Schutzkommission
beim Bundesministerium
des Innern

Risikokompetenz
Beurteilung von Risiken

Sebastian Festag & Uli Barth

7

SCHRIFTEN DER SCHUTZKOMMISSION

Risikokompetenz
Beurteilung von Risiken

Eine Veranstaltung der Schutzkommission
beim Bundesministerium des Innern und der
Gesellschaft für Sicherheitswissenschaft e.V.
29.–30. April 2014, Bundesministerium des Innern

In Zusammenarbeit mit der IVSS-Sektion
Maschinen- und Systemsicherheit.

SCHRIFTEN DER
SCHUTZKOMMISSION
BAND 7

Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe

Risikokompetenz
Beurteilung von Risiken

Sebastian Festag & Uli Barth

7

SCHRIFTEN DER SCHUTZKOMMISSION

Danksagung

Wir bedanken uns bei der Geschäftsstelle der Schutzkommission beim Bundesministerium des Innern für die organisatorische Unterstützung bei der Ausrichtung der Veranstaltung sowie der Gesellschaft für Sicherheitswissenschaft e.V. für die fachliche Unterstützung.

Ebenso bedanken wir uns herzlich bei allen Referenten und Moderatoren für die inhaltlichen Beiträge sowie bei Frau Anna Magdalena Barth für das ehrenamtlich geleistete Korrektorat.

Herausgeber:
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Postfach 18 67, 53008 Bonn
Tel.: 0228 . 99 550-0, Fax: 0228 . 99550-1620, www.bbk.bund.de

Verantwortlich für den Inhalt:
Dr. Sebastian Festag, Gesellschaft für Sicherheitswissenschaft e.V.,
c/o Hekatron Brühlmatten 9, 79295 Sulzburg
und
Prof. Dr. Uli Barth, Schutzkommission beim Bundesministerium des Innern,
c/o Bergische Universität Wuppertal, Fachbereich D – Abteilung Sicherheitstechnik, Lehrstuhl Methoden der Sicherheitstechnik/Unfallforschung,
Gaußstr. 20, 42119 Wuppertal

ISBN-10: 3-939347-64-7
ISBN-13: 978-3-939347-64-4

Gestaltung, Layout und Satz:
Bernd Kreuder | Online- und Printmedienproduktion
Köslinstr. 40, 53123 Bonn
www.kreuder.eu

Druck:
strohmeyer dialog druck GmbH
Hundsrückstraße 6, 37287 Wehretal-Langenhain
www.s-dd.de

Inhalt

Bildverzeichnis

Tabellenverzeichnis

Vorwort

Auf Initiative des Physikers Werner Heisenberg wurde die Schutzkommission ursprünglich von der Vorläuferorganisation der heutigen Deutschen Forschungsgemeinschaft (DFG) im Jahr 1951 gegründet. Die Gründung der Gesellschaft für Sicherheitswissenschaft (GfS e.V.) als Verein in Wuppertal im Jahre 1978 ist dem Engagement von Peter Constantin Compes zu verdanken, der damit für die Sicherheitswissenschaft und deren, zum Teil in verschiedenen Gebieten beheimateten Protagonisten, eine Austauschplattform bieten wollte. In den vergangenen drei Jahrzehnten führte die GfS zahlreiche Symposien durch, bei denen sicherheitswissenschaftliche Themen konstruktiv, teils auch kontrovers diskutiert wurden. Gleichwohl setzte sich die GfS mit ihren Symposien, aber auch mit ihren Fachpublikationen stets dafür ein, solche inhaltlichen Akzente zu setzen, mit denen die Sicherheitswissenschaft gestärkt werden sollte.

Eine Schnittmenge der Aufgabenbereiche beider Institutionen ist der Bevölkerungsschutz. Unter Bevölkerungsschutz werden alle Aufgaben und Maßnahmen eingeordnet, die sowohl auf einen angemessenen Zivilschutz als auch auf eine effektive Katastrophenhilfe abzielen. Im Kontext des Bevölkerungsschutzes erlangen die speziellen Aufgaben der Identifikation von Gefahren und Risiken, deren Bewertung sowie die Empfehlung effektiver und realisierbarer Sicherheits- und Schutzmaßnahmen vorrangige Bedeutung. Diese Aufgaben werden oft auch unter dem Begriff „Risikobeurteilung“ subsummiert. Die Aufgaben der Schutzkommission leiten sich aus dem Auftrag des „Zivilschutz- und Katastrophenhilfegesetzes“ ab, insbesondere dem Beratungsauftrag gegenüber der Bundesregierung. Die Aufgaben der GfS zielen satzungsgemäß auf die Fortschreibung der Sicherheitswissenschaft ab. In diesem Zusammenhang war und ist beiden Institutionen die sicherheitsgerichtete Forschung wichtig. Eine weitere Besonderheit, die gleichfalls den Mitgliedern beider Institutionen gemeinsam ist, ist das persönliche Ehrenamt, in dessen Rahmen sie ihre Ziele verfolgen und ihre Aufgaben wahrnehmen. Auch das vorliegende Buch sowie der ihm zugrunde liegende Workshop „Risikokompetenz“ ist das Resultat einer ehrenamtlichen Initiative von Mitgliedern, die dank der kooperativen Hebelwirkung

beider Organisationen in die Realität umgesetzt werden konnte. Im Workshop vereinten die beiden Institutionen schlussendlich eine 99-jährige sicherheitlichswissenschaftliche Historie zu dem Zweck eines synergetischen Impulses für die individuelle Verbesserung der Risikokompetenz und des Bevölkerungsschutzes in Deutschland.

Oftmals findet sich im Programmtitel von Veranstaltungen die allgemeine und aktuelle Problemstellung zu dem Leitthema, das behandelt werden soll, wieder. Mit dem vorliegenden Titel sind wir einen anderen Weg gegangen. Wir stellen eine Voraussetzung für einen allgemeinen Lösungsansatz zur Bewältigung der aktuellen Problemsituation – bei der Beurteilung von Risiken – voran. Damit sollen aber die Ergebnisse der Beiträge und möglichen Analogien nicht vorweg genommen sein.

In der ersten Sektion des Programms wird auf die allgemeine und aktuelle Situation zum Themenkomplex der Risikobeurteilung in Deutschland eingegangen. Dadurch soll ein Überblick über das Thema der Risikobeurteilung gegeben werden. Die nationale Situation ist nicht auf ihre Landesgrenzen beschränkt. Sie wird durch internationale und europäische Anforderungen und Aktivitäten beeinflusst, was im ersten Beitrag dieser Sektion erläutert wird. Im darauf folgenden Beitrag wird am Beispiel der Informationstechnologie – einer vergleichsweise neuen und trotzdem weitverbreiteten Technologie – erläutert, dass die technische Entwicklung sowie der Umgang mit dieser Technologie und deren Gefahren im Verbund erfolgen müssen. Der letzte Beitrag in dieser Sektion gibt einen Überblick über die etablierten Ansätze und Verfahren zur Risikobeurteilung. Dabei wird von den qualitativen zu den quantitativen Vorgehensweisen übergeleitet.

In der zweiten Sektion werden anhand von Beispielen Besonderheiten bei der Risikobeurteilung diskutiert. Im ersten Beitrag dieser Sektion werden die Gefahren für die Bevölkerung durch digitale Medien angesprochen. Sowohl in der Gesellschaft, als auch im Bevölkerungsschutz werden zunehmend solche Medien eingesetzt. Daraus ergeben sich neue Möglichkeiten, aber auch Gefahren. Im anschließenden Beitrag wird das Vorgehen zur Beurteilung von Risiken anhand einer bewährten Technologie, dem Eisenbahnwesen, erläutert. Der Eisenbahnverkehr ist im Kontext der Mobilität von Personen und von Gütern eine wichtige Infrastruktur der Bundesrepublik Deutschland. Gefahren im Zusammenhang mit dieser Infrastruktur betreffen einen großen Anteil der deutschen Bevölke-

rung. Während digitale Medien einen verhältnismäßig neuen Gefahrenbereich darstellen, soll der Einblick in das Eisenbahnwesen zeigen, wie die Auseinandersetzung mit Gefahren und Risiken in einem tradierten Bereich betrieben wird. Es wird interessant sein, die Vorgehensweisen, Befunde und Diagnosen beider Bereiche in der Diskussion einander gegenüberzustellen.

Die dritte und letzte Sektion behandelt Ansätze, um die gestreifte Problemstellung bei der Risikobeurteilung zu lösen. Der erste Vortrag in dieser dritten Sektion behandelt das Thema des menschlichen Verhaltens. Für die Gewährleistung von Sicherheit, aber auch für die Entstehung von Sicherheitsmängeln, ist das menschliche Verhalten von großer Bedeutung. In diesem Kontext werden Fallanalysen vorgestellt, die auf qualitativen und quantitativen Vorgehensweisen beruhen. Im Anschluss daran wird die aktuelle Diskussion zu methodischen Herausforderungen bei der Risikobeurteilung und deren Konsequenzen am Beispiel der Feuerwehrbedarfsplanung vorgestellt, wobei Schwierigkeiten und Lösungsansätze diskutiert werden. Der letzte Fachbeitrag der Sektion, aber auch der Veranstaltung, erläutert Ansätze zur fachübergreifenden Vermittlung von Kompetenzen im Umgang mit Gefahren und Risiken.

Das Programm des Workshops endete mit einer Plenardiskussion.

Über die Summe aller hier vorliegenden Fachbeiträge wollen wir einen Lösungsweg skizzieren, um den Schutz der Bevölkerung weiter nachhaltig zu verbessern.

April 2014

Prof. Dr. Uli Barth
Prof. Dr. Heinz-Willy Brenig
Dr. Sebastian Festag
Dr. Willi Marzi
Dr. Horst Miska
Prof. Dr. Peer Rechenbach

1

Eröffnung

Prof. Dr. Norbert Winker, Präsident der Gesellschaft für Sicherheitswissenschaft (GfS), Österreich

Der Begriff Risiko ist die Schnittstelle zwischen Technik und Recht. Während im Alltag Risiko ein Wagnis ist, sprechen wir in der Wissenschaft vom Produkt aus Auswirkung und Häufigkeit von Schadensereignissen. Wir wissen von der Existenz des Restrisikos, aber manchmal ist das größte Risiko der vermeintliche Glaube an die Sicherheit der Technik. Denken wir an die Katastrophe von Kaprun; die Seilbahn als solches war nicht riskant, aber in einem bestimmten Kontext, nämlich in einem sehr engen Tunnel mit entsprechender Länge ohne Beleuchtung, wurde die Situation komplexer. Sicherheit, Risiko und Angst als entgegengesetzte Pole wirken oft sehr widersprüchlich auf Menschen; z. B. ist der Risikobegriff in Fachkreisen ein Instrument der Analyse, in der Bevölkerung bewirkt er im Allgemeinen ein Gefühl der Angst. Wir wissen, das Unfallrisiko ist dann am größten, wenn wir uns am sichersten fühlen; auf den Arbeitsplatz bezogen:

- Kennen wir die Gefährdungsmöglichkeiten.
- Wissen wir alles über die damit verbundenen Risiken.
- Können wir alles kontrollieren.

Während für seltene Ereignisse das Risiko überschätzt wird, ist es für häufige unterschätzt (Daten nach H. P. Musahl, 2005):

- Geschätzte Unfallgefahr bei beruflichen Tätigkeiten: 15 % unterschätzt, 70 % zutreffend geschätzt und 15 % überschätzt.
- Anzahl der Unfälle bei den eingeschätzten Tätigkeiten: 40 % unterschätzt, 50 % zutreffend geschätzt und 10 % überschätzt.

Vor diesem Hintergrund ist es daher notwendig, um Arbeitssicherheit und Gesundheitsschutz in den Betrieben zu realisieren, die Prinzipien des Risikomanagements als Bestandteil eines erfolgreichen Unternehmens einzuführen und konsequent anzuwenden. Das heißt, das Evaluieren von Unfallrisiken ist nicht nur eine wichtige, sondern auch notwendige Aufgabe für die Prävention. Erst mit der Kenntnis der Größe der Risiken, der Eintrittswahrscheinlichkeit und der Ausmaße der Folgen können gezielt die notwendigen Gegenmaßnahmen getroffen werden.

Die GfS versucht, an dem Instrumentarium der Sicherheitswissenschaft weiterzuarbeiten, wobei einerseits Wert darauf gelegt wird, die Theorie als Hilfe für die Anwendung in der Praxis und andererseits auch zur Weiterarbeit von und mit Dritten anzuregen, um den gewünschten Erfolg für die Prävention zu erzielen.

Die GfS wünscht sich daher, mit dieser Veranstaltung einen effektiven Beitrag zur Weiterentwicklung der Sicherheitswissenschaft für den Praktiker zu leisten.

2

Impulse zum Risiko

Prof. Dr. Rolf-Dieter Wilken, Vorsitzender der Schutzkommission (SK), Deutschland

Die Schutzkommission beim Bundesministerium des Innern gibt es schon seit über 60 Jahren. Es vereinigt interdisziplinär berufene Fachleute aus den Bereichen Naturwissenschaften, Technik, Medizin und Gesellschaftswissenschaften sowie erfahrene Fachleute aus dem praktischen Zivil- und Katastrophenschutz. Das Thema „Risiko" ist deshalb ein Thema, das nicht nur im Wirtschaftsbereich als wichtig erkannt ist, sondern auch im Bevölkerungsschutz seinen Platz findet. Gerade bei der Abschätzung von Risiken und deren Verminderung und Vermeidung im Bevölkerungs- und im Katastrophenschutz muss die Risikoforschung nach unserer Meinung mehr Bedeutung gewinnen.

2.1 Die schwierige Definition von Risiko

Der Begriff Risiko (griechisch für Klippe, Gefahr) wird in verschiedenen wissenschaftlichen Disziplinen unterschiedlich definiert. Die verbreitete Definition lautet: Das Risiko wird als Produkt aus Eintrittswahrscheinlichkeit eines Ereignisses und dessen Konsequenz, bezogen auf die Abweichung von gesteckten Zielen, angesehen und ist in der Einheit der Zielgröße zu bewerten.

Das Risikokonzept des Wissenschaftlichen Beirats der Bundesregierung für Globale Umweltveränderungen (Wissenschaftlicher Beirat der Bundesregierung, 1999, XXIV) sieht ein gesellschaftliches Risiko. Zusammenfassend unterscheidet der Beirat in seinem Risikokonzept fünf Elemente:

1. Ein ideales Verständnis von Risiko, das den objektiven Grad der Gefährdung widerspiegelt.
2. Eine naturwissenschaftlich-technische Risikoabschätzung, die auf der Basis von Beobachtung und Modellbildung eine möglichst genaue Kenntnis der relativen Häufigkeiten von Schadensereignissen, gemittelt über Zeit und Region, anstrebt.
3. Eine allgemeine Risikowahrnehmung, die auf einer intuitiven Risikoerfassung und deren individueller oder gesellschaftlicher Bewertung beruht.
4. Eine intersubjektive Risikobewertung, die auf einem oder mehreren Verfahren der rationalen Urteilsfindung über ein Risiko in Bezug auf dessen Akzeptabilität bzw. Zumutbarkeit für die Gesellschaft als Ganzes oder bestimmter Gruppen und Individuen beruht.
5. Ein ausgewogenes Risikomanagement, das die geeigneten und angemessenen Maßnahmen und Instrumente zur Reduzierung, Steuerung und Regulierung von Risiken je nach Risikotyp zusammenfasst.

Und noch einmal „Risiko“: Was weiß denn schon die Bevölkerung davon? Risiko ist offensichtlich schwer zu vermitteln, denn die Mehrheit der Bürger und Bürgerinnen kann mit Wahrscheinlichkeiten – und eben auch Risiken – nicht umgehen! Auch dieses Thema muss angegangen werden!

2.2 Das Verständnis von Risiko

Die Wahrscheinlichkeit eines GAUs in einem Kernkraftwerk in Europa ist emotional hoch eingeschätzt, aber naturwissenschaftlich gesehen niedrig und berechenbar, aber dieses Risiko wird heute nicht mehrheitlich akzeptiert.

Das Restrisiko bei dem Tsunami in Japan 2011 war niedrig, aber die Folgen waren immens, als in einer Kaskade von Ereignissen nicht nur die japanischen Tsunami-Schutzmauern, sondern auch die küstennahen Kernkraftwerke erhebliche Schäden erlitten.

Hier wird über das „Restrisiko" eines „seltenen Naturereignisses/Naturkatastrophe" gesprochen. Das ist nicht nur für Experten schon sehr kompliziert.

Die Einheit des Schadensausmaßes hängt vom jeweiligen Sachgebiet ab. Es können Werte sein, die sich in Geldgrößen ausdrücken lassen, es kann sich aber auch um:

- befürchtete Tote,
- potenziell schwer Betroffene oder den
- Totalverlust eines Flugzeuges oder einer Fabrik handeln.

Selbstverständlich lässt sich nicht jedes Schadensausmaß in Geld ausdrücken, letztlich ist, mangels einheitlicher Definition für „Schaden", die Bewertung oft subjektiv.

Im Bereich des Katastrophenschutzes, genauer des Feuerwehrwesens, ist die Brandschutzbedarfsplanung mit den Themen Schutzziel und Hilfsfrist relevant. Dabei werden neben den obigen Faktoren die

- Maßnahmen zur Risikobewältigung (Mannschaftsstärke, Ausrüstung) und
- Risikoverminderung (vorzeitige Evaluierung der Risiken, politischer Konsens über Schutzziel bzw. behördliche Vorgabe des Zielerreichungsgrades) betrachtet.

Und hier ist das Restrisiko zu diskutieren. Unsicherheit und Ungewissheit können dem Begriff „Restrisiko" gleichgesetzt werden. Ja, man kann das. Allerdings kann man das auch infrage stellen. Bild 2.1 zeigt das Prinzip von Folgeanalysen. Und noch eine Folgeanalyse: Was macht die betroffene Bevölkerung? Auch das ist schwierig einzuschätzen.

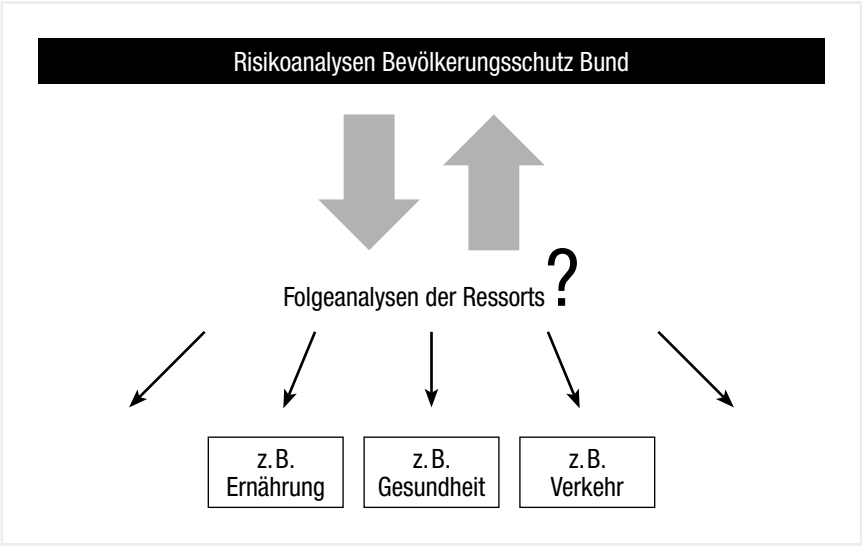

Bild 2.1 **Risikoanalysen Bevölkerungsschutz Bund**

2.3 Risiko als Prozess

1. Erkenntnislücken können durch gezielte Forschungsvorhaben geschlossen werden. Wir benötigen aber auch Weitsicht und damit auch eine ergebnisoffene Begleitforschung zu grundsätzlichen Fragen der Risiko-Definition und dem Umgang damit.
2. Durch das perspektivisch aufgezeigte Miteinander von Bürgern, Wissenschaft, Wirtschaft, Politik und Behörden auf Bundes- und Landesebene kann in Deutschland der Risikobegriff auf ein gemeinsam getragenes Maß geklärt werden.
3. Hieraus können konkrete Ansatzpunkte für den Aufgabenbereich des Bevölkerungsschutzes auf Ebene des Bundes abgeleitet werden.
4. Die Kommunikation über Risiken muss zwischen den Wissenschaftlern, den Akteuren und den interessierten Bürgern im Bevölkerungsschutz weiter entwickelt werden.

Wir brauchen [mehr] kompetente Mitbürger!

Wir sehen heute komplexe Risiken.

- Es ist zu beobachten, dass sich die Diskussion um Sicherheit aufgefächert hat, d. h., heute eine ganze Bandbreite von möglichen Risiken betrifft und sich nicht mehr auf nur wenige Bedrohungen konzentriert.
- In den 50er-Jahren sorgten sich die Menschen um einen neuen Krieg.
- Heute ängstigen sich die Menschen vor vielerlei.

Exkurs: Auto vs. Flugzeug – das subjektive Risiko

So hat es mich nicht überrascht, dass es nach dem 11. September 2001 noch viele weitere Tote zu beklagen gab: diejenigen Bürger nämlich, die nach diesem einschneidenden Datum nicht mehr ins Flugzeug, sondern ins Auto gestiegen sind. Ich erfuhr, dass dadurch 1.600 Amerikaner mehr als sonst durch Straßenunfälle ums Leben kamen. Der Terror schlägt zweimal zu […], schrieb dazu Gerd Gigerenzer (Gigerenzer: Risk Analysis 2006: 349).

Das subjektive und objektive Risiko:

- Kann man durch Umfragen ermitteln.
- Diese sind über die Zeit aber nicht stabil, sondern unterliegen Ereignissen und Meinungsbildnern.
- Sind aber heutzutage entscheidend für politische Entscheidungen und Wahlen.

Exkurs: Risiken der Transportsysteme
Der heutige Stand von rund 3.600 Verkehrstoten ist ein Ergebnis aus der Verbesserung der objektiven Sicherheit im Autoverkehr. Selbst mit dieser abnehmenden Zahl von Verkehrstoten aus dem Straßenverkehr lässt sich überzeugend vermitteln, dass der Verkehr auf der Straße die gefährlichste Form der Fortbewegung ist und das höchste Risiko birgt. Viele Umfragen zeigen, dass die Mehrheit der Bürger und Bürgerinnen das nicht glaubt. Hier muss auf intelligente Weise Aufklärung betrieben werden. Zu suchen ist hier ein ansprechender Ansatz.

5. Ethische / Soziale Dimension

Es kann heute nicht mehr nur um technisch errechenbare Risiken gehen. Heute müssen Risiken auch unter einer ethischen und sozialen Dimension gesehen werden. Die Schutzkommission diskutiert deshalb die Verantwortung des „Kompetenten Bürgers“ bei der Verringerung der Risiken. Dies betrifft beispielsweise die Sicherheit der kritischen Infrastrukturen, die von außen, aber auch von innen, gestört werden können und abhängig vom Verhalten der Bürgerinnen und Bürger sind.

Es muss darum gehen, die Zusammenhänge zwischen Kultur, Risikowahrnehmung und Katastrophenmanagement besser zu verstehen, so, z. B., den Einfluss des Klimawandels in Ländern der Dritten Welt auf die Sicherheitsstruktur in Europa abzuschätzen.

2.4 Ausblick

Die Entwicklung der Risikoforschung ist auf einem Vormarsch und vermag auf verschiedenen Wegen im Bevölkerungs- und Katastrophenschutz – was die originäre Aufgabe der Schutzkommission ist – zu neuen Ufern führen. Die Schutzkommission hat in enger Zusammenarbeit mit der Gesellschaft für Sicherheitswissenschaft e. V. die Tagung „Risikokompetenz: Beurteilung von Risiken“ durchgeführt, was deutlich macht, dass sie die neue Herausforderung annimmt und weiter entwickelt.

3

Einführung in das Programm und Vorstellung der Schutzkommission

Prof. Dr. Uli Barth, Bergische Universität Wuppertal, GfS, SK, Deutschland

Die Beratung der Bundesregierung in allen Themen des Bevölkerungsschutzes und der Katastrophenhilfe ist Teil des gesetzlich verankerten Auftrages der Schutzkommission beim Bundesminister des Innern (SK). Aufgabe der ehrenamtlich berufenen Mitglieder ist dementsprechend, insbesondere mögliche Gefahrenlagen frühzeitig zu erkennen und allfällige Präventivmaßnahmen anzuregen. Letzteres wird in dem von der SK kontinuierlich fortgeschriebenen Gefahrenbericht dem Bundesminister des Innern dargelegt. Im Zusammenhang mit der systematischen Beurteilung von Gefahrenlagen kommt der Identifizierung, der qualitativen und quantitativen Bewertung und Beurteilung entsprechender Risiken eine zunehmend wichtige Bedeutung zu. Letzteres erklärt sich insbesondere anhand der i. A. limitierten Ressourcen bei der Beurteilung selbst, bei der Risikokommunikation sowie bei der Konzeptionierung, Realisierung und Aufrechterhaltung entsprechender Sicherheits- und Schutzmaßnahmen.

Das nachfolgende Bild 3.1 vermittelt einen Überblick über den Zusammenhang von Ursache, Wirkung und Folge von relevanten Gefahren sowie präventiven und abwehrenden Maßnahmen des Bevölkerungschutzes. Es veranschaulicht dies in einem sogenannten Wirkmodell.

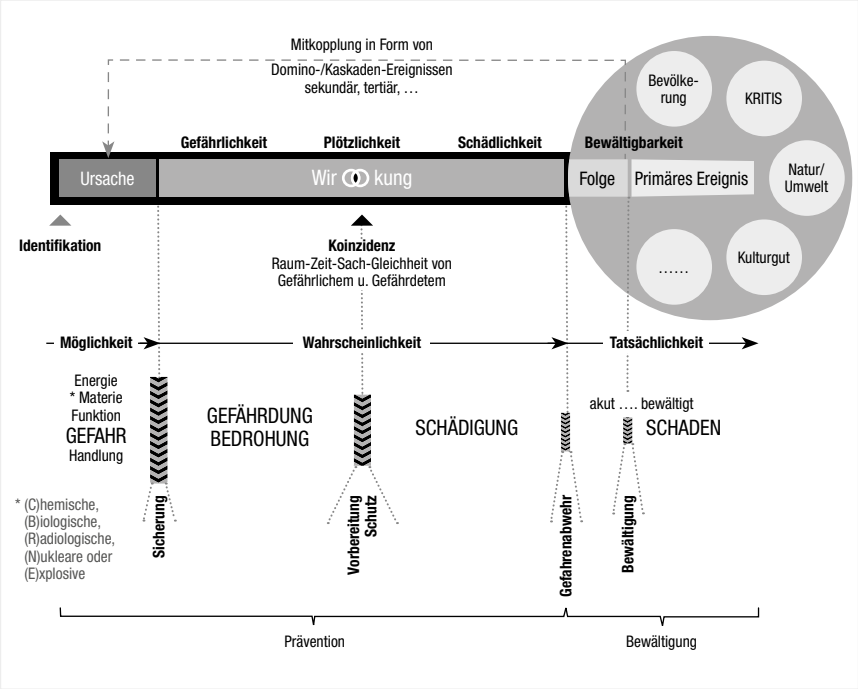

Bild 3.1: **Wirkmodell zum heutigen Beratungsauftrag der Schutzkommission**

3.1 Schutzkommission

Die nachfolgende Darstellung ist weitgehend gleichlautend von der Heimatseite der Schutzkommission beim Bundesminister des Innern übernommen worden (vgl. SK2014).

3.1.1 Gründung und Intention

Die Schutzkommission (SK) wurde im Jahr 1951 auf Anregung des Physikers Werner Heisenberg durch den damaligen Bundesinnenminister Gustav Heinemann als Kommission der Notgemeinschaft der Deutschen Wissenschaft – heute Deutsche Forschungsgemeinschaft DFG – mit der Aufgabe gegründet, „das Bundesministerium des Innern durch namhafte und unabhängige Wissenschaftler in allen Fragen zu beraten, die mit der Abwehr von Schäden durch atomare, biologische und chemische Angriffe zusammen hängen". Bereits 1961 wurde ihr ihre noch heute bestehende Form gegeben, kraft derer sie ehrenamtlich arbeitet, neue Mitglieder beruft, Unterausschüsse (heute „Fachbereiche") und Arbeitsgemeinschaften selbstständig bildet und ihre Vorsitzenden selbst wählt. An ihrer globalen Aufgabenstellung hat sich über die Jahrzehnte hinweg nichts Grundlegendes geändert. Allerdings haben sich die Schwerpunkte ihrer eigenen Forschungs- und anhaltenden Beratungstätigkeit – dem Wandel der geopolitischen Bedrohungslage entsprechend – über die mehr als 50 Jahre der Tätigkeit der Schutzkommission immer wieder verschoben.

3.1.2 Bedrohung und Aufgaben

In den ersten Jahrzehnten standen kriegerische Bedrohungsbilder im Vordergrund, die sich aus der globalen sicherheitspolitischen Lage und der Konfrontation von Ost und West ergaben und auch massive Einsätze von Kernwaffen als denkbar erscheinen ließen. Angesichts dieser Lage hat die Schutzkommission in ihrer Denkschrift aus dem Jahre 1961 mit Sorge festgestellt, dass insbeson-

dere beim Einsatz von Atomwaffen auch ein Teilschutz der Bevölkerung nur mit unverhältnismäßig hohem Aufwand zu erreichen wäre. In Konsequenz hat sie politische Entscheidungen eingefordert, insbesondere im Hinblick auf bautechnische Schutzmaßnahmen, auf Maßnahmen zur Stärkung der Selbsthilfefähigkeit der Bevölkerung, zum Aufbau eines robusten Warnsystems, zur Sicherstellung der Wasser- und Lebensmittelversorgung, zur Sicherstellung der medizinischen Versorgung der Bevölkerung, zur Bevorratung von Medikamenten und zur Bereitstellung von Krankenhauskapazitäten.

3.1.3 Epochaler Wandel vom Zivil- zum Bevölkerungsschutz

In den Jahrzehnten danach verschob sich die öffentliche Wahrnehmung dieser Bedrohungssituation trotz der ungebremsten massiven Aufrüstung in beiden Machtblöcken merklich – mit deutlichen Auswirkungen auf die Bereitschaft der Gesellschaft, für den Schutz ihrer Bevölkerung dauerhaft entsprechende Vorhaltungen zu finanzieren. Dies hatte gravierende, existenzbedrohende Auswirkungen auf die Arbeit der Schutzkommission. Zwar wurde in den 1970er und zu Beginn der 1980er-Jahre mit dem zunehmenden Ausbau der Kernenergie und der chemischen Industrie und – verursacht durch einzelne industrielle Unfälle wie z. B. in Seveso – die öffentliche Aufmerksamkeit auf mögliche Risiken der Großindustrie gelenkt, ohne dass diese jedoch als wirklich bedrohliche Risiken für die Bevölkerung in Deutschland eingestuft wurden.

Dies änderte sich freilich schlagartig mit dem Reaktorunfall am 26. April 1986 in Tschernobyl und seinen großräumigen Auswirkungen in ganz Europa. Die Folgen des Reaktorunfalls führten sehr schnell zu einer Neubewertung der Risikoeinschätzung von Großtechnologien und in weiten Teilen der Bevölkerung zu einer Erschütterung der bis zu diesem Zeitpunkt vorhandenen Vertrauensbasis. Für die Arbeit der Schutzkommission war diese Zeit verbunden mit vielfältigen Beratungen im Zusammenhang mit der Neuorganisation von technischen Einrichtungen und Organisationsformen zur Bewältigung von großräumigen Schadenslagen.

Der Zusammenbruch des Ostblocks und die damit verbundenen grundlegenden Veränderungen der sicherheitspolitischen Lage führten schließlich ab 1989 zu staatlichen Entscheidungen, insbesondere im Hinblick auf den Abbau von Maßnahmen und Vorhaltungen zur militärischen Verteidigung und – besonders tief einschneidend – des Zivilschutzes. Im Rahmen dieser Neuordnung des Zivil-

schutzes (in den Folgejahren auch immer häufiger Bevölkerungsschutz genannt) hat die Schutzkommission den Bundesminister des Innern durch beratende und warnende Voten auf vielfältige Art unterstützt.

3.1.4 Politikberatung und Forschungsplanung

Im Jahr 1996 erstellte die Schutzkommission mit ihrem „Ersten Gefahrenbericht“ eine umfassende Gefahrenanalyse, die u. a. Grundlage für die Forschungsplanung des Bundes im Bereich des Bevölkerungsschutzes wurde.

Das von der Schutzkommission stets vertretene Grundprinzip, dem zufolge Schutz- und Vorsorgemaßnahmen in Ausnahmensituationen auf Strukturen und Ressourcen aufbauen müssen, die auch in „normalen“ Zeiten genutzt und durch ständigen Einsatz erprobt werden, hat sich über die Jahrzehnte hinweg bewahrheitet. Es ist inzwischen mehr und mehr anerkannt.

Auch die Erkenntnisse der Terroranschläge vom 11. September 2001 in den Vereinigten Staaten haben daran grundsätzlich nichts geändert. Inzwischen hat sich die Welt aber insofern verändert, als dass nach weiteren Ereignissen dieser Art am 11. März 2004 in Madrid und am 7. Juli 2005 in London der Terrorismus mit all seinen Ausprägungen jetzt Gefahren auch in Europa denkbar sind, die noch vor wenigen Jahren undenkbar gewesen wären. Ereignisse dieser Art machen deutlich, dass es dringend erforderlich ist, nicht nur Gesundheit und materielle Lebensbedingungen der Menschen zu bewahren bzw. wiederherzustellen, sondern dass es entscheidend auch darauf ankommt, die ideellen Werte des Einzelnen und der Gesellschaft zu bewahren. Dies ist ein Feld, dem sich die Schutzkommission zukünftig verstärkt wird widmen müssen.

Die Schutzkommission arbeitet die gewonnenen Erkenntnisse solcher Ereignisse unter fachlichen Gesichtspunkten multidisziplinär auf und bewertet sie aus dem Blickwinkel der Wissenschaft. Im Jahr 2001 erarbeitete sie ihren „Zweiten Gefahrenbericht“ mit sechs Schwerpunkten. Ihre Empfehlungen bezüglich erforderlicher Maßnahmen richteten und richten sich nicht nur an den Bundesminister des Innern, sondern auch an die Innenminister der Länder. Sie gelten für die gesamte Aufenthaltsbevölkerung in unserem Land, also für seine Bürger wie für die, die sich sonst darin aufhalten.

Die Schutzkommission gibt auch Empfehlungen zur Planung und Durchführung neuer Forschung ab und unterstützt damit das 2004 neu errichtete Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) in seiner Aufgabenerfüllung. Außerdem bewertet sie in zunehmendem Maße in Form von „Aktuellen Stellungnahmen" wichtige Einzelthemen, wie z. B. zur Sicherstellung der medizinischen Versorgung in einem veränderten Gesundheitssystem und angesichts neuartiger Seuchenbedrohungen.

Das nachfolgende Bild 3.2 vermittelt einen Überblick über Funktionen, Mittel und Zweck der Schutzkommission und veranschaulicht die Zusammenhänge in einem sogenannten Prozessmodell.

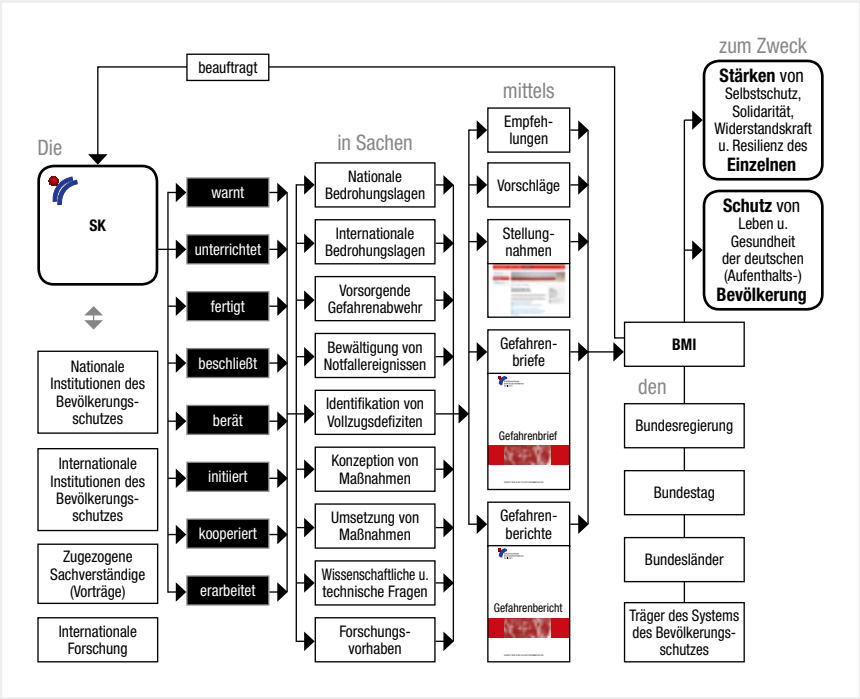

Bild 3.2: **Prozessmodell zum heutigen Beratungsauftrag der Schutzkommission**

3.1.5 Ehrenamt als Basis

Die Schutzkommission hat sich in ihrem langen Bestehen von mehr als sechs Jahrzehnten in vielfältiger Weise gewandelt und damit veränderten gesellschaftlichen Rahmenbedingungen Rechnung getragen. Ihre Arbeit war jedoch stets von den Prinzipien des ehrenamtlichen staatbürgerlichen Engagements und der wissenschaftlichen Fundierung geprägt. Diese Tugenden werden auch in Zukunft ihre Handlungsmaxime sein, damit die Bundesrepublik Deutschland die Herausforderungen des 21. Jahrhunderts zu beantworten vermag.

3.2 „Risikokompetenz: Beurteilung von Risiken“

Der Workshop Risikobeurteilung zielt darauf ab, den einschlägigen Wissensstand an der Grenze bewährter Methoden bzw. Verfahren und möglicher neuer Ansätze im Rahmen ausgewählter Fachvorträge durch einschlägig ausgewiesene interne und externe Referenten darzustellen. Der Workshop zielt ferner darauf ab, die Anwendungsgrenzen des klassischen/tradierten Risikobegriffs, der die Wahrscheinlichkeit und die Auswirkungsschwere eines Katastrophenereignisses verknüpft, zu hinterfragen (z. B. „black swans“) und allfällige, geeignete neue Ansätze zu identifizieren.

Zu diesem Zweck sieht der Projektantrag vor, dass der angedachte Workshop unter fachlicher Beteiligung der Gesellschaft für Sicherheitswissenschaft e.V. (GfS) geplant und veranstaltet werden soll. Die Gesellschaft für Sicherheitswissenschaft e.V. wurde 1978 in Wuppertal gegründet, um der Sicherheitswissenschaft ein Forum zu sein, das ihre Weiterentwicklung fördern und ein Zusammenwirken mit angrenzenden Fachgebieten ermöglichen soll (vgl. GfS2014). Im Verständnis der GfS ist die Sicherheitswissenschaft die Forschung und Lehre von der methodischen und systematischen Analyse und Kontrolle der Risiken, speziell der Mensch-Technik-Umwelt-Systeme, zum Zwecke der Verringerung der Häufigkeit und Schwere von Schäden und Verlusten mit risikologischen Strategien. Die GfS führt seit ihrer Gründung nationale und internationale Symposien durch und verfügt über eine eigene Publikationsreihe.

Da die GfS gleichfalls beabsichtigte, die Risikobeurteilung im Jahr 2014 zu thematisieren, bot sich eine fachliche Beteiligung in der Weise an, dass die inhaltliche Planung und Moderation des Workshops kooperativ von GfS und SK erfolgt. Dadurch wurde gleichsam die fachliche Expertise der GfS genutzt wie auch deren Netzwerk angesprochen und in den wissenschaftlichen Diskurs einbezogen. Die Veranstaltung des Workshops übernahm die SK, unterstützt durch deren Geschäftsstelle beim BBK.

Als Ergebnis aus diesem Workshop möchte die Schutzkommission

- Anregungen bezüglich der fachlichen und semantischen Bewertung und Beurteilung von Risiken im Rahmen der Politikberatung und für die deutsche Aufenthaltsbevölkerung formulieren sowie
- Empfehlungen zur Verbesserung aussprechen.

Das Ergebnis soll dazu beitragen, dass die Ausführungen im Gefahrenbericht und anderen Stellungnahmen der Schutzkommission noch präziser und verständlicher werden. Im Nachgang zu der Veranstaltung ist eine Veröffentlichung wesentlicher Inhalte und Ergebnisse mit dem vorliegenden Papier, als Veröffentlichung im Rahmen der Publikationen der Schutzkommission, hiermit gegeben. Die Ergebnisse und Empfehlungen aus dem Workshop wie auch die im 5. Gefahrenbericht veröffentlichten Fragestellungen fließen unmittelbar in die weitere Beratungsarbeit der Schutzkommission ein. Nach der Veröffentlichung stehen sie selbstverständlich auch interessierten Dritten zur Verfügung.

Literatur

Barth2013 Barth, U.: Vulnerabilitäts- und Resilienzanalyse. Vorlesung im akkreditierten Bachelorstudiengang „Sicherheitstechnik“, Studienschwerpunkt „Brand- und Bevölkerungsschutz“ an der Bergischen Universität Wuppertal, Wintersemester 2013/14.

BBK2008 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) [Hrsg.]: 50 Jahre Zivil- und Bevölkerungsschutz in Deutschland. ISBN-968-3-939347-13-2. Bonn, Oktober 2008.

Daase2013 Daase, C.; Engert, S.; Junk, J.: Verunsicherte Gesellschaft – Überforderter Staat: Zum Wandel der Sicherheitskultur. ISBN 978-3-593-39873-0, Campus Verlag GmbH, Frankfurt am Main, 2013.

Engelhard2011 Engelhard, N.; Schulze, J.; Barth, U.: Im tiefsten Frieden? Thesen zur asymmetrischen Bedrohung unter dem spezifischen Blickwinkel des Bevölkerungsschutzes. Bevölkerungsschutz 3 | 2011, S. 18ff., herausgegeben im Auftrag des Bundesministeriums des Innern (BMI) vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Provinzialstraße 93, 53127 Bonn, http://www.bbk.bund.de. Bonn, März 2011.

GfS2014 Gesellschaft für Sicherheitswissenschaft e.V. [Hrsg.]: Heimatseite der Gesellschaft für Sicherheitswissenschaft. http://www.gfs-aktuell.de/index.html abgerufen am 10.04.2014.

Gleißner2011 Gleißner, W.: Grundlagen des Risikomanagements im Unternehmen – Controlling, Unternehmensstrategie und wertorientiertes Management. ISBN 978 3 8006 3767 6, 2. Auflage, Verlag Franz Vahlen GmbH, München 2011.

Koch2013 Koch, C.: Risiko: Sozialwissenschaftliche, ökologische und systemtheoretische Perspektiven zur Unsicherheit. ISBN 978-3-643-12257-5, LIT Verlag Dr. W. Hopf, Berlin 2013.

Feinendegen2011 Feinendegen, L.: 60 Jahre Schutzkommission beim Bundesminister des Innern. http://www.schutzkommission.de abgerufen am 10.04.2014, 27. Mai 2011.

Renn2014 Renn, O.: Das Risikoparadox – Warum wir uns vor dem Falschen fürchten. ISBN 978-3-596-19811-5, S. Fischer Verlag GmbH, Frankfurt am Main 2014.

SK2014 Schutzkommission [Hrsg.]: Heimatseite der Schutzkommission. http://www.schutzkommission.de abgerufen am 06.04.2014.

4

Die Bedeutung der Risikokompetenz für die Beurteilung von Sicherheitssituationen

4.1 Einleitung

Dr. Sebastian Festag, Hekatron, GfS, Deutschland

Sowohl die Schutzkommission beim Bundesministerium des Innern als auch die Gesellschaft für Sicherheitswissenschaft e. V. befassen sich auf einer wissenschaftlichen Grundlage mit dem Schutz vor Gefahren. Das vorliegende Programm entstand in einer Zusammenarbeit und beschränkt sich in Anlehnung an die gemeinsame inhaltliche Schnittmenge auf den Schutz der Bevölkerung, wobei wir uns mit dem Programm auf die aktuellen Besonderheiten bei der Beurteilung von Risiken konzentrieren wollen.

Während die Gesellschaft für Sicherheitswissenschaft regelmäßig Fachbeiträge im Ausland leistet, ist es ihr mit dem vorliegenden Programm – nach einigen Jahren – wieder gelungen, in Deutschland eine sicherheitswissenschaftliche Fachdiskussion anzuregen. Und obwohl es sich bei dem hier zur Diskussion stehenden Inhalt um kein neues Thema handelt, fordert die aktuelle Situation zum Handeln auf.

Bevor ich auf den Inhalt des vorliegenden Programms eingehe, sollen einige grundlegende Überlegungen über die sicherheitswissenschaftliche Disziplin und die Philosophie der Gesellschaft für Sicherheitswissenschaft angesprochen werden. Beides, so scheint mir, ist in der letzten Zeit partiell in Vergessenheit geraten. Anschließend wird das Hauptthema „Risikobeurteilung und -kompetenz“ kursorisch erläutert, um erste Impulse zur Diskussion zu liefern, aber auch um zu Beginn des Programms zumindest in Teilen ein gemeinsames Verständnis zu fördern. Der Rahmen meines Beitrages zwingt mich, meine Ausführungen auf Grundlegendes und Dringliches zu beschränken.

4.2 Erste Schritte der Sicherheitswissenschaft

Die Auseinandersetzung mit Gefahren und Risiken ist kein neuer Gedanke. Seit jeher haben Menschen das Bedürfnis, sich vor Gefahren zu schützen. Mit dem Laufe der Zeit und dem technischen Fortschritt haben sich die Gefahren für die Menschen verändert. Manche Gefahren wurden erkannt und kontrolliert. Andere Gefahren entstanden neu oder verlagerten sich zu neuen Schwerpunkten. Für die zugrunde liegenden Kausalbedingungen zahlreicher Gefahren, vom Anlass über den Ablauf bis zum Ausgang, entwickelte sich mit der Zeit ein geordnetes Verständnis. Daraus wurden systematische und methodische Analyse- und Bewertungsverfahren abgeleitet, auf deren Grundlage sich geeignete Strategien zur Gefahren- bzw. Risikobewältigung stützen sollten (siehe Bild 4.1). Dieser gesamte Komplex zieht sich durch alle Lebensbereiche und hat Anschlüsse in allen wissenschaftlichen Disziplinen, wie Bild 4.2 veranschaulicht. Da Gefahren neben ihren fallspezifischen Eigenheiten auch grundsätzliche Komponenten beinhalten, mündete die Auseinandersetzung mit ihnen und ihren Charakteristika in einer eigenständigen und in sich geschlossenen Disziplin, der Sicherheitswissenschaft (z. B. Compes, 1991, vgl. auch Radandt, 2014). Sie bündelt die Erkenntnisse über Gefahren und entwickelt daraus eine eigene Fachsystematik, -methodik und -terminologie – was durch ihre interdisziplinäre Ausrichtung ermöglicht wird.

Ein großer Teil von Gefahren spielt sich hierzulande in „sozio-technischen“ Systemen ab, bei denen sowohl Menschen als auch Maschinen in einer gemeinsamen Umgebung zusammenwirken. Mit möglichen Gefahren solcher Systeme, im weitesten Sinne, befasst sich die Sicherheitstechnik (vgl. Festag, 2014 oder Hartwig & Festag, 2012). Unter Sicherheitstechnik werden Techniken im Sinne von Kunstfertigkeiten, […] um Sicherheit [weitestgehend] zu erreichen (Compes, 1975; siehe auch Seidel, 2008), verstanden, wobei auch Auslegungen in Form von Sicherheit der Technik und Sicherheit durch Technik existieren. Sicherheitstechnik ist ein Bestandteil der Sicherheitswissenschaft. Vergleichbar mit der Medizin hat sie das Ziel, Menschen und ihre Umwelt vor Gefahren zu schützen (z. B. Festag, 2014). Seit ihrer Gründung steigt der sachliche Bedarf an Forschung und Lehre auf diesem Gebiet entsprechend dem technischen Fortschritt immanent (vgl. Hartwig, 2005).

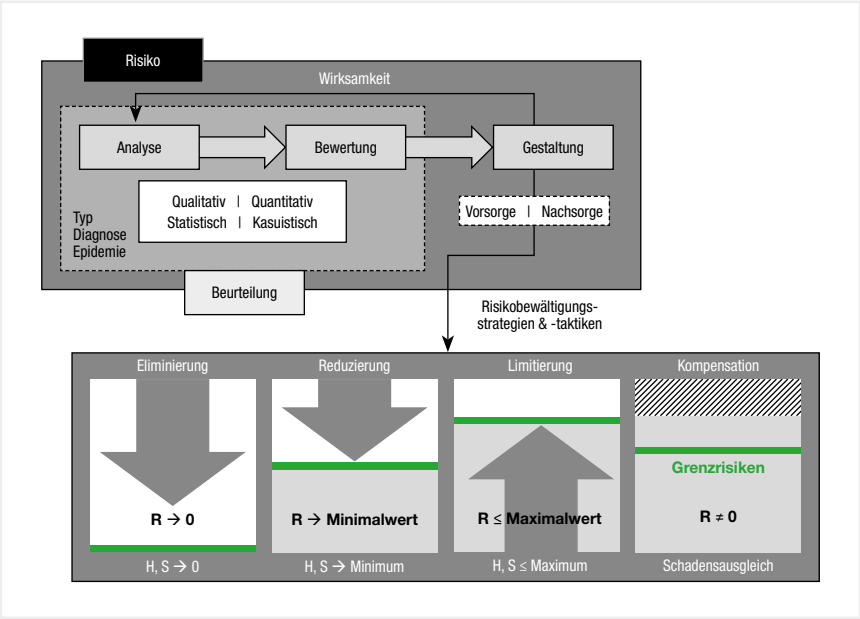

Bild 4.1: **Risikobeurteilung: Allgemeines Vorgehen (teilweise in Anlehnung an Compes, 1991)**

Sicherheitswissenschaft ist die Forschung und Lehre von der methodischen und systematischen Analyse und Kontrol le von Risiken zum Zwecke der Vermeidung bzw. Verringerung von Schäden und Verlusten mit risikologischen Strategien (vgl. GfS, 13.01.2014).

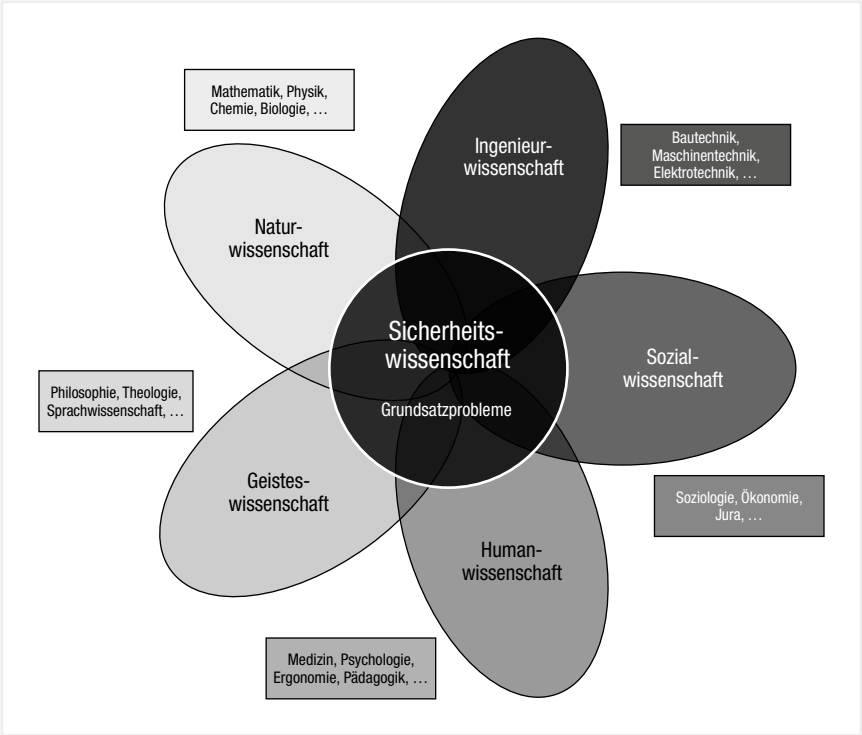

Bild 4.2: **Struktur der Sicherheitswissenschaft (in Anlehung an Compes, 1991, modifiziert)**

Um die an die Problemstellung heute unverändert angepasste Gründungsphilosophie der Sicherheitswissenschaft, ungeachtet universitärer und politischer Strömungen, weiterzuentwickeln bzw. aufrechtzuhalten, wurde am 23. März 1978 die Gesellschaft für Sicherheitswissenschaft als Verein in Wuppertal gegründet. Die Gesellschaft für Sicherheitswissenschaft hat die Ziele:

- die Sicherheitswissenschaft in ihrer fachübergreifenden Gestalt und Anwendung, insbesondere im Zusammenwirken mit anderen Wissenschaften, weiterzuentwickeln;
- die Erforschung und Untersuchung sicherheitswissenschaftlicher Fragestellungen zur Vermeidung von Gefahren zu fördern;

- Erkenntnisse und Erfahrungen auf allen Gebieten der Sicherheitswissenschaft zu verbreiten bzw. auszutauschen und
- den Nachwuchs im sicherheitswissenschaftlichen Bereich zu fördern.

Zu ihren Aufgaben gehören die:

- Beteiligung an der Entwicklung der Sicherheitswissenschaft, vor allem ihrer Fach-Systematik und -Methodik sowie der zugrundeliegenden Terminologie und Methodologie (z. B. der sicherheitswissenschaftlichen Risikologie);
- Unterstützung der Bemühungen um den Auf- und Ausbau der Forschung und Lehre der Sicherheitswissenschaft in den dafür kompetenten Institutionen;
- Anregung wissenschaftlicher Arbeit in ihrem Fachgebiet durch Auszeichnungen und Unterstützungen;
- Pflege von Verbindungen mit Institutionen, Stellen und Personen, die sich einschlägig mit der Sicherheitswissenschaft in Theorie und Praxis befassen und
- Initiierung und Förderung der wissenschaftlichen Diskussion von Fragestellungen und Lösungsvorschlägen des Fachgebiets durch Anregungen, u. a. durch Veröffentlichungen und Tagungen etc. (GfS, 13.01.2014).

Kommen wir nun zu dem vorliegenden Programm und konzentrieren uns auf das Hier und Heute und begreifen wir das Programmthema als ein Querschnittsthema der Sicherheitswissenschaft und Sicherheitstechnik.

4.3 Risikobeurteilung und -kompetenz

Eine Beurteilung setzt sich aus einer Analyse und Bewertung zusammen. An dieser Stelle ist es angebracht, zwischen den Begriffen Gefahr, Gefährdung und Risiko zu unterscheiden, da sie sich auf unterschiedliche Sachverhalte beziehen (siehe Bild 4.3).

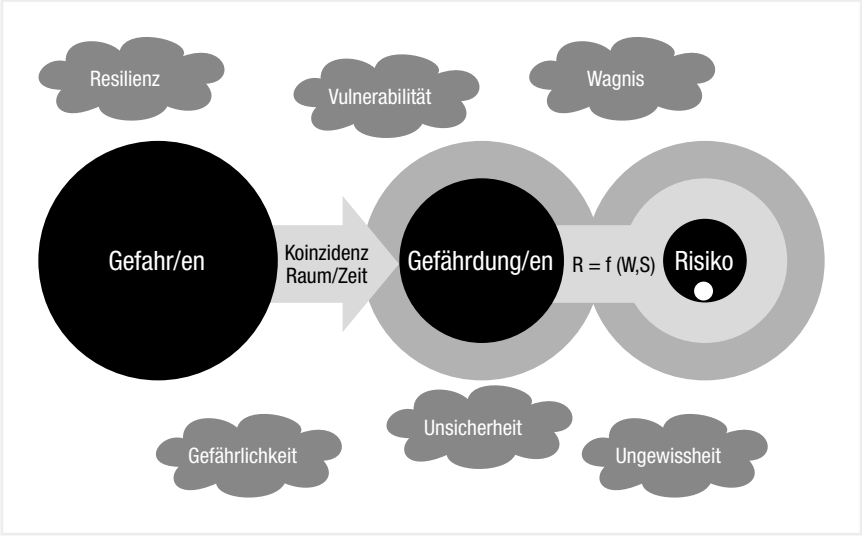

Bild 4.3: **Beurteilung der Sicherheitssituation – Begriffliches**

Es sei vorweggenommen, dass sich Begriffe oftmals keinem einheitlichen Verständnis unterziehen. Das gilt zwar grundsätzlich, allerdings kommt in der Sicherheitswissenschaft erschwerend hinzu, dass es sich bei ihr – vergleichsweise zu anderen Wissenschaften – um ein junges akademisches Grundlagenfach handelt und sich für einige zentrale Begriffe bis heute keine allgemein akzeptierte Bezeichnung entwickelt hat. Um die nachstehenden Gedanken nachvollziehbar zu gestalten, sei nur so viel gesagt: Vereinfacht wird von einer Gefahr gesprochen,

wenn von einer Quelle die Möglichkeit einer Schädigung ausgeht (vgl. Compes, 1991). Es ist auch die Rede von Ereignissen mit einem möglichen gefährlichen Ausgang. Überlagern sich die Wirkungsbereiche zwischen der Gefahr und einem zu schützenden Gut oder System (z. B. Personen, Sachen oder Werte) räumlich und zeitlich, wird aus der Gefahr eine Gefährdung (vgl. Skiba, 1973). Wird eine Gefahr über das Produkt aus der Eintrittswahrscheinlichkeit eines gefährlichen Ereignisses und dem Ausmaß des Schadens beschrieben, wird dagegen von einem Risiko gesprochen. Wichtige Sachverhalte werden bei diesem verkürzten Verständnis vernachlässigt. So wird zum Beispiel bei einem unerwünschten Ereignis von einem Risiko gesprochen, während bei einem erwünschten Ereignis von einer Chance die Rede ist. Die Einschätzung, ob etwas erwünscht oder unerwünscht ist, hängt dabei vom Betrachter und seiner Wahrnehmung ab. Diese kann von Individuum zu Individuum und innerhalb von Gesellschaften, den Zeitpunkten und in Abhängigkeit vom herangezogenen Bewertungsmaßstab variieren. Beim Schädlingsbekämpfungsmittel Dichlordiphenyltrichlorethan (DDT) ist das beispielsweise der Fall. Zunächst wurde für diese Entwicklung im Jahre 1948 der Nobelpreis verliehen. Als aber offensichtlich wurde, dass DDT über die Nahrungsmittelkette unter anderem zum Aussterben ganzer Vogelarten führte, wurde der Einsatz in einigen Staaten verboten (vgl. Hartwig, 1997). Hier kam es zu einer Neuorientierung des Wertesystems (insbesondere durch die Langzeitbetrachtung) und einer damit verbundenen Neuorientierung bei der (Risiko-)Bewertung.

Entsprechend der Abstufung der Begriffe gibt es sowohl Gefahrenanalysen als auch Gefährdungsanalysen und Risikoanalysen, wobei sich der Blickwinkel in dieser Reihenfolge im Allgemeinen verengt, während sich der Detailliertheitsgrad, Informationsgehalt sowie Analyseaufwand erweitern. Zur Analyse von Gefahren, Gefährdungen und Risiken stehen uns verschiedene Verfahren und methodische Ansätze zur Verfügung. Auch für die Bewertung der Situationen haben sich verschiedene Herangehensweisen eingebürgert. Hinzu kommt, dass die Beurteilung der Sicherheitssituation an fallspezifische Gegebenheiten gebunden ist.

4.3.1 Der Fehlschluss einer umfassenden Risikokontrolle

Im Laufe der Jahrzehnte haben sich neue und feinere Verfahren zur Analyse und Bewertung von Sicherheitsproblemen (von Gefahren bis zu Risiken) durchgesetzt. Doch trotz aller Spezialisierung lösen diese Verfahren heute nicht alle Sicherheitsprobleme. Und in diesem Zusammenhang tauchen mittlerweile

weitere und teilweise neue Begriffe auf, wie beispielsweise Vulnerabilität, Resilienz, Ungewissheit (Gigerenzer, 2013) oder „schwarze Schwäne“ (Thaleb, 2010). Dabei ist die dem Sachverhalt zugrunde liegende Problemstellung nicht nur eine terminologische, sondern vor allem eine methodische.

Unsere Umwelt ist ständig Veränderungen unterworfen, die zu einer kontinuierlichen Veränderung der Sicherheitssituation führen. Durch neue Systeme entstehen ständig neue und andersartige Probleme, die spezifische Analyse- und Bewertungsmodalitäten und neue sicherheitsgerechte Lösungen verlangen, wie z. B. bei Gefahren durch digitale Medien (vgl. Spitzer, 2013). Es verwundert daher nicht, dass wir mit Sicherheitsproblemen konfrontiert sind, zu denen erst Lösungen erarbeitet werden müssen. Zwischen den Sicherheitsproblemen und Lösungen ist eine kontinuierliche Anpassung erforderlich. Zur Lösung von Sicherheitsproblemen stehen uns heute zahlreiche Verfahren zur Verfügung. Sie sind stellenweise sehr aufwendig und kompliziert. Im Allgemeinen basieren die Verfahren auf der Grundlage weniger methodischer Zugänge, wobei uns die Beurteilung von schwerwiegenden Risiken unter methodischen Gesichtspunkten vor besondere Herausforderungen stellt.

Ungeachtet der Herausforderungen durch neue Systeme und der methodischen Zugänge, kommt ein Punkt hinzu, der an dieser Stelle wichtig ist. Von Fachleuten, aber auch von der Bevölkerung, werden im Umgang mit Gefahren und Risiken Kompetenzen abverlangt, die in weiten Teilen der Bevölkerung, aber oftmals auch bei Fachexperten (vgl. Gigerenzer, 2013), nicht vorhanden sind. Die Situation ist kritisch, weil alle Menschen von Gefahren betroffen sind. Ein solcher Mangel ist bei Fachspezialisten besonders problematisch, weil ihre Einschätzung oftmals als Grundlage für weitreichende Entscheidungen dient, von denen unter Umständen viele Personen betroffen sind. Eine besondere Rolle nehmen dabei Sicherheitsfachspezialisten ein, die davon gesondert zu betrachtend sind.

4.3.2 Das Problem bei der Beurteilung schwerwiegender und seltener Risiken

Kommen wir nochmal auf die methodischen Herausforderungen der Jetztzeit und die Beurteilung von Sicherheitssituationen zurück und wagen wir einen Versuch für eine vorläufige Problembeschreibung. Dazu ziehen wir zur Verdeutlichung Bild 4.4 heran und betrachten die Problemstellung als eine grundsätzliche auf der Basis von zwei ineinander verwobenen Elementen.

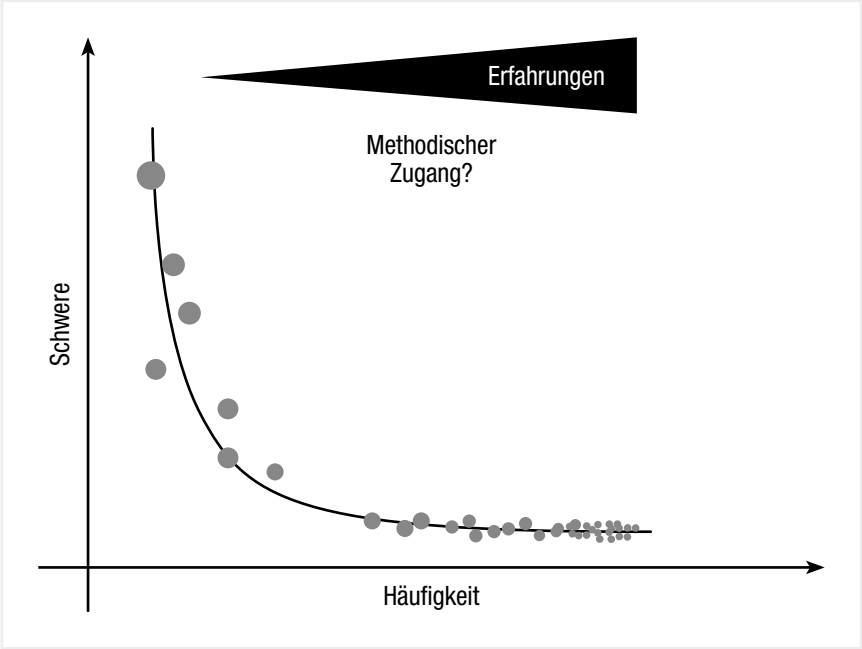

Bild 4.4: **Risikospektrum**

Erstens: Das Risikospektrum umfasst seltene und folgenreiche Ereignisse (schwerwiegende Risiken) bis zu häufigen und folgenarmen Ereignissen. Schwerwiegende Risiken, in der Nähe der Ordinate von Bild 4.4, unterliegen per Definition dabei besonderen Eigenschaften. Aufgrund ihrer höchst seltenen Ereigniseintrittswahrscheinlichkeit liegen für sie im Allgemeinen keine Erfahrungen aus der Vergangenheit vor, die in die Sicherheitsstrategien eingebunden werden können. Alle Vorgehensweisen und Instrumente, die sich auf Erfahrungen stützen, stehen zur Beurteilung der Situationen in diesen Fällen damit nicht – oder nur sehr eingeschränkt – zur Verfügung. Nebenbei bemerkt: Dieser Sachverhalt verschärft sich durch eine erfolgreiche und vorbeugende Sicherheitsarbeit. Denn ihr Ziel ist die Vermeidung von Gefahren bzw. Risiken, wenn möglich vor dem Ereigniseintritt. Damit werden gleichzeitig auch Erfahrungen verhindert (vgl. Musahl, 1997). Bei Risiken, die mit geringen Folgen verbunden sind, ist die Situation eine etwas andere. Aufgrund ihrer Frequenz existieren hier im Allgemeinen – wenn auch wenige – Erfahrungen.

