In Deutsches Atomforum e.V.: Berichtsheft der Jahrestagung Kerntechnik 2003. Berlin: INFORUM Verlags- und Verwaltungsgesellschaft. S 97-111

Sicherheitskritische Mensch-Maschine-Systeme: Rahmenbedingungen für sicherheitsgerichtetes Handeln

Michael Herczeg
Institut für Multimediale und Interaktive Systeme
Universität zu Lübeck

Kurzfassung

Sicherheitskritische Technologien sind inzwischen vielfältig mit unserem täglichen Leben verwoben. Komplexe Transportmittel, medizinische Systeme, Telekommunikationssysteme sowie verfahrens- und energietechnische Anlagen bestimmen unser tägliches Leben. Wir müssen davon ausgehen können, dass all diese Systeme mit den höchst möglichen Sicherheitsstandards betrieben werden und dass über die gesellschaftlich kommunizierten und akzeptierten Restrisiken hinaus keine weiteren Risiken eingegangen werden. Dies setzt voraus, dass die bei Herstellern und Betreibern, Zulieferern und Entsorgern, Zulassungsstellen, Aufsichtsbehörden beteiligten Personen, deren Organisationsstrukturen sowie die dort eingesetzten Technologien geeignete Randbedingungen erfüllen. Viele Störfälle und Unfälle zeigen, dass diese Erwartungen nicht immer erfüllt werden und in Form von sogenanntem menschlichen oder technischen Versagen die erwarteten Sicherheitsniveaus unterschritten und damit Restrisiken überschritten werden. Hierfür werden im Folgenden einige Problemfelder und Verbesserungsmöglichkeiten diskutiert, die insbesondere auch in der Kerntechnik besondere Relevanz aufweisen. Dabei sollen insbesondere Problemstellungen adressiert werden, die bei komplexen Mensch-Maschine-Systemen und damit zusammenhängenden Betriebskonzepten unabhängig von bestimmten Anwendungsbereichen grundsätzlich auftreten.

1. Risiken und Sicherheitskultur

Unser tägliches Leben wird zunehmend von der Verfügbarkeit und Funktionsfähigkeit technischer Systeme geprägt und abhängig. Wir erleben diese Systeme beispielsweise in Form von Fahrzeugen, Produktionsanlagen, Kraftwerken und medizintechnischen Geräten. Die meisten dieser komplexen Systeme müssen von Menschen überwacht und gesteuert werden. Aufgrund des hohen Sicherheitsbedarfs bei diesen Anwendungen sprechen wir auch von *sicherheitskritischen Mensch-Maschine-Systemen* [Herczeg 2000].

Dieser Bedeutung werden die Grundlagen und Methoden für die Analyse, die Entwicklung und den Betrieb dieser Systeme nur bedingt gerecht. Die besondere Schwierigkeit liegt in der Verknüpfung der in ihren Eigenschaften sehr unterschiedlichen Teilsysteme *Mensch* und *Maschine*, weiter gefasst *Mensch, Technik* und *Organisation*. Diese Problematik zeigt sich in

gelegentlichen Störfällen und Unfällen, deren Ursachen im Allgemeinen ähnlich unangemessen beschrieben werden, wie auch die Konzeption der Systeme unangemessen war.

Das Attribut *"sicherheitskritisch"* leitet sich aus dem Risiko des Versagens derartiger Systeme ab. Implizit findet sich im Risiko das Produkt aus der Wahrscheinlichkeit des Eintretens eines Ereignisses, hier insbesondere eines Störfalls oder Unfalls, und der Wirkung oder Tragweite des Ereignisses. Die Risiken, die aus Technologien resultieren, werden so weit wie möglich beziffert, typischerweise auf Grundlage der Berechnung *technischen Versagens* oder reziprok über die *Zuverlässigkeit* eines Systems.

In [Timpe 1976] wird menschliche Zuverlässigkeit definiert als *„die angemessene Erfüllung einer Arbeitsaufgabe über eine bestimmte Zeitdauer hinweg und unter zuverlässigen Bedingungen, die ebenfalls zeitveränderlich sein können“*. Eine ähnliche Definition findet sich bei [Bubb 1990]: *„Zuverlässigkeit (Reliability) ist die Wahrscheinlichkeit, dass ein Element eine definierte Qualität während eines vorgegebenen Zeitintervalls und unter vorgegebenen Bedingungen erbringt"*. Nach diesen ingenieurpsychologischen Definitionen ist die Zuverlässigkeit eine *Stabilitätsgröße* hinsichtlich des qualitativ definierten Erbringens von Leistungen über bestimmte Zeiträume unter bestimmten Randbedingungen.

Anders als technische Zuverlässigkeit wird somit die menschliche Zuverlässigkeit durch die Wahrscheinlichkeit beschrieben, eine Aufgabe unter vorgegebenen Bedingungen für ein gegebenes Zeitintervall im Akzeptanzbereich durchzuführen. Der grundsätzliche Unterschied zwischen der technischen und der menschlichen Zuverlässigkeit liegt im Unterschied zwischen der Ausführung einer *Funktion* (technisch) und der Ausführung einer *Aufgabe* (menschlich). Der Mensch arbeitet dabei typischerweise im Gegensatz zu einer Maschine zielorientiert und ist dabei in der Lage, trotz hoher Wahrscheinlichkeit fehlerhaften Ausführens einzelner Handlungsschritte, das Ziel dennoch mit hoher Wahrscheinlichkeit zu erreichen. Problematisch kann dabei in sogenannten sicherheitskritischen Anwendungen sein, dass es Handlungsfehler mit großer Wirkung und Tragweite (*fatale Fehler*) gibt, die nicht durch nachfolgende Handlungsregulationen korrigiert werden. Die hohe Wahrscheinlichkeit fehlerhafter einzelner menschlicher Handlungen kann dadurch die Sicherheit von Gesamtsystemen grundsätzlich in Frage stellen. Daraus entsteht oft der wenig hilfreiche Begriff *des menschlichen Versagens*, der im Hinblick auf die natürliche Eigenschaft menschlicher Handlungen fehlerbehaftet zu sein, eine nur scheinbar neue Form oder Qualität von Fehlern zu definieren scheint. Die menschliche Fehlerwahrscheinlichkeit (*Human Error Probability*, HEP) berechnet sich

$$HEP = n/N$$

wobei n die Zahl der Fehler, N die Zahl der Gelegenheiten ist. Die Zuverlässigkeit (*Reliabilität*, R) einer menschlichen Handlung ist das Komplement der Fehleranfälligkeit einer Handlung

$$R = 1 - HEP = 1 - n/N$$

Fehlerwahrscheinlichkeiten HEP wurden für Aufgaben in Kernkraftwerken mittels unterschiedlicher Methoden erhoben. Die wichtigsten Methoden dafür sind *Technique for Human Error Rate Prediction (THERP)* [Swain und Guttmann 1983] und *Operator Action Tree (OAT)* [Hall et al. 1982]. Die Erfassung von Fehlerwahrscheinlichkeiten kann für relevante Anwendungsfälle nur auf der Grundlage systematischer System- und Aufgabenanalysen erfolgen [Rasmussen 1985, Herczeg 1999, Herczeg 2001]. Die numerischen Fehlerwahrscheinlichkeiten für elementare Fehler im Kernkraftwerk wurden folgendermaßen erhoben [Swain und Guttmann 1983, Zimolong 1990]:

