

Einfluss des „Faktors Mensch“ auf die Sicherheit von Kernkraftwerken

Darmstadt, Dezember 2002

Dr. Roland Bähr, Öko-Institut e.V.
Beate Kallenbach-Herbert, Öko-Institut e.V.
Stephan Kurth, Öko-Institut e.V.

Öko-Institut e.V.
Büro Darmstadt
Elisabethenstr. 55-57
D-64283 Darmstadt
Tel.: 06151-81 91-0

Einfluss des „Faktors Mensch“ auf die Sicherheit von Kernkraftwerken

Im Auftrag von
Greenpeace Schweiz

Darmstadt, den 13. Dezember 2002

 **Öko-Institut e.V.**

Institut für Angewandte Ökologie • Institute for Applied Ecology • Institut d'écologie appliquée

**Geschäftsstelle
Freiburg**
Postfach 62 26
D-79038 Freiburg
Tel.: 07 61 / 45 29 5-0
Fax: 07 61 / 45 54-37

**Büro
Darmstadt**
Elisabethenstr. 55-57
D-64283 Darmstadt
Tel.: 0 61 51 / 81 91-0
Fax: 0 61 51 / 81 91-33

**Büro
Berlin**
Novalisstr. 10
D-10115 Berlin
Tel.: 0 30 / 28 04 86-80
Fax: 0 30 / 28 04 86-88

Einfluss des „Faktors Mensch“ auf die Sicherheit von Kernkraftwerken

Autoren:

Dipl.–Phys. Dr. Roland Bähr

Dipl.–Ing. (BA) Beate Kallenbach–Herbert

Dipl.–Ing. Stephan Kurth

13.12.2002

Inhaltsverzeichnis

1	Einleitung	1
2	Das Sicherheitskonzept von Kernkraftwerken.....	2
2.1	Das gestaffelte Sicherheitskonzept	2
2.2	Einordnung des Menschen im Sicherheitskonzept.....	5
2.3	Schlussfolgerungen zur Bedeutung des Menschen im Sicherheitskonzept	6
3	Menschliche Fehler im Betrieb von Kernkraftwerken	9
3.1	Ursachen von Fehlhandlungen	9
3.2	Einflussgrößen auf die Zuverlässigkeit von Personalhandlungen	13
3.2.1	Übertragbarkeit der allgemeinen Auslegungskriterien	13
3.2.2	Massnahmen zur Vermeidung von menschlichen Fehlern	15
3.2.3	Äussere Einflussgrößen.....	19
3.3	Beispiele	21
4	Bewertung von Personalhandlungen.....	24
4.1	Methode und Ziele der menschlichen Zuverlässigkeitsanalyse in der PSA.....	25
4.2	Unsicherheiten und Grenzen der Bewertung von Personalhandlungen in der PSA.....	30
4.3	Anwendbarkeit von PSA-Ergebnissen.....	35
5	Fazit	38
	Literatur	42

Abbildungsverzeichnis

Abbildung 3.1: Zuordnung fehlerbegünstigender Bedingungen aus der Literatur zu den Mensch-Maschine-System (MMS) – Komponenten aus /Sträter 1997/	13
Abbildung 3.2: Wesentliche Komponenten der Sicherheitskultur nach /INSAG 4/	18
Abbildung 4.1: Ablauf der Probabilistischen Sicherheitsanalyse (PSA) im Rahmen der periodischen Sicherheitsüberprüfung nach /BMU 1996/	26

Tabellenverzeichnis

Tabelle 2-1	Kernkraftwerke in der Schweiz.....	2
Tabelle 2-2	Ebenen des gestaffelten Sicherheitskonzepts.....	3

13.12.2002

1 Einleitung

Bei der Bewertung der Sicherheit von Kernkraftwerken stehen oft rein technische Betrachtungsweisen im Vordergrund, die sich z.B. an konstruktiven Merkmalen der Anlage orientieren. Die Diskussionen um die Sicherheit und Akzeptanz der Kernenergienutzung und die Bemühungen zur umfassenden Ursachenklärung von verschiedenen Vorkommnisse in Kernkraftwerken haben aber gezeigt, dass diese Betrachtungsweise allein nicht ausreichend ist, da damit wesentliche Einflussgrößen nicht erfasst werden. Unstrittig ist, dass für den sicheren Betrieb eines Kernkraftwerks weitere Aspekte zu beachten sind, die dem administrativen bzw. organisatorischen Rahmen sowie der Ebene der Personalhandlungen zuzuordnen sind.

In dem vorliegenden Diskussionspapier wird der Frage nachgegangen, welche Bedeutung dem Faktor Mensch in der Sicherheitskonzeption von Kernkraftwerken zukommt und wie die damit zusammenhängenden Sicherheitsaspekte angemessen eingeordnet und bewertet werden können.

Dazu wird zunächst das übergeordnete Sicherheitskonzept von Kernkraftwerken dargestellt und die Bedeutung von Personalhandlungen innerhalb dieses Sicherheitskonzepts diskutiert.

Nachfolgend werden Ursachen von Fehlhandlungen und mögliche Einflussgrößen, die sich auf die Zuverlässigkeit menschlicher Handlungen auswirken können, betrachtet und anhand von Beispielen verdeutlicht.

Unter Bezug auf die gängige Praxis werden anschliessend Vorgehensweisen und Grenzen bei der Berücksichtigung von Personalhandlungen bei der Sicherheitsbewertung von Kernkraftwerken aufgezeigt.

In einem abschliessenden Fazit werden die Erkenntnisse zum Einfluss des „Faktors Mensch“ auf die Sicherheit von Kernkraftwerken zusammengefasst.

2 Das Sicherheitskonzept von Kernkraftwerken

Weltweit sind etwa 440 Kernkraftwerke in Betrieb. In der Schweiz sind es 5 Leistungsreaktoren (3 Druckwasserreaktoren und 2 Siedewasserreaktoren) an den Standorten Beznau, Gösgen, Leibstadt und Mühleberg.

Tabelle 2-1 Kernkraftwerke in der Schweiz

Reaktor	Typ	Brutto-Leistung MW _{el.}	Inbetriebnahme kom. Leistungsb.
Beznau 1	DWR	380	9 / 1969
Beznau 2	DWR	372	12 / 1971
Mühleberg	SWR	372	11 / 1972
Gösgen	DWR	1020	11 / 1979
Leibstadt	SWR	1200	12 / 1984

DWR: Druckwasserreaktor SWR: Siedewasserreaktor

nach <IAEA 2001>

Die Anlagen unterscheiden sich im Detail in ihren Auslegungsmerkmalen und betrieblichen Abläufen. Die Art und der Umfang, wie Eingriffe des Personals in den einzelnen Anlagen vorgesehen oder möglich sind, weichen im Detail voneinander ab. Insofern ist auch die Bedeutung des *Faktors Mensch* im Sicherheitskonzept der einzelnen Anlage im Detail unterschiedlich zu beurteilen. Für eine übergreifende Betrachtung lassen sich jedoch auch allgemeingültige und grundlegende Aussagen zur Bedeutung menschlicher Eingriffe im Sicherheitskonzept der Anlagen machen, die nachfolgend aufgezeigt werden.

2.1 Das gestaffelte Sicherheitskonzept

Aufgrund des hohen Gefahrenpotenzials von Kernkraftwerken werden an die Auslegung und den Betrieb dieser Anlagen hohe Sicherheitsanforderungen gestellt. Durch die verschiedenen Sicherheitssysteme des Kernkraftwerkes und das Sicherheitskonzept insgesamt muss der erforderliche Schutz der Bevölkerung und der Umwelt vor unzulässigen Auswirkungen durch den Betrieb oder als Folge des Betriebs des Kernkraftwerkes sichergestellt werden. Zu Gewährleistung dieses Anspruchs müssen grundlegende *Sicherheitsfunktionen* bei allen Betriebszuständen des Reaktors und bei den zu unterstellenden Belastungen im Normalbetrieb und bei Störfällen durch Inanspruchnahme der Sicherheitssysteme eingehalten werden. Die verschiedenen Sicherheitsanforderungen lassen sich grundlegenden Sicherheitsfunktionen zuordnen, die oftmals auch als *Schutzziele* bezeichnet werden. Dies sind

- die Kontrolle der Reaktivität,
- die Kühlung der Brennelemente,

13.12.2002

- der Einschluss der Radioaktivität und
- die Begrenzung möglicher Strahlenexpositionen im Falle störfallbedingter Freisetzungen.

Zu Erfüllung der Sicherheitsfunktionen werden Anforderungen an die Auslegung und den Betrieb der erforderlichen technischen Systeme und die Nachweisführung im kerntechnischen Regelwerk konkretisiert. Diese Anforderungen werden ergänzt durch das Betriebsreglement und personell-organisatorische Massnahmen.

Oberste Grundsätze im Sicherheitskonzept sind die Vermeidung von Störfällen und die Beherrschung von Störfällen in der Weise, dass schwerwiegende Auswirkungen ausserhalb der Anlage ausgeschlossen werden können. Die höchste Priorität kommt dabei der Störfall-Vermeidung zu. D.h. unabhängig von der ohnehin geforderten Beherrschung von Störfällen sind bereits die System- bzw. Betriebszustände zu vermeiden, die einen möglichen Störfallablauf initiieren und zu einem Ansprechen eines Sicherheitssystems führen können.

Das Sicherheitskonzept eines Kernkraftwerks besteht aus verschiedenen Sicherheits-ebenen. Dieses gestufte Konzept wird von der IAEA unter dem Namen „*Defence in Depth*“ beschrieben (INSAG-10, INSAG-12) und im Deutschsprachigen als *gestaffeltes Sicherheitskonzept* bezeichnet. Das gestaffelte Sicherheitskonzept beruht darauf, dass mehrere aufeinander aufbauende Schutzbarrieren vorhanden sind, um Auswirkungen auf die Umgebung zu verhindern. Bei einem Fehler auf einer unteren Schutzbarriere greift die nächst höhere Barriere. Ein Leistungsbetrieb ist nach INSAG-12 nur zulässig, wenn das Mehrbarrierensystem nicht gefährdet ist und die auslegungsgemässen Funktionen übernehmen kann.

Tabelle 2-2 Ebenen des gestaffelten Sicherheitskonzepts

Ebene		Massnahme / Einrichtung	Sicherheitsziele
1	Normalbetrieb	Betriebliche Einrichtungen und Betriebsführung	Vermeidung und Beherrschung betrieblicher Störungen
2	Betriebsstörungen	Begrenzungseinrichtungen	Begrenzung grösserer betrieblicher Störungen und Rückführung auf den Normalbetrieb
3	Auslegungsstörfälle	Sicherheitseinrichtungen mit hohen Zuverlässigkeitsanforderungen	Beherrschung von Auslegungsstörfällen
4	Auslegungsüberschreitende Ereignisse bzw. nicht beherrschte Auslegungsstörfälle	Ergänzende Einrichtungen und Massnahmen mit vermindernten Anforderungen	Beherrschung bestimmter, sehr seltener Ereignisse; Vermeidung bzw. Minimierung von Freisetzungen

INSAG-12 unterscheidet noch eine weitere Ebene. Auf Ebene 5 sollen Strahlenbelastungen in der Umgebung nach Freisetzungen bei schweren Unfällen minimiert werden. Dies ist Gegenstand der Katastrophenschutzplanung.

Die *Ebene 1* umfasst die zum bestimmungsgemässen Betrieb der Anlage erforderlichen Systeme. Auf dieser Ebene sollen die Prozessparameter in den für den Normalbetrieb kennzeichnenden Bandbreiten gehalten werden. Bei Betriebsstörungen, die zu grösseren Abweichungen vom Normalbetrieb führen, greifen Begrenzungseinrichtungen (*Ebene 2*). Die Begrenzungseinrichtungen verhindern, dass unzulässige Betriebszustände erreicht werden, die zu Schäden an der Anlage führen können und das Ansprechen von Sicherheitssystemen erfordern. Sie führen die Anlage auf den Normalbetrieb zurück. Ein Versagen von betrieblichen Einrichtungen auf den Ebenen 1 und 2 führt alleine noch nicht dazu, dass die grundlegenden Sicherheitsfunktionen (Reaktivitätskontrolle, Kernkühlung, Aktivitätseinschluss) verletzt werden. Bei Vorliegen entsprechender Bedingungen werden Sicherheitssysteme (*Ebene 3*) zur Sicherstellung der Sicherheitsfunktionen angefordert. Wenn auch die Sicherheitssysteme versagen oder Bedingungen vorliegen, die bei der Auslegung nicht berücksichtigt wurden, d.h. der Störfall durch die Sicherheitssysteme nicht beherrscht wird, kann es zu grösseren Freisetzungen von Radioaktivität kommen. Bei Auftreten von Ereignissen mit Kernschäden aufgrund auslegungsüberschreitender oder nicht beherrschter Störfälle sollen durch zusätzliche Einrichtungen oder Massnahmen Freisetzungen in die Umgebung verhindert oder minimiert werden (*Ebene 4*).

Entsprechend dieser Gliederung ist grundsätzlich zu unterscheiden zwischen den Einrichtungen, die rein betriebliche Funktionen übernehmen, und den Einrichtungen, die aufgrund der vorgesehenen Funktionen einem Sicherheitssystem (Störfallbeherrschung) zuzurechnen sind. Dabei kann ein System sowohl Betriebs- als auch Sicherheitsfunktionen erfüllen.

Das beschriebene Konzept wird u.a. zur Bewertung von Vorkommnissen und zur Einordnung von sicherheitsrelevanten Aktivitäten entsprechend ihrer sicherheitstechnischen Bedeutung herangezogen. Vorkommnisse, die zu einem Abweichen vom Normalbetrieb führen können, lassen sich folgenden Bereichen zuordnen:

- Technik, z.B. technisches Versagen von Komponenten.
- Organisation, z.B. ungeeignete Betriebsführung bzw. organisatorische Rahmenbedingungen, mangelhafte Sicherheitskultur.
- Personal, z.B. menschliche Fehlhandlungen und Unterlassungen, Verstösse gegen das Betriebsreglement.

Zwischen diesen Bereichen bestehen Wechselwirkungen. Menschliches Verhalten und die Fehleranfälligkeit von Handlungen wird auch durch technische Faktoren beeinflusst, beispielsweise durch ergonomische Gestaltung der Schnittstellen zwischen Mensch und Maschine. Abhängigkeiten bestehen in grossem Ausmass zwischen dem Verhalten des Einzelnen und den organisatorischen Rahmenbedingungen. Verantwortungsbereich und –bewusstsein, Handlungsfreiraum, persönliche Motivation und der Stellenwert von Sicherheitsaspekten bei betrieblichen Entscheidungen werden durch entsprechende Rahmenbedingungen beeinflusst.

