Zeitschrift: Berichte der St. Gallischen Naturwissenschaftlichen Gesellschaft
Herausgeber: St. Gallische Naturwissenschaftliche Gesellschaft
Band: 85 (1991)

Artikel: Risiko-Management, Methodik zum Umgang mit Risiken
Autor: Bützer, Peter
DOI: https://doi.org/10.5169/seals-832753

Berichte der St.Gallischen Naturwissenschaftlichen Gesellschaft
85. Band Seiten 185–240 8 Figuren St.Gallen 1991

Risiko-Management, Methodik zum Umgang mit Risiken

Peter Bützer

Dr. sc. nat. ETH Peter Bützer, Rebhaldenstraße 2, 9450 Altstätten

Inhaltsverzeichnis

Zusammenfassung

Der Umgang mit Risiken, das Risikomanagement, läßt sich nur an vorgegebenen Zielen messen. Ein gewisses Maß an Risiken ist notwendig, und normalerweise auch mit einem Nutzen, Fortschritt oder Erleben verbunden. Verfügbarkeit, Zuverlässigkeit, Qualität und Sicherheit haben technisch meist dieselben Grundlagen. Für die Auslegung von Systemen oder die Bewertung von Maßnahmen ist es notwendig, daß Risiken mindestens semiquantitativ erfaßt, und damit vergleichbar gemacht werden. Voraussetzung dazu ist die Vorgabe eines Szenarios, das Erkennen der möglichen Gefahren, die Analyse der Situation, die Synthese der Erkenntnisse zu einer Beurteilung und die Entscheidung für konkrete Maßnahmen. Die Situationen in den Systemen selbst, an den Schnittstellen Mensch-Maschine und Mensch-Umwelt sind so komplex, daß intuitive Beurteilungen sehr oft falsch sind, ein systematisches Vorgehen daher notwendig wird. Die dazu eingesetzten Methoden sollten alle verfügbaren naturwissenschaftlichen Erkenntnisse ausschöpfen und gesicherte Phänomene ins Zentrum stellen. Zusätzlich muß die Simulation in sehr vielen Bereichen die Erfahrung ersetzen, sie wird für die Ausbildung und die Bildung immer wichtiger. Entscheidungen basieren auf Informationen, deren Informationsgehalt von den Unsicherheiten der Erkenntnisse und der Modelle abhängen. Es ist eine wissenschaftliche Aufgabe, diese Unsicherheiten und Grenzen darzustellen, die Lücken zu füllen, mindestens aber die Maßnahmen so abzustimmen, daß sie der Informationsbasis entsprechen. Da alle Katastrophen die Folge von Ereignisketten mehr oder weniger kleiner Fehler sind, ist es notwendig, diesen Details im Sinne einer Sicherheits-Kultur oder mit Schutzzielen alle Beachtung zu schenken.

Das Risiko wird definiert und mit einer Funktion beschrieben, welche die statistischen Auswertungen von Großunfällen, die Beanspruchung der Logistik unserer Gesellschaft und die psychologischen Aspekte der Risikoaversion gegen Großereignisse grob erfaßt. Folgerungen aus dieser Definition werden für die Auslegung der Systeme und die Ausbildung gezogen. Auf verschiedene Gesichtswinkel, Risiken zu betrachten, wird eingegangen, ebenso auf die zeitliche Dynamik. Mit den Unsicherheiten bei der Risikoanalyse wird auf die Grenzen dieser Methodik hingewiesen. Besonderes Schwergewicht wird auf das Erkennen von Gefahren, die Gefahrensuche, gelegt, welche die Grundlage für ein systematisches Vorgehen bildet. Das sogenannte Eisbergsyndrom ist ein Eckpfeiler für

die Diskussion von möglichen Maßnahmen, für Eingriffsarten, Schutzmöglichkeiten und Schutzziele. Einfache Methoden, die Sicherheit, die Wirksamkeit von Maßnahmen oder die Verfügbarkeit abzuschätzen sind dargestellt.

1. Einleitung

Die Naturwissenschaften haben unsere Welt ganz entscheidend verändert. Besonders die Technik, welche auf den naturwissenschaftlichen Fundamenten steht, hat sich in den vergangenen Jahrzehnten ungeheuer rasch entwickelt. Die Naturwissenschaften haben aber auch die wissenschaftlichen Grundlagen, und die Technik hat das ganze Instrumentarium zur Verfügung gestellt, die Auswirkungen der Technik auf die Umwelt erkennbar, meßbar und interpretierbar zu machen. Dieses Zusammenspiel von Naturwissenschaft, Technik und Umwelt ist seit Jahren Anlaß zu grundlegenden Arbeiten unter dem Gesichtswinkel des Risikos und der damit verknüpften Sicherheit. Der wissenschaftliche Ansatz hat sich in den letzten Jahrzehnten vom vorwiegend analytischen zum analytisch-synthetischen Vorgehen verändert. Vor allem die Bereiche, welche sich mit ganzen Organismen oder der Umwelt befassen, haben die neuen systemischen Methoden rasch aufgenommen. Kritische oder gefährliche physikalische, chemische oder toxikologische Eigenschaften eines Stoffes können nicht mehr losgelöst von Herstellung, Transport, Verteilung, Handhabung, Anwendung und Entsorgung diskutiert werden. An all diesen Schnittpunkten hat der Naturwissenschafter wesentliche methodische Beiträge zu liefern, die man Risikoanalyse nennen kann. Diese Analyse ist die Basis für die Risikobeurteilung, die Synthese und die daraus folgenden Maßnahmen. Wenn in dieser Arbeit die technischen Systeme im Vordergrund stehen, dann nur, um diese im großen Bezugsrahmen von Natur, Mensch, Fauna und Flora in ihren Auswirkungen einzuschätzen. Für eine solche Art Risikoanalyse eignet sich eine Anwendung von naturwissenschaftlichen Erkenntnissen aus Mathematik, Physik, Chemie, Biologie, Toxikologie und Systemdynamik. Es ist eine Auseinandersetzung in den Bereichen, in denen die Wissenschaft und die Technik auf die Natur und die Gesellschaft trifft. Die Kybernetik und die Chaostheorie haben gezeigt, daß es sich auch wissenschaftlich lohnt, ganze Systeme zu betrachten und daraus Folgerungen für einzelne, klar begrenzte Bereiche zu ziehen. Die vorliegende Arbeit weist auf einige

Möglichkeiten für das Risiko-Management und damit auch für methodische Ansätze in der Ökologie hin. Es ist eine Übersicht über verschiedenste wissenschaftliche Erkenntnisse und Methoden, die sich bei Risikoüberlegungen oder Sicherheitsbetrachtungen bewährt haben.

2. Grundlagen

2.1. Risikodefinition:

Risikodefinition:

Unter dem Begriff Risiko kann umfassend die Summe aller Möglichkeiten verstanden werden, welche die Erwartungen eines Systems aufgrund von Störprozessen nicht erfüllen (HALLER, 1986, 1990a).

Zur Beurteilung eines Risikos sind damit folgende Grundlagen notwendig:

1. Definition des betrachteten Systems (Abgrenzung, Struktur, Transformationen, Kopplungen).
2. Erwartungen an das System (→ Ziele).
3. Erkennen der Störprozesse (→ Gefahrensuche, Initiierungen, Wahrscheinlichkeiten).
4. Summieren der isolierten und integrieren der gekoppelten Störprozesse (→ Szenarien).
5. Ermitteln der möglichen Abweichungen von den Erwartungen.
6. Was darf nicht passieren ? (→ Maßnahmen).
7. Bestimmen des Risikos, Vergleich mit dem Nutzen.

Ein beschränktes Maß an Risiko ist nicht nur zulässig, sondern auch gesucht und notwendig (→ Fehlerproduktion, Mutationen). Risiken sind Motor des Fortschritts (→ Lernen, Selektion), solange sie nicht systembedrohend sind.

Das Verlangen nach absoluter Sicherheit kommt der Suche nach einem unbrennbaren Brennstoff gleich (BECKMANN, 1976).

Eine *systematische und methodisch einheitliche Erfassung, Analyse und Beurteilung von Risikosituationen* technischer Systeme ist notwendig weil (CONRAD, 1979):

1. die Informationskapazität des Menschen begrenzt ist,
2. die Tendenz besteht, bei komplexen Entscheidungssituationen intuitiv unzulässige Vereinfachungen zu treffen,
3. die Fähigkeit nicht vorhanden ist, kleine, aber doch realistische Wahrscheinlichkeiten zu beurteilen.

Jede Frage nach technischer Sicherheit eines *definierten Systems* (→ Zielsetzung vorausgesetzt) kann in zwei Fragen und daraus folgende Maßnahmen gegliedert werden [zum Teil (SCHNEIDER TH., 1985a)]:

Ist das sicher?

Was *kann* passieren?	Was darf *nicht* passieren?
Risikoanalyse	Risikobeurteilung
(Phänomene, Modelle)	(Vorschriften, Erwartungen)

Maßnahmen

In einer *technischen Risikoanalyse* ist die weitgreifende, allgemeine Risikodefinition auf die beiden Elemente, Häufigkeit eines unerwünschten Ereignisses (erkennen, summieren und/oder integrieren von Störprozessen) und Schwere der Ereignisauswirkungen (Tragweite, Ermitteln der Abweichungen von den Erwartungen), eingeschränkt. Dies ist deshalb notwendig, weil *technische Lastannahmen und die praktische Auslegung quantifizierbare und dimensionierte, mindestens aber vergleichbare Größen verlangen.* Diese Dimensionierungen schränken die Übertragbarkeit von Risikoanalysen ein, da sie sich auf willkürlich festgesetzte, oft schwer umrechenbare Einheiten wie Zugbelastung, Toxizität, Übertragungsfehler etc. abstützen. Freiwillig eingegangene Risiken müssen dabei anders bewertet werden als unfreiwillig aufgebürdete (RENN, 1986), der Maßstab ist somit nur innerhalb ähnlich wahrgenommener Gefahren gleich (→ Systeme mit Risiken).

Grenzen der Risikoanalyse:

Die Risikoanalyse kann bestenfalls Risiken oder Sicherheiten von Einzelereignissen vergleichen, sie kann sie nie absolut beschreiben (HEILMANN, URQUART, 1983, HEILMANN, 1986).

Ein Ereignis wird auch im täglichen Leben danach beurteilt, wie schwerwiegend die Auswirkungen sind und wie häufig ein ähnliches Ereignis

bisher aufgetreten ist. Die Projektion dieser Häufigkeit in die Zukunft, wird mathematisch mit der Wahrscheinlichkeit umschrieben. Die beiden zentralen Begriffe, Auswirkungen und Eintretenswahrscheinlichkeit, lassen sich wie folgt erfassen:

Auswirkungen (Tragweite, Verletzbarkeit im engeren Sinne):

Mögliche Schäden und Folgeschäden für alle erkannten Gefahren (technisch, ökologisch). Auswirkungen können beschrieben werden durch:

a) Auswertung von Experimenten (incl. scale up)
b) Auswertung abgelaufener Ereignisse, Statistiken
c) Vergleich mit ähnlichen Phänomenen
d) Simulation mit Modellen

Auswirkungen lassen sich nie unabhängig von einem Szenario umschreiben (NÜTTEN-HART, OSTEROTH, 1987, SCHNEIDER J., 1985), sie setzen ein Gefahrenpotential voraus, welches durch einen beschreibbaren Vorgang freigesetzt werden könnte. Das unterlegte Szenario gibt aber auch vor, welche Eintretenswahrscheinlichkeiten berücksichtigt werden müssen (→ Klassierung von Ereignissen). Systemgrenzen und Randbedingungen sind somit in erster Linie vom Szenario abhängig. Was mit diesem als Fragen nicht vorgegeben wird, kann als Antworten von der Risikoanalyse und -bewertung nicht erwartet werden.

Eintretenswahrscheinlichkeit (Häufigkeit, Störbarkeit im engeren Sinne, sie umschreibt ein zeitliches Intervall und keine zeitliche Distanz bis zu einem möglichen Ereignis):

Die Wahrscheinlichkeit eines Ereignisses kann in der Regel für Elemente/Komponenten oder begrenzte Systeme in der Größenordnung abgeschätzt werden. Sie ist der Reziprokwert von MTBF (mean time between failure [KLETZ, 1983]). Als Grundlage verwendet man zum Beispiel:

a) statistische Unterlagen
b) Vergleich mit ähnlichen Situationen
c) die Erfahrung
d) theoretische Abschätzungen

Für die Bestimmung der Eintretenswahrscheinlichkeit sind technische und menschliche, unabsichtliche und absichtliche, externe und interne Initiierungen zu beachten (siehe auch → drei Kategorien von Fehlern).

2.2. Risikoabschätzung

Es ist für die praktische Anwendung oft sinnvoll, den Risikobegriff zu quantifizieren, damit Vergleiche möglich und Verbesserungen erkennbar werden.

Risikodefinition für probabilistische Abschätzungen:

Risiko = Funktion (Eintretenswahrscheinlichkeit, Auswirkungen)

Für die mathematische Formulierung müssen folgende Forderungen erfüllt sein:

1. Die Funktion muß für den ganzen, real wichtigen Wertebereich definiert sein.
2. Wenn ein Faktor Null ist, dann muß auch das Risiko Null sein.
3. Die Einheiten müssen sinnvoll sein.

Eine Funktion, welche diese Forderungen erfüllt, ist die Multiplikation der Eintretenswahrscheinlichkeit (P) und der damit verknüpften Auswirkungen (A).

Die Eintretenswahrscheinlichkeit kann praktisch nur bei besonderen Systemen als zufälliges Ereignis (stochastisch) betrachtet werden, wie dies die mathematische Wahrscheinlichkeit fordert. Sie ist in den meisten Fällen entscheidend von Planung, Auslegung, Bedienung, Kontrolle, Wartung und Unterhalt, also von bestimmbaren, nicht zufälligen Einflüssen, abhängig. Diese Eigenschaften gilt es bei der Kombination von Wahrscheinlichkeiten zu berücksichtigen. Zwei Systeme mit gleicher Funktion, aber verschiedenartiger Auslegung, oder zwei identische Systeme an verschiedenen Orten zeigen unterschiedliche Eintretenswahrscheinlichkeiten. Die Unsicherheiten sind hier zwangsläufig recht groß. Verhältnismäßige Maßnahmen verlangen trotzdem mindestens eine Abschätzung der Größenordnungen. Dies ist immer sehr anforderungsreich. Auch Eigenschaften wie Motivation, Disziplin, Ausbildung, Übung, Können und Training, so schwierig erfaßbar sie auch sein mögen, müssen über geeignete Verfahren (zum Beispiel als Fuzzy-Sets) bei den Eintretenswahrscheinlichkeiten semiquantitativ berücksichtigt werden. Hier bietet sich zum Beispiel auch mit dem Matrixverfahren (BÜTZER, 1987a, DROSTE, MALLON, 1990) die Möglichkeit an, ein Kriterium in viele zusammenhängende Teilkriterien zu gliedern, diese nur grob, semiquantitativ zu beurteilen und über Kombinationen der Matrizen einen Überblick über das ganze System zu gewinnen.

Extremwertbetrachtung:

a) Chronische, kleine Ereignisse (Umweltbelastung):
   A ist größer als Null, aber relativ klein. P ist ungefähr 1, das heißt, das Risiko ist definiert.

b) Akute Großereignisse (Katastrophen):
   A ist sehr groß, deshalb muß P gegen Null gehen. Mathematisch gesehen ist das Produkt des Extremfalls, von Null mal Unendlich, nicht definiert.

Die bloße Multiplikation von Gefahrenpotential und Eintretenswahrscheinlichkeit, die Proportionalität, hat eine Gleichsetzung der chronischen, kleinen Ereignissen mit akuten, großen Ereignissen zur Folge. Dies entspricht nicht der Realität (BINSWANGER, 1986).

Da eine Zunahme der Auswirkungen die *Logistik* überproportional beansprucht und deshalb gegen große Auswirkungen eine *Aversion* vorhanden ist, läßt sich die eine mögliche Risikofunktion wie folgt definieren:

Die einfachste Risikofunktion:

$R = P \cdot A^l$

R: Risiko (Auswirkungen pro Zeit)
P: Eintretenswahrscheinlichkeit (pro Zeit)
A: Auswirkungen (Auswirkungen)
l: Logistik- oder Aversionsexponent (dimensionslos) (1–1,6) (LATINEN, 1987, BLOKKER, 1983a, BOHNENBLUST, 1985, CEFIC, 1988).

Die zum Ausmaß nichtlineare Bewertung ist auch unter dem Namen Bewertungsfunktion bekannt (KAHNEMANN D., TVERSKY A. 1982)

Für den Fall, daß mit zunehmenden Auswirkungen die logistische Beanspruchung progressiv zunimmt, könnte zum Beispiel der Ansatz gemacht werden: $R = P \cdot A^{(1-\log(P)/10)}$. Hier wird bei der menschlichen Grenze für die Erfaßbarkeit von Wahrscheinlichkeiten (BÜTZER, 1983) der Exponent $l = 1{,}4$ erreicht, der auch dem statistischen Wert bei Großereignissen entspricht (CEFIC, 1988). Begrenzungen der maximalen Auswirkungen, und noch stärker progressive Exponenten l, für Ereignisse mit nicht kontrollierbaren Folgen sind denkbar (SEIFRITZ, 1991).

Die einzelnen Parameter zeigen für die direkte Interpretation auch Grenzen.

Wahrscheinlichkeiten, Grenzen der Erfaßbarkeit:

Die intuitive Grenze der Erfaßbarkeit von Wahrscheinlichkeiten liegt etwa bei 1:10 000. Kleinere Werte können mit der persönlichen Erfahrung nicht interpretiert werden.