Exkurs: Erfahrungen

Erfahrungen sind für die Situationsverarbeitung von Menschen und die Beurteilung von Sicherheitssituationen wichtig. Über Erfahrungen und das Wiederholen von Verhaltensweisen bilden Menschen Regeln (z. B. Rasmussen, 1983), die zu Gewohnheiten und Einstellungen führen (vgl. Burkhardt, 1981). Das geschieht ständig und teilweise, ohne den Betroffenen bewusst zu sein. Je nach Verarbeitungstiefe ist die Rede vom wissens-, regel- oder fertigkeitsbasierten Verhalten (vgl. Rasmussen, 1986, Reason, 1990). Erfahrungen und Regeln vereinfachen uns das Leben. Durch sie müssen Menschen zum Beispiel nicht darüber nachdenken, wie sie mit dem Schlüssel die Haustüre öffnen oder über zahlreiche kleine Handlungsschritte Auto fahren. Menschen lernen kontinuierlich (auch in Sachen Sicherheit), womit Änderungen und Verfestigungen bis hin zu Automatismen im Verhalten verbunden sind. Je nach Interpretation und Wertung vorausgegangener Ereignisse führen Erfahrungen dazu, dass Verhaltensweisen seltener (Löschung und Abschwächung) oder häufiger (Verstärkung) werden (vgl. Musahl, 1997). Die Verstärkung wird in zwei Wirkungsweisen unterteilt. Es kommt zu einer positiven Verstärkung, wenn auf das Handeln für den Handelnden etwas subjektiv Positives folgt. Die Handlung wird dann über eine „Wenn-dann-Verknüpfung" gespeichert (vgl. Musahl, 2009) und bei zukünftigen und ähnlichen Situation erneut abgerufen (und verfestigt). Im Rahmen von Sicherheitsbetrachtungen wird das genutzt, indem z. B. sicherheitsgerechtes Handeln belohnt wird. Nach diesem Prinzip werden auch sicherheitswidrige Verhaltensweisen bestraft, wobei in diesem Fall bestimmte Verhaltensweisen seltener statt häufiger werden sollen. Menschliche Verhaltensweisen orientieren sich an Erfahrungen, die stark durch das tägliche Leben geprägt werden – also im „Normalzustand" der Systeme. Sie bestätigen uns im Alltag und können so zu einer negativen Verstärkung führen. Diese Erfahrungen sind im Ereignisfall oftmals untauglich. Musahl (2009) betont die Bedeutung dieser negativen Verstärkung bei der Sicherheitsarbeit. Diese im Menschen tief verwurzelten Abläufe sind wichtig (zum Schutz vor Reizüberflutungen), aber sie sind nicht unproblematisch, da sie die Realität verkürzen und Fehlschlüsse produzieren können, was wiederum bei der Beurteilung von Gefahren eine wichtige Rolle spielt. Schwerwiegende Risiken finden sehr selten statt und unterliegen diesem Muster im besonderen Maße (Wie oft erlebt ein Mensch – von Ausnahmen abgesehen – einen großen Brand und kann erfolgreiche Reaktionsweisen als Erfahrung für später abspeichern?).

Zweitens: Anhand von Erfahrungen, Informationen und Daten werden heute Modelle zur Prognose von Ereignissen entwickelt. Auf diese Weise sollen Lehren aus bereits stattgefundenen Ereignissen gezogen werden, die in die Bewältigung zukünftiger Ereignisse einfließen sollen. Solchen Prognosen sind stellenweise enorme Erfolge zu verdanken, weshalb sie sich heute allgemein einbürgern. Während sich mit der Zeit neben dem „Versuch und Irrtum" (trail and error) auch systemanalytische Vorgehensweisen durchsetzen, wurden in diesem Zuge schrittweise technische auf natürliche Anwendungen übertragen und ausgeweitet. Das Vorgehen bzw. die Verfahren stützen sich dabei auf eine Modellvorstellung unter Zuhilfenahme von (statistischen) Daten. Sie sind zur Abschätzung und Prognose von Risiken aber nur dann sinnvoll und nützlich, wenn Erfahrungen und bekannte Wirkungszusammenhänge existieren. Es ist davon auszugehen, dass diese Situation bei den folgenarmen Risiken (nahe der Abszisse in Bild 4.4) und vor allem bei „einfachen" technischen Systemen oftmals gegeben ist. Aber bei schwerwiegenden Risiken liegen die Dinge anders. Hier sind die (erfahrungsbasierten) Modellvorstellungen unvollständig, wo natürliche Phänomene einschließlich menschlicher Verhaltensweisen bedeutend sind. Da aber in der Geschichte auch für natürliche Phänomene Prognosen geglückt sind (z. B. Berechnung der Wiederkehr von Kometen oder bei der Verwendung von Proxydaten zur Bestimmung von Klimaveränderungen), hat sich schon vor einiger Zeit die Vorstellung einer allgemein modellierbaren und berechenbaren Welt – nach dem technischen Vorbild – eingeschlichen. Modelle sind aber Reduzierungen der Wirklichkeit. Das trifft besonders auf komplexe Systeme wie Menschen und die Natur zu.

Zur Überwindung der Situation – so viel können wir schon sagen – sind umfangreiche sicherheitswissenschaftliche Forschungsprogramme erforderlich, die sich auf ein detailliertes Verständnis über die Problemabläufe stützen. Neben der ausführlichen Erarbeitung von Erkenntnissen auf diesem umfangreichen Gebiet bedarf es der Steigerung des Problembewusstseins – zu dem das vorliegende Programm einen kleinen Beitrag liefern will. In einem weiteren Schritt ist die Schaffung eines generellen Sicherheitsverständnisses in der Bevölkerung notwendig.

4.3.3 Förderung von Kompetenzen

Der Kompetenzbegriff wird in verschiedenen Disziplinen unterschiedlich verwendet, wie Bild 4.5 verdeutlicht. Zur Herkunft des Begriffes siehe z. B. Seebold (2011) oder Henne, Kämper und Objartel (2002). In Anlehnung an das psychologische und pädagogische Kompetenzverständnis sind unter Gefahrenkompetenzen alle Fähigkeiten und Fertigkeiten von Menschen zur Lösung von Sicherheitsproblemen in (beliebigen) Situationen zu verstehen. Die Risikokompetenz hingegen begrenzt diese Fähigkeiten und Fertigkeiten auf die Abschätzung der Eintrittswahrscheinlichkeit von gefährlichen Ereignissen und deren Schweregrade. Dazu bedarf es zusätzlich zum allgemeinen Verständnis von Gefahren eines (risiko)logischen und in Anlehnung an Gigerenzer (2013) eines statistischen Denkens. Das erfordert allerdings, dass die zugrunde liegenden Wirkungszusammenhänge des betrachteten Risikos weitestgehend bekannt sind und Erfahrungen existieren. Bei neuen Risiken und Risiken mit teilweise unbekannten Abläufen sowie bei den schwerwiegenden Risiken (höchstseltene Ereignisse mit hohem Grad an Ungewissheit) sind diese Voraussetzungen oft nicht gegeben. Hier müssen alternative Wege erarbeitet werden – momentan scheinen Intuitionen und Emotionen dabei eine wichtige Rolle zu spielen. Sowohl für die Beurteilung solcher Gefahren und Risiken als auch für die Kompetenzvermittlung fehlt es an wissenschaftlichen Grundlagen und dementsprechend an Konzepten zur Problemlösung.

Trotz des Fehlens konkreter Lösungswege gilt es an dieser Stelle, etwas Allgemeines zu den Adressaten und Anknüpfungspunkten der Kompetenzvermittlung festzuhalten, um die Größenordnung der Aufgabe deutlich zu machen.

Die Vermittlung von Kompetenzen im Umgang mit Gefahren und Risiken betrifft die Allgemeinheit in einer generellen, die Fachspezialisten (Mediziner, Juristen, Pädagogen etc.) in einer zusätzlich universitär-speziellen und die Sicherheitsfachspezialisten in einer universitär-generellen und sicherheitswissenschaftlich-speziellen Weise (vgl. Compes, 1991). Die inhaltliche Auswahl und Tiefe muss an das jeweilige Fachgebiet und das Qualifikationsniveau kontinuierlich angepasst sein (siehe Bild 4.6).

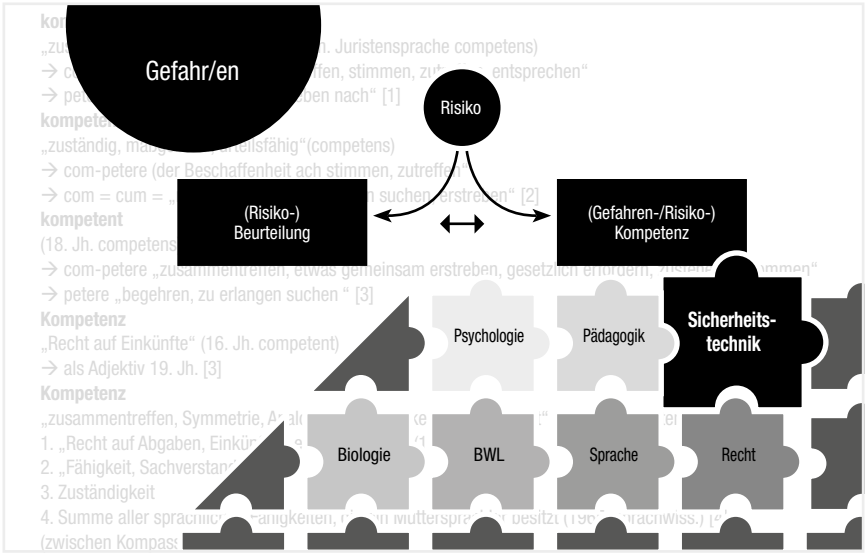

Bild 4.5: **Kompetenz – Begriffsabgrenzung**

Damit die Bevölkerung in der Lage ist, sich in subjektiv angemessener Weise mit Gefahren und Risiken auseinanderzusetzen, ist deren Ausstattung mit sicherheitsspezifischen Grundkompetenzen erforderlich, wobei eine frühe und übergreifende Kompetenzvermittlung notwendig ist, d. h. über alle Entwicklungs- und Sozialisationsstufen. Dafür bieten sich verschiedene Anknüpfungspunkte im Laufe eines Lebens an, wie Bild 4.7 zeigt. Der früheste Zeitpunkt liegt außerhalb unserer direkten Reichweite und betrifft die Veranlagung. Anders sieht das bei der Erziehung und Sozialisation aus. Heute erfolgt, zumindest in Teilen, eine Sensibilisierung beim Umgang mit Gefahren in Abhängigkeit von der Sport- und Freizeitgestaltung (z. B. beim Flugunterricht oder Sport).

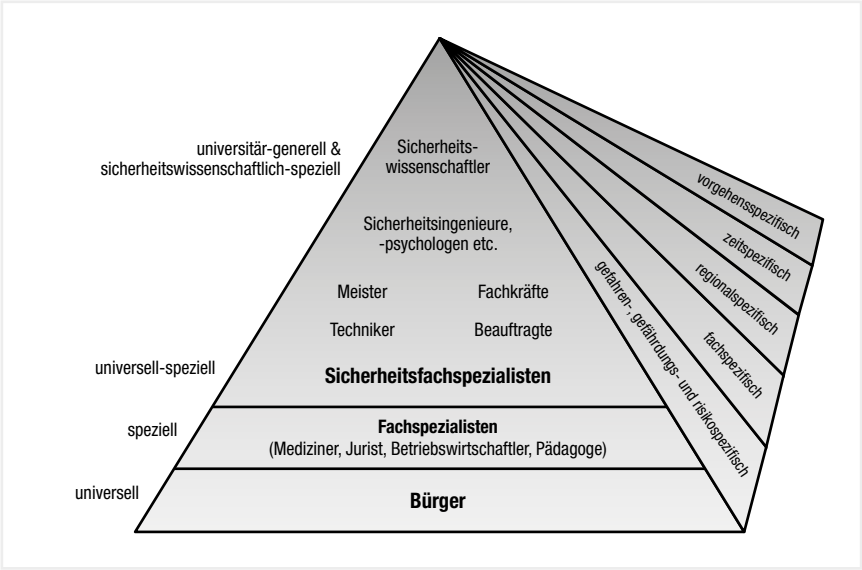

Bild 4.6: **Adressaten zur Förderung der Kompetenzen im Umgang mit Gefahren und Risiken**

Dieser Bereich sollte systematisch ausgebaut und weiterentwickelt werden. Bei der Erziehung und Sozialisation bietet sich vor allem die Zeit im Kindergarten, der Schule, der Ausbildung, dem Studium und im Berufsleben an. Bisher stand dabei das Berufsleben im Vordergrund der Sicherheitsarbeit, da so auf die bestimmten Gefahren des jeweiligen Arbeitsplatzes eingegangen werden kann. Allgemeine Gefahren- und Risikokompetenzen werden dabei aber nur selten vermittelt, was eine weitere Optimierungsmöglichkeit zur Kompetenzvermittlung bietet. In den Zeitphasen vor dem Arbeitsleben spielt die Kompetenzvermittlung im Umgang mit Gefahren und Risiken heute kaum eine Rolle, obwohl sie hier wichtig ist. Hier ist ein enormer Handlungsbedarf zu verzeichnen.

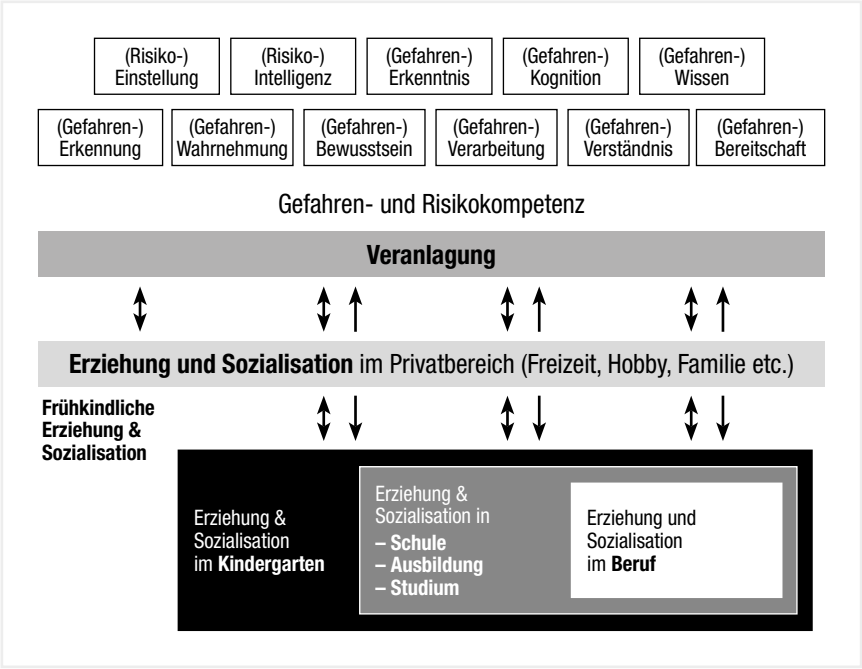

Bild 4.7: **Risikokompetenz – Vermittlungsansätze**

Neben der generellen Ausstattung der Bevölkerung mit Kompetenzen im Umgang mit Gefahren und Risiken sind die Fachspezialisten in Bezug auf ihre Fachgebiete in einer zusätzlichen Weise diesbezüglich zu fördern. Der Handlungsbedarf bei Fachspezialisten, wie zum Beispiel bei Ärzten, Anwälten, Politikern, Pädagogen oder Betriebswirten, ist groß. Ihre Entscheidungen haben einen erheblichen Einfluss auf die allgemeine Sicherheitssituation und gesellschaftliche Leistungsfähigkeit. So zeigen unsere Untersuchungen beispielsweise, dass die Vernachlässigung der Mitarbeiterreaktionen bei betrieblichen Beschlüssen von Führungskräften starke Auswirkungen auf die betriebliche Sicherheitssituation, aber auch auf die allgemeine Leistungsfähigkeit der Betriebe, haben (vgl. Festag & Hartwig, 2013). Den Führungskräften fehlt es häufig an einem sicherheitswissenschaftlichen Grundverständnis, womit ihnen dann die Konsequenzen und Kollateralschäden ihrer Entscheidungen nicht klar sind. Die Folgen daraus sind für die Industrie und Gesellschaft, wie wir sehen, katastrophal.

Aus diesem Grund ist das Eingehen von Gefahren- und Risikokompetenzen in die Breite der Curricula von fachfremden Studienprogrammen sinnvoll und notwendig.

Sicherheitsfachspezialisten nehmen bei diesem Thema naturgemäß eine besondere Rolle ein. Diese sind mit besonderen Kompetenzen im Umgang mit Gefahren und Risiken auszurüsten, wobei die Adressaten in verschiedenen Ebenen angesiedelt sind. Zu ihnen zählen beispielsweise Sicherheitsbeauftragte, Sicherheitsfachkräfte, Sicherheitstechniker und -meister sowie die akademischen Fachkräfte, wie Sicherheitsingenieure, -psychologen, -soziologen und Sicherheitswissenschaftler. Für deren Aus- und Weiterbildung wurden bereits gesonderte Ausbildungs- und Studienprogramme entwickelt. Hier ist allerdings eine kontinuierliche Anpassung an die gesellschaftlichen Gefahren und Bedürfnisse vorzunehmen. In diesem Zuge müssen neue Fachgebiete entwickelt und tradierte weitergepflegt werden (da hier bereits systematische Erkenntnisse vorhanden sind, die in übergeordneter Weise behilflich sind). Die akademische Ausbildung ist im sicherheitswissenschaftlichen Bereich zu stärken, auch um auf allen anderen Ebenen die entsprechenden Inhalte bereitstellen zu können. Vielleicht erhält das vorliegende Programm ein ausreichendes Gehör, um diese Bewegung mit einem Impuls antreiben zu können – es wäre wünschenswert.

Literatur

Burkhardt, F. (1981). Information und Motivation zur Arbeitssicherheit. Wiesbaden: Universum Verlagsanstalt.

Compes, P. C. (1975). Sicherheitstechnik an der Bergischen Universität Wuppertal. In Sicherheitsingenieur, Ausgabe 8, 374–377.

Compes, P. C. (1991). Forschung und Lehre der Sicherheitswissenschaft. In P.C. Compes (Hrsg.): Sicherheitswissenschaft in Theorie und Praxis im wiedervereinigten Deutschland: Konzepte – Realitäten – Defizite. XII. Internationales Sommer-Symposion der Gesellschaft für Sicherheitswissenschaft, 17.–18. Juni 1991 in Dresden, 17–48.

Festag, S. (2014). Einführung in das Programm. In S. Festag (Hrsg.): Umgang mit Risiken – Qualifizierung und Quantifizierung. XXVII. Sicherheitswissenschaftliches Symposion der Gesellschaft für Sicherheitswissenschaft, Juni 2013 in Wien, S. 1–4.

Festag, S. & Hartwig, S. (2013). Sicherheitsprobleme durch die Vernachlässigung der Mitarbeiterreaktionen auf betriebliche Managementbeschlüsse.
Technische Sicherheit, Band 3, Nr. 1
Januar/Februar, Springer Verlag, S. 17–22.

GfS (13.01.2014). Wir über uns. Webseite der Gesellschaft für Sicherheitswissenschaft e.V. URL: www.gfs-aktuell.de (Zugriffsdatum).

Gigerenzer, G. (2013). Risiko – Wie man die richtigen Entscheidungen trifft. München: Bertelsmann Verlag.

Hartwig, S. (2005). Eine Nation im freien Fall. Jena: Dr. Bussert Verlag.

Hartwig, S. (1997). Überlegungen zu den Risiken gefährlicher chemischer Stoffe in einer Industriegesellschaft. Christoph Zöpel (Hg.). Technikkontrolle in der Risikogesellschaft. Bonn: Verlag Neue Gesellschaft.

Hartwig, S. & Festag, S. (2012). Über risikoerhöhendes menschliches Verhalten durch falsche Führungsstrategien. Technische Sicherheit.
Band 2, Nr. 3, Springer Verlag, S. 24–29.

Henne, H., Kämper, H. und Objartel, G. (2002). Deutsches Wörterbuch – Bedeutungsgeschichte und Aufbau unseres Wortschatzes, Stichwort: Kompetenz. Tübingen: Max Niemeyer Verlag. S. 553 f., 10. Auflage.

Kegel, B. (2009). Epigenetik – Wie Erfahrungen vererbt werden. Köln: Dumont.

Musahl, H.-P. (2009). Prävention – eine wissenschaftliche Aufgabenstellung. B. Ludborzs & H. Nold (Hrsg.). Psychologie der Arbeitssicherheit und Gesundheit: Entwicklungen und Visionen
1980–2008–2020 (155–172). Kröning: Asanger Verlag.

Musahl, H.-P. (1997). Gefahrenkognition. Theoretische Annäherungen, empirische Befunde und Anwendungsbezüge zur subjektiven Gefahrenkenntnis. Heidelberg: Roland Asanger Verlag.

Radandt, S. (2014). Sicherheitswissenschaft als Instrument zum Umgang mit Risiken in der Industrie. In S. Festag (Hrsg.): Umgang mit Risiken – Qualifizierung und Quantifizierung. XXVII. Sicherheitswissenschaftliches Symposion der Gesellschaft für Sicherheitswissenschaft, Juni 2013 in Wien, S. 5–14.

Rasmussen, J. (1983). Skills, Rules, and Knowledge; Signals, Signs and Symbols, and Other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-13, No. 3
May.

Rasmussen, J. (1986). Information Processing and Human-Maschine Interaction: An Approach to Cognitive Engineering. North-Holland Series in System Science and Engineering: Elsevier Science Ltd.

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

Riemann, R. & Spinath, F. (2005). Genetik und Persönlichkeit. In P. Netter und J. Henning (Hrsg): Biopsychologische Grundlagen der Persönlichkeit. Heidelberg: Springer Verlag, S. 539–628.

Seebold, E. (2011). Kluge – Etymologisches Wörterbuch der deutschen Sprache, Stichwort: Kompetenz. Berlin/Boston: Walter de Gruyter,
S. 518 f. 25. Auflage.

Seidel, K. (2008). Chronologie der Sicherheitswissenschaft – Forschungsstudie über die Entwicklung der Wuppertaler Sicherheitstechnik. Bachelorthesis; Bergische Universität Wuppertal – Abteilung Sicherheitstechnik, Fachgebiet Methoden der Sicherheitstechnik/Unfallforschung.

Skiba, R. (1973). Die Gefahrenträgertheorie. Forschungsbericht Nr. 106, Bundesanstalt für Arbeitsschutz und Unfallforschung, Dortmund.

Spitzer, M. (2012). Digitale Demenz – Wie wir uns und unsere Kinder um den Verstand bringen. München: Droemer Verlag.

Taleb, N. N. (2010). Der Schwarze Schwan: Die Macht höchst unwahrscheinlicher Ereignisse. München: Deutscher Taschenbuch Verlag.

5

Aktuelle Situation

Einleitung

Prof. Dr. Siegfried Radandt, Forschungsgesellschaft für angewandte Systemsicherheit und Arbeitsmedizin e.V., GfS, Deutschland

Risiko- und Nutzenvergleiche sind zu zentralen Diskussionsthemen geworden. Welche Beziehungen zwischen Risiko und Nutzen gesehen werden, ist eine offene Frage. Die Öffentlichkeit versteht unter Risiko und Nutzen einer Technologie weit mehr als das, was normalerweise die Natur- und Ingenieurwissenschaft darunter verstehen will, nämlich die Kombination aus Wahrscheinlichkeit von unerwünschten Ereignissen und deren Konsequenzen. Auch spielen das Katastrophenpotenzial, qualitative Merkmale wie die Freiwilligkeit und Kontrollierbarkeit für die Beurteilung des Risikos einer Technologie eine wichtige Rolle.

Eine normative Festlegung auf eine bestimmte allgemeingültige Risikodefinition im Sinne der Ingenieurwissenschaft ist deshalb z. Zt. kaum konsensfähig. Nahezu alle EU-Richtlinien, die sich mit Sicherheitsfragen befassen, verlangen Risikobeurteilungsverfahren und möglichst auch eine Bewertung der Risiken. Wenn man sich mit der Definition des Risikos auseinandersetzt, kann man ermessen, dass das meist nicht einfach ist.

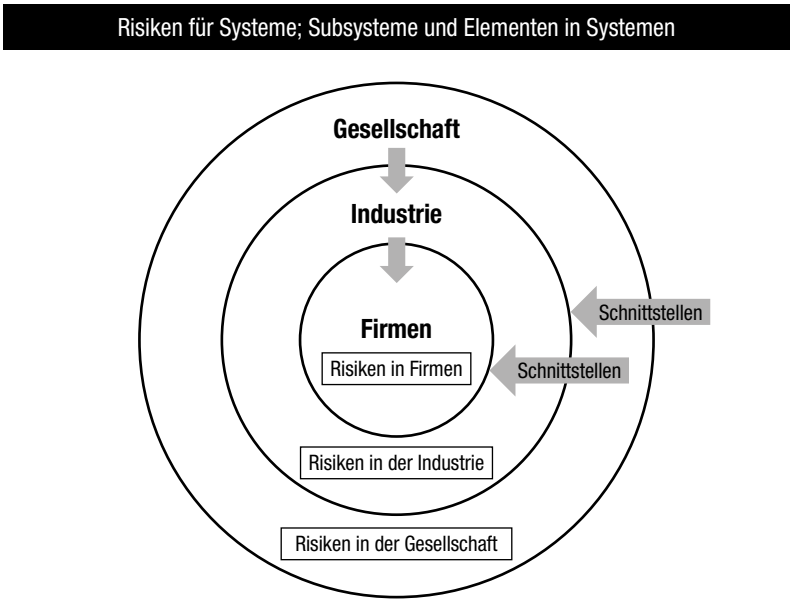

Bild 5.1: **Risiken für Systeme, Subsysteme und Elemente in Systemen**

Die Tatsache, dass sich Risiken nicht allein durch Gefährdungspotenziale, als unerwünschte Ereignisse und unvorhergesehene Geschehnisse beschreiben lassen, sondern eher durch die Wahrscheinlichkeit von deren Eintritt und die möglichen Auswirkungen führt zu Strategien im Umgang mit Risiken mit dem Ziel, solche negativen Ereignisse, Geschehnisse möglichst wenig wahrscheinlich werden zu lassen und im Falle ihres Eintritts die Auswirkungen möglichst gering zu halten. Risiken werden immer in den definierten Systemen (Betrachtungseinheiten) analysiert. Die Ursachen für diese Risiken liegen aber nicht immer im definierten System selbst, sondern oft auch außerhalb, was das Behandeln der Risiken schwierig macht (Bild 5.1 und Bild 5.2).

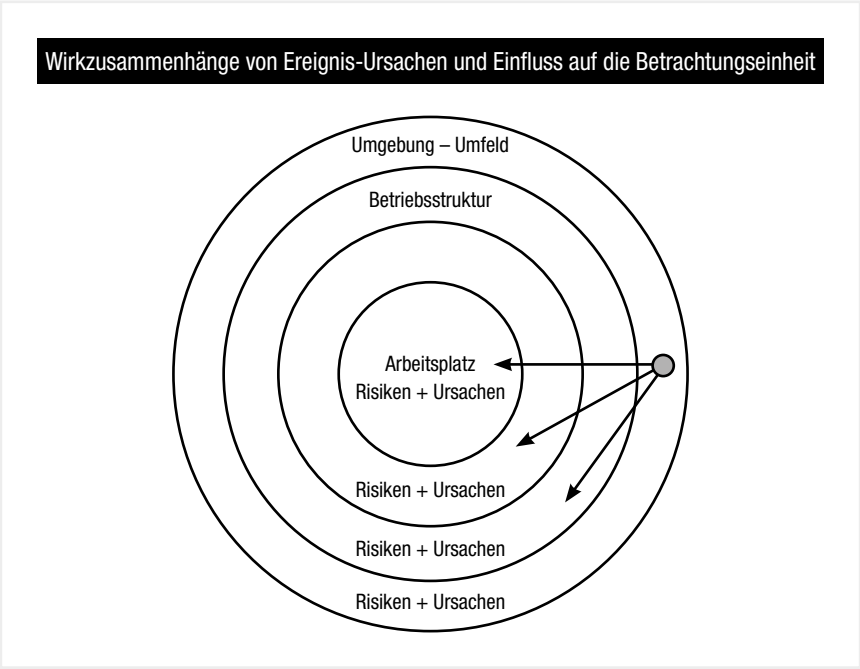

Bild 5.2: **Wirkungszusammenhänge von Ereignisursachen und Einfluss auf die Betrachtungseinheit**

Was können wir aus Unfallszenarien lernen?

Viele Informationen über die Art von Risiken erhält man aus Unfallereignissen. Aus Unfallszenarien lassen sich die folgenden Fragen ableiten (Radandt, 2014):

- Was kann schieflaufen?
- Wie leicht kann das passieren?
- Wenn es passiert, was sind die Konsequenzen?

Schwere Unfälle können Folgen haben, die über die Grenzen des jeweiligen Betriebsbereichs hinausreichen. Die ökologischen und wirtschaftlichen Kosten eines Unfalls werden nicht nur von dem davon betroffenen Betrieb, sondern auch von den außerhalb liegenden Bereichen getragen. Daher müssen Maßnahmen getroffen werden, die solche Auswirkungen begrenzen.

Eine Analyse der gemeldeten schweren Unfälle zeigt, dass in den meisten Fällen Management- bzw. organisatorische Mängel die Ursache waren. Es müssen deshalb grundlegende Prinzipien für die Managementsysteme festgelegt werden, die geeignet sein müssen, den Gefahren schwerer Unfälle vorzubeugen und sie zu verringern und die Unfallfolgen zu begrenzen.

Aus dem Europäischen MARS (Major Accident Reporting System) lassen sich einige Erkenntnisse ableiten. Die Rangfolge der Ursachen stellt sich wie folgt dar:

- Freisetzung gefährlicher Stoffe (Substanzen),
- Freisetzung gefährlicher Stoffe (Substanzen) in Verbindung mit Bränden und Explosionen,
- Explosionen,
- Brände und Explosionen,
- Brände,
- Freisetzung gefährlicher Stoffe (Substanzen) und Brände,
- Freisetzung gefährlicher Stoffe (Substanzen) und Explosionen,
- Freisetzung gefährlicher Stoffe und Wasserkontamination,
- Freisetzung gefährlicher Stoffe und Wasserkontamination und Brände und Explosionen.

Es gibt also die unterschiedlichsten Ereigniskombinationen mit teilweise erheblichen Dominoeffekten. Die Rangfolge der Konsequenzen ist dabei folgende:

- Materialverlust (35 %),
- Verletzungen bei Personen (26 %),
- Ökologische Schäden (12 %),
- Zerstörung der Umwelt (10 %),
- Todesfälle (9 %).

Für die Ereignisse verantwortlich waren:

- Organisationsmängel (über 50 %),
- Zuverlässigkeitsprobleme mit Anlagen und Einrichtungen (30 %),
- Zuverlässigkeitsprobleme mit Bedienpersonal (10 %)
- und Einflüsse von außen.

Aus einer Studie der BRD ist zu entnehmen, dass die Ereignisse zu 50 % während des normalen Prozessablaufs stattfanden, zu 15 % bei Instandhaltung und Reparatur, zu 15 % beim Lagern, zu 12 % bei Abschalt- und Abfahrprozessen, zu 7 % beim Be- und Entladen.

Verursacht wurden sie zu 35 % durch technische Fehler (Geräte, Befestigungen, Flansche, Behälter, Rohrleitungen, mechanische Schäden, Korrosion, Verschleiß), zu 20 % durch Bedienungs- und Handhabungsfehler, zu 8 % durch organisatorische Fehler, zu 15 % durch physikalische und chemische Reaktionen.

Weitere die Industriesicherheit beeinflussende Risiken können zu Gefährdungen führen durch:

- Versagen infolge von Fehlplanungen,
- zu geringen Kapazitäten,
- mangelnder Wartung und Instandhaltung, Organisationsmängeln, Fehlhandlungen wegen mangelnder Qualifikation und vor allem durch Sabotage und Eingriffe von außen (z. B. auch Terrorismus).

Solche gefährdeten Anlagen und Bereiche können z. B. sein: Kraftwerksanlagen und Energieversorgungssysteme, Wasserversorgungssysteme, Notfallsysteme, Verkehrsnetzwerk und Transportsysteme, Öl-Gas-Pipelines-Netzwerke, Lagerstätten für gefährliche Güter und Substanzen, Kommunikations- und Informationsnetzwerke, Bahn- und Hafenbetriebe, Flughäfen, Entsorgungssysteme.

Was tut man gegen einen gravierenden Störfall?

Für den Fall der Fälle gibt es ein Sicherheitssystem, das bestimmten Ideen folgt:

- Redundanz,
- Entmaschung,
- Diversität,
- Fail-Safe und andere Aspekte.

Da auch mehrfach vorhandene gleichartige Sicherheitssysteme aus der gleichen Ursache (z. B. Konstruktionsfehler) versagen können, werden für den gleichen Zweck technisch unterschiedliche Einrichtungen vorgesehen.

Damit ein ausfallendes Sicherheitssystem das Nachbarsystem nicht beeinträchtigt, besitzen sie keine gemeinsamen Komponenten. Außerdem werden sie räumlich getrennt und baulich besonders geschützt angeordnet. Wichtige Sicherheitssysteme werden mehrfach (redundant) angeordnet. Es sind mindestens zwei Systeme mehr vorhanden (n + 2), als für die eigentliche Funktion benötigt werden.

Um die Aussagen der verschiedenen Analysen innerhalb der Systembetrachtung richtig einordnen zu können, ist ein komplexes Denkschema erforderlich. Ein solches Denkschema beinhaltet folgende Denkschritte:

Das Festlegen und Definieren der Betrachtungseinheit
Hier geht es um die eigentliche Aufgabenstellung und Abgrenzung des Systems. Es kann sich dabei um ein fiktives System oder um ein reales System handeln. Die Vorgaben sind Zeit, Raum und Zustand. Das System ist dynamisch.

Die Problemanalyse
Hier werden alle Probleme, die im definierten System vorliegen, also auch die, die nicht ihren Ursprung im System selbst haben, gesucht und beschrieben.

Ursachen für die Probleme
Bei diesem Schritt werden alle möglichen Ursachen, die zu den gefundenen Problemen führen oder führen können, aufgelistet.

Wirkzusammenhänge feststellen
Die Abhängigkeiten von Wirkmechanismen werden dargestellt, Zusammenhänge von Ursachen ermittelt.

Prioritäten festlegen und Zielsetzungen formulieren
Um diesen Schritt zu vollziehen, muss eine Wertung der Wirkungen von Ursachen vorgenommen werden.

Maßnahmen zur Lösung der Probleme
Es werden alle Maßnahmen für die einzelnen Probleme aufgelistet. Da sich für eine Problemlösung oft mehrere mögliche Maßnahmen anbieten, findet hier bereits eine Vorauswahl der Maßnahmen statt. Dies ist in diesem Schritt aber nur bedingt möglich.

Widersprüche klären und Prioritäten setzen

Da sich Maßnahmen für Einzelprobleme teilweise widersprechen oder gar ausschließen können, müssen nach der Widerspruchsklärung Entscheidungen für oder gegen eine Maßnahme getroffen werden oder Kompromisse gesucht werden.

Maßnahmen für die definierte Betrachtungseinheit festlegen

Aus den Maßnahmen für die Einzelprobleme werden nun die Maßnahmen ausgewählt, die innerhalb des definierten Gesamtsystems anwendbar sind.

Frage nach der Lösung für das definierte System

Hier wird abgefragt, ob die gefundenen umsetzbaren Maßnahmen Lösungen für die Probleme des Systems sind. Abfrage, ob neue Probleme entstehen. In diesem Schritt wird abgefragt, ob durch die Problemlösung neue andere Probleme entstehen.

Das Risikomanagement selbst beinhaltet folgende Schritte (vgl. Bild 5.3 bzw. Bild 5.4 und Bild 5.5):

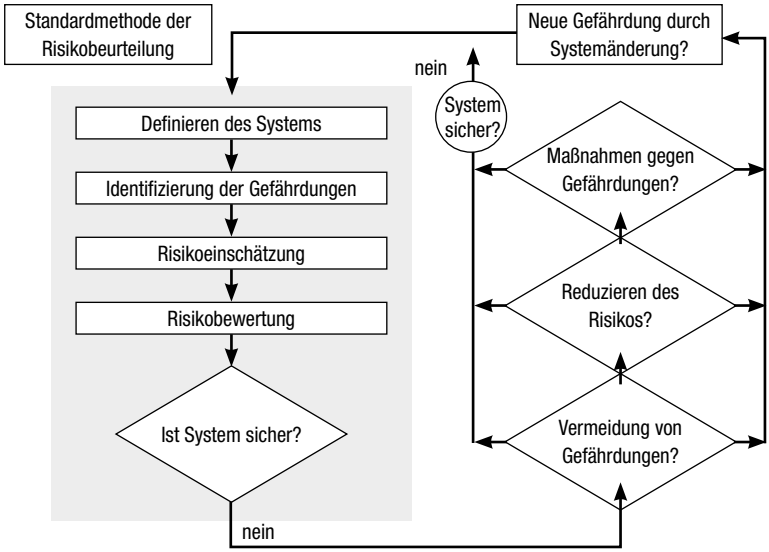

Bild 5.3: **Vorgehen nach Standardmethode**

1. Risikobeurteilung
   - Risikoanalyse (Identifikation von Ursachen, Abschätzen des Risikos)
   - Risikobewertung (Vergleich des abgeschätzten Risikos mit Risikokriterien)

2. Umgang mit Risiken
   - Vermeiden von Risiken
   - Risikoreduktion
   - Risikooptimierung
   - Risikotransfer
   - Festhalten an Risikostruktur

3. Akzeptanz von Risiken und Risikokommunikation

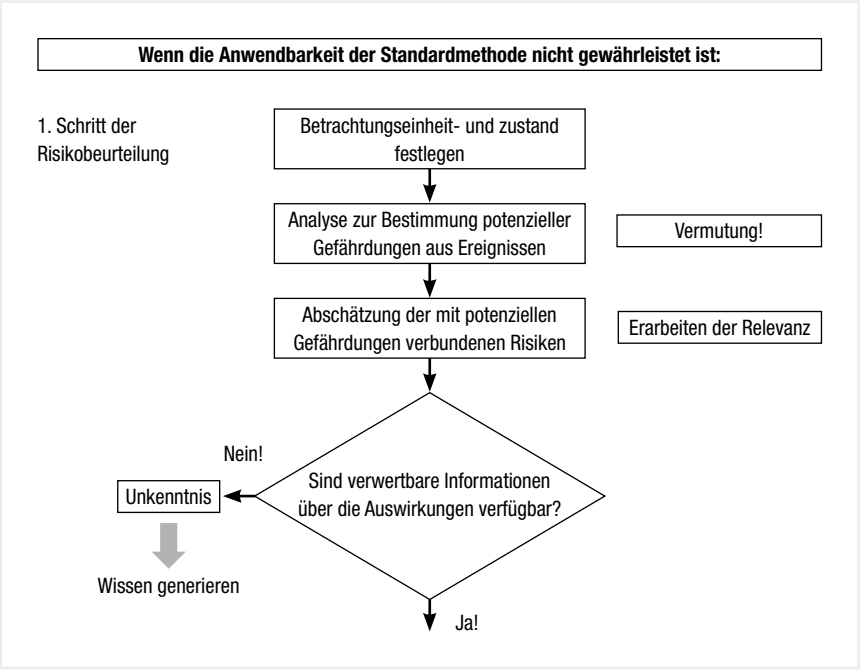

Bild 5.4: **Vorgehen I (wenn die Standardmethode nicht gewährleistet ist)**

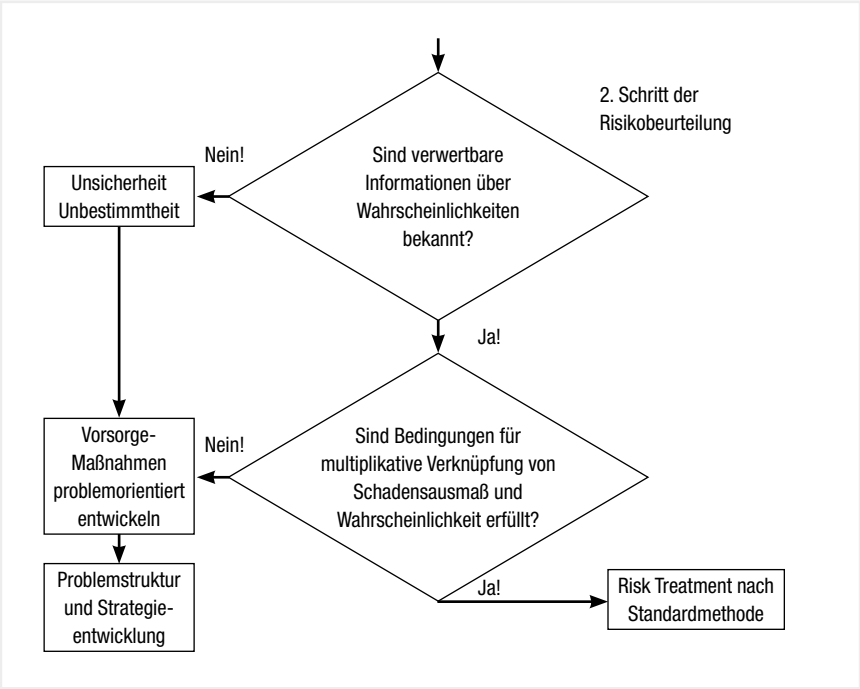

Bild 5.5: **Vorgehen II (wenn die Standardmethode nicht gewährleistet ist)**

Zwischen unbekannten und bekannten Risiken liegen die ungeklärten Risiken:

- Unbekannte Risiken: Mangels Ansatzpunkt scheidet jede Vorsorge aus.
- Ungeklärte Risiken: Aufgrund theoretischer und empirischer Befunde besteht ein Risikoverdacht oder eine Risikovermutung (auch bei Summations- und Kombinationsrisiken).
- Bekannte Risiken: Aufgrund theoretischen und empirischen Wissens ist ein konkreter Bedingungs- oder Wirkzusammenhang erkannt.

Unvollständige Informationen (mangelndes Wissen) – das Vorsorgeprinzip

Das Hauptproblem der Risikoanalyse liegt im Bereich unvollständiger Informationen. Nach Auffassung der EU-Kommission ist ein Rückgriff auf das sogenannte Vorsorgeprinzip dann möglich, wenn potenzielle Gefahren eines Phänomens, Produkts oder Verfahrens durch eine unvollständige Information (mangelndes Wissen) das Vorsorgeprinzip objektive wissenschaftliche Bewertung ermittelt wurde, wenn sich das Risiko aber nicht mit hinreichender Sicherheit bestimmen lässt. Der Rückgriff auf das Vorsorgeprinzip erfolgt somit im Rahmen der allgemeinen Risikoanalyse.

Die **zeitabhängigen Veränderungen der Systeme**, die eine Auswirkung auf Eigenschaften, Zustände, Situationen und dergleichen haben, bedingen Methoden, die es erlauben, komplexe sicherheits- und gesundheitsrelevante Zusammenhänge auch retrospektiv zu erkennen, komplexe Sicherheits- und Gesundheitsprobleme zu beschreiben.

Die **Dynamik von Systemen** ist gekennzeichnet durch das zeitliche Verhalten des Systems. Statische Systeme zeigen ohne Einflüsse von außen sowohl auf der Makroebene als auch auf der Mikroebene keine Veränderungen. Dynamische Systeme sind auf der Mikroebene dauernden Veränderungen unterworfen, können aber zumindest zeitweise auf der Makroebene einen stationären Zustand einnehmen.

Literatur

Radandt, S. (2014). Sicherheitswissenschaft als Instrument zum Umgang mit Risiken in der Industrie. S. Festag (Hrsg.): Umgang mit Risiken – Qualifizierung und Quantifizierung. XXVII. Sicherheitswissenschaftliches Symposion der Gesellschaft für Sicherheitswissenschaft. Reihe Sicherheit,
Berlin: Beuth-Verlag, S. 5–14.

6

Ansätze zur Risikobeurteilung in Deutschland – internationale und europäische Anforderungen

6.1 Einleitung

Dr. Willi B. Marzi, SK, Deutschland

Die Beschäftigung mit Risiken ist keine neue Aktivität, weder in Deutschland noch international. Es gibt in einzelnen Politikfeldern schon seit Jahrzehnten Ansätze, Verfahren und Festlegungen. MAK-Werte, die Seveso-Richtlinie und die Regelungen im Hochwasserschutz sind Beispiele, es gibt viele andere mehr.

Die systematische Beschäftigung mit Risiken im Bevölkerungsschutz ist hingegen eine – im Vergleich dazu – neuere Entwicklung. Ich möchte Ihnen im Folgenden einen kurzen Überblick über die Entwicklung in Deutschland und den aktuellen Sachstand auf diesem Sektor geben. Ergänzend beleuchte ich kurz die Entwicklungen in einigen unserer Nachbarländer, in der Europäischen Union und beispielhaft in der OECD. Was ist Gegenstand des Bevölkerungsschutzes? Das Glossar des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) aus dem Jahr 2011 führt dazu aus:

Der Bevölkerungsschutz beschreibt als Oberbegriff alle Aufgaben und Maßnahmen der Kommunen und der Länder im Katastrophenschutz sowie des Bundes im Zivilschutz.

Anmerkung: Der Bevölkerungsschutz umfasst somit alle nichtpolizeilichen und nichtmilitärischen Maßnahmen zum Schutz der Bevölkerung und ihrer Lebensgrundlagen vor Katastrophen und anderen schweren Notlagen sowie vor den Auswirkungen von Kriegen und bewaffneten Konflikten. Der Bevölkerungsschutz umfasst auch Maßnahmen zur Vermeidung, Begrenzung und Bewältigung der genannten Ereignisse. Die Definition umfasst somit nicht die allgemeine Gefahrenabwehr, wie sie beispielsweise von den Feuerwehren in ihrer alltäglichen Arbeit wahrgenommen wird.

Es gibt zwei Verantwortliche im Bevölkerungsschutz: den Bund und die Länder (die Kommunen sind Ausführende im Katastrophenschutz). Der Schutz der Zivilbevölkerung im Verteidigungsfall obliegt dem Bund (Art. 73 Nr. 1 GG). Für alles Übrige liegt die Zuständigkeit für den Schutz der Bevölkerung bei den Ländern. Dies umfasst die Auswirkungen von Natur- und technischen Katastrophen ebenso wie von Pandemien oder terroristischen Anschlägen. Das heißt aber nicht, dass dem Bund bei Katastrophen keine Rolle zuwächst. Beim Elbhochwasser im letzten Jahr waren die Bundeswehr, das Technische Hilfswerk und die Bundespolizei als Bundesinstitutionen in erheblichem Umfang im Einsatz. Diese Hilfsleistungen geschehen aber nur auf Bitten der Länder und Kommunen im Rahmen der Amtshilfe gemäß Art. 35 Abs. 2 und 3 GG.

Die unterschiedlichen Zuständigkeiten bedeuten aber nicht, dass Bund und Länder unkoordiniert ihre jeweiligen Aufgaben wahrnehmen. Als Folge der Anschläge am 11. September 2001 und des Hochwassers an Elbe und Oder im Sommer 2002 haben sich Bund und Länder im Jahre 2002 auf eine „Neue Strategie zum Schutz der Bevölkerung in Deutschland“ verständigt. Leitmotiv der „Neuen Strategie“ ist ein verstärktes partnerschaftliches Zusammenwirken über föderale Grenzen hinweg, Bevölkerungsschutz als Gemeinschaftsaufgabe allein im politischen Sinne. Kernelemente der „Neuen Strategie“ sind die intensive Verzahnung und Abstimmung der Planungen und Verfahren sowie die verbesserte Koordinierung und Zusammenarbeit von Bund und Ländern. Grundlage hierfür sollen Gefährdungs- und Risikoanalysen sein.

6.2 Entwicklungen in Deutschland im Zeitraum 2002 – 2010

In Umsetzung dieser Strategie hat der Bund im Jahr 2003 mit seiner zum BBK gehörenden Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) Problemstudien zu Risiken in Deutschland durchgeführt. Gegenstand dieser Studien waren die erkannten Gefahrenpotenziale aus Sicht des Bevölkerungsschutzes und deren Auswirkungen auf Staat, Wirtschaft und Gesellschaft. Die Problemstudien enthielten darüber hinaus Aussagen zu Möglichkeiten der Gefahrenprävention.

Als nächster Schritt erfolgte in den Jahren 2004/2005 die Erstellung von Gefährdungsabschätzungen durch die für den Katastrophenschutz zuständigen Länder. Die Abschätzungen erfolgten nach einheitlicher Struktur und auf der Grundlage eines Kennziffernkatalogs, auf den sich Bund und Länder verständigt hatten. Es wurden dabei ebenso technogene und anthropogene wie auch Naturgefahren als Auslöser für großflächige und/oder lang andauernde bzw. schwierig zu bewältigende Schadenslagen berücksichtigt.

Die Gefährdungsabschätzungen der 16 Länder wurden vom Bund ausgewertet, zusammengefasst und ergänzt. Damit stand Ende 2005 erstmals in der Geschichte des Bevölkerungsschutzes eine bundesweite Gefährdungsabschätzung zur Verfügung.

Das Ergebnis dieser Zusammenarbeit von Bund und Ländern führte dann im Jahr 2006 zu der Bitte der Länder an den Bund, eine einfach umsetzbare Methode für die Risikoanalyse im Bevölkerungsschutz zu entwickeln, die auf allen Verwaltungsebenen für alle Risiken anwendbar sein sollte. Das BBK hat sich dieser Aufgabe angenommen. Bei der Entwicklung der Methode konnte auf die Arbeiten zur Gefährdungsabschätzung ebenso zurückgegriffen werden wie auf die bei anderen Bundesbehörden, bei ausländischen Partnerbehörden und Wissenschaftseinrichtungen vorliegenden Erfahrungen. Von besonderer Bedeutung waren dabei die Arbeiten aus den Niederlanden, dem Vereinigten

Königreich und der Schweiz. Im Jahr 2010 konnte dann eine Methode für die Risikoanalyse im Bevölkerungsschutz vorgestellt werden, die den Belangen des Bundes ebenso Rechnung trug wie den von den Ländern genannten Kriterien.

Ein weiterer wichtiger Meilenstein war das Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (ZSKG), das am 9.4.2009 veröffentlicht wurde. Gemäß § 18 Abs. 1 Satz 1 und 2 des ZSKG erstellt der Bund im Zusammenwirken mit den Ländern eine bundesweite Risikoanalyse für den Zivilschutz. Das Bundesministerium des Innern unterrichtet den Deutschen Bundestag über die Ergebnisse der Risikoanalyse ab 2010 jährlich. Damit besteht nunmehr auch eine gesetzliche Grundlage für die Erstellung der Risikoanalyse.

6.3 Methode für die Risikoanalyse im Bevölkerungsschutz

Die Planung von Schutzmaßnahmen im Bevölkerungsschutz muss sich an den Gefahren und Risiken orientieren, mit denen die Bevölkerung konfrontiert werden kann. Die Risiken zu analysieren, ist ein zentraler Bestandteil des Risikomanagements auf allen Verwaltungsebenen (Bild 6.1).

Die Risikoanalyse wurde dafür als Instrument auf fachlicher Basis entwickelt. Sie ist ein Verfahren, mit dem Risiken sachlich nüchtern analysiert werden. Sie enthält keine politische Bewertung von Risiken oder erforderlichen Vorsorgemaßnahmen. Sie erlaubt darüber hinaus den Vergleich von Risiken. Die Risikoanalyse dient als politisches Entscheidungs- und administratives Planungsinstrument.

Risiko wird im Kontext mit der Risikoanalyse wie folgt definiert:

Maß für die Wahrscheinlichkeit des Eintritts eines bestimmten Schadens an einem Schutzgut unter Berücksichtigung des potenziel len Schadensausmaßes.

Das bedeutet, die Risikoanalyse beschäftigt sich mit Eintrittswahrscheinlichkeiten und Schadensausmaß. Die Bestimmung der Eintrittswahrscheinlichkeit bezieht sich auf eine Gefahr bestimmter Intensität. Das Schadensausmaß ist für die bei Eintritt des Ereignisses an unterschiedlichen Schutzgütern zu erwartenden Schäden zu bestimmen.

Bild 6.1: Risikomanagement (BT-Drucksache (2010), 17/4178 vom 9.12.2010)

Die Belastbarkeit der Ergebnisse von Risikoanalysen ist abhängig von den vorhandenen wissenschaftlichen Erkenntnissen und den vorhandenen Daten. Die immer vorhandenen Wissensdefizite müssen durch begründete Annahmen und Schätzungen aufgefangen werden. Wichtig für die Glaubwürdigkeit und Nachvollziehbarkeit ist dabei eine sorgfältige Dokumentation aller Einzelschritte der Risikoanalyse. Wird eine Risikoanalyse in Angriff genommen, so ist die für die Erreichung des Ziels notwendige Detailtiefe zu definieren, die es erlaubt, in endlicher Zeit zu Ergebnissen zu gelangen.

Die Erstellung einer Risikoanalyse für den Bevölkerungsschutz gliedert sich in vier Schritte:

- Erstellung des Szenarios,
- Ermittlung der Eintrittswahrscheinlichkeit,
- Ermittlung des Schadensausmaßes,
- Visualisierung des Risikos.

Bei der Erstellung des Szenarios ist zu beachten, dass die Detailtiefe groß genug sein muss, um Eintrittswahrscheinlichkeit und Schadensausmaß verlässlich abschätzen zu können. Je größer die Detailtiefe, desto überproportional umfangreicher und aufwendiger werden die nachfolgenden Schritte. Bei einer Risikoanalyse im Bundesmaßstab wird der Ansatz generischer sein als auf kommunaler Ebene. Die Auswahl der Szenarien sollte so erfolgen, dass Wahrscheinlichkeit und Schadensausmaß eine für die Verwendung im Risikomanagement vernünftige Größenordnung haben. Megakatastrophen sind für diesen Zweck ebenso wenig geeignet wie Ereignisse mit geringen Auswirkungen. Ein „Reasonable Worst Case" wird zugrunde gelegt, vorzugsweise basierend auf Ereignissen, die in historischer Zeit stattgefunden haben. Das Szenario hat die folgende Struktur:

- Definition der Gefahr/Ereignisart
- Beschreibung des Ereignisses:
  - Ort des Auftretens/räumliche Ausdehnung
  - Zeitpunkt
  - Auslösende Ereignisse
  - Intensität, Dauer und Verlauf
  - Vorhersagbarkeit/Vorwarnung/Kommunikation
  - Behördliche Maßnahmen
- Auswirkungen auf kritische Infrastrukturen/Versorgung
- Betroffene Schutzgüter
- Referenzereignisse
- Literatur/weiterführende Informationen

Die Ermittlung der Eintrittswahrscheinlichkeit hat zum Ziel, das Ereignis einer der nachstehenden Klassen zuordnen zu können. Die bislang durchgeführten Risikoanalysen des Bundes bewegen sich im Bereich der Klasse C (siehe Tabelle 6.1).

Eintrittswahrscheinlichkeits-Klassen	
A:	**sehr unwahrscheinlich** ein Ereignis, das statistisch in der Regel einmal in einem Zeitraum von über 10.000 Jahren eintritt
B:	**unwahrscheinlich** ein Ereignis, das statistisch in der Regel einmal in einem Zeitraum von 1.000 bis 10.000 Jahren eintritt
C:	**bedingt wahrscheinlich** ein Ereignis, das statistisch in der Regel einmal in einem Zeitraum von 100 bis 1.000 Jahren eintritt
D:	**wahrscheinlich** ein Ereignis, das statistisch in der Regel einmal in einem Zeitraum von 10 bis 100 Jahren eintritt
E:	**sehr wahrscheinlich** ein Ereignis, das statistisch in der Regel einmal in einem Zeitraum von über 10 Jahren oder häufiger eintritt

Tabelle 6.1: **Eintrittswahrscheinlichkeits-Klassen (BT-Drucksache, 2013, 18/208, Anhang 1)**

Der aufwendigste Schritt bei der Erstellung von Risikoanalysen ist die Ermittlung des Schadensausmaßes bezogen auf die zu berücksichtigenden Schutzgüter. Diese werden in vier Klassen von Schutzgütern – Mensch, Umwelt, Volkswirtschaft und immateriell – eingeteilt, die in weitere Schadensparameter unterteilt werden. Nicht jedes Szenario hat Auswirkungen auf alle Schutzgüter, zum Beispiel hat ein Humanseuchengeschehen keine Auswirkungen auf die Umwelt (Tabelle 6.2).

Schadensparameter	
Mensch	Tote Verletzte Hilfsbedürftige Vermisste
Umwelt	Schädigung geschützter Gebiete Schädigung von Oberflächengewässern/Grundwasser Schädigung von Waldflächen Schädigung landwirtschaftlicher Nutzfläche Schädigung von Nutztieren
Volkswirtschaft	Auswirkungen auf die öffentliche Hand Auswirkungen auf die private Wirtschaft Auswirkungen auf die privaten Haushalte
Immateriell	Auswirkungen auf die öffentliche Sicherheit und Ordnung Politische Auswirkungen Psychologische Auswirkungen Schädigung von Kulturgut

Tabelle 6.2: **Schadensparameter (BT-Drucksache, 2013, 18/208, Anhang 3)**

Die Klassifizierung der Schadensparameter erfolgt durch die Zuordnung zu Schadensklassen. In Abhängigkeit vom Schadensparameter ist die Schadensausmaß-Klasse durch Zahlen oder durch Beschreibungen definiert. Nachstehend sind zwei Beispiele für die Klassifizierung der Schadensparameter „Verletzte, Erkrankte“ (siehe Tabelle 6.3) und „Auswirkungen auf die öffentliche Sicherheit und Ordnung“ (siehe Tabelle 6.4) gezeigt. Dass Schadensparameter beschreibend definiert sind, bedeutet nicht, dass sie nicht quantifizierbar sind.

Schadensparameter (Verletzte/Erkrankte)	
A:	≤ 10 Verletzte/Erkrankte
B:	> 10 – 100 Verletzte/Erkrankte
C:	> 100 – 1.000 Verletzte/Erkrankte
D:	> 1.000 – 10.000 Verletzte/Erkrankte
E:	> 10.000 Verletzte/Erkrankte

Tabelle 6.3: **Schadensparameter: Verletzte, Erkrankte (BT-Drucksache, 2013, 18/208, Anhang 2)**

Anmerkung: Betrachtet werden hier Personen, die durch das Ereignis im Bezugsgebiet verletzt werden oder im Verlauf des Ereignisses bzw. in dessen Folge so erkranken, dass sie ärztlich oder im Gesundheitswesen betreut werden müssen (hier sind auch Langzeitschäden/Spätfolgen mit zu berücksichtigen).

Zur Ermittlung des gesamten Schadensausmaßes gelangt man durch Addition der einzelnen Schadensparameter und Division durch die Anzahl der Schadensparameter. Die Visualisierung des Ergebnisses der Risikoanalyse erfolgt durch die Darstellung in einer Risikomatrix (Bild 6.2). Eine weitere detailliertere Möglichkeit ist die Darstellung als Balkendiagramm, die weiter unten an einem konkreten Beispiel gezeigt wird. Die Ergebnisse von Risikoanalysen werden darüber hinaus in einer umfangreichen Dokumentation festgehalten, die den wertvollsten Teil darstellt. Auf dieser Grundlage können Fachbehörden des Bundes, der Länder und Kreise für ihren Bedarf detailliertere Analysen erstellen.

Schadensparameter (Verletzte/Erkrankte)	
A:	Aufrechterhaltung der öffentlichen Sicherheit und Ordnung ist problemlos möglich
B:	Aufrechterhaltung der öffentlichen Sicherheit und Ordnung ist auf regionaler Ebene mit leicht erhöhtem Aufwand möglich
C:	Aufrechterhaltung der öffentlichen Sicherheit und Ordnung ist auf regionaler bis überregionaler Ebene nur mit erhöhtem Aufwand möglich
D:	Aufrechterhaltung der öffentlichen Sicherheit und Ordnung ist überregional mit großem Aufwand verbunden bzw. regional gefährdet
E:	Aufrechterhaltung der öffentlichen Sicherheit und Ordnung ist überregional bis bundesweit gefährdet

Tabelle 6.4: **Schadensparameter: Auswirkungen auf die öffentliche Sicherheit und Ordnung (BT-Drucksache, 2013, 18/208, Anhang 2)**

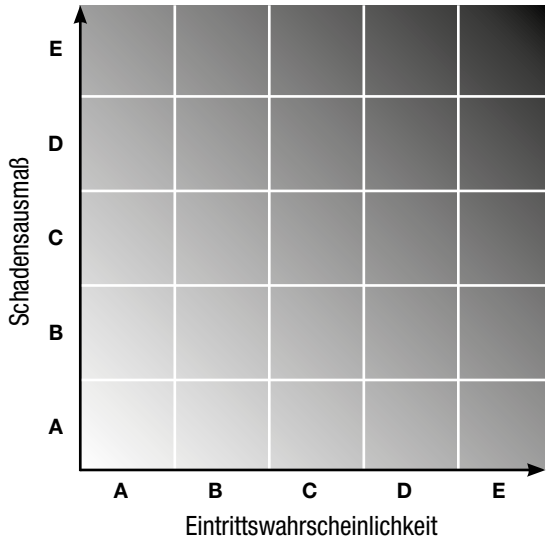

Bild 6.2: **Risikomatrix (Quelle BBK 4/2014)**

Die Risikoanalyse ist kein Selbstzweck, sie ist Teil des Risiko- und Krisenmanagements. Nächster Schritt nach der Analyse ist die Festlegung von Schutzzielen und die Risikobewertung. Die Verwaltung kann hierzu Vorschläge entwickeln, die Entscheidung liegt aber eindeutig bei der Politik. Hier stehen wir noch am Anfang.

6.4 Implementierung der Risikoanalyse im Bevölkerungsschutz

Die Implementierung der Risikoanalyse des Bundes im Bevölkerungsschutz erfordert ein interdisziplinäres Zusammenwirken über Ressortgrenzen hinweg. Der Lenkungsausschuss „Risikoanalyse Bevölkerungsschutz Bund“ sowie der Arbeitsausschuss „Risikoanalyse Bevölkerungsschutz Bund“ nehmen diese Aufgabe wahr.

Der Lenkungsausschuss unter der Federführung des BMI gibt einvernehmlich die Rahmenbedingungen vor. Die Schadensparameter und deren Klassifizierung werden in diesem Gremium festgelegt, ebenso wie die zu analysierenden Gefahren.

Der Arbeitskreis erarbeitet die Risikoanalyse. Er setzt sich aus Geschäftsbereichsbehörden der Bundesressorts zusammen. Die Federführung liegt bei der hauptsächlich betroffenen Behörde, dem „Risk Owner“. Die Zusammensetzung des Arbeitskreises hängt von der zu bearbeitenden Gefahr ab. Das BBK unterstützt in jedem Fall die Arbeit des Arbeitskreises. Erkenntnisse aus dem Arbeitskreis fließen in die Arbeit des Lenkungsausschusses ein (Bild 6.3).

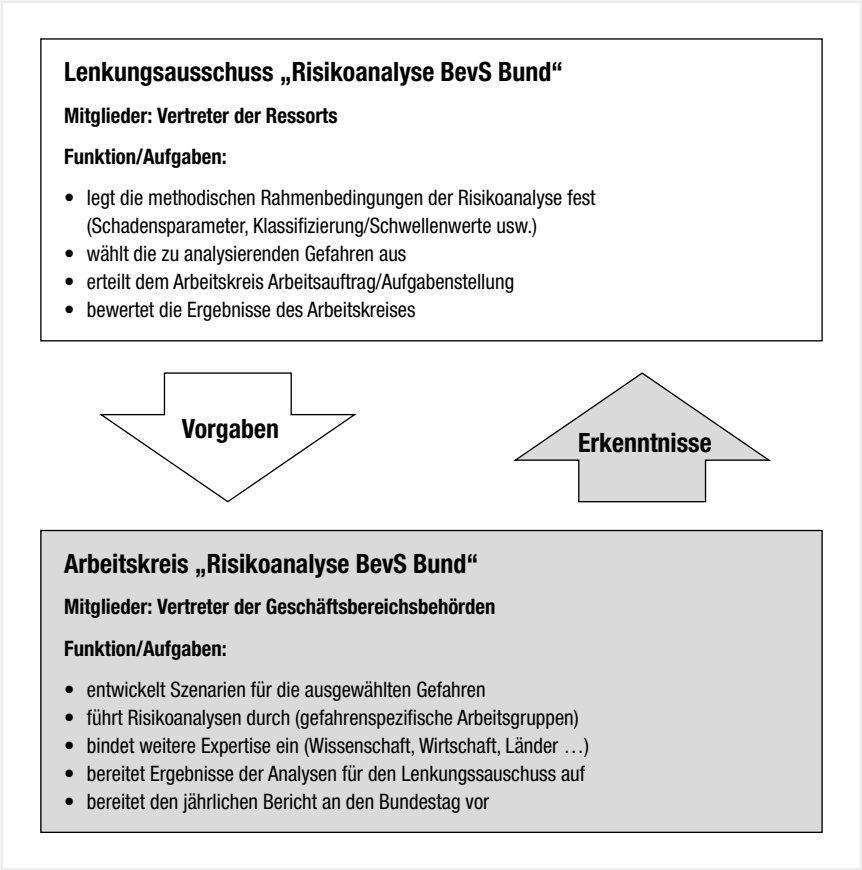

Bild 6.3: Lenkungsausschuss „Risikoanalyse BevS Bund“ (BT-Drucksache, 2011, 17/8250, vom 21.12.2011)

Bei der Auswahl der zu analysierenden Gefahren konnte neben den in den Ressorts vorliegenden Erkenntnissen auf eine Vielzahl einschlägiger Dokumente zurückgegriffen werden. Die wichtigsten sind nachstehend aufgeführt:

- Problemstudie Risiken für Deutschland,
- Gefährdungsabschätzungen der Länder und des Bundes,
- Gefahrenberichte der Schutzkommission,
- Grünbuch des Zukunftsforums Öffentliche Sicherheit,

- TAB-Bericht zur Gefährdung und Verletzbarkeit moderner Gesellschaften am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung,
- Deutsche Anpassungsstrategie an den Klimawandel.

