Zeitschrift: Schweizer Ingenieur und Architekt
Herausgeber: Verlags-AG der akademischen technischen Vereine
Band: 110 (1992)
Heft: 47

Artikel: Kernkraftwerke: Weiterentwicklung: Stand der Auslegung und Sicherheitsphilosophie
Autor: Fuchs, Hans
DOI: https://doi.org/10.5169/seals-77989

chen Konkretisierung des Vorhabens (Variantenbeschreibung und -evaluation) die kantonale Richtplanung als Koordinationsinstrument zum Einsatz. Nach der erfolgten räumlichen Festlegung des Vorhabens wird in der dritten Stufe das konkrete Projekt ausgearbeitet und die UVP (gemäss USG) durchgeführt.

An alle Beteiligten geht die Aufforderung, sich nicht auf die eigenen, bisweilen engen Bahnen zu beschränken, sondern sich vom sektoriellen Denken zu lösen und mehr Zusammenarbeit anzustreben, die eine zweckmässigere Organisation unseres Lebensraumes (und somit eine lebenswerte Umwelt) ermöglicht. Ein gangbarer Weg des Zusammenwirkens ist hier aufgezeigt worden. Entsprechende Anwendungen in der Praxis haben den Beleg der Tauglichkeit des Ansatzes gezeigt. Nun gilt es, bei der Planung und Projektierung grosser raum- und umweltrelevanter Vorhaben entsprechend konsequent zu handeln.

Adresse des Verfassers: *PD Dr. Peter Gresch*, und *Markus Eggenberger*, c/o Elektrowatt Ingenieurunternehmung AG, Bellerivestrasse 36, 8034 Zürich.

Sicherheit und Risiko

Kernkraftwerke: Weiterentwicklung

Stand der Auslegung und Sicherheitsphilosophie

Uran ist eine sehr konzentrierte Energiequelle, die sich ohne Reaktion mit der Atmosphäre nutzen lässt. Kernkraftwerke (KKW) können deshalb als geschlossene Systeme Energie erzeugen ohne stoffliche Wechselwirkung mit der Umgebung.

VON HANS FUCHS, BADEN/OLTEN

Diese umweltfreundliche «Trumpfkarte» der KKW hat aber auch ihre Kehrseite: Die bei der Kernspaltung entstehenden radioaktiven Spaltprodukte stellen ein Schadenspotential dar, das seit jeher eine vorbeugende Auslegung mit Sicherheitseinrichtungen verlangte. Diese wurden später ergänzt und erweitert aufgrund praktischer Erfahrungen und weiterentwickelter Methoden der Sicherheitsanalyse. Die erreichbare Sicherheit hängt dennoch weniger von Details dieser Methoden ab als vielmehr von der konsequenten Anwendung und Umsetzung der grundlegenden Erkenntnisse über die in KKW ablaufenden Prozesse.

Sicherheitsfunktionen bei einem Kernkraftwerk

Konventionell-thermische Kraftwerke arbeiten als offene Systeme: der kontinuierlich zugeführte Brennstoff reagiert mit dem Sauerstoff der Umgebungsluft, und die entstehenden Verbrennungsgase werden nach geeigneter Behandlung laufend an die Umgebung abgegeben. In Kernkraftwerken läuft demgegenüber die energieliefernde Kettenreaktion ohne Stoffaustausch mit der Umgebung – d. h. als *geschlossenes System* – ab.

Diesem für die Umwelt sehr vorteilhaften Umstand steht ein *Schadenspotential* gegenüber, das sich daraus ergibt, dass:

- ein neuer Reaktorkern potentiell die Energie für etwa ein Jahr Betrieb enthält
- auch nach Unterbruch der Kettenreaktion wegen des radioaktiven Zerfalls von Spaltprodukten noch etwas Wärme erzeugt wird. Diese sogenannte Nachwärme beträgt kurz nach dem Abschalten einige Prozent der vorherigen Reaktorleistung und sinkt nach etwa 3 Stunden unter 1% ab
- die bei der Kernspaltung entstehenden Reaktionsprodukte (namentlich die radioaktiven Spaltprodukte) sich in den Brennelementen akkumulieren, soweit sie nicht kurzfristig zerfallen.

Daraus folgen unmittelbar die drei elementaren *Sicherheitsfunktionen:*

☐ Beherrschen der Kettenreaktion und damit der Reaktorleistung durch

- selbstbegrenzende Auslegung (negativer Leistungskoeffizient),
- zuverlässige Abschaltmechanismen (Kontrollstäbe, Boreinspeisung).

☐ Abfuhr der Nachwärme,

☐ Einschluss/Rückhalten der radioaktiven Stoffe («Containment», Aktivitätsrückhaltung).

Diese Sicherheitsfunktionen sind seit Beginn der Kernreaktorentwicklung, d. h. seit den 1940er Jahren grundsätzlich bekannt; in Regelform fixiert wurden sie in den USA in den 60er Jahren, in der Sowjetunion spätestens 1982, inkl. der Forderung nach einem negativen Leistungskoeffizienten – tragisch, dass gerade diese Forderung bei Tschernobyl nicht eingehalten war. Bei diesem Unglücksreaktor führte deshalb 1986 das berüchtigt-fahrlässige Experiment zu einer sich von selbst beschleunigenden Kettenreaktion, die den Reaktorkern derart überhitzte, dass er buchstäblich platzte. Dieser Unfall demonstriert auch die Hierarchie der oben aufgeführten Sicherheitsfunktionen: die nicht beherrschte (unkontrollierte) Kettenreaktion zerstörte die Systeme zur Nachwärmeabfuhr ebenso wie die (unvollständigen) Einrichtungen zur Rückhaltung der radioaktiven Stoffe.

Klassisches Vorgehen zur Auslegung und Analyse von Kernkraftwerken

Auslegungsstörfälle

Zur Erfüllung der oben genannten Sicherheitsfunktionen sind eine Reihe von Einrichtungen (Strukturen, Systeme, Komponenten) erforderlich, die als *«Sicherheitseinrichtungen»* bezeichnet werden. Ihre Auslegung erfolgt anhand von sogenannten «Auslegungstörfällen». Dies sind angenommene Ereignisabläufe, die durch ein externes (z.B. Erdbeben) oder internes (z.B. Rohrbruch) Ereignis ausgelöst werden und die gemäss Tabelle 1 gruppiert werden können. «Transienten» sind durch Störungen ausgelöste Abweichungen vom Normalbetrieb, die zu einem vorübergehenden Ungleichgewicht zwischen Wärmeproduktion und Wärmeabfuhr im Reaktorkern führen. Als «Kühlmittelverlust» wird der Verlust von Primärkühlmittel (das die im Reaktorkern erzeugte Wärme abführt) bezeichnet.

