Zeitschrift: Schweizer Ingenieur und Architekt
Herausgeber: Verlags-AG der akademischen technischen Vereine
Band: 108 (1990)
Heft: 37

Artikel: Risikobestimmung - Eine Bestandesaufnahme der Methodik für Kernkraftwerke
Autor: Kröger, Wolfgang / Chakraborty, Sabyasachi
DOI: https://doi.org/10.5169/seals-77502

Sicherheit und Risiko

Risikobestimmung –

Eine Bestandsaufnahme der Methodik für Kernkraftwerke

Das Risiko, das mit dem Einsatz technischer Systeme verbunden ist, beschäftigt zunehmend die Fachwelt und die Öffentlichkeit. In der Kerntechnik dominiert die Sicherheitsforschung längst die Forschung insgesamt; zukünftige Reaktoren werden noch stärker als bisher unter das Primat der Sicherheit gestellt. Nach dem Leitsatz «What can happen will be» geht die Öffentlichkeit zwangsläufig vom Eintreten denkbarer Szenarien aus und macht deren denkbare Konsequenzen oft zum alleinigen Beurteilungsmasstab; – die erreichte Sicherheit oder der Nutzen bleiben weitgehend ausser acht. Aus fachlicher Sicht ist die verlässliche Bestimmung des Risikos eine wichtige Aufgabe und die Voraussetzung für den sachgerechten Umgang mit Technik.
Der folgende Beitrag ist ein Versuch, Begriffe und Methodik zu erläutern und am Beispiel der Kernenergie den erreichten Stand der Technik zu beleuchten, d.h. Möglichkeiten und Grenzen der Risikobestimmung aufzuzeigen.

VON WOLFGANG KRÖGER, ZÜRICH, UND SABYASACHI CHAKRABORTY, WÜRENLINGEN

Kernkraftwerke decken seit Jahren etwa 40% des Strombedarfs in der Schweiz ohne störfallbedingt erhöhte Emissionen radioaktiver Stoffe. Dieser Nutzen wird von der Öffentlichkeit kaum wahrgenommen. Vielmehr haben vor allem anderswo aufgetretene katastrophale Unfälle in das Bewusstsein gerückt, dass die «segensreiche» Technik mit Risiken verbunden sein kann, die in Art und Ausmass neuartig und unerwartet sind. Zusammen mit der in Zweifel gezogenen Glaubwürdigkeit des Expertenurteils hat sich in einigen Bereichen, vor allem in der Kernenergie, die Akzeptanzkrise besorgniserregend verschärft.

Die systematische Erforschung des Risikos ist eine gesellschaftliche Aufgabe. Ihre Notwendigkeit ist aber auch fachlich begründet:

□ Durch die Nutzung neuer Energiequellen sind im Laufe der Zeit die prozessbezogenen Energieumsätze um Grössenordnungen gestiegen; der 1 m-Fall eines Wassermoleküls – als Form der mechanischen Energie – setzt etwa 1 μeV (10^{-6}eV) frei, chemische Reaktionen liegen typischerweise im Bereich von 1 eV, während nukleare (Kern-)Reaktionen auf dem MeV-Niveau (10^{6}eV) ablaufen.

□ Die Menge und Konzentration potentiell gefährlicher Stoffe sind – insbesondere bei der Kernenergie – so gross geworden, dass aufwendige Sicherheitsvorkehrungen vonnöten sind; die Systeme sind sehr komplex geworden. Ansonsten übliche Sicherheitsstrategien wie «Versuch und Irrtum» sind hier nicht mehr praktikabel.

In Kerntechnik waren die Vorausanalyse von Störfällen und die Einführung formalisierter Bewertungsmethoden für die Sicherheit von Anfang an Bestandteil des Genehmigungsverfahrens. Für die Systemauslegung wurden «grösste» Störfälle/Unfälle angenommen («GAU-Konzept»), deren Auswahl innerhalb gewisser Grenzen eine Sache des Ermessens ist. Zur Beantwortung der Frage, welches Risiko solche Ereignisse verursacht, die die Auslegungsgrenzen überschreiten, wurde im Rahmen der amerikanischen Rasmussen-Studie eine probabilistische Analysemethodik entwickelt (PRA) und auf je eine Anlage mit Druck- und Siedewasserreaktor angewendet. Zwischenzeitlich wurde die Methodik weiterentwickelt, in Teilen standardisiert [1] und vielfach appliziert.

Grundsätzliches zur Methodik

In der Umgangssprache gebrauchen wir den Begriff «Risiko» dann, wenn ein unerwünschtes Ereignis zwar nicht mit Sicherheit eintreten wird, aber auch nicht völlig ausgeschlossen werden kann. Nach der allgemein gültigen mathematischen Definition ist das «Risiko» ein Mass für die Wahrscheinlichkeit eines Schadensereignisses und das Ausmass des durch sein unterstelltes Eintreten verursachten Schadens. An die Stelle des im strengen Sinne dimensionslosen Begriffes «Wahrscheinlichkeit» («Chance» für das Eintreten eines bestimmten Ereignisses oder Zustandes, manchmal auch gedanklich auf einen Zeitraum bezogen) tritt besser der Begriff «Eintrittshäufigkeit» (Ereignisse pro Zeiteinheit bzw. Jahr). Wichtig ist, dass der mathematische Risikobegriff nur zweidimensional ist; zudem hat sich eine lineare multiplikative Verknüpfung der beiden Komponenten eingebürgert, also

R = H (Ereignisse/Jahr) × S (Schaden/Ereignis)

Der Grund dafür liegt in der Erwartung des Menschen, dass zwischen der Eintrittshäufigkeit und dem Schadensausmass eine reziproke Beziehung besteht. Aus Ereignissen hoher Häufigkeit und kleinem Schadensausmass resultiert also rechnerisch das gleiche Risiko wie aus Ereignissen extremer Seltenheit und katastrophalen Schadensausmasses, woraus vor allem mit Blick auf Risikobewertungen Zweifel an der Vertretbarkeit dieser einfachen Produktbildung erkennbar werden. Im folgenden werden die beiden Komponenten möglichst separat gehalten und behandelt.

Jede, wie auch immer geartete Methodik zur Bestimmung des betriebs- bzw. unfallbedingten Risikos von Kernkraftwerken ist mit grundsätzlichen kognitiven und technisch-praktischen Problemen konfrontiert:

□ Im Zentrum des Interesses stehen mögliche Schadensereignisse, d.h. Einzelereignisse oder Ereignisketten, mit katastrophalen Konsequenzen für die Umgebung. Aufgrund getroffener Sicherheitsvorkehrungen sind diese von vornherein nicht sehr wahrscheinlich, so dass die Bestimmung und Handhabung von Unwahrscheinlichkeit bzw. Nichteintreten ansteht. Dennoch sind solche Ereignisse im engen fachlichen Sinne nicht auszuschliessen; über den Zeitpunkt eines unterstellten Eintretens sind keine Aussagen möglich, eine Grenze (Abschneidekriterium), bis zu der Ereignisse zu berücksichtigen wären, müsste vereinbart werden.

□ Das Nichteintreten solcher Ereignisse ist Zielgrösse der Auslegung. Eine direkt nutzbare Statistik gibt es – wunschgemäss – nicht. Die Häufigkeit von extrem unwahrscheinlichen Ereignisketten muss aus Kombination vieler kleiner Fehler/Ereignisse synthetisiert werden. Zusätzliche Unsicherheiten sind zwangsläufig die Folge; sicherheitstechnische Verbesserungen verschärfen meist paradoxerweise dieses Problem.

□ In der Praxis sind Wahrscheinlichkeiten und somit auch die Eintrittshäufigkeit von Schadensereignissen nur über Stichproben als Schätzwerte zu be-

stimmen, die mit Unsicherheiten behaftet sind. Diese lassen sich über den sog. Vertrauensbereich quantifizieren, der dem betreffenden Wert eine Aussagesicherheit zuweist. Die Streuung der oberen und unteren Fraktile, üblicherweise mit 5 und 95% Aussagesicherheit (d.h. 5 bzw. 95% aller Werte sind kleiner oder gleich den angegebenen Werten) und deren Abweichung vom Mittel- oder Erwartungswert werden um so grösser, je geringer die Kenntnisse sind, sprich je unwahrscheinlicher das Ereignis ist.