13.12.2002

2.2 Einordnung des Menschen im Sicherheitskonzept

Auf allen Ebenen des gestaffelten Sicherheitskonzepts sind Massnahmen bzw. Funktionen definiert, deren Wirksamkeit zur Erfüllung der Zielsetzung der jeweiligen Ebene erforderlich ist. Dies sind zum einen technische Anforderungen an die jeweils betroffenen Systeme. Zum anderen sind aber auch Eingriffe durch das Personal jeweils nach Art und Umfang unterschiedlich vorgesehen.

- Ein sicherer und störungsfreier (Normal-)Betrieb der Anlage wird in erster Linie durch hochwertige Auslegung und Fertigung sowie durch eine entsprechende Betriebsführung erreicht. Kennzeichnend dafür sind eine Vielzahl von Punkten, bei denen der Mensch entweder durch aktive Handlungen während des Betriebs oder durch Entscheidungen im Rahmen der Auslegung Einfluss hat.
 - Einplanen von Sicherheitsreserven bei der Auslegung der Bauwerke und Anlagen.
 - Optimierte Materialwahl sowie qualifizierte Verarbeitungsprozesse.
 - Optimierte Gestaltung der Schnittstelle zwischen Mensch und Maschine.
 - Umfassende Anweisungen, Vorschriften und Regeln für alle Tätigkeiten an sicherheitstechnisch relevanten Bereichen.
 - Kontinuierliche Ausbildung des Anlagenpersonals.
 - Sicherstellung eines Erfahrungsrückflusses und Auswertung der Betriebserfahrung der eigenen und fremder Anlagen.
 - Instandhaltung und Wartung aller sicherheitsrelevanten Systeme und Komponenten.
 - Überwachung und Steuerung der Betriebsparameter.
 - Ermittlung, Sicherstellung und Überwachung einer ausreichenden Qualität der Einrichtungen im Rahmen der Auslegung der Anlage und betriebsbegleitend.
 - Sicherstellung und Überprüfung der Funktionsfähigkeit von Sicherheitssystemen durch Inspektion, Prüfung, Wartung und Reparatur.
 - (Weiter-)Entwickeln der Sicherheitskultur.
- Betriebsstörungen in der Anlage sollen durch automatische Regelung oder durch ein selbst-regulierendes Anlageverhalten begrenzt werden. Personalhandlungen sind hier wie bei den betrieblichen Einrichtungen zur Qualitätssicherung sowie zur Sicherstellung und Überprüfung der Funktionsfähigkeit der Systeme erforderlich.
- Zur Beherrschung von Auslegungsstörfällen sollen nach der HSK-Richtlinie 101 /HSK 1987/ die Betriebs- und Sicherheitssysteme derart automatisiert werden, dass keine sicherheitsrelevanten Eingriffe des Betriebspersonals innerhalb der ersten 30 Minuten nach dem auslösenden Ereignis erforderlich werden. Im Weiteren wird eine Automatisierung empfohlen, wenn das Betriebspersonal während

eines Störfalles durch andere betriebsbedingte Tätigkeiten von sicherheitsrelevanten Handlungen abgelenkt werden könnte. Die Anlage soll dadurch selbsttätig in einen sicheren Zustand überführt werden. Nach Ablauf der 30 Minuten können auch nach Auslegungsstörfällen Handeingriffe erforderlich werden, um die Anlagen in einen sicheren Zustand zu überführen. Eine wichtige Aufgabe liegt auch darin, zu überprüfen, ob die Sicherheitseinrichtungen die erwartete Wirksamkeit im Anforderungsfall zeigen und der modellierte Störfallablauf eintritt. Ein Spektrum der Auslegungsstörfälle wird festgelegt, das maximale Beanspruchungen abdecken soll. Die bei der Auslegung getroffenen Annahmen und Randbedingungen sind entscheidend für die Wirksamkeit von Sicherheitseinrichtungen während Störfällen, für die Art und Höhe der störfallbedingten Beanspruchungen von sicherheitstechnisch bedeutsamen Anlagenteilen sowie für die zu erwartenden Auswirkungen in der Anlage und in der Umgebung.

- Da auch Ereignisse nicht völlig auszuschliessen sind, bei denen Belastungen auftreten können, die über den auslegungsgemäss berücksichtigten liegen, oder bei denen es zu Mehrfachausfällen von redundanten Sicherheitssystemen kommt, sollen weitergehende Schutzmassnahmen vorgehalten werden. Auch bei auslegungsüberschreitenden Ereignissen sollen die übergeordneten Schutzziele (Reaktivitätskontrolle, Brennelementkühlung, Aktivitätseinschluss) sichergestellt werden. Gegenüber der Beherrschung von Auslegungsstörfällen gelten hier aber verminderte Anforderungen. Automatisierung und Redundanzen sind beispielsweise für diese Ereignisse nicht in gleichem Umfang gefordert. Grundlage sind Störfall- und Notfallvorschriften ergänzt durch sog. Accident-Management-Massnahmen (AM-Massnahmen). Der Betriebsmannschaft kommt daher bei der Beherrschung eines schweren Unfalls und dem Einsatz von AM-Massnahmen eine entscheidende Rolle zu. Massnahmen auf dieser Ebene sind beispielsweise RDB-Druckentlastung, Wasserstoff-Abbau im Containment, Dampferzeugerbeheizung (DWR) mit Lösch- oder Brunnenwasser zur sekundärseitigen Wärmeabfuhr, Containment-Kühlsysteme, Fluten des geschmolzenen Kerns im Containment.

2.3 Schlussfolgerungen zur Bedeutung des Menschen im Sicherheitskonzept

Die betrieblichen Abläufe und die Massnahmen zur Beherrschung von Störfällen sind im Kernkraftwerk weitgehend automatisiert. Insbesondere in Störfall-Situationen sollen Personaleingriffe unter der dann vorliegenden aussergewöhnlichen Stressbelastung weitgehend vermieden werden. Dennoch spielt der Mensch eine wesentliche Rolle im Sicherheitskonzept, während des Betriebs der Anlage durch An- und Abschalten von Aggregaten, durch Regulieren der Leistung und Beeinflussen der Fahrweise, durch Testen, Reparieren, etc. Unter Einbeziehung der dem Betrieb vorgelagerten Konzeptionsphase lässt sich das technische System Kernkraftwerk

13.12.2002

sogar fast vollständig auf menschliche Aktivitäten und Entscheidungen zurückführen. Hierunter fallen Aktivitäten wie z.B. Planen, Herstellen, Programmieren, Prüfen.

Verschiedene sicherheitsrelevante Aktivitäten lassen sich nicht automatisieren, da sie zu einem gewissen Teil auch Kreativität und Spontaneität voraussetzen. Entsprechende Massnahmen betreffen insbesondere den organisatorischen Bereich wie zum Beispiel Qualitätssicherung, Ausbildung des Personals, Auswertung des Erfahrungsrückflusses und Entwicklung von Sicherheitskultur. Die Bedeutung dieser Faktoren auf das Sicherheitsniveau der Anlage und für die Einhaltung des vorrangigen Sicherheitszieles, der Störfallvermeidung, ist unbestritten.

Hinzu kommt, dass verschiedene Aufgaben oder Bereiche, in denen der Mensch massgeblich Einfluss nimmt, nicht auf ein System oder eine Ebene des Sicherheitskonzepts begrenzt sind, da es sich um übergeordnete Funktionen handelt. Qualitätssicherung und Sicherheitskultur sind beispielsweise umfassende Begriffe, die alle Betriebsphasen und alle Sicherheitsebenen betreffen. Grundlegende Mängel in der Qualitätssicherung können sich daher von der Auslegung bei entsprechender Anforderung bis in die Störfallebene fortsetzen. Ein nachlässiger Umgang mit Sicherheitsregeln bei betrieblichen Routineabläufen kann (potenziell) auch in Störfallsituationen ein zusätzliches Risiko darstellen, wenn dort ein gleichartiges Verhalten praktiziert wird. In der Organisation müssen die notwendigen Randbedingungen geschaffen werden, damit Sicherheitskultur im Ganzen und sicherheitsgerichtetes Handeln des Einzelnen unterstützt werden.

Eine wichtige Aufgabe besteht im Normalbetrieb wie bei Auslegungsstörfällen darin, die ordnungsgemässe Funktion von Sicherheitseinrichtungen zu überprüfen, zu beurteilen und im Notfall (bei Fehlfunktionen der Sicherheitseinrichtungen) regulierend eingreifen zu können. Massnahmen zur Beherrschung auslegungsüberschreitender Ereignisse beruhen in grossem Umfang auf aktiven Handlungen und Entscheidungen des Personals. Aufgrund der übergeordneten Funktion des Menschen im Sicherheitskonzept muss ein Eingriff durch das Personal prinzipiell auf allen Ebenen möglich sein.

Die Funktion des Menschen im Kernkraftwerk kann trotz einer weitgehenden Automatisierung der Anlage nicht auf die Betriebsführung reduziert werden sondern ist in höchstem Grade sicherheitsrelevant. Der Mensch kann in wesentlichen Bereichen nicht durch automatisch arbeitende, technische Systeme ersetzt werden. Eine Absicherung menschlicher Handlungen durch zusätzliche technische Systeme ist nur in Teilbereichen möglich.

Aus den dargestellten Zusammenhängen ergeben sich vielfältige Einflussmöglichkeiten des Menschen auf die Sicherheit der Anlage auf allen Ebenen des Sicherheitskonzepts. Deshalb müssen für eine Gesamtbetrachtung an den Menschen als Teil des Systems Kernkraftwerk vergleichbare Zuverlässigkeitsanforderungen wie an die technischen Sicherheitsfunktionen gestellt werden. Der menschliche Faktor in sich

und die Interaktionen mit den technischen Systemen sind daher in gleicher Weise zu analysieren und in einer Sicherheitsbewertung zu berücksichtigen wie die Zuverlässigkeit technischer Systeme.

13.12.2002

3 Menschliche Fehler im Betrieb von Kernkraftwerken

3.1 Ursachen von Fehlhandlungen

Nahezu alle Abläufe und Anlagenzustände, die auftreten können, können durch menschliche Handlungen beeinflusst werden. Der Mensch übernimmt Funktionen im Sicherheitssystem des Kernkraftwerks, die die technischen Funktionen ergänzen und manipulieren können. Im Anlagenkonzept ist vorgesehen, dass aktive Eingriffe erfolgen müssen oder können. Technische Funktionen und Tätigkeiten des Menschen können prinzipiell fehlerbehaftet sein. Eine Besonderheit gegenüber Fehlern an technischen Systemen liegt darin, dass der Mensch sich über vorgesehene oder vorgeschriebene Handlungsweisen selbsttätig hinwegsetzen kann.

- Menschen müssen auf das technische System einwirken können und können dabei
 - fehlerhafte Unterlassungen oder
 - falsche Handlungen bzw. Handlungen zur falschen Zeit ausführen.
- Menschen können auf das technische System einwirken, obwohl sie es nicht müssen oder gar nicht dürfen und können dabei Fehlhandlungen ausüben.

In /BfS 1998/ wird die folgende Gliederung von Fehlerarten vorgeschlagen:

- 1) **Zuverlässigkeit:** Fehler bei Handlungen, für die schriftliche Anweisungen vorliegen. Diese können in Systemen zur Bewertung des menschlichen Einflusses auf die Anlagensicherheit berücksichtigt werden (siehe Kapitel 4).
- 2) **Fahrlässigkeit:** Fehler im Bereich ungeplanter Handlungen. Personalhandlungen dieser Art sind nicht in Modellen erfassbar und daher hinsichtlich ihres Einflusses auf die Anlagensicherheit nicht bewertbar.
- 3) **Vorsätzlichkeit:** Bewusstes Herbeiführen von Schäden. Diese Handlungsmöglichkeit des Menschen wird nicht bei der Betrachtung der Anlagensicherheit sondern höchstens bei der Anlagen-Sicherung behandelt. (Im Zusammenhang mit der Anlagen-Sicherung berücksichtigte „Tätermodelle“ zur Abbildung möglicher Einwirkungen Dritter sind nicht öffentlich zugänglich).

Die menschliche Kreativität kann hilfreich bei der Bewältigung aussergewöhnlicher Situationen im Anlagenbetrieb sein, stellt aber auch ein zusätzliches und schwer beherrschbares Fehlerpotenzial dar. Es gibt verschiedene Faktoren, die zu diesem Verhalten beitragen und als spezifische Ursachen für menschliche Fehler angeführt werden können.

- **Ausbildungsmängel und fehlende Fachkenntnisse:** Ausbildungsmängel und fehlende Fachkenntnisse können dazu führen, dass die Situation und der Hand-

lungsbedarf falsch eingeschätzt werden und aus Unwissen Fehler gemacht werden.

- **Beeinträchtigungen des persönlichen Befindens:** Beeinträchtigungen des persönlichen Befindens durch Hunger, Durst, Müdigkeit, Krankheit und weitere Faktoren im sozialen Umfeld können zu Konzentrations- und Leistungsschwächen führen, die die Zuverlässigkeit menschlichen Handelns herabsetzen.
- **Bildung eines falschen Modells vom Anlagenzustand:** Informationen über den Anlagenzustand können sowohl von technischen Systemen als auch vom Menschen fehlerhaft festgestellt, aufgenommen und verarbeitet werden. Der Mensch neigt darüber hinaus dazu, aus Einzelinformationen Bilder zu entwerfen, die dazu führen können, dass weitere Informationen nur selektiv wahrgenommen werden oder fehlende Informationen eigenmächtig „konstruiert“ werden, um das selbstgemachte Bild zu ergänzen.

Gerade die Kenntnis der Komplexität und die Vielzahl von Informationen sowie die Vielfalt der technischen Verknüpfungen zeigt auch die Vielzahl möglicher Störungen. Jede Information steht daher unter dem Verdacht fehlerhaft produziert worden zu sein.

- **Einschränkung der Handlungsfreiheit in Stress-Situationen:** Bei einer plötzlichen Vielfalt von Anforderungen und Veränderung der äusseren Arbeitsbedingungen wird die Leistungsfähigkeit gemindert. Dies ist gerade dann zu erwarten, wenn der Anlagenbetrieb von der Routine abweicht. Überlegtes und strukturiertes Handeln wird dann in Frage gestellt oder ist in der bisher gewohnten Weise nicht mehr möglich. Dies führt zu Unsicherheiten und einer „Qualitätsminderung“ der Aktion. Folgende typische Reaktionen sind in Stresssituationen zu beobachten:
 - einem Meinungsführer unterordnen,
 - riskante Entscheidungen treffen,
 - nur nach Bestätigung einer vorgefassten Einschätzung der Situation suchen.

Dadurch sind wesentliche Elemente der Sicherheitskultur, die zu einem sicheren Betrieb der Anlage beitragen, gefährdet. Andererseits werden angesichts dieses Verhaltens in der hierarchischen Organisation des Kernkraftwerks zusätzliche Belastungen und Anforderungen auf den Verantwortlichen übertragen, der dann einem besonderen Druck ausgesetzt ist.

