

# Kommentare

## Gerd Winter Der Mensch als technische Gefahr

Zur atomrechtlichen Bedeutung menschlichen Versagens

*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 Stutzens 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.

Beispiele für menschliches Versagen wie diese, auch solche aus anderen Bereichen komplexer Technik mit hohem Schadenspotential, sind heute in aller Bewußtsein. Aber das Recht tut sich schwer, das Phänomen wahrzunehmen und Entscheidungen zuzuführen. In der Klage eines niederländischen Bürgers gegen die Genehmigung des KW Emsland, die von einer Bürgerinitiative unterstützt und von mir vertreten wird, soll dies versucht werden. Ich stelle im folgenden die Hauptargumente aus den klägerischen Schriftsätzen zusammen<sup>1</sup>.

<sup>1</sup> Schriftsätze genügen zwar nicht Ansprüchen wissenschaftlicher Objektivität, schon wegen der Einbindung in die Prozeßrolle. Ich würde die folgenden Ausführungen aber auch außerhalb dieser Rolle vertreten. Sie verdanken wesentliche Klärungen der Auseinandersetzung mit den Argumenten der gegnerischen Seite, insbesondere mit denen der beigeladenen KWU. Die Ausführungen zur Reaktortechnik und zu deren Interaktion mit dem Reaktorpersonal sind aber mit fachlicher Beratung zustandegewonnen, und zwar zum einen Teil durch Michael Sailer, Öko-Insitut Darmstadt, zum andern durch Theo Wehner, Fachbereich Psychologie, Universität Bremen. Auch Jan Holsheimer, Oldenzaal, Gerald Kirchner, Universität Bremen und Herbert Masslau, Lingen, haben Material und Ideen beigesteuert.

1. *Menschliches Fehlverhalten beim Betrieb der Anlage ist nicht praktisch auszuschließen.*

Ein KKW ist ein technisches System, das weitgehend automatisch betrieben wird. Dennoch spielt der Mensch eine Rolle. Er wirkt beim Betrieb mit, indem er anschaltet, abschaltet, die Leistung reguliert, testet, repariert etc. Auf der vorgelagerten Stufe betrachtet, löst sich das technische, automatisierte System sogar fast ganz in menschlichen Geist und menschliche Arbeit auf, weil der Mensch das KKW plant, herstellt und programmiert. Dennoch macht es heuristisch Sinn, Fehler des technischen Systems als vergegenständlichter geistiger und körperlicher Arbeit und Fehler der hinzutretenden Arbeit zu unterscheiden, und zwar bezogen auf jede einzelne der Stufen von der fertigen Anlage zurück bis zur Anlage in Reparatur, in Herstellung und in Planung. Menschliches Fehlverhalten auf einer früheren Stufe erscheint auf der späteren Stufe als technischer Fehler. Er wird nachweisbar als fehlerhaftes Arbeitsergebnis (z. B. als brüchige Schweißnaht). Zugleich wird aber die Sensibilität für Fehlerpotentiale geschärft, wenn man sich klarmacht, daß es sich um Arbeitsergebnisse (z. B. des unaufmerksamen Schweißers) handelt. Neben diesen heuristischen Gründen sprechen aber auch Gründe der Sache selbst für eine selbständige Konzipierung des technischen Systems: Komplexe Systeme scheinen gerade in ihrer Komplexität eine Eigenschaft zu besitzen, die mehr ist als die Summe ihrer Teile (und deren Herstellung). Zu dieser Eigenschaft gehört vermutlich die Generierung von Zufällen (konstruktiven und destruktiven), deren einzelne Erscheinungsform kaum vorhersehbar, deren Gesamtmenge aber ziemlich wahrscheinlich ist (was es problematisch macht, sie in den Bereich jenseits des menschlichen Erkenntnisvermögens zu verorten<sup>2</sup>). Die Gesamtmenge wird noch wahrscheinlicher oder gar »normal«, wenn der technisch bedingte Zufall mit menschlicher Spontaneität interagiert. Charles Perrow<sup>3</sup> hat dies mit vielen Beispielen belegt. Obwohl ich glaube, daß eine gute Risikobewertung auf der Metaebene des Gesamtsystems Maschine – Mensch ansetzen müßte, begnüge ich mich im folgenden mit dem m. E. notwendigen Zwischenschritt zu reklamieren, daß man den menschlichen Faktor zunächst genauso gründlich in sich und in der einzelnen Interaktion mit dem technischen System zu analysieren hat, wie dies bisher in zahllosen Verwaltungsverfahren und Prozessen mit dem technischen System geschehen ist.

Menschen *müssen* auf das technische System einwirken und können dabei fehlerhafte Unterlassungen (»errors of omission«) oder falsche Handlungen (»inaccurate performance«, »wrong timing«) ausführen; und sie *können* einwirken, obwohl sie es nicht müssen oder gar nicht dürfen, und können dabei Fehlhandlungen vornehmen (»errors of commission«)<sup>4</sup>.

Es gibt nun eine Reihe von »weichen« Faktoren, die den Menschen zu einer Stellgröße im Anlagenbetrieb machen, die manchmal überraschend hilfreich ist, manchmal (und nicht praktisch ausschließbar) aber auch überraschend dysfunktional.

Als *psychische Faktoren* sind zu nennen:

(1) Die Bildung *eines falschen mentalen Modells* von einem bestimmten Anlagenzustand. Bereits die technische Seite der Feststellung, Aufbereitung und Vermittlung von Informationen über den Anlagenstand ist fehleranfällig. Von Seiten des Menschen kommt die Neigung hinzu, aus einzelnen Informationen umfassende Wirk-

<sup>2</sup> Näheres unten zu Ziff. 2.

<sup>3</sup> Ch. Perrow, Normale Katastrophen, 1987.

<sup>4</sup> Vgl. J. Rasmussen, The Definition of Human Error and a Taxonomy for Technical System Design, in: ders./K. Duncan/J. Leplat (Hrsg.), New Technology and Human Error, 1987, S. 26.

lichkeitsbilder zu entwerfen, die dann so »überprüft« werden, daß weitere Informationen selektiv wahrgenommen oder gar erst passende Informationen erzeugt werden<sup>5</sup>.

Ein bekanntes Beispiel bietet der Unfallverlauf der TMI-Anlage. Nach der Hochdruckeinspeisung zeigte eine Meßanzeige unverändert fallenden Druck im Reaktor, eine andere dagegen steigenden Druck im Druckbehälter. Dies entsprach einerseits dem Kühlmittelverlust im Reaktor aufgrund des offenstehenden Überdruckventils, andererseits der beschleunigten Bildung von Dampfblasen infolge der zunehmenden Freilegung des Reaktorkerns. Für die Bedienungsmannschaft, die weder vom Kühlmittelverlust noch vom Offenstehen des Überdruckventils wußte, waren die Anzeigen widersprüchlich, weil beide eigentlich nur einen einheitlichen Druck anzeigen konnten. Eine Anzeige mußte falsch sein. Man »glaubte« der Druckhalteranzeige, weil ein Kühlmittelverlust zu unwahrscheinlich schien, und schaltete die Hochdruckkühlmitteleinspeisung ab, vermeintlich um das Kondensieren des Dampfes im Druckhalter zu vermeiden, tatsächlich aber den Kühlmittelverlust beschleunigend. Die Mannschaft fühlte sich in ihrem Modell des Anlagenzustands bestätigt, als der Druck im Druckbehälter tatsächlich fiel<sup>6</sup>.