□ Meist werden aus Beobachtungen abgeleitete Wahrscheinlichkeitsangaben zu Vorhersagen verwendet, was ein Gleichbleiben der Bedingungen voraussetzt. Oft beruhen verwendete Daten (Stichproben) nicht exakt auf den Grundeinheiten (z.B. Komponenten), für die eine Wahrscheinlichkeitsaussage gemacht werden soll; der notwendige Bewertungs- und Übertragungsprozess ist subjektiv («Expertenurteil»). Dieses sind Quellen zusätzlicher Unsicherheiten.

Diese grundsätzlichen Probleme stellen sich um so schärfer, je mehr die Risiken im absoluten Sinne bestimmt und anschliessend bewertet werden und je kleiner die errechneten Häufigkeiten werden bzw. je mehr sie sich einer direkten Überprüfung durch Erfahrungswerte prinzipiell entziehen. Heisst das nun, dass die PRA-Methodik zur Bestimmung des Risikos ein untaugliches Mittel bzw. das unfallbedingte Risiko eines Kernkraftwerkes nicht bestimmbar ist? Aus dem Vorhergesagten folgt die Notwendigkeit einer differenzierten Antwort, hier mit Blick auf die Komponente «Eintrittshäufigkeit» von Schadensereignissen:

□ Konzentriert man sich auf die heute marktgängige Technologie der Leichtwasserreaktoren (LWR), so sind von diesem Typ allein in den westlichen Ländern etwa 270 Anlagen in Betrieb, und etwa 3500 Reaktorbetriebsjahre an Erfahrung stehen zur Verfügung, so dass Eintrittshäufigkeiten für risikorelevante Ereignisse bzw. Ereignisketten im Bereich um 0,0001/a anhand von Betriebserfahrungen und aufgetretenen Störfällen überprüfbar sind.

□ Für viele Anlagen oder zumindest Baulinien sind aufgrund der Vielzahl eingesetzter Komponenten, der meist vierwöchigen Testintervalle und der akkumulierten Beobachtungszeiten verlässliche Aussagen in einem Häufigkeitsbereich möglich, in der Ereignisketten dominieren, die sich aus der Kombination von Einzelfehlern ergeben, und extrem seltene Einzelereignisse («rare events») sowie Mehrfachausfälle von Komponenten noch keine Rolle spielen können. Die untere Grenze dieses Bereiches wird allgemein bei 0,00001/a bis 0,000 001/a gesetzt.

□ Noch kleinere Eintrittshäufigkeiten mit einem Mindestmass an Vertrauenswürdigkeit lassen sich bestimmen, indem Ereignisketten weiter verfolgt und zusätzliche Komponentenausfälle einbezogen werden. Für den so eröffneten Häufigkeitsbereich ist eine ausreichende Vollständigkeit der betrachteten Ereignisse/Ereignisketten nicht mehr gewährleistet und eine Generalisierung, d.h. Gleichsetzung mit dem Gesamtrisiko, nicht ohne weiteres zulässig.

Ein ähnlich differenziertes Urteil gilt auch für die Bestimmbarkeit des Schadensausmasses, so dass die Bestimmbarkeit des Risikos im absoluten Sinne ohne «wenn und aber» nicht ausser Zweifel steht.

Allgemein anerkannt und naheliegender ist der Einsatz dieser probabilistischen Analysetechnik im vergleichenden Sinne, vor allem dann, wenn die Vergleichsfälle eine grosse Ähnlichkeit aufweisen. Dazu zählen:

- die Bewertung konkurrierender Auslegungen und Reaktorkonzepte,
- die Überprüfung des Sicherheitskonzeptes auf Ausgewogenheit,
- die Identifizierung von Schwachstellen, auch an Schnittstellen von Systemen, und Optimierungsmöglichkeiten, auch im Bereich des anlageninternen Notfallschutzes,
- die Verbesserung von Betriebsweisen und -vorschriften (z.B. Testintervalle) sowie die Ausbildung des Betriebspersonals,
- die Überprüfung des Kenntnisstandes und die Konkretisierung von Forschungsaufgaben.

Unbestritten ist auch, dass die PRA-Methodik mit ihrer Logik, Systematik und weitgehenden Willkürfreiheit die besten Einblicke in das komplexe System «Kernkraftwerk» gewährt und mögliche Störfälle/Unfälle gesamthaft und vernetzt beschreibt («Störfalltopologie»). Sie gestattet die Berücksichtigung sowohl technischen als auch menschlichen Versagens bzw. der Wechselwirkung des Menschen mit dem technischen System und die Einbeziehung spezifischer Betriebserfahrungen. Sie schafft so die Voraussetzung für rationale technische Einzelentscheidungen.

Eine probabilistische Risikoanalyse ist aufwendig und bedarf eines erfahrenen, multidisziplinär ausgebildeten Teams. Man unterscheidet drei Ebenen (vgl. Bild 1). Die erste Stufe bilden anlagentechnische Untersuchungen, mit dem Ziel, Ereignisse zu identifizieren

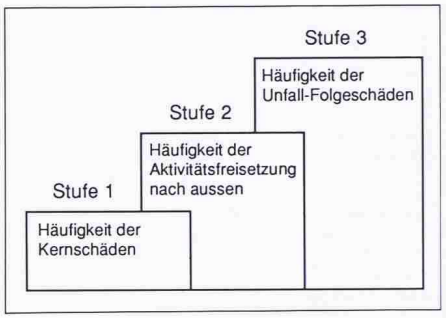


Bild 1. Stufen einer Risikoanalyse

und probabilistisch zu bewerten, die einen schweren Kernschaden nach sich ziehen. Kombiniert man dies mit der Funktion aktiver Containmentsysteme, so spricht man von der Stufe 1+. Die Stufe 2 schliesst die Behandlung ausgelöster physikalischer Vorgänge und die Bestimmung des sog. Quellterms radioaktiver Stoffe mit ein. Die Berechnung der Unfallfolgen (Stufe 3) berücksichtigt üblicherweise folgende Schadensarten:

- Verlust von Menschenleben infolge akuten Strahlensyndroms oder späten Strahlenkrebses
- Genetische Schäden infolge erhöhter radioaktiver Strahlung
- von Schutz- und Gegenmassnahmen betroffene Gebiete und Personen (Flächenkontamination).

Letztere bildet auch die Ausgangsgrösse für eine Abschätzung des finanziellen Schadens, des Verlustes an Landfläche und Kulturgut und liefert Anhaltspunkte für mögliche psychische Schäden und soziale Folgen der betroffenen Bevölkerung, die sich naturgemäss nur schwer quantifizieren lassen. Das Gesamtausmass solcher, die Auslegungsgrenzen überschreitenden Unfälle, wird deutlich.

Gegenstand der Analyse

Die in Kernreaktoren ablaufenden Spaltprozesse führen, neben der Energiefreisetzung, zur Bildung und Akkumulation radioaktiver Spaltprodukte unterschiedlicher Radiotoxizität. Das Inventar ist (mit 1 bis 2 Ci pro W) so hoch, dass Bruchteile davon freigesetzt in der Umgebung Schäden verursachen könnten und deshalb Mehrfachbarrieren gegen ein Austreten vorgesehen werden müssen.

Hinzu kommt, dass auch nach Unterbindung des nuklearen Spaltungsprozesses der Zerfall dieser Stoffe für Wärme in einer Menge sorgt, die auch nach Stunden im Prozentbereich der ursprünglichen Leistung liegt. Sie muss bei den heute üblichen grossen LWR mit Hilfe technischer Systeme abge-

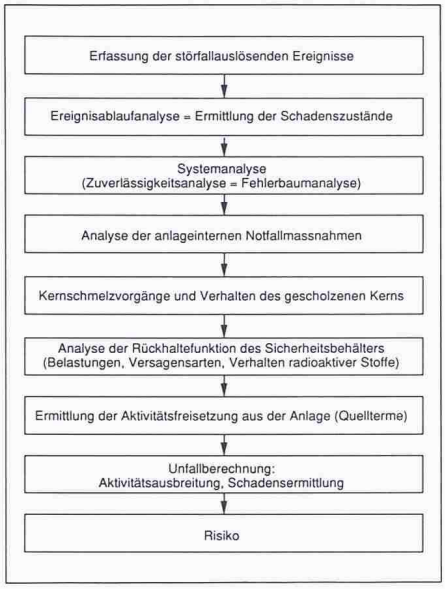


Bild 2. Schritte einer Risikoanalyse

führt werden; sie würde sonst zum Aufschmelzen der Brennstäbe und gegebenenfalls auch nachgeschalteter Barrieren und somit letztlich zur massiven Freisetzung radioaktiver Stoffe führen. Hinzu kommt, dass der Leistungsbetrieb nicht unter allen Umständen für den Reaktor der neutronenphysikalisch günstigste Zustand ist, so dass zur Regelung und sicheren Abschaltung – neben einer inhärent sicheren Auslegung – technische Systeme vorgesehen werden.