- **Monotonie:** Gleichartige Arbeitsabläufe und monotone Situationen kennzeichnen den Arbeitsalltag im Normalbetrieb der Anlage. Bekannte Verhaltensweisen zur Überwindung monotoner Situationen sind Ermüden, Schlafen, Unkonzentriertheit oder die Suche nach Ablenkungsbeschäftigungen bis hin zu Alkohol- oder Drogenkonsum. Die Leistungs- und Reaktionsfähigkeit kann dadurch erheblich eingeschränkt werden.

13.12.2002

- **Erfahrungen nur mit einer sicheren Anlage:** Die Eintrittshäufigkeit schwerer Reaktorstörfälle ist gering. Daher besteht für den Einzelnen – anders als bei Unfallszenarien in anderen Zusammenhängen, z.B. im Strassenverkehr – praktisch keine Möglichkeit Erfahrungen in der Realität zu sammeln. Aufgrund der bisher gemachten Erfahrungen wird die Anlage mit gutem Grund als sicher empfunden und Vorschriften, die der Sicherheit dienen, als überflüssig betrachtet. Die HSK /HSK 1998/ weist darauf hin, dass hohe Sicherheit möglicherweise gerade dazu führt, die Sicherheitsmotivation zu untergraben.

Training oder Simulation können den Ernstfall nicht vollständig abbilden und werden als inszeniert und nicht als Ernstfall empfunden. Es ist daher fraglich, ob angesichts der gemachten Erfahrungen Anzeichen für ernsthafte Störungen ernst genommen werden bzw. ob die Möglichkeit schwerwiegender Störungen überhaupt in Erwägung gezogen wird und wie das Personal, trotz aller Ausbildungs- und Trainingsmassnahmen, bei tatsächlichen Störfällen reagieren wird.

- **Anspruch, es besser machen zu wollen:** Das Personal stellt seine Einschätzung der Situation, die zum Teil rational und zum Teil emotional begründet ist, und den daraus abgeleiteten Handlungsbedarf über das Anlagendesign und formulierte Betriebsregeln. Anzeigen und Anweisungen werden guten Gewissens absichtlich ignoriert bzw. umgangen. Dieses kritische und distanzierte Verhalten gegenüber der Technik kann in bestimmten Situationen erwünscht und hilfreich sein. Es kann aber nicht ausgeschlossen werden, dass dieses Verhalten auch in falschen Situationen zum Tragen kommt und bei Fehleinschätzungen negative Auswirkungen auf die Sicherheit hat.
- **Unterschätzung von Nebeneffekten:** Bei der Beobachtung und Steuerung eines komplexen Systems konzentriert man sich bevorzugt auf die Haupteffekte der Handlungen auf ein bestimmtes Ziel. Dabei besteht die Gefahr, Nebeneffekte auf das übrige System zu übersehen. Die Denkweise ist oft durch lineare Abfolgen bestimmt. Exponentielle Entwicklungen werden dadurch unterschätzt.
- **Minimierung des eigenen Aufwands:** Schon aus Gründen der Bequemlichkeit aber auch zur Steigerung der Arbeitseffizienz ist man bestrebt, den eigenen Aufwand zu reduzieren. Diesem Bestreben steht entgegen, dass zusätzliche Sicherheit in der Regel auch mit mehr Aufwand verbunden ist.
- **Angst:** Mit den hohen Anforderungen an die Kompetenz und Zuverlässigkeit der Operateure, wächst auch der Druck auf den Einzelnen und die Angst zu versagen. Damit verbunden ist zum einen die Angst vor unabsehbaren Konsequenzen von Fehlhandlungen. Störfallsituationen sind oftmals mit der Gefahr radioaktiver Freisetzungen verbunden. Dies bedeutet auch eine Bedrohung der eigenen Gesundheit und des eigenen Lebens. Angst ist auch dann eine naheliegende Reaktion, die die persönlichen Entscheidungen beeinflussen kann.

Unabhängig davon kann auch die Befürchtung durch Fehler unangenehm aufzufallen und sich zu blamieren das Handeln beeinflussen. Insbesondere vor dem Hintergrund, dass Fehler erkannt werden müssen, um daraus zu lernen.

- **Blindes Vertrauen und mangelhafte Kommunikation:** In der Zusammenarbeit mit bekannten und erfahrenen Kollegen wird i.d.R. davon ausgegangen, dass die übertragenen Aufgaben stets gut und richtig erledigt werden. Dies ist Grundlage für eine vertrauensvolle Zusammenarbeit. Auf der anderen Seite verleitet dieses Vertrauen dazu, dass nicht in Erwägung gezogen wird, dass trotz aller Erfahrung Fehler gemacht werden können. Das kann auch hier zusätzlich begünstigt sein durch das Bestreben, den eigenen Aufwand zu reduzieren und zusätzliche Kontrollen zu sparen. Kommunikation und Kontrolle der Tätigkeiten können dann unzureichend sein. Fehleinschätzungen können die Folge sein, wenn daraufhin von einem falschen Bild ausgegangen wird (s.o.). Es gibt Beispiele, dass das verantwortliche Schichtpersonal in der Warte nicht genau über (Arbeits-)abläufe an anderer Stelle, z.B. vor Ort in der Anlage, informiert war, von falschen Voraussetzungen ausging und auf dieser Grundlage falsche Entscheidungen traf.

Der Gefahr von Fehleinschätzungen kann durch intensivere Kommunikation und verstärkte Kontrolle einzelner Arbeitsschritte begegnet werden. Die Motivation zur konsequenten Umsetzung solcher Massnahmen ist allerdings begrenzt, da diese als übertriebenes Misstrauen empfunden werden können, welches die eigene Leistung unbegründet in Zweifel zieht und so das Betriebsklima und die Zusammenarbeit belastet.

- **Spannungen und Rivalitäten:** Spannungen oder Rivalitäten zwischen den am Betrieb der Anlage beteiligten Gruppierungen wirken sich kontraproduktiv auf die Aufrechterhaltung bzw. Weiterentwicklung des Sicherheitsniveaus aus, da dann nicht mehr von einer unvoreingenommenen und vorrangig sicherheitsgerichteten Arbeits- und Denkweise ausgegangen werden kann.
 - Intern können Spannungen auftreten zwischen verschiedenen Bereichen (Entwicklung, Kontrolle, Reaktorpersonal) bzw. zwischen verschiedenen Hierarchieebenen, die zu einem wechselseitigen Zuschieben von Verantwortung führen können.
 - Extern können Spannungen zwischen Betreiber, Aufsicht (Behörde) und Gutachtern eine offene und vertrauensvolle Zusammenarbeit behindern.
- **Mangelhafte Sicherheitskultur:** Das menschliche Verhalten im sicherheitstechnischen Zusammenhang des Anlagenbetriebs wird auch dadurch beeinflusst, welchen Stellenwert der Sicherheit als Unternehmensziel eingeräumt wird und insbesondere, wie dieses Ziel im Betrieb tatsächlich praktiziert und das Arbeitsumfeld dadurch geprägt wird. Mangelhafte Sicherheitskultur kann zu nachlässigem Umgang mit den sicherheitstechnischen Regeln und den daraus abgeleiteten Massnahmen führen.

13.12.2002

Eine Zusammenstellung häufiger Fehlerbedingungen, zugeordnet zu der Komponente des Mensch-Maschine-Systems (MMS), in dem eine entsprechende Fehlerbedingung einen Fehler bewirken kann, zeigt die Abbildung 3.1 aus /Sträter 1997/. (Die Anordnung der Komponenten stellt keine Hierarchisierung dar).

<p><i>Umgebung</i></p> <p>Temperatur Beleuchtung Luftqualität Lärm Strahlung Vibration Sauberkeit</p>	<p><i>Situation</i></p> <p>Arbeitszeit Vergütungswesen Pausen Gruppenstruktur Schichtwesen Organisationsstruktur Prüfsituation</p>	<p><i>Auftragserteilung/-rückmeld.</i></p> <p>Kommunikationsmittel Gestaltung von Prozeduren Vom Management geforderte Aufgabe</p>
<p><i>Aufgabe</i></p> <p>Komplexität Risiko Bedeutung Schwierigkeit Zeitdruck Nutzen Dimension Präzision</p>	<p><i>Rückmeldung</i></p> <p>Oberfläche Wiederholfrequenz Inkonsistenz Hilfen Design Warnungen Kompatibilität</p>	
<p><i>Person</i></p> <p>Streß Informationsbelastung bei Aufmerksamkeit Interpretation und Entscheidung Motivation Erfahrung Gedächtnisbelastung (STM, LTM) Arbeitsmethoden Training Kognitive Belastung (Rechnen, skill-, rule-, knowlege-based) Persönlichkeit Intelligenz Fertigkeit Persönliche Konsequenzen Emotion Wissen Physikalische Faktoren Ermüdung Hunger / Durst Unterforderung</p>	<p><i>Tätigkeit</i></p> <p>Auswahl Handhabbarkeit Zugänglichkeit</p> <p>Monotonie Control-Display Verhältnis</p> <p>Control-Order Dynamik</p>	<p><i>System</i></p> <p>Zuverlässigkeit Wartungsintervalle Plötzlichkeit des Auftritts</p> <p>Automatisierungsgrad</p> <p>Verkettung Vermaschung</p>

Abbildung 3.1: Zuordnung fehlerbegünstigender Bedingungen aus der Literatur zu den Mensch-Maschine-System (MMS) - Komponenten aus /Sträter 1997/

3.2 Einflussgrößen auf die Zuverlässigkeit von Personalhandlungen

3.2.1 Übertragbarkeit der allgemeinen Auslegungskriterien

Allgemeine Auslegungskriterien für Sicherheitssysteme nennt die HSK in ihrer Richtlinie R 101, das kerntechnische Regelwerk enthält im Detail weitere Anforderungen und Ausführungsbestimmungen:

- Einzelfehlerkriterium,
- Instandhaltungskriterium,
- Funktionelle Unabhängigkeit von redundanten Strängen,

- Separation von redundanten Strängen,
- Prüfbarkeit von redundanten Strängen,
- Automatisieren von Sicherheitsfunktionen,
- ergonomische Gesichtspunkte.

Aufgrund des Stellenwertes des Menschen im Sicherheitskonzept des Kernkraftwerks sind nicht nur hohe Anforderungen an die Zuverlässigkeit von technischen Systemen sondern auch an die Zuverlässigkeit von Personalhandlungen zu stellen. Die o.g. Auslegungsgrundsätze sind aber nicht ohne weiteres auf Personalhandlungen übertragbar.

Redundanz

Mit dem Einzelfehlerkriterium und dem Instandhaltungskriterium wird festgelegt wie viele unabhängige Teilausfälle bzw. Unverfügbarkeiten (z.B. im Instandhaltungsfall) zu unterstellen sind. Sowohl technisches Versagen als auch menschliche Fehler, die die Funktion des Sicherheitssystems beeinflussen, sind dabei als mögliche Fehler zu beherrschen. Aus diesen Überlegungen ergibt sich, welche Anzahl von Redundanzen, erforderlich ist. Dabei gelten unterschiedliche Anforderungen auf den verschiedenen Sicherheitsebenen. Auf der Sicherheitsebene 4 im Bereich der auslegungsüberschreitenden Ereignisse wird i.d.R. zusätzlich zum auslösenden Ereignis kein Einzelfehler unterstellt. Im Bereich der Auslegungsstörfälle wird bei der Auslegung der Sicherheitssysteme dagegen von einem zusätzlichen Einzelfehler im Anforderungsfall ausgegangen. Von den Redundanzen eines Systems kann nur Kredit genommen werden, wenn sie nicht durch eine gemeinsame Ursache gleichzeitig betroffen sein können. Die Forderung nach funktioneller Unabhängigkeit und Separation von redundanten Strängen dient diesem Ziel. Das Redundanzprinzip ist zur Vermeidung von menschlichem Fehlverhalten nicht übertragbar. Es kann nicht mit Sicherheit davon ausgegangen werden, dass zwei oder drei Personen unabhängig voneinander Störungen oder technisches Versagen wahrnehmen und darauf gleichartig reagieren. Bei menschlichem Fehlverhalten ist grundsätzlich auch von der Möglichkeit gemeinsam verursachter Ausfälle auszugehen. Die Gründe dafür liegen zum einen in der unterschiedlichen Ausprägung individueller Fähigkeiten und den Einflüssen momentaner Befindlichkeiten und zum anderen in der Möglichkeit dass die Personen nicht vollständig unabhängig voneinander reagieren sondern ihre Entscheidungen aneinander koppeln.

Prüfbarkeit

Die Forderung nach Prüfbarkeit der Redundanzen dient der Überprüfung und Gewährleistung der Funktionsfähigkeit der Komponenten insbesondere im System der wiederkehrenden Prüfungen. Die Funktionsfähigkeit des Menschen lässt sich nicht in gleicher Weise überprüfen. Einerseits sind entscheidenden Parameter, die die Leistungsfähigkeit und Zuverlässigkeit kennzeichnen, nicht oder nur schwierig messtechnisch zu erfassen und sind darüber hinaus individuell und temporär verschieden.

13.12.2002

Andererseits sind einer ständigen Überwachung der Person auch ethisch Grenzen gesetzt. Die geforderten Fähigkeiten und Fertigkeiten sind daher im Wesentlichen nur ausserhalb des Reaktorbetriebs im Rahmen von speziellen Ausbildungs-, Test- und Prüfprogrammen erfassbar. Die Übertragbarkeit der Ergebnisse auf den realen Anlagenbetrieb ist aber begrenzt.

Automatisierung

Durch das Automatisieren von Sicherheitsfunktionen, soll der Möglichkeit von stressbedingten Fehlhandlungen in Störfall-Situationen vorgebeugt werden. Die Automatisierung bringt einerseits eine Entlastung des Personals im Reaktorbetrieb und bei der Beherrschung auslegungsgemäss zugrunde gelegter Störfallabläufe. Andererseits ist zu berücksichtigen, dass der Anteil der Automatisierung technischer Systeme auch daran zu bemessen ist

- dass sich letztendlich der Einfluss des Menschen bei steigender Automatisierung von der Betriebs- auf die Konstruktions- und Fertigungsphase verschiebt, somit nicht wirklich reduziert wird und
- dass auch nahezu vollständig automatisierte Systeme Ausfallwahrscheinlichkeiten besitzen, die den Eingriff des Personals erfordern, das mit steigendem Automatisierungsgrad und zunehmender Komplexität der Systeme
 - zunehmend weniger aufgrund von Routinehandlungen mit dem System vertraut ist und
 - ggf. nur unzureichende Informationen über den gegenwärtigen Betriebszustand des Systems und die Abläufe in der Anlage im Falle einer Störung erhält.

Der Automatisierung sind auch dadurch Grenzen gesetzt, dass letztlich ein Eingriff möglich sein muss, um auf nicht vorhergesehene Entwicklungen zu reagieren.

Ergonomie

Die Berücksichtigung ergonomische Gesichtspunkte dient der Optimierung der Schnittstellen zwischen Mensch und Maschine und der Minimierung damit zusammenhängender Fehlerquellen. Eine vollständige Verhinderung menschlicher Fehler ist aus bereits genannten Gründen damit nicht zu erreichen.

