und die *Zwischenereignisse* (Intermediate Events).
	Primäres Ereignis	Ein *Primäres Ereignis* (PE) repräsentiert den Ausfall einer Komponente oder einen Bedien-Fehler. Es wird nicht weiter aufgegliedert und stellt somit die feinste Auflösung des Fehlerbaums dar.
	Unentwickeltes Ereignis	Mit der Raute werden fehlerhafte Ereignisse symbolisiert. die nicht weiter aufgegliedert werden, da keine näheren Details bekannt sind order die weitere Verfeinerung des Fehlerbaums nicht erwünscht ist.
	Transfer Symbole	Das Dreick wird benutzt, um (Teil-) Bäume zu verbinden. Das IN-Symbol signalisiert den Input von einem anderen Baum (in der Regel auf einer neuen Seite). Und das OUT-Symbol erscheint an der Position des Top Event und bedeuter, dass diese Stelle den Input für einen anderen Baum liefert.
	ODER-Verknüpfung	Bei der ODER-Verknüpfung tritt das Ausgangsereignis ein, sobald mindestens ein Eingangsereignis eingetreten ist. Die ODER-Verknüpfung kann beliebig viele Eingänge haben.
	UND-Verknüpfung	Der Ausgang der UND-Verknäpfung ist genau dann wahr, wenn alle seine Eingänge wahr sind. Die Anzahl der Eingänge ist beliebig.
	X-ODER-Verknüpfung	Die X-ODER-Verknüpfung ist wahr, wenn genau einer der Eingänge wahr ist. Die Anzahl der Eingänge ist beliebig.
	X-ODER-Verknüpfung	Die M-VON-N-Verknüpfung ist wahr, wenn mindestens M der N Eingänge wahr sind. Die Anzahl der Eingänge ist beliebig.
	Bedingte Verknüpfung	Das Ausgangsereignis der bedingten Verknüpfung tritt ein, wenn des Eingangsereignis eintritt und die Bedingung B erfüllt ist.

Abb. 6.10 Symbole im Rahmen der Fehlerbaumanalyse (Vgl. Schwindt 2004)

In der Praxis ist der Einsatz von Fehlerbaum-Techniken oft auch gemeinsam mit Szenariotechniken und mit Ereignisbaum-Techniken zu beobachten. Letzterer Ansatz verfolgt das Ziel, dass alle Faktoren identifiziert werden, die zu einem Störfall führen können. Die Darstellung erfolgt ebenfalls als Baum.

Bei einer rein qualitativen Analyse (vgl. Abb. 6.9) werden die kausalen Zusammenhänge in einem System analysiert und grafisch dargestellt. Hierbei steht die Frage im Mittelpunkt, welche Komponenten besonders kritisch für das Gesamtsystem sind? Von

besonderem Interesse sind dabei der sogenannte „Single point of failure“ (SPOF). Hierunter versteht man eine besonders kritische Komponente. Wenn diese Komponente ausfällt, tritt das Top-Ereignis ein (siehe Dichtungsring und Explosion der Challenger). Insbesondere in der Luftfahrt ist die Vermeidung von „Single points of failure“ von herausragender Bedeutung.

Außerdem werden sogenannte „Cut Sets“ analysiert. Hierbei handelt es sich um Kombinationen von Komponenten, die alle gemeinsam ausfallen müssen, damit es zum Eintritt des Top-Ereignisses kommt.

Des Weiteren werden „Minimal Cut Sets“ analysiert. Hierbei handelt es sich um Systeme mit wenigen Komponenten und bereits der Ausfall einer Komponente ist ausreichend für den Ausfall des Gesamtsystems.

Bei der quantitativ ausgerichteten Fehlerbaumanalyse werden den einzelnen Ursachen Wahrscheinlichkeiten zugeordnet, die anschließend über bedingte Wahrscheinlichkeiten (auch konditionale Wahrscheinlichkeit) im Detail bewertet werden. Resultierend aus den Axiomen von Kolmogorow[39] gilt bei einer UND-Verknüpfung zweier unabhängiger Ereignisse:

$$P(A \cap B) = P(A) \cdot P(B)$$

Bei einer ODER-Verknüpfung für sich ausschließende (inkompatible) Ereignisse gilt:

$$P(A \cup B) = P(A) + P(B)$$

Bei einer ODER-Verknüpfung für unabhängige Ereignisse gilt:

$$P(A \cup B) = P(A) + P(B) - P(A) \cdot P(B)$$

Bei einer XOR-Verknüpfung[40] für unabhängige Ereignisse gilt:

$$P(A \cup B) = P(A) + P(B) - 2 \cdot P(A) \cdot P(B)$$

Die Fehlerbaumanalyse wird beispielsweise für die folgenden Fragestellungen eingesetzt:

- In der Planung von Industrieanlagen, vor allem in der Verfahrenstechnik, und im vorbeugenden Brandschutz.
- In der Software-Entwicklung wird sie verwendet, um die Fehler von Programmen zu analysieren.

[39] Benannt nach dem russischen Mathematiker Andrei Nikolajewitsch Kolmogorow.

[40] Hierbei handelt es sich um eine exklusiv-ODER-Verknüpfung (auch XOR Antivalenz Kontravalenz; von engl. e*X*clusive *OR* – exklusives Oder, entweder oder). Die Gesamtaussage ist dann wahr wenn entweder die erste Aussage oder die zweite Aussage wahr ist aber nicht beide.

Tab. 6.3 Stärken und Grenzen der Fehlerbaumanalyse. (Quelle: Romeike 2018a, S. 85)

Stärken	Grenzen
Baumstruktur ermöglicht klar strukturierte systematische Untersuchung.	Ermittelt „nur“ die Ausfallwahrscheinlichkeiten – basierend auf „einfacher“ boolescher Algebra.
Relativ einfache Analyse von Teilsystemausfällen auf allen kritischen Pfaden durch logische Verknüpfungen.	Vollständigkeit des Fehlerbaums ist nicht garantiert (insbesondere bei komplexen Systemen).
Kann als Methode für die Ursachenanalyse im Rahmen der Bow-tie Analysis genutzt werden.	Detailliertes Strukturwissen erforderlich.
ISO- und DIN-Standardisierung.	Nur bei einfachen Systemen übersichtlich.
Viele Umsetzungsbeispiele in diversen Branchen.	Keine Abbildung von Komponenten mit mehr als zwei Zuständen möglich.

- In der Flugsicherheit werden zur Bestimmung der definierten Sicherheit Fehlerbaumanalysen mittels Checklisten ausgeführt.
- In der Produktentwicklung, vor allem in der Automobilindustrie.
- Im Rahmen der PSÜ (Periodische Sicherheitsüberprüfung) für kerntechnische Anlagen, um die Wahrscheinlich für den Ausfall eines sicherheitstechnischen Systems angeben zu können.

In Tab. 6.3 sind die wesentlichen Stärken und Grenzen der Fehlerbaumanalyse zusammengefasst.

6.6 Bow-Tie-Analyse

Die Bow-Tie-Analyse eignet sich nahezu perfekt zur strukturierten Darstellung und Analyse von Risiken im Bereich der Produktion. Bereits in den frühen neunziger Jahren übernahm die Royal Dutch Shell Group die Bow-Tie-Analyse als Methode und Unternehmensstandard für die Analyse und das Management von Risiken. Später übernahmen weitere Unternehmen aus der Öl- und Gasindustrie sowie aus der Luftfahrtindustrie, dem Schienenverkehr, der Schifffahrt und im Chemie- und Gesundheitswesen die Bow-Tie-Analyse als Standard zur Strukturierung und Analyse von Risiken. Das Vorgehen sowie der Methode wurde bereits im Kap. 3 beschrieben.

Ein wesentlicher Mehrwert der Die Bow-Tie-Analyse liegt darin, dass Elemente verschiedener anderer Methoden vereint werden.[41] Dazu zählen insbesondere die

- Fehlerbaumanalyse (Fault Tree Analysis, FTA),
- die Ereignisbaumanalyse (Event Tree Analysis),

[41] Vgl. de Ruijter und Guldenmund (2016, S. 211–212) sowie Romeike und Spitzner (2013, S. 134–135).

- die Barrier Analysis sowie
- die Ursache-Wirkungs-Diagramme (Cause and Effect Diagram bzw. Ishikawa-Diagramm).

Die Methode wird in der Praxis dazu verwendet, ein Risiko sowie dessen Ursachen und Wirkungen zu identifizieren und in einem einzigen Diagramm strukturiert darzustellen (vgl. Abb. 6.11. Da ein Risiko in der Regel eine Vielzahl von Ursachen, aber auch Wirkungen aufweist, hat das Diagramm die Form einer Fliege (im Englischen: bow tie). Es unterstützt damit die Risikoidentifikation, aber auch die Risikokommunikation und die Entwicklung von Maßnahmen zur Risikosteuerung. Die Ursachen können mittels der Fehlerbaumanalyse (Fault Tree Analysis), die Wirkungen mittels der Ereignisbaumanalyse (Event Tree Analysis) erarbeitet werden. Wenn (quantitative) Daten zu Ursachen und Wirkungen verfügbar sind, kann die Bow-tie Analysis auch zur Risikobewertung genutzt werden.

Die Bow-tie Analysis integriert einzelne Elemente der oben genannten vier Methoden. In Abb. 6.12 ist am Beispiel der Nuklearkatastrophe von Fukushima vom 11. März 2011 und der Reihe von katastrophalen Unfällen und schweren Störfällen im japanischen

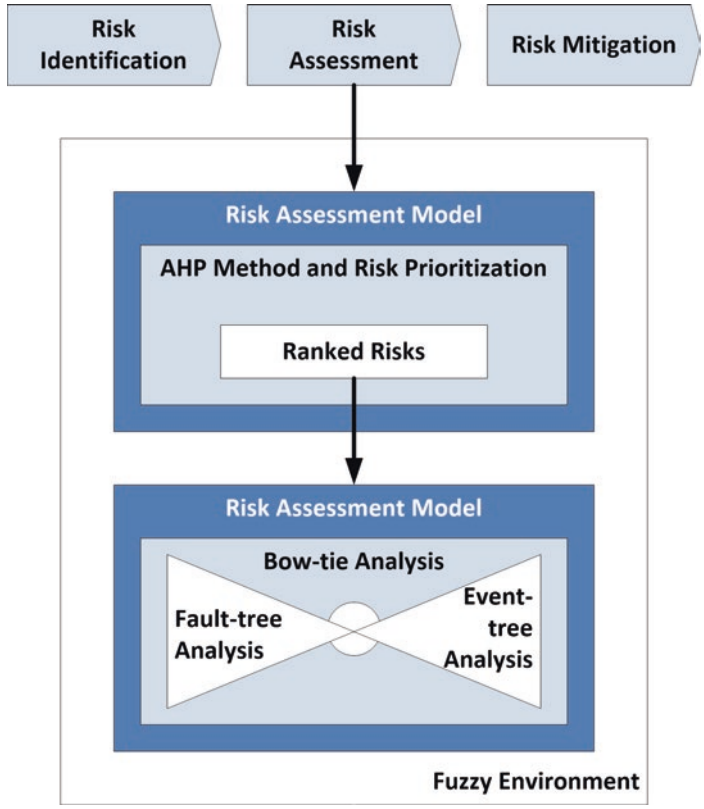


Abb. 6.11 Bow-Tie-Analyse. (Quelle: Romeike (2018a, S. 77) in Anlehnung an Mokhtari et al. (2011) und Mokhtari et al. (2012))

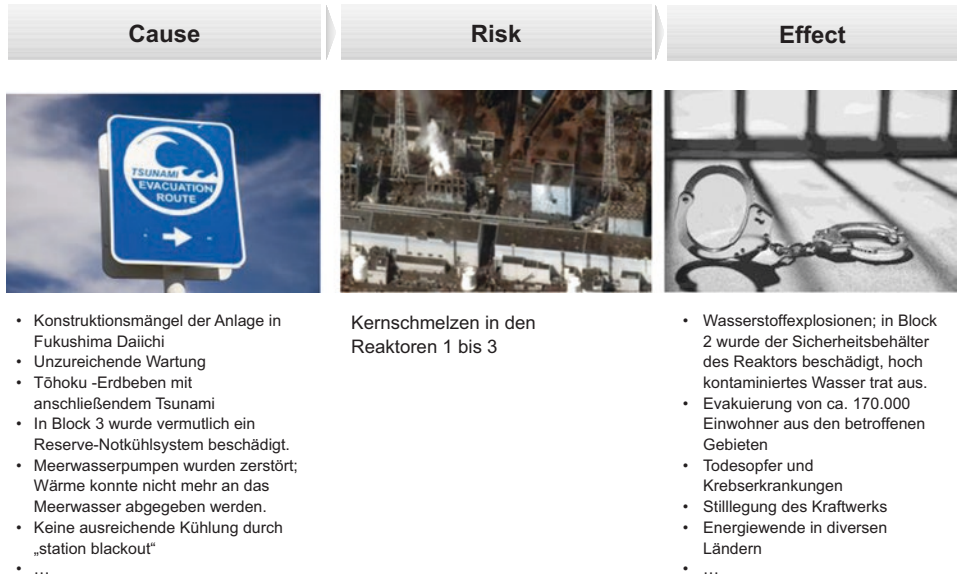


Abb. 6.12 Konkretes Praxisbeispiel: Nuklearkatastrophe von Fukushima vom 11. März 2011. (Quelle: Romeike 2019b, S. 43)

Kernkraftwerk Fukushima Daiichi (Fukushima I) eine Auswahl an Ursachen (Causes), Risiken (Risks) und Wirkungen (Effects) dargestellt. Die Übersicht vereinfacht stark und ist nicht als abschließend zu betrachten, da das Ursache-Wirkungsgeflecht im konkreten Fall um ein Vielfaches komplexer war.