Das Sicherheitskonzept hält als Mittel gegen solche Fehlinterpretationen Schulungsmaßnahmen bereit zum Zweck einer »Qualifizierung (nicht nur im technischen Sinn) des Betriebspersonals bis zu dem Grad, daß zu jedem Zeitpunkt ein erforderliches Eingreifen sachgemäß erfolgt«<sup>7</sup>. Schulung ist sicher wichtig, aber das falsche Konstruieren von Modellen aus Teilinformationen kann sie nicht praktisch ausschließen. Die zitierte Formulierung ist in ihrer Oberflächlichkeit eher Beweis für tatsächliche Unsicherheit.

(2) Die Einschränkung der Handlungsautonomie durch eine plötzliche Vielfalt von Anforderungen (*Stress*). Die Leistungsfähigkeit wird hier, wie man aus Prüfungssituationen weiß, gemindert. Das Personal neigt dazu, sich einem Meinungsführer unterzuordnen, nach Bestätigung seiner Vorstellung von der Situation zu suchen und riskante Entscheidungen zu treffen<sup>8</sup>.

Auch demgegenüber klingt es eher wie eine Beschwörung, wenn die Stellungnahme der Reaktorsicherheitskommission (RSK) v. 20. 6. 1979<sup>9</sup> in Ziff. 10.1 die »Befähigung des Personals unter medizinisch-psychologischen Gesichtspunkten empfiehlt« und andere Autoren meinen: »Der Stresssituation kann ein Schichtleiter durch Souveränität aufgrund seiner umfassenden Systemkenntnisse und seines flexiblen, operationalen Systemdenkens und seiner Erfahrung begegnen.«<sup>10</sup>

(3) Der menschliche Drang zur Überwindung von *monotonen Situationen*. Solche Situationen sind vermutlich die Regel während des Normalbetriebs. Zu den Reaktionen des menschlichen Organismus gehören auch Schlafen, Kartenspielen im Nebenraum, Drogen- und Alkoholkonsum – Verhaltensweisen, die nach Presseberichten über amerikanische KKW<sup>11</sup> durchaus vorkommen.

Auch im Zusammenhang mit deutschen KKW ist das Problem der »Schichtmüdigkeit« bekannt<sup>12</sup>.

Als Abhilfe werden die Stellung von Nebenaufgaben wie Diskutieren von besonde-

5 Vgl. J. Rasmussen, a. a. O. (»stereotype fixation«, »familiar short-cut«, »assumption«); D. Dörner, On the Difficulties People have in Dealing with Complexity, in: J. Rasmussen u. a., S. 103 ff.

6 Vgl. Ch. Perrow, Normale Katastrophen, 1987, S. 46–50, 121–123.

7 KTA Regel 3501 i. d. F. 6/85, BAnz Nr. 203a v. 29. 10. 1985. Der KTA (Kerntechnische Ausschuß) ist ein vom BuMin f. Umwelt, Naturschutz u. Reaktorsicherheit eingesetztes Sachverständigen-gremium, dessen Regelungen als VwVorschriften gelten.

8 S. dazu D. Dörner, a. a. O., S. 103 ff.

9 BAnz Nr. 16 v. 24. 1. 1980.

10 G. Mansfeld/A. Birkhofer, Grundsätzliche Bewertung der Anforderungsaspekte der Schichtleiteraufgaben im KKW, MS Garching v. 2. 11. 1981, S. 11.

11 Z. B. Nucleonics Week v. 2. 4. 1987; taz v. 27. 3. 1987.

12 S. Mansfeld/Birkhofer, a. a. O., S. 15.

ren Vorkommnissen, Erstellung von Störfallanalysen, Vorbereitung und Durchführung von Schulungsmaßnahmen und Aktualisierung von Instruktionen empfohlen und wohl auch angeboten<sup>13</sup>. Solche artifiziellen Beschäftigungstherapien können aber leicht als solche durchschaut und unterlaufen werden.

(4) Der Anspruch, es *besser machen* zu können als das Anlagendesign und die Betriebsregeln. Ein Beispiel bietet der Tschernobyl-Unfall. Die Operateure stellten ihr »process feel« über ihre Kenntnisse von Reaktorphysik, als sie das Experiment einleiteten. »Dabei vergaßen sie, die Gefährlichkeit des Tieres, das sie ritten«<sup>14</sup>.

Da dieser Anspruch in anderen Situationen durchaus funktional sein kann – im Falle Harrisburg z. B. löste sich das Personal nicht schnell genug von der Regel, daß ein Fluten des Druckhalters zu vermeiden ist, und schaltete die Hochdruckeinspeisung aus –, kann und sollte er nicht abkonditioniert werden. Daß er dann aber auch in falschen Situationen durchschlägt, kann nicht praktisch ausgeschlossen werden.

(5) Die Neigung, im Austausch mit komplexen Systemen dennoch *in linearen Sequenzen zu denken*. Menschen achten auf die Haupteffekte ihrer Handlungen auf ein bestimmtes Ziel, aber übersehen leicht Seiteneffekte auf das übrige System. Insbesondere werden exponentielle Entwicklungen allgemein wie auch bei solchen Seiteneffekten, unterschätzt<sup>15</sup>.

(6) Die Neigung, den *eigenen Aufwand* an Leistung zu reduzieren. Da Sicherheit zu erreichen ebenfalls eine zusätzliche Leistung ist, kann die genannte Neigung sicherheitsavers wirken. Andererseits ist der Fehler dann Indikator für einen dysfunktionalen Ablauf und macht deutlich, daß die jeweils korrekte Handlungsausführung mehr psychische Energie und Aufmerksamkeit erfordert als die fehlerhafte. Fehler sind insofern für die Fortentwicklung eines Systems funktional und insoweit »normal«<sup>16</sup>.

Die Liste der »weichen« psychischen Faktoren ließe sich verlängern. Insbesondere ist noch auf den Faktor *Angst* hinzuweisen. Störfallsituationen beschwören ja häufig auch die Gefahr radioaktiver Freisetzung im KKW selbst herauf. Nicht jede/jeder auf der Warte oder sonst in der Anlage leitend oder ausführend Tätige ist zu einem heroischen Opfer von Gesundheit oder Leben bereit. Viele werden Angst empfinden und manche dadurch ihre Entscheidungen – bis hin zur Flucht – beeinflussen lassen. Das gilt nicht nur bei der Bewältigung aktueller Notsituationen, sondern auch bei der Beseitigung oder Reinigung von radioaktiv verseuchten Anlageteilen.

