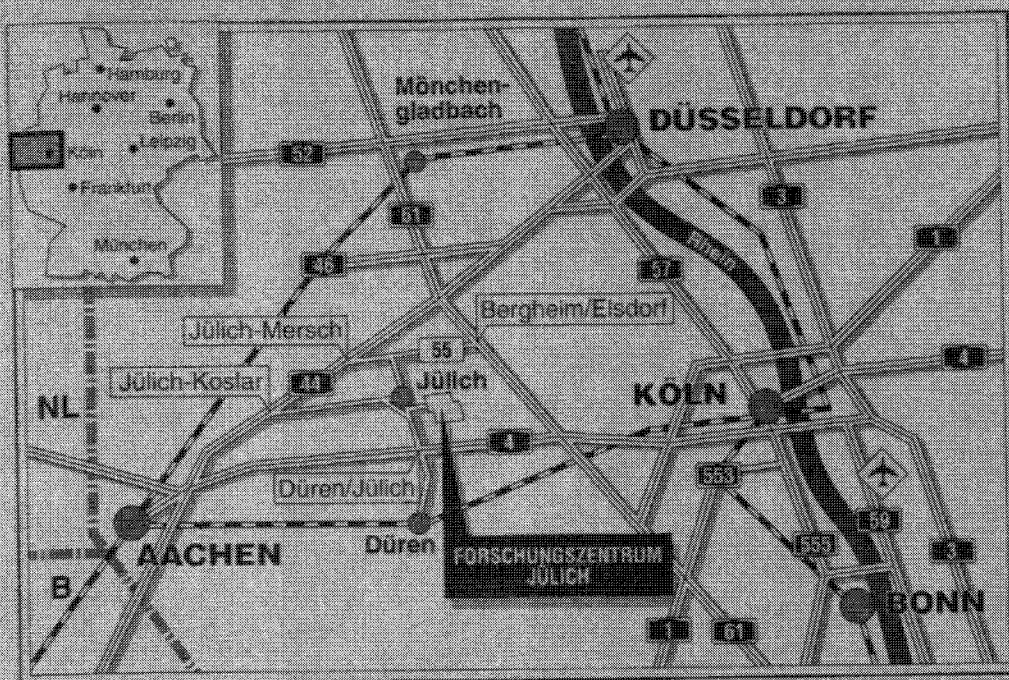


*Institut für Sicherheitsforschung
und Reaktortechnik*

**Entscheidungsfehler des Betriebspersonals
von Kernkraftwerken als Objekt
probabilistischer Risikoanalysen**

**Methodische Erweiterungen auf der Basis einer differenzierten
Betrachtungsweise sicherheitsgerichteter Ziele**

Bernhard Reer



Berichte des Forschungszentrums Jülich ; 2811

ISSN 0944-2952

Institut für Sicherheitsforschung und Reaktortechnik Jüli-2811

D 468 (Diss. BUGH Wuppertal)

Zu beziehen durch: Forschungszentrum Jülich GmbH · Zentralbibliothek

D-52425 Jülich · Bundesrepublik Deutschland

Telefon: 02461/61-6102 · Telefax: 02461/61-6103 · Telex: 833556-70 kfa d

Entscheidungsfehler des Betriebspersonals von Kernkraftwerken als Objekt probabilistischer Risikoanalysen

**Methodische Erweiterungen auf der Basis einer differenzierten
Betrachtungsweise sicherheitsgerichteter Ziele**

Bernhard Reer

Das diesem Bericht zugrundeliegende Forschungsvorhaben wurde mit Mitteln des Bundesministers für Forschung und Technologie (Förderkennzeichen 03THA202) gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Nuclear Power Plant Personnel Errors in Decision-Making as an Object of Probabilistic Risk Assessment

by Bernhard Reer

A B S T R A C T

The integration of human error - also called man-machine system analysis (MMSA) - is an essential part of probabilistic risk assessment (PRA). The current research in this field emphasizes intentional errors in decision-making: the operator thinks the intended wrong action to be correct. Such errors will result in extraneous acts which reduce system safety directly or indirectly (with an increased probability). Conflicting goals between action alternatives or similarities between system states are the main factors in causation of decision-based errors. Conflicts will entail errors due to individual risk acceptance. Similarities will entail expectation errors yielding incorrect system state identifications.

Here a new method is presented which allows for a systematic and comprehensive PRA inclusions of decision-based errors due to conflicts or similarities. For the error identification procedure, new question techniques are developed. These errors are shown to be identified by looking at retroactions caused by subordinate goals as components of the overall safety relevant goal.

New quantification methods for estimating situation-specific probabilities are developed. The factors conflict and similarity are operationalized in a way that allows their quantification based on informations which are usually available in PRA. The quantification procedure uses extrapolations and interpolations based on a poor set of data related to decision-based errors. Moreover, for passive errors in decision-making a completely new approach is presented where errors are quantified via a delay initiating the required action rather than via error probabilities. The practicability of this dynamic approach is demonstrated by a probabilistic analysis of the actions required during the total loss of feedwater event at the Davis-Besse plant 1985.

The extensions of the "classical" PRA method developed in this work are applied to a MMSA of the decay heat removal (DHR) of the medium sized high-temperature concept "HTR-500". Errors in decision-making - as potential roots of extraneous acts - are taken into account in a comprehensive and systematic manner. Five additional errors are identified. However, the probabilistic quantification results a nonsignificant increase of the DHR failure probability.

The conclusions of the presented work concern improvements of system safety and PRA validity. Activities to decrease individual risk acceptance will improve system safety; some ideas are given. An improved validity in quantifying risk acceptance can be reached by refinements of expert judgement models (e.g. SLIM) and by application of time-dependent models.

Entscheidungsfehler des Betriebspersonals von Kernkraftwerken als Objekt probabilistischer Risikoanalysen
von Bernhard Reer

K U R Z F A S S U N G

Die Einbeziehung von Operateurfehlern - auch Mensch-Maschine-Systemanalyse (MMSA) genannt - ist wesentlicher Bestandteil einer probabilistischen Risikoanalyse (PRA). Aktuelle Forschungsarbeiten zu methodischen Verbesserungen einer MMSA konzentrieren sich auf Fehler aufgrund falscher Handlungsabsichten bei Entscheidungen des Personals: Der Operateur hält die falsche Aktion, die er auszuführen gedenkt, für richtig. Solche Fehler führen zu ungeplanten Handlungen, die direkt oder mit einer erhöhten Wahrscheinlichkeit ein Sicherheitsdefizit zur Folge haben. Konflikte (zwischen Handlungsalternativen) und Ähnlichkeiten (zwischen Systemzuständen) gelten als Hauptfaktoren für die Entstehung solcher Entscheidungsfehler. In Konfliktsituationen kann Fehlverhalten aufgrund menschlicher Risikobereitschaft auftreten. Ähnlichkeiten können Erwartungsfehler auslösen, die zu einer falschen Identifizierung des Systemzustands führen.

In dieser Arbeit wird eine neue Methode vorgestellt, mit der sich Entscheidungsfehler aufgrund der Faktoren Konflikt und Ähnlichkeit systematisch und umfassend in eine MMSA integrieren lassen. Zur Identifizierung der entsprechenden Situationen im Störfallablauf wird eine neuartige Fragetechnik entwickelt. Es wird gezeigt, daß solche Fehler als Rückwirkungen untergeordneter Ziele auftreten können. Weiter wird gezeigt, daß solche Rückwirkungen über eine differenzierte Betrachtung sicherheitsgerichteter Ziele identifizierbar sind.

Zur Quantifizierung wird eine neue Methode entwickelt, mit der sich situationsspezifisch Wahrscheinlichkeiten für Entscheidungsfehler schätzen lassen. Es gelingt, die Faktoren Konflikt und Ähnlichkeit so zu operationalisieren, daß sie mit den Informationen, die einem PRA-Anwender üblicherweise zur Verfügung stehen, quantitativ zugänglich sind. Das darauf aufbauende Quantifizierungsverfahren basiert auf Extrapolation und Interpolationen zu den wenigen Daten, die zur Zeit über Entscheidungsfehler von Operateuren existieren. Außerdem wird für passive Entscheidungsfehler (Unterlassungen notwendiger Handlungen) ein völlig neuartiger Modellansatz vorgestellt, der solche Fehler nicht über Wahrscheinlichkeiten, sondern über Verzögerungszeiten quantifiziert. Die praktische Durchführbarkeit dieses dynamischen Ansatzes wird am Beispiel einer probabilistischen Analyse der konkreten Operateurmaßnahmen gezeigt, die während des Störfalls im Kernkraftwerk Davis-Besse (1985) angefordert wurden.

Die hier entwickelten Erweiterungen der "klassischen" MMSA-Methodik werden am Beispiel der Nachwärmeabfuhr (NWA) des Hochtemperaturreaktorkonzepts "HTR-500" angewendet. Entscheidungsfehler (als Ursachen ungeplanter Handlungen) werden systematisch und umfassend berücksichtigt. Fünf zusätzliche Entscheidungsfehler werden identifiziert. Unter Einbeziehung der entsprechenden Fehlerwahrscheinlichkeiten ergibt sich allerdings keine signifikante Erhöhung der Ausfallwahrscheinlichkeit bzw. Unverfügbarkeit der NWA.

Die Schlußfolgerungen dieser Arbeit gehen in zwei Richtungen: Erhöhung der Sicherheit einer Anlage und Erhöhung der Realitätsnähe einer PRA. Die Erhöhung der Sicherheit einer Anlage ist durch Maßnahmen zur Senkung der Risikobereitschaft erreichbar; hierzu werden einige Anregungen gegeben. Fortschritte bei der probabilistischen Quantifizierung menschlicher Risikobereitschaft sind durch die Weiterentwicklung von Expertenschätzmodellen (z.B. SLIM) und durch die Anwendung von dynamischen Modellen realisierbar.

Vorwort

Der hier vorliegende Bericht ist eine von dem Fachbereich Sicherheitstechnik der Bergischen Universität-Gesamthochschule Wuppertal genehmigte Dissertation (D468, Tag der mündlichen Prüfung: 15. Dezember 1992).

Bei der Erstellung dieser Dissertation habe ich das "know how" verschiedener Wissensgebiete genutzt; z.B: Technische Zuverlässigkeit, Reaktortechnik, Datenverarbeitung, Psychologie und Entscheidungstheorie.

Ich bedanke mich bei den Mitarbeitern des Forschungszentrums Jülich, die durch ihre sachkundigen Antworten zu meinen Fragen dazu beigetragen haben, daß ich dieses "know how" optimal nutzen konnte. Insbesondere Herrn Bongartz, Frau Degen, Herrn Hennings, Herrn Jahn, Frau Marx, Herrn Dr. Mertens, Herrn Dr. Müller-Späth, Herrn Dr. Verfondern und Herrn Dr. Völzer aus dem Institut für Sicherheitsforschung und Reaktortechnik sowie Herrn Jansen und Frau Marx aus dem Zentralinstitut für Angewandte Mathematik. Vielen Dank auch an Herrn Prof. Jungermann für seine Literaturhinweise zum Stand der psychologischen Fehlerforschung.

Ich bedanke mich bei Herrn Prof. Tietze, Herrn Prof. Kröger und Herrn Prof. Häcker für die freundliche Übernahme der Referate dieser interdisziplinären Dissertation.

Das diesem Bericht zugrundeliegende Forschungsvorhaben wurde mit Mitteln des Bundesministers für Forschung und Technologie (Förderkennzeichen 03THA202) gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Bernhard Reer

Inhaltsverzeichnis

Abkürzungsverzeichnis	1
1. Einleitung	7
1.1 Zielsetzung	7
1.2 Methodische Behandlung von Operateurfehlern in Risikostudien: Entwicklungsstand und aktuelle Trends	8
1.2.1 Der PRA-Leitfaden von 1983	8
1.2.2 Neuere Entwicklungen	10
1.2.2.1 Konfusionsmatrix und Zeitabhängigkeit	10
1.2.2.2 Kognitive Prozesse und Risikobereitschaft	11
1.3 Aufbau der Arbeit	20
1.4 Zusammenfassung von Abschnitt 1	21
2. Reales Beispiel: Der Störfall im KKW Davis-Besse 1985	23
2.1 Einführung	23
2.2 Das NWA-Konzept der Anlage	23
2.3 Der Störfall am 9.6.1985	23
2.4 Probabilistische Analyse der Operateurmaßnahmen	27
2.4.1 Dynamische Analysemethode für Operateurhandlungen (DAO)	27
2.4.1.1 Fehlermodell	27
2.4.1.2 Eingangsgrößen und Rechenprogramme	29
2.4.1.3 Konfliktmodellierung	35
2.4.2 Annahmen zur dynamischen Modellierung	36
2.4.3 Erfolgskriterien	36
2.4.4 Zeitbedarfsanalyse und Konfliktberücksichtigung	37
2.4.5 Ereignisbaumanalyse und Ergebniszusammenfassung	40
2.5 Zusammenfassung von Abschnitt 2	42
3. Hypothetisches Anwendungsbeispiel: Die Notkühlung des HTR-500	45
3.1 Einführung	45
3.2 Betrachtete Transiente	49
3.3 Modellierung gemäß Hauptziel "NWA ausreichend"	50
3.3.1 Zur Methode	50
3.3.2 Die ISF-Analyse	51
3.3.3 Einbeziehung menschlichen Verhaltens	53
3.3.3.1 Aufgabenanalyse	53
3.3.3.2 Naturkonvektion	55
3.3.3.3 Querverbindung	66
3.3.3.4 Reparatur	70
3.3.3.5 Zusammenfassende Bewertung der menschlichen Gegenmaßnahmen	79
3.4 Zusammenfassung von Abschnitt 3	82
4. Identifizierung von Rückwirkungen untergeordneter Ziele	85
4.1 Einführung	85
4.2 Identifizierung untergeordneter Ziele	85
4.2.1 Betriebliche Aspekte	85
4.2.2 Konkrete Systemzustände	90
4.3 Identifizierung von Rückwirkungen	91
4.3.1 Vergleich von Realisierungsalternativen des Hauptziels	91
4.3.1.1 Monotonie von Realisierungsalternativen	92
4.3.1.2 Monotonie von Übergangsmöglichkeiten	94
4.3.1.3 Zusammenfassung der für den HTR-500 identifizierten Konfliktsituationen	94
4.3.2 Ähnlichkeitsbetrachtungen zu WENN-DANN-Regeln	97
4.3.2.1 Ähnlichkeitsbetrachtungen zu widersprüchlichen Ausführungszielen	97

4.3.2.2 Unähnliche Erscheinungsformen einer Anwendungsbedingung	99
4.3.2.3 Zusammenfassung der für den HTR-500 identifizierten Diagnoseprobleme	101
4.4 Zusammenfassung von Abschnitt 4	102
5. Quantifizierung von Rückwirkungen untergeordneter Ziele	105
5.1 Einführung	105
5.1.1 Zielsetzung	105
5.1.2 Versuch einer Klassifizierung	105
5.1.3 Zur Bedeutung der Faktoren Diagnose und Risikoverhalten	108
5.2 Durch Konflikte verursachtes Fehlverhalten	110
5.2.1 Bisherige Berücksichtigung	110
5.2.1.1 Zwei Beispiele	110
5.2.1.2 Kommentar	111
5.2.2 Erkenntnisse der psychologischen Sicherheitsforschung zu Fehlverhalten	113
5.2.2.1 Persönlichkeitsbedingte Risikobereitschaft	113
5.2.2.2 Zeitliche Tendenzen im Risikoverhalten	119
5.2.2.3 Risikovergleich und Risikokompensation	122
5.2.3 Methodische Empfehlung zur Quantifizierung von Fehlverhalten	130
5.2.3.1 Theoretische Grundlage: SLIM	130
5.2.3.2 Berücksichtigte Einflußfaktoren (PSFs)	133
5.2.3.3 Kalibrierung	138
5.2.3.4 Unsicherheiten	141
5.2.3.5 Kritik	143
5.3 Durch Ähnlichkeiten verursachte Erwartungsfehler	151
5.3.1 Problembeschreibung	151
5.3.2 Versuch einer Einordnung in ein Klassifizierungsschema	153
5.3.3 Beispiele für quantitative Effekte von Erwartungen	159
5.3.3.1 Beispiel 1: Drehschalter betätigen	159
5.3.3.2 Beispiel 2: Grenzwertüberschreitung bemerken	159
5.3.3.3 Beispiel 3: Schriftliche Registrierung	159
5.3.4 Quantifizierungsvorschlag	161
5.4 Anwendungsbeispiel HTR-500	164
5.4.1 Überblick	164
5.4.2 Neue Fehlerwahrscheinlichkeiten	164
5.4.3 Modifizierung der NWA-Zuverlässigkeit ohne Gegenmaßnahmen	167
5.4.4 Modifizierung der Zuverlässigkeit der Gegenmaßnahmen	170
5.4.5 Ergebniszusammenfassung	174
5.5 Zusammenfassung von Abschnitt 5	176
6. Zusammenfassung	179
7. Schlußfolgerungen	183
8. Literaturverzeichnis	189
Anhang A: BMFT-Forschungsvorhaben zur Erweiterung der PRA-Zielsetzung. Kurzbeschreibung	197
Anhang B: HTR-500. NWA-System. Fehlerbäume aus ISF (1984)	199
Anhang C: HTR-500. Passive NWA per Naturkonvektion. Hypothetische Prozedur	205
Anhang D: HTR-500. Querverbindung zur Gebläsekühlung. Hypothetische Prozedur	207
Anhang E: Basisfehlerwahrscheinlichkeiten	209

Anhang F: Berücksichtigung von Stress	215
Anhang G: Berücksichtigung von Abhängigkeiten	217
Anhang H: HTR-500. Weitere Konfliktsituationen	219
Anhang I: HTR-500. Weitere Diagnoseprobleme	221
Tabellenverzeichnis	223
Abbildungsverzeichnis	225

4.3.2.2 Unähnliche Erscheinungsformen einer Anwendungsbedingung	99
4.3.2.3 Zusammenfassung der für den HTR-500 identifizierten Diagnoseprobleme	101
4.4 Zusammenfassung von Abschnitt 4	102
5. Quantifizierung von Rückwirkungen untergeordneter Ziele	105
5.1 Einführung	105
5.1.1 Zielsetzung	105
5.1.2 Versuch einer Klassifizierung	105
5.1.3 Zur Bedeutung der Faktoren Diagnose und Risikoverhalten	108
5.2 Durch Konflikte verursachtes Fehlverhalten	110
5.2.1 Bisherige Berücksichtigung	110
5.2.1.1 Zwei Beispiele	111
5.2.1.2 Kommentar	113
5.2.2 Erkenntnisse der psychologischen Sicherheitsforschung zu Fehlverhalten	113
5.2.2.1 Persönlichkeitsbedingte Risikobereitschaft	119
5.2.2.2 Zeitliche Tendenzen im Risikoverhalten	122
5.2.2.3 Risikovergleich und Risikokompensation	130
5.2.3 Methodische Empfehlung zur Quantifizierung von Fehlverhalten	130
5.2.3.1 Theoretische Grundlage: SLIM	133
5.2.3.2 Berücksichtigte Einflußfaktoren (PSFs)	138
5.2.3.3 Kalibrierung	141
5.2.3.4 Unsicherheiten	143
5.2.3.5 Kritik	151
5.3 Durch Ähnlichkeiten verursachte Erwartungsfehler	151
5.3.1 Problembeschreibung	153
5.3.2 Versuch einer Einordnung in ein Klassifizierungsschema	159
5.3.3 Beispiele für quantitative Effekte von Erwartungen	159
5.3.3.1 Beispiel 1: Drehschalter betätigen	159
5.3.3.2 Beispiel 2: Grenzwertüberschreitung bemerken	159
5.3.3.3 Beispiel 3: Schriftliche Registrierung	161
5.3.4 Quantifizierungsvorschlag	164
5.4 Anwendungsbeispiel HTR-500	164
5.4.1 Überblick	164
5.4.2 Neue Fehlerwahrscheinlichkeiten	167
5.4.3 Modifizierung der NWA-Zuverlässigkeit ohne Gegenmaßnahmen	170
5.4.4 Modifizierung der Zuverlässigkeit der Gegenmaßnahmen	174
5.4.5 Ergebniszusammenfassung	176
5.5 Zusammenfassung von Abschnitt 5	179
6. Zusammenfassung	183
7. Schlußfolgerungen	189
8. Literaturverzeichnis	197
Anhang A: BMFT-Forschungsvorhaben zur Erweiterung der PRA-Zielsetzung. Kurzbeschreibung	199
Anhang B: HTR-500. NWA-System. Fehlerbäume aus ISF (1984)	205
Anhang C: HTR-500. Passive NWA per Naturkonvektion. Hypothetische Prozedur	207
Anhang D: HTR-500. Querverbindung zur Gebläsekühlung. Hypothetische Prozedur	209
Anhang E: Basisfehlerwahrscheinlichkeiten	209

Anhang F: Berücksichtigung von Stress	215
Anhang G: Berücksichtigung von Abhängigkeiten	217
Anhang H: HTR-500. Weitere Konfliktsituationen	219
Anhang I: HTR-500. Weitere Diagnoseprobleme	221
Tabellenverzeichnis	223
Abbildungsverzeichnis	225

Abkürzungsverzeichnis

a	Jahr(e)
ANS	American Nuclear Society
app.	appendix
BE	Brennelement(e)
BHEP	Basic Human Error Probability
BMFT	Der Bundesminister für Forschung und Technologie, Bonn
bzgl.	bezüglich
CA	California
CCF	Common Cause Failure
CES	Cognitive Environment Simulation (WOODs u.a. 1990; WOODS u.a. 1988; WOODS u.a. 1987)
ch.	chapter
CREATE	Cognitive Reliability Analysis Technique (WOODS u.a. 1990; WOODS/ROTH 1987)
CV	Variationskoeffizient
DE	Dampferzeuger
d.h.	das heißt
DRS-A	Deutsche Risikostudie Kernkraftwerke, Phase A (GRS 1979)
DRS-B	Deutsche Risikostudie Kernkraftwerke, Phase B (GRS 1990)
DWR	Druckwasserreaktor
e	= 2.718... (EULER-Konstante)
Ed.	Editor
ENS	European Nuclear Society
EPC	Error Producing Condition (WILLIAMS 1988)
ERA	Mittelwert von RA
ERA*	Mittelwert von RA*
ERW	Mittelwert von RW
ERW*	Mittelwert von RW*
evtl.	eventuell
EW	Erwartungswert
EW < UG,OG >	EW und 90%-Unsicherheitsintervall
exp(x)	e hoch x
f	und die folgende
ff	und die folgenden
F	Fehlerwahrscheinlichkeit einer Gesamthandlung (ohne Berücksichtigung von Zeitabhängigkeiten)

F(t)	zeitabhängige Fehlerwahrscheinlichkeit einer Gesamthandlung (einschließlich zeitunabhängiger Fehler)
Fi	multiplikativer Effekt von PSF i
FLI	Failure Likelihood Index (Fehlerindex)
GAO	NWA-Gebläseabsperrorgan
GBÖ	NWA-Gebläseby-passorgan
gem.	gemäß
ggfs.	gegebenenfalls
GRS	Gesellschaft für Reaktorsicherheit, Köln und Garching
h	Stunde(n)
HAK	Hauptgebläseabsperrklappe
HCR	Human Cognitive Reliability (HANNAMAN u.a. 1984)
HD	high dependence
HEART	Human Error Assessment and Reduction Technique (WILLIAMS 1988)
HEP	Human Error Probability
Hg.	Herausgeber
HKS	Hauptkühlsystem
HRB	Hochtemperatur-Reaktorbau GmbH, Mannheim
HTR	Hochtemperaturreaktor
ID	Identifikationsnummer der BHEP lt. Anhang E
IfU	Institut für Unfallforschung, TÜV Rheinland, Köln
INTENT	"a Method for Estimating Human Error Probabilities for Decisionbased Errors" (GERTMAN u.a. 1992)
ISF	Institut für Nukleare Sicherheitsforschung, KFA; seit 1990: Institut für Sicherheitsforschung und Reaktortechnik (ISR)
Kap.	Kapitel
kg	Kilogramm
KFA	Kernforschungsanlage Jülich; seit 1990: Forschungszentrum Jülich
Ki	maximaler multiplikativer Effekt von PSF i
KKW	Kernkraftwerk(e)
KWU	Kraftwerk Union
LD	low dependence
lg	dekadischer Logarithmus
ln	natürlicher Logarithmus
log	Logarithmus
LWR	Leichtwasserreaktor(en)
lt.	laut

MAX	Maximum
MD	moderate dependence
MDN	Median
MDN < UF >	MDN und Unsicherheitsfaktor (Streufaktor)
menschl.	menschlich(e)(r)
MMSA	Mensch-Maschinesystemanalyse
min	Minute(n)
MIN	Minimum
MTTR	Mittlere Reparaturdauer
MWe	Megawatt elektrische Leistung
NNK	Nukleares Nebenkühlwassersystem
NRC	Nuclear Regulatory Commission, U.S.A.
NWA	Nachwärmeabfuhr
N.Y.	New York
o.ä	oder ähnliches
o.g.	oben genannte(n)
OG	95%-Obergrenze
OZUF	ohne zeitunabhängige Fehler
p	Wahrscheinlichkeit
p.	page(s)
P(t)	zeitabhängige Fehlerwahrscheinlichkeit (ohne Berücksichtigung zeitunabhängiger Fehler)
PRA	Probabilistische Risikoanalyse
PSA	Probabilistische Sicherheitsanalyse
PSF	Performance Shaping Factor
psig	pound per square inch Gasdruck ($\approx 0.07 \text{ kp/cm}^2$)
Q(t)	zeitabhängige Erfolgswahrscheinlichkeit (ohne Berücksichtigung zeitunabhängiger Fehler)
RA	akzeptiertes Risiko (Intervallskalenwert)
RA*	akzeptiertes Risiko (Verhältnisskalenwert)
RDB	Reaktordruckbehälter
RSG	Reaktorschutzgebäude
Rel.Eng.	Reliability Engineering
RW	wahrgenommenes Risiko (Intervallskalenwert)
RW*	wahrgenommenes Risiko (Verhältnisskalenwert)
s	Sekunde(n)
s.	siehe
S.	Seite(n)

S	Sonstiger Fehler
SLI	Success Likelihood Index (Zuverlässigkeitsindex)
SLIM-MAUD	"Success Likelihood Index Methodology implemented through the use of an interactive computer program called MAUD -- Multi-Attribute Utility Decomposition" (EMBREY u.a. 1984)
SNS	Swiss Nuclear Society
STD	Standardabweichung
s.o.	siehe oben
sog.	sogenannte(n)
s.u.	siehe unten
t	Zeit
T	Durchführungszeit
T.	Table
techn.	technisch(e)(r)
T0	Mindestzeit
T50	50%-Wert: Zeit, die in 50% aller Fälle unterschritten wird
T95	95%-Wert: Zeit, die in 95% aller Fälle unterschritten wird
THERP	Technique of Human Error Rate Prediction (SWAIN-Handbuch)
THTR	Thorium-Hochtemperaturreaktor (in Hamm-Uentrop)
u.	und
U	Unterlassungsfehler
u.a.	und andere, unter anderem
UF	Unsicherheitsfaktor zur Berechnung von OG ($=MDN \cdot UF$) und UG ($=MDN/UF$) einer Lognormalverteilung
u.g.	unten genannte(n)
UG	5%-Untergrenze
U.S.A.	United States of America
usw.	undsoweiter
V	Verwechslungsfehler
VAR	Varianz
Vlg.	Verlag
Vpn	Versuchsperson(en)
W	Wahrnehmungsfehler
w(...)	Wahrscheinlichkeit, daß ...
Wahrsch.	Wahrscheinlichkeit
wi	Wichtungsfaktor von PSF i
WT	Wärmetauscher
xi	Grad des Vorhandenseins von PSF i:

	x1 = besonderer Anreiz zu Fehlverhalten
	x2 = Zielkonflikt
	x3 = Schadenshöhe gering
	x4 = Schadenswahrscheinlichkeit gering
	x5 = Risikounterschätzung
	x6 = Fehlverhalten zu einfach
	x7 = richtiges Verhalten ungewöhnlich
Z	Zeitfehler (Durchführung nicht rechtzeitig)
z(p)	Inverse Funktion der Verteilungsfunktion, $p = \Phi(z)$, der standardisierten Normalverteilung
z.B.	zum Beispiel
zit.n.	zitiert nach
ZUF	zeitunabhängiger Fehler
$\Phi(z)$	Verteilungsfunktion der standardisierten Normalverteilung
_2	2. Operateur
_3	3. Operateur
_S	späte (nachträgliche) Korrektur versagt

1. Einleitung

1.1 Zielsetzung

Die Durchführung einer Mensch-Maschine-Systemanalyse (MMSA) - im Rahmen einer probabilistischen Risikoanalyse (PRA) für ein Kernkraftwerk (KKW) - dient u.a. der Identifizierung sicherheitsrelevanter Operateurfehler, der Quantifizierung ihrer Häufigkeit sowie der Ableitung von Schlußfolgerungen zur Fehlervermeidung. Mit dem steigenden Automatisierungsgrad in der Kerntechnik sinkt die Bedeutung von Operateurfehlern bei fertigungsorientierten Tätigkeiten. Aktuelle Forschungsarbeiten zu methodischen Verbesserungen einer MMSA konzentrieren sich daher auf Fehler aufgrund falscher Handlungsabsichten bei Entscheidungen des Personals: Der Operateur hält die falsche Aktion, die er auszuführen gedenkt, für richtig. Solche Fehler führen zu ungeplanten Handlungen, die direkt oder mit einer erhöhten Wahrscheinlichkeit ein Sicherheitsdefizit zur Folge haben. Ein interessanter Ansatz zur Berücksichtigung solcher Fehler besteht in Erweiterung der "klassischen" Zielsetzung einer PRA.

Die klassische Zielsetzung einer PRA (im Bereich Kerntechnik) ist die Identifizierung und Quantifizierung von Ereignisabläufen, die zur Spaltproduktfreisetzung führen können. An dieser Fragestellung orientieren sich die Fehler- und Ereignisbäume einer klassischen PRA. Das Thema dieser Arbeit ist die Erweiterung dieser klassischen Zielsetzung und die Untersuchung der sich daraus ergebenden Rückwirkungen auf die Zuverlässigkeit des Personals eines Kernkraftwerks. Die Erweiterung erfolgt durch Einbeziehung von Zielen untergeordneter Sicherheitsbedeutung. Zwei Arten solcher Ziele werden näher untersucht:

1. Betriebliche Aspekte (z.B. Komponentenschonung), die gegenüber dem klassischen Hauptziel Sicherheit, eine untergeordnete Priorität haben.
2. Konkrete Systemzustände (z.B. die Stellung von Armaturen), die zur Realisierung des Hauptziels erforderlich sind, aber auch in anderen Zusammenhängen relevant sind.

Die Untersuchung der aus diesen Zielen ableitbaren Rückwirkungen auf die Zuverlässigkeit des Personals beschränkt sich auf Entscheidungen in Störfallsituationen nach erfolgter Diagnose der richtigen Prozedur, die auf das auslösende Ereignis zutrifft. Von den zu erwartenden Rückwirkungen werden zwei Erscheinungsformen betrachtet:

1. Konflikte, die regelwidrige Entscheidungen (im Sinne einer bewußten Risikoan-nahme) auslösen können (vgl. HACKER 1980, S.346). Durch Konflikte hervorgerufene regelwidrige Entscheidungen werden hier kurz als Fehlverhalten bezeichnet. Solches Fehlverhalten kann z.B. auftreten, wenn sich durch vorschriftsmäßiges Verhalten ein Ziel untergeordneter Sicherheitsbedeutung nicht realisieren läßt.
2. Ähnlichkeiten, die erwartungsgebundene Fehlinterpretationen auslösen können (vgl. HACKER 1980, S.347ff). Erwartungsgebundene Fehlinterpretationen werden hier kurz als Erwartungsfehler bezeichnet. Solche Fehler können z.B. auftreten, wenn sich eine Kombination von Systemzuständen, die zur Realisierung des Hauptziels Sicherheit, erforderlich ist, nur in einem kritischen Detail von anderen Kombination von Systemzuständen unterscheidet, die einen sicherheitswidrigen Zustand bewirkt.

Die o.g. Fehler fallen in die Kategorie "Entscheidungsverhalten nach erfolgter Diagnose" ("postdiagnosis decision-making", SWAIN 1983, p. 12-9). Hier werden die unmittelbaren Folgen solcher Fehler auch als ungeplante Handlungen bezeichnet; denn sie sind zumeist mit der Verfolgung von Strategien verbunden, die nicht in der vorgeschriebenen Prozedur stehen. Solche Fehler werden - gemessen an ihrer Sicherheitsbedeutung - bisher nur unzureichend in einer PRA berücksichtigt. Deshalb wird hier eine Methode erarbeitet, die es ermöglicht, wesentliche Aspekte des Entscheidungsverhaltens nach erfolgter Diagnose in eine PRA zu integrieren.

Die hier vorliegende Untersuchung ist Teil eines vom BMFT finanzierten Forschungsvorhabens (s. Anhang A), mit dem im Oktober 1986 begonnen wurde. Dieses Vorhaben wurde 1990 um den Aspekt "Erwartungsfehler aufgrund von Ähnlichkeiten" erweitert.

1.2 Methodische Behandlung von Operateurfehlern in Risikostudien: Entwicklungsstand und aktuelle Trends

1.2.1 Der PRA-Leitfaden von 1983

Mit der Reaktorsicherheitsstudie WASH-1400 (1975) erschien die erste Untersuchung, die das von einem KKW ausgehende Risiko quantitativ (mit den Methoden der Wahrscheinlichkeitsrechnung) abschätzte. In Anlehnung an WASH-1400 (1975) wurde

in der Bundesrepublik Deutschland die Phase A der "Deutschen Risikostudie Kernkraftwerke" (DRS-A) erstellt (GRS 1979).

Das Erscheinen von WASH-1400 (1975) löste heftige Kritik an der PRA-Methodik aus (z.B. LEWIS u.a. 1978). Insbesondere wurde die Quantifizierbarkeit von Operateurfehlern in Frage gestellt. Die Kritik führte dazu, daß eine Vielzahl von Wissenschaftlern an Verbesserungen der in WASH-1400 (1975) angewendeten PRA-Methodik arbeiteten. Eine erste Zwischenbilanz dieser Arbeiten ist in dem PRA-Leitfaden "PRA Procedures Guide" (NRC 1983) dokumentiert. Dieser Leitfaden bildete die Grundlage für das "Reactor Risk Reference Document" (NRC 1987), in dem die Risikoanalysen von fünf Leichtwasserreaktoren miteinander verglichen wurden. In dieser vergleichenden Untersuchung wurden auch Unsicherheiten aufgrund von Expertenschätzungen zu wichtigen Detailfragen, die bei der praktischen Durchführung einer PRA auftreten, quantifiziert. Dabei wurde u.a. festgestellt, daß aufgrund dieser Unsicherheiten die Schwankungsbreite der Häufigkeit eines schweren Kernschadens eine Größenordnung betragen kann.

Zur Einbeziehung von Operateurfehlern (MMSA) in eine PRA wird im PRA-Leitfaden die Methode THERP ("Technique of Human Error Rate Prediction"; SWAIN 1980; SWAIN 1983) empfohlen. Diese Methode wurde auch in der DRS-B (GRS 1990) angewendet. Laut THERP läßt sich eine MMSA in zwei Bestandteile zerlegen:

- in einen qualitativen Teil, die sog. Aufgabenanalyse ("task analysis") zur Identifizierung kritischer Operateurfehler, und
- in einen quantitativen Teil, die menschliche Zuverlässigkeitsanalyse ("human reliability analysis") zur Berechnung der Fehlerwahrscheinlichkeiten.

Häufig - wie z.B. in dem MMSA-Beispiel, das im PRA-Leitfaden genannt wird (NRC 1983, ch.4) - werden diese beiden Teile nicht unabhängig voneinander durchgeführt. D.h., die Identifizierung kritischer Operateurfehler orientiert sich an solchen Fehlern, für die im SWAIN-Handbuch Wahrscheinlichkeiten tabelliert sind (s. Tab. 1 im folgenden Text). In SWAIN (1983, p.12-8) wird selbstkritisch angemerkt, daß mit den Fehlern 2 bis 7 keine umfassende Quantifizierung von Entscheidungsfehlern NACH erfolgter Diagnose möglich ist.

Ein weiterer Schwachpunkt der in SWAIN (1983) und NRC (1983) beschriebenen MMSA ist die zu starke Fixierung auf (offensichtlich) sicherheitsrelevante Aufgaben des Personals: "Only the tasks that are relevant to safety of the system are considered" (NRC 1983, ch.4). In allen Analysebeispielen (NRC 1983, ch.4; SWAIN

1983, ch.21) werden nur die Fehler von notwendigen Aufgaben betrachtet, deren Nichtdurchführung sicherheitsrelevant ist. Es gibt aber auch sicherheitsrelevante Fehler bei der Durchführung nicht notwendiger Aufgaben; z.B. der Verwechslungsfehler bei der nicht notwendigen manuellen Inbetriebnahme des Notspeisewassersystems während des Störfalls im KKW Davis-Besse (NRC 1985). Eine in französischen Kernkraftwerken durchgeführte Untersuchung ergab, daß 22% der beobachteten Fehler in die Kategorie UNPASSENDE UND NICHT ANGEFORDERTE AKTION fallen (GHERTMAN/DIETZ 1985). Aber auch nicht notwendige Aufgaben, bei denen keine sicherheitsrelevanten Fehler auftreten können, haben einen Einfluß auf die Sicherheit. Für ihre Durchführung wird nämlich Zeit benötigt. Diese Zeit könnte im Endeffekt die rechtzeitige Durchführung der notwendigen Aufgaben gefährden.

- | |
|--|
| <ol style="list-style-type: none"> 1. Nicht richtige Diagnose des Störfalls 2. Falsches Ablesen oder Nichtbemerken von Informationen beim Beobachten von Systemzustandsanzeigen 3. Nichtreagieren auf hörbaren Alarm 4. Durchführung einer Prozedur ohne Benutzung der dafür vorgesehenen schriftlichen Unterlage 5. Nicht richtiges Benutzen einer Checkliste 6. Unterlassung eines Schritts beim Abarbeiten einer Prozedur 7. Verwechslungsfehler beim Betätigen einer Komponente (Schalter, Handventil) oder beim Beobachten einer Systemzustandsanzeige |
|--|

Tab. 1. Operateurfehler im Störfall, die Bestandteil der Datenbasis des SWAIN-Handbuchs sind

1.2.2 Neuere Entwicklungen

1.2.2.1 Konfusionsmatrix und Zeitabhängigkeit

Zur Einbeziehung von Operateurfehlern in eine PRA gibt es - neben THERP - eine Vielzahl von Methoden. In SWAIN (1989) werden z.B. 14 Methoden miteinander verglichen. Fast alle Methoden beschränken sich auf den quantitativen Teil einer MMSA.

Außerdem gibt es eine Reihe von Verbesserungsvorschlägen zu THERP in wichtigen Detailfragen; z.B. die differenzierte Betrachtung des Fehlers "nicht richtige Diagnose" dahingehend, daß versucht wird zu identifizieren, um welche Fehldiagnose es sich handeln könnte (STAMPELOS/APOSTOLAKIS 1985; WAKEFIELD/ADAMS 1987; WAKEFIELD 1988; SWAIN/WESTON 1988). Diese Ansätze gehen auf die Methode

„Konfusionsmatrix“ (POTASH u.a. 1981) zurück. Diese Arbeiten betreffen zwar teilweise den hier untersuchten Faktor „ähnlichkeitsbedingte Erwartungen“, es fehlen aber konkrete Hinweise zur Quantifizierung.

Auch der Faktor „konfliktbedingte Risikobereitschaft“ wird in einigen Methoden erwähnt; z.B. SLIM („Success Likelihood Index Methodology“; EMBREY u.a. 1984, Vol.II, p.43). Konkrete Hinweise zur quantitativen Erfassung werden nicht genannt.

