Projektbeschrieb

Risikobewertung im Fall von Hochrisikosystemen

Systemanalytische Betrachtungen zur Risikoanalyse und Risikowahrnehmung

Übersicht:

Florian Erzinger
Dipl. Natw. ETH
Umweltchemiker

Risikobewertung im Fall von Hochrisikosystemen

Systemanalytische Betrachtungen zur Risikoanalyse und Risikowahrnehmung

Zusammenfassung

Komplexe Interaktionen beschreibt Charles Perrow als Prozesse, die zwischen einer Komponente des so genannten DEPOSE-Systems (design, equipment, procedures, operators, supplies and materials, environment; Konstruktion, Ausrüstung, Abläufe, Operateure, Material und Zubehör, Umwelt) und mindestens einer Komponente ausserhalb des normalen Betriebsablaufs auftreten, unabhängig davon, ob sie in der Konstruktion vorgesehen sind oder nicht. Komplexe Interaktionen können entweder geplant sein, aber den Operateuren nicht vertraut, oder aber ungeplant und unerwartet. In allen Fällen sind sie für das Bedienungspersonal entweder nicht sichtbar oder nicht unmittelbar durchschaubar.

Die andere für *Hochrisikosysteme*[1] zentrale, unabhängige Systemeigenschaft stellt gemäss Perrow der Grad der Kopplung dar. Enge Kopplung bedeutet, dass es zwischen zwei miteinander verbundenen Teilen kein Spiel, keine Pufferzonen oder Elastizität gibt. Sämtliche Vorgänge des einen Teils wirken sich unmittelbar auf die Vorgänge des anderen Teils aus. Eng gekoppelte Systeme verfügen bezüglich Zeitgebundenheit, Reversibilität der Prozesse als auch bezüglich Materialverbrauch kaum über Spielraum.

Aufgrund der systeminhärenten Charakteristika hohe Komplexität / starke Kopplung treten in derartigen Systemen durch interagierende Komponentenstörungen verursachte Unfälle wesentlich häufiger auf als in linearen und schwach gekoppelten Systemen. Die Systeme sind dem gemäss anfällig auf so genannte Systemunfälle. Führen diese gegebenenfalls zu katastrophalen Schäden an Menschen und / oder Umwelt, dann muss man – immer der Logik von Perrow folgend – von systeminhärenter Katastrophenanfälligkeit sprechen. In einer Metapher vergleicht Perrow diese systembedingte Katastrophenanfälligkeit mit dem Tod eines biologischen Systems, der ja ebenso nur sehr selten eintritt (nämlich gerade einmal pro Leben), von dem aber jedeR ohne Zögern sagt, dass es normal ist, dass er irgendwann eintritt. Aus dieser Überlegung auch der von Perrow gewählte Titel "Normale Katastrophen".

Die klassische Risikoanalyse stützt sich gemäss der Definition $R = W \cdot S$ nebst dem Schadenpotential auf die Eintretenswahrscheinlichkeit von solch katastrophalen Unfallereignissen ab. Dabei wird aber bei der Berechnung der Eintretenswahrscheinlichkeit die systembedingte Charakteristik des untersuchten Unfallereignisses vernachlässigt. Komponentenstörfälle werden unabhängig von einander zu einer Gesamtwahrscheinlichkeit aufsummiert. Die kumulative Eintretenswahrscheinlichkeit setzt sich damit aus statistisch unabhängigen, nicht interagierenden Einzelwahrscheinlichkeiten zusammen.

Dieser Fakt erhält dadurch zusätzliche Brisanz, dass im öffentlichen Risikodiskurs von "ExpertInnen"-Seite gerne ein sehr starker Fokus auf die enorm geringen errechneten Eintretenswahrscheinlichkeiten gelegt wird. Die so genannten "ExpertInnen" argumentieren dabei: "$W \approx 0$, also ist $R \approx 0$", bzw. noch einfacher: "$W \approx 0$, also kann W Null gesetzt werde und damit ist $R = 0$". Dass dieser Ansatz wissenschaftlich nicht haltbar ist, sollte eigentlich auch ohne Perrows systemanalytischen Überlegungen offensichtlich sein.

Dass Perrows Forderung der Erarbeitung eines systemorientierten, mathematisch-analytischen Ansatzes der Berechnung der verschiedenen Eintretenswahrscheinlichkeiten von Systemunfällen und damit einer neuartigen Risikobewertung sehr wohl berechtigt ist, kann exemplarisch am Beispiel

[1] Im nachfolgenden Text werden Fachbegriffe und Definitionen, die nicht zur Allgemeinbildung gehören oder die von den jeweiligen AutorInnen anders interpretiert werden, als dies allgemein der Fall ist, beim erstmaligen Erwähnen kursiv hervorgehoben und im Annex unter Kapitel "Begriffserläuterungen" erläutert.

der Kerntechnologie nachgewiesen werden. Prüft man die Nullhypothese "die beobachtete, relative Häufigkeit von drei grossen Unfällen, bei welchen beträchtliche Mengen radioaktives Material in die Umwelt freigesetzt wurden[2], auf ca. 9'000 Reaktorjahren Betriebserfahrung seit Beginn der Atomtechnologie entspricht der berechneten Wahrscheinlichkeit von ca. 1:1'000'000a", wie sie von "RisikoexpertInnen" angegeben wird, muss diese bei einem Signifikanzniveau α von 5% verworfen werden. Man muss also davon ausgehen, dass die Angabe $p_0 = 10^{-6}a^{-1}$ falsch ist und dass die reale Eintretenswahrscheinlichkeit solcher Unfälle wesentlich grösser ist. Dieser Fehler kann eigentlich nur mit der Charakteristik des hochkomplexen und stark gekoppelten Systems 'Kernkraftwerk' erklärt werden, in dem Störfälle eben nicht in unabhängigen Ereignissträngen untersucht werden können.

Basierend auf diesem Hintergrund strebe ich ein Dissertationsprojekt an, das sich mit folgenden Fragestellungen auseinandersetzt:

- Wie müsste eine Methodik zur Quantifizierung von Eintretenswahrscheinlichkeiten von Katastrophenereignissen aussehen, welche sich entlang der Biokybernetik am System und dessen grundlegenden Eigenschaften wie Komplexität und Kopplung orientiert?
- Wie lässt sich diese neu zu entwickelnde Methode – aus Gründen der Minimierung systemischer Modellierungsfehler - auf zwei möglichst unterschiedliche Hochrisikosysteme anwenden und mit Hilfe von Konfidenzintervallen ihre Validität evaluieren?
- Wie müsste ein qualitativ-quantitativer Ansatz für eine technisch-naturwissenschaftliche Risikobewertung aussehen, welche sich entlang dem integrierten Risikomanagement auf der Perrowschen Risikobewertung gemäss dem Nettokatastrophenpotenzial und den Substitutionskosten eines Hochrisikosystem basiert?
- Wie stehen die auf diese Weise erarbeiteten Resultate von Eintretenswahrscheinlichkeit und Risiko zu Werten herkömmlicher Risikoanalysen und auch zu Erkenntnissen aus der Sozialpsychologie zur kollektiven Wahrnehmung von Risiko?
- Was macht schliesslich eine risikoarme Technologie aus, und wie wird dies gesellschaftlich wahrgenommen?

Das Ziel der anvisierten Arbeit ist dem zufolge die Entwicklung eines systemorientierten methodischen Ansatzes, der eine für komplexe und stark gekoppelte Risikosysteme adäquate Risikoanalyse ermöglicht.

[2] Three Miles Island, USA: Kernschmelzeunfall, 1979; Tschernobyl, Ukraine: Kernschmelzekatastrophe, 1986; Tokai Mura, Japan: Kritikalitätsunfall, 1999.

Einleitung

Hochrisikosysteme technisch und gesellschaftlich

Mit der hoch entwickelten Industriegesellschaft ist ein Zerstörungspotenzial entstanden, das zu *Katastrophen* von zuvor ungeahnten Ausmassen führen kann. *Unfälle* mit katastrophalen Folgen sind nicht beabsichtigt, die Möglichkeit wird jedoch mehr oder weniger bewusst in Kauf genommen – von der Industrie, aber auch von der Gesellschaft. Dies gilt insbesondere für den Umgang mit so genannten Hochrisikosystemen, welche Gefahren singulärer Art in sich bergen und deren *Katastrophenpotenziale* mit heutiger Methodik nicht voraussehbar und handhabbar sind.

Komplexität und Kopplung als zentrale Parameter für eine systemorientierte Risikobewertung

Charles Perrow befasst sich im Buch "Normal Accidents: Living with High-Risk Technologies" mit den technischen Charakteristika von so genannter Hochrisikosysteme. Er legt ausgehend von den Systemparametern Komplexität und Kopplung dar, was diese stark risikobehafteten Technologien und Institutionen gemeinsam haben und worin sie sich unterscheiden. Auf Grund dieser Eigenschaften macht er verständlich, warum gewisse dieser Technologien und Institutionen in ihrer Risikoentwicklung[3] kaum kontrollierbar sind. Aus diesen Überlegungen leitet er ein Fundament für eine neuartige, technisch-systemanalytische Risikobewertung der verschiedenen Systeme ab[4].

Komplexität und Kopplung als Systemeigenschaften

Definition Komplexität und Linearität gemäss Perrow

Komplexe Interaktionen beschreibt Perrow als Prozesse, die zwischen einer Komponente des so genannten DEPOSE-Systems (design, equipment, procedures, operators, supplies and materials, environment; Konstruktion, Ausrüstung, Abläufe, Operateure, Material und Zubehör, Umwelt) und mindestens einer Komponente ausserhalb des normalen Betriebsablaufs auftreten, unabhängig davon, ob sie in der Konstruktion vorgesehen sind oder nicht. Komplexe Interaktionen können entweder geplant sein, aber den Operateuren nicht vertraut, oder aber ungeplant und unerwartet. In allen Fällen sind sie für das Bedienungspersonal entweder nicht sichtbar oder nicht unmittelbar durchschaubar. Dem gegenüber definiert Perrow lineare Prozesse als Interaktionen, die zwischen einer Komponente des DEPOSE-Systems und mindestens einer ihr unmittelbar im Betriebsablauf vorher gehenden oder nachfolgenden Komponente auftreten. Lineare Interaktionen treten im erwarteten und bekannten Betriebsablauf auf oder sind für die Operateure gut sichtbar, auch wenn sie ausserplanmässig vorkommen.

---

[3] Risikoentwicklung muss hier - wie dies die Definition von Risiko vorgibt – auf zwei Ebenen verstanden werden: Einerseits bezieht es sich auf die Abfolge und Interaktion verschiedener Störfälle in einem (technischen) *System*. Andererseits beinhaltet es aber auch den kaum vorausahnbaren Ablauf schädigender Auswirkungen eines Unfalls auf Menschen und Umwelt.

4 Die von "RisikoexpertInnen" angewandte probalistische Risikoanalyse evaluiert zu den Störfällen von risikotechnischem Interesse zweierlei: Einerseits deren ihre systembedingte Eintretenswahrscheinlichkeit (auch als wahrscheinliche Eintretensfrequenz zu bezeichnen), andererseits deren ihr Schadenspotenzial auf Mensch und Umwelt. Zur Berechnung der Eintretenswahrscheinlichkeit eines betrachteten Störfalls wird top-down die Frequenz eines jeden einzelnen Ereignisstrangs, der zu diesem Ereignis führt, erörtert und abschliessend aufsummiert. In diesem ingenieurwissenschaftlichen Verständnis wird Risiko (R) als Produkt aus Eintretenswahrscheinlichkeit (W) und Schadensausmass (S) eines aus einem Ereignisstrang resultierenden Störfalls definiert: $R = W \cdot S$. Im Fall von Systemen, bei denen mit potenziell grossen Schäden gerechnet werden muss, kann diese klassische Methodik in eine etwas differenziertere Risikobewertung umgeformt werden. Dabei wird die Ereignisschwere ab einem definierten Schwellenwert si mit einem jeweils festzulegenden Koeffizienten α gewichtet: $R = W \cdot S^{\alpha}$ mit α := Schadensgewichtungskoeffizient, wobei für $S < si$ gilt $\alpha = 1$, für $S \geq si$ gilt $1{,}2 < \alpha \leq 2$ (D. Okrent, 1984).

Auswirkung der Komplexität auf die Häufigkeit der Systemunfälle

Perrow geht davon aus, dass der Grad der Komplexität eines Systems einen direkten Einfluss auf das Auftreten so genannter *Systemunfälle* hat. Ist bei linear interagierenden Elementen ein Einwirken eines jedes Elements nur auf das nachfolgende möglich, ist dem gegenüber bei komplex interagierenden Elementen eine reziproke Wirkung auf alle anderen komplex verknüpften Elemente möglich (siehe Abb. 1 und 2). Dem zufolge steigt die Anzahl möglicher reaktiver Interaktionen bei der Zunahme der komplex interagierenden Systemelemente nicht proportional sondern viel mehr im Quadrat zu deren Anteil am Gesamtsystem. Dies hat einen bedeutenden Einfluss auf die Ereigniswahrscheinlichkeit von Systemunfällen – insbesondere in Anbetracht der Unvermeidbarkeit von Komponentenstörungen. Damit hat ein System mit einem erhöhten Grad komplex interagierender Elemente eine eindeutig andere Systemeigenschaft als ein beinahe vollständig linear funktionierendes System.

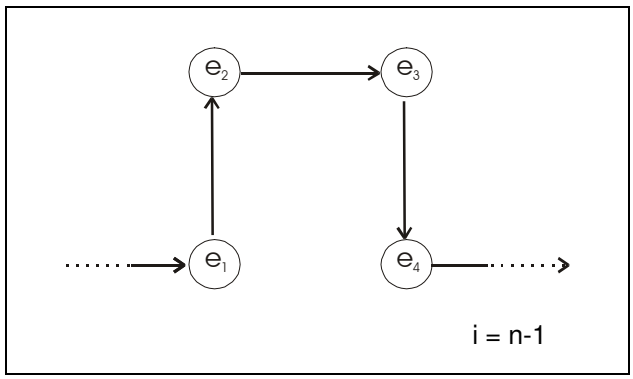

Abb. 1: Im vollständig linearen System wirkt jedes Element einzig auf sein nachfolgendes ein. Ein System mit n Elementen weist demzufolge n-1 Interaktionen auf.

(Grafik: F. Erzinger)

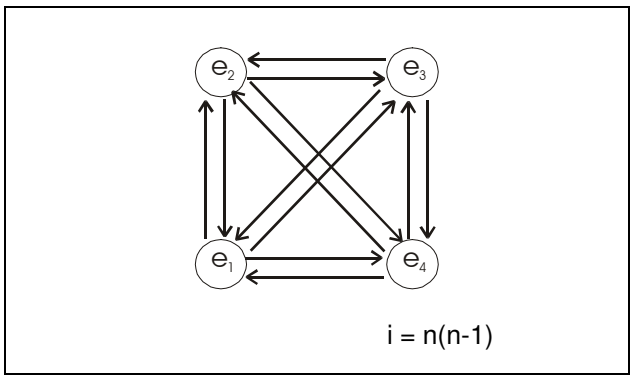

Abb. 2: Im vollständig komplexen System kann jedes Element auf jedes andere Element des Systems Wirkung ausüben. Ein System mit n Elementen weist demzufolge n·(n-1) Interaktionen auf.