3.2.2 Massnahmen zur Vermeidung von menschlichen Fehlern

Das Sicherheitskonzept muss auf mögliche Fehler reagieren. Es muss nicht nur Vorsorge gegen technisches Versagen getroffen werden sondern auch gegen menschliche Fehler. Zur Vermeidung menschlicher Fehler im Arbeitssystem Mensch-Maschine werden verschiedene Gedanken verfolgt (s.a. /HSK 1998/). Möglichkeiten und Grenzen dieser Massnahmen werden nachfolgend diskutiert.

Zum einen besteht die Möglichkeit, den Menschen durch automatisch arbeitende technische Systeme zu ersetzen. Ein anderer Weg besteht darin, den Menschen zu verbessern, d.h. ihn durch Ausbildung und Schulung sowie Bereitstellung günstiger Arbeitsbedingungen in die Lage zu versetzen, zuverlässig zu funktionieren. Die Abwägung von Vor- und Nachteilen bzw. Grenzen führt dazu, eine Optimierung des Zusammenwirkens zwischen Mensch und Maschine anzustreben. Dabei sind sowohl der Mensch und die Maschine als auch weitere, vorwiegend organisatorisch-administrative Bedingungen, die unter dem Begriff Sicherheitskultur gefasst werden, zu beeinflussen.

Optimierung der Technik

Auf die Frage, inwieweit ein Sicherheitsgewinn damit verbunden ist, den Menschen durch eine Automatik zu ersetzen, wurde im vorangegangenen Kapitel (Kapitel 3.2.1) bezüglich der Übertragbarkeit der allgemeinen Auslegungskriterien eingegangen. Demnach ist durch eine Vollautomatisierung der angestrebte Sicherheitsgewinn nicht zu erzielen. Eingriffe sind auch im Sicherheitssystem erforderlich und müssen als Möglichkeit bestehen bleiben. Durch hohen Automatisierungsgrad fehlt die Übung für Handeingriffe und die Unkompetenz des Operators wird antrainiert.

Eine grundlegende Forderung ist auch, dass die Technik fehlerverzeihend gestaltet werden muss. Das bedeutet eine Ausstattung mit Redundanzen in sicherheitskritischen Teilsystemen, mit umfangreichen Meldesystemen, mit Korrekturmöglichkeiten von Fehlhandlungen. Entsprechend dem Sicherheitskonzept darf eine einzelne Fehlhandlung keine schwerwiegenden Konsequenzen haben. Eine vollständige Absicherung menschlicher Eingriffe ist wegen der Charakteristik menschlicher Handlungen und der Stellung des Menschen im Sicherheitskonzept nicht möglich.

Optimierung der Personalhandlungen

Grosses Gewicht wird heute auf eine umfassende Ausbildung auch für die Beherrschung hypothetischer Unfälle gelegt. Unfallszenarien werden regelmässig in Übungen durchgespielt und z.T. im Simulator erprobt. Damit soll neben der Technik auch die Notfallorganisation und das menschliche Verhalten unter aussergewöhnlichen Stresssituationen geübt werden. Fehleinschätzungen und Fehlhandlungen, die durch Kenntnislücken oder fehlende Übung verursacht werden, sollen dadurch vermieden werden. Das Betriebspersonal soll so qualifiziert sein, dass jederzeit nur sachgerechte Eingriffe erfolgen. Durch Ausbildung und Training kann die Sicherheit im Umgang mit Vorgängen in der Anlage erhöht werden. Damit lässt sich eine hohe Fertigkeit bei Routinehandlungen erreichen. Das falsche Konstruieren von Modellen aus Teilinformationen kann damit aber nicht ausgeschlossen werden, insbesondere bei Abweichungen von der Routine.

Weiterhin wird versucht durch das Stellen von Nebenaufgaben mit sicherheitstechnischem Bezug und Angeboten von begleitenden Schulungsmassnahmen die Monoto-

13.12.2002

nie des Arbeitsablaufs zu unterbrechen. Der Erfolg dieser Massnahmen ist aber fraglich, da sie leicht als künstlich und aufgesetzt empfunden werden können.

Schulungsmassnahmen beziehen sich letztlich nur auf bekannte oder vorhersehbare bzw. modellierte Ereignisabläufe. Die dann erforderlichen Reaktionen (Eingriffe) können eingeübt werden. Im Rahmen von Schulungsprogrammen besteht darüber hinaus die Möglichkeit, auf Betriebserfahrungen, die zu zusätzlichen Erkenntnissen geführt haben, gezielt einzugehen. Insofern ist es notwendig, dass (menschliche) Fehler auftreten und zugelassen werden, damit daraus gelernt werden kann. Das Spektrum möglicher Ereignisabläufe lässt sich dadurch erweitern, bleibt aber letztlich beispielhaft. Der Umgang mit neuartigen Situationen, die im Modell nicht vorhergesehen waren, erfordert aber weiterhin eigenständige Entscheidungen, die von den o.g. möglichen Fehlerursachen beeinflusst werden können. Die Erfahrung zeigt, dass immer wieder Phänomene auftreten, die auf technisches Versagen oder auf menschliches Fehlverhalten zurückzuführen sind, die bis dahin nicht für möglich gehalten wurden und daher auch nicht explizit bei der Auslegung berücksichtigt wurden.

Die Vielzahl der möglichen Fehler, die im persönlichen Verhalten zum Teil psychische, zum Teil physische sowie ergonomische Ursachen haben, lassen sich durch Ausbildung und Schulung nicht mit Sicherheit ausschalten. Die Einflussgrössen sind charakteristisch für menschliches Verhalten und können und sollten zum Teil (aus Sicherheitsgründen) auch nicht abkonditioniert werden. Aufgrund der Vielzahl und Unberechenbarkeit der Einflussgrössen sind menschliche Fehler im Anlagenbetrieb unvermeidbar. Es ist bei menschlichem Fehlverhalten schwerer vorhersehbar als bei technischem Versagen, wie und in welchen Erscheinungsformen es auftritt.

Optimierung des Zusammenspiels von Mensch, Technik und Organisation - Sicherheitskultur

Weder eine Automatisierung der Technik alleine noch die umfassende Ausbildung und Schulung der Mitarbeiter alleine vermag Sicherheit zu garantieren. Ziel ist es daher, das Zusammenspiel von Mensch und Technik zu optimieren, um ein möglichst hohes Sicherheitsniveau zu erreichen. Dieses Zusammenwirken wird durch Organisation geregelt. Im sicherheitstechnischen Zusammenhang wurde der Begriff *Sicherheitskultur* entwickelt. Für die Anwendung in der Kerntechnik wurde folgende verbreitete Definition des Begriffs Sicherheitskultur von der Beratergruppe der IAEA, der International Nuclear Advisory Group INSAG, in /INSAG 4/ vorgelegt:

„Sicherheitskultur ist die Gesamtheit von Merkmalen und Einstellungen bei Organisation und Individuen, die als oberste Priorität durchsetzt, dass Sicherheitsfragen von Kernkraftwerken die ihrer Bedeutung entsprechende Aufmerksamkeit erhalten.“

Unter dem Begriff Sicherheitskultur werden in der Kerntechnik

- der organisatorische Rahmen, der auch als Sicherheitsmanagement bezeichnet wird, sowie
 - Verhalten, Einstellungen und Handlungsweisen aller beteiligten Mitarbeiter
- zusammengefasst. Abbildung 3.2 stellt die wesentlichen Komponenten der Sicherheitskultur nach /INSAG 4/ dar.



Abbildung 3.2: Wesentliche Komponenten der Sicherheitskultur nach /INSAG 4/

Die Abbildung 3.2 zeigt, dass als Voraussetzung für den sicheren Betrieb einer Anlage umfassende Anforderungen gestellt werden, die nicht im Bereich des Mensch-Maschine-Systems abzubilden sind. Dabei kommt dem oberen Management die Aufgabe zu, die Sicherheitsgrundsätze zu definieren und allen Mitarbeitern bekannt zu machen, sowie den für ein sicherheitsgerichtetes Handeln erforderlichen organisa-

13.12.2002

torischen Rahmen zu schaffen. Ausserdem wird von der Führungsebene erwartet, dass sie durch ihr eigenes Verhalten und durch Präsenz in der Anlage die Verpflichtung zum Sicherheitsbewusstsein demonstriert.

Jeder einzelne Mitarbeiter soll die Möglichkeiten, die ihm das Sicherheitsmanagement bietet, annehmen und durch entsprechende Handlungsweise unterstützen. Dabei ist nicht das mechanische Einüben bestimmter Aktionen anzustreben sondern ein sicherheitsgerichtetes Verhalten der Mitarbeiter, das aus einer entsprechenden inneren Einstellung resultiert.

Sicherheitskultur kann in einer Anlage nicht anhand konkreter Kriterien gemessen werden, da sie in den Bereich tief verwurzelter Werte und Normen eingreift, die die Handlungsweise der Mitarbeiter bestimmen. Sie zeigt sich jedoch indirekt in den Ergebnissen sicherheitsrelevanter Prozesse. Dabei ist eine Veränderung der Sicherheitskultur nur anhand längerfristiger Entwicklungen feststellbar. Für den Erhalt des Sicherheitsniveaus einer Anlage ist daher das ständige Streben aller Beteiligten nach Verbesserung der Sicherheitskultur eine wesentliche Voraussetzung.

3.2.3 Äussere Einflussgrössen

Auch äussere Faktoren wirken auf menschliches Fehlverhalten hin. Die Rahmenbedingungen unter denen ein Kernkraftwerk betrieben wird, werden nicht nur durch sicherheitstechnische Erwägungen sondern auch durch politisch-gesellschaftliche Gegebenheiten bestimmt. Kernkraftwerke sind Wirtschaftsbetriebe, die kommerziell elektrische Energie produzieren und verkaufen. Wirtschaftlicher Erfolg des Betriebs ist sowohl für das Unternehmen als auch für den einzelnen Mitarbeiter ein wichtiges Kriterium bei Entscheidungen in Konfliktfällen.

- Gewinnoptimierung ist eines der vorrangigen Unternehmensziele.
- Wirtschaftlicher Erfolg des Unternehmens dient der Erhaltung des Arbeitsplatzes und damit der persönlichen Absicherung.

Die Öffnung und Liberalisierung der Strommärkte in den letzten Jahren hat dazu geführt, dass nun sehr viel mehr Anbieter von elektrischer Energie konkurrieren können und die Preisgestaltung beeinflussen. Mögliche Reaktionen sind die Verringerung von kostenbestimmenden Sicherheitsauflagen im eigenen Land sowie der Export des Risikos, d.h. die Verlagerung der Stromproduktion in die Länder, die mit einem geringeren Sicherheitsniveau produzieren. Eine langfristige Lösung scheint nur bei einer weitgehender Harmonisierung der Anforderungen möglich, die aber politisch nur sehr schwierig durchzusetzen ist und zum anderen auch an der Vergleichbarkeit der Rahmenbedingungen in den einzelnen Ländern scheitern kann.

Als weiterer Einflussfaktor ist Kernenergiepolitik des Landes insgesamt zu nennen und die politische Entscheidung, die Kernenergieerzeugung zu fördern oder nicht. In verschiedenen europäischen Ländern sind Bestrebungen zum Atomausstieg auf der Grundlage entsprechender Gesetze oder Vereinbarungen im Gange. Hier stellt sich

die Frage, wie angesichts begrenzter Restlaufzeiten ohne wirtschaftliche Kompromisse die Bereitschaft erhalten werden kann, das bestmögliche Sicherheitsniveau zu gewährleisten.

Wettbewerb und Kostendruck führen dazu, die Anstrengungen zur Effizienzsteigerung und Rationalisierung zu intensivieren. In diesem Zusammenhang ist es zum einen das Ziel, die Unverfügbarkeitszeiten der Anlage möglichst gering zu halten. Alle Ereignisse, die zu Ausfällen oder Abschalten der Anlage führen, bedeuten Ausfall von Stromerzeugung und damit geringere Erlöse. Zum anderen wird auch versucht, alle wesentlichen Kostenfaktoren zu beeinflussen. Entscheidungskonflikte zwischen Wirtschaftlichkeit und Sicherheit sind unvermeidbar. Dabei besteht die Gefahr, dass Sicherheitsaspekte ökonomischen Interessen untergeordnet werden.

Insgesamt haben die wirtschaftlichen Optimierungsmassnahmen zum Ziel, dass die bestehenden Spielräume, die als Sicherheitsreserven bei der Auslegung eingeplant wurden, weitgehender ausgenutzt werden als vorher und eine zunehmende Annäherung an die Auslegungsgrenzen stattfindet. Obwohl die damit einhergehenden Änderungen nur im Rahmen der durch das Regelwerk vorgeschriebenen Anforderungen erfolgen dürfen, wird dadurch de facto das ursprünglich vorgesehene Sicherheitsniveau abgesenkt. Sicherheitsreserven sind bei der Auslegung zur Abdeckung bestehender Unsicherheiten und Kenntnislücken erforderlich. Durch Verringerung der Sicherheitsreserven wird die Vorsorge gegen Schäden durch Ereignisse oder Bedingungen, die bei Auslegung nicht genau bekannt waren, eingeschränkt.

Schnellabschaltungen sowie An- und Abfahrvorgänge verursachen neben dem Ertragsausfall verstärkte Materialbelastungen und verkürzen dadurch die Lebensdauer wichtiger Komponenten. Im Zweifelsfall, wenn zwischen dem Abschalten der Anlage und dem Weiterbetrieb zu entscheiden ist, können wirtschaftliche Erwägung den Ausschlag geben.

Da nur wenige Kostenfaktoren im Betrieb unmittelbar beeinflusst werden können, wird insbesondere versucht, durch Optimierung der Instandhaltung Kostenvorteile zu erringen. Dies kann erreicht werden durch Minimierung der reparaturbedingten Ausfallzeiten, Minimierung der Wartungsvorgänge Vergrößerung der Wartungsintervalle sowie Wechsel von der vorbeugenden Instandhaltung zur zustandsorientierten Instandhaltung. Dabei nimmt man Schäden bzw. Ausfälle von Komponenten in Kauf. Dies bedeutet aber immer auch eine Schwächung des Sicherheitskonzepts, da dadurch der Verfügbarkeit betrieblicher Komponenten eine geringere Bedeutung beigemessen wird.

Wirtschaftliche Zwänge sind nicht zuletzt auch ein Grund dafür, sich eher an dem durch das Regelwerk Geforderten als an dem sicherheitstechnisch Möglichen zu orientieren. Dadurch wird nur das vorgeschriebene, nicht aber das bestmögliche Sicherheitsniveau erreicht.