Aus neueren Risikostudien in den U.S.A. und Skandinavien ist ein Trend erkennbar, der in einer - gegenüber THERP - verbesserten Berücksichtigung des Faktors Zeit besteht (z.B. zusammenfassend in BLEY u.a. 1988 oder HIRSCHBERG 1990). Im Gegensatz zu THERP werden auch für Handlungen nach erfolgter Diagnose die Verteilungsfunktionen der Durchführungszeiten berücksichtigt. Das HCR-Modell („Human Cognitive Reliability“; HANNAMAN u.a. 1984) erlaubt eine flexible und differenzierte Schätzung von zeitbezogenen Verteilungsfunktionen. Anwendungen in HIRSCHBERG (1990) zeigten jedoch, daß das HCR-Modell für Handlungen nach erfolgter Diagnose unrealistische Fehlerwahrscheinlichkeiten liefert. BLEY u.a. (1988) schlagen eine kombinierte Verwendung von zeitabhängigen und zeitunabhängigen Fehlerwahrscheinlichkeiten. Dieser Vorschlag wird auch in der hier entwickelten „Dynamischen Analyseverfahren für Operateurhandlungen“ (REER) aufgegriffen (vgl. Abschnitt 2).

1.2.2.2 Kognitive Prozesse und Risikobereitschaft

Abb. 1 verdeutlicht einen weiteren Trend in der Entwicklung der MMSA-Methodik. Schlußfolgerungen zur Erhöhung der Sicherheit lassen sich nicht nur mit probabilistischen Methoden erreichen. Auch Fachleute aus der kognitiven Psychologie, Sicherheitspsychologie und Ergonomie beschäftigen sich mit der Entstehung von Fehlern in komplexen Mensch-Maschine-Systemen (VON KLEBELSBERG 1977; RASMUSSEN 1979; RASMUSSEN 1983; RASMUSSEN 1988; HACKER 1986; BURKARDT 1985; WEHNER/MEHL 1986; REINARTZ u.a. 1986; BUBB 1988; BUBB 1990; REASON 1988; REASON 1990; HOYOS/ZIMOLONG 1988; ZIMOLONG 1990; BECKER 1990; CARNINO u.a. 1990).

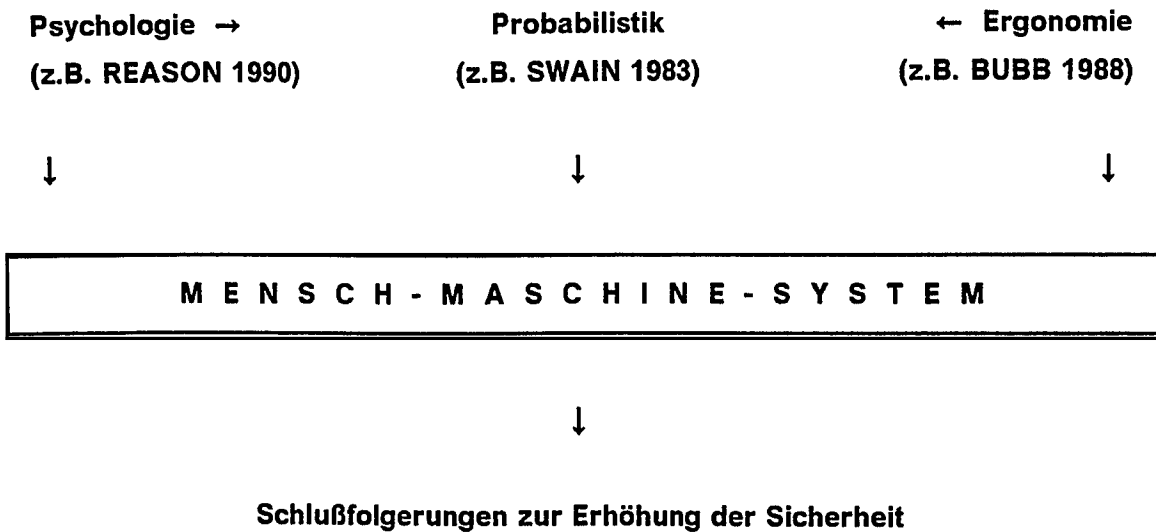


Abb. 1. Mögliche Schwerpunkte einer Mensch-Maschine-Systemanalyse

Einige Arbeiten gehen kritisch auf die probabilistischen Methoden einer MMSA ein (z.B. HOYOS/ZIMOLONG 1988; REASON 1990; ZIMOLONG 1990; CARNINO u.a. 1990).

Neuere probabilistische MMSA-Methoden konzentrieren sich auf die Nutzung von psychologischen Erkenntnissen aus den oben zitierten Arbeiten (z.B. WILLIAMS 1988; WOODS u.a. 1990; GERTMAN u.a. 1992). Bevor auf diese Methoden näher eingegangen wird, werden zunächst die wichtigsten psychologischen Erkenntnisse zur Fehlerforschung referiert. Diese Erkenntnisse bestätigen die hohe Bedeutung der Faktoren Konflikt und Ähnlichkeit für die Entstehung von Entscheidungsfehlern.

Erste Anwendungen der kognitiven Psychologie bei der Erforschung des Verhaltens von Operateuren wurden von JENS RASMUSSEN durchgeführt (z.B. RASMUSSEN 1979; RASMUSSEN 1983; RASMUSSEN 1988). RASMUSSEN unterteilt den kognitiven Prozeß (d.h. die Informationsverarbeitung bei der Durchführung einer Aufgabe) in acht Schritte (Abb. 2).

Level	Internal Mechanism		
KNOWLEDGE	Identification → ↑	Decision of task →	Planning ↓
RULE	↑ → Recognition → ↑	Association: state/task →	Stored rules for tasks ↓
SKILL	↑ Feature Formation → ↑ (INPUT)	Automated sensori-motor pattern	↓ (ACTION)

Abb. 2. Performance Levels of Skilled Operators:

Nach RASMUSSEN (1983), leicht vereinfacht. Siehe auch Abb. 9 auf Seite 35.

Das Besondere an dem Modell ist, daß die Frage, welche der acht Schritte "durchlaufen" werden, von dem zur Aufgabendurchführung erforderlichen kognitiven Niveau (Kenntnisbedarf) abhängt. RASMUSSEN unterteilt dieses Niveau in die drei diskreten Klassen SKILL-BASED (fertigkeitsbasiert: abgespeicherte Muster vorprogrammierter Instruktionen werden abgerufen), RULE-BASED (regelbasiert: bekannte Probleme werden mit Hilfe von WENN-DANN-Regeln gelöst) und KNOWLEDGE-BASED (wissensbasiert: neuartige Probleme werden durch analytisches Vorgehen unter Zugriff auf abgespeichertes Wissen gelöst).

Diese Unterteilung wird auch von REASON (1990) bei der Fehlerklassifizierung aufgegriffen (Tab. 2). In dieser Einteilung wird zwischen Flüchtigkeitsfehler und Irrtum unterschieden. Den Unterschied definiert REASON (1990, p.6ff) über die Frage, ob eine beabsichtigte oder unbeabsichtigte Aktion vorliegt. Eine Aktion ist unbeabsichtigt, wenn sie - unabhängig davon, ob sie zur Zielerreichung geeignet ist oder nicht - so ausgeführt wird, daß das angestrebte (beabsichtigte) Ziel nicht erreicht wird. Der dieser Nichterreichung des Zieles zugrundeliegende Fehler bei der Ausführung wird als Flüchtigkeitsfehler ("slip or lapse") bezeichnet. Dagegen ist eine Aktion beabsichtigt, wenn sie fehlerfrei ausgeführt wird. Ein Irrtum tritt auf, wenn sich mit dieser Aktion - trotz fehlerfreier Ausführung - das Ziel nicht erreichen läßt.

- | |
|--|
| <ol style="list-style-type: none"> 1. Fertigkeitsbasierte Flüchtigkeitsfehler
("skill-based slips and lapses") 2. Regelbasierte Irrtümer
("rule-based mistakes") 3. Wissensbasierte Irrtümer
("knowledge-based mistakes") |
|--|

Tab. 2. Basisfehlertypen nach REASON (1990):

Jeder Fehlertyp ("error type") wird von REASON noch in Fehlerarten ("error modes", s. Tab. 50 auf Seite 158) unterteilt; vgl. Abschnitt 5.3.2.

REASON (1990, p.97ff) geht davon aus, daß Fehler immer dann auftreten, wenn eine kognitive Unterspezifikation ("cognitive underspecification") vorliegt. Eine kognitive Unterspezifikation läßt sich im weitesten Sinne als "Informationsmangel" definieren. Der Mangel kann als fehlende, falsche oder irreführende Information in Erscheinung treten, und er kann äußere (z.B. defekter Meßfühler) oder innere (z.B. "schlechtes" Erinnerungsvermögen) Ursachen haben. Daher ist der Ansatz von REASON nicht neu. Bereits HACKER (1980) nannte den Informationsmangel als übergeordnete Ursache aller Fehlhandlungen.

Weiter geht REASON (1990, p.130ff) davon aus, daß beim Vorliegen einer kognitiven Unterspezifikation zwei Fehlerformen auftreten, auf die sich alle Fehlertypen (Tab. 2) zurückführen lassen:

1. Ähnlichkeitsanpassung ("similarity-matching"). Äußere aktuelle Anforderungsbedingungen werden ständig mit angeeigneten Wissensseinheiten (auf einer "gleich-zu-gleich"-Basis) verglichen. Dabei richtet sich der erste "Lauf" auf solche Wissensseinheiten, die der äußeren Anforderungsbedingung ähnlich sind.
2. Häufigkeitsschätzung ("frequency-gambling"). Wenn die Ähnlichkeitsanpassung zu keinem eindeutigen Ergebnis führt, dann wird die Wissensseinheit bevorzugt, die bislang am häufigsten aktiviert worden ist.

Auch dieser Ansatz ist nicht völlig neu. Bereits WEIMER (1925) ging davon aus, daß sich die Vielzahl der Erscheinungsformen menschlicher Fehler auf eine begrenzte Anzahl "psychischer Wurzeln", die von WEIMER als Fehlerarten bezeichnet werden, zurückführen läßt. Der wesentliche Unterschied zu dem Ansatz von WEIMER besteht in der Terminologie. Die von WEIMER genannte Fehlerart "Ähnlichkeitsfehler" entspricht der von REASON genannten Fehlerform "Ähnlichkeitsanpassung". Das gleiche gilt für den "Geläufigkeitsfehler" (WEIMER) und für die "Häufigkeitsschätzung"

(REASON). Der hier untersuchte Faktor "Ähnlichkeit" hat also eine grundlegende Bedeutung für die Entstehung von Operateurfehlern. Hinweise zur probabilistischen Quantifizierung dieses Faktors sind der Arbeit von REASON (1990) nicht zu entnehmen.

Der Faktor menschliche Risikobereitschaft wird von REASON (1990) nicht explizit als Fehlerursache genannt. Im Zusammenhang mit dem Reaktorunfall von Tschernobyl und dem Führungsglück von Seebrügge nennt REASON (1990, p.194f) jedoch - in Abgrenzung zu den in Tab. 2 genannten Fehlern - den Begriff "Zu widerhandlung" ("violation"). Eine Zu widerhandlung wird von REASON nicht als Fehler ("error") definiert. Die sicherheitswidrige Handlung ("unsafe act") wird von REASON als Oberbegriff für Fehler und Zu widerhandlungen verwendet (s. Abb. 3). REASON nennt in diesem Zusammenhang auch den Begriff "Sicherheitskultur". Er zitiert die UKAEA (1987), die die Meinung vertritt, daß aufgrund der Sicherheitskultur in Großbritannien dort keine Zu widerhandlungen so wie in Tschernobyl auftreten können (REASON 1990, p.213).

UNSAFE ACTS			
UNINTENDED ACTION		INTENDED ACTION	
SLIP *	LAPSE *	MISTAKE *	VIOLATION
↓	↓	↓	↓
Attentional failures Intrusion Omission Reversal Misordering Mistiming	Memory failures Omitting planned items Place-losing Forgetting intentions	Rule-based mistakes Misapplication of good rule Application of bad rule Knowledge-based mistakes Many variable forms	Routine violations Exceptional violations Acts of sabotage

Abb. 3. A Summary of the Psychological Varieties of Unsafe Acts:

* BASIC ERROR TYPE. Quelle: REASON (1990, p.207).

Andere Autoren - insbesondere aus der Arbeits-, Verkehrs- oder Sicherheitspsychologie - gehen ausführlich auf den Faktor Risikobereitschaft (bzw. Konflikt) ein (s. auch Abschnitt 5.2.2). Bereits in älteren Untersuchungen wird der Konflikt zwischen Si-

cherheitstendenz und Leistungstendenz als wesentlicher Faktor der Unfallentstehung hervorgehoben (MITTENECKER 1962). In der Arbeitspsychologie wird dieser Faktor auch als industrielles Risikoverhalten bezeichnet (z.B. HACKER 1980). Es wird betont, daß dieser Faktor einen Hauptbeitrag zur Entstehung von Fehlhandlungen liefert (z.B. VON KLEBELSBERG 1977; WILDE 1978; BURKARDT 1985; UNDEUTSCH 1985; HOYOS/ZIMOLONG 1988). Allerdings gibt es nur unzureichende Erkenntnisse zur quantitativen Erschließung menschlicher Risikobereitschaft (HOYOS/ZIMOLONG 1988, p.101; UNDEUTSCH 1985, S.139). Empirische Wahrscheinlichkeitsdaten sind selten. Verfügbare Daten (z.B. REHHAHN 1973) liegen in sehr undifferenzierter Form vor.

Aus den oben referierten psychologischen Erkenntnissen zu den Faktoren Konflikt und Ähnlichkeit ist keine konkrete Methode zur Einbeziehung der dadurch bedingten Entscheidungsfehler in eine PRA ableitbar. Aktuelle probabilistische Methoden enthalten jedoch Ansätze, mit denen sich zumindest Teilaspekte dieser Faktoren erfassen lassen.

Die Methode HEART ("Human Error Assessment and Reduction Technique"; WILLIAMS 1988) beschränkt sich auf die Quantifizierung bereits identifizierter Operateurfehler. Dem Benutzer werden Punktwerte und Unsicherheitsintervalle zu neun sehr allgemein beschriebenen Aufgaben angeboten. Die Punktwerte liegen zwischen 0.55 (Task: "Totally unfamiliar, performed at speed with no idea of the likely consequences") und 0.00002 (Task: "Respond correctly to system command even when there is an augmented supervisory system providing accurate interpretation of systems state"). Zur Modifizierung einer ausgewählten Fehlerwahrscheinlichkeit werden 38 Faktoren angeboten. Zu jedem Faktor wird eine - teilweise sehr allgemein gehaltene - Beschreibung der fehlererzeugenden Bedingung ("Error Producing Condition" - EPC) gegeben. Die Faktoren liegen zwischen $K=17$ ("Unfamiliarity with a situation which is important but which only occurs infrequently or which is novel") und $K=1.02$ ("Age of personnel performing perceptual tasks"). Der Benutzer hat nun die Aufgabe, die EPCs auszuwählen, die er für relevant hält. Zu jeder ausgewählten EPC ist dann auf einer Skala von 0 bis 1 ein Wert x zu schätzen, der die Stärke des Einflusses in der konkreten Situation angibt. Der multiplikative Effekt einer so bewerteten Bedingung wird dann über den Faktor

$$[1 + (K - 1) x]$$

berücksichtigt.

Einige EPCs betreffen auch Teilaspekte der Faktoren Risikobereitschaft und Ähnlichkeit; z.B. $K=2$ ("An incentive to use other more dangerous procedures") oder

K=4 ("Poor, ambiguous or ill-matched system feedback"). Ein Konzept zur Einbeziehung dieser Faktoren fehlt jedoch.

Etwas konkreter ist die Methode INTENT (GERTMAN u.a. 1992). INTENT spezialisiert sich auf Entscheidungsfehler aufgrund falscher Handlungsabsichten. Dem Benutzer werden hierzu 20 Basisfehler angeboten. Diese Fehler wurden mit Hilfe zweier Computerprogramme aus einer Datenbank und aus der nordamerikanischen Betriebserfahrung identifiziert. Bezüglich der Quellen, die zur Bildung falscher Handlungsabsichten führen, sind diese Fehler in vier Klassen eingeteilt:

1. Vier Fehler aufgrund der Inbetrachtziehung möglicher Handlungsfolgen ("Action sequence"); z.B.: "Tolerate an out of range situation with minor consequence".
2. Vier einstellungsbedingte Umgehungen ("Attitude leading to circumventions"); z.B.: "Violate procedure and device own formuli".
3. Sechs Fehler aufgrund verfestigter Verhaltensmuster ("Crew response set"); z.B.: "Competing goal states leads to a wröng conclusion".
4. Sechs von internen (z.B. Erinnerungsvermögen) und externen (z.B. schriftlichen Unterlagen) Hilfsmitteln abhängige Fehler ("Resource dependencies"); z.B.: "Crews consult inappropriate resources in emergency".

Zu jedem Fehler wird in GERTMAN u.a. (1992) die Untergrenze (UG) und Obergrenze (OG) der Wahrscheinlichkeit genannt; diese Nennungen basieren auf Expertenschätzungen. Außerdem ist ein Satz von 11 Einflußfaktoren (PSFs) verfügbar, deren Gewichte - in Abhängigkeit von dem jeweiligen Fehler - ebenfalls über Expertenschätzungen bestimmt wurden.

Vom Benutzer der Methode INTENT wird nun verlangt, daß er aus den 20 Fehlern den Fehler auswählt, der auf den Entscheidungsfehler zutrifft, für den eine Wahrscheinlichkeit geschätzt werden soll. Danach sind auf einer 5-Punkte-Skala Schätzungen zu den 11 PSFs abzugeben. Unter Berücksichtigung der PSF-Gewichte läßt sich dann aus diesen Schätzungen ein Zuverlässigkeitsindex (SLI) berechnen, der Werte von 0 bis 100 annehmen kann. Das Modell setzt nun voraus, daß die Fehlerwahrscheinlichkeit gleich dem $(100 - \text{SLI})\%$ -Wert der Lognormalverteilung mit UG als 5%- und OG als 95%-Wert ist.

INTENT ist im Prinzip zur Quantizierung von Entscheidungsfehlern geeignet. Es fehlen jedoch klare Hinweise zur Berücksichtigung der Hauptfaktoren Konflikt und Ähnlichkeit. Viele der 11 angebotenen PSFs (z.B. "Procedures") haben keinen direkten Bezug zu diesen Faktoren. Die Anwenderfreundlichkeit von INTENT wird durch die teilweise sehr unscharfen Definitionen zu den 20 Basisfehlern eingeschränkt. Das gleiche gilt für die PSF-Definitionen. PSFs, die Gegenstand separater Forschungsar-

beiten sind (oder sein könnten), werden nicht näher erläutert; z.B. der PSF "Human-Machine-Interface" oder der PSF "Safety Culture".

Auch die Methode CREATE ("Cognitive Reliability Analysis Technique"; WOODS u.a. 1990; WOODS/ROTH 1987) ist vom Prinzip her zur Einbeziehung von Entscheidungsfehlern (aufgrund falscher Absichten) in eine PRA geeignet. Aus dem derzeitigen Entwicklungsstand dieser Methode sind jedoch keine wesentlich neuen Erkenntnisse für die praktische Durchführung einer MMSA ableitbar.

CREATE (WOODS u.a. 1990, ch.5.4) definiert einen Operateurfehler als ein Mißverhältnis aus dem Problemlösungsbedarf (Störfallart, verfügbare Meßwerte über den Systemzustand usw.) und der Problemlösungsfähigkeit (Wissen über die Anlage, bevorzugte Strategie beim Lösen von Problemen usw.). In CREATE wird dieses Mißverhältnis differenziert betrachtet; d.h., zur Einbeziehung von Operateurfehlern in eine PRA werden auch Abweichungen von dem Standardfall ("textbook case") berücksichtigt. Zur probabilistischen Quantifizierung des Problemlösungsbedarfs verweist CREATE auf die Fehlerbaumtechnik (in Verbindung mit entsprechenden Zuverlässigkeitsdaten). Zur Schätzungen der Wahrscheinlichkeiten von Defiziten bei den Problemlösungsfähigkeiten werden nur sehr allgemeine Hinweise gegeben. Als Datenbasis wird THERP empfohlen. Zur Berücksichtigung signifikanter Abweichungen - vom normalen ("textbook case") Verhältnis zwischen Problemlösungsbedarf und Problemlösungsfähigkeit - wird auf Expertenschätzverfahren (z.B. SLIM) verwiesen. Es wird empfohlen, die Expertenschätzungen auf der Grundlage von Operateurbefragungen und Simulatordaten durchzuführen.

Negative Abweichungen vom Standardfall ("textbook case") eines Störfallablaufs werden in CREATE als Komplikationsfaktoren bezeichnet. Zur Identifizierung signifikanter Komplikationsfaktoren wird auf das mit sog. "künstlicher Intelligenz" arbeitende Computerprogramm CES ("Cognitive Environment Simulation"; WOODS u.a. 1990; WOODS u.a. 1988; WOODS u.a. 1987) verwiesen. Dieses Programm befindet sich noch in der Entwicklung. Eine erste Testreihe wurde für den Störfall "Leck im Dampferzeuger (DE)" eines Druckwasserreaktors (DWR) vom Typ "Westinghouse" durchgeführt. Mit CES läßt sich ermitteln, welche sicherheitsrelevanten Handlungsabsichten ein Komplikationsfaktor - der zuvor in das Programm eingegeben wurde - zur Folge haben könnte. Eine konkrete Methode zur Identifizierung der einzugebenden Komplikationsfaktoren wird nicht genannt. Dem Benutzer wird jedoch eine Liste möglicher Komplikationsfaktoren angeboten (Tab. 3). Der dem hier untersuchten Faktor "konfliktbedingte Risikobereitschaft" entsprechende Punkt 7 ist derzeit kein Bestandteil von CES (WOODS u.a. 1987, p.80).

1. Operateurfehler bei der Handlungsausführung.
2. Zusätzliche Komponentenfehler (z.B. festsitzende Ventile).
3. Fehlende Informationen (z.B. Ausfall eines Meßfühlers).
4. Gravierende Mehrfachausfälle (z.B. nicht isolierbares DE-Leck).
5. Situationen, in denen die Entdeckung der wesentlichen Ursache eines Störfalls erschwert wird (z.B. Ausfall wichtiger Anzeigeinstrumente oder Stromausfall vor DE-Leck).
6. Situationen, in denen Reaktionen für möglich gehalten werden könnten, die sich einander widersprechen.
7. Situationen, in denen eine Handlung erforderlich ist, die normalerweise ungewöhnlich ist (z.B. nach Ausfall des Speisewassers).

Tab. 3. Mögliche Komplikationsfaktoren (übersetzt aus WOODS u.a. 1990, p.44)

Da CES zur Vorhersage kritischer Handlungsabsichten die Eingabe von zuvor identifizierten Komplikationsfaktoren benötigt, stellt sich die Frage nach dem Aufwand-Nutzen-Verhältnis. Wenn z.B. ein PRA-Durchführer - aufgrund seiner natürlichen Intelligenz - den Ausfall des Meßfühler X als Komplikationsfaktor identifiziert hat, dann wird er in der Regel auch - ohne Anwendung eines mit künstlicher Intelligenz arbeitenden Computerprogramms - wissen, zu welchen Handlungsabsichten dieser Ausfall führen könnte. Der Zusatznutzen von CES liegt jedoch in der Identifizierung zusätzlicher Handlungsabsichten, die nicht von vornherein bei der Identifizierung eines Komplikationsfaktors sichtbar werden.

Außerdem können mit CES auch Eingaben bezüglich der Problemlösungsfähigkeiten des Personals verarbeitet werden. Der in dem Testbeispiel (WOODS u.a. 1990, ch.4) damit erreichte Erkenntnisgewinn ist allerdings trivial. Ein DE-Heizrohrbruch wurde mit Hilfe von CES simuliert. Für den Standardfall ("textbook case") zeigte der CES-Output, daß das Personal den Störfall sehr schnell diagnostiziert. In einem zweiten Fall wurden Komplikationen bezüglich der Störfallvariante eingegeben; u.a. ein Leck an einer Dichtung der Hauptkühlmittelpumpe. Hier zeigte der CES-Output eine erhöhte Diagnosezeit. In einem dritten Fall wurde zusätzlich noch das Wissensdefizit eingegeben, daß das Personal den - aufgrund des DE-Lecks - fallenden Druckhalter-Pegel auf die Dichtungsleckage an der Hauptkühlmittelpumpe zurückführt. Der CES-Output enthielt in diesem Fall das triviale Ergebnis, daß die Diagnose versagt.

Zur Ermittlung der Wahrscheinlichkeit, daß ein spezifisches Wissensdefizit vorliegt, wird in CREATE keine konkrete Methode genannt. Außerdem wird nicht auf die Schwierigkeiten eingegangen, die sich aufgrund der vielen Kombinationen von Wissensdefiziten ergeben. So könnte z.B. eine Schichtmannschaft Wissensdefizite bezüg-

lich der Systeme A und B aufweisen, die andere bezüglich der Systeme A und C, usw.

Der Wert der Methode CREATE liegt also in erster Linie darin, daß überhaupt versucht wird, über Komplikationsfaktoren Abweichungen vom Standardfall ("textbook case") in eine PRA mit einzubeziehen.

1.3 Aufbau der Arbeit

Die hier entwickelten methodischen Erweiterungen zur Einbeziehung konfliktbedingter Risikobereitschaft und ähnlichkeitsbedingter Erwartungsfehler umfassen drei Phasen: Die Identifizierung (Abschnitt 4.2) von Zielen untergeordneter Sicherheitsbedeutung, die Identifizierung der daraus ableitbaren Rückwirkungen auf die menschliche Zuverlässigkeit (Abschnitt 4.3) sowie deren Modellierung und Quantifizierung in Abschnitt 5.

Die konkrete Anwendung der methodischen Ergebnisse erfolgt am Beispiel eines hypothetischen Störfalls an einem Hochtemperaturreaktor mittlerer Leistung. Als Referenzanlage wird das Reaktorkonzept HTR-500 betrachtet. Zur Verdeutlichung der Auswirkungen der hier entwickelten und angewendeten methodischen Erweiterungen wird im Abschnitt 3 für den HTR-500 eine Analyse gemäß "klassischer" PRA-Zielsetzung durchgeführt. Diese Analyse wird dann im Abschnitt 5.4 durch die Ergebnisse der Abschnitte 4, 5.2 und 5.3 erweitert. Zunächst wird jedoch im Abschnitt 2 am Beispiel eines real aufgetretenen Störfalls im U.S. Kernkraftwerk (KKW) Davis-Besse eine praxisnahe Analyse zum Entscheidungsverhalten nach erfolgter Diagnose durchgeführt.

Jeder der ersten fünf Abschnitte (einschließlich der Einleitung) ist so aufgebaut, daß er als eigenständiger Kurzbericht gelesen werden kann. Die wichtigsten Aussagen und Ergebnisse werden jeweils am Abschnittende zusammengefaßt. Im Abschnitt 6 wird die gesamte Arbeit zusammengefaßt, im Abschnitt 7 werden die daraus abgeleiteten Schlußfolgerungen beschrieben. Der Abschnitt 8 enthält das alphabetisch sortierte Literaturverzeichnis der gesamten Arbeit.

1.4 Zusammenfassung von Abschnitt 1

Zielsetzung der Arbeit ist die Erweiterung der Methodik zur Einbeziehung von Operateurfehlern - auch Mensch-Maschine-Systemanalyse (MMSA) genannt - in eine probabilistische Risikoanalyse (PRA). Die methodischen Erweiterungen konzentrieren sich auf Entscheidungsfehler (nach richtiger Diagnose des Störfalls) aufgrund konfliktbedingter Risikobereitschaft oder ähnlichkeitsbedingter Erwartungsfehler. Die umfassende Berücksichtigung dieser Faktoren trägt signifikant zur Erhöhung der Realitätsnähe einer PRA bei; denn nach den Erkenntnissen der psychologischen Fehlerforschung gelten die Faktoren Konflikt und Ähnlichkeit als Hauptursachen für die Entstehung von Entscheidungsfehlern. Zur Identifizierung der entsprechenden Fehler wird ein neuartiger Ansatz verfolgt. Dieser Ansatz besteht in der Untersuchung möglicher Rückwirkungen, die von Zielen (und Systemzuständen) untergeordneter Sicherheitsbedeutung ausgehen.

Die im PRA-Leitfaden (1983) empfohlene MMSA-Methodik THERP (SWAIN-Handbuch) erlaubt nur eine unzureichende Berücksichtigung von Entscheidungsfehlern. Die Identifizierung konzentriert sich auf Fehler, die zur Nichtausführung notwendiger Handlungen führen und die mit den Daten aus dem SWAIN-Handbuch quantifizierbar sind. Die Daten des SWAIN-Handbuchs erlauben nur eine unzureichende Quantifizierung von Entscheidungsfehlern nach erfolgter Diagnose.

Auch neuere Methoden (z.B. HCR-Modell, CREATE, HEART oder INTENT) liefern keine praktikablen Verfahren zur Einbeziehung der Faktoren Konflikt und Ähnlichkeit. Aus diesen Methoden sind jedoch zwei signifikante Trends bei der Weiterentwicklung der MMSA ableitbar: (1) Berücksichtigung von Zeitabhängigkeiten und (2) Nutzung von Erkenntnissen aus der psychologischen Fehlerforschung (kognitive Psychologie, Sicherheitspsychologie, Arbeitspsychologie o.ä.).

Die hier durchgeführten Arbeiten bauen auf diesen Trends auf. Im Abschnitt 2 wird ein Ansatz vorgestellt, mit dem sich Entscheidungsfehler über den Faktor Zeit in eine MMSA integrieren lassen. In den Abschnitten 4 und 5 wird eine neue Methode vorgestellt, mit der sich - unter Ausnutzung psychologischer Erkenntnisse - die bislang praktizierte "klassische" MMSA-Methodik (Abschnitt 3) erweitern läßt.

2. Reales Beispiel: Der Störfall im KKW Davis-Besse 1985

2.1 Einführung

Am 9. Juni 1985 kam es im Kernkraftwerk (KKW) Davis-Besse zum Ausfall der Haupt- und Notspeisewasserversorgung. Dem Personal gelang es, durch sekundärseitige Maßnahmen die Nachwärmeabfuhr (NWA) wieder herzustellen.

Zu den Maßnahmen des Personals wird hier eine kurze probabilistische Analyse durchgeführt (Abschnitt 2.4), um den Einfluß von Entscheidungen in Konfliktsituationen zu diskutieren. Dabei wird weitgehend von den Randbedingungen ausgegangen, die während des Störfalls vorhanden waren.

Im Abschnitt 2.2 wird das NWA-Konzept der Anlage skizziert, im Abschnitt 2.3 wird der Störfall kurz beschrieben.

Anlagen- und Störfallbeschreibungen wurden der Quelle NRC (1985) entnommen.

2.2 Das NWA-Konzept der Anlage

Das U.S. KKW Davis-Besse hat einen Druckwasserreaktor (DWR) der Bauart "Babcock & Wilcox" mit 906 MWe Leistung. Die im Primärkreis erzeugte Wärme wird über zwei Dampferzeuger (DE) abgeführt. Im Normalbetrieb werden die DE von je einer dampfbetriebenen Hauptspeisewasserpumpe bespeist. Falls beide Pumpen ausfallen, wird automatisch das Notspeisewassersystem gestartet. Dieses System ist auf 2x100% ausgelegt. Jeder DE wird durch eine dampfbetriebene Notspeisewasserpumpe mit ca. 3970 l/min bespeist.

Nach Ausfall des Notspeisewassersystems besteht noch die Möglichkeit eine primärseitige NWA, über Druckentlastung in Verbindung mit Hochdruckeinspeisung (feed + bleed), herzustellen. Diese Maßnahme ist vom Personal einzuleiten. Eine primärseitige NWA führt zu einer Gebäudekontamination, was aufwendige Reinigungsarbeiten erforderlich macht.

2.3 Der Störfall am 9.6.1985

Um 1Uhr35 nachts schaltet sich die Hauptspeisewasserpumpe in Strang 1 (zu Dampferzeuger 1) automatisch wegen Drehzahlüberschreitung ab. Kurz darauf erfolgt

eine Reaktorschnellabschaltung bei 80% Leistung. Wegen des fälschlichen Schließens beider Hauptdampfisolationsventile fällt um 1Uhr41 die zweite Hauptspeisewasserpumpe aus, weil die für den Antrieb erforderliche Dampfversorgung (aufgrund der Ventilfehler) ausbleibt. Beide Dampferzeuger (DE) beginnen nun auszudampfen, weil sie nicht mehr mit Speisewasser versorgt werden.

Der Sekundärteil-Operator (2 Jahre Berufserfahrung) erhält vom Schichtleiter (8 Jahre Berufserfahrung) den Auftrag, das Notspeisewassersystem in Betrieb zu nehmen, obwohl die manuelle Inbetriebnahme nicht erforderlich ist, weil das System über das Kriterium DE-Füllstand automatisch gestartet wird. Während der manuellen Inbetriebnahme tritt ein Verwechslungsfehler auf: Der Sekundärteil-Operator betätigt das Schalterpaar, das bei DE-Lecks zu betätigen ist. Folge: Beide DE werden isoliert, der Dampfdruck der Notspeisewasserpumpenturbinen steigt und die Turbinen schalten sich wegen Drehzahlüberschreitung automatisch ab.

1Uhr41. Die gesamte sekundärseitige NWA ist ausgefallen. Versuche, durch Schalthandlungen in der Warte den Ausfall zu korrigieren, bleiben erfolglos.

Um 1Uhr44 wird damit begonnen, durch sekundärseitige Maßnahmen vor Ort die NWA wieder herzustellen. Der Verlauf dieser Maßnahmen ist in Abb. 4 skizziert; weitere Informationen zum chronologischen Ablauf sind Tab. 4 zu entnehmen. Das folgende Zitat aus dem Untersuchungsbericht der NRC bestätigt die in der Abbildung angedeutete Dramatik:

“Der Primärteil-Operator schickte zwei Operateure in den Notspeisewasserpumpenraum, um zu sehen, was falsch läuft - und er sagte, daß sie sich beeilen sollen. Der Pumpenraum liegt drei Ebenen unterhalb der Warte (...). Einer der Operateure trug den Schlüssel des Pumpenraums bei sich. Sie verletzten die Vorschrift ‘Laufen verboten’ als sie die Treppe hinunter rannten. Der eine Operateur hatte gegenüber dem anderen (mit dem Schlüssel) ca. 10 Fuß Vorsprung; dieser warf seinem Kollegen den Schlüssel zu, damit keine Verspätung entsteht.”

(übersetzt aus NRC 1985, p.3-7)

Zwei weitere Operateure laufen zu den DE-Isolationsventilen, die aufgrund des Verwechslungsfehlers fälschlich geschlossen wurden. Es gelingt ihnen, um 1Uhr48 Ventil 1 (an DE 1) und um 1Uhr49 Ventil 2 (an DE 2) zu öffnen.

Um 1Uhr44 entscheidet sich der stellvertretende Schichtleiter für die Inbetriebnahme einer zur Zeit nicht startbereiten Elektro-Pumpe. Er schließt diese Pumpe innerhalb von 4 min an das System an. Um 1Uhr51 bespeist die Pumpe den DE 1, dessen Bespeisung um 1Uhr35 ausgefallen war. Diese Pumpe hat zwar mit 568 l/min Durchsatz keine ausreichende NWA-Kapazität, aber sie kann in dem DE den Dampfdruck (1000 psig) erzeugen, der zum Start der Turbine der Notspeisewasserpumpe erforderlich ist. Außerdem ist es durch diese Pumpe möglich, daß auch noch in der Zeit zwischen 20 und 30 min nach NWA-Ausfall die primärseitigen Maßnahmen erfolgreich beendet werden können. Sonst liegt die Zeitgrenze bei 20 min (vgl. NRC 1985, ch.7).

Um 1Uhr49 trifft der Schichtleiter eine Entscheidung, die von der NRC als Fehlverhalten bewertet wird. Zu diesem Zeitpunkt ist laut Vorschrift die primärseitige NWA einzuleiten. Der Betriebsleiter (telefonisch) und der Sekundärteil-Operator empfehlen die Einleitung dieser Maßnahme. Die Erkennbarkeit des in der Prozedur vorgeschriebenen Kriteriums,

DE-Druck unter 960 psig und fallend

oder

DE-Füllstand unter 8 inch,

zur Einleitung der primärseitigen NWA wird dadurch erschwert, daß die Druckanzeige keinen Trendmelder hat und daß die Füllstandanzeige kein genaues Ablesen von 8 inch erlaubt.

Auch ca. 4 min nach dem Anforderungszeitpunkt der primärseitigen NWA unternimmt der Schichtleiter nichts in der Richtung.

Schließlich gelingt um 1Uhr53 den Operateuren im Pumpenraum das Öffnen des Abschalt-drosselventils an der 2. Pumpenturbine. Der Dampfdruck (ca. 950 psig) reicht aus, um die Pumpe zu starten: DE 2 ist wiederbespeist, die NWA ist sekundärseitig wieder hergestellt. Die primärseitige NWA ist nicht mehr nötig.

In einem späteren Interview sagt der Schichtleiter zu seiner Entscheidung in Bezug auf das Einleiten der Maßnahme feed + bleed:

“Nun, das ist ein ganz schön drastischer Schritt, und ich wollte warten bis ich -- nun, ich wollte es nicht frühzeitig tun. Ich wollte bis zu dem Punkt warten, an dem die Prozedur es vorschreibt.”