Gruppierung der Auslegungsstörfälle nach...			
.. auslösendem Ereignis		*.. Störfallablauf*	
äussere Ereignisse	*innere Ereignisse*	*Kühlmittelverlust*	*Transienten*
Ausfall des Fremdnetzes	Lecks, Rohrbruch	Leck im Primärkreislauf	Turbinenschnellschluss
Extreme meteorologische Zustände	Auswurf eines Regelstabs	Fehlerhaftes Öffnen von Absperrarmaturen des Primärkreislaufs	Auswurf eines Regelstabs
Erdbeben	Ausfall des Hauptspeisewassers	Rohrleitungsbruch im Primärkreislauf	Ausfall einer Hauptkühlmittelpumpe

Tabelle 1. Gruppierung der Auslegungsstörfälle mit Beispielen zugehöriger auslösender Ereignisse

- Kühlmittelverlust infolge Bruchs einer Hauptkühlmittelleitung
- Kernschmelzen infolge ungenügender Notkühlung
- teilweise Freisetzung von radioaktivem Material in die Containment-Atmosphäre:
  - 100 % der Edelgase
  - 50 % der Halogene, wovon die Hälfte verfügbar für Leckage nach aussen
  - 1 % der festen Spaltprodukte

Tabelle 2. «Maximum credible accident» (grösster anzunehmender Unfall) oder «Design basis accident» (Auslegungsstörfall) nach US-Regeln

Auslegung gegen äussere Ereignisse

Die Auslegung gegen äussere Ereignisse folgt z.B. bezüglich Windlasten oder Extremtemperaturen der auch bei konventionellen Kraftwerken üblichen Vorgehensweise, berücksichtigt allerdings auch viel weniger häufige Ereignisse. Analog werden die sicherheitstechnisch wichtigen Einrichtungen so bemessen, dass sie ihre Funktion auch während oder nach einem sehr seltenen Erdbeben wahrnehmen können. Die Methoden zur Erdbebenauslegung sind durch die umfangreichen Entwicklungen im Kernkraftwerksbau in entscheidender Weise gefördert worden.

Vom «Gau» zum massgeblichen Auslegungsstörfall

Massgeblich für die Wahl und die Ausgestaltung der Sicherheitseinrichtungen ist der sogenannte «maximum credible accident» (MCA), der im deutschen Sprachraum als «grösster anzunehmender Unfall» (GaU oder Gau) umschrieben wurde. Der MCA geht auf amerikanische Arbeiten der 1950er und frühen 1960er Jahre zurück und beschreibt den in Tabelle 2 zusammengefassten postulierten Ereignisablauf.

Er wurde später in «Design basis accident» (Auslegungsstörfall) umbenannt, weil er in den USA v.a. für die Dimensionierung des Sicherheitseinschlusses (Containment), die Qualifizierung von Sicherheitseinrichtungen, die Bewertung von Standorten und die Planung von Notfallmassnahmen als Grundlage herangezogen wurde [1–4]. Das gilt im wesentlichen auch heute noch; allerdings wurden seither die Notkühlsysteme auf diesen Kühlmittelverlust (grosser KMV oder grosser LOCA, loss of coolant accident) infolge des angenommenen Bruchs einer Hauptkühlmittelleitung derart ausgelegt, dass eine ins Gewicht fallende Beschädigung des Reaktorkerns mit hoher Zuverlässigkeit vermieden wird; die Freisetzungen gemäss Tabelle 2 sind daher für diesen Fall nicht mehr realistisch. Aus diesem Grund wurde der Auslegungsstörfall KMV teilweise leicht modifiziert; er bestimmt aber nach wie vor zur Hauptsache die Auslegung der meisten Sicherheitseinrichtungen.

Sicherheitsanalyse

Die klassische *deterministische Sicherheitsanalyse* überprüft im Detail, ob gemäss anwendbaren Erfahrungen alle die Auslegung möglicherweise beeinflussenden Störfälle adäquat berücksichtigt worden sind. «Adäquat» heisst praktisch «with adequate margins», d. h. mit auf der pessimistischen Seite liegenden Annahmen und ausreichenden Zuschlägen für eventuell noch verbliebene Ungewissheiten. Beim grossen KMV wird beispielsweise unterstellt, dass gleichzeitig das Fremdnetz nicht verfügbar ist und ein Strang des Notkühlsystems ausfällt («Einzelfehler»). Verschiedene Länder verlangen zudem, dass ein weiterer Strang wegen Instandhaltung als nicht einsatzfähig anzusehen sei. Die Wirksamkeit der verbleibenden Notkühlung wird dann nach vorsichtigen Rechenverfahren und Kriterien beurteilt [5]. Zusammengefasst untersucht man in der deterministischen Sicherheitsanalyse anhand von repräsentativen Auslegungsstörfällen, ob die Anlage derart konstruiert ist, dass sie den Schutz der *Bevölkerung* und des *Betriebspersonals* gewährleistet.

Besondere Prinzipien zur Auslegung von KKW

Oberstes Gebot bei der Auslegung ist die zuverlässige Erfüllung der bereits genannten Sicherheitsfunktionen bei allen vernünftigerweise anzunehmenden Störfällen: Dazu dienen namentlich die folgenden Prinzipien:

«Defence in depth», tiefgestaffelte Verteidigung

Dieses Prinzip zur Beherrschung eines Schadenpotentials kann am einfachsten anhand der *mehrfachen Barrieren* gegen die Freisetzung radioaktiver Stoffe aus einem KKW erklärt werden. Tabelle 3 erläutert die hintereinander gestaffelten Barrieren. Wie bei militärischen Einrichtungen ist deren Wirkung aber nur dann von Dauer, wenn Angriffe auf die Integrität der einzelnen Barrieren durch besondere Systeme abgewehrt werden. Bei einem angenommenen Bruch einer Hauptkühlmittelleitung verhüten beispielsweise die Notkühlsysteme eine Überhitzung des Brennstoffes und der Hüllrohre, und ein Schutzsystem veranlasst die Schliessung von Durchdringungen des Containments. Nebst bei diesen Massnahmen zur Erfüllung der Sicherheitsfunktion «Aktivitätsrückhaltung» (vgl. oben) wird «Defence in depth» in Form von *Schutzebenen* aber noch in viel allgemeinerer Art angewendet, wie Tabelle 4 erläutert. Teilweise wird die 4. Ebene noch weiter unterteilt nach anlageninternen und -externen Massnahmen.