Die Bow-tie Analysis wird aus den folgenden Elementen gebildet:[42]

- **„Top Event“ bzw. Risiko**, konkret im Kontext Risiko-Management die potenzielle Ziel-/Planabweichung: Das zentrale (unerwünschte) Ereignis, für das Ursachen und Wirkungen identifiziert werden sollen.
- **Ursachen (Causes):** Auf der linken Seite des „Top Events“ werden die identifizierten Ursachen für das unerwünschte Ereignis dargestellt. Dies kann mittels eines Ursache-Wirkungs-Diagramms oder mittels einer Fehlerbaumanalyse geschehen.
- **Wirkungen (Effects):** Auf der rechten Seite des „Top Events“ werden die möglichen Wirkungen des unerwünschten Ereignisses dargestellt. Auch hier kann ein Ursache-Wirkungs-Diagramm genutzt werden, alternativ aber auch eine Ereignisbaumanalyse. Die Anwendung von Fehlerbaum- und Ereignisanalyse unter Nutzung quantitativer Daten ermöglicht es, die Bow-tie Analysis auch zur Risikobewertung zu nutzen. Ein derartiger Ansatz wird beispielsweise bei Ferdous et al.[43] dargestellt; er wird durch die Anwendung der Fuzzy-Theorie erweitert.

[42] Vgl. de Ruijter und Guldenmund (2016, S. 213) sowie Romeike (2018a, S. 75 f.).

[43] Vgl. Ferdous (2013).

- **Schwellen (Barrier):** Sowohl links als auch rechts des „Top Events“ werden sogenannte Barrier platziert. Damit sind Schwellen oder Sperren gemeint, mit denen (dann bereits im Sinne einer Risikobewältigung) versucht wird, den Eintritt des unerwünschten Ereignisses und/oder die Wirkungen zu vermindern oder zu vermeiden. Die „Barrier“ im Bereich der Ursachen sind sogenannte präventive oder ursachenbezogene Maßnahmen. Die „Barrier“ im Bereich der Wirkungen sind reaktive Maßnahmen bzw. wirkungsbezogene Maßnahme, die beispielsweise die finanziellen Wirkungen abmildern (etwa in Form eines abgeschlossenen Versicherungsvertrags).
- **Management-System:** Teilweise werden die in Verbindungen stehenden Management-Systeme ebenfalls in das Diagramm eingezeichnet.

Es existieren verschiedene Variationen der Bow-Tie-Analyse, die davon abhängen, zu welchem Zweck die Analyse genutzt werden soll (Risikoidentifikation, Risikobewertung, Risikokommunikation) und aus welchen konkreten Elementen das Diagramm besteht bzw. welche Methoden angewandt werden.

Die Anwendung der Bow-tie Analysis kann begleitet werden durch weitere analytische Methoden, beispielsweise die „Analytic Hierarchy Method“ für die Priorisierung der Risiken oder eine Kritikalitätsbewertung basierend auf einem Scoringansatz (vgl. Abb. 6.13). Hierbei erfolgt beispielsweise die Bewertung der Kritikalität über einen Scoringansatz (beispielsweise mit Hilfe von Scorewerten von 1 bis 5). Die Kritikalität basiert immer auf der Bewertung der Wirkung der identifizierten Szenarien. In einem zweiten Schritt erfolgt die Bewertung nach „Ability to act“, d. h. welche präventiven oder auch reaktiven Maßnahmen überhaupt ergriffen werden können, um den Risikoeintritt zu verhindert oder die Wirkung zu reduzieren. Anschließend können die Risikoszenarien in einer einfachen Grafik visualisiert werden.

Ursache (Cause)	Risiko (Risk)	Wirkung (Effect)	Kritikalität (1-5)	Ability to Act (1-5)

Abb. 6.13 Scoringbasierte Ansatz zur pragmatischen Bewertung von Kritikalität und „Ability to act“. (Quelle: Eigene Abbildung)

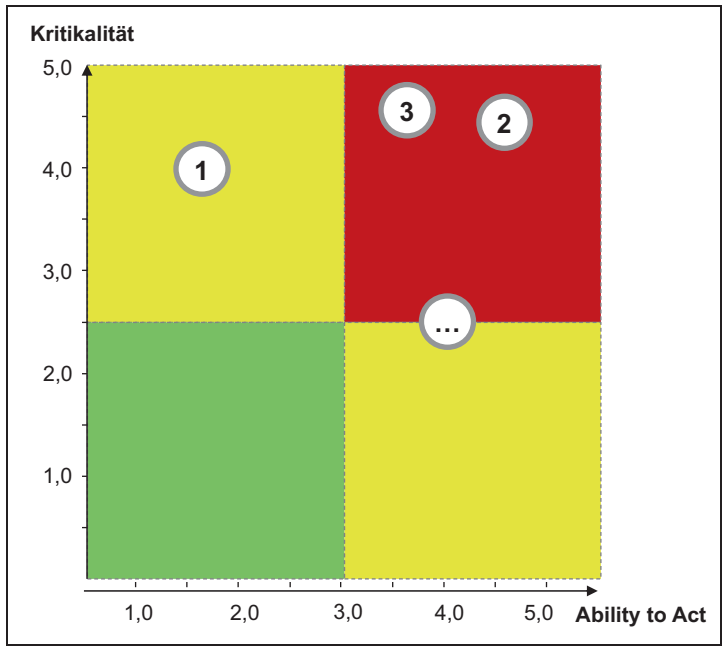


Abb. 6.14 Visualisierung der identifizierten Risiken nach Kritikalität und „Ability to act". (Quelle: Eigene Abbildung)

In einem weiteren Schritt sollten für alle kritische Szenarien detaillierte Maßnahmenpakete definiert werden. Zu diesem Zweck sollten die einzelnen Szenarien noch einmal im Detail analysiert werden und mit Hilfe geeigneter quantitativer Methoden (bspw. „worst case", „realistic case" und „best case" sowie ggf. Schätzung der Häufigkeit) bewertet werden (Abb. 6.14).

Die wesentlichen Stärken und Schwächen der Bow-Tie-Analyse sind in Tab. 6.4 zusammengefasst.

6.7 Key Risk Indicator, Key Performance Indicator, Key Control Indicator

Ein *Risikoindikator* bzw. *Key Risk Indicator* ist mit dem menschlichen Nervensystem vergleichbar. Es registriert Veränderungen innerhalb eines Organismus und löst Warnungen aus. Wenn die „Schmerzgrenze" überschritten ist, reagiert der Körper und versucht die negative Situation zu ändern, damit die Schmerzen eliminiert oder reduziert werden.

So basieren Frühwarnsysteme im Bereich des Katastrophenschutzes auf einer Sammlung von Umweltdaten (etwa Temperatur oder Schwingungen), die über viele Sensoren

Tab. 6.4 Stärken und Schwächen der von Bow-Tie Analysis. (Quelle: Romeike 2018b, S. 81)

Stärken	Schwächen
Strukturierte Methodik zur korrekten Abgrenzung von Ursachen, Risiken/Chancen und Wirkungen.	Komplexe Ursache-Wirkungszusammenhänge können nur sehr eingeschränkt abgebildet werden (komplexe Feedback-Loops und nicht lineare Abhängigkeiten).
Transparente und intuitive Visualisierung von Ursachen, Ereignissen und Effekten.	Wirkungen bilden oft die Ursache für andere „Top Events“. Dies kann im Bow-Tie-Diagramm nur sehr eingeschränkt abgebildet werden.
Bow-tie Analysis fördert ein strukturiertes Denken (Transparenz der Ursache-Wirkungs-Zusammenhänge).	
Eine gute strukturierte Bow-tie Analysis bietet eine exzellente Basis für die Definition von Frühwarnindikatoren bzw. Key Risk Indicator (ganz links in der Ursachenketten).	
Grafische Darstellung auch zur Risikokommunikation geeignet.	
Gute Verbindungsmöglichkeiten zu anderen – vor allem analytischen – Methoden.	
Auch präventive und reaktive Maßnahmen (Barrier) können in der Bow-tie Analysis abgebildet werden.	

erfasst werden. Die Messwerte der Sensoren werden fortlaufend auf Unregelmäßigkeiten überprüft. Beim Überschreiten definierter Schwellenwerte wird ein Alarm oder eine automatische Reaktion ausgelöst. So lassen sich Züge stoppen, Brücken sperren und Gasleitungen abdrehen.[44] Das wohl am meisten verbreitete Frühwarnsystem findet sich im Bereich des Brandschutzes. Dort werden mit Hilfe von Rauchdetektoren, Feuermeldern, Brandschutztüren, Sprinklern und Sirenen beim Überschreiten definierter Schwellenwerte Brände rechtzeitig gemeldet und größere Schäden somit vermieden. Nichts anderes im Bereich der Wirtschaft: Auch dort soll über Sensoren bzw. Frühwarnindikatoren rechtzeitig darauf hingewiesen werden, ob ein Unternehmen möglicherweise in „gefährliche Gewässer segelt“ oder ein „Leck in der Bordwand“ zu einem existenzbedrohenden Ungleichgewicht führt. Die Beachtung von Frühwarnindikatoren im Bereich der Wirtschaft war immer schon ein wichtiges unternehmenspolitisches Instrument zur Erreichung der Unternehmensziele.

Unternehmen hatten sich in der Vergangenheit nicht selten vor allem auf ihr „Bauchgefühl“ verlassen und auf Risiken primär situativ bzw. retrospektiv reagiert. Frühwarnsysteme bzw. Risiko-Management hat per definitionem jedoch nicht das Ziel, die Vergangenheit

[44] Vgl. Romeike (2005a, S. 22–27).

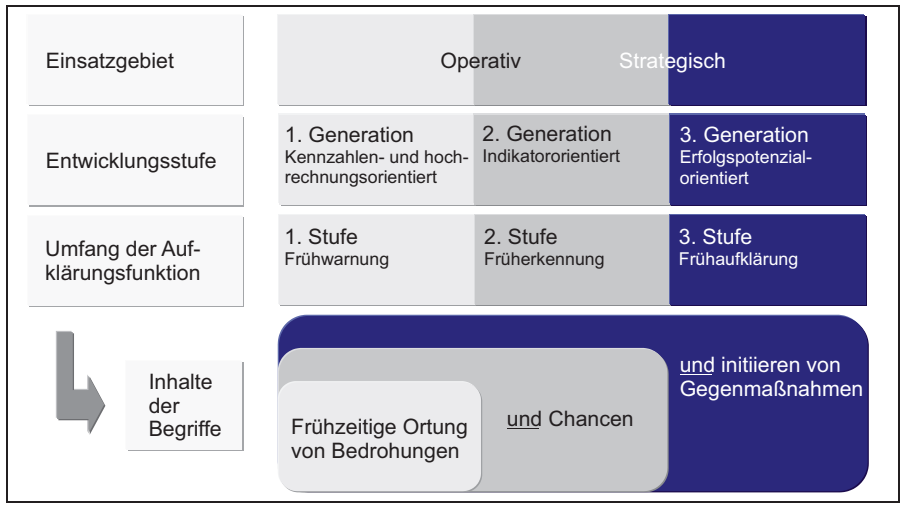


Abb. 6.15 Typologisierung von Frühaufklärungsansätzen (In Anlehnung an Krystek und Müller-Stewens 1993, S. 26)

zu erklären, sondern will zukünftige Chancen und Risiken antizipieren und helfen, bessere Antworten auf bessere Fragen zu finden. Risiko-Management sollte daher proaktiv (oder auch prospektiv) ausgerichtet sein.