Zu erwähnen sind weiterhin *gruppendynamische* Faktoren. Eine Spielform, nämlich das wechselseitige Vertrauen verschiedener, sich nicht genauer kennender Personen oder Gruppen wurde beim Tschernobyl-Unfall deutlich. Hier wirkten Operateure vor Ort und eine Moskauer Gruppe von den Versuch oktroyierenden Ingenieuren ohne Betriebserfahrung zusammen<sup>17</sup>.

Daß auch in der Bundesrepublik z. B. Spannungen zwischen Reaktorpersonal, staatlichen Kontrolleuren und Entwicklungsingenieuren auftreten können, die zum wechselseitigen Zuschieben von Verantwortung führen, ist nicht praktisch auszuschließen. Eine weitere Variante liegt darin, daß Spannungen aus nicht akzeptiertem Hierarchieverhältnis zwischen Schichtmeistern und den diesen neuerdings als Leiter vorgesetzten Schichtingenieuren entstehen.

13 A. a. O., S. 15 f.

14 J. Reason, The Tschernobyl Errors, in: Bulletin of the British Psychological Society 1987, S. 203.

15 Reason, a. a. O., S. 203; Doerner, a. a. O., S. 103 ff.; B. Brehmer, Development of Mental Models for Decision in Technological Systems, in: J. Rasmussen u. a., S. 111 ff.

16 Vgl. Th. Wehner, Über eine mögliche Umbewertung von Beinahe-Unfällen, Bremer Beiträge zur Psychologie Nr. 31, 1984.

17 Reason, a. a. O., S. 203.

Gruppendynamik wirkt sich auch so aus, daß menschlichem Fehlverhalten common mode-Qualität zuzusprechen ist. Es kann nicht unterstellt werden, daß zwei oder drei Reaktorfahrer unabhängig voneinander technisches Versagen wahrnehmen und darauf reagieren. So führt »die Nichtberücksichtigung von Koppelungen (zwischen mehreren Personen) bzw. die Annahme vollständiger personeller Redundanz in der Deutschen Risikostudie Kernkraftwerke dazu, daß für bestimmte Fehlhandlungen extrem niedrige Wahrscheinlichkeiten errechnet werden, selbst wenn die Wahrscheinlichkeit für eine Fehlhandlung eines einzelnen Reaktorfahrers relativ hoch ist. In einem extremen Fall (DRS Fachband 2 S. 241: Operatorhandlung L 580 OP RA 11/12: kein Einleiten des Abfahrens nach einem kleinen Leck am Druckhalter) wird für die Fehlhandlung eines einzelnen Reaktorfahrers eine Wahrscheinlichkeit von  $10^{-1}$  angenommen. Die unterstellte vollständige Redundanz in Form von 3 Reaktorfahrern führt zu einer Fehlerwahrscheinlichkeit von  $(10^{-1})^3 = 10^{-3}$ . Weiterhin wird für zwei Reaktorfahrer ein Fehlerentdeckungsfaktor von jeweils  $10^{-1}$  in Rechnung gestellt, so daß sich für die genannte Fehlhandlung insgesamt eine Wahrscheinlichkeit von  $10^{-3} \times (10^{-1})^2 = 10^{-5}$  ergibt«<sup>18</sup>.

Nicht zuletzt wirken auch *wirtschaftliche Faktoren* auf menschliches Fehlverhalten hin. Immerhin bedeutet jede Schnellabschaltung zum einen verstärkte Materialbelastung und damit Verkürzung der Lebensdauer wichtiger Komponenten, zum anderen Ausfall von Stromerzeugung und damit geringere Erlöse. Es ist praktisch nicht auszuschließen, daß diese Faktoren bei Entscheidungen z. B. über Schnellabschaltungen und deren Abschaltung mitspielen. Beispiele sind die Störfälle in den KKW Brunsbüttel und Biblis.

*2. Wie, in welchen einzelnen Erscheinungsformen es auftritt, ist bei menschlichem Fehlverhalten schwerer vorhersehbar als bei technischem Versagen; daß es auftritt, und zwar als Ganzes gesehen relativ häufig, ist dagegen leichter vorhersehbar.*

Mit der Formel, daß Unfälle »praktisch ausgeschlossen« sein müssen, hat das BVerfG einen sehr strengen Maßstab aufgerichtet. Quantifiziert man die Grenze, so ist von ungefähr 1 zu 1 Mio. pro Reaktorjahr auszugehen. Das ist jedenfalls der Wert, den Breuer in seinem einflußreichen Aufsatz von 1978<sup>19</sup> als quantitativen Anhaltspunkt für die primär »deterministisch« gemeinte Formel des »praktisch ausgeschlossenen« angeführt hat, und mit der Übernahme von Breuers Formel dürfte das BVerfG auch die quantifizierende Orientierung übernommen haben. Der Wert entspricht auch internationalen Gepflogenheiten. Z. B. heißt es in dem Policy Statement der amerikanischen Nuclear Regulatory Commission über »Safety Goals for the Operation of Nuclear Power Plants« v. 30. 7. 1986:

»In Übereinstimmung mit dem traditionellen Mehrstufen (defense-in-depth)-Ansatz und der Philosophie der Unfallfolgen-Begrenzung, die das zuverlässige Wirksamwerden von Containment-Systemen verlangt, sollte die Gesamt-Eintrittshäufigkeit für eine große Freisetzung von radioaktivem Material kleiner sein als 1:1 000 000 pro Reaktorjahr.«

Gemessen an diesem strengen Maßstab sind katastrophale Versagensverläufe mit maßgeblicher Einwirkung menschlichen Fehlverhaltens nicht praktisch ausgeschlossen. Zwar kann man die einzelne Erscheinungsform des fehlerhaften Eingriffs oder Unterlassens schwerer vorhersagen als die einzelne Erscheinungsform technischen Versagens, weil der Mensch sich spontaner verhält als die Technik.<sup>20</sup> Durch diese

<sup>18</sup> Öko-Institut, Risikountersuchung zu Leichtwasserreaktoren, 1983, Bd. 2, S. 302 f.

<sup>19</sup> Gefahrenabwehr und Risikoversorge im Atomrecht, DVBl. 1978, 829 (835 f. Sp.).

<sup>20</sup> Den ersten umfassenden Versuch einer Bestimmung und zugleich Quantifizierung der einzelnen Erscheinungsformen menschlichen Fehlverhaltens im KKW enthält die Studie von A. D. Swain und

Erschwernis wird menschliches Fehlverhalten aber nicht insgesamt zur Ungewißheit jenseits der Grenzen des menschlichen Erkenntnisvermögens, von der das BVerfG<sup>21</sup> annimmt, sie sei unentrinnbar und als sozial-adäquate Last hinzunehmen. Vielmehr läßt sich aus den oben aufgezählten Determinanten menschlichen Verhaltens und der Erfahrung, daß alle Schulung, Motivation und Administration diese Determinanten nur abmildern können, schlußfolgern, daß Fehlverhalten, insgesamt betrachtet, normal und keineswegs praktisch ausgeschlossen ist. Diese Erkenntnis ist ein *Wissen*, und zwar ein psychologisches, organisationssoziologisches und wirtschaftssoziologisches, das zwar nicht ein einzelnes Verhalten, wohl aber einen Komplex von Verhalten – eben das menschliche Versagen im Mensch-Maschine-System – vorauszusagen vermag.