Beispiele von Vorkehrungen im Rahmen der einzelnen Schutzebenen gibt Tabelle 5.

Zusammengefasst werden nach dem «Defence in depth»-Prinzip ungeachtet der umfassenden Massnahmen zur Perfektionierung der 1. und 2. Schutzebene noch weitere Schutzebenen vorgesehen, die bei dennoch angenommenem Versagen der vorhergehenden Ebenen Schutz oder zumindest Linderung bieten.

Redundanz und Diversität

Die eingangs zitierten drei Sicherheitsfunktionen werden z.T. durch passive Einrichtungen (Behälter, Barrieren), z.T. durch aktive oder passive Systeme wahrgenommen. Diese sogenannten Sicherheitssysteme werden zur Erhöhung der Zuverlässigkeit der Funktion mehrfach ausgeführt, d.h. es gibt mehr Systeme als erforderlich sind («Redundanz»). Dieses *«Mehr vom Gleichen»* kann aber dann nicht voll zum Tragen kommen, wenn gewisse Ursachen mehrere Systeme gleichzeitig beeinträchtigen könnten («common cause failures»). In solchen Fällen wird das Prinzip *«Mehr, aber verschieden»* (Diversität) angewendet: Verwendung unterschiedlicher Messgrössen für die Feststellung von Abweichungen, Einsatz verschiedenartiger Methoden zur Einspeisung von Notkühlwasser usw.

In der Sicherheitsanalyse wird anhand der Einzelfehler-Kriterien (vgl. weiter unten) überprüft, ob die Sicherheitssysteme ausreichend redundant sind. Ferner ist zu prüfen, ob die Systeme durch Diversität und/oder Separation (vgl. nachstehend) gegen Fehler aus gemeinsamer Ursache abgesichert sind.

Unabhängigkeit/Separation

Damit redundante Systeme eine *hohe Zuverlässigkeit* erreichen, müssen sie unabhängig sein, d.h. sie dürfen sich beispielsweise nicht auf ein gemeinsames Hilfssystem (zur Kühlung, Lüftung, Schmierung usw.) abstützen oder auch sonst nicht durch ein einzelnes Ereignis gemeinsam ausser Funktion setzen lassen.

Solch ein einzelnes Ereignis könnte ein Versagen eines druckführenden oder rotierenden Teils eines Systems sein, das zu *Folgeschäden* an den redundanten Systemen führt. Hier hilft Separation durch Distanz und/oder Barrieren, aber u.U. auch die schon erwähnte diversitäre Ausführung. Falls die Systeme aber die Eigenschaft haben, in die sichere Richtung zu versagen *(Fail-safe-Verhalten)*, so können besondere Trennmassnahmen entfallen.

Die Analyse bezüglich Unabhängigkeit/Separation erfordert eine sehr eingehende Prüfung des Systemverhaltens und der örtlichen Gegebenheiten – wen wundert es, dass Möchtegern-«Experten» gerade bei der Beurteilung von älteren Reaktoren in diesen Punkten oft zu völlig fehlerhaften Ergebnissen kommen...

Berücksichtigung der Faktoren Mensch und Zeit

Der Störfall 1979 im amerikanischen KKW Three Mile Island (TMI) hat eindringlich die Bedeutung einer *ergonomischen* Gestaltung des Kommandoraums aufgezeigt. In vielen Ländern wurden danach Verbesserungen eingeführt, um den Operateuren eine möglichst gute Übersicht über den Anlagenzustand zu geben und ihnen insbesondere bei Störungen und Störfällen eine klare Diagnose zu ermöglichen. Schon vorher waren natürlich Absicherungen gegen zu erwartende Bedienungsfehler eingebaut worden, z.B. in Form von *Verriegelungen*, Begrenzungen und Schutzsystemen. Nach TMI wurden insbesondere die Absicherungen gegen fehlerhaft belassene Armaturenstellungen verbessert (Schlüsselsicherungen, Positionsanzeigen usw.).

Der Mensch ist kein Roboter – er ist deshalb nicht sehr erfolgreich, wenn es gilt, innert sehr kurzer Zeit (Sekunden) wichtige Eingriffe vorzunehmen. Reaktoroperateure haben dagegen mehrfach bewiesen, dass sie auch höchst vertrakte und komplexe Situationen meistern können, wenn ihnen *genügend Zeit* zur Verfügung steht.

Beim KKW erfordert die 1. Sicherheitsfunktion (Beherrschen der Reaktorleistung, Abschalten) u.U. eine sehr rasche (innert Sekunden) und höchst zuverlässige Detektion und Reaktion. Diese werden deshalb nicht nur durch entsprechend sichere und schnelle Schutz-, Steuer- und Abschaltmechanismen realisiert, sondern mindestens teilweise auch durch inhärente (selbstbegrenzende) Eigenschaften des Reaktorkerns: ein auf einen negativen Leistungskoeffizienten ausgelegter Kern bremst bei übermässiger Leistung (Erwärmung) die Kettenreaktion infolge temperaturbedingt erhöhter Neutronenabsorption von selber.

Da bei Störungen auch andere Sicherheitsfunktionen zeitgerecht wahrgenommen werden müssen, werden auch diese automatisch durch den *Reaktorschutz* initiiert. Die Operateure müssen deshalb während der ersten 30 Minuten nach einem Störfall nicht eingreifen; teilweise ist diese *«Schonfrist»* («grace period») auch länger.

Die Faktoren Mensch und Zeit waren beim Tschernobyl-Reaktor praktisch völlig missachtet worden – es war deshalb pervers, den Operateuren die Schuld zuzuschieben. In Wirklichkeit hatten sie bei den Bedingungen des ominösen Experiments überhaupt keine Chance. Der Leistungskoeffizient des Reaktorkerns war positiv, und die einfahrenden Abschaltstäbe wirkten anfänglich in die falsche Richtung, d. h. sie beschleunigten den Leistungsausbruch (run-away-Reaktion) zusätzlich.