Bei den Auswirkungen werden vor allem diejenigen als schwerwiegend beurteilt, die sich unseren Sinnen entziehen (Radioaktivität, Strahlung, Toxizität, Mikroorganismen, Änderungen bei Genen etc.). Man hat deshalb Unterscheidungen vorgenommen, wie bekannt Risiken sind (STEWART, 1990).

Bei der formalen Definition der Risiken kann man sich zu Recht die Frage stellen, wie der Gegenpol, die Sicherheit, daraus abgeleitet werden könnte.

Sicherheit bezüglich dem betrachteten Risiko wird oft als $J\ S = 1/R$ ausgedrückt. Diese Definition liefert einen Wert für die Sicherheit gegenüber einem bestimmten Risiko. Verschwindet dieses Risiko ($R = 0$), dann wird die Sicherheit beliebig, undefinierbar groß. Die Definition hat somit ihre klaren Grenzen (andere Beziehungen zwischen Sicherheit und Risiko siehe: [BÜTZER, 1987c]). Eine Summation ist bei allen bekannten Definitionen bei unabhängigen Risiken möglich (BÜTZER, 1989a), nicht aber bei den daraus abgeleiteten Sicherheiten.

2.3. Unsicherheiten

Ein abgeschätzter Risikowert muß einen Informationsgehalt aufweisen, das ist dessen Ziel. Weil aber die Unsicherheiten den Informationsgehalt direkt beeinflussen, sind die zufälligen und die systematischen Fehler bei allen Parametern zu berücksichtigen. Bei komplexen Systemen mit sehr kleinen Eintretenswahrscheinlichkeiten sind die Unsicherheiten durch die vielen Kombinationen groß, der Informationsgehalt klein, und ein Ereignis ist daher durch den Informationszuwachs einmalig und spektakulär (BÜTZER, 1990a).

Unsicherheiten können in folgenden Bereichen auftreten (ENZYCLOPÄDIE, 1981a): (→ Gefahrensuche)

1. Bei den Lastannahmen (z.B. dynamische Windlasten bei Brücken)
2. Bei der Auslegung (z.B. falsche Berechnungen, falsches Material)
3. Beim Material (z.B. Qualität der Werkstoffe)

4. Durch die Umgebung (z.B. geologische Beschaffenheit, Wasser, Verkehr...)
5. Durch ungenaue Ausführung oder falsche Bedienung

Der Einfluß der Unsicherheiten auf die Risikoeinstufung läßt sich überschlagsmäßig abschätzen.

Unsicherheiten bei Eintretenswahrscheinlichkeit und Auswirkungen:
$R = (P + P_u) \cdot (A + A_u)^l$
P_u: Unsicherheit bei der Eintretenswahrscheinlichkeit
A_u: Unsicherheit bei den Auswirkungen

Auswirkungen der Unsicherheiten auf die Risikoabschätzung:
Annahme: Die Unsicherheiten sind etwa halb so groß wie die Werte selbst. Es werden nur die nichtkonservativen Abweichungen betrachtet, also die Abweichungen, welche das Risiko größer werden lassen. (In der Realität kann bei etwa einem Drittel aller Unfälle im chemischen Bereich die Ursache nicht ermittelt werden (BÜTZER, 1985a; BÜTZER, 1986.)

a) Extremfall: $l = 1$;
kleine Auswirkungen A, sehr großes P (häufige bis chronische Wirkungen)
Proportionaler, mathematischer Risikoansatz.

$R = 1{,}5 \cdot P \cdot 1{,}5 \cdot A$
$R = 2{,}25 \cdot P \cdot A$;
das Risiko kann maximal 2,25mal so groß sein wie der abgeschätzte Grundwert.

b) Extremfall: $l = 2$;
sehr große Auswirkungen, sehr kleines P (Großunfälle, Katastrophen)
Überproportionaler Einfluß der Auswirkungen.

$R = 1{,}5 \cdot P \cdot (1{,}5 \cdot A)^2$
$R = 3{,}4 \cdot P \cdot A^2$;
das Risiko kann maximal $3{,}4 \cdot A$ so groß sein wie das mit dem linearen Ansatz, ohne den Logistikexponenten berechnetes Risiko oder drei- bis viermal größer als das mit dem ‹logistischen› Ansatz abgeschätzte Risiko. Abweichungen um Potenzen sind im ersteren Fall möglich.

Aus diesen Beispielen kann der Schluß gezogen werden, daß das abgeschätzte Risiko sich alleine durch die Unsicherheiten bei den Basisgrößen um Faktoren unterscheiden kann.

Der prognostische Aussagewert ist bei kleinem P und großem A wesentlich kleiner als bei großem P und kleinem A. Mit zunehmender Unsicherheit bei den Grundwerten nimmt der *Informationsgehalt* ab. Eine sinnvolle Grenze für interpretierbare Werte dürfte bei 1 Bit, also einer möglichen Ja-Nein- Entscheidung, liegen (BÜTZER, 1975).

$I = \ln 2\ [(x_{max} - x_{min})/(2 \cdot s \cdot q^{1/2})]$
I: Informationsgehalt [Bit]
ln2: Logarithmus zur Basis 2
x_{max}: Oberer, maximaler Wert des betrachteten Bereichs
x_{min}: Unterer, minimaler Wert des betrachteten Bereichs
s: Standardabweichung (97,5% statistische Sicherheit)
q: Anzahl bestimmte Werte

Aus dieser Gleichung folgt, daß die Grenze von 1 Bit Informationsgehalt unterschritten wird, wenn der Nenner 25% des Zählers übersteigt. Dies dürfte bei Abschätzungen von Auswirkungen und Eintrittswahrscheinlichkeiten (→ 3 Kategorien von Fehlern), vor allem in komplexen Systemen, durch die Fehlerfortpflanzung sehr rasch der Fall sein. Bei einem System aus 13 linearen Komponenten, mit einer Unsicherheit von je 90%, sind 25% (bei q = 1) erreicht.

Risikoabschätzungen und Informationsgehalt:

Risikoabschätzungen machen nur einen Sinn, wenn sie mehr als 1 Bit Information (Ja-Nein-Entscheidung) enthalten. Mit zunehmenden Unsicherheiten bei den Grunddaten resp. den Grundannahmen oder Funktionen verringert sich der Informationsgehalt.

In komplexen Systemen mit vielen Parametern ist der Punkt rasch erreicht, wo gesamthaft kein Informationsgehalt mehr vorliegt.

2.4. Risikovergleiche

Da Risikoaussagen über unterschiedliche Varianten mit verschieden großen Fehlern behaftet sind, haben sie auch unterschiedliche Informations-

gehalte. Die Frage, was sicherer sei, ein System mit großen Auswirkungen und kleinen Wahrscheinlichkeiten oder ein System mit kleinen Wahrscheinlichkeiten, aber großen Auswirkungen, läßt sich nur mit einer Funktion durchführen, welche die Logistik (resp. Aversion) berücksichtigt (→ Logistikexponent). Dieser Exponent gibt den Economies of Scale eine sinnvolle Grenze und läßt Diskussionen über die Verteilung von Großrisiken in meherere kleinere Risiken zu (BÜTZER, 1989b). Wegen der Verschiedenartigkeit der Systeme sind Vergleiche trotzdem nur beschränkt durchführbar.

Risikovergleiche:

Direkte Risikovergleiche lassen sich mit größerer Zuverlässigkeit nur bei ähnlichen Auswirkungen oder vergleichbaren Eintretenswahrscheinlichkeiten machen.

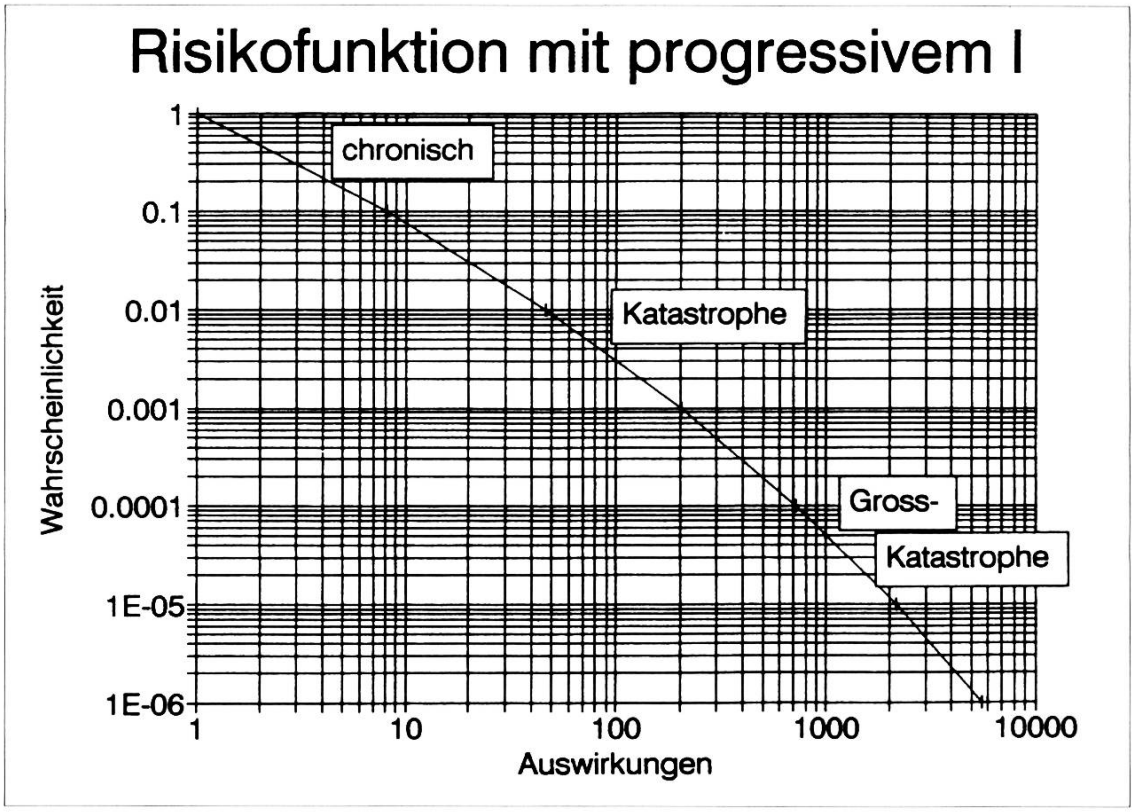


Fig. 1
Risiko als Funktion von Wahrscheinlichkeit (P) und Auswirkungen (A) mit einem progressiven Logistikexponenten (l). Grobe Einteilung in chronische und Katastrophen- Risiken (akute Risiken).

Prinzipiell lassen sich Katastrophenschutz (akute Ereignisse) und Umweltschutz (chronische Ereignisse) mit derselben Methodik angehen. Den kleinen, schwer interpretierbaren Wahrscheinlichkeiten bei Großereignissen stehen im Umweltschutz die kleinen, in einer Kausalkette schwer erfaßbaren Auswirkungen gegenüber. Diese Auswirkungen verlangen epidemiologische Auswertungen, deren Aussagen auf statistischen Verteilungen, wie die Wahrscheinlichkeiten bei den akuten Ereignissen, aufbauen.

Risiken in großen Systemen werden durch analytische Beurteilung von Komponenten und Modulen mit anschließender Synthese ermittelt. Diese Systematik mit mathematischen Hilfsmitteln erweitert die Grenze des menschlichen Gehirns, logische Schlüsse nur über fünf bis neun Stufen ziehen zu können (MILLER, 1956), setzt aber eine Gliederung der Problemstellung nach wichtigen Kriterien voraus, welche zum Beispiel mit morphologischen Methoden durchgeführt werden können (ZWICKY, 1989).

Die Einteilung von Störfällen kann mit einem Raster, auf der Eintretenswahrscheinlichkeit (P) und den möglichen Auswirkungen (A) aufgebaut werden:

Klassierung von Ereignissen/Störfällen

Szenario	Auswirkungen	Wahrscheinlichkeit
Normalfall	sehr klein	häufig
Auslegung	klein	selten
Hypothetisch	groß	sehr selten
Irrelevant?	sehr groß	nie (??)

Dafür, daß unerwünschte Ereignisse mit einer gewissen Wahrscheinlichkeit eintreten, sind, mit Ausnahme von unerwarteten Naturereignissen, Fehler verantwortlich. Man unterscheidet nach Gauß drei Kategorien (BASLER, 1961a) von Fehlern:

1. grobe Fehler
2. systematische Fehler
3. zufällige Fehler

Die groben Fehler haben das gemeinsame Merkmal, daß sie durch genügende Sorgfalt vermieden werden können.

Die systematischen Fehler werden meist durch eine Kumulation von kleinen Abweichungen aufgebaut, welche alle in eine Richtung zeigen.

Als zufällige oder stochastische Fehler bezeichnet man willkürliche Streuungen, die keinem bekannten Gesetz folgen. Sie gruppieren sich meist mehr oder weniger symmetrisch um ihren Mittelwert.

Eine Aufeinanderfolge von gekoppelten, sich folgenden Fehlern kann als Ereigniskette bezeichnet werden.

Große Katastrophen sind immer die Folge von Ereignisketten (→ Ereigniskaskaden, Dominoeffekte). Die Wahrscheinlichkeiten des Systems müssen deshalb als Kombinationen von Einzelwahrscheinlichkeiten bestimmt werden (→ Redundanz, Diversifikation). Simultane Mehrfachfehler sind an allen kritischen Stellen zu berücksichtigen (KEMENEY et al., 1979a). Die Wahrscheinlichkeit für einen Unfall bei einem Space Shuttle wurde zum Beispiel vor dem Unfall der Challenger-Raumfähre 1986 offiziell mit 1:100000 angegeben. Diese Angabe war zu optimistisch, weil Ereignisketten nicht genügend berücksichtigt waren. Eine Abschätzung der Wahrscheinlichkeit nach dem Unfall führte zu der Größenordnung von 1:300 (STEWART, 1990).

Der Wahrscheinlichkeitsbegriff baut auf bestimmten Voraussetzungen auf (zum Beispiel Gesetz der großen Zahl, Zufälligkeit) und hat gleichzeitig entscheidende Grenzen bei seiner Interpretation (zum Beispiel Unabhängigkeit sich folgender Ereignisse) – es ist ein sehr schwieriger Begriff. Unsere Intuition, Wahrscheinlichkeiten abzuschätzen, hört etwa im Bereich 1/10000, also bei 10^{-4} auf (BERNOULLI, 1738, KNOX, 1975, HOFSTADTER, 1982). Alle Wahrscheinlichkeiten, die tiefer als dieser Wert liegen, werden im täglichen Leben bei Risikoüberlegungen nicht mehr berücksichtigt (STEINER, 1981, SUVA, 1978), sie lassen sich nur noch rechnerisch ermitteln, es sind abstrakte Größen. Diese Grenze zeigt auch die Grenze unserer persönlichen Erfahrungen auf. Die Natur hat bei lebenswichtigen Prozessen wie zum Beispiel der Herstellung von Proteinen eine Wahrscheinlichkeit für Fehler, welche zwischen $2{,}6 \cdot 10^{-5}$ bis 10^{-5} schwankt (CRAMER, 1990). Eine ähnliche Größenordnung von 10^{-5} pro Jahr wird als Grenze bei technischen Risikobeurteilungen gefunden (BLOKKER, 1983b).

2.5. Ausbildung

Mit Großunfällen oder Katastrophen haben wir kaum Erfahrungen, weil sie sehr selten auftreten. Da sich Einzelfälle nicht verallgemeinern lassen,

bleiben sie Spezialfälle; die Erfahrungen sind somit nur sehr beschränkt übertragbar. Die Auslegung solcher Systeme und die Ausbildung des Personals für Reaktionen im Katastrophenfall kann sich deshalb bis auf wenige Ausnahmen nur an Modellen orientieren.

Ausbildung:

Die Einschätzung von Katastrophenrisiken, und damit auch die Ausbildung für die Notfallmaßnahmen, ist bei den sehr kleinen Wahrscheinlichkeiten, wegen mangelnder Erfahrung, außerordentlich anforderungsreich.

Systeme, welche ein *Lernverhalten* durch Erfahrung ohne schwerwiegende Folgen begünstigen, zeichnen sich durch eine große Fehlertoleranz, gekoppelt mit einer hinreichend großen Fehlerrate (Fehlerproduktion) aus. Man bezeichnet solche Systeme als *fehlerfreundliche Systeme* (VON WEIZÄCKER C., E. U., 1984). In der Natur spricht man in analogem Zusammenhang von Mutationen und Selektion. Voraussetzung bei diesen Systemen ist nicht die Fehlertoleranz durch ‹stilles›, unbemerktes Abfangen von Fehlern, sondern die Eigenschaft, auch kleine Fehler zu zeigen (→ Eisbergsyndrom). Ein fehlerfreundliches System muß so beschaffen sein, daß wichtige neue Erkenntnisse in Zeiträumen, welche mit den Fehlerraten korrelieren, in die Praxis umgesetzt werden können. Nur so ist es möglich, aus Fehlern zu Fortschritten, Verbesserungen und Innovationen zu kommen, den negativen Aspekt kritischer, aber noch kleiner Fehler positiv zu nutzen und damit ein System sicherer zu machen.

Fehlerfreundliche Systeme:

Diese Systeme setzen ein gewisses Maß an Fehlerproduktion und Fehlertoleranz voraus. Der ‹Lerneffekt› kann aber nur wirksam umgesetzt werden, wenn bei der Sicherheit nicht konkrete Maßnahmen verlangt, sondern Zielsetzungen vorgegeben werden.

In der Natur ist der überwiegende Teil der Mutationen (Veränderungen der Erbsubstanz) Verlustmutationen, also Fehler. Die Entwicklung und Innovation hat diese Fehler als Voraussetzung (PETERS, WATERMAN, 1990), eine Tatsache die bei der Größenoptimierung von Systemen und Anlagen beachtet werden muß.