Um es noch einmal in einem Beispiel zu verdeutlichen: Die Strafbarkeit von Diebstahl beruht auf der kriminologischen Erkenntnis, daß in einer Gesellschaft eine relativ hohe Wahrscheinlichkeit dafür besteht, daß Menschen stehlen (m. a. W. sich fehlverhalten). Man weiß dies von früheren Fällen, die sich statistisch auswerten lassen. Man könnte es aber auch ohne solche statistische Grundlage ableiten aus der Kenntnis der Determinanten menschlichen Verhaltens. Solche Determinanten sind nach der kriminologischen Theorie z. B. die sog. relative Deprivation (ökonomische Benachteiligung) des Täters, das »labelling« als auffällig und schließlich kriminell durch die Instanzen der sozialen Kontrolle in der kriminellen »Karriere« des Täters, Sozialisationsnachteile durch schwierige familiäre Verhältnisse, peer groups mit krimineller Tendenz etc. Die von der Gesellschaft im Gegenzug ergriffenen Maßnahmen, z. B. Sozialhilfe, Heime für auffällige Jugendliche, Bewährungshilfe, vermögen jene Determinanten kaum abzumildern (– wie das labelling zeigt, sind sie sogar teilweise kontraproduktiv –). Dieses Wissen erlaubt nicht vorherzusagen, *wer wo welchen* Gegenstand stehlen wird; es ist aber sicher genug um vorherzusagen, daß Diebstähle *in großer Zahl* vorkommen werden. Niemand käme nun auf die Idee, die Strafbarkeit des Diebstahls abzuschaffen, weil die einzelne Tat nicht vorhersehbar sei. So aber soll sich nach Auffassung der Gegenseite die atomrechtliche Genehmigungsbehörde verhalten: weil man das einzelne menschliche Fehlverhalten teilweise nicht vorhersagen kann, soll die Behörde das Phänomen als Ganzes vernachlässigen und – durch Genehmigung der Anlage – so tun, als spiele es keine Rolle.

Das Wissen darüber, daß man im einzelnen nichts weiß, ist durchaus etwas anderes als das »Wissen, nichts zu wissen«, das das BVerfG im Sinne hatte, als es von den Grenzen menschlichen Erkenntnisvermögens sprach, die unüberwindbar seien. Das BVerfG denkt dabei auf der erkenntnistheoretischen (sokratischen) Ebene des »ich weiß, daß ich nichts weiß«. Es zieht daraus nicht den Schluß philosophischer Askese, sondern gönnt der Gesellschaft Nutzen trotz ungewisser Technikrisiken, solange nicht neuer Verdacht oder neue Gewißheit auftaucht. Das hier vorgestellte Wissen ist dagegen kein erkenntnistheoretisches, sondern ein objektbezogenes (Erkenntnistheorie macht Metaaussagen über Objektaussagen. Eine Objektaussage

H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, hrsg. v. U.S. Nuclear Regulatory Commission, Washington 1983 (NUREG/CR – 1278 SAND80 – 0200 RX, AN). Die Studie zerlegt das menschliche Zutun im KKW in einzelne erforderliche Handlungen und quantifiziert deren Ausfall oder Fehlerhaftigkeit. Trotz enormer Detaillierung kann sie aber zugegebenermaßen 2 Schwächen nicht überwinden: Die Quantifizierung ist »gegriffen«, weil Vorerfahrungen fehlen, und die Vielfalt der nicht erforderlichen, dennoch aber vorgenommenen Eingriffe (z. B.: die Kerze bei Browns Ferry) ist schon qualitativ nicht vorhersehbar (a. a. O. S. 2–4; 2–17). Soweit es um menschliches Verhalten in Reaktion auf Störfälle geht, untersucht die Studie zudem nur »intern« bedingte Störfälle wie Kühlmittelverlust und Transienten, nicht auch extern bedingte wie Feuer, Erdbeben, Überschwemmung (a. a. O. S. 2–9).

21 BVerfGE 49, 89 (143).

ist z. B.: »Der Baum ist grün«. Eine erkenntnistheoretische Aussage ist z. B.: »Alles Wissen ist Konstruktion unseres Gehirns, auch die Beobachtung, daß der Baum grün ist«. Solches objektbezogene Wissen kann so detailliert sein, daß einzelne Erscheinungen vorhergesagt und u. U. verhindert werden können. Es kann aber auch so geartet sein, daß es nur das Auftreten von einer Klasse von Erscheinungen vorherzusagen und ihre gesamte Wahrscheinlichkeit abzuschätzen erlaubt. Das Wissen über menschliches Fehlverhalten gehört zu der zweiten Kategorie.

3. *Menschliches Fehlverhalten wird durch das technische System nicht so sicher verhindert oder in seinen Folgen aufgefangen, daß Unfälle praktisch ausgeschlossen sind.*

Das Sicherheitskonzept für KKW ist auf Störfallvermeidung und auf Störfallbeherrschung ausgelegt<sup>22</sup>. Das soll auch für Versagensabläufe gelten, an denen menschliches Fehlverhalten beteiligt ist.

Der *Vermeidung* von menschlich bedingten Störfällen dient z. B. ein verlässliches System der Information über den jeweiligen Anlagenzustand. Da der Anlagenzustand nicht unmittelbar beobachtbar ist, muß er abgebildet werden. Dies geschieht über mehrere Stufen, und zwar die Anreegebene (Meßwerterfassung mit Meßfühlern, Umformung in Anzeigen der Meßgeräte und in Spannungssignale für die nächste Ebene), die Logikebene (die Verarbeitung des Signals so, daß erkennbar ist, ob der Meßwert außerhalb des zulässigen Bereichs liegt; Umformung in Warn- und Anreagesignale) und die Steuerebene (Umwandlung von Anreagesignalen in Auslöser für Aktionen). Aus Zuverlässigkeitsgründen müssen die Systemkomponenten mehrfach redundant vorhanden sein. Dadurch entsteht aber die Möglichkeit widersprüchlicher Ergebnisse, die z. B. durch 2-von-3-Auswahlschaltungen (ein Signal wird produziert, wenn 2 von 3 Redundanzen das Gleiche anzeigen) vereinheitlicht werden. Außerdem muß durch weitere Bauteile dafür gesorgt werden, daß sich Fehler im System nicht auf alle Redundanzen ausbreiten können.

Dieser komplexe Aufbau des Informationssystems ist dem Reaktorpersonal selbstverständlich bekannt. Das schiere Wissen um die Vielfalt der technischen Verknüpfungen und damit auch möglichen Fehlverknüpfungen aber schürt das Mißtrauen in die Verlässlichkeit der produzierten Information. Jede Information steht, weil sie komplex produziert ist, unter dem Verdacht, fehlerhaft produziert worden zu sein – woraus dann falsche Schlüsse gezogen werden können. Der geschilderte Unfallverlauf von Harrisburg und auch der Störfall von Biblis sind hierfür Beispiele.