(Grafik: F. Erzinger)

Charakeristika komplexer Systeme

Komplex interagierende Systeme müssen gerade aufgrund ihrer schwer durchschaubaren Funktionsweise notwendigerweise über *kybernetisch* ablaufende Prozesse gesteuert werden. Dadurch ist nur ein kleiner Teil der gesamten Funktionsweise direkt einsehbar. Information über die Funktionsweise komplexer Systeme ist zudem oft ausschliesslich nur indirekt ermittelbar, d. h. für die Steuerung wichtige Systemparameter wie beispielsweise Druck, Hitze, Verfügbarkeit von Kühlflüssigkeit etc. können auf Grund der extremen Bedingungen nicht direkt gemessen werden. Diese schon für sich problematische Eigenschaft wird durch die geringe *Redundanz* derartiger Systeme verschärft. Auf Grund der für sie charakteristischen Vielzahl kybernetischer Regulationsprozesse und der äusserst geringen Redundanz sind Systeme, welche sich durch einen hohen Anteil komplexer Interaktionen auszeichnen, in ihrer Funktionsweise also nur beschränkt durchschaubar. *Common-Mode-Fehler*, welche auf Grund der oben dargelegten Interaktionsmuster für komplexe Systeme ebenso charakteristisch sind, führen bei der Steuerung des Systems unweigerlich zu Verwirrung, da sie in ihrer Konstellation für die Operateure in keiner Weise antizipierbar und auch nicht unmittelbar einsehbar sind.

Definition enge und lose Kopplung gemäss Perrow

Die andere für Hochrisikosysteme zentrale Systemeigenschaft stellt gemäss Perrow der Grad der Kopplung dar, wobei dessen Merkmale unabhängig von den zuvor diskutierten Dimensionen Komplexität und Linearität zu beobachten sind. Enge Kopplung bedeutet, dass es zwischen zwei miteinander verbundenen

Teilen (Definition von Teilen siehe *Systeme)* kein Spiel, keine Pufferzonen oder Elastizität gibt, sämtliche Vorgänge des einen Teils wirken sich unmittelbar auf die Vorgänge des anderen Teils aus. In eng gekoppelten Systemen sind anteilmässig mehr Prozesse zu beobachten, die zeitgebunden ablaufen, die also nicht in Bereitschaft stehen und warten, bis sie angesprochen werden, sondern vorzu auf einander einwirkend ablaufen. Eng gekoppelte Systeme zeichnen sich zudem dadurch aus, dass die darin stattfindenden Prozesse *unifinal* sind. Auch verfügen eng gekoppelte Systeme bezüglich Materialverbrauch kaum über Spielraum: Die zu verarbeitenden Mengen müssen präzise abgemessen sein, die Ressourcen sind untereinander nicht austauschbar, vergeudete Betriebsstoffe können das Verfahren überbelasten, ein schadhaftes Aggregat führt zur Abschaltung der gesamten Anlage, da eine kurzfristige Substituierung durch ein anderes Teil nicht möglich ist.

Charakeristika eng gekoppelter Systeme

Eng gekoppelte Systeme reagieren dem entsprechend aufgrund der mangelnden Pufferung und Elastizität auf Erschütterungen, Störungen oder erzwungene Änderungen wesentlich direkter als lose gekoppelte, teilweise sogar verstärkend (*positive Rückkopplung*). Im Störfall erschwert eine enge Kopplung eine prompte Regenerierung des Systems. Da in allen Systemen Schäden und Störungen auftreten, sind demnach die Mittel zu deren Behebung von entscheidender Bedeutung. Es muss grundsätzlich die Möglichkeit bestehen, zu verhindern, dass ein *Störfall* sich zu einem *Unfall* ausweitet. Auf Grund der zuvor genannten Systemeigenschaften müssen in eng gekoppelten Systemen Puffer, Redundanzen und Substitutionsmöglichkeiten von den Konstrukteuren eingeplant werden. Die Hilfsmassnahmen sind demzufolge weitestgehend auf vorgeplante und fest installierte Hilfsmittel beschränkt. Auch die Eigenheiten der engen Kopplung verleihen einem System also eine besondere Charakteristik.

’Normale Katastrophen’ als systeminhärente Ereignisse

Komponentenunfälle, Systemunfälle und Katastrophen

Eine von Menschen verursachte Katastrophe stellt einen Unfall dar, der die Leben Hunderter von Menschen auslöscht und jene von Tausenden verkürzt oder in ihrer Qualität schmälert. Die Katastrophe als *Systemunfall* tritt erst dann ein, wenn mehrere Bedingungen, mehrere Systemstörungen zusammenkommen. Aus diesem Grund ist die Wahrscheinlichkeit ihres Auftretens wesentlich geringer als jene eines *Komponentenunfalls*, bei dem nur ein Teil jener Bedingungen gegeben ist. Demgemäss sind Systemunfälle im Gegensatz zu Komponentenunfällen ungewöhnliche, sogar äusserst seltene Ereignisse.

Charakeristika von Systemunfällen

Wenn komplexe Interaktionen die konstruktiven Sicherheitsvorkehrungen ausser Funktion setzen oder umgehen, kommt es zu unerklärlichen und unvorhergesehenen Störungen. Ist das System zudem eng gekoppelt, sodass nur wenig Zeit und ein geringer Spielraum im Hinblick auf Hilfsmittel oder zufälligerweise einsetzbare Sicherheitsmassnahmen zur Systemregenerierung zur Verfügung stehen, dann lässt sich die Störung oft nicht mehr auf Komponenten oder Einheiten des Systems beschränken. Der Ausfall einer oder mehrerer Komponenten des DEPOSE-Systems wird dann Subsysteme oder das gesamte System lahm legen – es kommt zu einem Systemunfall. Dieser wird demzufolge zwar durch eine Komponentenstörung ausgelöst, wird jedoch auf Grund der Natur des Systems selbst leicht zu einem unvermeidlichen oder ’normalen’ Unfall.

Das Normale an der "normalen Katastrophe"

Mit dem ungewöhnlichen Begriff 'normale Katastrophe' will Perrow also deutlich machen, dass beim Vorliegen der oben dargelegten Systemeigenschaften vielfache und unerwartete Interaktionen zwischen Störungen des Systems und die dadurch provozierten Systemunfälle zwangsläufig vermehrt auftreten werden. ’Normal’ bezeichnet also eine immanente Eigenschaft des Systems und keine

Häufigkeit. Perrow vergleicht dieses Phänomen mit dem Tod: Er ereignet sich zwar nur einmal auf x Jahre Lebenszeit, dennoch ist es normal, dass er irgendwann eintritt.

Von der Systemanalyse zur Risikobewertung

Anfälligkeit auf Systemunfälle in Abhängigkeit von Komplexität und Kopplung

Gemäss einer systemanalytischen Bewertung verschiedener Institutionen und Technologien nach den antagonistischen Parametern lineare/komplexe Interaktionen und lose/enge Kopplung ordnet Perrow die von ihm untersuchten Systeme in einem entsprechenden zweidimensionalen Raum (s. Abb. 3). Dieser Raum tariert damit das gesamte Spektrum der systeminhärenten Unfallanfälligkeit aus. Gemäss den oben dargelegten Überlegungen stellt Perrow die Hypothese auf, dass alle im zweiten Quadranten (also rechts oben) eingezeichneten Systeme häufiger Systemunfälle zu verzeichnen haben als die übrigen – dies wiederum basierend auf der Annahme, dass Störungen und Pannen im DEPOSE-System nie völlig vermeidbar sind.

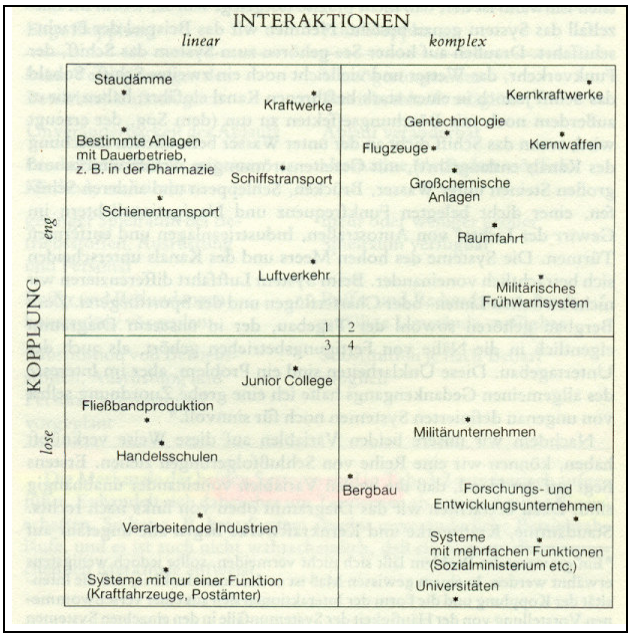

Abb. 3: Grad der Komplexität und Kopplung verschiedener Technologien und Institutionen.

(Quelle: C. Perrow, 1992)

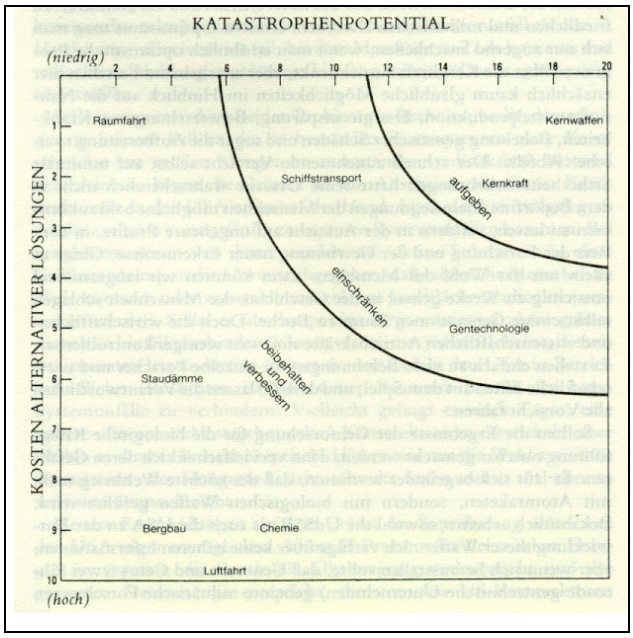

Abb. 4: Aus der Risikoanalyse abgeleitete politische Empfehlungen.

(Quelle: C. Perrow, 1992)

Komplexität und Kopplung als unabhängige Systemeigenschaften

Diese Kategorisierung erfolgt entlang Perrows subjektiven Einschätzungen, da der Systemanalyse zurzeit keine zuverlässigen Möglichkeiten der Parametrisierung der beiden Dimensionen Komplexität und Kopplung zur Verfügung stehen. Gegen die einzelnen Zuordnungen lassen sich durchaus Einwände erheben. Was aber anhand der sehr homogenen Verteilung der verschiedenen Risikosysteme in diesem zweidimensionalen Komplexität-Kopplung-Diagramm ersichtlich wird ist, dass sich die beiden Systemparameter Komplexität und Kopplung tatsächlich unabhängig von einander verhalten.

Qualitative Risikobewertung basierend auf Nettokatastrophenpotenzial und Substitutionskosten

Von dieser grundlegenden systemanalytischen Theorie zur Quantifizierung der Neigung zu Systemunfällen der verschiedenen Hochrisikosystemen, macht Perrow dann einen Schritt weiter zur qualitativen Risikobewertung, mit deren Hilfe er einen künftig vernünftigen Umgang mit den verschiedenen, uns zur Verfügung stehenden Technologien und Institutionen austariert. Zu diesem Zweck leitet

Perrow das *Nettokatastrophenpotenzial* von der jeweiligen Neigung eines Systems zu Systemunfällen mit katastrophalen Auswirkungen in Folge technischer oder organisatorischer Fehlleistungen einerseits und von dem jeweiligen Katastrophenpotenzial, welches einzig aus Komponentenunfällen resultiert, andererseits ab. Dem Nettokatastrophenpotenzial (bzw. in der Grafik nur mit katastrophenpotenzial bezeichnet) stellt Perrow die Kosten gegenüber, welche aufzuwenden wären, um Substitutionssysteme zu entwickeln, deren Risikopotenzial geringer ausfallen würden. Damit führt Perrow die Systemanalyse weiter zur Risiko-Kosten-Analyse und formuliert basierend auf dieser Verteilung (s. Abb. 4) eine Aussage über den aus seiner Perspektive angezeigten Handlungsimperativ: Systeme mit geringem Katastrophenpotenzial sollen auf jeden Fall beibehalten und bezüglich ihrer systemimmanenten Unfallanfälligkeit verbessert werden. Systeme mit mittlerem Katastrophenpotenzial sollen bei hohen Substitutionskosten beibehalten und verbessert werden, bei tiefen Substitutionskosten jedoch nur eingeschränkt zum Einsatz kommen und sukzessive durch Alternativsysteme ersetzt werden. Systeme mit grossem Katastrophenpotenzial schliesslich sollten bei hohen Substitutionskosten ebenso beibehalten und verbessert werden (in dieser Kategorie sieht Perrow jedoch keines der untersuchten Systeme), bei mittleren Kosten zur Entwicklung von Alternativtechnologien nur eingeschränkt zum Einsatz kommen, und bei niedrigen Substitutionskosten vollständig aufgegeben werden.

Nettokatastrophenpotenzial und Substitutionskosten als unabhängige Systemeigenschaften

Wiederum darf die vorgenommene Qualifizierung der einzelnen Systeme in Frage gestellt werden, basiert auch diese Kategorisierung der verschiedenen Hochrisikosysteme einzig auf Perrows erfahrungsgestützter, subjektiver Beurteilung der verschiedenen Technologien und Institutionen. Dennoch ist auch bei dieser Analyse eines klar zu erkennen: Die verschiedenen Hochrisikotechnologien und -institutionen unterscheiden sind in Bezug auf deren Katastrophenpotenzial und den gegenübergestellten Alternativlösungskosten eindeutig.

Neue Wege zu einer qualitativ-quantitativen Risikobewertung

Integrative Methodik zur ganzheitlichen Risikobewertung

Im Bereich der systemorientierten Risikoanalyse liefern verschiedene Forscher wie Sven Ternov und Roland Akselsson, Mohamed Modarres, Fredrik Vraalsen et al. und Josef Sharit unterschiedliche methodische Ansätze. Dabei sticht das Computertool von Sharit hervor, stützt es sich in seiner Systembeschreibung unter anderem doch gerade auf das Perrowsche Komplexität-Kopplung-Modell. Im Kontext des menschlichen Umgangs mit komplexen Systemen liefert auf der methodischen Ebene aber auch Frederic Vester mit dem Sensitivitätsmodell ein interessantes Werkzeug. Diese Systemanalyse-Software schafft unter anderem die Verbindung zur charakteristischen Funktionsweise organisierter Systeme der Natur, der so genannten *Biokybernetik*. Dem gegenüber geben Roland W. Scholz und Olaf Titje Einblick in eine erweiterte Sicht der Risikobewertung.