Kriterium für die Auswahl der Gefahren und Risiken war in erster Linie die Bundesrelevanz, d. h. Gefahren und Ereignisse, die länderübergreifend und/oder so gravierend sind, dass sie die Reaktionsmöglichkeiten eines einzelnen Landes übersteigen. Man verständigte sich 2011 auf die nachfolgende Liste, die Anfang dieses Jahres vom Lenkungsausschuss betätigt wurde. Pro Jahr können derzeit ein bis zwei Risikoanalysen durchgeführt werden. Der aktuelle Sachstand ergibt sich ebenfalls aus der Liste (Quelle BBK 4/2014):

- Außergewöhnliches Seuchengeschehen (z. B. Pandemie/Epidemie) *2012 abgeschlossen,*
- Beeinträchtigung/Ausfall von KRITIS,
- Dürre,
- Ereignisse durch Pflanzenpathogene und Schädlinge,
- extraterrestrische Gefahren (Sonnensturm, Meteoriteneinschlag, Weltraumschrott),
- Freisetzung von biologischen Stoffen,
- Freisetzung von chemischen Stoffen,
- Freisetzung von radioaktiven Stoffen in Vorbereitung,
- Hitzeperiode,
- Hochwasser *2012 abgeschlossen,*
- Kälteperiode,
- Niedrigwasser,
- seismische Ereignisse (natürlich oder induziert, z. B. durch Bergbau),
- Starkniederschlag (Regen, Schnee etc.),
- Sturm *2013 abgeschlossen,*
- Sturmflut aktuell in Bearbeitung,
- Tierseuchen,
- Wildfeuer (Waldbrand, Moorbrand, Heidebrand).

6.5 Risikoanalyse Wintersturm

Die Risikoanalyse „Sturm“ mit einem Szenario „Wintersturm“ wurde Ende 2013 abgeschlossen. Das Szenario war so gewählt, dass alle Länder, allerdings mit unterschiedlicher Intensität, betroffen sind. Der Ansatz war behördenübergreifend, insgesamt waren die folgenden 16 Institutionen beteiligt:

- Deutscher Wetterdienst (fachliche Federführung),
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
- Bundesanstalt für Materialforschung und -prüfung,
- Bundesnetzagentur,
- Bundesamt für Bauwesen und Raumordnung,
- Bundesanstalt für Landwirtschaft und Ernährung,
- Bundesanstalt Technisches Hilfswerk,
- Bundesamt für Güterverkehr,
- Luftfahrt-Bundesamt,
- Eisenbahn-Bundesamt,
- Bundesanstalt für Straßenwesen,
- Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben,
- Bundesamt für Naturschutz,
- Bundesanstalt für Immobilienaufgaben,
- Bundespolizei,
- Bundesamt für Seeschifffahrt und Hydrographie.

Die Analyse erfolgte auf der Grundlage vorliegender Erkenntnisse und Experteneinschätzungen. Der Abstraktionsgrad trug der übergeordneten Bundesperspektive Rechnung. Die Risikoanalyse kann bei Bedarf durch detaillierte Folgeanalyse ergänzt werden. Dies kann fachliche (Ressorts, Fachbehörden) als auch räumliche (Länder, Landkreise) Aspekte umfassen. Als Eintrittswahrscheinlichkeit wurde die Klasse C ermittelt: bedingt wahrscheinlich (ein Ereignis, das in der Regel einmal in einem Zeitraum von 100 bis 1.000 Jahren eintritt).

Die Klassifizierung des Schadensausmaßes für die Schadensparameter ist in Form eines Balkendiagramms dargestellt, siehe Bild 6.4.

Das gemittelte Gesamtschadensausmaß ist der Klasse C zuzuordnen.

Schutzgut	Schadensparameter		Schadensausmaß A B C D E
MENSCH	M_1	Tote	
	M_2	Verletzte, Erkrankte	
	M_3	Hilfebedürftige	
	M_4	Vermisste	
UMWELT	U_1	Schädigung geschützter Gebiete	
	U_2	Schädigung von Oberflächen-gewässern/Grundwasser	
	U_3	Schädigung von Waldflächen	
	U_4	Schädigung landwirtschaftlicher Nutzflächen	
	U_5	Schädigung von Nutztieren	
VOLKSWIRT-SCHAFT	V_1	Auswirkungen auf die öffentliche Hand	
	V_2	Auswirkungen auf die private Wirtschaft	
	V_3	Auswirkungen auf die privaten Haushalte	
IMMATRIELL	I_1	Auswirkungen auf die öffentliche Sicherheit und Ordnung	
	I_2	Politische Auswirkungen	
	I_3	Psychologische Auswirkungen	
	I_4	Schädigung von Kulturgut	

Bild 6.4: Schadensparameter für das Schadensausmaß (BT-Drucksache, 2013, 18/208, Anhang 3)

6.6 Internationale Aktivitäten

Wie bereits eingangs erwähnt, finden Entwicklung und Durchführung der Risikoanalyse unter Berücksichtigung der internationalen Aktivitäten statt. Es folgt ein intensiver Informationsaustausch auf vielen Ebenen. So findet z. B. parallel zu dieser Veranstaltung ein Workshop mit Österreich und der Schweiz (DACH-Format) zum Thema Risikoanalyse statt.

Hervorzuheben ist der bilaterale Erfahrungsaustausch auch mit den Niederlanden, dem Vereinigten Königreich, Dänemark, den USA und China. Kontakte bestehen zu zahlreichen weiteren Staaten. Grenzüberschreitende Pilotprojekte finden mit Nachbarstaaten statt.

Die EU hat sich des Themas angenommen und Ende 2010 die „Risk Assessment and Mapping Guidelines for Disaster Management" veröffentlicht. Das Papier enthält umfangreiche Informationen zur Risikoanalyse und -bewertung und zu den Methoden. Deutschland hat die EU-Kommission bei der Erstellung der Richtlinien intensiv unterstützt, unter anderem durch die Veranstaltung eines gemeinsamen internationalen Workshops im Frühjahr 2010 in Berlin. Es ist daher nicht verwunderlich, dass die Empfehlungen der Kommission kompatibel mit den deutschen Aktivitäten sind.

Die EU hat dann 2012 die Erstellung eines sektorübergreifenden Überblicks über die Hauptrisiken innerhalb der EU in Angriff genommen. Diese Aktivität krankt daran, dass die Mitgliedsstaaten sich in sehr unterschiedlichen Stadien der Implementierung der Risikoanalyse befinden und damit eine einheitliche Datenbasis nicht gegeben ist. Um den Implementierungsprozess zu befördern, unterstützt die Kommission die Mitgliedsstaaten aktiv beim Erfahrungsaustausch.

Die künftige italienische Ratspräsidentschaft plant eine weitere Initiative zum Risk Assesssment und hat zur Vorbereitung einen umfänglichen Fragebogen an die Mitgliedsstaaten übermittelt. Zu erwähnen sind weiterhin die Aktivitäten der

OECD. Die OECD hat ein „High Level Risk Forum“ eingerichtet, das einen breiteren All-Gefahren-Ansatz (Multi Hazard Approach) unter Einschluss von Wirtschafts- und Finanzkrisen verfolgt. Deutschland ist durch BMI/BBK vertreten.

2012 hat die OECD ein „Methodological Framework for Disaster Risk Assessment and Risk Financing“ erarbeitet. Dieser ausgezeichnete Überblick beleuchtet zusätzlich zum allgemeinen Risk Assessment auch die Rolle von Versicherern und Rückversicherern bei der Krisenbewältigung.

Die OECD bietet den Mitgliedsstaaten die Untersuchung ihres Krisenmanagementsystems an. Ergebnisse liegen zu Japan und Italien vor.

6.7 Fazit

Die deutsche Methode „Risikoanalyse im Bevölkerungsschutz“ hat sich bewährt und sie ist für alle Ebenen der Verwaltung anwendbar. Die Methode ist allerdings nicht in Stein gemeißelt, sie muss mit zunehmendem Erfahrungsschatz optimiert werden. Sofern Katastrophen eintreten, für die vergleichbare Risikoanalysen vorliegen, sollten diese anhand der gewonnenen Erfahrungen überprüft werden. Die Festlegung von Schutzzielen und der an dieser Messlatte vorzunehmende Soll-Ist-Abgleich existieren erst in sehr geringem Umfang. Hier bleibt ebenso wie bei der Risikobewertung noch viel zu tun. Die Risikoanalysen des Bundes sollten durch entsprechende Aktivitäten der Länder und Kreise ergänzt und vertieft werden.

Die deutsche Methode „Risikoanalyse im Bevölkerungsschutz“ ist mit den Empfehlungen von EU und OECD kompatibel. Somit sind auch die Ergebnisse gut für das geplante Risikokataster der EU verwendbar. Die bilaterale internationale Zusammenarbeit funktioniert sehr gut. Sie wird erleichtert durch sehr ähnliche Ansätze, wenngleich in der Art der Implementierung deutliche Unterschiede in den verschiedenen Staaten feststellbar sind.

Grenzüberschreitende Risiken und deren Bewältigung werden künftig mehr in den Fokus rücken.

Zusammenfassend kann festgestellt werden, dass wir bei der Risikobeurteilung auf einem guten Weg sind. Einiges ist bereits erreicht worden, aber vieles bleibt noch zu tun, unabhängig davon, dass die Risikobeurteilung ein kontinuierlicher Prozess ist und somit immer wieder an neue Rahmenbedingungen und Gefährdungen angepasst werden muss.

7

Sicherheitswissenschaft: Risikokompetenz ohne Informationstechnik?

Zusammenfassung

Dr. Ralf Mock, Zürcher Hochschule für angewandte Wissenschaften ZHAW, Schweiz

Durch die immer stärkere Vernetzung technischer Systeme, z. B. von Produktionssystemen, durch die Informationstechnik (IT) haben sich diese in einer Art und Weise verändert, die eine Anpassung der Sicherheitswissenschaft an diesen Wandel erforderlich machen. Diese Anpassung hat bisher nicht stattgefunden und der Sicherherheitswissenschaft droht, den Anschluss an die moderne Technik zu verlieren. Der Beitrag skizziert den Wandel über Beispiele aus der IT und leitet Anforderungen an und Lösungsansätze für die Sicherheitswissenschaft ab. Es gilt, die Gefahren, die aus dem IT-Einsatz entstehen, mit in den methodischen Apparat der Sicherheitswissenschaft aufzunehmen. Ebenso bedeutet dies, zusammen mit der Informatik Tools zu entwickeln, die sicherheitstechnische oder risikoanalytische Analysen von Systemen effizienter machen. Auch hier lassen sich Ansätze aus der Informatik nutzen, z. B. die Verwendung von Unified Modelling Language Diagrams (UML) und das Denken in Funktionsebenen technischer Systeme.

7.1 Einleitung

Sicherheitswissenschaft beschäftigt sich mit einer Vielzahl von Themen, für die sie einen methodischen Rahmen schafft. Der Beitrag greift jenen Teilbereich heraus, der sich in Theorie und Praxis mit Industrie- und Produktionssystemen befasst. In diesem Bereich hat die Sicherheitswissenschaft zwei Aufgaben: Technische Systeme sind so zu gestalten, dass ihr Betrieb für Mensch und Umwelt sicher ist. Hierfür liefern Ingenieurwissenschaften das notwendige Rüstzeug. Die zweite Aufgabe besteht in der Beurteilung dieser Systeme auf Sicherheit und damit allgemein auf Akzeptanz. Die Sicherheitswissenschaft teilt sich damit in einen objektiv-quantitativen und einen subjektiv-qualitativen Anteil auf. Die Risikoanalytik als Teil der Sicherheitswissenschaft spiegelt diese Zweiteilung wider. Sie identifiziert zunächst Gefährdungen und liefert Risikozahlen auf der Grundlage einer ingenieur-technischen Vorgehensweise. Das Risiko-Assessment beurteilt diese Risikozahlen anhand von Akzeptanzkriterien, um Entscheidungen treffen zu können, ob risikoreduzierende Maßnahmen erforderlich sind. Die Akzeptanzkriterien stammen aus nicht technischen Disziplinen wie regulatorischen Vorgaben, Ökonomie und Soziologie. Die zunehmende Vernetzung technischer Systeme durch die Informationstechnik (IT) bedeutet einen Wandel, der eine formal schlüssige, objektive Beschreibung von Systemen immer schwieriger oder zumindest aufwendiger macht. Damit ist der Rahmen dieses Beitrages grob umrissen: der Umgang der (angewandten) Sicherheitswissenschaft mit IT-abhängigen Infrastrukturen. Er skizziert dabei anlagentechnische und IT-infrastrukturelle Systeme und zugehörige Methoden der Risikoanalyse. Der Beitrag zeigt den Wandel durch die zunehmende Vernetzung technischer Systeme auf Komponenten- und Systemebene durch die IT beispielhaft auf. Neue Aufgaben und Probleme der Sicherheitswissenschaft werden abgeleitet sowie Lösungsansätze aus der Informatik. Der Beitrag schließt mit dem Versuch eines Fazits. Im Anhang finden sich kurze Exkurse zur IT Security und zu den angesprochenen IT-Techniken SCADA, RFID und NFC.

7.2 Systeme und Analysen

7.2.1 Anlagentechnisch

Die Sicherheitswissenschaft blickt auf eine lange Tradition zurück. Sie hat dabei ein in sich geschlossenes Konzept zur Analyse und Beurteilung technischer Systeme entwickelt. Typischerweise sind dies Anlagen und Organisationsstrukturen mit definierbaren Systemgrenzen. Dies spiegelt auch der Systembegriff wider:

Definition 1 (System). Eine Ansammlung von Entitäten, die auf die Erfüllung eines gewissen logischen Ziels hin agieren und zusammenwirken (nach [25]).

Diese Systemdefinition beruht somit darauf, dass ein System durch seine zusammenhängenden Entitäten, z. B. technische Komponenten, beschreibbar ist. Lassen sich diese Entitäten über ihre Systemgrenzen definieren, dann kommen die bekannten Werkzeuge der sicherheitstechnischen Systemanalyse zum Einsatz:

- semi-formal: HAZOP (Hazard and Operability Study), FMEA (Failure Mode and Effects Analysis), Bow-Tie-Diagramm u. a.,
- formal: Fehlerbaumanalyse (Fault Tree Analysis, FTA), System-Theoretic Accident Model and Processes; System-Theoretic Process Analysis (STAMP; STPA) Markov-Zustandsdiagramme, Prozess-Simulation (System Dynamics Models, Bayessche Netzwerke u. a.)

Der Blickwinkel der Analysen ist von innen nach außen gerichtet: Ein gefährlicher Stoff könnte aus einer gesicherten oder geschützten Umgebung in die Umwelt entweichen und diese schädigen. Diese Umwelt stellt den zu bewahrenden Wert dar (Asset). Der umfangreiche methodische Apparat der Sicherheitswissenschaft lässt sich anhand der probabilistischen Sicherheits- oder Risikoanalysen (PSA, PRA) in der nuklearen Energieerzeugung zeigen, z. B. [7]. Lees Standardwerk [13] zeigt Vergleichbares für die chemische Industrie.

7.2.2 IT-infrastrukturell

Die Sicherheitswissenschaft kann sich mit IT-infrastrukturellen Systemen auf zwei Abstraktionsebenen beschäftigen. Die umfassendere Ebene ist das Informationssystem (IS), definiert als:

Definition 2 (Informationssystem). Ein System […] zum Erfassen, Speichern und Verarbeiten von Daten sowie zur Übermittlung von Informationen, Wissen und digitalen Produkten (nach Enc. Brit. Online).

IS beschreiben nicht nur Computer-Technik, wie in der Definition angedeutet, sondern informationsverarbeitende Systeme allgemein. Dazu gehören Geschäftsprozesse, aber auch ein Vortrag vor Publikum.

Die Definition von IT ist dann der Übergang von abstrakten IS zu konkreten Geräten und Programmen.

Definition 3 (Informationstechnik). […] Oberbegriff für die Informations- und Datenverarbeitung sowie für die dafür benötigte Hard- und Software (informationstechnisches System [Wikipedia; 8. Jan. 2014]).

Die Analysen von IT-Systemen beruhen auf einer anderen Tradition als die traditionelle Sicherheitswissenschaft, wobei auch der Blickwinkel der Analysen ein anderer ist (vgl. [17]). Die IT dreht die Betrachtungsweise um: Die Umwelt bedroht den zu bewahrenden Wert (Asset), z. B. durch einen Hackerangriff auf Firmendaten. Zudem wird angenommen, dass eine bekannte Bedrohung (threat) nur zu Konsequenzen führt, wenn sie auf eine passende Schwachstelle (Vulnerability) trifft. Auf dieser Sichtweise beruht das Risk Assessment im Rahmen der IT Security, wie im Leitfaden NIST [1] deutlich wird (Bild 7.1).

Die üblichen (und raren) Methoden des IT Risk Assessment sind in Tabelle 7.1 zusammengestellt.

Die Methoden der Tabelle 7.1 sind dabei methodisch sehr einfach und beruhen auf Checklisten oder einem FMEA-ähnlichen Ansatz. CORAS beruht auf Graphen (genauer auf einem Typ der Unified Modelling Language Diagramme (UML), ist aber letztlich nur ein Werkzeug zur Unterstützung des Brainstormings.

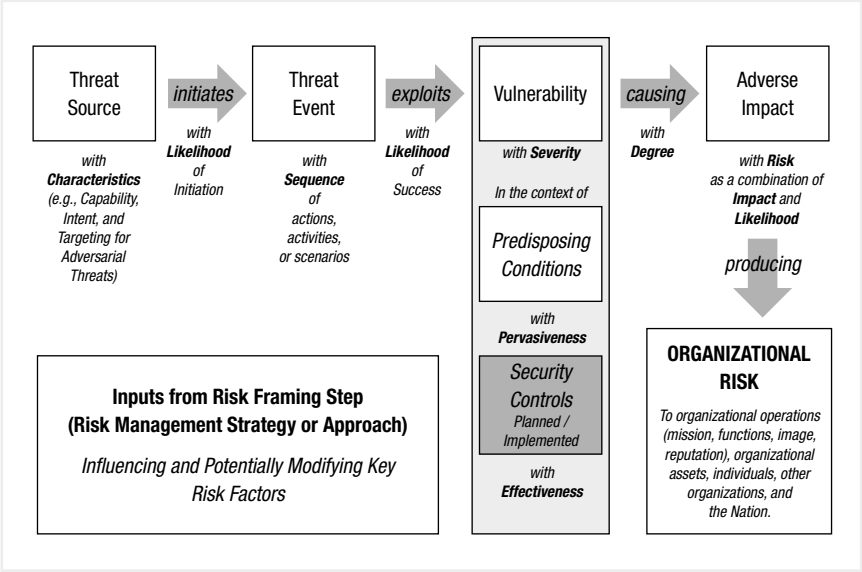

Bild 7.1: IT Risk Assessment (aus: [1])

Tool	Bezeichnung	Bem., Quelle
CRAMM	CCTA[1] Risk Analysis & Management Method	Ablaufdiagramme, -graphen [12]
CORAS	Platform for risk analysis of security critical systems	F., Maßnahmenliste [5, 4, 26]
MEHARI	Méthode Harmonisée d´Analyse de Risques	F.; [14]
OCTAVE	Operationally Critical Threat, Asset, & Vulnerability Evaluation	F., Version Allegro; [19, 3]
RiskPAC	–	F.; [23, 26]

Tabelle 7.1: Übliche Methoden des IT Risk Assessment

CCT A[1] = Central Computer and Telecommunications Agency, UK; F: Fragebogen.

7.3 Wandel

Bis jetzt hat die Sicherheitswissenschaft eine gewisse Anpassungs- und Erweiterungsfähigkeit bewiesen. Als Beispiel mag die PSA in der nuklearen Energieerzeugung dienen: Sie nutzt die Methoden der quantitativen Zuverlässigkeitsanalyse (FTA, abhängige Ausfälle), ermittelt Brandrisiken, die Erdbebenfestigkeit von Gebäuden, bezieht die Human Reliability Analysis (HRA) mit ein sowie Flugzeugabstürze, Unwetterschäden u. a. In der Schweiz führten in letzter Zeit internationale Fortschritte auf dem Gebiet der Erdbebenforschung und -modellierung zu einer Anpassung der probabilistischen Erdbeben-Gefährdungs-Analyse (PEGASOS) bzw. zum PEGASOS Refinement Project (PRP) [29]. Im Wesentlichen handelt es sich dabei um den Einbezug erweiterter Analyseanforderungen oder Ergänzungen in der Abgrenzung und Beschreibung der traditionell in der Sicherheitswissenschaft untersuchten Systeme.

7.3.1 Industrie 4.0

Mit dem (journalistischen) Schlagwort „Industrie 4.0" werden die vier Hauptstufen in der Geschichte industrieller Produktionsweisen charakterisiert: Dampfmaschine – Fliessband – Automation – Vernetzung. Der Ablauf ist gleichzeitig ein Indikator für die zunehmende Bedeutung vernetzter Informationssysteme bei zunehmendem IT-Einsatz. Was dieser Wandel für Sicherheits- und Risikoanalysen mit sich bringt, ist im Weiteren anekdotenhaft dargestellt.

Komponentenebene
Die Komponenten eines technischen Systems, z. B. einer Produktionsanlage, sind anlagenintern samt Kontroll- und Steuerungseinrichtungen vernetzt. Mit dem Übergang in Richtung „Industrie 4.0" kommen Schnittstellen nach außen hinzu. Die damit verbundenen neuen Möglichkeiten wurden von den Ingenieuren zunächst optimistisch aufgenommen, wie der Artikel *Anlagen notfalls vom Hotelzimmer aus überwachen* der VDI nachrichten vom 18. November 2005 zeigt. Internettechnologien erlaubten einen schnellen und kostengünstigen Zugriff

auf Maschinendaten. „Bei kleineren Unternehmen führen dabei nach Angaben von Fachleuten bereits einfache Expertensysteme zu erheblichen Prozessverbesserungen“. Dieser Überschwang hätte schon 2005 jeden Informatiker mehr als erstaunt, gehen doch die Anfänge der Computerviren bis 1985 zurück. Der Artikel *Steuerungssysteme im Visier der Hacker* der VDI nachrichten vom 26. April 2013 spiegelt diese Erkenntnis, wenn auch spät, deutlich wider. Ein aktueller Trend birgt hier eine weitere Überraschung: Bring Your Own Device (BYOD).

Definition 4 (Bring Your Own Device). Erlaubt Anwendern ein selbst ausgewähltes und erworbenes Kundengerät (Smartphones, Tablets etc.) zu verwenden, um Unternehmens-Applikationen auszuführen und um auf Daten zuzugreifen.

Nach Willis [31] bedeutet „das Aufkommen von BYOD-Programmen [...] die allerwichtigste radikale Veränderung im Client-Computing-Geschäftswesen für Unternehmen, seit PCs den Arbeitsplatz erobert haben“. Client Computing heißt, dass Anwender mit einem Server verbunden sind, der Anwendungen und Daten zentral speichert und verarbeitet. Ein BYOD-Programm in einem Unternehmen bedeutet für IT-Verantwortliche zunächst einen massiven Anstieg der zu berücksichtigenden Hardware- und Software-Varianten. OpenSignal führte 2012 eine Studie zu diesem Thema durch: Man fand 3997 unterschiedliche Android-Geräte bezüglich „Modell, Marke, Version des Android-Betriebssystems und Monitor-Größe“ [21]. Hinzu kommt, dass heutzutage BYODs von ihren Anwendern rasch ausgetauscht werden. So werden Mobiltelefone „in den USA und UK nach 18 und in Japan innerhalb von 12 Monaten ersetzt“ [30]. So ergeben sich neue Angriffs-Vektoren, um in eine Anlage einzudringen. Installiert man beispielsweise eine Spiele-App auf seinem BYOD-Smartphone, so kann dies auch bedeuten, dass Screenshots einer Firmen-Web-Dienst-Anwendung unbemerkt an Dritte verschickt werden (durch sog. „Sneaker“); Passwörter durch „keylogging“ abgefangen werden und schließlich die eigene Authentifizierung der Firmen-Zertifikate durch einen „Sniffer“ unterminiert wird. Die Arbeit [15] ordnet die Bedrohungen durch BYOD für ein Unternehmen folgenden Ursachen zu:

- **Mobile Geräte:** Offline-Attacken bei verlorenen oder entwendeten Geräten. Hier besteht ein großes Problem, da eine riesige Anzahl von Smartphones und Tablets (Hauptanteil), Laptops und USB-Laufwerken in Hotels, Kaufhäusern und Flughäfen liegen bleibt [30]. Neue Angriffs-Vektoren erwachsen durch sog. Schadgeräte (rogue hardware), z. B. entsprechend ausgestattete Lade- oder Dockingstationen für mobile Geräte.
- **Netzwerk:** Datenzugriff durch das Anzapfen des (verschlüsselten oder unverschlüsselten) Netzwerkverkehrs zum und vom mobilen Gerät.
- **Unternehmens-Infrastruktur:** ungenügende Umsetzung von Richtlinien, z. B. des IT-Grundschutzes im Unternehmen.
- **Eigentümer des mobilen Gerätes:** absichtlich oder unabsichtlicher Zugriff.
- **„Cloud“:** Transfer vertraulicher Daten vom Unternehmen zum Cloud-Dienstleister (z. B. DropBox).

BYOD ist für Unternehmen mittlerweile eine Tatsache, gleichgültig ob diese den Einsatz von BYOD wünschen oder nicht. Es wird jedoch noch schlimmer: Mit Wearables gelangen weitere Kleincomputer mit ihren Daten, Schnittstellen und Möglichkeiten in die Unternehmen. Als Konsequenz sollten der Zugriff auf Maschinendaten etwa via Client Computing und BYOD und die daraus resultierenden Schäden in Risk Assessments von Komponenten mit aufgenommen werden. Damit ist eine Anwendung wie das Remote Maintenance sicherheitstechnisch und hinsichtlich IT-Security zu hinterfragen.

Systemebene

Eine Vernetzung von Einzelkomponenten durch das Internet oder andere Kommunikationspfade hebt die Betrachtung von der Komponenten- auf die Systemebene. Die Systemgrenzen und damit die Ziele und Aufgaben einer Sicherheits- oder Risikoanalyse verschieben sich damit ebenfalls. So kann unbemerkt aus einem bisher abgeschotteten, mithin sicheren, Inselsystem, ein Teil des Internets werden. Als praktische Feststellung für Analysen folgt: Ein System und jedes seiner Komponenten sollte heutzutage als netzwerkfähiger Computer verstanden werden. Ein Dozent an der ZHAW gibt folgendes Beispiel: Die IT-Verantwortlichen eines Schweizer Hospitals bemerkten einen unüblich hohen Datenverkehr. IT-Security-Checks zeigten nichts Auffälliges. Hinzugezogene externe IT-Experten fanden nach einer mehrtägigen Suche die Ursache: eine Herz-Lungen-Maschine. Diese war im Zuge der Einführung der elektronischen Patientenakte ans Internet angeschlossen worden. Die Steuerung solcher Geräte nutzt adaptierte, aber sonst übliche Betriebssysteme, z. B. der Firma

Microsoft. Mit der Vernetzung wurde aus der Maschine ein ungeschützter Internet-Computer, der auch prompt aus dem Internet infiziert und als Teil eines Botnetzes missbraucht wurde.

Infrastruktursysteme, z. B. Wasserwerke, waren schon Ziele erfolgreicher Internet-Attacken auf der Basis von Insider-Wissen ehemaliger Mitarbeiter (vgl. [6]). Stuxnet wiederum kann als Beispiel einer zielgerichteten, aufwendigen Internet-Attacke gelten, die die Betriebsfähigkeit auf Systemebene beeinflusst. Angriffsziele hier waren zunächst das SCADA einer Uran-Anreicherungsanlage im Iran und in einer nächsten (einfacheren) Version die Manipulation eines Zentrifugen-Rotors der Anlage [11].

7.3.2 Systemgrenzen

Mit dem Wandel der Systeme von singulären, abgegrenzten Entitäten in vernetzte, offene Informationssysteme ändert sich der Untersuchungsgegenstand grundsätzlich. Eine klassische Risiko- oder Zuverlässigkeitsanalyse geht von definierten System- oder Komponentengrenzen aus, um letztlich bestimmen zu können, ob diese z. B. ausgefallen sind oder nicht. Auf der Zählung der Ausfälle beruhen dann die Berechnungen zur Ausfallwahrscheinlichkeit. Mit der Industrie 4.0 verliert der bisherige Systembegriff seine Bedeutung bzw. wesentliche Systemkomponenten sind für Analytiker nicht mehr sichtbar. Allenfalls lässt sich ermitteln, ob ein bestimmter Service verfügbar war. Hier ähnelt die Betrachtungsweise der Berücksichtigung der Energieversorgung in den Analysen. Inwieweit solche Analysen dann für ein darauf aufbauendes Risikomanagement nutzbar sind, ist fraglich, da mit dem Internet auch verschachtelte Verantwortungs- und Zugriffsketten aufgebaut wurden. Zum Beispiel führe eine Drittfirma die Remote-Instandhaltung von Ventilen in einem Unternehmen durch. Diese Drittfirma hat jedoch den Betrieb ihrer Service-Angebote auf eine „Cloud“ ausgelagert. Der Cloud-Betreiber wiederum hat einen Service-Level-Agreement-Vertrag (SLA) mit einem weiteren Anbieter geschlossen, um seinen Server-Park instand zu halten. Der Cloud-Betreiber betreibt zudem seine Dienste auf virtuellen Servern, was eine Zuordnung von Diensten auf bestimmte Geräte fast unmöglich macht. Wer, wann, welche Geräte und Programme betreibt, und wer auf welche Daten und Systeme Zugriff hat, ist praktisch nicht mehr festzustellen. Die Sicherheitswissenschaft hat in Bezug auf erweiterte und offene Systemgrenzen generell neue Aufgaben zu bewältigen. Ohne weiter

ins Detail zu gehen, seien diese neuen Aufgaben mit vernetzten Systemen mit den Schlagwörtern „Systems of Systems“ und „telcom needs power & power needs telcom“ angedeutet.

7.4 Stand der Sicherheitswissenschaft

7.4.1 Neue Aufgaben

Die Vernetzung von Systemen schafft für die Sicherheitswissenschaft neue Anforderungen, denen sie sich auf drei Ebenen stellen muss, um in ihren Ergebnissen von Nutzen zu bleiben. Bild 7.2 zeigt die Ebenen mit Bezug auf eine Internet-Attacke.

Wie die Beispiele und vor allem Bild 7.2 zeigen, ist ein Risk Assessment ohne Berücksichtigung der IT und der damit verbundenen Steuerungssysteme nicht vollständig und bleibt in ihren Aussagen zu optimistisch (Das gleiche Statement gab es vor dem Einbezug abhängiger Ausfälle sowie der HRA in die PSA.). In Anlehnung an Bild 2 erwachsen für die Sicherheitswissenschaft u. a. folgende neue Aufgaben:

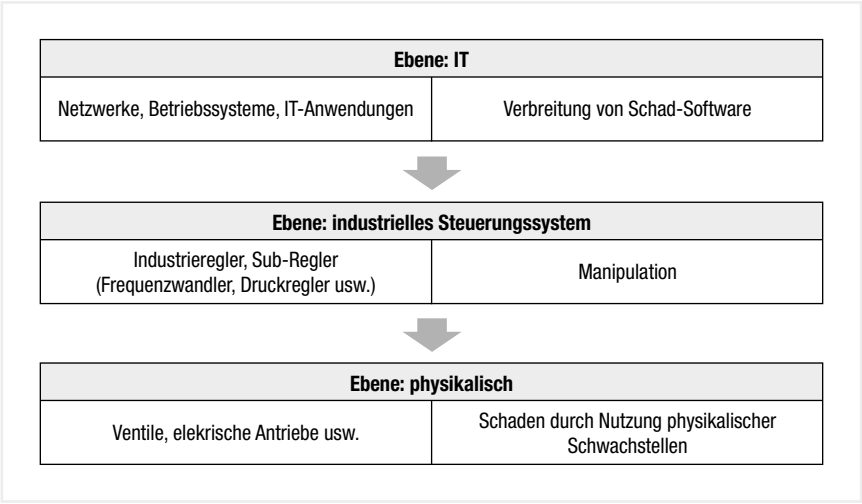

Bild 7.2: **Bedrohungsschichten einer Internet-Attacke gegen Industrieanlagen (nach [11])**

- **Daten/Services:** Diese Aufgabe umfasst vor allem den Schutz von Unternehmensdaten vor allen Arten der Cyber-Kriminalität. Betroffen sind dabei eher Dienstleistungen, Geschäftsprozesse und Datenschutz. Dies ist zunächst ein Gebiet der IT Security, die hier ein umfangreiches Instrumentarium zur Handhabung liefert (allerdings wenig im Rahmen eines Risk Assessments). Im Sinne der Industrie 4.0 bleibt ein Produktionssystem zunächst unbeeinflusst, ein Datendiebstahl evtl. sogar unbemerkt. In der Sprache der Sicherheitswissenschaft handelt es sich um ungefährliche Systemzustände. Der Übergang zu gefährlichen Systemzuständen ist jedoch fließend. Einflussnahme auf die Betriebssysteme computergestützter Komponenten, oder die Blockierung unternehmenseigener IT-Anwendungen betreffen dann auch das Produktionssystem. Eine Denial-of-Service-Attacke (DoS-Attacke), die den Zugriff auf Web-Dienste durch Überlastung der Server verhindert, ist ein Beispiel. Für Verantwortliche sind dann evtl. Informationen nicht mehr verfügbar, um Systemdaten abzurufen, im Notfall Maßnahmen zu koordinieren etc.
- **Daten/Steuerung:** Es sollte davon ausgegangen werden, dass es für jede moderne Produktionsanlage eine Bedrohung samt passender Schwachstelle gibt, um unautorisiert auf deren Mess- und Steuerungssysteme negativen Einfluss nehmen zu können. Damit entstehen neue, gefährliche Systemzustände, wie sie z. B. in einer Risikoanalyse zusätzlich zu berücksichtigen sind. Dies kann nur gelingen, wenn die IT-Schwachstellen in den Steuerungssystemen erkannt und beurteilt sind, wie sie z. B. durch den Einsatz von SCADA oder RFIDs entstehen.
- **Personen/Organisation:** Die Art und Weise, wie mit Programmen, SCADA, Web-Diensten etc. umgegangen wird, ist von Personen abhängig. Die Analyse ist eine Aufgabe der HRA, die hier ein neues Anwendungsfeld finden kann. Die Sicherheitswissenschaft sollte hier ein in sich geschlossenes Konzept liefern, das Unternehmen hilft, Strategien, Strukturen und Prozesse zu etablieren, um einen sicheren Umgang mit allen Systemen einschließlich der IT zu ermöglichen.
- **Personen/Lehre:** Aus der Erfahrung des Autors zum Risk Assessment für Anlagen- und IT-Systeme lässt sich zusammenfassen, dass in den IT-Abteilungen von Unternehmen die klassischen Methoden der Risikoanalyse fast völlig unbekannt sind, die Risikoanalytiker die Methoden des IT-Risk Assessment aber auch nicht kennen. Die Sicherheitswissenschaft hat hier die Chance, sich über die Hochschulen bekannter zu machen.

7.4.2 Die Musik spielt woanders …

Bleibt die Frage, ob die Sicherheitswissenschaft methodisch und praktisch für die neuen Aufgaben gerüstet ist. Aus den Erfahrungen des Autors heraus ist die Antwort eher ein Nein – es droht, dass sie für die Industrie 4.0 den Anschluss verpasst hat bzw. von der Informatik getrieben wird. Als persönliches Resümee des Autors „kriselt" die Sicherheitswissenschaft in der Praxis in den Bereichen Praxisnähe, Effizienz sowie Standards und Normen. Im Einzelnen:

Praxisnähe: Die Sicherheitswissenschaft hat viele Methoden der Systemanalyse hervorgebracht. Allerdings erstaunt das Bild in der Praxis immer wieder. Hier kommen nur wenige und methodisch einfache Ansätze zum Einsatz. Umfragen zeigen dies auch: Eine ältere Umfrage von 1999 [16] bei der chemischen Industrie (D, CH) nennt vor allem HAZOP und die Zurich Hazard Analysis (ZHA). FMEA, Fehlerbaumanalyse und Checklisten folgen in größerem Abstand. Die ZHA ist eine toolgestützte, vor allem in der Schweiz verbreitete und FMEA-ähnliche Methode der Zurich Insurance Company, um „alle Arten von Gefährdungen oder Vulnerabilitäten (sic!) systematisch zu identifizieren, anzusprechen und handzuhaben […]". Eine aktuellere Umfrage (D, A) von 2012 [2] nennt vor allem: Brainstorming, FMEA und verwandte, Root Cause Analysis, What-If-Analysis und Critical Incident Reporting System. Die Fehlerbaumanalyse spielt nur eine untergeordnete Rolle.

Mit Brainstorming, Checklisten und FMEA/HAZOP-Tabellen lassen sich die komplexen Strukturen vernetzter Systeme nur schlecht abbilden. Die Sicherheitswissenschaft scheint hier in den Unternehmen im Rückzug: Es ist bisher nicht gelungen, andere Methoden oder Tools zu etablieren. Die Bow-Tie-Analyse ist hier eine Ausnahme, sofern sie Barrieren und die zugehörigen Eskalationsfaktoren mit berücksichtigt. Sie wird dann zu einer Vulnerability-Analyse.

Effizienz: Zumindest für Unternehmen ist die Effizienz einer Methode ein Indikator für Brauchbarkeit und Praxisnähe. Auch hier hat die Sicherheitswissenschaft nachzuholen, wie die Erfahrung zeigt. In der nuklearen Energieerzeugung sind für PSAs größere Ressourcen vorhanden, was in Anbetracht des radioaktiven Inventars eines Reaktors angemessen ist. Ein Team von ca. vier Experten ist Jahre ausschließlich damit beschäftigt, eine PSA fertig zu stellen oder zu aktualisieren. Im Bedarfsfall wird Expertise zugekauft. Solche Ressourcen machen auch die Durchführung formal komplexer Methoden möglich.

Der Alltag (samt Gefährdungen) in vielen anderen Unternehmen sieht anders aus. Risikoanalysen sind dort eine Angelegenheit von Tagen, allenfalls wenigen Wochen, die eine oder zwei Personen durchführen. Das dürfte der Hauptgrund dafür sein, dass fast nur einfachste Methoden zum Einsatz kommen. Die IT hat eine ähnliche Erfahrung hinter sich: Risikoanalysen waren bis vor zehn oder fünfzehn Jahren in den IT-Abteilungen von Unternehmen durchaus im Trend. Seitdem gelten sie dort als „Verschwendung von Zeit und Geld". Die Unternehmen widerstehen daher der Versuchung meist nicht, geforderte sicherheitstechnische Analysen durch Expertenbefragungen und Expertenmeinungen zu ersetzen. Allerdings ist dann die Vorgehensweise nicht mehr von der Kunst des Wettens zu unterscheiden und man hat den Pfad der Ingenieurwissenschaften verlassen.

Die Sicherheitswissenschaft beachtet die Bedeutung geringer Ressourcen zu wenig in ihren Entwicklungen. Es könnte sein, dass die Unternehmen dank IT das Online-Monitoring ihrer Anlagen immer attraktiver finden werden und keine Notwendigkeit mehr für Sicherheitswissenschaft sehen. Es fehlen Tools, die die Risikoanalytiker unterstützen. Die Tool-Entwicklung ist jedoch wiederum eine Domäne der Informatik.

Standards und Normen: Ein weiterer Trend, der in vielen Unternehmen zu beobachten ist, ist die Gleichsetzung von Risiko Assessment mit Compliance Checks. Risk Assessments haben zum Ziel, auch bisher unerkannte Fehler in einem System zu finden und über einen Risikowert zu beurteilen. Ein Compliance Check dagegen geht den umgekehrten Weg. Anhand von Checklisten auf der Grundlage des „Stands der Technik" (Normen und gesetzliche Vorgaben) wird eine Abfrage auf bekannte Fehler durchgeführt. Unbekannte Fehler werden weder gesucht, noch gefunden. Die Güte der Ergebnisse hängt von der Qualität der zugrundeliegenden Norm ab. Ein System kann somit zwar legalistisch sicher, aber im Sinne der Risikoanalytik inakzeptabel sein. Die IT als Trendsetter führt fast nur noch Compliance Checks durch, wenn auch mittlerweile eine Grenze erreicht und erkannt ist (vgl. [17]).

Für die Unternehmen sind Normen von zentraler Bedeutung, für Hochschulen kaum. Dabei handelt es sich um einen bekannten Zielkonflikt der beiden Parteien. Aber auch bei den Normen, die für die Sicherheitswissenschaft und die Risikoanalytik relevant sind, scheint sich eher die Sichtweise der Vulnerability-Analyse, und damit jene der Informationstechnik, durchzusetzen (Zu den Zusammenhängen zwischen Risk, Vulnerability und Resilience siehe [22]). Ein

Beispiel ist der für alle ISO-Standards gültige Leitfaden ISO-Guide 73 [9] zum Risiko-Management: Eine Neuerung in Bezug auf die vorgängige Version [8] ist, dass der Begriff Vulnerability auftaucht (der ISO Guide 73 definiert Risiko neu als Abweichung von Zielvorgaben (Unter- und Übererfüllung), was aus einer Risikoanalyse ein „HAZOPing“ macht).

Die Sicherheitswissenschaft hat an Einfluss verloren, was die Entwicklung von Standards und Normen betrifft. Auch hier gewinnen die Methoden und Denkansätze der Informatik. Der Sicherheitswissenschaft droht, in ihren Entwicklungen den Anschluss zu verlieren. Sie hat die IT, aber auch deren Möglichkeiten, stark vernachlässigt.

7.4.3 Lösungsansätze

Aller neuer Aufgaben und Probleme zum Trotz gibt es nach Ansicht des Autors Ideen und Ansätze, z. B. aus der Informatik, die einen Einsatz in der Sicherheitswissenschaft lohnen.

Mit den bereits kurz angesprochenen UML-Diagrammen (UML) ist mittlerweile ein standardisiertes Paket zur Darstellung nahezu aller Arten komplexer Systeme entstanden. Die OMG-Website [20] nennt drei Hauptkategorien der UML 2.0 bei insgesamt 13 Diagramm-Typen:

1. **Strukturdiagramme:** Klassendiagramm, Objektdiagramm, Komponentendiagramm, Kompositionsstrukturdiagramm, Paketdiagramm, Verteilungsdiagramm

2. **Verhaltensdiagramme:** Use-Case-Diagramm, Aktivitätsdiagramm, Zustandsautomat

3. **Interaktionsdiagramme** (alle abgeleitet von den Verhaltensdiagrammen): Sequenzdiagramm, Kommunikationsdiagramm, Timingdiagramm, Interaktionsübersichtsdiagramm

Eine praxisnahe Einführung UML und deren Anwendung gibt [24], woraus auch das Klassendiagramm des Bildes 7.3 stammt.

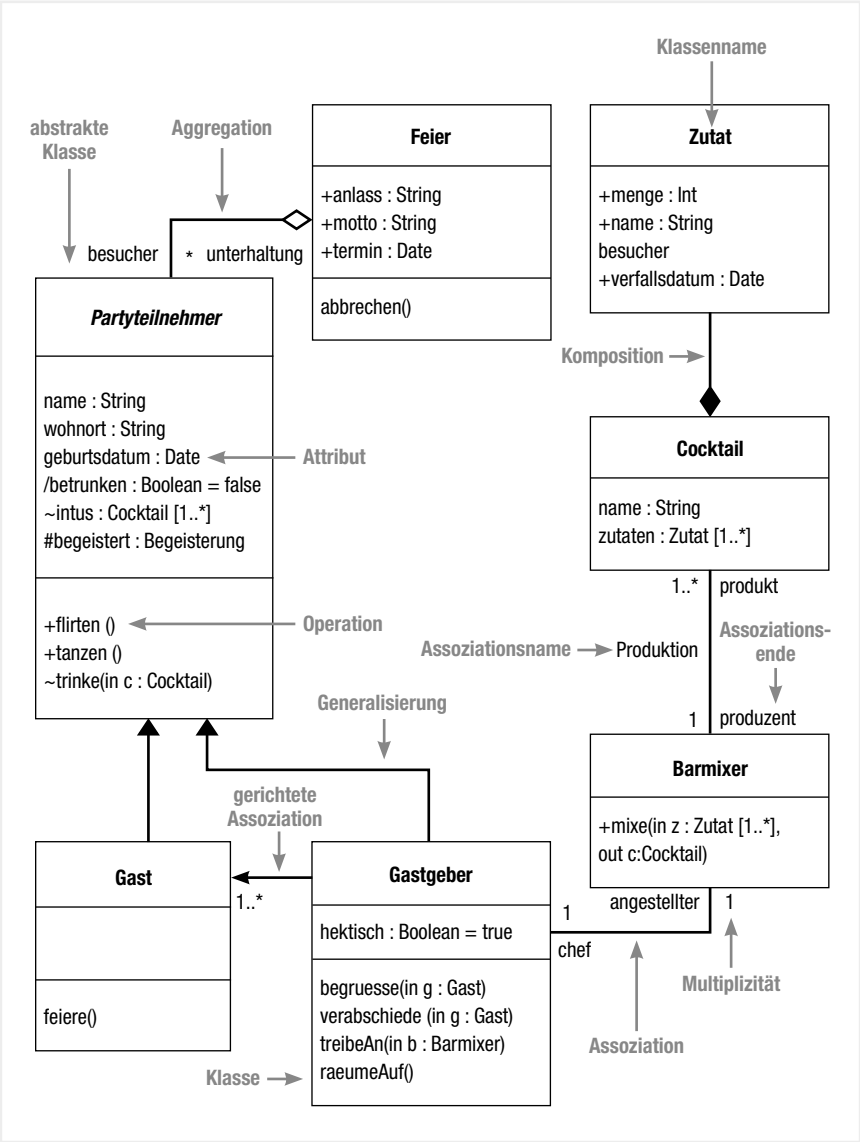

Bild 7.3: **Elemente des Klassendiagramms (Spezifikation der Klasse „Partyteilnehmer“) [24]**

Alle UML-Diagramme verfügen über eine eigene, definierte und standardisierte Notation, die Risikoanalysen zusätzliche Auswertemöglichkeiten bereitstellt. So lassen sich z. B. aus den Assoziationen eines Klassendiagramms (Kanten des Graphen) sowie aus den Operationen Hinweise ablesen, die sich für eine Risikoanalyse nutzen lassen [18]. Eine Aufgabe der Sicherheitswissenschaft besteht darin, hierfür geeignete Heuristiken zu entwickeln. Ein anderer Ansatz, der die Sicherheitswissenschaft unterstützen könnte, ist das Denken in Funktionshierarchien, wie in der Informatik üblich. Ein typisches Beispiel lieferte bereits Bild 2. Das Prinzip ist in der Informatik zur Darstellung von IT-Systemen stark ausgebaut. Das bekannteste Hierarchiemodell ist OSI (Open System Interconnection; siehe z. B. (Zbigniew Gargasz BLOG)) mit den Ebenen:

7: Anwendung: Verbindung zw. Anwendungsprogrammen, z. B. E-Mail
6: Darstellung: Vorbereitung der Daten für die Anwendungsschicht (Decodierung, Umwandlung, Verschlüsselung, Prüfung, […])
5: Kommunikation: Steuerung der Verbindungen und des Datenaustauschs
4: Transport: Zuordnung der Datenpakete zu einer Anwendung
3: Vermittlung: Routing der Datenpakete zum nächsten Knoten
2: Sicherung: Segmentierung der Pakete in Frames und Hinzufügen von Prüfsummen
1: Bitübertragung: Umwandlung der Bits in ein zum Medium passendes Signal und physikalische Übertragung
(0): Hardware

Insgesamt sollten Sicherheitswissenschaft und die Informatik interdisziplinäre Teams bilden. Dies würde auf zwei Ebenen helfen: Zum einen ist Informatik mittlerweile so komplex, dass das nötige Fachwissen für erweiterte Systemanalysen nur von dort kommen kann. Zum anderen haben die bisher getrennten Wege dazu geführt, dass Informatiker technische Tools auf der Höhe des Software-Engineerings entwickelt haben, die allerdings einen Mangel an sicherheitswissenschaftlichen Grundkenntnissen erkennen lassen. Andererseits haben Sicherheitswissenschaftler die entsprechenden Kenntnisse, können aber ihre Ideen und Methoden nicht in Tools umsetzen, die dem Stand und den Möglichkeiten der Informatik entsprechen. Zum Wechselspiel zwischen „eEngineering Risk Assessment“ und dem „IT Risk Assessment“ siehe auch [17].

7.5 Versuch eines Fazits

Die technischen Systeme der Industrie sind im Wandel begriffen, wobei die IT und die Informatik eine immer größere Rolle spielen. Bei Fragen zur Sicherheit und zum Risiko dieser Systeme berühren sich zwei Ingenieurdisziplinen, die sich mehr oder weniger unabhängig voneinander entwickelt haben. Dabei ist zu beobachten, dass die Informatik die Trends der Entwicklung setzt und die Sicherheitswissenschaft ins Hintertreffen geraten ist. Das mag auch daran liegen, dass man sich etwas auf dem umfangreichen und bewährten Methoden- und Normenapparat ausgeruht hat, wie er seit den späten 1940er-Jahren mit der Entwicklung der FMEA entstanden ist. Eine „Risikokompetenz ohne Informationstechnik" ist schlicht nicht mehr zeitgemäß.

Die Sicherheitswissenschaft könnte zwei Bereiche abdecken: Zum einen bedeutet dies den Einbezug der IT in ihre Art der (Risiko-)Analytik. Dies heißt zunächst, Identifikation, Beurteilung und Handhabung von Gefahren aus der IT als Teil ihrer Aufgabe zu verstehen und methodisch einzubauen. Hierbei sollten die Erfahrungen der IT mit komplexen und dynamischen Systemen genutzt werden. Zum anderen bietet eine Zusammenarbeit mit Informatikern die Chance, effiziente Tools der Risikoanalytik (und anderen Bereichen, z. B. der Arbeitssicherheit) zu entwickeln.

Die Sicherheitswissenschaft hat sich bis jetzt mit ihrem interdisziplinären Ansatz als anpassungsfähig erwiesen. Doch der Wandel erfolgt in einem nie gekannten Ausmaß – für eine Anpassung bleibt der Sicherheitswissenschaft nicht viel Zeit …

Literatur

[1] Guide for Conducting Risk Assessments – Information Security. National Institute of Standards and Technology (NIST), 2012.

[2] Andrlik, Christian: Die Risikoanalyse und -bewertung in der Praxis der Gefährdungsbeurteilung von Arbeitsplätzen (Dissertation). Bergische Universität Wuppertal, FB D – Abt. Sicherheitstechnik, Wuppertal, 2012.

[3] Caralli, A., J. F. Stevens, L. R. Young und W. R. Wilson: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Technischer Bericht, Software Engineering Institute, 2007.

[4] Cline, B. S.: The Information Security Assessment and Evaluation Methodologies: A DoD Framework for Control Self-assessment. ISACA Journal Online, 7:1 – 4, 2007.

[5] CRAMM: Central Communication and Telecommunication Agency Risk Analysis and Management Method. 2011. http://www.cramm.com.

[6] E., Mills und Beiersmann S.: Hacker greift texanisches Wasserwerk an. ZDNet, NetMediaInteractive, Nov. 21, 2011. http://www.zdnet.de/news/41558114/hacker-greift-texanisches- wasserwerk-an.htm, visited: Mar. 18, 2014.

[7] IAEA: Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants (Specific Safety Guide No. SSG-3)., International Atomic Energy Agency (IAEA), 2010.

[8] ISO/IEC-Guide73: Risk Management Vocabulary Guidelines for Use in Standards (ISO/IEC GUIDE 73:2002(E/F)). ISO/IEO, 2002.

[9] ISO/IEC-Guide73b: Risk Management – Vocabulary. Nummer ISO/IEC GUIDE 73:2009(E/F). ISO/IEO, 2009.

[10] ITIL: ITIL V3 – Glossar (31.08.2007; englische Basisversion: 3.1.24). IT Service Management Forum, 2007.

[11] Langner, Ralph: To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group, Nov. 2013. http: //www.langner.com/en/resources/papers/, visited: Mar. 19, 2014.

[12] Lund, M. S., B. Solhaug und K. Stolen: Modeldriven risk analysis: The CORAS approach. Springer, 2011. http://coras.sourceforge.net/.

[13] Mannan, Sam: Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control. Elsevier Butterworth-Heinemann, Burlington, Oxford, 2. Auflage, 2005.

[14] MEHARI: MEHARI 2010: Fundamental concepts and functional specifications. Club de la Sécurité de l'Information Français, August 2010. http://www.clusif.fr/en/clusif/present/; visited: Jan., 2014.

[15] Merki, Oliver: Bring Your Own Device (BYOD) from a risk management perspective (Bachelor thesis). Zürich University of Applied Sciences ZHAW, Feb., 26 2014.

[16] Mock, R. und J. van Mahnen: Risk Analysis Methods in Processing Industry: A Swiss – German Survey. Band 2, Seiten 1145–1156. Society for Risk Analysis-Europe (SRA-E), 8th Conference, ISPN, 1999.

[17] Mock, R., H. Straumann und A. Fischer: A Second Chance for Risk Assessment in IT System Analysis? Proc. of European Safety and Reliability Conference (ESREL 2013), Seiten 2237–2244, 2014.

[18] Mock, R., B. Truninger, P. Brunner und T. Hruz: Enhancement of IT Risk Assessments by UML (Accepted Paper). Proc. of European Safety and Reliability Conference (ESREL 2014), 2014.

[19] OCTAVE: Operational ly Critical Threat, Asset, and Vulnerability EvaluationSM . 2008. http://www.cert.org/octave/.

[20] OMG: Introduction to OMG's Unified Modeling Language (UML). Website, Object Management Group (OMG), Apr. 18 2013. http://www.omg.org.

[21] OpenSignal: The many faces of a little green robot. OpenSignal, Inc., 2012. http://opensignal.com/reports/fragmentation.php; visited: Mar., 2013.

[22] Pasman, H. J., B. Knegtering und W. J. Rogers: A holistic approach to control process safety risks: Possible ways forward. Reliability Engineering & System Safety, 117:21-29, 2013.

[23] RiskPAC: Business Continuity Planning & Risk Assessment. Open Systems Technologies Int., 2009. http://www.opensystems-bs.com, visited Jan. 21, 2013.

[24] Rupp, Chris und Stefan Queins: UML 2 glasklar – Praxiswissen für die UML-Modellierung. Carl Hanser Verlag, Munich, 4. Auflage, 2012.

[25] Schmidt, J. W. und R. E. Taylor: Simulation and analysis of industrial systems. Richard D. Irwin, Homewood, Ill., 1970.

[26] Schreider, T.: Risk Assessment Tools: A Primer. Information Systems Control Journal, 2, 2003.

[27] Stoneburner, G., A. Goguen und A. Feringa: Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST), 2002.

[28] Suprina, Darren: Security Risks With RFID. RFID Journal Live!, 2005. http://www.rfidjournal.com/articles/view?1564, visited: Mar. 19, 2014.

[29] swissnuclear: Themen Erdbebensicherheit: PEGASOS Vorwort. swissnuclear, Fachgruppe der Kernenergie der swisselectric, 2014. http://www.swissnuclear.ch/de/pegasos-vorgeschichte.html, visited: Mar.18, 2014.

[30] Wilhelm, W., A. Yankov und P. Magee: Mobile Phone Consumption Behaviour and the Need for Sustainability Innovations. Journal of Strategic Innovation and Sustainability, 7(2):20–40, 2011.

[31] Willis, D. A.: Bring Your Own Device: New Opportunities, New Challenges. Gartner, 2012.

Anhang

EXKURS: IT-SECURITY

Die international verbreitete IT Information Library [10] definiert:

Definition 5 (IT Security). Der Prozess, bei dem die Vertraulichkeit, Integrität und Verfügbarkeit der Assets, Informationen, Daten und IT Services einer Organisation sichergestellt werden.

Der Beitrag behält die englische Bezeichnung bei. Dieser Begriff hat sich eingebürgert, obwohl die Übersetzung „IT-Schutz" korrekt wäre. Die drei Ziele der IT Security, d. h. Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability), sind der kleinste gemeinsame Nenner (kurz CIA): Vertraulichkeit beschreibt die Anforderung, Daten vor unautorisiertem Lesen zu schützen. Integrität betrifft Datenintegrität (Daten dürfen nicht auf unautorisierte Weise verändert werden) oder Systemintegrität (das datenverarbeitende System ist frei von unautorisierter Manipulation). Verfügbarkeit ist die Forderung, Daten vor unautorisiertem Löschen bzw. das System vor unautorisiertem Ressourceneinsatz zu schützen. Die Verletzung der IT-Security-Schutzziele kann dabei absichtlich oder zufällig erfolgen (CIA vereinfacht nach [27]).

EXKURS: SCADA

Langner [11] definiert SCADA als:

Definition 6 (SCADA (Supervisory Control And Data Acquisition)). Gruppe von Computer-Programmen, die zur Anzeige und Analyse von Prozessbedingungen verwendet werden.

Derselbe Autor betont auch, dass, im Gegensatz zu verbreiteten Annahmen, SCADA „nur eine Komponente einer automatisierten Anlage [ist] und nicht direkt mit Stellgliedern, wie Ventilen, Pumpen oder Motoren, interferiert". Dies werde durch Industrieregler (industrial controllers) bewirkt, die in Realzeit betrieben würden und weder Anzeige noch Tastatur hätten. Eine entsprechende Attacke beeinflusst eine Produktion insofern, da die angezeigten nicht mehr mit den realen Prozessparametern übereinstimmen („Man-in-the-Middle-Angriff") und Operateure in die Irre führt.

EXKURS: RFID

Die Brockhaus Enzyklopädie Online; 15. Jan. 2013 definiert

Definition 7 (RFID (Radio Frequency Identification)). Technologie zur automatischen Identifizierung und Datenerfassung von Objekten, die mit einem RFID-Tag (z. B. einem aufgeklebten Funketikett) versehen werden, das eine Antenne und elektronische Bauelemente enthält. Es handelt sich somit um eine Sende-und-Empfänger-Technik, mit der Daten übermittelt und ausgelesen werden können. Wichtig im Zusammenhang mit diesem GfS-Beitrag ist, dass über RFID (oder noch einfacher über das Einlesen von Barcodes) „Schaddaten" eingelesen werden können, die zumindest den Betriebsablauf einer Anlage stören können. „Unternehmen sollten sich den Security-Risiken, wie Profilbildung (Profiling), Abfangen von Daten (Eavesdropping), Dienstleistungsverhinderungen (Denial of Service Attacks) und Bestandsstau (inventory jamming), bewusst sein" (nach [28]).

EXKURS: Near Field Communication

Die Near Field Communication (NFC) ist ein internationaler Übertragungsstandard zum kontaktlosen Datenaustausch per Funk über kurze Strecken von wenigen Zentimetern und einer Datenübertragungsrate von maximal 424 kBit/s. Die Übertragung erfolgt verbindungslos (mit passiven HF-RFID-Tags) oder verbindungsbehaftet (zwischen gleichwertigen aktiven Transmittern). Die verbindungslose Nutzung ist nach üblicher Definition nicht sicher gegen Angriffe von „Dritten" (nach Wikipedia; 3. März 2014).

8

Überblick über Ansätze zur Risikobeurteilung – qualitative und quantitative Verfahren

Zusammenfassung

Prof. Dr. Heinz-Willi Brenig, Fachhochschule Köln, Deutschland

Methoden und Vorgehensweisen zur Risikoabschätzung und -bewertung industrieller Anlagen und Prozesse werden seit vielen Jahren mit Erfolg eingesetzt. Bei der Beurteilung konkreter industrieller Vorhaben im Rahmen einer Anlagenzulassung stehen die technischen, organisatorischen und das Sicherheitsmanagement betreffenden Fragen im Vordergrund. In der Raumordnung und Bauleitplanung geht es insbesondere um Schutzabstände zwischen industrieller und wohnlicher Nutzung im Sinne sekundärer Schutzmaßnahmen, ergänzend zu den technischen und sonstigen Maßnahmen der Anlagenauslegung. Bei der Betrachtung unter dem Gesichtspunkt des Katastrophenschutzes nehmen Kriterien für eine eventuelle Evakuierung der Bevölkerung einen breiten Raum ein. Zunehmend werden die etablierten qualitativen/quantitativen Verfahren nicht nur zur Beurteilung von technischen Risiken eingesetzt, sondern z. B. auch zur Analyse und Bewertung der Gefahren für die Bevölkerung durch den Ausfall kritischer Infrastrukturen, zur Bewertung der Auswirkungen des Klimawandels sowie zur Sicherheitsbetrachtung von Großveranstaltungen. Die vorhandenen Methoden müssen daher weiterentwickelt und an die neuen Randbedingungen angepasst werden. Im Mittelpunkt stehen dabei der Umgang mit offenen Systemgrenzen und sich zeitlich verändernden Randbedingungen (dynamische Prozesse) sowie die Weiterentwicklung des Vulnerabilitäts- bzw. Resilienzansatzes.

8.1 Einleitung

Das Risiko von Prozessen, Systemen, Anlagen und Veranstaltungen kann durch Maßnahmen des Risikomanagements minimiert und dadurch die Sicherheit verbessert werden. Ziel des Risikomanagements ist es, das Restrisiko auf ein akzeptables Maß zu beschränken.

Gesetze, Richtlinien und Normen sind das Ergebnis retrospektiver Risikobetrachtungen. Vorschriften und Regelungen basieren auf umfassenden Schadensanalysen sowie darauf aufbauenden Festlegungen und Maßnahmen zur Verhinderung der Wiederholung bekannter Ereignisse.

Die zunehmende Komplexität der Anlagen und Prozesse sowie der notwendige Grad an Sicherheit erfordern eine vorausschauende systematische Gefahrensuche und Gefahrenbeurteilung, die prospektive Risikoanalyse (ES-CIS, 1996). Risikomanagement ist – wie es hier betrachtet wird – stets präventiv.

Ein Risikomanager will Schäden gar nicht erst entstehen lassen. Das Risiko-Assessment (Risikoanalyse und Risikobewertung) ist das zentrale Werkzeug des Risikomanagers. Es liefert die notwendigen Grundlagen für die zu treffenden Entscheidungen und die Festlegung von Maßnahmen zur Verhinderung von unerwünschten Ereignissen sowie zur Begrenzung möglicher Auswirkungen.

Der vorliegende Beitrag gibt ausgehend von der historischen Entwicklung einen Überblick über qualitative und quantitative Verfahren zur Risikobeurteilung. Die Diskussion über die Vor- und Nachteile der deterministischen und probabilistischen Verfahren wird schon seit mehreren Jahrzehnten geführt. In (DECHEMA, 2006) wird u. a. dazu ausgeführt:

- die deterministische und die probabilistische Vorgehensweisen widersprechen einander nicht,
- der Einsatz von probabilistischen Methoden kann auch ohne gesetzlich festgelegte Risikoakzeptanzgrenzen zweckmäßig sein.

Inzwischen ist in Europa ein eindeutiger Trend zur quantitativen Risikobewertung, insbesondere zur Beurteilung von technischen Risiken, im Bereich der Arbeitssicherheit sowie im Brandschutz erkennbar. Risikobewertungen werden zunehmend auch im Bevölkerungsschutz sowie zur Beurteilung von Veranstaltungen eingesetzt. Ausgehend von den Ereignissen in Fukushima stoßen die bekannten Vorgehenseisen aber dann an ihre Grenzen, wenn es sich um sehr seltene Ereignisse mit hohem Gefahrenpotenzial handelt. Die vorhandenen Systeme müssen daher weiterentwickelt und an die neuen Herausforderungen angepasst werden.

Zudem ist in vielen Fällen noch die Frage nach den Akzeptanz- bzw. Toleranzgrenzen ungeklärt. Die Aussage des Bundesverfassungsgerichtes im sogenannten Kalkur-Urteil von 1978 (BVerfG, 1978): „Das Gesetz überläßt es damit weithin der Exekutive über Art und insbesondere über das Ausmaß von Risiken, die im Einzelfall hingenommen oder nicht hingenommen werden, zu befinden; auch über das Verfahren zur Ermittlung solcher Risiken trifft es selbst keine näheren Regelungen“ hat bis heute weiter Gültigkeit.

8.2 Begriffe und Definitionen

Die relevanten Begriffe zum Themenbereich „Risikoermittlung und Risikobewertung“ werden in den einzelnen Fachgebieten zum Teil unterschiedlich verwendet. Bis heute herrscht in der Praxis ein Sprachgewirr – Sicherheitsingenieure, Versicherungskaufleute, Juristen usw. verstehen unter dem Begriff Risiko jeweils etwas anderes. Zur Vereinheitlichung des Wortgebrauchs und um Missverständnisse vorzubeugen, werden daher zunächst einige Begriffe vorgestellt und erläutert.