Risiken technischer Systeme erstrecken sich auf die Bevölkerung, die Umwelt und die Wirtschaft. Bei Analyse, Beurteilung und Maßnahmen sind Prioritäten zu setzen (→ Schutzziele).

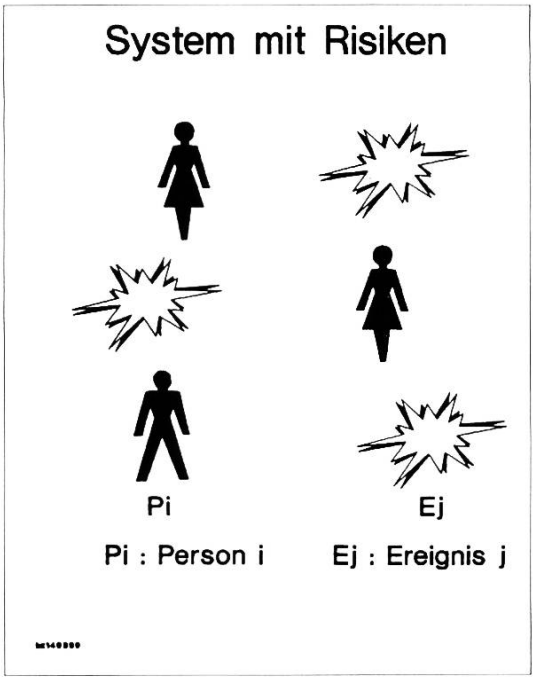
Prioritäten bei Maßnahmen:

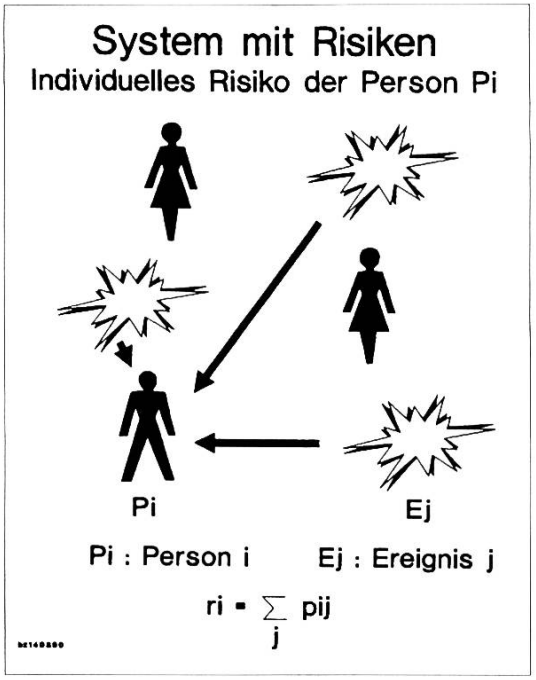
Bereiche: Mensch → Umwelt → Sachgüter
Wirkungen: irreversibel → reversibel
Ansatzpunkt: Gefahrenpotential → Initiierungen

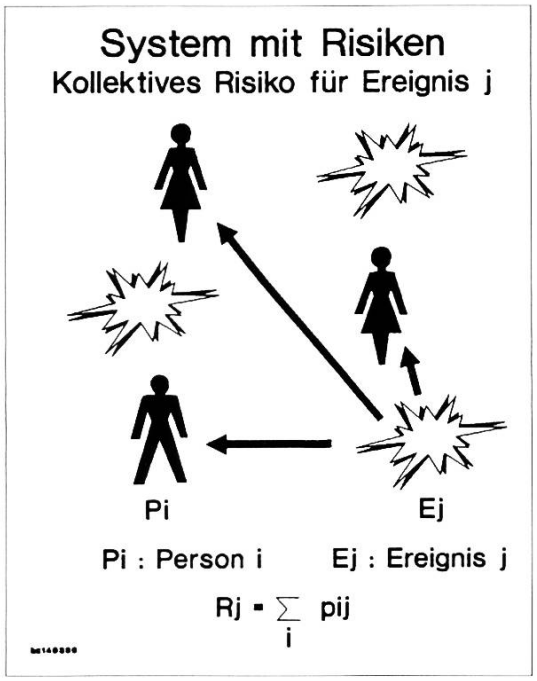
Wird der Mensch, in einem sehr weiten Sinne, bei den Schutzzielen an erste Stelle gesetzt, dann sind die nachfolgenden Bereiche indirekt schon weitgehend mitberücksichtigt. Dies ist aber nur dann der Fall, wenn Akkumulationen, Synergismen, Latenzzeiten, Rückkopplungen, ganz allgemein große, umfassende Systeme berücksichtigt werden. Akkumulationen werden zum Beispiel in der Ökologie erst in großräumigen Nahrungsketten durch Summationen kleiner Dosen mit Verzögerung erkannt. Ist der Mensch nicht am Ende einer solchen Anreicherung, dann bietet sein Schutz keine genügende Sicherheit für die Umwelt.

Irreversible oder sehr langfristig reversible Auswirkungen müssen vermieden werden, weil sie sich nur sehr schwer verantworten lassen.

Maßnahmen bei den Gefahrenpotentialen sind deterministischer, solche bei den Initiierungen probabilistischer Natur (→ Eintretenswahrscheinlichkeit). Für die Lagerung brennbarer Flüssigkeiten und Gase wurden Maßnahmen vorgeschlagen, welche das gefährlichste Szenario, den BLEVE (Boiling Liquid Expansion Vapour Explosion), verhindern sollen (FAUSKE, 1989). Bei Benzin, einem brennbaren Stoff, kann ein Brand nie ausgeschlossen werden. Es sind immer Auslöser denkbar. Wird diese Flüssigkeit, zum Beispiel bei neuen biotechnologischen Verfahren, durch Wasser ersetzt, eine Maßnahme beim Gefahrenpotential, dann ist ein Brand mit Sicherheit ausgeschlossen. Initiierungen, welche vom Menschen ausgehen, sind prinzipiell im Sinne von *Serendipity* kaum vollständig erfaßbar. Bei vorgegebenem, sehr großem Gefahrenpotential kann ein vertretbares Schutzziel nur noch über die Reduktion der Eintretenswahrscheinlichkeit erreicht werden (FRITZSCHE, 1986). Wie weit dies überhaupt sinnvoll ist, müßte vor allem mit der Verläßlichkeit der Risikoaussagen als Kernpunkt diskutiert werden (→ Unsicherheit der Basisdaten, Komplexität der Modelle, Informationsgehalt).







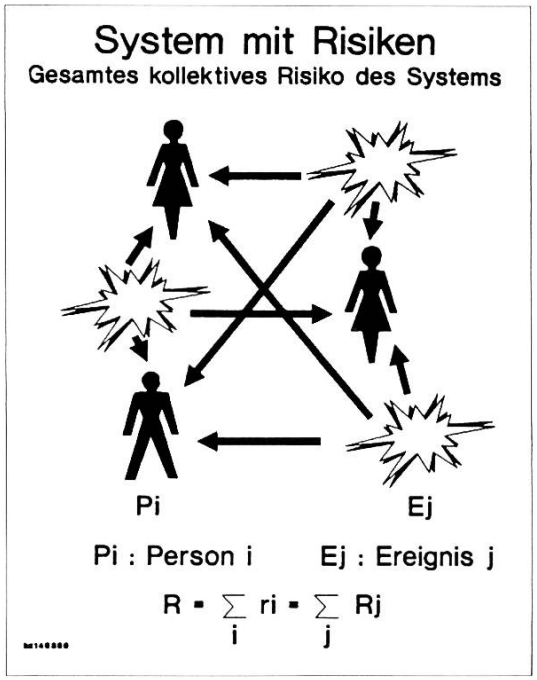


Fig. 2
Risiken, welche von den Ereignissen Ej ausgehen und die Personen Pi betreffen.

Verschiedene Gesichtswinkel für ein System mit Risiken:
Ganz generell lassen sich in einem System mit Risiken drei Gesichtswinkel der Risikoanalyse erkennen (zum Teil nach SCHNEIDER TH., 1985b). Als einfaches System betrachten wir 3 Ereignisse (E1, E2, E3, allgemein Ej), von denen Risiken ausgehen, und 3 Personen (P1, P2, P3, allgemein Pi). (Figur 2, S. 20)

Das *individuelle Risiko* ist das Risiko einer Person Pi, welche den Ereignissen E1, E2 und E3 ausgesetzt ist. Dies ist die Sicht von Einzelpersonen, welche alle Risiken der verschiedenen Quellen summiert. Hier treten sehr häufig *unfreiwillig eingegangene,* von außen geschaffene Risiken auf.

Das *kollektive Risiko* ist das Risiko mehrerer Personen E1, E2, E3, also eines Kollektivs, die einem Ereignis Ej ausgesetzt sind. Dies ist zum Beispiel die Sicht, der von einem einzelnen Unternehmen *eingegangenen Risiken.*

Das *gesamte kollektive Risiko* umfaßt das ganze System, also alle Personen E1, E2, E3 und alle Ereignisse E1, E2, E3. Dies ist die Sicht der Risiken, es muß aber auch die allgemeinste Sicht der Nutzen für die Gesellschaft sein.

2.7. Zeitliche Phasen

Technische Systeme durchlaufen folgende Phasen:
- Zielsetzung
- Planung und Projektierung
- Bau, Inbetriebnahme
- Betrieb, Kontrolle, Wartung
- Änderungen, Umbau und Erweiterungen
- Abbruch und Entsorgung

Für ein realisiertes System sagt die sogenannte ‹Badewannenkurve› aus, daß bei der Inbetriebsetzung die Frühausfälle, ‹Kinderkrankheiten›, Anlaufschwierigkeiten (→ Fehlerentdeckung und Fehlerbeseitigung), mangelnde Kenntnisse und fehlendes Training zu vermehrten Störungen führen. Dieser Zeitspanne folgt dann eine ‹Normalphase› mit den günstigsten Voraussetzungen (relativ hohe → Zuverlässigkeit [KÖCHEL, 1983]), also wenig Störungen. Abnützungserscheinungen, Verschleißausfälle, ‹Alterskrankheiten› und unkritische Gewöhnung machen ein System mit der Zeit wieder zunehmend unsicherer.

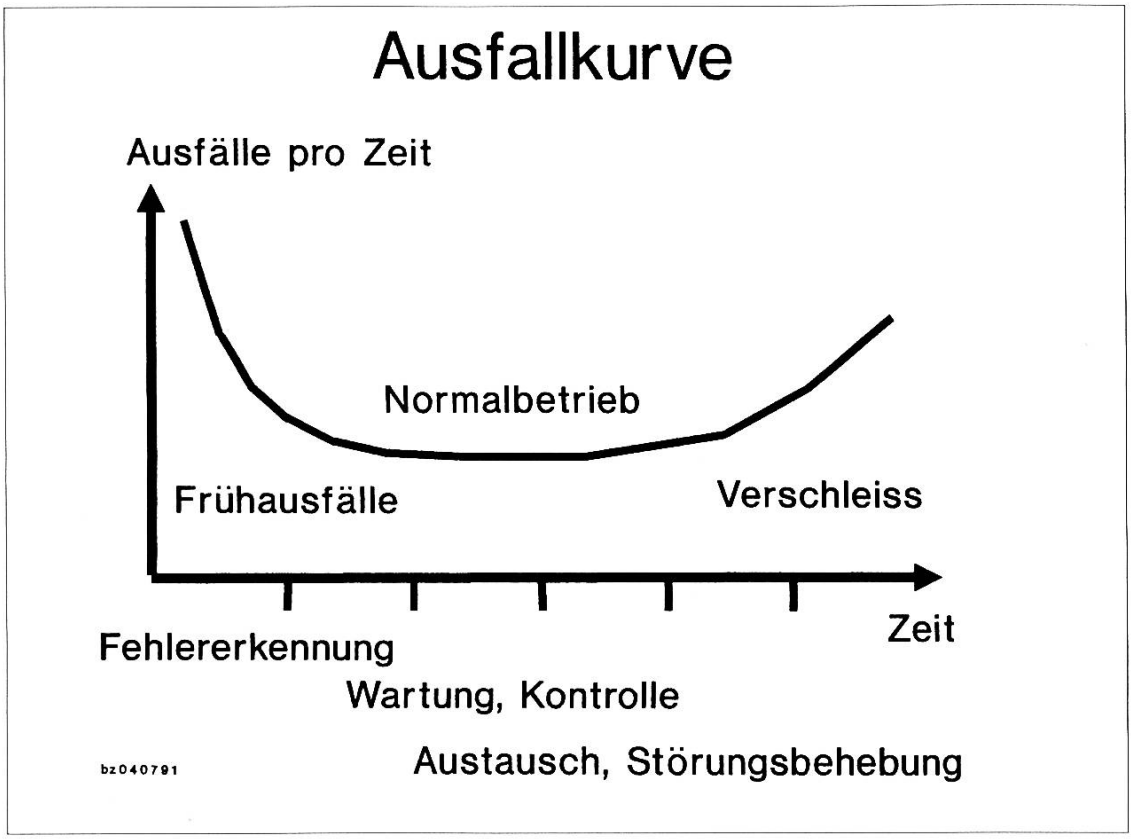


Fig. 3
Arten und Phasen von Systemausfällen, die ‹Badewannenkurve›. Jede dieser Phasen verlangt andere Qualifikationen bei der Ausbildung.

Sicherheit ist kein statischer Zustand, sondern eine dynamische Größe, die dauernd aufrechterhalten (KEMENEY et al., 1979b) und im Lichte neuer, gesicherter Erkenntnisse verbessert werden muß.

Meist wird bei technischen Anlagen zwischen Risiken des *Normalbetriebs* und Risiken im *Störfall* unterschieden. Diese Unterscheidung stammt aus der Nukleartechnik. Eine Definition, wann ein Störfall vorliegt, ist allgemeingültig nicht bekannt. Grundsätzlich kann jede Abweichung vom Normalzustand oder vom gewünschten Ziel als Störung bezeichnet werden, sie wird mit der Risikoanalyse erfaßt.

Der Begriff der Risikoanalyse technischer Systeme umfaßt die Risikoermittlung (Hazardidentification). Sie besteht aus der Gefahrensuche, deren Abschätzung nach Wahrscheinlichkeit und Wirkung sowie die möglichen Auswirkungen auf die Umgebung.

Nicht erkannte Gefahren:
Der wichtigste Teil der Risikoanalyse ist die *Gefahrensuche,* denn Gefahren, welche nicht erkannt worden sind, können mit keinem Aufwand und keiner Methode in ihrem Risiko analysiert und beurteilt werden.

Die Bezeichnung Gefahrenschnüffler für den Sicherheitsingenieur weist auf die Bedeutung dieser Qualifikation hin (ZWICKY, 1972). Wie wichtig Gefahrensuche sein kann, sei an drei Beispielen dargelegt. Die Legionärskrankheit wurde über die Klimaanlage eines Hotels verbreitet (PURKIS, WILSON, 1989), seither wurde den Klimaanlagen und Kühltürmen mehr Beachtung geschenkt. In einer Papiermühle trat ein großer Schaden durch eine Wasserstoffexplosion auf. Die Ursache waren Wasserstoffbakterien, welche sich unerwartet in einem Pulp-Tank gebildet hatten (ROWBOTTOM, 1989). Nicht isolierte, freistehende Tanks mit brennbaren Flüssigkeiten zeigen durch die Temperaturänderungen ein ‹Atmen›, welches zur Bildung explosionsfähiger Gas-Luft-Gemische in den Tanks und bei fehlender Flammensperre zu Explosionen geführt hat (LAPP, ROUSSAKIS, 1989). Es sind auch Explosionen von mit füssigem Stickstoff tiefgefrorenem Fleisch bekanntgeworden.

Als *wichtigste Methoden der Gefahrensuche* (ESCIS, 1981a, LEES, 1980a, PHILIPSON, 1982) für menschliche und technische Fehler sind bekannt:

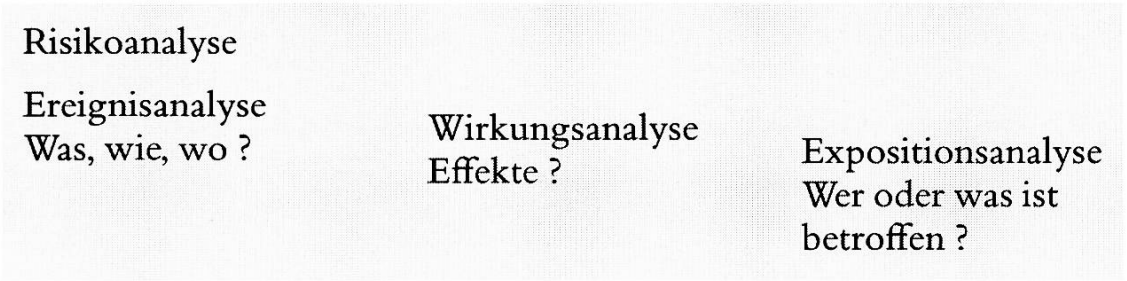
1. Intuitive Gefahrensuche (Brainstorming [DAENZER, 1976a])
2. Induktive Methoden (KUHLMANN, 1981)
   - Merkpunkte, Checklisten (DAENZER, 1976b)
   - Ausfalleffekt-Analyse (DIN 25448, 1980), Störfallablaufanalyse (DIN 25419, 1977), Abweichungsanalyse (Failure Mode and Effect Analysis)
   - Hazard and Operability Study (KLETZ, 1983), PAAG-Verfahren (IVSS, 1980)
   - Verfahrenssicherheitsstudie
   - Morphologische Verfahren (ZWICKY, 1966)
3. Deduktive Methoden (Fehlerbaumanalyse [DIN 25424, 1981], Ereignisbaum [LEES, 1980b])
4. Systemanalyse (JANSEN, 1990)
   - MORT (Management Oversight and Risk Trees) (FREI, 1979)
   - Sicherheitsrevisionen, Safety Audits

5. Mit bekannten, beschriebenen Risiken vergleichen: zum Beispiel (ESCIS, 1978, 1988, DORIAS, 1984, ROTH, WELLER, 1990, MARSHALL, 1987, LAGADEC, 1987)
6. Menschliche Fehler (WILLIAMS, 1985, WAHLLEY, KIRWAN, 1989, BURKARDT, 1990, KLETZ, 1985a)

Schwerwiegende Fehler bei der Gefahrensuche führen dazu, daß man ein Problem der Sicherheit richtig löst, aber nicht das richtige Problem löst. In diesem Bereich spielt die Intuition und die Kreativität sowie die selektive Wahrnehmung (PERROW, 1984) jedes Individuums eine bedeutende Rolle; ein Team bringt aus diesem Grunde große Vorteile. Die intuitive Beurteilung muß trotzdem immer rational hinterfragt werden, sonst läuft man Gefahr, vordergründig triviale und oberflächlich gesehen einsichtige, wissenschaftlich aber falsche Aussagen als gegeben hinzunehmen (KLETZ, 1990). So ist die Feststellung allgemein anerkannt, daß Eisen nicht brennt. Dies ist in dieser umfassenden Form falsch, denn feines Eisenpulver verbrennt in der Luft bei entsprechend kleiner Korngröße; feiner Eisenstaub entzündet sich sogar selbst, er ist pyrophor. Für einen Chemiker ist es beispielsweise überraschend, daß 1991 noch neue Beobachtungen bei Reaktion von Chlorwasserstoff mit Ammoniak gemacht werden konnten (BÜTZER, 1991b).