Dem *Beherrschen* von Störfällen dient vor allem das Reaktorschutzsystem mit der Reaktorschnellabschaltung und dem Notkühlssystem zur Nachwärmeabfuhr. Für 30 Minuten nach Störfalleintritt sind menschliche Eingriffe überflüssig. Die erforderlichen Reaktionen werden automatisch eingeleitet<sup>23</sup>. Aber menschliche Eingriffe bleiben auch in dieser Zeitspanne immerhin möglich. Sie sind durch das Betriebsbuch auch nicht verboten<sup>24</sup>. U. U. können sie sogar effektiver sein als die Automatik. Sie können die Automatik aber in riskanter Weise überbrücken, indem z. B. Auslösesignale für die Schnellabschaltung oder das Hochdrucknotkühlssystem auf Testbetrieb geschaltet werden. Ein Beispiel hierfür ist der Störfall im KKW Brunsbüttel. Hinzu kommt, daß die Automatik nur in den »Drehbuchstörfällen« (M. Sailer) richtig reagiert. Bei nicht vorhergesehenen Abläufen wie etwa Biblis 1988 kann wieder nur der Mensch helfen.

<sup>22</sup> Sicherheitskriterien für KKW v. 21. 10. 1977, BAnz Nr. 206 v. 3. 11. 1977, Ziff. 1.1.

<sup>23</sup> KTA Regel Ziff. 4. S. 3.

<sup>24</sup> Helf/Geyer/Müller, Grundsätze der Behandlung von Störfällen im Betriebsbuch von KKW-Druckwasserreaktoren, Kerntechnik 1987, S. 102.

Zudem sind menschliche Eingriffe in einem späteren Zeitpunkt keineswegs verzichtbar. Störfälle sind nach 30 Minuten noch nicht beherrscht. Vielmehr muß die Abführung der Nachwärme über längere Zeit gewährleistet sein. Andernfalls kann es auch noch Stunden nach Störfallbeginn zu einer Aufheizung des Kerns bis hin zur Kernschmelze kommen.

Das technische System des Reaktorschutzes, das menschliches Fehlverhalten (ebenso wie auch technisches Versagen) im Normalbetrieb auffangen soll, ist also seinerseits menschlichem Fehlverhalten ausgesetzt, sei es, indem Personal überflüssigerweise eingreift und dabei Fehler macht, sei es, indem Personal notwendige Eingriffe unterläßt oder fehlerhaft ausführt.

*4. Menschliche Eingriffe, die auf ein Vermeiden oder Auffangen von Störfällen hinwirken, sind nicht redundant.*

Redundant heißt in der Sicherheitstechnik eine zusätzliche Maßnahme, auf die es für die Gewährleistung der Integrität des technischen Systems nicht entscheidend ankommt. An den technischen Terminus wird teilweise die rechtliche Bewertung angeknüpft, daß redundante Maßnahmen der Restrisikominimierung dienen, nicht der Gefahrenabwehr und Risikovorsorge<sup>25</sup>. Könnten menschliche Eingriffe als redundant eingestuft werden, so wäre das bei solchen Eingriffen auftretende Fehlverhalten ein Umstand im Restrisikobereich, nicht ein Gefahrenmoment. Es wäre dem subjektiven Rechtsschutz Dritter nicht zugänglich.

Für das Auffangen von Störfällen ist oben bereits gezeigt worden, daß menschliche Eingriffe nicht redundant, sondern, z. B. für langfristige Wärmeabfuhr, konstitutiv sind.

Für das Vermeiden von Störfällen sind menschliche Eingriffe ebenfalls konstitutiv. Das liegt auf der Hand, soweit es Instandhaltungsarbeiten angeht. Fehlverhalten kann dabei z. B. darin bestehen, daß Ventile versehentlich nicht wieder geöffnet oder geschlossen werden. Beispiele bieten die Vorfälle in Harrisburg und Biblis.

Bestritten wird die konstitutive Rolle menschlicher Eingriffe an neuralgischer Stelle, nämlich hinsichtlich der Berstsicherheit des Reaktordruckbehälters (RDB). Der RDB gilt mit Abschluß seiner Herstellung einschließlich der produktionsabhängigen Prüfung als »basissicher«<sup>26</sup>. Fehler im technischen Ergebnis gelten angesichts des Werkstoffs, der Schweißqualität und der Prüfung als »praktisch ausgeschlossen«<sup>27</sup>. Zwar sind nach den RSK-Leitlinien im späteren Betrieb weitere Maßnahmen vorgesehen, nämlich begleitende zerstörende Prüfungen (Einhängeproben), wiederkehrende Druckprüfung und zerstörungsfreie wiederkehrende Prüfungen (Ultraschallprüfung), damit Risse entdeckt werden<sup>28</sup>. Diese Maßnahmen sind stark vom Faktor Mensch abhängig. Doch gelten sie als redundant. Menschliches Fehlverhalten rückt damit ins Restrisiko und ist unter Drittschutzaspekten rechtlich unbeachtlich.

Der VGH Mannheim, der diese Auffassung vertritt<sup>29</sup>, gerät allerdings in Widersprüche, wenn er an anderer Stelle meint, die Wiederholungsprüfungen seien für die Feststellung von Rissen doch unverzichtbar. Dieses Argument benötigt er, um Zweifel am Leck-vor-Bruch-Kriterium beiseite zu schieben: möge auch darauf, daß der RDB, bevor er bricht, zunächst unübersehbar leckt, kein Verlaß sein, jedenfalls

<sup>25</sup> VGH Mannheim, Urteil v. 30. 3. 1982 (Wuhl), Urteilsabdruck S. 183–214.

<sup>26</sup> VGH Mannheim, a. a. O., S. 206 f.; ebenso RSK-Leitlinien für Druckwasserreaktoren v. 14. 10. 1981, BAnz Nr. 69 v. 14. 4. 1982, Beilage Nr. 19/82, Ziff. 4.1.2.

<sup>27</sup> VGH Mannheim, a. a. O., S. 193.

<sup>28</sup> RSK-Leitlinien, a. a. O., Ziff. 4.1.4.

<sup>29</sup> A. a. O., S. 207 f.

weise er Risse auf, bevor er bricht oder leckt, und diese seien durch – dann ja wohl konstitutive – Wiederholungsprüfungen feststellbar.

Sollen die Prüfungen also zugleich redundant und konstitutiv für die Sicherheit sein? Diesen Widerspruch versucht der VGH mit einem Argument aufzulösen, das etwa in dem imaginären Punkt anzusiedeln ist, in dem die strange loops von Hofstädter oder Escher zusammentreffen. Der VGH sagt nämlich, daß Wiederholungsprüfungen, die sich als wirklich erforderlich weil positiv erwiesen, zeigten, daß »ein RDB mit Basissicherheit im Sinne des Sachverständigen nicht mehr vor(liege)«. Wenn der RDB aber nicht basissicher ist, dann kann die Prüfung auch nicht zur Basissicherheit gehören, sondern muß redundant sein.