Zur Gewährleistung der Abschaltung (ohne Schäden am Reaktor), der sicheren Nachwärmeabfuhr und des gesicherten Einschlusses radioaktiver Stoffe ist eine Sicherheitsphilosophie mit gestaffelten Massnahmen («defense-in-depth») entwickelt worden. Die Anforderungen an die vorzusehenden Sicherheitseinrichtungen ergeben sich aus der Vorsorge gegen die deterministisch zu unterstellenden Auslegungsstörfälle mit abdeckendem Charakter. Sicherheitssysteme, wie beispielsweise die Notkühl- und Nachwärmeabfuhrsysteme, gehen automatisch in Betrieb und sind redundant und möglichst diversitär aufgebaut, was vor allem bedeutet, dass mehr Systeme (Stränge) vorhanden sind, als zur Funktionserfüllung erforderlich wären (meist 4 statt 2). Der Beweis ist zu erbringen, dass der Eintritt des «GAU» nicht zu Strahlendosen in der Umgebung oberhalb vorgegebener Grenzwerte führen würde. Relevante Risikobeiträge sind dementsprechend nur dann zu erwarten, wenn zusätzlich Versagen eines der Reservesysteme unterstellt wird, die im Reaktorkern erzeugte Wärme nicht abgeführt werden kann und der Reaktorkern schmilzt («Super GAU»).

Methodische Einzelaspekte

Die erste Aufgabe innerhalb der anlagentechnischen Untersuchungen einer Risikoanalyse, deren Schritte Bild 2 erläutert, besteht darin, störfallauslösende Ereignisse zu identifizieren, die zu einer Aktivitätsfreisetzung führen könnten. Man unterscheidet dabei anlageninterne und -externe Auslöser. Bei den anlageninternen auslösenden Ereignissen gibt es wiederum zwei Gruppen, die sog. Kühlmittelverluststörfälle als Folge von Brüchen, Rissen und Undichtigkeiten im Reaktorkreislauf oder in Anschlussleitungen; eingeschlossen ist auch das fehlerhafte Öffnen oder Offenbleiben von Ventilen oder Absperrarmaturen. Die zweite Gruppe sind transiente Ereignisse, unter denen man Störungen mit einem Ungleichgewicht zwischen Wärmeerzeugung und Wärmeabfuhr versteht (vgl. Tabelle 1).

Anlagenexterne auslösende Ereignisse (Erdbeben, Flugzeugabsturz etc. und Brände innerhalb der Anlage) führen im Prinzip zu den gleichen Systemzuständen, können aber nachfolgend wichtig werdende Systeme und Strukturen mit beeinträchtigen – ein Brand kann eine Transiente auslösen und gleichzeitig, bei fehlender räumlicher Trennung, redundante Nachwärmeabfuhrsysteme schwächen.

In den Analysen weitgehend unberücksichtigt bleibt das Versagen von passiven Grosskomponenten: so auch des Reaktordruckbehälters, weil aufgrund seiner Auslegung und Überwachung dieses ausgeschlossen werden kann oder extrem unwahrscheinlich ist und das ausgelöste Unfallszenario angeblich durch andere, wahrscheinlichere mit abgedeckt wird. Der Nachweis ausreichender Vollständigkeit der betrachteten Ereignisse und Ereignisketten ist naturgemäss schwierig und im mathematischen Sinne nicht zu erbringen. Dieses Problem stellt sich weniger scharf, wenn schon Ereignisketten relativ hoher Eintrittshäufigkeiten zu katastrophalen Spaltproduktfreisetzungen führen («Einhüllende»); es verschärft sich bei weiterer Steigerung der Anlagensicherheit und wird für die sog. inhärent/passiv sicheren Reaktoren zu einem Kernpunkt bzw. neuen Herausforderung. Böswillige zerstörerische Handlungen Dritter (Sabotage, Terrorismus/Waffeneinwirkung) wurden bisher in keiner probabilistischen Risikoanalyse berücksichtigt bzw. entziehen sich weitgehend einer expliziten Behandlung.

Bei der Analyse möglicher Folgen eines auslösenden Ereignisses bedient man sich induktiver Ereignisablaufdiagramme (event trees), für die das Funktionieren oder Versagen von Systemen bzw. das Eintreten oder Nichteintreten eines Ereignisses angenommen wird (Binär-Abfrage, siehe Bild 3). Teilausfälle oder Zeitabhängigkeiten bleiben meist (pessimistisch) unberücksichtigt.

Die zugehörigen Wahrscheinlichkeiten lassen sich meist nicht direkt aus der Statistik ableiten; dazu wird in der Regel die deduktive Fehlerbaummethode eingesetzt (Bild 4). Dabei ist zu beachten, dass neben den Funktionsausfällen von Komponenten, die voneinander unabhängig sind, solche auftreten können, die mehrere (redundante) Komponenten quasi gleichzeitig betreffen. Die Wahrscheinlichkeit dafür kann dann

Auslösendes Ereignis für einen Kühlmittelverlust	Eintrittshäufigkeit pro Jahr	Auslösendes Ereignis für Transienten	Eintrittshäufigkeit pro Jahr
		Betriebstransienten	10^{-2} - 10
– Lecks in der Hauptkühlmittelleitung	$10^{-7} - 10^{-3}$		
– Lecks am Druckhalter	$10^{-4} - 10^{-5}$	– Ausfall der Hauptspeisewasserversorgung	
– Lecks in einem Dampferzeuger	$10^{-3} - 10^{-5}$	– Ausfall der Hauptwärmesenke	
– Leck in einer Anschlussleitung des Reaktorkühlkreislaufes	10^{-7}	– Ausfall der elektrischen Eigenbedarfsversorgung	
		Seltene Transienten	$< 10^{-2}$
		– Speisewasserleitungsbruch – Frischdampfleitungsbruch – Reaktivitätsstörfall	

Tabelle 1. In PRA üblicherweise berücksichtigte anlageninterne auslösende Ereignisse mit Häufigkeitsbereichen. Ausgangszustand ist der Vollastbetrieb, der andere Anlagenzustände abdecken soll, was aber vor allem für An- und Abfahrvorgänge jeweils zu prüfen ist. Die aufgeführten Ereignisse repräsentieren meist eine Klasse von Einzelereignissen, die einen ähnlichen Ablauf auslösen können.