- Analoganzeige falsch ablesen: 0,003
- Graphen falsch ablesen: 0,01
- Störanzeige übersehen: 0,003
- Stellteil unter hohem Stress in die falsche Richtung bewegen: 0,5
- Ventil nicht schließen: 0,005
- Checkliste nicht benutzen: 0,01
- Checkliste nicht in der richtigen Reihenfolge abarbeiten: 0,5

Aus diesen Analysen für elementare Aufgaben lässt sich bereits ableiten, dass die menschliche Zuverlässigkeit im Betrieb von Kernkraftwerken gerade in sicherheitskritischen Situationen äußerst begrenzt ist und daher zwangsläufig durch geeignete organisatorische oder technische Maßnahmen flankiert werden muss. Grundsätzlich kann sogar festgestellt werden, dass völlig fehlerfreie Handlungen praktisch nicht auftreten und hohe Sicherheitsanforderungen (Zuverlässigkeit des Gesamtsystems) nur durch fehlertolerante Gestaltung von Mensch-Maschine-Systemen erreicht werden können. Fehlertolerante Mensch-Maschine-Systeme kompensieren auftretende menschliche oder technische Fehler durch geeignete technische oder organisatorische Schutz- oder Kompensationsmechanismen. Viele Fehlhandlungen werden nur deshalb sichtbar, weil sie in bestimmten, vor allem sicherheitskritischen Systemen nicht durch Ausgleichshandlungen korrigiert werden können, bevor sie sich auswirken. Sichtbare Abweichungen (Störfälle und Unfälle) sind oft nur *„missglückte Optimierungsversuche, mit nicht akzeptablen Folgen“* [Rasmussen 1982].

Bei sicherheitskritischen Systemen muss die Zuverlässigkeit auch über Arbeitsaufgaben (Normalbetrieb) hinaus auf Problemsituationen (anomaler Betrieb, Störfälle) erweitert werden (vgl. auch [KTA 2000]). Hierzu kann auch der Begriff der Aufgabe gegenüber der gängigen Definition auch auf den geeigneten Umgang mit unerwarteten Ereignissen erweitert werden. Während bei der Abarbeitung von Routineaufgaben, bei denen die Zuverlässigkeit vor allem aus der korrekten Bearbeitung der Aufgabe besteht, besteht sie bei unerwarteten Ereignissen und Situationen aus der unvoreingenommenen und systematischen Beobachtung, Identifikation und Bewertung der Ausgangssituation (Ist-Zustand) und der Wahl der Zielsituation (Soll-Zustand), die mit geeigneten, vor allem sicheren Handlungen erreicht werden muss [Rasmussen 1984].

In vielen Zuverlässigkeitsbetrachtungen sozio-technischer Systeme, insbesondere auch Mensch-Maschine-Systemen, wird auf die Berücksichtigung der menschlichen Zuverlässig-

keit verzichtet, da diese ungleich schwieriger als die technische Zuverlässigkeit (oft gemessen in *Mean Time Between Failures, MTBF*) zu erheben oder zu schätzen ist. Auf ihre Berücksichtigung zu verzichten, heißt jedoch außergewöhnlich hohe Fehlerwahrscheinlichkeiten im Gesamtsystem außer Acht zu lassen und dadurch uneinschätzbare Risiken zu übersehen. Die berechnete technische Zuverlässigkeit wird dabei unter bestimmten Umständen praktisch bedeutungslos.

Der Zuverlässigkeitsbegriff in der zivilen Nutzung der Kernkraft orientiert sich aus juristischer Sicht dabei an der Interpretation des Atomgesetzes (AtG) und dient nicht etwa der Verurteilung oder Ahndung meldepflichtiger Ereignisse, sondern vielmehr der *Vermeidung eines Gefährdungspotentials für die Zukunft*, in dem durch das Verhalten einzelner Personen oder ihrem Zusammenwirken in der Betreiberorganisation das Restrisiko erhöht wird. Dies folgt indirekt aus dem Atomgesetz (insb. §7 Abs. 2 Nr. 1 und 2 sowie §17 Abs. 3 Nr. 2 AtG). Damit verfolgt die Voraussetzung von Zuverlässigkeit des verantwortlichen Personals einen im öffentlichen Interesse liegenden *Schutzzweck* (§1 Nr. 2 und 3 AtG).

„Unzuverlässig“ im Sinne des Atomgesetzes ist, wer grundlegende Mängel oder Schwächen

- *bei den verantwortlichen Personen oder*
- *in der Organisation des Betriebs oder*
- *in der Aus- und Fortbildung des Betriebspersonals*

erkennen lässt und diese ein „erhöhtes Risiko“ bedeuten [Ipsen 1998]. Das erhöhte Risiko bezieht sich dabei auf das rechtlich und damit gesellschaftlich tolerierte Restrisiko, ohne dass dieses quantitativ oder qualitativ festgestellt wäre.

Aus der Erkenntnis, dass die Risiken nicht vollständig erfasst werden können und die Vermeidung von schadensträchtigen Ereignissen nicht durch Technologie alleine gesichert werden kann, muss in sicherheitskritischen Anwendungen ein besonderer Augenmerk auf das sozio-technische triadische System *Mensch-Technik-Organisation* gerichtet werden. Dies geschieht auch in der Kernkraft inzwischen mit dem Begriff der *Sicherheitskultur* bzw. des *Sicherheitsmanagements*, soweit es um die Entwicklung und Bewertung von Sicherheitskultur geht [RSK 2002].