8.2.1 Risikomanagement

Der Begriff Risikomanagement wird im alltäglichen Sprachgebrauch vielfältig benutzt:

- Banker managen damit ihr Kredit-Engagement,
- Versicherungsmakler benutzen es als Reklame-Floskel,
- Consultants reduzieren es vielfach auf ihre Kernkompetenzen, z. B. Brandsicherheit.

Mit der ISO 31000 wurde 2008 erstmals eine Norm veröffentlicht, die die Grundsätze für das Risikomanagement einheitlich beschreibt. Bezüglich einer Definition für den Begriff „Risikomanagement“ verweist diese Norm auf den ISO/IEC Guide 73. Davon ausgehend hat die Störfallkommission in (SFK, 2004) den Begriff folgendermaßen definiert:

„Risikomanagement ist ein Prozess, der die Elemente der Risikoabschätzung und der Risikokommunikation, die in allen Phasen der Prozesse möglich und auch sinnvoll sind, im Hinblick auf die herrschende oder noch herzustellende Risikoakzeptanz miteinander verknüpft.“

Für den Bevölkerungsschutz wurden ausgehend von Schutzzielen, die auf den Grundrechten basieren, folgende Definitionen gewählt:
„Kontinuierlich ablaufendes, systematisches Verfahren zum zielgerichteten Umgang mit Risiken, das die Analyse und Bewertung von Risiken sowie die Planung und Umsetzung von Maßnahmen, insbesondere zur Risikovermeidung, -minimierung und -akzeptanz, beinhaltet“ (BBK, 2011).

8.2.2 Risiko

In Bereichen des täglichen Lebens, in verschiedenen Branchen, in vielen wissenschaftlichen Bereichen, wird der Risikobegriff heute verwendet und angewandt. Zweifelsfrei beinhaltet der Begriff in seiner Gesamtheit die Elemente: „Schadensart, Ungewißheit des Schadenseintritts – beschrieben durch die Eintrittshäufigkeit eines Schadens – und das mögliche Schadenausmaß“ (Kafka, 1992).

In der Norm ISO/IEC Guide 73 findet sich folgende Definition: „Unter Risiko versteht man die Kombination aus Häufigkeit oder Wahrscheinlichkeit und der Auswirkungen eines zum Schaden führenden Ereignisses“.

Für den Bevölkerungsschutz (BBK, 2011) gilt folgende Definition: „Maß für die Wahrscheinlichkeit des Eintritts eines bestimmten Schadens an einem Schutzgut unter Berücksichtigung des potentiellen Schadensausmaßes“.

Im technischen Bereich wird das Risiko gemäß der nationalen Norm DIN VDE 31000 Teil 2 wie folgt definiert: „Das Risiko, das mit einem bestimmten technischen Vorgang oder Zustand verbunden ist, wird zusammenfassend durch eine Wahrscheinlichkeitsaussage beschrieben, die die zu erwartende Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses und das beim Ereigniseintritt zu erwartende Schadensausmaß berücksichtigt.“

Das Risiko sollte, wie von Blaise Pascal (1623–1662) gefordert, sowohl zur Wahrscheinlichkeit als auch zum Schadensausmaß proportional sein. Dies führt zu der in der Literatur üblichen Definition des Risikos R als Produkt von Wahrscheinlichkeit P und Schadensausmaß C. Dieses Produkt kann als Erwartungswert des Schadens als Folge eines Ereignisses aufgefasst werden und wird daher gelegentlich auch mit Schadenserwartung bezeichnet.

Die Definition des objektiven, mathematisch gefassten Risikobegriffs (Mock, R., 2002) basiert auf der logischen ingenieurwissenschaftlichen Erfahrung und Erfassung eines Tatbestandes unter den Kriterien:

- der Nachprüfbarkeit,
- einer möglichst weitgehenden Unabhängigkeit vom Beobachter,
- einer bestimmten Methode, z. B. Statistik und deren Ergebnisse.

8.2.3 Sicherheit, Gefahr, Restrisiko

In Anlehnung an den ISO/IEC Guide 51 gibt Bild 8.1 die Beziehung der zentralen Begriffe *Sicherheit, Gefahr* und *Restrisiko* untereinander wieder.

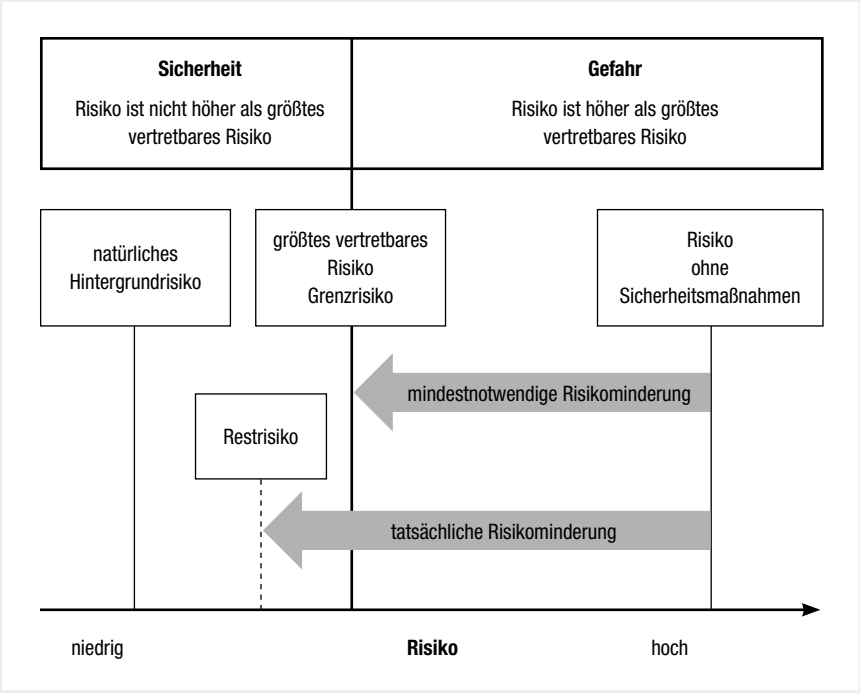

Bild 8.1: **Risikoansatz zur Beurteilung technischer Risiken in Anlehnung an (SFK, 2004)**

Als Grenzrisiko wird dabei allgemein das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes bezeichnet. Das Grenzrisiko wird durch objektive und subjektive Einflüsse bestimmt und lässt sich im Allgemeinen nicht quantitativ erfassen.

8.2.4 Risikoanalyse

Die Risikoanalyse ist eine systematische Auswertung verfügbarer Informationen, um Gefährdungen zu identifizieren und Risiken einzuschätzen. Die vollständige Erfassung und sachgerechte Bewertung aller Risiken ist Voraussetzung für eine erfolgreiche Risikopolitik. Die systematische Gefahrensuche ist der anspruchsvollste Schritt der Risikoanalyse. Zur Beantwortung dieser Fragen werden nach (Peters, Meyna, 1986) verschiedene Methoden der Risikoanalyse verwendet, die sich gegenseitig ergänzen.

Die chemische Industrie in der Schweiz (ESCIS, 1996) unterscheidet die analytischen Verfahren gemäß Tabelle 8.1 in intuitive, induktive und deduktive Verfahren.

Methode	Beispiel
Intuitiv	Brainstorming
Induktiv (Was kann passieren?)	Checklisten Ereignisablaufanalysen PAAG-Verfahren Bedienungsfehleranalysen
Deduktiv (Wie kann es passieren?)	Fehlerbaumanalysen

Tabelle 8.1: **Methoden und Beispiele (ESCIS, 1996)**

Eine andere gängige Einteilung ist die Unterscheidung in deterministische, risikoqualifizierende und probabilistische Methoden: Hinsichtlich des Arbeitsaufwandes und des damit verbundenen Detaillierungsgrades kann grundsätzlich zwischen den qualitativen und quantitativen Verfahren unterschieden werden. Die qualitativen Verfahren sind in der Regel mit weniger Aufwand und vergleichbar schnell durchzuführen. Sie dienen daher häufig einer ersten schnellen Identifikation und groben Bewertung der vorhandenen Gefahren. Sowohl Schadensausmaß als auch Eintrittshäufigkeit werden verbale Kategorien (Ein-

tritt: häufig oder sehr unwahrscheinlich; Schaden: katastrophal oder vernachlässigbar) zugeordnet und die Ergebnisse in Form einer Risikomatrix dargestellt (siehe BBK, 2010).

Quantitative Verfahren erfordern in der Regel einen deutlich höheren Arbeitsaufwand; dies betrifft insbesondere die Beschaffung der notwendigen statistischen Daten. Bei der quantitativen Risikoanalyse wird das Risiko als Produkt aus Schadensausmaß und Häufigkeit dargestellt und kann somit als Erwartungswert des Schadens aufgefasst werden. Quantitative Risikoanalysen weisen häufig sowohl Zahlen für das individuelle als auch das kollektive Risiko aus. Das individuelle Risiko gibt dabei die Häufigkeit an, mit der eine einzelne Person aufgrund eines unerwünschten Ereignisses zu Schaden – in der Regel das Todesfallrisiko – kommt. Das kollektive Risiko beschreibt die Häufigkeit, dass mehrere Personen gleichzeitig durch ein Ereignis getötet werden bzw. einen Schaden erleiden (CPR 18 E, 1999).

Die etablierten Methoden der Risikoanalyse und Bewertung – ISO 31010; Risk Management und Risk Assessment techniques, 2009 – gehen davon aus, dass die Gefahren bekannt sind sowie ausreichende statistische Daten und Erfahrungen vorliegen, um diese nach Art und Ausmaß eindeutig zu beschreiben. Das Risiko ist kalkulierbar und kann damit auch gehandhabt werden. Für neue Fragestellungen, z. B. Auswirkungen des Klimawandels und Auswirkung des Ausfalls kritischer Infrastrukturen für die Bevölkerung, reichen diese Methoden in der Regel nicht mehr aus, da Gefahren und Auswirkungen im Vorfeld nicht immer direkt erkenn- und eindeutig bestimmbar sind. Zudem müssen nach (Mock, R., 2002) feste Systemgrenzen überschritten werden sowie die zunehmende Verbindung von „Wissenschaft und Bevölkerung“ und die Globalisierung Berücksichtigung finden.

Dies wird vor allem durch die Einführung der neuen Größe „Vulnerabilität“ deutlich. Eine traditionelle Risikoanalyse beschränkt sich auf unfallbedingte Ereignisse innerhalb der physikalischen Systemgrenzen, wobei die untersuchten Bedrohungen oft auf die technischen Gefährdungen beschränkt bleiben. Eine Vulnerabilitätsanalyse arbeitet mit offenen Systemzuständen und untersucht Ereignisse zeitabhängig, bis der alte Zustand oder eine stabile Situation erreicht ist.

Die zunehmende Bedeutung der Vulnerabilität für die kritischen Infrastrukturen wird in (Lenz, 2009) deutlich. Danach wir Vulnerabilität „als gefahrenspezifische Anfälligkeit einer kritischen Infrastruktur für Beeinträchtigung oder Ausfall ihrer Funktionsfähigkeit, welche zur Unterbrechung der Versorgung der Bevölkerung mit wichtigen Gütern und Diensten führen kann“ betrachtet.

8.3 Historische Entwicklung/Anwendungsbeispiele

8.3.1 Historische Entwicklung

Die Entwicklung und Anwendung risikobasierter Sicherheitsbetrachtungen im Bereich der Technik ist eng mit der technischen Entwicklung in Luft- und Raumfahrt, der Kerntechnik sowie komplexen Prozessanlagen gekoppelt. Der Aspekt der Sicherheit muss bei Anlagen mit hohem Gefahrenpotenzial bereits in der Planungsphase durch prospektive Risikoanalysen Berücksichtigung finden. Risikostudien, die wesentlich zur Entwicklung der Methode der Behandlung technischer Risiken beigetragen haben, sind in (Hauptmanns, 2013) aufgeführt (vgl. Tabelle 8.2):

Studie	Gegenstand
Amerikanische Studie für Kernkraftwerke (1975)	Druckwasser- und Siedewasserreaktoren amerikanischer Bauart
Deutsche Risikostudie Phase A und B	Kernkraftwerk Biblis (Druckwasserreaktor)
Canvey Island Studie (1978)	Chemieanlagenkomplex nahe London (England)
Rijnmond Studie (1982)	Chemieanlagen in der Rheinmündung (Niederlande)

Tabelle 8.2: **Auszug: Risikostudien**

In den zurückliegenden Jahrzehnten hat auch im Brandschutz ein Umdenken hin zu risikobasierten Methoden stattgefunden. Brandschutz wird vermehrt durch die Anwendung wissenschaftlicher und praxisbasierter Ingenieurmethoden sichergestellt. Dies wird durch das Grundlagendokument Brandschutz (EU Amtsblatt, 1994), das von der Europäischen Kommission 1994 veröffentlicht wurde, deutlich. Danach sind: „Ingenieurmethoden für die Brandsicherheit ein Ansatz zur Bewertung des erforderlichen Sicherheitsniveaus und zur Bemessung und Berechnung der notwendigen Schutzmaßnahmen."

Im Bevölkerungsschutz ist heute die Risikoanalyse ein wichtiges Instrument zur Festlegung von notwendigen Schutzmaßnahmen, z. B. bei Hochwasserschadenslagen. Die dazu notwendigen Grundlagen wurden vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe entwickelt und im Jahr 2010 veröffentlicht (BBK, 2010).

Seit der Katastrophe bei der Loveparade 2010 in Duisburg werden auch für den Sektor Veranstaltungssicherheit/Besuchersicherheit vermehrt Risikobetrachtungen (Sicherheitskonzept) von den Genehmigungsbehörden eingefordert und umgesetzt. Beispielhaft sei hier der Bericht des Ministeriums für Inneres und Kommunales NRW „Sicherheit von Großveranstaltungen im Freien“ von 2012 (MIK, 2012) aufgeführt.

Mit dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) von 1998 hat das Risikomanagement auch verstärkt Eingang in den Wirtschaftssektor gefunden. Erst- und Rückversicherer stehen hinsichtlich der Risikopolitik mit Einführungen der Regelungen nach dem Solvency II Act (2009) vor tiefgreifenden Veränderungen. Eine vergleichbare Entwicklung gibt es im Bankensektor mit der Einführung des Reformpaketes BASEL III.

8.3.2 Anwendungsbeispiele

Methoden des Risikomanagements werden hauptsächlich zur:

- Beurteilung der Anlagensicherheit (SEVESO III Richtlinie) und damit zusammenhängend für die Flächennutzungsplanung, den Umweltschutz und die Arbeitssicherheit,
- Beurteilung kritischer Infrastrukturen (KRITIS), für den Katastrophen- und Bevölkerungsschutz sowie zur
- Beurteilung der Risikolage von Unternehmen (KonTraG), Banken (BASEL III) und Versicherungen (Solvency II) eingesetzt.

Die klassischen Anwendungsgebiete ingenieurbasierter Verfahren sind die Risikoanalyse im Bereich der Betriebssicherheit von Maschinen und Apparaten, die Gefährdungsbeurteilung im Arbeitsschutz und die Sicherheitsanalyse zur Bewertung der Anlagensicherheit.

Betriebssicherheit von Maschinen

Die Maschinenrichtlinie verlangt für jede Maschine eine Risikobeurteilung und gegebenenfalls eine Risikominderung, bis das Restrisiko kleiner als das tolerierbare Risiko ist. Für die Verfahren der Bewertung dieser Risiken von Maschinen sind verschiedene Normen anzuwenden (z. B. DIN EN ISO 14121). Der Hersteller einer Maschine ist gemäß EU-Richtlinien für technische Produkte und Anlagen verpflichtet nachzuweisen, dass die Sicherheit seines Produktes dem „Stand der Technik" entspricht.

Auszug aus der Maschinenrichtlinie (Maschinenrichtlinie 2006/42/EG); Anhang 1: „Allgemeine Grundsätze":

„Der Hersteller einer Maschine oder sein Bevollmächtigter hat dafür zu sorgen, dass eine Risikobeurteilung vorgenommen wird, um die für die Maschine geltenden Sicherheits- und Gesundheitsschutzanforderungen zu ermitteln. Die Maschine muss dann unter Berücksichtigung der Ergebnisse der Risikobeurteilung konstruiert und gebaut werden."

Gemäß (Preiss, 2009) ist der Begriff des „Standes der Technik" insbesondere im Zusammenhang mit Sicherheit ein oftmals strapazierter; er wird in diversen Gesetzen gefordert und definiert, z. B. im Bundesimmissionsschutzgesetz. Dieser Begriff ist dynamisch angelegt und den sich verändernden gesellschaftlichen Anforderungen jeweils anzupassen.

Mit der CE-Kennzeichnung erklärt der Hersteller gemäß EU-Verordnung, dass das Produkt den geltenden Anforderungen genügt, die in den Harmonisierungsrechtsvorschriften der Europäischen Union festgelegt sind.

Für die Beurteilung der funktionalen Sicherheit von Maschinensteuerungen wird, ausgehend von der Risikoermittlung mit dem Risiko Graph nach DIN EN 61508, die zulässige Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde gemäß den Vorgaben des SIL-/PL-Konzeptes quantitativ vorgegeben (BGIA, 2008).

Gefährdungsbeurteilung im Arbeitsschutz

Das Arbeitsschutzgesetz und die Betriebssicherheitsverordnung enthalten als grundlegende Forderung die Gefährdungsbeurteilung. Damit können Gefahren erkannt und geeignete Gegenmaßnahmen festgelegt, und die Arbeitsplätze

sicherer gestaltet werden. Der Unternehmer/Arbeitgeber ist grundsätzlich dafür verantwortlich, alle erforderlichen Maßnahmen des Arbeitsschutzes zu treffen. Seit Oktober 2002 ist die Betriebssicherheitsverordnung (Verordnung über Sicherheit und Gesundheitsschutz bei der Bereitstellung von Arbeitsmitteln und deren Benutzung bei der Arbeit, über Sicherheit beim Betrieb überwachungsbedürftiger Anlagen und über die Organisation des betrieblichen Arbeitsschutzes; Betriebssicherheitsverordnung-BetrSichV) in Kraft. Diese Vorschrift regelt die Bereitstellung und Nutzung von Arbeitsmitteln, den Betrieb von überwachungsbedürftigen Anlagen und den betrieblichen Explosionsschutz. Zentrales Element für die Bewertung der Arbeitssicherheit ist die Gefährdungsbeurteilung. Die Gefährdungsbeurteilung erfolgt im Allgemeinen qualitativ durch eine subjektive Bewertung der ermittelten Risiken unter Einbeziehung der betrieblichen Erkenntnisse, mit Blick auf die Festlegung der Rangfolge erforderlicher Maßnahmen (Büchner, 2007).

Sicherheitsanalysen in der Anlagensicherheit

Risikoabschätzungen bei Anlagen werden derzeit sowohl in Bezug auf die immissionsschutzrechtliche Anlagenzulassung der unter die StörfallVerordnung fallenden industriellen Anlagen im Sinne einer Einzelfallbetrachtung als auch grundsätzlich im Zusammenhang mit der Raumordnung und Bauleitplanung sowie des Katastrophenschutzes diskutiert.

Der Sicherheitsbericht ist das zentrale Element der Störfallverordnung (Zwölfte Verordnung zur Durchführung des BundesImmissionsschutzgesetzes; 12. BImSchV) und ein wichtiges Dokument im Rahmen der Störfallvorsorge (Richter, 2007). Gemäß den Anforderungen der Störfallverordnung enthält der Sicherheitsbericht u. a. die Ermittlung und Analyse von zu berücksichtigenden Gefahren und Hinweise zur Verhinderung bzw. Begrenzung der möglichen Auswirkungen. Art der Ereignisse, die Eintrittshäufigkeit und die Randbedingungen für das Wirksamwerden der Gefahrenquellen sowie das Ausmaß und die möglichen Folgen sind abzuschätzen. In Deutschland finden vorrangig deterministische Verfahren Anwendung. Dabei handelt es sich um qualitative Verfahren, die durch Vorgabe bestimmter fester, deterministischer Randbedingungen für ein fiktives Szenario die Auswirkungen auf die Arbeitnehmer, die Nachbarschaft, die Umwelt sowie Sachwerte untersuchen (Katzer, 2001).

Als sicherheitstechnisch akzeptabel (Grenzrisiko) gilt eine Anlage dann, wenn:

- eine umfassende Risikoanalyse durchgeführt wurde,
- das zugängliche Fachwissen angewandt wurde,
- die Sicherheitsmaßnahmen dem Stand der Technik entsprechen.

Das verbleibende Restrisiko resultiert aus:

- bewusst in Kauf genommenen Risiken,
- erkannten, aber falsch beurteilten Risiken,
- nicht erkannten Gefahren.

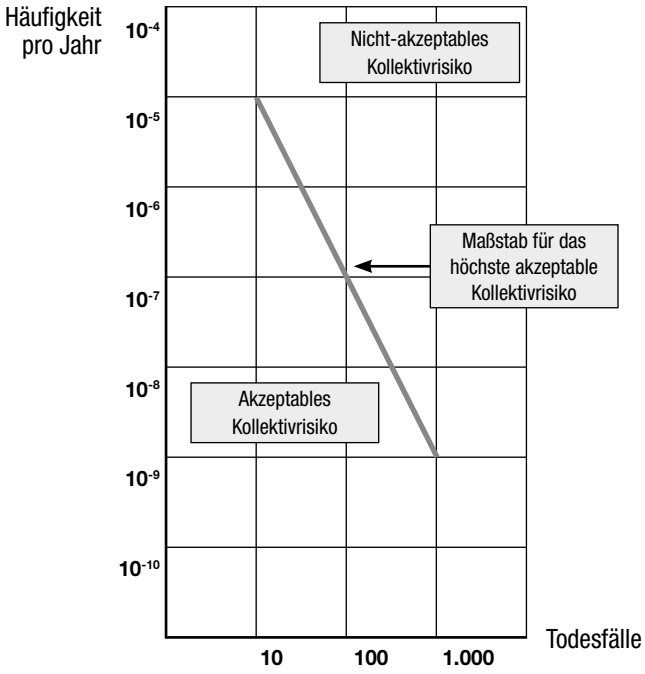

Bild 8.2: Grenzwerte für das Kollektivrisiko in den Niederlanden (SFK, 2004)

In einigen Nachbarländern, wie den Niederlanden, Belgien oder der Schweiz, werden quantitative Risikoabschätzungen vorgenommen und dienen als wichtiges Beurteilungskriterium für die Genehmigung von Anlagen und die Raumordnungsplanung. Dabei wird z. B. in den Niederlanden auf Basis des sogenannten „Purple Book" (CPR 18 E, 1999) die Anzahl der zu erwartenden Todesfälle (individual and societal risk) pro Jahr ermittelt (z. B. 1 Todesfall in 10.000 oder 100.000 Jahren). Das Individualrisiko wird dabei in sogenannten ISO-Risikolinien, das kollektive Risiko (Bild 8.2) in Form der FN-Grafik dargestellt.

In der Schweiz werden neben den Auswirkungen auf den Menschen auch die Auswirkungen auf Umwelt (Boden und Gewässer) sowie Sachgüter quantitativ berücksichtigt (SFK, 2004).

Risikoanalyse im Brandschutz

Basis des Brandschutzes in der Vergangenheit war die Schadenserfahrung. Insbesondere Großschadensereignisse führten im Nachherein zur Überprüfung und Weiterentwicklung von Bauvorschriften. Die Festlegung der notwendigen Schutzmaßnahmen erfolgte anhand eines normierten Brandverlaufs (Einheitstemperaturkurve, ETK) und daraus abgeleiteten standardisierten Bauteilen. Der Brandschutz der Zukunft baut – weiterhin ausgehend von der Schadenserfahrung – auf Methoden des Brandschutzingenieurwesens auf. Ausgehend von der Risikoanalyse wird auf Basis einzelner Brandszenarien (natural fire safety concept) ein zielorientiertes Brandschutzkonzept entwickelt.

Die Industriebaurichtlinie (Richtlinie über den baulichen Brandschutz im Industriebau – IndBauR; 2001) lässt die Anwendung eines probabilistischen Sicherheitskonzeptes zu. Dabei wird in begrenztem Maße zugelassen, dass die Lasteinwirkung Brand auf ein Bauteil größer ist als die zulässige Belastbarkeit; es kommt zum Versagen des Bauteils. Ausgehend von den vorhandenen baulichen, anlagentechnischen und abwehrenden Brandschutzmaßnahmen sowie deren Zuverlässigkeit und einer definierten Brandeintrittshäufigkeit pro Jahr darf durch den Lastfall Brand die Versagenswahrscheinlichkeit des Gebäudes einen festgelegten Grenzwert nicht überschreiten (Schneider, 2000). Für einen eingeschossigen Industriebau beträgt die zulässige Versagenswahrscheinlichkeit durch den Lastfall Brand beispielsweise 10^{-5} Einstürze pro Jahr (Bild 8.3).

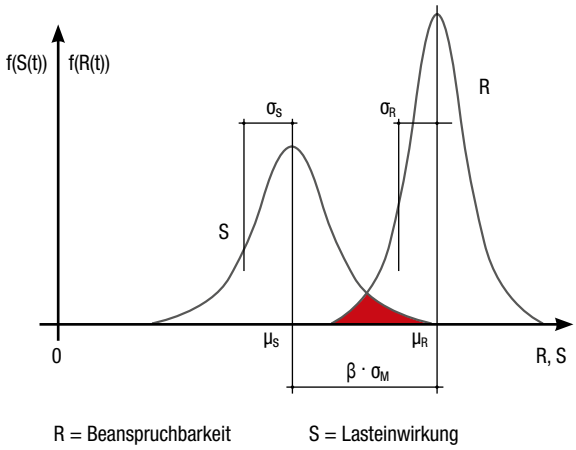

Bild 8.3: **Probabilistisches Sicherheitskonzept (IndBauRl) (Schneider, 2000)**

Mit den in Deutschland zum 1. Juli 2012 eingeführten Eurocodes (EN 1990 bis EN 1999) ist ein einheitliches Sicherheitsniveau in der Baubranche innerhalb Europas garantiert. Diese Normen gehen von einem risikobasierten Sicherheitskonzept aus. Eine Besonderheit bezüglich der Handhabung der Eurocodes ist die gleichzeitige Berücksichtigung (multiple Risiken) verschiedenartiger Belastungsfaktoren. Dabei wird zwischen ständig vorhandenen Lasten (Eigengewicht des Gebäudes) und zeitlich befristeten, sich verändernden Lasten (z. B. Windstaudruck, Schneelast) unterschieden. Die Kombinationsregeln und die Kombinationswerte wurden so festgelegt, dass die Wahrscheinlichkeit der Überschreitung der Bemessungswerte der Lastwirkungen für alle Lastkombinationen und für alle einzelnen Lasten annähernd gleich ist. „Bei einer veränderlichen Lasteinwirkung entspricht der charakteristische Wert entweder einem oberen Wert, der während der festgelegten Benutzungsdauer mit einer vorgegebenen Wahrscheinlichkeit nicht überschritten wird, oder einem festgelegten Nennwert, wenn eine Wahrscheinlichkeitsverteilung unbekannt ist. Für eine zeitabhängige veränderliche Einwirkung ist der Wert in der Regel so festgelegt, dass er mit einer Wahrscheinlichkeit von 98 % während der Benutzungsdauer von einem Jahr nicht überschritten wird bzw. nicht häufiger als einmal in 50 Jahren erreicht oder überschritten wird“ (Baumgart, 2014).

Risikoanalysen im Bevölkerungsschutz

Für ein schlagkräftiges Bevölkerungsschutzsystem ist nach (Unger, 2006) „der frühzeitige Aufbau eines geeigneten Risikomanagementsystems, national wie international, von besonderer Bedeutung. Dieses sollte neben der genauen Identifikation und Analyse der Risiken auch die Planung von Maßnahmen zu ihrer Ausschließung oder zumindest Minimierung umfassen."

Der Leitfaden „Methode für die Risikoanalyse im Bevölkerungsschutz" (BBK, 2010) beschreibt ausführlich die vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) entwickelte Methode zur Risikoanalyse im Bevölkerungsschutz. Nach (BBK, 2010) ist es damit möglich, „für das Gebiet der Bundesrepublik Deutschland auf systematische Weise das Schadensausmaß zu ermitteln, das bei Eintritt unterschiedlicher Gefahren zu erwarten ist, und dient dazu, Risiken durch unterschiedliche Gefahren in anschaulicher Weise vergleichbar zu machen. Auf Grundlage dieser Erkenntnisse können zielgerichtet wirksame Maßnahmen zum Schutz der Bevölkerung und ihrer Lebensgrundlagen ergriffen werden".

Die Bewertung des Risikos (Schutzzielfestlegung) erfolgt auf der Basis einer Risikomatrix. Derzeit fehlen jedoch noch klare gesetzliche Vorgaben bezüglich der Akzeptanzgrenzen für die jeweils zu betrachtenden Gefahrenlagen.

Sicherheitskonzepte für Großveranstaltungen

Für Großveranstaltungen (ab 5.000 Besucher) und Veranstaltungen mit besonderem Gefahrenpotenzial fordert der Gesetzgeber seit wenigen Jahren die Erstellung eines Sicherheitskonzeptes. Die Grundlage aller sicherheitsrechtlichen Einschätzungen – sowohl aufseiten der Behörden als auch der Veranstalter – ist nach (München, 2011) neben der Beurteilung aufgrund rechtlicher Vorgaben eine umfassende Risikobeurteilung. Die maßgebenden Faktoren sind dabei die zu berücksichtigenden Gefahren und deren Eintrittshäufigkeiten. Bei dieser Betrachtung muss gemäß (AGVS, 2012) unterschieden werden zwischen:

- vernünftigerweise nicht auszuschließenden und
- vernünftigerweise auszuschließenden Gefahrenquellen.

Vernünftigerweise nicht auszuschließende Gefahrenquellen können zu Ereignissen führen, die zu verhindern sind. Vernünftigerweise auszuschließende Gefahrenquellen können zu Ereignissen führen, deren Eintreten zwar nicht zu

verhindern ist, gegen deren Auswirkungen jedoch – unabhängig von den Maßnahmen zur Verhinderung – Vorkehrungen zu treffen sind. Das Versagen einer Schutzmaßnahme (nicht durch den Veranstalter zu verantworten) zur Verhinderung eines unerwünschten Ereignisses stellt beispielsweise eine solche Gefahrenquelle dar.

Risikoanalysen werden i. d. R. bereits in der Konzeptphase einer Veranstaltung durchgeführt. Dabei können zunächst detailliert nur solche Gefahren Berücksichtigung finden, die nach Art und Auswirkung eindeutig beschreibbar sind. Werden im Rahmen der konkreten Planungsphase und weiteren Umsetzung weitere Gefahren und Risiken erkennbar, müssen diese nachträglich untersucht und bewertet werden. Es sind jedoch auch Gefahren vorstellbar, die erst mit (durch) dem (den) konkreten Ablauf einer Veranstaltung entstehen und im Vorfeld nicht erkennbar sind bzw. bei deren Eintritt konkrete Gegenmaßnahmen (i. d. R. reaktiv) situationsbezogen und spontan getroffen werden müssen. Diese sind insbesondere:

- Ereignisse und Gefahren, die der künstlerischen Freiheit der Akteure geschuldet sind, z. B. spontane oder kurzfristig veränderte Räumlichkeiten oder besondere Aktionen,
- nach Art und Ausmaß unvorhersehbares Verhalten einzelner Besucher/Besuchergruppen, z. B. bewusster Verstoß gegen sicherheitsrelevante Anweisungen der Veranstalter/Sicherheitskräfte,
- sicherheitsrelevante Abweichungen (erst zu Beginn oder während der Veranstaltung erkennbar) von den ursprünglichen Planungsdaten, z. B. veränderte Verkehrslage im Umfeld oder spontane Parallelveranstaltungen, Bindung des eingeplanten Sanitätsdienstes an anderen Einsatzorten.

Durch Schutzmaßnahmen werden die vorhandenen Risiken gemäß dem Schutzziel „Jeder Besucher muss sich jederzeit frei, ohne Gefahren, äußere Einflüsse und mittels eigener Entscheidung innerhalb des Besucherbereichs bewegen können“ auf ein insgesamt von allen Seiten akzeptiertes Maß gesenkt.

8.4 Risikobewertung

Nachdem die Risiken identifiziert und nach Art und Ausmaß analysiert wurden, schließt sich die Risikobewertung an. Dazu werden den einzelnen Risiken qualitative/quantitative Schutzziele zugeordnet. Ist das ermittelte Risiko größer als das Schutzziel oder nicht zumutbar, wird diesem durch entsprechende Maßnahmen begegnet. Hierdurch werden inakzeptable Risiken auf ein akzeptables Maß gesenkt. Die Risikobewertung (BBK, 2011) ist ein Verfahren, mit dem:

- festgestellt wird, in welchem Ausmaß das zuvor definierte Schutzziel im Falle eines bestimmten Ereignisses erreicht wird,
- entschieden wird, welches verbleibende Risiko akzeptabel ist, und
- entschieden wird, ob Maßnahmen zur Minimierung ergriffen werden müssen.

„Wie sicher ist sicher genug?" – die Frage nach dem akzeptablen Risiko stellt sich immer dann, wenn man zur Einsicht gelangt, dass keine absolute Sicherheit existiert. Dabei werden die einzelnen Risiken den Bereichen inakzeptabel und akzeptabel zugeordnet. Wenn sich keine trennscharfe Abgrenzung zwischen diesen Bereichen bestimmen lässt, kann ein Übergangsbereich definiert werden. Bei der Beurteilung der Akzeptanz eines Risikos werden neben objektiven Kriterien auch subjektive Faktoren der Risikowahrnehmung, wie Selbstbestimmungsgrad und persönlicher Nutzen, berücksichtigt. Die Bestimmung des akzeptablen Risikos ist ein gesellschaftlicher Prozess, an dem alle betroffenen relevanten Gruppen beteiligt werden müssen. Grundlage dieser Betrachtung ist die Schutzzieldefinition. Ein Schutzziel (Akzeptanzgrenze) ist eine normative Festlegung, welche basierend auf qualitativen oder quantitativen Werten allgemein den kritischen vom nicht kritischen Bereich im Rahmen der Risikoermittlung trennt (Brenig & Ludäscher, 2012) (siehe Bild 8.4).

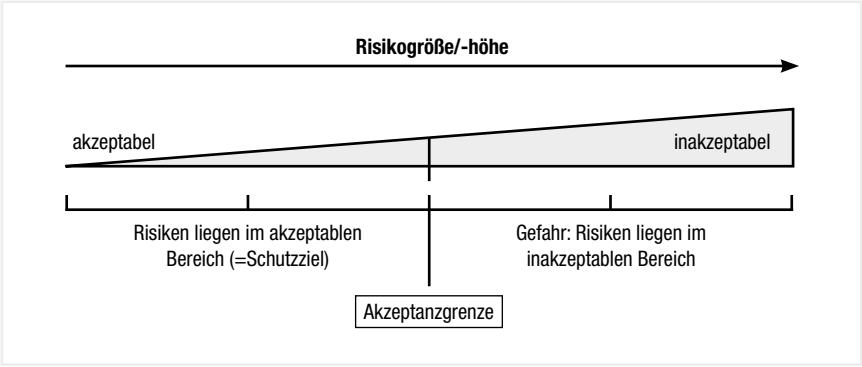

Bild 8.4: Klassifizierung von Risiken

Liegen die bewerteten Risiken über der Akzeptanzgrenze und somit im inakzeptablen Bereich, müssen so lange Maßnahmen zur Risikosenkung ergriffen werden, bis die Vorgaben erfüllt sind. Ziel ist es, alle Risiken dem akzeptablen Bereich zurechnen zu können. Nach (Fritzsche, A., 1986) kann ein Risiko grundsätzlich als akzeptabel angesehen werden, wenn das zugrunde liegende Ereignis bei der Mehrheit der Betroffenen keine Besorgnis hervorruft.

Bei der Bewertung von Risiken kann zwischen qualitativen, semiquantitativen und quantitativen Verfahren unterschieden werden.

Im Störfallrecht wird das zulässige Grenzrisiko – das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes – in Deutschland im Allgemeinen nicht qualitativ festgelegt. Die Anlage muss dem Stand der Technik entsprechen.

Grundansatz für die quantitative Festlegung von Schutzzielen ist die Feststellung, dass das natürliche Sterbefallrisiko durch technische Risiken nicht signifikant erhöht werden darf. In der einschlägigen Literatur (Merz, 1995) finden sich überwiegend Werte in der Größenordnung von 10^{-4} bis 10^{-6} für das individuelle Todesfallrisiko pro Person und Jahr.

Im Gegensatz zu den politischen Vorgaben in Deutschland verfolgen zahlreiche Länder bei der Bewertung von technischen Risiken überwiegend quantitative Ansätze. Beispielhaft sind hier die entsprechenden Werte des MAJOR INDUSTRIAL ACCIDENTS COUNCIL OF CANADA (MIACC) für das Todesfallrisiko durch technische Risiken in Kanada angegeben (siehe Bild 8.5).

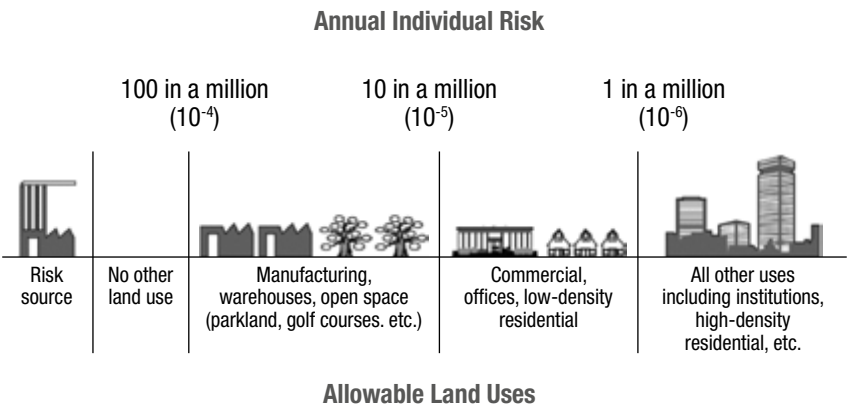

Bild 8.5: **Bewertung technischer Risiken in Kanada (MIACC, 1994)**

Im Rahmen der Störfallvorsorge in der Schweiz hat der Kanton Zürich bei einer Eintrittshäufigkeit von 10^{-5} Ereignissen pro Jahr für Personen,

Umwelt- und Sachwerte die folgenden akzeptierten Risikogrenzwerte festgelegt (SFK, 2004).

Akzeptables Risiko bei einer Eintrittswahrscheinlichkeit von 10^{-5} $1/a$:

- < 10 Tote
- < 1 % verunreinigte Gewässeroberfläche Zürichsee
- < 10 % verunreinigte Gewässeroberfläche Greifensee
- < 0,5 km^2 verunreinigte Gewässeroberfläche Flüsse
- < 0,1 km^2 verunreinigter Boden < 50Mio. *SFr.* Sachschaden

8.5 Definition von Schutzzielen und Schwellenwerten

Schutzziele trennen das akzeptable vom nicht akzeptablen Risiko. Schwellenwerte bilden die Basis für die Schutzzieldefinitionen. Schwellenwerte beschreiben allgemein Übergänge bzw. Stufen bezüglich des Schadensausmaßes und hängen wesentlich von den Bewältigungskapazitäten zur Begrenzung und Wiederherstellung der Zustände eines Schutzgutes ab.

Gemäß (BBK, 2011) wird unter dem Schutzziel „der angestrebte Zustand eines Schutzgutes, der bei einem Ereignis erhalten bleiben soll", verstanden. Bezüglich der Definition von Schutzzielen unterscheidet (Hess, 2008) zwischen der Akzeptanz- und der Toleranzgrenze. Das akzeptierte Risiko wird definiert als Risiko, das ein Individuum (oder eine Gruppe) bereit ist, aufgrund eigener Entscheidung und als Resultat ihrer alltäglichen, intuitiven Risikobewertung ohne Widerspruch hinzunehmen (informelle Bewertung).

Das tolerierbare Risiko basiert auf Normen oder empirischen Überlegungen (formelle Bewertung). Die Tolerierbarkeit des Risikos wird definiert, indem entweder aufgrund normativer Kriterien ein Risiko als erlaubt oder zulässig bezeichnet wird oder indem ein Risiko festgelegt wird, für das die Aussicht besteht, dass es für Individuen und/oder Gruppen tolerierbar ist.

Die Auswertung der Literatur (KRITIS-Kapa, 2012) hinsichtlich der nationalen Schutzziele hat ergeben, dass diese sehr heterogen sind und ein eindeutiger Trend nicht erkennbar ist. Die überwiegende Anzahl der Schutzziele basiert auf Schwellenwerten, die in Forschungsarbeiten und empirischen Studien, z. B. ORBIT-Studie (Dr. Porsche AG, 1978) zur Ermittlung der Hilfsfrist im abwehrenden Brandschutz, begründet sind.

Eine Zusammenstellung der unterschiedlichen Vorgehensweisen in Europa im Hinblick auf die Risikobewertung von industriellen Anlagen enthält das im 5. Forschungsrahmenprogramm der EU durchgeführte Vorhaben ARAMIS (Accidental Risk Assessment Methodology for Industries in the Context of the Seveso Directive, (ARAMIS, 2004)).

In der Literatur sind verschiedene Vorgehensweisen und Methoden zur Entwicklung von Schutzzielen beschrieben. Laut (Green, 1983) gibt es zwei Hauptansätze zur Bestimmung von akzeptablen Risiken:

„Der von Starr verbreitete Ansatz der Revealed Preferences benützt die Analyse vergangenen Verhaltens gegenüber Risiko zur Begründung zukünftiger Entscheidungen. Der andere Ansatz verwendet psychometrische Methoden, um festzustellen, welche Risiken von der Bevölkerung bewusst als akzeptabel gesehen werden."

Einen umfassenden Überblick über die verschiedenen Ansätze für sowohl qualitative als auch quantitative Schutzzielfestlegungen enthält die Dissertation von (Hess, 2008). Wesentliche Einflussfaktoren zur Festlegung der Schutzziele können dem Bild 8.6 entnommen werden.

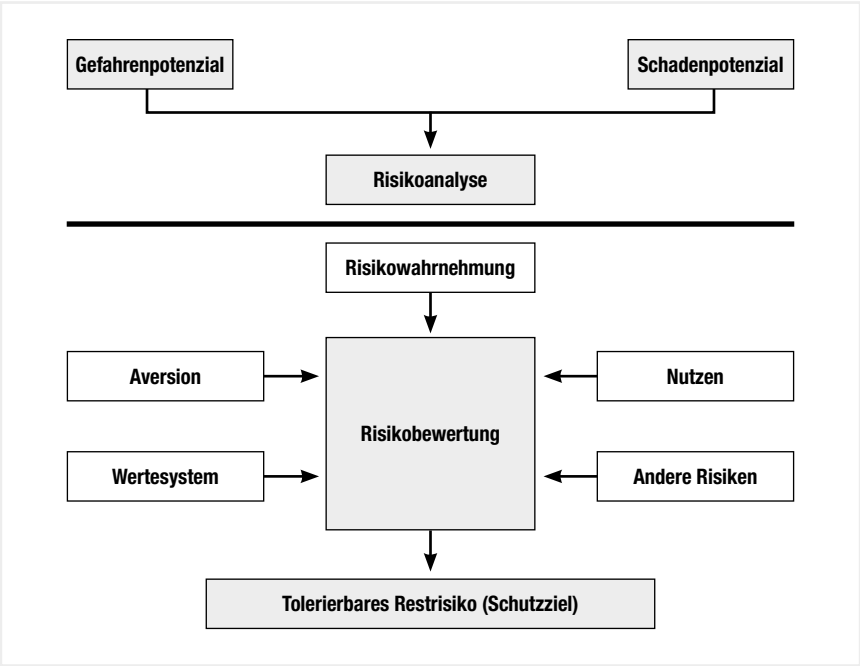

Bild 8.6: Schutzziele und ihre Einflussfaktoren (Hess, 2008)

Besondere Ansätze für Schutzzieldefinitionen sind das MEM-Konzept (Minimale Endogene Mortalität) sowie das ALARA-(As Low As Reasonable Achievable-) bzw. ALARP-(As Low As Reasonable Practicable-)Prinzip.

Grundlage des MEM-Konzeptes ist die minimale endogene Mortalität. Vor dem Hintergrund der natürlichen Sterberate von Jugendlichen in Europa stellen (Kulhmann & Bresser, 1981) die These auf, dass dieser Wert durch technische Risiken nicht überschritten werden darf und dass die zulässige Häufigkeit für das Individualrisiko um eine Zehnerpotenz kleiner sein muss.

Der ALARA-Ansatz, der ursprünglich aus dem Bereich des Strahlenschutzes kommt, orientiert sich an gesetzlich definierten Randbedingungen sowie Festlegungen und verlangt, dass die Belastung der Bevölkerung durch technische Risiken möglichst gering ausfällt. Das ALARP-Prinzip geht vom gleichen Grundsatz aus und versucht, das Risiko zusätzlich unter Berücksichtigung von wirtschaftlichen und sozialen Aspekten (Kosten-Nutzen-Analyse für die Gesellschaft) zu minimieren. Das ALARP-Prinzip legt drei Bereiche fest (Liggesmeier, 2012), in denen das Gesamtrisiko eingeordnet werden kann:

- Das Risiko ist unerheblich und kann ohne weitere Maßnahmen akzeptiert werden.
- Das Risiko ist größer als allgemein akzeptiert, unterschreitet aber die Grenze der oberen Tolerabilität.
- Das Risiko ist unakzeptabel groß.

Im ersten Fall muss das Risiko nicht weiterbetrachtet werden. Im Übergangsbereich ist eine Überprüfung erforderlich, ob sich das Risiko nicht verringern lässt; dies erfolgt nach dem Prinzip reasonably practicable. Ist das Risiko im ersten Ansatz nicht akzeptabel, müssen in jedem Fall Risikominderungsmaßnahmen ergriffen werden.

8.6 Fazit und Ausblick

Zur Bewertung industrieller Anlagen und Prozesse werden in Deutschland und Europa zunehmend risikobasierte Verfahren eingesetzt. Während dabei in Deutschland vornehmlich qualitative Methoden zum Einsatz kommen, setzen sich im europäischen Ausland die quantitativen Verfahren durch.

Zuverlässige und aussagefähige Methoden und Vorgehensweisen liegen für die klassischen technischen Anwendungsbereiche ausreichend vor. Defizite bestehen bezüglich der Verfügbarkeit von stochastischen Eingangsdaten.

Die Anwendung probabilistischer Verfahren bedarf in Deutschland noch einer intensiven Diskussion mit allen Betroffenen. Im Mittelpunkt steht dabei der notwendige politische und gesellschaftliche Konsens im Hinblick auf die Festlegung von (quantitativen) Schutzzielen. Ein möglicher Weg zur Festlegung von Schutzzielen ist die Ermittlung der vorhandenen Bewältigungskapazitäten für eine Schadenslage (z. B. Anzahl und Verfügbarkeit von Notstromaggregaten bei Stromausfall), sowohl aufseiten der Verursacher als auch den Einrichtungen und Organisationen der Gefahrenabwehr und den Betroffenen. Die vorhandenen Kapazitäten dienen als Grundlage, um Schwellenwerte für kritische Ereignisse und daraus abgeleitet für Schutzziele zu ermitteln. Der klassische Ansatz der Risikoanalyse mit Risiko als Produkt aus Eintrittshäufigkeit und Schadensausmaß stößt dann an seine Grenzen, wenn es sich um sehr seltene Ereignisse mit hohem Schadenspotenzial (SK, 2011), (ETH, 2012) handelt. Dies haben Großschadensereignisse in der jüngsten Vergangenheit, wie das Ereignis in Fukushima, deutlich gemacht. Die nur vereinzelt vorliegenden Schadenserfahrungen aus der Vergangenheit lassen nach Auffassung des Verfassers verlässliche und belastbare statistische Aussagen nicht zu und führen hinsichtlich der Akzeptanz solcher Risiken zu erheblichem Diskussionsbedarf mit der betroffenen Bevölkerung. Für sehr seltene Ereignisse mit hohem Schadenspotenzial sind Vorgehen erforderlich, bei denen in erster Linie mögliche Auswirkungen analysiert und die Resilienz des Systems bewertet und gegebenenfalls unabhängig von spezifischen Szenarien gestärkt wird. Die Auswahl und Festlegung

von notwendigen und geeigneten Schutzmaßnahmen kann in der Regel nur reaktiv und unspezifisch in enger Zusammenarbeit mit den staatlichen Stellen sowie den Betroffenen erfolgen.

Die Anwendung der klassischen Risikoverfahren für die Beurteilung technischer Risiken, bei denen gemäß den Forderungen von Blaise Pascal das Risiko proportional der Eintrittshäufigkeit und dem Schadensausmaß ist, setzt ausreichende Informationen über Art und Ablauf der Ereignisse, über die zu berücksichtigenden Gefahren sowie eine ausreichende Vorlaufzeit für die prospektive Risikoanalyse und die Festlegung der zu treffenden Schutzmaßnahmen (präventiv und reaktiv) voraus. Bezogen auf die Erweiterung des Anwendungsbereiches der risikobasierten Methoden sind diese Randbedingungen jedoch nicht immer gegeben. Dies betrifft vor allem die Fälle, in denen:

- die Gefahren und damit verbundenen möglichen Auswirkungen im Vorfeld nicht eindeutig festlegbar sind, z. B. Auswirkungen des Klimawandels,
- Gefahren und Risiken sich zeitabhängig verändern oder sogar erst zeitversetzt eintreten können, z. B. im Rahmen von Großveranstaltungen,
- sicherheitsrelevante Abweichungen von den ursprünglichen Planungsdaten jederzeit denkbar, aber nicht eindeutig bestimmbar sind,
- Menschen eine Doppelfunktion als zu schützendes Objekt sowie gleichzeitig als potenzielle Gefahrenquelle besitzen und das Verhalten der Menschen über einen längeren Zeitraum nur bedingt steuerbar und vorhersehbar ist, z. B. im Bevölkerungsschutz.
- Ereignisse oder Gefahren bei Veranstaltungen, die der künstlerischen Freiheit der Akteure geschuldet sind, z. B. spontane oder kurzfristig veränderte Räumlichkeiten.

Die Behandlung solcher Gefahren erfordert eine Weiterentwicklung der etablierten Methoden und Vorgehensweisen. Im Mittelpunkt stehen dabei der Umgang mit offenen Systemgrenzen und zeitlich sich verändernden Randbedingungen (dynamische Prozesse) sowie die Weiterentwicklung des Vulnerabilitätsansatzes.

Für diese neuen Ansätze und Methoden sollte nach Ansicht des Verfassers nicht mehr der klassischen Risikobegriff nach Blaise Pascal, sondern der allgemeinere Begriff „systematische Sicherheitsbetrachtung“ verwendet werden.

Literatur

AGVS. (2012). Sicherheitskonzept für Veranstaltungen (Entwurf). XEmp.

ARAMIS. (2004). Accidental Risk Assessment Methodology for Industries in the Context of the Seveso II Directive. EU Vorhaben, EVG1-CT-2001-00036 (5th Framwork Programme).

Baumgart. (2014). Sicherheitskonzpt (DIN EN 1990 bis 1998). TH Darmstadt.

BBK. (2010). Methode für die Risikoanalyse im Bevölkerungsschutz (Band 8). Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

BBK. (2011). Ausgewählte zentrale Begriffe des Bevölkerungsschutzes (BBK Glossar). Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

BGIA. (2008). Funktionale Sicherheit von Maschinensteuerungen. BGIA Report 2/2008.

Brenig, H., & Ludäscher, S. (2012). Sicherheitskultur in den Ingenieurwissenschaften. WittenHerdecke.

Büchner, N. R. (2007). Gefährdungsbeurteilung – Praxishilfe –. Düsseldorf: Bezierksregierung Düsseldorf; Maschinenbauberufsgeonssenschaft MMBG.

BVerfG. (1978). BVerfG Beschluss vom 08.08.1978; BVerfG 49,89.

CPR 18 E. (1999). Guidelines for quantitative Risk Assessment. Den Haag: Committee for the prevention of Disasters.

DECHEMA. (2006). Quantitative Risikoanalyse – Quo vadis?, Vol. 7 Praxis der Sicherheitstechnik. Tutzing Symposium: DECHEMA e.V.

Dr. Porsche AG. (1978). Definitionsstudie, KT 7612. Grundlagenuntersuchung für die Entwicklung verbesserter Feuerwehrfahrzeuge zur Optimierung der Leistungsfähigkeit beim Einsatz. Weissach: Entwicklungszentrum Weissach.

ESCIS. (1996). Einführung in die Risikoanalyse – Systematik und Methoden. Basel: Expertenkommission für Sicherheit in der chemischen Industrie der Schweiz.

ETH. (2012). Factsheet Fukusima und die Grenzen der Risikoanalyse, 3RG Report. Zürich: Center for Security Studies (CCS), ETH Zürich.

EU Amtsblatt. (1994). Grundlagendokument Brandschutz, Nr. 2 Wesentliche Anforderungen, Nr. C62/63.

Fritzsche, A. (1986). Wie sicher leben wir? Risikobeurteilung und -bewältigung. TÜV Rheinland.

Green, C. (1983). Die „Revealed Preferences"-Theorie: Annahmen und Mutmaßungen. In B. R. u. Sicherheitsforschung, Gesellschaft, Technik und Risikopolitik (S. 53-59). Bonn: Springer Verlag.

Hauptmanns, U. (2013). Prozess- und Anlagensicherheit. Springer Verlag.

Hess, J. (2008). Schutzziele im Umgang mit Naturrisiken. Zürich: ETH Zürich (Dissertation Nr. 17956).

Kafka, W. (1992). Gefahr, Gefährdung, Risiko. Garching: Gesellschaft für Reaktorsicherheit.

Katzer, H. (2001). Die quantitative Risikoanalyse zur Bewertung störfall-bedingter Gefahren. Essen: Landesumwelt NRW; Jahresbericht 2001.

KRITIS-Kapa. (2012). Risiko Stromausfall: Grundlagenermittlung zur Festlegung von Schutzzielen auf Basis von Kapazitäten. Bonn: Beschaffungsamt des Bundesministeriums des Innern ; B 1.25 – 0055/10/VV : 1.

Kulhmann, A., & Bresser, H. (1981). Einführung in die Sicherheitswissenschaft. Wiesbaden: Vieweg.

Lenz, S. (2009). Vulnerabilität kritischer Infrastrukturen; Heft 4. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Liggesmeier, P. (2012). Safety and Reliability of Embedded Systems. Abgerufen am 08 2012 von Tu Kaiserslautern, AG Software Engineering, Prof. Dr. Liggesmeier: gde.informatik.unikl.de.

Merz, A. (1995). Bewertung von technischen Risiken. Zürich: ETH Zürich, Hochschulverlag.

MIACC. (1994). Hazard Substances Risk Assessment. Ottawa: Major Industrial Accidents Council of Canada.

MIK. (2012). Sicherheit von Großveranstaltungen im Freien. Düsseldorf: Ministerium für Inneres und Kommunales, NRW.

Mock, R. (2002). Risikoanalyse – ein Werkzeug für neue Herausforderungen? ETH Zürich.

München, L. (2011). Sicherheitsrechtliche Beurteilung bei Großveranstaltungen. München.

Peters, Meyna. (1986). Handbuch der Sicherheitstechnik (Band 2). München: Carl Hanser Verlag.

Preiss, R. (2009). Methoden der Risikoanalyse in der Technik. Wien: TÜV Austria.

Richter, B. (2007). Anlagensicherheit. Essen: Hüthig GmbH.

Schneider, U. (2000). Grundlagen der Ingenieurmethoden im Brandschutz. Wien: Werner Verlag.

SFK. (2004). Risikomanagement im Rahmen der StörfallVerordnung (SFKGS41). Störfallkommission.

SK. (2011). 4. Gefahrenbericht der Schutzkommission. Bonn: Bundesmt für Bevölkerungsschutz und Katastophenhilfe.

Unger, C. (2006). 2. Europäischer Katastrophenschutzkongress Bonn.

9

Eine allgemeine Aussage

Prof. Dr. Wolfgang Stoll, Institut für Umweltfragen, Deutschland, GfS

Der große deutsche Philosoph Arthur Schopenhauer meinte, dass, was der Mensch Schicksal nenne, nichts anderes sei als die Aneinanderreihung seiner eigenen dummen Streiche.

In unserer alternden Gesellschaft wollen wir ganz generell hoch abgesichert sein. Es ist das Privileg der Jugend, sich darzustellen – nicht zuletzt durch Mut, der bis zum Draufgängertum geht, indem sie sich (nur zu häufig drogenbefeuert) in gefährliche Grenzsituationen begibt. Es ist gerade dieser Gegensatz, aus einem geradezu langweilig abgesicherten Feld den ultimativen „Kick" zu erleben, der so nahe als möglich an die Grenze des gerade noch beherrschbaren Verhaltens heranführt.

Früher galt der Satz: „Wer sich in Gefahr begibt, kommt darin um." Heute ist es leider Mode geworden, auf dem schmalen Grat zwischen „sicher" und „gefährdet" zu tanzen. Damit werden ursprünglich ganz einfache Verhaltensregeln zu statistisch hinterlegten Wahrscheinlichkeiten von Gelingen oder Versagen. Unsere moderne Welt aus Waren und Dienstleistungen wird von den Konkurrenten aktiv beworben mit den positiv sinnstiftenden Argumenten: schöner, größer, funktioneller und preiswerter.

Nur zwei handlungseinschränkende Werbeargumente sind in den letzten hundert Jahren hinzugetreten: umweltfeundlich und sicher.

Dass wir in dem Aktionsfeld, in dem wir herum trampeln, möglichst wenig Schaden stiften sollten, ist eine Erkenntnis, die mit der Besiedlungsdichte und dem Naturverbrauch immer drängender wurde. Es verwundert nicht, dass das Argument, irgendetwas sei umweltfreundlich oder würde wenigstens keinen Schaden stiften, zum wichtigen Werbeargument wurde. Ob es jeweils auch zutrifft, dafür gibt es tief gestaffelte Untersuchungsorganisationen, die sich trotz der ganz verschiedenartigen Fragestellungen einheitlich als Umweltwissenschaft darstellen und die dann auch als solche akzeptiert, gelegentlich auch gefürchtet, jedenfalls aber in den Beurteilungsprozess eingebunden werden.

Das ist beim Attribut „Sicher“ noch nicht so weit, obwohl die militanten Umweltorganisationen massiv in dieses Gebiet ausufern. Das Bedürfnis, hier auch mit wissenschaftlichen Kriterien gleichzuziehen, ist aber ganz deutlich.

Es ist die Summe der uns im modernen Leben begegnenden Risiken, die in ihrer Vielgestaltigkeit den einfachen Hausverstand weit überfordern und eines wissenschaftlich hinterlegten Abwägungsprozesses bedürfen.

Daraus schöpft die Sicherheitswissenschaft als eine relativ neue und keineswegs überall anerkannte Disziplin ihre Berechtigung. Es ist schon alleine der Risikobegriff, der sachfremd abgetrennt von der Chance medienwirksam als „Aufreger“ benutzt wird. Das mag zwar die Aufmerksamkeit und damit die Auflagen in den Medien steigern, die einseitige Herausstellung des Risikos führt aber nicht zu vertieften Erkenntnissen und schon gar nicht zu besonnenen Handlungsanweisungen.

Um all die unbestimmten Ängste der Bürger werbend zu nutzen, werden im Gegensatz dazu positiv besetzte Attribute zur Werbung benutzt. Das können, wie oben erwähnt, Hinweise auf die Umweltfreundlichkeit oder die Preisvorteile sein. Am allgemeinsten ist aber das Attribut, ein Produkt sei „sicher“, was hier so viel wie eine maximale Chance verbunden mit einem Minimalrisiko bei der Anwendung heißen soll. Während die Umweltfreundlichkeit kein Wettlaufargument bildet, lässt sich keine Werbeabeilung freiwillig das für ein Produkt mühsam und im Wettstreit mit der Konkurrenz aufgebaute Sicherheitsattribut verallgemeinernd wegnehmen. Damit steht es einer vergleichenden wissen-

schaftlichen Bearbeitung nicht zur Verfügung. Dabei wird in der Ausgestaltung dieses Attributes gerne absichtlich übersehen, dass es trotz aller spezifischen Produkteigenschaften letztlich der handelnde oder unterlassende Mensch ist, der dieses Attribut erst wirksam werden lässt. Es würde der Werbewirtschaft und auch den im Wettbewerb stehenden Unternehmen jedoch sehr nützen, gerade den Menschen in seinem risikobewussten oder auch leichtsinnigen Handeln im Umgang mit den Produkten und den dafür empfohlenen Verhaltensweisen wissenschaftlich zu begleiten. Dies würde marktschreierische Übertreibungen dämpfen und erst den objektiven Hintergrund für die Produktentwicklung und Bewertung liefern.

Was also mit dem allgemein gesteigerten Umweltbewusstsein – einschließlich der selbstgewissen Übertreibungen durch militante Umweltorganisationen – bereits gelungen ist, müsste bei entsprechenden Anstrengungen auch mit dem kollektiven Risikobewusstsein gelingen, wenn eine objektive wissenschaftliche Durchdringung nicht nur von Amts wegen, sondern auch als objektives Werbeargument von der erzeugenden Industrie aktiv gefördert und als Bestandteil der Entwicklungsanstrengungen mit einbezogen würde.

Diese Tagung kann nur als ein kleiner Beitrag zur Bewusstseinsbildung auf diesem langen und beschwerlichen Weg betrachtet werden.

Als ein Beispiel von vielen soll hier wegen des im deutschen Risikoverständnis immer noch wichtigen Themas über die augenblickliche Risikokompetenz bei der Beurteilung ionisierender Strahlung berichtet werden.

Nehmen wir einen praktischen Fall:

Eine größere Versorgungs-Rohrleitung wird im Freien verlegt. Die Stoßstellen werden geschweißt. Ein Trupp aus Vorarbeiter, Schweißer und zwei Hilfskräften, einer davon erstmalig und etwas älter, sind an der Arbeit. Die Schweißnaht wird mit einer Strahlenquelle (Kobalt-60) auf Fehler durchleuchtet. Der ältere Hilfsarbeiter sieht auf dem Lehmboden im Graben unter dem Rohr ein bleistiftgroßes glänzendes Metallstück liegen und steckt es in die Tasche. Der Vorarbeiter bemerkt nach kurzer Zeit das Fehlen der Kobalt-Quelle, die aus der Bleihülle heraus gefallen war – er fragt und bekommt sofort die Quelle aus der Hosentasche des Hilfsarbeiters zurück und verwahrt sie wieder im Bleibehälter. Der Vorfall wird nicht gemeldet, aber der Arbeiter erzählt ihn abends sei-

ner Frau. Ein Jahr später wird bei dem Hilfsarbeiter Leukämie diagnostiziert. Er stirbt wenig später. Die Frau verlangt von der Berufsunfallversicherung eine Witwenrente, wird aber abgewiesen. Begründung: Ein älterer Bruder des Arbeiters war ebenfalls einige Jahre zuvor an Leukämie gestorben. Außerdem hatte der Arbeiter schon vorher mehrere Male zur Linderung seines Rheumas radioaktive Thermalbäder aufgesucht. Der Rechtsbeistand der Frau argumentiert gegenüber der Berufsgenossenschaft, dass ein Fall von Leukämie in dem familiären Umfeld nicht zähle, weil es keine genetische Vorbelastung für Leukämie gebe und dass außerdem die Anwendung von ionisierender Strahlung zu medizinischen Zwecken keine anrechenbare Vorbelastung darstelle. Die Berufsgenossenschaft obsiegt jedoch mit der Feststellung, Strahlenschäden seien nicht kausal zuzuordnen und daher grundsätzlich nicht versicherbar.

Das Dilemma ist augenfällig: Schäden durch ionisierende Strahlung sind statistisch verteilt, die Rechtsprechung aber fordert beweisbare Kausalität. So haben im Westen nach dem Tschernobylunfall etwa 10.000 Frauen ihren Fötus abtreiben lassen, obwohl es dafür nicht die geringste statistische Evidenz gab. Es gehört zu den Akzeptanzproblemen der Kernenergie, dass es für strahlungsbasierte Schadensvermutung keine Versicherung gibt.

In den USA wurde in einem vergleichbaren Fall (Strahlenbelastung von Soldaten in Feldversuchen mit Atomsprengladungen) eine Kohorte von 7.000 Fällen von Klagen von Soldatenwitwen durch eine anteilige Ursachenzuordnung nach Wahrscheinlichkeit (Probabiltiy of Causation) entsprechend anteilig abgegolten. Das geht offenbar im relativ fallelastischen amerikanischen Gewohnheitsrecht, wäre aber bei unserem paragraphengestützten Rechtssystem undenkbar.

Es gehört zu den Grundfesten der (US-amerikanischen) Meinungsführer im Schutz vor ionisierender Strahlung, die in der ICRP den Ton angeben, dass man wegen der im Niedrigdosisbereich nicht nachweisbaren Folgen annimmt, jede Exposition sei schädlich, würde sich aber nach dem linearen Dosis-Wirkungs-Prinzip (LET) nur statistisch in Gesundheitsfolgen (da aber u. U. auch in Karzinomen) manifestieren.