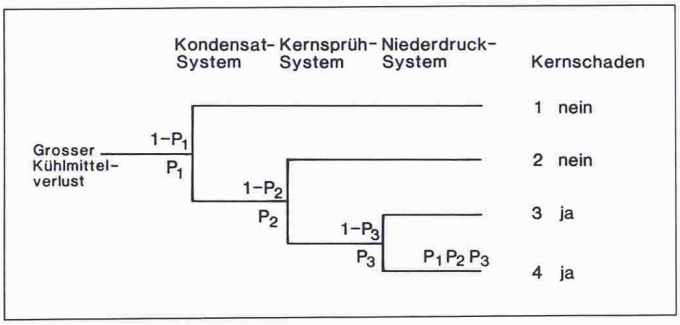


Bild 3. Ereignisablaufdiagramm

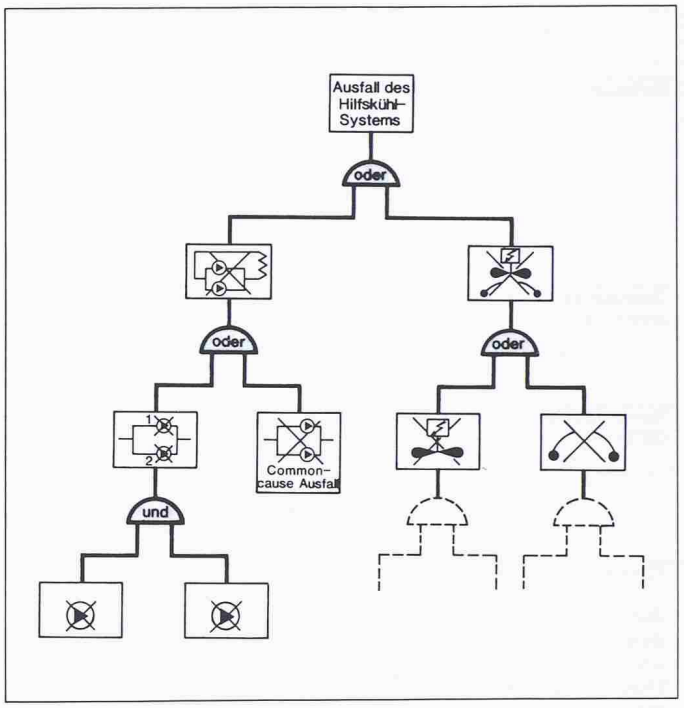


Bild 4. Der stark vereinfachte Fehlerbaum eines Hilfskühlsystems (Beispiel) ergibt sich durch logische Kombination aller Ausfälle von Systemteilen, die einen Ausfall des Gesamtsystems nach sich ziehen. Das Hilfskühlsystem ist z.B. ausgefallen, wenn die Umwälzpumpe 1 und die Umwälzpumpe 2 durch Einzelfehler oder beide Pumpen gleichzeitig durch Common-cause-Fehler ausfallen. Sind die analysierten Systemteile durch ein logisches «oder» verknüpft, so addieren sich die Ausfallwahrscheinlichkeiten in erster Näherung; sind sie durch ein logisches «und» verknüpft, so multiplizieren sie sich

nicht mehr über Multiplikation der Einzelausfälle bestimmt werden; man spricht von abhängigen oder Common-cause-Ausfällen.

Funktionelle Abhängigkeiten, z.B. fehlerhafte Wartung, können durch eine detaillierte Fehlerbaumanalyse erfasst werden, ebenso Folgeausfälle, sofern sie nicht – wie für moderne Kernkraftwerke meist möglich – wegen räumlich getrennter Anordnung oder entsprechender Konstruktion ausgeschlossen werden können. Schwieriger gestaltet sich die Erfassung des Teils abhängiger Ausfälle, der auf gemeinsame äussere Fehler zurückgeht, wie beispielsweise eine gemeinsame Ölversorgung. Zunächst bietet sich die Auswertung von Betriebserfahrungen an. Der Erfolg ist aber begrenzt, da nur wenige Beobachtungen für sie vorliegen bzw. überhaupt vorliegen können. Für modern aufgebaute redundante Sicherheitssysteme erwartet man, dass sie mit einer Wahrscheinlichkeit von 1:10 000 oder 100 000 bei Anforderung ausfallen oder nicht verfügbar sind. Ein bisher nicht beobachteter Common-cause-Systemausfall ist also kein ausreichender Grund dafür, ihn für die Risikoanalyse auszuschliessen. Sie werden inzwischen über parametrische Modelle (vgl. Tabelle 2) erfasst und begrenzen oft die mit aktiven Systemen erreichbare Zuverlässigkeit. Problematisch sind weniger die Modellvorstellungen und ihre Berücksichtigung über Eingänge im Fehlerbaum, als die Quantifizierung der jeweiligen Parameter, oft kann nur auf Null-Ausfall-Statistiken zurückgegriffen werden.

Die Behandlung abhängiger Ausfälle dominiert die (berechnete) Zuverlässigkeit hoch zuverlässiger Systeme, ist aber mit erheblichen methodischen Defiziten und Datenunsicherheiten behaftet.

Bei der Berechnung eines Fehlerbaumes wird vereinfachend von einer zeitlichen Konstanz der Ausfalldaten ausgegangen. Früh- oder Verschleissausfälle («Badewannenkurve») werden ebenso vernachlässigt wie Schwankungen während der Hauptnutzungsphase, was nicht unumstritten ist.

Ein Schwerpunkt jeder PRA ist die Analyse des «Menschen» als Bestandteil des Gesamtsystems. Trotz weitgehender Standardisierung von Prozeduren und Automatisierung der Anlage kann er – wie weltweit bewiesen – das Geschehen im Vorfeld und während eines Unfalles wesentlich beeinflussen.

Man hat dem Rechnung zu tragen; die PRA-Methodik bietet dazu die prinzipielle Möglichkeit, ist aber noch nicht zufriedenstellend weit entwickelt, was angesichts der Komplexität, der Variabilität und der Vielschichtigkeit menschlichen Verhaltens nicht verwundert.

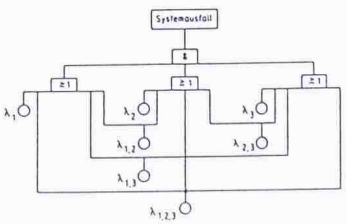
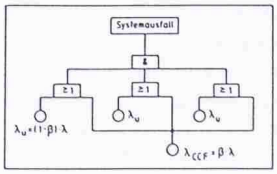
Arten	Behandlung	
Folgeausfälle	Ausschluss wegen räumlicher Trennung, Konstruktion etc., Fehlerbaum explizit	
Funktionelle Abhängigkeiten	Fehlerbaum explizit	
Gemeinsamer "äusserer" Fehler	Betriebserfahrungen; parametrische Modelle - Fehlerbaum implizit	
	Marshal-Olkin-Modell Eigene Ausfallrate für gemeinsamen Ausfall jeder Komponentenkombination; bei meist benutzter Homogenisierung hängt λ (i aus m) nur von i ab, d. h. $\lambda_{1,2} = \lambda_{1,3} = \lambda_{2,3}$.  	β-Faktor-Modell Gleichzeitiger Ausfall aller redundanten gleichartigen Komponenten; $\beta = \frac{\lambda_{CCF}}{\lambda_{ges}}$  Multiple-Greek-Letter-Modell ähnlich Marshall-Olkin-Modell, Parameter anders bestimmt $\beta = \frac{\lambda(\geq 2 \text{ aus } m)}{\lambda_{ges}}$ $\gamma = \frac{\lambda(\geq 3 \text{ aus } m)}{\lambda(\geq 2 \text{ aus } m)}$, usw.

Tabelle 2. Die Ursachen für abhängige Ausfälle lassen sich in drei Gruppen unterscheiden, die explizit oder implizit im Fehlerbaum berücksichtigt werden.

Modelle	Berücksichtigung der Faktoren/Techniken	Bemerkungen
Performance shaping factors (PSF)	– Qualität der Betriebsvorschriften – Qualität des Trainings des Betriebspersonals, der Information über Anlagenstatus, der Kontrolle, – Verfügbare Zeit für Handlung, – Rückgängigkeit der Handlungen – Motivation	Quantifikationsprozess schwierig (Wie kann man beispielsweise Motivation messen?) hohes Mass an subjektiver Einschätzung
Technique for Human Error rate Prediction (THERP)	– Verwendung der Fehlerbaumtechnik – Wartungsaktivitäten – beschränkte Anzahl unabhängiger Operateurhandlungen	Kenntnisbedingtes Verhalten ausgelassen
Human Cognition Reliability Model (HCR)	– Fertigkeits–, regel und kenntnisbedingte PSF – Medianwert der Ansprechzeit für eine Aufgabe, hergeleitet aus Simulatordaten oder Expertenschätzung	Das Modell muss modifiziert werden für die Anwendung auf eine lange Zeitspanne
SLIM–MAUD–Modell: Quantifizierung der Fehler Wahrscheinlichkeiten für prozedurale und kognitive Aufgaben	– PSF – Gewichtsfaktoren für jeden PSF	Vorwiegend psychologisch orientiertes Modell
Systematic Human Application Reliability Procedure (SHARP)	– Identifikation von Handlungen, Auswahl der wichtigen Handlungen und Aufgabenanalyse – Einbau der Handlungen in S modellen – Wahl des Quantifizierungsverfahrens – Standarddokumentation	Gemeinsame Struktur und Dokumentationsschema für verschiedene Zuverlässigkeits– und Quantifikationsmodelle
Worledge Model: Schlüsselkonzept ist mentale Informationsverarbeitung	Aktionsfelder – Diagnose – Auswahl des Prozedere – Wahrnehmung des Anlageverhaltens – Vermeidung des sich irrens	Dieses Modell ist viel vollständiger als die anderen Führt nicht direkt zu Zuverlässigkeitskenngrössen Fehler wegen Funktionsstörung der Ausrüstungen nicht abgedeckt Langzeit–Handlungen nicht genügend erfasst.
AIPA–Modell: Bestimmung der Wahrscheinlichkeit eines menschlichen Fehlverhaltens	– Verhältnis: Verfügbare Zeit für eine Handlung/für die Durchführung benötigte Zeit (MTOR)	Breitere Anwendung gefunden; Expertenschätzung nötig, falls keine ausreichende Betriebserfahrung vorliegt. Beim hohen Stress Anpassung mit einem Zuschlag zu MTOR erforderlich.