13.12.2002

Ein bedeutsamer Kostenfaktor ist das Personal. Ein Reduzierungspotenzial besteht hier, indem der eigene Personalbestand reduziert wird und indem verstärkt auf „billigeres“ Fremdpersonal zugegriffen wird. Anforderungen an die Mindest-Personalstärke werden auch durch Sicherheitsaspekte bestimmt. Die aus sicherheitstechnischer Sicht notwendigen und vorgeschriebenen Tätigkeiten müssen jederzeit gewährleistet sein. Dazu bestehen eindeutige Vorgaben. Insofern erscheint es zunächst selbstverständlich, dass der Betreiber aus wirtschaftlichem Eigeninteresse für einen ausreichenden Personalbestand sorgt. Auch hier sind aber Entscheidungskonflikte möglich, wenn es zu Personalengpässen kommt, bei denen im Zweifelsfall ökonomische Interessen über die Sicherheit gestellt werden. Der Vorfall im belgischen Kernkraftwerk Tihange (s.u) ist dafür ein Beispiel. Der verstärkte Einsatz von Fremdpersonal ist i.d.R. durch die günstigere Kostenstruktur der Fremdfirmen begründet. Sofern durch die Auslagerung von Tätigkeiten sicherheitsrelevante Bereiche betroffen sind, bestehen an die Qualifikation und Zuverlässigkeit der dort Beschäftigten die gleichen Anforderungen wie bei eigenem Personal. Hierzu stellt sich die Frage, wie von dem für alle Vorgänge letztlich verantwortlichen Betreiber diese Anforderungen überprüft und sichergestellt werden können.

Grundsätzlich besteht die Schwierigkeit, nachzuweisen, dass bestimmte Ereignisse auf äussere Faktoren, z.B. ökonomische Interessen, zurückzuführen sind. Daher lassen sich hier nur die grundlegenden Einflussmöglichkeiten beschreiben. Nach gegenwärtigem Verständnis kann in erster Linie durch eine ausgebildete Sicherheitskultur nachteiligen Entwicklungen begegnet werden (s.o.).

3.3 Beispiele

Im folgenden sind in unsystematischer Zusammenstellung Beispiele für Ereignisse in Kernkraftwerken aufgeführt, an denen menschliche Fehlhandlungen in wesentlichem Umfang mitbeteiligt waren. Anhand dieser Beispiele lassen sich einige der beschriebenen Fehlerursachen, unterschiedlich stark ausgeprägt, nachvollziehen. Gleichzeitig werden auch mögliche Konsequenzen deutlich.

- *Browns, Ferry I, 1975*: Kabelführungen sind undicht. Das Reparaturpersonal untersucht mit einer brennenden Kerze die Herkunft der Zugluft. Dabei entzündet sich die Kunststoffverkleidung wichtiger Kabel, was die Reaktorwarte teilweise blind macht.
- *Brunsbüttel, 1978*: Bei auf das Maschinenhaus gerichtetem Wind steigt dort der Luftdruck. Dadurch wird immer wieder überflüssigerweise das Anregekriterium für die Reaktorschnellabschaltung „Druck im Maschinenhaus hoch“ ausgelöst. Die Bedienungsmannschaft überbrückt deshalb routinemässig das Anregekriterium, wenn der Druck steigt. Das geschieht auch, als eines Tages der Druck durch kontaminierten Dampf erzeugt wird, der wegen eines abgerissenen Stützens aus der Turbine ins Maschinenhaus und von dort ins Freie strömt. Nach 3

Stunden schaltet der Reaktor ab wegen der Wassermenge, die sich auf dem Boden des Maschinenhauses gesammelt hat.

- *Harrisburg, 1979:* Nach Ausfall der Speisewasserpumpen wird der Reaktor schnellabgeschaltet. Die Nachwärmeabfuhr müsste von den Notspeisewasserpumpen übernommen werden. Die vor diesen befindlichen Absperrarmaturen sind jedoch nach Wartungsarbeiten versehentlich nicht wieder geöffnet worden. Die Wärmeabfuhr unterbleibt, was nach 8 Minuten bemerkt wird. Aufgrund weiterer Fehleingriffe kommt es zu einem partiellen Kernschmelzen.
- *Tschernobyl, 1986:* Zur Vorbereitung eines Generatorexperiments am laufenden Reaktor wird der Reaktor nach mehreren Bedienungsfehlern durch fast vollständiges Herausziehen der Abschaltstäbe steuerlos gemacht, so dass beim Leistungsanstieg zum Beginn des Experiments eine schnelle Leistungsexkursion eintritt, die den Reaktorkern weitgehend zerstört.
- *Biblis, 1988:* Beim Anfahren des Reaktors steht eine Ventilklappe offen, die die Rohrleitung eines Notkühlsystems vom Kern absperren soll. Das entsprechende (korrekte) Lichtsignal wird von dem Reaktorpersonal als Fehlfunktion eines Messwertgebers interpretiert. Nach 15 Stunden wird der Irrtum festgestellt. Der Reaktor wird nicht abgeschaltet (was Produktionsausfälle nach sich zöge). Man öffnet kurzzeitig ein hinter dem ersten befindliches zweites Ventil zu einer Prüfleitung, um durch den so entstehenden Wasserfluss die Klappe des ersten Ventils zu bewegen. Zugleich fließt damit aber kontaminiertes Wasser in den Ringraum ausserhalb des Kerns.
- *Biblis, 1994:* In den Motor einer Hauptkühlmittelpumpe im AKW Biblis A gerät ein Fremdkörper, der bei Revisionsarbeiten dort liegen gelassen wurde. Der Fremdkörper löst zuerst einen Kurzschluss und dann einen Brand aus. Der Reaktor ist zum Zeitpunkt des Ereignisses abgeschaltet.
- *Biblis, 1997:* Weil in einer Pumpe im AKW Biblis B ein Arbeitshelm vergessen wurde, fällt sie aus. Der Pumpenraum wird überflutet. Der Reaktor ist zum Zeitpunkt des Ereignisses nicht am Netz.
- *Barsebeck 1998:* Im AKW Barsebeck kam es zu einem Totalausfall des Not- und Hilfskühlsystems, nachdem bei Testarbeiten am System vor Ort irrtümlich die falschen Leitungen geschlossen worden waren. Der Totalausfall des Kühlsystems führte schliesslich zum Ausfall aller vier Hauptkühlmittelpumpen. Eine Reaktor-Schnellabschaltung wurde manuell eingeleitet. Die fehlerhaft geschlossenen Ventile wurde kurze Zeit später auf Anweisungen des Kontrollraums wieder geöffnet.
- *Unterweser, 1998:* Bei einer Schnellabschaltung im AKW Unterweser wird festgestellt, dass an einer Hauptleitung alle Sicherheitsventile seit zwei Tagen gesperrt sind. Das Personal bemerkte diesen Fehler nicht, weil die Ventilschlüssel am falschen Haken hingen.

13.12.2002

- *Tihange, 2001*: Im belgischen Kernkraftwerk Tihange konnte im Juli 2001 ein Kontrollrundgang im Kraftwerk aufgrund von Personalmangel nicht durchgeführt werden.

4 Bewertung von Personalhandlungen

Aufgrund des oben beschriebenen weitreichenden Einflusses des Menschen auf die Sicherheit von Kernkraftwerken ist international unbestritten, dass Personalhandlungen auch in die Sicherheitsbewertung der Anlagen eingehen müssen.

Bei der Bewertung von Personalhandlungen in technischen Systemen können nach /Sträter 1997/ zwei wesentliche Ziele und Verfahrensweisen unterschieden werden:

- Die retrospektive Beurteilung analysiert tatsächlich aufgetretene Ereignisse und Auffälligkeiten, mit dem Ziel die Ursachen beobachteter Fälle zu ermitteln und mögliche Verbesserungsmaßnahmen abzuleiten.
- Bei der prospektiven Beurteilung werden potentielle Fehler technischer Systeme analysiert. Mit probabilistischen Ansätzen werden auch Personalhandlungen analysiert und quantitativ bewertet. Neben der Modellierung des zu betrachtenden Ablaufs sind dafür auch Daten über die Eintrittswahrscheinlichkeit bestimmter Störungen sowie über den Störungsablauf und ggf. über das Schadensausmass erforderlich. Die Ergebnisse der retrospektiven Beurteilung sollten in die prospektive Bewertung mit einfließen.

In der probabilistischen Sicherheitsanalyse (PSA) wird aufbauend auf Daten der bisherigen Betriebserfahrungen versucht, Eintrittswahrscheinlichkeiten für bestimmte Störfallereignisse zu ermitteln. Als mögliche Einflussgrößen sind dabei sowohl technische Störungen als auch Fehlhandlungen zu berücksichtigen.

Zunächst erfolgt eine kurze Beschreibung der Vorgehensweise bei der PSA und der Einbindung der menschlichen Zuverlässigkeitsanalyse, ihrer Hintergründe und ihrer Ziele. Anschliessend werden Grenzen und Unsicherheiten bei der Bewertung der menschlichen Zuverlässigkeit zusammengestellt und daraus resultierende Einflüsse auf die Anwendbarkeit von PSA-Ergebnissen kurz diskutiert.

13.12.2002

4.1 Methode und Ziele der menschlichen Zuverlässigkeitsanalyse in der PSA

Die IAEA empfiehlt für Kernkraftwerke alle 10 Jahre eine periodische Sicherheitsüberprüfung (PSÜ) durchzuführen, in der das aktuelle Sicherheitsniveau der Anlagen am Stand von Wissenschaft und Technik gemessen und bewertet wird. Die HSK hat zur Durchführungen der PSÜ im Jahr 2001 den Leitfaden „Periodische Sicherheitsüberprüfung von Kernkraftwerken“ /HSK 2001/ veröffentlicht, der im Kapitel „Grundsätze der Periodischen Sicherheitsüberprüfung“ die Bedeutung des Einflusses des Betriebspersonals auf die Sicherheit der Anlage hervorhebt:

„Neben den technischen Massnahmen hängt die Sicherheit des Kernkraftwerks entscheidend von der Ausbildung und dem Sicherheitsbewusstsein des Betriebspersonals sowie den organisatorischen Massnahmen und deren Wechselwirkung ab.“ /HSK 2001/

Innerhalb der periodischen Sicherheitsüberprüfung (PSÜ) werden mit der probabilistischen Sicherheitsanalyse (PSA) die zu erwartende Häufigkeit von Schadenszuständen sowie ggf. daraus resultierende Freisetzungen radioaktiver Stoffe als quantitatives Mass für die Sicherheit der zu untersuchenden Anlage ermittelt. Gemäss dem HSK-Leitfaden für die Durchführung einer PSÜ /HSK 2001/ ist anhand einer PSA nachzuweisen, dass:

- *„bei auslegungsüberschreitenden Störfällen schwere Kernschäden durch interne Massnahmen weitgehend verhindert bzw. die Auswirkungen bei schweren Kernschäden verringert werden können,*
- *das Kernkraftwerk ein ausreichendes Sicherheitsniveau besitzt,*
- *das Sicherheitskonzept des Kernkraftwerks ausgewogen ist.“*

Die HSK unterscheidet je nach Umfang der Analysen folgende Formen der PSA /HSK 2001/:

- *„Analyse und Quantifizierung von Störfallabläufen im Leistungsbetrieb, die zu einem schweren Kernschaden führen können (Level 1),*
- *Analyse und Quantifizierung der physikalischen Phänomene nach einem Kernschaden, der Massnahmen zur Verringerung der Unfallfolgen sowie Zeitpunkt, Art und Häufigkeit möglicher Aktivitätsfreisetzungen (Level 2),*
- *Analyse und Quantifizierung von Störfallabläufen beim An- und Abfahren sowie im Stillstand des Kernkraftwerks zu Revisionszwecken, die zu einem Brennstoffschaden führen können.“*

In die PSA sind auch Personalhandlungen als Einflussgröße in die Bewertung der Anlagensicherheit einzubeziehen, siehe z.B. /IAEA 1992/. Abbildung 4.1 zeigt ein Ablaufschema für eine PSA, das verdeutlicht, in welchem Bereich des Gesamtablaufs der Einfluss von Personalhandlungen (grau schraffierte Felder) berücksichtigt wird.

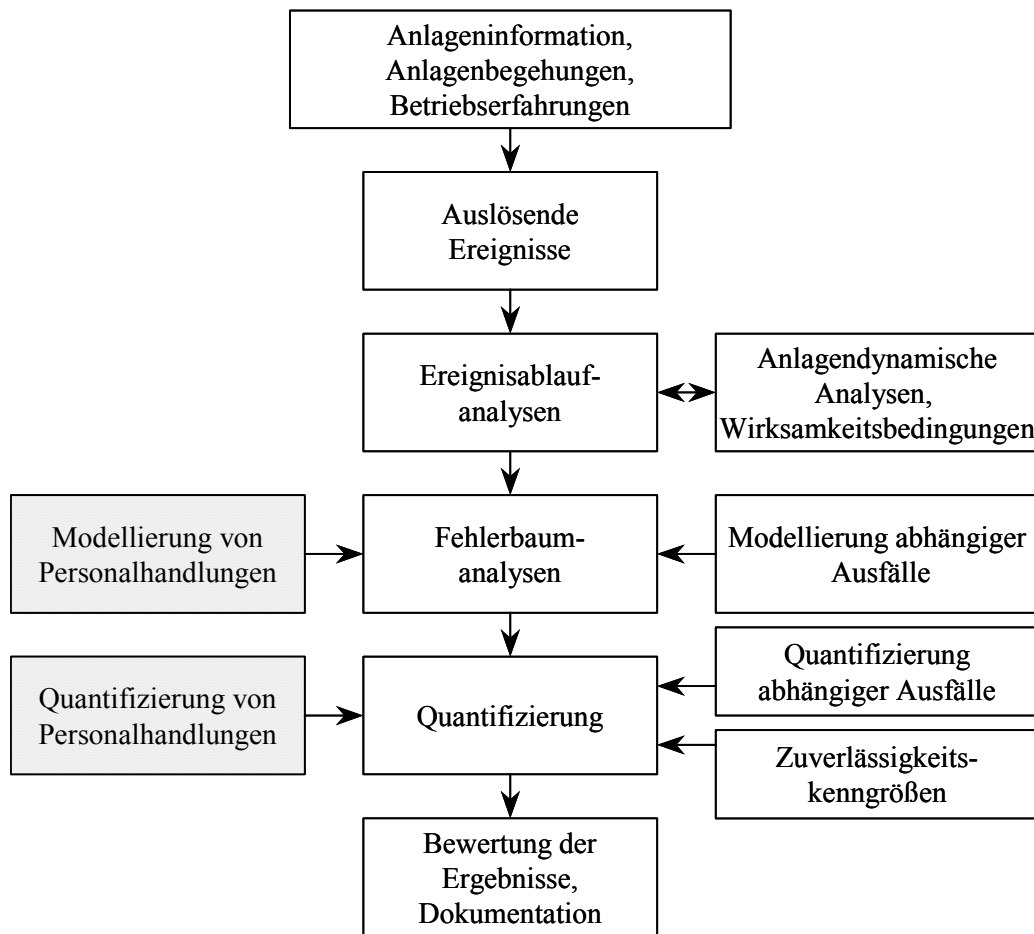


Abbildung 4.1: Ablauf der Probabilistischen Sicherheitsanalyse (PSA) im Rahmen der periodischen Sicherheitsüberprüfung nach /BMU 1996/

Das Ablaufschema zeigt, dass die Fehlerbaumanalyse des Ausfalls einer Systemfunktion den Beitrag der Personalhandlungen und den Beitrag technisch bedingter Ausfälle an der Ausfallwahrscheinlichkeit der entsprechenden Systemfunktion zusammenführt. Der menschliche Fehler wird in diesem Modell wie der technisch bedingte Ausfall einer Komponente behandelt. Dafür wird im Schritt „**Modellierung der Personalhandlungen**“ zunächst die Identifizierung derjenigen Personalhandlungen vorgenommen, die die zu untersuchende Systemfunktion beeinflussen können. Diese Handlungen sind zur weiteren Bearbeitung entsprechend den Anforderungen des gewählten Bewertungsverfahrens modellässig darzustellen.