2.9. Gliederung einer Risikoanalyse

Die Risikoanalyse muß in drei Stufen durchgeführt werden (BAUMGARTNER et al., 1977):



Die Risikoanalyse ist die Basis für die Risikobeurteilung und das Risiko-Management.

- *Risikobeurteilung,* Risikobewertung. Technische Risiken stehen in einem größeren Rahmen, sozial, ökonomisch und ökologisch. Die Beurteilung muß auch diese Aspekte berücksichtigen.

– *Risiko-Management.* Dieses hat die Aufgabe, mit allen notwendigen Maßnahmen sicherzustellen, daß die gesteckten Ziele erreicht werden können. Risikoanalyse und Risikobeurteilung liefern dabei die notwendigen Grundlagen.

Die Risikoanalyse technischer Systeme ist in praktisch allen Anwendungsfällen bereits für kleine Systeme ein *interdisziplinärer Prozeß,* erst recht die Risikobeurteilung. Sie kann keiner einzelnen Fachrichtung zugeordnet werden. Interdisziplinarität verlangt einerseits ausgezeichnete Spezialisten, andererseits von allen Beteiligten eine gemeinsame Grundlage.

2.10. Zuverlässigkeit

Der Wunsch nach zuverlässigen Maschinen ist so alt wie die Maschinen selbst. Bei den Ingenieurwissenschaften ist die Zuverlässigkeitsanalyse als Tradition deshalb etabliert. Sie setzt sich aus Methoden zur Erfassung, Kontrolle und Prognose der Zuverlässigkeit technischer Anlagen zusammen. Die Methoden sind weitgehend standardisiert in Regelwerken, Normen, Leitlinien und Handbüchern festgehalten. Das Ziel dieser Analyse ist eine möglichst quantitative Bewertung der Zuverlässigkeit des betrachteten Systems und der Gewinn von Einsichten über Gründe möglicher Versagensarten. Die Zuverlässigkeiten betreffen Erfahrungswerte meist auf der Ebene von Komponenten, seltener für Module. Für Systeme wird die Zuverlässigkeit deshalb aus den Komponentendaten ermittelt, wobei die Kopplungen der Komponenten im System entsprechend berücksichtigt werden. Dieser Bereich wird im englischen Sprachgebrauch als ‹Engineering Risk Analysis› bezeichnet.

Die Zuverlässigkeit von technischen Elementen kann oft mit statistischen oder wahrscheinlichkeitstheoretischen Modellen auf der Basis der Konstruktion, der Materialeigenschaften und der möglichen Beanspruchungen berechnet werden. Um die geforderte Zuverlässigkeit erreichen zu können, werden Lastannahmen, Beanspruchungen oder Szenarien festgelegt. So ist es zum Beispiel in der Schweiz seit einiger Zeit üblich, Flußverbauungen auf das 100jährliche Hochwasser auszubauen (JÄGGI, 1988). Die Auslegung erfolgt dann mit einer Sicherheitsmarge (→ Sicherheitsfaktor, Sicherheitsabstand), um Unsicherheiten abzufangen (BIRKHOFER, KÖBERLEIN, 1987a). Übrig bleibt ein Risiko (→ verbleibendes Risiko), und erreicht ist meist eine mit den getroffenen Annahmen übereinstimmende Zuverlässigkeit.

Zuverlässigkeit, drei Schritte:

Lastannahmen/Szenarien
Auslegung
Risiko

Die Zuverlässigkeitsanalyse beschäftigt sich definitionsgemäß nicht mit den weiteren Folgen eines Systemausfalls; diese Fragestellung wird im Rahmen der Störfall- oder Risikoanalyse auf der Basis von Szenarien bearbeitet. Die Diskussion von Szenarien verlangt ihrerseits wieder die Modellierung und Simulation des Systems, ein weiterer Schwerpunkt aller Ingenieurdisziplinen. Auch Auswirkungen über verschiedene Belastungspfade, Akkumulationen, Potenzierungen oder Synergismen werden nicht berücksichtigt, da die Zuverlässigkeitsanalyse fast ausschließlich objektbezogen durchgeführt wird. Ein sehr oft synonym verwendeter Begriff, die Verfügbarkeit, läßt sich auch auf Sicherheitssysteme anwenden, auch wenn diese im Normalfall abgeschaltet sind oder im Stand-by gehalten werden. So kann man sich für diese Systeme die Frage stellen, ob bei der Stromversorgung kritischer Anlagen ein Dieselgenerator als Notstromaggregat zum elektrischen Netz, oder das öffentliche Netz besser als Back-up-System für den eigenen Generator zu verwenden ist. Die Beurteilung dieser Varianten muß vor dem Hintergrund erfolgen, daß das rechtzeitige Starten eines Notstromdiesels auch bei guter Wartung bestenfalls mit 80% eingesetzt werden kann.

3. Risikoanalyse

3.1. Systematik

Die Risikoanalyse umfaßt die 3 wichtigen Elemente:
- Ereignisanalyse
- Wirkungsanalyse
- Expositionsanalyse

Die *Ereignisanalyse* verlangt, daß die Risiken zuerst einmal erkannt (→ Gefahrensuche, Hazardidentification) und in ihren Wahrscheinlichkeiten abgeschätzt werden können (→ Störbarkeit). Es stehen die Fragen im Vordergrund: Was kann schiefgehen, auf welche Weise und wie häufig kann das passieren? Bei der Erfassung der Grunddaten ist darauf zu ach-

ten, daß die *Kombinationen von einzelnen Basis-Parametern* viel häufiger zu praxisnahen und damit aussagekräftigen Größen führen (PITT, 1982, BÜTZER, 1985b, ROUSSELIN, FALCY, 1986). So können aus einer Zugfestigkeit ohne Elastizität, einer Druckfestigkeit ohne Fließverhalten, einer Verbrennungsenergie ohne Reaktionsgeschwindigkeit kaum direkt aussagekräftige Folgerungen gezogen werden.

Die *Wirkungsanalyse* befaßt sich mit möglichen Wirkungen von Ereignissen. Dabei müssen die physikalischen, chemischen, toxikologischen und biologischen Wirkungen in ihrem Umfang und insbesondere auch ihrer Dynamik erfaßt werden (Emission).

Morphologie der Dynamik (zeitlicher Ablauf):

Merkmal	Ausprägungen	
Eintritt	sofort	verzögert
Folge	simultan	gestaffelt
Ablauf	rasch	langsam
Wirkung	akut	chronisch
Folgen	reversibel	irreversibel

Die zeitliche Komponente von Ereignissen ist für die Bewältigung ganz wesentlich. Ein verzögerter Eintritt, wie er zum Beispiel bei kleinen Konzentrationen von Luftschadstoffen und häufig bei rückgekoppelten Prozessen auftritt, erschwert die Beurteilung der Zusammenhänge zwischen Ursache und Wirkung und des zeitgerechten Vollzugs von Maßnahmen (z.B. Treibhauseffekt, Ozonloch, Schwermetallanreicherungen etc.).

Simultane Ereignisse führen, besonders wenn sie örtlich konzentriert auftreten, zu einer Überbeanspruchung der Logistik (z.B. Polizei, Feuerwehr, Sanität) und einer entsprechenden Aversion (→ Logistik-, Aversionsexponent).

Ein langsamer Ablauf (chronische Ereignisse) ermöglicht es, in einen laufenden Prozeß noch steuernd einzugreifen. Notfallmaßnahmen haben unter diesen Voraussetzungen eine Chance auf Erfolg. Ganz anders zeigt sich die Situation bei akuten, sehr rasch ablaufenden Ereignissen.

Irreversible Folgen lassen, im Gegensatz zu reversiblen, keine Möglichkeiten mehr zu, den Ausgangszustand in einem vernünftigen Zeitraum wieder herzustellen, sie verdienen deshalb spezielle Beachtung.

3.2. Das Eisbergsyndrom

Ganz unspezifisch gilt für alle Bereiche das Eisbergsyndrom (LEES, 1980c), das heißt, Ereignisse mit kleinen Auswirkungen treten häufig auf, größere Auswirkungen sind schon seltener, und ganz große Auswirkungen sind sehr selten. Die Folge davon ist, daß große Systeme oder kritische Zustände gut abgesichert und deshalb komplex aufgebaut sind (PERROW, 1988). Die Katastrophen bei Systemen mit tiefgestaffelten Sicherheitsmaßnahmen (→ z.B.: Redundanz, Barrierenprinzip) sind die Folge von Ereigniskaskaden. Deren Wahrscheinlichkeiten, die statistische Anzahl Ereignisse pro Zeit, errechnen sich als Kombinationen von Einzelwahrscheinlichkeiten (→ Klassierung von Ereignissen/Störfällen), sie sind bei korrekter Auslegung meist sehr klein.

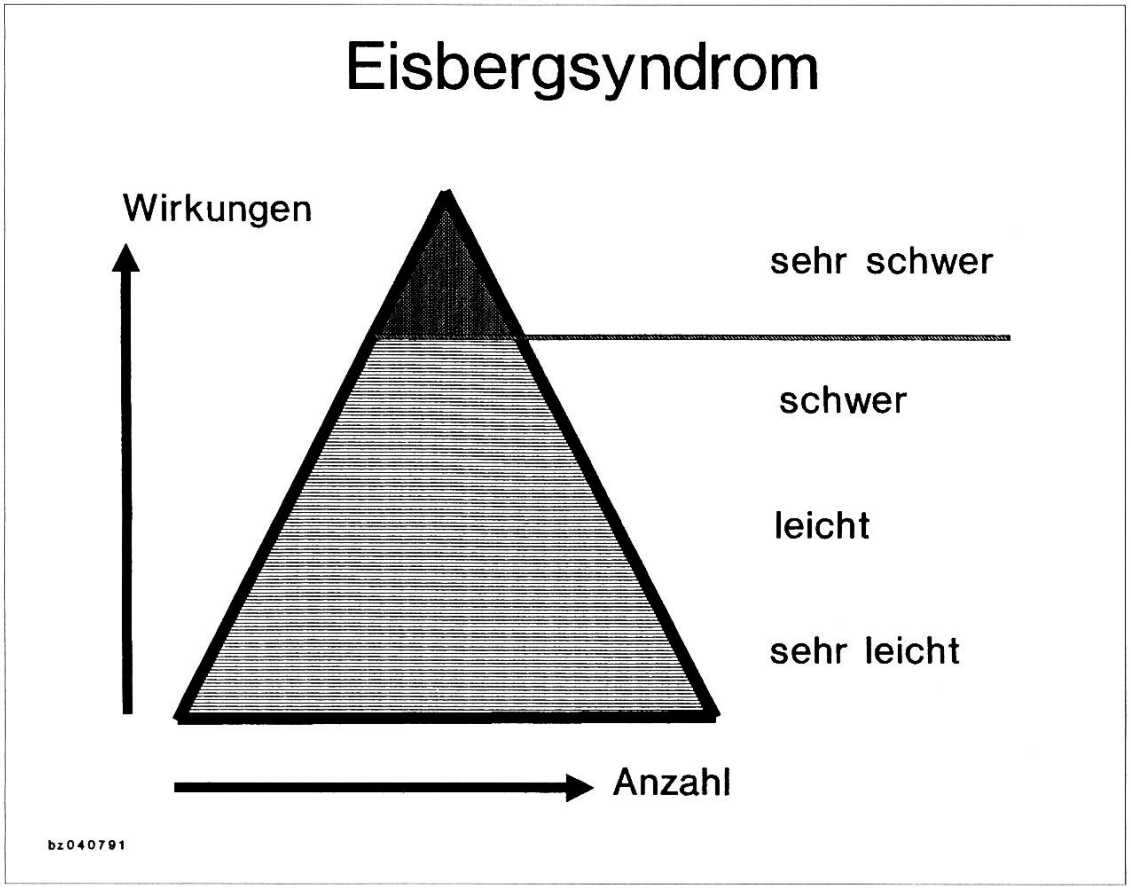


Fig. 4
Korrelation zwischen Auswirkungen, Schwere der Ereignisse und deren Anzahl oder Häufigkeit. Da meist nur die sehr schweren Auswirkungen allgemein in Erscheinung treten, wie die Spitze eines Eisbergs, spricht man vom ‹Eisbergsyndrom›.

Würden zusätzlich die Bagatellunfälle oder die Fastunfälle berücksichtigt, so wäre der Fuß der Pyramide noch viel breiter. Es ist immer die Spitze des ‹Eisbergs›, welche sich am tragischsten und spektakulärsten zeigt, die seltenen, aber sehr großen Ereignisse (*LPHCE:* low probability, high consequence events). Leider ist es nicht möglich, diese Spitze des Eisbergs zu kappen und damit die größten Auswirkungen zu verhindern. Der Abbau des Eisbergs von der Basis, also bei den Fast- und Bagatellereignissen, ist auf die Dauer am wirksamsten. Die entscheidende Voraussetzung, mit größeren Systemen verantwortungsvoll umzugehen, ist die Lernbereitschaft, kleine Fehler als Glieder einer möglichen Ereigniskette, mit letztlich großen Konsequenzen, ernst zu nehmen (→ Sicherheits-Kultur, → Fehlerfreundlichkeit). Dies gilt ganz besonders auch im Bereich der Ökologie mit ihren teilweise sehr langen Wirkungsketten.

Die *Expositionsanalyse* geht von der Fragestellung aus: ‹Wer wird von den Auswirkungen betroffen?›. An diesem Punkt werden die möglichen Schäden erfaßt. Dabei müssen alle möglichen Pfade der Belastung, auch Synergien, berücksichtigt werden (Immission). Diese Analyse wird oft auch als Konsequenzanalyse bezeichnet (→ Verletzbarkeit). Die Auswirkungen sind eine Funktion von *Fläche und Effekt.* Bloße Angaben von Wirkungsdistanzen sind falsch.

In erster Linie müssen Risikoanalysen den Anspruch der Vollständigkeit erfüllen. Sie dürfen sich nicht auf quantitativ erfaßbare Größen beschränken, obwohl qualitativ umschriebene Parameter eine Bewertung in vernetzten, realitätsnahen Systemen sehr erschweren. Eine Möglichkeit bieten die morphologischen Ansätze und das Sensitivitätsmodell (VESTER, 1986). Eine weitere Möglichkeit, integrale Risikoanalysen mit ‹weichen› und unsicheren Fakten vorzunehmen, bietet das Matrixverfahren (BÜTZER, 1987b).

4. Risikobeurteilung

Die Risikobeurteilung hat zum Ziel, Nutzen und Gefahren in den Bereichen:

technisch – sozial – ökonomisch – ökologisch

gegeneinander abzuwägen (HARTWIG, 1983). Das gesamte System ist in die Betrachtung einzubeziehen (→ System mit Risiken). Die Frage, ob *zentrale Großlösungen* besser sind als *dezentrale Ansätze,* ist Teil der Be-

urteilung (bei Abfällen z.B.: concentrate and contain oder dilute and disperse). Einer breiten Verteilung der Risiken sind Vor- und Nachteile, Kosten und Nutzen von geballten Großrisiken mit aufwendigen Sicherheitsmaßnahmen gegenüberzustellen (BÜTZER, 1989a). Große Gefahrenpotentiale an einem Ort führen zwangsläufig zu einer gemeinsam gleichen, mindestens aber sehr ähnlichen Beurteilung der lokal Betroffenen. Solidarisierung und gemeinsame, abgestimmte Reaktionen sind zu erwarten, auch wenn unterschiedliche Einschätzungen der Wahrscheinlichkeiten und der Wirksamkeit der Sicherheitssysteme üblich sind (→ Ablaufschema). Alleine die Strukturen der Gefahrenpotentiale erlauben somit Aussagen über die lokal empfundene Situation.

Begriffe wie *kollektive Risiken, Solidarität,* akute und chronische, direkte und indirekte Wirkungen, Synergismen, Akkumulation, mittelbarer und unmittelbarer Nutzen, Kurzzeit- und Langzeitaspekte haben in der Folge dieser mehrdimensionalen Betrachtungsweise große Bedeutung. Sie geben ein äußerst differenziertes Bild. Die Risikobeurteilung verlangt einen Blick in die Zukunft und ist auf einer unsicheren und unvollständigen Informationsbasis abgestützt. Sie verlangt den Dialog mit der Gesellschaft, geht es doch auch darum zu erkennen, welche Risiken, verbunden mit ihrem Nutzen, toleriert werden.