Sharits Ansatz eines systemorientierten Risikoanalyse-Tools entlang der Idee von Perrow

Sharits Computertool zur systemorientierten Risikoanalyse basiert auf zwei unterschiedlichen Komponenten: Auf der einen Seite dient die Perrowsche Komplexität-Kopplung-Theorie der Parametrisierung des jeweiligen Systemcharakters eines (Hoch-)Risikosystems. Auf der anderen Seite nutzt Sharit das so genannte Konzept der Multiplen Systemperspektiven, um das zu untersuchende System auf verschiedenen, alternativen (also sich nicht gegenseitig ausschliessenden) Abstraktionsniveaus zu beschreiben. Die drei Modellierungsebenen, die zur optimalen Aufschlüsselung der Systemkomplexität beachtet werden sollen, sind die technische, die organisatorische und die menschliche. Auf jedem der drei Abstraktionsniveaus wird zwar das gesamte System untersucht, jedoch unter Nutzung unterschiedlicher Analyseterminologien. Auf jeder dieser drei Ebenen können Informationen über das Gesamtsystem

erschlossen werden, die sich durch die alleinige Untersuchung einer der anderen Ebenen so nicht entdecken liessen. Zudem ermöglicht das Konzept der Multiplen Systemperspektiven durch die Interaktion der aus den unterschiedlichen Untersuchungsebenen gewonnen Informationen einen erweiterten Einblick in die reale Komplexität eines Systems. Die interaktive Verknüpfung der verschiedenen Informationsebenen ermöglicht schliesslich ein einzigartig breites und vollständiges Verständnis der Funktionsweise eines Systems. Durch die Verknüpfung dieser beiden Systemanalysekomponenten schafft es Sharit, die Idee von Perrow, ein System gemäss den beiden Hauptcharakteristika Kopplung und Komplexität, auf eine viel versprechende Weise in eine parametrisierbare Risikoanalysemethodik mit klar systemorientiertem Ansatz umzusetzen.

Komplexität gemäss Vester

Auf der anderen Seite nähert sich Vester dem Problem der systemanalytischen Beschreibung von Komplexität von dem Verständnis der (Mikro-)Biologie. Komplexität hat gemäss Vester sehr viel mit Vernetzung zu tun, kommt eigentlich erst durch Vernetzung zustande. Komplexe Systeme bestehen gemäss ihm grundsätzlich aus mehreren verschiedenen Teilen, welche in einer bestimmten dynamischen Ordnung zueinander stehen und so zu einem Wirkungsgefüge vernetzt sind. Komplexe Systeme verhalten sich anders als nur gerade die Summe ihrer Einzelteile, bzw. Subsysteme, da sich durch die Vernetzung Eigenschaften ausbilden, die es zuvor, als die verschiedenen Interaktionen noch nicht bestanden, tatsächlich nicht gab. Zu nennen wären hier Eigenschaften wie Rückkopplung, Schwellen- und kritische Werte oder selbstregulatorische Effekte, so genannte *Regelkreise*. Dem entsprechend geht auch Vester davon aus, dass wir nach dem Entstehen eines solchen Systems sein Verhalten nicht mehr aus den Einzelkomponenten ableiten können, aus denen es zusammengesetzt ist. Komplexe Vorgänge verlangen zu ihrem Verständnis demzufolge ein Denken in Zusammenhängen, das sich an der Struktur organisierter Systeme und ihrer speziellen Dynamik orientiert.

Systemanalyse entlang der *Biokybernetik*

Um also ein Planen und Handeln im Sinne der *Bionik* zu ermöglichen, hat Vester ein neues Instrument der Systemmodellierung und -Analytik entwickelt, welches die Anwendung der kybernetisch-systemischen Sichtweise erleichtert, wenn nicht überhaupt erst möglich macht: Das so genannte Sensitivitätsmodell. Auf Grund der Reduktion der Variablen auf ein handhabbares und relevantes Set von Systemparametern und der Integration sowohl quantitativer als auch qualitativer Systemdaten in die Modellierung eines komplexen Systems mit Hilfe spezieller Methoden des Datenscreenings und dank der Beschreibung und Bewertung der wirkenden Beziehungsgefüge zwischen einzelnen Subsystemen mit Hilfe der Theorie der *'fuzzy logic'* gewährleistet diese computergestützte Arbeitshilfe eine Systembeschreibung und -Abgrenzung, welche der Realität ausserordentlich nahe kommt. Damit liefert das Vestersche Sensitivitätsmodell den systemanalytischen Approach für die Diskussion der systeminhärenten Katastrophenanfälligkeit in Abhängigkeit der Parameter Komplexität und Kopplung und wenn notwendig noch weiterer Systemeigenschaften.

qualitativ-quantitativer Ansatz für eine technisch-naturwissenschaftliche Risikobewertung

Als Werkzeug für einen qualitativ-quantitativen Ansatz für eine technisch-naturwissenschaftliche Risikobewertung schlagen Scholz und Titje das so genannte integrierte Risikomanagement vor. Dabei sollen Risikosysteme auf ihre strukturellen Eigenschaften analysiert werden, womit eine Reduktion der Komplexität der Fallanalyse bewirkt werden kann. Die Methode soll des weitern Einsicht geben in den situativen und semantischen Kontext der Risikowahrnehmung der verschiedenen TeilnehmerInnen ("ExpertInnen" / "Laien") des Risikodisputs und deren Handlungsmotive. Und als Drittes versprechen Scholz und Titje, dass mit dieser erweiterten Form der Risikoanalyse die Integration von verschiedenen Sichtweisen – mit ökonomischen, soziologischen, umwelttechnischen und kultu-

rellen Aspekten – ermöglicht wird. Damit ermöglichte das integrierte Risikomanagement von Scholz und Titje einen qualitativ-quantitativen Ansatz der Risikoanalyse entsprechend der Vesterschen Risikobewertung basierend auf dem Nettokatastrophenpotenzial und den Substitutionskosten eines Hochrisikosystems.

Sozialpsychologische Aspekte der Risikodiskussion

Komplexe Systeme und Risikosysteme in der Sozialpsychologie und in der Philosophie

Auch aus Bereichen der Sozialpsychologie und der Philosophie wird die Theorie von Perrow durch andere Arbeiten gestützt und erweitert. Zu nennen sind hier unter anderem Paul Slovic, der sich mit der Thematik der Risikowahrnehmung befasst, Dietrich Dörner, der die Handhabungstechniken von komplexen Systemen verschiedener Gesellschaftsgruppen untersucht, und Bernd Guggenberg, der sich von einem sozialphilosophischen Punkt an die Frage der Bedeutung von Hochrisikosystemen für eine Gesellschaft annähert.

"ExpertInnen"- und "Laien"-Urteile in der Risikobewertung

So geht Slovic in seinen Untersuchungen der Frage nach, warum "ExpertInnen" und "Laien" in ihrer Bewertung von Hochrisikosystemen in gewissen Fällen zu dermassen unterschiedlichen Resultaten kommen. In empirischen Untersuchungen verschiedener Risikobewertungskriterien erkannte er den von Forschern so bezeichneten 'Angstrisiko'-Faktor. Diesen sieht Slovic verknüpft mit der mangelnden Kontrolle über die Aktivitäten der Betreiber eines Systems und den möglichen tödlichen Folgen bei auftretenden Pannen. Weiter fliesst die Vermutung eines unausgewogenen Verhältnisses zwischen Risiko und Nutzen – das charakteristische Merkmal der 'Risikogesellschaft' wie sie Ulrich Beck beschrieben hat - einschliesslich der Risiken für künftige Generationen in diese Bewertung ein. Zu all diesen Kriterien des 'Angstrisiko'-Faktors kommt schliesslich die Überzeugung, dass die Risiken in Zukunft zunehmen und sich nur schwer verringern lassen werden. Ein weiterer Faktor, den Slovic in den untersuchten Bewertungsstrukturen entdeckte, ist jener des 'Unbekanntheitsrisikos'. Diesen bringt er in Verbindung mit Risiken, die den potenziell Betroffenen unbekannt sind, die sie nicht beobachten können, die neuartig sind und welche mit Spätfolgen verbunden sind.

Analogien zwischen der Risikowahrnehmung und der Risikobewertung

Das erstaunliche an der Theorie der emotionenbezogenen Risikobewertung von Slovic und der Komplexität-Kopplung-Matrix von Perrow ist, dass die beiden Beurteilungsmethoden zu ausserordentlich ähnlichen Resultaten führen. Dabei beruht das Bewertungsschema von Slovic auf einer Theorie sozial geprägter Heuristiken, welche das Katastrophenpotenzial so wie weitere, subjektiv wahrgenommene Dimensionen zu einem Gesamturteil zu integrieren suchen. Die Risikobeurteilung, wie sie Perrow herleitet, beruht dagegen aber auf einer Kosten-Nutzen-Rechnung, basierend auf einer technisch-naturwissenschaftlichen Systemanalyse und der Qualifizierung der Systeme nach deren Katastrophenpotenzial und Substituierbarkeit.

Menschliches Unvermögen im Umgang mit sehr geringen Wahrscheinlichkeiten

Zum Thema Risikowahrnehmung kommen auch von Stone, Yates und Parker wichtige Beiträge: So stellen sie fest, dass Menschen offenbar nicht dazu geschaffen sind, mit kleinen Wahrscheinlichkeiten zu hantieren: Sehr kleine Wahrscheinlichkeiten werden im subjektiven Kalkül häufig auf "Null" gesetzt, vielleicht weil der kognitive Aufwand für den Umgang mit sehr kleinen Wahrscheinlichkeiten zu gross ist.

'Logik des Misslingens' im Umgang mit komplexen Systemen

Dörner führte mit Hilfe eines computersimulierten 'Entwicklungsspiels' folgendes Experiment durch: In einem fiktiven, komplex interagierenden Gesellschafts- und Ökosystemgefüge eines virtuellen afrikanischen Landes sollten die Versuchspersonen mit möglichst adäquaten Massnahmen einen Entwicklungsprozess in Richtung 'nachhaltiger Gesellschaft' initiieren und dann auch über einen gewis-

sen Zeithorizont fortführen. Das Ergebnis war in seiner Klarheit und Aussage erschütternd: Die Untersuchungspersonen zeichneten sich durchs Band weg durch die mehr oder minder ausgeprägte Unfähigkeit aus, Probleme in einem komplex funktionierenden System richtig zu bewerten und zu lösen. Auffallend dabei war auch, dass die am Versuch beteiligten "ExpertInnen" genauso wie die übrigen Versuchspersonen ein Chaos schufen und das virtuelle Land in ein Desaster führten, obschon sie alle eigentlich Verbesserungen des Systems anstrebten. Bei genauer Evaluation der Verhaltensmuster der Versuchspersonen stellten sich verschiedene stereotype, fundamentale Denk- und Planungsfehler im Umgang mit komplexen Problemstellungen heraus, es wurde eine 'Logik des Misslingens' erkennbar, welche in direktem Zusammenhang mit dem Funktionieren des virtuellen Landes als komplexes System zusammenhing. Das Experiment zeigte, dass Menschen komplexe Systeme in aller Regel nicht richtig bewerten können. Unabhängig von ihrer erlernten intellektuellen Fähigkeit, nicht-komplexe Problemstellungen richtig lösen zu können, sind sie ganz offensichtlich nicht fähig, Probleme in komplex interagierenden Systemen adäquaten und nachhaltigen Lösungen zuzuführen.

Fehlertolerante Systeme zur Wahrung der Evolutionsfähigkeit

Guggenberg sieht die Ironie von komplexen, kybernetischen Abläufen im Zusammenhang mit Hochrisikosystemen in der Tatsache, dass gerade jene höchst entwickelten Strukturen in Technologie und Wissenschaft, die heute auf Grund ihres enormen Gefahrenpotenzials die Möglichkeit der menschlichen Irrtumserfahrung beeinträchtigen und unterbinden, sich selbst in aller Regel eben dieser Produktivkraft des Irrtums verdanken. Er sieht die Gefahr komplexer Hochrisikosysteme demzufolge auch auf einer gesellschaftsethischen Ebene im durch sie erforderlichen Irrtumsverlust auf Grund der Fehlerintoleranz dieser Systeme.

Mustererkennung zur Informationsreduktion

Schliesslich gibt es auch im Kontext der Vester'schen Theorie aus der Arbeitspsychologie wichtige Erkenntnisse. So hält Hacker fest, dass Menschen in der Lage sind, aus wenigen Informationen viel zu schliessen. Häufig sehen wir "mit einem Blick", wie der Zustand einer Anlage ist, wir müssen nicht erst mühsam jedes Detail prüfen. Darin liegt ja genau die menschliche Effizienz: Wir sind in der Lage, Muster zu erkennen. Die Kehrseite der Medaille: Wenn etwas (scheinbar) zu einem Muster passt, das wir kennen, dann sind wir sehr schnell bereit, die bekannte Diagnose zu fällen, das neue Problem dem alten Muster zuzuordnen. Weiter zeigen Untersuchungen von Hacker auch, dass gut ausgebildete und erfahrene Arbeitskräfte nicht unbedingt mehr, sondern oft sogar weniger Informationen aufnehmen als schlecht ausgebildete – aber sie nehmen die wichtigeren auf, während sich Neulinge von allem möglichen verwirren lassen. Information filtern ist also nicht schlecht, sondern unvermeidlich und nötig für effizientes Handeln.

Der Diskurs über Wahrscheinlichkeit und Schadenpotential

Ist der Risikodiskurs wirklich ein Laien-ExpertInnen-Diskurs?

Die ganze Risikodiskussion – die notwendigerweise eine gesamtgesellschaftliche Diskussion ist, da alle Elemente der Gesellschaft einer bestimmten Weltregion gleichermassen den möglichen Folgen eines katastrophalen Unfalls ausgesetzt sind – wirft nun die Frage auf, woran sich im so genannten Laien-ExpertInnen-Diskurs der Konflikt überhaupt entzündet. Um den Inhalt dieses gesamtgesellschaftlichen Diskussionsprozesses zu verstehen, sind die nachfolgenden Bemerkungen sehr hilfreich:

"Currently, the risk concept is used and applied widely. However, it is still a disputed and multifaceted concept. This is highlighted by the statement that experts more often discuss the meaning of risk than how big a risk is" (R. W. Scholz & O. Tietje, 2002)

"Whoever controls the definition of risk controls the rational solution to the problem at hand. If risk is defined one way, then one option will rise to the top as the most cost-effective or the safest or the best. If it is defined another way, perhaps incorporating qualitative characteristics and other contextual factors, one will likely get a different ordering of action solutions. Defining risk is thus an exercise in power." (P. Slovic, 1999)

Risikodefinition im Zentrum des Risikodiskurs'

Kern des Risikodiskurses ist dem zufolge nichts weniger als die Definition von Risiko, bzw. die Interpretation von bereits bestehenden Definitionen von Risiko. In Zentrum steht die in der Fussnote 3 und im Annex bereits dargelegte inginieurwissenschaftliche Definition von Gesamtrisiko, gemäss der das Produkt aus Wahrscheinlichkeit und Schaden für jeden untersuchten *Ereignisstrang top-down* analysiert und schliesslich kumulativ bilanziert wird (wobei hier der Einfachheit zu Liebe α = 1 gesetzt wird; siehe Fussnote 3):

$$R_{tot} = \sum_{i=1,u=1}^{n,u} W_i \cdot S_u \approx W_{tot} \cdot S_{tot}$$

i := Bezeichnung der verschiedenen Ereignisstränge, die zu demselben spezifischen Schaden (S_u) führen können.