Das Rätsel löst sich, wenn man zwei Argumentationsebenen auseinanderhält, die hier offensichtlich vermischt werden: das Bestimmen von Sicherheitserfordernissen und das Auswählen geeigneter Termini für diese Erfordernisse. Nennen wir die Erfordernisse einmal nicht »basissicher« bzw. »redundant«, sondern »BASAFE« bzw. »REDUND«. Es kann nun sein (und es ist so, anderes anzunehmen wäre Hybris), daß die reale Sicherheit Prüfungen unverzichtbar macht. Diese Prüfungen kann man ohne weiteres als »BASAFE« bzw. »REDUND« *bezeichnen*. Nur ändert ein solches Herausdefinieren nichts daran, daß die Prüfungen auf der Ebene der realen Sicherheit konstitutiv sind. Der Trick besteht darin, bei der Bezeichnung wie beim realen Gegenstand gleichermaßen von »basissicher« bzw. »redundant« zu sprechen. Dann kann man mit den Ebenen »Wechsel Dich« spielen und sagen, daß eine Maßnahme wie die Prüfung (definitiv) nicht zur Basissicherheit gehört und (real) doch ihr Bestandteil ist. Das ist die Logik des Autoverkäufers, der sagt: »Dieses ›Supersicher-Cabrio‹ kann, wie der Name schon sagt, gar nicht unsicher sein!«, und zwar (im abgewandelten Palmströmschluß) »weil nur sein kann, was auch »Sein« heißt«.

*5. Hinsichtlich des menschlichen Fehlverhaltens besteht sowohl auf der Stufe der Genehmigung wie auf der des Erlasses von technischen Verwaltungsvorschriften ein Ermittlungs- und Bewertungsdefizit.*

Nach der neueren Rechtsprechung des BVerwG sind Analyse und Bewertung des Risikos menschlichen Fehlverhaltens primär Sache der Exekutive und nicht der Gerichte.<sup>30</sup> Die Exekutive hat in Wahrnehmung ihres Beurteilungsspielraums und kraft Ermächtigung durch § 28 Abs. 3 StrlSchV in den Störfalleitlinien verbindlich festgelegt, daß Versagensverläufe jenseits der dort aufgezählten Störfälle zu vernachlässigen sind. Solche Versagensverläufe wären dann – so könnte man pointieren – *durch Legaldefinition* »praktisch ausgeschlossen«, so sehr sie *de facto* auch nicht praktisch ausschließbar sein mögen.

Unterstellt man die Richtigkeit dieses Ansatzes, so bleibt die Genehmigungsbehörde doch nicht gänzlich von gerichtlicher Kontrolle verschont. Vielmehr ist zu prüfen, ob sie

»die Datenbasis, auf deren Grundlage sie entschieden hat, als ausreichend, also den Anforderungen des § 7 Abs. 2 AtG entsprechend, ansehen durfte, und ob die damit verbundenen Bewertungen ihr als hinreichend vorsichtig erscheinen konnten«<sup>31</sup>.

Ist dies im Grundsatz zu bejahen, so kann die Behörde sich aber dennoch über einzelne Daten geirrt oder bei der Bewertung gegen allgemeine oder gesetzliche Wertungsprinzipien verstoßen haben. Es ist deshalb eine Beweisaufnahme veranlaßt,

<sup>30</sup> BVerwGE 72, 300 (316) – Wyhl –.

<sup>31</sup> BVerwG, DVBl. 1988, ISO – Brokdorf –.

»wenn sich aus dem prozessualen Vorbringen eines Verfahrensbeteiligten herleiten läßt, daß die der angefochtenen Genehmigung zugrundeliegenden Annahmen und Bewertungen der Genehmigungsbehörde im Hinblick auf den Stand von Wissenschaft und Technik als widerlegbar erscheinen«.

Man wird diese Regeln gerichtlicher Kontrolldichte nicht nur auf die Entscheidung der Genehmigungsbehörde über die konkrete Anlage, sondern, insoweit sich die Behörde auf Verwaltungsrichtlinien stützt, auch auf diese Richtlinien anzuwenden haben. Auch diesbezüglich ist zunächst nach Ermittlungs- und Wertungsdefiziten und, liegen sie nicht vor, nach gemäß dem Stand von Wissenschaft und Technik falschen Annahmen und Wertungen zu fragen<sup>32</sup>.

a) Soweit es die Risikoanalyse und -bewertung bei der Genehmigung angeht, ist festzustellen, daß die Behörde im vorliegenden, für die allgemeine Praxis exemplarischen Fall die Problematik menschlichen Fehlverhaltens fast gänzlich ausgeblendet und sich vollständig auf die technischen Komponenten konzentriert hat.

Personalfragen erscheinen in der Begründung zur (1. Teil-)Genehmigung nur als Fragen der Zuverlässigkeit und Fachkunde i. S. v. § 7 Abs. 2 Ziff. 1 und 2 AtG. Dabei wird verkannt, daß Fehler in der Interaktion von Mensch und nuklearem System gerade auch bei höchster Zuverlässigkeit und Fachkunde des Personals auftreten. Daß neben § 7 Abs. 2 Ziff. 1 und 2 auch § 7 Abs. 2 Ziff. 3 AtG Anforderungen an das Personal stellt – nämlich, daß Fehlverhalten praktisch ausgeschlossen sein muß –, wird überhaupt nicht gesehen. Es werden lediglich einige Konsequenzen aus dem Harrisburg-Störfall gezogen, z. B. die Verbesserung der Information des Betriebspersonals über die physikalischen Zustandsgrößen im Reaktorkern und Kühlsystem. Das sind Einzelheiten, aber keine systematische Analyse der möglichen fehlerhaften Eingriffe und Unterlassungen und auch keine Bewertung der Tatsache relativ großer Wahrscheinlichkeit von Fehlverhalten als Gesamterscheinung. Diese Analyse und Bewertung werden schließlich auch nicht eingelöst in einer vagen und floskelhaften Genehmigungsaufgabe, die lautet:

»Es ist sicherzustellen, daß das mit der Errichtung und dem Betrieb der Anlage befaßte Personal jederzeit in der Lage ist, die unter Voranstellung der Sicherheit richtigen Entscheidungen zu treffen und die erforderlichen Handlungen durchzuführen«.