Die Risikobeurteilung ist somit nicht die Domäne der technischen oder ökonomischen Experten. Jede Risikobeurteilung darf aber wissenschaftliche Fakten nicht ohne bessere Begründung ignorieren oder gar umkehren. Sie muß sich an einem Ziel orientieren, hat die *gesicherten Phänomene zu berücksichtigen* und muß um *konsistente Modelle oder Theorien* besorgt sein.

Schritte zur Risikobeurteilung:

- Die Risikoerhebung (Gefahrensuche) erfolgt nach Strukturen, sie sorgt für die Vernetzung.
- Die Risikoanalyse nimmt zusätzlich die Funktionen auf, sie erfaßt die Kopplungen.
- Die Risikobeurteilung konzentriert sich vorwiegend auf Szenarien und Folgen, sie ist prognostisch im Sinne von: wenn, dann.

5. Risiko-Management

Bei einem Unfall werden nur zu oft Phänomene sichtbar, die es schwer verständlich machen, daß sie übersehen worden sind (→ Gefahrensuche, Ereignisketten). Es ist aber qualitativ und von der Anzahl möglicher Kombinationen gesehen auch quantitativ ein gewaltiger Unterschied, ob Abläufe retrospektiv nachvollzogen oder prospektiv erkannt werden müssen. So betrachtet ist es immer einfach, nach einem Unfall das Fehlen von Sicherheit nachzuweisen, aber nur selten kann man zeigen, welche Ereignisse mit Sicherheitsmaßnahmen verhindert worden sind Die Fehlersuche nach einem Störfall darf sich nicht darauf konzentrieren, Schuldige zu suchen, sondern sollte sich danach ausrichten, die Grundlagen bereitzustellen, um die Systeme für die Zukunft zu verbessern.

5.1. Vorgehen

Notwendig für ein Projekt sind die Schritte (ESCIS, 1981b, siehe auch → Ablaufschema für das Risiko-Management):

1. Zielsetzung, die ethisch vertretbar ist,
2. Durchführung einer umfassenden Risikoanalyse,
3. zugängliches Wissen und das wissenschaftliche Instrumentarium optimal nutzen,
4. Sicherheitsmaßnahmen, welche den Gesetzen, dem Stand der Technik, den Erkenntnissen der Risikoanalyse sowie wichtigen Sicherheitsgrundsätzen entsprechen.

5.2. Eingriffsarten

Prinzipiell gibt es verschiedene Ansatzpunkte, um mit Risiken umzugehen. Zeitlich, dynamisch lassen sich folgende Eingriffsarten unterscheiden:

5.2.1. präventiv (vorbeugend):

Gewisse Ereignisse werden prinzipiell ausgeschlossen.

Eliminieren oder verringern von Gefahrenpotentialen, reduzieren von Initiierungen und erhöhen der Zuverlässigkeit sind wichtige Maßnahmen. Die präventive Eingriffsart ist die wirkungsvollste, birgt aber immer die Gefahr in sich, daß Risiken nicht eliminiert oder verringert,

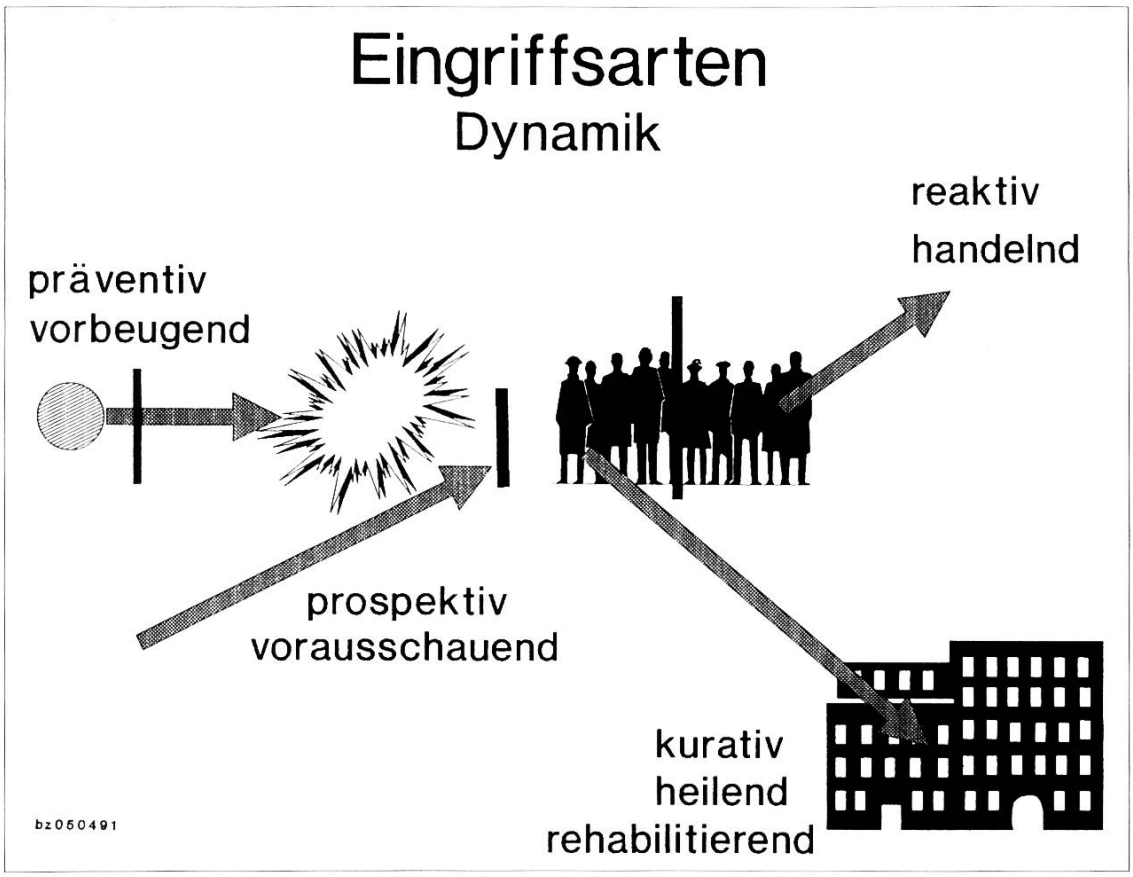


Fig. 5
Mögliche Eingriffsarten bei möglichen Ereignissen unter dem Gesichtspunkt der zeitlichen Dynamik.

sondern absichtlich oder unabsichtlich verlagert werden. (z.B. FCKW, Brand- und Toxizitätsreduktion auf Kosten der Umweltbelastung etc.).

5.2.2. *prospektiv* (vorausschauend):

Das Ereignis wird grundsätzlich nicht ausgeschlossen, der Ablauf soll aber so kontrolliert werden, daß die Auswirkungen nicht zu groß sind.

Planen von Gegenmaßnahmen bei möglichen Ereignissen, verringern der Tragweite, verringern der Exposition, Aufbau von wirkungsvollen Warn- und Kontrollanlagen sind einige Möglichkeiten (z.B. Ölsperren, flammhemmende Textilien, Abwasserreinigung etc.).

5.2.3. *reaktiv* (unmittelbar auf ein Ereignis handelnd):

Das eingetretene Ereignis soll in seinen Auswirkungen mit den Mitteln, die durch prospektive Maßnahmen zur Verfügung gestellt wurden, begrenzt werden.

Notfallmaßnahmen, um die Auswirkungen eines eingetretenen Ereignisses durch rasches Reagieren zu verringern. Alarmsysteme und -organisation, Auffangbereiche improvisiert bereitstellen, Notfalldienste aufbieten etc. Geht der Alarmierung eine *Warnung* voraus, dann sind Maßnahmen effizienter, sie sind in diesem Fall teilweise prospektiv. Eine *Pikettstellung* führt durch den Zeitgewinn zu mehr Handlungsfreiheit (z.B. Feuerwehr, Rettungshelikopter etc.).

Entscheidungen, die unter Zeitdruck getroffen werden müssen sind immer kritisch:

Maßnahmen im Ereignisfall, eine Gratwanderung:

- Wer *zu geringe Maßnahmen* anordnet, verliert das Vertrauen (Leichtsinnige sind schlechte Berater)
- Wer *zu extreme Maßnahmen* anordnet, verliert die Glaubwürdigkeit (Maximalmaßnahmen verlangen keine Fachleute)

5.2.4. kurativ (heilend):

Die eingetretenen Schäden werden beseitigt, verringert, abgegolten, mindestens aber an einer weiteren Ausbreitung gehindert.

Wiederherstellung, Behandlung von Verletzten, Reinigung von Kontaminationen, Rehabilitation, Wiederaufbau etc. (z.B. Sanierung von kontaminierten Böden, Entgiftung des Trinkwassers bei der Gewinnung etc.).

Für die praktische Durchführung von Maßnahmen hat es sich bewährt, die verschiedenen Eingriffsarten mit möglichen Eingriffsbereichen zu kombinieren.

Drei verschiedene Eingriffsbereiche:

T: technisch,
O: organisatorisch,
P: personell.

Die Kombinationen von Eingriffsarten und Eingriffsbereichen zeigen sich als Maßnahmenmatrix:

Eingriffsbereiche	technisch	organisatorisch	personell
Eingriffsarten	präventiv	prospektiv	reaktiv	kurativ

Maßnahmen werden entsprechend der Risikosituation sehr häufig in Schritten, Stufen, nach Klassen oder Gruppen getroffen (BIEDERMANN, 1987, KIER, MÜLLER, 1986). Ein Beispiel dazu sind die Interpretationen der sieben Gefahrenstufen des Lawinenbulletins (EGGER, 1988). Dieser Umstand ermöglicht es, schon bei der Risikoanalyse, aber auch bei der Risikobeurteilung, die Parameter morphologisch einzuteilen. Damit wird eine semiquantitative Beurteilung möglich. Die Klassenanzahl jedes Parameters ist dabei durch die Erfaßbarkeit und die Unsicherheit gegeben (Streubereich, → Fehler). Die Anwendug eines Matrixverfahrens drängt sich hier auf.

Der Intuition sind bei technischen Maßnahmen und noch viel mehr im naturwissenschaftlich-technischen Forschungs- und Entwicklungsbereich sehr enge Grenzen gesetzt. Die Bemessung setzt praktisch immer sehr gute Kenntnisse der Prozesse und Funktionen von Material und Dimensionierung voraus. Zum Teil können Schwachstellen mit geeigneten Hilfsmitteln erkannt werden. Für brennbare Gase wurden zum Beispiel dreidimensionale Auswertungen mit Erfolg verwendet (BÜTZER, 1988). Im ökologischen Bereich sind die Anforderungen an die Systematik wegen der hohen Vernetzung besonders hoch. Selbst Gestaltungs- und Pflegemaßnahmen in Rietgebieten sind von Fachleuten nicht ohne systemanalytische Hilfsmittel erkennbar (BÜTZER, 1990b).

5.3. Anforderungen an Notfallsysteme

Die Flexibilität des Menschen, Improvisationsgabe und Kreativität kann bei nicht vorhergesehenen, außerordentlichen Situationen von keinem automatischen System erreicht werden. Dies ist vor allem bei Notfallsystemen, weniger bei Sicherheitssystemen der Fall. Sollen diese Fähigkeiten aber genutzt werden können, müssen drei Voraussetzungen erfüllt sein (BIRKHOFER, KÖBERLEIN, 1987b):

1. Es muß ausreichend Zeit für eine überlegte Reaktion zur Verfügung stehen.
2. Die Informationen über die gesamte relevante Situation müssen ausreichend sein.
3. Die Erfahrung, Ausbildung und die Fertigkeiten müssen den Anforderungen entsprechen.

Große Ansprüche an das Vorgehen können bei schwierigen Situationen unter Zeitdruck nicht mehr gestellt werden. Als Minimum muß aber ein

Ziel aller Maßnahmen sein, *irreversible Schäden zu vermeiden* und reversible Schäden soweit als möglich zu begrenzen.

Maßnahmen, welche nach Eintritt des Ereignisses die Folgen verringern oder begrenzen, werden mit dem Begriff *sekundäre Sicherheit* zusammengefaßt. Beispiel:

Beim Auto ist das Zweikreisbremssystem primäre (präventiv), die Sicherheitsgurten sekundäre Sicherheit (prospektiv).

Maßnahmen, welche darauf abzielen, die Auslöser auszuschalten, faßt man unter *primärer Sicherheit* zusammen. Das Gefahrenpotential ist in diesem Fall nicht wesentlich in die Maßnahmen einbezogen. Hierzu gehören auch die Notfallsysteme. Bei der Planung kann die Sicherheit erhöht werden, indem sekundäre Sicherheiten, wo immer möglich und vertretbar, durch primäre Sicherheiten ersetzt werden.

5.4. Schutzmöglichkeiten

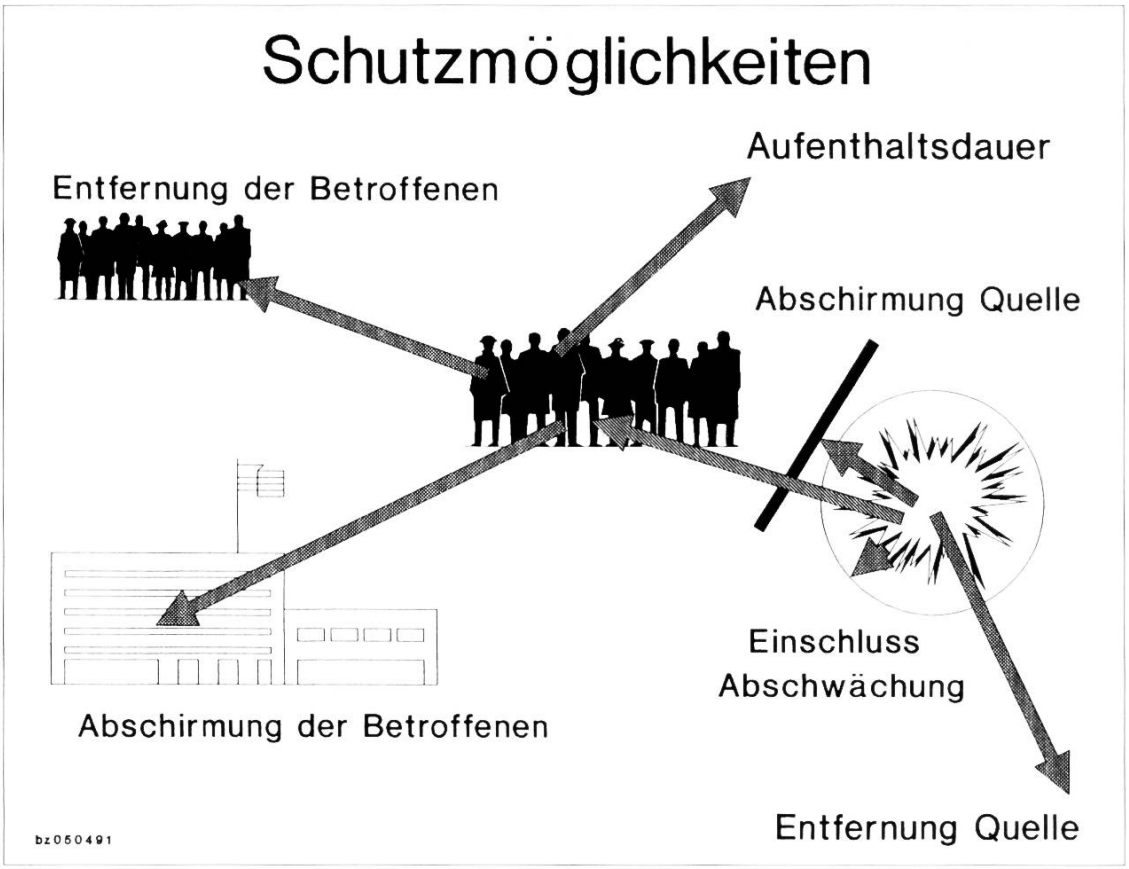


Fig. 6
Prinzipielle Möglichkeiten für den Schutz von Personen gegenüber einem Ereignis.

Sekundäre Sicherheit läßt das Ereignis prinzipiell zu und zielt auf den nachträglichen Schutz ab. Für den Schutz von Personen bestehen verschiedene Möglichkeiten, die sich aber nur teilweise auf die Umwelt oder Sachgüter übertragen lassen:

Dieses Schutzkonzept ist im wesentlichen auf den drei Faktoren Distanz, Abschirmung und Zeit (Aufenthaltsdauer) aufgebaut. Angewandt auf die Quelle und die Umgebung, ergeben sich insgesamt sechs Varianten.

Ein sicheres Schutzkonzept ist alleine nicht tragfähig. Es muß nebst den Strukturen und den Verhaltensanweisungen immer auch ein Informationskonzept enthalten. Dieses stellt die Verbindungen Risikoverursacher und Betroffenen sicher, macht Schutzmaßnahmen einsichtig und wirksam (siehe → System mit Risiken) und ermöglicht den notwendigen Dialog (HALLER, 1990b).