1. Barriere:	Matrix des Brennstoffs (Uranoxid)
2. Barriere:	Hüllrohre der Brennstoff-Tabletten
3. Barriere:	Reaktordruckbehälter und Primärkreislauf
4. Barriere:	Sicherheitseinschluss (Containment)

Tabelle 3. Hintereinander gestaffelte Barrieren gegen die Freisetzung radioaktiver Stoffe aus einem KKW

1. Ebene:	Vorbeugen	Normalbetrieb
2. Ebene:	Abweichungen korrigieren	Betriebsstörungen
3. Ebene:	Schützen	Auslegungsstörfälle
4. Ebene:	Auswirkungen begrenzen	Auslegungsüberschreitende Störfälle, schwere Unfälle

Tabelle 4. Hierarchie der Schutzebenen und zugeordnete Anlagenzustände

1. Vorbeugen	Fehler vermeiden: Qualitätssicherung, behördliche Prüfung/Aufsicht, periodische Tests/Inspektionen, Instandhaltung, Ausbildung/Training...
2. Abweichungen korrigieren	selbstbegrenzende/selbstkorrigierende Eigenschaften (Stabilität), Regel- und Begrenzungseinrichtungen, Reparaturen/Ersatz...
3. Schützen	Reaktorschutzsystem, Sicherheitseinrichtungen, Diagnosehilfsmittel, Störfallanweisungen...
4. Auswirkungen begrenzen	Sicherheitseinrichtungen, Notfallmassnahmen intern (accident management) und extern

Tabelle 5. Beispiele von Vorkehrungen im Rahmen der einzelnen Schutzebenen

Die Einzelfehlerkriterien und ihre Weiterentwicklung

Vom einfachen Konzept...

Nach den ursprünglichen amerikanischen Vorschriften [6] ist ein Einzelfehler: *«ein Ereignis, das den Verlust der Si-*

Ein EF ist bei wichtigen Sicherheitsfunktionen zu unterstellen und z.T. mit Instandhaltung (REP) wie folgt zu kombinieren:

	EF	*REP*
Reaktorschutz	x	x
Reaktorabschaltung	x	x
Nachwärmeabfuhr	x	x
Notstrom	x	x
Wärmeabfuhr aus Sicherheitseinschluss	x	

Weder EF noch REP ist zu unterstellen bei sehr seltenen Ereignissen:

- Betriebstransiente mit Versagen der Schnellabschaltung
- Flugzeugabsturz
- Explosionsdruckwelle
- Ereigniskette mit sehr geringer Eintrittswahrscheinlichkeit

Tabelle 6. Einzelfehler (EF) – Kriterien nach deutschen Vorschriften

Anlagenzustand	*Häufigkeit F des auslösenden Ereignisses pro Reaktorjahr*	*Max. Dosis am Kraftwerkszaun*
1	Normalzustand	5 mrem/a
2	$F > 10^{-1}$	durchschn. 5 mrem
3	$10^{-1} > F \geq 10^{-2}$	2.5 rem
4	$10^{-2} > F \geq 10^{-4}$	6.3 rem
5	$10^{-4} > F \geq 10^{-6}$	25 rem

Tabelle 7. Kategorisierung der auslösenden Ereignisse nach neueren amerikanischen Einzelfehlerkriterien [8]

cherheitsfunktion einer Komponente zur Folge hat».

Praktisch konzentrierte man sich dabei auf sogenannte *«aktive»* Komponenten, bei denen eine mechanische Bewegung für die Erfüllung der Sicherheitsfunktion nötig ist. Das führte dazu, dass z.B. bei einem Not-Einspeisesystem ein Strang mehr installiert wurde als für die Noteinspeisung erforderlich gewesen wäre. Da ein Einzelfehler irgendwo auftreten kann, erhielten alle Sicherheitssysteme mit aktiven Komponenten je einen zusätzlichen Strang (d.h. pro System mit n Strängen insgesamt (n + 1) Stränge).

In einfacher Form wird das Einzelfehlerkonzept u.a. auch bei Strom- oder Wasserverteilnetzen angewendet; man spricht dort von «zwei Zuleitungen» oder «single contingency».

... zu Weiterentwicklungen in Deutschland

Bereits zu Beginn der 1970er Jahre wurde in Deutschland zusätzlich zu einem Einzelfehler noch der *Instandhaltungsfall* postuliert, was bei wichtigen Sicherheitssystemen zu je zwei «Reservesträngen» führte, d.h. insgesamt zu (n + 2) Strängen. Nach [7] ist ein Einzelfehler (EF):

- unabhängig vom auslösenden Ereignis
- nicht eine Folge des Anforderungsfalls.

Der Einzelfehler

- kann Folgefehler auslösen
- deckt Common-Cause-Fehler nicht ab, ebensowenig mögliche Kombinationen unabhängiger Ereignisse.

Grundsätzlich kann der EF aktiv oder passiv sein; bei Auslegung entsprechend der sicherheitstechnischen Funktion braucht ein passiver EF jedoch nicht unterstellt zu werden. Weitere Erläuterungen hierzu gibt Tabelle 6.

Die Forderung nach (n+2) Strängen gilt u.a. auch in Grossbritannien, Schweden, Finnland, der Schweiz sowie im wesentlichen in der ehemaligen UdSSR.

... und in den USA

Die früher streng deterministischen Einzelfehlerkriterien wurden mit probabilistischen Elementen ergänzt, insbesondere wurden die auslösenden Ereignisse bzw. ihre Kombination mit gleichzeitig auftretenden anderen Ereignissen nach *Häufigkeitsklassen* unterteilt, denen unterschiedliche Grenzwerte für die Auswirkungen zugeordnet sind. Zu diesen Klassen gehören auch Anforderungen bezüglich Funktionsfähigkeit und zugehörigen Grenzwerten der mechanischen Beanspruchung. Details geben [8, 9] sowie Tabelle 7. Die Kategorisierung nach Häufigkeitsklassen ist sinngemäss z. B. auch von Frankreich und der Schweiz übernommen worden.