Übertrüge man eine solche Auflage auf den Bereich technischen Versagens, so könnte ein ganzes KKW mit der einzigen Auflage genehmigt werden, daß Unfälle auszuschließen und Störfälle zu beherrschen sind. Einer solchen Entscheidung würde man wohl kaum bescheinigen, daß sie ohne Ermittlungs- und Bewertungsdefizit zustande gekommen ist. Das Gleiche muß für die Klausel hinsichtlich des menschlichen Versagens gelten.

b) Soweit sich die Genehmigungsbehörde auf *Verwaltungsvorschriften* gestützt hat, ist festzustellen, daß diese ihrerseits hinsichtlich menschlichen Fehlverhaltens ein Bewertungs- und Ermittlungsdefizit aufweisen. Die Vorschriften äußern sich einerseits zwar über die Interaktion von Mensch und Technik im KKW und weisen dem Personal weitreichende Handlungsmöglichkeiten und -notwendigkeiten zu. Dabei wird auch eine ganze Reihe von sensiblen Anlagezuständen der Entscheidung durch das Betriebspersonal überantwortet. Hierzu gehören insbesondere auch Eingriffe in das Reaktorschutzsystem, sei es im betrieblichen Anforderungsfall, sei es bei Funktionsprüfungen oder sei es bei Instandhaltungsarbeiten. Die Spielräume des Handelns oder Nichthandelns, die auch dem Fehlverhalten Raum geben, werden andererseits, wenn überhaupt, nur durch normative Verhaltenszielvorgaben, teils (– im Betriebshandbuch –) auch durch Handlungsanweisungen, gesichert. Die

<sup>32</sup> Vgl. BVerwG DVBl. 1988, 539.

psychologischen, soziologischen und ökonomischen Determinanten kommen nicht in den Blick, und es wird gar nicht erst versucht, auch sie zu bearbeiten.

Beispiele solcher riskanter Schaltstellen zwischen Mensch und Technik im KKW ergeben sich aus folgenden Zitaten:

»Das Reaktorschutzsystem *soll* Schutzaktionen automatisch auslösen. Handmaßnahmen wie Auslösen, Unterbrechen oder Rückstellen von Schutzaktionen sind nur *in begründeten Ausnahmefällen* vorzusehen. Das Sicherheitssystem ist so auszulegen, daß notwendige, von Hand auszulösende Schutzaktionen zur Beherrschung von Störfällen nicht vor Ablauf von 30 Minuten *erforderlich* werden.«<sup>33</sup>

Die Hervorhebungen (n. i. O.) weisen auf den Spielraum für menschliche Eingriffe hin. Ziel- oder Verhaltensanweisungen fehlen gänzlich. Auch widerspricht die Eröffnung dieses Spielraums dem Sicherheitskriterium 6.1. Satz 3, das postuliert:

»Von Hand gegebene Befehle *dürfen* notwendige Schutzaktionen *weder* beeinträchtigen *noch* verhindern können«.

Ein weiteres Beispiel für riskante Handlungsspielräume enthält Ziff. 4.8. (2) der KTA-Regel 3501, die lautet:

»Für den Betrieb der Reaktoranlage bei Instandhaltungsarbeiten im Betriebssystem, wie z. B. Instandsetzung einer Hauptkühlmittelpumpe, *kann* eine Anpassung des Reaktorschutzsystems erforderlich sein. Wird diese *von Hand* vorgesehen, so muß sie an fest vorgegebenen Eingriffsstellen durchgeführt werden können«.

Einen ähnlichen Spielraum eröffnet Ziff. 5.2.2.1 lit. e Abs. 3 u. 4 KTA-Regel 3301:

»Für die Berücksichtigung einer Funktionsprüfung in einem weiteren Strang *braucht* keine zusätzliche Redundanz vorgesehen zu werden, wenn die Funktionsbereitschaft des Stranges im Einsatzfall rechtzeitig wiederhergestellt werden kann.

Bei der Planung von Instandhaltungsmaßnahmen sind *grundsätzlich* die gleichen Anforderungen zu erfüllen. *Es darf* jedoch, unter Berücksichtigung des Zeitverhaltens der Reaktoranlage, auf die Erfüllung des Einzelfehlerkriteriums verzichtet werden, wenn bei einem zusätzlichen Ausfall die Systemfunktionen rechtzeitig wiederhergestellt oder die NWA (Nachwärmeabfuhr) auf andere Weise sichergestellt werden kann, wobei auch Hilfsmaßnahmen *zulässig* sind«.

Die zitierten Passagen (Hervorhebungen n. i. O.), die noch weiter ergänzt werden könnten, zeigen, daß riskante Handlungsspielräume eröffnet werden. Von Ziel- und Verhaltensvorgaben, die in den »wenn«-Sätzen enthalten sind, erhofft man sich, daß die Spielräume nicht zu Fehlverhalten führen.

Flankiert werden die vermeintlichen Sicherungen durch Anforderungen an die Fachkunde des Personals, die in mehreren Richtlinien geregelt sind. Auch diese Richtlinien gehen aber auf das Syndrom von psychologischen, soziologischen und ökonomischen Determinanten nicht ein. Dem Problem am nächsten ist noch Ziff. 4.14 KTA-Regel 3501, die eine Reihe von Gegenmaßnahmen gegen »Fehler durch Irrtümer und Fahrlässigkeit bei notwendigen Handeingriffen« nennt. Abgesehen davon, daß zu nicht notwendigen Handeingriffen bzw. notwendigen Unterlassungen nichts gesagt wird, setzt die KTA-Regel aber auch nur auf Schulung, Fachkunde, Schalttechnik und administrative Anweisungen, und dies im übrigen auf sehr allgemeine Weise, die längst nicht den Konkretisierungsgrad der technischen Regeln erreicht.

Nach allem dürfte deutlich sein, daß auch auf der Richtlinienebene ein Ermittlungsdefizit vorliegt. Die Richtlinien stehen, metaphorisch gesprochen, noch auf dem Erziehungsniveau des Kaiserreichs, als Kinder mit Anweisungen fremdbestimmt erzogen wurden, statt dadurch, daß man auf ihre Anlagen, Energien und Wünsche einging.

33 KTA-Regel 3501 Ziff. 4.5.3.

Auch die Risikostudien, die zur Stützung der Richtlinien durchgeführt worden sind, sind unter dem Gesichtspunkt menschlichen Fehlverhaltens völlig unzureichend. So kommen Hauptmanns u. a.<sup>34</sup> in ihrer umfassenden Untersuchung über Methoden der Risikoanalyse zu der Feststellung:

»Die Bewertung menschlichen Verhaltens in Zuverlässigkeitsuntersuchungen und in Risikostudien erfolgte bisher auf der Grundlage einer relativ groben Analyse der Aufgaben des Personals oder durch eine subjektive Einschätzung der Aufgabenstellung durch den Bewertenden.«

In der Tat hat die Deutsche Risikostudie (DRS), auf die sich die Risikoanalyse und -bewertung vieler technischer Verwaltungsvorschriften stützen, menschliches Fehlverhalten in seinen Erscheinungsformen nur völlig unzureichend und in seinen Determinanten überhaupt nicht untersucht<sup>35</sup>:

»Es werden praktisch nur geplante Eingriffe berücksichtigt, wie sie im Betriebshandbuch vorgesehen sind. Nicht geplante Eingriffe, die sich sowohl in negativer als auch in positiver Richtung auswirken können, werden nicht quantifiziert.«

Soweit die DRS menschliches Fehlverhalten berücksichtigt, gelangt sie nur zu einer »grobe(n) Ermittlung der entsprechenden Wahrscheinlichkeit« und operiert mit so pauschalen Alltagstheorien wie derjenigen, daß »die Wahrscheinlichkeit von menschlichem Fehlverhalten umso höher angesetzt (wird), je weniger Zeit seit Eintritt des auslösenden Ereignisses verstrichen ist« (a. a. O. S. 82). Die Implikationen dieses Satzes, nämlich, daß mit Zeitablauf menschliches Fehlverhalten unwahrscheinlicher wird, ist immerhin problematisch; denn Streß entsteht auch aus näher rückenden fatalen Ereignissen in der Zukunft wie etwa dem drohenden Bersten einer druckumschließenden Komponente bei sich fortsetzendem Druckaufbau.