Eintretenswahrscheinlichkeit und Schadenspotential als zwei verschiedene Fokusse der Risikobewertung mit unterschiedlichen Resultaten

Bei der Diskussion um das gesellschaftlich zu tolerierende Mass an Risiko konzentrieren sich die so genannten ExpertInnen[5] auf den Faktor Wahrscheinlichkeit, die als Laien bezeichneten Diskussionsteilnehmenden eher auf den Faktor des potenziellen Schadens. Die "ExpertInnen", welche die Eintretenswahrscheinlichkeit von katastrophalen Schadensereignissen als ausserordentlich gering angeben und deshalb W_{tot} kurzerhand als praktisch Null setzen, pflegen diesen Fokus wohl aus verschiedenen Gründen: Erstens wäre der potenzielle Gesamtschaden im Falle von Hochrisikosystemen in der Komplexität der unterschiedlichen Ereignisbäumen (*bottom-up Analyse* für jedes Schadensereignis S_u) ausserordentlich schwierig zu quantifizieren, und zweitens wäre die Diskussion nach dem gesellschaftlich tolerierbaren Gesamtschaden nach Grossunfällen wie Seveso, Bhopal oder Tschernobyl etc. makaber (die zu klärende Frage wäre da ja, "wie viele Tote und Verletzte sind wir als Kollektiv im Fall jedes einzelnen Hochrisikosystems bereit gegebenenfalls zu opfern?") und würde für die Technik befürwortenden "ExpertInnen" in die falsche Richtung führen. Die "Laien" auf der anderen Seite misstrauen der wissenschaftlichen Auseinandersetzung über Eintretenswahrscheinlichkeiten von Katastrophenereignissen wohl eher instinktiv in Anlehnung an "*Murphy's Law*", indem für sie klar ist, dass einerseits W ≈ 0 eben noch lange nicht W = 0 ist und dass andererseits beispielsweise auch eine Wahrscheinlichkeit von 1 : 1'000'000 wie im Fall von Kernkraftwerken noch lange keine Garantie dafür ist, dass erst eine Million Reaktorlaufjahre verstreichen müssen, bis der erste Reaktorunfall eintreten kann. Für sie steht viel mehr im Zentrum, was geschehen würde, falls das hoch Unwahrscheinliche eben doch eintreten würde.

[5] So genannte ExpertInnen, bzw. Laien deswegen, weil durch diese Begriffe ja eigentlich schon von vorne weg klar festgelegt ist, wer kompetent ist, und wer nicht – was ja gemäss Dörner (siehe vorher gehendes Kapitel) gar nicht immer so zutreffen muss.

Streitpunkt Eintretenswahrscheinlichkeit von Katastrophenereignissen

Dennoch ist es, wie der Diskussionsverlauf der letzten Jahre gezeigt hat, für die "Laien" ausserordentlich schwierig, sich dem von ihnen gescheuten und von den "ExpertInnen" immer wieder bedienten Diskurs über die ausserordentlich geringe Eintretenswahrscheinlichkeit von Katastrophenereignissen im Falle von Hochrisikotechnologien zu entziehen. Man kann demzufolge sagen, die Eintretenswahrscheinlichkeit von Katastrophenereignissen bei den verschiedenen Hochrisikosystemen stellt den Zankapfel in der öffentlichen Risikodiskussion dar.

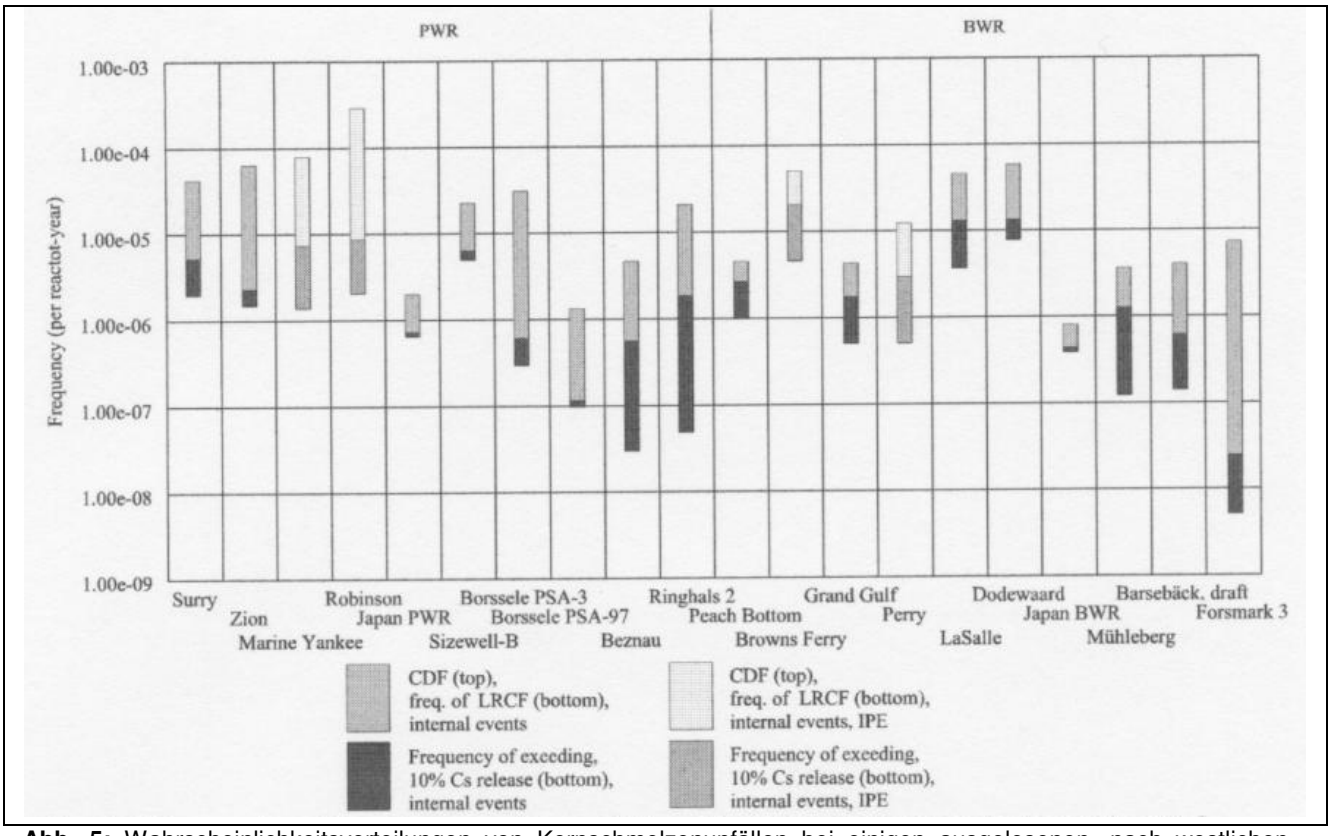

Abb. 5: Wahrscheinlichkeitsverteilungen von Kernschmelzenunfällen bei einigen ausgelesenen, nach westlichen Standards gebauten Kernkraftwerken, geordnet nach den verschiedenen möglichen Ereignissen Kernschmelze, grosser Freisetzungsverhinderungsstörfall, Freisetzung von über 10% des reaktorinternen Cäsiumbrennstoffs, interne Störfälle (CDF für "core damage frequencies", LRCF für "large release containment failure") und Verfahrensarten wie *Druckwasserreaktor* oder *Siedewasserreaktor*[6] (PWR für "pressurized water reactor", BWR für "boiling water reacter"). (Quelle: W. Kröger, 2004)

Prüfung der Risikoanalyse mit Hilfe von statistischen Tests

Quantifizierung der systeminhärenten Eintretenswahrscheinlichkeit von Systemunfällen auf dem Prüfstand

Perrows Konzept der systemischen Risikobewertung besitzt mit den beiden Grundvariablen Komplexität und Kopplung einen vollkommen neuen und sehr überzeugenden Ansatz zur Quantifizierung der systeminhärenten Eintretenswahrscheinlichkeit von Systemunfällen. Ein Problem bei der vorliegenden Kategorisierung kann jedoch auch Perrow nicht von der Hand weisen: Es ist durchaus denkbar, dass sich seine subjektiv vorgenommenen Quantifizierungen der Komplexitätsgrade und der Kopplungsintensitäten aus einer vagen Vorstellung von der Häufigkeit von Systemunfällen in den einzelnen Systemen ableiten statt aus einer objektiven Analyse der Eigenschaften des betreffenden

[6] Kerntechnologiespezifische Fachausdrücke werden im Kapitel "Technisches zur Kernenergie" im Annex erläutert.

Systems, unabhängig von der Art der auftretenden Störungen. Dies würde bedeuten, dass beispielsweise einer Technologie, die nur eine geringe Anzahl Unfälle verursacht, unbewusst eine geringe Komplexität und eine schwache Kopplung zugewiesen wird. Anhand dieser Vorannahme wird dann nach Belegen gesucht, die diese stützen. Diese Zirkularität lässt sich gemäss Perrow nur durch die Erhebung klar parametrisierbarer Daten auf der Grundlage strenger Begriffsdefinitionen durchbrechen, welche uns eine objektive Prüfung dieser Hypothese erlauben würde. An diesem Punkt sind also Wege der Quantifizierung von Perrows Theorie gefragt, um Aussagen über die Validität seiner Methode zur Ermittlung von Eintretenswahrscheinlichkeiten von Systemunfällen machen zu können.

Frage nach der Validität der Resultate der klassischen Risikoanalyse

Auf der anderen Seite ist aber auch die klassische Risikoanalyse nach mehreren Jahrzehnten ambivalenter Erfahrungen mit verschiedenen Typen von Risikosystemen und bei einem wie zuvor dargelegt offensichtlich weiterhin divergierenden Diskurs über die Einstufung des Risikos bei Hochrisikosystemen zwischen "Laien" und "ExpertInnen" an dem Punkt angelangt, wo sie verpflichtet ist, gleich wie dies Perrow zu seiner eigenen Theorie fordert, die Frage nach der Richtigkeit ihrer Analyseresultate zu stellen. Insbesondere die von Risikoanalytikern angegebenen Eintretenswahrscheinlichkeiten für Katastrophenfälle müssten mit Hilfe statistischer Test's auf deren Validität geprüft werden.

Unwahrscheinliche Eintretenswahrscheinlichkeiten für Katastrophenfälle

Führt man beispielsweise eine solche mögliche statistische Prüfung approximativ für die Kernenergie durch, kann folgende Aussage gemacht werden: Die Nullhypothese "die beobachtete, relative Häufigkeit von drei grossen Unfällen, bei welchen beträchtliche Mengen radioaktives Material in die Umwelt freigesetzt wurden[7], auf ca. 9'000 Reaktorjahren Betriebserfahrung (W. Kröger, 2004) seit Beginn der Atomtechnologie entspricht der berechneten Wahrscheinlichkeit von ca. 1:1'000'000a", wie sie von "RisikoexpertInnen" angegeben wird (siehe Abb. 5 Durchschnitt der dunkel gefärbten Balkenabschnitte), muss bei einem Signifikanzniveau α von 1% klar verworfen werden[8]. Dies bedeutet nichts anderes, als dass man für den vorliegenden Fall davon ausgehen kann, dass die von den "ExpertInnen" berechnete Eintretenswahrscheinlichkeit von Reaktorunfällen grösseren Ausmasses $p_0 = 10^{-6}a^{-1}$ weniger als 1% wahrscheinlich ist. Oder nochmals anders formuliert: Man muss davon ausgehen, dass die Angabe $p_0 = 10^{-6}a^{-1}$ falsch ist und dass die reale Eintretenswahrscheinlichkeit solcher Unfälle wesentlich grösser ist, d.h. dass diese Ereignisse in Wahrheit wesentlich häufiger zu erwarten sind als einmal auf eine Million Jahre.

Grenzen der probabilistischen Risikoanalyse

Will man den "RisikoexpertInnen" keine absichtliche Datenfälschung unterstellen, muss der Grund für die Fehlerhaftigkeit dieser berechneten Eintretenswahrscheinlichkeiten in der fehlenden Applizierbarkeit der probabilistischen Risikoanalyse als sehr linear funktionierendes Modellierungssystem (für ein in Tat und Wahrheit sich überaus komplex verhaltendes und stark gekoppeltes System wie die Kerntechnologie!) angenommen werden. In gleicher Weise wie hier gezeigt, kann der Konfidenzgehalt verschiedener Eintretenswahrscheinlichkeiten von

[7] Three Miles Island, USA: Kernschmelzeunfall, 1979; Tschernobyl, Ukraine: Kernschmelzekatastrophe, 1986; Tokai Mura, Japan: Kritikalitätsunfall, 1999 (genauere Beschreibung der Unfälle finden sich im Kapitel "Historisches zur Kernenergie" im Annex). Die drei Ereignisse werden hier – trotz ihren unterschiedlichen Eintretensursachen - bezüglich ihrer Eintretenswahrscheinlichkeiten gleichwertig behandelt, da alle drei zu einem Austritt einer erheblichen Menge radioaktiven Materials führten. Ausführliche Beschreibungen der drei Unfälle finden sich im Annex im Kapitel "Historisches zur Kernenergie".

[8] Die Ableitung dieser statistischen Schlussfolgerung wird im Annex im Kapitel "Statistisches zur Kernenergie" ausführlich dargelegt.

Systemunfällen für jedwelches andere komplexe und stark gekoppelte System geprüft werden.

Ziele einer systemorientierten Risikobewertung

Notwendigkeit und anzustrebende Logik einer neuartigen Methodik zur Risikobewertung

Dieses Beispiel soll im Zusammenhang mit dem vorliegenden Projektbeschrieb zweierlei illustrieren. Erstens zeigt es klar, dass die Notwendigkeit, eine neuartige Methodik zur Risikobewertung zu entwickeln, tatsächlich gegeben ist und zweitens soll es ermutigen, diese neue Art der Risikobewertung ausserhalb der Logik der klassischen Risikoanalyse zu suchen. Denn auf Grund dessen, dass die an linearen Systemen durchaus erfolgreich angewandte probabilistische Risikoanalyse, angewandt auf ein komplexes, stark gekoppeltes System, ein derart falsches Ergebnis liefert, lässt den Schluss zu, dass in diesem Fall ganz offensichtlich systematische Fehler vorliegen. Oder in der Sprache der Statistiker ausgedrückt: Dass hier an der *Messgenauigkeit* und nicht an der *Präzision* gearbeitet werden muss, ganz im Sinne von "lieber ungefähr richtig, als präzise falsch".

Anzustrebende Fragestellungen für eine anzustrebende Dissertation

Die grundlegenden Fragen, welchen die in diesem Projektbeschrieb skizzierte Dissertationsarbeit nachgehen soll, sind also folgende:

- Wie müsste eine Methodik zur Quantifizierung von Eintretenswahrscheinlichkeiten von Katastrophenereignissen aussehen, welche sich entlang der Biokybernetik am System und dessen grundlegenden Eigenschaften wie Komplexität und Kopplung orientiert?
- Wie lässt sich diese neu zu entwickelnde Methode – aus Gründen der Minimierung systemischer Modellierungsfehler - auf zwei möglichst unterschiedliche Hochrisikosysteme anwenden und mit Hilfe von Konfidenzintervallen ihre Validität evaluieren?
- Wie müsste ein qualitativ-quantitativer Ansatz für eine technisch-naturwissenschaftliche Risikobewertung aussehen, welche sich entlang dem integrierten Risikomanagement auf der Perrowschen Risikobewertung gemäss dem Nettokatastrophenpotenzial und den Substitutionskosten eines Hochrisikosystem basiert?
- Wie stehen die auf diese Weise erarbeiteten Resultate von Eintretenswahrscheinlichkeit und Risiko zu Werten herkömmlicher Risikoanalysen und auch zu Erkenntnissen aus der Sozialpsychologie zur kollektiven Wahrnehmung von Risiko?
- Was macht schliesslich eine risikoarme Technologie aus, und wie wird dies gesellschaftlich wahrgenommen?