Durch die IAEA wird Sicherheitskultur folgendermaßen definiert [IAEA 1991]: *„Sicherheitskultur ist die Gesamtheit von Merkmalen und Einstellungen bei Organisationen und Individuen, die durchsetzt, dass Sicherheitsfragen von Kernkraftwerken die ihrer Bedeutung als oberste Priorität entsprechende Aufmerksamkeit erhalten.“*

Außerdem wird darauf hingewiesen [IAEA 1998]: *„Sicherheitskultur ist ebenso die Vereinigung von Werten, Maßstäben, moralischen Prinzipien und Normen akzeptablen Verhaltens. Diese richten sich darauf, ein selbstdiszipliniertes Herangehen zur Steigerung der Sicherheit über rechtliche und aufsichtliche Anforderungen hinaus aufrecht zu erhalten. Deshalb muss Sicherheitskultur den Gedanken und Handlungen aller Individuen auf sämtlichen Ebenen der Organisation innewohnen.“*

Die Wahrnehmung, dass der Umgang mit dem Risiko sicherheitskritischer Mensch-Maschine-Systeme im sozio-technischen Begriff der Sicherheitskultur mündet, sollte nicht daran vorbei führen, dass die Randbedingungen für das Funktionieren und Wirken für die einzelnen Komponenten Mensch, Technik und Organisation verstanden und im Zusammenhang optimiert werden müssen.

2. Faktor Individuum

Der Mensch ist im Gesamtsystem Mensch-Technik-Organisation nicht nur der wichtigste Bezugspunkt sondern, wie bereits dargestellt, auch der am schwierigsten fassbare Faktor. Während sowohl Technologie als auch Organisation definierbare und im weitesten Sinne auch berechenbare Faktoren sind, stellt sich das Verhalten von Menschen als nur bedingt modellierbar und überprüfbar dar. Menschliche Handlungen im Bereich der Prozessführung lassen sich, wie mit vielen arbeits- und kognitionspsychologischen Modellen [Leontjew 1977, Rasmussen 1983, Norman 1986, Herczeg 1994] beschrieben, durch die Analyse und Beschreibung *mentaler Modelle* erfassen. Diese Modelle beschreiben die teils bewusste, teils unbewusste schrittweise Abbildung von Aufgabenstrukturen über Verfahrensweisen und einzelne Aktionen auf technische Modalitäten bis hin zu sensomotorischen Handlungen. Von den Operateuren sensorisch erfasste Signale werden zeichenartig wahrgenommen, reguliert und kognitiv bis zur Bewertung der Zielerreichung verarbeitet und dazu abstrahiert (siehe Abbildung 1).

Dem Prozessführungssystem (z.B. Leitwarte, Cockpit) kommt beim Handlungsprozess die wichtige Aufgabe zu, dem Operateur geeignete Interaktionsmöglichkeiten mit dem Prozess bereitzustellen. Voraussetzung für die Interaktion mit dem Prozess ist die hinsichtlich der Aufgaben und Problemstellungen angemessene Wahrnehmung des Prozesszustandes. In vielen Prozessführungsbereichen wird dies unter *Situational Awareness* zusammengefasst [Herczeg 2002]. Prozesswahrnehmung, ob als Wahrnehmung des Normalzustandes oder als Diagnose anomaler Zustände ist der Ausgangspunkt für durchgeführte aber auch bewusst unterlassene Handlungen. Aufgrund der wenig aggregierten teilautomatisierten Prozess-führung in Kernkraftwerken durch die aus technischen Zuverlässigkeitsgründen dominante *One-Sensor-One-Display-Methodik* bleibt die Diagnostik einer Problemsituation eine wesentliche Leistung der Operateure ohne besondere Unterstützung durch die Leitwarte. Hierauf sind zumindest teilweise eine Reihe von Störfällen (z.B. Three Mile Island, Brunsbüttel ME E 01/2002) und Unfällen (z.B. Tschernobyl) in der Kerntechnik zurück-zuführen. Verbesserungsmöglichkeiten sind neben technischen Verbesserungen in den Leitwarten vor allem in der verbesserten Qualifizierung des verantwortlichen Personals in der sicherheitsgerichteten Diagnostik und einer methodisch-technischen Unterstützung diagnos-tischer Prozesse zu sehen.