Trotz ihrer Weiterentwicklung sind die Einzelfehlerkriterien nach wie vor einfach anwendbare Werkzeuge für die Auslegung und Analyse von KKW. Werden sie konsequent und unter Berücksichtigung der Ergonomie und der Common-Cause-Problematik eingesetzt, so ist ein sehr hoher Sicherheitsgrad erreichbar.

Der Einsatz probabilistischer Methoden

Von ersten Ansätzen...

Ein in einem militärischen Reaktor 1957 in England aufgetretener Störfall führte zum systematischen Einsatz probabilistischer Methoden: Sammlung von Ausfalldaten, Zuverlässigkeitsanalysen von Komponenten und Systemen im Zusammenspiel mit dem Betriebspersonal, Vorschlag einer Grenzkurve (F. R. Farmer) nach dem Prinzip: «je häufiger ein unerwünschtes Ereignis, desto geringer müssen die Folgen sein» und umgekehrt «je schlimmer die mögliche Tragweite, desto unwahrscheinlicher das Ereignis».

Bemerkenswert ist, dass solche Methoden auch für Chemieanlagen eingesetzt wurden (die von der gleichen Behörde beaufsichtigt werden wie die Nuklearanlagen).

... über Pionierarbeiten ...

Prof. Rasmussen stützte sich namentlich auf die englischen Vorarbeiten ab, als er 1973–75 den nach ihm benannten Bericht über die mit dem Betrieb kommerzieller KKW in den USA verbundenen Risiken erstellte. Er benützte vorwiegend die Ereignisbaum-/Fehlerbaumanalyse und verwendete Zuverlässigkeitsdaten aus dem nuklearen und konventionellen Bereich. Es zeigte sich, dass das Risiko von Kernkraftwerken deutlich geringer ist als dasjenige traditioneller Technologien oder natürlicher Ereignisse. Bedeutsam für die Weiterentwicklung der Sicherheitsmethodik war aber die Erkenntnis, dass das Risiko von KKW nicht durch den Auslegungsstörfall «grosser Kühlmittelverlust» bestimmt wird, sondern durch den *«kleinen»* Kühlmittelverlust bzw. durch *Transienten.*

Der Rasmussen-Bericht initiierte in Deutschland eine analoge Untersuchung (Deutsche Risikostudie), die schon bald zu konkreten Verbesserungen beim untersuchten Reaktor führte. In den USA fand dagegen die Rasmussenstudie (Prophet im eigenen Vaterland!) vorerst wenig Anwendung.

... zu breiter Anwendung ...

Nach dem Störfall im amerikanischen KKW Three Mile Island (1979) brach sich zunehmend die Erkenntnis Bahn, dass eine probabilistische Analyse die Schwächen dieser Anlage hätte aufzeigen können, die offensichtlich bei der (zu wenig konsequenten) deterministischen Überprüfung übersehen wurden. Weltweit sind seither probabilistische Sicherheitsanalysen als wertvolle *Ergänzung* zu den klassischen Methoden erkannt und vermehrt eingesetzt worden [10, 11]. Teilweise ergaben sich Bestätigungen: so zeigte die probabilistische Analyse des KKW Mühleberg, dass diese Anlage dank der auf deterministischer Basis realisierten Nachrüstungen einen Sicherheitsstand erreicht hat, der demjenigen moderner Anlagen gleichkommt. Gelegentlich traten aber auch Schwachstellen zutage, z.B. übersehene Vermaschungen redundanter Stränge durch Hilfssysteme in einigen amerikanischen KKW. Von besonderer Bedeutung sind auch die gewonnenen Erkenntnisse über den möglichen Ablauf *auslegungsüberschreitender* Störfälle, die die Planung anlageninterner Notfallmassnahmen (accident management) ermöglichen.

Wo stehen wir heute?

Weltweite Erfahrungen und Zielsetzungen

Zur Zeit sind weltweit mit KKW (von denen etwa 425 in Betrieb stehen) rund 6000 Reaktorbetriebsjahre akkumuliert worden. Dabei sind 2 Kernschadensfälle aufgetreten: Three Mile Island 1979 (ohne merkliche Folgen für die Umgebung) und Tschernobyl 1986 (mit gesundheitlichen Folgen im Rahmen leider gewohnter ziviler Katastrophen und mit rekordverdächtigen wirtschaftlichen Konsequenzen). Beide Fälle gaben weltweit bei KKW Anlass zu Überprüfungen, Verbesserungen oder Nachrüstungen. Ein Beratungsgremium (INSAG) der Internationalen Atomenergieorganisation (IAEO) stellte in diesem Zusammenhang ein Kompendium bewährter Sicherheitsgrundsätze [12] zusammen und schlug darin als Ziel für bestehende Anlagen eine Kernschadenshäufigkeit von $< 10^{-4}$ pro Reaktorjahr vor, wobei die Wahrscheinlichkeit für eine die Umgebung gefährdende Aktivitätsfreisetzung um mindestens einen Faktor 10 kleiner sein soll. Für neue KKW wurde eine Kernschadenshäufigkeit von $< 10^{-5}$ pro Reaktorjahr gefordert, ebenfalls mit einer um den Faktor 10 kleineren Wahrscheinlichkeit für eine grössere Aktivitätsfreisetzung.

Sind die Ziele erreichbar?

Vergleicht man Three Mile Island (1979) mit den bisherigen gut 5000 Reaktorjahren in Leicht- und Schwerwasserreaktoren, so stellt man fest, dass 1/5000 zwar grösser als 10^{-4}, aber statistisch damit verträglich ist. Analysen und Auswertungen von Vorläuferereignissen aus den USA zeigen [13], dass die Kernschadenshäufigkeit dort von etwa 10^{-3} > pro Reaktorjahr zur Zeit von TMI jetzt auf rund 10^{-4} bis 10^{-5} *gesunken* ist.

Bedenklicher wird der Vergleich des Tschernobyl-Unfalls 1986 mit den jetzt rund 240 Reaktorbetriebsjahren mit diesem Typ. Zum Zeitpunkt des Unfalls betrug die empirische Häufigkeit für ein derart schweres Versagen fast 10^{-2} pro Reaktorjahr! Daraus wird verständlich, dass umfangreiche Verbesserungen erforderlich waren und dass dieser Reaktortyp kaum mehr weitergebaut wird.