Tabelle 3. Modelle zur Quantifizierung menschlicher Zuverlässigkeit sind mit ihren Konzeptansätzen und Bewertungsschritten dargestellt. Sie werden auf Handlungen vor Störfallauslösung und Beherrschung oder Eindämmung eines Störfalls eingesetzt; störfallauslösende Personalhandlungen sind in der Regel in empirisch ermittelten Häufigkeiten enthalten.

Im Rahmen einer PRA werden nur die Betriebsmannschaft in der Warte und das Wartungspersonal als Personengruppe berücksichtigt. Mangelhafte Management-Funktionen werden dementsprechend vernachlässigt, obwohl sie die Anlage vor Störfalleintritt in einen Zustand minderer Sicherheit führen können; der Mangel an Sicherheitskultur auf den verschiedenen Ebenen der Anlagenauslegung, der Aufsicht und dem Betrieb gilt als eine der Hauptursachen für «Tschernobyl». Diese Problematik, die sich langsam entwickelt und deshalb nicht schwer zu korrigieren sein dürfte, kann durch eine PRA noch stärker ins Bewusstsein gerückt, aber nicht gelöst werden.

Handlungen des genannten Personals können in verschiedenen Zeitbereichen liegen und werden innerhalb einer PRA methodisch unterschiedlich behandelt (vgl. Tabelle 3). Als Typus fehlerhafter Handlungen während eines Störfalls wird die Unterlassung oder unzureichende Ausführung einer geplanten Handlung berücksichtigt, für die aufgrund sicherheitstechnischer Anforderungen in der Regel mehr als 30 Minuten Zeit bleiben. Manipulationen des Reaktorschutzsystems werden, aufgrund getroffener technischer Vorkehrungen, nicht zugelassen, ebensowenig störfallverschlimmernde oder mildernde ungeplante Handlungen.

Der Grund für diese insgesamt wohl eher pessimistische Vorgehensweise liegt auch darin, dass solche ungeplanten Handlungen auf einem kenntnisbedingten Verhalten (knowledge-based) basieren, was sich einer Beschreibung über Zuverlässigkeitskenngrössen (noch?) entzieht. Dieses geschieht aber für:

- fertigkeitsbedingtes (skill-based) Verhalten, das aufgrund vorhandener Erfahrungen bzw. Übungen quasi-automatische Reaktionen auslöst, und
- regelbedingtes (rule-based) Verhalten, das nach Erkennen der Eingangsinformation aufgrund bereits vorhandener Regeln vorgeplante Aktionen zuordnet und durchführt.

Zur Bewertung menschlichen Fehlverhaltens wurden eine Vielzahl von Methoden und Modellen entwickelt. Am verbreitetsten ist der sog. THERP-Ansatz [2], der folgende Schritte vorsieht:

- Bestimmung der Ausfallkombination, die unter Berücksichtigung menschlicher Fehlhandlungen zum Versagen der interessierenden Systemfunktion führen.
- Erfassung und Analyse der zur interessierenden Systemfunktion gehörigen Aufgaben des Personals (Aufgabenanalysen).
- Zerlegung einer Personalhandlung in Handlungsschritte und Darstellung in einem Ablaufdiagramm (z.B. Human Reliability Analysis Tree)
- Zuordnung der Handlungsschritte zu den entsprechenden Kategorien und Schätzung der Fehlerwahrscheinlichkeiten als Teil der Gesamtanalyse.

Derzeit wird intensiv an der Weiterentwicklung der Methoden gearbeitet. So wird der THERP-Ansatz erweitert um die Bewertung von Abhängigkeiten mehrerer aufeinanderfolgender Handlungsschritte einer Person, von gemeinsamen Handlungen mehrerer Personen und der Kontrolle von Handlungen einer Person durch eine zweite. Darüber hinaus werden Betriebserfahrungen und Störfallberichte systematisch erfasst und ausgewertet mit dem Ziel, geeignete Daten für die Bewertung menschlichen Fehlverhaltens zu gewinnen. Hinzu kommen Experimente und Übungen an Trainingssimulatoren, deren Auswertung Zuverlässlichkeitsgrössen erbringen soll.

Zur Quantifizierung der Eintrittshäufigkeit von Ereignisketten bzw. der Freisetzung von radioaktiven Stoffen sind zwei Kategorien von Daten erforderlich:

- Eintrittshäufigkeit auslösender Ereignisse und
- Zuverlässigkeitskenngrössen für sicherheitstechnisch-relevante Komponenten, wie die Ausfallrate oder die Nichtverfügbarkeit bei Anforderung.

Datenbasis sind naturgemäss Betriebserfahrungen und Schadenstatistiken/Aufzeichnungen (Erdbeben) im weitesten Sinne. Je nachdem, ob die ausgewerteten Störfallberichte, Wartungs-, Prüf- und Reparaturprotokolle usw. aus der analysierten Anlage stammen oder ob allgemeine Informationen genutzt wurden, spricht man von anlagenspezifischen oder generischen Daten bzw. Analysen. Oft ist eine Mischung festzustellen (Beispiel: deutsche Risikostudie Phase B). Anlagenspezifische Informationen werden so weit wie möglich genutzt; zur Ergänzung und Kontrolle greift man auf andere Quellen zurück, wobei inzwischen existierende Datenbanken die Arbeit erleichtern.

Die Daten werden als Zufallsvariable betrachtet, meist wird eine logarithmische Normalverteilung angenommen. Die Datenbasis verbreitert sich fortlaufend; die verbleibenden Unsicherheiten sind dann am grössten, wenn es sich um seltene oder neuartige oder extrem zuverlässige Komponenten handelt. Aussagen über extrem seltene Einzelereignisse entbehren meist jeglicher statistischer Grundlage.

Die Unsicherheiten, die den Ergebnissen einer PRA anhaften, lassen sich in drei Arten unterscheiden:

- Unsicherheiten von Parameterwerten aufgrund unvollständiger Basisdaten
- Unsicherheiten in der Modellierung
- Unsicherheiten bezüglich der Vollständigkeit der Analyse.

Eine PRA verursacht diese Unsicherheiten nicht, sondern lässt Bestehendes zu Tage treten. Die Bewertung der Unsicherheiten erhöht die Aussagekraft einer Analyse. Die Methoden zur Quantifizierung von Unsicherheiten sind bei den anlagentechnischen Untersuchungen am weitesten entwickelt: Den Eingangsparametern der Fehlerbäume und Ereignisablaufdiagramme werden Unsicherheiten zugewiesen und dann mit gängigen Methoden (z.B. «Monte-Carlo-Spiele») fortgepflanzt. Der Vertrauensbereich der Endergebnisse berücksichtigt aber keine Unsicherheiten hinsichtlich Modellierung und Vollständigkeit. Dazu werden zusätzliche Betrachtungen angestellt und Techniken eingesetzt, die aber mehr qualitativen Charakter haben:

□ Die grösste Unsicherheit in der Modellierung liegt darin, dass das technische System nicht richtig und vollständig im Fehlerbaum abgebildet wurde. Dementsprechend sind Anlagenbegehungen und Vorort-Überprüfungen sowie eine Überprüfung der Gesamtanalyse durch Externe («peer review») unerlässlich.