5.5. Maßnahmen bei Risiken

Das Risiko-Management bei technischen Systemen zielt auf eine Risikominderung ab. Es baut dabei auf den Grundsätzen auf:

Maßnahmen bei Risiken (HALLER, 1975, KLETZ, 1985b):

früh eingreifen, ändern
vermeiden, ersetzen
vermindern, verkleinern
verdünnen, verteilen
substituieren
vereinfachen
überwälzen
versichern
selbst tragen

Früh eingreifen oder ändern hat zum Ziel, günstige Situationen zu schaffen, welche dem Gefahrenpotential, den Auslösern oder dem Menschen schon auf der Stufe der Planung angepaßt worden sind. Wirklich ganzheitliche Ansätze sind nur auf der Planungsstufe möglich, denn Ganzheiten zeigen auch Eigenschaften, die ihre Teile nicht aufweisen (MOSER, 1985). Früh eingreifen ermöglicht bei den Abfällen, von der ‹end of the pipe›-Technologie weg und zur Abfallvermeidung, Abfall-

verminderung und Wiederverwendung (Recycling) zu kommen. Die Funktionalität eines Produkts kann mit dieser Zielsetzung nicht nur aus der Sicht der Anwendung, sondern auch aus der Sicht der Umwelt optimiert werden (FCKW, PCB, chlorierte KW, Hydrauliköle, Motoren etc.).

Aufgepfropfte Sicherheitsmaßnahmen, zum Beispiel aktive Maßnahmen (Regelventile etc.), sollten durch integrierte, sichere Systeme, zum Beispiel inhärent sichere Auslegung (wie dünnere Rohre zur Mengenstrombegrenzung), ersetzt werden. Dies ist schon deshalb wünschenswert, weil zusätzliche Sicherheitssysteme die Eigenschaft haben, im Normalfall nicht aktiv zu sein, trotzdem kontrolliert und gewartet werden müssen und bei einem Fehler die normalen Abläufe meist stören oder unterbrechen. Sicherheitssysteme sollten aus ökonomischen Überlegungen immer mehr durch sichere Systeme ersetzt werden, welche sich auch im Normalbetrieb ohne Eingriffe von außen durch eine hohe Verfügbarkeit auszeichnen. Damit gehen Sicherheit und Verfügbarkeit, also Ökonomie, parallel. Ergonometrische Gesichtspunkte müssen die Mensch-Maschine-Schnittstelle so beeinflussen, daß der Mensch eine große Chance hat, richtig zu handeln (z.B. Anzeige- und Steuersysteme). Ökologisch-kybernetische Maßnahmen sollten schließlich darauf abzielen, daß sich die Systeme möglichst weitgehend selbst in einem dynamischen Gleichgewicht stabilisieren (negative Rückkopplung).

Einfache Systeme sind sehr oft die sicheren Systeme.

Überprüfung der aktuellen Situation:

Es ist sicherheitstechnisch und ökonomisch sinnvoll sich bei Planung und Betrieb die Frage zu stellen:

1. **Was kann vereinfacht werden (Abläufe, Komponenten, Systeme)?**
2. **Was sind die Folgen der Vereinfachung?**

In Alarm-, Krisen- und Katastrophensituationen, also unter Zeit-, Handlungsdruck und Streß, versprechen nur optimale Situationen Aussicht auf Erfolg (KEMENEY et al., 1979c) (→ Anforderungen an Notfallsysteme). Dies kann schwergewichtig durch Maßnahmen erreicht werden, welche auf der Stufe der Planung berücksichtigt worden sind (BÜTZER, 1991a). Leicht verständliche, gut überblickbare und einsichtig reagierende Systeme können unter schwierigen Bedingungen besser beherrscht werden.

Grundsatz für die Auslegung von Überwachungs-, Steuerungs- und Notfallsystemen:

Change situations, not people!

Diese Aussage gilt nicht nur für die technischen, sondern noch in vermehrtem Maße für die organisatorischen Rahmenbedingungen, insbesondere die Kompetenzverteilung. Es wäre falsch zu glauben, die Planung könne sicherstellen, daß jeder Unfall korrekt und zeitgerecht gemeistert wird. Situatives Verhalten wird immer notwendig bleiben. Eine Auswertung der größten Unfälle in Erdölindustrieanlagen der letzten 30 Jahre (PALMER, MARSHALL, 1991) hat gezeigt, daß das menschliche Versagen nur zu 14,8% zu allen Fällen beigetragen hat, 54,7% waren auf dynamisches Versagen (Explosion in der Anlage, Überdruck, Temperaturexkusion, meteorologische Einflüsse, Verlust des Containments etc.), 30,5% auf statische Ursachen (Rohrbruch, Behälterbruch, Schweißfehler, Korrosion oder Erosion) zurückzuführen. Daß in einer solchen Umgebung die Möglichkeiten des Menschen für Eingriffe außerordentlich beschränkt sind, ist selbstredend.

Konkrete Maßnahmen sind sehr oft mit den Begriffen: *Redundanz, Barrierenprinzip* (UK HEALTH AND SAFETY EXECUTIVE, 1979), *Diversifikation, Fail Safe,* Save Life, Wartung, Kontrolle, Instandhaltung, Ausbildung, Training usw. verbunden. Die technischen Maßnahmen bewirken eine Erhöhung der *Fehlertoleranz des Systems.* Dabei gilt der Grundsatz, daß ein einfacher Fehler nie zu einem Ereignis mit großen Konsequenzen führen darf.

Redundante Sicherheitssysteme können zu einer Verminderung der Verfügbarkeit führen, da bei einem Systemfehler eine Unterbrechung möglich ist (→ Konflikt bei Auswahlschaltungen [VDI/VDE, 1967]). Sie sind damit aus der Sicht der Ökonomie kurzfristig nicht attraktiv.

Bei Redundanzen ist dem gleichzeitigen Ausfall mehrerer Systeme durch *eine* gemeinsame Ursache *(common mode failure)* besondere Beachtung zu schenken (Korrosion, elektrische Felder, Erdbeben, Brand, Wasser etc.). Besonders bei vielen Redundanzen, wie sie bei Systemen mit großen Gefahrenpotentialen üblich sind, kann als Folge einer unbeachteten Kopplung die Möglichkeit bestehen, durch einen einzigen Fehler gestaffelte Sicherheitssysteme zu überwinden. Auch diversifizierte Systeme können solche sehr kritischen Fehler nur dann vermeiden, wenn sie wirklich unabhängig sind (Energieversorgung, örtliche Trennung

etc.). Nicht alle möglichen Sicherheitsmaßnahmen müssen daher sinnvoll sein.

Maßnahmen sollten minimale Anforderungen erfüllen, wenn sie technisch und juristisch nicht als willkürlich gelten sollen:

Kriterien zur Beurteilung von Maßnahmen

- notwendig
- angemessen
- verhältnismäßig

Die Maßnahmen sind so zu optimieren, daß mit einem vertretbaren Aufwand ein möglichst großer Sicherheitszuwachs erreicht werden kann. Ob sich dazu der Aufwand pro gerettetes Menschenleben als Maß eignet (SCHNEIDER, 1988), ist als Frage offen. Diese Optimierung setzt aber voraus, daß als Maßnahmen *Ziele* und nicht konkrete Anweisungen vorliegen.

Grenzwerte als maximal zulässige Belastungen, Konzentrationen oder Dosen (STEPHAN et al., 1985) können sich als Schutzziele nur dann eignen, wenn sie chronische Ereignisse betreffen. Zudem muß die Voraussetzung gegeben sein, regelnd einzugreifen. Die Natur selbst hat diesen Weg, zum Beispiel mit der Begrenzung von Konzentrationen natürlicher, reaktiver Stoffe (Sauerstoff, Ozon, Peroxide, Aldehyde, saurer Regen [PRINZ et al., 1983] etc.), vorgezeichnet. Grenzwerte müssen auf einem Maximalwert und einem Sicherheitsfaktor (DE MORSIER, 1988) aufgebaut sein. Dieser Sicherheitsfaktor sollte um so größer sein, je unsicherer die Grundlagen sind, mit denen der Maximalwert festgelegt ist. Die Verhältnismäßigkeit, im Vergleich zu natürlichen Werten, hat eine entscheidende Bedeutung und muß als Gegebenheit der belebten Natur berücksichtigt werden. Die Natur zeigt ein nichtlineares Verhalten von Dosis und Effekt und verlangt damit zu Konzentrationen oder Immissionen nichtproportionale Maßnahmen – ein kritischer Punkt für die Beurteilung der Verhältnismäßigkeit.

Grenzwerte können wohl für chronische, nicht aber für akute Ereignisse mit großen Gefahrenpotentialen festgelegt werden. Dies würde nämlich voraussetzen, daß man alle möglichen Szenarien genau kennt. Da bei Katastrophen die Möglichkeit der Regelung per Definition mindestens zu einem wesentlichen Teil versagt, kann die Einhaltung eines Grenzwertes nicht gewährleistet werden. Werden trotzdem Grenzwerte

festgelegt, dann zwingt das dazu, das Gefahrenpotential zu verringern oder entscheidend zu verändern.

5.6. Sicherheitsfaktor und Sicherheitsabstand

Die Begriffe Sicherheitsfaktor und Sicherheitsabstand, wie sie für die Auslegung üblich sind, lassen sich allgemein wie folgt definieren:

Der *Sicherheitsabstand* (A), auch Sicherheitszone, ist definiert (BASLER, 1961b) als Differenz von Auslegungsmaß (Festigkeitsmaß, Q) und Lastmaß (P) und beträgt:
$Z = Q - P$

Der *Sicherheitsfaktor* (N) ist definiert als Verhältnis von Auslegungs- und Lastmaß, dem Verhältnis einer Grenzfestigkeit zu einer auftretenden Beanspruchung oder dem Verhältnis einer Grenzkonzentration (Grenzwert) zur auftretenden zulässigen Konzentration:
$N = Q/P$

Werden für Q und P die Werte eingesetzt, welche einer bestimmten Wahrscheinlichkeit entsprechen, dann wird N im Bauwesen als Sicherheitsbeiwert, bei Verwendung der Mittelwerte als Sicherheitsfaktor bezeichnet (ENZYCLOPÄDIE, 1981b).
Zwischen dem Sicherheitsabstand und dem Sicherheitsfaktor besteht die Beziehung:
$Z = Q \cdot (N-1)/N$

Die hier gegebenen Definitionen können leicht auf unterschiedlichste Bereiche übertragen werden. Es wird dann allerdings notwendig sein, den Begriff Festigkeitsmaß durch die entsprechende Größe der Auslegung, und das Lastmaß durch die Werte der Lastannahmen (z.B. auch Schwell- oder Grenzwerte) zu ersetzen.

5.7. Wirksamkeit von Maßnahmen

Maßnahmen haben zum Ziel, eine schlechte in eine annehmbare Situation überzuführen. Es ist sicher auch im Sinne der Optimierung bei biologischen Systemen legitim, das Ziel mit einem minimalen Aufwand zu erreichen.

Grobe Abschätzung der Wirksamkeit von Maßnahmen, Optimierung:
Beispiel:
75% menschliche Fehler, entsprechend 75 Fehlerpunkten
25% technische Fehler, entsprechend 25 Fehlerpunkten
Total: $(75^2 + 25^2)^{1/2} = 79{,}6$ Fehlerpunkte
Annahme: Es besteht die Möglichkeit 10 Fehlerpunkte zu reduzieren.

a) Reduktion beim technischen System von 25 auf 15 Fehlerpunkten:
Total: $(75^2 + 15^2)^{1/2} = 76{,}5$ Fehlerpunkte, Reduktion 3,9%

b) Reduktion bei den menschlichen Fehlern von 75 auf 65 Fehlerpunkten:
Total: $(65^2 + 25^2)^{1/2} = 69{,}6$ Fehlerpunkte, Reduktion 12,6%

Folgerung: Bei diesem System ist eine Investition bei den menschlichen Fehlern, bei gleichen Kosten pro Fehlerpunkt, rund dreimal effektiver als beim technischen System.

5.8. Verbesserungen bei komplexen Systemen

Große, komplexe Systeme enthalten immer Fehler. Die Erfahrungen mit Computerprogrammen bestätigen dies (MELLOR, 1989, HOARE, 1986). Man rechnet mit 30 bis 100 Fehlern auf 1000 Zeilen Code, die sich durch Fehlersuche und Testen auf unter 10 verringern können (WRAY, 1988). Das Auffinden und Beseitigen der Fehler, die Verbesserung des Systems, folgt einer asymptotisch abnehmenden Funktion (→ Frühausfälle bei der Badewannenkurve), das heißt, die letzten Fehler sind nur schwierig und mit größtem Aufwand zu entdecken.

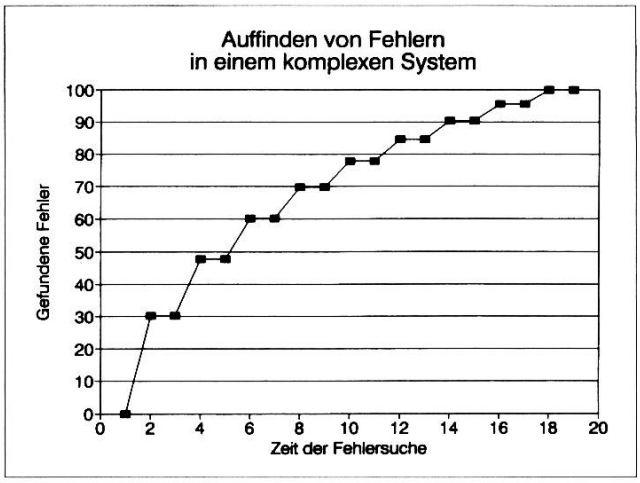


Fig. 7
Fehlerentdeckung und -beseitigung in komplexen Systemen

Wir haben uns aus Erfahrung damit abzufinden, daß bei hochkomplexen Systemen, wie dies große Computerprogramme sind, immer noch Fehler vorhanden sind.

5.9. Sicherheitsparadoxon und Risikokompensation

Eine große Gefahr bei allen Sicherheitsmaßnahmen besteht darin, daß sie wohl am betrachteten Ort den gewünschten Effekt erzielen, an anderer Stelle aber zu Risiken führen können (→ Sicherheitsparadoxon; Beispiel: Sicherheitsventile bei toxischen oder brennbaren Stoffen). Die Erhöhung der Sicherheit kann aber auch bewußt oder unbewußt durch zunehmende Risikobereitschaft kompensiert werden (→ Risikokompensation [STEWART, 1990]; Beispiel: Verwendung von Antiblockiersystemen bei Autos, Verwendung der Sicherheitslampen in Bergwerken).

Sicherheit kann Risiken schaffen:
Der nicht sofort erkennbaren Risikoverlagerung, dem *Sicherheitsparadoxon,* oder der erhöhten Risikobereitschaft als Folge einer Risikominderung, der *Risikokompensation,* ist große Beachtung zu schenken; sie ist ein wichtiger Teil des Risiko-Managements.

5.10. Verfügbarkeit

Sicherheit, Zuverlässigkeit, Verfügbarkeit und Qualität (SAQ, 1989) werden bei technischen Systemen wegen der simultanen Wirkungen zu Recht sehr oft synonym verwendet. Dies ist nur so lange richtig, als sie auf präventiven Maßnahmen aufbauen. Die Verfügbarkeit oder die Zuverlässigkeit sind mit der Ausfallrate, und damit mit der Sicherheit, formal verknüpft:

Verfügbarkeit: A = MTBF/(MTBF + MTTR)

A: Verfügbarkeit (availability), dimensionslos

MTBF: mean time between failure, durchschnittliche Zeitdauer des störungsfreien Betriebs, Erwartungswert (Mittelwert) für die ‹Klarzeit› bis zur nächsten Reparatur.
Ausfallrate = 1/MTBF

MTTR: mean time to repair, durchschnittliche Ausfallzeiten oder Reparaturdauer, Erwartungswert für die Dauer einer verfügbarkeitswirksamen Reparatur.
Reparaturrate = 1/MTTR

Sicherheitsmaßnahmen haben die Eigenschaft, zur Produktivität nur Kosten beizutragen, als Zinsen von Investition und Betriebskosten. Der Unterhalt von Sicherheitseinrichtungen und das Training für Störungen, sind auf Situationen ausgerichtet, die nur allzugerne verdrängt werden.

Meist führt das Ansprechen der Sicherheitseinrichtung zu einem Unterbruch im Betrieb. Verfügbarkeit des Betriebs und Sicherheit gegen außen sind in diesem Fall nicht kongruent. Man ist deshalb dazu übergegangen, die Sicherheitseinrichtungen oder Überwachungsanlagen doppelt auszulegen und Maßnahmen erst einzuleiten, wenn beide Einrichtungen ansprechen. Dies nennt man eine 2-von-2-Auswahlschaltung (VDI/VDE, 1967). Die unnötigen Unterbrüche nehmen durch diese Maßnahme um einen Faktor von ca. 700 ab. Die Sicherheit ist dadurch aber auch um einen Faktor 70 kleiner. Ein Kompromiß wäre eine Schaltung, bei welcher 2 von 3 gleichzeitig vorhandenen Sensoren ansprechen müßten, man spricht dann von einer 2-von-3-Schaltung. Gegenüber einem Sensor ist diese Situation für die Sicherheit etwa halb so effizient, für falsche, durch die Sicherheitseinrichtung unnötig ausgelöste Unterbrüche aber 250mal besser.

Eine wichtige Aufgabe von Führung, Organisation und Ausbildung sollte darin bestehen, die Sicherheitsmaßnahmen in einem permanenten Prozeß wirksam zu halten, besser noch Sicherheitsmaßnahmen in Maßnahmen zur Erhöhung der Verfügbarkeit überzuführen.

Zielsetzung für sichere Systeme:

Bei einem sicheren System wird die Verfügbarkeit für den Betrieb und die Sicherheit nach außen mit denselben Maßnahmen erreicht.

Das (n-1)-Kriterium als Beispiel für Maßnahmen (HASS et al., 1981):

Das (n-1)-Kriterium ist erfüllt, wenn für eine beliebige, technisch mögliche oder betrieblich sinnvolle Ausgangssituation der Betrieb den Ausfall eines Betriebsmittels ohne unzulässige Einschränkung übersteht (→ Verfügbarkeit). Dieses Prinzip des einfachen Ausfalls (einfache → Redundanz) kann auch in sehr komplexen Systemen angewandt werden, welche keine einfachen quantitativen Aussagen zulassen. Ein typisches Beispiel sind die Verbundnetze der Elektrizitätswerke. Es handelt sich bei diesem (n-1)-Kriterium um eine Zielvorgabe der Sicherheit, welche in einem großen Freiraum eine technische, ökonomische und ökologische Optimierung zuläßt.