13.12.2002

des gewählten Bewertungsverfahrens modellässig darzustellen. Im nächsten Schritt, der „**Quantifizierung**“, ist eine Fehlerwahrscheinlichkeit für die Personalhandlung (Human Error Probability, HEP) zu ermitteln. Zur Bestimmung dieser Fehlerwahrscheinlichkeit dient die Human Reliability Analyse (HRA).

Eine Beschreibung der für eine Zuverlässigkeitsanalyse durchzuführenden Schritte liegt z.B. in /IAEA 1992/ oder /Swain 1983/ vor. Unter Bezug auf /IAEA 1992/ ergibt sich die folgende Gliederung des Ablaufs der Zuverlässigkeitsanalyse:

I. Systemanalyse:

Die Systemanalyse dient dazu, die nachfolgend mit einem HRA-Verfahren zu analysierenden Personalhandlungen, die die Fehlerwahrscheinlichkeit des Systems beeinflussen können, zu erfassen und hinsichtlich ihrer Relevanz einzustufen. Dieser Vorgang umfasst die folgenden Schritte:

1. Definition:

In diesem Schritt ist sicherzustellen, dass alle Handlungen berücksichtigt werden, die im Rahmen des zu analysierenden Ablaufs relevant sind, d.h. für die eine HRA durchzuführen ist. Zu diesem Zweck werden gemäss /IAEA 1992/ drei Kategorien und fünf Typen menschlicher Handlungen unterschieden. Die Einteilung beruht auf der Annahme, dass die Einwirkung des Menschen bei den in der PSA untersuchten Ereignissen vor, während und nach dem Beginn eines Ereignisses erfolgen kann und dass sie einen Unfall mildern oder verschlimmern kann.

- Kategorie A (Typ 1): Personalhandlungen, die während des bestimmungsgemässen Betriebes der Anlage durchgeführt werden und Wartungs- und Instandhaltungsmassnahmen umfassen, die aufgrund fehlerhaften Abschlusses die Systemverfügbarkeit beeinträchtigen. Fehler dieser Kategorie gehen in der PSA in die Bestimmung der Ausfallwahrscheinlichkeit einer technischen Komponente ein.
- Kategorie B (Typ 2): Fehlerhafte Personalhandlungen, die ein auslösendes Ereignis zur Folge haben. Fehler dieser Kategorie werden i.A. in der PSA in der Annahme über die Häufigkeit auslösender Ereignisse berücksichtigt.
- Kategorie C: Personalhandlungen als Reaktion auf einen eingetretenen Störfall. Hier werden drei Typen unterschieden:
 - Typ 3: geplante Handlungen, die den Ereignisablauf positiv beeinflussen,
 - Typ 4: fehlerhafte Ausführungen von Handlungen, die den Ablauf negativ beeinflussen,
 - Typ 5: ungeplante Handlungen, die den Ereignisablauf positiv beeinflussen.

Der Schwerpunkt der Untersuchungen mit den Methoden der HRA liegt auf den Handlungen der Kategorie C, Typ 3, ggf. sind auch die Kategorien A und B einzubeziehen.

2. Screening:

In diesem Schritt sind die Personalhandlungen zu identifizieren, die für einen Störfallablauf Anlage entscheidend sind (Konzentration auf Schlüsselhandlungen).

II. Analyse unter Anwendung eines HRA-Verfahrens

Die Analyse der relevanten Personalhandlungen erfolgt in einem qualitativen Vorgang (Schritte 3 bis 5) und einem anschliessenden quantitativen Vorgang (Schritt 6). Die Umsetzung der durchzuführenden Schritte wird im Detail durch das spezifisch ausgewählte HRA-Verfahren bestimmt. Ziel aller Verfahren ist die quantitative Bewertung der Zuverlässigkeit von Personalhandlungen, um diese, vergleichbar einer technischen Komponente, bei der Ermittlung von Versagenswahrscheinlichkeiten von Systemen in der PSA zu verwenden.

Zur Analyse und Quantifizierung von Personalhandlungen existiert eine Vielzahl von Verfahren. Häufig angewandte Verfahren sind

- THERP (Technique for Human Error Rate Prediction),
- ASEP (Accident Sequence Evaluation Program),
- HCR (Human Cognitive Reliability) - Model,
- PHRA (Probabilistic Human Reliability Analysis) und
- SLIM (Success Likelihood Index Method)

Beispielhaft wird nachfolgend den Analyseschritten gemäss /IAEA 1992/ die Vorgehensweise nach dem THERP-Verfahren zugeordnet, die u.a. in /BfS 1996/ beschrieben ist.

3. Qualitative Analyse:

In diesem Schritt ist eine detaillierte Beschreibung wichtiger Personalhandlungen durch Definition von Schlüsselfaktoren zu entwickeln.

Die Personalhandlung wird im THERP-Verfahren zu diesem Zweck in Teilaufgaben zerlegt, für die mögliche Fehlhandlungen identifiziert werden, die eine Ursache für das Versagen des betrachteten Systems oder Ablaufs darstellen können. Ggf. ist eine weitere Zerlegung der Teilaufgaben in Einzelmassnahmen erforderlich. Als Informationsquellen für die Handlungsanalyse werden z.B. Betriebshandbuch, Notfallhandbuch, Wartenbelegungspläne, Schichtbuch, Organisationshandbuch, Systembeschreibungen sowie Ergebnisse von Simulator-schulungen verwendet.

4. Repräsentation:

Entsprechend dem gewählten HRA-Verfahren sind die wesentlichen Personalhandlungen in einer logischen Repräsentation, d.h. einem Modell, darzustellen.

13.12.2002

Im THERP-Verfahren erfolgt die Modellierung der definierten Teilaufgaben in einem HRA-Ereignisbaum. Diese Darstellung stellt die Schnittstelle zwischen dem qualitativen und dem quantitativen Teil der Analyse dar.

5. Einfluss/Zusammenfassung:

Falls erforderlich sind in diesem Schritt der Ereignisabläufe und die Systemmodell anzupassen, wenn die detaillierte qualitative Analyse potentielle neue Einflussfaktoren auf das Systemverhalten ergeben hat.

6. Quantifizierung:

Den verschiedenen Personalhandlungen werden quantitative Daten zur Angabe von Fehlerwahrscheinlichkeiten zugewiesen. Ausserdem ist eine Sensitivitätsanalyse durchzuführen und die Unsicherheitsbandbreite zu bestimmen.

Die Quantifizierung der Fehlerwahrscheinlichkeiten von Teilaufgaben erfolgt im THERP-Verfahren durch die Zuweisung von „nominalen Fehlerwahrscheinlichkeiten“ und die Berücksichtigung leistungsbeeinflussender Einflussfaktoren (siehe Abbildung 3.1). Diese Angaben können teilweise aus einem umfangreichen Tabellenwerk für einzelne Teilaufgaben entnommen werden. Sofern keine Angaben vorhanden sind, wird der Beitrag leistungsbeeinflussender Einflussfaktoren durch Schätzungen ermittelt.

Anschliessend werden Abhängigkeiten zwischen den einzelnen im Ereignisbaum dargestellten Teilaufgaben bewertet (z.B. die Möglichkeit einen Fehler, der in einer Teilaufgabe gemacht wird mit einer anderen Handlung zu beheben. Aus den Fehlerwahrscheinlichkeiten der einzelnen Teilaufgaben wird abschliessend eine Gesamtfehlerwahrscheinlichkeit für die betrachtete Personalhandlung ermittelt.

III. Dokumentation

7. Dokumentation:

Alle Schritte der Untersuchung sind so zu dokumentieren, dass sie nachvollziehbar, verständlich und reproduzierbar sind.

Die Ergebnisse der HRA-Analyse werden in die Analyse eines Ablaufs in der PSA eingebunden. (Da der erforderliche Detaillierungsgrad der Analyse iterativ zu ermitteln ist, muss die PSA nach Einfügen der HRA-Ergebnisse erneut berechnet werden, um über Bedarf weiterer Detaillierung der Analyse zu entscheiden).

4.2 Unsicherheiten und Grenzen der Bewertung von Personalhandlungen in der PSA

Die Analyse des Einflusses von Personalhandlungen auf die Sicherheit von Kernkraftwerken in der PSA beruht auf dem Ansatz, die menschliche Handlung als Komponente des Mensch-Maschine-Systems zu beschreiben. Sie wird dabei weitgehend analog zu technischen Systemen modelliert und hinsichtlich ihrer Fehlerwahrscheinlichkeit quantifiziert.

Aus diesem Ansatz resultieren

- verschiedene Unsicherheiten, die das Ergebnis der Analyse beeinflussen, sowie
- Grenzen bei der Ermittlung und Bewertung des menschlichen Einflusses auf sicherheitsrelevante Abläufe.

Unsicherheiten bei der Bewertung von Personalhandlungen in der PSA

Die probabilistische Analyse der Sicherheit komplexer Anlagen ist generell mit Unsicherheiten verbunden, die z.B. auf die Begrenzung der untersuchten Ereignisse und Abläufe, auf Unzulänglichkeiten in der Modellierung der Abläufe und auf Ungenauigkeiten bei der Quantifizierung von Versagenswahrscheinlichkeiten einzelner Komponenten zurückzuführen ist. Die bestehenden Unsicherheiten lassen sich je nach Ursache mit unterschiedlicher Genauigkeit quantifizieren.

Bei der Analyse der menschlichen Zuverlässigkeit führen insbesondere zwei Aspekte zu wesentlichen Unsicherheiten, die sich auch auf das Gesamtergebnis der PSA auswirken:

- die Modellierung der menschlichen Handlung als Systemkomponente und
- die Definition der Eingangsdaten für die Quantifizierung der Personalhandlungen.

Die modellmässige Abbildung von Personalhandlungen erfordert eine Abstraktion und Vereinfachung der real erfolgenden Vorgehensweise. Die dadurch entstehenden Unsicherheiten sind um so grösser je komplexer der modellierte Ablauf ist. Relevante Faktoren sind z.B.

- Die Konzentration auf ausgewählte Personalhandlungen, die im Hinblick auf die Fehlerwahrscheinlichkeit eines Ablaufs für relevant gehalten werden.
- Die Beschränkung auf solche Handlungen, die mittels eines HRA-Verfahrens analysiert werden können. Dies schliesst alle ungeplanten Handlungen, die in Art und Häufigkeit aufgrund der menschlichen Kreativität nicht quantifiziert werden können, systematisch aus.

13.12.2002

- Die diskrete Betrachtung der einzelnen Handlungen oder Teilhandlungen, die innerhalb eines Ablaufs erforderlich sind.
- Die Vernachlässigung der Betrachtung von Schnittstellen zwischen den einzelnen betrachteten Komponenten des analysierten Systems.
- Die Reduzierung der Betrachtungen auf das Mensch-Maschine-System ohne Berücksichtigung organisatorischer Einflüsse, die das analysierte System insgesamt (nicht nur einzelne Personalhandlungen) betreffen.

Darüber hinaus stellt die Modellbildung immer nur einen der möglichen Abläufe dar, ist jedoch keine Vorhersage, dass genau dieser Ablauf auch eintritt.

Die Quantifizierung von Fehlerwahrscheinlichkeiten bei Personalhandlungen unterscheidet sich wesentlich von der Bestimmung der Ausfallwahrscheinlichkeiten technischer Komponenten. Während Ausfallwahrscheinlichkeiten technischer Komponenten empirisch ermittelt werden können, erfolgt die Quantifizierung von Personalhandlungen in der Regel auf Grund von Expertenschätzungen, die sich auf Betriebserfahrungen stützen.

Diese Vorgehensweise setzt voraus,

- dass über die zu quantifizierende Handlung ausreichende Betriebserfahrungen vorliegen und
- dass der reale Handlungsablauf auf eine standardisierte Situation, für die aufgrund von Betriebserfahrungen eine Aussage über die Fehlerwahrscheinlichkeit vorliegt, abgebildet wird.

Da die Möglichkeiten menschlicher Handlungen und die sie beeinflussenden Parameter eine grosse Vielzahl möglicher Varianten eines Handlungsablaufs bedingen, ist die Quantifizierung der Fehlerwahrscheinlichkeit zwangsläufig mit Unsicherheiten verbunden, die erheblich grösser sind als die Unsicherheiten bei der Quantifizierung von Ausfallwahrscheinlichkeiten technischer Komponenten.

Insgesamt zeigt sich, dass die Modellierung menschlicher Handlungen und die Quantifizierung der Wahrscheinlichkeit von Fehlern mit erheblichen Unsicherheiten verbunden ist, die vielfach nicht hinreichend quantifiziert werden können. Die Möglichkeiten der Analyse von Personalhandlungen spiegeln insofern nicht die Bedeutung menschlicher Handlungen für die Sicherheit von Kernkraftwerken wider.

Grenzen der Bewertung von Personalhandlungen in der PSA

Die gängigen Methoden zur Erfassung des Einflusses von Personalhandlungen in der PSA weisen Grenzen auf, die verschiedentlich in der Literatur diskutiert werden. Diese ergeben sich zum einen daraus, dass die gängigen HRA-Verfahren aufgrund

der notwendigen Eingangsdaten zur qualitativen Analyse der Personalhandlungen sowie zur quantitativen Bewertung nur für geplante Handlungen anwendbar sind. Zum anderen werden durch die Zerlegung der betrachteten Systeme in einzelne Handlungen und Teilhandlungen Aspekte vernachlässigt, die das System als Ganzes betreffen.

Berücksichtigung nicht geplanter Handlungen

Die Modellierung von Personalhandlungen als Komponente im Mensch-Maschine-System baut auf bekannten Abläufen und vorgeschriebenen Regeln auf. Entsprechend sind diesem System Grenzen gesetzt bei der Berücksichtigung von Handlungen in neuartigen Situationen bzw. ungeplanten Handlungen, die auf dieser Grundlage nicht abbildbar sind.

Wissensbasiertes Verhalten

Ungeplante Handlungen können nach dem dreistufigen Verhaltensmodell nach Rasmussen, das Verhaltensweisen in Abhängigkeit von der Art der kognitiven Beanspruchung des Operateurs unterscheidet, dem Bereich des wissensbasierten Verhaltens zugeordnet werden.