Druckwasserreaktor	*Siedewasserreaktor*
- kleine Lecks - Notstromfall - Brand - Erdbeben kritisch für alte Anlagen - Ausfall des Ventilationssystems in wichtigen Räumen Als weiteres wichtig für einige Reaktoren: - Ausfall Hauptspeisewasser - Verlust der Komponentenkühlung - Dampferzeuger-Heizrohrlecks	Als Transienten dominieren - Ausfall Hauptspeisewasser - Überspeisung - Schliessung der Frischdampf-Isolationsventile Als externe Ereignisse dominieren Feuer und Erdbeben

Tabelle 4. Häufig auftretende Ereignisse

Auslösende Ereignisse (Rang)	*Kernschmelzszenarien*	*Beitrag zu Kernschmelzhäufigkeit*
Feuer (1)	Reaktorschnellabschaltung, Ausfall Hauptspeisewassersystem (HPSW), keine bleed- and feed-Kühlung, Leck an der Dichtung der Hauptkühlmittelpumpe	14%
Erdbeben (2)	Notstromfall, Reaktorschnellabschaltung, Ausfall HPSW, keine bleed- and feed-Kühlung, Leck an der Dichtung der Hauptkühlmittelpumpe	7%
Erdbeben (3)	Reaktorschnellabschaltung, keine feed- and bleed-Kühlung, Ausfall HPSW	6%
Notstromfall (8)	Reaktorschnellabschaltung, keine Dampferzeugerkühlung, keine feed- and bleed-Kühlung, Ausfall der Rezirkulations-Kühlung	4%

Tabelle 5. Risikoszenarien am Beispiel des Druckwasserreaktors

□ Betriebserfahrungen bzw. Berichte über besondere Vorkommnisse nutzt man in dem Sinne, dass Ereignisse gezielt ausgewertet werden, die als Vorläufer schwerer Unfälle gelten können («precursor studies»). Eine amerikanische Studie dieser Art ergab auf der Basis von 1500 Reaktorjahren (1969–79, 1980 und 1981 ausgewertet [3]) eine Kernschmelzhäufigkeit im Bereich von 0,0017 bis 0,0045 pro Reaktor-Jahr, dominiert durch den TMI-Unfall.

□ Änderungen an der Anlage und in den Betriebserfahrungen könnten dazu führen, dass die Analyse nicht mehr in allen Punkten gilt. Um das zu vermeiden, muss sie ständig der Realität angepasst werden («living PRA»).

Die Unsicherheiten im Bereich der phänomenologischen Untersuchungen sind z.T. grösser und noch schwerer zu quantifizieren, oft lässt die Datenbasis das gar nicht zu. Viele der eingesetzten Simulationsmodelle sind im Rahmen internationaler Forschungsprogramme über Experimente und Vergleichsrechnungen validiert worden, bei einigen ist das aber (noch) nicht der Fall. Auf einigen Gebieten bestehen noch erhebliche Kenntnislücken (z.B. Wasserstoffbildung und -verteilung). Ein Gefühl für die Bedeutung bestehender Unsicherheiten können systematische Sensitivitätsanalysen (mit Variation der Parameter innerhalb vernünftiger Bandbreiten) vermitteln.

Schlussfolgerungen aus Risikostudien

Allein in den USA sind zwischenzeitlich an die vierzig anlagenspezifischen Risikoanalysen durchgeführt worden, davon wiederum 21 von einer Ingenieur-Unternehmung [6].

Ein Schlüsselergebnis aus einer PRA ist jeweils die Liste der risikobestimmenden Ereignisse und Ereignisabläufe und die Abschätzung der Kernschmelzhäufigkeit mit ihren relevanten Beiträgen. Gerade für die Risikomanagement-Entscheidung sind solche Angaben hilfreich, um Ressourcen für die Verbesserung der Sicherheit vernünftig einzusetzen. Die zahlreichen PRA-Studien zeigen eine Rangfolge für auslösende Ereignisse (vgl. Tabelle 4), die zum Kernschmelzen führen können.

Die Quantifizierung der Risikoszenarien erlaubt die Bildung einer Rangfolge der risikobestimmenden Szenarien. Das Beispiel für einen Druckwasserreaktor ist in Tabelle 5 dargestellt. Die Tabelle 6 enthält Risikoszenarien mit

Kernkraftwerke	*Szenarien*	*Häufigkeit (pro Jahr)*	*Kernschmelzhäufigkeit (%)*
P2	Erdbeben, Notstromfall	$5{,}6 \cdot 10^{-5}$	11
P3	Sturm, Notstromfall	$3{,}6 \cdot 10^{-5}$	27
P4	kleines Leck	$8{,}2 \cdot 10^{-5}$	59
P10	Ausfall der Komponentenkühlung	$3{,}8 \cdot 10^{-5}$	12
P11	kleines Leck mit Ausfall der Sumpf-Rezirkulationsventile	$1{,}4 \cdot 10^{-5}$	6
P13	Ausfall der Kommandoraum-Ventilation	$1{,}6 \cdot 10^{-5}$	30

Tabelle 6. Risikoszenarien mit dem höchsten Rang für 6 untersuchte KKW mit Druckwasserreaktoren

Rangfolge	*Systemfunktion*	*Häufigkeit (Ereignis pro Jahr)*	*Prozentualer Beitrag zur Kernschmelzhäufigkeit*
1.	Reaktor-Schnellabschaltung	$4{,}1 \times 10^{-4}$	53
2.	Dieselgenerator	$3{,}2 \times 10^{-4}$	40
3.	Schliessen der Sicherheitsventile	$8{,}2 \times 10^{-5}$	10
4.	Schliessen der Druckentlastungsventile	$6{,}8 \times 10^{-5}$	8
5.	Manuelle Druckentlastung	$4{,}2 \times 10^{-5}$	5

Tabelle 7. Relative Bedeutung der Systemfunktion durch PRA

dem höchsten Rang für 6 untersuchte Kernkraftwerke mit Druckwasserreaktoren.

Einen weiteren interessanten Einblick in die relative Bedeutung der Systemfunktion erhält man durch PRA (vgl. Tabelle 7).

Die Ergebnisse der verschiedenen Risikostudien beinhalten unterschiedliche Detailierungs- oder Genauigkeitsgrade, die Studien beziehen sich auf Anlagen, die voneinander abweichen hinsichtlich technischer Stand, Alter, Betriebsweise usw. Ausserdem unterscheiden sich die Studien auch im gewissen Umfang in der Methodik. Praktisch alle durchgeführten PRAs haben gewisse Schwachstellen der Anlagen hinsichtlich Auslegung, Konfiguration und Betriebsvorschriften aufgedeckt, was zu den nötigen Verbesserungsmassnahmen («fixes») geführt haben. Deshalb spiegeln die einmal publizierten Risikozahlen nicht unbedingt den aktuellen Stand der Anlage wieder.

Ein besonders wichtiger Aspekt ist die Klarstellung der Risikowerte, d.h. ob es sich um Mittelwerte, Medianwerte, Punkt-Abschätzung, beste Abschätzung oder oberer/unterer Grenzwert handelt und wie die Fehlerbandbreiten berechnet worden sind. Gemäss der neusten US-Studie NUREG-1150 [5] entspricht die Unsicherheitsbandbreite bei der Kernschmelzhäufigkeit etwa einer Grössenordnung. Danach zu urteilen hiesse, dass die Unterschiede um Faktoren 5–10 bei den Kernschmelzhäufigkeiten im Bereich der inhärenten Unsicherheiten der Methodologie mit praktischer Anwendung liegen.