Diese Annahme ist nicht nur singulär unter allen Toxizitätserkenntnissen, wo ganz generell die „Menge das Gift macht“, um Paracelsus zu zitieren, und daher weitaus zu konservativ, sondern wird nun auch von namhaften Forschern und vor allem von Balneologen als unsinnig gebrandmarkt. Sie ist aber in ihrer

Rigorosität gleichzeitig das Rückgrat der Kernenergieablehnung und – weil intellektuell einfach – auch nicht mehr aus der Welt zu schaffen. Es hat aber nicht an Versuchen gefehlt, die Wirkung von ionisierender Strahlung nicht nur statistisch nach dem obigen LET-Prinzip überkonservativ zu bewerten, sondern auch im Einzelfall zu konkreten Bewertungen von eventuellen Strahlenschäden zu kommen. Als einziges Verfahren mit einer bedingten Aussagekraft hat sich bisher die Zählung von Chromosomen-Aberrationen entwickelt. Dabei werden in einem aufwendigen Zählverfahren die Zahl und Form der gegenüber der Normalform veränderten Chromosomen in Blut- oder Gewebszellen bestimmt und daraus auf eventuelle Strahlenschäden geschlossen. Es gibt natürlich auch chemische Noxen, Krankheiten und altersbedingte Veränderungen am Chromosomensatz, aber im Regelfall kann man solche Störgrößen von Strahlenschäden unterscheiden. Man muss allerdings das auslösende Bestrahlungsereignis zeitlich zuordnen können, da Zellen mit beschädigtem Chromosomensatz von den Reparaturenzymen des Körpers ausgeschieden werden und somit viel kürzer leben als normale Zellen. Jedenfalls ist die Abwesenheit von Chromosomen-Aberrationen für das Fehlen von Strahlenschäden schlüssig. Solange das aber aus Kostengründen nicht routinemäßig angewandt wird, bleibt es bei dem anonymen und damit nicht als örtlich und zeitlich begrenzt zuordenbaren Herdgeschehen als Bedrohung, die kollektiv Angst macht.

Es sind solche Risiken, bei denen zwar eine fachliche Kompetenz zur Beurteilung bestünde, aber sie sind im Umfeld hysterischer Ängste nicht objektivierbar.

10

Digitale Medien: Risiken und Nebenwirkungen für die Gesellschaft

Zusammenfassung

Prof. Dr. Dr. Manfred Spitzer, Universitätsklinikum Ulm

Digitale Informationstechnik ist Teil des modernen Lebens: Schon Kinder kaufen im Internet, spielen an der Konsole, plaudern über Facebook mit Freunden und machen mit Google ihre Hausaufgaben. Deswegen könne man den richtigen Umgang mit den digitalen Medien nicht früh genug lernen. – Diese Ansicht entpuppt sich bei genauerem Hinsehen als schwerer Irrtum. Kinder sind keine Erwachsenen. Ihre besonders lernfähigen Gehirne brauchen bestimmte Erfahrungen, um Verbindungen zwischen Nervenzellen im Gehirn ausbilden zu können, d. h. ihr Gehirn überhaupt erst zu bilden, wie anhand von Beispielen aus der Entwicklungspsychologie, der experimentellen Psychologie und der Gehirnforschung dargestellt wird: Wer sprechen lernt, braucht den Umgang mit sprechenden Menschen. Sitzen kleine Kinder hingegen vor Bildschirmen und Lautsprechern, bleiben sie in ihrer Sprachentwicklung zurück (Kuhl et al. 2003, Zimmerman et al. 2007). Wer Kinder im Vorschulalter mathematisch besonders fördern will, der sollte Fingerspiele mit ihnen machen, denn Zahlen werden vom Gehirn über die Finger erworben, nicht durch Daddeln an einem iPad (Gracia-Bafalluy & Noël 2008, Noël 2005). Und wer handschriftlich Inhalte aufschreibt, verankert sie tiefer, als wer nur auf einer Tastatur tippt (Mueller & Oppenheimer 2014).

Zugleich ist aus der Bildungsforschung bekannt: Wer schon als Kleinkind viel Zeit vor Bildschirmmedien verbringt, zeigt in der Grundschule vermehrt Störungen bei der Sprachentwicklung sowie Aufmerksamkeitsstörungen (Spitzer 2012). Eine Playstation im Grundschulalter verursacht nachweislich schlechte Noten im Lesen und Schreiben (Weis & Cerankosky 2010) und ein Computer im Jugendzimmer wirkt sich negativ auf die Schulleistungen aus (Fuchs & Woesmann 2004). Hinzu kommt die Suchtgefahr, denn Computerspiele sind programmiert, um Sucht zu erzeugen. Weitere Folgen digitaler Medien, zu denen mittlerweile auch das Smartphone gehört, sind Ängste und Abstumpfung, Schlafstörungen und Depressionen, Übergewicht und Gewaltbereitschaft (Spitzer 2014).

Es ist besorgniserregend, dass Kinder heute täglich etwa doppelt so viel Zeit mit digitaler Informationstechnik verbringen wie in der Schule. Diese Risiken und Nebenwirkungen digitaler Informationstechnik werden von Eltern, Erziehern und Lehrern seit Jahren beobachtet, finden jedoch gesellschaftlich und politisch aufgrund massiver Lobbyarbeit der Medien und der Hersteller von Informationstechnik kaum Beachtung.

10.1 Digital genial? – Mediennutzung in der Kindheit

Wenn man Medienpädagogen glaubt, dann gibt es für Kleinkinder nichts Besseres als digitale Informationstechnik. „Dank der intuitiven Oberfläche können Kleinkinder – mit und ohne Beteiligung von Erwachsenen – die verschiedenen Programme, Spiele, Videosequenzen usw. selbsttätig und spielerisch erkunden", schreibt der Frühpädagoge Martin Textor in der Zeitschrift *Kita aktuell*, nicht ohne anzumerken: „Allerdings besaßen im Jahr 2012 erst 15 % der Familien einen Tablet-PC". Da gibt es also Nachholbedarf, denn „diese Geräte sind für kleine Kinder geradezu prädestiniert". Und der *Medienpädagogische Forschungsverbund Südwest* fügt in seiner entsprechenden Studie (2012, S. 20) hinzu: „Ohne Tastatur, nur mittels Touchscreen, stehen Internetangebote oder Apps quasi sofort per ‚Knopfdruck' zur Verfügung. Lese- oder Schreibkompetenzen sind zur Nutzung von Inhalten nicht mehr zwingend erforderlich, die oftmals visuell gesteuerte Menüführung erlaubt potentiell selbst Vorschulkindern die Nutzung."

Glaubt man der Schrift *Digital genial* der Krippenerzieherin Antje Bostelmann und des Kunstpädagogen Michael Fink, können Kleinkinder den Tablett-PC nutzen, um „ihre Umgebung genauer wahr[zu]nehmen", indem sie „beispielsweise […] mit der eingebauten Kamera ein Foto" machen oder Filme drehen. „Eine Dolmetscher App ermöglicht es, mit einem gerade eingewanderten Kind zu sprechen" und „Dank einer Pflanzenbestimmungs-App können bei einem Waldspaziergang Bäume, Sträucher, Blumen, Pilze usw. identifiziert und weitere Informationen über sie abgerufen werden". Das Fazit von Herrn Textor: „Es gibt also viele Möglichkeiten, wie sich Tablet-PCs im Kindergarten sinnvoll einsetzen lassen. Die Kosten sind gering, da die Geräte und Apps recht preiswert sind […]."

Im Nachbarland Österreich hat mittlerweile das Kultusministerium (zusammen mit der Europäischen Union) das Handbuch für die Aus- und Weiterbildung von Kindergartenpädagog(inn)en Safer Internet im Kindergarten gefördert. Dort findet man im ersten Kapitel (*Die frühe Kindheit als „Medienkindheit"*) das Folgende: „Keine Seltenheit mehr: Einjährige Babys, die gerade das Laufen

lernen, finden sich am iPad der Eltern erstaunlich gut zurecht – besser vielleicht als in der eigenen Wohnung. […] Es liegt daher auf der Hand, dass *mediale Frühförderung ein immer wichtigerer Bestandteil der Bildungsarbeit* werden muss“ (Buchegger 2013, S. 6).

Auch für die Schulen wird immer wieder Nachholbedarf festgestellt, werde doch Deutschland ansonsten den Anschluss an die digitale Welt verpassen (Anon. 2014). Daher werden Tablet-PCs und Laptop-Computer für den Unterricht ab der ersten Klasse empfohlen und in den Niederlanden unter der Bezeichnung „Steven Jobs Klassen“ bereits eingeführt. In Uruguay wird seit einigen Jahren jeder Erstklässler mit einem eigenen Computer ausgestattet.

Die auch hierzulande heftig vorangetriebene Digitalisierung von Klassenzimmern steht in krassem Gegensatz zu dem, was wir zu den Auswirkungen von digitaler Informationstechnik an Schulen wissen: Die großen deutschen Studien zur Computernutzung im Unterricht haben festgestellt, ebenso wie die entsprechenden internationalen Studien, dass Computer an Schulen weder das Lernen noch die Schulleistungen verbessern, nicht einmal die Fähigkeit zur Benutzung von Computern oder des Internets fördern und insgesamt zu mehr gestörter Aufmerksamkeit führen (Abb. 2–4). Das Problem der Sucht wird in diesen Studien erst gar nicht angesprochen. Auch die im November 2014 publizierte internationale Vergleichsstudie zur Nutzung digitaler Informationstechnik an Schulen (ICILS; vgl. Bos et al. 2014) enthält weder einen Bezug zu Schulnoten noch einen Hinweis zur suchterzeugenden Wirkung digitaler Medien.

Betrachtet man die Mediennutzung von Kindern und Jugendlichen in Deutschland nach ihrem Ausmaß – 7,5 Zeitstunden täglich (Rehbein et al. 2009) – so wird deutlich, dass es hier um ein Problem geht (bei 3,75 Zeitstunden täglich für den gesamten Schulstoff[1]), dem eine gesamtgesellschaftliche Bedeutung im Hinblick auf die Bildung und die Gesundheit der Bevölkerung zukommt. Digitale Informationstechnik hat Risiken und Nebenwirkungen, insbesondere bei Kindern und Jugendlichen; hiervon und den damit verbundenen gesamtgesellschaftlichen Folgen handelt dieser Beitrag.

1 Wer 35 Wochenstunden Schule hat, verbringt dort im Durchschnitt (35 x 3/4 x 5/7) : 7 = 3,75 Zeitstunden täglich, denn eine Schulstunde hat die Dauer einer Dreiviertelstunde und Schule findet nur an 5 von 7 Wochentagen statt.

10.2 Computer und Gehirne

Digitale Medien nehmen uns geistige Arbeit ab – so wie uns Rolltreppen, Fahrstühle und Autos körperliche Arbeit abnehmen. Die negativen Folgen mangelnder körperlicher Aktivität für Muskeln, Herz und Kreislauf sind bekannt, und wir tun viel, um ihnen entgegenzuwirken und uns körperlich fit zu halten. Wichtig ist nun die vergleichsweise junge Einsicht: Mit unserem Gehirn verhält es sich ebenso, denn nur wenn wir es trainieren, werden und bleiben wir geistig fit. Unser Gehirn entwickelt nur dann seine geistige Leistungsfähigkeit, wenn wir es in Kindheit und Jugend in jeglicher Hinsicht bestmöglich nutzen und damit überhaupt erst ausbilden.

Bei einem Computer liegen die Leistungsfähigkeit seiner wesentlichen Komponenten, der Verarbeitungseinheit (Central Processing Unit, CPU) und Speichereinheit (Festplatte) fest, sie ändern sich nach seiner Produktion nicht mehr und haben eine bestimmte Kapazität, die sich in Rechenschritten/Sekunde (CPU) bzw. Mega-, Giga- oder Terabyte (Festplatte) bemisst. Die Verarbeitungs- und Speicherkapazität des Gehirns dagegen bildet sich erst durch seine Benutzung, sie ist weder bei der Geburt schon vorhanden noch entsteht sie von selbst. Unsere Sprachzentren beispielsweise sind zwar biologisch angelegt, benötigen zu ihrer Ausbildung jedoch Hunderttausende sprachlicher Inputs, aus denen das Gehirn mittels Extraktion statistischer Regeln allgemeine Wörter (Vokabeln), deren Bedeutungen (Semantik) und die Regeln der Kombination von Wörtern zu komplexeren Bedeutungsstrukturen (Grammatik) ableitet. Ohne sprachlichen Input geschieht dies nicht und das Ganze muss bis etwa zum 13. Lebensjahr erfolgt sein. Danach ist die Plastizität der Sprachzentren nicht mehr gegeben, die für deren Bildung notwendig ist. Ganz allgemein gilt: Zur Ausbildung geistiger Leistungsfähigkeit bedarf es der *aktiven Auseinandersetzung* mit entsprechenden Erfahrungen, *mit allen Sinnen* und dem *gesamten Gehirn*.

Zu den wichtigsten Erkenntnissen der Gehirnforschung aus den letzten 30 Jahren gehört die Einsicht, dass sich das Gehirn mit jedem Gebrauch ändert – man spricht von Neuroplastizität bzw. ihrer Konsequenz: Lernen. Erst hierdurch ent-

faltet das Gehirn überhaupt seine Leistungsfähigkeit. Im Gegensatz zum Computer hat ein Gehirn weder eine CPU noch eine Festplatte. Stattdessen besteht es aus etwa hundert Milliarden Nervenzellen, von denen jede über bis zu zehn Tausend *Verbindungen* mit anderen Zellen vernetzt ist. Die Nervenzellen verarbeiten Informationen (in Form elektrischer Impulse), indem sie sich diese wechselseitig zuspielen. Hierbei überqueren diese Impulse die Verbindungsstellen der Nervenzellen – die *Synapsen* – die hierdurch ihre Stärke der Verbindung ändern. Die „Hardware" Gehirn ändert sich somit durch ihre Benutzung (d. h. die auf ihr laufende Software). Diese Änderungen der Synapsenstärken sind die Speicherung! Damit geht die Verarbeitung von Informationen *automatisch mit Speicherung* einher. Beide Funktionen werden also nicht von zwei unterschiedlichen Modulen bewerkstelligt, sondern sind zwei Aspekte eines Prozesses: des Gebrauchs von Nervenzellen. Dieser führt daher auch zu einer zunehmend besseren Verarbeitungsleistung während Kindheit und Jugend (Bild 10.1).

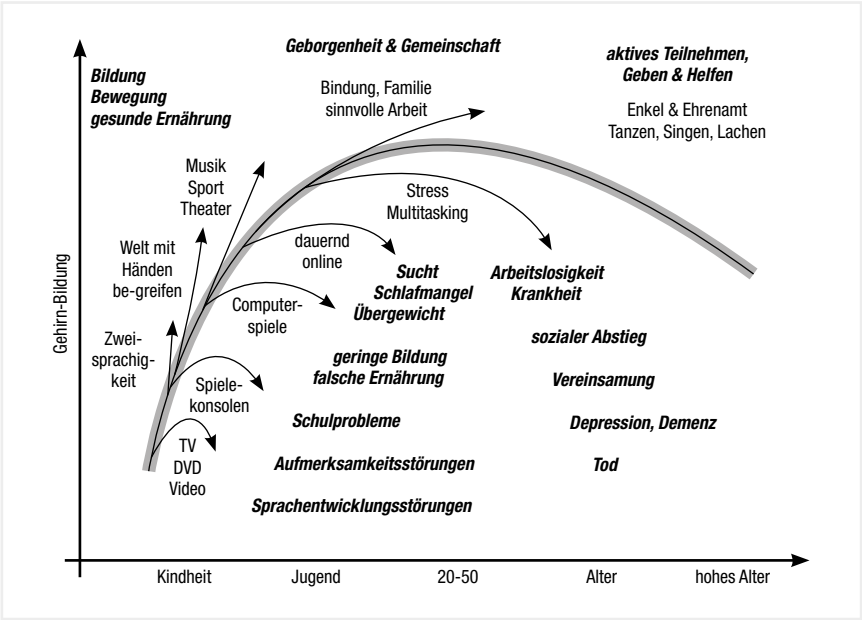

Bild 10.1: Schematische Darstellung der Entwicklung der geistigen Leistungsfähigkeit des Gehirns und einiger Faktoren, die sich positiv bzw. negativ darauf auswirken (aus Spitzer 2012)

Hinzu kommt ein weiterer wesentlicher Gesichtspunkt: Kleine Kinder lernen sehr schnell (d. h. ihre Synapsen ändern sich beim Gebrauch in einem vergleichsweise stärkeren Ausmaß), gerade weil sie noch gar nichts wissen oder können und so rasch wie möglich das Laufen und Sprechen lernen sowie die Welt und ihre Mitmenschen begreifen müssen. Schon im Schulalter ändern sich die Synapsen langsamer und bei Erwachsenen ist deren Veränderungsgeschwindigkeit vergleichsweise gering (Bild 10.2).

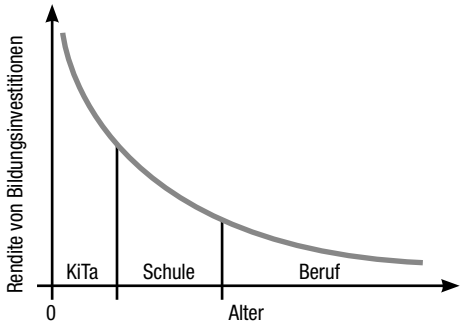

Bild 10.2: Bildungsrendite in Abhängigkeit vom Lebensalter des zu Bildenden (nach Heckman 2006). Der Kurvenverlauf ist letztlich Ausdruck eines allgemeineren biologischen Sachverhalts der Gehirnentwicklung, nämlich der Abhängigkeit des Ausmaßes der Veränderung synaptischer Verbindungen bei deren Gebrauch vom Lebensalter (vgl. Spitzer 2010, 2012).

Betrachten wir zur Illustration ein Beispiel: Kleinkinder mit einem normalsichtigen (100 %) und einem schwächeren Auge (z. B. 70 %) dürfen nicht ihrer spontanen Entwicklung überlassen werden. Denn die Sehzentren in ihrem Gehirn verarbeiten bevorzugt die scharfen Bilder vom 100 % sehfähigen Auge und berücksichtigen die unschärferen Bilder vom Auge mit nur 70-prozentiger Sehkraft nur wenig. Dies beeinträchtigt das Entstehen von Verbindungen vom schwächeren Auge zu den Sehzentren, und wenn man nichts tut, ist aus dem schwächeren Auge mit fünf Jahren ein *blindes* Auge geworden. Dieser Prozess ist dann unumkehrbar, d. h. Verbindungen, die in jungen Jahren nicht geknüpft wurden, können später nicht mehr entstehen. Man spricht hier auch von Entwicklungsfenstern, sensiblen Phasen oder Perioden. Wann diese Perioden beginnen und enden, hängt von der jeweiligen Gehirnfunktion und dem Ablauf der Entwicklung der an dieser Funktion beteiligten Module ab. So sind die Seh-

zentren bei der Geburt schon aktiv und entwickeln sich früh. Ihre maximale Zahl an Verbindungen (Synapsen) erreichen sie im 8. Lebensmonat, wonach weitere Strukturierung (man spricht auch von der Ausbildung innerer Repräsentationen, d. h. von Lernen) mit einer *Abnahme* der Zahl der Verbindungen (nur diejenigen, die gebraucht werden, bleiben bestehen) einhergeht.

Um diesen sehr ungünstigen Spontanverlauf bei einseitig schwachsichtigen Kindern zu verhindern, muss man ihnen das gesunde Auge mit einer Art „Piratenklappe" verschließen. Dadurch zwingt man das Gehirn, die Signale vom schwachen Auge zu verarbeiten (statt nur die besseren Signale vom scharf sehenden Auge), und es ist genau diese Verarbeitung, die für die „Verdrahtung" des schwachen Auges sorgt. Erst die Verarbeitung von Impulsen vom Auge führt also dazu, dass das Auge überhaupt das Sehen *lernt*! Unterbleibt das Training, ist das Auge zeitlebens unwiderruflich blind!

10.3 Gehirnentwicklung

Nicht anders ist es beim bereits oben angeführten Spracherwerb. Unterbleibt dieser bis zum Alter von etwa 13 Jahren, kann die Sprachentwicklung danach nicht mehr erfolgen. Das kritische Zeitfenster ist mithin länger offen, die Sprache entwickelt sich später als das Sehen. Von großer Bedeutung ist, dass es auf das an das Kind gerichtete Sprechen ankommt, also nicht einfach nur darauf, ob akustischer Input („Berieselung") vorhanden ist, sondern darauf, dass dieser aktiv verarbeitet wird. Hierfür ist die Eltern-Kind-Interaktion wesentlich. Eine Studie an sozial eher schwachen Familien konnte zeigen, dass die Anzahl der in einem Zeitraum von 10 Stunden an das Kind gerichteten Wörter von unter 670 bis mehr als 12.000 variiert (Weisleder & Fernald 2013). Entsprechend gab es Unterschiede zwischen dem Vokabular und der Geschwindigkeit der Sprachverarbeitung im Alter von zwei Jahren. Dies passt sehr gut zu einer fast zwei Jahrzehnte alten Studie, in deren Rahmen 42 Familien mit kleinen Kindern über mehrere Jahre hinweg im Hinblick auf die Anzahl und Art der über den Tag an die Kinder gerichteten Wörter beobachtet und untersucht wurden: Im Alter von drei Jahren hatten die Kinder aus Familien mit höherem sozioökonomischen Status etwa 30 Millionen mehr Wörter gehört als Kinder aus sozial schwachen Familien (Hart & Risley TR 1995).

Gleichzeitig mit dem sehr raschen Aufnehmen von Informationen erfolgt die biologische Entwicklung des Gehirns: Das Gehirn des Neugeborenen hat nur etwa ein Viertel (350 Gramm) des Gewichts und der Größe des Gehirns eines erwachsenen Menschen (1.300 – 1.400 Gramm), obwohl sowohl die Nervenzellen als auch deren Verbindungsfasern bereits vorhanden sind und nach der Geburt zahlenmäßig kaum zunehmen. Es ist vor allem *Fett*, das im Laufe der Entwicklung des Gehirns nach der Geburt das Gehirn so groß werden lässt. Dabei handelt es sich um eine ganze besondere Art von Fett, *Myelin* genannt, mit dem bestimmte Zellen (den Schwann'schen Zellen) die Nervenfasern ummanteln. Diese *Myelinisierung* der Nervenfasern bewirkt, dass die Impulse nicht mehr langsam (maximal mit etwa 3 m/s) entlang einer Nervenfaser *laufen*, sondern schnell (mit bis zu 115 m/s) entlang der Faser *springen*.

Dieser Unterschied ist für die Gehirnfunktion sehr bedeutsam, denn das Gehirn ist modular aufgebaut, d. h. verarbeitet Informationen vor allem dadurch, dass diese zwischen verschiedenen, jeweils einige cm voneinander entfernt liegenden Modulen Dutzende Male hin und her fließt. Hieraus erklärt sich die enorme Bedeutung der Myelinisierung. Die Zeit, die Impulse von einem Modul zu einem anderen benötigen, beträgt bei einer Nervenleitgeschwindigkeit von 3 Metern pro Sekunde bei einer Distanz von 10 cm etwa 30 Millisekunden. Dies mag kurz erscheinen, ist jedoch für eine Informationsverarbeitung, die letztlich darin besteht, dass Impulse zwischen unterschiedlichen Modulen vielfach hin und her fließen, sehr lang. Der rasche Austausch zwischen Modulen setzt eine schnelle Leitung der Impulse voraus, woraus sich wiederum ergibt, dass ein Modul, dessen Verbindungsfasern noch nicht myelinisiert sind, nur wenig zur Informationsverarbeitung beitragen kann. Damit ist eine nichtmyelinisierte Nervenfaserverbindung im Gehirn so etwas wie eine *tote Telefonleitung* – physikalisch vorhanden, aber praktisch ohne Funktion.

Durch die Anfärbung von Fett in Gehirnschnitten ließ sich schon vor etwa einhundert Jahren nachvollziehen, wann bzw. in welcher Reihenfolge Verbindungsfasern zur Ausreifung kommen (Bild 10.3). Zum Zeitpunkt der Geburt sind nur die primären sensorischen und motorischen Areale myelinisiert, also Bereiche, die für die ersten einfachen Verarbeitungsschritte von Umweltsignalen (Sehen, Hören, Tasten) verantwortlich sind oder direkt die Muskulatur ansteuern. Signale von der Außenwelt und an die Außenwelt können daher nur auf einfache Weise bearbeitet werden. Der Säugling macht erste Erfahrungen und reagiert auf sie auf einfachste Weise: Man zwickt ihn ins Bein und das Bein zuckt.

Im Gehirn des Neugeborenen werden die Informationen jedoch *noch nicht sehr tief* verarbeitet, d. h. noch nicht auf komplexe raum-zeitliche Muster hin untersucht. Erst durch die zunehmende Zuschaltung (durch Myelinisierung) von Arealen, deren Input die Aktivitätsmuster „einfacherer" Areale darstellen, kann dies erfolgen. Diese zunehmende Verarbeitungstiefe entsteht somit erst durch die biologische Reifung des Gehirns im Sinne der Myelinisierung nach der Geburt. Es werden zunehmend neue, „höhere" Gehirnbereiche durch schnelle Fasern mit bereits funktionierenden Gehirnarealen verbunden, sodass immer mehr Gehirnareale in die Informationsverarbeitung einbezogen werden und der Komplexitätsgrad der Verarbeitung zunimmt. Teile des Frontallappens des Menschen sind aufgrund dieser Entwicklung erst zur Zeit der Pubertät oder sogar erst danach funktionell voll mit dem Rest des Gehirns verbunden.

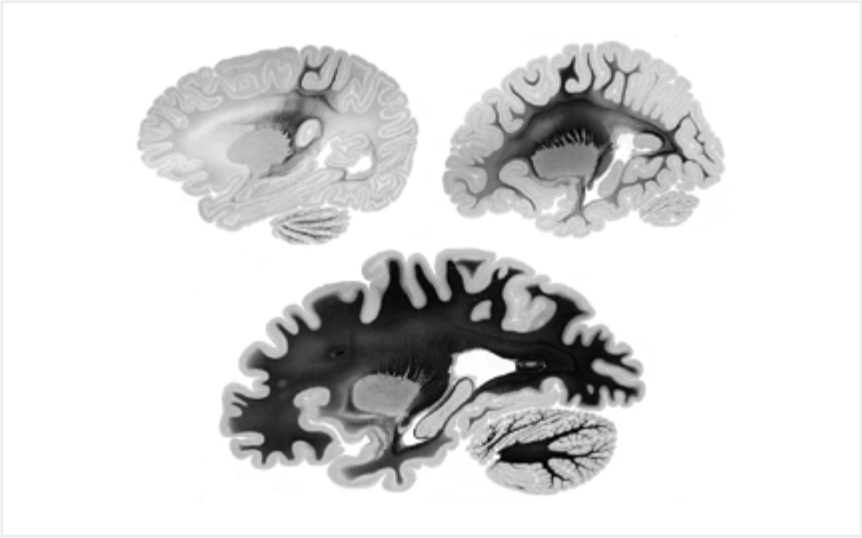

Bild 10.3: Darstellung der Myelinisierung von Faserverbindungen kortikaler Areale durch die Anfärbung von deren Fett (d. h. des Myelins) mit schwarzem Farbstoff, wie sie der deutsche Anatom Paul Flechsig bereits 1920 publizierte. Links oben ist das Gehirn eines Neugeborenen als Schnittbild zu sehen, rechts das Gehirn eines Kindes im Kindergartenalter und unten das Gehirn eines Erwachsen. Beim Säugling sind nur wenige Areale mit schnell leitenden Fasern verbunden.

Diese verglichen mit anderen Primaten sehr stark *verzögerte Gehirnentwicklung beim Menschen* wurde lange als Nachteil angesehen. Computersimulationen neuronaler Netzwerke, die sich eigens mit den Wechselwirkungen von Gehirnreifung und Lernen beschäftigten, zeigen jedoch, *dass die Reifung des Gehirns letztlich einen guten Lehrer ersetzt*. Dieser sorgt dafür, dass wir beim Lernen mit dem Einfachen beginnen und dann die Komplexität immer mehr steigern. Im alltäglichen Lebensvollzug während der ersten Lebensjahre (d. h. ohne Lehrer) sind wir jedoch den verschiedensten Reizen ausgesetzt, deren Struktur von „ganz einfach" bis „hoch komplex" reicht. Die Tatsache, dass sich das Gehirn entwickelt und zunächst überhaupt nur einfache Strukturen verarbeiten *kann*, stellt jedoch sicher, dass das Gehirn zunächst auch nur Einfaches lernt (Verarbeiten ist immer auch Lernen!).

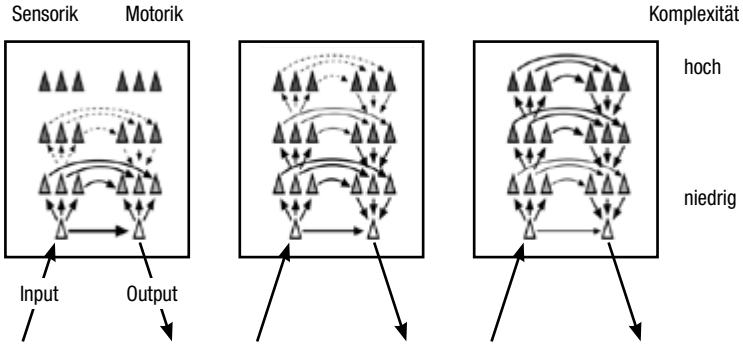

Bild 10.4: Schema zur Gehirnentwicklung vom Säugling (links) zum Erwachsenen (rechts). Nur die Neuronen in „niedrigen", „einfachen" Arealen sind beim Säugling bereits mit schnellen Fasern verbunden und damit „online".

Insgesamt folgt die Gehirnentwicklung dem einfachen Prinzip „von draußen nach innen" (Bild 10.4). Bei der Geburt schon entwickelt sind einfache Zentren der Sensorik und Motorik, d. h. Bereiche des Gehirns, die Verbindungen zur Außenwelt haben, entweder über die Sinnesorgane einschließlich des Tastsinns von der gesamten Körperoberfläche (Input) oder über motorische Fasern zu den Muskeln (Output). „Höhere" Zentren der komplexen Informationsverarbeitung zwischen Input und Output hingegen entwickeln sich erst und werden zugeschaltet, sodass ein System resultiert, dessen Datenanalysefähigkeit mit zunehmendem Alter einen zunehmenden Komplexitätsgrad erreicht. Das Frontalhirn – der Sitz von Denken, Bewerten, Willensakten, Zielen und Handlungsplänen sowie Simulationen künftiger Ereignisse (Probehandeln) – bildet im Hinblick auf seine Entwicklung das Schlusslicht und ist mit etwa 20 Jahren (oder etwas danach) erst voll entwickelt.

10.4 „Paradoxe Festplatte“ und kognitive Reserve

Zugleich zeigt die Erfahrung von Menschen mit ausgereiftem Gehirn Folgendes: Wer als Erwachsener schon drei Sprachen beherrscht, wird die vierte rascher lernen als derjenige, der nur seine Muttersprache gelernt hat. Wer schon drei Musikinstrumente beherrscht, lernt das vierte schneller als ein Erwachsener, der erst ganz von vorne zu musizieren beginnt, und beim Gebrauch von Werkzeugen oder dem Erlernen von Chemie oder Physik ist es ebenso: Je mehr ein Mensch als Kind und Jugendlicher gelernt hat, desto besser lernt er als Erwachsener.

Zum Vergleich: Wenn die Festplatte eines Computers zu 50 % beschrieben ist, beträgt die verbleibende Kapazität noch die Hälfte, wenn sie zu 90 % beschrieben ist, bleiben noch 10 % Kapazität. Mit dem Gehirn verhält es sich offensichtlich anders: „Ich kann schon drei Sprachen, da geht jetzt nichts mehr, denn meine Sprachzentren sind nahezu voll.“ – Diesen Satz belächeln wir mit Recht, denn die Erfahrung zeigt das genaue Gegenteil! Das Gehirn verhält sich wie eine *paradoxe* Festplatte: Je mehr schon gespeichert ist, desto größer die Kapazität! Der Grund hierfür liegt in der – verglichen mit einem Computer – fundamental anderen Architektur des Gehirns: Bereits gespeicherte Inhalte ermöglichen es dem Gehirn, neue Inhalte effizienter zu speichern, wie sich an den oben angeführten Beispielen verdeutlichen lässt. Das Beherrschen mehrerer Sprachen behindert das Erlernen einer weiteren Sprache nicht, sondern ermöglicht es vielmehr! Daraus folgt: Für lebenslanges Lernen sorgen wir in Kindergarten und Schule. Und es folgt auch: Wer mit 20 noch nichts gelernt hat, wird sich später mit dem Lernen sehr schwer tun.

Hinzu kommt: Je mehr das Gehirn in jungen Jahren gelernt hat, desto differenzierter arbeitet es und desto leistungsfähiger ist es. Dies drückt sich in einer erhöhten kognitiven Reserve im Alter aus, d. h. in einer besseren Ausgangslage bei Erkrankungen, die zu neuronalem Zelltod und damit zu geistigem Abbau führen (Valenzuela & Sachdev 2006).

Betrachten wir hierzu ein weiteres Beispiel: Wer zweisprachig aufgewachsen ist und zeitlebens die zweite Sprache bei Gelegenheit spricht, bekommt die Symptome einer Demenz – unabhängig von deren Typ – mit einer Verspätung von etwa fünf Jahren, wie fünf internationale Studien mittlerweile zeigen konnten (Alladi et al. 2013, Bialystok et al. 2007, Chertkow et al. 2010, Craik et al. 2010, Schweitzer et al 2012). Dabei ist es *nicht* so, dass die krankheitsbedingten pathologischen Veränderungen, also die kleinen Infarkte (bei Multi-Infarkt-Demenz) oder die Ablagerung von Plaques und Fibrillen (bei Alzheimer-Demenz), später auftreten; vielmehr verfügt ein gut gebildetes Gehirn über mehr *Reserven*, die es nutzen kann, wenn die Hardware langsam kaputtgeht. Da Zweisprachigkeit in den meisten Fällen nicht das Resultat von Begabung (Genetik) ist, sondern durch die Umstände (unterschiedliche Herkunft oder Auswanderung der Eltern) bedingt ist, zeigt diese Studie die Auswirkungen geistiger Tätigkeit auf einen späteren geistigen Abstieg (lat: *de* – herab; *mens* – der Geist), d. h. eine sich entwickelnde Demenz, sehr klar. Es gibt übrigens kein Medikament, mit dem sich das Auftreten einer Demenz auch nur annähernd so gut verzögern ließe wie dies für Zweisprachigkeit nachgewiesen ist. Krankhafte Veränderungen bei Alzheimer-Demenz werden also durch geistige Tätigkeit nicht verhindert. Vielmehr kann ein gebildeter Geist deutlich kranker sein als ein schwacher Geist, ohne dass man dies merkt.

Vor dem Hintergrund dessen, was hier stark zusammengefasst und auf wenige Prinzipien reduziert zur Gehirnentwicklung gesagt wurde, ergeben sich die negativen Auswirkungen digitaler Informationstechnik auf die Entwicklung der geistigen Leistungsfähigkeit junger Menschen unmittelbar als Konsequenz von deren vielschichtiger Beeinträchtigung der natürlichen Gehirnbildung, die immer als Wechselwirkung zwischen biologischen Reifungs- und psychologischen Lernprozessen zu verstehen ist.

10.5 Daten zu Risiken und Nebenwirkungen

Wer schon als Kleinkind viel Zeit vor Bildschirmmedien verbringt, zeigt in der Grundschule vermehrt Störungen der Sprachentwicklung und Aufmerksamkeitsstörungen (Zimmerman et al. 2007), erreicht nach großen Langzeitstudien insgesamt ein deutlich geringeres Bildungsniveau (Hancox et al. 2005) und wird aufgrund antisozialer Verhaltensweisen mit höherer Wahrscheinlichkeit kriminell (Robertson et al. 2013). Eine Spielekonsole verursacht bei Grundschulkindern nachweislich schlechte Noten im Lesen und Schreiben sowie Verhaltensprobleme in der Schule (Weis & Cerankosky 2010); ein Computer im Jugendzimmer von 15-Jährigen wirkt sich negativ auf die Schulleistungen aus (Fuchs & Wössmann 2004) und im Jugendalter führen Internet und Computer zu einer Verringerung der Selbstkontrolle und zur Sucht (Fröhlich & Lehmkuhl 2012, Gentile 2009, Kim 2011).

Computer-, Internet- und neuerdings auch *Smartphone-Sucht* sind ernst zu nehmende Risiken digitaler Informationstechnik. Die Suchtbeauftragte der Bundesregierung gibt die Zahl der computerspiel- bzw. internetabhängigen Vierzehn- bis Vierundzwanzigjährigen mit einer Viertelmillion an, zu denen noch 1,4 Millionen als in dieser Hinsicht „problematisch" geltenden Computer- und Internetnutzer hinzukommen. Der Anteil Smartphone-Süchtiger beträgt in Südkorea, einem Land mit sehr starker Smartphone-Nutzung, etwa 18 % (Daten des dortigen Wissenschaftsministeriums). Zudem führt Smartphone-Nutzung zu Unaufmerksamkeit (Zheng et al. 2014), Depressionen (Rosen et al. 2013a, Thomée et al. 2011, Yen et al. 2009), Ängsten und geringerem akademischem Erfolg (Lepp et al. 2014), Einsamkeit (Beranuy et al. 2009), Schlafstörungen (Murdock 2013, White et al. 2011) sowie zu mehr Alkohol- und Tabak-Konsum und Schulversagen (Sánchez-Martínez & Otero 2009). Die Nutzung sozialer Netzwerke wie Facebook macht junge Menschen nicht sozialer, sondern depressiver, ängstlicher, unzufriedener und einsamer, wie neuere Studien zeigen (Kross et al. 2013, Rosen et al. 2013). Auch stört Facebook den Schlaf (Wolniczak et al. 2013). Zudem wissen wir aus der allgemeinen Gehirnforschung, dass sich das soziale Gehirn des Menschen durch soziale Erfah-

rungen entwickelt (Powell et al. 2012), weil wir vom Gehirn insgesamt (siehe oben) und vom sozialen Gehirn bei Primaten wissen (Sallet et al. 2011), dass es sich mit seiner Verwendung überhaupt erst bildet. Wenn junge Mädchen in den USA im Alter zwischen 8 und 12 Jahren täglich 2 Stunden mit anderen Mädchen verbringen, jedoch 7 Stunden auf Facebook (Pea et al. 2012), dann muss uns das alarmieren: Denn in diesem Alter ist das soziale Gehirn voll in seiner Entwicklung, kann sich aber nicht entfalten, wenn realer sozialer Kontakt durch einen Bildschirm ersetzt wird (Spitzer 2012). Entsprechend wurde in der weltweit größten Längsschnittstudie hierzu herausgefunden, dass der Gebrauch von Bildschirmmedien bei Jugendlichen mit geringerer Empathie gegenüber Eltern und Freunden einhergeht (Richards 2010).

Die negativen Auswirkungen digitaler Medien auf Kinder und Jugendliche im körperlichen, sozialen und kognitiven Bereich sind besorgniserregend. Hinzu kommen deren Suchtpotential und deren langfristige Risiken für körperliche und geistige Erkrankungen. Vor allem bei Kindern und Jugendlichen ist daher eine Konsumbeschränkung dringend erforderlich, um diesen bekannten und durch sehr viele Studien eindeutig nachgewiesenen Nebenwirkungen zu begegnen. Wer 35 Wochenstunden Schule hat, verbringt täglich 3,75 Stunden mit dem Schulstoff. Der durchschnittliche Konsum digitaler Medien liegt dagegen bei 7,5 Stunden täglich. Junge Menschen verbringen also doppelt so viel Zeit mit digitalen Medien wie mit dem gesamten Schulstoff zusammengenommen.

Konkrete Studien zur Anwendung digitaler Informationstechnik im Bildungsbereich bestätigen das hier gezeichnete Bild und zeigen – ganz entgegen den vielen diesbezüglichen Behauptungen – keineswegs einen positiven Effekt der Digitalisierung unserer Bildungseinrichtungen auf den Bildungserfolg. Computer nehmen uns geistige Arbeit ab und sind daher für das Lernen ebenso ungeeignet, wie das Auto als Trimm-dich-Gerät ungeeignet ist: Es nimmt uns körperliche Arbeit ab und trainiert daher nicht unseren Körper.

Die große vom Bundeswissenschaftsministerium, der Europäischen Union und der deutschen Telekom geförderte Studie „Schulen ans Netz. 1.000 mal 1.000: Notebooks im Schulranzen“ hatte weder bessere Noten noch besseres Lernverhalten der Schüler zum Ergebnis: „Insgesamt kann die Studie somit keinen eindeutigen Beleg dafür liefern, dass die Arbeit mit Notebooks sich grundsätzlich in verbesserten Leistungen und Kompetenzen sowie förderlichem Lernverhalten von Schülern niederschlägt.“ Allerdings waren „die Schüler im Unterricht

mit Notebooks tendenziell unaufmerksamer“ (Schaumburg et al. 2007, S. 120). Nicht einmal der Umgang mit Computern wurde in den Computer-Klassen gelernt: „Im Informationskompetenz-Test wurden keine Unterschiede zwischen Notebook- und Nicht-Notebook-Schülern gefunden“ (S. 121).

Drei Jahre später hatte das „Hamburger Netbook Projekt. Sekundarstufen Schulen“ die gleichen Ergebnisse, zeigten sich doch „keine signifikanten Unterschiede in der Kompetenzentwicklung“ (Müller & Kammerl 2010, S. 118) zwischen Schülern in Klassen mit bzw. ohne Computer. Auch der Umgang mit Medien wurde nicht gelernt: „Ein eindeutiger Trend zu einer Stärkung der Medienkompetenz im Umgang mit Computer und Internet konnte in Folge des Netbook-Einsatzes nicht verzeichnet werden“ (Müller & Kammerl 2010, S. 118). Die Schüler besaßen vielmehr zu 90 % „bereits bei Projektbeginn einen eigenen Computer zu Hause. Das Computer- und Internetwissen haben sich die Schüler hauptsächlich selbst beigebracht (58 %) oder es wurde ihnen von Familienmitgliedern (28 %) vermittelt. Die Schule spielt hier eine untergeordnete Rolle (8 %)“ (Müller & Kammerl 2010, S. 117).

10.6 Drei Beispiele: Baby-TV, Lesen in der Grundschule und Suchmaschinen für Referate

Stellvertretend für die vielen Beispiele von negativen Auswirkungen von frühem Bildschirmmedienkonsum auf die Gehirnbildung seien hier nur zwei genannt. Babys verbringen den Hauptteil ihres Lebens mit Schlafen. Wenn sie dann für einen wesentlichen Teil ihrer wachen Zeit einem Medium ausgesetzt werden, von dem sie – im Gegensatz zur wirklichen Welt und wirklichen Menschen – nichts lernen können, dann lernen sie insgesamt weniger. Wer also sein Baby zum Erwerb der Muttersprache vor einen Bildschirm setzt, der riskiert einen negativen Einfluss auf dessen Sprachentwicklung, wie eine Studie an über 1.000 Babys und deren Eltern zeigte (Bild 10.5). Man befragte die Eltern genau nach den Mediennutzungsgewohnheiten ihrer Kinder und führte mit den Kleinen dann einen Sprachtest durch. Das Ergebnis: Wer Baby-TV oder Baby-DVDs schaut, kennt deutlich weniger Wörter, ist also in seiner Sprachentwicklung verzögert. Der Effekt war beim Konsum von Babyprogrammen besonders stark ausgeprägt. Wenn ein Elternteil täglich vorlas, ergab sich hingegen ein positiver Effekt auf die Sprachentwicklung.

Zur Verdeutlichung der Risiken und Nebenwirkungen digitaler Medien im schulischen Bereich sei eine chinesische Studie angeführt, die verdeutlicht, was geschehen kann, wenn man diese nicht berücksichtigt (Tan et al. 2013). Man untersuchte die Lesefähigkeit von nahezu 6.000 Schülern der Klassen 3, 4 und 5 mit den gleichen Tests, die man schon 20 und 10 Jahre vorher verwendet hatte, als der Anteil der Schüler mit schweren Lesestörungen (Analphabeten) bei 2 bis 8 % lag. Bekanntermaßen verwendet die chinesische Schrift etwa 5.000 Symbole, die von Schulkindern nur dann behalten werden, wenn man sie oft mit der Hand schreibt. Wenn nun Chinesen am Computer schreiben, verwenden sie eine ganz normale Tastatur und schreiben Lautschrift, also z. B. „li“, woraufhin der Computer dann eine Liste von Wörtern anzeigt, die alle wie „li“ klingen. Dann wird mit der Maus das Zeichen mit der gemeinten Bedeutung angeklickt und der Computer setzt es anstatt „li“ ein. Diese Methode, chinesisch zu schreiben – genannt Pinyin-Methode –, ist sehr effizient und wird daher in chinesischen Grundschulen in der zweiten Hälfte der Klasse 3 gelehrt.

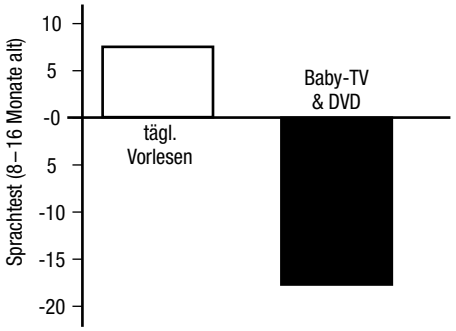

Bild 10.5: **Auswirkung des täglichen Vorlesens (links) oder Konsums von speziell für Babys produzierten Programmen (Baby-TV oder Baby-DVD) auf das Ergebnis eines Sprachtests (Abweichung der Rohwerte vom Mittelwert) bei Kindern im Alter von acht bis 16 Monaten**

Das Erlernen dieser Fähigkeit ist jedoch von der „Nebenwirkung" begleitet, dass über 40 % der Schüler in Klasse 4 nicht mehr lesen können; in Klasse 5 sind es über 50 %. Zudem zeigte sich, dass diejenigen Schüler, die zu Hause noch gelegentlich mit der Hand chinesisch schreiben, in Klasse 4 und 5 auch noch eher des Lesens mächtig sind als diejenigen, die praktisch vollständig auf digitale Eingabe umsteigen. Die Risiken und Nebenwirkungen digitaler Medien sind kaum besser zu verdeutlichen!

Wer meint, dass wir hierzulande deutlich besser dran seien, der irrt: Auch in Deutschland wurde die kursive Handschrift in manchen Ländern bereits abgeschafft. Die Kinder schreiben Druckbuchstaben und erlernen daher nicht mehr die komplexen Motorprogramme, die auch ihrem Gedächtnis helfen, wenn sie etwas aufschreiben. In den USA wurde im Frühjahr 2013 in 46 Bundesstaaten die Handschrift vom Curriculum der Grundschule gestrichen! Klassenziel für das Ende von Klasse 4 ist jetzt, mit 10 Fingern tippen zu können. Wir wissen jedoch aus entsprechenden Studien, dass Tippen keineswegs in seiner Komplexität der Handschrift entspricht und dass Handgeschriebenes im Gedächtnis besser hängen bleibt als auf der Tastatur Getipptes (Longcamp et al. 2005, 2008, 2011, Mueller & Oppenheimer 2014). Erlernen Schulkinder also nicht mehr das Schreiben mit der Hand, kommt dies der Beraubung junger Menschen eines wichtigen Werkzeugs zur Steigerung ihrer Merkfähigkeit gleich.

Man schadet also ihrem Bildungsprozess. Betrachten wir ein drittes Beispiel: An vielen Schulen werden Referate dann mit besseren Noten gewürdigt, wenn sie mithilfe der modernen Informationstechnik erstellt und gehalten wurden. Es komme darauf an, dass die Schüler nicht nur die Inhalte des Referats anhand von irgendwelchem Material erarbeiteten, sondern dass sie gleichzeitig auch noch den Umgang mit digitaler Informationstechnik, also mit Computer, dem Internet, Suchmaschinen und Präsentationssoftware erlernten.

Eine im Fachblatt *Science* publizierte Studie amerikanischer Wissenschaftler hat jedoch ergeben, dass Informationen, die entweder per Buch, per Zeitung, per Zeitschrift oder per Google gewonnen werden, dann am wenigsten im Gedächtnis haften bleiben, wenn sie gegoogelt wurden (Sparrow et al. 2011). „Das kann ich ja googeln", scheint sich unser Gehirn zu sagen und die Inhalte dann eben nicht abzuspeichern. Wer also etwas googelt, anstatt es in einem Buch zu lesen, hat eine geringere Chance, damit sein Wissen zu erweitern. Nun wird vonseiten der Verfechter dieses Ansatzes betont, dass die Schüler doch heute Medienkompetenz erlernen müssten, weil man ja alles googeln könne und man daher auch noch kaum noch etwas zu wissen brauche. Es wird gesagt, dass es in den Bildungseinrichtungen gar nicht mehr um das Aneignen eines Fundus an Wissen gehe, sondern nur noch um die Kompetenz des Umgangs mit Wissen, das man beispielsweise aus dem Internet herunterladen könne. Diese Ansicht erweist sich bei näherem Hinsehen als unhaltbar! Um eine Suchmaschine wie Google zu verwenden, braucht man weder Medienkompetenz noch einen Internetführerschein. Man braucht nur einmal zuzusehen, wie jemand Google bedient: auf den Browser klicken, das Feld aufrufen, dann die Suchbegriffe eintragen und auf Los klicken. – Einmal gesehen, gleich gekonnt! Wenn Google einem dann aber innerhalb von 0,1 Sekunden 10.000 Hits auf den Bildschirm wirft, dann braucht man etwas – und zwar notwendig –, um damit etwas anfangen zu können: *Vorwissen!*

Weiß man gar nichts, so wird man auch nicht googeln (weil man auch keine Frage hat). Weiß man fast nichts, so nützt einem Google nichts, weil man bei den vielen Dingen, die Google auf dem Bildschirm anzeigt, nicht die Spreu vom Weizen trennen kann. Ganz allgemein gilt: Je besser man sich in einem Fachgebiet auskennt, desto besser kann man in diesem Fachgebiet auch suchen und etwas finden. Darüber hinaus gibt es keine allgemeine Kompetenz, die es ermöglicht noch besser zu googeln. Das Gerede von „Medienkompetenz" entpuppt sich damit als inhaltsleer. Ebenso ist es sehr misslich, dass von vielen of-

fiziellen pädagogischen Stellen davon die Rede ist, dass heute „Wissen“ nicht mehr notwendig sei und es nur noch auf „Kompetenz“ ankomme. Dies ist völliger Unsinn! Es ist gerade das Wissen über ein bestimmtes Sachgebiet, das es mir erlaubt, die Informationen in diesem Sachgebiet zu bewerten und somit mit ihnen umzugehen. Damit ist Wissen eine Grundvoraussetzung für die Benutzung des Internets. Wenn aber nun Wissen mithilfe von Google am allerschlechtesten im Kopf hängen bleibt, dann folgt zwingend: Wenn man wirklich will, dass unsere Schüler in den Bildungseinrichtungen darauf vorbereitet werden, später in der Berufswelt Suchmaschinen und das Internet zu nutzen, dann darf man in der Schule eines auf keinen Fall tun: googeln.

Zudem gilt für das Halten von Referaten, dass beim Suchen von Informationen mittels Suchmaschinen, beim Auffinden von Informationen irgendwo im Netz und bei dem Verfrachten dieser Informationen mittels „Copy“ und „Paste“ von beispielsweise Wikipedia nach PowerPoint kaum mentale Aktivität (im Sinne tiefer Verarbeitung) im Kopf des Schülers abläuft. Früher hat man exzerpiert, das Exzerpt geordnet und dann noch einmal in Reinschrift, beispielsweise auf eine Transparentfolie, übertragen. All diese Aktivitäten wurden von entsprechenden geistigen Aktivitäten und damit von entsprechenden Veränderungen im Gehirn, die wir als Lernen bezeichnen, begleitet. Nichts dergleichen geschieht bei der Benutzung von Informationstechnik!

10.7 Was ist zu tun?

Langzeitstudien an gut tausend Neugeborenen konnten zeigen, dass der Medienkonsum im Kindergartenalter deutliche negative Auswirkungen auf den Bildungserfolg im Erwachsenenalter hat und dass zudem der Medienkonsum im Kindergartenalter für einen Teil des Übergewichts im Erwachsenenalter verantwortlich ist. Schulabbrecher kommen zudem viel leichter „auf die schiefe Bahn" bzw. enden in einer Suchtkarriere. Übergewicht wird gerade in den letzten Jahren immer häufiger als suchtähnliches Verhalten interpretiert, insbesondere im Lichte neuer Daten aus der Gehirnforschung.

Nimmt man die angeführten Datensätze im Zusammenhang, so ergibt sich eine recht dichte Indizienkette von Medienkonsum im Kinder- und Jugendalter zu Gesundheits- und Bildungsproblemen im Jugend- und Erwachsenenalter. Diese Kette geht weit darüber hinaus, was landläufig diskutiert wird, nämlich das Erlernen inadäquater Haltungen und Gewohnheiten durch digitale Medien im Kindes- und Jugendalter. Der Zusammenhang reicht vielmehr tiefer: Medienkonsum senkt die Chance zur Ausbildung von Selbststeuerungsfähigkeit und diese wiederum ist ein Schutzfaktor.

Aus dieser Sicht ergeben sich praktische Konsequenzen: Wer meint, dass im Kindergarten oder in der Grundschule mehr Mediennutzung stattfinden sollte, damit die Kinder und Jugendlichen „Medienkompetenz" erlangen, muss nachweisen, dass die vermuteten Vorteile größer sind als die mit Sicherheit vorhandenen Nachteile. Einen solchen Nachweis bleiben diejenigen, die Computernutzung gerade im Kindesalter stark propagieren, bislang schuldig. Wenn zudem Computer an Schulen in höheren Klassen nicht zu vermehrter Kenntnis im Umgang mit Computern führen, sei die Frage erlaubt, wie man dann den Einsatz von Computern zur Medienkompetenz-Stärkung in Kindergärten oder Grundschulen rechtfertigen soll. Medienkompetenz soll in aller Regel über mehr Mediennutzung vermittelt werden und diese Mediennutzungszeit macht eine Mediensuchtentwicklung wahrscheinlich und reduziert zudem die Selbststeuerungsfähigkeit als wichtigsten Schutzfaktor gegenüber einer Suchtent-

wicklung. Medienkonsum in der Kindheit bewirkt damit nicht nur eine geringere Chance auf Bildung und Gesundheit, sondern erhöht zugleich das Risiko für abweichendes Verhalten bis hin zur Sucht. Dies betrifft sowohl stoffgebundenes Suchtverhalten wie Alkohol- und Tabakmissbrauch (Sánchez-Martínez & Otero 2009) als auch nicht stoffgebundenes Suchtverhalten wie die Mediensucht.

Wir können nicht zulassen, dass einige wenige Konzerne die Gehirne der nächsten Generation massiv schädigen. Daher ist es an der Zeit, die Risiken und Nebenwirkungen digitaler Medien ernst zu nehmen. Denn für alle jungen Menschen unter 18 Jahren haben wir Erwachsenen die Verantwortung. Und der müssen wir uns stellen.

Literatur

Alladi, S. et al. (2013). Bilingualism delays age at onset of dementia, independent of education and immigration status. Neurology 81: 1–7.

Anonymus (2014). Anschluss verpasst. Die Zeit.

Beranuy, M., Oberst, U., Carbonell, X., Chamarro, A. (2009). Problematic internet and mobile phone use and clinical symptoms in college students: The role of emotional intelligence. Comput Hum Behav 25: 1182–1187.

Bialystok, E., Craik F. I. M, Freedman, M. (2007). Bilingualism as a protection against the onset of symptoms of dementia. Neuropsychologia 45: 459–464.

Bostelmann, A., Fink, M. (2014). Digital Genial: Erste Schritte mit Neuen Medien im Kindergarten. Bananenblau Verlag, Berlin.

Buchegger, B. (2013). Unterrichtsmaterial Safer Internet im Kindergarten. ÖIAT Österreichisches Institut für angewandte Telekommunikation (www.saferinternet.at).

Chertkow, H. et al. (2010). Multilingualism (but not always bilingualism) delays the onset of Alzheimer´s disease: Evidence from a bilingual community. Alzheimer Disease and Associated Disorders 24: 118–125.

Craik, F. I. M., Bialystok, E., Freedman, M. (2010). Delaying the onset of Alzheimer disease: Bilingualism as a form of cognitive reserve. Neurology 75: 1717–1725.

Fröhlich, J., Lehmkuhl, G. (2012). Computer und Internet erobern die Kindheit. Vom normalen Spielverhalten bis zur Sucht und deren Behandlung. Schattauer, Stuttgart

Fuchs, T., Wössmann, L. (2004). Computers and student learning: bivariate and multi variate evidence on the availability and use of computers at home and at school. CESifo Working Paper 2004; 1321 (www.CESifo.de).

Gentile, D. (2009). Pathological video-game use among youth ages 8–18: A national study. Psychological Science 20: 594–602.

Gottwald, A., Valendor, M. (2010). Hamburger Netbook-Projekt. Behörde für Schule und Berufsbildung, Hamburger Straße 31, 22083 Hamburg.

Gracia-Bafalluy M, Noël MP. Does anger training increase young children's numerical performance? Cortex 2008; 44: 368–375.

Hart, B., Risley, T. R. (1995). Meaningful Differences in the Everyday Experience of Young American Children. Paul H. Brookes Publishing Co., Baltimore, MD, USA.

Heckman, J. J. (2006). Skill formation and the economics of investing in disadvantaged children. Science 312: 1900–1902.

Kim, S. South Korea ditching textbooks for tablet PCs. USA Today (20.7.2011). Associated Press www.usatoday.com/tech/news/2011 – 7 – 20 – south – korea – tablet – pc_n.htm.

Lepp, A., Barkley, J. E., Karpinski, A. C. (2014). The relationship between cell phone use, academic performance, anxiety, and satisfaction with life in college students. Computers in Human Behavior 31: 343–350.

Longcamp, M., Boucard, C., Gilhodes, J. C., Anton, J. L., Roth, M., Nazarian, B., Velay, J. L. (2008). Learning through hand- or typewriting influences visual recognition of new graphic shapes: Behavioral and functional imaging evidence. Journal of Cognitive Neuroscience 20: 802–815.

Longcamp, M., Hlushchuk, Y., Hari, R. (2011). What differs in visual recognition of handwritten vs. printed letters? An fMRI study. Human Brain Mapping 2011; 32: 1250–1259.

Longcamp, M., Zerbato-Poudou, M. T., Velay, J. L. (2005). The influence of writing practice on letter recognition in preschool children: A comparison between handwriting and typing. Acta Psychologica 119: 67–79.

Medienpädagogischer Forschungsverbund Südwest (2012). miniKIM 2012. Kleinkinder und Medien. Landesanstalt für Kommunikation Baden-Württemberg (www.mpfs.de). Selbstverlag, Stuttgart.

Müller, P. A., Oppenheimer, D. M. (2014). The pen is mightier than the keyboard: Advantages of longhand over laptop note taking. Psychological Science 25: 1159–1168.

Murdock, K. K. (2013). Texting while stressed: Implications for students' burnout, sleep, and well-being. Psychology of Popular Media Culture 2: 207–221.

Noël, M. P. Finger gnosia: A predictor on numerical abilities in children? Child Neuropsychology 2005; 11: 413–430.

Parker, Jones O. et al. (2012). Where, when and why brain activation differs for bilinguals and monolinguals during picture naming and reading aloud. Cerebral Cortex 22: 892–902.

Pea, R., Nass, C., Meheula, L., Rance, M., Kumar, A., Bamford, H., Nass, M., Simha, A., Stillerman, B., Yang, S., Zhou, M. (2012). Media use, face-to-face communication, media multitasking, and social well-being among 8- to 12-year-old girls. Developmental Psychology 48: 327-336.

Powell, J., Lewis, P. A., Roberts, N., García-Fiñana, M., Dunbar, R. I. M. (2012). Orbital prefrontal cortex volume predicts social network size: An imaging study of individual differences in humans. Proceedings of the Royal Society, published online 1 February 2012 (doi: 10.1098/rspb.2011.2574).

Rehbein, F., Kleimann, M., Mößle, T. (2009). Computerspielabhängigkeit im Kindes- und Jugendalter. Empirische Befunde zu Ursachen, Diagnostik und Komorbiditäten unter besonderer Berücksichtigung spielimmanenter Abhängigkeitsmerkmale. Kriminologisches Forschungsinstitut Niedersachsen (KFN) Schriftenreihe Bd. 108.

Richards, R. et al. (2010). Adolescent screen time and attachment to peers and parents. Archives of Pediatrics & Adolescent Medicine 164: 258–262.

Robertson, L. A., McAnally, H. M., Hancox, R. M. (2013). Childhood and adolescent television viewing and antisocial behavior in early adulthood. Pediatrics 131: 439–446.

Rosen, L. D., Whaling, K., Rab, S., Carrier, L. M., Cheever, N. A. (2013) Is Facebook creating „iDisorders"? The link between clinical symptoms of psychiatric disorders and technology use, attitudes and anxiety. Computers in Human Behavior 29: 1243–1254

Sallet, J., Mars, R. B., Noonan, M. P., Andersson, J. L., O'Reilly, J.X., Jbabdi, S., Croxon, P. L., Jenkinson, M., Miller, K. L., Rushworth, M. F. S. (2011). Social network size affects neural circuits in macaques. Science 334: 697–700.

Sånchez-Martínez, M., Otero, A. (2009). Factors associated with cell phone use in adolescents in the community of Madrid (Spain). CyberPsychology & Behavior 12: 131–137.

Schaumburg, H., Prasse, D., Tschackert, K., Blömeke, S. (2007). Lernen in Notebook-Klassen. Endbericht zur Evaluation des Projekts „1.000 mal 1.000: Notebooks im Schulranzen". Schulen ans Netz e. V., November 2007, Bonn.

Schweizer et al. (2012). Bilingualism as a contributor to cognitive reserve: Evidence from brain atrophy in Alzheimer's disease. Cortex 48: 991–996.

Sparrow, B., Liu, J., Wegner, D. M. (2011). Google effects on memory: cognitive consequences of having information at our fingertips. Science 333: 776–778.

Spitzer, M. (2010). Medizin für die Bildung, Spektrum, Heidelberg.
Spitzer, M. (2012). Digitale Demenz. Droemer, München.
Spitzer, M. (2014). Smartphones. Nervenheilkunde 33: 9–15.

Tan, L. H., Xu, M., Chang, C. Q., Siok, W. T. (2013). China‘s language input system in the digital age affects children‘s reading development. PNAS 111: 1119–1123.

Textor, M. (2014). Tablet-PCs – ein neues Medium für Kleinkinder in Familie und Kita. „Kita aktuell“ 10/2014: 225–226.

Thomeé, S., Hårenstam, A., Hagberg, M. (2011). Mobile phone use and stress, sleep disturbances, and symptoms of depression among young adults – a prospective cohort study. BMC Public Health 11: 66 (doi:10.1186/1471-2458-11-66).

Valenzuela, M. J., Sachdev, P. (2006). Brain reserve and cognitive decline: A non-parametric systematic review. Psychological Medicine 36: 1065–073.

Weis, R., Cerankosky, B. C. (2010). Effects of video-game ownership on young boys‘ academic and behavioral functioning: A randomized, controlled study. Psychological Science 21: 463–470.

Weisleder, A., Fernald, A. (2013). Talking to children matters: Early language experience strengthens processing and builds vocabulary. Psychological Science 24: 2143–2152.

White AG Buboltz, W., Igou, F. (2011). Mobile phone use and sleep quality and length in college students. International Journal of Humanities and Social Science 1: 51–58.

Wolniczak, I., Cáceres-DelAguila, J. A., Palma-Ardiles, G., Arroyo, K. J., Soli´s-Visscher, R. et al. (2013). Association between Facebook Dependence and Poor Sleep Quality: A Study in a Sample of Undergraduate Students in Peru. PLoS ONE 8(3): e59087. doi:10.1371/journal.pone.0059087.

Yen, C., Tang, T., Yen, J., Lin, H., Huang, C., Liu, S. (2009). Symptoms of problematic cellular phone use, functional impairment and its association with depression among adolescents in Southern Taiwan. Journal of Adolescence 32: 863–873.

Zheng, F., Gao, P., He, M., Li, M., Wang, C., Zeng, Q., Zhou, Z., Yu, Z., Zhang, L. (2014). Association between mobile phone use and inattention in 7202 Chinese adolescents: a population-based cross-sectional study.
BMC Public Health 14: 1022–1028.

Zimmerman, F. J., Christaki,s D. A., Meltzoff, A. N. (2007).
Associations between media viewing and language devlopment in children under age 2 years. Journal of Pediatrics 151:364–368.