(übersetzt aus NRC 1985, p.6-3)

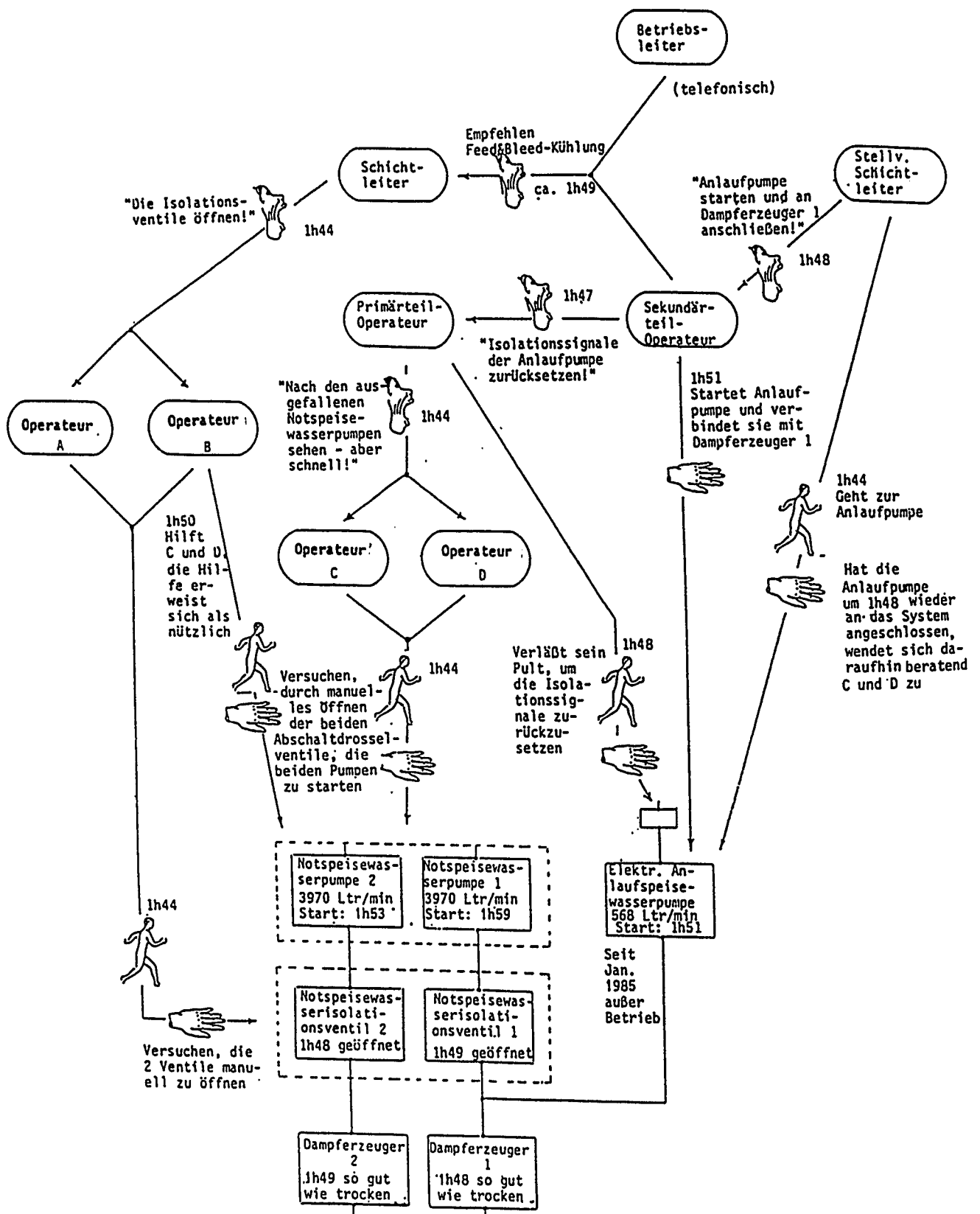


Abb. 4. Störfall im KKW Davis-Besse 1985. Sekundärseitige Maßnahmen

-05:00	KKW Davis-Besse, 9.6.1985, 1Uhr35 nachts. Ausfall einer Hauptspeisewasserpumpe (Sekundärkreis) wegen Drehzahlüberschreitung.
-04:30	Reaktor- und Turbinenschnellabschaltung bei 80% Leistung.
00:00	Ausfall der zweiten Hauptspeisewasserpumpe wegen fehlender Dampfversorgung. Die im Primärkreis nuklear erzeugte Nachwärme wird nicht mehr abgeführt, weil beide Dampferzeuger (DE) (sekundärseitig) nicht mehr bespeist werden. 141 bar und 290 °C im Primärkreis. In ca. 20 min ist mit einem Sieden (bei 328 °C) des Primärkühlmittels zu rechnen.
01:41	Ausfall Notspeisewasser (Sekundärkreis) wegen des fälschlichen Schließens bei der DE-Isolationsventile.
04:00	5 der 8 Operateure beginnen damit, durch Handmaßnahmen vor Ort die (sekundärseitige) DE-Bespeisung wieder herzustellen.
08:49	Das Abblaseventil (am Druckhalter des Primärkreis) öffnet bei 168 bar und schließt 3 sec später.
08:51	Druck in beiden DE unter 66.2 bar und fallend. (Kriterium für das Einleiten der primärseitigen Hochdruckeinspeisung "feed" und Druckentlastung "bleed".)
10:09	Abblaseventil öffnet das zweitemal bei 168 bar und schließt 3 sec später.
11:09	Eine vor 3 min an das System angeschlossene E-Pumpe bespeist mit ca. 568 l/min einen DE - entspricht 14% der Leistung einer Notspeisewasserpumpe.
11:08	Abblaseventil öffnet das drittemal bei 168 bar und 300 °C, schließt aber nicht wieder.
11:42	148 bar und 308 °C. Der Primärkühlmittelverlust über das offene Abblaseventil wird durch Schließen (per Handmaßnahme) des Abblaseabsperrentils beendet.
13:22	Notspeisewasser (3970 l/min) in einem DE verfügbar.

Tab. 4. Der Störfall im KKW Davis-Besse. Die Zeit (min) bis zur Wiederherstellung der DE-Bespeisung: erstellt nach NRC (1985)

2.4 Probabilistische Analyse der Operateurmaßnahmen

2.4.1 Dynamische Analyseverfahren für Operateurhandlungen (DAO)

Die probabilistische Quantifizierung der Personalhandlungen nach NWA-Ausfall (1Uhr41) erfolgt zeitabhängig. Es wird die in REER beschriebene "Dynamische Analyseverfahren für Operateuraktionen (DAO)" angewendet. Diese Methode wurde in der 1990 begonnenen PRA des Jülicher Forschungsreaktors FRJ-2 (DIDO) erstmals angewendet.

2.4.1.1 Fehlermodell

Das Modell erweitert das THERP-Modell (SWAIN 1983) dadurch, daß zur Quantifizierung von Operateurfehlern nach erfolgter Diagnose zusätzlich die Verteilungsfunktionen $Q_i(t)$, $i=0...n$, als Eingangsgrößen verwendet werden, wobei n die Anzahl der möglichen zeitunabhängigen Fehler nach erfolgter Diagnose ist (siehe unten).

Die Verteilungsfunktion $Q(t)$ einer Zufallsgröße T gibt die Wahrscheinlichkeit an, daß T kleiner als t ist:

$$Q(t) = w(T < t),$$

t durchläuft dabei alle Werte der positiven reellen Zahlengeraden (von 0 bis ∞).

Wenn T z.B. eine Lebensdauer ist, dann ist $Q(t)$ die Ausfallwahrscheinlichkeit.

Hier ist T (als Zufallsvariable) eine Durchführungszeit. Deshalb ist $Q(t)$ die Erfolgswahrscheinlichkeit und

$$P(t) = 1 - Q(t) = w(T \geq t)$$

die (zeitabhängige) Fehlerwahrscheinlichkeit.

$Q_0(t)$ ist die Verteilung der Durchführungszeit der Gesamthandlung (nach erfolgter Diagnose) unter der Bedingung, daß kein zeitunabhängiger Fehler auftritt. $Q_i(t)$, $i \geq 1$, ist die Verteilung unter der Bedingung, daß der zeitunabhängige Fehler ZUF_i auftritt. Für die gesamte Fehlerwahrscheinlichkeit gilt demnach:

$$F(t) = P_0(t) + [1 - P_0(t)] \left\{ 1 - \prod_{i=1}^n [1 - w(ZUF_i) P_i(t)] \right\}$$

$$\simeq P_0(t) + \sum_{i=1}^n [w(ZUF_i) P_i(t)]$$

mit

$$P_0(t) = 1 - Q_0(t) = w(T|OZUF \geq t),$$

$$P_i(t) = 1 - Q_i(t) = w(T|ZUF_i \geq t),$$

$w(ZUF_i)$ = Wahrscheinlichkeit für den zeitunabhängigen Fehler ZUF_i ,

$T|OZUF$ = Durchführungszeit, wenn kein zeitunabhängiger Fehler auftritt,

$T|ZUF_i$ = $T|OZUF + K_i$ = Durchführungszeit, wenn ZUF_i ,

K_i = Korrekturzeit für ZUF_i ,

t = verfügbare Zeit,

n = Anzahl der identifizierten zeitunabhängigen Fehler, die zum Versagen der Gesamthandlung führen.

Zeitunabhängige Fehler (ZUF_i , $i=1\dots n$) beziehen sich auf die Teilhandlungen einer entsprechend der Methode THERP zerlegten Gesamthandlung. Die Eigenschaft "zeitunabhängig" bezieht sich nur auf die direkte Definition des Fehlerkriteriums, z.B. das Auslassen einer Teilhandlung. Diese Eigenschaft bezieht sich nicht auf indirekte Einflüsse, wie z.B. Stress aufgrund von Zeitdruck.

Dagegen gelten die zeitabhängigen Fehler ($T|OZUF \geq t$, $T|ZUF_i \geq t$, $i=1\dots n$) für die Gesamthandlung. Auch hier bezieht sich die Eigenschaft "zeitabhängig" auf das ei-

gentliche Fehlerkriterium ($T \geq t$), nämlich, daß die Gesamthandlung nicht innerhalb der verfügbaren Zeit durchgeführt wird.

Im Vergleich zum SWAIN-Modell,

$$F = 1 - \prod_{i=1}^n [1 - w(ZUF_i)] \approx \sum_{i=1}^n w(ZUF_i),$$

erhält man also mit $P_0(t)$ eine zusätzliche Fehlerursache und mit $P_i(t)$, $i=1\dots n$, zusätzliche Korrekturfaktoren für die zeitunabhängigen Fehler, wie z.B. Unterlassungs-, Verwechslungs- oder Ablesefehler (vgl. Tab. 1 auf Seite 10).

2.4.1.2 Eingangsgrößen und Rechenprogramme

Das oben beschriebene Modell hat die zeitunabhängigen Eingangsgrößen $w(ZUF_i)$, $i=1\dots n$, (Fehlerwahrscheinlichkeiten) und die zeitabhängigen Eingangsgrößen $Q_i(t)$, $i=0\dots n$, (Verteilungen). Die zeitunabhängigen Größen können mit Hilfe der Fehlerwahrscheinlichkeiten aus dem SWAIN-Handbuch bestimmt werden.

Zur Schätzung der jeweiligen zeitabhängigen Verteilung wird die entsprechende Gesamthandlung in überschaubare Teilschritte zerlegt. Zu jedem Schritt werden zwei Schätzungen benötigt:

1. Kognitives Niveau (nach RASMUSSEN 1979): Schwierigkeitsgrad der Teilaufgabe bzw. zur Durchführung erforderlicher Kenntnisbedarf in den Abstufungen
SKILL: klein, durch gut eingeübte Tätigkeiten durchführbar,
RULE: mittel, durch Anwendung bekannter Regeln durchführbar,
KNOWLEDGE: hoch, durch umfangreiches Nachdenken (Kombinieren) durchführbar.
Je höher das kognitive Niveau, desto mehr Schritte werden (von der Erkennung bis zur Handlungsausführung) in dem Leitermodell in Abb. 9 benötigt.
2. Eine Punktschätzung für den Zeitbedarf:
Mindestzeit T_0 : kleinste Zeit, die zur Durchführung benötigt wird (= größte Zeit mit 100% Fehlerwahrscheinlichkeit) ODER
Medianzeit T_{50} : Zeit mit 50% Fehlerwahrscheinlichkeit.

Aus den Daten des HCR-Modells (vgl. HANNAMAN/WORLEDGE 1988, p.246) lassen sich weitere Quantile der Durchführungszeit berechnen:

$$T_0 = 0.5 T_{50}, T_{95} = 3.62 T_{50} \quad (\text{knowledge})$$

$$T_0 = 0.6 T_{50}, T_{95} = 2.63 T_{50} \quad (\text{rule})$$

$$T_0 = 0.7 T_{50}, T_{95} = 1.72 T_{50} \quad (\text{skill})$$

Die Quantile werden durch eine dreiparametrische Lognormalverteilung,

$$Q(t) = \Phi[(\ln(t - T_0) - \mu)/\sigma],$$

angenähert, mit

$$\mu = \ln(T_{50} - T_0)$$

und

$$\sigma = \{\ln[(T_{95} - T_0)/(T_{50} - T_0)]\}/1.645.$$

Für Erwartungswert und Varianz gilt:

$$EW = T_0 + \exp(\mu + \sigma^2/2)$$

$$VAR = STD^2 = [\exp(\sigma^2) - 1] \exp(2\mu + \sigma^2)$$

Im Vergleich zum HCR-Modell (HANNAMAN u.a. 1984) weist diese Vorgehensweise folgende Besonderheit auf: Durch die mögliche Verwendung von T_0 -Werten (Mindestzeiten) kann eine Wahrscheinlichkeit berechnet werden, deren Wert nur von deterministischen Eingaben abhängt. Dagegen sind die vom HCR-Modell verlangten T_{50} -Werte probabilistischer Natur, weil darin die probabilistische Aussage enthalten ist, daß der Wert mit der Wahrscheinlichkeit 0.50 unterschritten wird. Der vom kognitiven Niveau abhängige Quotient T_0/T_{50} (knowledge: 0.5; rule: 0.6; skill: 0.7) stellt die "Verbindung" zwischen Deterministik und Probabilistik her.

Zur Verknüpfung der einzelnen Schritte (z.B. A und B) einer Gesamthandlung sind folgende, in REER näher beschriebene Rechenprogramme verfügbar:

1. AVORB (Abb. 5):

B beginnt erst, wenn A beendet ist; A und B sind erforderlich (der häufigste Fall).

Für die Gesamthandlung gilt:

$$T_0 = T_0(A) + T_0(B), EW = EW(A) + EW(B), VAR = VAR(A) + VAR(B).$$

Die Parameter T_0 , EW und VAR werden durch eine dreiparametrische Lognormalverteilung angenähert.

2. AUNDB (Abb. 6):

Gleichzeitiger Beginn, A und B erforderlich.

Per Simulation wird n-mal $\text{MAX}(\text{TA}, \text{TB})$ bestimmt und diese n Werte werden durch eine dreiparametrische Lognormalverteilung angenähert.

3. AODERB (Abb. 7):

Gleichzeitiger Beginn, A oder B erforderlich.

Per Simulation wird n-mal $\text{MIN}(\text{TA}, \text{TB})$ bestimmt und diese n Werte werden durch eine dreiparametrische Lognormalverteilung angenähert.

4. ATXB (Abb. 8):

B beginnt erst, wenn A beendet ist, jedoch frühestens zu einem fest vorgegebenen Zeitpunkt TX.

Über folgende Bedingungsgleichung wird per Simulation n-mal die gesamte Durchführungszeit T bestimmt:

$$T = TX + TB \mid TA < TX, \quad T = TA + TB \mid TA \geq TX.$$

Diese n Werte (für T) werden dann durch eine dreiparametrische Lognormalverteilung angenähert.

Alle Verknüpfungsregeln setzen voraus, daß die Durchführungszeiten (TA und TB) der Teilhandlungen voneinander unabhängig sind.

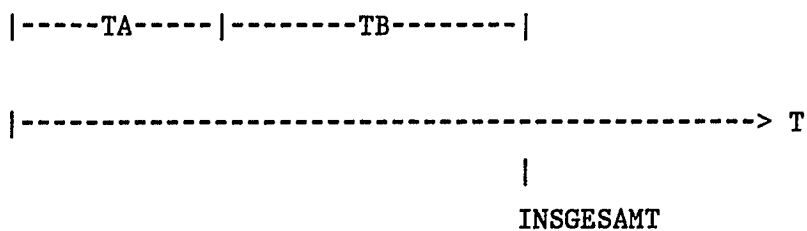


Abb. 5. Dynamische Handlungsstruktur: Erst A, dann B

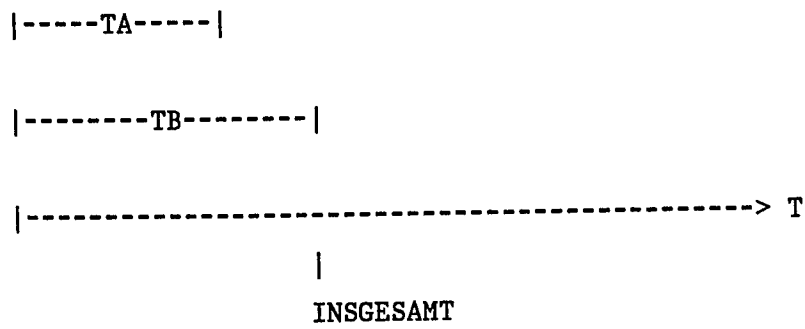


Abb. 6. Dynamische Handlungsstruktur: A und B

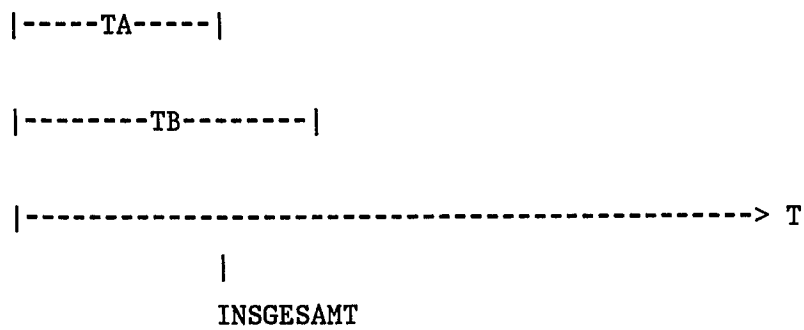
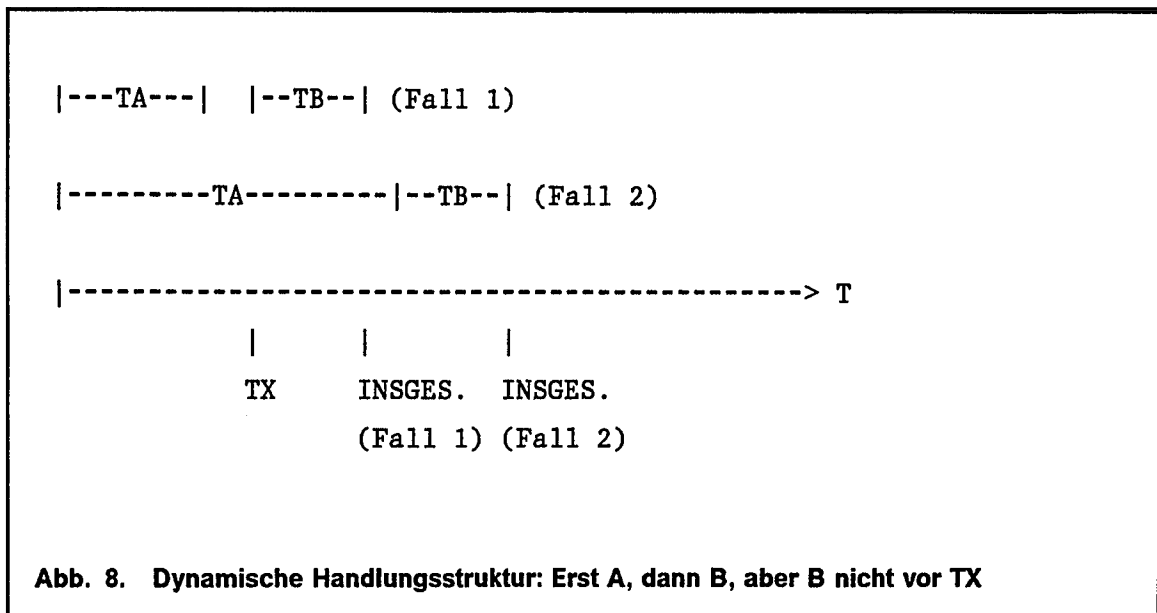


Abb. 7. Dynamische Handlungsstruktur: A oder B



Es kann nicht nachgewiesen werden, ob das hier angesetzte Lognormalverteilungsgesetz auch in Bereichen kleiner zeitabhängiger Fehlerwahrscheinlichkeiten $P(t)$, $t \rightarrow \infty$, gültig ist. Deshalb wird hier empfohlen, Fehlerwahrscheinlichkeiten, die unterhalb einer festzulegenden Grenze, $P^* = P(t^*)$, liegen, über die Obergrenze der Tschebyscheff-Ungleichung zu berechnen:

$$P(t) \leq \text{STD}^2 / (t - \text{EW})^2$$

mit

EW = Erwartungswert der Durchführungszeit T,

STD = Standardabweichung der Durchführungszeit T.

Diese obere Abschätzung gilt - unabhängig vom Verteilungstyp - für jede Zufallsgröße mit dem Erwartungswert EW und der Standardabweichung STD. Zur Gewährleistung eines stetigen Übergangs zwischen $P(t) > P^*$ und $P(t) < P^*$ ist es sinnvoll, unterhalb P^* liegende Werte für $P(t)$ über folgende obere Abschätzung zu berechnen:

$$P(t) \leq \text{STD}^2 / (t - t^* + t^{**} - \text{EW})^2$$

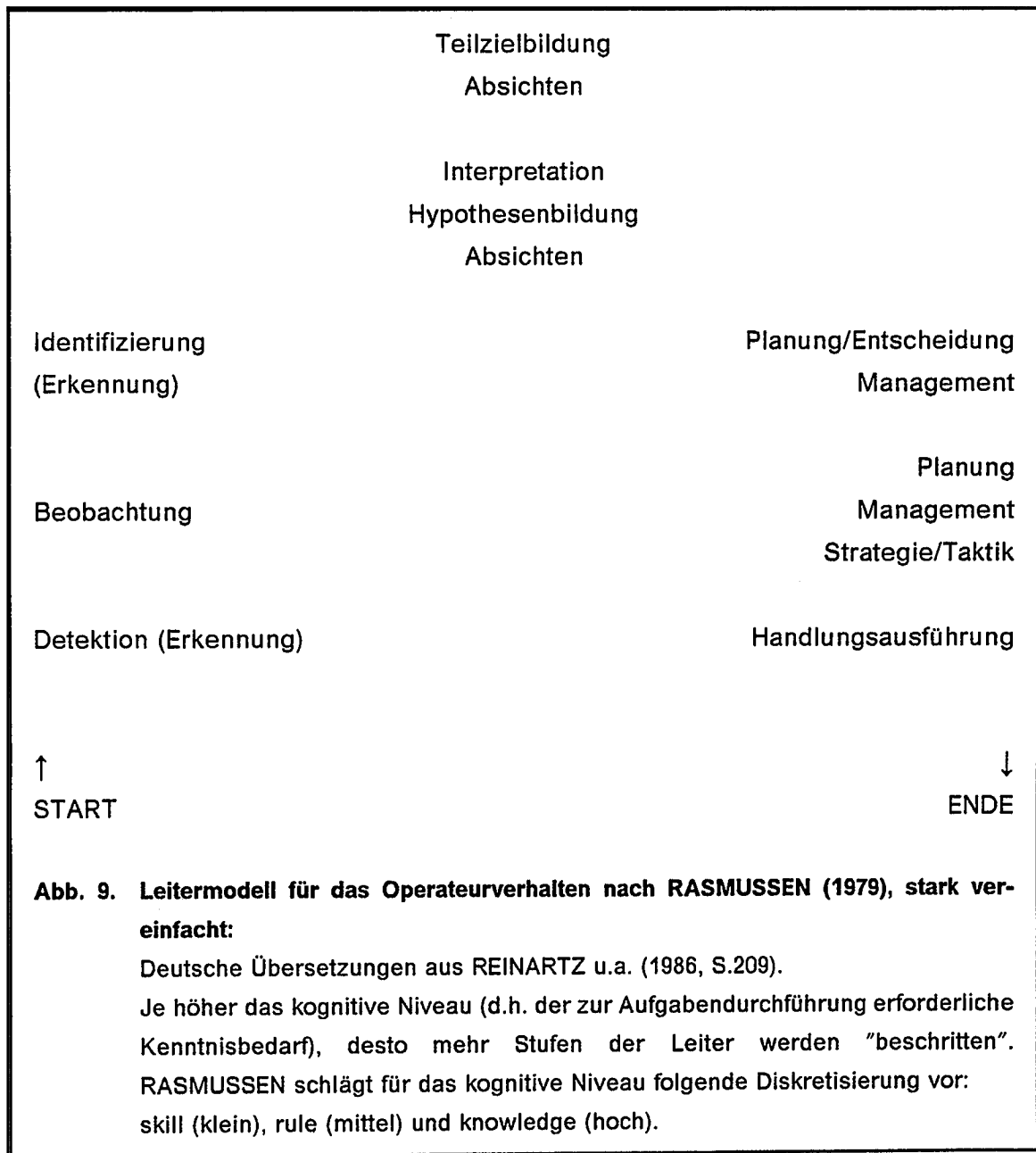
mit

$$t^{**} = \text{EW} + (P^*)^{-0.5} \text{STD},$$

$$t^* = (1 - P^*) \cdot 100\% \text{-Wert der dreiparametrischen Lognormalverteilung (s.o.).}$$

Im Vergleich zum HCR-Modell (HANNAMAN u.a. 1984) hat die Methode zwei wesentliche Vorzüge:

- Die als Eingangsdaten benötigten Schätzungen werden nicht für die Gesamthandlung, sondern für überschaubare Teilschritte angegeben. Dadurch sinkt die Anforderung an das Beurteilungsvermögen des Schätzers.
- Mit den o.g. Rechenprogrammen ist praktisch jede Struktur eines Handlungsablaufs modellierbar.



2.4.1.3 Konfliktmodellierung

Die oben beschriebene Methode hat den Vorteil, daß Konflikte in schwierigen Entscheidungssituationen - die zu passiven Fehlverhalten (Unterlassung der vorgeschriebenen Aufgabe) führen können - als Zeitverzögerungen modelliert werden können (Abschnitt 2.4.4). Diese Art der Berücksichtigung von Konflikten wird hier als t-Modell bezeichnet - im Gegensatz zum p-Modell, das Konflikte durch Wahrscheinlichkeiten für Fehlverhalten modelliert. Zur Anwendung benötigt man Daten über

Zeitverzögerungen in schwierigen Entscheidungssituationen. Da diese Daten nur in seltensten Fällen verfügbar sein werden, ist man auf Schätzungen angewiesen.

Die empirische Aussagekraft der im Fall Davis-Besse beobachteten Zeitverzögerung (4 min) bzgl. des Einleitens von feed + bleed wird durch die folgenden zwei Punkte beeinträchtigt:

- Die Zeitverzögerung wurde nicht durch das Einleiten von feed + bleed beendet, sondern durch den Erfolg der sekundärseitigen Maßnahmen.
- Es gab ergonomische Probleme bei der Erkennbarkeit des Kriteriums für die Einleitung von feed + bleed.

2.4.2 Annahmen zur dynamischen Modellierung

Die richtige Diagnose des Störfalltyps wird vorausgesetzt. Es wird der gleiche NWA-Ausfallzustand angenommen, der während des o.g. Störfalls auftrat. Daher wird auch von den gleichen Personalhandlungen ausgegangen, die zur Wiederherstellung der NWA erforderlich sind. Dies ist im Vergleich zu einer allgemein gültigen Analyse optimistisch, da in diesem konkreten Fall die sekundärseitigen Maßnahmen einen relativ kleinen Zeitbedarf hatten.

Außerdem wird hier der Einfachheit halber nur die "reine" Zeitabhängigkeit modelliert. Die zeitunabhängigen Fehler werden also vernachlässigt:

$$w(\text{ZUF}_i) \simeq 0 \quad \text{für alle } i = 1 \dots n$$

2.4.3 Erfolgskriterien

Die Erfolgskriterien für die Wiederherstellung der NWA nach Ausfall der DE-Bespeisung sind in Tab. 5 zusammengestellt. Die Kriterien 1, 3 und 4 wurden der Quelle NRC (1985, ch.7) entnommen. Das Kriterium 2 wurde ergänzt, weil die Versagensursache von Kriterium 1, Dampfdruck unter 1000 psig, nicht mehr gilt, wenn die Elektro-Pumpe einen DE bespeist.

Der Siedebeginn liegt bei ca. 20 min.

- | | |
|----|---|
| 1. | (A) Start einer Notspeisewasserpumpe innerhalb 10 min |
| | ODER |
| 2. | (A) Start einer Notspeisewasserpumpe UND
(C) Start der Elektro-Pumpe
innerhalb 30 min |
| | ODER |
| 3. | (B) Einleiten von feed + bleed innerhalb 20 min |
| | ODER |
| 4. | (B) Einleiten von feed + bleed UND
(C) Start der Elektro-Pumpe
innerhalb 30 min |

Tab. 5. KKW Davis-Besse. NWA-Erfolgskriterien nach Ausfall der DE-Bespeisung

2.4.4 Zeitbedarfsanalyse und Konfliktberücksichtigung

Das jeweilige Erfolgskriterium für die in Tab. 5 genannten Handlungen A, B und C ist die Durchführung des jeweils letzten Schritts. In Tab. 6 bis Tab. 8 sind die einzelnen Schritte aufgeführt. Die Erstellung der Schritte für die Handlungen A und C basierte auf den störfallspezifischen Randbedingungen. Die Schritte für B wurden der Quelle NRC (1985, ch.4.5) entnommen. Es wird angenommen, daß mit Handlung B erst nach 10 min begonnen wird. Für Handlung B wird in dieser Modellierung also von folgender einfacher Regel ausgegangen: Wenn innerhalb 10 min kein Notspeisewasser, dann feed + bleed einleiten. Von Handlung B wurden hier die Schritte 1, mit feed + bleed-Prozedur beginnen, und 4, den Primärkreis öffnen, als kritisch eingestuft. Zu diesen kritischen Schritten wurde eine Empfindlichkeitsbetrachtung bezüglich ihres Zeit- und Kenntnisbedarfs durchgeführt:

(I) Das Personal sieht keinen Konflikt: Die Schritte werden ohne signifikante Verzögerung durchgeführt (Mindestzeit 1 bzw. 0.5 min, regelbasiertes Verhalten).

(II) Das Personal nimmt diese Schritte als Entscheidungsproblem wahr (Konflikt) und denkt im Mittel 5 min darüber nach (wissensbasiertes Verhalten).

Aufgrund von Verhaltensweise II steigt der mittlere Zeitbedarf (T50 ab Anforderung) für die Einleitung von feed + bleed von
 $13.7 - 10 = 3.7$ (Verhaltensweise I)

auf

$22.3 - 10 = 12.3$ (Verhaltensweise II)

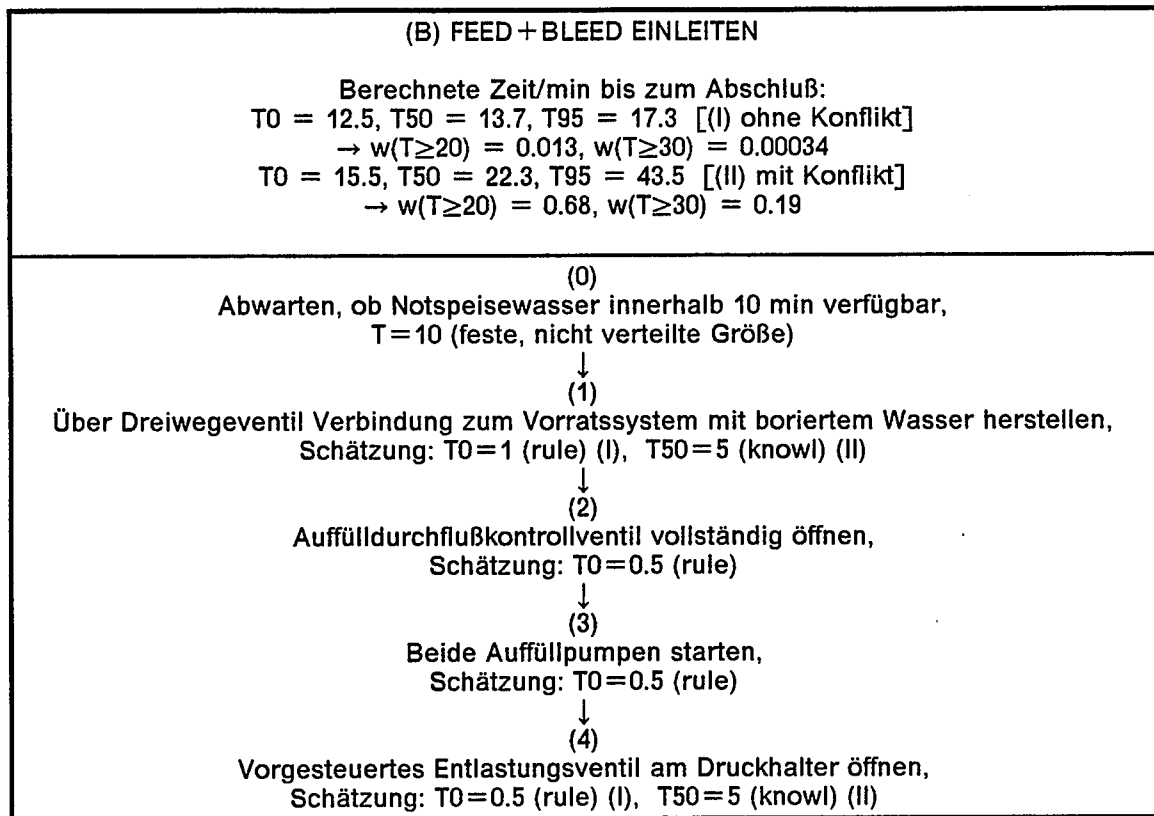
(s. Tab. 7).

Im nächsten Abschnitt werden die Ergebnisse der Zeitbedarfsanalyse probabilistisch ausgewertet.

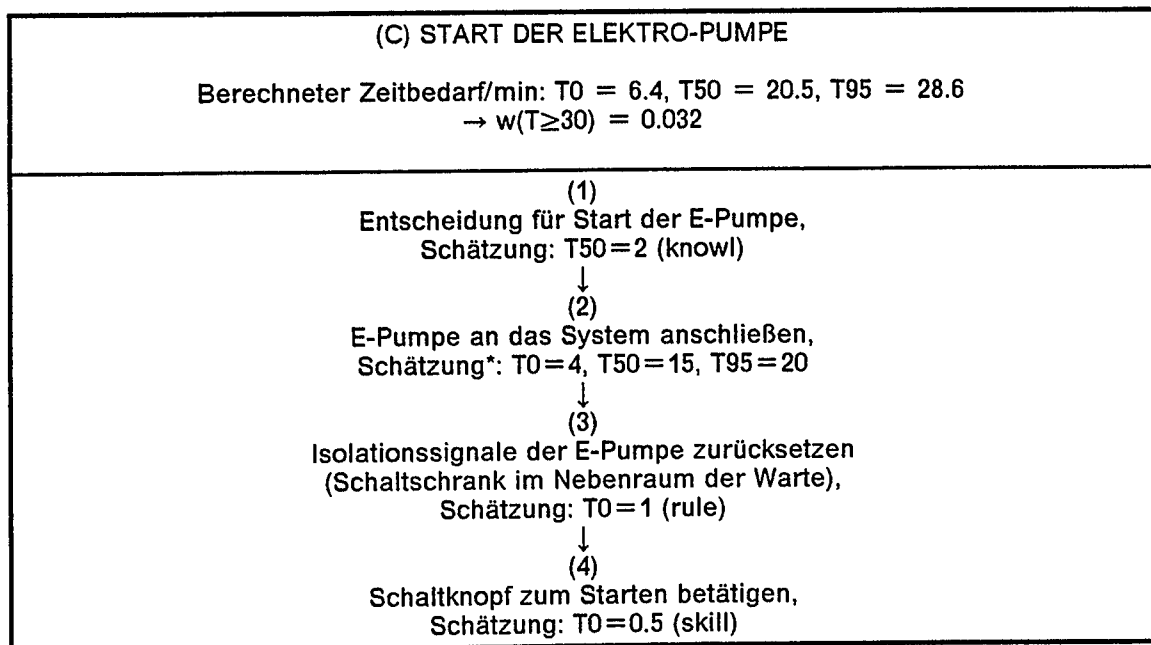
(A) NOTSPEISEWASSERPUMPE STARTEN berechneter Zeitbedarf/min: $T_0 = 6$, $T_{50} = 11.2$, $T_{95} = 24.1$ $\rightarrow w(T \geq 10) = 0.64$, $w(T \geq 30) = 0.022$	
(1) Entscheidung für Maßnahmen vor Ort, Schätzung: $T_0 = 1$ (knowl) ↓	
(2)-(5) DE-Isolationsventil und Abschaltdrosselventil an mindestens einem Strang öffnen, berechneter Zeitbedarf/min: $T_0 = 5$, $T_{50} = 8.5$, $T_{95} = 19.5$	
(2)-(3) Isolationsventil öffnen, berechneter Zeitbedarf/min: $T_0 = 2$, $T_{50} = 3.2$, $T_{95} = 6.3$	(4)-(5) Drosselventil öffnen, berechneter Zeitbedarf/min: $T_0 = 5$, $T_{50} = 8.1$, $T_{95} = 17.1$
(2) Zu dem Isolationsventil hinlaufen, Schätzung: $T_0 = 1$ (skill) ↓ (3) Handrad betätigen, Schätzung: $T_0 = 1$ (rule)	(4) Zu dem Drosselventil hinlaufen, Schätzung: $T_0 = 2$ (skill) ↓ (5) Handrad betätigen, Schätzung: $T_0 = 3$ (rule)

Tab. 6. Zeitbedarfsanalyse für den Start einer Notspeisewasserpumpe:

Die Schritte 2 und 3 können gleichzeitig mit den Schritten 4 und 5 durchgeführt werden, da genügend Personal vorhanden ist.



Tab. 7. Zeitbedarfsanalyse für das Einleiten von feed + bleed



Tab. 8. Zeitbedarfsanalyse für den Start der Elektro-Pumpe:

* Informationsbasis: 15 min bis 20 min sind vorgesehen, der stellvertretende Schichtleiter benötigte 4 min (NRC 1985, p.3-8)

2.4.5 Ereignisbaumanalyse und Ergebniszusammenfassung

Wenn alle Erfolgskriterien (Tab. 5) versagen, dann tritt Kernschmelzen (KS) ein. Wenn die sekundärseitigen Maßnahmen versagen, dann ergibt sich eine NWA mit Gebäudekontamination (G). Es kann also von dem in Abb. 10 dargestellten Ereignisbaum ausgegangen werden. Nach Auswertung des Ereignisbaumes erhält man somit folgende Wahrscheinlichkeit für Kernschmelzen (aufgrund von Zeitfehlern) (Zeitlimits in min):

$$w(KS) = w(TA \geq 10) w(TB \geq 20) w(TC \geq 30) + [1 - w(TC \geq 30)] w(TA \geq 30) w(TB \geq 30)$$

Es wird vorausgesetzt, daß die Durchführungszeiten TA (Notspeisewasserpumpe starten), TB (feed + bleed einleiten) und TC (E-Pumpe starten) voneinander unabhängig sind.

Die für die o.g. Gleichung benötigten Wahrscheinlichkeiten wurden im letzten Abschnitt bestimmt (Tab. 6 bis Tab. 8). Man erhält somit:

$$w(KS) \simeq 0.0205 w(TB \geq 20) + 0.021 w(TB \geq 30)$$

$$= 2.7E-4 \quad [(I) \text{ ohne Konflikt}]$$

$$= 1.8E-2 \quad [(II) \text{ mit Konflikt}]$$

Die Konfliktmodellierung mit der hier unterstellten Erscheinungsform, zögerliches Verhalten, bewirkt also eine Erhöhung der Kernschmelzwahrscheinlichkeit um den Faktor 67.