5.11. Simulationen komplexer Systeme

Bei komplexen, großen Systemen kommt der Simulation mit realitätsnahen Modellen immer größere Bedeutung bei Planung, Risikoanalyse oder Ausbildung zu. Hier ist das Prinzip von ‹Trial and Error› nicht mehr ohne große Folgen anwendbar (siehe z.B. [BÜTZER, CHAKRABORTY, 1977]), von der Größe der Systeme nicht mehr möglich oder wegen der langen Zeiträume nicht sinnvoll (→ Ökologie). ‹Trial until Error› muß von simulierten Systemen für die Ausbildung abgenommen werden. Man kann bei *Simulationen* dieser Systeme deshalb von einem zeitlich sehr kurzen Regelkreis sprechen, bei welchem die Erfahrung mit dem simulierten System rasch in neue Maßnahmen oder ein angemesseneres Verhalten umgesetzt werden kann. Das Verhalten bei hochentwickelten, validierten, simulierten Systemen kann zur Qualifikation wichtiger Personen herangezogen werden (KEMENEY et al., 1979d). Trotzdem darf nicht übersehen werden, daß die eigentlichen Phänomene bei einer Substitution der wirklichen Vorgänge nie real sein können und immer vereinfacht sind. Auch Zielsetzungen aus verschiedenen Gesichtswinkeln (→ siehe System mit Risiken) gehen in solche Simulationen nur selten ein.

5.12. Ablaufschema

Alle Maßnahmen bauen auf der Risikobeurteilung auf, sie stehen wohl immer am Schluß, sind aber ein wichtiger Teil eines Regelkreises:

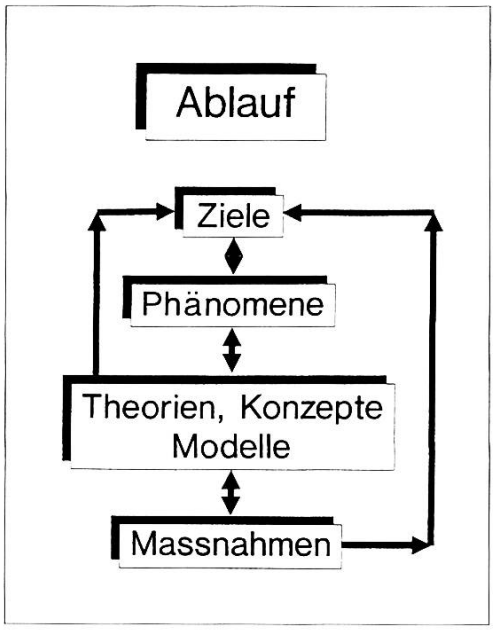


Fig. 8
Ablaufschema für das Risiko-Management

Die Diskussionen über Risiken zentrieren sich meist um die handfesten und damit objektiven Maßnahmen. Die Ursache für die unterschiedlichen, hier anscheinend objektiven Gegensätze sind fast stets darin zu finden, daß schon die Ziele verschieden sind, an denen das Risiko gemessen werden soll (→ Risikodefinition). Da es nicht die Naturwissenschaften und die Kenntnisse der Technik sind, welche bei gleichen Zielen, Phänomenen und Theorien zu unterschiedlichen Interpretationen führen, muß ein Konsens im Dialog zuerst bei den Zielen gefunden werden. Risikoanalyse, Risikobeurteilung und die daraus folgenden Maßnahmen sind nach diesen Randbedingungen auszurichten. Den harten Kern der Dialoge müssen gesicherte Phänomene und wissenschaftlich anerkannte Fakten bilden. Wo dieser Drehpunkt fehlt, sind vernünftige Entscheide nicht möglich.

5.13. Was an Risiken bleibt

Das Risiko nach diesen Maßnahmen setzt sich aus drei bestimmenden Faktoren zusammen.

Das verbleibende Risiko:

1. bewußt in Kauf genommene Risiken (Ethik, Verantwortung, Gesetze/Vorschriften/Regeln),
2. erkannte, aber falsch beurteilte Risiken (auch Unsicherheiten, Streuungen),
3. nicht erkannte Gefahren (→ Gefahrensuche).

Die Punkte 2 und 3 sind verantwortlich für das, was man mit *Restrisiko* bezeichnen könnte. Dieses umfaßt nur Bereiche, welche zum Zeitpunkt der Risikoanalyse mit den verfügbaren wissenschaftlichen Kenntnissen, praktischen Erfahrungen und methodischen Hilfsmitteln nicht erfaßt werden konnten.

5.14. Eine Sicherheits-Kultur?

Die Entscheide des Risiko-Managements müssen durch das Eisbergsyndrom geprägt sein. Vor allem sind daraus die richtigen Folgerungen zu ziehen. Es nützt bei einem Eisberg nämlich wenig, die kleine, sichtbare Spitze zu kappen, der Eisberg taucht selbständig $^1/_7$ bis $^1/_9$ auf und zeigt

danach eine noch breitere Spitze. Sinnvoll und besonders wirksam ist nur der Abbau des Eisbergs an der Basis; eine lange, umfangreiche Arbeit mit wenig spektakulären Resultaten. Damit wird aber gleichzeitig die sehr gefährliche Spitze abgebaut. Alle großen Katastrophen, die Spitze des Eisbergs, hatten die Auslöser in einer Kette von Details (→ Domino-, Kaskadeneffekte, Ereignisketten), die jedes für sich isoliert nicht besonders gravierend waren. Diesen geringfügigen Fehlern, der breiten Basis des Eisbergs, muß die entsprechende Bedeutung zukommen. Bei kleinen Details kann von jedermann täglich gezeigt werden, wie ernst die Sicherheitsaspekte nicht nur bei den anderen, sondern bei sich selbst genommen werden, so ganz unter dem Motto: ‹Gutes Beispiel, halbe Predigt (VOLK, 1991).› So ein Ansatz ist aus Erfahrung sehr erfolgversprechend (GOTTSCHALL, 1983).

Ansatz an der Basis: Sicherheits-Kultur (IAEA, 1988)

Ein sinnvolles Risiko-Management muß darauf ausgehen, in einem permanenten Prozeß auch, und vor allem, die kleinen Schäden zu erkennen, zu vermeiden und wirksam zu begrenzen. Nur so können katastrophale Ereigniskaskaden auf einer frühen Stufe abgebrochen werden. Dies ist eine ständige, praktische und damit glaubwürdige Demonstration, daß die Sicherheitsanliegen ernst genommen werden.

Die Festlegung von *Schutzzielen* muß sich ebenfalls an den Grundsatz halten, daß kleine Schäden vermieden werden müssen. Nur so ist es möglich, von den unsinnigen Diskussionen über die noch tolerierbare Anzahl von Todesfällen hinwegzukommen. Das Schutzziel kann sich mit dieser Optik an den kleinen Fällen messen und erreicht mit den Maßnahmen die Spitze des ‹Eisbergs› mit besonders großer Effizienz.

Technische Risikoanalyse, Risikobewertung und die Schutzziele können höchstens so viel Vertrauen finden, wie sie verstanden werden. Mit zunehmender Komplexität der Technik und wachsender Informationsmenge wird es immer wichtiger, den eigentlichen Inhalt anschaulich, erfaßbar und verständlich zu machen.

6. Einige wichtige Begriffe

(siehe auch [BERTHOLD, LÖFFLER, 1981, KUHLMANN, 1977, BÜTZER, 1987b]):

Akkumulation: Anhäufung, aus lat. *accumulatio.*

Alarm: Gefahrmeldung, Beunruhigung aus spätmhd. *alerm,* frühmhd. *Alarm[a],* aus frz. *à l'arme, alarme,* it. *allarme,* militär. Ruf: ‹*all'arme!*›, zu den Waffen!

Common Mode Failure: Ausfall zufolge gemeinsamer Ursache, gekoppelter Ausfall (auch: Common-Mode-Ausfall).

Beispiele:
- Wackelkontakt in der Zuleitung zu den beiden Rücklichtern
- Falsches Schmieröl für die Düsentriebwerke verwendet
- Fehlanzeige mehrerer Gasmelder durch Fremdgas
- Mehrere Notstromdiesel starten wegen Stillstandschäden nicht

Diversifikation: divers: verschieden; aus lat. *diversus* ‹entgegengesetzt, völlig verschieden›, aus *di-* (in Zus. vor v für *dis-*) ‹auseinander›, und *vertere* ‹sich neigen, sich erstrecken, liegen›.

Beispiele:
- Notstromaggregat (z.B. Diesel)
- Fußbremse: hydraulisch; Handbremse: mechanisch
- Sauerstofftank beim Spital und Flaschenbatterie
- Rücklicht (aktiv) und Rückstrahler (passiv)

Information: lat. *informatio* ‹Auskunft, Benachrichtigung›.

Inhärente Sicherheit: inhärent: (einer Sache) anhaftend, innewohnend; aus lat. *inhaerens,* Gen. *-entis,* Part. Präs. von *inhaerere* ‹an etwas haften, hängen, kleben›, aus *in* ‹in, an, auf› und *haerere* ‹haften, hängen, kleben›.

Beispiele:
- Umfallen nach einem Schock, damit der tiefe Blutdruck reicht, um das Gehirn zu durchbluten
- Schmelzsicherung: Ist der Strom zu hoch, dann wird die Leitung durch diesen Strom selbst unterbrochen
- Klemmkeil: Je größer der Zug, desto stärker die Verankerung

Initiierung: das zugrunde liegt, aus lat. Adj. *initialis* ‹am Anfang stehende, anfänglich›. Hier werden interne, externe, absichtliche, unabsichtliche Initiierungen unterschieden.

Intuition: aus mlat. *intuitió* ‹unmittelbare Anschauung›, lat. *in-tuéri* ‹ansehen, betrachten›, hier ‹Eingebung, ahnendes Erfassen›.

intuitiv: aus mlat. *intuitivis* ‹durch unmittelbare Anschauung (nicht auf Denken) erkennbar, auf Eingebung beruhend›. Sich unter einem Baum, in welchen der Blitz eingeschlagen hat, besonders sicher zu fühlen, mag intuitiv verständlich sein, es ist aber mit wissenschaftlichen Argumenten begründet, besonders gefährlich.

Katastrophe: im antiken Drama: entscheidende Wende, die zur Lösung des Konflikts und zum Untergang des Helden führt; allg.: Unheil, Verhängnis, Zusammenbruch; aus griech. *kata,* ‹gänzlich, völlig›, und *strephein,* ‹drehen, wenden, kehren›.

Kybernetik: Wissenschaft von den dynamischen, selbstregulierenden Systemen (in Natur und Technik), geprägt zu griech. *kybernetikós,* ‹zum Steuern gehörig, geeignet›. Heute auch oft im Zusammenhang mit Biokybernetik verwendet.

Phänomen: lat. *phaenomenon* ‹[Luft]erscheinung, gr. *phanómenon* ‹das Erscheinende, das Einleuchtende, die Himmelserscheinung›, in dieser Arbeit: das Erscheinende, griech. *phaino* ‹zeige›, *phos* ‹Licht›, wahrnehmbare Erscheinung.

Redundanz: Überflüssiges; die bei einer Information über das zum Verständnis Notwendige hinausgehenden Wörter und Zeichen; über engl. *redundance* ‹Überschuß, Übermaß›, aus lat. *redundantia* ‹Überfülle, Überströmen›, zu *redundare* ‹überströmen, im Überfluß vorhanden sein›, eigentlich ‹wieder zurückströmen›, aus *red-* (vor Vokalen für *re-)* ‹zurück› und undare ‹wogen, wallen›, zu *unda* ‹Welle›.

Beispiele:

- Mehrmotoriges Verkehrsflugzeug
- Zweikreisbremssystem beim Auto
- Doppelte Rückleuchten beim Auto
- Doppelnaht bei Turnhosen

Regelung: Auslösen von Vorgängen aufgrund der Abweichungen vom Sollwert, damit ein Zustand oder Vorgang gegen störende Außeneinflüsse konstant gehalten wird.

Risiko: Wagnis, Gefahr, Verantwortung, 16. Jh. *risico:* in Gefahr bringen, Möglichkeit eines Verlustes, Mißerfolges, gefährlich, riskant.

Risiko-Management: Führungsfunktion, welche ein definiertes System steuert, mit der Absicht Störprozesse zu vermeiden, welche das Erreichen der gesetzten Ziele gefährden könnten.

Schutz: Maßnahmen, um Personen, Umwelt und Sachwerte vor Gefahr und Schaden zu bewahren (mittelhochdeutsch: Umdämmug, Aufstauung des Wassers, neuhochdeutsch: Abschirmung, Sicherung),

Sicherheit, Hilfe bei Gefahr, Sicherung: Vorrichtung zum Schutz oder zur Sicherheit.

Serendipity: Persisches Märchen: ‹The Three Princes of Serendip›, interpretiert von Hugh Warpole: ‹These three princes on their travel through Serendip (heute Sri Lanka) were always making discoveries by accidents and sagacity of things they were not in quest of ... you must observe that *no* discovery of a thing you are looking for comes under this description.›

Sicherheit: Objektiv: Nichtvorhandensein einer Gefahr; subjektiv: die Gewißheit eines Einzelnen, einer Gruppe oder einer Gemeinschaft, vor möglichen Gefahren geschützt zu sein.

simulieren: aus lat. *simulare* ‹ähnliches machen, nachbilden, nachahmen, etwas zum Schein vorgeben, sich den Anschein von etwas geben, etwas vortäuschen›, entlehnt von lat. *similis* ‹ähnlich›.

System: Aufbau, Gefüge, gegliedertes Ganzes; aus griech. *systema* ‹Zusammenstellung, Gebilde, Gesamtheit›. DIN 19226: Abgegrenzte Anordnung von aufeinanderfolgenden Gebilden. Diese Anordnung wird durch eine Hüllfläche von ihrer Umgebung abgegrenzt oder abgegrenzt gedacht. Durch diese Hüllfläche werden Verbindungen des Systems mit seiner Umgebung geschnitten.

Toleranz: aus lat. *tolerantia* ‹ertragen, erdulden, Geduld›.

tolerieren: dulden, gewähren lassen aus lat. *tolerare* ‹tragen, ertragen, erdulden›.

Wahrscheinlichkeit: Ein Maß für den Grad der Möglichkeit noch unverwirklichter Ereignisse. Die objektive Bestimmung kann aus dem apriorischen (logischen) und dem aposteriorischen (statistischen) Wahrscheinlichkeitsbegriff zusammengefaßt werden. Der subjektive Wahrscheinlichkeitsbegriff spielt vor allem in der Entscheidungstheorie eine Rolle. Eine Person bestimmt aus Erfahrung, Intuition oder der subjektiven Bereitschaft auf ein Ereignis zu reagieren, die Wahrscheinlichkeit des betreffenden Ereignisses.

Ziel: gotisch: zum Ziel strebend als Name des Speers, das Eingeteilte, das Abgemessene, räumlicher oder zeitlicher Endpunkt, Punkt, den man erreichen will, das, wonach man strebt, worauf eine Handlung oder Absicht gerichtet ist.

Zuverlässigkeit: (techn.) Eigenschaft eines technischen Systems, die sich durch die Wahrscheinlichkeit ausdrückt, während einer vorgegebenen Zeitspanne eine geforderte Funktion unter gegebenen Bedingungen zu erfüllen.

7. Literaturverzeichnis

BASLER E. (1961a): Untersuchungen über den Sicherheitsbegriff von Bauwerken, Schweizer Archiv, April, S. 136

BASLER E. (1961b): Untersuchungen über den Sicherheitsbegriff von Bauwerken, Schweizer Archiv, S. 133

BAUMGARTNER G., GLAUSER E., HEIMGARTNER E., SCHNEIDER TH. (1977): Kernkraftwerke als Sicherheitsproblem, Schweiz. Bauzeitung, Heft 44, S. 784f.

BECKMANN (1976): The Health Hazards of not Going Nuclear, The Golem Press, Boulder, Colorado

BERNOULLI D. (1738): ‹Specimen Theoriae Novae de Mensura Sortis›, 1738, nach der Referenz von Miller D. W., Starr M. K. (1967): The Structure of Human Decision, Englewood Cliffs N.J., Prentice-Hall

BERTHOLD W., LÖFFLER U. (1981): Lexikon sicherheitstechnischer Begriffe in der Chemie, Verlag Chemie, Weinheim

BIEDERMANN R. (1987): Talsperren; Planung für Notfälle, Wasser, Energie, Luft, Heft 5/6, S. 71

BINSWANGER CH. (1986): Vermeidung von Restrisiken als Weg zu einer umweltgerechten Wirtschaft, NZZ, Mittwoch, 31. Dezember, Nr. 303, S. 49

BIRKHOFER A., KÖBERLEIN K. (1987a): Sicherheitsrelevante technologische Trends und ihr Einfluß auf den Bedarf an Risikoabsicherung, in: Gesellschaft und Unsicherheit, Verlag Versicherungswirtschaft e.V., Karlsruhe, S. 164

BIRKHOFER A., KÖBERLEIN K. (1987b): Sicherheitsrelevante technologische Trends und ihr Einfluß auf den Bedarf an Risikoabsicherung, in: Gesellschaft und Unsicherheit, Verlag Versicherungswirtschaft e.V., Karlsruhe, S. 167

BLOKKER E. F. (1983a): Erfahrung bei der Durchführung von Risikoanalysen für einige Anlagen der petrochemischen Industrie in Rijnmond, in: Hartwig S., Große technische Gefahrenpotentiale, Springer-Verlag, Berlin/Heidelberg/New York, S. 161

BLOKKER E. F. (1983b): Erfahrung bei der Durchführung von Risikoanalysen für einige Anlagen der petrochemischen Industrie in Rijnmond, in: Hartwig S., Große technische Gefahrenpotentiale, Springer-Verlag, Berlin/Heidelberg/New York, S. 161ff.