- **Fertigkeitsbasiertes Verhalten:** kennzeichnet Abläufe, die als Routinen auf der Basis umfangreicher Erfahrungen und Übung nahezu als „automatisch“ durchgeführt werden.
- **Regelbasiertes Verhalten:** kennzeichnet Abläufe, die auf der Basis bestehender fester Regeln nach einem festen Schema durchgeführt werden.
- **Wissensbasiertes Verhalten:** ist in Situationen erforderlich, die neuartig sind und für die kein eingeübter Handlungsablauf zur Verfügung steht. Planung und Ausführung des Ablaufs basieren auf dem verfügbare Wissen des Personals.

Für die Analyse des Einflusses menschlicher Handlungen mit den derzeit gängigen HRA-Verfahren in der PSA sind nur die beiden ersten Verhaltensweisen zugänglich. Damit bleiben genau die Handlungen im Bereich des wissensbasierten Verhaltens in der Analyse unberücksichtigt, in denen sich der Mensch durch seine Kreativität und seine Fähigkeit, vorhandenes Wissen und Fähigkeiten auf unbekannte Situationen zu transferieren, deutlich von den technischen Systemen unterscheidet.

Bezogen auf die oben dargestellten Handlungskategorien und -typen bedeutet dies, dass Personalhandlungen der Typen C4 (fehlerhafte Ausführungen von Handlungen, die den Ablauf negativ beeinflussen) und C5 (ungeplante Handlungen, die den Ablauf positiv beeinflussen) nicht in der Zuverlässigkeitsanalyse berücksichtigt werden können, da keine geeigneten Verfahren zur Verfügung stehen, um die damit zusammenhängenden ungeplanten bzw. wissensbasierten Verhaltensweisen zu erfassen. Entsprechende Hinweise finden sich z.B. in /GRS 2001/, /BfS 1998/ und /Sträter 1997/. In /GRS 2001/ wird weiterhin darauf hingewiesen, dass situationsspezifische (ungeplante) Handlungen auch dann erforderlich sein können, wenn zwar

13.12.2002

vorgeplante Massnahmen verfügbar sind, die situationsspezifischen Randbedingungen aber erheblich von den Randbedingungen abweichen, die für die vorgeplanten Massnahmen zugrunde gelegt wurden.

Insgesamt ergibt sich daraus bereits im ersten Schritt der Zuverlässigkeitsanalyse, der Definition der zu berücksichtigenden Personalhandlungen, eine erhebliche Einschränkung des erfassbaren Handlungsspektrums.

Fahrlässige und vorsätzliche Fehler

Auch im Hinblick auf die erfassbaren Fehlerarten ergeben sich Einschränkungen durch die Begrenzung der Anwendbarkeit gängiger HRA-Verfahren auf geplante Handlungen. Wie in Kapitel 3.1 beschrieben können prinzipiell drei Fehlerarten unterschieden werden:

- Zuverlässigkeit,
- Fahrlässigkeit,
- Vorsätzlichkeit.

Mögliche Fehler, die dem Bereich **Zuverlässigkeit** zuzuordnen sind, sind beispielsweise Ausführungsfehler, Bedienungsfehler oder Auslassungsfehler. Fehler in diesem Bereich betreffen in den meisten Fällen geplante Handlungen, die beispielsweise in schriftlichen Regeln oder Anweisungen vorgeschrieben sind.

Der Fehlerart **Fahrlässigkeit** werden in /BfS 1998/ beispielsweise die Ignoranz von Regeln und des Risikos, mangelhaftes Betriebshandbuch, ungeeignete Schichtbesetzung, Mängel in Management, Organisation und Personalqualifikation zugeordnet. Diese Aspekte aus dem Bereich der Sicherheitskultur sind nach den Anforderungen des Mensch-Maschine-Systems nicht modellierbar, da sie u.a. nicht anhand geplanter Handlungen beschrieben werden können.

Auf den Umgang mit **vorsätzlich** verursachten Fehlern wurde bereits im Kapitel 3.1 hingewiesen. Sie werden in der PSA nicht berücksichtigt.

Während vorsätzliche Fehler ggf. mit Analysen im Bereich der Anlagensicherung teilweise berücksichtigt werden können, entsteht durch die mangelnde Berücksichtigung fahrlässig verursachter Fehler in der PSA ein Defizit bei der Sicherheitsbewertung. Dieses Defizit kann derzeit auch mit anderen Methoden der Sicherheitsbewertung, z.B. der Bewertung von Sicherheitskultur, nicht kompensiert werden. Einzelne Voraussetzungen, die zur Entstehung fahrlässiger Fehler führen können, sind zwar mit Methoden zur Bewertung von Sicherheitskultur qualitativ erfassbar. Es besteht jedoch derzeit kein Verfahren, mit dem diese qualitativen Ergebnisse in die quantitative Bewertung des Mensch-Maschine-Systems in der PSA eingebunden werden können.

Berücksichtigung des Einflusses von Organisation und Management

Die menschliche Zuverlässigkeitsanalyse in der PSA bildet die menschliche Handlung als eine Komponente im Mensch-Maschine-System ab. Dabei werden die für den zu analysierenden Ablauf wichtigen Personalhandlungen in Teilhandlungen oder Einzelmassnahmen zerlegt. Durch die entkoppelte Betrachtung einzelner Personalhandlungen bzw. Teilhandlungen werden zwangsläufig Aspekte vernachlässigt, die die zu analysierende Systemfunktion als Ganzes betreffen. Dies gilt insbesondere für den Einfluss organisatorischer Aspekte sowie der Kommunikation zwischen den beteiligten Gruppen. Im organisatorischen Bereich können z.B.

- unklare Zuständigkeits- und Verantwortungsstrukturen,
- unzureichende Ressourcen (personell und materiell),
- fehlende Festlegung von Sicherheitszielen sowie
- unzureichende Auswertung von Betriebserfahrungen

negativen Einfluss auf die Wahrscheinlichkeit von Fehlhandlungen der Personals zeigen. Sie werden jedoch im Ergebnis der Zuverlässigkeitsanalyse nicht abgebildet.

In /TÜV-N 1999/ wird darauf hingewiesen, dass die Festlegungen, die z.B. im Betriebshandbuch, Prüfhandbuch sowie in Qualitätsanweisungen bezüglich Management und Organisation sicherheitsrelevanter Abläufe bestehen (Struktur, Aufgaben und Zuständigkeiten des Kraftwerkspersonals, Aufgaben der Operateure zum bestimmungsgemässen und störungsbedingten Anlagenbetrieb sowie Massnahmen zur Instandhaltung), in der PSA als vollständig wirksam angenommen werden. Untersuchungen zeigen jedoch, dass damit eine unzulässige Reduzierung der für die Anlagensicherheit relevanten Einflussgrössen vorgenommen wird. Dies gilt sowohl für die Kerntechnik als auch für andere Risikotechnologien. Untersuchungen zur Bedeutung von Organisation und Management für die Anlagensicherheit sind daher dringend geboten.

Hier setzen die Methoden zur Bewertung der Sicherheitskultur an. Sie unterscheiden sich allerdings wesentlich von den HRA-Verfahren, da die zu bewertenden Aspekte nicht anhand definierter Kriterien quantitativ erfassbar sind. Die Bewertung erfolgt daher im Allgemeinen qualitativ anhand von Indikatoren. Eine Einbindung in die PSA ist auf dieser Basis mit den heute gängigen Verfahren nicht möglich.

Aufgrund von Unsicherheiten und Grenzen der Verfahren zur Bewertung der menschlichen Zuverlässigkeit kann der Einfluss von Personalhandlungen auf die Anlagensicherheit nur unzureichend erfasst werden. In den Kapitel 2 und 3 wurde jedoch bereits der weitreichende Einfluss des Menschen in den vielfältigen Situation des Anlagenbetriebs diskutiert. Insbesondere im Bereich der Störfallvermeidung und

13.12.2002

Störfallbeherrschung, d.h. den „Nicht-Routine-Situationen“ ist der Mensch als Wissensträger gefordert. In Störfallsituationen, d.h. im Bereich der Ebenen 4 und 5 des gestaffelten Sicherheitssystems, nimmt die Zahl der ungeplanten Handlungen und nicht vorhersagbaren Situationen zu. Genau diese Aktionen lassen sich jedoch mit den gängigen HRA-Verfahren nicht erfassen. Insofern ergeben sich aus den Unsicherheiten und Grenzen der menschlichen Zuverlässigkeitsanalyse auch nicht zu vernachlässigende Auswirkungen auf die Anwendbarkeit von PSA-Ergebnissen.

4.3 Anwendbarkeit von PSA-Ergebnissen

Probabilistische Sicherheitsanalysen werden in der Kerntechnik als Ergänzung deterministischer Bewertungen der Anlagensicherheit eingesetzt und untersuchen die Wahrscheinlichkeit des Eintretens schwerer Unfälle (ausgedrückt als Kernschmelzhäufigkeit). PSAs können dagegen nicht dazu dienen, die Einhaltung des Standes von Wissenschaft und Technik bei einer Anlage zu überprüfen, da hierfür das deterministische, d.h. von der Wahrscheinlichkeit bestimmter Ereignisse unabhängige sicherheitstechnische Regelwerk heranzuziehen ist.

PSAs ermöglichen die Überprüfung der Ausgewogenheit des Sicherheitskonzepts von Anlagen, indem ermittelt wird, ob bestimmte unfallauslösende Ereignisse in besonderem Masse zur Gesamtkernschmelzhäufigkeit beitragen. Auf diese Weise können sie die gezielte Verbesserung der Anlagensicherheit unterstützen. In diesem Fall sind die Einschränkungen, die sich aus den oben genannten Ursachen aufgrund der unzureichenden Bewertbarkeit von Personalhandlungen ergeben akzeptabel, da das PSA-Ergebniss nur eine ergänzende Information zur Planung von Verbesserungsmaßnahmen darstellt.

Aktuelle Entwicklungen der Sicherheitsbetrachtung basieren jedoch auf einem wesentlich erweiterten Umfang der Nutzung von PSA-Ergebnissen. Während in PSAs der Stufe 1 die Häufigkeit unbeherrschter Anlagenzustände (Kernschmelzhäufigkeit) ermittelt wird, soll mit der erweiterten Betrachtung des Schadensausmasses in PSAs der Stufe 2 eine Quantifizierung des Anlagenrisikos erfolgen. Das so quantifizierte Anlagenrisiko erhält im internationalen Raum zunehmende Bedeutung in kerntechnischen Sicherheitskonzepten.

Besonders deutlich zeigt sich diese Ausprägung im Aufsichtsverfahren der für die US-amerikanischen Kernkraftwerke zuständigen Aufsichtsbehörde NRC (Nuclear Regulatory Commission). Diese hat unter dem Stichwort „Risk-Informed-Regulation“ bereits für wesentliche Entscheidungsprozesse ihres Aufsichtsverfahrens Bewertungskriterien auf der Basis der Ergebnisse probabilistisch ermittelter Kennwerte des Anlagenrisikos eingeführt.

Auch in der aufsichtlichen Tätigkeit der zuständigen Schweizer Behörde HSK werden probabilistische Aussagen über die Anlagensicherheit vielfach zur Entscheidungsfindung herangezogen. So führte beispielsweise bereits im Jahr 1990 der

Schweizer Bundesrat im Verfahren um die endgültige Betriebsbewilligung für das Kernkraftwerk Mühleberg aus (siehe /Öko-Institut 1991/) aus:

„Das Kernkraftwerk Mühleberg wird nach den gleichen deterministischen Auslegungskriterien beurteilt wie das Kernkraftwerk Leibstadt. Die wichtigsten schweizerischen Auslegungskriterien für die Sicherheitssysteme von Kernkraftwerken sind in der Richtlinie R-101 festgelegt. ... Diese dem neuesten Stand der Technik entsprechenden Anforderungen können von der Anlage Mühleberg trotz umfangreichen Nachrüstungen nicht lückenlos erfüllt werden. ... Jede Anlage ist somit für sich zu beurteilen. Dabei spielt die probabilistische Sicherheitsanalyse eine wichtige Rolle.“

Entsprechende Ausführungen finden sich auch im Bericht über die Ergebnisse der Fallstudie Kernkraftwerke im Nationalfonds-Projekt „Risk Based Regulation“ /Schmocker/. In der Kurzbeschreibung des Bewilligungsverfahrens für Schweizer Kernkraftwerke heisst es dort:

„In der Schweiz sind bei neu zu errichtende Kernanlagen die zum Zeitpunkt der Bewilligung gültigen Regelwerke und Richtlinien anzuwenden. Da der Stand von Wissenschaft und Technik einer ständigen Weiterentwicklung unterliegt, können bei anstehenden Bewilligungen für ältere Anlagen nicht in jedem Punkt die heutigen Anforderungen an die Anlage erfüllt werden. In diesem Fall ist es Aufgabe der Aufsichtsbehörde zu prüfen, wie weit ältere Anlagen nachgerüstet werden müssen oder ob Abweichungen toleriert bzw. anderweitig kompensiert werden können. Als wichtige Beurteilungshilfen werden dabei auch die Ergebnisse von anlagenspezifischen Probabilistischen Sicherheitsanalysen (PSA) herangezogen.“

In /Schmocker/ werden auch Richtwerte vorgestellt, die als Bewertungskriterien für die zulässigen Häufigkeiten und Mengen von Freisetzungen radioaktiver Stoffe, d.h. als Mass für das Freisetzungsrisiko, herangezogen werden könnten. Allerdings wird auch festgestellt, dass derzeit noch keine allgemein akzeptierten probabilistischen Sicherheitskriterien im Sinne von Grenzwerten bestehen, dass die vorgeschlagenen Richtwerte jedoch für bestimmte Anwendungen herangezogen werden könnten. Eine ausschliesslich risikobasierte Aufsicht wird mit Hinweis auf Schwierigkeiten bei der PSA-Modellierung für kaum realisierbar gehalten.

Die Anwendung in der Bewilligungspraxis bei älteren Anlagen lässt jedoch deutliche Tendenzen zu einer verstärkten Risikoorientierung im Schweizer Aufsichtsverfahren erkennen.

13.12.2002

Bei den beschriebenen Ansätzen der aufsichtlichen Praxis wird das mit Hilfe der PSA ermittelte Anlagenrisiko zur Grundlage aufsichtlicher Anforderungen und Entscheidungen gemacht. Derartige Entscheidungen können dazu führen, dass Sicherheitsdefizite, die auf der Basis deterministischer Bewertungen ermittelt wurden, akzeptiert werden, wenn ein bestimmter Wert für ein zulässiges Anlagenrisiko unterschritten wird.

Damit wird dem PSA-Ergebnis ein Stellenwert zugewiesen, der unter Berücksichtigung der genannten Grenzen und Unsicherheiten bei der Bewertung von Personalhandlungen – sowie auch im Hinblick auf unabhängig von der HRA bestehende Defizite der PSA-Verfahren – nicht zu rechtfertigen ist. Solange keine geeigneteren Verfahren zur Verfügung stehen, die den Einfluss des Menschen auf die Anlagensicherheit in vollem Umfang erfassen, stellt die Verwendung quantitativer Werte für das Anlagenrisiko eine unzulässige Vernachlässigung des Faktors Mensch in der Anlage dar.