Dieses Verhalten hat aber auch einen positiven Effekt. Für die Wahrscheinlichkeit einer sekundärseitigen NWA, d.h. ohne Gebäudekontamination, gilt:

$$w(0) = 1 - w(TA \geq 10) + [w(TA \geq 10) - w(TA \geq 30)] [1 - w(TC \geq 30)] w(TB \geq 20)$$

$$\simeq 0.36 + 0.6 w(TB \geq 20)$$

$$= 0.37 \quad [(I) \text{ ohne Konflikt}]$$

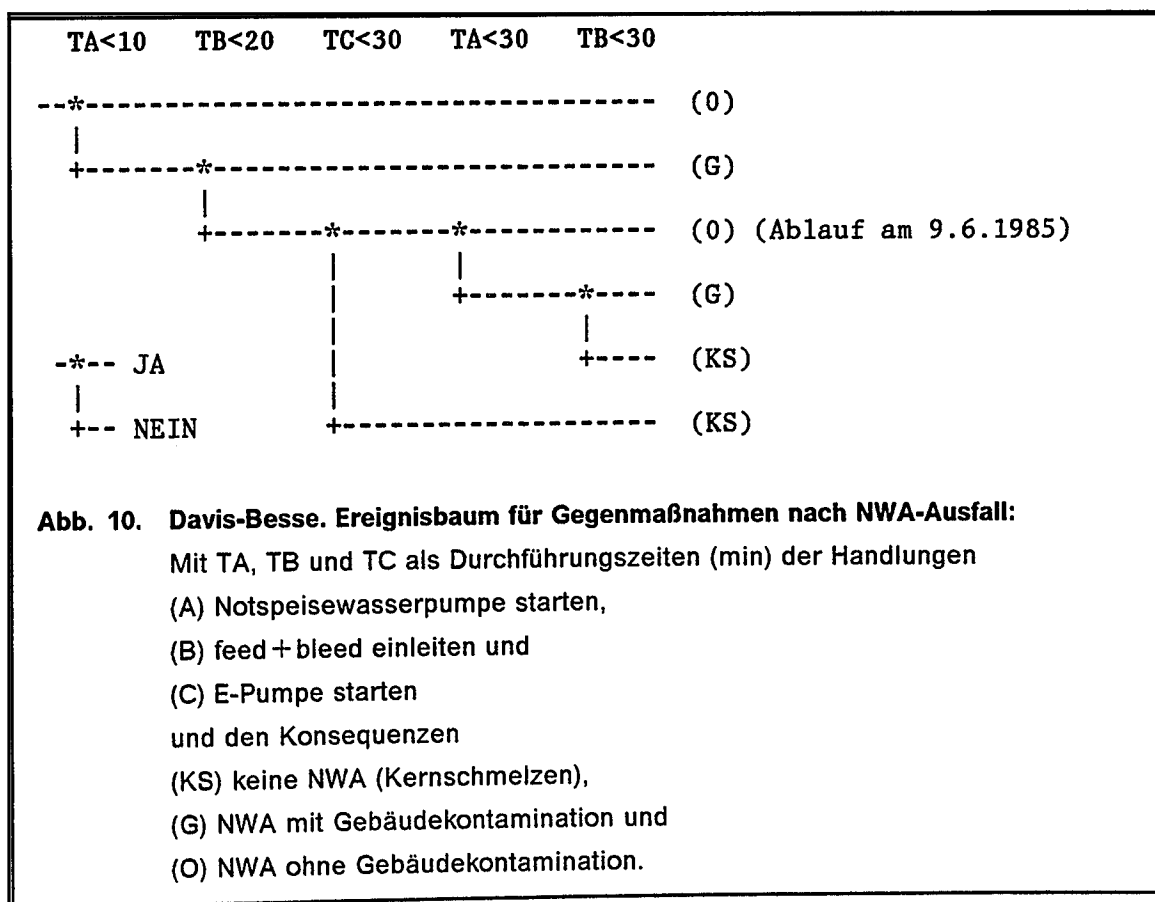
$$= 0.77 \quad [(II) \text{ mit Konflikt}]$$

Das zögerliche Verhalten bewirkt also, daß sich die Wahrscheinlichkeit einer NWA ohne Gebäudekontamination ca. um den Faktor 2 erhöht. Dieser Effekt hat - im Ver-

gleich zu dem o.g. negativen Effekt - noch zwei weitere positive Aspekte (aus psychologischer Sicht):

- Er bewegt sich in einem wahrnehmbaren (d.h. nicht hypothetischen) Wahrscheinlichkeitsbereich.
- Er betrifft keinen unerwünschten Schaden, sondern ein erwünschtes Erfolgsergebnis.

Der qualitative Trend der hier berechneten Wahrscheinlichkeiten deutet daraufhin, daß sich der Schichtleiter im KKW Davis-Besse am 9.6.1985 von 1Uhr49 bis 1Uhr53 (nachts) in einer Konfliktsituation befand. Ob er diese Situation als Konflikt wahrgenommen hatte, kann hier nicht gesagt werden.



2.5 Zusammenfassung von Abschnitt 2

Am 9.6.1985 kam es im 906-MWe-DWR Davis-Besse (USA) aufgrund zweier technischer Fehler und eines Bedienungsfehlers zum Ausfall der Haupt- und Notspeisewasserversorgung.

Ohne weitere Gegenmaßnahmen des Personals führt ein solcher Ausfall zum Hochdruckkernschmelzen. Dem Personal stehen sekundärseitige (Dampferzeugerbespeisung) und primärseitige (Primärkreisdruckentlastung und -hochdruckeinspeisung, kurz: feed + bleed) Maßnahmen zur Verfügung, um die Nachwärmeabfuhr (NWA) wiederherzustellen und somit das Kernschmelzen zu verhindern.

Das Personal von Davis-Besse verhinderte das Kernschmelzen durch sekundärseitige Maßnahmen: Nach ca. 12 min war Strang 2, nach ca. 18 min Strang 1 des 2x100% Notspeisewassersystems verfügbar. Alle 8 Operateure des Schichtpersonals waren an der Durchführung dieser Maßnahmen beteiligt. Die durchgeführten Maßnahmen lassen sich vereinfacht in 2 Diagnoseeinheiten, 5 mündliche Anweisungseinheiten und 5 manuelle Tätigkeitseinheiten untergliedern. 3 der 5 Tätigkeitseinheiten wurden ohne personelle Redundanz durchgeführt.

Am Verhalten des Schichtleiters war eine Fixierung auf die sekundärseitige NWA zu beobachten. Nach ca. 8 min, als die sekundärseitigen Maßnahmen noch nicht erfolgreich abgeschlossen waren, hätte er lt. Vorschrift die primärseitige NWA einleiten müssen. Er unterließ aber das Einleiten der primärseitigen NWA (feed + bleed), obwohl er vom Betriebsleiter und vom Sekundärteiloperator eine entsprechende Empfehlung erhielt.

Das Verhalten des Schichtleiters ist ein Beispiel für eine Rückwirkung in Form von Fehlverhalten, die durch ein Ziel untergeordneter Sicherheitsbedeutung hervorgerufen wurde. Das Hauptziel "NWA" kann auf zwei Wegen erreicht werden: sekundärseitig oder primärseitig. Die primärseitige NWA hat aufgrund der Primärkreisdruckentlastung den Nebeneffekt, daß das Gebäude kontaminiert wird. Daraus ist das untergeordnete Ziel "keine Gebäudekontamination" ableitbar, welches aber nur sekundärseitig zu realisieren ist. Daraus ist eine eindeutige Präferenz der sekundärseitigen NWA ableitbar.

Eine Rückwirkung auf das Hauptziel in Form von Fehlverhalten aufgrund eines Konflikts kann auftreten, wenn die Vorschrift eine Alternative (primärseitige NWA) anfordert, mit der das untergeordnete Ziel nicht erreicht werden kann.

In diesem Abschnitt wurde eine dynamische Analyse der Gegenmaßnahmen des Personals für den während des Störfalls aufgetretenen NWA-Ausfallzustand durchgeführt. Die probabilistische Quantifizierung beschränkte sich auf Zeitfehler, d.h. auf die Frage der rechtzeitigen Durchführung ohne Berücksichtigung der 'klassischen' (zeitunabhängigen) Operateurf Fehler wie Unterlassung oder Verwechslung.

Unter der Annahme, daß sich das Personal praktisch regelbasiert verhält und die kritischen Schritte (wie z.B. das Öffnen des Primärkreises) der primärseitigen Maßnahmen ohne signifikante Verzögerung durchführt, ergibt sich eine Versagenswahrscheinlichkeit der Gegenmaßnahmen von $2.7E-4$. Dieser Wert erhöht sich ca. um den Faktor 67 auf $1.8E-2$, wenn man zu den kritischen Schritten einen wahrgenommenen Konflikt unterstellt, der sich durch zögerndes Verhalten bemerkbar macht.

Im Fall Davis-Besse läßt sich zögerndes Verhalten (bzgl. feed + bleed) nicht nur subjektiv begründen (schlichte Abneigung gegen eine Kühlung mit offenem Primärkreis) sondern auch objektiv. Denn aufgrund der positiven Systemeigenschaft, daß auch noch in der Zeit zwischen 10 min und 30 min nach Ausfall der Dampferzeugerbeheizung sekundärseitige Maßnahmen wirksam sein können, ist das regelwidrige Hinauszögern der primärseitigen NWA - bei gleichzeitiger Weiterverfolgung der sekundärseitigen Maßnahmen - eine machbare Alternative zur Verhinderung der Gebäudekontamination.

Diese objektive Begründung schlägt sich auch im Ergebnis der probabilistischen Quantifizierung nieder: Durch zögerndes Verhalten erhöht sich die Wahrscheinlichkeit einer NWA ohne Gebäudekontamination ca. um den Faktor 2 von 0.37 auf 0.77.

3. Hypothetisches Anwendungsbeispiel: Die Notkühlung des HTR-500

3.1 Einführung

Die Anwendung der in den Abschnitten 4 und 5 erarbeiteten methodischen Verbesserungen (gem. erweiterter Zielgrößenberücksichtigung) erfolgt am Beispiel der Zuverlässigkeit des Systems zur Nachwärmeabfuhr (NWA) des HTR-500. In diesem Abschnitt wird für das NWA-System, in Anlehnung an die Ergebnisse der technischen Zuverlässigkeitsanalyse in den "Sicherheitstechnischen Untersuchungen zum Störfallverhalten des HTR-500" (ISF 1984), eine Mensch-Maschine-Systemanalyse (MMSA) durchgeführt. Diese MMSA bezieht sich auf einen Teilaspekt der klassischen Zielsetzung, Vermeidung radiologischer Schäden, einer PRA: Wiederherstellung der NWA nach technischem Versagen.

Der HTR-500 ist ein Kernkraftwerkskonzept mit Hochtemperaturreaktor. Zu Beginn der hier durchgeführten Forschungsarbeiten befand sich der HTR-500 in der Planungsphase (als Nachfolgeprojekt des THTR-300 in Hamm-Uentrop). Im Verlauf der Forschungsarbeiten fiel - im Zusammenhang mit der öffentlichen Diskussion der Kernenergienutzung - aus wirtschaftlichen und energiepolitischen Gründen die Entscheidung, das Konzept des HTR-500 vorerst nicht weiter zu verfolgen; vgl. KIRCHNER (1991) zur HTR-Entwicklung in der Bundesrepublik Deutschland.

Tab. 9 enthält die Hauptauslegungsdaten des HTR-500. In Abb. 11 ist der Reaktor-druckbehälter mit Einbauten dargestellt. Abb. 12 auf Seite 48 enthält ein Prinzipschaltbild zu den wichtigsten Sicherheitseinrichtungen.

Im Normalbetrieb wird der aus kugelförmigen, tennisballgroßen Brennelementen (BE) bestehende Reaktorkern von oben nach unten von Helium (dem Kühlgas) durchströmt. Die nuklear erzeugte Wärme wird über 8 Dampferzeuger (DE) abgeführt.

Bei Störfällen bzw. Betriebsstörungen, die eine Unterkritikalität des Reaktorkern erforderlich machen, kann die nukleare Wärmeerzeugung (je nach Störfalltyp) auf zwei Arten gestoppt werden:

1. "Langsame" Abschaltung durch Einfahren der Reflektorstäbe in die seitlichen, dafür vorgesehenen Bohrungen.

2. Automatische Schnellabschaltung (RESA) durch Einfallen der Reflektorstäbe.

Zur Abfuhr der trotz Unterkritikalität noch entstehenden Nachwärme sind ebenfalls (je nach Störfalltyp) zwei Möglichkeiten vorgesehen: (1) per Hauptkühlsystem (HKS) oder (2) per NWA-System.

Eine Rekritikalität (d.h. ein Wiederkritischwerden) aufgrund der Abkühlung des Kerns (nach mehreren Stunden NWA-Betrieb) kann durch Auslösen der Langzeitabschaltung (d.h. Einfahren der Kernstäbe in den Kugelhaufen) verhindert werden.

Thermische Reaktorleistung	1250 MW
Thermische Leistung der Dampferzeuger	1266 MW
elektrische Nettoleistung	500 MW
Nutzungsdauer	40 Jahre
mittlere Arbeitsverfügbarkeit	80 %
mittlere Leistungsdichte im Kern	6 MW/m ³
Wärmeverluste	6.5 MW
Gebläsewellenleistung gesamt	22.5 MW
Druck (Gebläseaustritt)	50 bar
Kühlgasdurchsatz je Gebläse	69.2 kg/s
Heliumtemperatur (Austritt DE-Bündel)	260 °C
Heliumtemperatur (Eintritt DE)	700 °C
Heliuminventar	14600 kg
Druckverluste:	
Reaktorkern	0.77 bar
Dampferzeuger (DE)	0.43 bar
Gasführungen	0.10 bar
Gebläseabspernung	0.10 bar
Gebläsedruckerhöhung	1.40 bar
Frischdampfdruck vor Turbine	180 bar
Frischdampf Temperatur vor Turbine	525 °C
Speisewassertemperatur	190 °C
Kondensatordruck	0.06 bar

Tab. 9. HTR-500. Hauptauslegungsdaten bei 100% Last (HRB 1983, S.26)

Weitere Einzelheiten zum HTR-500 sowie allgemeines zur HTR-Technik können z.B. in KUGELER/SCHULTEN (1989) nachgelesen werden.

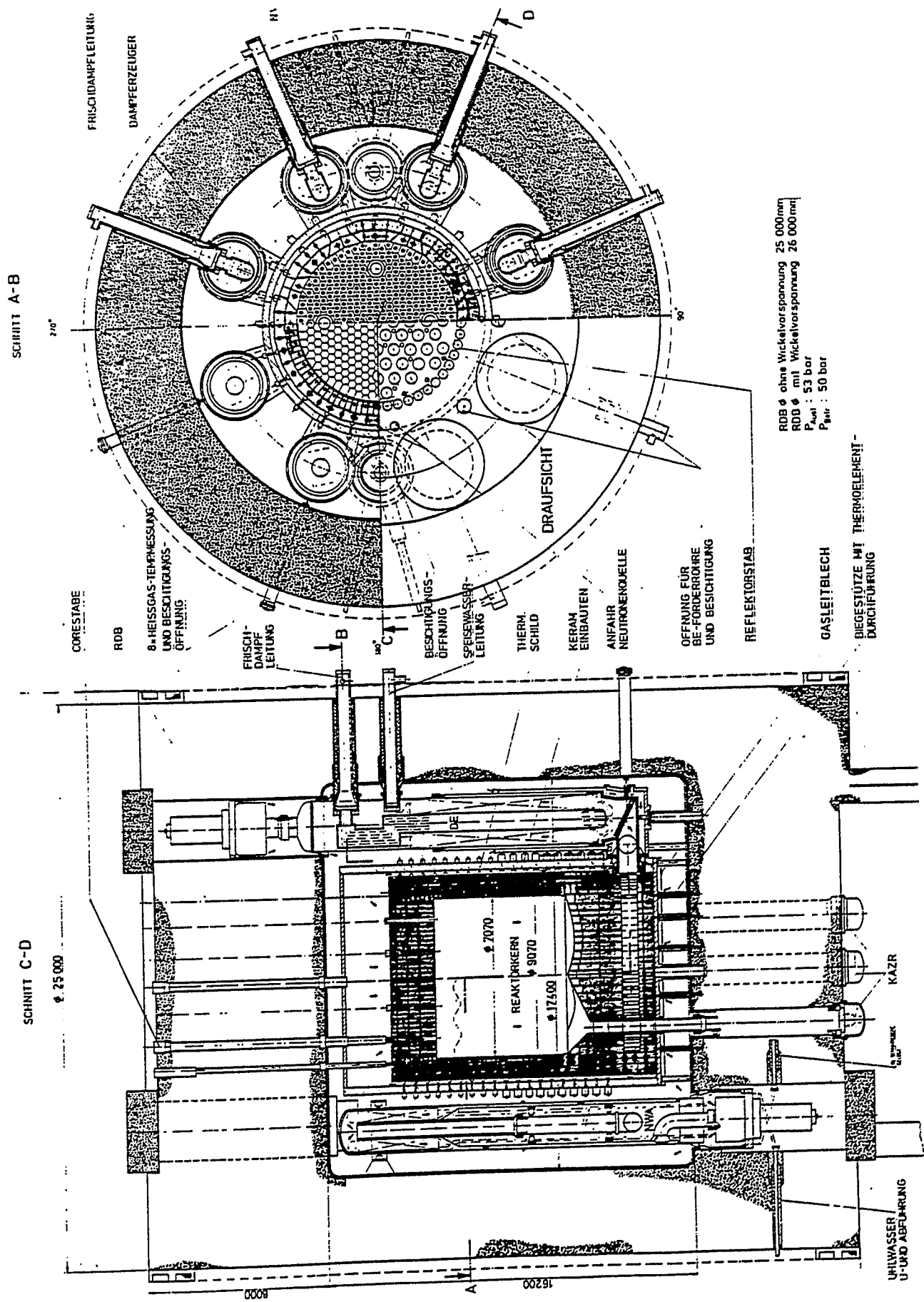
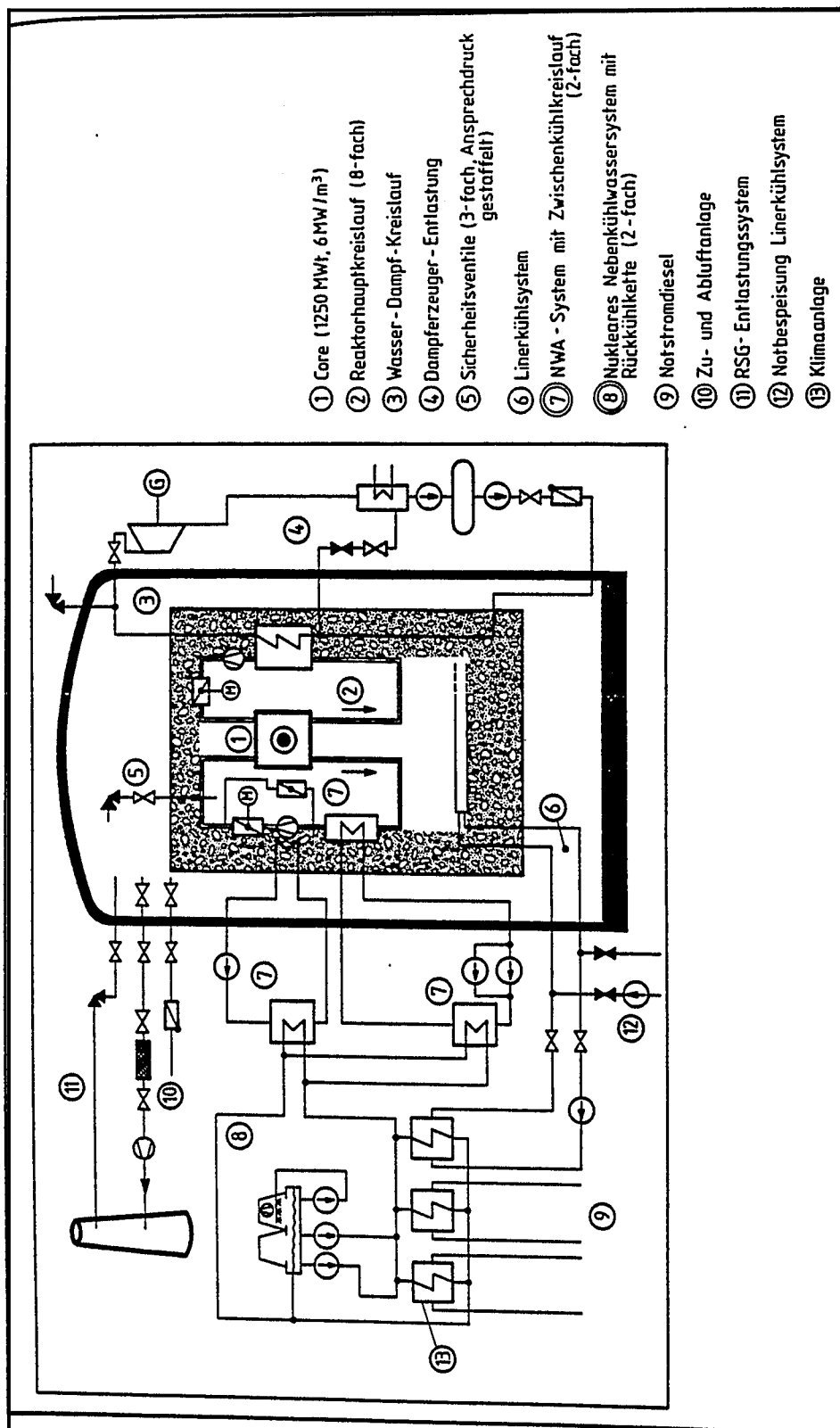


Abb. 11. HTR-500. Reaktordruckbehälter mit Einbauten (aus HRB 1983, S.29)



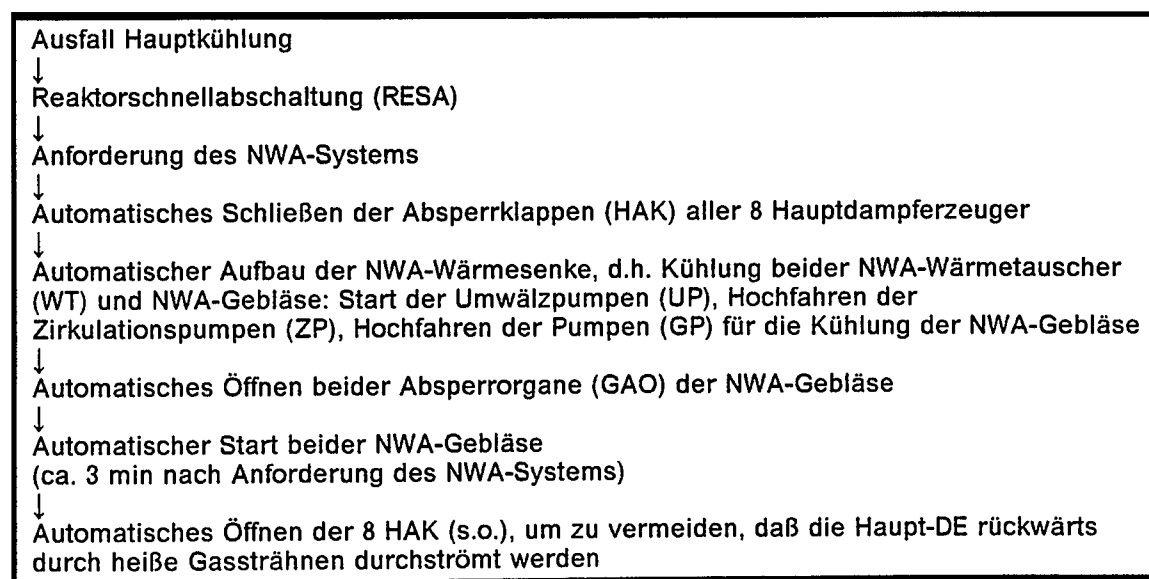
○ Notstromversorgte Systeme

Abb. 12. HTR-500. Anlagenübersicht (aus ISF 1984, S.7)

3.2 Betrachtete Transiente

Als Anforderung an das NWA-System wird hier die Transiente "Ausfall des Hauptkühlsystems (HKS)" betrachtet. Unter dieser Bezeichnung (vgl. ISF 1984) werden alle Ereignisse zusammengefaßt, die bei Reaktor unter Druck (d.h. kein Störfall mit Leck im Primärkreis als auslösendes Ereignis) und intakter Eigenbedarfsversorgung (d.h. kein Notstromfall) eine Unterbrechung der Wärmeabfuhr über die betrieblichen Dampferzeuger verursachen. Dieser Störfall hat von allen in ISF (1984) betrachteten auslösenden Ereignissen mit 0.4 pro Reaktorjahr die größte Eintrittshäufigkeit.

Der Störfall löst folgende Systemreaktionen aus:



Tab. 10. Systemreaktionen nach Ausfall der Hauptkühlung:

vgl. ISF (1984, S.13) und HRB (1983, S.98f)

Für das auslegungsgemäß funktionierende NWA-System gelten folgende technische Daten:

Abgeführte maximale Wärmemenge	50 MW
Kühlgasdurchsatz im Kern	14 kg/s (2.5%)
Rückdurchströmung abgeschalteter DE	8 kg/s (1.5%)
Kühlgasmassenstrom je NWA-Kreislauf	22 kg/s (4%)
Kühlwasserdurchsatz je WT	98 kg/s

Tab. 11. NWA-Daten bei Reaktor unter Druck (ISF 1984, Kap. II)

3.3 Modellierung gemäß Hauptziel "NWA ausreichend"

3.3.1 Zur Methode

Im Abschnitt 3.3.3 wird eine NWA-Zuverlässigkeitsanalyse unter Einbeziehung menschlicher Gegenmaßnahmen (nach technischem NWA-Versagen) durchgeführt. Diese Analyse basiert auf dem Ergebnis der vom ISF (1984) durchgeführten "reinen" technischen NWA-Zuverlässigkeitsanalyse (ohne Gegenmaßnahmen).

In Anlehnung an die ISF-Analyse werden Wahrscheinlichkeiten technischer Fehler als Punktwerte (Erwartungswerte ohne Unsicherheiten) berücksichtigt. Im Gegensatz zur ISF-Analyse werden Wahrscheinlichkeiten menschlicher Fehler mit Unsicherheiten berücksichtigt. Das Ergebnis enthält deshalb nur Unsicherheiten aufgrund von Schwankungen in der menschlichen Zuverlässigkeit.

Zur Schreibweise. Unsicherheiten werden wie folgt angegeben:

- MDN < UF > ,

MDN Median,

UF Unsicherheitsfaktor für das zweiseitige 90%-Intervall (s.u.)

oder

- EW < UG, OG > ,

UG = MDN/UF,

OG = MDN•UF,

EW Erwartungswert,

UG 5%-Untergrenze der 90%-Intervalls,

OG 95%-Untergrenze der 90%-Intervalls (maximal 1)

3.3.2 Die ISF-Analyse

Mit den Untersuchungen des ISF (1984) zum HTR-500 liegt ein erstes Dokument zur Beurteilung des Risikos eines modernen HTR mittlerer Leistungsgröße vor. Der Bericht des ISF war ein wertvolles Hilfsmittel der hier durchgeführten Arbeiten.

Für das NWA-System (nach Ausfall der Hauptkühlung bei Reaktor unter Druck und intakter Eigenbedarfsversorgung) wurde eine Ausfallwahrscheinlichkeit (pro Anforderung) von $2.4E-4$ ermittelt. Der Anhang B enthält die vom ISF erstellten Fehlerbäume für das NWA-System. In Tab. 12 sind die vom ISF verwendeten Daten aufgelistet.

Nr.	Ereignis	Wahrscheinlichkeit pro Anforderung* ²
(1)	Ausfall der Ansteuerung* ¹	$1.5E-3$
(2)	Pumpen-Ausfall* ¹ : Kein Start bzw. Hochlauf	$5.4E-3$
(3)	Gebläse-Ausfall	$5.4E-3$
(4)	Trafo-Ausfall	$8.2E-4$
(5)	Umrichter-Ausfall	$4.5E-3$
(6)	Ausfall eines Absperrorgans (GAO) am NWA-Gebläse, Ausfallart: öffnet nicht	$2.7E-3$
(7)	Ausfall einer Hauptabsperrrklappe (HAK), Ausfallart: schließt nicht	je HAK: $7.0E-3$ 1v8: $5.6E-2$
(8)	Ausfall eines Bypassorgans (GBO) am NWA-Gebläse, Ausfallart: öffnet nicht	je GBO: $7.0E-3$ 1v2: $1.4E-2$
(9)	Abhängiger Ausfall (CCF), wenn Ereignis 1 (B-Faktor)	$1.0E-2$
(10)	Abhängiger Ausfall (CCF), wenn Ereignisse 2 bis 8 (B-Faktor)	$1.0E-1$
(11)	Bypassorgane vom Operateur nicht geöffnet* ³	$3.6E-2$

Tab. 12. NWA-Ausfalldaten in ISF (1984): Originalquelle für (1) bis (10): ISF/GRS (1981)

* Anmerkungen zu Tab. 12

1. Reparierbar (lt. interner Unterlage), 8 h mittlere Reparaturdauer.
2. Vierwöchentliches Testintervall für (1) bis (6), für (7) und (8) 875 h mittlere Ausfallentdeckungszeit aufgrund von 5 angenommenen Reaktorschnellabschaltungen pro Jahr.

3. Hierzu wurde in ISF (1984, S.19) folgende Abschätzung vorgenommen: "Die Wahrscheinlichkeit des Nichtöffnens der beiden Umleitklappen setzt sich aus einem Anteil für mechanische Ursachen und einem Beitrag aus der Operateurhandlung zusammen. Die aus der Klappenmechanik stammende Ausfallwahrscheinlichkeit beträgt $1,4 \cdot 10^{-2}/A$ (...). Die Operateurhandlung läßt sich ohne genaue Kenntnis des Handlungsrahmens nur abschätzen; es erscheint konservativ, für die Gesamtwahrscheinlichkeit des Ausfalls der beiden Umleitklappen den der Trendanalyse zugrunde gelegten Wert von etwa $5 \cdot 10^{-2}/A$ anzunehmen."

Demnach wurde für den Operateurfehleranteil folgende Wahrscheinlichkeit (pro Anforderung) angesetzt:

$$w(N_M) \simeq 0.05 - 0.014 = 0.036.$$

In der vom ISF berechneten Wahrscheinlichkeit von $2.4E-4$ für den NWA-Ausfall sind zwei Arten von Gegenmaßnahmen, die vom Personal durchzuführen sind (Accident Management), enthalten:

1. Herstellen einer Naturkonvektion durch Öffnen beider Bypaßorgane an den NWA-Gebläsen, wenn die Zwangskonvektion (per NWA-Gebläse) ausgefallen ist. Folgende Voraussetzungen für die Wirksamkeit wurden zusätzlich berücksichtigt:
 - beide Stränge der Wärmesenke verfügbar und
 - alle 8 Hauptabsperklappen (HAK) geschlossen.
2. Reparatur ausgefallener Bauteile.

Zur Schätzung der Beiträge zur Wahrscheinlichkeit des NWA-Ausfalls wurde hier in Tab. 13 eine Handrechnung für die Komponenten der Zwangskonvektion durchgeführt. Es ergibt sich eine Wahrscheinlichkeit des NWA-Ausfalls aufgrund dieser Komponenten von $2.4E-3$. Ca. 60% dieser Ausfälle sind nicht reparierbar. Durch Berücksichtigung von Ausfallursachen aus der NWA-Wärmesenke erhöht sich dieser Wert nur unwesentlich (Tab. 14).

AUSFALL	Strang 1 bzw. 2	CCF Strang 1&2
Ansteuerung Gebläsekühlung	1.5E-3	1.5E-5
Gebläsekühlpumpe	5.4E-3	5.4E-4
Ansteuerung Gebläseabsperrorgan	1.5E-3	1.5E-5
Gebläseabsperrorgan	2.7E-3	2.7E-4
Ansteuerung Gebläse	1.5E-3	1.5E-5
Gebläse	5.4E-3	5.4E-4
Gebläse-Trafo	8.2E-4	8.2E-5
Gebläse-Umrichter	4.5E-3	4.5E-4
S U M M E	2.3E-2	1.9E-3
NICHT REPARIERBARER ANTEIL	1.3E-2	1.3E-3
I N S G E S A M T	$(2.3E-2)^2 + 1.9E-3 = 2.4E-3$	
NICHT REPARIERBARER ANTEIL	$(1.3E-2)^2 + 1.3E-3 = 1.5E-3 (\approx 60\%)$	

Tab. 13. Ausfallwahrscheinlichkeit der Zwangskonvektion (per Gebläse)

Wahrsch.	Ausfall
2.4E-3	NWA (Technik) insgesamt (100 %)
4.0E-7	Wärmesenke Strang 1 und 2 (0.02%)
2.2E-6	Wärmesenke Strang 1 bzw. 2 und Zwangskonvektion Strang 2 bzw. 1 (0.1 %)

Tab. 14. Beitrag der Wärmesenke zur NWA-Ausfallwahrscheinlichkeit

3.3.3 Einbeziehung menschlichen Verhaltens

3.3.3.1 Aufgabenanalyse

Die durchgeführte Aufgabenanalyse orientiert sich an der Logik der Fehlerbäume (Anhang B) des ISF (1984) und an den lt. Hersteller (HRB 1983, S.100ff) vorgesehenen Gegenmaßnahmen nach NWA-Ausfall:

1. Naturkonvektion (kurzfristig realisierbar)
2. Querverbindung zwischen funktionierenden Kreisläufen (mittelfristig realisierbar)
3. Reparatur (langfristig realisierbar)

Tab. 15 enthält den hier angenommenen Handlungsablauf nach Ausfall der Hauptkühlung. Die hypothetischen Aufgabenbeschreibungen zu den Prozeduren Naturkonvektion und Querverbindung sind im Anhang C und D aufgeführt. Ihre probabilistische Bewertung beruht auf folgenden Annahmen:

- Die schriftliche Prozedur liegt ohne Checkliste vor.
- Die schriftliche Prozedur wird benutzt. Bei Nichtbenutzen würde sich die Wahrscheinlichkeit für einen Unterlassungsfehler (pro Schritt) um den Faktor 5 erhöhen. Wegen der kleinen Wahrscheinlichkeit ($0.005 < 10^{-5}$) für das Nichtbenutzen ist dieser Effekt vernachlässigbar.
(vgl. SWAIN 1983, ch.15&16)
- Mittelhoher Stress, erfahrenes Personal.
- Das Nichtbemerken eines NWA-Ausfalls nach richtiger Diagnose für den Ausfall der Hauptkühlung wird vernachlässigt, weil vorausgesetzt wird, daß ein hörbares Signal (Alarm) hierfür existiert.
- Es wird vorausgesetzt, daß genügend Personal (8 Operateure) verfügbar ist, so daß die Reparatur evtl. ausgefallener Bauteile parallel zur Maßnahme Naturkonvektion bzw. Querverbindung erfolgen kann.

PHASE I: SOFORTMASSNAHMEN, Schritte 1 bis 6

1. Diagnose: Erkennen, daß Prozedur für Maßnahmen nach Ausfall der Hauptkühlung bei Reaktor unter Druck und intakter Eigenbedarfsversorgung anzuwenden ist.
2. Prozedur zur Hand nehmen.
3. Überprüfen, ob RESA.
Ggfs. von Hand auslösen.
4. Überprüfen, ob NWA-Start.
Ggfs. Handstart.
5. Überprüfen, ob NWA-Wärmesenke verfügbar.
6. Überprüfen, ob ausreichende NWA per Zwangskonvektion (Gebläse).
Wenn nein, weiter mit Schritt 8 (Phase II)

PHASE II: ACCIDENT-MANAGEMENT-DIAGNOSE bei NWA-Ausfall, Schritte 7 bis 11

7. Diskussion, Maßnahmenplanung.
8. Notfallprozedur zur Hand nehmen.
9. Überprüfen, ob beide NWA-Wärmetauscher ausreichend gekühlt.
Wenn ja, weiter mit nächstem Schritt.
Wenn nein, weiter mit übernächstem Schritt.
10. Überprüfen, ob alle 8 Hauptabsperrrklappen (HAK) geschlossen.
Wenn ja, weiter mit Prozedur "Naturkonvektion" (Anhang C).
Wenn nein, weiter mit nächstem Schritt.
11. Überprüfen, ob eine der folgenden Ausfallkombinationen vorliegt:
 - a. Wärmesenke Strang 1 und Zwangskonvektion Strang 2.
 - b. Wärmesenke Strang 2 und Zwangskonvektion Strang 1.
 - c. Gebläsekühlung Strang 1 und Gebläse Strang 2.
 - d. Gebläsekühlung Strang 2 und Gebläse Strang 1.

Wenn ja, Prozedur "Querverbindung" (Anhang D) anwenden.
Wenn nein, Prozedur "Reparatur" anwenden.

Tab. 15. Hypothetischer Handlungsablauf nach Ausfall der Hauptkühlung

3.3.3.2 Naturkonvektion

Zeitbedarfsanalyse (ZBA)

Die ZBA wird mit der "Dynamischen Analyseverfahren für Operateurhandlungen" (REER) durchgeführt. Der Abschnitt 2.4.1 enthält eine Kurzbeschreibung der Methode.

Die folgenden Tabellen enthalten die Eingabedaten und die Ergebnisse der Zeitbedarfsanalyse. Die Zeitquantile für die Diagnose wurden direkt dem Modell aus SWAIN (1983) entnommen. Die Ergebnismwahrscheinlichkeiten werden als Erwartungswerte mit $UF=5$ interpretiert.

Ohne unentdeckte zeitunabhängige Operateurfehler (z.B. Tab. 18, U11N) ergibt sich ein Mindestzeitbedarf T_0 von ca. 10 min ($T_{50} = 20$ min, $T_{95} = 39$ min). Daraus erhält man für die Wahrscheinlichkeit der nicht rechtzeitigen Durchführung:

$$EW = 0.14 \text{ (lt. Tab. 16 für } t = 30 \text{ min)}$$

$$UF = 5 \text{ (geschätzt)}$$

$$\rightarrow MDN = 0.089 \text{ (Lognormalverteilung)}$$

Für die Durchführungszeit, wenn ein nicht sofort entdeckter (zeitunabhängiger) Operateurfehler auftritt, wurde ein Mindestwert von 18 min berechnet ($T_{50} = 41$ min, $T_{95} = 81$ min). Die nachträgliche Korrektur - für den Fall, daß nach Beendigung der gesamten Maßnahme ein Fehler vorliegt - hat demnach eine Fehlerwahrscheinlichkeit von

$$0.87 < 0.11, 1.0 > = 0.54 < 5 > \text{ (late recovery).}$$

Eingabedaten	
Handlung	Zeitbedarf (min), Kenntnisbedarf
Naturkonvektion durchführen: (1)-(13N)	
Sofortmaßnahmen: (1)-(6)	
(1) Diagnose: Ausfall Hauptkühlung	T0 = 1, T50 = 2, T95 = 12
(2) Entsprechende Prozedur holen	T0 = 1 (skill)
(3) Prüfen, ob RESA	T0 = 0.5 (skill)
(4) Prüfen, ob NWA-Start	T0 = 0.5 (skill)
(5) Prüfen, ob NWA-Wärmesenke verfügbar	T0 = 0.5 (rule)
(6) Prüfen, ob NWA per Gebläse verfügbar	T0 = 0.5 (rule)
Maßnahmen nach NWA-Ausfall: (7)-(13N)	
(7) Diskussion, Maßnahmenplanung	T50 = 2 (knowl)
(8) Notfallprozedur holen	T0 = 1 (rule)
(9) Prüfen, ob beide NWA-WT gekühlt	T0 = 0.5 (rule)
(10) Prüfen, ob 8v8 HAK geschlossen	T0 = 0.5 (rule)
(11N) Prüfen, ob 2v2 GAO geschlossen	T50 = 2 (knowl)
(12N) GBO-Verriegelung aufheben	T0 = 1 (rule)
(13N) Beide GBO öffnen	T0 = 0.5 (rule)
↓	
Verteilungsparameter der Durchführungszeit T/min:	
EW = 22.1, STD = 9.2, T0 = 9.5, T50 = 19.7, T95 = 39.4	
↓	
$w(T \geq 30) = 0.14$	

Tab. 16. Naturkonvektion. Zeitbedarfsanalyse ohne zeitunabhängige Operateurfehler

Eingabedaten	
Handlung	Zeitbedarf (min), Kenntnisbedarf
Naturkonvektion durchführen: (1)-(13N)	T0 = 9.5, T50 = 19.7, T95 = 39.4
Zeitunabh. Operateurfehler korrigieren: (14N)-(17N)	
(14N) Bemerken, daß Naturkonvektion unwirksam	T0 = 5 (knowl)
(15N) Diskussion, Korrekturplanung	T50 = 2 (knowl)
(16N) Fehlersuche	T0 = 2 (knowl)
(17N) Fehler korrigieren	T0 = 0.5 (rule)
↓	
Verteilungsparameter der Durchführungszeit T/min:	
EW = 46, STD = 18.4, T0 = 18, T50 = 41.2, T95 = 80.8	
↓	
$w(T \geq 30) = 0.87$	

Tab. 17. Naturkonvektion. Zeitbedarfsanalyse, wenn zeitunabhängiger Operateurfehler

Fehlereffektanalyse (klassische MMSA)

Tab. 18 enthält die als Ausfallursache der Naturkonvektion betrachteten (zeitunabhängigen) Operateurfehler ohne Korrekturfaktoren (recovery). Der erste Buchstabe vor der Aufgabennummer hat folgende Bedeutung:

- D Diagnosefehler
- W Wahrnehmungsfehler
- U Unterlassungsfehler
- V Verwechslungsfehler

Die Identifikationsnummer (BHEP-ID, lt. Anhang E) verweist auf die verwendete Basisfehlerwahrscheinlichkeit und deren Quelle. Die Auswertung erfolgte mit dem hier entwickelten Rechenprogramm HRATREE. HRATREE wurde in das Programm SAS integriert.