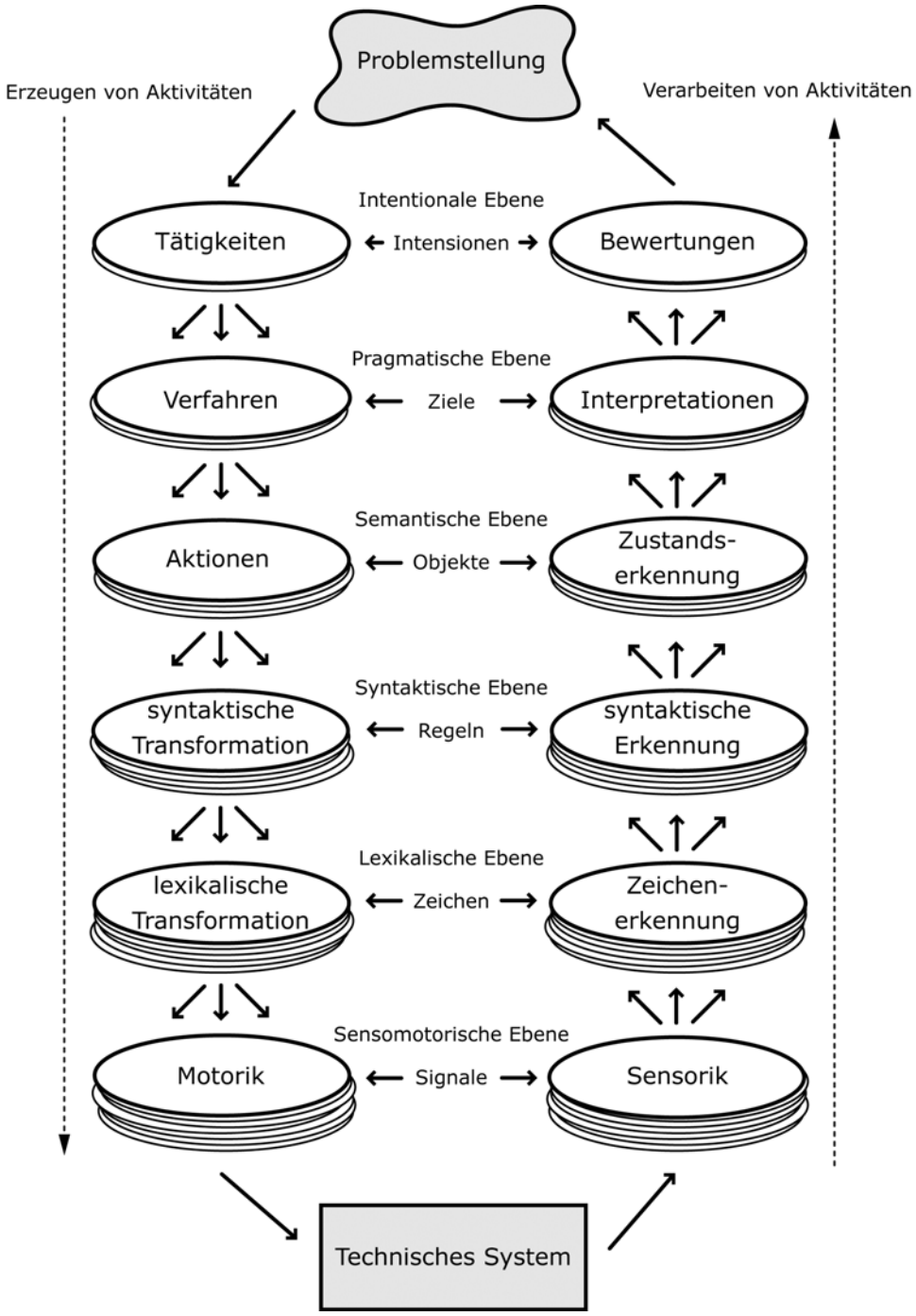

Abbildung 1: 6-Ebenen-Modell für Mensch-Technik-Interaktion

Die genannten Handlungsmodelle gehen von einer Normierung menschlichen Verhalten aus, wenn sie die richtige oder falsche Erkennung, Interpretation und Bewertung von Prozesssignalen auf der Grundlage von Wissen (*Knowledge*), Erfahrung (*Rules*) und Fertigkeiten (*Skills*) beschreiben [Rassmussen 1983]. Sie abstrahieren vor allem vom individuellen Verhalten der Operateure und dabei insbesondere von deren motivatorischem Zustand unabhängig von deren Qualifizierung. Die Motivation auf Grundlage persönlicher

Dispositionen und situativer Anreize zeigt ihre Bedeutung gerade im Bereich des sicherheitsgerichteten Handelns. Zu beobachten sind beispielsweise folgende Verhaltensweisen:

- Verfolgen des einfacheren oder bequemeren Modells
- frischere Erinnerungen/Beobachtungen werden bevorzugt verarbeitet
- bevorzugte Suche nach Beobachtungen, die das vorhandene Modell stützen, anstatt nach Beobachtungen zu suchen, die es widerlegen

Darüber hinaus wird die individuelle, teils auch die kollektive *Risikowahrnehmung* und bei der daraus folgenden Handlung auch die *Risikobereitschaft* in Entscheidungssituationen durch eine Reihe individual- und sozialpsychologischer Effekte beeinflusst, die weitgehend außerhalb der bekannten Handlungs- und Diagnostikmodelle liegen [Röbke et al. 1973] (siehe auch Abbildung 2):

- zu glauben, dass den durch riskante Handlungen entstehenden Gefährdungen noch rechtzeitig ausgewichen werden kann, reduzieren die Risikowahrnehmung
- erlebte Erfolge (Vorteile) ohne Unfall nach riskantem Verhalten erhalten oder erhöhen die Risikobereitschaft
- persönliche Nichtbetroffenheit bei beobachteten Unfällen führen nur temporär zu sicherheitsorientierten Verhaltensänderungen
- wenn das Unfallereignis selten eintritt, wird die Risikowahrnehmung reduziert

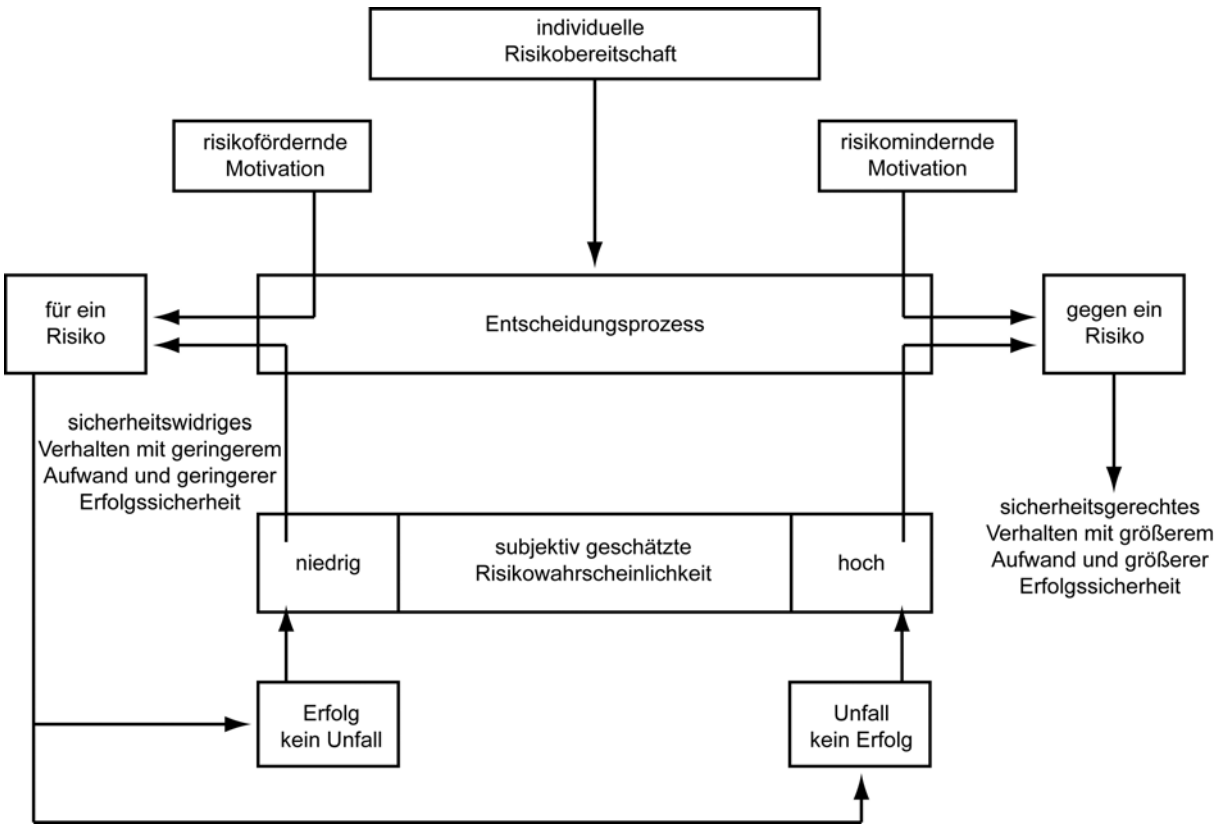

Abbildung 2: Einflüsse auf sicherheitswidriges Verhalten [Röbke et al. 1973]