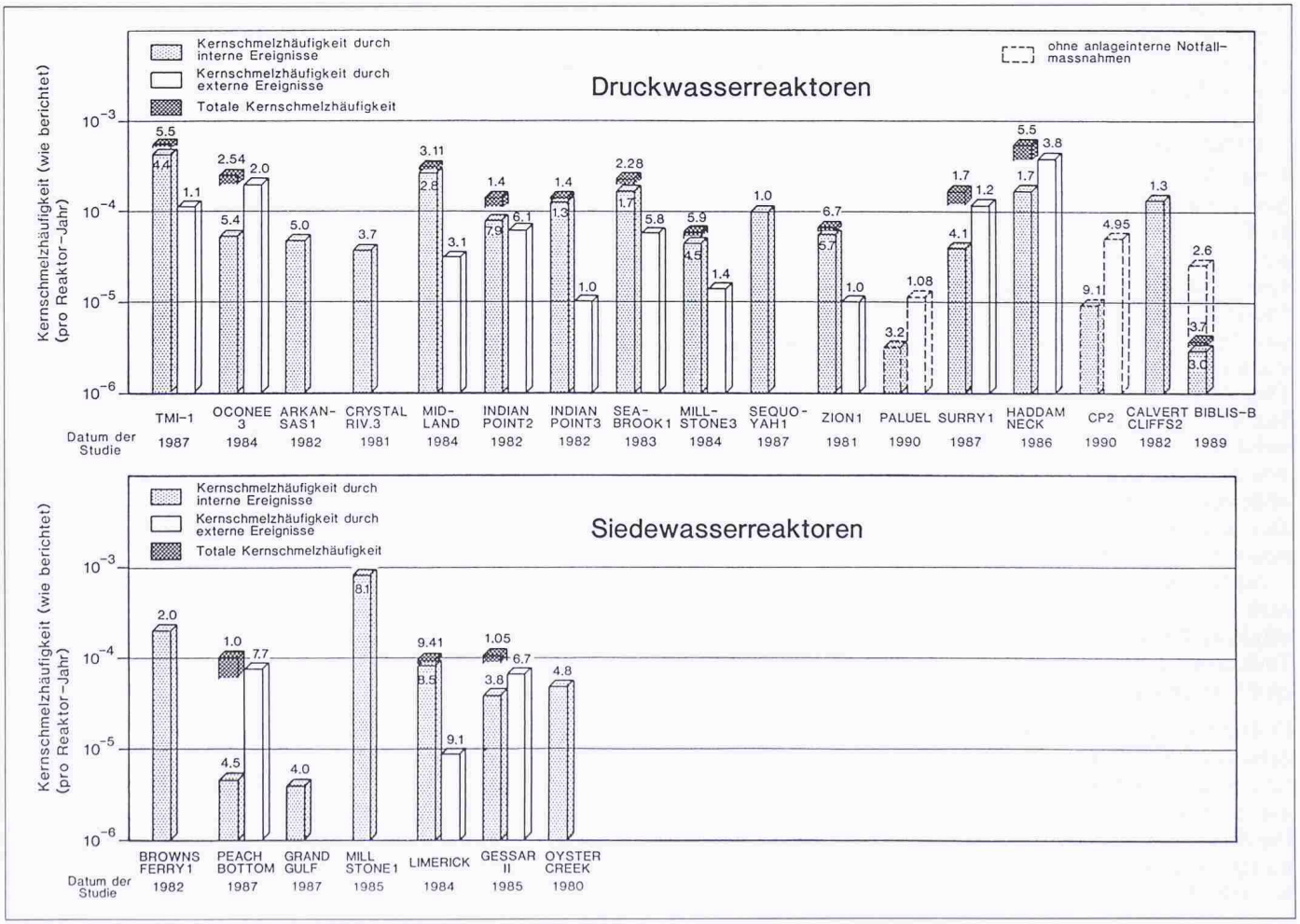


Bild 5. Resultate einiger Risikostudien

Dennoch ist die Präsentation der Kernschmelzhäufigkeiten, wie sie in Bild 5 dargestellt sind, instruktiv für die Feststellung des Variationsbereichs der Häufigkeiten und des über viele unterschiedlichen Anlagen gemittelten Wertes der Kernschmelzhäufigkeit. Gewisse Abweichungen der Kernschmelzhäufigkeitswerte der Risikostudien lassen auch auf systemtechnische Besonderheiten schliessen.

Stand der internationalen Diskussion

Seit dem Erscheinen der WASH-1400-Studie sind einige bedeutende Fortschritte und Entwicklungen auf dem Gebiet probabilistischer Risikoanalysen zu verzeichnen (vgl. Tabelle 8). Gesichtspunkte der internationalen Diskussion sind:

- Das Spektrum untersuchter störfallauslösender Ereignisse ist grösser geworden. Übergreifende Ereignisse wie anlageninterne Brände und Erdbeben tragen massgeblich zum Risiko bei, wobei diese Ereignisse stark anlagen- und standortspezifisch sind. Methodische Fortschritte sind erzielt worden. Im allgemeinen sind die Analysen aufwendiger geworden, phänomenologisch unterschiedliche Unfallabläufe werden systematisch erfasst.
- Grobe Defizite im methodischen Bereich zur Quantifizierung von common-cause-Ausfällen und von menschlichem Fehlverhalten sind ausgeglichen worden.
- Mit der systematischen Auswertung der vorhandenen Betriebserfahrung sind die Ergebnisse der Risikostudien realistischer, die Datenbasis für Zuverlässigkeitsanalysen ist breiter und differenzierter geworden.
- Verbesserte Modelle und differenzierte Daten zur Beschreibung der atmosphärischen Ausbreitung radioaktiver Stoffe liegen vor. Hinzu gekommen ist eine für die Unfallfolgenabschätzung realistischere Modellierung der Notfallschutzmassnahmen.
- Die Unsicherheiten der Risikobestimmung können heute genauer und deutlicher beschrieben werden. Vor allem die Unsicherheitsbandbreite der unfallspezifischen Quellterme für radiaktive Stoffe ist aber noch zu gross für eine verlässliche Risikobestimmung. Man kann nicht deutlich genug auf die Unsicherheiten, Fehlerbandbreiten und Einschränkungen der Risikostudien und auf die Vorläufigkeit der Ergebnisse hinweisen.
- Die Risikobeiträge bestimmter Ereignisse, wie z.B. ungeplante Handmassnahmen, Sabotage, sind derzeit wohl qualitativ, aber nicht quantitativ abschätzbar.
- Die Einschätzung des NRC-Operating-Direktors Taylor aus dem Jahr 1981 «... operating experiences along with the available PRA studies seem to suggest that to bring the ‹best estimate› core melt frequency into the domain of 0,00001/Reactor-Year, or less may be a heroic job and one that would be difficult to ‹demonstrate› it achieved» kann nach heutiger Erfahrung als erreicht gelten.
- Eine einmal für eine Anlage durchgeführte PRA ist nicht als abgeschlossen zu betrachten, denn für die Validierung der Ereignisabläufe und Fehlerbäume muss die Auswertung der Betriebserfahrung herangezogen werden. Erst eine «living PSA/PRA» kann die methodischen Schwächen aufdecken und die Ergebnisse laufend den neuen Erkenntnissen anpassen.
- Die zukünftige Herausforderung der probabilistischen Risikoanalyse liegt in der Anwendung auf verbindliche Vorgaben über maximal zuverlässige Wahrscheinlichkeitswerte bestimmter Anlagenzustände oder Freisetzungen («safety goals»).
- Es ist ausser Zweifel, dass die PRA heute die einzige Methode ist, die in der Lage ist, überhaupt die Sicherheit der komplexen Anlagen angemessen zu quantifizieren.

Aspekte	1975 - 1985 PRA's	1990 PRA's
	Vorgänge im Reaktorkühlkreislauf (in-vessel)	
Naturumlauf	Nein	Ja
Induziertes Versagen	Nein	Ja
Lokales Versagen	Nein	Ja
Anlagen-interne Notfallmassnahmen	Nein	Ja
Versagensarten des Sicherheitsbehälters (ex-vessel)		
– Starke Dampfbildung (stream spike)	Ja	Ja
– Versagen des Sicherheitsbehälters durch Wasserstoffverbrennung	Ja	Ja
– Heftige Dampfexplosion, die den Reaktordruckbehälter zerstört und die Integrität des Sicherheitsbehälters gefährdet	Ja	ja
– Direkte Kontakte der Schmelze mit dem Sicherheitsbehälter	Nein	Ja
– Gezielte Druckentlastung des Sicherheitsbehälters	Nein	Ja
– Sicherheitsbehälter wird durch freiwerdende Spaltprodukte von vornherein umgangen (Bypass-Ereignisabläufe)	Ja	Ja
– Feinfragmentation der Schmelze und Aufheizung der Sicherheitsbehälter-Atmosphäre (Direct Containment Heating), wenn der Reaktordruckbehälter unter höherem Druck versagt)	Nein	Ja
(Quellterme) - Phämoneme und Prozesse zur Spaltproduktfreisetzung		
– Spaltproduktrückhaltung im Primärkreis	Ja (unvollst.)	Ja
– Wiederverdampfung abgelagerter oder kondensierter Spaltprodukte	Nein	Ja
– Chemische Form des Jodes	Nein (teilweise)	Ja
– Spaltproduktrückhaltung im Reaktorgebäude	Nein	Ja
– Spätere Freisetzung von Sumpfwasser oder Wasser-Pool	Nein	Ja
– Hochdruckfreisetzung	Nein	Ja

Tabelle 8.