Zusammengefasst sind somit die von der INSAG postulierten Ziele mit *bewährten* Reaktortypen erreichbar.

Auf dem Weg zu einer Sicherheitskultur

Die aufgeführten Beispiele und andere Sicherheitsüberprüfungen zeigen, dass weiterentwickelte Methoden für die Auslegung und Analyse zwar hilfreich sind – entscheidend ist aber vor allem die konsequente und gründliche Anwendung mindestens *einer Methode* sowie die Umsetzung der gewonnenen Erkenntnisse in die Praxis.

Lit. [12] und insbesondere [14] definieren dazu den Begriff «Sicherheitskultur». Diese umfasst alle Eigenschaften und Grundhaltungen von Individuen und Organisationen, die dazu beitragen, der nuklearen Sicherheit die erforderliche *Priorität* zu geben. Dies beginnt bei der aufmerksamen, vor- und umsichtigen, aber auch kommunikativen Haltung jedes einzelnen Mitglieds der Betriebsequipe und geht über die entsprechende Einstellung bei der Kraftwerksleitung und ihren übergeordneten Gremien sowie der staatlichen Aufsicht bis zur Gesetzgebung. In umgekehrter Richtung werden alle institutionellen und materiellen Voraussetzungen geschaffen, die einen sicherheitstechnisch vorbildlichen Betrieb der Anlagen ermöglichen.

Fehlen solche Voraussetzungen, dann bleiben z.B. gravierende Auslegungsfehler unkorrigiert bestehen ohne Wissen der Betreiber (wie bei Tschernobyl) oder Anzahl und Ausbildung der Operateure werden – ebenso wie die Mittel für den Unterhalt – derart ungenügend, dass die Anlage abgestellt werden muss (wie in Bulgarien).

Es wird somit Aufgabe einer übergeordneten Sicherheitskultur, im internationalen Rahmen Mittel und Wege zu schaffen, um auch bei den jetzigen «schwarzen Schafen» von KKW die Sicherheit auf einen international akzeptablen Stand zu heben – auf diese Weise lassen sich die Sicherheitsziele der INSAG erreichen.

Könnte «es» trotzdem morgen passieren?

Angenommen, es gäbe 500 Reaktoren weltweit, die alle die Forderung $< 10^{-4}$ Kernschadensfälle pro Reaktorjahr erfüllen, so wäre im Schnitt alle 20 Jahre mit einem Ereignis ähnlich Three Mile Island zu rechnen und alle 200 Jahre mit einem Ereignis mit grosser Freisetzung. Daraus liesse sich der Schluss ziehen, dass diese Reaktorpopulation wahrscheinlich die nützliche Lebensdauer erreichen würde, ohne die Umgebung ernsthaft zu gefährden. Natürlich kommt gleich der Einwand, auch ein wenig wahrscheinliches Ereignis könnte morgen passieren. Hier wird jedoch übersehen, dass ein schwerwiegender KKW-Unfall nicht mit einer Lottozahl vergleichbar ist, die ohne Vorwarnung bei der nächsten Auslosung erscheinen kann.

Anders ausgedrückt: kein schwerer KKW-Unfall ohne *Vorwarnung!*

Der Grund für die Vorwarnungen liegt darin, dass ein solcher Unfall nur aufgrund von hintereinander und unabhängig auftretenden, wenig wahrscheinlichen Einzelereignissen überhaupt denkbar ist, d.h. aufgrund einer *Verkettung* einer Reihe solcher Ereignisse. Solche Vorwarnungen, Einzelereignisse oder Vorläuferereignisse gab es übrigens vor Three Mile Island mehrfach – allerdings wurden sie damals noch nicht richtig interpretiert.

Das hat sich seither gründlich geändert: Vorläuferereignisse werden heute weltweit den Betreibern bekanntgemacht und ausgewertet; das ermöglicht Verbesserungen bei den betroffenen Gliedern möglicher Ereignisketten, so dass schlimme Folgen noch unwahrscheinlicher gemacht werden können.

Bei einem bezüglich der Kontrolle der Reaktorleistung richtig ausgelegten Reaktor laufen solche Ereignisketten aus physikalischen Gründen zudem nicht schlagartig ab, so dass dem Betriebspersonal Zeit für überlegte Eingriffe zur Verfügung steht (das war beim krass fehlerhaft ausgelegten und betriebenen Tschernobyl-Reaktor nicht der Fall!). Dank besonderer Einrichtungen kann selbst eine unwahrscheinlich weit fortgeschrittene Ereigniskette noch unterbrochen und der Folgeschaden vermindert werden.

Zusammengefasst kann bei den in einer guten Sicherheitskultur abgestützten

Reaktoren faktisch ausgeschlossen werden, dass ein schwerer Unfall «morgen» oder während ihrer Lebensdauer passiert. Wenn es bei Reaktoren aber an fast allem mangelt (wie oben an den Beispielen Tschernobyl und Bulgarien angedeutet), muss leider mit Störfällen gerechnet werden, die bis zu einem schweren Unfall gehen können.

Welche Entwicklungen sind abzusehen?

Bedürfnisse und Wünsche

Elektrizität wird weiterhin und sogar zunehmend der *«Lebenssaft»* der entwickelten und der sich entwickelnden Länder bleiben. Die starke Zunahme der Weltbevölkerung und ihrer Bedürfnisse führt zu einer gesteigerten Nachfrage nach Strom. Da aber eine entsprechend stärkere Nutzung *fossiler* Energieträger kaum (um)weltverträglich ist, müssen vermehrt *umweltneutrale* Techniken wie die Kernenergie eingesetzt werden. Voraussetzung ist allerdings, dass dabei dem verständlichen Wunsch «kein weiteres Tschernobyl» entsprochen werden kann. Das wird oft auch mit «unempfindlich gegen menschliches Versagen» oder *«inhärent sicher»* ausgedrückt. Wie weit sind solche Wünsche realisierbar?