Die für die Zuverlässigkeit besonders bedeutsame Form der Fehlhandlung, der Regelverstoß (*Violation*), ist häufige Ursache für Unfälle [Reason 1990, Reason 1991]. Folgende Einflussfaktoren werden in der Luftfahrt hinsichtlich der Betriebssicherheit als besonders wichtig eingestuft [VC HF]:

- für alle Beteiligten offenkundige Defizite in der Sicherheitskultur
- Konflikte zwischen Management und Arbeitsebene
- schlechte Moral
- unzulängliche Überwachung und Überprüfung
- stillschweigendes Hinwegsehen über Regelverstöße als Gruppennorm
- verzerrte Wahrnehmung von Risiken
- empfundene Nachlässigkeit und geringe Aufmerksamkeit des Managements
- geringer Schwung und Stolz in der Arbeit (mangelnde Berufsethik)
- "Macho-Kultur", die das Eingehen von Risiken unterstützt
- Gutgläubigkeit, dass keine negativen Folgen entstehen werden
- geringe Selbstachtung
- erlernte Hilflosigkeit
- empfundene Lizenz zum Regelverstoß
- widersprüchliche oder anscheinend bedeutungslose Regeln
- Alter und Geschlecht: jüngere Männer neigen eher zum Regelverstoß

Wenn auch diese Faktoren weniger untersucht sind als die Faktoren zur Entstehung anderer Fehlerformen, so sind sie doch in vielen Unfall- und Beinaheunfallsituationen als Begleiterscheinungen zu beobachten.

3. Faktor Organisation

Hinsichtlich sicherheitsgerichteten Handelns im Betrieb kommen der Organisation faktisch einerseits sicherheitsstärkende als auch sicherheitsschwächende Rollen zu. Die KTA-Basisregel 7 [KTA 2000] bezieht überorganisatorisch auch alle am Betrieb einer Anlage Beteiligte (Behörden, Gutachter, Hersteller, Lieferanten) neben dem Betriebspersonal mit ein.

Das Potenzial der betrieblichen Organisation sicherheitsgerichtetes Verhalten zu fördern, lässt sich weitgehend aus den oben genannten personenbezogenen Aspekten ableiten. Die Grundlage für sicherheitsgerichtetes Verhalten von Mitarbeitern im Betrieb bildet die persönliche Fachkompetenz, Betriebserfahrung sowie das berufsethische Commitment des Einzelnen. Die definierte Ausbildung, Auswahl und laufende Weiterbildung des verantwortlichen Personals im Hinblick auf die funktionale Beherrschung der Prozesse ist dabei der Ausgangspunkt, oftmals aber leider auch schon der Endpunkt organisatorischer Maßnahmen für das Betreiben sicherheitskritischer Systeme. Es fehlen meist Aus- und Weiterbildungselemente, die das Personal beispielsweise in systematischer Diagnostik, konservativen Entscheidungsfindung sowie sozialpsychologischen (gruppendynamischen) Effekten schulen und sensibilisieren. Aber schon die falsche Selektion des verantwortlichen Personals bei der

Rekrutierung führt dazu, dass es zu keiner Erhöhung der Sicherheit durch besonders risikobewusste Mitarbeiter kommt. *Assessment Centers*, die persönliche Dispositionen und Verhaltensweisen analysieren, wie sie beispielsweise in der Luftfahrt angewendet werden, fehlen weitgehend im Bereich der Kernkraftwerke, aber auch in den meisten anderen sicherheitskritischen Anwendungsfeldern.

In vielen beobachteten Störfällen und Unfällen sicherheitskritischer Systeme ist zu beobachten, dass es gerade sozialpsychologische Effekte sind, die zu Fehlverhalten im Betrieb führen. So führen Konsensdruck und falsch verstandene hierarchische Rollen zu Betreiberverhalten, das entgegen besseren Wissens Einzelner sicherheitsgefährdendes Verhalten einer Schicht oder eines Arbeitsstabes fördert oder erst möglich macht. Dies kann nur vermieden werden, wenn Entscheidungsprozesse während der diagnostischen Phase enthierarchisiert, systematisiert und objektiviert werden. Hilfreich können dabei instrumentierte Methoden sein, die die Faktenlage und die Folgerungen transparent machen und dokumentieren. Die Entscheidungen in Folge der Diagnostik müssen dann allerdings durch eindeutige und klare Zuständigkeiten und damit verbundene Verantwortungen an einzelne Personen gebunden werden. Unschärfen in der Zuordnung von Entscheidungskompetenzen und damit zusammenhängenden Verantwortungen verringern die Sicherheit, indem sie beispielsweise eher betrieblich bequeme oder ökonomische und damit weniger sicherheitsgerichtete Entscheidungen fördern. Ein besonders ausgeprägtes Beispiel dafür war das meldepflichtige Ereignis ME E 01/2002 des Kernkraftwerks Brunsbüttel, bei dem der Weiterbetrieb des Kraftwerks über fast 2 Monate trotz unklarer technischer Situation nach einem schweren Störfall erfolgte.

Anknüpfend an die oben dargestellten Beobachtungen für regelwidriges Verhalten im Betrieb ist festzustellen, dass insbesondere die *Toleranz* derartigen Verhaltens in der Organisation Auslöser für eine hohe Risikobereitschaft darstellt. So wurde von Gottschalk und Gürtler bei einer Untersuchung mit 2364 Arbeitsunfällen festgestellt, dass bei 84,4% der Unfälle *„betriebsübliche Verstöße gegen Unfallverhütungsregeln“* beteiligt waren [Gottschalk, Gürtler 1959]. Es sind somit auf Grundlage individueller Dispositionen vor allem organisationspsychologische und (betriebs-)kulturelle Phänomene, die die Bedeutung der Gruppe und des Führungspersonals für mangelndes sicherheitsgerichtetes Verhalten in den Vordergrund rücken. Die Toleranz oder gar Akzeptanz riskanten Verhaltens durch die Gruppe und insbesondere durch Vorgesetzte reduziert die individuelle Risikowahrnehmung und erhöht damit die Risikobereitschaft des Einzelnen und letztlich des ganzen Betriebs.