Es ergibt sich eine Fehlerwahrscheinlichkeit von insgesamt $0.16 < 3.9 >$ (ohne recovery und ohne Berücksichtigung der Ergebnisse der dynamischen Analyse in Tab. 16).

BHEP-ID	PSF	MDN < UF >	FEHLER
1.0020	-	0.01 < 10 >	(D1) Keine Diagnose für die Prozedur nach HKS-Ausfall* ¹
2.2403	-	0.001 < 3 >	(W9) Nicht bemerkt, daß Wärmetauscher in beiden Strängen verfügbar: deshalb weiter mit Schritt 11
3.111	2* ²	0.02 < 5 >	(U10) Nicht geprüft, ob alle HAK geschlossen: deshalb weiter mit Schritt 11
2.403	-	0.001 < 3 >	(W10) Nicht bemerkt, daß alle HAK geschlossen: deshalb weiter mit Schritt 11
3.111	2* ²	0.67•0.02 < 5 >	(U11N) Nicht geprüft, ob beide Absperrorgane (GAO) der NWA-Gebläse geschlossen* ³
2.2403	-	0.67•0.001 < 3 >	(W11N) Nicht bemerkt, daß 1v2 GAO auf* ³
4.221	5* ⁴	0.67•0.025 < 10 >	(V11N) Verwechslungsfehler beim Schließen der GAO* ³
4.221	5* ⁴	0.025 < 10 >	(V12N) Verwechslungsfehler bei Aufheben der Verriegelung der Bypassorgane (GBO) der NWA-Gebläse* ⁵
3.111	2* ²	0.02 < 5 >	(U13N) GBO nicht geöffnet

Tab. 18. Naturkonvektion. Operateurfehler ohne recovery und ohne Zeitfehler:

Es wird angenommen, daß die automatische Auslösung der Systemreaktion ÖFFNEN DER HAK (nach 30 min) nur dann erfolgt, wenn beide Wärmetauscher NICHT bespeist werden. Falls diese Annahme nicht zutrifft, dann müßte noch die Aufgabe ÖFFNUNGSSIGNAL DER HAK AUSSERKRAFTSETZEN ergänzt werden.

* Anmerkungen zu Tab. 18

1. Zulässige Diagnosezeit (ca. 20 min)
= zulässige Zeit für Naturkonvektion (30 min) minus
Mindestzeit der Durchführung nach Diagnose (ca. 10 min, Tab. 16).
2. Lt. Anhang F für Aufgaben vom Typ SCHRITTWEISE (entspricht RULE oder SKILL)
3. Die Bedingung, beide GAO geschlossen (vgl. HRB 1983, S.154), wurde vom ISF nicht berücksichtigt. Wenn man von der Anforderungsreihenfolge "GAO - Gebläse - Trafo - Umrichter" ausgeht, so ergibt sich für die Wahrscheinlichkeit eines NWA-Ausfalls mit geöffneten GAO folgende Abschätzung (vgl. Tab. 13 auf Seite 53):
1.1E-3 CCF (Gebläse, Trafo oder Umrichter)
+ 2.5E-4 Unabhängiger Ausfall (Gebläse, Trafo oder Umrichter) Strang 1
(1.1E-2) UND unabhängiger Ausfall Strang 2 (2.3E-2)

+ 2.5E-4 Unabhängiger Ausfall (Gebläse, Trafo oder Umrichter) Strang 2
 (1.1E-2) UND unabhängiger Ausfall Strang 1 (2.3E-2)
 = 1.6E-3 INSGESAMT, d.h. in
 (1.6E-3/2.4E-3)100% = 67% aller NWA-Aufälle

Die Wahrscheinlichkeiten für U11N bis V11N wurden deshalb mit dem Korrekturfaktor 0.67 multipliziert.

4. Lt. Anhang F für Aufgaben vom Typ DYNAMISCH (entspricht KNOWLEDGE).
5. Unterlassung ist durch U13N abgedeckt (Annahme).

Frühe Korrekturen (early recovery)

Zur Methode

Frühe Korrekturen (unmittelbar nach Beendigung des Aufgabenteils) durch personelle Redundanz während der Durchführung werden mit dem Abhängigkeitsmodell von SWAIN (1983) berücksichtigt.

Allgemein gilt für die Wahrscheinlichkeit $w(AB)$ des Auftretens der Fehler A (Operateur 1) und B (Operateur 2):

$$w(AB) = w(A) w(B|A)$$

Das Hauptproblem bei der Bestimmung von $w(AB)$ liegt in Bestimmung der bedingten Fehlerwahrscheinlichkeit $w(B|A)$ des zweiten Operators. Nach dem Abhängigkeitsmodell von SWAIN (ch.10; siehe Anhang G in dieser Arbeit) gilt für die Fehlerwahrscheinlichkeit $w(B|A)$ des zweiten Operators (B) unter der Bedingung des gleichen Fehlers durch den ersten Operateur (A):

$$w(B|A) = [1 + (n-1) w(B)]/n$$

mit

$w(B)$ = Fehlerwahrscheinlichkeit für B bei Unabhängigkeit,

$n = 2$ bei hoher Kopplung (HD),

$n = 7$ bei mittlerer Kopplung (MD) und

$n = 15$ bei leichter Kopplung (LD) zwischen A und B.

Dieses Modell läßt sich in das Beta-Faktor-Modell überführen, indem man β gleich $1/n$ setzt:

$$w(B|A) = \beta + (1-\beta)w(B)$$

mit

$\beta = 0.5$ (HD), $\beta \approx 0.15$ (MD) und $\beta = 0.05$ (LD).

Wenn $w(B)$ klein ist, $MDN(B) < 0.01$, empfiehlt SWAIN für $w(B|A)$ näherungsweise die folgenden Werte für Median (MDN), Untergrenze (UG) und Obergrenze (OG) anzu-
setzen:

HD: $MDN = 0.5$, $UG = 0.15$, $OG = 1.0$;

MD: $MDN = 0.15$, $UG = 0.05$, $OG = 0.50$;

LD: $MDN = 0.05$, $UG = MDN(B)$, $OG = 0.15$.

Die Näherungen bedeuten, daß der unabhängige Anteil $(1-\beta)w(B)$ vernachlässigt wird. Für große $w(B)$, $MDN(B) \geq 0.01$, berechnet SWAIN den MDN von $w(B|A)$ über die o.g. Gleichung durch Einsetzen von Medianen (vgl. Anhang G). Formal richtig wäre es, den Erwartungswert (EW) durch Einsetzen von Erwartungswerten zu berechnen.

Beispiel:

GEGEBEN: $w(B) = 0.05 < 5 >$, MD zwischen A und B; GESUCHT: $EW(B|A)$.

LÖSUNG:

Über EW:

$$EW(B) = 0.08 \text{ (Lognormalverteilung)}$$

$$EW(\beta) = 0.2 \text{ (Lognormalverteilung)}$$

$$EW(B|A) = 0.2 + 0.8 \cdot 0.08 = 0.26$$

Über MDN (SWAIN):

$$MDN(B|A) = 0.15 + 0.85 \cdot 0.05 = 0.1925$$

$$OG(B|A) = 0.5 + 0.5 \cdot 0.05 = 0.525 \text{ (Obergrenze)}$$

$$\rightarrow UF = 0.525 / 0.1925 = 2.7$$

$$\rightarrow EW(B|A) = 0.23 \text{ (Lognormalverteilung)}$$

Wegen der Vergleichbarkeit zu anderen Analysen wird hier die Berechnungsmethode nach SWAIN (über MDN) verwendet. Angesichts der willkürlichen Festlegungen zu den Kopplungsgraden, zu den Unsicherheitsfaktoren und zu dem Verteilungstyp ha-

ben die Unterschiede zwischen den beiden Berechnungsmethoden nur ein geringes Gewicht: Genausogut hätte man auch 0.1 oder 0.2 als MDN des Beta-Faktor bei mittlerer Kopplung annehmen können.

Kopplungsgrade

Es wird angenommen, daß die erforderlichen Aufgaben von zwei Operateuren durchgeführt werden. Dabei wird eine mittlere Kopplung angenommen, d.h. bei jedem 7. Fehler (MDN) des ersten Operateurs besteht eine vollständige Abhängigkeit zum zweiten Operateur. Für Unterlassungsfehler wird noch mit hoher Kopplung eine Korrekturmöglichkeit durch einen dritten Operateur (z.B. Schichtleiter) angenommen, der sich gelegentlich (zu ca. 50%) danach erkundigt, ob die entsprechende Teilaufgabe überhaupt durchgeführt wurde. Da die Antwort bei Teilaufgaben, die nicht vergessen, aber falsch durchgeführt wurden, "ja" lauten wird, beschränkt sich die Anwendung dieses Korrekturfaktors auf Fehler vom Typ Unterlassung. In Abb. 13 sind die Ergebnisse der Einbeziehung früher Korrekturen aufgrund personeller Redundanz zusammengefaßt. Es ergibt sich eine Versagenswahrscheinlichkeit der Naturkonvektion aufgrund menschlicher Fehler von $0.034 < 5.7 >$ (EW = 0.06). Das 90%-Unsicherheitsintervall $< 0.0056, 0.19 >$ deckt den vom ISF angesetzten Erwartungswert von 0.036 gut ab. Der Diagnosefehler (EW = 0.027) liefert den Hauptbeitrag, was auf ein Zeitproblem hindeutet.

QUANTIFIZIERUNGSPROBLEM

FEHLER: KEINE NATURKONVEKTION WEGEN OPERATEURFEHLER,
OHNE ZEITFEHLER, OHNE ERWARTUNGSFEHLER UND FEHLVERHALTEN

1) KONTROLLAUSDRUCK DER EINGABEDATEN

CUT_SET	FEHLER1	MDN1	UF1	FEHLER2	MDN2	UF2	FEHLER3	MDN3	UF3	FEHLER4	MDN4	UF4
1	D1	0.0100	10		.	.		.	.		.	.
2	W9	0.0010	3	W9_2	0.15	3.3		.	.		.	.
3	U10	0.0200	5	U10_2	0.16	3.2	U10_3	0.51	1.9		.	.
4	W10	0.0010	3	W10_2	0.15	3.3		.	.		.	.
5	U11N	0.0130	5	U11N_2	0.16	3.2	U11N_3	0.51	1.9		.	.
6	W11N	0.0007	3	W11N_2	0.15	3.3		.	.		.	.
7	V11N	0.0170	10	V11N_2	0.16	3.2		.	.		.	.
8	V12N	0.0250	10	V12N_2	0.16	3.2		.	.		.	.
9	U13N	0.0250	5	U13N_2	0.16	3.2	U13N_3	0.51	1.9		.	.

2) CUT SETS SORTIERT NACH GROESSE (EW) UND AUFSUMMIERT

FEHLER1	FEHLER2	FEHLER3	FEHLER4	EW	EW_SUM	MDN_SUM	UF_SUM
D1				0.026635	0.026635	0.010000	10.0000
V12N	V12N_2			0.013680	0.040315	0.018228	7.9459
V11N	V11N_2			0.009302	0.049617	0.024980	6.8701
U13N	U13N_2	U13N_3		0.004562	0.054179	0.028966	6.3021
U10	U10_2	U10_3		0.003649	0.057828	0.032281	5.9078
U11N	U11N_2	U11N_3		0.002372	0.060200	0.034501	5.6731
W9	W9_2			0.000244	0.060444	0.034735	5.6492
W10	W10_2			0.000244	0.060688	0.034969	5.6255
W11N	W11N_2			0.000171	0.060859	0.035133	5.6090

3) ERGEBNISWAHRSCHEINLICHKEIT, WENN CUT SETS NICHT EXKLUSIV

MDN	UF	EW	VAR	STD	UG	OG
0.033862	5.73	0.059532	0.007409	0.006081	.0058995	0.19437

Abb. 13. Naturkonvektion. Operateurfehler mit Korrektur, ohne Zeitfehler:

Fehlerbeschreibungen in Tab. 18 auf Seite 59,

_2: 2. Operateur, _3: 3. Operateur

Späte Korrektur und dynamische Modellierung

Für die Fehler D1 bis W10 (Tab. 18 auf Seite 59) ist keine nachträgliche Korrektur möglich, weil sie dazu führen, daß die Naturkonvektion gar nicht erst eingeleitet wird. Für die Fehler U11N bis U13N wurde der in Tab. 17 auf Seite 57 nach dynamischer Modellierung berechnete Korrekturfaktor $0.54 < 5 >$ (EW = 0.87) angesetzt.

Außerdem wurde (als logische Konsequenz der dynamischen Modellierung) der in Tab. 16 auf Seite 57 quantifizierte Zeitfehler, $0.089 < 5 >$ (EW = 0.14), als zusätzliche Fehlerursache berücksichtigt. Damit ergibt sich eine Fehlerwahrscheinlichkeit von insgesamt $0.13 < 4.3 >$ (EW = 0.19) (Abb. 14 auf Seite 64). Das Unsicherheitsintervall $< 0.03, 0.56 >$ enthält den vom ISF geschätzten Wert (0.036) nur knapp.

QUANTIFIZIERUNGSPROBLEM

FEHLER: KEINE NATURKONVEKTION WEGEN OPERATEURFEHLER,
MIT ZEITFEHLER, OHNE ERWARTUNGSFEHLER UND FEHLVERHALTEN

1) KONTROLLAUSDRUCK DER EINGABEDATEN

CUT_SET	FEHLER1	MDN1	UF1	FEHLER2	MDN2	UF2	FEHLER3	MDN3	UF3	FEHLER4	MDN4	UF4
1	D1	0.0100	10									
2	W9	0.0010	3	W9_2	0.15	3.3						
3	U10	0.0200	5	U10_2	0.16	3.2	U10_3	0.51	1.9			
4	W10	0.0010	3	W10_2	0.15	3.3						
5	U11N	0.0130	5	U11N_2	0.16	3.2	U11N_3	0.51	1.9	N_S	0.54	5
6	W11N	0.0007	3	W11N_2	0.15	3.3				N_S	0.54	5
7	V11N	0.0170	10	V11N_2	0.16	3.2				N_S	0.54	5
8	V12N	0.0250	10	V12N_2	0.16	3.2				N_S	0.54	5
9	U13N	0.0250	5	U13N_2	0.16	3.2	U13N_3	0.51	1.9	N_S	0.54	5
10	N_Z	0.0085	5									

2) CUT SETS SORTIERT NACH GROESSE (EW) UND AUFSUMMIERT

FEHLER1	FEHLER2	FEHLER3	FEHLER4	EW	EW_SUM	MDN_SUM	UF_SUM
N_Z				0.14282	0.14282	0.00850	5.00000
D1				0.02664	0.16946	0.11197	4.47039
V12N	V12N_2		N_S	0.01192	0.18138	0.12083	4.40519
V11N	V11N_2		N_S	0.00811	0.18949	0.12768	4.31341
U13N	U13N_2	U13N_3	N_S	0.00398	0.19346	0.13168	4.23339
U10	U10_2	U10_3		0.00365	0.19711	0.13546	4.15723
U11N	U11N_2	U11N_3	N_S	0.00207	0.19918	0.13759	4.11647
W9	W9_2			0.00024	0.19942	0.13784	4.11144
W10	W10_2			0.00024	0.19967	0.13810	4.10643
W11N	W11N_2		N_S	0.00015	0.19982	0.13826	4.10338

3) ERGEBNISWAHRSCHEINLICHKEIT, WENN CUT SETS NICHT EXKLUSIV

MDN	UF	EW	VAR	STD	UG	OG
0.128706	4.30	0.190701	0.043471	0.208498	0.029929	0.55350

Abb. 14. Naturkonvektion. Operateurfehler mit Korrektur und Zeitfehler:

Fehlerbeschreibungen in Tab. 18 auf Seite 59

_2: 2. Operateur, _3: 3. Operateur, _S: späte Korrektur, _Z: Zeitüberschreitung

Auswertung und Kritik

Aus den Wahrscheinlichkeiten technischer ($EW = 0.07$) und menschlicher ($EW = 0.19$) Fehlerursachen der Naturkonvektion ergibt sich folgender Reduktionsfaktor $w(N)$ für die NWA-Ausfallwahrscheinlichkeit:

$$w(N) = w(N_T) + [1 - w(N_T)] w(N_M) = 0.07 + (1 - 0.07) 0.19 = 0.25$$

mit

$w(N_T)$ = Wahrscheinlichkeit (EW) für technisches Versagensursachen,

$w(N_M)$ = Wahrscheinlichkeit (EW) für menschliche Versagensursachen.

Dem hohen Beitrag ($EW = 0.14$; siehe "N_Z" in Abb. 14, Output 2) des Zeitfehlers ist zu entnehmen, daß die Zuverlässigkeit der Naturkonvektion in erster Linie ein Zeitproblem ist.

Diese Erkenntnis ist auch ohne aufwendige Analyse einsichtig. Für Auslegungsstfälle gilt die 30-Minuten-Regel: Innerhalb der ersten halben Stunde ist kein aktiver Eingriff des Personals erforderlich. Der hier betrachtete Anforderungsfall (ca. $1.0E-3/a$), NWA-Ausfall ($2.4E-3$) nach Ausfall der Hauptkühlung ($0.4/a$), ist ein auslegungsüberschreitender Störfall. Ein solcher Störfall stellt hohe kognitive Anforderungen an das Personal: Diagnose des Störfalltyps; Erkennen, daß ein auslegungsüberschreitender Störfall vorliegt; Entscheiden, welche Notfallprozedur anzuwenden ist. Und insbesondere: Die Bereitschaft, innerhalb der ersten 30 min überhaupt einen aktiven Eingriff vorzunehmen (s. Abschnitt 5).

Das Zeitproblem bekommt noch ein größeres Gewicht, wenn man zu der hier aus HRB (1983, S.101) abgeleiteten zulässigen Zeit (30 min nach NWA-Ausfall) eine Empfindlichkeitsbetrachtung vornimmt. Da laut HRB (1983, S.154) die Bypaßorgane sowieso nach 30 min automatisch geöffnet werden, stellt sich die Frage, warum überhaupt noch diesbezüglich eine Personalhandlung notwendig ist, wenn 30 min zulässig sind.

Eine Antwort ergibt sich aus den Rechnungen von HOLZKAMP (1988, S.92f). Es wurden - allerdings für den HTR-550, eine leicht modifizierte Version des HTR-500 - die Fälle sofortiges ($t = 0$) und verspätetes ($t = 30$ min) Öffnen der Bypaßorgane gerechnet. Für 30 min ergab sich eine Umkehr der auslegungsgemäßen Strömungsrichtung und somit keine ausreichende NWA.

Wenn man aufgrund dieser Rechnungen die zulässige Zeit auf 20 min reduziert, dann würde die Fehlerwahrscheinlichkeit auf über 50% ansteigen.

3.3.3.3 Querverbindung

Die in HRB (1983) genannte Gegenmaßnahme "Querverbindung" wurde vom ISF (1984) nicht berücksichtigt. Deshalb wird hier zunächst die technische Möglichkeit dieser Maßnahme probabilistisch bewertet.

Technisches Versagen

Durch Herstellen einer Querverbindung zwischen funktionierenden Kreisläufen können die in Tab. 15 auf Seite 55 unter Schritt 11 genannten Ausfallkombinationen korrigiert werden. Die Kombinationen a oder b sind nur in ca. 0.1 % aller NWA-Ausfälle zu erwarten (Tab. 14 auf Seite 53). Sie werden hier vernachlässigt.

Die Kombinationen c oder d (Gebläsekühlung ausgefallen) sind in ca. 10% aller NWA-Ausfälle zu erwarten. Für ihr Nichteintreten wurde folgende Abschätzung (Zahlenwerte in Tab. 13 auf Seite 53) durchgeführt:

1.9E-3 NWA-Ausfall wegen CCF

+ (1.6E-2)² Unabhängiger NWA-Ausfall (ohne Gebläsekühlung)

+ (6.9E-3)² Unabhängiger Ausfall der Gebläsekühlung

≈ 2.2E-3 = w(NWA_TQ_{TVP})

(technisches NWA-Versagen UND Querverbindung aufgrund technischer Ursachen vor Prozedurausführung unmöglich)

Ohne Berücksichtigung technischer Fehler während der Prozedur QUERVERBINDUNG erhält man also für das Ereignis "Querverbindung technisch unmöglich, wenn technisches NWA-Versagen":

$$w(Q_{TVP}|NWA_T) = w(NWA_T Q_{TVP})/w(NWA_T) = 2.2E-3/2.4E-3 \approx 0.9$$

mit

w(NWA_T) = Wahrscheinlichkeit für das technische Versagen der NWA.

Der Prozedurbeschreibung im Anhang D ist zu entnehmen, daß u.a. 6 Ventile zu betätigen sind. Unter der Annahme, daß es sich um (vor Ort zu bedienende) jährlich ($t=8760h$) getestete Handventile (Ausfallrate: $\lambda_i=4.7E-6/h$, EW aus ISF/GRS 1981) handelt, ergibt sich pro Ventil eine Ausfallwahrscheinlichkeit von

$$p_i = 0.5 t \lambda_i = 0.5 \cdot 8760 \cdot 4.7E-6 = 0.021$$

Für 1v6 Ventile gilt eine Ausfallwahrscheinlichkeit (ODER-Verknüpfung) von

$$p_{1v6} = 1 - (1 - p_i)^6 = 1 - (1 - 0.021)^6 = 0.12,$$

die hier gleich der Ausfallwahrscheinlichkeit $w(Q_{TWP})$ der Querverbindung aufgrund technischer Ursachen während Prozedurausführung gesetzt wird. Unter der Annahme, daß der 1v6-Ventil-Ausfall von dem technischen Versagen der NWA unabhängig ist, erhält man folgende bedingte Ausfallwahrscheinlichkeit der Querverbindung aufgrund technischer Ursachen (vor ODER während Prozedurausführung):

$$\begin{aligned} w(Q_T|NWA_T) &= w(Q_{TVP}|NWA_T) + w(Q_{TWP}) - w(Q_{TVP}|NWA_T) w(Q_{TWP}) \\ &= 0.9 + 0.12 - 0.9 \cdot 0.12 \approx 0.91 \end{aligned}$$

Operateurfehler

Da sich durch die Querverbindung die NWA-Ausfallwahrscheinlichkeit selbst bei 100%-ger menschlicher Zuverlässigkeit maximal um den Faktor 0.91 reduzieren läßt, wird hier auf eine aufwendige Zeitbedarfsanalyse verzichtet. Auch die Wahrscheinlichkeit für eine Fehldiagnose wird vernachlässigt, weil - mit Ausnahme der zulässigen NWA-Ausfalldauer (5 h bis 10 h) - keine zeitlichen Wirksamkeitsbedingungen erkennbar sind. Die hier durchgeführte menschliche Zuverlässigkeitsanalyse beschränkt sich also nur auf die "klassischen" Operateurfehler während der Durchführung.

Handlungen außerhalb der Warte

Außerhalb der Warte sind 6 Handventile zu betätigen (s. Anhang D). Für jedes Ventil wird ein Unterlassungsfehler (ID=3.111, s. Anhang E) und ein Verwechslungsfehler (ID=4.1121) unterstellt. Unter Annahme einer regelbasierten Tätigkeit bei mittelhohem Stress (PSF=2, s. Anhang F) und einfacher personeller Redundanz mit mittlerer Kopplung (s. Anhang G) ergeben sich folgende Wahrscheinlichkeiten:

- pro Ventil
 - Unterlassung:

$$\text{MDN} = 2 \cdot 0.01 \cdot 0.16 = 0.0032$$

$$\text{UF} = \exp\{[(\ln 5)^2 + (\ln 3.2)^2]^{0.5}\} = 7.3$$

$$\rightarrow \text{EW} = 0.0066, \text{STD} = 0.012$$
 - Verwechslung:

$$\text{MDN} = 2 \cdot 0.001 \cdot 0.15 = 0.0009$$

$$\text{UF} = \exp\{[(\ln 5)^2 + (\ln 3.3)^2]^{0.5}\} = 7.4$$

$$\rightarrow \text{EW} = 0.0019, \text{STD} = 0.0035$$
 - Unterlassung oder Verwechslung:

$$\text{EW} \simeq 0.0066 + 0.0019 = 0.0085$$

$$\text{STD} \simeq (0.012^2 + 0.0035^2)^{0.5} = 0.0125$$

$$\rightarrow \text{MDN} = 0.0048, \text{UF} = 5.8$$
- 1v6 Ventilen:

$$\text{EW} = 1 - (1 - 0.0085)^6 \simeq 0.05$$

$$\text{STD} \simeq (6 \cdot 0.0125^2)^{0.5} = 0.031$$

$$\rightarrow \text{MDN} = 0.042, \text{UF} = 2.6$$

Die Fehlerwahrscheinlichkeit der Querverbindung aufgrund von Operateurfehlern außerhalb der Warte beträgt demnach $0.042 < 2.6 >$.

Handlungen in der Warte, Gesamtbewertung

Tab. 19 enthält die Fehlerwahrscheinlichkeiten (ohne recovery) der berücksichtigten Handlungen in der Warte. Abb. 15 enthält alle Fehler (inner- und außerhalb Warte) einschließlich Korrekturfaktoren.

Aus diesen Fehlern wurde eine Wahrscheinlichkeit von $0.053 < 2.3 >$ ($\text{EW} = 0.06$) für das Mißlingen der Querverbindung aufgrund menschlicher Fehler berechnet. Den Hauptbeitrag liefern die Fehler außerhalb der Warte ($\text{EW} = 0.05$). Für den Reduktionsfaktor (EW) der Gegenmaßnahme Querverbindung erhält man:

$$\begin{aligned} w(Q) &= w(Q_T | \text{NWA}_T) + w(Q_M) - w(Q_T | \text{NWA}_T) w(Q_M) \\ &= 0.91 + 0.06 - 0.91 \cdot 0.06 \simeq 0.92 \end{aligned}$$

mit

$w(Q_T|NWA_T)$ = bedingte Ausfallwahrscheinlichkeit aufgrund technischer Ursachen,
 $w(Q_M)$ = Ausfallwahrscheinlichkeit aufgrund menschlicher Ursachen.

Menschliche Ursachen (0.06) liefern also nur einen unwesentlichen Beitrag zur Erhöhung der aufgrund technischer Ursachen (0.91) sowieso schon sehr hohen Versagenswahrscheinlichkeit der Querverbindung. Selbst nach einer Verdreifachung der Operateurfehlerwahrscheinlichkeit von 0.06 auf 0.18 würde sich nur eine Erhöhung des Reduktionsfaktors von 0.92 auf 0.93 ergeben.

BHEP-ID	PSF	MDN <UF>	FEHLER, BEMERKUNG
3.111	5	0.02 <5>	(U11Q) Nicht überprüft, ob eine Ausfallkombination vorliegt, die eine Querverbindung ermöglicht
2.2403	-	0.001 <3>	(W11Q) Nicht bemerkt, daß ... (s.o.)
3.111	2	0.02 <5>	(U13Q) Nach Abschluß der Handlungen vor Ort nicht überprüft, ob Bypaßorgan (GBO) am noch nicht angeforderten Gebläse geschlossen. Effekt: Gebläse werden mit geöffneten GBO gestartet → Gebläseschaden (Annahme)
2.2403	-	0.001 <3>	(W13Q) Nicht bemerkt, daß 1v2 GBO geöffnet. Effekt: s.o.
3.111	2	0.02 <5>	(U14Q) Gebläse nicht gestartet

Tab. 19. Querverbindung. Operateurfehler in der Warte ohne recovery

QUANTIFIZIERUNGSPROBLEM

FEHLER: QUERVERBINDUNG VERSAGT WEGEN OPERATEURFEHLER,
ZEITFEHLER VERNACHLAESSIGT, OHNE FEHLVERHALTEN UND ERWARTUNGSFEHLER

1) KONTROLLAUSDRUCK DER EINGABEDATEN

CUT_SET	FEHLER1	MDN1	UF1	FEHLER2	MDN2	UF2	FEHLER3	MDN3	UF3	FEHLER4	MDN4	UF4
1	U11Q	0.020	5.0	U11Q_2	0.16	3.2	U11Q_2	0.51	1.9		.	.
2	W11Q	0.001	3.0	W13Q_2	0.15	3.3		.	.		.	.
3	UV12Q	0.042	2.5		.	.		.	.		.	.
4	U13Q	0.020	5.0	U13Q_2	0.16	3.2	U13Q_3	0.51	1.9		.	.
5	W13Q	0.001	3.0	W13Q_2	0.15	3.3		.	.		.	.
6	U14Q	0.020	5.0	U14Q_2	0.16	3.2	U14Q_3	0.51	1.9		.	.

2) CUT SETS SORTIERT NACH GROESSE (EW) UND AUFSUMMIERT

FEHLER1	FEHLER2	FEHLER3	FEHLER4	EW	EW_SUM	MDN_SUM	UF_SUM
UV12Q				0.049048	0.049048	0.042000	2.50000
U11Q	U11Q_2	U11Q_2		0.003649	0.052697	0.045620	2.41925
U13Q	U13Q_2	U13Q_3		0.003649	0.056347	0.049245	2.34867
U14Q	U14Q_2	U14Q_3		0.003649	0.059996	0.052074	2.28639
W11Q	W13Q_2			0.000244	0.060240	0.053137	2.27971
W13Q	W13Q_2			0.000244	0.060484	0.053399	2.27309

3) ERGEBNISWAHRSCHEINLICHKEIT, WENN CUT SETS NICHT EXKLUSIV

MDN	UF	EW	VAR	STD	UG	OG
0.052747	2.28	0.059879	0.001035	0.032174	0.023036	0.12078

Abb. 15. Querverbindung. Operateurfehler mit Korrekturmöglichkeiten:

Fehlerbeschreibungen in Tab. 19;

_2: 2. Operateur, _3: 3. Operateur, UV12Q: außerhalb Werte

3.3.3.4 Reparatur

Zulässige Reparaturzeit

Die zulässige Reparaturzeit t ist gleich der zulässigen NWA-Ausfallzeit. Die zulässige Ausfallzeit ist der letztmögliche Zeitpunkt einer verzögerten Inbetriebnahme der NWA (vgl. ISF 1984, S.30). Dieser letztmögliche Zeitpunkt hängt u.a. von folgenden Schäden aufgrund thermischer Belastungen ab:

- Versagen der Heißgasleitungen, NWA-Wärmetauscher oder NWA-Gebläse. Für die Heißgasleitungen wird in ISF (1984, S.57) ein Grenzwert von 1100 °C genannt.
- Absturz des Deckenreflektors. Grenzwert lt. ISF (1984, S.123f): 800 °C.

- Schmelzen der Kernstabhüllrohre. Grenzwert lt. ISF (1984, S.139): 1400 °C.

Hier wird nur der erste Punkt betrachtet, weil er im Vergleich zu den anderen beiden den größten Einfluß auf die Möglichkeit eines NWA-Spätstarts hat.

Die thermodynamischen Verhältnisse an diesen Komponenten hängen u.a. von folgenden Systemzuständen nach NWA-Ausfall ab:

1. NWA-Wärmesenke wirksam? D.h. Wärmetauscher gekühlt und Bypaßorgane (GBO) geöffnet?
 - a. 2v2 wirksam
 - b. nur 1v2 wirksam
 - c. 2v2 unwirksam
2. Zustand der Hauptabsperrrklappen (HAK) nach 30 min (wenn Wärmesenke unwirksam)?
 - a. 8v8 auf
 - b. 1v8 auf UND 1v8 zu
 - c. 8v8 zu
3. Schließversagen des RDB-Sicherheitsventils (nach Öffnen bei ca. 55 bar)?
 - a. nein
 - b. ja

Tab. 20. Zustandsvariablen nach NWA-Ausfall

Vom ISF (1984, S.78) wurde zu einer der möglichen Kombinationen aus den o.g. Zuständen eine NWA-Spätstartrechnung durchgeführt: (1c, 2c, 3a). Bis auf Punkt 3a wurde die jeweils ungünstigste Bedingung angesetzt. Die Rechnung ergab, daß nach einem um 6,5 h verzögerten Spätstart die Heißgastemperaturen im Mittel unterhalb des zulässigen Werts (1100°C) liegen. Es konnte aber nicht ausgeschlossen werden, daß lokale Strähnen auftreten, die 1100°C erreichen. Das ISF (1984, S.30) hält daher 5 h für eine konservative Abschätzung der zulässigen Reparaturzeit.

Die HRB (1983, S.9) hält 5 h bis 10 h für zulässig, nennt aber eine Reparaturwahrscheinlichkeit von 50% (S.101), die sich für 5 h bei einer mit dem Mittelwert (MTTR) 8 h (ISF 1984, S.20) exponentiellverteilten Reparaturdauer ergeben würde. Im Gegensatz zum ISF unterstellt die HRB (S.158) bei ausgefallener Wärmesenke den Zustand 2a (8v8 HAK auf). Dieser Zustand bewirkt lt. ISF (1984, S.57) eine Kaltgasbeimischung beim Spätstart, sodaß auch noch nach 10 h die Heißgastemperatur unterhalb 1100°C liegen wird.

Auch der Vergleich von Abb. 16 mit Abb. 17 zeigt, daß der Zustand "8v8 HAK auf" einen günstigen Einfluß auf den Temperaturverlauf hat: Die maximale Temperatur

bleibt unterhalb des Auslegungsgrenzwertes 1250°C (vgl. BLINDERT 1988, S.33) der Brennelemente. Diese Aussage ist jedoch nur bis 10 h abgesichert. Denn bis 10 h ist der in HRB gerechnete Fall, konstant 50 bar, mit dem realistischen Fall, Ansprechen des Sicherheitsventils nach 1 h bis 5 h und Versagen in Offenstellung (ISF 1984, S.30), vergleichbar (HRB, S.170). Nach 10 h ergeben sich - auch dann, wenn es gelingt, die Druckentlastung über das Sicherheitsventil bei 30 bar zu stoppen - im realistischen Fall wesentlich ungünstigere Temperaturverläufe (vgl. ISF 1984, S.80) als bei konstant 50 bar.

Als Ergebnis der Diskussion der thermodynamischen Verhältnisse wird hier folgende Annahme zur zulässigen Reparaturzeit getroffen:

- 5 h, wenn nicht beide Wärmesenken wirksam (d.h. Zustand 1b oder 1c in Tab. 20) UND nicht alle HAK auf (d.h. Zustand 2b oder 2c in Tab. 20);
- sonst: 10 h.

Bei 5 h wird der Temperaturverlauf in Abb. 16, bei 10 h der in Abb. 17 bzw. der in Abb. 18 (wenn Zustand 1a in Tab. 20) unterstellt. In Tab. 21 auf Seite 77 sind diese Annahmen und die sich daraus ergebenden Konsequenzen zusammengefaßt.

Die Wahrscheinlichkeit, daß nicht 10 h sondern 5 h verfügbar sind berechnet sich wie folgt (Zahlenwerte aus Tab. 13 auf Seite 53 und Tab. 14 auf Seite 53):

Wärmesenke unwirksam (0.015), WEIL
1v2 GBO geschlossen (0.014) ODER
1v2 WT nicht gekühlt (0.001)

UND

1v8 HAK zu nach 30 min (0.109), WEIL
1v8 HAK anfangs auf (0.056) UND 1v8 HAK öffnet nicht nach 30 min (≈ 1.0)
ODER
8v8 HAK anfangs zu (0.944) UND 1v8 HAK öffnet nicht nach 30 min (0.056)

Es wurde angenommen, daß ein anfänglicher Schaden an den HAK mit der Wahrscheinlichkeit 1.0 auch eine spätere Fehlfunktion (nach 30 min) zur Folge hat.

Als Ergebnis erhält man eine Wahrscheinlichkeit von 0.0016. Das Ereignis kann nur eintreten, wenn die Naturkonvektion technisch unmöglich ist (0.07). In der Wahr-

scheinlichkeit 0.0016 ist das Ereignis "Naturkonvektion technisch unmöglich" enthalten. Deshalb gilt für das Ereignis "nur 5 h Zeit", unter der Bedingung, daß Naturkonvektion technisch unmöglich:

$$w(R5|N_T) = [w(N_T R5)]/w(N_T) = 0.0016/0.07 = 0.023.$$

mit

$w(N_T R5)$ = Wahrscheinlichkeit, daß Naturkonvektion technisch unmöglich UND nur 5 h Zeit für Reparatur,

$w(N_T)$ = Wahrscheinlichkeit, daß Naturkonvektion technisch unmöglich.

Wenn die Naturkonvektion aufgrund technischer Ursachen versagt, ist also in nur 2.3% aller reparierbaren NWA-Ausfälle eine reduzierte (5 h) Reparaturzeit verfügbar.