Die evolutionäre Linie

Die meisten Länder mit kerntechnischer Industrie setzen die vorliegenden Erfahrungen mit Druck- und Siedewasserreaktoren ein für die Entwicklung sog. *«fortgeschrittener»* Leichtwasserreaktoren. Diese benutzen die besten und bewährtesten Elemente bisheriger Reaktoren, verwenden für die Sicherheitsfunktion «Abfuhr der Nachwärme» z.T. selbsttätige («passive») Eigenschaften und Systeme, sind noch bedienungs- und wartungsfreundlicher sowie toleranter gegen menschliche Fehler. Dank der Abstützung auf einen breiten Erfahrungsschatz und des überblickbaren Einsatzes neuartiger Elemente ist kein Prototyp als Demonstrationsanlage erforderlich und das INSAG-Ziel $< 10^{-5}$ Kernschadensfälle pro Reaktorjahr kann deutlich übertroffen werden. Trotzdem wird z.T. das Containment selektiv so verstärkt, dass auch bei einem gravierenden Kernschaden keine ins Gewicht fallende Freisetzung in die Umgebung erfolgen würde. Auch ohnedies wäre aber bereits das Ziel $< 10^{-6}$ grössere Freisetzungen/Reaktorjahr erreicht, d.h. bei einer Population von 1000 solcher Reaktoren wäre statistisch erst nach 1000 Jahren mit einem schwerwiegenden Unfall zu rechnen – bzw. ein solcher könnte bei einigermassen funktionierender Sicherheitskultur ausgeschlossen werden. Die Methoden für die Auslegung und Sicherheitsanalyse dieser Reaktoren sind im wesentlichen die heute vorhandenen, ebenso die Sicherheitsprinzipien. Gewisse Akzentverschiebungen bezüglich Redundanz und Diversität dürften sich allerdings im Hinblick auf die sicherheitstechnisch optimale Kombination aktiver und passiver Systeme ergeben.

Die innovative («revolutionäre») Linie

Die Idealvorstellung eines innovativen Reaktors wäre eine Anlage, die nur sozusagen widerwillig auf Leistung gebracht werden kann und die bei allen denkbaren Störungen in einen abgeschalteten, sicheren Zustand zurückfällt. Dieses Ideal eines «inhärent sicheren» Reaktors kann natürlich schon deshalb nicht strikt realisiert werden, weil der abgeschaltete Zustand nur sicher ist, wenn auch die Nachwärme abgeführt wird. Verschiedene Entwürfe aus den USA, Schweden, England, Japan versuchen sich aber dem Ideal anzunähern, indem sie alle Sicherheitsfunktionen möglichst passiv zu realisieren trachten. Je nach Funktion ist das aber nur in unterschiedlichem Masse möglich – von «völlig ohne externen Input, ohne Bewegung» bis zu «aktiver Input, passive Ausführung für beschränkte Zeit».

Solche Konstruktionen sind von den Prinzipien her einfach und haben dadurch den Vorteil relativ hoher Transparenz: die Abstützung auf selbsttätige/«natürliche» Mechanismen lässt sich in den Grundzügen leicht erklären. Detaillierte Sicherheitsnachweise sind aber alles andere als trivial – bereits für die präzise Definition von «passiv» musste man sich auf ein abgestuftes Vokabular einigen [15]; die Nachwärmeabfuhr via Naturkonvektion erfordert grosse und auch im Störfall unbehinderte Querschnitte; die Langzeitintegrität komplex geformter Behälter ist aufrechtzuerhalten usw. Ein Prototyp oder zumindest grosstechnologische Tests sind als Demonstration erforderlich.

Generell verspricht man sich von den innovativen Entwicklungen einen stark vereinfachten Aufbau und ein noch ausgeprägter «gutmütiges» Verhalten, d.h. eine umfassendere Toleranz gegenüber menschlichem Versagen und kurzfristigen «Einbrüchen» der Sicherheitskultur. Diese Zielsetzung erscheint erreichbar – ob das Endprodukt in dieser kapitalhungrigen Welt auch wirtschaftlich den Durchbruch schaffen kann, ist allerdings eine andere Frage.

Unrealistisch dürfte dagegen ein auch gegenüber längerdauernd defizitärer Sicherheitskultur toleranter Reaktor sein, weil sich seine guten Eigenschaften unter solchen Umständen nicht dauerhaft erhalten liessen. Mit anderen Worten: einen für einen mausarmen Betreiber in zusammengebrochenen zivilisatorischen Strukturen geeigneten Reaktor wird es wohl nie geben ...

Literatur

[1] *J. J. Di Nunno et al.:* Calculation of Distance Factors for Power and Test Reactor Sites, TID-14844, US Atomic Energy Commission, March 23, 1962

[2] US Nuclear Regulatory Commission Regulatory Guide 1.3: Assumptions for Evaluating the Potential Radiological Consequences of a Loss of Coolant Accident for Boiling Water Reactors, Rev. 2, June 1974

[3] US NRC: Regulatory Guide 1.4: ibid., for Pressurized Water Reactors, Rev. 2, June 1974

[4] US NRC: Code of Federal Regulations, 10 CFR 50.34 (f)

[5] US NRC: Code of Federal Regulations, 10 CFR 50.46

[6] ibid., 10 CFR 50, Appendix A: General Design Criteria for Nuclear Power Plants

[7] Bundesminister des Innern, Bonn: Interpretationen zu den Sicherheitskriterien für KKW, 2. März 1984

[8] ANSI/ANS-58.9-1981: Single Failure Criteria for Light Water Reactor Safety Related Fluid Systems, Febr. 17, 1981

[9] *Fuchs, H.:* Entwicklung der Sicherheitsanalyse technischer Systeme; SVA-Vertiefungskurs «Fortgeschrittene Sicherheitsanalyse» 4.–5. Nov. 1991 (SVA, Postfach 5032, 3001 Bern)

[10] *Kröger, W.;* Chakraborty, S.: Risikobestimmung – eine Bestandesaufnahme der Methodik für Kernkraftwerke; Schweizer Ingenieur und Architekt Nr. 37, 13. Sept. 1990, 1022–1030

[11] Teil E im SVA – Vertiefungskurs [9]

[12] INSAG: Basic Safety Principles for Nuclear Power Plants; IAEA Safety Series No.75-INSAG-3 (1988)

[13] *Kouts, H.:* The Safety of Nuclear Power; International Conference on the Safety of Nuclear Power: Strategy for the Future, IAEA Wien 2.–6. Sept. 1991.