c) Neben dem Ermittlungs- ist ein Bewertungsdefizit festzustellen, und zwar sowohl auf der Ebene der Genehmigungsentscheidung wie der der Richtlinien. Das Bewertungsdefizit besteht darin, daß nirgends – weder in der Begründung zur Genehmigung noch in den Richtlinien (der geeignete Platz wären die Sicherheitskriterien und die KTA-Regel 3501) – auch nur der Versuch gemacht wird,

- die Erscheinungsformen und Determinanten menschlichen Fehlverhaltens sinnvoll zu klassifizieren,
- ihre Eintrittswahrscheinlichkeit – sei es deterministisch oder probabilistisch – zu gewichten, und zwar nicht nur bezogen auf einzelne Erscheinungsformen, sondern insbesondere auf die Gesamtheit des im einzelnen nicht genau prognostizierbaren Phänomens,
- die Eintrittswahrscheinlichkeit so auszudrücken, daß der Abstand zur Schwelle des »praktisch ausgeschlossen« ( $10^{-6}$  pro Jahr) deutlich wird,
- eine das menschliche Fehlverhalten zentral verarbeitende Sicherheitsphilosophie zu entwickeln, die den Erscheinungsformen und Determinanten auf systematische und nicht nur wie bisher eklektizistische Weise Gegenstrategien gegenüberstellt, Lücken der Auffangmöglichkeiten identifiziert, Risikovergleiche anstellt und Restrisiken abwägt.

*6. Folgt man der Auffassung, daß ein Ermittlungs- und Bewertungsdefizit vorliegt, ist die Genehmigung schon deshalb aufzuheben.*

Das angerufene Gericht darf die Frage nicht selbst spruchreif machen, sondern muß die weitere Aufklärung und richtigere Bewertung der Genehmigungsbehörde überlassen<sup>36</sup>. Diese könnte sich bei den die Richtlinien verfassenden Instanzen rückversichern und ggf. auf eine Revision der Richtlinien drängen. Sie könnte aber die

<sup>34</sup> U. Hauptmanns/M. Hertztrich/W. Werner, Technische Risiken. Ermittlung und Beurteilung, 1987, S. 34.

<sup>35</sup> Deutsche Risikostudie Kernkraftwerke. Hauptband, 1979, S. 82.

<sup>36</sup> BVerwG DVBl. 1988, 1170 (1175) und DVBl. 1988, 149.

Sachlage auch selbst aufklären und bewerten. Denn nach § 28 Abs. 3 StrlSchV darf die Behörde sich auf die genormten Auslegungsstörfälle stützen; sie *muß* dies aber nicht, kann also autonom handeln.

7. *Folgt man jener Auffassung jedoch nicht*, nimmt man also an, die Genehmigungsbehörde und die die Richtlinien erlassenden Instanzen hätten das Phänomen menschlichen Fehlverhaltens hinreichend recherchiert und berücksichtigt, *so bleibt den klagenden Personen nur zu behaupten und zum Beweis zu stellen, daß die Behörde sich im Ergebnis geirrt hat, und Unfälle wegen der nicht geringen Wahrscheinlichkeit menschlichen Fehlverhaltens nicht praktisch auszuschließen sind.*

Erweist sich diese Behauptung als richtig, so stellt sich das Problem, daß dieses Ergebnis auch für die meisten anderen Reaktoren gilt, andererseits das Atomgesetz Kernspaltungsanlagen aber grundsätzlich zuläßt. Dieser Widerspruch kann auf zweierlei Weise aufgelöst werden:

8. Erste Alternative: *Das Atomgesetz läßt KKWe mit besonders hohem Schadenspotential nicht zu.*

Man könnte argumentieren: Der sehr strenge Maßstab des »praktisch ausgeschlossen« mit seiner quantitativen Konnotation von ca. 1 zu 1 Mio. pro Jahr folgt aus dem besonders hohen Schadenspotential u. a. auch der Baulinie '80. Die Relation »je höher der Schaden, desto geringer die Eintrittswahrscheinlichkeit« ermöglicht andererseits, Anlagen mit kleinerem Schadenspotential zuzulassen, auch wenn bei diesen das unvermeidbare menschliche Fehlverhalten oberhalb der Schwelle des *strengen* »praktisch ausgeschlossen« liegt. Schließlich ist weder aus dem Wortlaut noch aus der Entstehungsgeschichte des AtG zu entnehmen, daß das AtG jede beliebige Kernanlagengröße zuläßt. Das zeigt auch die Gegenprobe: Eine – unterstellt ebenso sichere – Anlage mit 20 000 statt zur Zeit 3000 MW elektrischer Leistung würde man auf der Grundlage des geltenden AtG wohl kaum genehmigen.

Der Nachteil einer solchen Argumentation besteht darin, daß sie zu einer Zulässigkeit der zur Zeit in Entwicklung befindlichen kleinen Kernspaltungsanlagen führen könnte. Doch steht bei diesen die rechtsdogmatische Aufgabe an, einen Grundsatz zu entwickeln, der die Aufteilung eines Großrisikos in eine Vielzahl von Kleinrisiken mit gleicher Gesamtsumme verbietet. Ein solcher Grundsatz hätte Parallelen im abwasserrechtlichen Verdünnungsverbot und in der immissionsrechtlichen Ablehnung der Hochschornsteinpolitik.

9. Zweite Alternative: *Nimmt man dagegen – m.E. wider die Entstehungsgeschichte – an, daß der Atomgesetzgeber in Kenntnis praktisch nicht auszuschließenden Fehlverhaltens Anlagen auch hohen Schadenspotentials hat zulassen wollen, so ist § 7 AtG verfassungswidrig.*

Denn Art. 2 Abs. 2 GG verbietet eine Gesundheitsgefährdung, also eine Beeinträchtigung oberhalb der Schwelle des »praktisch ausgeschlossen«, wenn das Grundrecht nicht explizit eingeschränkt wird.<sup>37</sup> Das Zitiergebot zwingt dazu, daß öffentlich bewußt wird, für welche Zwecke Gesundheit und Leben geopfert werden sollen.

Das Bundesverfassungsgericht hat zwar akzeptiert, daß nicht nur der Normalbetrieb, sondern auch Unfallrisiken emittierender Anlagen – als Grundrechtsgefährdung – verfassungswidrig sein können, aber die Unfallrisiken von KKWen verneint, daß die Opfergrenze überschritten sei.<sup>38</sup> Seine ganze Diktion zeigt jedoch, daß es dabei nur an technisches Versagen gedacht hat. Über den Faktor menschliches Versagen wird es sich noch äußern müssen.

<sup>37</sup> Art. 19 Abs. 1 S. 2 GG.

<sup>38</sup> Vgl. BVerfGE 49, 89 (141).