Eine Verfeinerung der Fehlerklassifikationen von Reason [Reason 1990] differenziert im besonders kritischen Bereich der bewussten Fehler zwischen Risiken (*Risks*) und Regelverstößen (*Violations*) und möchte so auf die vor allem organisatorisch bzw. sozial tolerierte Risikobereitschaft innerhalb einer Betreiberorganisation hinweisen (siehe Abbildung 3).

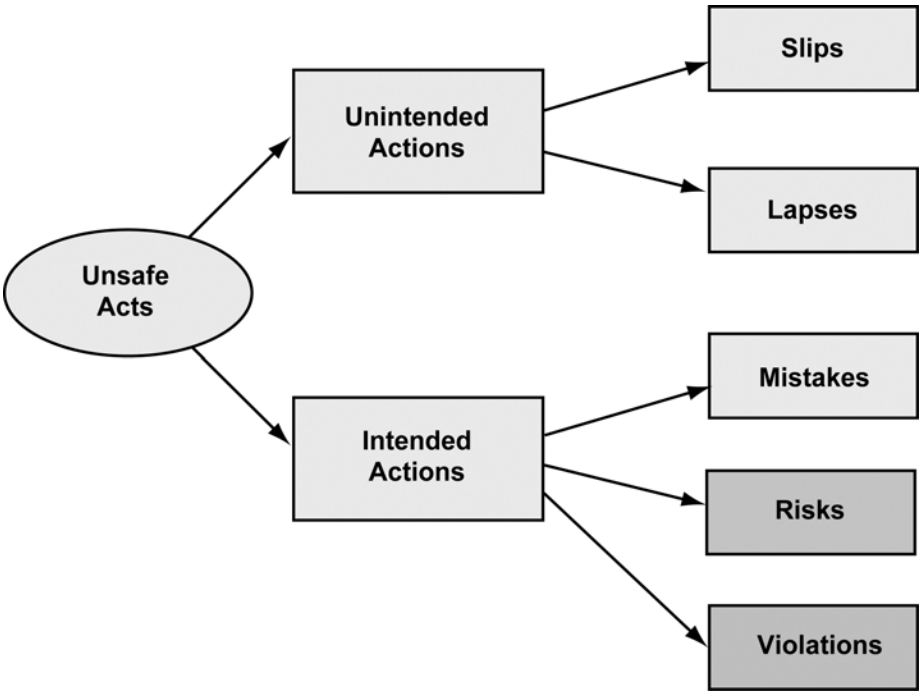

Abbildung 3: Fehlerklassen

4. Faktor Technik

Prozessführungssysteme, wie zum Beispiel Leitwarten von Kernkraftwerken, haben die Funktion komplexe physikalische Prozesse in einer Weise zu transformieren und zu präsentieren, so dass sie von menschlichen Operateuren wahrgenommen und verstanden werden können. Umgekehrt schaffen sie den Operateuren Einflussmöglichkeiten in die Steuerungs- und Regelungsprozesse.

Bei diesem bidirektionalen Transformationsvorgang zwischen Mensch und Prozess entstehen neben anderen Verzerrungen einerseits Vereinfachungen, die dazu führen, dass wichtige Prozesseigenschaften nicht oder falsch wahrgenommen werden und andererseits Artefakte, die keine Entsprechung in der Realität haben (siehe Abbildung 4). Beides führt zu Situationen, die die Sicherheit reduzieren und gefährden. Bei der Konzeption und Realisierung von Prozessführungssystemen ist deshalb darauf zu achten, dass solche Schwachstellen entweder vermieden, oder, wenn dies nicht möglich ist, den Operateuren im Rahmen ihrer Aus- und Weiterbildung bewusst gemacht werden. Die Konsequenz, die Operateure daraus zu ziehen haben ist, dass im Falle zweifelhafter Systemzustände vom schlechtesten Fall auszugehen ist (*Worst-Case-Annahmen*) und entsprechende Maßnahmen zu ergreifen sind, um den Systemzustand sicher zu analysieren. Dies kann beispielsweise letztendlich das Abschalten einer Anlage bedeuten, um genauere Analysen durchführen zu können.