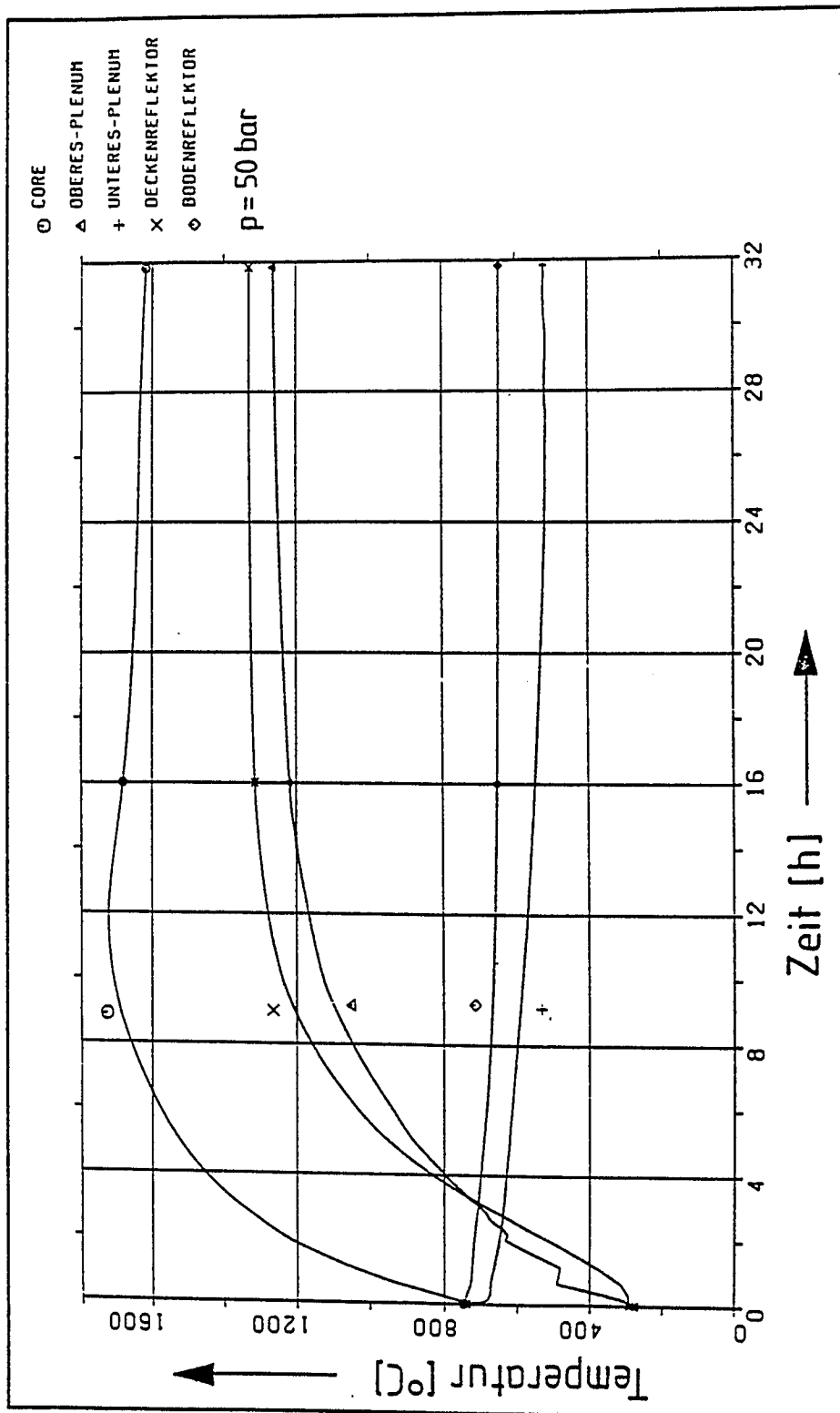


Abb. 16. Kernaufheizung ohne Wärmetauscherbespeisung, HAK geschlossen:
(ISF 1984, S. 76 u. 57)

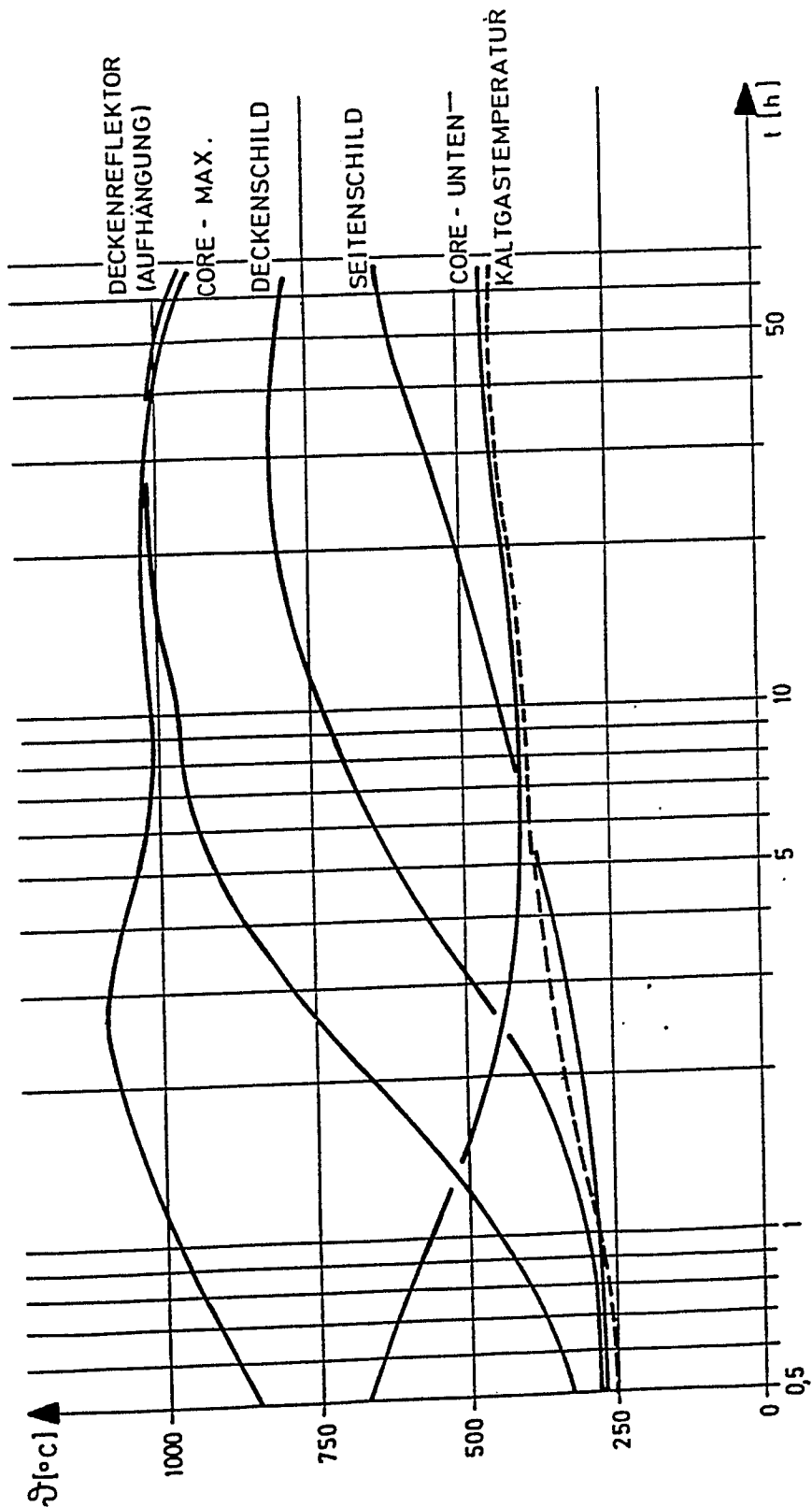


Abb. 17. Kernaufheizung ohne Wärmetauscherbespeisung, HAK nach 0.5 h geöffnet:
(HRB 1983. S. 163 u. 154)

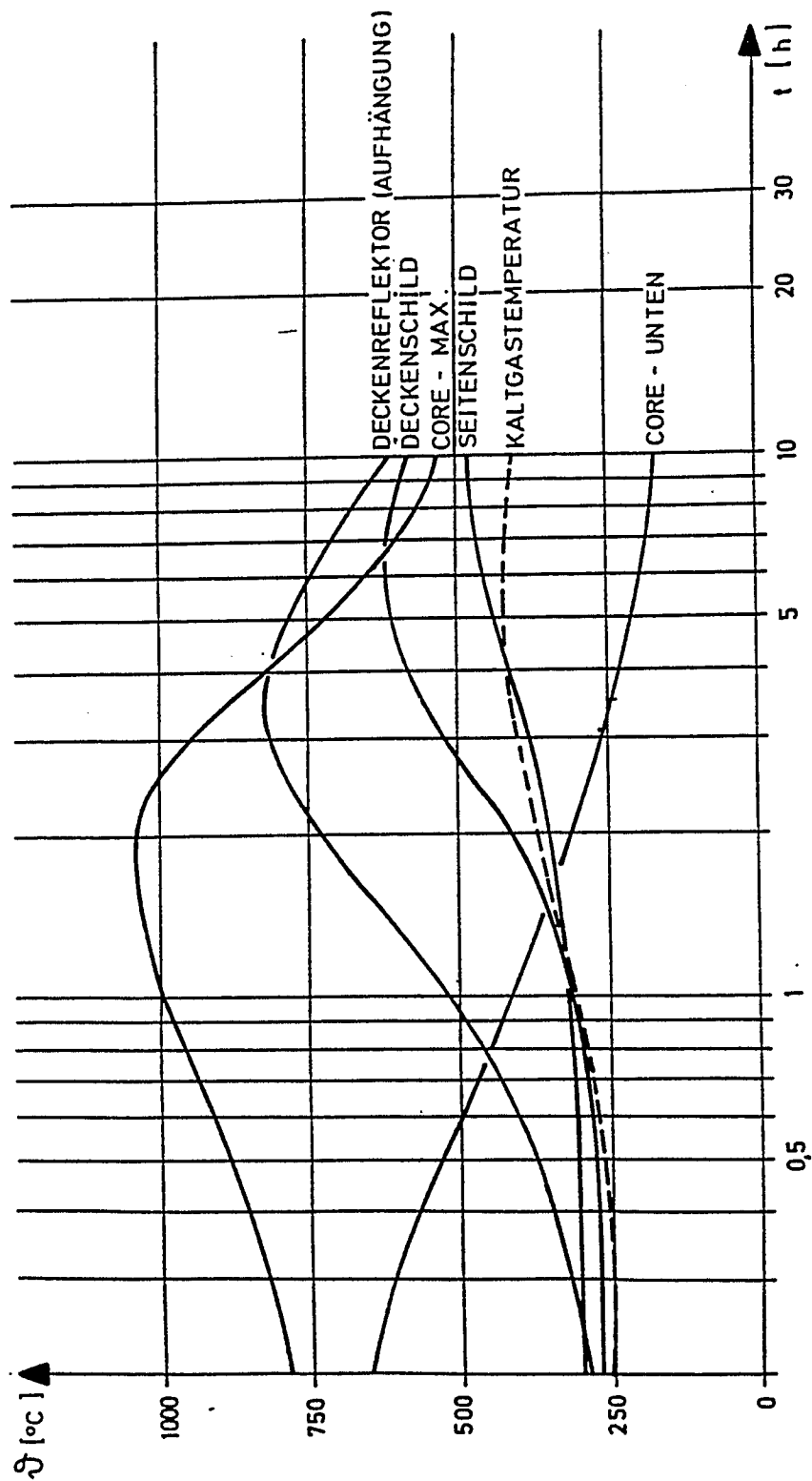


Abb. 18. Kernaufheizung ohne Zwangskonvektion, beide Wärmetauscher bespeist:
(HRB 1983, S. 162 u. 156)

NWA-Ausfallzustand → Belastung ↓	Wärmesenke in beiden Strän- gen wirksam	Wärmesenke nicht in beiden Strängen wirk- sam UND alle HAK geöffnet	Wärmesenke nicht in beiden Strängen wirk- sam UND nicht alle HAK geöff- net
NWA-Spätstart unmöglich, wenn...	$T \geq 10 \text{ h}$	$T \geq 10 \text{ h}$	$T \geq 5 \text{ h}$
Temperaturverlauf bis 10 h	Abb. 18	Abb. 17	Abb. 16
Brennelemente $1600^{\circ}\text{C}^{*1}$, wenn...	NWA-Spätstart unmöglich		
Kernstabhüllrohre $1400^{\circ}\text{C}^{*2}$, wenn...	NWA-Spätstart unmöglich		$T \geq 3 \text{ h}$
Brennelemente $1250^{\circ}\text{C}^{*3}$, wenn...	NWA-Spätstart unmöglich		$T \geq 2 \text{ h}$
Deckenreflektor 800°C^{*4} , wenn...	$T \geq 3 \text{ h}$	$T \geq 3 \text{ h}$	$T \geq 4 \text{ h}$
Primärkreis-Druck 55 bar ^{*5} , wenn...	$T \geq 1 \text{ h}$	$T \geq 1 \text{ h}$	$T \geq 5 \text{ h}$
Kernstabhüllrohre 850°C^{*6} , wenn...	$T \geq 0.5 \text{ h}$	$T \geq 0.5 \text{ h}$	$T \geq 0 \text{ h}$

Tab. 21. HTR-500. Kernaufheizung. Belastungsannahmen:

T = Reparaturdauer

* Anmerkungen zu Tab. 21

1. Verlust der Spaltproduktrückhaltefunktion (ISF 1984, S.81)
2. Schmelzpunkt (ISF 1984, S.139)
3. Auslegungsgrenzwert (vgl. BLINDERT 1988, S.33)
4. Absturz (ISF 1984, S.123f)
5. Druckentlastung über Sicherheitsventil (vgl. HRB 1983, S.157f; ISF 1984, S.8)
6. Austausch erforderlich (HRB 1983, S.169)

Reparaturversagenswahrscheinlichkeit

In Anlehnung an ISF (1984) wird von einer exponentiellverteilten Reparaturdauer T ausgegangen. D.h. für die Wahrscheinlichkeit einer nicht rechtzeitigen Reparatur gilt:

$$P(t) = w(T \geq t) = e^{-t/x}$$

mit

x = MTTR = mittlere Reparaturdauer,

t = zulässige Reparaturzeit.

Vom ISF (1984, S.20) wurde für x ein Punktwert von 8 h, ohne Unsicherheiten, verwendet. Entsprechend des hier gewählten Ansatzes, daß zu allen menschlichen Einflüssen Unsicherheiten berücksichtigt werden, wird x als Zufallsgröße mit einem Erwartungswert E_x von 8 h interpretiert. Zur Schätzung der Standardabweichung D_x wird auf die in REER durchgeführten Auswertungen von Reparaturstatistiken (GRS 1980, S.66) zurückgegriffen. Diese Auswertungen ergaben für vergleichbare Reparaturfälle (MTTR-Werte für Pumpen; vgl. Tab. 12 auf Seite 51, Anmerkung 1) einen Variationskoeffizienten, $CV = D_x/E_x$, von ca. 0.7. Daraus erhält man folgende Standardabweichung:

$$D_x = 0.7 \cdot 8 \text{ h} = 5.6 \text{ h}$$

Mit den bekannten Regeln der Fehlerfortpflanzung lassen sich nun Erwartungswert $EP(t)$ und Standardabweichung $DP(t)$ der Reparaturversagenswahrscheinlichkeit bestimmen:

$$EP(t) = e^{-t/E_x}$$

$$\simeq 0.5 \text{ für } t = 5 \text{ h}$$

$$\simeq 0.3 \text{ für } t = 10 \text{ h}$$

$$P'(t) = \partial[P(t)]/\partial x = (t/x^2) e^{-t/x}$$

$$EP'(t) = [t/(E_x)^2] e^{-t/E_x}$$

$$DP(t) \simeq \{(D_x)^2 [EP'(t)]^2\}^{0.5}$$

$$= 5.6 \cdot 5/8^2 \cdot 0.5 \simeq 0.22 \text{ für } t = 5 \text{ h}$$

$$= 5.6 \cdot 10/8^2 \cdot 0.3 \simeq 0.26 \text{ für } t = 10 \text{ h}$$

Unter der Voraussetzung einer Lognormalverteilung von $P(t)$ erhält man:

$$MDN = EP(t) \{1 + [DP(t)]^2/[EP(t)]^2\}^{-0.5}$$

$$= 0.46 \text{ für } t = 5 \text{ h}$$

$$= 0.23 \text{ für } t = 10 \text{ h}$$

$$UF = e^{1.645 \{ \ln[1 + [DP(t)]^2/[EP(t)]^2] \}^{0.5}}$$

= 2 für t = 5 h
 = 3.4 für t = 10 h

Für 5 h beträgt die Reparaturversagenswahrscheinlichkeit $0.46 < 2 >$, für 10 h $0.23 < 3.4 >$. Der Median fällt mit zunehmender Zeit, der Unsicherheitsfaktor steigt. Ein plausibler Trend.

3.3.3.5 Zusammenfassende Bewertung der menschlichen Gegenmaßnahmen

Um die - methodisch nicht uninteressante - Vorgehensweise durchzuhalten, daß technische Fehler ohne , menschliche Fehler aber mit Unsicherheiten berücksichtigt werden, wurden die Kombinationen technischer Möglichkeiten nach NWA-Ausfall aufgelistet und probabilistisch bewertet. Das Ergebnis sind 10 Kombinationen, die sich einander ausschließen (Tab. 22).

Technisch möglich				Zusammenfassung	
(N)* ¹ Naturkon- vektion	(Q)* ² Querverbin- dung	(R)* ³ Reparatur	(R10)* ⁴ 10 h Zeit für Reparatur	NEIN-Kette	Wahrsch.
JA	JA	JA	JA	___	3.7E-2
JA	JA	NEIN	NEIN	__R	5.6E-2
JA	NEIN	JA	JA	_Q_	2.8E-1
JA	NEIN	NEIN	NEIN	_QR	5.6E-1
NEIN	JA	JA	JA	N__	2.7E-3
NEIN	JA	JA	NEIN, 5h	N_R10	6.4E-5
NEIN	JA	NEIN	NEIN	N_R	4.2E-3
NEIN	NEIN	JA	JA	NQ_	2.0E-2
NEIN	NEIN	JA	NEIN, 5h	NQR10	4.8E-4
NEIN	NEIN	NEIN	NEIN	NQR	4.2E-2

Tab. 22. Wahrscheinlichkeiten technischer Möglichkeiten nach NWA-Ausfall:

* Anmerkungen zu Tab. 22

1. N=NEIN, wenn 1v2 WT nicht gekühlt, 1v2 GBO Öffnungsversagen oder 1v8 HAK Schließversagen.
 $w(N=NEIN) = 0.07$
2. Q=JA, wenn Ausfall Zwangskonvektion (ohne Gebläsekühlung) Strang 1 bzw. 2 und Ausfall Gebläsekühlung Strang 2 bzw. 1 oder

Ausfall Wärmesenke Strang 1 bzw. 2 und Ausfall Zwangskonvektion Strang 2 bzw. 1.

$$w(Q=JA) = 0.1$$

3. R=NEIN, wenn Ausfall von jeweils GAO, Trafo, Umrichter oder Gebläse in Strang 1 und 2.

$$w(R=NEIN | Q=JA) = 0.6$$

$$w(R=NEIN | Q=NEIN) = 0.67$$

4. R10=NEIN, wenn 1v2 GBO Schließversagen oder 1v2 WT nicht gekühlt und 1v8 HAK nach 30 min Öffnungsversagen.

$$w(R10=NEIN | R=NEIN) = 1.0$$

$$w(R10=NEIN | N=JA) = 0$$

$$w(R10=NEIN | N=NEIN) = 0.023$$

Die Wahrscheinlichkeit jeder Kombination gilt unter der Bedingung, daß die NWA aufgrund technischer Ursachen ausgefallen ist ($2.4E-3$). Die Summe der Wahrscheinlichkeiten ergibt (abgesehen von Rundungsfehlern) 1.

Eine wichtige Aussage der Tab. 22 ist, daß auch bei 100%-iger menschlicher Zuverlässigkeit die NWA-Ausfallwahrscheinlichkeit ($2.4E-3$) nur um den Faktor $4.2E-2$ (NEIN-Kette NQR) auf $1.0E-4$ reduzierbar ist.

In Abb. 19 sind die menschlichen Fehlerwahrscheinlichkeiten dieser Kombinationen aufgelistet, zusammengefaßt und ausgewertet. Insgesamt ergibt sich eine Versagenswahrscheinlichkeit der Gegenmaßnahmen von $0.14 < 2.8 >$ (EW = 0.17; Abb. 19, Output 2, "EW_SUM"). Die Hauptbeiträge hierzu liefern die Ketten

- Naturkonvektion mißlingt wegen Operateurfehler und Reparatur und Querverbindung technisch unmöglich (EW ≈ 0.11) und
- Naturkonvektion, Querverbindung und Reparatur technisch unmöglich (EW = 0.042).

Wenn man die hier für die meisten Fälle angesetzte zulässige Reparaturzeit von 10 h auf 5 h reduziert, dann erhöht sich die Versagenswahrscheinlichkeit nur geringfügig von 0.17 auf 0.19.

Die Wahrscheinlichkeit des NWA-Ausfall reduziert sich (aufgrund des Faktors 0.17) von $2.4E-3$ auf $4.1E-4 < 1.2E-4, 9.4E-4 >$. Durch das Unsicherheitsintervall (aufgrund menschlicher Variationsursachen) wird der vom ISF (ohne aufwendige Analyse

menschlichen Verhaltens; s. Tab. 12., Anmerkung 3) berechnete Wert (2.4E-4) mit ausreichender Sicherheit erfaßt.

QUANTIFIZIERUNGSPROBLEM

FEHLER: GEGENMASSNAHMEN ERFOLGLOS, FEHLER1: TECHNIK,
FEHLER2-4: PERSONAL, OHNE FEHLVERHALTEN UND ERWARTUNGSFEHLER

1) KONTROLLAUSDRUCK DER EINGABEDATEN

CUT_SET	FEHLER1	MDN1	UF1	FEHLER2	MDN2	UF2	FEHLER3	MDN3	UF3	FEHLER4	MDN4	UF4
1	—	0.03700	1	N	0.13	4.3	Q	0.053	2.3	R	0.23	3.4
2	—R	0.05600	1	N	0.13	4.3	Q	0.053	2.3		.	.
3	—Q	0.28000	1	N	0.13	4.3		.	.	R	0.23	3.4
4	—QR	0.56000	1	N	0.13	4.3		.	.		.	.
5	N—	0.00270	1		.	.	Q	0.053	2.3	R	0.23	3.4
6	N_R10	0.00006	1		.	.	Q	0.053	2.3	R10	0.46	2.0
7	N_R	0.00420	1		.	.	Q	0.053	2.3		.	.
8	NQ—	0.02000	1		.	.		.	.	R	0.23	3.4
9	NQR10	0.00048	1		.	.		.	.	R10	0.46	3.4
10	NQR	0.04200	1		.	.		.	.		.	.

2) CUT SETS SORTIERT NACH GROESSE (EW) UND AUFSUMMIERT

FEHLER1	FEHLER2	FEHLER3	FEHLER4	EW	EW_SUM	MDN_SUM	UF_SUM
—QR	N			0.10786	0.10786	0.07280	4.30000
NQR				0.04200	0.14986	0.11777	3.13272
—Q—	N		R	0.01636	0.16622	0.13436	2.92466
NQ—			R	0.00607	0.17228	0.14092	2.83750
—R	N	Q		0.00065	0.17293	0.14162	2.82841
NQR10			R10	0.00029	0.17323	0.14194	2.82434
N_R		Q		0.00025	0.17348	0.14222	2.82082
—	N	Q	R	0.00013	0.17361	0.14236	2.81901
N—		Q	R	0.00005	0.17366	0.14241	2.81833
N_R10		Q	R10	0.00000	0.17366	0.14241	2.81830

Abb. 19. Gegenmaßnahmen. Menschliche und technische Fehler. Gesamtbewertung:

Fehler 1: Technik (s. Tab. 22);

Fehler 2-4: Personal (N = Naturkonvektion, Q = Querverbindung, R = Reparatur)

3.4 Zusammenfassung von Abschnitt 3

Der HTR-500, das Konzept eines mit Helium gekühlten Hochtemperaturreaktors mittlere Leistung (500 MWe), ist die Referenzanlage der hier vorliegenden Arbeit. Die Anwendung der methodischen Erweiterungen erfolgt am Beispiel der Zuverlässigkeit des Systems zur Nachwärmeabfuhr (NWA) nach Ausfall des Hauptkühlsystems (bei Reaktor unter Druck und intakter Eigenbedarfsversorgung) - eine Transiente, die am häufigsten (ca. alle zwei Jahre) das NWA-System anfordern wird.

Das NWA-System besteht aus zwei Kreisläufen, von denen jeder zu 100% die Nachwärme abführen kann. Nach NWA-Anforderung wird zunächst die NWA-Wärmesenke aufgebaut, um die Wärmetauscher des Primärkreises und die Hilfsgebläse zu kühlen. Ca. 3 min später werden beide Hilfsgebläse gestartet, welche die Nachwärme des Primärkreises zu den Wärmetauschern transportieren.

Ausgehend von den Ergebnissen der technischen Zuverlässigkeitsanalyse des ISF (1984) wurde der Einfluß menschlichen Verhaltens gemäß der klassischen Zielsetzung, NWA AUSREICHEND, auf die NWA-Ausfallwahrscheinlichkeit analysiert. Wahrscheinlichkeiten technischer Fehler wurden als Punktwerte (ohne Streuungen), Wahrscheinlichkeiten menschlicher Fehler als Zufallsgrößen (mit Streuungen) modelliert. So konnte der separate Einfluß der Variabilität menschlicher Handlungen auf die Unsicherheit des Endergebnisses berechnet werden.

Ohne Gegenmaßnahmen des Personals liegt die Ausfallwahrscheinlichkeit der NWA bei $2.4E-3$. Laut Hersteller HRB kommen als Gegenmaßnahmen drei Möglichkeiten in Betracht: (1) Herstellen einer NATURKONVEKTION (passive NWA) durch Öffnen der Bypaßorgane an den NWA-Gebläsen, (2) Umschaltmaßnahmen zur Herstellung einer QUERVERBINDUNG zwischen funktionierenden Kreisläufen und (3) REPARATUR ausgefallener Bauteile. Diese Maßnahmen sind nicht immer technisch möglich: Selbst bei 100%-iger menschlicher Zuverlässigkeit ist durch sie nur eine Reduktion der NWA-Ausfallwahrscheinlichkeit auf $1.0E-4$ erreichbar.

Nach Durchführung einer Analyse technischer und menschlicher Fehlerursachen ergab sich eine Reduktion auf $4.1E-4$ mit $< 1.2E-4, 9.4E-4 >$ als 90%-Unsicherheitsintervall. Der vom ISF (1984) berechnete Wert ($2.4E-4$) wird durch dieses Intervall abgedeckt.

Die hier durch geführte Analyse der Gegenmaßnahmen nach NWA-Ausfall unterscheidet sich von der in ISF (1984) durchgeführten Analyse in drei wesentlichen Punkten:

1. Für die Maßnahme NATURKONVEKTION wurde eine aufwendige Operateurfeleranalyse durchgeführt; in ISF (1984) wurde hierzu eine erste Abschätzung vorgenommen (s. Tab. 12, Anmerkung 3).
2. Die Maßnahme QUERVERBINDUNG wurde berücksichtigt; in ISF (1984) nicht.
3. Die verfügbare Zeit für die Maßnahme REPARATUR wurde in Abhängigkeit vom NWA-Ausfallzustand modelliert; in ISF (1984) wurde konservativ für alle reparierbaren Ausfallzustände eine verfügbare Zeit von 5 h angesetzt.

Eine Analyse der Beiträge zum Versagen der Gegenmaßnahmen ergab, daß deren Zuverlässigkeit in erster Linie ein Zeitproblem, in zweiter Linie ein technisches Problem und erst in dritter Linie ein Problem der "klassischen" (zeitunabhängigen) Operateurfehler (wie z.B. Unterlassungs- oder Verwechslungsfehler) ist. Die NATURKONVEKTION hat zwar einen relativ kleinen Zeitbedarf ($EW = 22$ min), die zulässige Zeit dieser Maßnahme ist aber ebenfalls klein (30 min). Die REPARATUR hat zwar eine hohe zulässige Zeit (5 h bis 10 h), aber ihr Zeitbedarf ist auch sehr hoch ($EW = 8$ h). Die QUERVERBINDUNG weist zwar ein günstiges Verhältnis zwischen verfügbarer und benötigter Zeit auf, aber sie ist in nur 10% aller NWA-Ausfälle technisch möglich.

Der effektivste Weg, die NWA-Zuverlässigkeit noch weiter zu erhöhen, liegt in der Reduktion des Zeitbedarfs der NATURKONVEKTION, z.B. durch einen Störfallrechner, der den NWA-Ausfallzustand analysiert und die Operateure sehr schnell auf die Notwendigkeit der NATURKONVEKTION hinweist. Vor dem Hintergrund, daß bei Auslegungsstörfällen innerhalb der ersten 30 min keine aktive Personalhandlung erforderlich ist, bleibt die Zuverlässigkeit von Personalhandlungen innerhalb der ersten 30 min nach einem auslegungsüberschreitenden Störfall jedoch stets ein ernstes Problem.

4. Identifizierung von Rückwirkungen untergeordneter Ziele

4.1 Einführung

Folgende untergeordnete Ziele werden hier näher untersucht:

1. Betriebliche Aspekte (z.B. Komponentenschonung), die gegenüber dem "klassischen" Hauptziel SICHERHEIT (d.h. Vermeidung radiologischer Konsequenzen) eine untergeordnete Priorität haben.
(Nähere Erläuterungen im Abschnitt 4.2.1.)
2. Konkrete Systemzustände (z.B. die Stellung von Armaturen), die zur Realisierung des Hauptziels erforderlich sind, aber auch in anderen Zusammenhängen relevant sind.
(Nähere Erläuterungen im Abschnitt 4.2.2.)

Die Identifizierung solcher Ziele ist äußerst hilfreich für eine realitätsnahe Einbeziehung menschlichen Verhaltens in eine probabilistische Risikoanalyse (PRA). Im Abschnitt 2 wurde anhand eines konkreten Störfalls gezeigt, daß aus der Existenz des Ziels KEINE GEBÄUDEKONTAMINATION eine logische Begründung für das zögerliche Verhalten des Personals bezüglich des Einleitens der primärseitigen Nachwärmeabfuhr (NWA) ableitbar ist. In Abschnitt 4.2 wird eine Methode zur Identifizierung solcher Ziele vorgeschlagen. Eine Methode zur Identifizierung der daraus ableitbaren Rückwirkungen (vgl. Abschnitt 1.1) auf die Sicherheit wird im Abschnitt 4.3 vorgestellt.

4.2 Identifizierung untergeordneter Ziele

4.2.1 Betriebliche Aspekte

Das hier vorgeschlagene Verfahren zur Identifizierung von Konfliktsituationen (als Ursachen von Entscheidungsfehlern im Sinne einer bewußten Risikoannahme) beginnt mit der Identifizierung betrieblicher Aspekte, die gegenüber dem Hauptziel SICHERHEIT eine untergeordnete Priorität haben. Dabei wird von folgender Fragestellung ausgegangen:

Welche Nachteile können auftreten, obwohl das betrachtete Hauptziel realisiert wird?

Die VERMEIDUNG eines aufgrund dieser Frage identifizierten NACHTEILS wird dann als Ziel untergeordneter Bedeutung definiert.

Das verwendete Grundscheema ist in Tab. 23 dargestellt.

1.	Konkrete Definition des Hauptziels, z.B. NWA RESA GEBÄUDEABSCHLUSS
2.	Untergliederung möglicher Realisierungen des Hauptziels, z.B. nach den Kriterien REDUNDANZGRAD, BETRIEBSWEISE ANFORDERUNG SYSTEMFREMDER KOMPONENTEN? MENSCHLICHE EINGRIFFE ERFORDERLICH? STRATEGIEN MENSCHLICHER EINGRIFFE SYSTEMAUSFALLZUSTÄNDE SYSTEMAUSFALLZEITEN
3.	Identifizierung von Nachteilen der Realisierungen, z.B. anhand der Kriterien SUBJEKTIVE ASPEKTE UNGEWOHNTHEIT KOMPLIZIERTHEIT NICHT ÜBERSCHAUBARER ZEITRAHMEN OBJEKTIVE, ZEITUNABHÄNGIGE ASPEKTE KOMPONENTENSCHÄDEN REINIGUNGSARBEITEN BEHÖRDLICHE UNTERSUCHUNGEN DES AUSMASSES EINGETRETENER SCHÄDEN DER URSACHE AUFGETRETENER AUSFÄLLE OBJEKTIVE, ZEITABHÄNGIGE ASPEKTE SCHÄDEN AUFGRUND ZEITABHÄNGIGER TEMPERATURBELASTUNGEN DRUCKERHÖHUNGEN/VERRINGERUNGEN FÜLLSTÄNDE/MENGEN

Tab. 23. Verfahren zur Identifizierung von Nachteilen trotz Hauptzieleinhaltung

Der Ablauf in Tab. 23 beginnt mit der Definition des Hauptziels. Das Hauptziel bezieht sich auf das Ereignis, für dessen Nichteintreten die Wahrscheinlichkeit zu berechnen ist. Hier: HTR-500. NWA AUSREICHEND.

Die nächsten beiden Schritte bilden für viele Untergliederungskriterien eine Einheit. Oftmals ergeben sich die Nachteile direkt aus den Untergliederungskriterien. In Tab. 24 wurden diese beiden Schritte für das hier betrachtete Hauptziel HTR-500-NWA AUSREICHEND durchgeführt.

Kriterium	Erläuterung	Beispiel HTR-500
Redundanzgrad	Gibt es Realisierungen des Hauptziels, die vorhandene Sicherheitsreserven ausnutzen? Z.B. ausreichende Funktion trotz Ausfall von zum System gehörenden Komponenten.	(-) NWA mit nur einem Kreislauf
Systemfremde Komponenten	Welche nicht zum System gehörende Komponenten werden zusätzlich angefordert? Welche Schäden bei Ausfall?	Bei funktionierender NWA und Reaktor unter Druck: Öffnen der Hauptabsperrrklappen im Primärkreis nach 30 min. (-) Bei Öffnungsversagen: Rückwärtsdurchströmung der Hauptdampferzeuger durch heiße Gasströmen
Menschliche Eingriffe	Gibt es Realisierungen des Hauptziels aufgrund menschlicher Gegenmaßnahmen nach technischem Versagen? Wenn ja, welche Alternativen?	Ja: • Naturkonvektion • Querverbindung • Reparatur
Subjektive Nachteile menschlicher Gegenmaßnahmen	Welche subjektiven Nachteile haben die möglichen Alternativen der Gegenmaßnahmen?	(-) Naturkonvektion ungewohnt, weil passive NWA und weil Öffnen der Gebläsebypaßorgane erforderlich - ein Zustand, der bei aktiver NWA-Betriebsweise zum Gebläseschaden führen würde (-) Querverbindung kompliziert (-) Zeitbedarf der Reparatur ist schwer übersehbar
Zeitunabhängige, objektive Nachteile der Gegenmaßnahmen	Welche objektiven, zeitunabhängigen Nachteile sind zu erwarten, obwohl die Gegenmaßnahmen zum Ziel führen?	Wenn NWA per Naturkonvektion: (-) Austausch der Kernstäbe erforderlich (-) Behördliche Untersuchungen zur Wirksamkeit einer passiven NWA Wenn NWA per Querverbindung: (-) Nur ein Kreislauf

Tab. 24. HTR-500. Nachteile (-) trotz ausreichender NWA: (wird fortgesetzt)

Kriterium	Erläuterung	Beispiel HTR-500
Zeitabhängige, objektive Nachteile	Welche zeitabhängigen Schäden sind zu erwarten, obwohl daß zeitliche Kriterium des Hauptziels eingehalten wird?	Zeitliches Kriterium: NWA-Spätstart möglich (entspricht 5 h bzw. 10 h zulässige NWA-Ausfalldauer). Mögliche Schäden trotz Wiederherstellung der NWA innerhalb der zulässigen Zeit per Reparatur oder Querverbindung (vgl. Tab. 21 auf Seite 77): (-) Primärkreisdruckentlastung ins Reaktorschutzgebäude (-) Abschmelzen der Kernstabhüllrohre (-) Versagen des Deckenreflektors (-) Überschreiten der Auslegungstemperatur der Brennelemente
Systemausfallzustand	Welchen Einfluß haben unterschiedliche Systemausfallzustände auf die o.g. zeitabhängigen Nachteile?	Bei nicht wirksamer Wärmesenke hat nach 30 min der geplante NWA-Ausfallzustand (A) ALLE HAUPTABSPERRKLAPPEN GEÖFFNET gegenüber dem ungeplanten NWA-Ausfallzustand (B) ALLE HAUPTABSPERRKLAPPEN GESCHLOSSEN folgende Nachteile (vgl. Abschnitt 3.3.3.4): (-) Nach ca. 1 h (anstatt 5 h) Druckentlastung in das Reaktorschutzgebäude (-) Nach ca. 3 h (anstatt 4 h) Versagen des Deckenreflektors Dagegen hat B gegenüber A folgende Nachteile: (-) Austausch der Kernstäbe erforderlich (-) Schmelzen der Kernstabhüllrohre nach ca. 3 h (-) Erreichen der Auslegungstemperatur der Brennelemente nach ca. 4 h Außerdem würde sich bei B die zulässige Zeit zur Wiederherstellung der NWA von 10 h auf 5 h reduzieren.
Tab. 24 (Fortsetzung)		

Tab. 25 enthält die Wahrscheinlichkeiten (Erwartungswerte) einiger Schadensereignisse aus Tab. 24. Diese Ereignisse betreffen den wirtschaftlichen Aspekt der Folgen eines Störfalls: Inwieweit ist nach einem - aus radiologischer Sicht - beherrschten Störfall der Weiterbetrieb der Anlage beeinträchtigt?

Der Tabelle ist z.B. zu entnehmen, daß in ca. 10 % aller Anforderungen an das NWA-System des HTR-500 mit Schadensereignissen zu rechnen ist, die aufgrund notwendiger Ursachenklärungen (zum Ausfall eines Kreislaufs oder einer Hauptabsperrklappe) eine mehr oder weniger lange Verzögerung der Wiederinbetriebnahme nach sich ziehen könnten. Die Wahrscheinlichkeit ($4.9E-4$) des extremen Schadensereignisses DECKENREFLEKTORVERSAGEN unterscheidet sich nur unwesentlich von der Wahrscheinlichkeit ($4.1E-4$) des in Abschnitt 3 berechneten TOP-Ereignisses NWA-AUSFALL UND SPÄTSTART UNMÖGLICH. Der Wert $4.9E-4$ liegt

ziemlich zentral innerhalb des zu dem Wert $4.1E-4$ gehörenden 90%-Unsicherheitsintervalls $< 1.2E-4, 9.4E-4 >$ (MDN = $3.4E-4$, UF = 2.8).

Technisches NWA-Versagen, $w(NWA_T) = 2.4E-3$	Kein technisches NWA-Versagen, $w(\neg NWA_T) = 1 - 2.4E-3 = 0.9976$
UND	ABER
Austausch der Kernstäbe erforderlich ^{*1} : $F(t) \approx 2.4E-3$	NWA funktioniert nur in einem Kreislauf: $w(\neg NWA_T K) = 0.046 \cdot 0.9976 \approx 0.046$
Druckentlastung des Primär- kreises ^{*2} : $F(t) \approx 5.8E-4$	Heiße Strömen im Dampferzeuger, weil nicht alle Hauptabsperrklappen nach 30 min geöffnet: $w(\neg NWA_T H) = 0.056 \cdot 0.9976 \approx 0.056$
Deckenreflektorversagen ^{*3} : $F(t) \approx 4.9E-4$	Nur ein Kreislauf ODER heiße Strömen: $w[\neg NWA_T (K \vee H)] = (.046 + .056 - .046 \cdot .056) \cdot .9976 \approx 0.10$

Tab. 25. HTR-500. Wirtschaftlich bedeutsame Ereignisse nach Ausfall der Hauptkühlung:

* Anmerkungen zu Tab. 25

1. $t = 0.5$ h. Da nach einer NWA per Naturkonvektion immer der Austausch der Kernstäbe erforderlich ist (HRB 1983, S.156ff+169), entfällt hier der Reduktionsfaktor $w(N)$. Ebenso der Reduktionsfaktor $w(Q)$ (s.u.).
2. $t = 1$ h. Der Reduktionsfaktor $w(Q)$ entfällt, weil angenommen wird, daß die Herstellung der NWA per Querverbindung mindestens eine Stunde dauern wird.
3. $t = 3$ h.

Ausfalldauergrenzwerte und Wahrscheinlichkeiten aus Abschnitt 3. Der Temperaturverlauf in Abb. 18 auf Seite 76 wurde wegen seiner sehr kleinen Eintrittswahrscheinlichkeit vernachlässigt. Die Wahrscheinlichkeiten für Ereignisse in Kombination mit dem technischen Versagen der NWA wurden über folgende Gleichung berechnet:

$$F(t) = w(NWA_T) w(N) w(Q) \{w(R_T) + [1 - w(R_T)] w(T \geq t)\}$$

mit

(NWA_T) Technisches NWA-Versagen: $w(NWA_T) = 2.4E-3$,

(N) Naturkonvektion versagt (menschl. u. techn. Fehler): $w(N) = 0.25$,

(Q) Querverbindung versagt (menschl. u. techn. Fehler): $w(Q) = 0.92$,

(R_T) Reparatur techn. unmöglich: $w(R_T) = 0.6$, $w(R_T|Q) = 0.65$,

t = zulässige Reparaturzeit,

T = Reparaturdauer, exponentiellverteilt mit $MTTR=8h$:

$$P(t) = w(T \geq t) = \exp(-t/MTTR),$$

$$P(0.5h) \simeq 0.95, P(1h) \simeq 0.9, P(3h) \simeq 0.7.$$

4.2.2 Konkrete Systemzustände

Das hier vorgeschlagene Verfahren zur Identifizierung von Diagnoseproblemen (als Ursachen von Entscheidungsfehlern im Sinne einer nicht richtigen Interpretation) beginnt mit der Identifizierung konkreter Systemzustände, die zur Realisierung des Hauptziels SICHERHEIT erforderlich sind. Hierzu werden WENN-DANN-Regel betrachtet, die für die Beherrschung von Störfällen von Bedeutung sind:

1. WENN Situation A, DANN Systemzustand B (nur Interpretation).
2. WENN Situation A, DANN Reaktion B (Interpretation und Aktion).