[14] INSAG: Safety Culture; IAEA Safety Series No.75-INSAG-4 (1991)

[15] IAEA-TECDOC-626: Safety related terms for advanced Nuclear Plants (Sept. 1991)

Fazit

Die Methoden zur Auslegung und Sicherheitsanalyse von Kernkraftwerken

haben einen hohen Stand erreicht. Sie gestatten das mit dem sehr umweltfreundlichen geschlossenen System «Kernreaktor» verbundene Risiko auf einen akzeptablen Wert zu reduzieren. Dies erfolgt durch eine möglichst zuverlässige Wahrnehmung der Sicherheitsfunktionen

- Beherrschen der Reaktorleistung
- Abfuhr der Nachwärme
- Rückhaltung radioaktiver Stoffe.

Das Image der Kernenergie leidet immer noch darunter, dass bei der Auslegung des Tschernobyl-Reaktors bezüglich der eminent wichtigen ersten Funktion konstruktive Todsünden begangen wurden. Die Hauptaufgabe wird denn auch weiterhin sein, markante Sicherheitsdefizite bei anderen potentiell «schwarzen Schafen» zu identifizieren und zu beheben oder die betreffenden Reaktoren abzustellen. Dazu sind keine neuen Analysemethoden nötig, sondern «nur» die erforderlichen Finanzmittel.

Generell ist die Zurverfügungstellung der benötigten Ressourcen als ein Element der «Sicherheitskultur» erkannt worden. Diese umfasst jene Eigenschaften und Grundhaltungen aller Beteiligten, die der nuklearen Sicherheit Priorität verschaffen. Sie schliesst insbesondere auch die Fähigkeit ein, aus aufgetretenen Störungen und Vorläufereignissen die nötigen Schlussfolgerungen zu ziehen und damit die Sicherheit weiter zu erhöhen.

Solche Erkenntnisse fliessen auch in die «evolutionäre» Entwicklungslinie der nächsten Generation von Reaktoren ein, die die bisherigen Konzepte optimiert und selektiv selbsttätige (passive) Elemente für die Erfüllung von Sicherheitsfunktionen einsetzt. Während dafür die bisherigen Auslegungs- und Analysemethoden ausreichen, sind für die Entwicklung innovativer («revolutionärer») Kernreaktoren noch ergänzende Nachweisverfahren zu erarbeiten.

Ganz generell aber gilt: selbst die besten Methoden bringen wenig, wenn sie nicht auch praktisch zum Wohl der energiehungrigen Menschheit eingesetzt werden!

Adresse des Verfassers: *Hans Fuchs*, Dr. sc. techn., Colenco Power Consulting AG, Täfernhof/Mellingerstr. 207, 5405 Baden. Ab Januar 1992: c/o ATEL, Bahnhofquai 12, 4601 Olten.

Kostenplanung

Erfahrungen mit der Elementmethode aus der Sicht einer Generalunternehmung

Die Hauptfragen, die uns im Zusammenhang mit der Kostenermittlung unter Zuhilfenahme der Elementmethode gestellt werden, sind etwa die folgenden: Wie ist das Prinzip? Wann und für was die Elementmethode? Wie genau ist sie? Wie gross ist der Aufwand einer Kostenermittlung? Wo sind die Schwachstellen? Hat das Ganze Zukunft? Wir haben versucht, derartige Fragen zu beantworten und die mit der Elementmethode gemachten Erfahrungen weiterzugeben.

Prinzip

Die Gliederung einer Kostenermittlung nach Elementen mit der Elementkostengliederung EKG (Norm SN 506

VON GIUSEPPE DE NARDO, KÜSNACHT

502) spricht für sich selbst und zeigt ein klares Denken nach dem Verursacherprinzip. Das Ganze ist nichts Neues. Es ist ein Fragen nach den kostenverursachenden Bauteilen, ein Suchen nach Ursachen, warum und welche Kosten wo entstehen und welches die Einflussfaktoren sind.

Das war wahrscheinlich auch ein Grund, warum die Elementmethode bis vor kurzem Baukostenanalyse (BKA) hiess. Kosten analysieren heisst, diese zu untersuchen, nachdem sie bereits entstanden sind. So ist die Methode nicht zu verstehen: Sie muss von der ersten Idee an begleitend eingesetzt werden und in jeder Phase möglichst transparent sein.

Wann und wozu

Das Bedürfnis und Bestreben, die Baukosten immer «im Griff» zu haben, verlangt nach einer Systematik. Die Elementkostengliederung bietet eine Methode an, die von der Struktur her immer gleich ist, jedoch im Genauigkeitsgrad den entsprechenden Projektphasen angepasst werden kann. Der Anwendungsbereich reicht von Nutzungsstudien, Machbarkeitsstudien bzw. Vorprojekten bis hin zum detaillierten Kostenvoranschlag.

Phasengerechte Kostenermittlung durch stufenweises Vorgehen

Es ist entscheidend, die Methode von Anfang an, und nicht erst missbräuchlich am Schluss, als Instrument zur Überprüfung des Kostenvoranschlages anzuwenden. Allzuoft wurde ohne klare Ziel-, Zeit- und Kostenvorgaben drauflos gearbeitet. Das Resultat war Enttäuschung für alle am Projekt Beteiligten. Es ist deshalb von äusserster Wichtigkeit, dem Kostenfaktor in jeder Phase das nötige Gewicht zu verleihen.

Genauigkeit

Die Kostengrobschätzung nach Kubikmetern ist angesichts des stark steigenden Anteils der Haustechnik und der lokalen Bauvorschriften untauglich geworden. Die Objekt-Einflussfaktoren wie Grösse, Funktion, Zeit, Qualität, Form, Komplexität und Markt können hier nur schlecht berücksichtigt werden.

Die jeweilige Bearbeitungsphase ist ein wesentlicher Faktor für die Beurteilung der Endkostenprognosen. Da geht es nicht um die Frage der Methode, son-

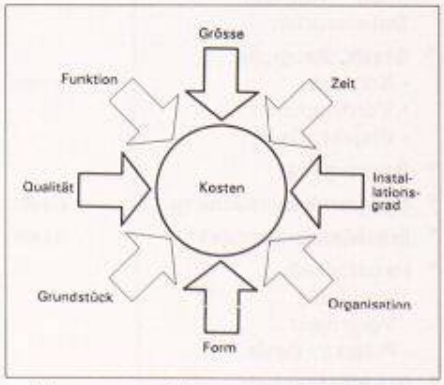

Bild 1. Die Einflussgrössen auf Bauaufgabe und Baukosten