Allgemein können drei unterschiedliche Arten bzw. Generationen von Frühaufklärungssystemen unterschieden werden (vgl. Abb. 6.15):

- Kennzahlen- und hochrechnungsorientierte,
- Indikatororientierte und
- Strategische Frühaufklärungssysteme.

Kennzahlen- und hochrechnungsorientierte Frühaufklärungssysteme basieren auf einem periodischen Vergleich von Kennzahlen bzw. auf innerjährlichen Hochrechnungen von Über- und Unterschreitungen bestehender Jahrespläne (Budgets) und eignen sich daher vor allem für das operative Controlling.[45] Hierbei werden insbesondere Soll-Ist-Zahlen bzw. Soll-Wird-Zahlen verglichen. Beim Unter- bzw. Überschreiten definierter Schwellenwerte sollen adäquate Warnmeldungen ausgelöst werden. Kritisch ist hierbei anzumerken, dass kennzahlen- und hochrechnungsorientierte Frühaufklärungssysteme auf vergan-

[45] Vgl. Romeike (2006, S. 453 ff.).

genheitsorientierten Daten basieren und eine längerfristige Früherkennung von Chancen und Risiken nicht möglich ist.

Zentrale Elemente von *indikatororientierten Frühaufklärungssystemen* sind Indikatoren (leading indicators), die Informationen über die zukünftige Entwicklung der Umweltveränderungen im unternehmensinternen und externen Bereich liefern.[46] Die Definition und Erhebung von Indikatoren sollte sinnvollerweise im Rahmen von existierenden Planungs- und Berichtssystemen bzw. im Zusammenhang mit einer implementierten Balanced Scorecard erfolgen. Die größte Herausforderung bei indikatorbasierten Frühaufklärungssystemen besteht bei der Selektion geeigneter Indikatoren, da Kausalzusammenhänge in einer komplexen Wirtschaftswelt nur selten über singuläre und statische Indikatoren erklärt werden können. Indikatoren spiegeln nicht selten lediglich die bisherigen Erfahrungen und Kenntnisse wider und blenden potenzielle neue Entwicklungen und Kausalitäten aus. Adäquate Indikatoren müssen insbesondere eindeutig, vollständig und rechtzeitig verfügbar sein, frühzeitig auf zukünftige Entwicklungen hinweisen sowie unter ökonomischen Gesichtspunkten sinnvoll erfasst werden können. In den vergangenen Jahren haben insbesondere global operierende Konzerne große Anstrengungen unternommen, um adäquate (Key)-Risk-Indikatoren zu definieren und zu erfassen.

Strategischen Frühaufklärungssystemen liegt das Konzept der schwachen Signale von Ansoff zugrunde.[47] Ansoff geht davon aus, dass tief greifende Umbrüche (etwa im ökonomischen, sozialen und politischen Bereich) nicht zufällig ablaufen, sondern sich lange im Voraus durch schwache Signale (weak signals) ankündigen. Oft handelt es sich um Informationsrudimente, das heißt unscharfe und wenig strukturierte Informationen, wie beispielsweise Gefühle, dass mit Bedrohungen bzw. Chancen zu rechnen ist (etwa basierend auf Presseberichten, Studien von Zukunftsforschungsinstituten, Informationen aus Diskussionsforen im Internet oder Informationen bezüglich der allgemeinen wirtschaftlichen Entwicklung), nur vagen Informationen über mögliche Quellen und Ursachen latenter Gefahren, nur vagen Informationen bzgl. konkreter Bedrohungen und Chancen, aber klarer Vorstellung hinsichtlich strategischer Relevanz. Schwache Signale verstärken sich häufig im Zeitablauf und weisen immer stärker auf Trend-/Paradigmawechsel hin.

Nach Ansoff gibt es unerwartete Diskontinuitäten nur, weil die Empfänger dieser Signale nicht darauf reagieren. Zur Vorbeugung von strategischen „Überraschungen" müssen schwache Signale rechtzeitig geortet werden. Dies bedingt eine Sensibilisierung aller Mitarbeiter für schwache Signale, da mit zunehmender Konkretisierung der Signale die Reaktionsfähigkeit des Unternehmens abnimmt. Insbesondere erfordert die Umsetzung des Konzepts von schwachen Signalen eine Abkehr von starren und streng hierarchisch strukturierten Denk- und Organisationsstrukturen. Frühaufklärungssysteme der dritten Generation werden auch unter dem Begriff des *„strategischen Radars"* bzw. *„360-Grad-Radar"* zusammengefasst, da das Ortungssystem offen und ungerichtet ist. Das „strategische Ra-

[46] Vgl. Romeike (2006, S. 453 ff.).

[47] Vgl. Krystek und Müller (1999, S. 181 ff.) sowie Ansoff (1976, S. 129–152).

dar“ verwendet vor allem die Instrumente des „Scanning“ und „Monitoring“. Ersteres stellt ein ungerichtetes Abtasten des gesamten Unternehmensumfeldes dar und bezweckt das Erkennen trendartiger Entwicklungen. Diese werden im Rahmen des Monitorings gezielteren und tief greifenderen Analysen unterzogen.

Ziel dabei ist es, möglichst viele unscharfe Signale zu empfangen, die erst in einem weiteren Schritt hinsichtlich ihres Verhaltens- bzw. Ausbreitungsmuster sowie ihrer Ursachen und Wirkungen analysiert werden. In einem weiteren Schritt wird die Relevanz der analysierten Signale beurteilt und hinsichtlich ihrer Dringlichkeit in eine Rangordnung gebracht. Erst in einem abschließenden Schritt werden adäquate Reaktionsstrategien entwickelt und umgesetzt. Bei der Analyse von strategischen Frühaufklärungssystemen können Instrumente aus dem strategischen Marketing (Erfahrungskurve, Produktlebenszyklus etc.) und auch andere etablierte und praxiserprobte Methoden (Szenario-Technik, Portfoliomethode, Delphi-Verfahren, Trend-Impact-Analyse etc.) verwendet werden.

Die Eigenschaften eines guten Risikoindikators können wie folgt beschrieben werden:

- Ein Risikoindikator wird regelmäßig gemessen.
- Ein Risikoindikator sollte das Risiko reflektieren.
- Ein Risikoindikator benötigt Schwellenwerte, die definieren, ab wann korrigierende Aktionen und Maßnahmen eingeleitet werden sollen.
- Ein Risikoindikator wird zeitnah gemessen.
- Ein Risikoindikator zeigt die Veränderungen des Risikoprofils präventiv an, bevor bestimmte Ereignisse akut werden.
- Ein Risikoindikator sollte effizient gemessen werden.

Die regelmäßige Messung ist eine Voraussetzung für die Erkennung von ungünstigen Trends. Darüber hinaus hängt es von der verbleibenden Reaktionszeit nach einer Warnmeldung ab, wie oft gemessen werden muss. Wenn die Reaktionszeit kurz ist, muss die Messfrequenz entsprechend hoch sein. Wenn die Reaktionszeit sehr lang ist und trotzdem mit einer hohen Messfrequenz gemessen wird, kommt es sehr leicht zur Vernachlässigung der Warnmeldungen. In solchen Fällen würde das Ziel der Implementierung von Risikoindikatoren geradezu verfehlt.

In einem nächsten Schritt müssen für den Risikoindikator Schwellenwerte definiert werden. Unternehmen und Unternehmenslenker sind daran interessiert zu erfahren, wann eine Situation gefährlich oder gar kritisch wird. Oftmals werden diese Situationen mit Ampelfarben abgebildet. Die Schwellenwerte müssen für jeden Risikoindikator individuell bestimmt werden. In der Unternehmenspraxis sind regelmäßig die Risikoindikatoren mit einer „Warnmeldefunktion“ verknüpft, die nach einer Überschreitung der festgelegten Schwellenwerte den verantwortlichen Personenkreis informiert.

Ein Risikoindikator soll *zeitnah* gemessen werden. Die Messfrequenz wird durch die notwendige Reaktionszeit und durch die zu erwartende Schadenshöhe bestimmt. Die Bestimmung wird unter der Randbedingung der Wirtschaftlichkeit optimiert.

Es scheint so selbstredend, dass die Risikoindikatoren die *Veränderungen im Risikoprofil* abbilden sollen. Die Erfüllung dieser Anforderung ist in der Praxis keineswegs so trivial, wie vermutet werden könnte. Dass Risiko-Indikatoren effizient gemessen werden sollen, ist eher eine Randbedingung als eine funktionale Eigenschaft.

In der Folge der rasanten Entwicklungen in den Bereichen Artificial Intelligence (AI), Big Data, Datenanalysen und Predictive Analytics haben sich in den vergangenen Jahren die Möglichkeiten zur Früherkennung von potenziellen Risiken und schwachen Frühwarnindikatoren massiv verbessert.

Bereits heute wissen wir, dass sich aus Facebook- und Twitter-Nachrichten politische Einstellungen ableiten lassen und diese Informationen auch genutzt werden.[48] Aus Daten und Algorithmen sollen sich potenzielle Straftaten antizipieren lassen, bevor sie überhaupt geplant oder begangen wurden.[49] Beispielsweise hat der Streaming-Dienst Netflix mit Unterstützung von Predictive Analytics sehr treffsicher prognostiziert, wie die richtige Mischung aus Drama, Witz und Liebe in einer Geschichte aussehen muss, damit ein Film erfolgreich ist. Die Grundlage hierfür bildeten die Daten über das Zuschauerverhalten. Bereits seit einiger Zeit schätzen Kreditinstitute mit Hilfe eines Kredit-Scorings das Risiko ab, mit dem eine Person oder ein Unternehmen die zukünftigen Ratenzahlungen eines Kredits nicht leisten könnte. Und auch Erst- und Rückversicherungen prognostizieren über Data Mining und Predictive Analytics zukünftige Schäden.[50] Und der Datentsunami nimmt weiter zu und damit auch die Möglichkeiten hieraus Muster und Frühwarnindikatoren abzuleiten. Möglicherweise werden wir schon bald erkennen, dass Milliarden von Informationen unterschiedlicher Qualität sinnvoller sind als wenige, dafür aber akkurate Daten.

Doch es sind nicht nur die schieren Datenmengen, die einen Boom im Kontext Artificial Intelligence und maschinelles Lernen hervorgerufen haben. Ein weiterer Treiber liegt in der Miniaturisierung der leistungsfähigen Mikroprozessoren, die heute in jedem Smartphone stecken. Seit dem Jahr 1994 ist die Zahl der Bauelemente auf einem Mikrochip um mindes-

[48] So wurde im Jahr 2018 bekannt, dass das inzwischen insolvente britische Beratungsunternehmen Cambridge Analytica die Daten von 87 Millionen Facebook-Nutzern weitergegeben hatte, die unter anderem für Manipulationen im Wahlkampf von Donald Trump verwendet wurden. Vgl. https://www.washingtonpost.com/technology/2019/02/14/us-government-facebook-are-negotiating-record-multi-billion-dollar-fine-companys-privacy-lapses/ (abgerufen am 1. August 2019). Christopher Wylie, ein früherer Mitarbeiter bei Cambridge Analytica, kam auch die Entscheidung der Briten für den Brexit durch gezielte Wählermanipulation über Facebook zustande: „Ich glaube nicht, dass der Brexit geschehen wäre, hätte es nicht die von Cambridge Analytica entwickelte Datentechnologie und das Netzwerk von Handelnden gegeben“, sagte Wylie bei einer Anhörung im Europaparlament.