11

Risikobewertung im Eisenbahnwesen

11.1 Entwicklung der Betrachtung von Risiken und der Sicherheit im Eisenbahnwesen

Dipl.-Ing. Matthias Heidl, Eisenbahn-Bundesamt, Deutschland

Die Sicherheit hat bei der Eisenbahn seit jeher einen hohen Stellenwert. Wie bei anderen Verkehrsträgern gibt es zwar auch bei der Eisenbahn systembedingte Risiken. Systemmerkmale, die zu einer Erhöhung des Risikos führen, sind insbesondere die großen bewegten Massen, die in Verbindung mit dem geringen Reibwert zwischen Rad und Schiene zu langen Bremswegen führen. Die Spurführung ermöglicht kein Ausweichen, womit kaum Reduktionsfaktoren zur Vermeidung eines drohenden Zusammenstoßes gegeben sind. Die Zwangsführung im Gleis ist aber andererseits auch sicherheitsfördernd, weil sie kaum Fahrfehler eines Triebfahrzeugführers zulässt. Die systembedingten Risiken der Eisenbahn wurden schon früh durch spezielle technische Maßnahmen in der Signaltechnik kompensiert. So ist die Signalabhängigkeit, die die Fahrtstellung eines Signals erst zulässt, wenn alle zugehörigen Weichen im Fahrweg in der richtigen Stellung verschlossen sind, schon seit dem 19. Jahrhundert Standard. Ab Anfang des 20. Jahrhunderts gibt es Zugbeeinflussungssysteme, die bei Missachtung eines Signals eine Zwangsbremsung auslösen. So konnte sich die Eisenbahn als durchaus sicheres Verkehrsmittel auch gegenüber anderen Verkehrsträgern behaupten. Neue Herausforderungen bestehen jedoch in der Öffnung des Netzzugangs (in Deutschland seit Mitte der 90er-Jahre). Ehemals wurde die Schnittstelle zwischen Infrastruktur und Betrieb der Züge durch eine Eisenbahngesellschaft als Betreiber des Gesamtsystems abgedeckt, heute fahren auf dem bundeseigenen Eisenbahnnetz der DB Netz AG mehr als 300 Eisenbahnverkehrsunternehmen, darunter auch ausländische.

Durch die Staatsbahnen wurden viele Vorschriften im Wesentlichen zur Festlegung von Sicherheitsanforderungen erstellt. Unfälle und gefährliche Ereignisse wurden systematisch ausgewertet und führten zur Fortschreibung und Weiterentwicklung der Vorschriften und zur Einführung spezieller sicherungstechnischer Anlagen und technischer Abhängigkeiten wie der bereits erwähn-

ten Signalabhängigkeit und Zugbeeinflussungssystemen. Sicherheit war ein übergeordnetes Ziel der Staatsbahnen, das sich in einem regelwerksbasierten Ansatz ausdrückte, der anlassbezogen einem ständigen Verbesserungsprozess unterlag. Systematische Risikoanalysen waren dabei eher selten. Dieser regelwerksbasierte Ansatz ist auch heute noch in den grundlegenden Bestimmungen der Eisenbahn-, Bau- und Betriebsordnung enthalten (siehe Text auf Folie 5). Die Anforderungen der Sicherheit gelten dann als erfüllt, wenn alle Regeln (gesetzliche und untergesetzliche Regelwerke) eingehalten sind. Bei Abweichungen von diesen Regeln muss mindestens die gleiche Sicherheit wie bei Einhaltung der Regeln erreicht werden, d. h. neue, nicht geregelte Techniken müssen dasselbe Sicherheitsniveau erreichen wie bestehende, durch Regeln abgedeckte Systeme. Hieraus ergibt sich das wesentliche und einzig gesetzlich geregelte Risikoakzeptanzkriterium, das heute auch bei Risikoanalysen anzuwenden ist. Mit der Entwicklung europäischer Normen kamen neue und zusätzliche Anforderungen zur Bewertung von Risiken bei der Entwicklung von Bahntechnik auf. Insbesondere die EN 50126 fordert einen auf die Entwicklung und Beherrschung von Sicherheitsanforderungen ausgerichteten Lebenszyklus (V-Modell), der heute grundsätzlich bei jeder neuen technischen Entwicklung im Eisenbahnsystem einzuhalten ist. Hierbei sind zunächst die Risiken zu analysieren und in Bezug auf Akzeptanzkriterien werden die Sicherheitsanforderungen festgelegt (z. B. als tolerierbare Gefährdungsrate für eine Funktion), deren Umsetzung später wiederholt zu verifizieren und zu validieren ist. Die Einhaltung der aus einer Risikoanalyse abgeleiteten Sicherheitsanforderungen wird somit im gesamten Entwicklungsprozess verfolgt. Anhand der Daten aus /14/ und /15/ sind die inzwischen europäisch vorgegebenen Sicherheitsindikatoren gegeben, die zeigen, wie sich das Unfallgeschehen und damit im Umkehrschluss die Sicherheit im deutschen Eisenbahnsystem und im europäischen Vergleich entwickelt hat. Dabei ist ein leicht abnehmender Trend der Unfälle und der Unfallopfer zu erkennen, d. h. das hohe Sicherheitsniveau der Eisenbahn wird weiter verbessert. Aus der Darstellung der einzelnen Unfallarten ist weiterhin erkennbar, dass der deutlich überwiegende Teil der Unfälle auf externe Verursacher zurückgeht (insbesondere Unfälle an Bahnübergängen und der Teil der Personenunfälle, der durch unbefugtes Betreten der Bahnanlagen verursacht wird). In diesem Bereich sind risikoreduzierende Maßnahmen der Eisenbahnen selbst nur sehr begrenzt möglich.

11.2 Die Anforderungen der EU-Sicherheitsrichtlinie

Ein weiterer wesentlicher Meilenstein in den rechtlichen Vorgaben an das Eisenbahnsystem zur Gewährleistung der Sicherheit ist die Inkraftsetzung der EU-Richtlinie für die Eisenbahnsicherheit 2004/49. Hintergrund für den Erlass dieser Richtlinie ist die europaweite Öffnung der Eisenbahnnetze, die durch mehr Wettbewerb die Attraktivität des Verkehrsträgers Schiene und damit eine Verkehrsverlagerung auf die Schiene fördern soll. Durch diese Öffnung der Schienennetze entsteht jedoch eine neue Schnittstelle zwischen sehr vielen Eisenbahnverkehrsunternehmen einerseits und den Infrastrukturbetreibern andererseits sowie zwischen den unterschiedlichen Techniken, Regeln und Verfahren der einzelnen EU-Mitgliedsstaaten. Diese neuen Schnittstellen führen zwangsläufig zu einem neuen Risikopotenzial, das eben durch diese europäische Sicherheitsrichtlinie kompensiert werden soll.

Diese Richtlinie enthält folgende wesentlichen Vorgaben, die generell auf Aufrechterhaltung und Verbesserung des Sicherheitsniveaus ausgerichtet sind (siehe Bild 11.1):

- Die Eisenbahnverkehrsunternehmen und die Eisenbahninfrastrukturunternehmen müssen ein Sicherheitsmanagementsystem einrichten. Dieses Sicherheitsmanagementsystem besteht aus Prozessen und Verfahren, die die Beherrschung aller Risiken zum Ziel haben. Die grundsätzlichen Anforderungen und Inhalte der Prozesse sind in einem Anhang der Sicherheitsrichtlinie vorgegeben. Das Sicherheitsmanagementsystem muss von der Sicherheitsbehörde geprüft und zertifiziert werden. Nur bei positivem Prüfergebnis erhalten die Unternehmen eine Sicherheitsbescheinigung oder -genehmigung (alle 5 Jahre), die Voraussetzung für die Teilnahme am Eisenbahnbetrieb ist.

- Es werden gemeinsame Sicherheitsindikatoren (CSI) definiert, mit denen das erreichte Sicherheitsniveau der Unternehmen und der Mitgliedsstaaten transparent gemessen werden kann. Aus den Indikatoren soll der Handlungsbedarf für Verbesserungsmaßnahmen erkennbar sein.

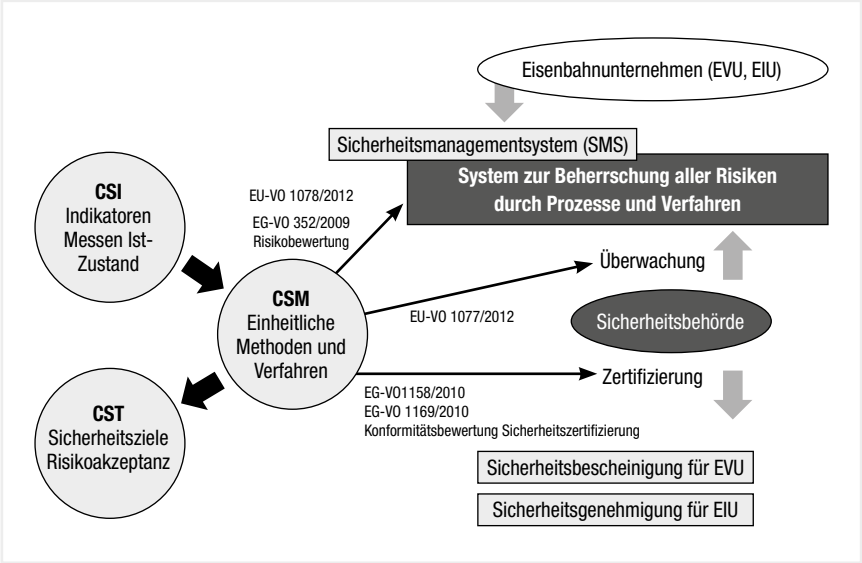

Bild 11.1: **Ziele und Inhalte der EU-Sicherheitsrichtlinie**

- Als Zielgröße für das zu erreichende Sicherheitsniveau werden gemeinsame Sicherheitsziele (CST) festgelegt, die später ggf. auch als Risikoakzeptanzkriterium herangezogen werden sollen. Gegenwärtig sind diese Ziele noch nicht einheitlich festgelegt, sondern wurden je Mitgliedsstaat spezifisch aus einem vierjährigen Mittel ausgewählter CSI abgeleitet. D. h. der mehrjährige Durchschnitt des bestehenden Sicherheitsniveaus ist das Sicherheitsziel, es ist damit nur begrenzt als Orientierungsgröße nutzbar.

- Weiterhin werden in der Sicherheitsrichtlinie gemeinsame Sicherheitsmethoden (CSM) gefordert, die die gegenseitige Anerkennung der Ergebnisse durch gleiche Verfahren in den Mitgliedsstaaten sicherstellen sollen. Die Sicherheitsrichtlinie beschreibt die Methode nicht selbst, sondern benennt nur deren Regelungsgegenstand. Die Methoden an sich werden von der europäischen Eisenbahnagentur in Sektorarbeitsgruppen ausgearbeitet und durch EU-Verordnung in Kraft gesetzt. Solche Methoden gibt es für die Erteilung der Sicherheitsbescheinigung und Sicherheitsgenehmigung durch die Sicherheitsbehörden, für die Durchführung der Überwachungsmaßnahmen

innerhalb der Eisenbahnunternehmen und durch die Sicherheitsbehörden. Schließlich gibt es eine gemeinsame Sicherheitsmethode für die Durchführung der Risikobewertung, auf die im Folgenden detailliert eingegangen wird.

- Da bis zu einer vollständigen europäischen Harmonisierung weiterhin auch nationale Regeln für die Gewährleistung der Sicherheit notwendig sind, beschreibt die Sicherheitsrichtlinie auch ein Verfahren zur Auswahl und Notifizierung nationaler Sicherheitsvorschriften. Die Umsetzung der Sicherheitsrichtlinie in nationales Recht erfolgte in Deutschland im Allgemeinen Eisenbahngesetz (AEG). Dort wird insbesondere die Notwendigkeit einer Sicherheitsbescheinigung oder Sicherheitsgenehmigung für die Eisenbahnunternehmen geregelt. Hinsichtlich der Anforderungen für eine Sicherheitsbescheinigung wird im AEG direkt auf die EU-Sicherheitsrichtlinie verwiesen, die hierfür das Sicherheitsmanagementsystem fordert. Ein geforderter Prozess im Sicherheitsmanagementsystem bezieht sich auf die Bewertung der Risiken und die Risikokontrolle bei allen technischen, betrieblichen und organisatorischen Änderungen. Im Rahmen dieses Prozesses sind die Eisenbahnunternehmen verpflichtet, die CSM zur Risikobewertung umzusetzen und damit alle Änderungen entsprechend zu behandeln (siehe Bild 11.2).

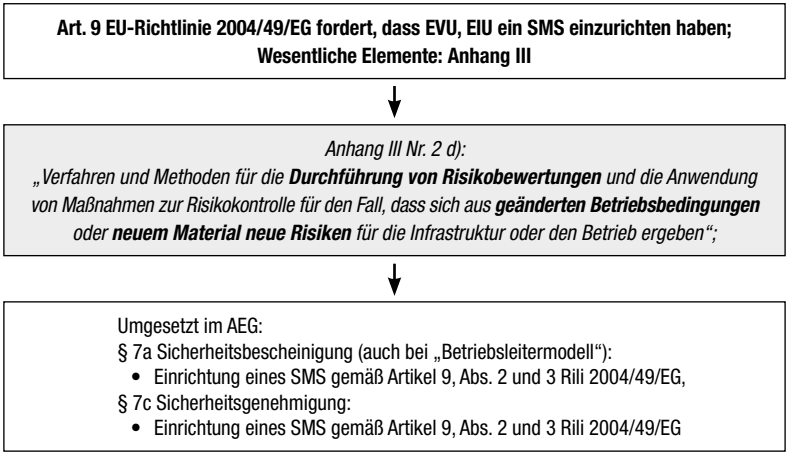

Bild 11.2: Bezug der Risikobewertung zur Sicherheitsrichtlinie

11.3 Die gemeinsame Sicherheitsmethode zur Risikobewertung CSM-RA

Im Folgenden werden das Ziel, der Inhalt und Ablauf des Verfahrens zur Evaluierung und Bewertung der Risiken nach der durch EU-Verordnung 352/2009 erlassenen gemeinsamen Sicherheitsmethode (CSM-RA) erläutert (siehe Bild 11.3).

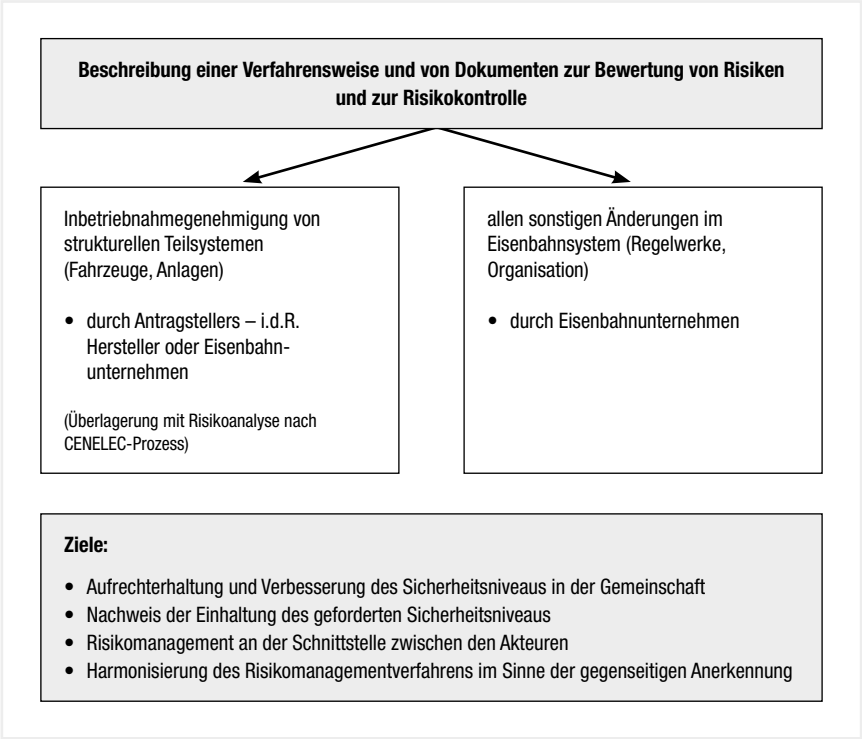

Bild 11.3: Gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken – EU-Verordnung Nr. 352/2009 (CSM-RA)

Neben den Eisenbahnunternehmen, die die Sicherheitsmethode zur Risikobewertung vor allem bei Änderungen ihrer internen Regelwerke sowie bei der Einführung neuer Technik anwenden müssen, gilt diese auch für die Antragsteller, die einen Antrag auf Inbetriebnahmegenehmigung für ein strukturelles Teilsystem nach der europäischen Interoperabilitätsrichtlinie 2008/57 stellen. Die Interoperabilitätsrichtlinie regelt insbesondere die Harmonisierung der technischen Anforderungen an die Teilsysteme der Eisenbahn (das sind Fahrzeuge, Infrastruktur, Zugsicherung, Zugsteuerung und Signaltechnik sowie Energie), um möglichst mit gleichen Anforderungen einen ungehinderten grenzüberschreitenden Verkehr und einen freien Wettbewerb der Hersteller zu gewährleisten. Da hierbei die Sicherheit eine entscheidende Randbedingung darstellt, wird in der Interoperabilitätsrichtlinie eine Inbetriebnahmegenehmigung durch die Sicherheitsbehörde gefordert, insbesondere, um die nicht harmonisierten Anforderungen und die Integration in das bestehende Eisenbahnsystem zu prüfen und somit das Sicherheitsniveau aufrechtzuerhalten bzw. zu steigern. Für die vergleichbare Bewertung der Risiken im Betrachtungsfeld der Inbetriebnahmegenehmigung ist ebenfalls zwingend die Sicherheitsmethode zur Risikobewertung anzuwenden. Sie ist hier aber mit der bisher nach CENELEC-Normen durchzuführenden Risikoanalyse teilweise identisch, d. h. es können durchaus gleiche Arbeitsschritte und Dokumente verwendet werden. Durch die CSM zur Risikobewertung bei einer Inbetriebnahmegenehmigung soll neben den oben genannten Zielen auch eine leichtere gegenseitige Anerkennung der Ergebnisse durch ein harmonisiertes Verfahren erreicht werden. Außerdem soll sichergestellt werden, dass Sicherheitsanforderungen, die nicht durch einen Beteiligten allein beherrscht werden können, den jeweiligen anderen Beteiligten systematisch zugewiesen werden (d. h. Abgrenzung der Verantwortung an den Schnittstellen).

Die CSM-RA sieht zunächst eine Vorprüfung vor, ob die beabsichtigte Änderung oder Inbetriebnahme des strukturellen Teilsystems sicherheitsrelevant und signifikant ist (siehe Bild 11.4). Damit soll das sehr aufwendige Risikomanagementverfahren bei einfachen Sachverhalten und Entscheidungen vermieden werden. Bei einer nicht sicherheitsrelevanten oder nicht signifikanten Änderung darf dann ein beliebiges, nicht geregeltes Verfahren zum Nachweis der ausreichenden Sicherheit angewendet werden. Die Entscheidung über die nicht gegebene Signifikanz und Sicherheitsrelevanz ist dann aber mit einer entsprechenden Begründung zu dokumentieren, so dass sie auch später für die behördliche Überprüfung nachvollziehbar ist.

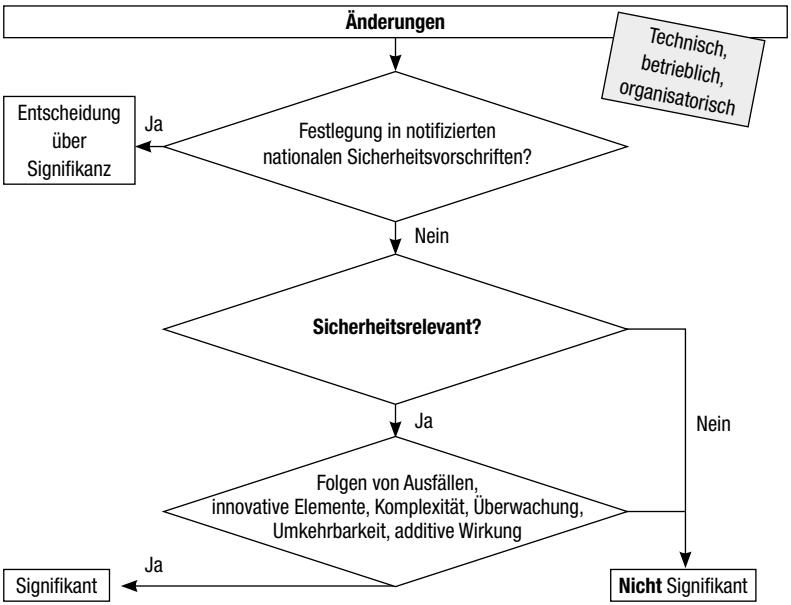

Bild 11.4: **Bestimmung der Signifikanz nach CSM-RA**

In der Praxis führt die Nicht-Signifikanz aber oft dazu, dass keine weitere Sicherheitsbetrachtung durchgeführt wird, was weder durch die CSM-RA noch durch nationale Rechtsvorschriften legitimiert ist. Bei einer behördlichen Überprüfung wird bei einer festgestellten Abweichung von Regelwerken dann mindestens ein Nachweis der gleichen Sicherheit nachgefordert.

Die Signifikanzentscheidung muss sich an den folgenden Kriterien orientieren:
- Folgen von Ausfällen (Was kann schlimmstenfalls passieren?)
- Innovative Elemente (Ist etwas neu ohne Erfahrungswerte?)
- Komplexität der Änderung
- Überwachung (Sind Überwachungsmaßnahmen zur Risikokontrolle möglich?)
- Umkehrbarkeit der Änderung (Kann die Änderung ohne Weiteres zurückgenommen werden?)
- Additive Wirkung (Wirkung mehrerer Änderungen im System gleichzeitig)

Bei der Signifikanzprüfung müssen zu allen diesen Kriterien Aussagen getroffen werden. Es fehlt in der CSM-Verordnung jedoch jegliche Vorgabe, bei welcher Ausprägung der Kriterien Signifikanz vorliegt oder keine Signifikanz vorliegt. Insofern besteht noch Verbesserungspotenzial, denn damit kann der Verantwortliche für die Risikobewertung, das ist derjenige, der in seinem Zuständigkeitsbereich die Änderung vornimmt, selbst nach eigener Interpretation der Kriterien entscheiden, ob eine Signifikanz vorliegt. Dies führt in der Praxis oft zu einer freizügigen Interpretation der Kriterien dahingehend, dass keine Signifikanz vorliegt. Damit wird dann die systematische Analyse der Risiken umgangen, sofern nicht gleichzeitig eine Risikoanalyse nach EN 50126 durchgeführt wird.

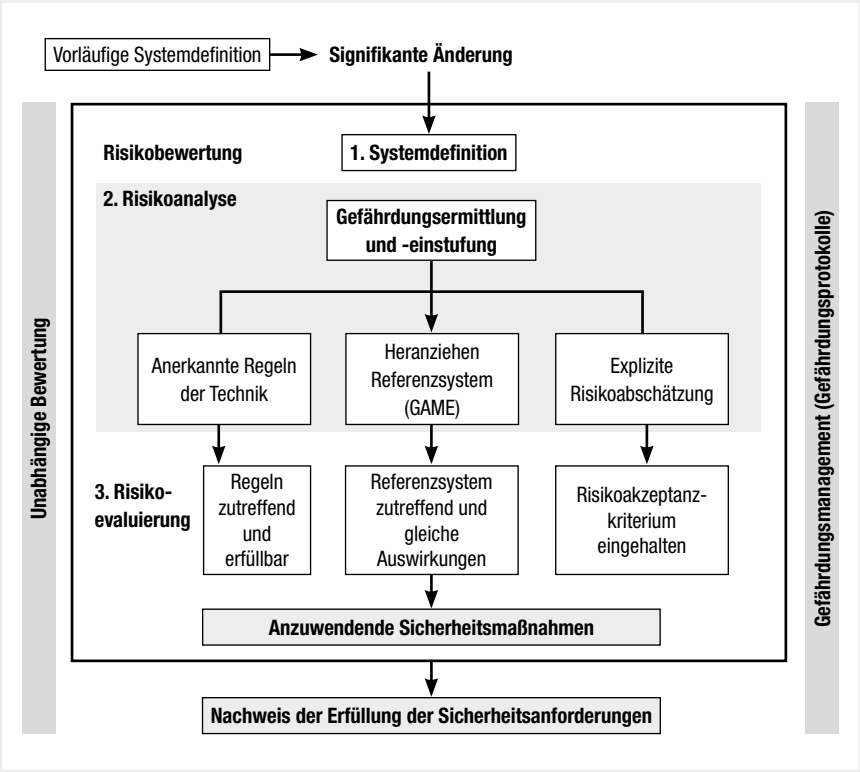

Bild 11.5: Risikomanagementverfahren nach CSM-RA

Wenn eine Signifikanz vorliegt, muss das Risikomanagementverfahren, wie in Bild 11.5 zusammenfassend dargestellt, durchgeführt werden. Das Verfahren beginnt mit einer Systemdefinition, in der die Grenzen des betrachteten Systems und seine Bestandteile festgelegt werden. Die Systemdefinition ist wichtig, um die Betrachtung innerhalb des Gesamtsystems der Eisenbahn in einer beherrschbaren Größenordnung zu halten, innerhalb der die betrachtete Änderung stattfindet. Die Abgrenzung ist auch wichtig für die Anwendbarkeit eines Vergleichssystems bzw. für die Gültigkeit eines Risikoakzeptanzkriteriums. In der Systemdefinition wird auch festgelegt, welche Randbedingungen als gegeben vorausgesetzt werden, z. B. die Anwendung bestimmter Regelwerke, die für die weitere Betrachtung gültig sind. Im Folgenden werden nur noch die Risiken betrachtet, die innerhalb der Systemgrenze oder durch Wechselwirkung des Systems mit der Umgebung entstehen.

Ausgehend von der Systemdefinition werden anschließend in der Gefährdungsidentifikation alle Gefährdungen ermittelt, die durch das System oder seine Wechselwirkung mit der Umwelt entstehen können. Hierbei sollen systematische Verfahren, wie z. B. eine Fehlerart- und -auswirkungsanalyse (FMEA) verwendet werden. Grundsätzlich müssen hierfür alle Zustände des Systems und alle Funktionen betrachtet werden und es muss zu jedem denkbaren Ausfall und jedem denkbaren Fehler festgestellt werden, welche Gefahren daraus entstehen können. Die Wahrscheinlichkeit der Gefährdung darf zunächst noch keine Rolle spielen. Es ist weitverbreitete Praxis, dass dieser Schritt in einem Expertenteam ausgeführt wird. Alle ermittelten Gefährdungen sind in einem Gefährdungsprotokoll zu erfassen. Anschließend besteht die Möglichkeit, Gefährdungen, die als sehr unwahrscheinlich oder weitgehend akzeptabel angenommen werden, mit einer entsprechenden Begründung aus der weiteren Betrachtung auszuschließen. In einem nächsten Schritt werden zu jeder Gefährdung im Gefährdungsprotokoll geeignete Abwehrmaßnahmen bzw. Schutzmaßnahmen festgelegt. Dies sind, soweit vorhanden und anwendbar, Maßnahmen aus den vorhandenen Regelwerken. Liegen keine Regelwerke vor, sind erstmals geeignete Maßnahmen vorzuschlagen, die dem Schadensausmaß oder der Eintrittswahrscheinlichkeit der Gefährdung entgegenwirken.

Anschließend muss für jede Gefährdung anhand von 3 Prinzipien zur Risikoakzeptanz, auf die nachfolgend eingegangen wird, festgestellt werden, ob diese akzeptabel sind:

- Anwendung von anerkannten Regeln der Technik,
- Vergleich mit einem Referenzsystem,
- explizite Risikoabschätzung.

Sind die Gefährdungen aufgrund der vorgeschlagenen Maßnahmen und der Akzeptanzprinzipien akzeptabel, sind die Maßnahmen als Sicherheitsanforderung umzusetzen, anderenfalls muss in einem iterativen Verfahren nach weiteren Maßnahmen gesucht werden.

Die Erfüllung der Sicherheitsanforderungen muss im weiteren Verlauf der technischen Entwicklung und vor der Inbetriebnahme wiederholt geprüft und bewertet (Verifizierung und Validierung) und z. B. in einem Sicherheitsnachweis bestätigt werden. Auch nach der Inbetriebnahme muss durch Überwachungsmaßnahmen die Wirksamkeit der Sicherheitsmaßnahmen geprüft werden.

Die gesamte Durchführung des Risikomanagementverfahrens muss durch eine unabhängige Bewertungsstelle überprüft werden. Die unabhängige Bewertung soll bestätigen, dass alle Verfahrensgrundsätze richtig umgesetzt wurden und dass auch die Entscheidungen im Verfahren angemessen und richtig erscheinen. Hierzu erstellt die unabhängige Bewertungsstelle einen Sicherheitsbewertungsbericht, der auch die Behörden bei der Zulassung der Technik entlasten soll. Die Überprüfung durch eine unabhängige Bewertungsstelle soll das Vertrauen in das Risikomanagement erhöhen und Fehler und Beeinflussungen des Ergebnisses durch den Vorschlagenden vermeiden. Die unabhängige Bewertungsstelle muss hierzu eine besondere Fachkunde und Methodenkompetenz nachweisen, künftig ist hierfür ein formales Anerkennungsverfahren vorgeschrieben.

11.4 Die Prinzipien der Risikoakzeptanz nach CSM-RA

Das einfachste und naheliegendste Risikoakzeptanzprinzip ist die Einhaltung von anerkannten Regeln der Technik (siehe Bild 11.6). Wenn für eine identifizierte Gefährdung bereits darauf ausgerichtete Regeln (Vorschriften, Produktnormen) vorliegen, die allgemein bekannt und zugänglich sind und die sich in der Praxis bewährt haben, können diese Regeln angewendet werden und die Gefährdung ist damit akzeptiert. Keine weiteren Maßnahmen sind notwendig. Dieses Prinzip stimmt mit dem eingangs zitierten § 2 Abs. 1 der EBO überein. Es muss bei Anwendung der anerkannten Regeln der Technik als Akzeptanzkriterium lediglich ein Zusammenhang herstellbar und begründbar sein, dass die Regel zur Beherrschung der jeweiligen Gefährdung geeignet und dafür vorgesehen ist. Bei dem historisch gewachsenen Regelwerk der Eisenbahn ist eine Zuordnung der Regeln zu konkreten Gefährdungen aber meist nicht vorhanden. Der Zusammenhang muss somit bei erstmaliger Anwendung erst durch fachkundige Analyse des Regelungsinhalts hergestellt werden. Mit fortlaufender praktischer Anwendung haben sich bei der DB sog. Gefährdungslisten herausgebildet, in der die typischen Gefährdungen des Eisenbahnsystems bzw. der einzelnen Fachbereiche und die zu ihrer Beherrschung vorhandenen Regelwerke zusammengefasst sind. Diese Listen werden dann zur Gefährdungsidentifikation und zur Ableitung geeigneter anerkannter Regeln der Technik bei den verschiedenen Risikobewertungen immer wieder ausgewertet.

Definition:
schriftlich festgelegte Regeln, die bei ordnungsgemäßer Anwendung dazu dienen können, eine oder mehrere spezifische Gefährdungen zu kontrollieren.

Anforderung an anerkannte Regeln der Technik:

- im Eisenbahnsektor allgemein bekannt oder begründet und für die Bewertungsstelle akzeptabel
- für die Kontrolle der betreffenden Gefährdungen in dem zu bewertenden System zutreffend
- allen Akteuren, die sie anwenden wollen, öffentlich zugänglich

Risiken aus Gefährdungen*, die durch anerkannte Regeln der Technik abgedeckt werden,* **sind vertretbar:**

- Das Risiko muss nicht weiter analysiert werden
- Anwendung der anerkannten Regel der Technik wird Sicherheitsanforderung im Gefährdungsprotokoll

Bild 11.6: Risikoakzeptanzkriterium anerkannte Regeln der Technik

Wenn anerkannte Regeln der Technik nicht vorhanden sind oder davon abgewichen werden soll, kommt als weiteres Prinzip der Risikoakzeptanz der Vergleich mit einem Referenzsystem infrage. Hierbei ist ein anderes System zu suchen, das vergleichbare Eigenschaften wie das Bezugssystem hat, das sich in der Praxis bewährt hat und das aktuell noch zulassungsfähig ist. Auch sollten der rechtliche Rahmen und das Niveau der Risikoakzeptanz, z. B. durch den Grad der Selbstbestimmung, übertragbar sein. Ein Vergleich zwischen Eisenbahn und Straßenverkehr ist wegen der viel stärkeren Selbstbestimmung im Straßenverkehr nicht angemessen. Vergleiche zwischen Luftverkehr und Eisenbahnverkehr oder zwischen verschiedenen vorhandenen technischen Lösungen innerhalb des Eisenbahnverkehrs erscheinen durchaus möglich. Wenn die Vergleichbarkeit mit dem Referenzsystem begründet ist, können die Sicherheitsmaßnahmen oder Sicherheitsregeln des Referenzsystems (z. B. aus einem dort bereits vorhandenen Gefährdungsprotokoll oder aus einem Sicherheitsnachweis) auf das Betrachtungssystem übertragen werden, wobei die Risiken damit als akzeptiert gelten. Es ist bei Anwendung des Referenzsystems auch möglich, qualitativ oder quantitativ auf Systemebene zu begründen, dass die Gefährdungen durch Maßnahmen mit einem vergleichbaren Sicherheitsniveau abgedeckt werden.

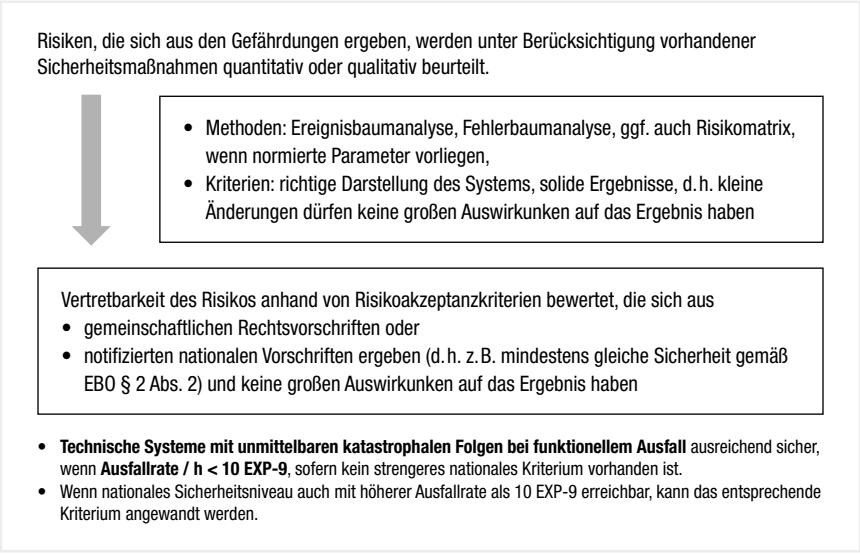

Bild 11.7: **Kriterium: explizite Risikoabschätzung**

Wenn auch kein Referenzsystem zur Verfügung steht, muss eine sogenannte explizite Risikoabschätzung durchgeführt werden (siehe Bild 11.7). Hierzu wird die betreffende Gefährdung unter Berücksichtigung der Wirkung aller Sicherheitsmaßnahmen und weiterer Reduktionsfaktoren qualitativ (z.B. mit einer Häufigkeits-Konsequenzenmatrix) oder quantitativ mittels einer Fehlerbaumanalyse (siehe Bild 11.8) oder einer Folgenanalyse (Ereignisbaumanalyse – siehe Bild 11.9) bewertet. Die ermittelten Risiken aus einem Fehlerbaum oder Ereignisbaum werden dann mit einem Risikoakzeptanzkriterium verglichen. Wenn die ermittelten Risiken kleiner sind als das Risikoakzeptanzkriterium, ist die Gefährdung akzeptiert. Nicht trivial ist hierbei die Auswahl eines geeigneten Risikoakzeptanzkriteriums, dieses muss zwingend durch das jeweilige Rechtssystem akzeptiert sein. Im deutschen Eisenbahnsystem ist bisher gemäß EBO § 2 Abs. 2 nur ein Risikoniveau erlaubt, das vergleichbar ist mit dem, das sich bei Anwendung der anerkannten Regeln der Technik ergibt. Nach CSM-RA ist bei Ausfall von technischen Systemen mit katastrophalen Folgen eine Ausfallrate von 10^{-9}/h im europäischen Eisenbahnsystem grundsätzlich akzeptiert. Dieses Kriterium darf jedoch nur angewendet werden, wenn es national kein schärferes Kriterium gibt. In Bezug auf das oben genannte deutsche Kriterium

aus der EBO ist hierbei immer eine Einzelfallprüfung erforderlich, d. h. es muss festgestellt werden, ob das Sicherheitsniveau der anerkannten Regeln der Technik nicht höher ist als 10^{-9}/h. Dies kann insbesondere bei hoch sicheren Systemen der Signaltechnik nach Analyse der real existierenden Systemarchitekturen und technischen Lösungen durchaus der Fall sein.

Künftig könnten durch die europäische Rechtssetzung mit den oben erwähnten gemeinsamen Sicherheitszielen aus der Sicherheitsrichtlinie (Commen Safety Targets – CST) durchaus weitere Risikoakzeptanzkriterien geschaffen werden.

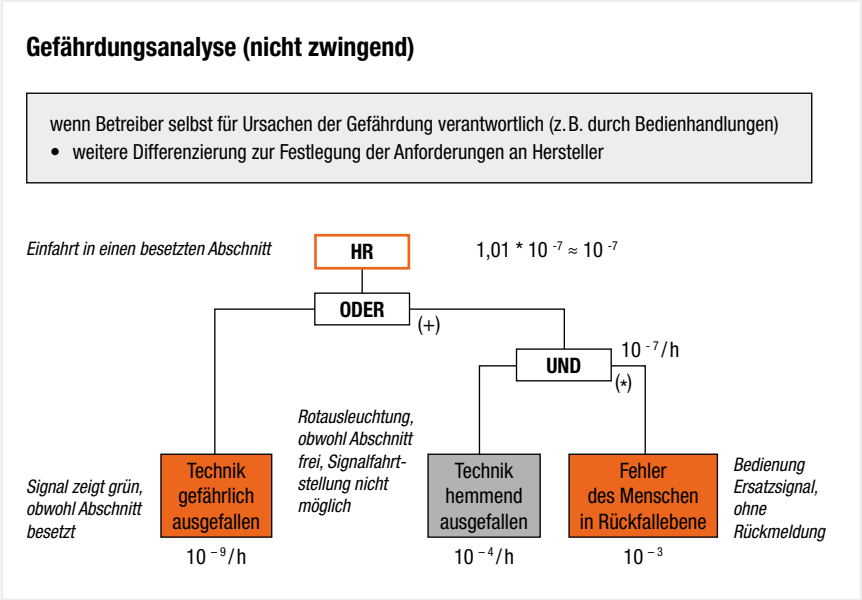

Bild 11.8: **Vorgehen bei expliziter Risikoabschätzung: Gefährdungsanalyse**

Weitere Risikoakzeptanzkriterien sind in der bereits vor Einführung der CSM-RA gültigen EN 50126 beispielhaft genannt (Bild 11.10). Die beispielhafte Nennung erlaubt jedoch nicht die Anwendung in allen Ländern oder in allen Fällen. Typisch für das britische Eisenbahnsystem ist das ALARP-Prinzip, in dem die Risiken in einem sog. ALARP-Bereich liegen und innerhalb dieses Bereiches soweit reduziert werden müssen, wie die Risikominderungen verhältnismäßig sind. Für die Verhältnismäßigkeit spielen Kosten-Nutzen-Betrachtungen und der Wert des Lebens durchaus eine Rolle. Nachteilig ist, dass eine genaue und nachvollziehbare Definition des ALARP-Bereiches nicht vorgenommen wird. Eine Anwendung dieses Akzeptanzkriteriums im deutschen Eisenbahnwesen ist nicht üblich, da kein Bezug zu dem Risikoakzeptanzkriterium nach EBO § 2 Abs. 2 herstellbar ist. Auch das MEM-Kriterium bildet diese rechtliche Vorgabe nicht hinreichend ab. Es kann deshalb nur dann in Deutschland angewendet werden, wenn für eine identifizierte Gefährdung bzw. ein Risiko bisher keinerlei Regelwerke greifbar sind, aus denen ein Bezugsniveau abgeleitet werden könnte, d. h. das Risiko bisher nicht erkannt und oder unbewusst akzeptiert wurde und nach erstmaliger Identifizierung oder nach einem allgemein nicht akzeptierten Ereignis eine sinnvolle Begrenzung gesucht wird. Das MEM-Kriterium leitet aus einem statistisch nachgewiesenen Todesfallrisiko durch Einwirkung technischer Systeme (z. B. $2 \cdot 10^{-4}$/a nach EN 50126), das auf den Anteil des betrachteten Systems heruntergebrochen wird bzw. an dem ein neu eingeführtes System nur einen marginalen Anteil haben darf, ein akzeptables Risiko ab. Im Eisenbahnwesen sind dennoch einige Beispiele für die Anwendung des MEM-Kriteriums bekannt.

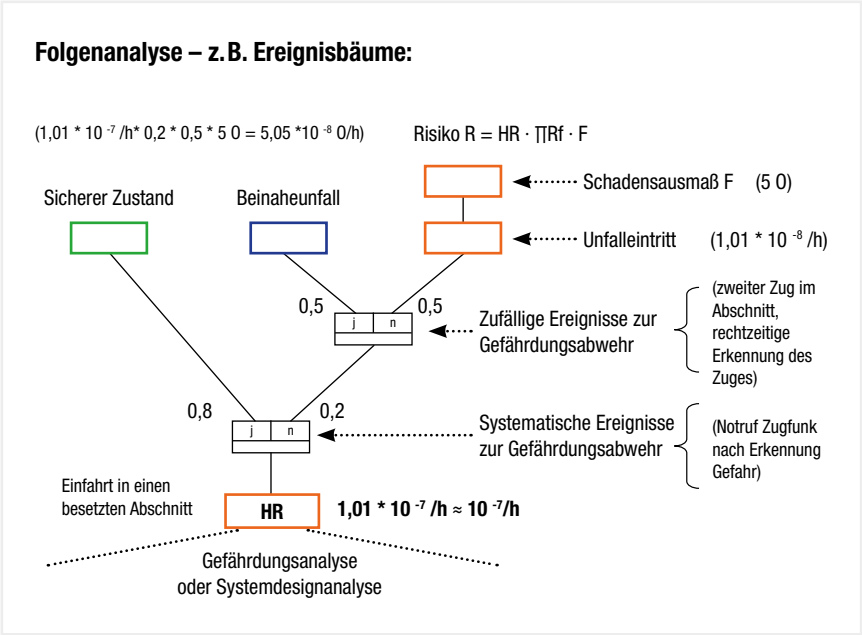

Bild 11.9: **Vorgehen bei expliziter Risikoabschätzung: Folgenanalyse**

Am besten für das deutsche Rechtssystem ist das GAMAB-Prinzip geeignet, wonach das Sicherheitsniveau der zu betrachtenden oder der neuen Systeme mindestens so hoch sein muss, wie das Sicherheitsniveau eines vergleichbaren bestehenden Systems (Bild 11.11). Dieses Prinzip wird auch in der CSM-RA beim Vergleich mit dem Referenzsystem ausdrücklich erwähnt. Es lässt sich weiterhin als Risikoakzeptanzkriterium auf eine explizite Risikoanalyse übertragen,

Bewertung der Risiken bei expliziter Risikoabschätzung:

Risikoakzeptanzkriterien nach EN 50126

ALARP – (As Low As Reasonably Practicable)
Nutzen-Kosten-Betrachtung, Risiken sind auszuschließen, sofern Kosten dazu nicht unverhältnismäßig

- Kein einheitlicher Bewertungsmaßstab,
- für deutsche Sicherheitsanforderungen (EBO) nicht geeignet

MEM – (Minimum Endogenous Mortality)
Ermittlung des akzeptierten Niveaus für das technische System anteilmäßig aus tatsächlicher Todesfallrate einer repräsentativen Person

- externe Vorgabe eines akzeptierten Risikos einheitlich und sinnvoll,
- problematisch ist Aufteilung auf die einzelnen Systeme,
- für deutsche Sicherheitsanforderungen (EBO) nicht geeignet

Bild 11.10: Vorgehen bei expliziter Risikoabschätzung: Risikoakzeptanzkriterien

da das Risiko eines bestehenden Systems anhand der Unfallzahlen messbar ist und damit als Zielwert auf eine explizite Risikoanalyse übertragen werden kann. Wenn man als vergleichbares bestehendes System ein System definiert, das weitgehend den anerkannten Regeln der Technik entspricht, kommt man damit auch auf das bereits viel zitierte Akzeptanzkriterium im § 2 Abs. 2 EBO. Für die Nutzung dieses Risikoakzeptanzkriteriums bei expliziten Risikoanalysen stehen grundsätzlich zwei Wege zur Verfügung, die im deutschen Eisenbahnsektor häufig gerade bei Risikoanalysen zu technischen Systeminnovationen angewendet werden:

1. Es wird das Risiko des bestehenden Systems anhand von Unfallstatistiken bestimmt. Die Auswahl der relevanten Unfälle muss sich dabei an der Systemdefinition des Betrachtungssystems orientieren. Die Unfälle müssen dabei detailliert betrachtet werden, um solche Unfälle, die einen offensichtlichen Verstoß gegen anerkannte Regeln der Technik zur Ursache haben und die folglich nicht akzeptiert sind, auszuschließen. Weiterhin werden in der

Regel Großereignisse, die mit einer Risikoaversion in Verbindung stehen, ausgeschlossen. Der langjährige Mittelwert der verbleibenden Unfälle stellt das Akzeptanzkriterium dar.

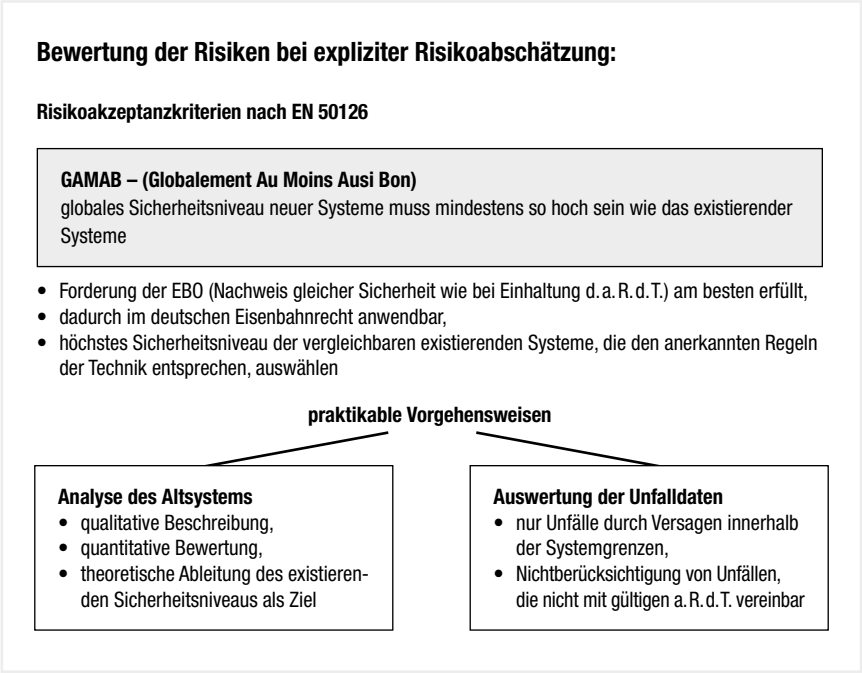

Bild 11.11: Risikoakzeptanzkriterien nach EN 50126

2. Es wird zunächst mit einer Ursachenanalyse und/oder Folgenanalyse (Ereignisbaumanalyse) das Risiko des bestehenden Systems ermittelt. Dabei wird ebenfalls auf Ereignisauswertungen oder Expertenschätzungen zurückgegriffen. Das abgeleitete Risiko ist das Bezugsrisiko, das dem Bezugssystem zugrunde gelegt wird.

Die Abläufe des Bezugssystems werden dann in separaten Fehlerbäumen oder Ereignisbäumen dargestellt. Mit den sich dort ergebenden funktionalen Abhängigkeiten kann aus dem bekannten Bezugsrisiko nach 1. oder 2. durch Rückrechnung z. B. eine tolerierbare Gefährdungsrate als Sicherheitsziel errechnet werden.

11.5 Beispiele für Risikoanalysen im Eisenbahnbereich und Erfahrungen

Im Folgenden wird die Anwendung der vorstehend beschriebenen Analyseverfahren an drei Beispielen aus der Praxis beschrieben. Alle Beispiele beziehen sich noch auf die Vorgaben zu einer Risikoanalyse nach EN 50126 bei Einführung eines neuen Systems. Die Systemdefinition, die Gefährdungsidentifikation, die Risikoevaluierung anhand einer expliziten Risikoanalyse und der Nachweis der Einhaltung der Sicherheitsanforderungen würden jedoch auch den Anforderungen der CSM-RA entsprechen. Lediglich eine unabhängige Bewertung durch eine Bewertungsstelle wurde nicht durchgeführt.

Bei der Risikoanalyse zur Einführung des Elektronischen Buchfahrplans (EBULa) (siehe Bild 11.12) ging es um den Ersatz der gedruckten Buchfahrpläne auf dem Führerstand, aus dem der Triebfahrzeugführer z. B. die zulässige Geschwindigkeit, die Signalstandorte, die Grenzen der Weichenbereiche und die Fahrzeiten durch eine tabellarische Bildschirmanzeige entnimmt. Die Daten werden nach Eingabe der Zugnummer automatisch aufgerufen. Als Risikoakzeptanzkriterium wurde das Risiko des alten Verfahrens, das durch Betriebsvorschriften und damit durch anerkannte Regeln der Technik beschrieben war, herangezogen. In Fehlerbaumanalysen wurden die menschlichen Fehler beim Erstellungsprozess der Buchfahrpläne analysiert und quantifiziert. Anschließend wurden die Fehler bei der Dateneingabe, der Datenverteilung und der finalen Bearbeitung im Bordgerät bei dem neuen Verfahren betrachtet. Für die noch nicht festgelegten Werte der technischen Verarbeitung wurden aus dem Bezugsrisiko tolerable Gefährdungsraten abgeleitet, die von ihrer Größenordnung im Bereich eines SIL=0 lagen und damit keine besonderen technischen Maßnahmen erforderten und mit PC-Technik erreicht werden konnten /12/. Die Einhaltung dieser Werte wurde schließlich in einem langjährigen Probebetrieb noch ohne Sicherheitsverantwortung (mit Parallelnutzung des gedruckten Buchfahrplans und EBuLa) nachgewiesen (vgl. Bild 11.12, dortige Bilder aus /8/).

1.

- Analyse des Altsystems mit gedrucktem Buchfahrplan und menschlichem Fehler im Erstellungsprozess durch Fehlerbäume
- Das dabei entstehende Risiko ist Bezugsrisiko – Risikoakzeptanzkriterium

2.

- Analyse des neuen Systems mit Fehlerbäumen bei Dateneingabe und Datenverarbeitung, bei denen Risiko des Altsystems theoretisch eingehalten werden musste (Gefährdungsraten im Bereich von SIL=0)
- Nachweis der Einhaltung praktisch durch Probebetrieb ohne Sicherheitsverantwortung

Bild 11.12: **Beispiel I für Risikoakzeptanz bei expliziter Risikoabschätzung**

Bei der Risikoanalyse zur Geschwindigkeitserhöhung bei Bahnsteigvorbeifahrten mit 230 km/h war nachzuweisen, dass die zusätzlich getroffenen Schutzmaßnahmen für die Reisenden auf dem Bahnsteig als Vorkehrungen ausreichend sind, um einen Aufenthalt von Reisenden im Gefahrenbereich zu vermeiden und um das Sicherheitsniveau gegenüber den bisher üblichen Bahnsteigvorbeifahrten mit 200 km/h nicht zu reduzieren (Bild 11.13). Hierzu wurde das bestehende Bezugsrisiko bei Bahnsteigvorbeifahrten mit 200 km/h zunächst aus den Unfallstatistiken unter Berücksichtigung der Unfälle, die der Systemdefinition entsprechen, ermittelt. Einzelne nicht klar zuordenbare Unfälle bzw. solche, bei denen Regelwerksverstöße zu vermuten waren, wurden ausgeschlossen. Anschließend wurde für das Nachweissystem die Verbreiterung des Gefahrenbereichs am Bahnsteig bei Vorbeifahrten mit 230 km/h durch aerodynamische Untersuchungen ermittelt. Danach wurde die größere Aufenthaltswahrscheinlichkeit der Reisenden in dem verbreiterten Gefahrenbereich durch Umrechnung aus einem beobachteten Ist-Zustand abgeleitet. Aus der potenziell größeren Reisendenanzahl im Gefahrenbereich ergibt sich eine Erhöhung des Unfallrisikos. Abschließend wurde durch Expertenschätzung die Wirkung der Absperrmaßnahmen zur Reduzierung der Reisenden im

Gefahrenbereich und damit zur Reduzierung des Risikos bewertet. Es musste schließlich gezeigt werden, dass die Maßnahmen so wirksam sind, dass das Risiko mit den Maßnahmen kleiner ist als das Bezugsrisiko (im Sinne eines Sicherheitszuschlags wegen Ungenauigkeiten). Nach der theoretischen Analyse wurde die Richtigkeit der Betrachtung im Rahmen einer Betriebserprobung mit verstärkten Kontrollmaßnahmen im Sinne eines ergänzenden Nachweises zur Wirksamkeit der Sicherheitsanforderungen überprüft (Beschreibung des Verfahrens /9/, Skizze der Maßnahmen aus /10/)

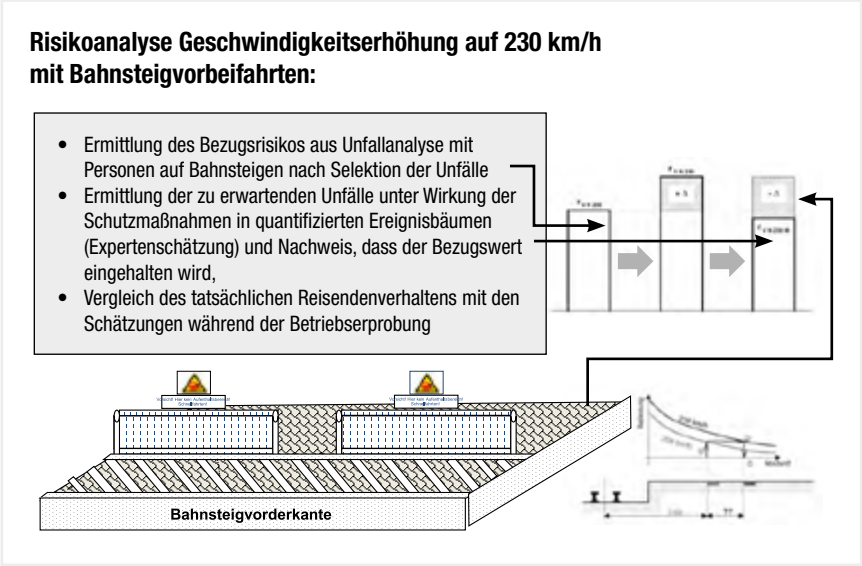

Bild 11.13: **Beispiel II für Risikoakzeptanz bei expliziter Risikoabschätzung**

Bei der Risikoanalyse zur Wirbelstrombremse war nachzuweisen, dass die Gefährdung durch eine nicht abgeschaltete Wirbelstrombremse eines ICE 3 auf einer nicht ertüchtigten Umleitungsstrecke zu keiner unzulässigen Risikoerhöhung führt (Bild 11.14). Die Gefährdung ergibt sich ausschließlich bei der Einschaltung von Bahnübergängen (BÜ) mit Fernüberwachung, weil hierbei nicht ertüchtigte Schienenkontakte durch die Wirbelstrombremse unerkannt zerstört werden können und die Sicherung des Bahnübergangs für den folgenden Zug nicht aktiviert wird. Zur Ermittlung des Risikos wurden zunächst die betrieblichen Abläufe mit ihren Fehlern, die zur Nichtabschaltung der Wirbel-

strombremse führen können, in Verbindung mit der Wahrscheinlichkeit einer Bremsung in einer Einschaltstrecke eines BÜ in Ereignisbäumen dargestellt. Das sich hieraus ergebende Risiko war zwar sehr gering, stellte aber dennoch eine geringfügige Erhöhung gegenüber dem bisherigen Zustand dar /13/. Dieses Risiko wurde in Relation zum tatsächlichen Risiko an Bahnübergängen gebracht, womit gezeigt werden konnte, dass dieser Anteil tatsächlich marginal und somit vernachlässigbar ist. Eine Erhöhung des Risikos im System wurde zusätzlich dadurch ausgeschlossen, dass permanent Maßnahmen zur Erhöhung der Sicherheit an BÜ bzw. zur Beseitigung von BÜ durchgeführt werden, deren Risikoreduktion deutlich über der marginalen Risikozunahme liegt.

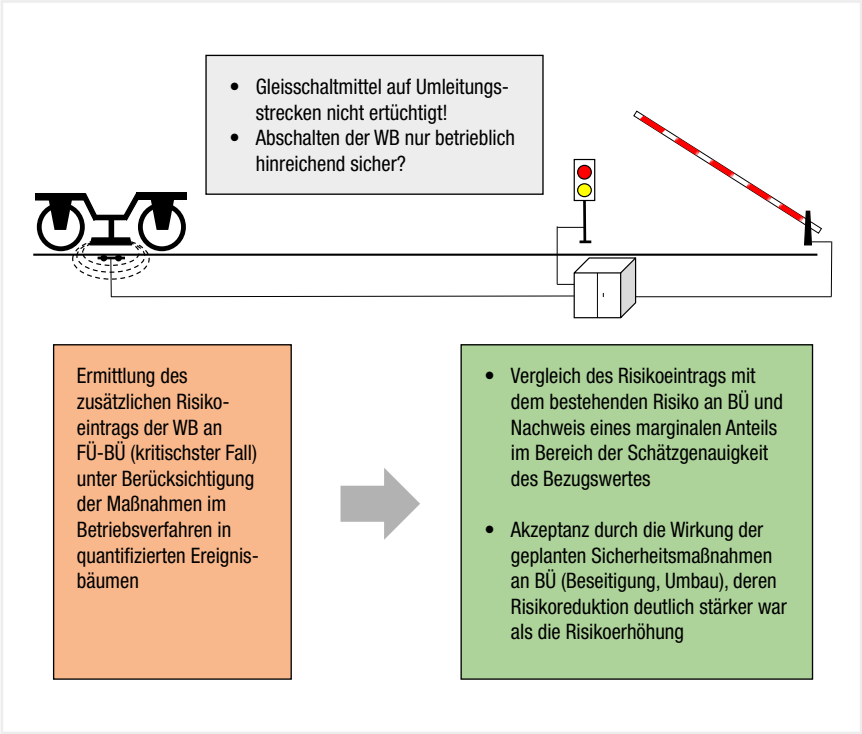

Bild 11.14: **Risikoanalyse – Wirbelstrombremse (WB)**

In den vorstehend beschriebenen Risikoanalysen waren auch menschliche Fehler zu erfassen. Eine eisenbahnspezifische Methodik zur Bewertung des menschlichen Fehlers wurde durch die Dissertation von Hinzen geschaffen (Bild 11.15 aus /11/). Hierbei werden die Umweltbedingungen, das Stressniveau und die Komplexität der Handlungen als Eingangsgrößen beschrieben. Eine möglichst exakte Beschreibung und Bewertung des menschlichen Handelns durch eine wissenschaftlich begründete Methodik ist für die Vertrauenswürdigkeit der Risikoanalysen eine wichtige Grundlage. Dabei ist zu berücksichtigen, dass die menschlichen Fehler einen hohen Beitrag zum Unfallgeschehen im Eisenbahnwesen leisten, sodass die Reduzierung der unmittelbar vom Menschen ausgeführten Aufgaben einen Beitrag zur weiteren Verbesserung der Sicherheit leisten kann, den es durch Risikobetrachtungen zu identifizieren gilt.

Die Ergebnisse von Risikoanalysen dürfen jedoch nicht als „ewige Wahrheit“ bzw. als feststehende Vorgaben betrachtet werden. Sie sind ein notwendiges und sinnvolles Hilfsmittel zur Bestimmung der Sicherheitsanforderungen am Beginn des Entwicklungsprozesses. Ihre Aussagen enthalten oft Ungenauigkeiten aufgrund von Schätzungen und können auch durchaus bewusst in eine bestimmte Zielrichtung gelenkt werden. Neben zu optimistischen Schätzungen liegen nach den Erfahrungen des Eisenbahn-Bundesamtes Fehlermöglichkeiten auch in der nicht gegebenen Unabhängigkeit von Ereignissen und in der falschen Verknüpfung von Größen, wenn die Einheiten nicht zueinander passfähig sind. Ein rechtlich fragwürdiges Risikoakzeptanzkriterium kann ebenfalls zu einem falschen Ergebnis führen. Es ist deshalb sinnvoll, dass Risikoanalysen von einer unabhängigen Bewertungsstelle oder einer Behörde kritisch geprüft werden und dass die Gefährdungsprotokolle auch mit den Erkenntnissen aus der Überwachung des Ist-Zustandes fortgeschrieben werden, wie es durch die CSM-RA gefordert wird.

Menschliche Verhaltensebene	Günstige Umweltbedingungen			Ungünstige Umweltbedingungen		
	Stress durch Unterforderung	Optimales Stressniveau	Stress durch Überforderung	Stress durch Unterforderung	Optimales Stressniveau	Stress durch Überforderung
fertigkeitsbasiert	$2 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$2 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	$5 \cdot 10^{-3}$	$1 \cdot 10^{-2}$
regelbasiert	$2 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	$2 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$	$1 \cdot 10^{-1}$
wissensbasiert	$2 \cdot 10^{-1}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-1}$	1,0	$5 \cdot 10^{-1}$	1,0

Bild 11.15: Bewertung der Fehlerwahrscheinlichkeit des Menschen nach Hinzen: (Eingangswerte für Risikoanalysen)

Literatur

/1/ Eisenbahn-Bau- und Betriebsordnung (EBO) – aus www.juris.de.

/2/ VERORDNUNG (EG) Nr. 352/2009 DER KOMMISSION vom 24. April 2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates.

/3/ DURCHFÜHRUNGSVERORDNUNG (EU) Nr. 402/2013 DER KOMMISSION vom 30. April 2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken und zur Aufhebung der Verordnung (EG) Nr. 352/2009.

/4/ Allgemeines Eisenbahngesetz (AEG) – siehe www.juris.de.

/5/ RICHTLINIE 2004/49/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 29. April 2004 über Eisenbahnsicherheit in der Gemeinschaft und zur Änderung der Richtlinie 95/18/EG des Rates über die Erteilung von Genehmigungen an Eisenbahnunternehmen und der Richtlinie 2001/14/EG über die Zuweisung von Fahrwegkapazität der Eisenbahn, die Erhebung von Entgelten für die Nutzung von Eisenbahninfrastruktur und die Sicherheitsbescheinigung.

/6/ RICHTLINIE 2008/57/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Juni 2008 über die Interoperabilität des Eisenbahnsystems in der Gemeinschaft.

/7/ DIN-EN 50126 Bahnanwendungen Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Deutsche Fassung EN 50126:1999.

/8/ Führerraumanzeige des Fahrplans mit EBuLa – Sachstand und Ausblick – Vortrag der DB Netz AG-Informationssysteme Kundeninteraktion/Vertrieb im Rahmen Fortbildung der Mitarbeiter/innen der betrieblichen Eisenbahnaufsicht, 03. bis 05.05.2011/Altenahr.

/9/ Folien Basler & Partner AG zur Sicherheitsnachweisführung, VDE 2, Sicherheit an Bahnsteigen, Besprechung mit dem EBA am 05. Januar 2001.

/10/ VDE 2 – Konzeptvorschlag für infrastrukturelle Vorkehrungen, DB Station & Service, SET Ja/SBB Ku; Stand: 30.04.2001.

/11/ Hinzen: „Der Einfluß des menschlichen Faktors auf die Sicherheit der Eisenbahn“, Dissertation an der RWTH Aachen, 1993.

/12/ Risikoanalyse EBuLa – vorgelegt mit Schreiben vom 17.05.2002 – TS CS (Dr.-Ing. Corinna Salander-Ludwig).

/13/ Zusicherung zum Betriebsverfahren zum Einsatz der Wirbelstrombremse auf Stre-cken mit nicht WB-fest ausgerüsteter Leit- und Sicherungstechnik, Bewertung durch eine Risikoanalyse – EBA-Bescheid 3420 – Arb 09/02 vom 17.01.2003.

/14/ Berichte des Eisenbahn-Bundesamts gemäß Artikel 18 der Richtlinie über Eisenbahnsicherheit in der Gemeinschaft (Richtlinie 2004/49/EG, „Sicherheitsrichtlinie“) über die Tätigkeiten als Sicherheitsbehörde für die Jahre 2007-2012 – siehe www.eisenbahn-bundesamt.de.

/15/ Intermediate report on the development of railway safety in the European Union – 2013, European Railway Agency.

12

Lösungsansätze

Dr. H.-J. Bischoff; Sektion Maschinen- und Systemsicherheit der IVSS, GfS, Deutschland

In einer globalen Wirtschaft, mit deren Anforderungen und Auswirkungen sich die internationale Politik (insbesondere G 20) und Wirtschaft befassen, wird auch die Arbeitswelt zunehmend globaler. Die Entwicklung dort wird international bisher nicht angemessen berücksichtigt.

In einer globalisierten Welt ist das Arbeitsleben stark durch sich daraus entwickelnde Phänomene beeinflusst. Sicherheit, Gesundheit und gesunde Umwelt sind Bereiche, denen mehr Aufmerksamkeit gewidmet werden muss. Wenn wir Sicherheit und Gesundheit bei der Arbeit als öffentliches Gut verstehen, müssen die Rollen der Akteure auf diesem Gebiet näher bestimmt werden. Neue Risiken entstehen in der allgemeinen Umwelt und besonders in den Arbeitsumgebungen und daraus sich ergebende neue Herausforderungen für Sicherheit und Gesundheit müssen angemessen behandelt werden.