Die Antworten auf diese Fragen führten mit Hilfe eines systemorientierten Ansatzes zu einer für komplexe und stark gekoppelte Risikosysteme adäquaten Risikoanalyse. Das Vorgehen, wie diese Antworten erarbeitet werden könnten, müsste wie folgt aussehen, wobei das hier skizzierte Verfahren in drei Schritten anvisiert werden könnte, welche gleichfalls zu drei verschiedenen Publikationen führen würden.

<u>Schritt I</u>

- Evaluierung der verschiedenen systemorientierten Risikoanalyse-Tools, insbesondere jenes von Sharit. Unter Umständen muss das Tool von Sharit verbessert und erweitert werden mit anderen systemanalytischen Elementen wie sie andere Experten auf diesem Gebiet – allen voran Vester – aufzeigen.

Schritt II

- Prüfung der Datenlage verschiedener Risiko- und Hochrisikosysteme, vorzugsweise aus dem ersten, zweiten oder vierten Quadranten des Perrowschen Komplexität-Kopplung-Diagramm.
- Praxisbezogene Anwendung des systemorientierten Risikoanalysetools auf zwei verschiedene Risiko- und Hochrisikosysteme, mit gegebenenfalls gleichzeitig iterativer Verbesserung der Methodik.
- Validierung der so berechneten Systemunfall-Eintretenswahrscheinlichkeit mit Hilfe von Konfidenzintervallen von entsprechenden statistischen Test's.

Schritt III

- Entwicklung eines qualitativ-quantitativer Ansatzes für eine technisch-naturwissenschaftliche Risikobewertung, welche den Scholzschen Ansatz des integrierten Risikomanagement und den Perrowschen Gedanken der Risikobewertung gemäss dem Nettokatastrophenpotenzial und den Substitutionskosten eines Hochrisikosystems vereint.
- Vergleich der so erarbeiteten Daten mit jenen Werten, die mit Hilfe herkömmlicher, probabilistischer Risikoanalysemethoden errechnet werden und auch mit den aktuellen Kenntnissen der Sozialpsychologie im Bereich der Risikowahrnehmung.

Annex

Zusatzinformation

Technisches zur Kernenergie

Der *Druckwasserreaktor* (siehe Abb. 6) ist eine Bauform des Kernreaktortyps der Leichtwasserreaktoren. Beim Druckwasserreaktor wird das Wasser in einem Primärkreislauf, der unter erhöhtem Druck (ca.155bar) steht, in den Reaktorkern geleitet, wo es erhitzt wird, aber flüssig bleibt. Von dort fliesst es in einen Dampferzeuger, wo es zum Erhitzen des Wassers im Sekundärkreislauf dient, danach fliesst es wieder zurück in den Reaktorkern. Das Wasser im Sekundärkreislauf verdampft durch die Hitze im Dampferzeuger. Als Dampf wird es über Rohrleitungen einer Turbine zugeleitet, die an einen Generator gekoppelt ist, in dem dann elektrische Energie erzeugt wird. Danach wird das Wasser in einem Kondensator abgekühlt und wieder dem Dampferzeuger zugeführt. Der Druckwasserreaktor ist insofern sehr sicher, da bei einer erhöhten Temperatur des Kühlwassers die Reaktivität abnimmt. Die Moderation der Neutronen wird verringert und die Leistung des Reaktors sinkt. Versagen sowohl die Kühl- als auch die Notfallsysteme so werden durch die Nachzerfallswärme zwar die Brennelemente zerstört, das radioaktive Inventar jedoch vom Containment weiterhin von der Umwelt isoliert.

Der *Siedewasserreaktor* (siehe Abb. 7) gehört wie auch der Druckwasserreaktor zu den Leichtwasserreaktoren. Im Gegensatz zum Druckwasserreaktor ist hier aber kein zweiter Wasserkreislauf vorhanden. Das Wasser wird direkt vom Reaktor, wo es verdampft, über eine Rohrleitung einer Turbine zugeführt, die mittels Generator die elektrische Energie erzeugt.

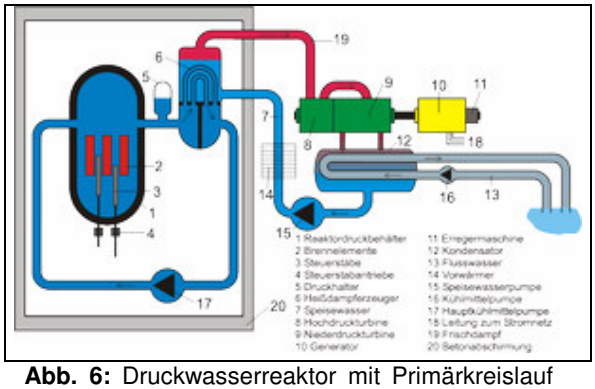

Abb. 6: Druckwasserreaktor mit Primärkreislauf links und Sekundärkreislauf rechts.

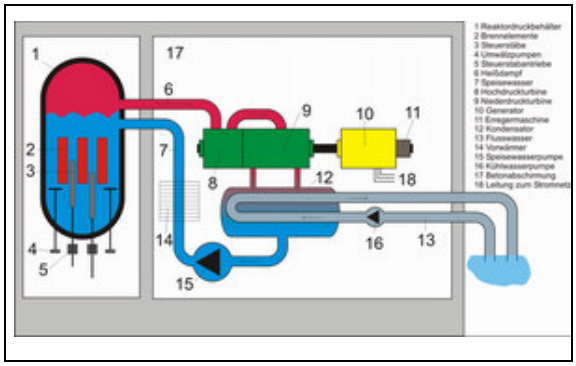

Abb. 7: Siedewasserreaktor mit einem einzigen Kühlwasserkreislauf.

Der *Leichtwasserreaktor* ist ein Reaktortyp, bei dem leichtes Wasser als Kühlmittel und Moderator verwendet wird. Als Brennstoff werden bei diesem Reaktortyp Uran-Brennstäbe mit einem etwa 3%igen Anteil an ^{235}U verwendet.

Der *Schwerwasserreaktor* ist ein Reaktortyp, bei dem schweres Wasser (D_2O) als Kühlmittel und Moderator verwendet wird. Schweres Wasser ist dadurch gekennzeichnet, dass das Wasserstoffatom (H) mit der Massenzahl 1 durch das schwerere Wasserstoffisotop Deuterium (D) mit der Massenzahl 2 ersetzt wird. Als Brennstoff kann bei diesem Reaktortyp Uran mit natürlicher Isotopenzusammensetzung oder auch leicht angereichertes Uran verwendet werden. Eine Anreicherung des ^{235}U-Isotops wie beim Brennstoff für Leichtwasserreaktoren ist also nicht erforderlich. Dies liegt daran, dass die Neutronen in schwerem Wasser weniger stark absorbiert werden als in normalem Wasser und damit die Reaktivität erhöht wird.

Ein *RBMK*[9] ist ein Kernreaktor sowjetischer Bauart, der Mitte der 1960er Jahre entwickelt wurde. Dabei konnte man auf Erfahrungen mit den ersten sowjetischen Kernkraftwerken Obninsk und Bjelojarsk zurückgreifen. Ziel war es, in relativ kurzer Zeit und ohne grössere Investitionen in die Entwicklung neuer Technologien eine grössere Anzahl von Leistungsreaktoren zu errichten. Beim RBMK handelt es sich um einen graphitmoderierten Siedewasser-Druckröhrenreaktor. Anstelle eines Druckbehälters besitzt er eine grosse Anzahl von Druckrohren, in denen sich der Kernbrennstoff befindet. Das Hauptproblem der RBMK ist die Tatsache, dass als Moderator Graphit, als Kühlmittel jedoch Wasser zum Einsatz kommt, im Gegensatz zu Leicht- bzw. Schwerwasserreaktoren, in denen Wasser beide Aufgaben erfüllt. Kommt es zu einer Überhitzung, sodass Wasser verdampft, sinkt die Kühlwirkung. Bei den Wasserreaktoren sinkt gleichzeitig die Moderatorwirkung in einem Mass, dass diese sich in gewissen Grenzen selbst abregeln. Da Graphit aber hitzebeständig ist, nimmt in einem RBMK die Moderatorwirkung bei Überhitzung nicht ab, konstruktionsbedingt kann es sogar zu einer Steigerung kommen.

Ein *Brutreaktor* ist ein Atomreaktor, der nicht nur der Energieerzeugung, sondern auch zur Erzeugung weiteren spaltbaren Materials dient. Natururan enthält zu 99,3% das nicht spaltbare Isotop ^{238}U und nur zu 0,7% das spaltbare Isotop ^{235}U. Für den Betrieb herkömmlicher Kernspaltungsreaktoren muss - technisch sehr aufwändig und teuer - der Anteil ^{235}U vor Herstellung der Brennelemente auf ca. 3-4% angereichert werden. Beim Schnellen Brüter wird ^{238}U durch Neutroneneinfang zunächst in ^{239}U umgewandelt, das dann durch zwei Betazerfälle in spaltbares ^{239}Pu zerfällt. Dadurch erzeugt der Reaktor selbst das nötige Spaltmaterial, allerdings in ausreichender Menge nur in einem Reaktor, der ohne Moderator arbeitet. Die hier vorherrschenden schnellen Neutronen haben dem Schnellen Brüter seinen Namen gegeben. Aufgrund der hohen Temperaturen und des zur Vermeidung der Verstrahlung des Kühlmittels notwendigen niedrigen Neutronenquerschnitts des Kühlmittels wird flüssiges Natrium zur Kühlung verwendet. Im Betrieb ist der Einsatz des Natriums potenziell problematisch. Natrium brennt spontan, sobald es mit Luft in Berührung kommt. Ein kleines Leck im Kühlkreislauf des Reaktors hätte sofort einen Brand zur Folge. Daneben ist ein Natriumbrand nicht leicht unter Kontrolle zu bringen, da Natrium mit Wasser heftig reagiert und dabei zudem noch - ebenfalls höchst brennbares - Wasserstoffgas entsteht. Heutige Feuerwehrtechnik ist bei einem Brand von mehr als einigen hundert Kilogramm Natrium im Wesentlichen machtlos. Grosse Brutreaktoren benötigen aber mehrere Tonnen Natrium.

Mit dem Begriff *Kritikalität* beschreibt man in der Kerntechnik die Neutronenbilanz einer kerntechnischen Anlage. Sie wird zahlenmässig ausgedrückt durch den Multiplikationsfaktor k (Verhältnis von Neutronenerzeugung zu Neutronenverlust) oder die Reaktivität ρ. Überwiegt innerhalb der Neutronenbilanz der Neutronenverlust ($k < 1$), handelt es sich um eine unterkritische Anordnung. Eine kritische Anordnung wird bei ausgeglichener Neutronenbilanz ($k = 1$) erreicht. Ist die Neutronenerzeugung grösser als der Neutronenverlust ($k > 1$), spricht man von einer überkritischen Anordnung. In dieser Situation wir durch die Kernspaltung lokal also mehr radioaktive Strahlung produziert als durch die Spaltung weiterer Atomekerne absorbiert wird. Häufig setzt man den Begriff Kritikalität allerdings auch direkt mit einem ungewollten überkritischen Zustand gleich. In diesem Falle spricht man auch von einem Kritikalitätsstörfall.

Containment bedeutet Eindämmung bzw. Zusammenhalten und bezeichnet unter anderem eine Sicherheitseinrichtung in Kernkraftwerken. Unter dem Begriff Containment wird bei einem Kernkraftwerk eine Sicherheitseinrichtung verstanden, die oft auch als Sicherheitsbehälter bezeichnet wird. Der Containmentbehälter hat die Form einer Kugel. Der Innendurchmesser beträgt beim Siedewasserreaktor in Krümmel beispielsweise etwa 30 Meter, die Wandstärke rund 3 Zentimeter. In einigen Zentimeter Abstand von der Außenwand befindet sich meist noch eine Dichthaut aus Stahl von etwa 4 Millimeter Wandstärke. Der Zwischenraum wird ständig abgesaugt, um eine unkontrollierte Aktivitätsabgabe zu verhindern.

[9] RBMK ist in etwa die russische Abkürzung für Grosskraftreaktor mit Kanälen.

Das Containment stellt eine der technischen Barrieren dar gegen das Austreten radioaktiver Stoffe, insbesondere bei Störfällen. Im Einzelnen sind in einem Kernreaktor (von innen nach außen betrachtet) folgende Barrieren zu nennen:

- Das Kristallgitter des Brennstoffs selbst
- Die Brennstabhülle
- Den Reaktordruckbehälter
- Der Sicherheitsbehälter (Containment)
- Rückhalteeinrichtungen für flüssige und gasförmige Stoffe (z.B. Filter).

Der Sicherheitsbehälter mit den dazu gehörigen Einrichtungen als vierte dieser Barrieren umschließt der Reaktordruckbehälter und den daran anschließenden Teil des Kühlmittelkreislaufs. Es gibt Sicherheitsbehälter mit oder ohne Druckabbausystem. Sicherheitsbehälter mit Druckabbausystem werden bei Siedewasserreaktoren verwendet. Das Druckabbausystem bewirkt, dass bei einer Leckage der austretende Dampf in Wasserbecken geleitet und dort kondensiert wird. Dadurch können solche Sicherheitsbehälter für einen geringeren Druck ausgelegt bzw. kleiner ausgeführt werden. Sicherheitsbehälter ohne Druckabbausystem (Volldrucksicherheitsbehälter) halten dem Druck stand, der beim völligen Ausdampfen des Kühlmittels entsteht.

Historisches zur Kernenergie

Die genauen Abläufe der drei hier beschriebenen Reaktorunfälle sind bis heute nicht zweifelsfrei geklärt. Hier wiedergegeben wird jeweils der Hergang, wie er von "ExpertInnen"-Seite gesichert erscheint. Zum besseren Verständnis kernenergie-spezifischer Ausdrücke ist das vorhergehende Kapitel "Technisches zur Kernenergie" zu lesen.

Seit dem Unfall von Three Mile Island ist Tokai Mura der drittschwerste Atomunfall weltweit. Es wird darüber diskutiert, ob der Unfall auf einer Skala von 7 Schweregraden als Grad 4 oder Grad 5 - wie Three Mile Island - eingereiht werden soll. Der Tschernobyl-Unfall war in dieser IAEA-Klassierung der Unfälle auf Stufe 7 eingereiht worden.