[49] Romeike und Eicher (2016) sowie Romeike (2019a, S. 56 ff.).

[50] Vgl. Schiller (2019).

tens den Faktor 10.000 gestiegen und parallel dazu die Rechenleistung. Die stärksten Supercomputer konnten Mitte der 1990er-Jahre etwa 100 Milliarden Rechenoperationen pro Sekunde bewältigen – das schafft heute jedes gute Smartphone.[51] Und zugleich sank der Stromverbrauch auf weniger als ein 100.000stel. Gleichzeitig hat jedes Smartphone und jedes Auto eine Vielzahl von Sensoren: hochauflösende Kameras, Rotations- und Beschleunigungssensoren, Messgeräte für Magnetfelder und Umgebungslicht, Satellitenortung, Fingerabdrucksensoren, Mikrofone und vieles mehr.

So könnten beispielsweise Wetterdaten aus den Sensoren der Fahrzeuge verwendet werden, um auf einer lokalen Ebene Frühwarninformationen über Wetterextreme abzuleiten oder Stromnetze zu steuern.

Ein weiterer Treiber sind maschinelle Lernverfahren, etwas aus dem Bereich Deep Learning. Hierunter wird allgemein eine Klasse von Optimierungsmethoden künstlicher neuronaler Netze verstanden. Bereits in den 1960er-Jahre wurden von Alexey Ivakhnenko die ersten Deep-Learning-Systeme (des Feedforward-Multilayer-Perzeptron-Typs) entwickelt. Dort erst die enorme Rechenleistung, die wir heute durch spezielle Prozessoren[52] zur Verfügung haben, ermöglichte die enormen Anwendungsfelder und Fortschritte.

Doch einen Mehrwert aus den Exabytes an Daten wird erst dann generiert, wenn neue Erkenntnisse daraus abgeleitet oder Entscheidungsprozess optimiert werden. In diesem Kontext sind Datenanalysten davon überzeugt, dass Predictive Analytics einer der wichtigsten Big-Data-Trends ist, insbesondere im Bereich des Risiko-Managements. Eine gute Orientierung liefert hierbei das Analytics-Reifegradmodell von Gartner. Hierbei werden vier Reifegradstufen unterschieden (vgl. Abb. 6.16).

Bei der *Descriptive Analytics* geht es um die Frage **„Was ist passiert?“**, das heißt eine Analyse von Daten aus der Vergangenheit, um potenzielle Auswirkungen auf die Gegenwart zu verstehen (siehe Business Intelligence).

Bei *Diagnostic Analytics* geht es um die Frage **„Warum ist etwas passiert?“**, das heißt eine Analyse der Ursache-Wirkungs-Beziehungen, Wechselwirkungen oder Folgen von Ereignissen (siehe Business Analytics).

Bei *Predictive Analytics* geht es um die Frage **„Was wird passieren?“**, das heißt eine Analyse potenzieller Zukunftsszenarien sowie eine Generierung von Frühwarninformationen. Basierend auf Technologien des Data Mining, Artificial Intelligence, statistischer

[51] Der US-amerikanische Zukunftsforscher und Director of Engineering bei Google, Ray Kurzweil, weist darauf hin, dass wir heute für 1000 Dollar etwa die Leistungsfähigkeit des Gehirns einer Maus mit rund 100 Millionen Nervenzellen kaufen können – bei einer Vertausendfachung wären wir im Jahr 2040 dann beim Komplexitätsgrad des menschlichen Gehirns angelangt. Vgl. Kurzweil (2012, S. 257 f.).

[52] Die sogenannten Tensor Processing Units (TPUs) sind anwendungsspezifische Computerchips, die von Google entwickelt wurden, um Anwendungen im Rahmen von maschinellem Lernen zu beschleunigen. Die dritte Generation wurde im Jahr 2018 vorgestellt. Die TPU 3.0 Pods bestehen aus 8 Racks mit insgesamt 1024 TPUs und 256 Server-CPUs. Die Rechenleistung von einem Pod liegt bei knapp über 100 PFLOPS (Floating Point Operations Per Second, d. h. Gleitkomma-Operationen pro Sekunde).

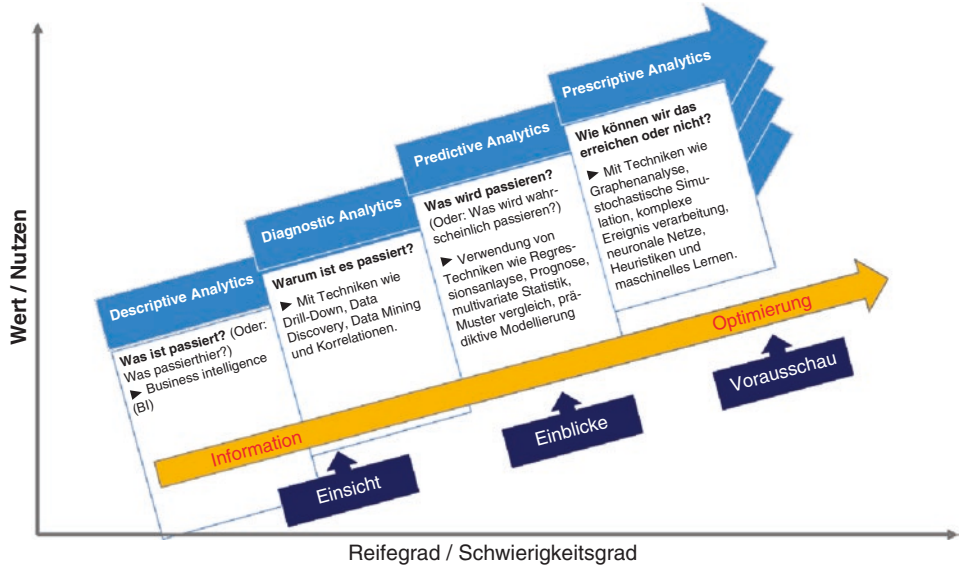


Abb. 6.16 Analytics-Reifegradstufen. (Quelle: Romeike und Eicher 2016, S. 168)

Methoden und Operations-Research erfolgt eine Berechnung von Wahrscheinlichkeiten zukünftiger Ereignisse.

Bei *Prescriptive Analytics* geht es um die Frage **„Wie müssen wir handeln, damit ein zukünftiges Ereignis (nicht) eintritt?“**, das heißt im Kern werden – basierend auf den Ergebnissen von Predictive Analytics – Maßnahmen simuliert, etwa basierend auf stochastischen Szenarioanalysen sowie Sensitivitätsanalysen.[53]

Die Internet-Suchmaschine Google hat mit „Google Flu Trends“ bereits im Jahr 2008 gezeigt, wie mithilfe von Algorithmen und Big Data die jährlichen Grippewellen besser prognostiziert werden können.[54] Die Idee von Google war, die Suchanfragen seiner Nutzer zu analysieren und hieraus Frühwarninformationen für eine Grippewelle abzuleiten (vgl. Abb. 6.17). Der Datenanalysten von Google verglichen über einen fünfjährigen Zeitraum die 50 Millionen am häufigsten von US-Bürgern eingegebenen Suchbegriffe mit den realen Krankheitsdaten, wie sie von der Seuchenschutzbehörde Centers for Disease Control and Prevention (CDC) archiviert werden. Die Google-Analysten fanden aus 50 Millionen Suchbegriffen und 450 Millionen Begriffskombinationen 45 Begriffe, die stark mit dem Auftreten einer Grippe korrelierten. Anfangs präsentierte „Google Flu Trends“ sehr gute Prognosen. Im Jahr 2013 prognostizierte Google jedoch doppelt so viele Fälle, wie tatsächlich auftraten. Auch die Pandemie H1N1 2009/10 (Schweinegrippe) wurde von Google nicht als Szenario erkannt. Die Gründe hierfür sind vielfältig: Erstens schlossen

[53] Vg. Romeike (2015).

[54] Vgl. Lazer, Kennedy, King, und Vespignani (2014).

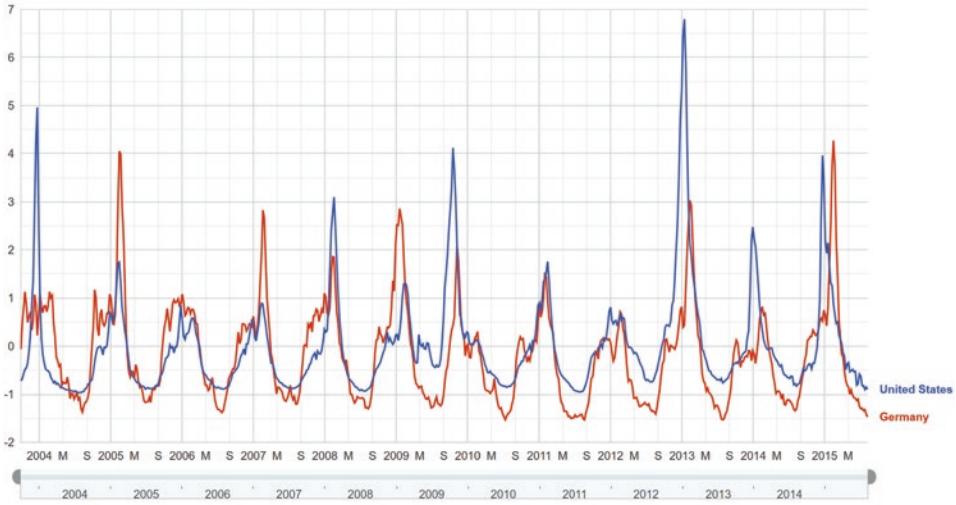


Abb. 6.17 Flue Search Activity (Vergleich Deutschland und USA). (Quelle: Google Inc.)

die Datenanalysten aus historischen Korrelationen auf zukünftige Veränderungen. Diese gemessene Korrelation muss jedoch nicht für die Zukunft gelten. Wird beispielsweise viel über Grippeepidemien berichtet, suchen die Nutzer auch verstärkt nach Informationen im Netz. Ein weiterer Grund lag darin, dass Epidemiologen eine Grippe anderes definierten als der Laie, der vielleicht nur eine leichte Erkältung hat und im Netz aber nach „Grippe" sucht. Kurzum: Die zu Grunde liegenden Daten waren unscharf und lieferten daher auch fehlerhafte Prognosen und Frühwarninformationen.[55]

6.8 CIRS

Unter einem *Critical Incident Reporting-System* (CIRS) wird ein Berichtssystem zur in der Regel anonymen Meldung von kritischen Ereignissen (critical incident) und Beinahe-Schäden (near misses) verstanden. In der Industrie und im Handel dient ein CIRS der *Prävention von zukünftigen Risikoeintritten*. Im Gesundheitswesen wird CIRS als ein In-

[55] Vgl. Romeike (2019a).

[56] Vgl. beispielsweise Fehlerberichts- und Lernsystem für Hausarztpraxen, www.jeder-fehler-zaehlt.de oder die externe Schadenfalldatenbank für operative Risiken (im Bereich Banken und Versicherungen) der Operational Riskdata eXchange Association (ORX). Die Datenbank enthält mehr als 700.000 Schadensfälle im Gesamtwert von über 500 Milliarden Euro und bietet Mitgliedern Zugang zu verschiedenen Standardberichten, einschließlich Benchmarks zu Schadensfällen.

strument zur Verbesserung der Patientensicherheit eingesetzt. Dahinter steckt die Erkenntnis, dass man nicht jeden Fehler selber machen muss, um daraus zu lernen.[56]

Herbert William Heinrich, ein US-amerikanischer Pionier im Bereich der industriellen Schadenprävention und Mitarbeiter der Travelers Insurance Company, hat im Jahr 1931 aus einer Beobachtung von 550.000 Unfällen eine Ursache-/Wirkungsanalyse durchgeführt.[57] Seine Untersuchungen kamen zu dem Ergebnis, dass in Kliniken Trivialereignisse, wenn sie in einer unglücklichen Verkettung auftreten, in äußerst seltenen Fällen zu schweren Störungen von Gesundheit oder zum Verlust von Leben führen.