In diesem Zusammenhang sei nur hingewiesen auf neue Trends in wirtschaftlichen Strukturen und Arbeitsbedingungen. Das Gewichtung in der Gesellschaft mit einer Entwicklung von der Primärgesellschft (vor allem Landwirtschaft, Fischerei) über die Sekundärgesellschaft (vor allem industrielle Produktion) zur Tertiärgesellschaft (vor allem Dienstleistungen, Informationstechnologien) hat sich radikal verändert. Die Welt ist mehr und mehr verbunden durch die rasante Entwicklung und Verbreitung von Kommunikations- und Informationstechnologien. Dadurch hat sich der Zeitenrhythmus der ganzen Welt wesentlich verändert, hin zur „24-Stunden-/7-Tage-Gesellschaft“. Die Situation der Beschäftigten ist viel weniger stabil geworden. Wir haben heute in vielfacher Hinsicht „Wanderarbeitnehmer“: Innerhalb einzelner Staaten (z. B. neue/alte Bundesländer), in Mega Cities, für bestimmte Projekte (z. B. große Bauprojekte); für die Erbringung von Dienstleistungen (z. B. Ernte, Pflege); durch Neugliederung von Wirtschaftsunternehmen (z. B. Outsourcing), aber auch durch die Entwicklung

gemeinsamer Märkte wie z. B. EU, Mercosur, NAFTA. Die besonders aus dem Prinzip 24/7 resultierenden Anforderungen der Leistungen „ just in time“ führen zu neuen, besonders psychischen, aber auch körperlichen Beanspruchungen und Belastungen. Die Medienpräsenz ist allumfassend und verbreitet heute Informationen über globale Ereignisse sozusagen in Echtzeit. Dies hat Auswirkungen auf einige weltweite Demokratisierungs- und Humanisierungsprozesse sowie auf Umweltbelange, wie Umweltschutz, das Gleichgewicht von Ökosystemen, nachhaltige Entwicklung. Zum anderen nehmen diese Entwicklungen Einfluss auf Arbeitszeiten und in Konsequenz auch auf Arbeitsbedingungen. Outsourcing, Downsourcing und die Verlagerung von Produktionen auf neue Produktionsstätten, häufige Veränderungen durch Fusionen und Auflösungen von Firmen, Verlagerung von Arbeiten in Niedriglohnländer führen zur Auflösung von Betriebsstrukturen, die in der industriellen Gesellschaft sehr stabil waren. Solche Fragmentierungen schaffen neue Risikobereiche im modernen Arbeitsleben mit der großen Herausforderung, diese Risiken in sich häufig ändernden Situationen zu identifizieren, zu beurteilen und zu managen (Näheres siehe Bischoff, Herausgeber „Risks in Modern Society“, Kapitel 2, Jorma Rantanen – Springer-Verlag).

Die Konsequenzen sind weniger im Bereich von Arbeitsunfällen zu spüren. Die größere Veränderung ergibt sich im Bereich von Gesundheitsgefahren und Berufskrankheiten.

Einige beispielhafte Lösungsansätze für diese neuen Herausforderungen in der Arbeitswelt bestehen in:

Stärkung der Position der Internationalen Vereinigung für Soziale Sicherheit (IVSS)

Sie ist die weltweit führende internationale Organisation für Institutionen, Regierungsstellen und Behörden, die sich mit den verschiedenen Fragen der sozialen Sicherheit beschäftigen. Die IVSS wurde 1927 gegründet mit Sitz beim Internationalen Arbeitsamt in Genf. Derzeit hat die IVSS ca. 350 Mitgliedsinstitutionen aus über 150 Ländern aus den verschiedenen Bereichen der sozialen Sicherheit.

Für arbeitsbedingte Risiken spielt eine besondere Rolle der Besondere Ausschuss für Prävention mit seinen dreizehn internationalen Sektionen. Er ist vor allem an der Ausgestaltung und Umsetzung von Präventionsaktivitäten der IVSS beteiligt und kümmert sich um horizontale und vertikale Fragestellungen für die Sicherheit und Gesundheit bei der Arbeit. Dabei verfolgen die Sektionen vergleichbare Ziele in ihren jeweiligen Aufgabenbereichen: benutzerorientierte praktische Unterstützung; Erarbeitung praxisorientierter Lösungen; Durchführung internationaler Veranstaltungen für Experten zur Diskussion ausgewählter Fragestellungen; Erarbeitung von Publikationen für den Bereich Sicherheit und Gesundheit bei der Arbeit. Die IVSS-Sektion Maschinen- und Systemsicherheit beschäftigt sich aktuell mit Fragen der Risikobeurteilung, einschließlich dem Explosionsschutz, der Bedeutung von Steuerungen beim Einsatz in Maschinen und Anlagen, Maßnahmen gegen die Manipulation von Schutzeinrichtungen, der Bedeutung von Ergonomie und dem Human Factor.

Hauptzielgruppen sind Hersteller und Betreiber von Maschinen und Anlagen.

Außerdem koordiniert die Sektion das Arbeitsprogramm des Besonderen Ausschusses für kleine und mittlere Betriebe.

Lösungsansätze für die Arbeitswelt – ein paar Aspekte

Aspekt 1 – Verpflichtung zur Risikobeurteilung:
Der europäische Binnenmarkt steht für den freien Verkehr von Waren, Personen, Dienstleistungen und Kapital. Eine Einschränkung des freien Warenverkehrs in der EU ist nur in besonderen Ausnahmefällen zulässig. Für Bereiche mit höherem Risiko, z. B. der Einsatz von Maschinen, gilt ein EU-Recht mit einer Harmonisierung technischer Vorschriften. Dort sind grundlegende Sicherheitsanforderungen verbindlich festgelegt. Die Spezifizierung dieser Anforderungen erfolgt in harmonisierten Normen.

Dieses EU-Regelwerk hat eine hohe wirtschaftliche Bedeutung für Design und Herstellung von Maschinen in der EU. Die weiter gehende Erwartung ist, dass sichere Maschinen die Zahl von Unfällen und Gesundheitsschäden sowohl am Arbeitsplatz als auch im Privatbereich reduzieren.

Für den Hersteller ergeben sich die entsprechenden gesetzlichen Pflichten aus Artikel 114 des EU-Vertrages in Verbindung mit der Maschinenrichtlinie, Anhang 1. Sie sind konkretisiert z. B. in der EN ISO 12100 „Sicherheit von Maschinen".

Im Anhang 1 der Maschinenrichtlinie sind grundlegende Sicherheits- und Gesundheitsanforderungen für die Konstruktion und den Bau von Maschinen geregelt. Diese Anforderungen sind bindend. Wenn die damit gesetzten Ziele aufgrund des Standes der Technik nicht erreichbar sind, ist eine Maschine soweit wie möglich auf diese Ziele hin zu konstruieren und zu bauen. Der Hersteller muss für die Vornahme einer Risikobeurteilung sorgen, um die für die Maschine geltenden Anforderungen zu ermitteln. Konstruktion und Bau der Maschine müssen unter Berücksichtigung der Ergebnisse dieser Risikobeurteilung erfolgen. Die Pflichten des Herstellers bei der Risikobeurteilung sind in der Maschinenrichtlinie, Anhang 1, konkret vorgegeben. Ebenso die Rangfolge der zu treffenden Maßnahmen: Risikobeseitigung oder Risikominimierung durch Integration in sichere Konstruktion und Bau der Maschine → notwendige Schutzmaßnahmen gegen nicht zu beseitigende Risiken → Unterrichtung der Benutzer über Restrisiken, ggf. spezielle Ausbildung oder Einarbeitung der an Maschinen tätigen Personen sowie persönliche Schutzausrüstungen.

Für den Betreiber ergibt sich die gesetzliche Verpflichtung aus Artikel 153 EU-Vertrag sowie der Arbeitsschutzrahmenrichtlinie, Artikel 9. Danach muss der Arbeitgeber über die Evaluierung der am Arbeitsplatz bestehenden Gefahren für Sicherheit und Gesundheit, auch hinsichtlich der besonders gefährdeten Arbeitsgruppen, verfügen und er muss die durchzuführenden Schutzmaßnahmen und notwendigen Schutzmittel festlegen.

Hierbei handelt es sich um europäische Mindestregelungen, die durch nationale Bestimmungen im Sinne eines weitergehenden Beschäftigtenschutzes erweitert werden können.

Da die einschlägigen EU-Richtlinien für Hersteller und Betreiber von Maschinen seit ca. 25 Jahren in Kraft und den Entwicklungen auf dem Gebiet der Technik angepasst worden sind, müsste man eigentlich davon ausgehen, dass die Risikokompetenz zur Beurteilung von Risiken in der Arbeitswelt in hohem Maße besteht. Ein Grund für weiter gehenden Handlungsbedarf ergibt sich jedoch aus der eingangs beschriebenen starken Veränderung der Arbeitswelt, besonders in den letzten Jahren.

Aspekt 2 – „Comprehensive Approach zur Förderung von Maschinen- und Systemsicherheit“:
Mit den beschriebenen Pflichten zur Risikobeurteilung als Klammer ist die IVSS-Sektion Maschinen- und Systemsicherheit zurzeit dabei, zur Verbesserung der Risikokompetenz über die gesamte Lebensdauer von Maschinen in einem internationalen Projekt beizutragen, das in verschiedene Module für unterschiedliche Zielgruppen gegliedert ist:

1. „Sicherheit lehren und lernen“: Sicherheit muss schon an der Hochschule für künftige Ingenieure gelehrt und gelernt werden. Dies ist bisher kein Pflichtthema in den Lehrplänen trotz der oben beschriebenen Verpflichtungen zur Risikobeurteilung sowohl für Hersteller als auch für Betreiber. In die allgemeine Ausbildung künftiger Ingenieure, z. B. Maschinenbau, Elektrotechnik, ist das Thema noch nicht integriert. Wir haben dazu ein Konzept entwickelt, das Experten noch um konkrete Module erweitern, die auf unterschiedliche Zeiteinheiten für die Lehre im allgemeinen Studium ausgerichtet sind.

2. „Sicherheit integrieren“: Mit einer Risikobeurteilung erfüllt der Hersteller nicht nur eine gesetzliche Pflicht, sondern verbessert auch seine Marktchancen durch entsprechende Berücksichtigung von Stand der Technik und wissenschaftlicher Weiterentwicklung. Auch Unfallversicherungsträger und Präventionsdienste in vielen Ländern tragen durch Beratung und Kontrolle der Hersteller zur Weiterentwicklung bei.

3. „Sicherheit berücksichtigen“: Die Berücksichtigung von Anforderungen aus Risikobeurteilungen beim Handel mit Maschinen und Einkauf von Maschinen muss eine größere Bedeutung erlangen. Hier gibt es vielfältige Angebote zur Unterstützung durch Unfallversicherungsträger. In diesem Zusammenhang sind auch die Instrumente der Marktüberwachung und Marktbeobachtung anzusprechen. Marktüberwachung ist eine offizielle Aufgabe autorisierter Institutionen in den EU-Mitgliedsstaaten. Marktbeobachtung ist ein erfolgreiches Instrument, insbesondere durch die Konkurrenz von Maschinen- und Anlagenherstellern.

4. „Sicherheit anwenden“: Sicherheit und Gesundheit bei der Arbeit sind ein öffentliches Gut und ein ethisches Anliegen. Es führt zum einen zu Rechten der Beschäftigten, deren Prinzipien z. B. in der einschlägigen EU-Rahmenrichtlinie beschrieben und in nationalen Bestimmungen verankert sind, deren

Adressaten die Arbeitgeber sind. Untersuchungen zeigen zum anderen, dass „gesunde und sichere Betriebe“ in Sachen Produktivität und Qualität überdurchschnittliche Ergebnisse erzielen und damit ihre Konkurrenzfähigkeit verbessern. Dass Präventionsdienste und Unfallversicherungsträger die Betreiber verstärkt beraten, hat also zwei gute Gründe.

Schließlich gibt es durch Versicherungsträger unterschiedliche Anreizsysteme zur Förderung von Sicherheit und Gesundheit bei der Arbeit in Umsetzung von Ergebnissen von Risikobeurteilungen: Bonus-Systeme, Malus-Systeme, kombinierte Bonus-Malus-Systeme; besondere Prämien für überdurchschnittliche Präventionsaktivitäten von Betrieben; weite Spannbreite des Mitgliedsbeitrags abhängig von Risiken und Unfallgeschehen in Betrieben.

Aspekt 3 – die große Welt der Kleinbetriebe:
Wenn man nach einem europäischen Kriterium die Anzahl der Beschäftigten nimmt, um einen Betrieb von der Größe her zuzuordnen, gilt für die EU: Mikrobetriebe – bis 9 Beschäftigte (Kleinstbetriebe) /Kleinbetriebe – bis 50 Beschäftigte/mittlere Betriebe – bis 250 Beschäftigte/große Betriebe – mehr als 250 Beschäftigte.

Legt man diese Zählweise zugrunde, gibt es über alle Branchen in den EU-Mitgliedsstaaten: 93 % Mikrobetriebe, knapp 6 % Kleinbetriebe, 1 % mittlere Betriebe und nur 0,2 % große Betriebe.

Auch wenn international die Zählweise nicht identisch ist, sind die Ergebnisse doch ähnlich. Eine neue Erhebung in den USA hat z. B. für 2014 ergeben, dass 85 % aller dort tätigen Betriebe nicht mehr als fünf Beschäftigte haben.

Aus diesen Zahlen ergibt sich eine besondere Schwierigkeit für funktionierende Lösungsansätze: die große Zahl von Klein- und Mittelbetrieben. Sie sind für persönliche Beratung oder Kontrolle nur schwer erreichbar, weil dafür – selbst bei erheblicher Personalaufstockung – die personellen Ressourcen nicht ausreichen. Zum anderen ist die Motivation für mehr Prävention gegen arbeitsbedingte Risiken nicht leicht zu erreichen, wenn – abhängig von der Branche – im Kleinstbetrieb ein Unfall sich nur alle vier bis acht Jahre ereignet und vor dem Hintergrund einer nicht unerheblichen Fluktuation von Betriebsinhabern Unternehmer viele noch nie einen Arbeitsunfall in ihrem Betrieb erlebt haben.

Mitglieder aus verschiedenen IVSS-Sektionen: AUVA Wien, BGN Mannheim, Carsat Strasbourg, IAPA Toronto, INAIL Rom, INRS Paris, Suva Luzern, Prevent Brüssel mit besonderem Know-how beim Umgang mit Kleinstbetrieben haben deshalb die „Zehn Schlüssel zum Erfolg" erarbeitet. Sie geben Hinweise zur Einschätzung der Risikokompetenz von Betrieben.

Die zehn Schlüssel zum Erfolg:

1. Gesunde Unternehmen brauchen gesunde Beschäftigte.
2. Agieren statt reagieren.
3. Sich als Arbeitgeber aktiv einbringen.
4. Alle beteiligen.
5. Gute Arbeitsbedingungen rechnen sich.
6. Die Beteiligten informieren.
7. Intern kommunizieren.
8. Aus Vorfällen lernen.
9. Gefahren an der Quelle beseitigen.
10. Sich auf dem Laufenden halten.

Siehe Download unter: http://safety-work.org

Außerdem haben mehrere Partner eine Website entwickelt: www.safety-work.org. Es handelt sich um eine Internetseite insbesondere für Kleinbetriebe und deren Partner mit unterschiedlichen Beispielen guter Praxis.

Für eine interne Bewertung haben wir dazu einen Selbsttest eingestellt, mit dem der einzelne Betrieb bewerten kann, wie er hinsichtlich der Umsetzung der „Zehn Schlüssel zum Erfolg" steht. Dies ersetzt nicht die gesetzliche Verpflichtung zur Risikobeurteilung. Es berücksichtigt aber die wesentlichen Themen, um den Grad der Risikokompetenz eines Betriebes zu ermitteln.

13

Menschliches Verhalten und Risikokompetenz – Fallanalysen

13.1 Einführung

Dr. Sebastian Festag, Bergische Universität Wuppertal, GfS, Deutschland

Sicherheitsprobleme treten auf sehr unterschiedliche Weise in Erscheinung, als Bagatellen, Unfälle, Katastrophen, Störungen, Belastungen, Erkrankungen oder Anschläge. Vielen dieser Ereignisse ist gemeinsam, dass menschliche Verhaltens- und Reaktionsweisen innerhalb des Ereignisablaufes eine wichtige Rolle spielen. Ein wesentlicher Teil davon steht wiederum mit den technischen und organisatorischen Rahmenbedingungen unserer Umwelt im Zusammenhang. Das liegt einerseits an den physiologischen Faktoren und andererseits an Faktoren, die auf das psychische und soziale Verhalten der Betroffenen zurückgehen. Sie sind ein wichtiger Teil der aktuellen Problemlage.

Im Rahmen von Untersuchungen haben wir dazu mehrere unterschiedliche Situationen unter sicherheitswissenschaftlichen Gesichtspunkten analysiert (vgl. [1]). Zwei Fälle, die sich im betrieblichen Umfeld ereigneten, greife ich für den vorliegenden Beitrag heraus. Im Folgenden stelle ich diese beiden Fallanalysen vor und werte sie anschließend gemeinsam unter Berücksichtigung des Themas der hier zur Diskussion stehenden Veranstaltung aus.

13.2 Die Schließung eines Industriebetriebes

Bei dem ersten Fall handelt es sich um die Analyse der endgültigen Schließung eines in Deutschland ansässigen Produktionsbetriebes. Bis zu seiner endgültigen Schließung gehört der Betrieb, nach mehreren unternehmerischen Übernahmen und Zusammenschlüssen, einem großen Konzern an, mit zahlreichen über die Welt verteilten Standorten. Die Schließung des Betriebes erfolgte aufgrund der wirtschaftlichen Schieflage. Von der Schließung sind über 300 Mitarbeiter des Betriebes betroffen. Zur Überwindung der wirtschaftlichen Schieflage entwickelte der Betrieb zuvor ein Produkt mit neuen und einzigartigen Eigenschaften. Da das Produkt nach einer Einstellungszeit stabil hergestellt werden konnte und sich in den Markt einführen ließ, setzte sich die Hoffnung auf ein langfristiges Überleben des Betriebes und eine Kehrtwende in der angespannten betriebswirtschaftlichen Situation durch. Das Produkt war erfolgreich, sodass Mitarbeiter des hier angesprochenen Betriebes aufgefordert wurden, an der Überführung der Produkteigenschaften auf ein neu gegründetes Schwesterwerk im Ausland, mit größeren Maschinen bei gleichzeitig weniger Personalstellen und einer implizit hohen Erwartung an die Wirtschaftlichkeit, behilflich zu sein. Währenddessen wurde von der Konzernführung der Beschluss der Schließung des untersuchten Betriebes aus Gründen „langfristig unprofitabler Ergebnisse“ sowie zur „Steigerung der Unternehmensrentabilität“ und der „wirtschaftlichen Ertragskraft“ gefasst.

Diese Schließungsphase wurde von uns beobachtet und ausgewertet, wobei unter anderem 91 meldepflichtige, nicht meldepflichtige, Fremdfirmen- und Wegeunfälle mit 631 Ausfalltagen zur Bewertung der Sicherheitssituation vor und 89 Unfälle mit 418 Ausfalltagen zur Bewertung während der Schließungsphase in die Untersuchung eingehen.

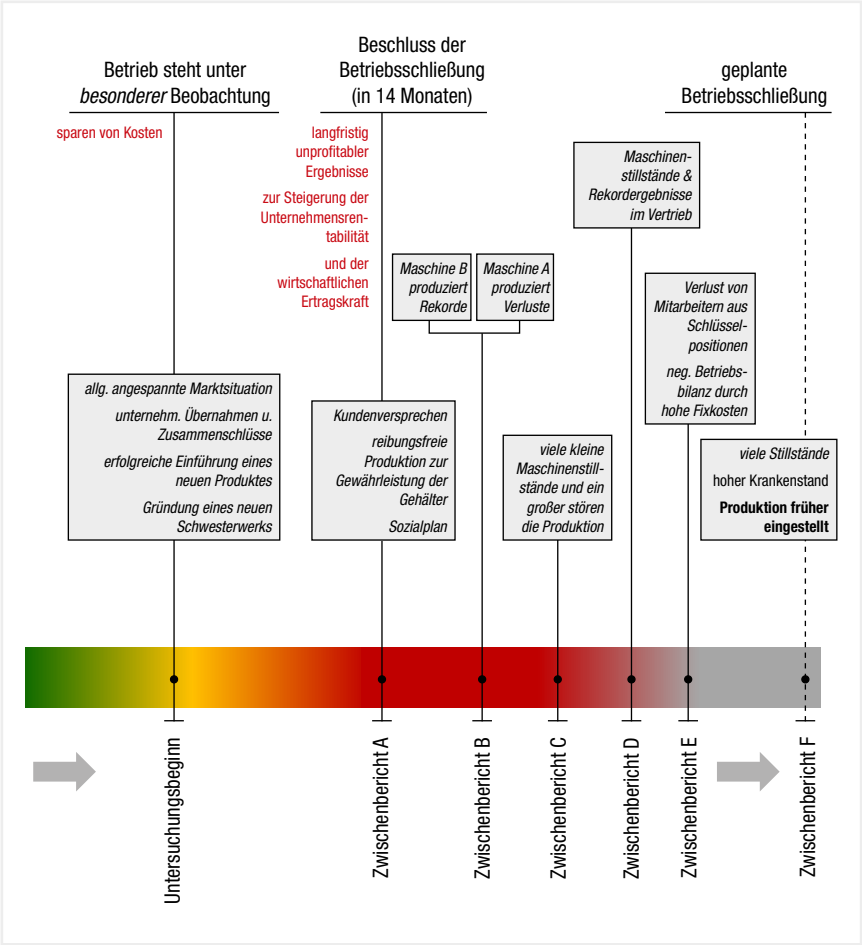

Bild 13.1: **Fallanalyse A: Betriebsschließung – Chronologie – (vgl. Festag, 2012)**

Bild 13.1 zeigt wichtige Ereignisse während der Schließungsphase, die aus Bekanntmachungen des Betriebes hervorgehen. Wie aus den Abläufen und unseren Untersuchungsergebnissen hervorgeht, sinken nach der Verkündung der Schließung zunächst die Unfallzahlen im Vergleich zum Vorjahreszeitraum, um dann im Laufe der Zeit über ihr gewöhnliches Maß hinaus zu steigen (siehe Bild 13.2).

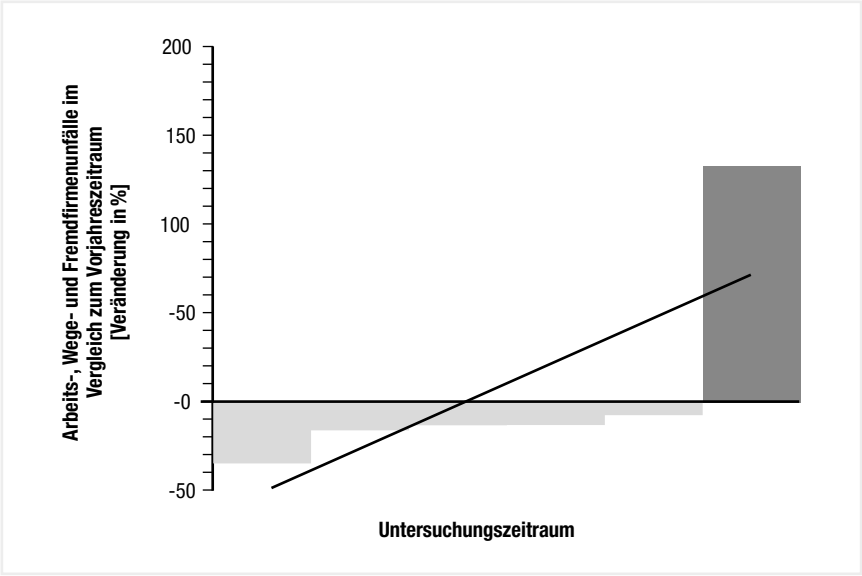

Bild 13.2: Fallanalyse A: Betriebsschließung – Ergebnisse – (vgl. Festag, 2012)

Das Sinken der Unfallkennzahlen zum Beginn der Schließungsphase deuten wir als Hoffnung zur Kehrtwende bei den Mitarbeitern, da nach der Verkündung der Betriebsschließung das Aufhalten des Beschlusses – je nach Betriebsergebnis – offengelassen wurde. Das Ansteigen der Unfallkennwerte im Laufe der Zeit sehen wir dagegen als Resignation und Frust, da die Endgültigkeit der Betriebsschließung zunehmend erkennbar wurde. Dieser Effekt ist tatsächlich sogar noch größer, da zum Ende des Untersuchungszeitraumes weniger Mitarbeiter im Betrieb beschäftigt waren. Zum Ende der Betriebsschließung gingen nicht mehr genügend Mitarbeiter ihrer Arbeit nach, sodass die Produktion zudem frühzeitig eingestellt werden musste. Mit dem zeitlichen Verlauf spitzte sich die Situation weiter zu. Es kam vermehrt zu Unfällen, Produktionsstörungen und Maschinenstillständen. Darüber hinaus ereigneten sich Sachbeschädigungen, Beleidigungen und persönliche Übergriffe mit Personenschäden.

13.3 Die Stilllegung einer Produktionsanlage

Der zweite Fall behandelt die Analyse der Stilllegung einer Produktionsanlage eines Industrieunternehmens (vgl. auch [2]). Bei der Produktionsanlage handelt es sich um eine von drei parallel und unabhängig voneinander gefahrenen Produktionsanlagen. In dem betroffenen Betrieb waren insgesamt etwa 1.000 Mitarbeiter beschäftigt, wovon im Zuge der Anlagenstilllegung etwa ein Drittel der Personalstellen abgebaut wurde.

In der Untersuchung wurden neben den Angaben über die Mitarbeiteranzahl – als Maß der Beschlussumsetzung –, zahlreiche Leistungs- und Sicherheitskennwerte des Betriebes über 10 Jahre monatsweise ausgewertet. Entsprechend der Abfolge der Führungsbeschlüsse wurde vor der Ankündigung der Anlagenstilllegung der „normale“ bzw. „störungsfreie“ Betriebsverlauf anhand der Kennwerte als Referenzzeitraum charakterisiert. Daraufhin wurden die Abläufe an der betroffenen (Anlage A) und den benachbarten Produktionsanlagen (Anlage B und C) von der Ankündigung bis zur tatsächlichen Stilllegung und dem Zeitraum danach miteinander verglichen und unter der Anwendung des Interquartildistanzverfahrens zur Bewertung auf den Referenzzeitraum bezogen.

Die Analyse lieferte ein erstaunliches Ergebnis. An der direkt betroffenen Produktionsanlage verbesserte sich während der Anlagenstilllegung die Situation in Bezug auf die Produktionsleistung und dem Auftreten von Störungen und Unfällen, während sie sich an den benachbarten Produktionsanlagen zum Teil statistisch signifikant verschlechterte (Bild 13.3).

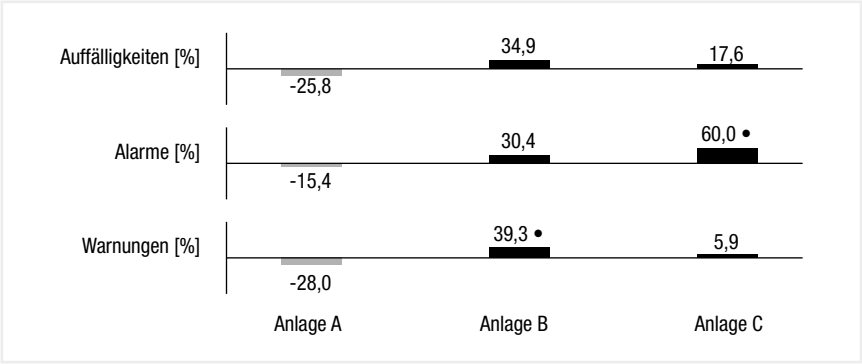

Bild 13.3: **Fallanalyse B: Anlagenstilllegung – Ergebnisse I – (vgl. [1])**

Ähnlich wie bei der Betriebsschließung führen wir das bei den Mitarbeitern der direkt betroffenen Anlage auf eine „Hoffnung zur Kehrtwende" und bei den Mitarbeitern der indirekt betroffenen benachbarten Anlagen auf Frustrationen und Aggressionen zurück. Nach der Anlagenstilllegung verschlechtert sich die Situation an den beiden benachbarten und weiterbetriebenen Produktionsanlagen weiter, wie Bild 13.4 anhand der weißen Balken zeigt. Zwischen Produktions- bzw. Sicherheitskennwerten und der Mitarbeiteranzahl ergaben sich sogar teilweise statistisch bedeutsame Zusammenhänge. Mit sinkender Mitarbeiteranzahl erhöhten sich die Sicherheitsprobleme.

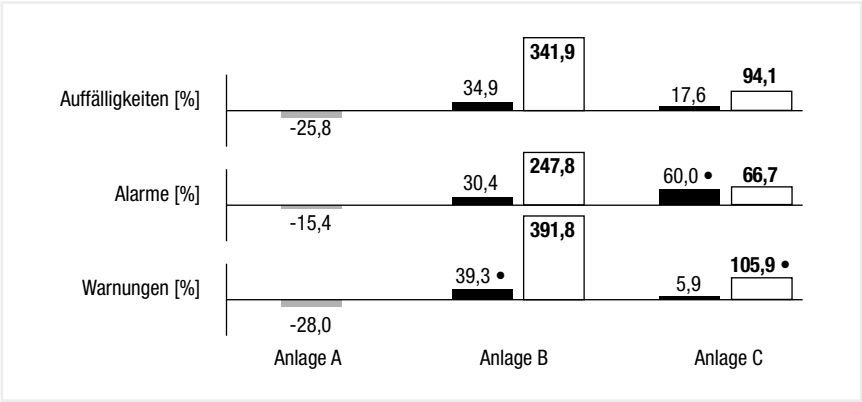

Bild 13.4: **Fallanalyse B: Anlagenstilllegung – Ergebnisse II – (vgl. [1])**

13.4 Zusammenfassung und Fazit

Zunächst wurde durch die Fallanalysen offensichtlich, dass die Führungsbeschlüsse erhebliche Kollateralschäden produziert haben. Ersichtlich wird zudem, dass das Verhalten der Mitarbeiter sehr unterschiedlich und zum Teil sehr unerwartet ist. Die Nichtberücksichtigung solcher Verhaltens- bzw. Reaktionsweisen kann bei Managementbeschlüssen, wie sie hier angesprochen wurden, zu erheblichen Problemen und Gefahren führen. Sie werden auf einer systemisch wirkenden Weise begünstigt. Zwar kennen wir die exakten Mechanismen nicht, trotzdem lässt sich bereits so viel sagen, dass durch das mangelnde Verständnis solcher Abläufe – insbesondere im Zusammenhang mit menschlichen Reaktionsweisen – Sicherheitsprobleme erzeugt bzw. verstärkt werden; auch wenn Gegenteiliges mit dem Vorgehen angestrebt wird.

Bild 13.5 zeigt diesen kontraproduktiven Mechanismus (siehe [3]). Die Analysen zeigen, dass menschliche Verhaltens- und Reaktionsweisen beim allgemeinen Vorgehen, aber auch bei dem Ableiten von Sicherheitsstrategien, nicht hinreichend berücksichtigt werden und dadurch Probleme erzeugen bzw. verstärken können.

Es ergeben sich zwei weitere Befunde:

1. Wie wir anhand der Fallanalysen sehen, tauchen in beiden Fällen auch sicherungsrelevante (security) Probleme auf. Das erfordert die Verzahnung mit der Sicherheitstechnik (safety) sowie die Integration in die Sicherheitswissenschaft.

2. Im Normalbetrieb eines Ablaufes und im Modus der gewöhnlichen Störungsbeseitigung sind Sicherheits- bzw. sicherheitstechnische Maßnahmen heutzutage oftmals etabliert. Wie wir hier gesehen haben, ist der Bedarf an Sicherheitsmaßnahmen außerhalb des „Normalzustandes“ hoch bzw. dann sogar unter Umständen noch höher (solchen Maßnahmen werden in kritischen Zeiten, aber oftmals nur wenig Raum gegeben, z. B. weil die Betriebsführung während der Stilllegung einer Produktionsanlage mit dem Überleben des Betriebes beschäftigt ist (vgl. [4]).

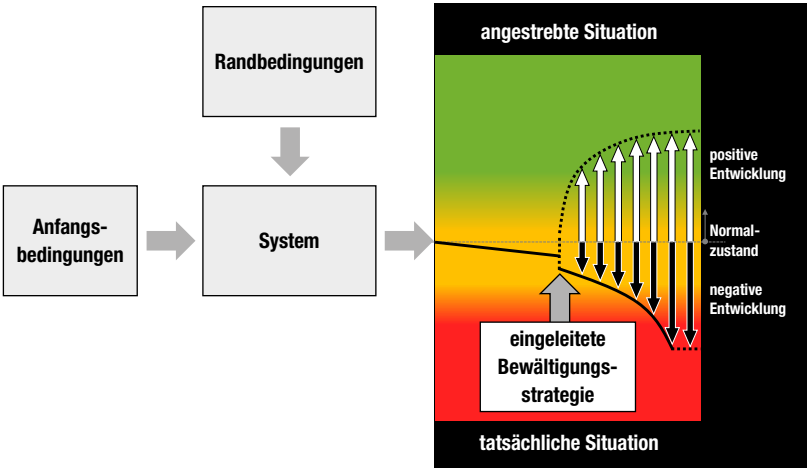

Bild 13.5: Kontraproduktiver Mechanismus (vgl. Festag, 2012; siehe auch Festag & Hartwig 1/2013)

Welche Lehre können wir aus den Fällen ziehen, um dieser Situation entgegen zutreten?

Zunächst gilt es festzuhalten, dass wir heute nur ein sehr lückenhaftes Bild über und Verständnis von solchen Abläufen – wie wir sie analysierten – haben. Prinzipiell ist aber festzustellen, dass Führungskräfte von Betrieben Kompetenzen im Umgang mit Gefahren und Risiken in Bezug auf die Reichweite ihrer Entscheidungen benötigen. Davon sind nicht nur die Fachkräfte für Sicherheit, Sicherheitsingenieure etc. betroffen, sondern alle Führungskräfte.

Innerhalb der Auseinandersetzung mit Risiken sind menschliche Verhaltensweisen und individuelle Befindlichkeiten zu berücksichtigen. Es gibt keine allgemeingültige einfache Lösung für Sicherheitsprobleme dieser Art. Es müssen neue und andere Strategien zur Risikobewältigung entwickelt werden. Diese Strategien müssen die Reaktionen der Betroffenen als individuelle Ganzheit berücksichtigen und an die Fallgegebenheiten gebunden sein.

Literatur

[1] Festag, S. (2012). Systemsicherheit und menschlicher Faktor. Über das Versagen von Strategien zur Risikobewältigung. Dissertation, Bergische Universität Wuppertal – Abt. Sicherheitstechnik.

[2] Festag, S. & Hartwig, S. (2013). Sicherheitsprobleme durch die Vernachlässigung der Mitarbeiterreaktionen auf betriebliche Managementbeschlüsse. Technische Sicherheit, Band 3, Nr. 1 Januar/Februar, Springer Verlag, S. 17–22.

[3] Festag, S. (5/2014). Das Versagen von unangepassten Sicherheitsstrategien. Technische Sicherheit, Band 5, Nr. 5 – Mai, Springer Verlag, S. 51–55.

[4] Burkhardt, F. (1981). Information und Motivation zur Arbeitssicherheit. Wiesbaden: Universum Verlagsanstalt.

14

Methodische Herausforderungen bei der Risikobeurteilung und deren Konsequenzen am Beispiel der Feuerwehrbedarfsplanung

14.1 Einführung

Ing. Adrian Ridder, M.Sc., Bergische Universität Wuppertal, GfS, Deutschland

Für die Feuerwehrbedarfsplanung (synonym u. a. auch „Brandschutzbedarfsplanung", „Gefahrenabwehrplanung", „Bedarfs- und Entwicklungsplanung") werden methodische Grundlagen zur Fundierung der Entscheidungen über die Frage benötigt, „wie viel Feuerwehr" nötig ist für eine Kommune. Während historisch derartige Entscheidungen oftmals auf Grundlage von Erfahrungen und Intuition getroffen wurden, existieren aktuelle Entwicklungen hin zu softwaregestützten Algorithmen und datenbasierten Entscheidungsunterstützungsmodellen. Es kann festgestellt werden, dass auch die Anwendung von risikoanalytischen Verfahren zum Teil rechtlich verlangt wird (z. B. IM SA 2009, BRANDENBURG 2004:§3) und die Risikoanalyse als notwendige, „unabdingbare Voraussetzung für die richtige Bedarfsplanung" (AGBF BUND 1998; vgl. auch AK BSBP NRW 2001) betrachtet wird, man mithin erhofft, durch ihren Einsatz eine zielgerichtetere und genauere Bedarfsplanung erreichen zu können als bei einfacheren, gröberen Verfahren. In der Literatur findet sich eine Anzahl in- und ausländischer Methoden zur Risikoanalyse bei der Bedarfsplanung (z. B. AK BSBP NRW 2001, FAASCH 1972, SCHUBERT 2001:6, GRABSKI 2007, AG RISIKOANALYSE 2009, BBK 2010:15, LSTE, VAN DER SCHAAF & JEULINK 1992), gleichwohl wird die Erkenntnis konstatiert, dass die für eine valide Risikoanalyse notwendigen wissenschaftlichen Grundlagen fehlen (vgl. AK BSBP NRW 2001).

Basierend auf der Auswertung einer Vielzahl von Bedarfsplänen von über 30 Methoden zur Feuerwehrbedarfsplanung und von Einsatzdaten aus zwei Großstädten, einem Landkreis sowie der ADAC-Luftrettung wurden nachfolgende Gedanken entwickelt, die einen Beitrag zur wissenschaftlichen Diskussion über die Bedarfsplanung am Beispiel der Feuerwehr darstellen.

14.2 Begriffsmodell

Die im Rahmen der vorliegenden Arbeit verwendeten Begrifflichkeiten werden an das Ursache-Wirkungs-Modell von (COMPES 1973) sowie internationale Normen angelehnt. Im Folgenden werden die Begriffe „Risiko“ und „Schutzziel“ kurz erläutert, da hier teils stark unterschiedliche Interpretationen existieren:

Grundsätzlich versteht man nach ISO 31000 unter Risiko ganz allgemein die Auswirkung von Ungewissheit[1] auf Ziele. Eine Auswirkung stellt dabei eine Abweichung von Erwartungen dar, während man unter „Ungewissheit“ den Zustand versteht, der sich aus dem gänzlichen oder teilweisen Fehlen von Informationen oder Wissen über ein Ereignis, seine Auswirkung oder seine Wahrscheinlichkeit ergibt. Diese Risiko-Definition wird konkretisiert durch die Erkenntnis, dass Risiken häufig durch eine Kombination der Auswirkungen und der Wahrscheinlichkeit eines Ereignisses beschrieben werden können (ISO 31000:2009:1). Es bleibt festzuhalten, dass die oft verwendete Formel „Risiko ist Eintrittswahrscheinlichkeit multipliziert mit der Schadensschwere“ zumindest stark verkürzt, wenn nicht gar unkorrekt ist, da die Art des Zusammenhangs von Eintrittswahrscheinlichkeit und Schadensschwere nicht a priori für alle Anwendungsbereiche festlegbar ist.

Durch eine Veröffentlichung der Arbeitsgemeinschaft der Leiter der Berufsfeuerwehren in Deutschland wurde ein sog. „Schutzziel“ geprägt, das beschreibt, mit wie vielen Feuerwehrangehörigen in welcher Zeit in wie viel Prozent der Fälle die Feuerwehr vor Ort sein soll (vgl. AGBF BUND 1998:2). In der folgenden Verwendung dieses Konzeptes entwickelten sich fast schon dogmatische

1 Nach dem ÖSTERREICHISCHEN NORMUNGSINSTITUT (ON) 2010 wird das im englischen Original verwendete Wort „uncertainty“ mit „Unsicherheit“ ins Deutsche übersetzt; dies ist als Antonym zu „Sicherheit“ im behandelten Kontext jedoch missverständlich. „Ungewissheit“ beschreibt ausdrucksstärker den gemeinten Umstand, nämlich den Fakt, dass wichtige Informationen nicht vorliegen und somit „nicht gewusst“ werden. Im Folgenden wird durchgängig „Ungewissheit“ für „uncertainty“ verwendet.

Tendenzen hinsichtlich der Unantastbarkeit dieses Konzeptes und der konkret definierten Zahlenwerte. Dazu ist anzumerken, dass im hier betrachteten Kontext der Begriff oft unkorrekt verwendet wird. Denn ein Schutzziel besteht nicht nur aus Erreichungsgrad, Funktionsstärke und Hilfsfrist, sondern im Bereich der Gefahrenabwehr ist ein Schutzziel der angestrebte Zustand eines Schutzguts, der bei einem Ereignis erhalten bleiben soll (vgl. z. B. BBK 2011). Somit beschreiben die o. g. drei Komponenten vielmehr „zur Schutzzielerreichung abgeleitete Maßnahmen" und nicht das Schutzziel selbst. Das lautet nämlich gemäß unserem Wertemodell primär „körperliche Unversehrtheit der zu rettenden Personen". Insofern kann einem Schutzziel auch keine „uneingeschränkte Gültigkeit" (KNORR 2012) (oder Ungültigkeit) attestiert werden, da es aufgrund unserer Rechtsordnung vorgegeben ist. Auch die zur Schutzzielerreichung abgeleiteten Maßnahmen können nicht gültig oder ungültig sein, da es hier keinen absoluten Maßstab geben kann und eine Festlegung des mittels dieser Maßnahmen ausgedrückten Sicherheitsniveaus vor allem ein politisch-gesellschaftlicher Prozess ist, in dem eine – je nach örtlichen Gegebenheiten u. U. stark verschiedene – Akzeptanz oder Aversion des Risikos einer Personenschädigung zum Ausdruck kommt (vgl. RIDDER 2013:6). Ergo bleibt bei von der AGBF abweichenden Definitionen von „Planungszielen" (so ein aus Sicht des Verfassers passenderer Begriff) das – moralisch aufgeladene – Schutzziel der Rettung von Menschen unangetastet und es werden vielmehr die zur Erreichung dieses Zieles vorgesehenen Maßnahmen angepasst.

14.3 Der risikobasierte Ansatz: Hintergründe und Stand der Technik

In verschiedenen Rechtsgrundlagen und bestehenden Methoden zur Bedarfsplanung wird gefordert bzw. postuliert, dass ein risikobasierter Ansatz verwendet werden sollte. Die relevanten methodischen Hintergründe sind nachfolgend kurz beschrieben.

Der Risikomanagement-Prozess gemäß ISO 31000 (siehe Bild 14.1) zeigt, dass der Hauptschritt „Risikobeurteilung" den Prozess von der Risikoidentifikation über die Risikoanalyse bis hin zur Risikobewertung umfasst. Ein wichtiger Schritt ist die Risikoidentifikation, da nur Risiken, die in diesem Schritt erkannt werden, im späteren Verlauf Berücksichtigung finden. Dabei sollten möglichst viele Risiken und Risikokombinationen einschließlich ihrer Ursachen und Folgen erkannt werden. Die Risikoanalyse ist der Prozess zur Erfassung des Wesens eines Risikos und zur Bestimmung der Risikohöhe. Unter „Risikohöhe" versteht man dabei das Ausmaß eines Risikos oder einer Kombination von Risiken, das als bestimmte Kombination von Auswirkungen und ihrer Wahrscheinlichkeit zum Ausdruck gebracht wird (ISO Guide 73:2009), (ISO 31000:2009). Die Risikoanalyse soll somit Verständnis für Risiken schaffen, ein aussagekräftiges Synonym könnte in dieser Hinsicht der Begriff der „Risikocharakterisierung" sein (CRC 1996), (EUROPÄISCHE KOMMISSION 2000).

Basierend auf der Risikoanalyse wird im nächsten Schritt der Risikobewertung bewertet, ob die vorliegende Risikohöhe zu hoch oder akzeptabel ist, und entschieden, welche Risiken gemindert werden müssen und mit welcher Priorisierung dies geschehen soll. Übersteigt die Risikohöhe die Risiko-Akzeptanzkriterien, sind Maßnahmen abzuleiten und umzusetzen (Risikobewältigung).

Der primäre Zweck von Risikoanalysen besteht darin, Entscheidungsträger für Entscheidungen über den Mitteleinsatz zu informieren und fundierte, sachgerechte Entscheidungen zu ermöglichen (vgl. SCHUBERT 2001:3; ISO 31000:2009; EUROPÄISCHE KOMMISSION 2000). Ziel des Prozessschrittes der Risikoanalyse ist es damit, eine potenziell gefährliche Situation so akkurat, genau und

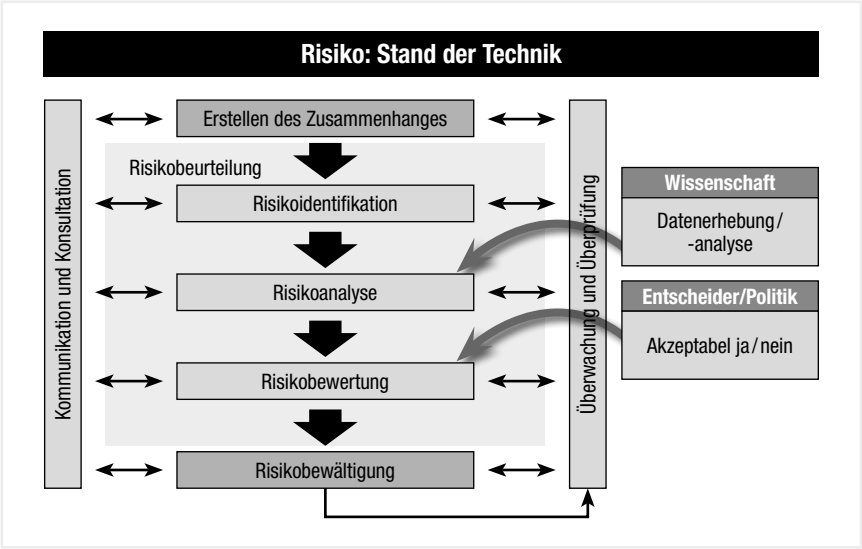

Bild 14.1: **Risikomanagement-Prozess (nach ISO 31000:2009)**

entscheidungsrelevant wie möglich zu beschreiben, die signifikanten Sorgen der Stakeholder zu behandeln und die so gewonnene Information für die Öffentlichkeit und interessierte Kreise verständlich und zugänglich zu gestalten (CRC 1996:16). Das BBK hat diesen Sachverhalt wie folgt treffend beschrieben:

„Die Aufbereitung und Bereitstellung der Ergebnisse der Risikoanalyse für politische Entscheidungsträger und die Bevölkerung ist wichtiger Bestandteil des Risikomanagements. Denn während die Analyse der Risiken ein nüchterner, wissenschaftlicher Prozess ist, werden die Risikobewertung und die daraus folgende Abwägung und Auswahl von risikomindernden Maßnahmen in erheblichem Umfang von politischen und gesellschaftlichen Aspekten mitbestimmt. Hierzu muss ein entsprechender Dialog zwischen Fachbehörden, Wissenschaft, Politik und Bevölkerung stattfinden, wobei die erkannten Risiken ebenso zu kommunizieren sind wie Erkenntnislücken und Unsicherheiten“ (BBK 2010:46).

Ein solcher Dialog ist in der Anwendung der Feuerwehrbedarfsplanung in Deutschland erst im Entstehen begriffen und bedarf weiterer unterstützender Forschung.

14.4 Relevante Risiken

Von elementarer Bedeutung für Risikobeurteilungen ist die Frage, welches konkrete Risiko beurteilt werden soll. Je nach Anwendungsgebiet stehen unterschiedliche Risiken zur Diskussion, z. B. das Gesundheitsrisiko aus dem Anbau von Genmais, das Ausfallrisiko eines Bauteils in einem Pkw oder das Brandtodesrisiko für Zivilisten u. v. m. Letzteres wird z. B. in einem ausländischen Ansatz zur Feuerwehrbedarfsplanung in Form des Brandtodesrisikos der Bewohner in Abhängigkeit des Gebäudetyps verwendet (VAN DER SCHAAF & JEULINK 1992). Andere Methoden der Feuerwehrbedarfsplanung versuchen ein „Risiko" (das nicht weiter spezifiziert wird) zu beschreiben, mit dem fassbar gemacht werden soll, mit welcher Wahrscheinlichkeit Ereignisse auftreten und welches Ausmaß diese haben werden, um darauf basierend die Feuerwehr zu planen. Dazu werden bei der Gefahrenanalyse Zusammenhänge unterstellt zwischen einzelnen Faktoren der betrachteten Gebietskörperschaft und dem Risiko (Auftreten und Ausmaß) von Ereignissen (z. B. bei den Verfahren nach SCHUBERT 2001, GRABSKI 2007 ausgehend von Einwohnerzahl, Art der Flächennutzung und Art der vorhandenen Objekte) oder es werden Szenario-Ereignisse gebildet (z. B. BBK 2010:15, LSTE o.J.) und basierend darauf die Zuordnung in „Risikostufen/-klassen" vorgenommen. Diese unterstellten Zusammenhänge sind bis dato hypothetisch und nicht validiert, d. h. es sind keine Forschungsarbeiten bekannt, die derartige Zusammenhänge bestätigen würden. Erste Ansätze zur Überprüfung einiger Hypothesen wurden von (HILDEBRAND 2013), (LANGER 2013) und (EDNER 2013) unter Anleitung des Verfassers angestellt.

Für den Szenarien-Ansatz existierten bis zur Arbeit von (SCHMID 2014) keine methodischen Ansätze dazu, wie Szenarien holistisch designt und vergleichbar angewendet werden können. Die Bewertung der Eintrittswahrscheinlichkeit der erkannten Gefahren basiert zum einen auf der Schätzung subjektiver Wahrscheinlichkeiten – im Gegensatz zur frequentistischen Wahrscheinlichkeit (vgl. BJERGA & FLAGE 2013:3198) –, zum anderen werden retrospektive Daten herangezogen.

Der oben beschriebene tradierte Ansatz zur Feuerwehrbedarfsplanung versucht, den klassischen Risiko-Ansatz von „Eintrittswahrscheinlichkeit mal Schadensschwere“ umzusetzen. Um dabei jedoch weiter bestehende Ungewissheiten und Unzulänglichkeiten aufzudecken, kann die allgemeinere Definition des Risikos nach ISO 31000 („Risiko beschreibt die Auswirkung von Ungewissheit auf Ziele“) herangezogen werden. Versucht man, die Verfahrensweise aktueller Methoden für die Feuerwehrbedarfsplanung in Form der ISO-Definition zu beschreiben, ergibt sich Folgendes:

Ziel: Jede Zone (Dorf, Stadtteil o. Ä.) in die korrekte Risikoklasse einordnen und die entsprechende Bewältigungskapazität so definieren, dass alle dort erwarteten Belastungen adäquat abgearbeitet werden können, d. h. für jedes dort als berücksichtigenswert betrachtete Ereignis eine ausreichende Bewältigungskapazität zur Verfügung stellen.

Ungewissheiten: Zeitpunkt der Entstehung des Ereignisses, Art und Ausmaß des Ereignisses, notwendige Bewältigungskapazität zur Bewältigung des Ereignisses, Korrektheit der Zuordnung von Zone in Risikoklasse und von Risikoklasse zu Bewältigungskapazität.

Auswirkungen (Abweichungen von den Erwartungen): mehr zeitgleiche Ereignisse als erwartet, nicht erwartetes Ereignis tritt auf, Art und Ausmaß des Ereignisses anders bzw. größer als erwartet, größere Bewältigungskapazität notwendig als erwartet.

Im tradierten Ansatz der Bedarfsplanung besteht unter Verwendung des ISO-Risikobegriffs („Auswirkungen von Ungewissheit auf Ziele“) das Risiko also darin, dass die getroffenen Annahmen darüber, welche Risikoklassen zu definieren sind, welche Zone in welche Risikoklasse gehört und welche Bewältigungskapazität für welche Risikoklasse nötig ist, nicht korrekt sind und somit nicht alle dort auftretenden Ereignisse bewältigt werden können. Anschaulich kann man von einem „Zuordnungsrisiko“ sprechen. Dieses Zuordnungsrisiko birgt konzeptionell eine hohe epistemische Ungewissheit (vgl. AGUIRRE 2013:3221).

Alternativ zum Zuordnungsrisiko lässt sich – ebenfalls gemäß ISO-Definition – ein „Überlastungsrisiko“ als das für die Feuerwehrbedarfsplanung relevante Risiko definieren, das geringere epistemische Ungewissheiten aufweist:

Ziel: bei Ereignissen in definierter Zeit effektiv Schaden minimieren.

Ungewissheiten: Ort des Ereignisses, Zeitpunkt der Entstehung des Ereignisses, Art und Ausmaß des Ereignisses, notwendige Bewältigungskapazität zur Bewältigung des Ereignisses.

Auswirkungen (Abweichungen von diesen Erwartungen): Das Ziel kann aus verschiedenen Gründen nicht vollumfänglich erreicht werden. Also besäße im Anforderungs- bzw. Belastungsfall das System „Feuerwehr" keine ausreichende Leistungsfähigkeit[1]. Somit wäre hier von einem „Überlastungsrisiko" für das System „Feuerwehr" zu sprechen. Dieses lässt sich wie folgt definieren:

„Abweichung der tatsächlichen von den planerisch als erwartbar festgelegten Gefahren-Charakteristika (Ort, Zeit, Art, Ausmaß, notwendige Bewältigungskapazität), wodurch bei Ereignissen nicht mehr in definierter Zeit mit vorbestimmter Effektivität Schaden minimiert werden kann, die Leistungsfähigkeit der Feuerwehr also nicht ausreichend ist („Überlastungsfall"). Das Überlastungsrisiko lässt sich charakterisieren durch den im Überlastungsfall entstehenden Schaden und seine Eintrittswahrscheinlichkeit."

Vom Begriff der „Überlastung" ist die „Überforderung" zu unterscheiden: Eine Überforderung liegt vor, wenn ganz allgemein die Belastung größer ist als die aktuelle Leistungsfähigkeit des Systems Feuerwehr. Im hier betrachteten Kontext sind dabei drei Fälle zu unterscheiden: Es kommt zur Überforderung (siehe Bild 14.2) und die Leistungsfähigkeit der Feuerwehr liegt dabei:

1. unterhalb,

2. genau bei,

3. oberhalb

1 Oder eine zu große, denn definitionsgemäß beschreiben Risiken sowohl positive wie negative Abweichungen. Grundsätzlich kann man in praxi jedoch davon ausgehen, dass eher eine zu geringe Leistungsfähigkeit der typische und kritische Anwendungsfall ist.

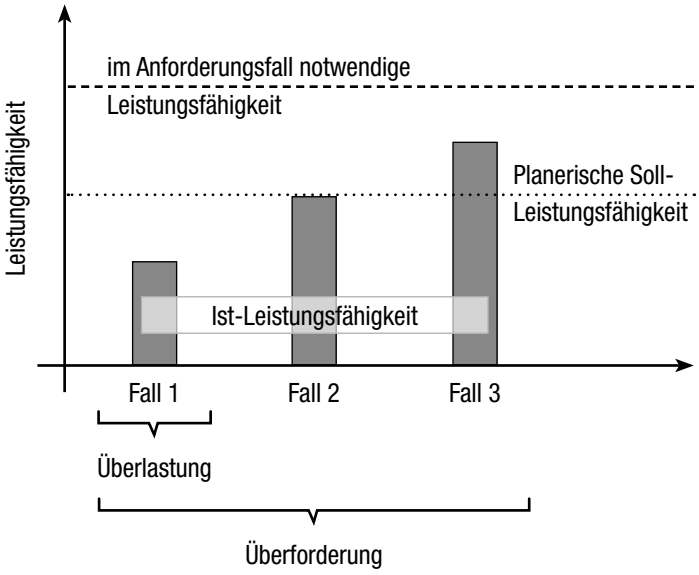

Bild 14.2: **Zur Unterscheidung von Überlastung und Überforderung**

der planerischen Soll-Leistungsfähigkeit („Sicherheitsniveau"). Die Fälle 2 und 3 stellen dabei zwar eine Überforderung, jedoch keine „Überlastung" im hier verwendeten Sinne dar, da die Feuerwehr ihre auftragsgemäße Leistungsfähigkeit erreicht oder sogar übertroffen und damit das geforderte Sicherheitsniveau gewährleistet hat. Eine „Überforderung" in diesen Fällen wurde definitionsgemäß planerisch von den Entscheidungsträgern akzeptiert und als Restrisiko hingenommen.

Anders gestaltet sich Fall 1: Dies stellt sowohl eine Überforderung als auch eine Überlastung dar, da in diesem Fall das planerisch vorgesehene Sicherheitsniveau nicht erreicht wurde.

14.5 Beurteilung der Anwendbarkeit der Risikoanalyse zur Bedarfsplanung

14.5.1 Grenzen der grundsätzlichen Anwendbarkeit des Risikoansatzes

Der risikobasierte Ansatz unterliegt wie jedes Konzept Einschränkungen und Grenzen hinsichtlich seiner grundsätzlichen Nutzbarkeit für unterschiedliche Anwendungen, wie eben auch der Feuerwehrbedarfsplanung.

Zum einen ist die „Uneindeutigkeit" der Aussagen von Risikobetrachtungen zu nennen: Menschen erhoffen – besonders in Fragen technischen Risikos – klare, belastbare Aussagen. Risikobewertungen können jedoch systemimmanent eine solche „ glasklare" Aussage mit scharfer Abgrenzung eines sicheren Bereichs vom unsicheren nicht liefern, sondern beinhalten immer Wahrscheinlichkeitsaussagen. Risikobewertungen wirken daher oftmals nicht überzeugend auf die Öffentlichkeit (SLOVIC 2002:313).

Außerdem bestehen auch in der Quantifizierung von Risiken Grenzen der Anwendbarkeit. Als grundsätzliche Probleme bei einer Nutzung des risikobasierten Ansatzes sind in der Literatur u. a. folgende Punkte bekannt (vgl. MEYNA 1982:166–168, CRC 1996:16):

1. Mangelndes Verständnis und Unvollständigkeit der Kenntnis von Ursächlichkeiten und Abhängigkeiten bei der Schadensentstehung.

2. Datenungewissheiten: Zum einen ist hier eine „unwahre" Ermittlung der Eintrittswahrscheinlichkeit zu nennen. Prospektiv, also in die Zukunft gerichtet, kann nur sehr grob und unter massiver Beeinflussung durch die subjektive Beurteilung des Analysierenden die Wahrscheinlichkeit zukünftiger Ereignisse abgeschätzt werden, eine Quantifizierung ist kaum seriös leistbar (vgl. SCHUBERT 2001:8). Eine retrospektive (vergangenheitsbezogene) Erhebung von Eintrittshäufigkeiten liefert zwar für eingetretene Ereignisse realistische und objektive Daten; nicht eingetretene Ereignisse würden dadurch jedoch systematisch untergewichtet, da sie ja nicht stattgefunden haben und ihre

Häufigkeit daher „null“ war (vgl. ebd.). Davon abgesehen ist grundsätzlich fragwürdig, inwiefern eine Extrapolation vergangenheitsbezogener Daten in die Zukunft statthaft ist. Hier gilt es, das Postulat von (KNIGHT 1921) zu beachten, der feststellte, dass man im Bereich der statistischen Wahrscheinlichkeitslehre die „wahre“ Wahrscheinlichkeit nicht aus bestehenden Daten berechnen kann, sondern sie auf induktivem Wege aus der Untersuchung einer großen Anzahl von Fällen ableiten muss. Diese Einschränkung führt somit zu einer logischen Schwäche, da die Statistik somit bestenfalls eine Wahrscheinlichkeit davon angeben kann, was die wahre Wahrscheinlichkeit ist.

3. Die Datenbasis ist nicht immer vollständig, teils mit Streubereichen behaftet und oft liegen Daten nicht exakt für den thematisierten Anwendungsfall vor, weshalb man sich mit Daten von „ähnlichen“ Systemen bzw. Sachverhalten behilft.

Aus den vorgenannten Punkten resultiert eine große Streubreite bei den Eingangsdaten und damit beim ermittelten Risiko selbst. Die Aussagekraft von ermittelten Risikowerten ist somit begrenzt und mit einer bestimmten Streubreite behaftet, die sich im optimalen Fall als Vertrauensbereich subjektiv quantifizieren lässt (vgl. MEYNA 1982:166–168).

Außerdem wohnt dem risikobasierten Ansatz die potenzielle Anwendungsschwäche inne, dass in einem simplifizierten Ansatz das Produkt aus Schadenseintrittswahrscheinlichkeit und Schadensschwere gebildet wird, was zu Fehlinterpretationen des Ergebnisses führen kann. Denn dabei kommt die Verwendbarkeit des Risikobegriff insbesondere bei seltenen Ereignissen wie Großschadenslagen an ihre Grenze, da Ereignisse mit häufigerem Auftreten, jedoch geringerem Schaden durch die Verrechnung als schwerwiegender bewertet werden. Sogenannte low-probability/high-impact-Ereignisse hingegen, wie sie Großschadenslagen und je nach Einsatzgebiet auch der klassische „kritische Wohnungsbrand“ (HILDEBRAND 6.2.13) darstellen, werden bei einer derartigen Betrachtungsweise unterbewertet, bagatellisiert und fallen oft, etwa aus Gründen der „Wahrung praktischer Vernunft“ oder aus „ökonomischen Erwägungsgründen“, aus der Betrachtung heraus (vgl. TALEB 2010, SHEFFI 2006, ZIO 2007). Die Existenz von derartigen kaum beseitigbaren Ungewissheiten bei der Betrachtung von Sicherheitsfragen ist schon länger erkannt (KNIGHT 1921) und rückt in jüngerer Vergangenheit wieder verstärkt in den Fokus (BOECKELMANN & MILDNER 2011), (RIDDER & BARTH 2012).

14.5.2 Einschränkungen der Anwendbarkeit der Risikoanalyse für die Bedarfsplanung

Bei der Feuerwehrbedarfsplanung wird ein komplexes und kompliziertes System (vgl. RENN et al. 2007:164–165) untersucht. Die bestehenden Ungewissheiten über die weitgehend noch unbekannten Wechselwirkungen innerhalb des Systems können dort auch mit viel Aufwand kaum reduziert werden, womit eine hohe epistemische Ungewissheit systemimmanent verbleibt, zusätzlich zur grundsätzlich nicht beseitigbaren aleatorischen Ungewissheit.

Zur Frage, ob die Methode der Risikoanalyse für die Feuerwehrbedarfsplanung angewendet werden kann, muss man sich vor Augen führen, worauf eine Risikoanalyse grundsätzlich abzielt: Es wird versucht, ein Risiko zu ermitteln und zu hinterfragen, welche Ansatzpunkte zur Senkung seiner Auswirkungen und seiner Eintrittswahrscheinlichkeit bestehen (vgl. Zio 2007). Die Risikoanalyse thematisiert nicht, welche Maßnahmen zu ergreifen sind, wenn der mit dem Risiko abgeschätzte Schaden sich dann tatsächlich manifestiert und es zum Schadensereignis kommt. Dazu wäre eine direkte Ableitbarkeit der notwendigen Bewältigungskapazität aus dem ermittelten Risiko notwendig, wofür jedoch noch kein methodischer Zugang existiert.

Grundsätzlich erscheint der Ansatz einer Risikoanalyse zur Beplanung einer Feuerwehr zwar notwendig, um örtlich angepasste Lösungen zu finden und somit den gesetzlichen Auftrag der Kommunen für die feuerwehrliche Gefahrenabwehr zu erfüllen. Würden die örtlichen Bedingungen nicht berücksichtigt, wäre eine einheitliche Standard-Feuerwehreinheit in einer bundesweit einheitlichen Hilfsfrist die logische Konsequenz; macht man sich die Folgen eines solchen Ansatzes klar wird jedoch ersichtlich, dass eine solche Lösung nicht tragfähig wäre, da somit beispielsweise in einer Großstadt wie Berlin und in einem 1000-Einwohner-Dorf die gleiche Feuerwehrleistungsfähigkeit notwendig wäre, was unangemessen erscheint. Jedoch ist die Planung einer solchen angepassten „Versorgung“ mit Feuerwehrleistung nicht allein mit der Methode „Risikoanalyse“ darstellbar, da keine unmittelbare Übersetzung von Risiko in notwendigerweise vorzuhaltende Bewältigungskapazität möglich ist. Ein weiteres grundsätzliches Problem mit dem Risikoansatz besteht in der Notwendigkeit der Existenz von entsprechenden Risikoakzeptanzkriterien für die Bewertung von Risiken, die in Deutschland derzeit nicht existieren.

Weiterhin ist das Paradoxon der Berücksichtigung der Eintrittswahrscheinlichkeit zu berücksichtigen: Einerseits ist mit dem Eintritt eines Ereignisses jeder Größenart jederzeit zu rechnen, andererseits kann aus praktischen und finanziellen Gründen nicht überall für alle Ereignisse die notwendige Bewältigungskapazität vorgeplant werden. Erfahrungsgemäß stellt sich der Status quo so dar, dass mit einem „Grundstock" an Bewältigungskapazität eine große Bandbreite von Ereignissen abgedeckt werden kann („Grundschutz"). Darüber hinaus gibt es in erster Näherung eine zweite Bewältigungsstufe, für die zusätzliche Kapazitäten vorgehalten werden (siehe Bild 14.3); wächst das Ereignis quantitativ an, wird es weiterhin mit den gleichen oder zusätzlichen Kapazitäten derselben Art abgearbeitet, ggf. ergänzt um Reserve-Einheiten o. Ä. (Szenario 5 in Bild 14.3). Für eine dritte Stufe (Szenario 6 in Bild 14.3) werden üblicherweise noch gesonderte Bewältigungskapazitäten vorgehalten, allen darüber hinausgehenden Szenarien und Ereignissen kann – wenn überhaupt – noch durch quantitative Verstärkung, jedoch nicht mehr qualitativ entgegengewirkt werden (der dargestellte Zusammenhang ist als hypothetisch zu betrachten, je nach örtlicher Feuerwehrorganisation können auch mehr oder weniger „Stufen" vorliegen).