Three Miles Island

Am 28. März 1979 fiel gegen 4 Uhr früh im Block 2 der Kernkraftanlage von Three Miles Island, Pennsylvania, USA, die Hauptpumpe im zweiten nichtradioaktiven Kühlkreislauf dieses *Druckwasserreaktors* aus. Dieser Ausfall verhinderte die Kühlung des Dampferzeugers. Als Folge davon schaltete sich zuerst die Turbine und dann der Atomreaktor ab. Sofort stieg der Druck im Primärsystem (dem radioaktiven Teil) des Reaktors an. Um einen Überdruck zu vermeiden, öffnete sich ein Sicherheitsventil. Dieses Ventil hätte sich wieder schliessen sollen, sobald der Druck um einen bestimmten Wert gefallen war. Dies geschah jedoch nicht. Pro Minute entwich eine Tonne Kühlwasser. Die Anzeigen im Kontrollraum zeigten jedoch nicht an, dass das Ventil noch offen war. Dies führte dazu, dass der Druck im Kühlkreislauf weiter absank. In diesem Moment sprach das Notkühlsystem nicht an, da dieses 42 Stunden vor dem Unfall anschliessend an einen Test nicht wieder geöffnet worden war. Nach 8 Minuten wurde das geschlossene Ventil bemerkt und geöffnet. Nach dem es geöffnet war, begann das Notkühlsystem ordnungsgemäss zu funktionieren und versorgte die Dampferzeuger mit Wasser.

Während der Druck im Primärsystem weiter sank, bildeten sich Luftblasen ausserhalb des Druckbehälters. Aufgrund dieser Luftblasen verteilte sich das Wasser anders und der Druckbehälter füllte sich mit Wasser. Der Füllstandsanzeiger, der dem Bediener anzeigt, wie viel Wasser zum Kühlen vorhanden ist, zeigte fälschlicherweise an, dass das System voll Wasser wäre. So stoppte der Bediener den Wasserzufluss. Er wusste nicht, dass wegen des defekten Sicherheitsventils der Füllstandsanzeiger einen falschen Wert wiedergab.

Nach fast 80 Minuten langsamen Temperaturanstiegs begannen die Pumpen des Primärkreislaufs zu stottern, da nicht mehr Wasser, sondern Dampf angesaugt wurde. Die Pumpen wurden abgeschaltet und man glaubte, dass die natürliche Zirkulation den Wasserfluss aufrechterhalten würde. Doch der Dampf im System der Rohrleitungen blockierte den primären Kühlkreislauf. Das

nicht zirkulierende Wasser verwandelte sich in zunehmendem Masse in Dampf. Nach rund 130 Minuten seit der ersten Fehlfunktion war der obere Teil des Reaktors nicht mehr von Kühlflüssigkeit umgeben. Bei hohen Temperaturen stellt Zirkonium (sehr strahlenhart[10]), welches sich in der Halterung der Brennstäbe befindet, einen Katalysator dar. Das Wasser oder der Wasserdampf reagiert dabei zu Wasserstoff und Sauerstoff. Diese Reaktion fand nun an den sehr heissen Brennstäben statt. Der Kühlbehälter riss und radioaktives Kühlwasser gelangte ins Betriebsgebäude. Um 6 Uhr war Schichtwechsel im Kontrollraum. Die neu Angekommenen bemerkten, dass die Temperatur in den Vorratstanks zu hoch war und nutzten ein Reserveventil, um den Verlust von Kühlwasser zu beenden. Bis zu diesem Zeitpunkt – also bereits 165 Minuten seit dem Beginn des Störfalls – waren schon 950 m³ Kühlwasser aus dem primären Kühlkreislauf entwichen, als dann erstmals radioaktiv verstrahltes Wasser die Sensoren erreichte. Zu diesem Zeitpunkt war die Radioaktivität im primären Kühlkreislauf 300 Mal höher als erwartet.

Den Bedienern im Kontrollraum war nicht bewusst, dass der primäre Kühlkreislauf sehr wenig Wasser enthielt und mehr als die Hälfte des Kerns nicht mehr mit Kühlwasser bedeckt war. Ungefähr 7 Stunden nach dem Beginn wurde neues Wasser in diesen Kühlkreislauf gepumpt. Ein Reserve-Sicherheitsventil wurde geöffnet, um den Druck zu reduzieren. Nach 9 Stunden explodierte der Wasserstoff im Reaktor. Doch dies blieb grösstenteils unbeachtet. Es waren fast 16 Stunden vergangen, als die Pumpen im Primärkreislauf wieder angestellt wurden und die Kerntemperatur zu fallen begann. Ein grosser Teil des Kerns war entweder geschmolzen oder verdampft und das System war immer noch hochradioaktiv.

Während der nächsten Woche wurden sowohl Wasserstoff als auch Wasserdampf aus dem Reaktor entfernt. Dies geschah zum einen durch Kondensatoren, aber auch, was sehr umstritten war, durch einfaches Ablassen in die Atmosphäre. Es wird geschätzt, dass während des Zwischenfalls 45'000Ci[11] an radioaktivem Gas (in Form von Krypton-85) entwichen. Die Beseitigung der Schäden dauerte über 12 Jahre und kostete etwa 1 Milliarde €.

Tschernobyl

Am 26. April 1986 ereignete sich im Block 4 des Kernreaktors Tschernobyl eine katastrophale Kernschmelze und Explosion. Als Auslöser allgemein anerkannt ist eine bauartbedingte Eigenheit des Reaktors (sog. *RBMK-Reaktor*) in Verbindung mit schweren Fehlern der Betreiber der Anlage, welche genau die Prozeduren missachteten und die Sicherheitssysteme abschalteten, die den sicheren Betrieb gewährleisten sollten.

Ausgangspunkt der Katastrophe war ein Experiment, bei welchem geprobt werden sollte, dass bei einem totalen Stromausfall genügend elektrische Leistung zur Verfügung steht, um den Reaktor sicher abzuschalten. Kernreaktoren erzeugen ja nicht nur Strom, sondern verbrauchen auch beispielsweise für den Betrieb der Kühlpumpen, Mess- und Anzeigetechnik usw. erhebliche Mengen an elektrischem Strom. Für den sicheren Betrieb eines Reaktors muss sichergestellt sein, dass diese Minimalenergie jederzeit entweder aus dem Netz oder aus anlageinternen Dieselgeneratoren entnommen werden kann. Bei dem anstehenden Test sollte geprüft werden, ob die Leistung der bei der Abschaltung langsam auslaufenden Turbine die Zeit bis zum Anlaufen von Dieselgeneratoren (etwa 40-60 Sekunden) überbrücken kann. Ein früherer Versuch im Block 3 des Kraftwerks war zuvor gescheitert, weil die Spannung zu schnell absank. Nun sollte es mit einem verbesserten Spannungsregler wiederholt werden.

Als erster Schritt sollte dabei die Leistung des Reaktors von ihrem Nennwert bei 3'200MW auf 1'000MW reduziert werden, wie bei einer Regelabschaltung üblich. Aus bis heute ungeklärten Gründen konnte die Leistung jedoch nicht bei diesem Wert stabilisiert werden, sondern sank weiter

[10] Die Härte von radioaktiver Strahlung gibt ein Mass für deren Durchdringungskraft in der bestrahlten Materie und damit beim Menschen für deren ihre Schädigungswirkung auf die verschiedenen menschlichen Gewebe und Organe.

[11] 1 Curie = $3.7 \cdot 10^{10}$Bq = $3.7 \cdot 10^{10}$sec.$^{-1}$ (radioaktive Zerfälle pro Sekunde).

bis auf nur etwa 30MW. Da die Neutronenflussrate in diesem Bereich extrem niedrig ist, sammelte sich Xenon-135 im Reaktorkern. Dieses Isotop, das durch den Zerfall von Iod-135 entsteht, ist ein sehr guter Neutronen-Absorber. Im normalen Betrieb wird es durch Neutronenaufnahme zu Xenon-136 verbrannt. Bei diesem niedrigen Leistungsniveau jedoch stieg der Xenon-135-Gehalt immer weiter an und vergiftete den Reaktor. Die Operatoren, die in diese Prozesse keine Einsicht hatten, versuchten die gefallene Leistung durch Entfernen weiterer *Regelstäbe* wieder zu steigern. Durch die starke Neutronenabsorbtion gelang es, die vermeintliche Stabilisierung jedoch nur auf einem viel zu niedrigen Niveau von etwa 200MW oder 7% der Nennleistung.

Obwohl sich so zu diesem Zeitpunkt viel weniger Regelstäbe im Kern befanden, als für einen sicheren Betrieb notwendig waren, wurde der Reaktor nicht abgeschaltet sondern das Signal zum Beginn des Testlaufs gegeben. Da für den Test die vier Hauptkühlmittelpumpen die Verbraucher darstellten, wurden diese nun auf volle Leistung geschaltet. Der Reaktor wurde unterkühlt, bis fast gefrorenes Kühlmittel durch den Reaktor floss. Weitere Regelstäbe mussten entfernt werden, um die Leistung zu stabilisieren. Dies wäre der letzte Moment gewesen, an dem man den Reaktor noch durch eine Notabschaltung hätte retten können. Der befand sich zu diesem Zeitpunkt in einem äusserst instabilen Zustand, in dem jede kleinste Veränderung eines Parameters unvorhersehbare Folgen haben konnte. Allein um ihn in diesem Zustand zu betreiben, mussten zuvor alle automatischen Sicherheitssysteme überbrückt werden und die Operatoren mehrere Warnanzeigen ignorieren.

Als nächster Schritt wurde dann das Hauptgasventil der Turbine geschlossen, deren Auslaufenergie man ja messen wollte. Dadurch veränderte sich der Druck im Kühlmittelkreislauf kurzzeitig, Kühlmittel verdampfte. Im Gegensatz zu westlichen Leichtwasserreaktoren, in denen das Kühlmittel gleichzeitig Moderator ist, haben Reaktoren des RBMK-Typs im unteren Leistungsbereich einen positiven sog. Dampfblasen- oder Voidkoeffizienten. Das bedeutet, dass mit zunehmendem Verdampfen des Kühlmittels die Reaktivität des Reaktors steigt. Dadurch begann ein fataler Teufelskreis: Das plötzliche Verdampfen des Kühlmittels lies die Reaktivität in kürzester Zeit in die Höhe schnellen. Das im Kern angesammelte Xenon-135, das bis dahin als zusätzlicher Neutronenabsorber gedient hatte, zerfiel, der Reaktor heizte sich auf und mehr Kühlmittel verdampfte. Die Leistung stieg weiter und weiter an. Schliesslich befahl der Schichtleiter die Notabschaltung des Reaktors.

Dazu wurden alle zuvor aus dem Kern entfernten Steuerstäbe wieder in den Reaktor eingefahren, doch hier zeigte sich ein weiterer Konstruktionsfehler des Reaktortyps: durch die an den Spitzen der Steuerstäbe angebrachten Graphitblöcke wurde bei Einfahren eines vollständig herausgezogenen Stabes die Reaktivität kurzzeitig erhöht (Graphit ist ja der eigentliche Moderator der Reaktion). Die durch das gleichzeitige Einführen aller Regelstäbe (über 250) massiv gesteigerte Neutronenausbeute liess die Leistung in Millisekunden explorieren. Die Hitze verformte die Kanäle der Regelstäbe, sodass sie nicht weit genug in den Reaktorkern eindringen konnten, um ihre angedachte Wirkung zu entfalten.

Die Hitze liess die Brennelemente reissen und mit dem umgebenden Wasser reagieren. Wasserstoff und Sauerstoff entstanden in grossen Mengen. Schliesslich riss der Druck des verdampfenden Kühlmittels das über 1'000 Tonnen schwere Dach der Reaktorhalle weg. Das Graphit des Reaktorkerns fing durch die einströmende Frischluft sofort Feuer und liess das entstandene Knallgas explodieren. Grosse Mengen an Radioaktivität wurden durch die Explosionen und den anschliessenden Brand des Graphit-Moderators in die Umwelt freigesetzt. Insbesondere das leicht flüchtige Iod-131 und Cäsium-137 bildeten gefährliche Aerosole, die in einer radioaktiven Wolke teilweise hunderte oder gar tausende Kilometer weit getragen wurden, bevor sie der Regen aus der Atmosphäre auswusch. Radioaktive Metalle mit höherem Siedepunkt wurden hingegen vor allem in Form von Staubpartikeln freigesetzt, die sich in der Nähe des Reaktors niederschlugen.

Um den Brand zu löschen und damit auch die Freisetzung radioaktiver Stoffe zu stoppen, pumpten Feuerwehrleute in den ersten zehn Stunden nach dem Unfall Kühlwasser in den Reaktorkern. Nach zehn Stunden wurde dieser Löschversuch erfolglos abgebrochen. Vom 27. April bis zum 5. Mai flogen mehr als 30 Militärhubschrauber über den brennenden Reaktor. Sie warfen unter anderem

2'400 Tonnen Blei und 1'800 Tonnen Sand ab. Damit sollte der Brand erstickt und die Strahlung abgeschirmt werden. Diese Effekte wurden jedoch nicht erreicht. Im Gegenteil, unter dem abgeworfenen Material staute sich die Wärme. Die Temperatur im Reaktor stieg wieder an, und damit auch die Menge der austretenden Radioaktivität. In einer letzten Löschphase wurde der Reaktorkern mit flüssigem Stickstoff gekühlt. Erst ab dem 6. Mai waren der Brand und die radioaktive Emission unter Kontrolle.

Die für die Löscharbeiten eingesetzten 600 Männer der Werksfeuerwehr und des Betriebspersonals sind die am höchsten verstrahlte Personengruppe. 134 von ihnen erhielten Dosen an Radioaktivität zwischen 0,7 und 13Sv[12]. Das heisst, sie erhielten innerhalb von Stunden eine Strahlungsmenge ab, die bis zu 13'000 mal über dem Wert von 1mSv liegt, dem in der Europäischen Union gültigen Grenzwert für die effektive Dosis, der Einzelpersonen aus der Bevölkerung durch ein Kernkraftwerk in einem Jahr ausgesetzt werden dürfen. 203 Menschen wurden sofort ins Krankenhaus eingeliefert, 31 Helfer starben nach kurzer Zeit. Insgesamt waren an den Aufräumungsarbeiten in Tschernobyl bis 1989 rund 800'000 Männer beteiligt, die bis heute unter den gesundheitlichen Folgen dieser Einsätze leiden. 300'000 von ihnen sollen Strahlendosen von mehr als 0,5Sv erhalten haben. Wie viele von ihnen an den Folgen bisher gestorben sind, ist umstritten. Nach Angaben staatlicher Stellen der drei betroffenen Staaten der früheren Sowjetunion sind bisher rund 25'000 Liquidatoren gestorben. 135'000 Menschen wurden aus der Umgebung evakuiert, darunter 45'000 aus der nahe gelegenen Stadt Pripjat. Es wird sehr widersprüchlich beurteilt, welche gesundheitlichen Folgen von der Verstrahlung herrühren. Es ist jedoch eindeutig, dass der sprunghafte Anstieg der Schilddrüsenkrebserkrankungen seit 1987 aufgrund seiner Ausmasse nur auf die Katastrophe von Tschornobyl zurückgeführt werden kann.

Tokai Mura

Der *Kritikalitätsunfall* in der JCO-Uranium-Konversionsfabrik in Tokai Mura, Japan, ereignete sich am 30. September 1999, um 10.35 Uhr. Die JCO ist eine von zwei japanischen Firmen, die Atombrennstoff herstellen. Die JCO produziert unter anderem auch jährlich 715 Tonnen Brennmaterial für Leichtwasserreaktoren, und seit Herbst 1998 auch für den experimentellen *Schnellen Brüter* Joyo.