„Heinrichs Gesetz" (Heinrich's law) hat zum Inhalt, dass katastrophale Ereignisse nicht unvorhersehbar sind oder überraschend eintreten.[58] Gerade kleine Fehler oder gefährliche Situationen ohne negative Auswirkungen dürfen nicht einfach mit der Bemerkung „Ist ja gerade noch mal gut gegangen" abgetan werden. Basierend auf Heinrichs Gesetz bilden 300 Beinahe-Unfälle (oder „leichte Fehler" oder „kleine Verschwendungen") die statistische Grundlage für 29 mittelschwere Vorkommnisse (oder „sichtbare/spürbare Fehler" oder „deutliche kostenwirksame Verschwendungen") und diese wiederum sind die statistische Basis für einen Katastrophenfall (oder „Kunstfehlerklage"). Mittelschwere Unfälle und Katastrophen deuten sich also an in Form von Frühwarninformationen, abgeleitet aus Frühwarnindikatoren. So wird der Grenzübergang vom Bagatellfehler (also dem allseits akzeptierten und arbeitstäglich tolerierten kleinen Fehler) zum mittelschweren Problem ebenso wie der Übergang zur Katastrophe gerade dann in der Praxis beobachtbar vollzogen, wenn Außergewöhnliches passiert bzw. Organisation und Mitarbeiter unter Zeitdruck geraten.

Heinrichs Gesetz rät, durch verstärkte Fehlererkennung, Fehlervermeidung und Fehlerbehebung bereits am „stumpfen Ende" des Risikoeisbergs die Unglücksfälle am „spitzen Ende" zu verhindern (vgl. Abb. 6.18).

Da Herbert William Heinrich für die Basis seiner „Gesetzmäßigkeit" keine empirischen Daten und Dokumente vorweisen konnte, geriert „Heinrichs Gesetz" auch in Kritik.[59] So wird u. a. kritisiert, dass seine Studien auf Unfällen basieren, die in den 1920er-Jahren passierten. Sicherheit bei der Arbeit und die Arbeitsplätze selbst haben sich bis heute substanziell verbessert.

Außerdem wird von Kritikern die unterstellte 300-29-1 Ratio (Heinrichs Dreieck, siehe Abb. 6.18) kritisiert, da es danach nicht möglich ist, von Einzelfalldaten, die mit den üblichen Erfassungsmethoden von 1926 dokumentiert wurden, auf die verletzungsfreien Unfälle zu schließen. Vielmehr führen aktuelle Untersuchung von Unfällen zu dem Ergebnis, dass die Unfälle, die zum Tode oder zu schwerwiegende Verletzungen führten, nicht mit

[57] Vgl. Heinrich, Petersen, Roos, Brown, und Hazlett (1980).

[58] Vgl. von Eiff und Middendorf (2004, S. 537–542).

[59] Vgl. hierzu insbesondere Manuele (2002) und Manuele (2003).

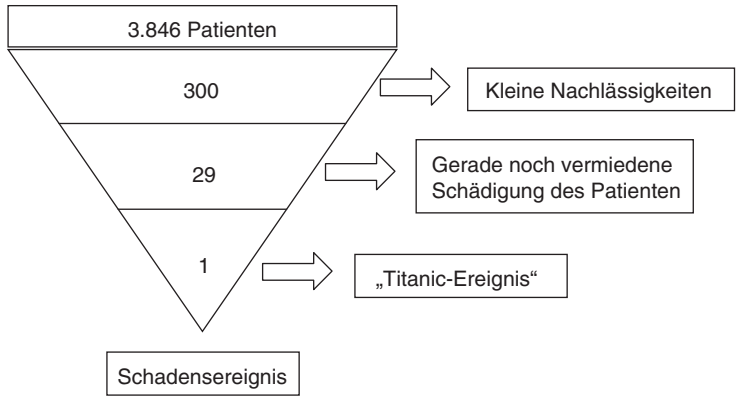


Abb. 6.18 Heinrichs Gesetz. (Quelle: Romeike und Hager 2013, S. 271)

denen von Unfällen, die häufig auftreten und mit leichten Verletzungen ausgehen, kausal zusammenhängen.

Trotz dieser Kritik kann Heinrichs Gesetz vom Prinzip auch auf Unternehmen aus Industrie und Handel übertragen werden. Auch dort (siehe auch die Ausführungen zu Frühwarnindikatoren im vorangegangenen Kapitel) treten Ereignisse häufig nicht unvermittelt und plötzlich ein. Vielmehr gehen sogenannte „Vorläufer“ – also Frühindikatoren einer möglichen Veränderung – voraus. Strukturbrüche und Krisen lassen sich daher frühzeitig noch vor ihrem eigentlichen Eintreten wahrnehmen.

Wie bereits skizziert, geht insbesondere der *„Weak Signal“-Ansatz von Ansoff* davon aus, dass unerwartete exogene Störungen nicht vollständig unvorhersehbar eintreten. Frühaufklärungsinformationen werden quasi mit einem „360-Grad-Radar“ überall und zu jeder Zeit als „schwache Signale“ gewonnen. Dabei kann es sich beispielsweise um folgende, unscharf strukturierte Informationen handeln:[60]

- die Verbreitung neuartiger Meinungen und Ideen in Medien,
- die plötzliche Häufung gleichartiger Ereignisse mit strategischer Relevanz für das betreffende Unternehmen,
- Meinungen und Stellungnahmen von Organisationen und Verbänden bzw. von Schlüsselpersonen aus dem öffentlichen Leben,
- Tendenzen der Gesetzgebung und Rechtsprechung.

„Schwache Signale“ werden bevorzugt über öffentlich zugängliche Kommunikationsorgane wie etwas das Internet verbreitet. Eine besondere Problematik „schwacher Signale“ besteht aus der anfänglich vorherrschenden Ignoranz bei den Empfängern, die in eine regelrechte „Ignoranzfalle“ münden kann. Trotz einer hohen Manövrierfähigkeit wer-

[60] Vgl. Romeike (2005b, S. 22–27).

den daher häufig „schwache Signale“ nicht ernst genommen. Erst bei einer zunehmenden Häufung von Signalen und gleichzeitig abnehmender Ignoranz bei den Signalempfängern wächst die Bereitschaft zu Reaktionsstrategien.

Das Konzept der „schwachen Signale“ von Ansoff weist eine Reihe von Schwächen auf. Insbesondere wird die Frühzeitigkeit der Problemerkennung erkauft mit einer größeren Unsicherheit und erhöhten Subjektivität in der Signalinterpretation. Außerdem können die Ereignisse und deren Einfluss auf die Strategieumsetzung und die Potenziale nur qualitativ gemessen werden.

6.9 PAAG und HAZOP

Die PAAG-Methode und die HAZOP-Methode beinhaltet eine systematische Vorgehensweise zum Auffinden möglicher Zielabweichungen und Störungen in Systemen aller Art. Etabliert hat sich die Methode insbesondere als Instrument der Sicherheitstechnik in der Prozess-, Pharma- und Petrochemie.

Von der methodischen Seite ist die *PAAG-Methode* und die *HAZOP-Methode* mit der Design-FMEA vergleichbar. Die HAZOP-Methode (von englisch Hazard and Operability) war ursprünglich für Chemieanlagen konzipiert, wird heute aber auch für Anlagen in anderen Industrien eingesetzt, hauptsächlich bei der Planung von Neuanlagen, aber auch bei der Planung von Umbauten und bei der Bewertung von bestehenden Anlagen. In Deutschland ist die HAZOP-Methode auch als *PAAG-Verfahren* bekannt. PAAG basiert auf den Bausteinen **P**rognose, **A**uffinden der Ursache, **A**bschätzen der Auswirkungen, **G**egenmaßnahmen definieren.

In einer HAZOP-Studie wird untersucht, welche Abweichungen vom bestimmungsgemäßen Betrieb einer Anlage zu welchen Problemen bezüglich Sicherheit und Betrieb einer Anlage führen können. Die Studie wird in der Unternehmenspraxis regelmäßig in einem interdisziplinären Team durchgeführt, welches Kompetenzen über die eingesetzten Substanzen, den Prozess, die Anlage und die Automatisierungstechnik zusammenführt. Im Rahmen der Analyse wird systematisch jede Komponente einer Anlage untersucht, was geschehen könnte, wenn ein charakteristischer Betriebsparameter dieser Komponente vom vorgesehenen Wert bzw. Wertebereich abweichen sollte.

Dabei werden eine oder mehrere Sollfunktionen für die betrachtete Komponente (Anlagenteil, Verfahrensabschnitt, Aggregat, Apparat etc.) definiert, mit denen die vorgesehene Funktionalität beschrieben wird. Anhand von einfachen Leitworten (ja/nein, mehr/weniger, sowohl als auch, teilweise, anders als) wird dann die „Ausführung“ der Sollfunktion entsprechend geändert, die daraus resultierenden Konsequenzen diskutiert und so Ursachen für Ablaufstörungen bis hin zu Störfällen erkannt.

Üblicherweise basiert eine HAZOP-Studie auf einer gemeinsamen Betrachtung der Fließbilder der Anlage. Den Fließbildern lassen sich die Stoffströme und zum Teil auch die Informationsflüsse innerhalb der Anlage entnehmen.

Tab. 6.5 Leitworte der PAAG-/HAZOP-Methode. (Quelle: Eigene Tabelle basierend auf Sommer 2008)

Leitwort	Erläuterung
Nein oder nicht	Die definierte Sollfunktion wird nicht erfüllt oder findet nicht statt.
Mehr	Quantitativer Zuwachs von Prozessgrößen, etwas erfolgt zu viel.
Weniger	Quantitative Abnahme von Prozessgrößen, etwas geschieht zu wenig.
Sowohl als auch	Zusätzlich zum bestimmungsgemäßen Prozess geschieht noch etwas anderes.
Teilweise	Die Sollfunktion wird nur unvollständig erfüllt bzw. einzelne Teile der Sollfunktion sind nicht vollständig vorhanden.
Umkehrung	Etwas geschieht in umgekehrter Richtung oder in umgekehrter Reihenfolge.
Anders als	Elemente der Sollfunktion werden durch etwas anderes ersetzt.

Zentraler Baustein der Methodik ist die Anwendung so genannter Leitworte, mittels derer die Abweichungen und Störungen „generiert“ werden (vgl. Tab. 6.5).

Je nach Unternehmen kann die Methodik individualisiert werden. So kann man sich beispielsweise auf vier Leitworte (nein, mehr, weniger, anders als) beschränken, anhand derer die Diskussion gesteuert wird. Die Methodik wird immer durch Kreativitätsmethoden begleitet. In der Regel erfolgt dies basierend auf einem Brainstorming von Experten verschiedener Fachrichtungen.

6.10 Krisenmanagement

> *„Wenn mich jemand fragt, wie ich am besten meine Erfahrungen aus 40 Jahren auf hoher See beschreiben würde, so könnte ich diese Frage lediglich mit ‚unspektakulär‘ beantworten. Natürlich gab es schwere Stürme, Gewitter und Nebel, jedoch war ich nie in einen Unfall jeglicher Art verwickelt, der es wert wäre, über ihn zu berichten. Ich habe während dieser langen Zeit kaum in Schiff in Seenot erlebt […] Ich habe weder ein Wrack gesehen noch bin ich selbst in Seenot geraten oder habe ich mich sonst in einer misslichen Lage befunden, die in irgendeiner Form drohte zum Desaster zu werden.“*

Dieses Zitat stammt von Edward John Smith und datiert auf das Jahr 1907. Und E. J. Smith wurde der „Stolz Großbritanniens“ – das Luxusschiff RMS Titanic – anvertraut. Doch bereits die Jungfernfahrt von Southampton nach New York war ihre letzte Reise. Überhöhte Geschwindigkeit, blindes Vertrauen in die Technik und ein riesiger Eisberg verursachten ein Inferno: Die Reise der Titanic wurde am 14. April gegen 23:40 Uhr jäh unterbrochen, als der Ausguck Frederick Fleet direkt voraus einen Eisberg entdeckte, dreimal die Alarmglocke läutete und die Warnung direkt telefonisch an die Brücke weiterleitete, wo sie vom 6. Offizier James P. Moody entgegengenommen wurde. Die Titanic kollidierte bei voller Reisegeschwindigkeit ungebremst mit ihrer vorderen Steuerbordseite mit dem circa 300.000 Tonnen schweren Eisgebilde. In der ersten Stunde strömten zwischen 22.000 Tonnen und 25.000 Tonnen Wasser in das Schiff.