Hier wird die zweite Form betrachtet. Für PRA-Zwecke ist folgende Unterteilung dieser Regeln sinnvoll:

- **Diagnoseregeln:** Das sind Regeln, deren Beachtung vom Personal verlangt wird.
Beispiel HTR-500, Schritt 9 in Tab. 15 auf Seite 55: WENN beide NWA-Wärmetauscher ausreichend gekühlt, DANN weiter mit nächstem Schritt (Überprüfen, ob alle 8 Hauptabsperklappen geschlossen).
- **Regeln der Systemtechnik:** Das sind Regeln über die vom System automatisch ausgelösten Reaktionen.
Beispiel HTR-500: WENN NWA-Betrieb per Zwangskonvektion (Gebläse) UND Reaktor unter Druck, DANN alle 8 Hauptabsperklappen nach 30 min öffnen (s. Tab. 10 auf Seite 49).

Sowohl aus dem WENN-Teil als auch aus dem DANN-Teil dieser Regeln lassen sich Ziele ableiten. Ein Ziel im WENN-Teil (z.B. beide Wärmetauscher gekühlt) wird hier als Anwendungsbedingung bezeichnet, ein Ziel im DANN-Teil (z.B. Hauptabsperklappen auf) als Ausführungsziel.

Zur Identifizierung konkreter Systemzustände ist es nun erforderlich, diese o.g. Ziele einer differenzierten Betrachtungsweise zu unterziehen. So führt z.B. folgender konkreter Systemzustand zur Realisierung des Ziels BEIDE WÄRMETAUSCHER GEKÜHLT:

- STRANG 1: Zirkulationspumpe fördert mit 100% NWA-Kapazität, Umwälzpumpe startet nicht.
- STRANG 2: Zirkulationspumpe fördert mit weniger als 100% NWA-Kapazität, Umwälzpumpe fördert mit 100% NWA-Kapazität.

Weitere Systemzustände hierzu sind in Tab. 29 aufgelistet.

4.3 Identifizierung von Rückwirkungen

Im Abschnitt 4.3.1 wird eine Methode vorgeschlagen, die von den im Abschnitt 4.2 identifizierten Nachteilen (aufgrund betrieblicher Aspekte) ausgeht. Mit dieser Methode lassen sich sicherheitsrelevante Rückwirkungen identifizieren, die zu ungeplanten Handlungen aufgrund einer bewußten Risikoannahme (Fehlverhalten) führen können.

Im Abschnitt 4.3.2 wird eine Methode zur Identifizierung von Rückwirkungen vorgeschlagen, die aufgrund erwartungsgebundener Fehlinterpretationen (Erwartungsfehler) zu ungeplanten Handlungen führen können. Diese Methode basiert auf konkreten Systemzuständen, die sich aus Regeln der Form

WENN Situation X, DANN Reaktion Y

ableiten lassen.

4.3.1 Vergleich von Realisierungsalternativen des Hauptziels

Die hier vorgestellte Methode basiert auf den in Tab. 24 auf Seite 87 identifizierten Nachteilen, die trotz Hauptzieleinhaltung eintreten können. Diese Methode dient der Erkennung von Situationen mit Zielkonflikt: Die geplante Handlung ist mit Nachteilen verbunden, die durch eine ungeplante (riskante) Handlung vermieden werden können. Ob eine solche Situation auch vom Personal als Konflikt wahrgenommen wird, kann nicht vorausgesagt werden.

In Tab. 26 ist das Verfahren skizziert, daß hier zur Identifizierung von Konfliktsituationen verwendet wurde.

1.	Bildung von Realisierungsalternativen zu den Kriterien REDUNDANZGRAD SYSTEMFREMDE KOMponenten STRATEGIEN MENSCHLICHER GEGENMASSNAHMEN SYSTEMAUSFALLZUSTÄNDE
2.	Zu jedem Kriterium: Bewertung der Alternativen hinsichtlich möglicher Nachteile
3.	Zu jeder Menge von Alternativen innerhalb eines Kriteriums: Alternativen (A1,A2 ...) auf MONOTONIE hin überprüfen: Gibt es ein Alternativpaar (A1,A2) derart, daß A1 nicht zu allen Nachteilen günstigere Bewertungen aufweist als A2? Wenn ja: KONFLIKT Wenn nein: Übergangsmöglichkeiten (Ü1,Ü2 ...) von der Alternative A2 in die eindeutig bessere Alternative A1 auf MONOTONIE hin überprüfen: Gibt es zwei Übergangsmöglichkeiten (Ü1,Ü2) derart, daß Ü1 nicht zu allen Nachteilen günstigere Bewertungen aufweist als Ü2? Wenn ja: KONFLIKT Wenn nein: kein KONFLIKT erkennbar

Tab. 26. Verfahren zur Identifizierung von Konflikten

Das in Tab. 26 skizzierte Verfahren basiert auf der Auswertung von sog. "Realisierungs-Nachteil-Matrizen" (z.B. Tab. 27). Eine solche Matrix entsteht, in dem man jede Realisierungsalternative mit Angaben (ja, nein, etwas o.ä.) zu den Nachteilen bewertet, die mit dem in Tab. 23 auf Seite 86 skizzierten Verfahren identifiziert wurden. Zur Identifizierung von Konflikten werden nun (1) die Realisierungsalternativen selber und (2) die Übergangsmöglichkeiten zwischen diesen Alternativen auf Monotonie hin untersucht.

4.3.1.1 Monotonie von Realisierungsalternativen

Dieser Ansatz basiert auf folgender Fragestellung:

Gibt es ein Alternativpaar, z.B. (A1,A2), zur Hauptzielrealisierung, für das gilt, daß die eine Alternative (z.B. A1) nicht zu allen Nachteilen günstigere Bewertungen aufweist als die andere (z.B. A2)?

Beispiel HTR-500. Zu dem Differenzierungskriterium STRATEGIEN MENSCHLICHER GEGENMASSNAHMEN erhält man die in Tab. 27 dargestellte Matrix.

ALTERNATIVE → NACHTEIL ↓	Naturkonvektion	Querverbindung	Reparatur
(1)-(3) Subjektive Nachteile			
(1) Ungewohntheit	ja	etwas	nein
(2) Kompliziertheit	nein	ja	manchmal
(3) Zeitbedarf schwer überschaubar	nein	etwas	ja
(4)-(6) Objektive, zeitunabhängige Nachteile, wenn Gegenmaßnahme frühzeitig (innerhalb 30 min) erfolgreich			
(4) Behördliche Untersuchungen zur Wirksamkeit der NWA	ja	nein	nein
(5) Austausch der Kernstäbe erforderlich	ja	nein	nein
(6) NWA-Betriebsweise mit nur einem Kreislauf	nein	ja	nein

Tab. 27. HTR-500. Nachteile erfolgreicher Gegenmaßnahmen nach NWA-Ausfall

Lt. Tab. 27 liegt keine Monotonie vor. Die Alternative Naturkonvektion hat z.B. gegenüber der Alternativen Reparatur den Vorteil, daß ihr Zeitbedarf sich in einem überschaubaren Rahmen bewegt. Dagegen steht u.a. der Nachteil, daß sie mit außergewöhnlichen Eingriffen verbunden ist (vgl. Tab. 24 auf Seite 87). Die aus diesem Konflikt resultierende Rückwirkung auf die Erreichung des Hauptziels NWA AUSREICHEND könnte z.B. in dem Nichteinleiten der Naturkonvektion bestehen. Das Personal könnte sich darauf beschränken, die NWA auf "gewöhnliche" Art wiederherzustellen, z.B. durch die Reparatur einer ausgefallenen Pumpe. Der potentielle Entscheidungsfehler besteht also in dem absichtlichen Verzicht auf eine mögliche Maßnahme, die dem sicherheitsgerichteten Hauptziel ("Kernaufheizung verhindern") dient. Eine Analyse, die voraussetzt, daß das Verhalten des Personal ausschließlich sicherheitsgerichtet ist, würde diesen Entscheidungsfehler nicht berücksichtigen.

4.3.1.2 Monotonie von Übergangsmöglichkeiten

Für Alternativpaare (A1,A2), die die Monotonieeigenschaft erfüllen (d.h. z.B., daß A1 für jeden bewerteten Nachteil günstiger ist als A2) erfolgt die Identifizierung möglicher Konflikte anhand folgender Fragestellungen:

1. Gibt es Übergangsmöglichkeiten von der schlechteren Alternative (z.B. A2) in die eindeutig bessere (z.B. A1)? Gibt es nur eine Übergangsmöglichkeit, die ungeplant (weil zu riskant) ist, dann stellt das Eintreten der schlechteren Alternative eine potentielle Konfliktsituation dar.

Gibt es sowohl geplante als auch ungeplante Übergangsmöglichkeiten, dann sind diese Möglichkeiten hinsichtlich etwaiger Nachteile zu bewerten. Die so entstehende Matrix ist dann anhand folgender Fragestellung auf Monotonie hin zu untersuchen:

2. Gibt es eine ungeplante Übergangsmöglichkeit, die nicht in allen Nachteilbewertungen ungünstiger ist als die geplante(n) Übergangsmöglichkeit(en)?

Beispiel HTR-500. Jeder Kreislauf der NWA-Wärmetauscherbespeisung verfügt über zwei Pumpen mit 100% NWA-Kapazität pro Pumpe. Deshalb gibt es - bei Ausfall eines Kreislaufs - für den Übergang auf eine günstigere NWA mit zwei Kreisläufen neben der Reparatur des ausgefallenen Kreislaufs (eine geplante Maßnahme) auch noch die Möglichkeit einer Querverbindung, so daß der mit 2x100% funktionierende Kreislauf auch noch den ausgefallenen Kreislauf mit bespeist (eine ungeplante Maßnahme, weil Eingriff in funktionierendes Sicherheitssystem). Die ungeplante Querverbindung hat gegenüber der geplanten Reparatur den Vorteil, daß der Zeitbedarf im überschaubaren Rahmen bleibt.

4.3.1.3 Zusammenfassung der für den HTR-500 identifizierten Konfliktsituationen

Mit dem in Tab. 26 auf Seite 92 skizzierten Verfahren wurden für den HTR-500 die Konfliktsituationen 1, 2, 4 und 5 in Tab. 28 identifiziert. (Weitere Situationen für den HTR-500, die aber nicht auf das hier betrachtete NWA-Beispiel zutreffen, sind im Anhang H aufgelistet.)

Es liegt in der Natur menschlichen Verhaltens, daß nicht jede Situationen mit potentiellen Zielkonflikten durch ein festes Schema vorhersagbar sind. So konnte z.B. die Situation 3 in Tab. 28 nicht anhand des in Tab. 26 auf Seite 92 skizzierten Verfahrens identifiziert werden. Es handelt sich um eine Situation, die mit der zu Beginn des

Störfalls (1985) im KKW Davis-Besse (NRC 1985) aufgetretenen Situation vergleichbar ist (Abschnitt 2). Kurz nach Ausfall der Hauptkühlung wurde der voreilige und unnötige Entschluß gefaßt, daß Notspeisewassersystem von Hand zu starten.

Die Persönlichkeitsvariable AKTIVITÄT (nach Jenkins) mit den beiden Ausprägungen EILIG/UNGEDULDIG und GELASSEN/GEDULDIG könnte ein Indikator für das Auftreten solcher Entscheidungen sein. In psychologischen Tests an 24 KKW-Operateuren (GERTMAN u.a. 1985) wurde festgestellt, daß auf 12 Operateure die Ausprägung EILIG/UNGEDULDIG zutrifft (siehe auch Tab. 35 auf Seite 117).

Hier wird deutlich, daß ein Konflikt, der aus neutraler Sichtweise vorhanden ist, nicht immer aus subjektiver individueller Sichtweise vorhanden sein muß:

Ungeduldige Operateure entscheiden sich sofort für einen Handstart eines angeforderten Systems - ohne die Frage, "Handstart ODER Abwarten, was die Startautomatik macht", als Entscheidungsproblem wahrzunehmen. Geduldige nehmen diese Frage auch nicht als Problem wahr: Sie warten ruhig ab, ob die Startautomatik funktioniert. Diese Aussagen basieren auf der Annahme, daß die Entscheidung für einen unnötigen Eingriff nur von der o.g. Persönlichkeitsvariablen AKTIVITÄT abhängt.

Im Abschnitt 5.4 werden die Konfliktsituationen 1, 3 und 4 (Tab. 28) quantifiziert. Die Situationen 2 und 5 werden vernachlässigt, weil von ihnen keine signifikante Beeinträchtigung der Sicherheit ausgeht. Der Wegfall der QUERVERBINDUNG (Situation 2) trägt nur unwesentlich zur Erhöhung der Versagenswahrscheinlichkeit der Gegenmaßnahmen nach NWA-Ausfall bei (siehe Abschnitt 3.3.3.3). Das gleiche gilt für die Verringerung der zulässigen NWA-Ausfallzeit von 10 h auf 5 h (Situation 5). Dadurch würde sich die Versagenswahrscheinlichkeit der Gegenmaßnahmen nur von 0.17 auf 0.19 erhöhen (siehe Abschnitt 3.3.3.5).

SITUATION	UNGEPLANTES VERHALTEN (bewußte Risikoannahme)	(+) VORTEILE UND (-) NACHTEILE UNGEPLANTEN VERHALTENS
(1) Technisches Versagen der NWA. Personal hat erkannt, daß die Gegenmaßnahme NATURKONVEKTION anwendbar ist.	Nichteinleiten der NATURKONVEKTION. Stattdessen: Verfolgung anderer Strategien zur Wiederherstellung der NWA (z.B. Reparatur).	(+) Passive NWA (per NATURKONVEKTION) wird subjektiv als ungewöhnlich empfunden. (+) Zur Realisierung der NATURKONVEKTION ist es erforderlich, beide Bypaßorgane (GBO) an den NWA-Gebläsen zu öffnen. Der Zustand BEIDE GBO AUF ist ungewöhnlich, weil er bei aktiver NWA zum Schaden an den Gebläsen oder zu deren automatischen Abschaltung (Komponentenschutz) führen würde. (+) Es ist damit zu rechnen, daß von behördlicher Seite die Wirksamkeit einer passiven NWA angezweifelt wird. Langwierige Untersuchungen zu möglichen Folgeschäden an verschiedenen Komponenten des Primärkreises könnten die Wiederinbetriebnahme verzögern. (+) Nach einer passiven NWA per NATURKONVEKTION ist der Austausch der Kernstäbe erforderlich. (-) Eine Maßnahme zur Wiederherstellung der NWA entfällt.
(2)* Technisches Versagen der NWA. NATURKONVEKTION versagt. Personal erkennt, daß die Gegenmaßnahme QUERVERBINDUNG anwendbar ist.	Nichteinleiten der QUERVERBINDUNG. Stattdessen wird versucht, die NWA per Reparatur wiederherzustellen.	(+) Die Prozedur (s. Anhang D) zur Herstellung der QUERVERBINDUNG könnte subjektiv als ZU KOMPLIZIERT empfunden werden. (+) Die "Überkreuzbetriebsweise" (z.B. Wärmesenke Strang 1 und Gebläse Strang 2) könnte subjektiv als ungewöhnlich empfunden werden. (+) Das in der Prozedur (Anhang D) angeforderte Abschalten funktionierender Komponenten könnte subjektiv als ungewöhnlich empfunden werden. (+) Die QUERVERBINDUNG ermöglicht einen NWA-Betrieb mit einem Kreislauf. (-) Wie oben.
(3) NWA wird angefordert. Das Zwischenkühlwassersystem zur Kühlung der Wärmetauscher und der Gebläse ist noch nicht hochgefahren.	Frühzeitige Entscheidung für einen Handstart der Gebläse.	(+) Das Abwarten (ca. 3 min) bis zum automatischen Start der Gebläse könnte subjektiv als lästig empfunden werden. (+) Neugierde/Ungeduld: Interesse an einer frühzeitigen Gewißheit über das technische Funktionieren der NWA. (-) Gebläse-Ausfall, wenn nicht bemerkt wird, daß das Zwischenkühlwassersystem noch nicht hochgefahren ist.

Tab. 28. HTR-500. Konfliktbedingte Rückwirkungen auf die NWA-Zuverlässigkeit nach Ausfall der Hauptkühlung: (wird fortgesetzt)

SITUATION	UNGEPLANTES VERHALTEN (bewußte Risikoan- nahme)	(+) VORTEILE UND (-) NACHTEILE UNGEPLANTEN VERHALTENS
(4) Aufgrund eines Ausfalls in der Wärmesenke funktioniert die NWA nur mit einem Kreislauf. Ein Kreislauf in der Wärmesenke funktioniert planmäßig mit 2x100%.	Entscheidung für eine ungeplante Querverbindung durch "Anzapfen" des mit 2x100% funktionierenden Kreislaufs derart, daß dieser Kreislauf zu 100% den ausgefallenen Kreislauf bespeist.	(+) Möglichkeit eines schnellen Übergangs (ohne langwierige Reparatur) zu einer NWA mit zwei Kreisläufen. (-) Eingriff in ein funktionierendes System. Ein Fehler während des Eingriffs könnte zum Totalausfall der NWA führen.
(5)* Technisches NWA-Versagen. Naturkonvektion versagt. Wärmesenke unwirksam. Automatisches Öffnen der Hauptabsperklappen (ca. 30 min nach Störfallbeginn) steht bevor.	Das automatische Öffnen der Klappen wird verhindert.	(+) Verlängerung der Zeit bis zur Druckentlastung des Primärkreises von ca. 1 h auf 5 h. (+) Verlängerung der Zeit bis zum Deckenreflektorversagen von 3 h auf 4 h. (-) Verringerung der zulässigen NWA-Ausfallzeit von 10 h auf 5 h. (-) Verringerung der Zeit bis zum Erreichen der Auslegungstemperatur (1250°C) der Brennelemente von 10 h auf 4 h. (-) Verringerung der Zeit bis Abschmelzen der Kernstabhüllrohre von 10 h auf 3 h.
* Sicherheitstechnische Bedeutung vernachlässigbar, s. Text.		
Tab. 28 (Fortsetzung)		

4.3.2 Ähnlichkeitsbetrachtungen zu WENN-DANN-Regeln

Zur Identifizierung von Rückwirkungen dieser Ziele auf Hauptziel SICHERHEIT wird hier eine Methode vorgeschlagen, die auf folgenden zwei Ansätzen basiert:

1. Ähnlichkeitsbetrachtungen zu widersprüchlichen Ausführungszielen.
2. Unähnliche Erscheinungsformen einer Anwendungsbedingung.

Diese beiden Ansätze werden im folgenden Text erläutert.

4.3.2.1 Ähnlichkeitsbetrachtungen zu widersprüchlichen Ausführungszielen

Dieser Ansatz besteht in der Identifizierung von Regeln mit (untereinander) widersprüchlichen Ausführungszielen und in der anschließenden Beurteilung möglicher Ähnlichkeiten.

Beispiel HTR-500, Ausfall der Hauptkühlung bei Reaktor unter Druck. Bei nicht verfügbarer NWA-Wärmesenke ist nach 30 min der Zustand ALLE HAUPTABSPERRKLAPPEN (HAK) GESCHLOSSEN das vorgesehene Ausführungsziel (automatische Auslösung). Die Realisierung dieses Ziels mindert das Ausmaß der Kernaufheizung. Nach den in Tab. 21 auf Seite 77 getroffenen Annahmen erhöht sich dann die zulässige NWA-Ausfallzeit von 5 h auf 10 h. Bei verfügbarer Wärmesenke ist jedoch die Beibehaltung des Zustands ALLE HAK GESCHLOSSEN vorgesehen, weil dann eine passive NWA per Naturkonvektion möglich ist. Das Nichtbemerken der ausgefallenen Wärmesenke könnte demnach bewirken, daß die Operateure das automatische Öffnen der HAK wieder aufheben, weil sie sehr stark auf die Gegenmaßnahme Naturkonvektion fixiert sind.

Außerdem könnte aufgrund folgender Ähnlichkeit das Nichtbemerken einer ausgefallenen Wärmesenke mit erhöhter Wahrscheinlichkeit auftreten:

Die häufigste Erscheinungsform des Zustands WÄRMESENKE AUSGEFALLEN beinhaltet das Zustandsbild, daß in jedem Strang der Wärmesenke eine Zirkulationspumpe mit normaler Leistung fördert (vgl. Abb. 12 auf Seite 48 und Tab. 10 auf Seite 49). Dieses Zustandsbild ähnelt dem einer verfügbaren Wärmesenke - mit dem Unterschied, daß die Zirkulationspumpen nicht hochgefahren sind (vgl. Tab. 29 auf Seite 100). Die Operateure könnten daher aufgrund der (erfreulichen) Tatsache, daß die Zirkulationspumpen fördern, vergessen zu überprüfen, ob diese Pumpe auch mit der für einen NWA-Betrieb erforderlichen Leistung fördern. Hinzu kommt, daß die Operateure aufgrund des (unerfreulichen) Startversagens der Umwälzpumpen abgelenkt sind und unter Stress stehen.

Der Ausfall der Wärmesenke ist jedoch mit einer vernachlässigbar kleinen Wahrscheinlichkeit zu erwarten: Selbst unter Einbeziehung des Nuklearen Nebenkühlwassersystems (NNK) liegt die Wahrscheinlichkeit bei ca. $1.0E-5$.

Anmerkung:

Das NNK wurde hier - in Anlehnung an die Analyse des ISF (1984) - nicht unter dem Begriff NWA-System zusammengefaßt. In ISF (1984) wurde der Ausfall des NNK in den Ereignisablaufdiagrammen berücksichtigt. Bei einer solchen Modellierung ist jedoch zu beachten, daß das Ereignis AUSFALLS EINES NNK-KREISLAUFS zum Versagen der Naturkonvektion führt, weil dann ein Wärmetauscher nicht ausreichend gekühlt wird (vgl. Abschnitt 3.3.2).

Hinzu kommt, daß die Folgen des o.g. Erwartungsfehlers nicht besonders signifikant sind: Eine Verringerung der zulässigen Reparaturdauer von 10 h auf 5 h bewirkt eine Erhöhung der Versagenswahrscheinlichkeit (EW) der Gegenmaßnahmen nach NWA-Ausfall von 0.17 auf 0.19 (vgl. Abschnitt 3.3.3.5). Auf eine Einbeziehung dieses Fehlers kann daher verzichtet werden.

Ein weiterer Erwartungsfehler ist aufgrund der in Abschnitt 4.2 erkannten Fehlverhaltenmöglichkeit VOREILIGE ENTSCHEIDUNG FÜR GEBLÄSEHANDSTART zu berücksichtigen (s. Situation 3 in Tab. 28 auf Seite 96). Es wird angenommen, daß diese Entscheidung zum Ausfall der Gebläse führt, wenn diese gestartet werden, bevor das Zwischenkühlwassersystem (ZKS) hochgefahren ist. Daraus sind folgende Regeln mit widersprüchlichen Ausführungszielen ableitbar:

- 1) WENN ZKS hochgefahren, DANN Gebläse starten.
- 2) WENN ZKS nicht hochgefahren, DANN Gebläse nicht starten.

Das ZKS wird erst hochgefahren, nachdem das Nukleare Nebenkühlwassersystem (NNK) hochgefahren ist (vgl. Abb. 12 auf Seite 48). Der Zustand NNK HOCHGEFAHREN, ZKS NICHT HOCHGEFAHREN ist eine Erscheinungsform des WENN-Teils der zweiten Regel. Dieser Zustand hat eine gewisse Ähnlichkeit mit dem WENN-Teil der ersten Regel. Die Beendigung der Hochfahrprozedur für das NNK könnte demnach - insbesondere bei dem eiligen Operateur - die Erwartung auslösen, daß das ZKS hochgefahren ist.

4.3.2.2 Unähnliche Erscheinungsformen einer Anwendungsbedingung

Dieser Ansatz basiert auf der Bildung von Erscheinungsformen der Anwendungsbedingung EINER Regel und in der anschließenden Beurteilung ihrer Unähnlichkeit mit der Anwendungsbedingung als Ganzes.

Beispiel HTR-500, Ausfall der Hauptkühlung und technisches Versagen der NWA (vgl. Tab. 15 auf Seite 55 und Abb. 12 auf Seite 48). Eine Anwendungsbedingung für die Ergreifung der Gegenmaßnahme NATURKONVEKTION ist die ausreichende Bespeisung BEIDER Wärmetauscher. Im Zwischenkühlwassersystem (ZKS) der Wärmesenke des HTR-500 sind u.a. folgende vier Zustandsbilder möglich:

ZIRKULATIONS Pumpe		UMWÄLZ Pumpe		GEBLÄSEKÜHL Pumpe	
STRANG 1	STRANG 2	STRANG 1	STRANG 2	STRANG 1	STRANG 2
100%	100%	100%	0%	100%	100%
100%	100%	100%	100%	< 100%	100%
100%	< 100%	100%	0%	100%	100%
< 100%	< 100%	0%	0%	100%	100%

Tab. 29. HTR-500. Beispiele für mögliche Zustandsbilder der NWA-Wärmesenke

Die ersten beiden Zustände erfüllen die Anwendungsbedingung **BEIDE WÄRMETAUSCHER VERFÜGBAR**. Der dritte Zustand erfüllt diese Bedingung nicht, ebenso der vierte. Es ist davon auszugehen, daß die ersten beiden Zustände der Anwendungsbedingung **BEIDE WÄRMETAUSCHER VERFÜGBAR** unähnlich sind, weil ihr Erscheinungsbild **EINEN** Ausfall enthält. Oder anders formuliert: Der Zustand **EINE Pumpe ausgefallen** hat eine Ähnlichkeit zu dem Zustand **EIN WÄRMETAUSCHER NICHT VERFÜGBAR**. Ein solche Ähnlichkeit kann eine erwartungsgebundene Fehlinterpretation hervorrufen, die zu einem ungeplanten Verzicht auf die Naturkonvektion führen könnte, obwohl diese Maßnahme möglich wäre.

Für die Wahrscheinlichkeit, daß nach einem technischen NWA-Ausfall das Ereignis **PUMPEN AUSFALL IN DER WÄRMESSENKE** auftritt gilt folgende Abschätzung (vgl. Abschnitt 3, Zahlenwerte aus Tab. 13 auf Seite 53):

- 0.1 Ausfall 1v2 Gebläsekühlpumpen, wenn NWA-Ausfall
 (praktisch gleich dem Ereignis **QUERVERBINDUNG MÖGLICH**)
- + 0.022 Ausfall 1v4 Pumpen im Zwischenkühlwassersystem
 ($p \approx 4 \cdot 5.4 \text{E-}3$)
- ≈ 0.12 **INSGESAMT**

Ein ähnliches Diagnoseproblem könnte bei der Anwendung von Regeln auftreten, die die Maßnahme **QUERVERBINDUNG** als Ausführungsziel haben (Schritt 11 in Tab. 15 auf Seite 55). Es gibt Ausfallzustände, bei denen die **QUERVERBINDUNG** möglich ist, obwohl zwei Pumpen in der Wärmesenke ausgefallen sind. Der Reiz **ZWEI PUMPEN AUSGEFALLEN** könnte die Fehlinterpretation **ZWEI WÄRMETAUSCHER NICHT VERFÜGBAR** auslösen. Aufgrund dieser Fehlinterpretation würden die Operateure nicht erkennen, daß die Querverbindung möglich ist. Da eine Erhöhung der menschlichen Fehlerwahrscheinlichkeit nur geringfügig zur Erhöhung der gesamten Versagenswahrscheinlichkeit der Querverbindung beiträgt (vgl. Abschnitt 3.3.3.3), wird dieser Erwartungsfehler hier nicht berücksichtigt. Hinzu kommt der Korrekturfaktor

aufgrund der geringen Eintrittswahrscheinlichkeit des Ereignisses ZWEI PUMPEN AUSGEFALLEN.

4.3.2.3 Zusammenfassung der für den HTR-500 identifizierten Diagnoseprobleme

Aufgrund der oben getroffenen Vorauswahl werden hier folgende Erwartungsfehler (aufgrund besonderer Diagnoseprobleme) in die Zuverlässigkeitsanalyse der NWA des HTR-500 mit einbezogen:

1. Nichtbemerken ($p = ?$), daß beide Wärmetauscher ausreichend gekühlt, unter der Bedingung, daß ein NWA-Ausfall mit Pumpenausfall in der Wärmesenke vorliegt ($p = 0.12$).

Es wird angenommen, daß dieser Fehler zum Nichteinleiten der Naturkonvektion führt.

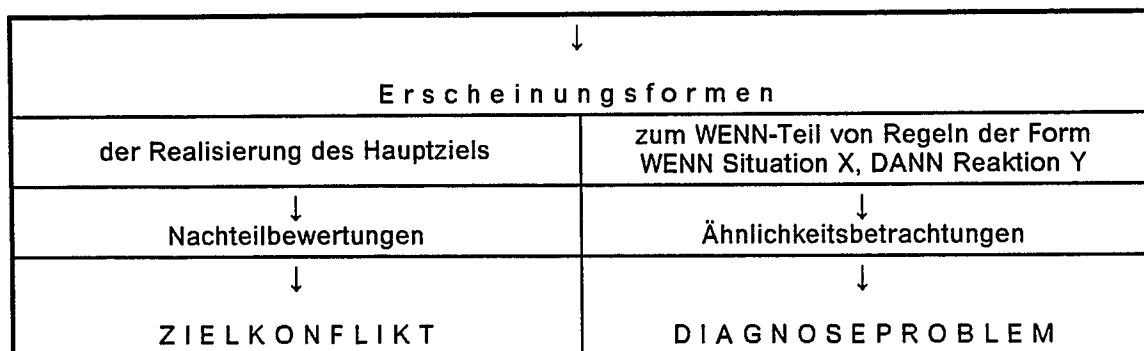
2. Nichtbemerken ($p = ?$), daß das Zwischenkühlwassersystem noch nicht hochgefahren ist, unter der Bedingung, daß das Nukleare Nebenkühlwassersystem hochgefahren ist ($p \simeq 1$) und daß die Entscheidung für einen frühzeitigen Handstart der NWA-Gebläse getroffen wird ($p = ?$).

Es wird angenommen, daß dieser Fehler zum Ausfall der NWA-Gebläse führt, wenn die o.g. Entscheidung getroffen wird.

Der Anhang I enthält weitere Diagnoseprobleme, die während HTR-500-typischer Störfallabläufe auftreten könnten. Die sich aus diesen Problemen ergebenden Erwartungsfehler wurden hier nicht berücksichtigt, weil sie entweder nicht auf den hier betrachteten NWA-Fall zutreffen oder weil sie erst nach Abschluß der Rechnungen identifiziert wurden.

4.4 Zusammenfassung von Abschnitt 4

Aus Zielen, die dem Hauptziel SICHERHEIT untergeordnet sind (z.B. Komponentenschonung) oder in die sich das Hauptziel untergliedern läßt (z.B. notwendige Stellung von Armaturen), sind Rückwirkungen auf die zuverlässige Realisierung des Hauptziels identifizierbar. Diese Rückwirkungen können in Form von erhöhten Wahrscheinlichkeiten ungeplanter Personalhandlungen aufgrund von Konflikten oder Diagnoseproblemen in Erscheinung treten. Auf das hier betrachtete Hauptziel, die Zuverlässigkeit der NWA des HTR-500, wurden aufgrund von Konflikten drei und aufgrund von Diagnoseproblemen zwei Rückwirkungen identifiziert, die einen signifikanten Einfluß haben könnten. Die verwendete Methode zur Identifizierung der entsprechenden Situationen im Störfallablauf läßt sich in Stichworten wie folgt zusammenfassen:



Tab. 30. Identifizierung von Situationen mit Zielkonflikt oder Diagnoseproblem

Zur Identifizierung möglicher Konflikte im Störfallablauf wurden - auf der Grundlage von vier Differenzierungskriterien - mögliche Realisierungsalternativen des Hauptziels gebildet. Anhand verschiedener Checklisten wurden die Alternativen auf mögliche Nachteile hin untersucht und bewertet. Unter der Annahme, daß sich das Personal - neben der Erreichung des Hauptziels SICHERHEIT - auch die Vermeidung dieser Nachteile zum Ziel setzt, sind Konflikte immer dann zu erwarten, wenn die Priorität der Alternativen bezüglich ihrer Nachteile nicht eindeutig ist. Also wenn z.B. bezüglich der Hauptzielerreichung Alternative A gegenüber der Alternativen B Vorrang hat, Alternative A aber einen Nachteil aufweist, der bei Alternative B nicht vorhanden ist.

Die hier vorgeschlagene Methode zur Identifizierung von Diagnoseproblemen (nach Diagnose für die richtige Störfallprozedur) basiert auf der Bildung von Erscheinungsformen des WENN-Teils von Regeln der Form
WENN Situation X, DANN Reaktion Y.

Zur Identifizierung von Diagnoseproblemen, die zum Nichtausführen des DANN-Teils führen können, wurden verschiedene Erscheinungsformen gebildet, die den DANN-Teil erfüllen. Zu diesen Erscheinungsformen wurde gefragt, wie "unähnlich" sie den WENN-Teil erfüllen; oder anders formuliert, ob sie Reize enthalten, die die Assoziation erwecken können, daß der WENN-Teil nicht erfüllt ist.

Zur Identifizierung von Diagnoseproblemen, die zum fälschlichen Ausführen des DANN-Teils führen können, wurden zunächst Regeln mit widersprüchlichem DANN-Teil identifiziert. Zu den WENN-Teilen wurden verschiedene Erscheinungsformen gebildet und auf Ähnlichkeiten hin untersucht: Kann eine Situation, die die Reaktion Y erfordert, mit einer anderen Situation verwechselt werden, die die gegenteilige Reaktion erfordert?

5. Quantifizierung von Rückwirkungen untergeordneter Ziele

5.1 Einführung

5.1.1 Zielsetzung

Im Abschnitt 4 wurde eine Methode erarbeitet, die es erlaubt, im Störfallablauf Situationen zu identifizieren, in denen folgende Fehler auftreten könnten:

- Durch Konflikte verursachtes Fehlverhalten:
Richtiges Verhalten ist mit negativen Anreizen verbunden bzw. Fehlverhalten hat einen besonderen Anreiz (vgl. HACKER 1980, S.346).
- Durch Ähnlichkeiten verursachte Erwartungsfehler (im Sinne einer Fehlinterpretation nach erfolgter Diagnose für die richtige Störfallprozedur).
Unterschiedliche Situationen unterscheiden sich nur in einem kritischen Detail. Ein Teilsignal kann eine Erwartung auslösen, die zu einer falschen Entscheidung führt, weil das übrige Informationsangebot gar nicht mehr oder nur noch flüchtig genutzt wird (vgl. HACKER 1980, S.347ff).

Ziel ist es nun, ein Verfahren zu entwickeln, daß es erlaubt, zu diesen Fehlern situationsspezifische Wahrscheinlichkeiten (im Rahmen der für menschliche Fehler üblichen Unsicherheiten, s. Anhang F) anzugeben. Die Schätzung von Wahrscheinlichkeiten menschlicher Fehler ist ein Schritt in der Einbeziehung von menschlichem Verhalten in eine PRA. Dieser Schritt ist nicht unumstritten (vgl. APOSTOLAKIS u.a. 1988).

Die Quantifizierung von Fehlverhalten durch direkte Verwendung von Wahrscheinlichkeiten wird hier als p-Modell bezeichnet - im Gegensatz zu dem t-Modell (Abschnitt 2), in dem eine indirekte Quantifizierung über eine geschätzte (oder empirisch beobachtete) Zeitverzögerung erfolgt.

5.1.2 Versuch einer Klassifizierung

Tab. 31 enthält eine geeignete Systematik zur Einordnung der hier betrachteten Fehler. Erwartungsfehler betreffen die Abfragen 2 bis 4. Fehlverhalten betrifft in erster Linie die Abfrage 5, kann aber auch die Abfragen 2 bis 4 betreffen (s.u.).

In der psychologischen Sicherheitsforschung werden die Abfragen 2 bis 4 auch unter dem Begriff Gefahrenkognition zusammengefaßt (HOYOS 1980, S.91). In der PRA-Terminologie (z.B. SWAIN 1983, p.12-6) wird hierzu auch der Begriff "Diagnose" genannt. Eine ausführliche Diskussion zur Klassifizierung von Erwartungsfehlern erfolgt in Abschnitt 5.3. Vorerst werden diese Fehler dem menschlichen Faktor Diagnose zugeordnet.

Konflikte werden in der psychologischen Sicherheitsforschung als wichtige Ursache von Fehlern in den Bereichen Vorsorgeverhalten und Risikoverhalten angesehen (HOYOS 1980, S.112f). Vorsorgeverhalten betrifft die Kontrolle möglicher Folgen, nach dem man sich der Gefahr ausgesetzt hat, z.B. Sicherheitsgurt tragen. Risikoverhalten ist als Steuerung der Gefahrenkognition (s.o.) definiert. Diese Steuerung hat zwei Aspekte (vgl. HOYOS 1980, S.112):

1. Beseitigung der Ungewißheit über den Ausgang einer gefährlichen Situation durch Informationssuche.
Fehlverhalten: Zu früher Abbruch der Informationssuche.
Vorteil: Zeitersparnis.
Nachteil: Erhöhte Wahrscheinlichkeit einer Fehleinschätzung.
Hierzu schreibt HOYOS (1980, S. 125): "In vielen Fällen wird Schnelligkeit höher bewertet als Fehlerlosigkeit (z.B. bei Taxifahrern)".
2. Steuerung der Gefährdung durch Abwägen der Anreize und des Risikos.
Fehlverhalten: Akzeptierung eines Gefährdungsniveaus durch Abweichung von einer Vorschrift.
Vorteil: Dem Anreiz entsprechend (z.B. weniger Anstrengung).
Nachteil: Dem Gefährdungsniveau entsprechend, z.B. erhöhte Verletzungsgefahr.

Fehlverhalten aufgrund von Konflikten kann also (1) indirekt, nicht vorschriftsmäßige Vorgehensweise bei der Informationssuche zur Erkennung und Einordnung der Gefahr, und (2) direkt, vorschriftswidriges Akzeptieren eines Gefährdungsniveaus, in Erscheinung treten. Der Schwerpunkt dieser Arbeit liegt auf der direkten Erscheinungsform. Es wird angenommen, daß die indirekte Erscheinungsform schon durch die in einer PRA für Wahrnehmungs- und Interpretationsfehler (Anhang E, ID = 1 und 2) verwendeten Wahrscheinlichkeiten erfaßt ist.

Für Fehlverhalten (aufgrund von Konflikten) und Erwartungsfehler (aufgrund von Ähnlichkeiten) wird hier folgende begriffliche Einordnung vorgenommen:

- Fehlverhalten ist eine negative Ausprägung der Variable Risikoverhalten. Hier beschränkt sich die Verwendung des Oberbegriffs Risikoverhalten auf die direkte Erscheinungsform: Vorschriftswidriges oder vorschriftsmäßiges Verhalten bezüglich eines wahrgenommenen Gefährdungsniveaus (s.o.). Fehlverhalten (im Sinne einer bewußten Risikoannahme) wird hier also dem Oberbegriff Risikoverhalten zugeordnet.
- Erwartungsfehler sind Ursachen - neben anderen Ursachen - von Fehlern in der Diagnose (d.h. dem Erkennen und Einordnen einer Gefährdung). Erwartungsfehler werden hier dem Oberbegriff Diagnose zugeordnet.

1. Existiert eine Möglichkeit, die vor dem Anstieg der Gefahr warnt? JA NEIN → ↓ 2. Wird diese Information wahrgenommen? JA NEIN → ↓ 3. Wird diese Information richtig verstanden? JA NEIN → ↓ 4. Ist eine Möglichkeit zur Vermeidung der Gefahr bekannt? JA NEIN → ↓ 5. Wird versucht, die Gefahr dadurch zu vermeiden? JA NEIN (bewußte Risikoannahme) → ↓ 6. Kann dadurch die Gefahr vermieden werden? JA NEIN → ↓	D R O H E N D E G E F A H R
K E I N E G E F A H R	

Tab. 31. Modell zur Entstehung gefährlicher Situationen (SURRY 1966):
Deutsche Version aus RADL&TIETZE (1976)

5.1.3 Zur Bedeutung der Faktoren Diagnose und Risikoverhalten

Aus der nuklearen Betriebserfahrung sind schwere Störfälle bekannt, in denen die menschlichen Faktoren Diagnose und Risikoverhalten eine wichtige Rolle spielten (Tab. 32).