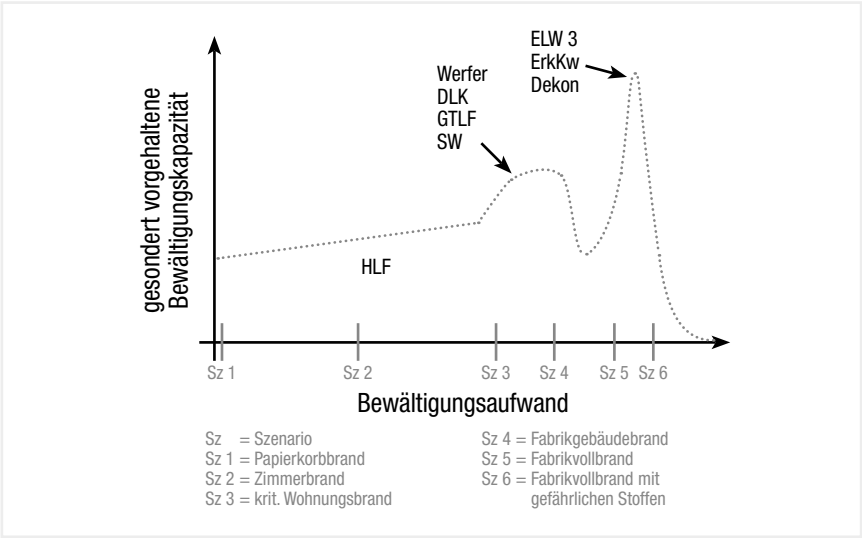

Bild 14.3: Schematische Darstellung der gesondert vorgehaltenen Bewältigungskapazität über Szenarien mit steigendem Bewältigungsaufwand

Ein solcher mehrstufiger Ansatz scheint sich in der Vergangenheit als zweckmäßig erwiesen zu haben zum Umgang mit dem Eintrittswahrscheinlichkeit-Paradoxon. Entgegen anderer Meinungen aus der Literatur, die die Berücksichtigung von Eintrittswahrscheinlichkeiten für diesen Bereich als „nicht seriös" bezeichnen und die jederzeitige Eintrittsmöglichkeit aller Ereignisse betonen (vgl. z. B. IM HESSEN 2000:4), scheint diese Größe dennoch berücksichtigenswert zu sein. Zwar gilt es dabei, Effekte wie die Schwankungen der Häufigkeiten über Jahre hinweg zu berücksichtigen. Zur praktischen Handhabung wird oftmals eine Mittelwertbildung vorgenommen. Dabei ist jedoch zu berücksichtigen, dass viele Risiken zeitlich nicht konstant sind und unterschiedliche (z. B. ansteigende und abfallende) Trends bestehen können, die bei Mittelwertbildung u. U. unterdrückt werden (vgl. FRITZSCHE 1992:28). Jedoch sind kurzfristige Voraussagen (nicht mehr als ein Jahr in die Zukunft) möglich auf Grundlage der Analyse von vergangenen Daten und deren Extrapolation; eine weiter gehende Vorhersage ist jedoch nicht möglich, da nur extrapoliert wird und keine Kenntnis über Kausalitäten vorhanden ist (vgl. CHAIKEN & ROLPH 1971:14). Bei solchen Betrachtungen können auch generelle Häufigkeitsindikatoren zugrunde gelegt werden, wie z. B. die Anzahl an Notrufen, Verletzten und Einsätzen in bestimmten Gebieten, da durch diese Häufigkeiten eine rein quantitative Beanspruchung der Feuerwehr vorliegt, der Rechnung getragen werden muss.

Gleichzeitig kann die Eintrittswahrscheinlichkeit bestimmter Ereignisse jedoch nicht alleinig ausschlaggebend sein für die Frage, ob für ein Ereignis Bewältigungskapazität vorgehalten werden sollte oder nicht; bei Anwendung der Risikoanalyse nach der „reinen" Lehre besteht sonst die Gefahr, dass durch die Übergewichtung der Eintrittswahrscheinlichkeit gegenüber der Schadensschwere die Feuerwehr keine Bewältigungskapazität vorhalten würde, da das Ereignis ja „zu selten" wäre. Hier ist jedoch der Vorhaltungscharakter der Gefahrenabwehr zu betonen, denn die Feuerwehr ist in dieser Hinsicht quasi die letzte Rückfallebene; hier nicht vorgehaltene Ressourcen werden (mit einigen Ausnahmen im Katastrophenschutz) auch von niemandem sonst vorgehalten, womit potenziell schwere Gefahrenlagen nicht mehr adäquat angegangen werden könnten.

Insofern erscheint die Verknüpfung der Methodiken von Gefahren- und Risikoanalyse sinnfällig, da bei der Gefahrenanalyse auch seltene Ereignisse vollumfänglich in die Betrachtungen mit einbezogen werden (vgl. auch SCHUBERT 2001:10–11).

14.6 Risikoakzeptanz

Wie oben schon beschrieben ist die Frage relevant, ab wann ein Risiko „klein genug“ ist, um den damit behafteten Sachverhalt als „sicher“ betrachten zu können. Dazu wurden Prinzipien zur Risikoakzeptanz entwickelt wie die Reduktion des Risikos auf ein „As Low As Reasonably Practical/Possible“-(ALARP-) Level oder die Anlehnung des akzeptierten Risikos an die „minimale endogene Mortalität“ (MEM) (EN 50126).

Allgemein akzeptierte Risikokriterien sind in Deutschland derzeit nicht vorhanden, sei es für Bereiche wie Anlagensicherheit (vgl. STEPHAN U. A. 2013:1264) als auch für die Feuerwehrbedarfsplanung. Im Ausland existieren in anderen technischen Bereichen allgemeine Akzeptanzkriterien in Form von akzeptierten Todesfallwahrscheinlichkeiten (10^{-y} Tote pro Person und Jahr, z. B. in HEALTH AND SAFETY EXECUTIVE 2001), diese können aber nicht einfach übernommen werden, da Risikoakzeptanz eine Frage der zugrunde gelegten Werte und Moralvorstellungen ist und somit eine politisch-gesellschaftliche Entscheidung, keine risikowissenschaftliche. Die Frage der Risikoakzeptanz muss darüber hinaus weiter gefasst werden. Risikoanalytisch begründeten Entscheidungen ist inhärent, dass ein wie auch immer geartetes Risiko schlussendlich als nicht weiter reduzierbar akzeptiert werden muss. Bis dato herrscht in der Diskussion über die Feuerwehrbedarfsplanung jedoch ein sicherheitsorientierter Ansatz vor, d. h. es wird davon ausgegangen, dass grundsätzlich die Sicherheit aller Beteiligten gewährleistet wird, also „immer jeder“ gerettet werden kann. Zwar ist den beteiligten Entscheidern vermutlich bewusst, dass dies faktisch nicht möglich ist. Eingang in die relevanten Planungsgrundlagen hat dieses Bewusstsein jedoch bis dato noch nicht gefunden (bzw. nur implizit in Form von sog. Erreichungsgraden), da andernfalls bereits beispielsweise darüber diskutiert worden wäre, wie viele Brandtote in Deutschland pro Jahr akzeptabel sind, in wie vielen Fällen es akzeptabel wäre, wenn die Feuerwehr nicht rechtzeitig eintrifft, oder wie oft es akzeptabel ist, dass sie nicht in ausreichender Bewältigungskapazität vor Ort wäre.

Weitere relevante Prinzipien zur Risikoakzeptanz sind das Prinzip des „de minimis"-Risikos (ARNDT 2011) und das sog. „Vorsorgeprinzip" (ARNDT 16.5.11, Kommission der Europäischen Gemeinschaften 2000).

Grundsätzlich bleibt festzuhalten, dass politisch verantwortet werden muss, was ein „zumutbares Risiko" ist und welche Risiken „zu hoch" sind. Die politische Verantwortlichkeit ergibt sich aus dem Umstand, dass aufgrund der Natur des Risikobegriffs wissenschaftlich keine „absoluten" und „festen" Vorgaben darüber ermittelt werden können, was „sicher" ist und was nicht. Die dennoch zu treffende Entscheidung muss ethisch-moralisch bewertet werden, was nicht der Anwendungsbereich der ingenieursmäßigen Betrachtung ist. Vielmehr müssen die Politiker als Volksvertreter diese Entscheidung unter Wahrung jeweiliger gesellschaftlicher Konventionen und Konsense treffen (vgl. auch EUROPÄISCHE KOMMISSION 2000:4). Dies gilt für den grundsätzlichen Umgang mit Risiken genauso wie für die Feuerwehrbedarfsplanung, wie z. B. in (LSTE o. J.) zum Ausdruck gebracht:

„Das angestrebte Sicherheitsniveau ist eine Entscheidung des kommunalen Aufgabenträgers. Die Willensbildung und der Beschluss dieses Sicherheitsniveaus erfolgen durch die gewählten Mandatsträger und führen zu einer Selbstbindung."

14.6.1 Definition von Überlastungsrisiko-Akzeptanzkriterien

Auch für das beschriebene Überlastungsrisikos müssen Risikoakzeptanzkriterien definiert werden. Jede Überschreitung dieser Kriterien stellt einen Überlastungsfall dar und wird zur Berechnung dessen Eintrittswahrscheinlichkeit verwendet. Dazu ist zu klären, was jeweils unter „definierter Zeit" sowie unter „vorbestimmter Effektivität" der Schadensminimierung zu verstehen ist. Der aus Sicht der Schadensentstehung wichtigste Parameter ist dabei die notwendige Effektivität, also die Frage, wie der Sollzustand aussehen soll; entsprechende zeitliche Festlegungen lassen sich dem unterordnen. Je nach Level der örtlich zu definierenden Risikoakzeptanz können unterschiedliche akzeptable Sollzustände definiert werden, unterteilt nach Sach- und Personenschaden. Diese lassen sich anhand von verschiedenen Parametern unterschiedlicher Ausprägungsoptionen matrizenhaft beschreiben (s. folgende Tabelle).

So muss grundsätzlich der Zeitraum definiert werden, in dem die Einhaltung der Akzeptanzkriterien geprüft werden soll; eine Möglichkeit ist die Vorgabe, dass Personen- und Sachschaden während des gesamten Ereignisverlaufes unterhalb der Risikoakzeptanzkriterien bleiben sollen. Das ist insofern das strengere Kriterium, da diese Maßgabe nur Sinn macht, wenn sie mit Anforderungen an die Eintreff- und Entwicklungszeit verknüpft wird, denn nur so kann die Feuerwehr darauf Einfluss nehmen. Bei der anderen Vorgabe würde sich die Feuerwehr auf ihren unmittelbaren Einflussbereich beschränken, indem nur die Zeit ihrer Anwesenheit an der Einsatzstelle zur Betrachtungsgrundlage erklärt würde.

Parameter	Mögliche Ausprägungsoptionen	
Personenschaden:		
Betrachtungszeitraum	gesamte Ereignisdauer	nach Einsatzbereitschaft der Fw an der Einsatzstelle
Anzahl der Betroffenen	1	n
Schadensschwere[1]	verletzt	tot
Bezugsgröße	pro Ereignis	pro Zeitraum (z. B. 1 a)
Sachschaden[2]:		
Betrachtungszeitraum	gesamte Ereignisdauer	nach Einsatzbereitschaft der Fw an der Einsatzstelle
Unvermeidbare[3] Schadensausweitung über Ausgangsstelle hinaus	keine	Brandraum, Brandwohnung, Brandetage/-gebäude, andere Bereiche
Grad der Schädigung	oberflächlich, beseitigbar	vollständig, irreparabel
Bezugsgröße	pro Ereignis	pro Zeitraum[4]

1 Detailliertere Abstufungen, z. B. mit Unterscheidung reversibler/irreversibler Verletzungen sind denkbar, erscheinen jedoch wenig praktikabel in der Umsetzung.
2 Monetäre Schadenskategorien sind erfahrungsgemäß seitens der Feuerwehr kaum zu erfassen und würden reine Schätzwerte darstellen, die kaum valide wären.
3 U. U. ist eine Ausweitung des Sachschadens unvermeidlich, z. B. durch Abnehmen des Daches bei der TH, um die Rettung zu ermöglichen.
4 Dann jeweils mit Angabe der zulässigen prozentualen Anteile, z. B. „in nicht mehr als 30 % der Ereignisse Schadensausweitung auf die Brandwohnung nach Eintreffen der Feuerwehr".

Tabelle 14.1: **Parameter für Risikoakzeptanzkriterien**

Weiterhin müsste postuliert werden, wie viele Betroffene welcher Schadensschwere als akzeptabel betrachtet werden, also z. B. fünf Tote pro Jahr oder zwei Verletzte pro Einsatz. Als ergänzender Indikator könnte der Anteil der tatsächlich geretteten von den gefährdeten Personen ermittelt werden, der genauere Aussagen über die Leistungsfähigkeit der Feuerwehr zulässt (vgl. RIDDER, KIßLINGER & BARTH 2014).

Im Bereich des Sachschadens ist zu den grundlegenden Parametern zu ergänzen, welche Schadensausweitung über die Ausgangsstelle hinaus akzeptiert wird, detailliert durch die Angabe des jeweiligen Schädigungsgrades pro geschädigtem Bereich/Gegenstand.

Einschlägige statistische Erfahrungswerte in Abhängigkeit der Eintreffzeit vorausgesetzt, lässt sich aus den gewählten Risikoakzeptanzkriterien unmittelbar ableiten, welche Eintreffzeiten als akzeptabel betrachtet werden können.

14.6.2 Risikoakzeptanzkriterien als Qualitätsindikatoren

Die so definierten Risikoakzeptanzkriterien können unmittelbar auch als Qualitätsindikatoren verwendet werden; gegenüber tradierten Konzepten wie z. B. (AGBF BUND 1998) stellt diese Vorgehensweise insofern einen Paradigmenwechsel dar, als dass keine Input-, sondern eine Output-orientierte Betrachtungsweise verwendet wird. Denn statt zu messen, wie schnell wie viele Funktionen in welchem Anteil der Fälle vor Ort waren (ohne Berücksichtigung des Einsatzverlaufes und -erfolges i. S. v. Outcomes), wird gemessen, wie gut die gesetzten Ziele erreicht wurden, in erster Näherung unabhängig von den eingesetzten Ressourcen.

Die dazu notwendigen Daten werden in heutigen fortschrittlichen Berichtswesen-Systemen von Feuerwehren schon erhoben, müssten ggf. zusätzlich detailliert werden und eine gleichbleibend hohe Güte der berichteten Daten durch Optimierung des Erfassungsprozesses sollte sichergestellt werden.

14.7 Fazit

Die Berücksichtigung von Risiken bei der Feuerwehrbedarfsplanung sollte sich von einer intuitiven, erfahrungsbasierten Sichtweise der Feuerwehrpraktiker hin zu einem informierten Umgang mit Entscheidungsalternativen durch die politischen Mandatsträger entwickeln. Vor allem diesen Entscheidungsträgern muss seitens der Fachleute (Feuerwehrangehörige und Sicherheitswissenschaftler) methodische Hilfestellung zur Entwicklung einer „Risikokompetenz" gegeben werden.

Die Risikobeurteilung ist kein isoliert zu betrachtendes methodisches Werkzeug, sondern einzubetten in einen umfänglichen Risikomanagement-Prozess; vor allem entsprechende Risikoakzeptanzkriterien sind vorzugeben. Risiken existieren nicht „da draußen" und warten darauf, gemessen zu werden. Obwohl diese Gefahren real sind, gibt es kein „reales Risiko" oder „objektives Risiko" (SLOVIC 2002). Immer bedarf es der Interpretation durch den Bewertenden, um eine Aussage darüber treffen zu können, ob eine Situation „sicher" ist bzw. ob ihr ein „akzeptables" Risiko innewohnt, oder ob das Risiko „zu hoch" ist. Diese Einschätzung ist somit immer relativ, hängt stark von den kulturellen und gesellschaftlichen Normen und sonst üblichen Sicherheitsniveaus ab und kann daher stark schwanken. Sie darf somit nicht als absolute, „harte" Grenze betrachtet werden, die quasi naturgesetzliche Geltungskraft hätte.

Für eine alleinige Anwendung der Risikobeurteilung als Planungsmethodik bestehen zu viele Anwendungsgrenzen, weshalb eine auf den Untersuchungsgegenstand angepasste Methodik zur Risikobeurteilung nötig ist. Eine Bedarfsplanung ganz ohne Berücksichtigung von „Risiko" (Eintrittswahrscheinlichkeit & Schadensschwere) ist nicht machbar. Eine Bedarfsplanung ist jedoch aktuell auch nicht rein risikobasiert machbar, sondern muss – aufbauend auf einer Gefahrenanalyse – ergänzt werden um den Ansatz des Bewältigungsaufwandes und der Bewältigungskapazität sowie den szenariobasierten Ansatz.

Weitere Forschungen sind nötig zur Verbesserung des methodischen Zugangs und zur Erhebung statistischer Grunddaten. Nur so kann der Übergang von der intuitiven, subjektiven Einschätzung von Risiken hin zu einem analytisch fundierten und von den verantwortlichen Stellen getragenen, bewussten Umgang mit Risiken gelingen.

Danksagung

Das diesem Bericht zugrunde liegende Forschungsvorhaben „TIBRO – Innovative Sicherheitsarchitektur der nichtpolizeilichen Gefahrenabwehr“ wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 13N12174 gefördert. Die Verantwortung für den Inhalt liegt beim Autor.

Literatur

2004. Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz des Landes Brandenburg: (Brandenburgisches Brand- und Katastrophenschutzgesetz – BbgBKG).
2009. Verordnung über die Mindeststärke und -ausrüstung der Freiwilligen Feuerwehren: MindAusrVO-FF.

AG Arbeitshinweise Risikoanalyse (AG Risikoanalyse) 2009. Arbeitshinweise Risikoanalyse. AGBF Bund 1998. Empfehlungen der Arbeitsgemeinschaft der Leiter der Berufsfeuerwehren für Qualitätskriterien für die Bedarfsplanung von Feuerwehren in Städten. URL: http://www.agbf.de [Stand 12.7.12].

Aguirre, Felipe, u. a. 2013. On the distinction between aleatory and epistemic uncertainty and its implications on reliability and risk analysis, in Steenbergen, Raphael D., u. a. (Hg.): Safety, Reliability and Risk Management: Beyond the Horizon: ESREL 2013. London: Taylor & Francis Group Ltd, 3221–3227.

Arbeitskreis Brandschutzbedarfsplan NRW (AK BSBP NRW) 2001. Hinweise und Empfehlungen für die Anfertigung von Brandschutzbedarfsplänen für die Gemeinden des Landes Nordrhein-Westfalen.

Arndt, Volker 16.5.11. Methoden der Schwachstellen- und Risikoanalyse. Frankfurt am Main.

Arndt, Volker 2011. Vom Risiko zum Sicherheitskonzept: Bewährte Methoden und Werkzeuge. atp edition – Automatisierungstechnische Praxis(1-2), 28–31.

Bjerga, T. & Flage, R. 2013. On black swans in relation to some common uncertainty classification system, in Steenbergen, Raphael D., u. a. (Hg.): Safety, Reliability and Risk Management: Beyond the Horizon: ESREL 2013. London: Taylor & Francis Group Ltd, 3197–3202.

Boeckelmann, Lukas & Mildner, Stormy-Annika 2011. Unsicherheit, Ungewissheit, Risiko: Die aktuelle wissenschaftliche Diskussion über die Bestimmung von Risiken. SWP-Zeitschriftenschau(2). Online im Internet: URL: http://www.swp-berlin.org [Stand 2013-05-06].

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) 2010. Methode für die Risikoanalyse im Bevölkerungsschutz. Bonn. (Wissenschaftsforum, 8).

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) 2011. BBK-Glossar: Ausgewählte zentrale Begriffe des Bevölkerungsschutzes. (Praxis des Bevölkerungsschutzes, Band 8). Bonn.

Chaiken, Jan M. & Rolph, John E. 1971. Predicting the Demand for Fire Service. P-4625. URL: http://www.rand.org.

Committee on Risk Characterization (CRC) 1996. Understanding Risk: Informing Decisions in a Democratic Society: Informing Decisions in a Democratic Society. Washington D.C.: National Academies Press.

Compes, Peter C. 1973. Modell zur Unfallkausalität und zum Störfall im „Mensch-Umgebungs-System“, in Thiele & Gottschalk (Hg.): Literatur-expertise über theoretische Grundlagen des Arbeitsschutzes. Dortmund.

Edner, Dennis 2013. Analyse von in der Feuerwehr-Bedarfsplanung verwendeten Hypothesen anhand realer Einsatzdaten einer großstädtischen Feuerwehr. Master-Thesis. Bergische Universität Wuppertal (BUW).

European Committee for Electrotechnical Standardization (CENELEC) 1999. Bahnanwendungen: Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS). (Bd. 29.280; Bd. 45.020).

Faasch, Hans-Günther 1972. Strukturuntersuchung des Einsatzdienstes der Feuerwehr Hamburg. BrandSchutz – Deutsche Feuerwehrzeitung (11), 355–358.

Fritzsche, Andreas F. 1992. Wie gefährlich leben wir?: Der Risikokatalog. Köln: Verl. TÜV Rheinland.

Grabski, Reinhard 2007. Erarbeitung einer Risikoanalyse für die Ausrüstung sowie die Anzahl der zu besetzenden Funktionen einer Gemeindefeuerwehr: Instituts-Bericht Nr. 437. Heyrothsberge.

Health and Safety Executive 2001. Reducing Risks, Protecting People: HSE's decisions-making process: HSE Books. Online im Internet: URL: http://www.lob.de.

Hessisches Ministerium des Innern und für Sport (IM Hessen) 2000. Gefährdungsanalyse für das Land Hessen. Wiesbaden. URL: http://www.rheingau-taunus.de [Stand 24.09.2012].

Hildebrand, Thomas 6.2.13. Statistische Einsatzdatenanalyse zur Abschätzung der Relevanz des kritischen Wohnungsbrandes für unterschiedlich strukturierte Gemeinden. Bachelor-Thesis. Bergische Universität Wuppertal (BUW).

International Organization for Standardization (ISO) 2009. Risk management – Vocabulary. Genf: ISO.

International Organization for Standardization (ISO) 2009. Risk management – Principles and guidelines. Genf: ISO.

Knight, Frank H. 1921. Risk, Uncertainty, and Profit. Boston M. A. URL: http://www.econlib.org [Stand 06.05.2013].

Knorr, Karl-Heinz 2012. Sitzung des Arbeitskreises Grundsatzfragen (AK-G) der AGBF-Bund: Die Schutzzieldefinition ist weiter uneingeschränkt gültig. BrandSchutz – Deutsche Feuerwehrzeitung(2), 132–133.

Kommission der Europäischen Gemeinschaften (Europäische Kommission) 2000. Mitteilungen der Kommission: Die Anwendbarkeit des Vorsorgeprinzips. Brüssel. URL: http://eur-lex.europa.eu [Stand 16.9.2013].

Landesschule und Technische Einrichtung für Brand- und Katastrophenschutz Brandenburg (LSTE) o. J. Hinweise und Empfehlungen zur Durchführung einer Gefahren- und Risikoanalyse und zur Erstellung eines Gefahrenabwehrbedarfsplanes im Land Brandenburg. Eisenhüttenstadt.
URL: http://www.lste.de [Stand 26.9.2013].

Langer, Sandro 2013. Analyse von in der Feuerwehr-Bedarfsplanung verwendeten Risikofaktoren für Wohngebäude anhand realer Einsatzdaten. Bachelor-Thesis. Bergische Universität Wuppertal (BUW).

Meyna, Arno 1982. Einführung in die Sicherheitstheorie: Sicherheitstechnische Analyseverfahren; mit 28 Tabellen. München, Wien: Hanser.

Österreichisches Normungsinstitut (ON) 2010. Risikomanagement – Grundsätze und Richtlinien (ISO 31000:2009). (03.100.01).
Wien: Österreichisches Normungsinstitut.

Renn, Ortwin, Schweizer, Pia-Johanna, Dreyer, Marion & Klinke, Andreas (2007): Risiko. Über den gesellschaftlichen Umgang mit Unsicherheit. München: Oekom-Verlag.

Ridder, Adrian 2013. Methodische Ansätze zur datenbasiert-analytischen Risikobeurteilung zur strategischen Planung von Feuerwehren, in Hochschule Magdeburg-Stendal & Otto-von-Guerike-Universität Magdeburg (Hg.): Tagungsband. Magdeburg.

Ridder, Adrian & Barth, Uli 2012. Methodische Ansätze zur organisationalen Business Resilience am Beispiel einer Werkfeuerwehr. vfdb-Zeitschrift für Forschung, Technik und Management im Brandschutz 61(3), 111–122.

Ridder, Adrian, Kißlinger, Albert & Barth, Uli (2014): Methodische Zugänge zur zukünftigen strategischen Planung von Feuerwehren. In: Vereinigung zur Förderung des deutschen Brandschutzes e.V. (vfdb) (Hg.): Tagungsband der 62. Jahresfachtagung der Vereinigung zur Förderung des Deutschen Brandschutzes e.V. Dortmund, 16.–18.06.14. Vereinigung zur Förderung des deutschen Brandschutzes e.V. (vfdb), S. 29–52.

Schmid, Christian 2014. Methodische Ansätze zum systemischen Szenario-Design für die strategische Planung von Feuerwehren unter Berücksichtigung gefährdungs- und risikobasierter Ansätze.
Master-Thesis. Bergische Universität Wuppertal (BUW).

Schubert, René 2001. Risikoanalyse. Hausarbeit im Rahmen der Staatsprüfung für den höheren feuerwehrtechnischen Dienst. Essen.

Sheffi, Yossi 2006. Worst-case-Szenario: Wie Sie Ihr Unternehmen auf Krisen vorbereiten und Ausfallrisiken mindern ; [Lieferengpässe und Produktionsstörungen – Energiepreissteigerungen und Währungsschwankungen – Streiks und Naturkatastrophen]. Landsberg am Lech: mi.

Slovic, Paul 2002. The perception of risk.
London: Earthscan Publications.

Stephan, Thomas A. et al. 2013. Probabilistische Analysen zur Anwendung in der Anlagensicherheit.
Chemie – Ingenieur – Technik 85(8), 1263–1271.

Taleb, Nassim 2010. The black swan: The impact of the highly improbable.
2. Aufl. London: Penguin.

van der Schaaf, J. & Jeulink, J. 1992. Handleiding Brandweerzorg: Systeem voor de beoordeling van de gemeentelijke brandweerzorg. Den Haag.
URL: https://www.infopuntveiligheid.nl [Stand 05.08.2013].

Zio, Enrico 2007. An introduction to the basics of reliability and risk analysis.
Singapore: World Scientific. (Series in Quality, Reliability and Engineering Statistics, Bd. Vol. 13Bd).

15

Ansätze zur Vermittlung von Risikokompetenz

15.1 Risiken und ihre Rolle im System Mensch – Technik – Gesellschaft

Prof. Dr. Dr. Juraj Sinay; Technische Universität in Kosice, GfS, Slowakische Republik

„Safety first – Sicherheit an erster Stelle" – „Vision Zero – Vision der Nullzahl von Unfällen", dies sind Gedanken, die in der Gegenwart auf allen Gebieten des gesellschaftlichen Lebens eine absolute Priorität haben. In der Zeit, in der sich die Gesellschaft um eine komplexe Beurteilung der Sicherheit des Systems Mensch – Technik – Gesellschaft bemüht, steht dieser Gedanke in Bezug nicht nur zur klassischen Sicherheit und zum Arbeits- und Gesundheitsschutz oder der Sicherheit von Maschinen und Maschinensystemen, sondern auch in Bezug zum Bevölkerungsschutz. Die Erfahrung sowie die gesellschaftliche und technologische Entwicklung haben bestätigt, dass es unter gegenwärtigen Bedingungen des Gesellschaftszustandes nicht möglich ist, die Rolle des Menschen zu ersetzen, und dass die Schnittstelle Mensch – Technik – Gesellschaft ständig aktuell bleibt.

Das Risikomanagement kann als Integration einzelner Gebiete wahrgenommen werden, deren Ziel ist, die Sicherheit im System Mensch – Technik – Gesellschaft zu gewähren. Daraus kann abgeleitet werden, dass das Risikomanagement den Bestandteil der Wissenschaft über die Sicherheit bildet. Noch vor einigen Jahren behaupteten die Experten, dass die Sicherheitstechnik in die Gruppe der technischen Wissenszweige gehöre. Es wurde vorausgesetzt, dass sich die Automatisierung in den meisten Bereichen der Technik schnell durchsetzen wird, wodurch sich der menschliche Faktor in einem wesentlich kleineren Maße an der Entstehung der negativen Erscheinungen in der Technik sowie im Rahmen der gesellschaftlichen Beziehungen beteiligen wird. Die Entwicklung der Technik auch als Bestandteil des gesellschaftlichen Lebens bestätigte eindeutig, dass es eine Menge Gebiete gibt, in denen man die Rolle des Menschen nicht ersetzen kann.

Die Risiken in einer modernen Industriegesellschaft sind von einer Menge Faktoren abhängig, die oft nicht Gegenstand der gegenwärtigen wissenschaftlichen und technischen Bereiche sind – es handelt sich um neue und neu entstehende Risiken. Die Sicherheitstechnik und damit auch die Systeme der Risikosteuerung entwickeln Methoden und Verfahren so, dass es möglich ist, den Einfluss möglichst komplex – also aus allen Bereichen – zu berücksichtigen, die an der Risikoentstehung beteiligt sind. Der Fachmann auf dem Gebiet der Sicherheit und des Arbeits- und Gesundheitsschutzes, in der Sicherheit von technischen Systemen, aber auch auf dem Gebiet des Bevölkerungsschutzes sollte Kenntnisse und Erfahrungen bzw. Fertigkeiten eines Maschinenbauers, Elektrikers, Physikers, Chemikers, Psychologen, Soziologen, Arztes eventuell anderer Fachleute in sich integrieren. Selbstverständlich können weder ein einzelner Mensch noch eine kleine Gruppe von Fachleuten in der Lage sein, so eine umfangreiche Datenbasis von Informationen zu gewinnen, diese auszuwerten und sie nachher entsprechend einzusetzen. Deshalb wird von einem qualifizierten Fachmann im Bereich der Sicherheit gefordert, dass er sich durch die Fähigkeit auszeichnet, neue Informationen aufzunehmen, diese zu sortieren, ihre Wichtigkeit und Bedeutung zu beurteilen und nachfolgend Bedingungen für die Teamarbeit zu schaffen. Die Bedingung dazu ist, dass alle legislativen Vorschriften, ob auf der Ebene der Europäischen Union z. B. die Richtlinien 391/89/ES oder 42/2006/ES, die anspruchsvollen Bedingungen definieren, die an die Integration der Anforderungen der Sicherheit in eigene Produkte bzw. Produktionstechnologien gestellt sind.

Die Tätigkeiten im Rahmen des Risikomanagements erfordern die Kenntnis von komplizierten (mehrparametrischen) Beziehungen zwischen der Technik (Maschinen und Maschinensysteme), der Arbeitsorganisation und dem Humanfaktor (Bedienung, Beschäftigte). Die Intensität dieser Tätigkeiten wird durch die Bedürfnisse der Gesellschaftssysteme, durch die Entwicklungsstufe und das Niveau der vorhandenen Erkenntnisse als auch durch Forschungsergebnisse im Bereich der Risiken bestimmt.

Neue Einstellungen im Rahmen des Sicherheitsmanagements erfordern in all ihren Formen, dass sich jeder Mensch der Risiken bewusst wird, mit denen er am Arbeitsplatz wie auch im täglichen Leben umgehen muss. Es ist auch in dieser Phase wichtig, in der der Mensch der Gestalter von Gegenständen (z. B. Maschinen, Maschinensysteme, Arbeitsplätze) zur Nutzung in unterschiedlichen Industrietechnologien ist, d. h. er hat die Möglichkeit, die Risiken schon am Anfang ihres technischen Lebens zu beeinflussen.

In diesem Zusammenhang ist das Zitat von Prof. Henning Kagermann aus dem DE Magazin Deutschland 4/2013 angebracht, wo er im Artikel „Eine Vision für die Wirtschaft von morgen“ auf Seite 31 anführte: „Auf technischer Ebene ist entscheidend, Sicherheit als Konstruktionsprinzip – Security by design – zu etablieren.“

Zur Sicherung der Bedingungen einer sicheren Arbeit ist die Anwendung von effektiven Vorbeugungsmaßnahmen mit dem Ziel notwendig, dem humanen Faktor auf dem Arbeitsplatz eine intensive Aufmerksamkeit zu widmen. In diesem Zusammenhang ist es die Pflicht des Maschinen- und des Maschinensystembenutzers, die Risiken am Arbeitsplatz zu identifizieren und Maßnahmen zu ihrer Abschaffung bzw. Minimierung zu treffen und damit die Bedingungen zum Einsatz wirksamer Vorbeugungsmaßnahmen zu schaffen. Die Fähigkeit, diese Maßnahmen zu realisieren, erfordert eine multidisziplinäre Einstellung, was wiederum die Einführung der Systeme zur Ausbildung der Fachleute voraussetzt, um angemessene Kompetenzen zu gewinnen.

15.2 Kompetenz und Qualifikationen

Ungefähr seit 1990 wird in den Fachkreisen von der Kompetenz als Qualifizierung der Fachleute gesprochen. Die Qualifizierung wird als Voraussetzung zur Durchführung bestimmter Tätigkeiten erforderlich. Dies ist dadurch gegeben, dass sie vor allem die Erfüllung der definierten Bedingungen zur Durchführung der Tätigkeiten im Rahmen eines konkreten Tätigkeitsgebietes umfasst, die an die persönlichen Voraussetzungen gebunden sind. Die Kompetenzen werden im Allgemeinen nicht auf konkrete Berufe oder Tätigkeiten bezogen, sondern mehr auf allgemeine Fähigkeiten (Veranlagungen) des Menschen zur Bewältigung wichtiger Anforderungen, die aus dem Charakter der Applikation von effektiven Vorbeugungsmaßnahmen hervorgehen. Sie richten sich nicht nur auf theoretische, im Ausbildungsprozess erworbene Erkenntnisse, sondern die erworbenen Erfahrungen werden berücksichtigt. Der Begriff „Schlüsselqualifikationen“ wird manchmal als Synonym zum Begriff „Kompetenz“ verwendet.

Die Kompetenz schließt Erfahrungen, Fertigkeiten, Kenntnisse als Bestandteil der Qualifikation, Erkenntnisse und Kommunikationsfähigkeiten mit ein. Eine der entscheidenden Kompetenzen ist die sog. Fachkompetenz oder Kompetenz in einem Fachbereich.

15.2.1 Kompetenzen im Rahmen des Risikomanagements

Die Kompetenzen für das Gebiet der Risikosteuerung schließen ein
(siehe Bild 15.1):

- Kenntnisse (Erkenntnisse) in verschiedenen Wissensbereichen und ihre koordinierte Nutzung in einzelnen Gebieten als Bestandteil einer komplexen Risikobeurteilung,
- praktische Erfahrungen und Fertigkeiten im Bereich der Applikation von Risikomanagementsystemen, erworben während konkreter Tätigkeiten der Maschinen und Maschinensysteme.

- Weder Sicherheit, noch Risiken kennen Staatsgrenzen – sie sind Bestandteil der globalisierten Arbeitsmärkte.
- Existenz des europäischen Ausbildungs- und Forschungsraumes und seine Tätigkeit in den Strukturen in der Welt,
- Identifizieren der minimalen Anforderungen auf den Kompetenzkern, die die Basis zur Schaffung eines Pakets von geforderten Kenntnissen in Form einer Ausbildungsgrundlage bilden müssen – dieses Paket muss Grundanforderungen enthalten, die aus der europäischen Legislatur unter den EU-Bedingungen sowie aus den nationalen Legislaturvorschriften hervorgehen.

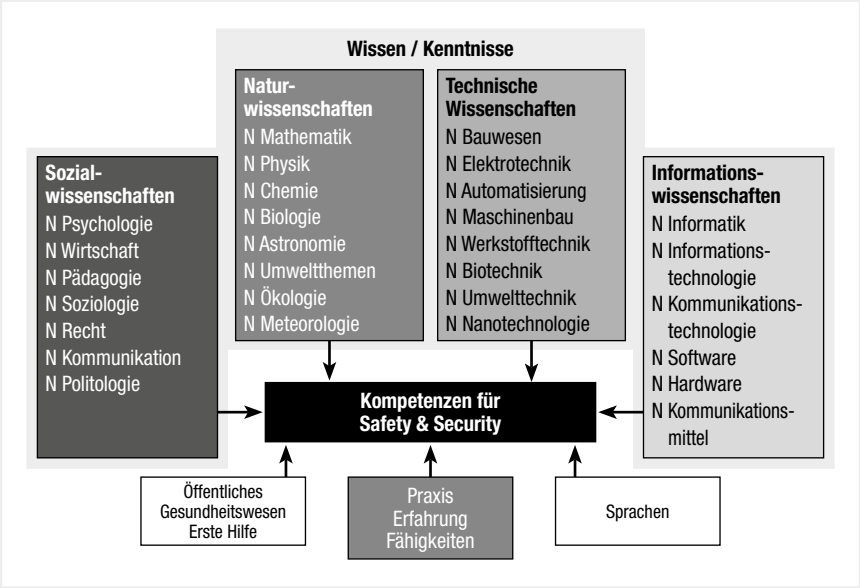

Bild 15.1: **Definieren der Kompetenzbestandteile für das Gebiet Safety wie auch Security**

- Möglichkeit der Bildung von internationalen Ausbildungsnetzen, die die Bedingungen der nationalen Ausbildungssysteme in allen ihren Formen berücksichtigen,
- Nutzung des Feedbacks zwischen dem Gestalter bzw. Konstrukteur und dem Benutzer von Maschinen und Maschinensystemen und ihren Gestaltern laut Bild 15.2,
- aktive Tätigkeit im Rahmen des Transfers von Erkenntnissen.

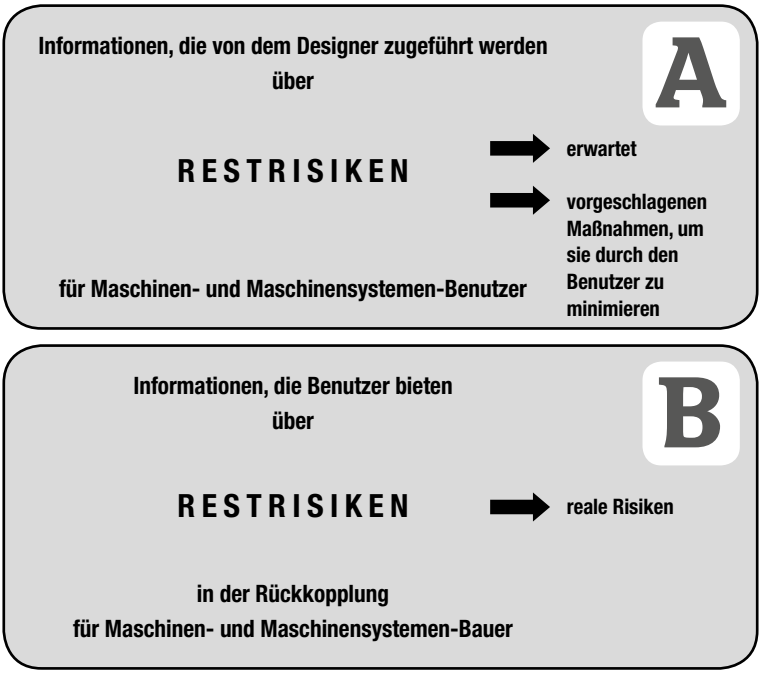

Bild 15.2: Kommunikationen zwischen den Akteuren der Nutzung von Maschinen und Maschinensystemen

Die Fachleute im Bereich der Risikosteuerung und damit auch im Rahmen des Arbeits- und Gesundheitsschutzes nutzen ihre Kompetenzen vor allem auf diesen Gebieten:

1. Risikosteuerung (Arbeits- und Gesundheitsschutz) innerhalb der Gesellschaft bzw. des Betriebes, in Übereinstimmung mit der gültigen Legislative im Einverständnis mit den Prinzipien der Firmenkultur,

2. Gewährung eines aktiven Gesundheitsschutzes aller Menschen in Zusammenarbeit mit dem Topmanagement der Firma, mit den Topmanagern und in Zusammenarbeit mit den nationalen Autoritäten für das Gebiet des Arbeits- und

Gesundheitsschutzes mit dem Ziel, Gefahren, Gefährdungen, Risikobeurteilung auf verschiedenen Tätigkeitsgebieten im Rahmen des Unternehmens zu identifizieren,

3. Risikoabschaffung und -minimierung als Bestandteil effektiver Vorbeugungsmaßnahmen.

15.2.2 Aufgaben- und Kompetenzstellung

Die Verantwortungs- und Aufgabengebiete der leitenden Mitarbeiter im Bereich der Arbeitssicherheit sowie die geforderten Kompetenzen müssen genau festgelegt werden. Dies gilt auch für die Entscheidungsbereiche. Es handelt sich dabei um folgende Anforderungen:

- Die leitenden Mitarbeiter kennen ihre Pflichten auf dem Gebiet des Sicherheits- und des Gesundheitsschutzes.
- Die Pflichten des Arbeitgebers werden schriftlich formuliert und an die Fachleute für Risikosteuerung in der Firma delegiert.
- Die Aufgaben aller Akteure im Risikomanagementsystem sind gegenseitig abgestimmt und so definiert, dass sie genug Zeit zu ihrer Realisierung zur Verfügung haben.
- Die Kompetenzen der leitenden Mitarbeiter sind genau definiert.
- Form und Inhalt der Vertretbarkeit sind gewahrt.

15.3 Ausbildung als Bestandteil des Erwerbens von Kompetenzen

Die Kompetenz eines Fachmanns muss von seinen Fachkenntnissen ausgehen. Nur in diesem Falle kann er Partner von Fachleuten in der Etappe des Planens und Konstruierens, des Ankaufs, des Entwurfes von geeigneten technologischen und logistischen Prozessen, der Auswahl der passenden Materialien, der Herstellung, des Prüfens und der Wahl der Strategie der Instandhaltung sowie bei der Realisierung verschiedener Ausbildungsgebiete sein.

Das rechtzeitige Identifizieren von komplexen Beziehungen ist das Wesen des Definierens der Risiken und Voraussetzung für Entscheidungsprozesse der Topmanager vor, während und nach einer negativen Erscheinung (Krise). Deshalb müssen auf dem Gebiet der Ausbildung solche Bedingungen geschaffen werden, dass die leitenden Fachleute im Bereich der Sicherheit (Risikosteuerung) nicht nur Fachkenntnisse gewinnen, sondern auch Fähigkeiten, alle Tätigkeiten im Rahmen der Vorbeugungsmaßnahmen zu leiten.

Einige der Module zur Gewinnung von Kompetenzen im Rahmen der Risikosteuerung können folgenderweise definiert werden (siehe Bild 15.3):

- Identifizierung von Risiken – multidisziplinäre Einstellung,
- Risikoanalyse und -abschätzung – Verknüpfung der naturwissenschaftlichen (mathematische Statistik) und der technischen Einstellung,
- Methodenapplikation zur Risikominimierung – Vorbeugung – in Form der multidisziplinären Einstellung,
- Training und Ausbildung unter Berücksichtigung des juristischen Rahmens,
- Management der kritischen Situationen – Erfahrungen und Fertigkeiten im Rahmen der Risikosteuerung unter den Bedingungen der Industriepraxis,
- effektive Kommunikation (Arbeit mit Öffentlichkeit, Vermittlung von Informationen über den Risikoeinfluss in der Gesellschaft).

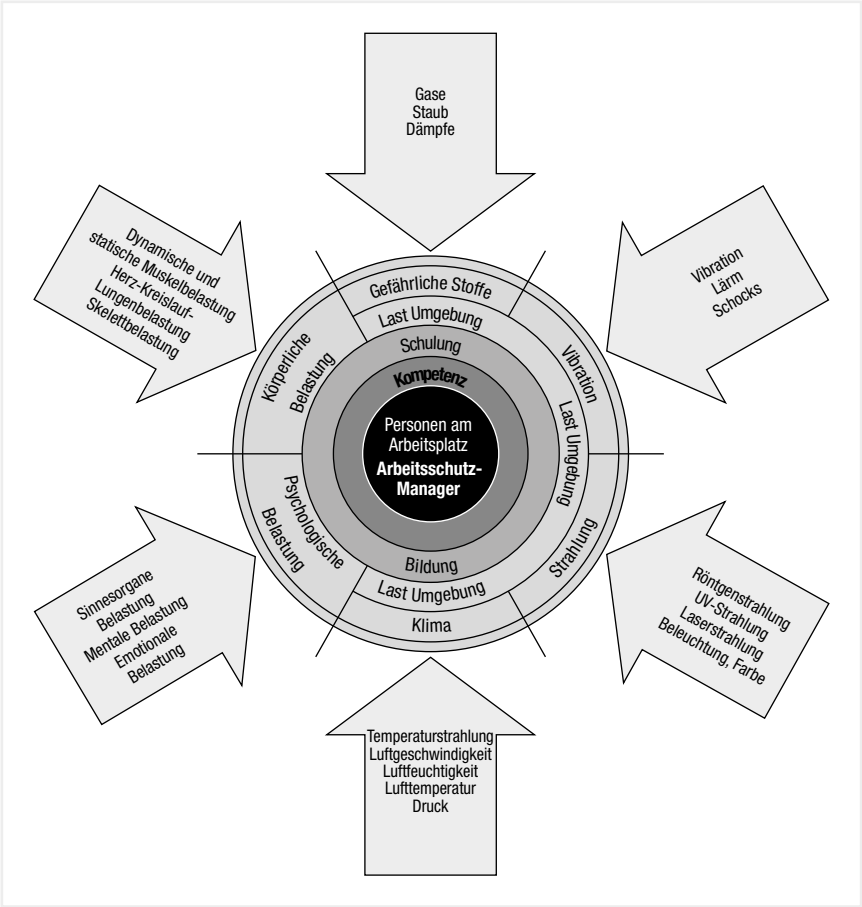

Bild 15.3: **Modell der Kompetenzvermittlung durch einen Fachmann im Bereich der Risikosteuerung**

Die Entwicklung auf allen Gebieten der Arbeitssicherheit stellt erhöhte Ansprüche an die Beschäftigten zum Lernen. Heutzutage bildet das lebenslange Lernen einen Bestandteil der Bereitschaft zur Bewältigung der Änderungen auf dem Arbeitsmarkt. Dies gilt für die Studenten des Bachelor- als auch die des Ingenieurstudiums an den Hochschulen, an denen die Sicherheit als ein selbstständiges Studienprogramm oder als Bestandteil der Studienpläne anderer Studienbereiche unterrichtet wird. Die zur Lösung der Fragen der Sicherheit und des

Arbeits- und Gesundheitsschutzes in einem Unternehmen erforderliche Fachkompetenz muss von den Fachleuten für diesen Bereich gewährleistet werden, allerdings die Unternehmenskultur der Sicherheit muss von allen Beschäftigten gewährleistet werden, die sich der Bedeutung und der Vorbeugungsaufgabe im Rahmen aller Tätigkeiten im Unternehmen bewusst sind.

Die gegenwärtigen Ausbildungssysteme vor allem auf dem Gebiet des Bachelor- und des Ingenieurstudiums sowie in der Forschung zeichnen sich durch eine „Aufgeschlossenheit" aus, nicht nur im Bereich der Ausbildungs- und Lehrermobilitäten, beim Austausch von wissenschaftlichen und fachlichen Informationen, sondern auch bei gesellschaftlichen Lösungen im Rahmen der internationalen Forschungsteams. Der Grund für diese Aktivitäten ist das Streben, auf dem Arbeitsmarkt gut ausgebildete Fachleute zu haben, die fähig sind, in verschiedenen Ländern zu arbeiten, in denen die Mutterkonzerne als Bestandteil der globalen Wirtschaft ihre Firmen haben. Die Ausbildung der Fachleute im Bereich der Sicherheit und des Arbeits- und Gesundheitsschutzes als auch der Sicherheit von technischen Systemen als Bestandteil der Schaffung von Kompetenzen der Fachleute für Risikomanagementsysteme kann in der Zukunft realisiert werden, ob in Form des Hochschulstudiums oder in Form der lebenslangen Bildung, z. B. mittels folgender Modelle:

1. im spezialisierten Studienprogramm mit Arbeitsbezeichnung „Sicherheit von technischen Systemen, Sicherheit und Arbeits- und Gesundheitsschutz" auf allen Studienstufen, also Bachelor-, Ingenieur- und Doktorstudium (siehe Bild 15.4),
2. mittels der lebenslangen Bildung, nach Abschluss vor allem des technisch (naturwissenschaftlich) ausgerichteten Studienprogramms (siehe Bild 15.5).

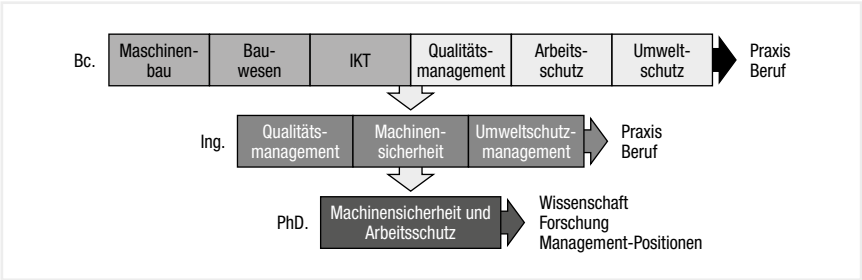

Bild 15.4: **Modell des spezialisierten Studiums**

In einer modernen Gesellschaft wird unter anderem erwartet, dass die Sicherheit als Eigenschaft aller Erzeugnisse und Technologien das erstrangige Ziel aller Tätigkeiten ist. Um dieses Ziel erreichen zu können, ist es wichtig, dass das Gewinnen von Erkenntnissen und Erfahrungen in klassischen Ingenieurbereichen Bestandteil der Studienprogramme ist, wie z. B. Maschinenbaubereiche, Produktionstechnologien, Bauwesen, Montanwissenschaften, Elektrotechnik.

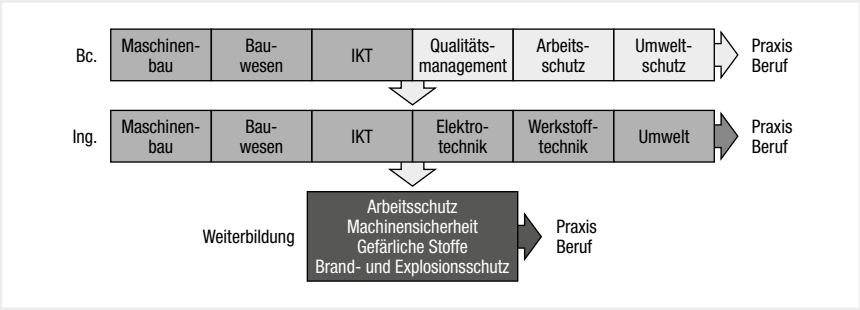

Bild 15.5: **Modell der lebenslangen Bildung**

Infolge der Globalisierung der Arbeitsmärkte, der Entwicklung von neuen Techniken und Technologien entstehen neue Risiken. Die an die entstehenden internationalen Arbeitsmärkte gestellten Anforderungen sind durch die Integration der europäischen Legislatur in die Legislatur der einzelnen Mitgliedsstaaten bedingt. Diese Tatsache schafft die Bedingungen für die Zusammenarbeit auf dem Gebiet der Forschung und Hochschulbildung. Damit dieser Prozess effektiv wird, veröffentlicht die Europäische Union Ausschreibungen für Projekte, die die Netzbildung zwischen den relevanten Institutionen auf dem Gebiet der Forschung und Ausbildung ermöglichen. Die Projekte sind vor allem darauf gerichtet, dass Bedingungen für eine einheitliche „europäische“ Kultur der Sicherheit in übernationalen Gesellschaften geschaffen werden.

Das rechtzeitige Identifizieren der komplexen Beziehungen bildet das Wesen des Definierens von Risiken und die Voraussetzung für Entscheidungsprozesse der Topmanager vor, während und nach einer negativen Erscheinung (Krise). Deshalb müssen die Bedingungen auf dem Gebiet der Ausbildung so geschaffen werden, dass die leitenden Fachleute im Bereich der Sicherheit (Risikosteuerung) nicht nur fachliche Fertigkeiten, sondern auch Fähigkeiten gewinnen, alle Tätigkeiten im Rahmen der Vorbeugungsmaßnahmen zu steuern.

Einige der Module zur Gewinnung von Kompetenzen im Rahmen der Risikosteuerung können folgenderweise definiert werden:

- Risikoidentifizierung – multidisziplinäre Einstellung,
- Risikoanalyse und -abschätzung – Verbindung der naturwissenschaftlichen (mathematische Statistik) und technischen Einstellung,
- Applikation der Methoden zu Risikominimierung – Prävention,
- rechtlicher Rahmen – Legislatur – der Gesellschaft + die nationale,
- Management der kritischen Situationen – gesellschaftliche Einstellung, Politologie, Psychologie, Soziologie u.ä.
- Prinzipien einer effektiven Kommunikation (Arbeit mit Öffentlichkeit, Vermittlung der Informationen über Risikowirkung in der Gesellschaft),
- Fallstudien innerhalb der Firma, Gesellschaft, der öffentlichen Institutionen u. Ä.

15.4 Schlussfolgerung

Die erhaltenen Kompetenzen müssen formuliert und nachfolgend so erworben werden, dass die Experten im Bereich des Risikomanagements (Sicherheit und Arbeits- und Gesundheitsschutz) fähig sind, Systemkonzeptionen zur Risikominimierung als eine effektive Vorbeugungsform zu schaffen, diese in die Praxis in den Firmen bzw. verschiedenen Gesellschaftszweigen einzuführen, ihre Weiterentwicklung zu verfolgen und den neuen Techniken und Technologien einschließlich der Maschinen und Maschinensysteme anzupassen. Ein wichtiges Gebiet ist auch die Leitung der Personen unter gewöhnlichen Arbeitsbedingungen sowie unter den Bedingungen der Störungszustände unter Berücksichtigung der Tendenzen der Bildung von Systemen zur Steuerung einer integrierten Sicherheit, dort also, wo die Tätigkeiten im Rahmen von Safety und Security (z. B. Energetik, vor allem Kernenergetik, Gewinnung und Übertragung von energetischen Medien) realisiert werden.

Die Anforderung der Gesellschaft wie auch der Volkswirtschaft ist, das Sicherheitsmanagement (Safety sowie Security) nicht isoliert zu realisieren, sondern dass es zum Bestandteil einer integrierten Einstellung im Rahmen des Risikomanagements – also *Safety* + *Security* – wird, dem auch Systeme zur Vermittlung der Kompetenzen der Fachleute für ihre Steuerung, aber auch den Topmanagern für ihre Integration im Rahmen der komplexen Managementsysteme einer Firma anzupassen sind. Die Inhalte des Vortrages sind Teilergebnisse des Projektes der Agentur für Wissenschaft und Forschung der Slowakischen Republik Nr. APVV – 0337-11.

Literatur

[1] Sinay, J.: Safety Management in a Competitive Business Environment. CRC Press – 2014, S. 204 – ISBN 978-1482203851.

[2] Technologische Kompetenz – 110622-CP-1-2003-1-DE-Grundtvig-G1 S. 23 bis 35.

[3] Zauberformel „Kompetenz“ – Beitrag zur Klärung eines strapazierten Begriffs – BAUA Aktuell 3-2009, S. 5 bis 9.

[4] Sinay, J.: Anforderungen an eine moderne Arbeitsgesellschaft – Arbeitsschutztag Sachsen-Anhalt, Landesarbeitskreis für Arbeitssicherheit und Gesundheitsschutz in Sachsen-Anhalt. Otto von Guericke Universität Magdeburg/SRN, 2010.

Fazit

Wie wir gesehen haben, sind Kompetenzen im Umgang mit Gefahren und Risiken – was oftmals unter dem Schlagwort „Risikokompetenz“ zusammengefasst wird – für einen wirksamen Schutz der Bevölkerung wichtig. Es handelt sich dabei um ein großes Themengebiet. Es ist unser Anliegen, die Kompetenzen im Umgang mit Gefahren und Risiken sowie den Bevölkerungsschutz auf der Grundlage bisheriger Erkenntnisse weiterzuentwickeln. Auf diesem Wege müssen neue Erkenntnisse in Bewährtes eingearbeitet werden.

Entsprechend dem Wesen der Sicherheitswissenschaft ist dazu eine interdisziplinäre Auseinandersetzung erforderlich. Es ist dabei wichtig, sich den Unterschied zwischen einer multidisziplinären und interdisziplinären Auseinandersetzung bewusst zu machen. Im letzteren Fall werden die Inhalte nicht nur aus verschiedenen Bereichen betrachtet und untersucht, sondern auf dieser Grundlage in ein eigenständiges Instrumentarium und in eine autonome Terminologie und Methodologie überführt und weiterentwickelt. Dabei werden die Erkenntnisse kritisch geordnet und konzentriert, wodurch Analogien und Unterschiede zu anderen Gebieten aufgedeckt werden können.

Bei der Betrachtung von Gefahren und Risiken sind Langzeitfolgen zu berücksichtigen. Das trifft auch auf die Wirksamkeitskontrolle von Beurteilungsmethoden und Bewältigungsstrategien zu. Erst dadurch können Risiken und Chancen in ihrer Gesamtheit bewertet und Verzerrungen durch kurzeitige Betrachtungen vermieden werden. Methoden sollen im Kontext bevölkerungsschutzrelevanter Risiken eine größere zeitliche Spannweite bieten. Mit anderen Worten, **methodisch sollen auch Beurteilungen möglich sein, die über den Eintritt(-szeitpunkt) eines unerwünschten Ereignisses hinausreichen und beispielsweise Kaskaden oder/und Domino-Effekte berücksichtigen sowie die Bewältigung bewerten.**

Wie aus den vorliegenden Beiträgen ersichtlich wird, gibt es die (eine) Universalmethode zur Beurteilung bevölkerungsschutzrelevanter Risiken nicht. Im konkreten Untersuchungsfall muss aus der Vielzahl der verfügbaren Methoden die für die entsprechende Zielsetzung optimale ausgewählt und angemessen umgesetzt werden. Infolge der großen Menge an Beurteilungsmethoden sowie der variierenden Kompliziertheit bei der Anwendung erfordert das eine profunde Methodenkompetenz in Theorie und Praxis.

Es wird eine zunehmende Anzahl an Beurteilungsverfahren praktiziert, von der zivilen Ebene des Katastrophenschutzes[1] über die industrielle Ebene der Umwelt- und Anlagensicherheit[2] bis hin zu der betrieblichen Ebene der Betriebs- und Arbeitssicherheit[3].

Aus dem Vergleich zwischen Methoden, die einerseits auf tradierte und andererseits auf neue Technologien angewendet werden, resultiert der Eindruck, der gegenwärtige Stand bei den Methoden sei hinter die technologische Entwicklung zurückgefallen. **In dem methodischen Defizit begründet sich unmittelbar ein grundlegender, unabhängiger und sicherheitswissenschaftlicher Forschungsbedarf bezüglich innovativer und effektiver Methoden bzw. Verfahren, die auf die Gegebenheiten neuer Technologien ausgerichtet sind.**

Neben dem Bedarf an effektiven Methoden besteht in der praktischen Anwendung auch ein zunehmender Bedarf an effizienten Methoden. Es wurde beispielhaft angeführt, dass in der Kernenergietechnik bzw. Reaktorsicherheit der Bearbeitungsaufwand für eine Risikobeurteilung in der Größenordnung von Personenmonaten

1 Siehe auch Methode für eine Risikoanalyse im Bevölkerungsschutz (BBK).

2 Siehe auch Sicherheitsanalysen, StörfallV oder VDI 3783; Erkennen und Beherrschen exothermer chemischer Reaktionen, TRAS 410; Ereignisablaufanalyse, DIN 25419; PAAG-Verfahren.

3 Siehe auch Gefährdungsbeurteilung, TRBS 1201; Leitmerkmalmethoden, BAuA und LASI; Gefährliche explosionsfähige Atmosphäre – Beurteilung der Explosionsgefährdung, TRBS 2152 Teil 1/TRGS 721; Leitfaden zur Untersuchung von Arbeitsunfällen, BAuA; Gefährdungsbeurteilung – Sieben Schritte zum Ziel, BGI 570/Merkblatt A 016; Gefährdungsbeurteilung – Gefährdungskatalog, BGI 571/Merkblatt A 017).

bis -jahren lag. In der chemischen Industrie werden gelegentlich einige Personenmonate, oft aber nur -wochen bis -tage akzeptiert, und in der Informationstechnologie reduziert sich der Zeitaufwand oftmals auf Personenstunden. **Augenscheinlich gibt es, parallel zu dem technologischen Fortschritt, auch einen Trend zu immer kürzeren Bearbeitungszeiten bei Risikobeurteilungen.**

Im Zuge des Trends nach Effektivität und Effizienz rückt offensichtlich der Bedarf an eine umfassende und vollständige Risikobeurteilung oftmals mehr und mehr in den Hintergrund. Mit anderen Worten, mit dem Bewusstsein um die in der Realität meist bestehenden Ungewissheiten werden von den Analysten vermehrt auch Unsicherheiten bei der Beurteilung als auch bei der Sicherheitskonzeption toleriert. **Gut wiedererkennbar ist dies an den zunehmend diskutierten Ansätzen der Vulnerabilitätsanalyse und dem Resilienzkonzept und den damit erhofften Chancen für den Bevölkerungsschutz.**

In der Grundlagenforschung nimmt die DFG eine wichtige Rolle ein. Bis heute ist dort keine eigenständige sicherheitswissenschaftliche Grundlagenforschung etabliert – trotz der bereits erwähnten Historie der Institution, die eng mit dem Bevölkerungsschutz verbunden ist. Das Förderungsdefizit wird dadurch verstärkt, dass die Schutzkommission heute nicht mehr auf eigene Fördermittel zugreifen kann, um eine angemessene Eigenforschung zum Zwecke des Bevölkerungsschutzes betreiben zu können.

Derzeit wird der Bevölkerungsschutz in der Bundesrepublik Deutschland in wesentlichen Teilen durch das Engagement der rund 1,7 Millionen „ehrenamtlichen“ Kräfte geleistet, wobei die ehrenamtlichen Ressourcen oftmals durch aktiv im Einsatzgeschehen hauptberufliche Kräfte unterstützt werden. Es ist ein erklärtes Ziel des Bundesministeriums des Innern und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, die ehrenamtliche Arbeit in den mitwirkenden Organisationen zu fördern und für die Zukunft zu sichern. Viele Bundesländer beschäftigen sich derzeit intensiv mit der Stärkung des Ehrenamtes, z. B. bei Feuerwehren und Hilfeleistungsorganisationen. In NRW wurde beispielsweise ein Projekt gestartet, das sich mit der nachhaltigen Stärkung des Ehrenamtes in den Feuerwehren befasst. Neben ehrenamtlichen Einsatzkräften leisten zahlreiche ehrenamtlich engagierte Bürger wichtige Beiträge zum Bevölkerungsschutz in Deutschland und bringen dadurch Ressourcen in den Bevölkerungsschutz ein. Das findet oftmals weniger in der aktiven Gefahrenabwehr, sondern beispielsweise in der Planung, Beratung oder Konzeption statt.

Die Kompetenzen der Bevölkerung im Umgang mit Gefahren und Risiken sind mit zahlreichen Implikationen verbunden und auf vielen unterschiedlichen Ebenen zu fördern. Dabei können wir auf Bewährtes zurückgreifen, aber müssen dieses den Anforderungen und der Entwicklung entsprechend im Gleichschritt weiterentwickeln. Hier sind die Entwicklungen auseinandergelaufen.

November 2014 Dr. Sebastian Festag & Prof. Dr. Uli Barth

Nachwort

Mit dem Workshop „Risikokompetenz“ wurde der thematisierte Gegenstand keinesfalles endgültig abgehandelt. Das lag auch nicht in der Absicht der Veranstaltungsplaner. Vielmehr eröffnen die Zusammenkunft und der Diskurs eines Teilnehmerkreises aus Mitgliedern der Schutzkommission beim Bundesministerium des Innern, Mitgliedern der Gesellschaft für Sicherheitswissenschaft e.V. und weiteren, an dem Sachthema interessierten, Experten wahrscheinlich eine Reihe weiterer Möglichkeiten zur kontroversen und konstruktiven Auseinandersetzung mit diesem für den Schutz der Bevölkerung in Deutschland und für die Sicherheitswissenschaft unbestritten wichtigen Thema.

Die zum Ende des Workshops unter allen Teilnehmern durchgeführte Evaluation unterstrich diesen Tenor. Des Weiteren ergab die Evaluierung aber auch, dass bei folgenden Veranstaltungen der diesmal bewusst angelegte technische Fokus in soziotechnologischer Hinsicht erweitert werden soll. Ferner wurde angeregt, bereits bei der Planung des Veranstaltungsprogramms mehr Raum für Diskussionen und Gespräche vorzusehen.

November 2014

Prof. Dr. Uli Barth
Prof. Dr. Heinz-Willy Brenig
Dr. Sebastian Festag
Dr. Willi Marzi
Dr. Horst Miska
Prof. Dr. Peer Rechenbach

ISBN-10: 3-939347-64-7
ISBN-13: 978-3-939347-64-4