Kapitän Smith erteilte den Funkern gegen 0:15 Uhr den Befehl, Notrufe an andere Schiffe zu senden. Das nächste Schiff, das darauf antwortete, war die Carpathia, welche fast vier Stunden bis zur Unglücksstelle brauchte. Nachdem mehrere Besatzungsmitglieder in der Ferne Lichter eines Schiffes ausgemacht hatten, wurde ab 0:45 Uhr versucht, durch regelmäßigen Abschuss von Seenotraketen Kontakt zu dem Schiff aufzunehmen, doch blieb eine Antwort aus. Bei der durch den Kapitän um 0:05 Uhr angeordneten Evakuierung wurde etwa 65 Minuten nach der Kollision das erste Rettungsboot in das Wasser hinabgelassen.

Gegen 2:10 Uhr war Kesselraum Nummer vier, die siebte wasserdichte Abteilung vom Bug aus gesehen komplett geflutet. Rund 40.000 Tonnen Wasser drückten den Bug in die Tiefe, das Wasser erreichte nun die Schiffsbrücke und begann, das Bootsdeck zu überspülen.

Experten hatten zuvor bestätigt, dass das Schiff wegen seiner 16 wasserdichten Abteilungen unsinkbar sei. Unglücklicherweise durchbohrte der Eisberg sechs davon. Von den 2220 Personen kamen 1513 ums Leben – einer davon war der Kapitän E. J. Smith.

Aus der Titatic-Katastrophe kann man eine Reihe von *Lehren für das Krisenmanagement* und auch Risiko-Management in Unternehmen ziehen. Nachfolgend sind einige „Lessons learned“ skizziert:

- Das Schiff ist nachweislich zu schnell durch gefährliches Gewässer gefahren. E. J. Smith war als risikofreudiger Draufgänger berühmt. Bei Sturm und schlechtem Wetter fuhr er regelmäßig „unter Volldampf“. So wird berichtet, dass E. J. Smith regelmäßig das Schiff mit voller Fahrt durch die Sandbänke der Süd-West-Landzunge hindurchmanövrierte, die Entfernungen mit Augenmaß abschätzte und an jeder Seite nur wenige Zentimeter Platz zwischen Schiffswand und Sandbänken war.
- E. J. Smith war ein weißhaariger „Gentleman“ mit perfekter Ausstrahlung und bei Mannschaften, Passagieren und Reederei sehr beliebt. Dadurch war er gleichzeitig auch „unantastbar“ und immun für jegliche Kritik.
- Die Reederei (als Aufsichtsorgan) hatte die tatsächliche Kompetenz von E. J. Smith sowohl falsch eingeschätzt als auch niemals überprüft.
- Bereits bei der Jungfernfahrt des Schwesterschiffes der Titanic, der Olympic, verursacht Smith als verantwortlicher Kapitän aufgrund eines Navigationsfehlers im Hafen von New York eine Havarie mit einem anderen Schiff. Dieser Frühwarnindikator wurde von keiner Seite beachtet.
- E. J. Smith bekam die Kommandos über die beiden großen Schiffe im Alter von 60 Jahren. Trotz seiner langjährigen Erfahrungen als Kapitän hatte er keinerlei Erfahrungen mit derart großen Schiffen.
- Die Titanic galt als unsinkbar aufgrund neuer Sicherheitskonzepte (siehe oben). Man verließ sich auf die quer verlaufenden Schotts. Vorab wurden jedoch keinerlei Tests durchgeführt.
- An Bord gab es keinerlei präventive Sicherheitsstandards oder präventive Notfallübungen. Es gab vielmehr zu wenige Rettungsringe und Rettungsboote.

- Alle Frühwarnindikatoren, insbesondere Eisbergwarnungen, die via Telegramm und Funk eingingen, wurden ignoriert. Die Fahrt wurde mit ungedrosselter Geschwindigkeit fortgesetzt.
- Trotz der Eisbergwarnungen wurde die Route nicht weit genug nach Süden verlegt, um das ehrgeizige Ziel und den Zeitplan von E. J. Smith nicht zu gefährden.
- Erst etwa 30 Minuten nach der Kollision erfolgte der erste SOS-Funkspruch.
- An Bord der Titanic gab es keinen „offiziellen" Alarm. Vielmehr klopften Stewards an die Türen der 1. Klasse und wiesen auf den Unfall hin. Die Passagiere der 3. Klasse wurden erst wach, als das Wasser durch die Türen und Fenster kam.
- Von den vorhandenen 1178 Rettungsbootplätzen wurden nur 705 genutzt. Statt der teilweise möglichen Kapazität von 65 Passagieren wurden viele Boote nur zur Hälfte besetzt; eines der für 40 Passagiere ausgelegten Rettungsboote wurde sogar bereits gefiert, als sich darin nur zwölf Personen befanden.
- Die SS Californian, die sich in der Nähe befand, kam nicht zu Hilfe, weil deren Bordfunker dienstfrei und sich schlafen gelegt hatte. Bis heute ist aber strittig, ob die Lichter, die von der Titanic aus gesehen wurden, tatsächlich die der Californian waren, denn zum damaligen Zeitpunkt waren die Positionen von Schiffen nicht jederzeit genau bestimmbar.

Wie auf den Ozeanen geraten auch in der komplexen Wirtschaftswelt des 21. Jahrhunderts immer mehr Flaggschiffe in akute Seenot oder versinken komplett. Ob Enron, WorldCom, Schlecker, Quelle, Nokia oder Kodak – die Topmanager dieser Unternehmen erkannten die Risiken zu spät, ignorierten die Frühwarnindikatoren oder waren schlichtweg korrupt. Und auch der Staat liefert uns regelmäßig Beispiel für ein eher reaktives Krisenmanagement an Stelle eines antizipativen Krisenmanagements (Krisenvorsorge). So basierten fast alle Maßnahmen zur Bekämpfung der COVID-19-Pandemie – in der Folge des neuartigen Coronavirus SARS-CoV-2 – auf Ad-hoc-Maßnahmen, die nicht zuvor geplant waren. Dies erstaunt umso mehr, als dass ausgewiesene Experten seit vielen Jahren auf die Risiken einer Pandemie hinweisen. Der exzellente Statistiker und Professor für Internationale Gesundheit, Hans Rosling, hat bereits vor vielen Jahren auf die fünf globalen Risiken hingewiesen, die uns beunruhigen sollten. Als Top-1-Risiko beschreibt er in seinem Buch „Factfulness" das Risiko einer globalen Pandemie.[61] In renommierten Fachzeitschriften, wie etwa Nature, Science und Nature Reviews Microbiology, wurden Studienergebnisse über die Risiken einer globalen Epidemie veröffentlicht, die beispielsweise durch Coronaviren verursacht werden können. Und auch die Risikoanalyse „Pandemie durch Virus Modi-SARS" aus dem Jahr 2012 wurde von Wissenschaftlern und Experten des Robert Koch-Instituts (RKI) und zahlreichen Bundesämtern erstellt und den Mitgliedern des Deutschen Bundestages präsentiert. Das fiktive Szenario beschrieb eine von Asien ausgehende, globale Verbreitung eines neuartigen Erregers „mit außergewöhnlichem Seuchengeschehen". Hierfür wurde der hypothetische, jedoch mit realistischen Eigenschaften

[61] Vgl. Rosling; Rosling Rönnlund; Rosling (2020, S. 285 ff.).

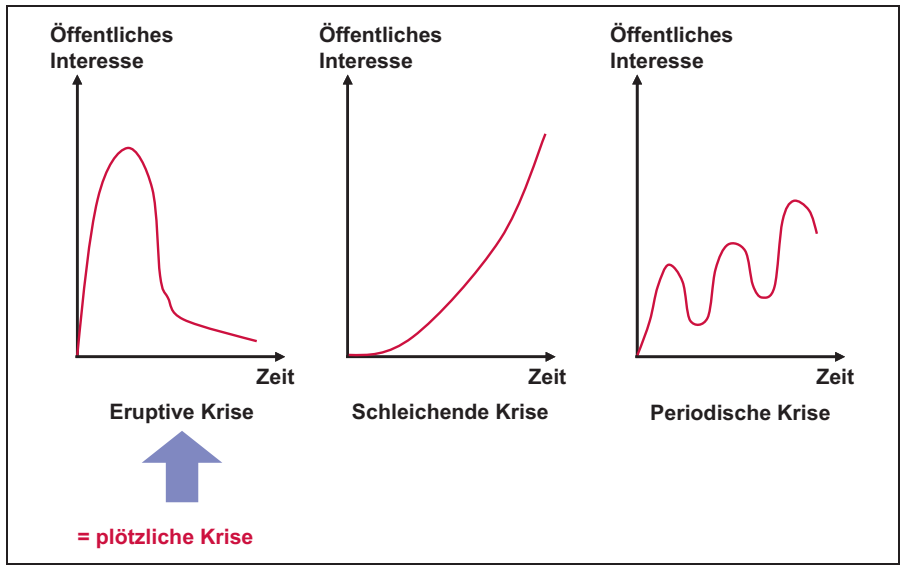


Abb. 6.19 Krisentypologien. (Quelle: Romeike und Hager (2013, S. 276) in Anlehnung an Töpfer (1999, S. 275))

versehene Erreger „Modi-SARS“ zugrunde gelegt. So stellt sich die Frage, warum aus dem konkreten Pandemie-Szenario keine präventiven und Risiko reduzierenden Maßnahmen abgeleitet und umgesetzt wurden.

Die typischen Verläufe von Krisen sind in Abb. 6.19 idealtypisch dargestellt. Eine *eruptive Krise* kann dadurch charakterisiert werden, dass sich kurz nach dem Kriseneintritt ein stark ansteigendes öffentliches Interesse zeigt. Dieses Interesse nimmt jedoch relativ schnell – in Abhängigkeit von den Krisenbewältigungsmaßnahmen – stetig ab. Als Beispiele können hier Katastrophen in der Folge von Flugzeugabstürzen oder Großbrände genannt werden.

Bei einer *schleichenden Krise* ist das öffentliche Interesse anfänglich sehr gering und nimmt im Zeitablauf, ausgelöst durch Multiplikator- und Akzeleratorwirkungen, exponentiell zu. Im Höhepunkt des Krisenverlaufs eskaliert die Krise. Eine schleichende Krise weist häufig darauf hin, dass entweder kein oder nur ein unzureichendes Krisenmanagement betrieben wurde.

Ein vielzitiertes Beispiel ist die geplante Versenkung der Brent Spar, bei der es sich um einen schwimmenden Öltank in der Nordsee handelt. Der im Besitz des Shell-Konzerns und Esso befindliche Tank wurde in den Medien oftmals irrtümlich als Förderplattform bezeichnet. Als Pipelines, die das Öl zum Ölterminal Sullom Voe befördern, die Aufgabe des Öltransports übernahmen, wurde die mit einer Höhe von 140 Metern, einem Durchmesser von 30 Metern und einem Gewicht von 14.500 Tonnen zu den kleineren Tanks zählende Brent Spar überflüssig und sollte 1995 im Meer versenkt werden. Nach anfänglichem Desinteresse in der Bevölkerung gelang es der Umweltorganisation Greenpeace – u. a. durch

die Besetzung von Brent Spar durch Aktivisten der Umweltschutzorganisation Greenpeace – ein starkes öffentliches Interesse zu mobilisieren. Dies mündete u. a. in einem Boykott von Shell-Tankstellen. Auch einige deutsche Behörden ließen ihre Autos nicht mehr bei Shell tanken. Daraufhin sanken die Umsätze der deutschen Shell-Tankstellen um bis zu 50 Prozent.

Bei einer *periodischen Krise* ist ein ständiges Auf und Ab des öffentlichen Interesses zu beobachten. Insgesamt steigt jedoch das öffentliche Interesse insgesamt. Bei dieser Krisenerscheinungsform ist im Allgemeinen festzustellen, dass „[…] das Unternehmen keine Lerneffekte erzielt und damit auch keine Maßnahmen zur Krisenbewältigung und Krisenvorsorge durchführt".[62]

Ergänzend zum eher präventiv ausgerichteten Risiko-Management verfolgt eine sowohl präventiv als auch reaktiv ausgerichtetes *Notfall- und Krisenmanagement* das Ziel, die negativen Konsequenzen aus einem Notfall bzw. einer Krise – wie beispielsweise Reputationsverlust oder Wiederherstellungskosten – zu eliminieren bzw. zu reduzieren sowie den Fortbestand des Unternehmens sicherzustellen.