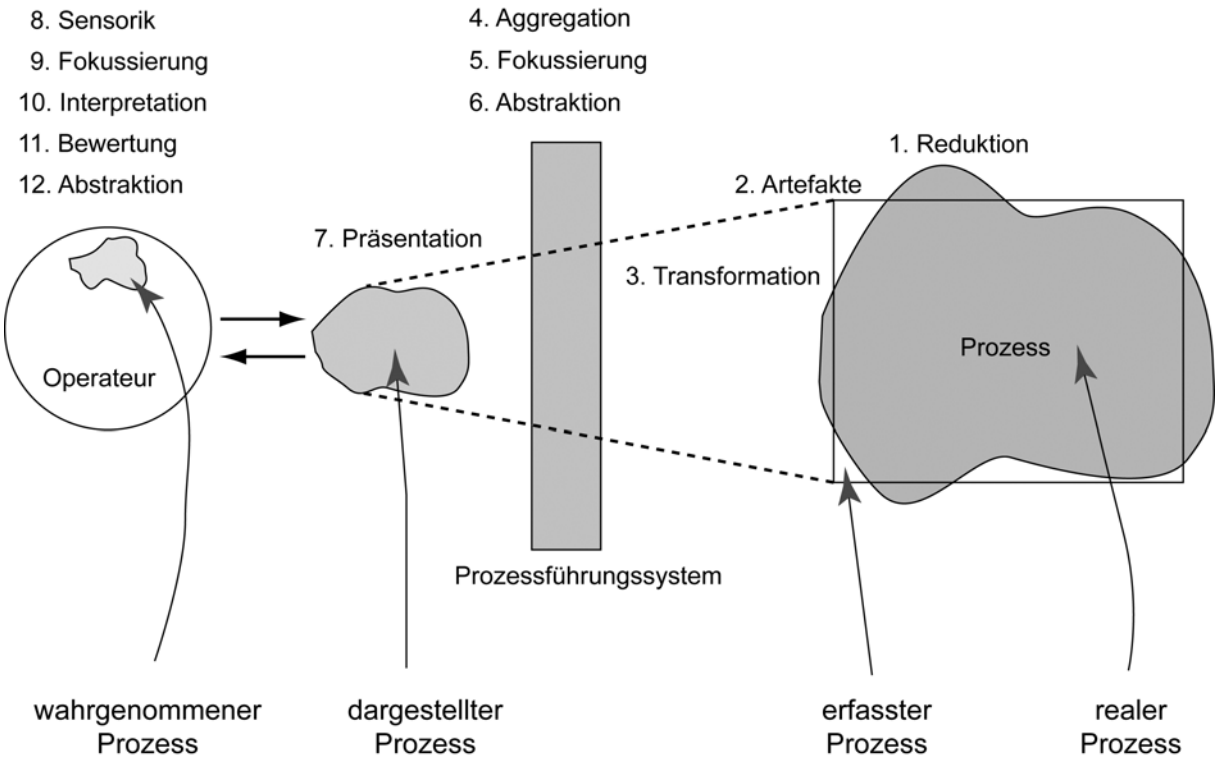

Abbildung 4: Verzerrungen in der Prozesswahrnehmung

Damit es zu möglichst wenig Abbildungsproblemen zwischen dem zu steuernden Prozess und den Operateuren kommt, ist es wichtig, die Transformation kohärent zu menschlichen Fertigkeiten und mentalen Modellen zu gestalten. Dies heißt sowohl menschliche sensomotorische Fertigkeiten zu berücksichtigen, als auch die kognitiven Modelle zu kennen und daraus abgeleitet geeignete Begrifflichkeiten und Konzepte zu verwenden. In der Kernkraft besteht durch den höchsten Sicherheitsanspruch das besondere Problem, dass durch Computertechnologie die kognitiv benötigten Abstraktionen und Visualisierungen zwar hergestellt werden können, gleichzeitig dadurch aber die Sicherheit des Gesamtsystems durch aufgrund ihrer Komplexität sehr fehleranfällige Computertechnologie geschwächt wird. Die vielfach praktizierte Einführung von computergesteuerten Monitoren zur meist graphischen Visualisierung von hoch aggregierten Systemzuständen und Trends unterstützt die verbesserte Wahrnehmung und Bewertung des Prozesses, reduziert aber gleichzeitig die Sicherheit durch technisch wesentlich fehleranfälligere Technologien gegenüber den sehr zuverlässigen weil einfachen *One-Sensor-One-Display-Bausteinen*. Die Operateure verlassen und konzentrieren sich auf die oft komfortablen und hilfreichen Visualisierungen und verkennen die Unzulänglichkeiten der zugrunde liegenden Technologie.

Eine weitere wichtige technische Option ist die ausgeprägte Mensch-Maschine-Arbeitsteilung durch *Automatisierungen* und *Teilautomatisierungen* in Prozessführungssystemen [Sheridan 1988]. Hierbei werden durch das System Funktionen realisiert, die dem Menschen Aufgaben

und auch Entscheidungen abnehmen. Dies gilt vor allem für zeitkritische Regelungsaufgaben oder für genau definierbare Routineaktivitäten. Darüber hinaus besteht die Möglichkeit durch Systemfunktionen menschliche Aktivitäten zu kontrollieren und daraufhin zu überprüfen, ob geeignete Systemzustände vor Ausführen der Aktionen vorliegen und ob die Aktionen voraussichtlich wieder in sichere Zustände führen werden. Im Zweifelsfall verhindern *Interlocks* oder andere Schutzfunktionen kritische Handlungen. Bei der Realisierung von Unterstützungs- und Schutzfunktionen zeigt eine Vielzahl von Ereignissen, dass eine möglichst aufgaben- und zielorientierte Modellierung der Zustände und Funktionen die Voraussetzung für eine wirkungsvolle und sichere Mensch-Maschine-Arbeitsteilung und gegenseitige Kontrolle von Mensch und Maschine darstellt [Herczeg 2002]. Dies ist allerdings bislang in der Praxis allenfalls ansatzweise realisiert.

5. Zusammenfassung

Sicherheitsgerichtetes bzw. sicherheitsgefährdendes Verhalten beim Betrieb eines sicherheitskritischen Systems entsteht aus dem komplexen Zusammenspiel vieler menschlicher, technischer und organisatorischer Faktoren. Diese Faktoren können einzeln untersucht, geprägt und optimiert werden. Dabei kommt dem Zusammenspiel von Mensch, Technik und Organisation besondere Bedeutung zu. Viele Probleme resultieren aus den sehr unterschiedlichen Eigenschaften und Fähigkeiten von Mensch und Maschine, eingebettet in eine meist starre organisatorische Struktur. Der deshalb notwendige, aber nur teilweise verstandene organisatorische Schutzschirm gegen das Versagen des Gesamtsystems ist ein sozio-technisches Phänomen, das oft auch als *Sicherheitskultur* bezeichnet wird. Dabei kann auf Grund von Erfahrungen aus Anwendungsbereichen, die wie zum Beispiel die Luftfahrt seit Jahren hohe Sicherheitsstandards realisieren, geschlossen werden, dass nur langfristig ausgerichtete und ganzheitliche Ansätze erfolgreich sein können, die Mensch, Technik und Organisation in Kohärenz bringen.

Bei der Entwicklung und Einführung von Sicherheitsmanagement-Systemen, wie derzeit im Bereich der Kernkraft, muss vermieden werden, an den oben genannten Erfahrungen vorbei nur weitere formalistische Organisationselemente zu schaffen, die aus denselben Gründen wie die bereits bestehenden Sicherheitsvorschriften oder Sicherheitsmechanismen wenig wirksam sind oder sogar vorsätzlich unterlaufen werden. Sicherheitskultur entsteht nur durch in den beteiligten Individuen verankerte Verhaltensweisen, die den realen Menschen und die reale, d.h. auch die informelle Organisation berücksichtigen. Technische Systeme können neben den üblichen Prozessführungs- und Schutzfunktionen helfen, durch die Unterstützung einer verbesserten Situational Awareness auch die Risikowahrnehmung zu objektivieren und damit die Risikobereitschaft auf das gesellschaftlich akzeptierte Maß zu begrenzen.