Was genau ablief, ist heute noch nicht bis in alle Details geklärt, doch scheint, dass die Arbeiter 16 Kilogramm relativ hoch angereichertes Uran, das 18,8% des spaltbaren Uranisotops ^{235}U enthielt, in einen Präzipitationstank einfüllten. Eigentlich hätten sie aber nur maximal 2,4kg Uran dieser Isotopenanreicherungsqualität in den Tank füllen dürfen. Dies führte dazu, dass im Tank eine kritische Masse entstand und eine unkontrollierte radioaktive Kettenreaktion begann. Möglicherweise hatten die JCO-Arbeiter die Checkliste verwechselt und mit einer Liste für Leichtwasserreaktoren gearbeitet. Der Brennstoff für Leichtwasserreaktoren enthält nämlich nur 5 Prozent des spaltbaren Uran-235. Maximal 16 kg dieses Uranmixes dürfen zusammengeschüttet werden, da das spaltbare Uran-235 weniger konzentriert ist und deshalb bis zu einer Menge von 16 kg keine Kritikalität verursachen kann.

Bis heute ist auch unklar, in welcher Form sich das Uran befand und welche Lösung im Tank war. Es scheint unbestritten, dass im Doppelwandzylinder des Tanks Wasser zirkulierte, das die Wärme – die bei einer derartig *exothermen* chemischen Reaktion entsteht – hätte abführen sollen. Wahrscheinlich sollte Uranoxid (U_3O_8) in Salpetersäure (HNO_3) aufgelöst werden, damit Urannitrat entsteht. In einem weiteren Schritt hätte man daraus wohl Uranoxid (UO_2) gewinnen wollen, welches man zu Brennstoff-Tabletten presst.

Im Grunde genommen war die Situation im Präzipitationstank vergleichbar mit einem Reaktor: Das Wasser im Kühlmantel wirkte als Neutronenreflektor, moderierte also eine zunehmende Ketten-

[12] 1 Sievert = 100 rem = $1Jkg^{-1}$ (erhaltene Energiedosis pro Körpermasse). 10Sv ist die Ganzkörperdosis, die einem Knochenmarksempfänger vor der Knochenmarkstransplantation verabreicht wird, mit dieser Dosis wird das Knochenmark des Patienten vollständig eliminiert. Die in der Schweiz erlaubte Dosis für Ausnahmefälle liegt bei 50 mSv.

reaktion. Der Unterschied zu einem Reaktor war einzig: Im Urantank lief dieser Vorgang unkontrolliert ab, der Tank konnte nicht als Reaktordruckgefäss dienen und das Gebäude nicht als zweite Barriere im Sinne eines *Containments*. Das Gebäude war nicht in der Lage radioaktive Gase zurückzuhalten.

Drei der Arbeiter waren tödlichen bis annähernd tödlichen Dosen von Radioaktivität ausgesetzt. Die nachträgliche Dosimetrie zeigte, dass ein 35-jähriger Mann 17Sv abbekommen hatte, ein 39-Jähriger 10Sv und ein 54-Jähriger 3Sv. Die beiden Schwerstbestrahlten wurden einer Nabelvenenbluttransplantation unterzogen und sind inzwischen verstorben, der erste im Dezember 1999, der zweite im April 2000. Weitere 18 Arbeiter wurden mit Dosen von 20 bis 103mSv bestrahlt, dies innerhalb von zwei bis drei Minuten. Erlaubte Dosis für Ausnahmefälle wäre in Japan für Notfallaktionen 100mSv. Insgesamt bekamen 55 Menschen nachweislich überhöhte Strahlendosen ab.

Mehr als 4 Stunden nach Beginn der Kettenreaktion wurden 150 EinwohnerInnen aus 50 Haushalten evakuiert. An der Grenze der Evakuationszone (Umkreis von 350 Metern) mass man eine erhöhte Strahlung von 840 µSv/h (zum Vergleich: Die Strahlung im Mittelland beträgt 0,075 µSv/h). Nach 7 Stunden 55 Minuten wurden 310‘000 Einwohner im Umkreis von 10 Kilometern aufgefordert, in ihren Wohnungen zu bleiben und Fenster und Türen geschlossen zu halten. 19 Stunden 5 Minuten nach dem Unfall erreichte die Radioaktivität bei der Anlage 18 mSv/h Neutronen- und 20 mSv/h Gammastrahlung, was fünf Mal mehr war als 12 Stunden früher. 20 Stunden und 25 Minuten nach Beginn des Unfalles deklarierte die "Science and Technology Agency", dass die Kritikalität aufgehört habe, Borwasser sei in den Tank gepumpt worden, die Kettenreaktion sei gestoppt. Die Neutronenzähler am Unfallort registrierten langsam absinkende Neutronenwerte.

Es kam aber nicht nur zur Direktstrahlung aus der Anlage der JCO. Durch den Spaltprozess wurden auch radioaktive Isotope wie Strontium-91 (0,021Bq/m^3 in der Luft 900m südöstlich der Anlage), Iod-131 (20Bq/m^3 in der Luft und 54,7Bq/kg auf Blättern 100 m von der Anlage entfernt), Natrium-24 (64Bq/kg 300m westlich der Anlage und 1,7Bq/kg 3km westlich der Anlage) aber auch Cäsium-137 in erheblichen Mengen freigesetzt[13].

Statistisches zur Kernenergie

Zum heutigen Zeitpunkt stehen auf dem gesamten Globus 440 Reaktoren unterschiedlicher Bauarten (siehe erstes Kapitel des Annex'). Für alle Reaktoren zusammen weist die Kernenergiebranche eine Betriebserfahrung (bezeichnet mit n) von ca. 9'000 Reaktorjahren aus. Seit Beginn der Atomtechnologie ereigneten sich weltweit drei grosse Unfälle (k), bei welchen beträchtliche Mengen radioaktives Material in die Umwelt gelangten (siehe vorhergehendes Kapitel). Dem gegenüber steht die Eintretenswahrscheinlichkeit von entsprechend gravierenden Unfällen (p_0), die von "ExpertInnen" mit Hilfe von probabilistischen Risikoanalysemethoden auf ca. 1:1'000'000 berrechnet wird (siehe Abb. 5 Durchschnitt der dunkel gefärbten Balkenabschnitte).

Für *binomial* verteilte Ereignisse (X := # Ereignisse = Bin(n=9'000a, $p_0=10^{-6}a^{-1}$)), wie dies Reaktorunfälle oder andere Störfälle darstellen, kann man die Nullhypothese H_0 "die beobachtete, relative Häufigkeit eines Ereignisses E entspricht der angenommenen, berechneten Wahrscheinlichkeit p_0 (oder: $P(E) = p_0$)" mit einem einseitigen u-Test prüfen, so fern die Anzahl unabhängiger Wiederholungen (n) eines Versuchs (hier also der Versuch, ob grob gesagt: " e i n Reaktor während e i n e m Jahr Laufzeit in die Luft geht oder nicht") einen bestimmten, von p_0 abhängigen Grenzwert überschreitet:

[13] Der für ^{131}Jod erlaubte Wert liegt bei 10Bq/m^3.

Für: $$n \geq \frac{9}{p_0 \cdot (1 - \cdot p_0)} \quad (1)$$

gilt: $$u = \frac{k - n \cdot p_0}{\sqrt{n \cdot p_0 \cdot (1 - \cdot p_0)}} \quad (2)$$

Bei einem Signifikanzniveau α von 1% muss die Nullhypothese H_0 verworfen werden, wenn:

$$|u| > u_{1-\alpha} = 2{,}326 \quad (3)$$

Setzt man den oben angegeben Wert $p_0=10^{-6}a^{-1}$ in die Formel (1) ein, ergibt dies:

$$\frac{9}{p_0 \cdot (1 - \cdot p_0)} = 9'000'009 \text{ a}$$

Da diese Zahl wesentlich grösser ist als die Reaktorlaufjahre n = 9'000a, ist im vorliegenden Fall die Voraussetzung für ein solches Testverfahren nicht gegeben. Da die Anzahl Ereignisse aber relativ wenige sind, kann die Wahrscheinlichkeit der oben beschriebenen Nullhypothese auch problemlos direkt berechnet werden.

Die Wahrscheinlichkeit, dass sich während der Beobachtungsperiode drei oder mehr Unfälle ereignen, entspricht der Summe aller möglichen Ereignisse abzüglich der Wahrscheinlichkeiten, dass nur zwei Unfälle oder dass nur ein Unfall oder dass gar kein Unfall eintritt:

$$P_{p_0}[X \geq 3] = 1 - P[X = 0] - P[X = 1] - P[X = 2] \quad (4)$$

Gemäss der Newtonschen Formel (5) kann also die Wahrscheinlichkeit für die Fälle X = 0, X = 1 und X = 2 mit k = 0, 1 und 2 und n = 9'000a und $p_0 = 10^{-6}a^{-1}$ exakt berechnet werden:

$$P[X = k] = \binom{n}{k} p_0{}^k (1 - p_0)^{n-k} = \frac{n!}{k!(n-k)!} p_0{}^k (1 - p_0)^{n-k} \quad (5)$$

mit: k = 0 → $P[X = 0] = 0{,}991$

k = 1 → $P[X = 1] = 0{,}00892$

k = 2 → $P[X = 2] = 0{,}0000401$

Bereits die Wahrscheinlichkeit, dass bei einer theoretischen Eintretenswahrscheinlichkeit von $10^{-6}a^{-1}$ in 9'000 Jahren Reaktorlaufzeit gerade ein oder mehr Unfälle grösseren Ausmassens eintreten, liegt klar unter dem Signifikanzniveau von 1%. Die Wahrscheinlichkeit, dass sogar drei oder mehr Unfälle grösseren Ausmassens eintreten, liegt demgemäss weit unter 0,1‰:

$$P_{p_0}[X \geq 1] = 1 - P[X = 0] \leq 0{,}01$$

$$P_{p_0}[X \geq 3] = 1 - P[X = 0] - P[X = 1] - P[X = 2] \leq 0{,}0001$$

Demzufolge muss die Nullhypothese "P(E) = p_0" verworfen werden. Das heisst, es ist sehr unwahrscheinlich, dass die von den "RisikoexpertInnen" berechnete Eintretenswahrscheinlichkeit von Reaktorunfällen grösseren Ausmassens p_0 tatsächlich bei 1:1'000'000 liegt. Im Gegenteil, es muss angenommen werden, dass die reale Eintretenswahrscheinlichkeit solcher Unfälle wesentlich grösser ist, d.h. dass diese Ereignisse in Wahrheit wesentlich häufiger zu erwarten sind als einmal auf eine Million Reaktorlaufjahre.

Begriffserläuterungen

Binomial verteilte Ereignisse können per Definition immer nur entweder eintreten oder nicht eintreten. Man spricht demgemäss auch von 0/1-Ereignissen, da das Ereignis nur entweder den Wert 0, oder den Wert 1 "annehmen" kann.

Bionik bezeichnet die Wissenschaft, welche elektronische Probleme nach dem Vorbild biologischer Funktionen zu lösen versucht.

Mit *Biokybernetik* wird einerseits die selbststabilisierende Entwicklungsweise natürlicher Systeme und andererseits auch die Wissenschaft selbst, welche sich mit den Gesetzmässigkeiten der Steuerung und Regelung dieser lebenden Systeme befasst, bezeichnet.

Common-Mode-Fehler sind Störfalle, die in einer direkten Kausalität von einander generiert werden. Es sind also Fehler, die vom System in Abhängigkeit von einander generiert werden, in der Sprache der Statistik sind es also von einander abhängige Ereignisse.

Ein *Ereignisstrang* bezieht sich auf die Abfolge von Einzelereignissen (*Störfällen*), die zusammenwirkend zu einem *Unfall* führen, im Sinn von: "Zuerst fällt Komponente A aus (mit Häufigkeit X), dann passiert B (mit Häufigkeit Y), zusammen führt dies dazu, dass Sicherheitssystem C anspringen müsste, was aber mit einer Wahrscheinlichkeit von Z nicht passiert, was wiederum zu usw., usw. führt, bis dies alles dann schlussendlich den betrachteten Störfall verursacht". Für anschaulichere Beispiele von derartigen Ereignissträngen siehe Kapitel "Historisches zur Kernenergie" im Annex. Jeder spezifische Unfall kann in der Regel durch unterschiedliche Ereignisstränge herbeigeführt werden. Die Summe dieser Teilwahrscheinlichkeiten der unterschiedlichen Ereignisstränge ergibt dann die Eintretenswahrscheinlichkeit des betrachteten Unfalls (siehe Fehlerbaum unter "*Top-Down-Riskobetrachtungen*", Abb. 8).

Bei *exothermen* chemischen Reaktionen wird jeweils mehr Reaktionenergie in Form von Wärme freigesetzt als diese verbraucht. Damit lauft eine exotherme Reaktion, einmal initiiert, von alleine ab.

Die Theorie der *'fuzzy logic'* besagt, dass in der Systemanalyse ein gewisses Mass an Unschärfe in der Datendichte zu einem echten Informationsgewinn führt. Grund dafür ist die durch diese Methodik erwirkte Mustererkennung, die sich einerseits von einer Datenreduktion auf die wesentlichen Schlüsselparameter, als auch von der Vernetzung dieser Teilinformationen zu einem konsistenten Gesamtbild ableitet und damit zu einem vollständigeren Systemverständnis verhilft.

Hochrisikosysteme charaktrisieren sich gemäss Charles Perrow durch einen hohen Kompklexitätsgrad und eine starke (positive) Kopplung der verschiedenen darin stattfindenen Abläufe. Auf dieser beiden Eigenheiten weisen sie eine erhöhte, systemimmanente Anfälligkeit für Systemunfälle auf. Beispiele für Hochrisikosysteme finden sich in Abb. 4 auf Seite 6 des vorliegenden Projektbeschriebs.

Katastrophen stellen Unfälle dar, welche die Leben Hunderter von Menschen auslöschen und jene von Tausenden verkürzen oder in ihrer Qualität schmälern.

Komponentenunfälle bedeuten den Ausfall mindestens einer Komponente (Teil, Einheit oder Subsystem), dessen unmittelbare Folgeschäden auf Grund des Betriebsablaufs vorhersehbar sind. *Systemunfälle* dagegen bedeuten den Ausfall mehrerer Komponenten, wobei zwischen den einzelnen Defekten Wechselwirkungen auftreten, die nicht vorhersehbar sind. Dazu gehören mindestens zwei Störungen, die weitgehend unabhängig von einander in verschiedenen Einheiten und Subsystemen auftreten und die zu Interaktionen führen.

Mit *Kybernetik* (vom griechischen *kybernetes*, der Steuermann) wird die Erkennung, Steuerung und selbsttätige Regelung ineinandergreifender, vernetzter Abläufe bei minimalem Energieaufwand bezeichnet. Kybernetisch funktionierende Systeme werden also über selbstregulierende Prozesse gesteuert. Dabei lässt sich das Gesamtsystem nur noch auf der Ebene ganzer Systemaggregate kontrollieren, nicht aber auf jener der einzelnen Systemteile.