BOHNENBLUST H. (1985): Die Anwendung eines risikoorientierten Sicherheits-Modells zur Beurteilung der Neubaustreckentunnel der

Deutschen Bundesbahn, in: Yadigaroglu G., Chakraborty S., Risikountersuchungen als Entscheidungsinstrument, Verlag TÜV Rheinland, Köln, S. 341

BURKARDT F. et al. (1990): Human Factors, Human Factors Study Group, Loss Prevention Working Party, European Federation of Chemical Engineers, February

BÜTZER P. (1975): Einige informationstheoretische Aspekte der chemischen Analytik, EIR-Bericht 287, Würenlingen, August

BÜTZER P. (1983): Sicherheit und Risiko, Wissenschaftliche Beilage, Kantonsschule Heerbrugg

BÜTZER P. (1985a): Ursachen und Wirkungen von chemischen Störfällen, Chemie für Labor und Betrieb, 9, S. 433

BÜTZER P. (1985b): Umgang mit toxischen Stoffen – Erfahrung und Gefahrenpotential, Ein störfallorientierter Index für Stoffe im gasförmigen Zustand, Swiss Chem, 7, S. 25

BÜTZER P. (1986): Risikoanalyse: Die zeitliche Verteilung chemischer Störfälle, chimia, 40, S. 372

BÜTZER P. (1987a): Die Begriffe Sicherheit und Risiko als Grundlage für Schutzziele, Bundesamt für Umweltschutz, Bern

BÜTZER P. (1987b): Risikoanalyse mit einem Matrixverfahren, Swiss Chem, Heft 4, S. 37f.

BÜTZER P. (1987c): Die Begriffe Sicherheit und Risiko als Grundlage für Schutzziele und Schutzmaßnahmen, Bundesamt für Umwelt, Wald und Landschaft, Bern, S. 14

BÜTZER P. (1988): Gefährdungsanalyse von Flüssiggas (Propan, Butan) und Erdgas, Grundlagen, Staatskanzlei des Kt. St.Gallen, Oktober 1988

BÜTZER P. (1989a): Sicherheitstechnik und Störfallverordnung: Konzentrierte oder verteilte Risiken?, chimia, 43, 180

BÜTZER P. (1989b): Schutzziele und notwendige Maßnahmen im Zusammenhang mit der Störfallverordnung (StFV), Swiss Chem, Heft 11, 37

BÜTZER P. (1990a): Risikoanalyse und Informationsgehalt, Naturw. Rdsch., 43, S. 8

BÜTZER P. (1990b): Vernetzte Zusammenhänge bei Bodeneigenschaften, Verein Pro Riet Rheintal, Dezember

BÜTZER P. (1991a): Alarmplanung in einer Gemeinde, Die Schweizer Gemeinde, Heft 2, 1991, S. 34

Bützer P. (1991b): Streifenförmige Ablagerung des Reaktionsprodukts bei einer Gasphasenreaktion, chimia, 45, S. 269
Bützer P., Chakraborty S. (1977): A Geosphere Transport Model for Risk Evaluation, in: Risk Analysis and Geologic Modelling in Relation to the Disposal of Radioactive Wastes into Geological Formation, Proceedings, OECD Nuclear Energy Agency, Ispra (Italy), May, S. 130
CEFIC (1988) (Conseil Européen des Federations de l'Industrie Chimique): Statistics on the Major Accidents in the OECD Countries (20.6.88), Paris
Conrad J. (1979): Was kann und soll die Risikoforschung?, Umschau, Heft 19, S. 593
Cramer F. (1990): Korrekturlesen und dann Gut zum Druck, Chem. Rdsch., 44
Daenzer W.F. (1976a): Systems Engineering, Verlag Industrielle Organisation, Zürich, S. 193
Daenzer W.F. (1976b): Systems Engineering, Verlag Industrielle Organisation, Zürich, S. 173
de Morsier A. (1988): Früherkennung von Umweltrisiken bei Umweltchemikalien, in: Risiko und Risikomanagement, Helbing & Lichtenhahn, Basel und Frankfurt a. M., S. 47
DIN 25 419 (Deutsche Normen), (1977): Störfallablaufanalyse, Deutsches Institut für Normung e.V., Köln
DIN 25 448 (Deutsche Normen), (1980): Ausfalleffektanalyse, Deutsches Institut für Normung e.V., Köln
DIN 25 424 (Deutsche Normen), (1981): Fehlerbaumanalyse, Deutsches Institut für Normung e.V., Köln
Dorias H. (1984): Gefährliche Güter, Springer-Verlag, Berlin/Heidelberg/New York/Tokyo
Droste B., Mallon M. (1990): Eine gezielte Auswertung von Unfällen beim Umgang mit Flüssiggas (LPG), Schadenprisma, 3, S. 41
Egger H.J. (1988): Der verzweifelte Kampf gegen die Uhr, NZZ, Montag, 7. März, Nr. 55, S. 49
Enzyclopädie (1981a): Naturwissenschaft und Technik, Sicherheit (Bautechnik), Verlag Moderne Industrie, Landsberg a. Lech, Band 4, S. 3958
Enzyclopädie (1981b): Naturwissenschaft und Technik, Sicherheit (Bautechnik), Verlag Moderne Industrie, Landsberg a. Lech, S. 3956

ESCIS (1978): (Expertenkommission für Sicherheit in der chemischen Industrie der Schweiz), Statische Elektrizität, Heft 2, Chemische Rundschau
ESCIS (1981a): (Expertenkommission für Sicherheit in der chemischen Industrie der Schweiz), Einführung in die Risikoanalyse, Heft 4, Chemische Rundschau
ESCIS (1981b): (Expertenkommission für Sicherheit in der chemischen Industrie der Schweiz), Einführung in die Risikoanalyse, Heft 4, Chemische Rundschau, S. 5
ESCIS (1988): (Expertenkommission für Sicherheit in der chemischen Industrie der Schweiz), Thermische Prozeß-Sicherheit, Heft 8, Chemische Rundschau
Fauske H. K. (1989): Preventing Explosions During Chemicals and Materials Storage, Plant/Operations Progress, 8, S. 181
Frei R. (1979): MORT, ein Sicherheitskonzept, SUVA, Luzern
Fritzsche A. F. (1986): Wie sicher leben wir?, TÜV Rheinland, S. 87f.
Gottschall D. (1983): Das gute Beispiel kommt von oben, Manager Magazin, Heft 6, Juni
Haller M. (1975): Sicherheit durch Versicherung?, St.Gallen
Haller M. (1986): Risiko-Management – Eckpunkte eines integrierten Konzepts, in: SzU, Band 33, Wiesbaden, S. 18f.
Haller M. (1990a): Der ‹Risikodialog› als Chance, NZZ, Mittwoch, 31. Januar, Nr. 25, S. 65
Haller M. (1990b): Risiko-Management und Risiko-Dialog, in Schütz M., Risiko und Wagnis, Die Herausforderung der industriellen Welt, Erster Band, Pfullingen, S. 229–256
Hartwig S. (1983): Große technische Gefahrenpotentiale, Springer-Verlag, Berlin/Heidelbarg/New York
Hass D., Leusden P., Schwarz J., Zimmermann H. (1981): Das (n-1)-Kriterium in der Planung von Übertragungsnetzen, Elektrizitätswirtschaft, Heft 25, S. 923
Heilmann K. (1986): Sicherheits-Skala, edition agrippa Köln, 1986
Heilmann K., Urquart J. (1983): Keine Angst vor der Angst, Kindler, München
Hoare T. (1986): Maths adds safety to computer programs, New Scientist, 18. September, S. 53
Hofstadter D. R. (1982): Metamagikum, Spektrum der Wissenschaft, Juli 1982, S. 8

IAEA (1988): Basic Safety Principles for Nuclear Power Plants, safety series No. 75-INSAG-3, IAEA, Wien
IVSS (1980): (Internationale Vereinigung für Soziale Sicherheit), Der Störfall im chemischen Berieb, Berufsgenossenschaft der chemischen Industrie, Heidelberg
JÄGGI M. (1988): Sicherheitsüberlegungen im Flußbau, NZZ, Mittwoch, 20. Juli, Fernausgabe Nr. 166, S. 21
JANSEN M. (1990): Die Anwendung systemanalytischer Methoden zur Beurteilung der Sicherheit von Flüssiggasanlagen, Schadenprisma, 3, S. 50
KAHNEMANN D., TVERSKY A. (1982): Risiko nach Maß – Psychologie der Entscheidungspräferenzen, Spektrum der Wissenschaft, März, S. 89
KEMENEY J. G. et al. (1979a): Der Störfall von Harrisburg, Erb-Verlag, Düsseldorf, S. 87
KEMENEY J. G. et al. (1979b): Der Störfall von Harrisburg, Erb-Verlag, Düsseldorf, S. 89
KEMENEY J. G. et al. (1979c): Der Störfall von Harrisburg, Erb-Verlag, Düsseldorf, S. 96
KEMENEY J. G. et al. (1979d): Der Störfall von Harrisburg, Erb-Verlag, Düsseldorf, S. 95
KIER B., MÜLLER G. (1986): Technisch-wissenschaftliche Grundlagen für Richtlinien zur Gefahrenabwehrplanung in der Umgebung von Anlagen der chemischen Industrie, Umweltbundesamt (BRD), Texte 28/86
KLETZ T. A. (1983): Hazan & Hazop, The Institution of Chemical Engineers, Rugby
KLETZ T. A. (1985a): An Engineer's View of Human Error, The Institution of Chemical Engineers, Rugby
KLETZ T. A. (1985b): Cheaper, Safer Plants or Wealth and Safety at Work, The Institution of Chemical Engineers, Rugby, S. 119–120
KLETZ T. A. (1990): Improving Chemical Engineering Practices: A New Look at Old Myths of the Chemical Industry, Hemisphere Publishing Corporation, New York/Washington/Philadelphia/London
KNOX E. G. (1975): Negligible risks to health, Community Health, Bristol, Band 6, S. 244
KÖCHEL P. (1983): Zuverlässigkeit technischer Systeme, Harri Deutsch, Thun und Frankfurt/Main

KUHLMANN A. (1977): Alptraum Technik?, Verlag Hoppenstedt/Verlag TÜV Rheinland, Köln
KUHLMANN A. (1981): Einführung in die Sicherheitswissenschaft, Friedr. Vieweg & Sohn, TÜV Rheinland, Köln, S. 51f
LAGADEC P. (1987): Das große Risiko, Franz Greno Verlag, Nördlingen
LAPP K., ROUSSAKIS (1989): Safeguards cut tank explosion risk during gas flaring, Oil & Gas Journal, August 14, S. 41
LATINEN H. (1987): Actual and Potential Severity of Chemical Accidents in Finnland 1978–1985, Proc. World Conf. Chemical Accidents, July, CEP Consultants, Edinburgh 1987, S. 292
LEES F. P. (1981a): Loss Prevention in the Process Industries, Butterworths, London/Boston, S. 188
LEES F. P. (1981b): Loss Prevention in the Process Industries, Butterworths, London/Boston, S. 193
LEES F. P. (1981c): Loss Prevention in the Process Industries, Butterworths, London/Boston, S. 8
MARSHALL V. C. (1987): Major Chemical Hazards, Ellis Horwood Ltd., Chichester
MELLOR P. (1989): Can you count on computers?, New Scientist, 11. Februar, S. 52
MILLER G. A. (1956): The Magical Number Seven Plus or Minus Two: The Limits on our Capacity for Proceeding Information, Psychological Review, S. 63f.
MOSER F. (1985): Zwischen ‹superindustrialisierter› und ‹nachökonomischer› Gesellschaft – Gedanken zum Problemkreis: Technik, Ökonomie, Ökologie, chimia, 39, S. 104
NÜTTEN-HART I., OSTEROTH D. (1987): Die Zukunft fest im Griff? Was ist und wie funktioniert die Szenario-Technik?, Chemie für Labor und Betrieb, Heft 6, S. 288
PALMER K. N., MARSHALL V. C. (1991): Large Property Damage Losses, Loss Prevention Bulletin 099, June, S. 27
PERROW CH. (1984): Das Management von Systemen und Technologien mit hohem Risikopotential, gdi impuls, 2, S. 55
PERROW CH. (1984): Normale Katastrophen, Campus Verlag GmbH, S. 125
PETERS T. J., WATERMAN R. H., Auf der Suche nach Spitzenleistungen, Moderne Verlagsgesellschaft mbH, München, S. 165f.
PHILIPSON L. L. (1982): Risk Assessment Methodologies, Foresight, Mai, S. 4

PITT M.J.A. (1982): A vapour hazard index for volatile chemicals, Chemistry and Industry, S. 804
PRINZ B., ARNDT U., JUHNKE I., KLOCKOW D., KNABE W., MAYER R., SCHOLZ F., SCHWELA D., SCHWIRTEN D., WIECHMANN H., WINKLER K. (1983): Säurehaltige Niederschläge – Entstehung und Wirkungen auf terrestrischen Ökosystemen, VDI, Düsseldorf, S. 12, 21
PURKIS T., WILSON J. (1989): Cleaning up the cooling towers, New Scientist, 16. September, S. 52
RENN O. (1986): Akzeptanzforschung: Technik in der gesellschaftlichen Auseinandersetzung, Chemie in unserer Zeit, 20, S. 46
ROTH L., WELLER U. (1990): Chemie-Brände, ecomed Verlag, Landsberg/Lech
ROUSSLEIN X., FALCY M. (1986): Le nez les produits chimiques et la sécurité, INRS, Cahiers de notes documentaires Nr. 124, 3e trimestre, S. 331
ROWBOTTOM R. S. (1989): Bacteria cause fatal explosion at corrugating medium mill, Pulp & Paper Canada 90:4, S. 75
SAQ (1989): (Schweizerische Arbeitsgemeinschaft für Qualitätsförderung), SAQ-Leitfaden zur SN-ISO Normenreihe 9000, SAQ Bern
SCHNEIDER J. (1985): Hazard Scenarios and Structural Design, IABSE Periodica, 4, S. 65
SCHNEIDER J. (1988): Zwischen Sicherheit und Risiko, Schweiz. Ing. und Arch., Heft 18, S. 505
SCHNEIDER TH. (1985a): Ein quantitatives Entscheidungsmodell für Sicherheitsprobleme im nicht-nuklearen Bereich, in Yadigaroglu G., Chakraborty S. (Hrsg.), Risikountersuchungen als Entscheidungsinstrument, TÜV Rheinland, Köln, S. 113–143
SCHNEIDER TH. (1985b): Ein quantitatives Entscheidungsmodell für Sicherheitsprobleme im nicht-nuklearen Bereich, in Yadigaroglu G., Chakraborty S. (Hrsg.), Risikountersuchungen als Entscheidungsinstrument, TÜV Rheinland, Köln, S. 125
SEIFRITZ W. (1991): Kernenergie und Treibhausproblematik, Die Suche nach neuen Lösungswegen, Techn. Rdsch., Heft 21, S. 60
STEINER C. (1981): Die tödlichen Bergunfälle in der Schweiz im Jahre 1980, Die Alpen (Monatsbulletin des Schweizer Alpen-Clubs), S. 117
STEPHAN U., ELSTNER P., MÜLLER K.R. et al. (1985): Fachlexikon ABC Toxikologie, Verlag Harri Deutsch, Thun, Frankfurt/M, S. 173
STEWART I. (1990): Risky Business, New Scientist, Inside Science, Nr. 33, S. 4

SUVA (1978): (Schweiz. Unfallversicherungs-Anstalt), Ergebnisse der Unfallstatistik der zwölfjährigen Beobachtungsperiode 1973–1977
UK Health and Safety Executive (1979): Safety Assessment Principles for Nuclear Power Reactors, HM Nuclear Installations Inspectorate, April
VDI/VDE (1967): (Verein Deutscher Ingenieure, Verband Deutscher Elektrotechniker), VDI/VDE-Richtlinie 2180, Sicherung von Anlagen der Verfahrenstechnik, Möglichkeiten der Signalverarbeitung, Verein Deutscher Ingenieure, Verband Deutscher Elektrotechniker, Blatt 2, Oktober
Vester F. (1986): Ballungsgebiete in der Krise, Deutscher Taschenbuch-Verlag, 2. Auflage, S. 130
Volk H. (1991): Gutes Beispiel, halbe Predigt, Techn. Rdsch., Heft 21, S. 68
von Weizäcker C., von Weizäcker E. U. (1984): Fehlerfreundlichkeit, in: Kornwachs K., Offenheit – Zeitlichkeit – Komplexität. Zur Theorie der offenen Systeme, Frankfurt am Main/New York
Whalley S. P., Kirwan B. (1989): An Evaluation of Five Human Error Identification Techniques, 6th Int. Symp. ‹Loss Prevention and Safety Promotion in the Process Industries›, June 19–22, Oslo, S. 31-1
Williams. J. C. (1985): Validation of Human Reliability Assessment Techniques, Reliability Engineering, 11, S. 149
Wray T. (1988): The everyday risks of playing safe, New Scientist, 8. September, S. 61
Zwicky F. (1966): Entdecken, Erfinden, Forschen im morphologischen Weltbild, Droemersche Verlagsanstalt, Th. Knaur Nachf., München/Zürich
Zwicky F. (1972): Jeder ein Genie, Herbert Lang & Cie AG, Bern, S. 116
Zwicky F. (1989): Morphologische Forschung, Verlag Baeschlin, Glarus, 2. Auflage