5 Fazit

Die bisherigen Erfahrungen mit dem Betrieb von Kernkraftwerken haben gezeigt, dass eine rein auf technische Aspekte beschränkte Betrachtungsweise allein nicht ausreichend für die Bewertung der Sicherheit von Kernkraftwerken ist. Weitere, wesentliche Einflussgrößen sind zu beachten, die dem administrativen bzw. organisatorischen Rahmen sowie der Ebene der Personalhandlungen zuzuordnen sind. Daraus ergibt sich die Frage, welche Bedeutung dem Faktor Mensch in der Sicherheitskonzeption von Kernkraftwerken zukommt und wie die damit zusammenhängenden Sicherheitsaspekte angemessen eingeordnet und bewertet werden können.

Bei der Einordnung menschlicher Handlungen in das Sicherheitskonzept von Kernkraftwerken sind einige Besonderheiten zu beachten. Das Kernkraftwerk ist ein in hohem Masse automatisiertes technisches System. Dennoch sind auf allen Ebenen Eingriffe durch den Menschen vorgesehen und möglich. Bezieht man die Konzeptionsphase mit ein, lassen sich letztlich nahezu alle Abläufe und Ereignisse im Kernkraftwerk auf menschlichen Einfluss zurückführen. Bei Fehlfunktionen von Sicherheitssystemen oder in der Auslegung nicht vorgesehenen Ereignissen muss trotz aller Automatisierung ein regulierender Eingriff durch den Menschen möglich sein. Menschliche Handlungen und die Interaktionen mit den technischen Systemen sind daher bei der Sicherheitsbewertung angemessen zu berücksichtigen.

Im Normalbetrieb eines Kernkraftwerks sind Personalhandlungen zu einem grossen Teil schriftlich in den Vorschriften und Anweisungen fixiert. Dennoch ergibt sich in einer spezifischen Situation aufgrund äusserer Einflüsse und Randbedingungen eine Vielzahl möglicher Handlungsweisen und -abläufe. Im Fall von Störungen und Störfällen, wird mit steigender Komplexität der Störung zunehmend die spontane, auf Wissen, Erfahrungen und Kreativität basierende Handlung des Operators gefordert. Der Detaillierungsgrad bestehender Vorschriften wird zunehmend geringer. Der Einfluss des Menschen im Sicherheitskonzept ist daher in allen Phase des Betriebs von Kernkraftwerken ein wesentlicher Faktor, der ausserhalb des Normalbetriebs, z.B. während Instandhaltungsmassnahmen und Störungen zusätzliche Bedeutung erhält.

Als Einflussfaktoren, die die menschliche Handlung beeinflussen, wirken sowohl der organisatorische Rahmen und das Sicherheitsbewusstsein der Mitarbeiter, zusammengefasst unter dem Begriff „Sicherheitskultur“, die physische und psychische Verfassung und die konkreten Arbeitsbedingungen als auch äussere Randbedingungen wie wirtschaftliche und politische Rahmenbedingungen der Kernenergienutzung.

Es ist eine grundlegende Erfahrung, dass in jedem technischen System, trotz aller Sorgfalt bei Auslegung, Herstellung und Betrieb, Störungen auftreten können. Alle technischen Komponenten haben nur eine begrenzte Haltbarkeit bzw. Laufzeit. Die Möglichkeit technischen Versagens muss daher akzeptiert werden. Darüber hinaus führen aber auch die vielfältigen Einflussmöglichkeiten des Menschen in der Kon-

13.12.2002

zeption und im Betrieb eines Kernkraftwerks, die komplexen technischen Abläufe, die beherrscht werden müssen, und die Besonderheiten menschlichen Verhaltens dazu, dass der Faktor Mensch nicht ausgeschlossen werden kann und mit Fehlhandlungen gerechnet werden muss. Die Technik unterstützt den Menschen in der Steuerung der Anlage und soll ihn entlasten, um Fehlhandlungen zu vermeiden. Ein vollständiger Ersatz des Menschen durch die Technik ist aber nicht möglich, da einerseits wichtige, an individuelle Entscheidungen gebundene Funktionen, nicht durch Automatismen ersetzt werden können und die Technik selbst fehleranfällig ist. Andererseits führt eine zunehmende Automation dazu, dass die Abläufe in der Anlage nicht mehr nachvollzogen werden können und das Personal dadurch die Fähigkeit verliert, zu jeder Zeit sicherheitsgerichtet eingreifen zu können.

Die Bestrebungen zur Beherrschung des „Human Factor“ laufen daher darauf hinaus, die Schnittstelle von Mensch und Maschine zu optimieren. Eine Fehlerfreiheit kann aber auf keiner Seite garantiert werden. Durch Schulung des Personals wird versucht, Fehlentscheidungen und Fehlhandlungen zu minimieren. Dabei kommt der Erfahrungsauswertung eine entscheidende Rolle zu, da letztlich nur bekannte Phänomene und Abläufe trainiert werden können. Der Kenntniszuwachs ist demnach auf das Auftreten von Fehlern angewiesen. Die Schwierigkeit besteht darin, dass nicht vorhergesagt werden kann, wann, wo und in welcher Kombination Fehler auftreten und ein Eingreifen des Menschen erforderlich wird. Dies trifft in besonderem Masse auf Kombinationen zwischen technischem Versagen und menschlichen Fehlhandlungen zu. Die spezifischen Belastungen im Arbeitsumfeld in Störfallsituationen können in Schulungsmassnahmen nicht simuliert werden. Dem Erfolg von Schulungsmassnahmen sind daher Grenzen gesetzt. Eine absolut fehlerverzeihende Technik, bei der ein Fehler sicher erkannt und durch spätere (manuelle oder automatische) Massnahmen korrigiert werden kann, ist wegen der nur unzureichend modellierbaren Handlungsabläufe nicht möglich.

Aus den geschilderten Zusammenhängen ergibt sich, dass der Mensch ebenso wie die Technik als Sicherheitsfaktor wahrgenommen werden muss. Dabei lässt sich die Frage nicht einfach beantworten, ob der Mensch das grössere Risiko darstellt oder die Technik. Beim Umgang mit Risikotechnologien gilt jedoch, dass sie jederzeit durch den Menschen beherrschbar sein müssen. Insofern kommt dem Menschen eine weitreichende und herausragende Stellung im Sicherheitskonzept zu. Dem weitreichenden Einfluss des Menschen auf die Anlagensicherheit stehen erhebliche Unsicherheiten und Grenzen bei der Berücksichtigung des menschlichen Faktors bei der Sicherheitsbewertung von Anlage gegenüber.

Für eine sicherheitstechnische Gesamtbewertung muss davon ausgegangen werden, dass sowohl technische Systeme als auch Personalhandlungen fehlerhaft sein können. Die Ausfallraten technischer Funktionen können z.T. aufgrund bekannter Zusammenhänge zwischen dem vorliegenden Belastungskollektiv und einer Wirkung sowie aufgrund einer statistischen Auswertung zufällig auftretender Fehler ermittelt

werden. Die „Ausfallraten“ menschlicher Handlungen können dagegen nur mit sehr viel grösseren Unsicherheiten angegeben werden. Das Funktionieren des Menschen kann nicht mit einer Sicherheit wie der Ablauf in einem technischer System vorhergesagt werden. Die Kreativität des Menschen kann zudem neuartige Abläufe initiieren. Der Mensch kann sich ausserdem bewusst, u.U. auch in bester Absicht, über eingeübte Handlungsmuster hinwegsetzen. Die Anwendbarkeit statistischer Gesetzmässigkeiten ist daher fraglich. Ein grosser Anteil der Einflussgrössen auf menschliches Verhalten kann quantitativ nicht bewertet werden. Die verbreitetste Methode zur Sicherheitsbewertung unter Einbeziehung der menschlichen Zuverlässigkeit stellt die probabilistische Sicherheitsanalyse (PSA) im Rahmen der periodischen Sicherheitsüberprüfung von Kernkraftwerken dar. Das Ziel der PSA ist die Quantifizierung der Wahrscheinlichkeit schwerer Kernschäden bzw. in einem weiteren Schritt die Ermittlung des Anlagenrisikos unter Berücksichtigung des Ausmasses möglicher Freisetzungen. Um den Beitrag des Menschen in diese Sicherheitsbetrachtungen einzubinden, werden Modelle der menschlichen Handlung erstellt, für die eine Fehlerwahrscheinlichkeit ermittelt wird. In der internationalen Diskussion ist weitgehend unumstritten, dass die Methoden zur Quantifizierung der Wahrscheinlichkeit menschlicher Fehler erhebliche, nicht oder nur bedingt quantifizierbare Unsicherheiten sowie Grenzen bezüglich der erfassbaren Handlungsabläufe und äusseren Einflüsse aufweisen. Dennoch werden die Ergebnisse von PSAs als Mass für die Sicherheit der Anlagen in zunehmendem Umfang z.B. für aufsichtliche Entscheidungen herangezogen.

Die Angabe von Zahlenwerten, z.B. für die Wahrscheinlichkeit menschlicher Fehlhandlungen, ist nur mit solchen Unsicherheitsbereichen möglich, die die Aussagekraft des Ergebnisses erheblich einschränken. Dabei können sich die Unsicherheiten prinzipiell sowohl als Sicherheitsgewinn als auch als zusätzliches Sicherheitsrisiko erweisen. Eine sichere Vorhersage einer bestimmten Fehlhandlung zu einem bestimmten Zeitpunkt ist ebenso wenig möglich wie die Garantie eines fehlerfreien Ablaufs. Eine Zahlenangabe, z.B. für die Wahrscheinlichkeit menschlicher Fehlhandlungen, ist immer unvollständig, da die nicht quantifizierbaren Einflussgrössen darin nicht abgebildet werden können. Aus diesen Gründen ist eine Verknüpfung mit den aus den Ausfallraten technischer Funktionen abgeleiteten Grössen problematisch und liefert ein nicht zutreffendes Bild über das Sicherheitsniveau der Anlage insgesamt.

Aufgrund des weitreichenden Einflusses des Menschen auf die Anlagensicherheit ist die Berücksichtigung menschlicher Handlungen bei der Sicherheitsbewertung von Kernkraftwerken unerlässlich. Die derzeitige Beschränkung der menschlichen Zuverlässigkeitsanalyse auf geplante Handlungen, die alle Handlungen in nicht planbaren Situationen, nicht vorgeplante menschliche Handlungsweisen sowie die Einflüsse von Organisation und Management, d.h. die Sicherheitskultur der Anlage, unberücksichtigt lässt, führt zu Ergebnissen der probabilistischen Sicherheitsanalyse, die die Bedeutung des menschlichen Faktors in unangemessener Weise vernachlässigen.

13.12.2002

Quantitative Aussagen über die Wahrscheinlichkeiten schwerer Kernschäden bzw., das Risiko von Freisetzungen radioaktiver Stoffe sind daher zur Beschreibung der Sicherheit von Kernkraftwerken unter Berücksichtigung des Einflusses des „Faktors Mensch“ nicht geeignet und können zu Fehleinschätzungen führen.

Literatur

BfS 1996	Bundesamt für Strahlenschutz: Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Salzgitter, Dezember 1996
BfS 1998	Schott, H.; H.P. Berg; R. Görtz (Bundesamt für Strahlenschutz): Tendenzen zur Weiterentwicklung der Analyse von Personalhandlungen in der probabilistischen Sicherheitsanalyse von Kernkraftwerken, Salzgitter, Juni 1998
BMU 1996	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU): Leitfaden Probabilistische Sicherheitsanalyse, Dezember 1996 veröffentlicht in: Bekanntmachung der Leitfäden zur Durchführung von Periodischen Sicherheitsüberprüfungen (PSÜ) für Kernkraftwerke in der Bundesrepublik Deutschland, August 1997
GRS 2001	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH: Anforderungen an die Erstellung probabilistischer Sicherheitsanalysen der Stufe 2 im Hinblick auf die Vergleichbarkeit der Ergebnisse, Entwurf Stand Oktober 2001
HSK 1987	Hauptabteilung für die Sicherheit der Kernanlagen (HSK): HSK-Richtlinie R 101, Auslegungskriterien für Sicherheitssysteme von Kernkraftwerken mit Leichtwasser-Reaktoren, Mai 1987
HSK 1998	Frischknecht, A., Humbel, C., Prêtre, S.: Human Factor in den schweizerischen Kernkraftwerken, Juni 1998
HSK 2001	Hauptabteilung für die Sicherheit der Kernanlagen (HSK): HSK-Richtlinie R-48/d, Periodische Sicherheitsüberprüfung von Kernkraftwerken, November 2001
IAEA 1992	International Atomic Energy Agency: Procedures for conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, Wien, 1992
IAEA 2001	International Atomic Energy Agency: Nuclear Power Reactors in the World, Reference Data Serie No. 2, April 2001 Edition, ISBN 92-0-101301-9, Wien 2001
INSAG 4	International Atomic Energy Agency (International Nuclear Safety Advisory Group): "Safety Culture", 75-INSAG-4, Wien 1991
INSAG 10	International Atomic Energy Agency (International Nuclear Safety Advisory Group): "Defense in Depth in Nuclear Safety", INSAG-10, Wien, Juni 1996
INSAG 12	International Atomic Energy Agency (International Nuclear Safety Advisory Group): "Basic Safety Principles for Nuclear Power Plants", 75-INSAG-3 rev. 1, INSAG-12, Wien 1999
Öko-Institut 1991	Öko-Institut e.V.: Beurteilung der zur Erlangung einer endgültigen Betriebsbewilligung für das KKW Mühleberg öffentlich aufgelegten Unterlagen, Teil A, Beurteilung ausgewählter Themen des Sicherheitsberichts, Darmstadt, März 1991
Schmocker	Schmocker, U. und P. Meyer, HSK: Risikoorientierte Aufsicht über die Schweizer Kernanlagen, Teil I, Bericht über die Ergebnisse der Fallstudie Kernkraftwerke im Nationalfonds-Projekt „Risk Based Regulation“ (1997 – 1999)
Sträter 1997	Sträter, O.: Beurteilung der menschlichen Zuverlässigkeit auf der Basis von Betriebserfahrungen, Dissertation, Januar 1997
Swain 1983	Swain A.D.; H.E. Guttman: Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plan Applications, Albuquerque, 1983

13.12.2002

TÜV-N 1999	Balfanz, H.P.: Einflussfaktoren von Organisation und Anlagenmanagement auf die Anlagensicherheit und deren Berücksichtigung in der PSA, TÜV Nord e.V., Hamburg, April 1999
Winter 1989	Winter, G.: Der Mensch als technische Gefahr – Zur atomrechtlichen Bedeutung menschlichen Versagens; in: Kritische Justiz, 1989, Heft 1