Die Unterscheidungsmerkmale zwischen *Risiko-Management, Notfallorganisation und Krisenmanagement* sind in Abb. 6.20 skizziert.

Der Zyklus des Krisenmanagements kann klassischerweise und idealtypisch in fünf Phasen aufgeteilt werden (vgl. Abb. 6.21).

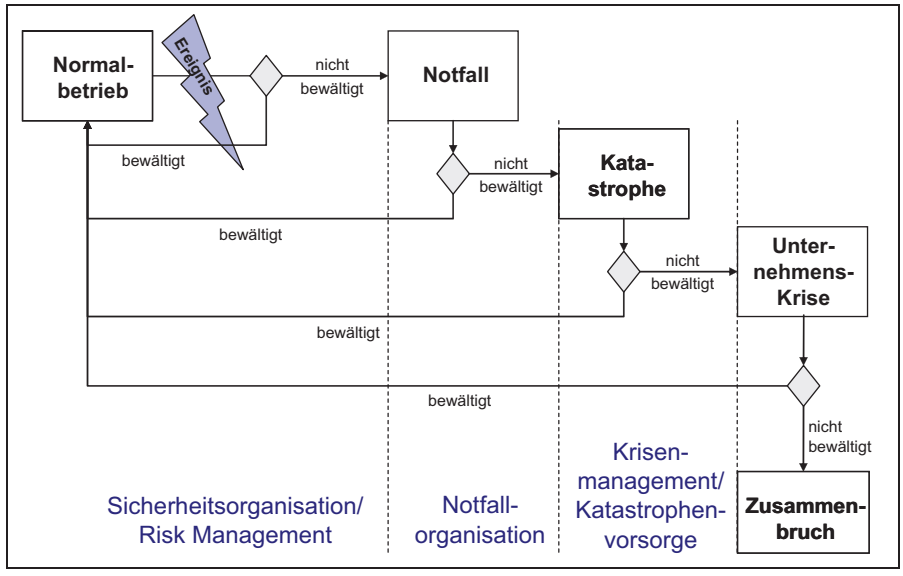


Abb. 6.20 Risiko-Management, Notfallorganisation, Krisenmanagement. (Quelle: Romeike 2004, S. 71)

[62] Vgl. Töpfer (1999, S. 275).

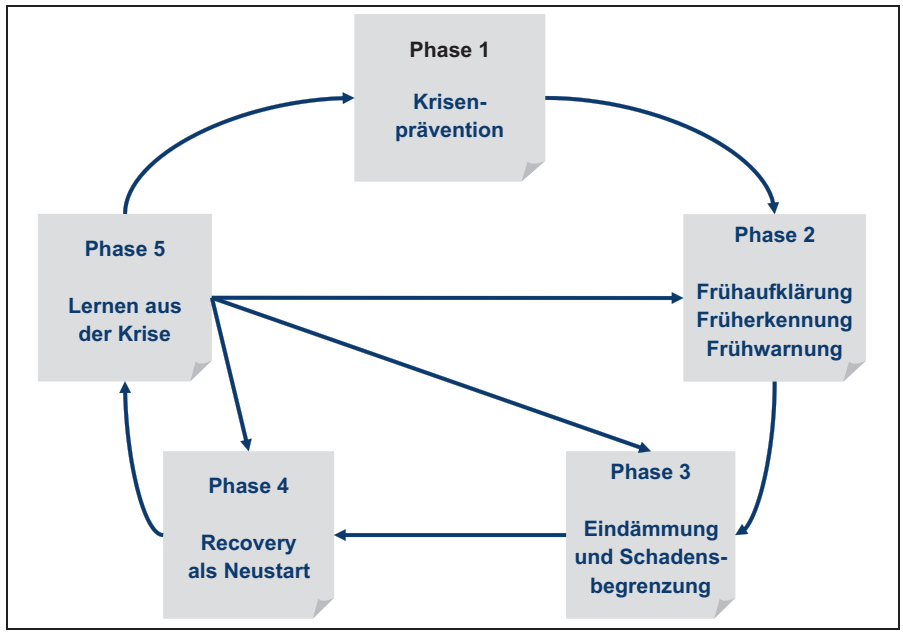


Abb. 6.21 Zyklus des Krisenmanagementprozesses (Vgl. Romeike und Hager 2013, S. 277)

Phase 1 – Krisenprävention: In der ersten Phase, der Krisenprävention, werden die Maßnahmen definiert, die eingeleitet wurden, um die potenzielle Krise zu vermeiden oder auch eine akute Krise in die richtigen Bahnen zu lenken. Krisenprävention hat vor allem etwas mit Krisenbewusstsein zu tun. Man muss das Undenkbare vorausdenken („Think the unthinkable") und potenzielle Krisenursachen antizipieren. Ziel der ersten Phase sollte die Erstellung eines Krisenplans (evtl. auch als Bestandteil eines Risiko-Management-Handbuches) sein. Hier sollten potenzielle Krisen sowie organisatorische, technische und personelle Maßnahmen beim Anbahnen einer Krise dargestellt werden. Wichtig sind ferner Aussagen zur Krisenkommunikation und zu Verantwortlichkeiten. Der Krisenplan sollte nicht als starre Prozessdefinition verstanden werden, sondern vielmehr als grobe Leitlinie. Um bei einer sich anbahnenden Krise schnell zu reagieren, können außerdem „Darksites" im Internet helfen. Diese werden im Krisenfall online geschaltet.

Phase 2 – Frühaufklärung, Früherkennung und Frühwarnung: Wie bereits im Kapitel über Frühwarnindikatoren dargestellt, sollte ein Unternehmen im Bereich der Frühaufklärung versuchen, schwache Signale („weak signals" im Sinne von Ansoff) für eine Krise abzufangen und über mögliche Krisenursachen aufzuklären (360-Grad-Radar). Im Bereich der Früherkennung und -warnung sollten typische Krisenindikatoren beim Überschreiten bestimmter Toleranzgrenzen rechtzeitig erkannt werden und latente Krisen in die richtigen Bahnen gelenkt werden. In Abb. 6.22 ist ein typischer Krisenverlauf ohne Krisenmanagement dargestellt. In Abb. 6.23 ist demgegenüber ein

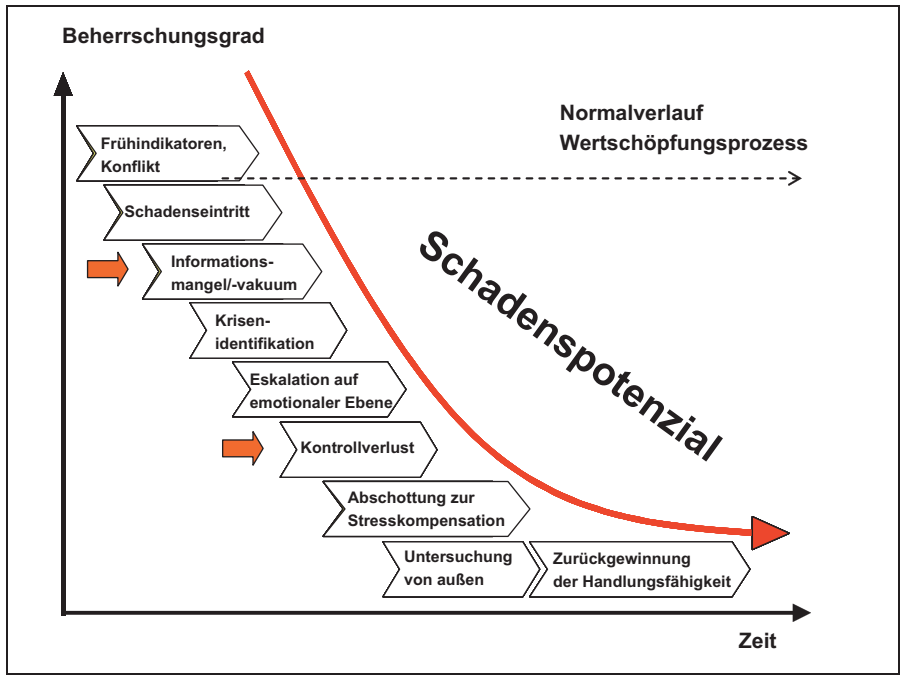


Abb. 6.22 Potenzieller Krisenverlauf ohne Krisenmanagement. (Quelle: Romeike und Hager 2013, S. 279)

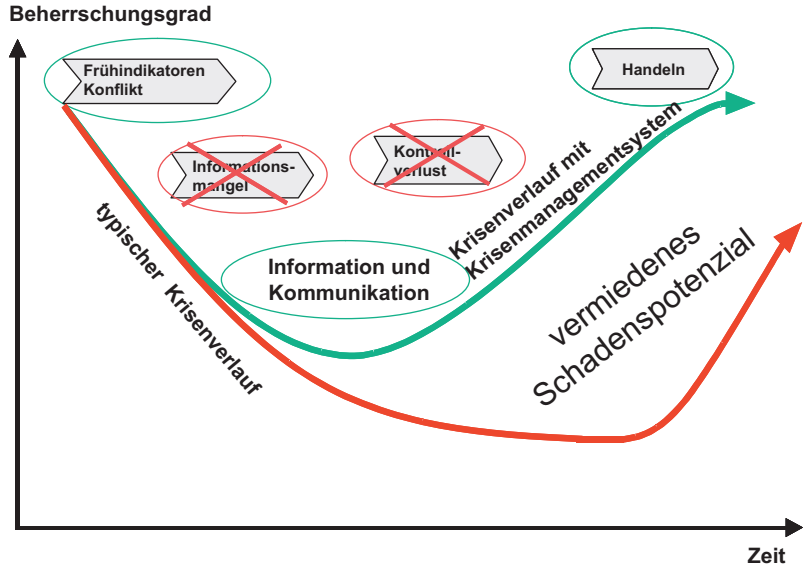


Abb. 6.23 Potenzieller Krisenverlauf mit Krisenmanagement. (Quelle: Romeike und Hager 2013, S. 280)

idealtypischer Verlauf unter Berücksichtigung der Wirkung eines Krisenmanagements skizziert.

Das Krisenmanagement bietet verschiedene Methoden und Werkzeuge der Frühaufklärung und -erkennung. Als Beispiele seien hier die bereits beschriebene Methode der Szenarioanalyse oder das Medienmonitoring genannt.

3. **Phase – Eindämmung und Schadensbegrenzung:** Welche Maßnahmen wurden nach Eintritt der Krise zur Schadensbegrenzung ergriffen? Vor allem ein präventiv erstellter Krisenplan bietet hier eine wertvolle Hilfe. In der Prozessphase der Schadensbegrenzung ist insbesondere eine gezielte Krisenkommunikation wichtig. Vor allem in der Vergangenheit aufgebaute Netzwerke zu Medien sind in diesem Kontext nicht zu unterschätzen.
4. **Phase – Recovery als Neustart durch Beseitigung der negativen Folgewirkungen:** Wie können die negativen Folgewirkungen einer Krise beseitigt werden? Wie erreicht man das Vertrauen der Kunden oder Shareholder zurück? Auch in dieser Phase spielt eine gezielte Kommunikation eine ganz wesentliche Rolle. Dies beginnt vor allem bei dem Versuch des Wiedererlangens des Vertrauens der Mitarbeiter, Kunden und Shareholder. Die Wiederaufnahme des Normalbetriebs, vor allem auch der geregelten Werbemaßnahmen nach der Zeit des permanenten medialen Drucks und der Rechtfertigungen ist enorm wichtig, um das Ziel des Recovery möglichst rasch erreichen zu können.
5. **Phase – Lernen aus der Krise (Krisennachbereitung):** Die Erfahrungen, die während der Krise gesammelt werden, sollten im Sinne einer „Lernenden Organisation" in der Lernphase wieder als Feedback in die Organisation zurückfließen. So können sich Unternehmen auf zukünftige Krisen besser vorbereiten.