Indikatorenbasierte Sicherheitsmanagement-Systeme [IAEA 2000] werden möglicherweise erlauben, bestimmte vorhandene Sicherheitsdefizite in einer Betriebsorganisation zu erkennen. Es sind in den entsprechenden Konzepten bislang allerdings kaum Mechanismen zu

finden, die die oben genannten individuellen und sozialen risikofördernden Dispositionen und Verhaltensweisen wirksam und nachhaltig zu ändern in der Lage wären. Die Methoden sind stattdessen vor allem an bekannte Prozessmodelle und Qualitätssicherungsverfahren angelehnt. Sie postulieren bislang einfach, dass bei erkannten Defiziten auch geeignete Regulierungsmaßnahmen verfügbar seien, die in zeitlich akzeptablem Rahmen die notwendigen Veränderungen herbeiführen können. Es könnte somit leicht passieren, dass ein großes und aufwändiges organisatorisches Instrumentarium entsteht, das bekannte Probleme identifiziert aber nicht löst. Wünschenswert wären Prozessmodelle, die sich stärker auf die Maßnahmen konzentrieren.

Literatur

[Bubb 1990] H. Bubb: *Bewertung und Vorhersage der Systemzuverlässigkeit.* Ingenieurpsychologie, Enzyklopädie der Psychologie, Band 2, Verlag für Psychologie, Hogrefe, Göttingen,1990, pp. 285-312.

[Gottschalk, Gürtler 1959] F. Gottschalk, H. Gürtler: *Handbuch der Unfallverhütung.* Stuttgart-Düsseldorf. 1959.

[Hall et al 1982] R.E. Hall, J. Fragola, J. Wreathall: *Post-Event Human Decision Errors: Operator Action Tree/Time Reliability Correlatio*n. Brookhaven National Laboratory, NUREG/CR-3010, US Nuclear Regulatory Commission, Washington D.C.,1982.

[Herczeg 1999] M. Herczeg: *A Task Analysis Framework for Management Systems and Decision Support System*s, Proceedings of the AoM/IAoM 17th International Conference on Computer Science, San Diego, California, August 6-8, 1999, Journal of Computer Science and Information Management (CSIM), The International Association of Management (IAoM) and Maximilian Press Publisher, 1999.

[Herczeg 2000] M. Herczeg: *Sicherheitskritische Mensch-Maschine-Systeme*. FOCUS MUL, No. 1, 2000.

[Herczeg 2001] M. Herczeg: *A Task Analysis and Design Framework for Management Systems and Decision Support System*s. International Journal of Computer & Information Science, The International Association for Computer & Information Science (ACIS), Vol. 2, No. 3, September 2001.

[IAEA 1991] IAEA INSAG 4: *Safety Culture.* Safety Series No. 75, International Nuclear Safety Advisory Group, IAEA, 1991.

[IAEA 1998] IAEA: *Developing Safety Culture in Nuclear Activities - Practical Suggestions to assist Progress.* Safety Report Series No. 11, IAEA, 1998.

[IAEA 2000] IAEA: *Operational Safety Performance Indicators for Nuclear Power Plants.* IAEA-TECDOC-1141, IAEA, May 2000.

[Herczeg 2002] M. Herczeg: *Intention-Based Supervisory Control*. In: Berichte des FA 5.4 Anthropotechnik der Deutschen Gesellschaft für Luft und Raumfahrt e.V. (DGLR), 2002.

[Ipsen 1998] K. Ipsen: *Die „Zuverlässigkeit" im Sinne des Atomgesetze*s. Energiewirtschaftliche Tagesfragen. 48. Jg., Heft 11, 1998.

[KTA 2000] *KTA 2000 - KTA-Sicherheitsgrundlagen.* Kerntechnischer Ausschuss. Bundesamt für Strahlenschutz. 2001.

[Leontjew 1977] A.N. Leontjew*: Tätigkeit, Bewusstsein, Persönlichkeit.* Klett Verlag, 1977.

[Norman 1986] D.A. Norman. *Cognitive Engineering*. In Norman, D.A., Draper S.W. (Hrsg.). *User Centered System Design*. Lawrence Earlbaum Associates, 1986.

[Rasmussen 1982] J. Rasmussen: *Human Errors. A Taxonomy for describing Human Malfunction in Industrial Installation*s. Journal of Occupational Accidents, 4, 1982, pp. 311-333.

[Rasmussen 1983] J. Rasmussen: *Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models*, IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-13, No. 3, May/June 1983.

[Rasmussen 1984] J. Rasmussen: *Strategies for State Identification and Diagnosis in Supervisory Control Tasks, and Design of Computer-Based Support Systems.* in Advances in Man-Machine Systems Research, Vol. 1, 1984, pp 139-193.

[Rasmussen 1985] J. Rasmussen: *Human Error Data - Facts or Fiction.* Report M-2499, Risø National Laboratory, 1985.

[Reason 1990] J. Reason: *Human Error*. Cambridge University Press, 1990.

[Reason 1991] J. Reason: *Identifying the Latent Causes of Aircraft Accidents Before and After the Event.* 22nd Annual Seminar, The International Society of Air Safety In-vestigators, Canberra, 1991.

[Röbke et al. 1973] R. Röbke, B. Schulte, K. Thimm: *Verhaltensvariabilität des Menschen als Unfallursache.* Bundesanstalt für Arbeitsschutz und Unfallforschung Dortmund. Wirtschaftsverlag NW. 1973.

[RSK 2002] Reaktor-Sicherheitskommission: *Memorandum der RSK zur Gewährleistung einer angemessenen Sicherheitskultu*r. Anlage 2 zum Ergebnisprotokoll der 352. Sitzung der Reaktor-Sicherheitskommission am 13.6.2002.

[Sheridan 1988] T.B. Sheridan: *Task Allocation and Supervisory Control*, In: M. Helander (Ed.): *Handbook of Human-Computer Interaction*, Elsevier Science Publishers B.V. (North Holland), Amsterdam, 1988, pp. 159-173.

[Swain, Guttmann 1983]: A.D. Swain, H.E. Guttmann: *Handbook of human reliability analysis with emphasis on nuclear power plant operation*s. Sandia National Labs, US Nuclear Regulatory Commission, Washington D.C., 1983.

[Timpe 1976] K.P. Timpe: *Zuverlässigkeit in der menschlichen Arbeitstätigkei*t., Zeitschrift für Psychologie, 1, 1976, pp. 37-50.

[VC HF] R. Wiedemann et al.: *VC Human Factor Konzept.* Hrsg. Vereinigung Cockpit e.V., ohne Jahresangabe, laufende Aktualisierung.

[Zimolong 1990] B. Zimolong: *Fehler und Zuverlässigkeit.* in Ingenieurpsychologie, Enzyklopädie der Psychologie, Band 2, Verlag für Psychologie, Hogrefe, Göttingen, 1990, pp. 313-345.