Schlussbetrachtungen

Die Methodik probabilistischer Risikoanalysen (PRA) ist für Kernkraftwerke weit entwickelt und vielfach umfassend angewandt. Sie weist aber einige grundsätzliche Grenzen und Defizite in Schlüsselbereichen (abhängige Ausfälle, menschliches Fehlverhalten) auf. Die Überprüfbarkeit der Ergebnisse im streng wissenschaftlichen Sinne ist nicht gegeben oder nur ansatzweise möglich; die Aussagen sind ohnehin nur als Schätzwerte zu betrachten. Hinsichtlich der Aussagekraft von PRA ist ein differenziertes Urteil vonnöten:

□ Quantitative Risikoanalysen liefern wertvolle Erkenntnisse über die Relevanz von Ereignissen/Ereignisketten, anlageninternen Notfallschutzmassnahmen und anlagentechnische Ver-

besserungen («Schwachstellenanalyse»). Gesicherte Relativaussagen sind möglich und helfen, die Ausgewogenheit des Sicherheitskonzeptes zu beurteilen.

□ Die Kernschmelzhäufigkeit kann als Beurteilungsmassstab der Anlagensicherheit herangezogen werden, wenn die Werte innerhalb des Vertrauensintervalls um weniger als einen Faktor 10 schwanken, was meist der Fall ist.

Nach den vorliegenden Studien liegt die Kernschmelzhäufigkeit für westliche Anlagen im Bereich von 0,0001 bis 0,00001 pro Reaktor-Jahr. Die Aussagekraft dieser Ergebnisse ist relativ hoch:

Zur Überprüfung können empirische Daten herangezogen werden, methodische Defizite sind zwar bedeutsam, aber noch nicht dominierend, sie können mit plausiblen Annahmen überbrückt werden; sie werden durch aufgetretene Ereignisse/Unfälle nicht widerlegt - *Tschernobyl ist nicht übertragbar.*

In diesem Bereich könnten die Ergebnisse auch im Sinne von Absolutaussagen genützt werden; der Nachweis, dass quantitative Sicherheitsanforderungen («safety goals») erfüllt werden, wäre möglich.

□ Bei einer Nutzung der Ergebnisse von Risikoanalysen im Bereich noch kleinerer Häufigkeiten ist grosse Vorsicht geboten: Eine ausreichende Vollständigkeit betrachteter Ereignisse/Ereignisabläufe ist nur schwer zu erreichen bzw. nachzuweisen, wichtige Ereignisse (Einwirkungen Dritter) entziehen sich einer adäquaten Behandlung, methodische Defizite liessen sich durch konservative Ansätze mindern, was aber auch zu unrealistischen Ergebnissen führen könnte (Beispiel «Kaputtrechnen» hochredundanter Systeme über einen hohen fiktiven Anteil abhängiger Ausfälle).

Die Methodik probabilistischer Risikoanalysen sollte unter Nutzung von Betriebserfahrungen im Bereich der Kerntechnik weiter entwickelt und ihren Möglichkeiten entsprechend eingesetzt werden. Vorrangiges Ziel muss aber auch sein, sie für den Einsatz in anderen industriellen Bereichen zu qualifizieren und langfristig Risikovergleiche zu ermöglichen.

Adresse der Verfasser: Prof. Dr. *W. Kröger*, Paul-Scherrer-Institut (PSI), 5232 Villigen, *S. Chakraborty*, Hauptabteilung für die Sicherheit der Kernanlagen (HSK), 5303 Würenlingen.

Literatur

[1] American Nuclear Society and the Institute of Electrical and Electronics Engineers: PRA Procedures Guide, NUREG/GR-2300, January 1983

[2] *Swain, A.D., Guttmann H.E.:* Handbook of Human Reliability Analysis with Emphasis on Nuclear Power plant Application, Final Report, NUREG/CR-1278, August 1983

[3] *Minarick J.W. et al.:* Precursors to Potential Severe Core Damage Accidents: 1984 and 1986, A Status Report, NUREG/CR-4674 (1987), and NUREG/CR-4674 (1988)

[4] *Hauptmanns U., Herttrich M., Werner W.:* Technische Risiken, Ermittlung und Bewertung, Springer-Verlag 1987

[5] U.S. Nuclear Regulatory Commission, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (1989) NUREG-1150

[6] *Garrick B. John:* Lessons Learned from 21 Nuclear Plant Probabilistic Risk Assessments, Nuclear Technology, Vol. 84 (March 1989)

Blitzschutz von Gebäuden mit empfindlichen elektronischen Systemen

Zweck des Blitzschutzes ist es, Personen und Material vor den schädlichen Einwirkungen des Blitzschlages zu bewahren. Diese Aufgabe hat in den letzten Jahren infolge der starken Ausbreitung von EDV-Anlagen beziehungsweise empfindlichen elektronischen Systemen (Alarmanlagen, Personalsuchanlagen, usw.) stark an Bedeutung gewonnen. Verantwortlich dafür ist nicht zuletzt die Betriebssicherheit der Systeme, der immer mehr Gewicht zukommt. Dieser Beitrag zeigt, wie durch Anpassung des Schutzgrades an die systemeigene Stör- oder Zerstörfestigkeit und schon beim Bau des Gebäudes getroffene Massnahmen ein effizienter und kostengünstiger Schutz bewerkstelligt werden kann.

Einleitung

Stör- und Zerstörfestigkeit der EDV-Anlagen

Störungen, die auf ein System einwirken, rufen, sofern sie einen genügenden Pegel aufweisen, eine Verfälschung der

VON WERNER HIRSCHI UND HUBERT SAUVAIN, ROSSENS

Nutzgrössen hervor. Als Störfestigkeit wird der Störpegel bezeichnet, bei welchem diese Verfälschung gerade noch zulässig ist [1]. Analog dazu nennt man den Störpegel, der knapp unterhalb der Grenze zwischen Verfälschung und Zerstörung liegt, die Zerstörfestigkeit.

Stör- und Zerstörfestigkeit der logischen Grundbauteile nehmen leider mit fortschreitender Technologie ab. Die Energie, die notwendig ist, um ein Logik-Element (z.B. integrierter Schaltkreis) zum Schalten zu bringen, wird aus verständlichen Energie-Spargründen immer kleiner. Dies bewirkt, dass auch die Energie, die notwendig ist, um dieses Element zu stören, sinkt, und dass somit die Wahrscheinlichkeit einer Störung durch äussere Beeinflussungen erhöht wird. In gleicher Weise führt die fortschreitende Miniaturisierung zu einer Erhöhung der Zerstörempfindlichkeit. Es braucht immer weniger Energie, um ein logisches Grundelement mit seinem kleiner werdenden Volumen und den dünner werdenden Verbindungen zum Nachbarelement zu zerstören (Bild 1, [2]).

Die zunehmende Vernetzung der EDV-Anlagen führt ebenfalls zur Verminderung der Stör- und Zerstörfestigkeit. Der Schutzgrad der einzelnen Anlagen leidet sehr unter der zunehmenden Zahl und Länge von Verbindungskabeln zur Aussenwelt. Diese Kabel fangen Störenergie aus der Umgebung ein und verstärken unter Umständen ihre Wirkung noch.

Mittlerweile bemühen sich die Hersteller - zum Beispiel durch Einhaltung von Normen - die Systeme so auszulegen, dass sie in der Lage sind, in ihrer späteren Betriebsumgebung störungsfrei zu funktionieren. Es gibt jedoch gewisse Bereiche, die schwer abzudecken sind, weil sie eher von der Infrastruktur des Anwenders abhängen. Dies trifft beim Blitzschutz besonders zu.