Basierend auf der Analyse von diversen Krisenverläufen können die folgenden *zwölf Grundsätze des Krisenmanagements* formuliert werden:

1. Jede Krise ist anders.
2. Krisenvorsorge – wie auch Risiko-Management – ist eine Investition in die Zukunft.
3. Die Formulierung eines Krisenplans bedeutet immer eine Gratwanderung zwischen standardisierten Inhalten und Prozessen sowie vollständiger Flexibilität.
4. Das Denken in Worst-case-Szenarien („Think the unthinkable") reduziert die Wahrscheinlichkeit von existenzbedrohenden Krisen.
5. Während einer Krise muss das Top-Management als „Kapitän" agieren, ein Krisenteam als Task Force und ein Kommunikationsprofi als Kommunikator.
6. Präventives Medientraining führt zu einer höheren Souveränität.
7. Ein Sparring mit einem (externen) Review-Team hilft, Krisengefahren zu lokalisieren, zu präzisieren und zu vermeiden und reduziert das Risiko von Betriebsblindheit.
8. Der Wille zur Aufklärung muss kommuniziert werden. Als primäres Ziel muss eine rasche Transparenzschaffung über die Krisenursachen verfolgt werden.

9. Die Interessen der Kunden und der Öffentlichkeit stehen an erster Stelle.
10. In der Krise ist es wichtig, dass bereits etablierte Kommunikationsnetzwerke genutzt werden.
11. Eindeutige Botschaften in der Krisenkommunikation verstärken die Glaubwürdigkeit.
12. Vertrauen ist das höchste Gut in einer Krise.

Literatur

Allianz Global Corporate & Specialty (2019): Allianz Risk Barometer – Top Business Risks for 2019, München 2019.

Allmann, A.: Erdbeben, Tsunami, Atomunfall – die Dreifach-Katastrophe von Tohoku, in: Münchener Rückversicherungs-Gesellschaft (Hrsg.): Topics Geo (Ausgabe 2012, Naturkatastrophen 2011 – Analysen, Bewertungen, Positionen), München 2012, S. 7–11.

Ansoff, H. I.: Managing Surprise and Discontinuity – Strategic Response to Weak Signals (dt. Übersetzung: Die Bewältigung von Überraschungen – Strategische Reaktionen auf schwache Signale), in: Zeitschrift für betriebswirtschaftliche Forschung 28 (1976), S. 129–152.

Arvanitoyannis, I./Varzakas, T.: Application of ISO 22000 and Failure Mode and Effect Analysis (FMEA) for Industrial Processing of Salmon: A Case Study, Critical Reviews in Food Science and Nutrition, 48, 2008, p 411–429.

Automotive Action Group (AIAG)/Verband der Automobilindustrie e. V. (VDA): Fehler-Möglichkeits- und -Einfluss-Analyse (FMEA) Handbuch, Berlin 2017.

Bojar, P.: Application of FMEA method for assessment of risk in land transportation of hazardous materials, in: Journal of KONES Powertrain and Transport Vol. 19 No. 3, 2012, S. 41–47.

Bowersox, D. J.; Closs, D. J.; Cooper, M. B.: Supply chain logistics management, Boston 2007.

Erben, R. F.: Sandbank – Wie Barings & Co. Schiffbruch erlitten hat, in: RISKNEWS, 1. Jg. (2004), H. 1, S. 46–50.

Ferdous, R./Khan, F./Sadiq, R./Amyotte, P./Veitch, B.: Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach, in: Process Safety and Environmental Protection, Vol. 91, 2013, S. 1–18.

Feynman, R. P.: Kümmert Sie, was andere Leute denken? 7. Auflage, Piper Verlag, München 1996.

Götze, U.: Szenario-Technik in der strategischen Unternehmensplanung, Wiesbaden 1993.

Heinrich, H. W.; Petersen, D.; Roos, N. R.; Brown, J.; Hazlett, S.: Industrial Accident Prevention: A Safety Management Approach, 1980.

Herlyn, W.: PPS im Automobilbau – Produktionsprogrammplanung und -steuerung von Fahrzeugen und Aggregaten. Hanser Verlag, München 2012.

Huth, M./Romeike, F.: Risikomanagement in der Logistik. Konzepte – Instrumente – Anwendungsbeispiele, Springer Gabler Verlag, Wiesbaden 2016.

Huth, M.: Einführung in die Logistik. Ventus Publishing, London 2012.

Jüttner, U.: Supply chain risk management: Understanding the business requirements from a practitioner perspective, in: International Journal of Logistics Management, Vol 16/2005, S. 120–141.

Kahn, H.; Wiener, A. J.: The Year 2000. A Framework for Speculation on the next 33 Years, New York, Toronto 1968.

Kersten, W.; Hohrath, P.; Winter, M.: Risikomanagement in Wertschöpfungsnetzwerken – Status quo und aktuelle Herausforderungen, in: Fachhochschule des bfi Wien (Hrsg.): Supply Chain Risk Management, Wien 2008.

Krystek, U.; Müller, M.: Frühaufklärungssysteme – Spezielle Informationssysteme zur Erfüllung der Risikokontrollpflicht nach KonTraG, in: Controlling, Heft 4/5 (1999).

Krystek, U./Müller-Stewens, G.: Frühaufklärung für Unternehmen: Identifikation und Handhabung zukünftiger Chancen und Bedrohungen, Stuttgart 1993.

Kurzweil, R.: How to Create a Mind, New York 2012.

Lazer, D./Kennedy, R./King, G./Vespignani, A.: The Parable of Google Flu: Traps in Big Data Analysis, in: Science, 343 (6176), 2014, S. 1203–1205.

Linder, S./Spitzner, J: Effektives Risiko- und Chancenmanagement in turbulenten Zeiten – Wie Sie Szenarien und Simulationen richtig nutzen, in: Risk, Compliance & Audit (RC&A), Ausgabe 5/2010, S. 12–18.

Majima, I.: JIT, Kostensenkung durch Just-In-Time Production, München 1994.

Manuele, F. A.: Heinrich Revisited: Truisms or Myths. National Safety Council, 2002, ISBN 0-87912-245-5.

Manuele, F. A.: On the Practice of Safety. John Wiley & Sons, 2003, ISBN 0-471-27275-2.

Meyer-Schönherr, M.: Szenario-Technik als Instrument der strategischen Planung, Ludwigsburg/Berlin 1992.

Mokhtari, K./Ren, J./Roberts, C./Wang, J.: Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals, in: Journal of Hazardous Materials, Vol. 192, Issue 2, 2011, S. 465–475.

Mokhtari, K./Ren, J./Roberts, C./Wang, J.: Decision support framework for risk management on sea ports and terminals using fuzzy set theory and evidential reasoning approach, in: Expert Systems with Applications, Vol. 39, Issue 5, 2012, S. 5087–5103.

Münchener Rückversicherungs-Gesellschaft (Hrsg.): Topic 95, München 1996.

Ono, T.: Toyota Production System: Beyond Large-Scale Production, Cambridge 1988.

Porter, M.: Competitive Advantage: Creating and Sustaining Superior Performance, New York 1985.

Romeike, F.: Lexikon Risiko-Management, Weinheim 2004.

Romeike, F.: Frühwarnsysteme im Unternehmen, Nicht der Blick in den Rückspiegel ist entscheidend, in: RATING aktuell, April/Mai 2005a, Heft 2, S. 22–27.

Romeike, F.: Frühaufklärungssysteme als wesentliche Komponente eines proaktiven Risikomanagements, in: Controlling, Heft 4–5/2005b (April/Mai), S. 271–279.

Romeike, F.: Integriertes Risiko-Controlling und -Management im global operierenden Konzern, in: Schierenbeck, H. (Hrsg.): Risk Controlling in der Praxis, Zürich 2006, S. 429–463.

Romeike, F.: Szenarioanalyse: Lernen aus der Zukunft, in: FIRM Jahrbuch 2015, Frankfurt/Main 2015, S. 118–120.

Romeike, F.: Risikomanagement, Springer Gabler Verlag, Wiesbaden 2018a.

Romeike, F.: Toolbox – Fehlermöglichkeits- und Einflussanalyse (FMEA), in: GRC aktuell, Ausgabe Mai 2018, 02/2018b, S. 73–77.

Romeike, F.: Risk Analytics und Artificial Intelligence im Risikomanagement, in: Rethinking Finance, Ausgabe 3/2019, Juni 2019a, S. 45–52.

Romeike, F.: Toolbox – Die Bow-Tie-Analyse, in: GRC aktuell, Ausgabe Februar 2019, 01/2019b, S. 39–44.

Romeike, F.: Toolbox – Fehlerbaumanalyse, in: GRC aktuell, Ausgabe August 2019, 03/2019c.

Romeike, F./Spitzner, J.: Von Szenarioanalyse bis Wargaming – Betriebswirtschaftliche Simulationen im Praxiseinsatz, Wiley Verlag, Weinheim 2013.

Romeike, F./Hager, P.: Erfolgsfaktor Risiko-Management 3.0 – Methoden, Beispiele, Checklisten, Praxishandbuch für Industrie und Handel, 3. Auflage, Springer Gabler Verlag, Wiesbaden 2013.

Romeike, F./Eicher, A. (2016): Predictive Analytics: Looking into the future, in: FIRM Yearbook 2016, S. 168–171.

Romeike, F./Eicher, A.: Predictive Analytics – Looking into the future, in: FIRM Jahrbuch 2016, Frankfurt/Main 2016, S. 168-171.

Rosling, H.; Rosling Rönnlund, A.; Rosling, O.: Factfulness: Wie wir lernen, die Welt so zu sehen, wie sie wirklich ist, 5. Auflage, Ullstein Verlag, Berlin 2020.

Ruijter, A. de/Guldenmund, F.: The bowtie method: A review, in: Safety Science, Vol. 88, 2016, S. 211–218.

Schiller, F.: Big Data in der Lebensversicherung, in: RISIKO MANAGER 04/2019, S. 4–7.

Schwindt, E.: Gefahrenanalyse mittels Fehlerbaumanalyse, Paderborn 2004 (Ausarbeitung im Rahmen des Seminars Analyse, Entwurf und Implementierung zuverlässiger Software).

Seibold, E.: Entfesselte Erde – Vom Umgang mit Naturkatastrophen, Stuttgart 1995, S. 70.

Sennheiser A.; Schnetzler M.: Wertorientiertes Supply Chain Management, Heidelberg/Berlin 2008.

Sommer, J.: Das PAAG-Verfahren – Methodik, Anwendung, Beispiele. Hrsg.: IVSS Sektion Chemie. 4. Auflage. Heidelberg 2008.

Sträter, D.: Szenarien als Instrument der Vorausschau in der räumlichen Planung. In: Akademie für Raumforschung und Landesplanung (Hrsg.): Regionalprognosen. Methoden und ihre Anwendung, S. 417–440, Hannover 1988 (Veröffentlichungen der Akademie für Raumforschung und Landesplanung: Forschungs- und Sitzungsberichte, 175).

Töpfer, A.: Plötzliche Unternehmenskrisen – Gefahr oder Chance?, Grundlagen des Krisenmanagement, Praxisfälle, Grundsätze zur Krisenvorsorge, Neuwied/Kriftel 1999.

Toyota Motor Corporation: The Toyota Production System – Leaner manufacturing for a greener planet. TMC, Public Affairs Division, Tokyo 1998.

United Nations Centre for Regional Development (UNCRD): Comprehensive Study of the Great Hanshin Earthquake, Nagoya 1995.

von Eiff, W.; Middendorf, C.: Klinisches Risikomanagement – kein Bedarf für deutsche Krankenhäuser?, in: Das Krankenhaus, 7/2004, S. 537–542.

Werdich, M.: FMEA – Einführung und Moderation, 2. Auflage, Springer Vieweg, Wiesbaden 2012.

Werdich, M: Die RPZ ist tot – Es lebe die AP, Internet: https://www.risknet.de/themen/risknews/die-rpz-ist-tot-es-lebe-die-ap/ [Abruf am 29.07.2019].

Wildemann, H.: Das Just-In-Time-Konzept, München 2001.

World Economic Forum (Hrsg.): Global Risks 2012, An Initiative of the Risk Response Network, Cologny/Geneva 2012.