Murphy's Law, zu Deutsch das Gesetz von Murphy, ist kein eigentlich naturwissenschaftlich formuliertes Gesetz (Mr. Murphy war Militärpilot und keineswegs Mathematiker). Dennoch animiert

es immer wieder Naturwissenschafter verschiedener Provenienzen, die Logik dieses antiintuitiven Paradigmas in einzelnen seiner Erscheinungsbildern zu verstehen. Das viel zitierte Gesetz besagt, dass etwas schief gehen wird, wenn es nur eine Möglichkeit gibt, dass es schief geht. Laut Frederic Vester gibt es noch zwei weitere Sätze dieses Gesetzes, die in der breiten Bevölkerung weniger bekannt sind: Etwas wird auch dann noch schief gehen, wenn es eigentlich gar keine Möglichkeit gibt, dass es schief gehen kann, und, sollte etwas tatsächlich nicht schief gehen, wird man später feststellen, dass es besser gewesen wäre, wenn es schief gegangen wäre.

Als *Negative Rückkopplung* wird die Funktionsweise eines Systems genannt, welche über interne Regelkreise bewirkt, dass bei Abweichen eines Systemparameters von seinem Sollwert auf Grund systemexterner Störungen dieser wieder in seinen ursprünglichen Wert zurück pendelt (i. e. stellt der Messfühler einen zu hohen Wert fest, so wird dieser durch das Stellglied verringert, ist der Wert zu niedrig, so wird er erhöht). *Regelkreise* ermöglichen einem System, Störgrössen, welche von aussen auf einen empfindlichen Systemteil, also auf die 'Regelgrösse' treffen, aufzufangen und diese Störung selbsttätig auszugleichen oder sogar zu integrieren. Bei einer derartigen Selbstregulation werden die Sollwerte natürlicher Systeme automatisch in einem systemverträglichen Bereich gehalten. Das System wird damit fehlerfreundlich, robust gegen Störungen und immun gegen Schwankungen in seinem Umfeld. *Positive Rückkopplung* bedeutet systemmechanistisch das Gegenteil: Wird ein Systemparameter nach oben oder nach unten ausgelenkt, so unterstützt das System selbst dieses Signal und lenkt den Systemparameter durch interne Kräfte zusätzlich zur externen Störung in die selbe Richtung aus (i. e. ein nach oben veränderter Wert wird über den Regler noch weiter erhöht, ein nach unten ausgelenkter noch weiter nach unten gedrückt).

Das *Nettokatastrophenpotenzial* wird aus drei Systemeigenschaften berechnet, welche sowohl die systemimmanente Eintretenswahrscheinlichkeit eines katastrophalen Ereignisses, als auch dessen Schadensausmass integrieren: Nettokatastrophenpotenzial = Neigung eines Systems zu Systemunfällen mit katastrophalen Auswirkungen in Folge technischer Fehlleistungen ∩ Neigung eines Systems zu Systemunfällen mit katastrophalen Auswirkungen in Folge organisatorischer Fehlleistungen ∩ jeweiliges Katastrophenpotenzial, welches einzig aus Komponentenunfällen resultiert.

Präzision bezeichnet die durchschnittliche Abweichung von Messwerten von deren ihrem Mittelwert, genannt Standardabweichung eines Messwerts. Die Messgenauigkeit dagegen gibt an, wie weit der gemessene Mittelwert von dem realen, nie abschliessend bekannten Wert abweicht.

Redundante Systeme weisen eine mehrfache Kennzeichnung derselben Information auf, sodass beim Wegfallen eines dieser Informationselemente die Gesamtinformation weiterhin gesichert ist.

Ein *Regelstab*, oder auch Steuerstab genannt, dient zur Regelung und zur Abschaltung eines Kernreaktors. Wenn sich ein Regelstab im Reaktorkern befindet, absorbiert er einen Teil der durch die Kernspaltung freigesetzten Neutronen, sodass diese nicht für weitere Kernspaltungen zur Verfügung stehen. Auf diese Weise wird das unkontrollierte Anwachsen der Kettenreaktion im Reaktor verhindert. Die Leistung eines Neben anderen Möglichkeiten zur Regelung eines Kernreaktors kann also durch das mehr oder weniger tiefe Einfahren der Steuerstäbe in den Reaktorkern geregelt werden. Durch das vollständige Einfahren der Steuerstäbe kann die Kettenreaktion völlig unterbunden und der Reaktor abgeschaltet werden. Im Normalbetrieb befindet sich immer ein Teil der in einem Kernreaktor vorhandenen Steuerstäbe ausserhalb des Reaktorkerns, um im Notfall den Reaktor sicher abschalten zu können.

Störfälle betreffen Schäden oder Ausfälle einzig an Teilen oder Einheiten eines Systems, selbst wenn dadurch die Funktion des Gesamtsystems völlig unterbrochen oder so sehr beeinträchtig wird, dass es abgeschaltet werden muss. *Unfälle* dem gegenüber betreffen Schäden oder Ausfälle an Subsystemen oder am System insgesamt, die zur völligen Unterbrechung des Funktionsablaufs des Systems führen oder diesen so sehr beeinträchtigen, dass das System sofort abgeschaltet werden muss.

Systeme werden in vier Ebenen unterschiedlicher Komplexität eingeteilt: Teile, Einheiten, Subsysteme und das System selbst.

Top-Down-Riskobetrachtungen gehen von einem Komponenten- oder Systemunfall aus, von welchem den Betrachtenden interessiert, welche zuvor eingetretenen Störfallereignisse dazu geführt haben. *Bottom-Up-Riskobetrachtungen* gehen demgegenüber von einem Störfallereignis aus, von welchem interessiert, welche möglichen nachfolgenden Komponenten- oder Systemunfälle, oder gegebenenfalls auch Schäden an Mensch und Umwelt es induzieren kann.

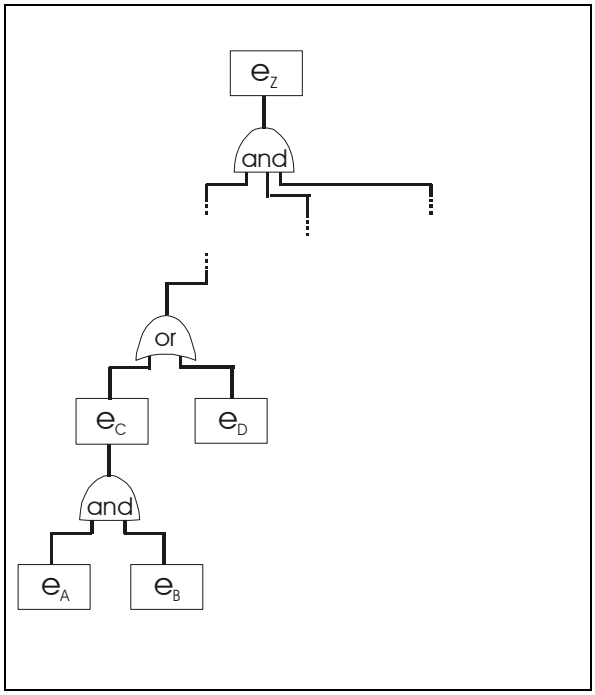

Abb. 8: Top-down Analyse, deduktive Analyse, bzw. Fehlerbaum sind synonyme Fachausdrücke für das gleiche methodische Vorgehen: Es wird untersucht, welche unterschiedlichen Ereignisse e_A, e_B, e_C, etc. jeweils das untersuchte finale Ereignis e_Z verursachen können.

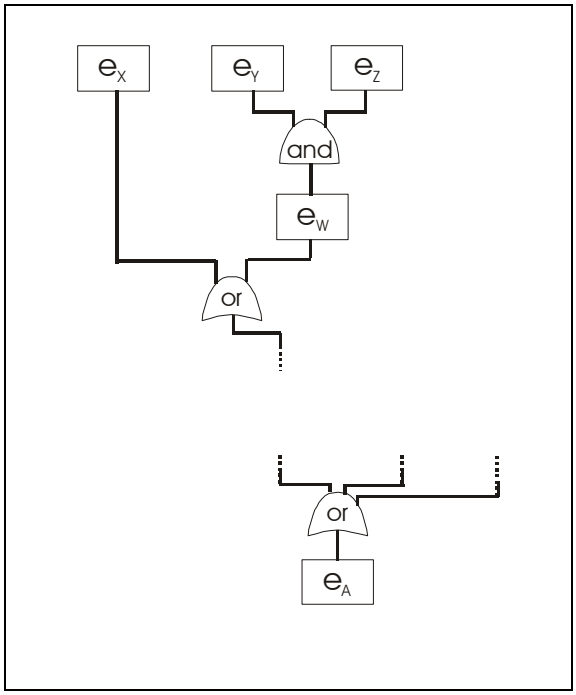

Abb. 9: Bottom-up Analyse, induktive Analyse, bzw. Ereignisbaum sind synonyme Fachausdrücke für das gleiche methodische Vorgehen: Es wird untersucht, welche unterschiedlichen Ereignisse e_Z, e_Y, e_X, etc. durch das untersuchte initiale Ereignis e_A verursachen kann.

Unifinalität bedeutet, dass das Produkt eines Prozesses nur über eine klar vordefinierte Abfolge von Teilprozessen fertiggestellt werden kann. Dem gegenüber kann das Produkt eines *äquifinalen* Verfahrensprozesses auf verschiedenen, gleichwertigen Wegen fertiggestellt werden.

Bibliografie

Beck U. (1986): Die Risikogesellschaft; Auf dem Weg in eine neue Moderne. Suhrkamp Verlag, Frankfurt a. M.

Dörner D. (1992): Die Logik des Misslingens; Strategisches Denken in komplexen Situationen. Rowohlt Verlag GmbH, Reinbek bei Hamburg.

Dörner D. & Schaub H. (1995): Handeln in Unbestimmtheit und Komplexität. Organisationsentwicklung, vol. 3, pg. 34-47.

Dörner D. (1980): On the Difficulties People have in dealing with complexity. Simulation & Gaming, vol. 11, iss: 1, pg. 87.

Dörner D. (1975): Wie Menschen eine Welt verbessern wollten, und sie dabei zerstörten. Bild der Wissenschaft, Februar, pg. 48-53.

Fischhoff B., Slovic P. & Lichtenstein S. (1978): How safe is safe enough? A psychometric Study of Attitudes towards technological Risks and Benefits. Policy Sciences, vol. 9, pg. 127-152.

Guggenberg B. (1987): Das Menschenrecht auf Irrtum; Anleitung zur Unvollkommenheit. Carl Hanser Verlag, München, Wien.

Guggenberg B. (1987): Das Menschenrecht auf Irrtum; Anleitung zur Unvollkommenheit. Universitas, vol. 4, pg. 307-317

Gran B. A. et al. (2004): An Approach for Model-Based Risk Assessment. Computer Safety, Reliability and Security, Proceedings Lecture Notes in Computer 3219, pg. 311-324.

Hacker W. (1986): Arbeitspsychologie: Psychische Regulation von Arbeitstätigkeiten. Huber, Bern.

Hungerbühler K., Ranke J. & Mettier T. (1999): Chemische Produkte und Prozesse: Grundkonzepte zum umweltorientierten Design. Springer-Verlag, Heidelberg.

Kohda T. & Inoue K. (2004): A Simplified Risk Analysis Method of Complex Systems using the Global System Model. Annual Reliability and Maintainability Symposium, pg. 397-404.

Kröger W. (2004): Risk Analysis and Protection Strategies for Operation of Nuclear Power Plants. In press.

Kröger W. (2000): Balancing Safety and Economics. Nuclear Engineering and Design, vol. 195, pg. 101-108.

Kröger W. (1990): Basic Risk Analyses for High-Temperature Reactors. Nuclear Engineering and Design, vol. 121, pg. 299-309.

Kühle H. J. & Badke P. (1986): Die Entwicklung von Lösungsvorstellungen in komplexen Problemsituationen und die Gedächtnisstruktur. Sprache & Kognition, vol. 2, pg. 95-105.

Modarres M. (1999): Functional Modeling of Complex Systems with Applications. Annual Reliability and Maintainability Symposium, pg. 418-425.

Okrent D. (1984): Industrial Risks. Proceedings of the Royal Society of London. Series A, vol. 376 (Mathematical and Physical Sciencies), London.

Okrent D (1981): Nuclear Reactor Safety: On the History of the Regulatory Process. The University of Wisconsin Press, Madison - Wisconsin & London.

Perrow C. (2004): A personal note on Normal Accidents. Organization & Environment, vol. 17, iss. 1, pg. 9-14

Perrow C. (1986): The Habit of courting Disaster. The Nation, vol. 243, iss. 11, pg. 329-356.

Perrow C. (1984): Normal Accidents: Living with High-Risk Technologies. Campus Verlag, New York.

Perrow C. (1981): Normal Accident at Three Mile Island. Society, vol. 18, pg. 17-26.

Schaub H. & Strohschneider S. (1992): Die Auswirkungen unterschiedlicher Problemlöseerfahrung auf den Umgang mit einem unbekannten komplexen Problem. Zeitschrift für Arbeits- und Organisationspsychologie, vol. 36, pg. 117-126.

Scholz R. W. & Tietje O. (2002): Embedded Case Study Methods: Integrating Quantitative and Qualitative Knowledge. Sage publications, London.

Sharit J. (2000): A Modeling Framework for Exposing Risks in Complex Systems. Risk analysis, vol. 20, no. 4, pg. 469-482.

Slovic P. et al. (2004): Risk as Analysis and Risk as Feelings:Some Thoughts about Affect, Reason, Risk and Rationality. Risk Analysis, vol. 24, iss. 2, pg. 311-322.

Slovic P. (2004): The Sociopolitics of Risk: Challenges for Risk Assessment. Toxicology, vol. 202, iss. 1-2, pg. 33-127.

Slovic P. (2001): The Perception of Risk. Earthscan, London.

Slovic P. (2001): The Risk Game (Reprinted from 'The Risk Game' (1998)). Journal of Hazardous Materials, vol. 86, pg. 17-24.

Slovic P. (1999): Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield. Risk Analysis, vol. 19, iss. 4, pg. 689 (reprinted from Environment, Ethics, and Behavior, 1997, pg 277-313).

Slovic P. (1993): Perceived Risk, Trust, and Democracy. Risk analysis, vol. 13, pg. 675-682.

Slovic P. (1987): Perception of Risk. Science, vol. 236, pg. 280-285.

Slovic P., Fischhoff B. & Lichtenstein S. (1984): Behavioral Decision Theory Perspectives on risk and safety. Acta Psychologica, vol. 56, pg. 183-203.

Starr C. (1969): Social Benefits versus Technological Risk: What is our Society willing to pay for Safety? Science, vol. 165, pg. 1232-1238.

Stone E. R., Yates J. F. & Parker A. M. (1994): Risk communication: Absolute versus relative expressions of low-probability risks. Organizational Behavior and Human Decision Processes, vol. 60, pg. 387-408.

Ternov S. & Akselsson R. (2004): A method, DEB analysis, for proactive risk analysis applied to air traffic control. Safety Science, vol. 42, iss. 7, pg. 657-673.

Vester F. (2001): Die Kunst vernetzt zu denken; Ideen und Werkzeuge für einen neuen Umgang mit Komplexität. Deutsche Verlags-Anstalt GmbH, Stuttgart.

Vraalsen F. et al. (2005): The CORAS Tool for Security Risk Analysis. Trust Management, Proceedings Lecture Notes in Computer Science 3477, pg. 402-405.

Websites

http://de.wikipedia.org/wiki/Liste_der_nuklearen_Unfälle

http://de.wikipedia.org/wiki/Three_Mile_Island

http://www.chernobyl.info/index.php?navID=167&projectID=48

http://www.ippnw.ch/content/pdf/2000_2/Gau_in_Tokaimura.pdf