1. SWR Brunsbüttel, 18.6.1978:
Frischdampfleckage im Maschinenhaushaus. Das Personal überbrückte ein Reaktorschutzsignal, daß die Schnellabschaltung (RESA) ausgelöst hätte. Durch die Verhinderung der RESA können Aktivitätsspitzen vermieden werden, die "zur Ausschöpfung der zulässigen Abgabewerte führen und den Weiterbetrieb für den Rest des Jahres unmöglich machen können" (SMIDT 1979, S.283).
2. DWR TMI-2 (Harrisburg), 28.3.1979:
Ausfall der Dampferzeugerbespeisung und Kühlmittelverlust wegen Versagen des Abblaseventils am Druckhalter in Offenstellung. Aufgrund der Fehlinterpretation "Abblaseventil geschlossen" (nach richtiger Diagnose des Ausfalls der Bespeisung) schalteten die Operateure die Hochdruckeinspeisepumpen aus und ließen sogar noch (über das Volumenregelsystem) Wasser aus dem Primärkreis heraus, weil sie glaubten, der Primärkreis wäre voll Wasser. Die falsche Stellungsanzeige des Abblaseventils und der wegen Blasenbildung ansteigenden Füllstand im Druckhalter legten diese Interpretation nahe. Andere Anzeigen, die auf ein offenes Abblasenventil hindeuteten, z.B. die Temperatur am Abblasestrang, blieben unbeachtet oder wurden als unbedeutend angesehen.
(vgl. GRS 1979, S.249f)
3. DWR Davis-Besse, 9.6.1985 (s. auch Abschnitt 2):
Ausfall der Dampferzeugerbespeisung. Der Schichtleiter leitete die feed + bleed-Kühlung nicht zum vorgeschriebenen Zeitpunkt ein, sondern wartete den Erfolg der sekundärseitigen Maßnahmen ab, der dann auch ca. 4 min später eintrat.
(NRC 1985)
4. RBMK Tschernobyl, 20.4.1986:
Ein Test, der die Wirksamkeit der Turbinennachlaufzeit für die Energieversorgung im Notstromfall nachweisen sollte, wurde durchgeführt. Während des Test kam die Anlage in einen Zustand, der aus Sicherheitsgründen einen Abbruch des Tests erforderte. Trotzdem versuchte das Personal den Test weiter durchzuführen. Eine Leistungsexkursion trat auf, die aufgrund der systemtechnischen und situationsspezifischen Gegebenheiten zu einem schweren Reaktorunfall führte. Eine wesentliche Ursache des Unfalls lag in der riskanten Weiterführung des Tests.
(vgl. KRÖGER&CHAKRABORTY 1989, S.63)

Tab. 32. Reale Störfallbeispiele mit Fehlern in den Bereichen Diagnose und Risikoverhalten

SABRI u.a. (1981) führten eine Ursachenanalyse durch, deren Aussagekraft sich nicht nur auf Einzelfälle beschränkt. 444 Vorkommnisse der U.S. LWR-Betriebserfahrung wurden untersucht. 89 wurden als signifikant (höchste Meldekategorie bzgl. Sicherheitsdefizit) eingestuft und näher untersucht. Die Verteilung der 93 menschlichen Fehler, die während dieser Vorkommnisse auftraten und an deren Entstehung bzw. Entwicklung einen Anteil hatten, ist in Tab. 33 dargestellt. Aus den angegebenen Definitionen (alles Originalzitate) läßt sich entnehmen, daß die Kategorien

PERCEPTION und COGNITION unter dem Begriff Diagnose zusammengefaßt werden können und daß die Kategorie BEHAVIOR dem Risikoverhalten entsprechen könnte. Mit diesen Zuordnungen ergibt sich insbesondere für das Wartenpersonal eine hohe Bedeutung dieser Faktoren: Von 55 Fehlern fallen 7 in die Kategorie Diagnose und 13 in die Kategorie Risikoverhalten.

CATEGORY	ERRORS	OPE- RA- TORS	MAIN- TE- NANCE	OTHERS
PERCEPTION: how a stimulus is perceived	• failure to note leak, crack, dirt • failure to detect signal, read gauge, read tag, radiation level • failure to note warning light, alarm • detection of wrong signal, false alarm • incorrect interpretation of instrument, meter readings • failure to relate signal to state of system	5	0	0
COGNITION: how it is interpreted	• misunderstanding of procedures • misunderstanding of techn. specs. • misidentification of alarm	2	1	2
DECISION: how it effects in a decision	• inferior choice from several alternate actions • failure to act in appropriate time • given all necessary information, poor strategy selection	6	0	2
RESPONSE: how it results in a response	• incorrect adjustment • inadvertent manipulation of a valve • failure to complete checklist in sequence • incorrect calibration	29	18	2
BEHAVIOR: behavioral errors are human- initiated and may result from an arbitrary action on the part of the human which does not require an external stimulus	• use of incorrect procedure • disregard procedure	13	11	1
UNKNOWN	-	0	3	0

Tab. 33. Verteilung von 93 Fehlern des KKW-Personals (SABRI u.a. 1981):

Die Verteilung wurde an 89 signifikanten Vorkommnissen der U.S. LWR-Betriebserfahrung beobachtet. 52 Vorkommnisse betrafen das Wartenpersonal (operators), 32 das Instandhaltungspersonal (maintenance) und 5 das sonstige Personal (others)

Auch andere Untersuchungen (z.B. zur Verkehrssicherheit, FELL 1976) deuten auf eine hohe Bedeutung der Faktoren Diagnose und Risikoverhalten hin. In der Arbeitssicherheitsforschung wird insbesondere die Bedeutung des Risikoverhaltens hervorgehoben: "It is a common held view that individual risk acceptance is a major factor in accident causation" (DUNN 1972). MITTENECKER (1962, S.77f) spricht von einem Konflikt zwischen Leistungstendenz und Sicherheitstendenz, mit dem sich die Entstehung von Arbeitsunfällen erklären läßt (vgl. auch HACKER 1980, S.126). In der Phase B der "Deutschen Risikostudie Kernkraftwerke" (GRS 1990, S.471) wird ein Zielkonflikt als mögliche menschliche Ursache des Versagens der primärseitigen NWA (feed + bleed) genannt.

Den Wahrscheinlichkeiten des Auftretens von Fehlern in den Bereichen Diagnose und Risikoverhalten kommt also eine hohe Bedeutung zu. Im Abschnitt 5.2 wird daher ein Modell zur Schätzung der Wahrscheinlichkeit von Fehlverhalten, daß durch Konflikte hervorgerufen wird, vorgeschlagen (Bereich Risikoverhalten), im Abschnitt 5.3 ein Modell zur Schätzung der Wahrscheinlichkeit für Erwartungsfehler, die durch Ähnlichkeiten hervorgerufen werden (Bereich Diagnose). Im Abschnitt 5.4 wird die NWA-Zuverlässigkeitsanalyse des HTR-500 (Abschnitt 3) unter Verwendung dieser Modelle erweitert.

5.2 Durch Konflikte verursachtes Fehlverhalten

5.2.1 Bisherige Berücksichtigung

Konflikte werden als mögliche Ursachen von Fehlentscheidungen nach erfolgter Diagnose genannt (SWAIN 1983, p.12-9). Die folgenden zwei Beispiele zeigen, daß es keine einheitlichen Regeln zur Schätzung der entsprechenden Fehlerwahrscheinlichkeiten gibt.

5.2.1.1 Zwei Beispiele

Kleiner Kühlmittelverluststörfall

Im "PRA Procedures Guide" (NRC 1983, ch.4) wird die Einbeziehung menschlichen Verhaltens am Beispiel eines kleinen Kühlmittelverluststörfalls (DWR) erläutert. Dieser Störfall erfordert u.a. Gegenmaßnahmen des Personals außerhalb der Warte, die ca. 1 h bis 1.5 h nach Störfallbeginn angefordert werden. Für das Nichteinleiten dieser Maßnahmen, richtige Diagnose vorausgesetzt (NRC 1983, p.4-17ff), wird ein

Basiswert von 0.01 (MDN) verwendet. Als Quelle wird SWAIN (1980, p.20-31) genannt. In dieser Quelle wird dieser Wert als Fehlerwahrscheinlichkeit der Aufgabe "Ausführen einer Vorschrift (carry out a plant policy)" genannt. Als Datenbasis werden in SWAIN (1980, p.19-11) industrielle Erfahrungen (ohne weitere Quellenangabe) für das gelegentliche Ignorieren von Vorschriften genannt.

Dieser Basiswert wird noch durch Stress um den Faktor 2 erhöht und aufgrund von personeller Redundanz ca. um den Faktor 2 (hohe Kopplung, vgl. Anhang G) reduziert. Im Endeffekt bleibt es bei 0.01 (MDN).

Einleiten von feed + bleed

Im "Handbook of Human Reliability Analysis" (SWAIN 1983, ch.21) wird in einem Anwendungsbeispiel für die Wahrscheinlichkeit des Nichteinleitens der Primärkreisdruckentlastung "bleed" und Hochdruckeinspeisung "feed" nach erfolgter Diagnose ein Basiswert von 0.001 (MDN) verwendet. Als Begründung wird gesagt, daß dieser Wert für Fehler im Störfall immer dann zu verwenden ist, wenn keine anderen Daten (zu diesen Fehlern) verfügbar sind. Das Bewertungsproblem wird wie folgt kommentiert: "If the problem has been diagnosed correctly, it is very unlikely that the operator would fail to realize the help was needed".

SWAIN verzichtet auf eine Modifizierung durch Stressfaktoren, nimmt aber eine Modifizierung aufgrund vierfacher personeller Redundanz (d.h. drei zusätzliche Operateure mit Korrekturgelegenheit) vor. Im Endeffekt ergibt sich ein Wert von $3.5E-6$ (MDN).

Zum Vergleich: WAKEFIELD&ADAMS (1987, p.112) empfehlen die Wahrscheinlichkeit 0.01 für das Nichteinleiten von feed + bleed.

5.2.1.2 Kommentar

In beiden Beispielen wurden unterschiedliche Basiswerte verwendet. Die situationspezifische Modifizierung beschränkte sich auf die Faktoren PERSONELLE REDUNDANZ (in NRC und SWAIN) und STRESS (nur in NRC).

Der Einbeziehung personeller Redundanz ist zu entnehmen, daß Fehlverhalten nach erfolgter Diagnose nicht als Ergebnis einer bewußten kognitiven Abwägung (Entscheidung) aufgefaßt wurde, sondern als Ergebnis einer unbewußten (zufälligen) Unterlassung (im Sinne von etwas vergessen). Die Ursachen, die SWAIN (1983, P.16-6) für das gelegentliche Ignorieren von Vorschriften (MDN = 0.01) nennt, erlauben keine

Festlegung: Es werden Ursachen vermutet, die sowohl auf bewußtes Fehlverhalten (etwas für unnötig halten, etwas anderes für effektiver halten) als auch auf unbewußtes Fehlverhalten (etwas übersehen, abgelenkt sein) hindeuten.

Die konkreten Fehler, für die SWAIN die Verwendung der Wahrscheinlichkeit 0.01 (MDN) des gelegentlichen Ignorierens von Vorschriften empfiehlt, deuten eher auf bewußtes Fehlverhalten hin: Der Operateur kennt die richtige Verhaltensweise, weicht aber trotzdem von ihr ab (Tab. 34).

ORIGINALZITAT	ÜBERSETZUNG
Plant procedures or plant policies spelling out details and practices to follow in valve changing will not be followed; shortcuts or personal preferences will be followed instead	Prozeduren oder Vorschriften, die Einzelheiten enthalten, die bei Zustandsänderungen an Ventilen zu befolgen sind, werden nicht befolgt; stattdessen wird eine abkürzende oder dem Personal näher liegende Vorgehensweise angewendet
Nonuse of written procedures during valve changing or restoration	Nichtbenutzen einer schriftlichen Prozedur während Zustandsänderungen an Ventilen
Nonuse of control room written procedures under operating conditions that are normal	Nichtbenutzen einer schriftlichen Prozedur für Aufgaben des Wartepersonals unter normalen Betriebsbedingungen

Tab. 34. Verwendung der Wahrscheinlichkeit 0.01 (MDN) regelwidrigen Verhaltens:
SWAIN (1980, p.13-7,14-2,15-9,19-11)

Die subjektive Meinung des PRA-Durchführers, ob die Wahrscheinlichkeit 0.01 (MDN) für absichtliches oder unabsichtliches Ignorieren von Vorschriften gilt, kann einen entscheidenden Einfluß auf das Ergebnis einer menschlichen Zuverlässigkeitsanalyse haben:

- Wird unabsichtliches Fehlverhalten angenommen, dann ist - bei Verwendung von 0.01 als Basiswert - der Beitrag von regelwidrigem Verhalten nach erfolgter Diagnose zur Gesamtausfallwahrscheinlichkeit durch Korrekturfaktoren (aufgrund personeller Redundanz) reduzierbar. Dieses Vorgehen ist mit der Gefahr verbunden, daß der menschliche Faktor Risikoverhalten nicht angemessen berücksichtigt wird, sondern durch personelle Redundanz "wegdiskutiert" wird (s. feed + bleed-Beispiel).
- Wird absichtliches Fehlverhalten angenommen, dann ist - wenn man wie in GRS (1989, S.469) voraussetzt, daß die Entscheidungen vom Schichtleiter in alleiniger Verantwortung getroffen werden - personelle Redundanz nicht wirksam. D.h., die Fehlerwahrscheinlichkeit einer Aufgabe kann nicht kleiner als 0.01 (MDN) sein,

weil man stets (unter Bezugnahme auf das SWAIN-Handbuch) diesen Wert für ihr regelwidriges Nichteinleiten ansetzen kann.

Hier wird von der zweiten Interpretation (0.01 für bewußtes Fehlverhalten) ausgegangen. Aufgrund dieser Interpretation ergibt sich die Frage nach Einflußfaktoren (PSFs), die zur situationsabhängigen Modifizierung (sowohl in Richtung 1 als auch in Richtung 0) dieser Wahrscheinlichkeit zu verwenden sind. HALL u.a. (1982, p.26) nennen z.B. einen "reluctance factor" von 3, der immer dann anzuwenden ist, wenn eine gewisse Abneigung gegen die richtige Verhaltensweise besteht. Zur Berücksichtigung eines solchen PSFs wären zwei Schätzungen nötig:

1. Inwieweit trifft der PSF auf die in der PRA zu quantifizierende Situation zu?
2. Inwieweit ist der PSF schon durch die Wahrscheinlichkeit 0.01 berücksichtigt?

Diesem Vorgehen entsprechend wird hier im Abschnitt 5.2.3 ein Modell erarbeitet. Zunächst werden im Abschnitt 5.2.2 einige Erkenntnisse aus der psychologischen Sicherheitsforschung zum menschlichen Risikoverhalten referiert.

5.2.2 Erkenntnisse der psychologischen Sicherheitsforschung zu Fehlverhalten

5.2.2.1 Persönlichkeitsbedingte Risikobereitschaft

Die grundsätzliche Ursache von Fehlverhalten (im Sinne einer bewußten Risikoanahme) ist das Vorhandensein menschlicher Risikobereitschaft. Als synonyme Begriffe für Fehlverhalten werden hier auch die Begriffe riskantes oder sicherheitswidriges Verhalten verwendet. Die Existenz des Phänomens Risikobereitschaft führt zu der Frage, ob einige Menschen mehr zu riskantem Verhalten neigen und andere weniger.

In diesem Abschnitt werden zunächst die sicherheitspsychologischen Erkenntnisse zur persönlichkeitsbedingten Risikobereitschaft kurz referiert. Anschließend werden Schlußfolgerungen für das Auftreten von Fehlverhalten in Störfallsituationen abgeleitet.

Sicherheitspsychologische Erkenntnisse

Neigen einiger Menschen mehr zu riskantem Verhalten und andere weniger?

Diese Frage betrifft die "Unfällertheorie". MARBE (1926, S.104), einer der ersten Vertreter dieser Theorie, geht von der Existenz eines Menschen vom Typ "Unfäller" aus, den er als Gegenteil zum "Sicherheitsmensch" postuliert: "Es gibt *geborene* Unfälle, Schadens- und Unglücksstifter, geborene Pechvögel und Glückskinder."

Ergebnisse aus der Unfallstatistik, wie z.B. 50 % der Unfälle wurden von 70 % der Belegschaft verursacht, verleiten dazu, die Unfällertheorie als erwiesen anzusehen. Da es sich aber bei einem Unfall um ein seltenes Ereignis handelt, ist folgendes zu beachten: "Je geringer die durchschnittliche Ereignishäufigkeit einer Population, desto stärker ist die Konzentration der Ereignisse (Unfälle, Fehlhandlungen) auf eine kleine Minderheit" (HACKER 1980, S.356). Zur korrekten statistischen Überprüfung der Unfällertheorie gibt es folgende statistische Verfahren (vgl. HACKER 1980, S.355ff):

- Das Ausscheidungsverfahren. Man beobachtet die Unfallentwicklung, nachdem man die Personen, die die meisten Unfälle verursachten, ausgeschieden hat.
- Verfahren mit Hilfe eindimensionaler Verteilungen. Man berechnet über die Poissonverteilung, $p(k)$, die Häufigkeiten, $n(k)$, der Kategorien 0 Unfälle pro Person, 1 Unfall pro Person, 2 Unfälle pro Person usw., die sich ergeben würden, wenn keine individuellen Unterschiede in der Unfallneigung vorhanden wären. Danach überprüft man, ob sich signifikante Unterschiede zu den tatsächlich beobachteten Häufigkeiten dieser Kategorien ergeben.

$$n(k) = N p(k)$$

mit

$$p(k) = (\lambda^k / k!) \exp(-\lambda),$$

$$\lambda = m/N,$$

$n(k)$ = Anzahl der Personen mit k Unfällen, $k = 0, 1, 2, \dots$,

$p(k)$ = Wahrscheinlichkeit, daß k Unfälle pro Person auftreten,

N = Anzahl der Personen insgesamt,

m = Anzahl der Unfälle insgesamt.

- Verfahren mit Hilfe zweidimensionaler Verteilungsstatistik. Man berechnet den Korrelationskoeffizienten der Unfallhäufigkeiten von Personen zwischen zwei vergleichbaren Zeiträumen. Eine signifikante Korrelation würde die Unfällertheorie bestätigen: Personen mit hohen Unfallhäufigkeiten im ersten Zeitraum hätten auch vorwiegend hohe Unfallhäufigkeiten im zweiten Zeitraum.

Über die Gültigkeit der Unfälletheorie gibt es Meinungsverschiedenheiten. HACKER (1980, S.360) hält sie für widerlegt, UNDEUTSCH (1985, S.360) für erwiesen. SKIBA (1979, S.359f) faßt die Diskussion wie folgt zusammen:

„Trotzdem kann die von K.MARBE (1923, 1926) zuerst aufgestellte These, daß es Unfälle aufgrund persönlichkeitsgebundener Merkmale gebe, als gesichert gelten, auch wenn etwa ein Drittel aller Untersuchungen keinen signifikanten Nachweis dieser These erbrachte. Nur ist zu berücksichtigen, daß im Gegensatz zu der Hypothese von K.MARBE im allgemeinen das Problem des persönlichkeitsbewirkten Unfällers hinter dem des örtlich, also durch besondere Gefährdungen am Arbeitsplatz, bewirkten Unfällers zurücktritt.“

Die Diskussion über den Beitrag persönlichkeitsgebundener Eigenschaften zur Vermeidung von Fehlhandlungen wird auch in SWAIN (1980, p.2-5f) geführt. Hier wird zwischen dem „human-caused error“ (HCE - durch den Menschen selber verursacht) und dem „situation-caused error“ (SCE - durch die Arbeitsbedingung verursacht) unterschieden. In der Psychologie werden hierzu die Begriffe „Typen- und Eigenschaftstheorie“ und „Situationismus“ verwendet (vgl. HÄCKER 1980, S.328). Lt. SWAIN ist der HCE seltener als der SCE, weil Personen, die häufig durch Fehlhandlungen auffallen, nicht lange ihren Job behalten werden. Daraus wird der Vorrang eines an der Arbeitssituation orientierten Ansatzes zur Verhütung von Fehlhandlungen abgeleitet. Ein HCE-orientierter Ansatz wird für wenig effektiv gehalten. Dagegen hält UNDEUTSCH (1985, S.138) einen auf die Arbeitssituation beschränkten Ansatz für nicht ausreichend.

HOYOS (1980, S.175) ist der Meinung, daß aufgrund einfacher Unfallverteilungen keine Aussage über die Gültigkeit der Unfälletheorie gewonnen werden könnten. Er bezieht sich auf die „differentielle“ Hypothese in MAREK&STEN (1977), die drei Erklärungen einer Unfallverteilung, die in einer Population beobachtet wird, zuläßt:

1. Innerhalb der Population gibt es Individuen, die sich - bei gleicher Gefährdung durch die Arbeitssituation - im Unfallrisiko unterscheiden.
2. Es gibt Individuen, die eine gleiche (persönlichkeitsgebundene) Neigung zu Unfällen haben, sich aber trotzdem im Unfallrisiko unterscheiden, weil sie unterschiedlichen Gefährdungen ausgesetzt sind.
3. Es gibt Kombinationen aus unterschiedlichen Unfallneigungen und unterschiedlichen Gefährdungen.

Schlußfolgerungen

Wenn die Unfälle Theorie zutrifft, stellt sich die Frage der Persönlichkeitsmerkmale für Risikobereitschaft.

Unfallneigung läßt aber nicht zwangsläufig auf Risikobereitschaft schließen, weil Unfälle auch andere individuelle Ursachen (z.B. mangelnde Geschicklichkeit) haben können. Nach kritischer Prüfung der in der Literatur (z.B. UNDEUTSCH 1985, S.151ff; HOYOS 1980, S.163ff; HACKER 1980, S.363; SKIBA 1979, S.360) genannten Merkmale für Unfallneigung wurde "Feldabhängigkeit" (auch Extraversion oder Extroversion genannt) als ein Merkmal eingestuft, daß auch auf Risikobereitschaft hindeuten könnte:

Feldabhängiges Wahrnehmen ist mehr ganzheitlich, global und undifferenziert. Extravertierte Menschen sind weltzugewandt, aufgeschlossen für Anregungen und Eindrücke der Außenwelt, beschäftigen sich aber relativ wenig mit ihrem eigenen Innenleben. Extravertiertes Verhalten ist durch den Komplex folgender Merkmale charakterisiert: sozial aufgeschlossen und aktiv (geselligkeitslieben und mitteilungsbedürftig), impulsiv und spontan mit Neigung zum Risiko, optimistisch, emotional oft wenig gesteuert, Tendenzen zur Ungeduld und aggressivem Verhalten.

(vgl. JUNG 1921)

Zu einigen Merkmalen extravertierten Verhaltens liegen an KKW-Operateuren erhobene Daten vor (Tab. 35). GERTMAN u.a. (1985) ermittelten durch psychologische Tests an 7 von 24 Operateuren das Merkmal "typ-A-aktiv", das extravertiertem Verhalten recht nahe kommt. Typ-A-Operateure haben Eigenschaften wie Ehrgeiz, Aggressivität und Ungeduld.

Lt. SHEALY (1975) ist das Merkmal EXTERNALE KONTROLLE ein Indikator für Risikobereitschaft. Personen mit dieser Eigenschaft haben eine Tendenz zur Impulsivität (d.h. zu unüberlegten Entscheidungen). In Kombination mit einem hohen Bedürfnis nach Leistung deutet dieses Merkmal auf mäßige bis starke Risikobereitschaft hin, in Kombination mit einem geringen Bedürfnis nach Leistung auf hohe Risikobereitschaft (Tab. 36).

Merkmal	Ausprägung	Häufigkeit
(1) AKTIVITÄT (insgesamt)	TYP-A-AKTIV: Ehrgeiz, Streben nach Erfolg, aggressiv, ungeduldig, ruhelos	7
	TYP-B-AKTIV: zufrieden, geduldig, gelassen	17
(2) AKTIVITÄT: Eile und Ungeduld	TYP-A-AKTIV: eilig, ungeduldig	12
	TYP-B-AKTIV: geduldig, gelassen	12
(3) AKTIVITÄT: Verbundenheit mit der Berufstätigkeit	TYP-A-AKTIV: starke Verbundenheit, sehr engagiert	8
	TYP-B-AKTIV: geringe Verbundenheit	16
(4) AKTIVITÄT: Überanstrengung und Ehrgeiz	TYP-A-AKTIV: ehrgeizig, auf Wettbewerb eingestellt	3
	TYP-B-AKTIV: wenig ehrgeizig	21
(5) KONTROLLE	EXTERNALE KONTROLLE: kaum Glaube an die Beeinflußbarkeit von Geschehnissen, impulsiv	11
	INTERNALE KONTROLLE: Glaube an die Beeinflußbarkeit von Geschehnissen, wenig impulsiv	13

Tab. 35. An 24 Operateuren beobachtete Persönlichkeitsmerkmale:

Quelle: GERTMAN u.a. (1985, p.22).

Merkmal KONTROLLE nach Rotters. Aktivitätsmerkmale nach Jenkins. Die Aktivitätsmerkmale korrelieren mit der Anfälligkeit für Herzinfarkt (p.9).

Bedürfnis nach Leistung			
hoch		gering	
externale Kontrolle (impulsiv)	internale Kontrolle (wenig impulsiv)	externale Kontrolle (impulsiv)	internale Kontrolle (wenig impulsiv)
↓ mäßig bis sehr risikofreudig	↓ kalkuliertes Risiko- verhalten	↓ sehr risikofreudig	↓ risikomeidend

Tab. 36. Leistungsbedürfnis, Kontrolle und Risikoverhalten (SHEALY 1975)

Wenn man die Aussagen von SHEALY (1975) auf die Untersuchungsergebnisse von GERTMAN u.a. (1985) anwendet, dann folgt aufgrund der Häufigkeit der Ausprägung EXTERNALE KONTROLLE, daß 11 der 24 Operateure "mäßig bis sehr" oder "sehr risikofreudig" sind. Wenn man hohes Bedürfnis nach Leistung mit Ehrgeiz gleichsetzt, dann folgt aufgrund der Häufigkeit zu der Ausprägung TYP-A-AKTIV des Merkmals 4 in Tab. 35, daß 3 Operateure "mäßig bis sehr risikofreudig" sind oder ein "kalkuliertes Risikoverhalten" aufweisen. Die Anzahl der sehr risikofreudigen Operateure wäre gleich der Häufigkeit der Kombination EXTERNALE KONTROLLE und WENIG EHRGEIZIG. Diese Kombination ist der Untersuchung von GERTMAN u.a. (1985) nicht zu entnehmen, da nur eindimensionale Verteilungen angegeben sind. Da aber nur 3 Operateure als besonders ehrgeizig eingestuft wurden, ergibt sich für die Anzahl der sehr risikofreudigen Operateure folgende Mindestzahl:

$$11 - 3 = 8.$$

Welche Schlußfolgerungen ergeben sich für die Ermittlung von Daten für Fehlverhalten in Konfliktsituationen?

Zunächst ist festzustellen, daß es anscheinend (durch psychologische Tests ermittelbare) Merkmale für die Risikobereitschaft gibt. Da es zwischen diesen Merkmalen Kombinationseffekte gibt, ist die Aussagekraft eines einzelnen Merkmals - für sich gesehen - gering. Zur Berücksichtigung dieser Kombinationseffekte wären aufwendige Tests erforderlich. Der Sinn solcher Tests ist fraglich, wenn man - ähnlich wie in MAREK&STEN (1977), s.o. - zusätzlich einen Kombinationseffekt zwischen Persönlichkeitsvariablen und Situationsvariablen unterstellt.

Bezüglich der hier untersuchten Fragestellung kommt noch eine weitere Unsicherheit hinzu, wenn man in Betracht zieht, daß Risikobereitschaft auch positive Aspekte hat. Lt. SCHAARSCHMIDT (1971) sollte der erfolgreiche Operateur ein Verhalten aufweisen, daß weder auf sehr hohe Risikobereitschaft noch auf sehr hohe Risikomeidung ausgerichtet ist. Diese Auffassung steht mit Tab. 36 im Einklang: Operateure mit einem hohen Bedürfnis nach Leistung sind keine Risikomeider.

Es sind auch Fälle aus dem PRA-Bereich denkbar, in denen Risikobereitschaft nicht zwangsläufig mit Fehlverhalten korrelieren muß, nämlich immer dann, wenn die richtige Verhaltensweise riskante Aspekte aufweist, wie z.B. das Öffnen des Primärkreises bei der feed + bleed-Kühlung (s. Abschnitt 2). Das Öffnen widerspricht dem normalerweise anzustrebenden Ziel KEIN KÜHLMITTELVERLUST. Das Risiko läßt sich wie folgt formulieren: Der Primärkreis wird geöffnet, obwohl - wie sich im nachhinein

herausstellt - diese Maßnahme unnötig gewesen wäre, weil die eine andere Maßnahme zur Kühlung innerhalb kurzer Zeit abgeschlossen gewesen wäre.

In dem hier entwickelten Modell werden - entsprechend der PRA-üblichen Vorgehensweise - die o.g. Persönlichkeitsvariablen nicht berücksichtigt. Die Existenz des von ihnen ausgehende Einflusses auf das Auftreten von Fehlverhalten bewirkt jedoch, daß die hier berechneten Wahrscheinlichkeiten mit erheblichen - und in der Regel nur subjektiv quantifizierbaren - Unsicherheiten behaftet sind.

5.2.2.2 Zeitliche Tendenzen im Risikoverhalten

Neben individueller Unterschiede können auch zeitliche Unterschiede in der Neigung zu sicherheitswidrigen (riskantem) Verhalten auftreten. Hier wird eine zeitliche Variationsursache kurz andiskutiert: Der Einfluß positiver oder negativer Erfahrungen über den Ausgang getroffener Entscheidungen.

Das Regelkreismodell von SKIBA

SKIBA (1979, S.309) versucht einige Gesetzmäßigkeiten menschlichen Risikoverhaltens über ein Regelkreismodell zu beschreiben. Dieses Modell stellt eine spezielle Anwendung der sog. TOTE-Einheit dar (Test-Operate-Test-Exit) (MILLER u.a. 1960). Das Modell von SKIBA basiert auf zwei Variablen mit jeweils zwei Ausprägungen:

- Verhalten: sicherheitsgerecht oder sicherheitswidrig.
- Ausgang (Ergebnis) des Verhaltens: positiv (kein Unfall) oder negativ (Unfall).

Aus den Kombinationen dieser Variablen leitet er folgenden Rückwirkungen auf die zukünftigen Neigung zu sicherheitswidrigem bzw. sicherheitsgerechtem Verhalten ab:

1. Sicherheitswidriges Verhalten mit negativen Folgen erhöht die Neigung, sich demnächst sicherheitsgerecht zu verhalten.
2. Sicherheitswidriges Verhalten ohne negative Folgen erhöht die Neigung, sich auch weiterhin sicherheitswidrig zu verhalten.
3. Sicherheitsgerechtes Verhalten ohne negative Folgen kann die Neigung zu weiterem sicherheitsgerechten Verhalten entweder erhöhen oder verringern:

- Erhöhung, weil der Ausgang KEIN UNFALL als Erfolgserlebnis wahrgenommen wird.
- Verringerung, weil das häufige Auftreten des Ausgangs KEIN UNFALL ein nachlassendes Risikobewußtsein zur Folge hat.

Insgesamt ergibt sich lt. SKIBA eine Verschiebung zu sicherheitswidrigem Verhalten. Daraus leitet SKIBA die Schlußfolgerung ab, daß sich mit Maßnahmen, die der Motivierung in Richtung sicherheitsgerechtes Verhalten dienen, nur dann ein dauerhafter Erfolg erzielen läßt, wenn diese Maßnahmen ständig wiederholt werden. Ohne ständige Motivierung zu sicherheitsgerechtem Verhalten tendiert also das Regelkreismodell zu sicherheitswidrigem Verhalten. Diese Tendenz begründet SKIBA mit der (1) Seltenheit negativer Ausgänge und mit (2) Verdrängungsmechanismen zu der Möglichkeit ihres Eintretens.

(1) Da es sich bei einem Arbeitsunfall um ein seltenes Ereignis handelt, ist hierfür eine entsprechend geringe Erwartung vorhanden. Als Beleg für die Seltenheit nennt SKIBA (1979, S.310) folgende persönliche Mitteilung von REHHAHN (1973p), die auf Untersuchungen in einem Stahlwerk beruht:

- ein Unfall auf 4000 Regelverstöße und
- ein Unfall auf 40000 Arbeitsverrichtungen.

(2) "Weil das Unfallerlebnis negativ ist, also mit unserem natürlichen Wunschdenken nicht vereinbart werden kann, verdrängt der Mensch das Denken an die Möglichkeit des Unfalls" (SKIBA 1979, S.310).

Als weitere Begründung nennt SKIBA (1979, S.311) "die Tatsache, daß risikoreiches Verhalten oft weniger anstrengend und bisweilen auch als positiv empfunden wird und Ansehen verschafft".

Das Farmerspiel

Die Ergebnisse des Farmerspiels (SLOVIC u.a. 1977) ergaben eine Verschiebung in Richtung Risikomeidung. 30 Versuchspersonen (Vpn) sollten sich in die Situation eines Farmers (Wert der Farm 200000 \$) hineinversetzen. Es wurden 15 Runden gespielt. Ähnlich wie bei MONOPOLY erhielt jede Vpn pro Runde ein Einkommen von 6000 \$. In jeder Runde wurden 5 Verlustrisiken ausgespielt:

(1) 0.002×247500 \$, (2) 0.01×49500 \$, (3) 0.05×9900 \$, (4) 0.10×4950 \$ und (5) 0.25×1980 \$.

Vor jeder Risikoaussspielung wurde die Vpn gefragt, ob sie sich für 500 \$ gegen das Risiko versichern möchte. In einem zweiten Farmerspiel erhielten die Vpn - in Abhängigkeit von ihrem erspielten Kapital - Belohnungen zwischen 2.50 \$ und 20 \$.

Die Ergebnisse des Risikoverhaltens in der ersten und letzten Runde sind in Tab. 37 dargestellt. Für jedes Risiko war der Anteil der gekauften Versicherungen in der letzten Runde höher als in der ersten. Besonders hoch war diese Erhöhung für die Risiken mit mittelhoher Eintrittswahrscheinlichkeit. Dieser Trend war auch über alle 15 Spielrunden hinweg feststellbar: Durchschnittlich wurden nach jeder Runde mehr Versicherungen gekauft als gekündigt (SLOVIC u.a. 1977, p.252).

Farmerspiel	Spiel 1 (ohne Belohnung)		Spiel 2 (mit 2.50 - 20 \$ Belohnung)	
	1. Runde	15. Runde	1. Runde	15. Runde
Verlustrisiko/\$				
0.002 x 247500	33 %	50 %	35 %	72 %
0.01 x 49500	47 %	67 %	35 %	67 %
0.05 x 9900	56 %	83 %	65 %	76 %
0.10 x 4950	53 %	76 %	60 %	67 %
0.25 x 1980	72 %	76 %	64 %	67 %

Tab. 37. Anteil der 30 Vpn, die sich für 500 \$ versicherten (SLOVIC u.a. 1977)

Die Einflüsse negativer Erfahrungen auf das Risikoverhalten in der jeweils nächsten Runde waren gering: 15.4 % der Vpn, für die ein Verlust ausgespielt wurde, gegen den sie nicht versichert waren, entschieden sich in der nächsten Runde für eine Versicherung gegen diesen Verlust. Dieser Prozentsatz unterschied sich nur unwesentlich von dem Prozentsatz (13 %) der Vpn, die sich in der nächsten Runde versicherten, obwohl zuvor kein Verlust ausgespielt wurde.

Insgesamt ist also - im Gegensatz zu den Hypothesen von SKIBA - eine Tendenz zum risikomeidenden Verhalten feststellbar. Da zu dieser Tendenz auch Entscheidungen zu Risiken mit hoher Eintrittswahrscheinlichkeit beigetragen haben, ist die empirische Aussagekraft des Farmerspiels in Bezug auf die Hypothesen von SKIBA als gering einzustufen; denn ein Arbeitsunfall ist ein seltenes Ereignis (s.o.). Außerdem ist die Vergleichbarkeit zwischen Entscheidungen im Arbeitsalltag und Entscheidungen zu Versicherungen nur bedingt möglich. So ist z.B. im Farmerspiel risikomeidendes Verhalten direkt als Erfolg erlebbar, nämlich dann, wenn ein Verlust ausgespielt wird, gegen den man versichert ist. Für einen Arbeiter, der sich sicherheitsgerecht verhält, ist jedoch nur selten erfahrbar, ob sicherheitswidriges

Verhalten zur Erzielung des Ergebnisses KEIN UNFALL erforderlich war oder ob das gleiche Ergebnis auch mit sicherheitswidrigen Verhalten eingetreten wäre.

5.2.2.3 Risikovergleich und Risikokompensation

Theorie

Zur Beurteilung der Qualität einer Arbeitsbedingung sind stets folgende zwei Größen als Kriterien heranzuziehen (HACKER 1980, S.47f):

- Das Arbeitsergebnis, z.B. Stückzahl pro Zeiteinheit, und
- der Aufwand (die Anstrengung), mit dem (der) das Arbeitsergebnis erzielt wurde.

HACKER (1980) nennt ein Beispiel (RYAN&SMITH 1954) dafür, daß es vom Bezug der Motivierung abhängt, ob bzw. wie sich eine Veränderung der Arbeitsbedingung in einer Veränderung des Arbeitsergebnisses niederschlägt. Eine Verschlechterung der Arbeitsbedingung durch Temperaturerhöhung von 20°C auf 40°C führt nur dann zu einer Verringerung des Ausstoßes, wenn die Motivierung auf eine konstante Anstrengung gerichtet ist. Häufig ist aber die Motivierung auf einen konstanten Ausstoß gerichtet, so daß die verschlechterte Arbeitsbedingung durch eine erhöhte Anstrengung wieder kompensiert wird.

Eine ähnliche Gesetzmäßigkeit beinhaltet die Theorie der Risikokompensation (WILDE 1978) für den Bereich Risikoverhalten. Vorsichtsmaßnahmen können als Anstrengung interpretiert werden, Unfallhäufigkeit kann als negatives Arbeitsergebnis interpretiert werden.

Nach der Theorie von WILDE schätzt der Mensch das Risiko einer auszuübenden Tätigkeit ab. Dieses wahrgenommene Risiko RW vergleicht er mit dem Risiko RA , das er bereit ist, bei dieser Tätigkeit zu akzeptieren. Ist $RW > RA$, dann erhöht er seine Vorsichtsmaßnahmen. Ist $RW < RA$, dann verringert er sie. Das akzeptierte Risiko RA ist beobachtbar als Differenz zwischen dem wahrgenommenen Risiko RW und dem Risiko RV , das nach Ergreifung der Vorsichtsmaßnahmen noch vorhanden ist. Zu dem akzeptierten Risiko RA stellt WILDE die These auf, daß es (für die jeweilige Tätigkeit) eine individuelle Konstante ist.

Diese These hat weitreichende Konsequenzen. Demnach werden technische Verbesserungen zur Erhöhung der Sicherheit durch nachlassende Vorsicht wieder kompensiert. Beispiel: Die Umstellung von Zwei- auf Vierradbremmen hatte zur Folge,

daß die Autofahrer ihren Abstand zum vorausfahrende Fahrzeug kürzer wählen (UNDEUTSCH 1985, S.139).

Aber auch Ausbildungsmaßnahmen mit dem Ziel, die Risikowahrnehmung zu verbessern, haben wegen langfristiger Rückkopplungen nur eine begrenzte Wirksamkeit: Das vorhandene Risiko wird seltener unterschätzt, die Vorsichtsmaßnahmen werden verstärkt, die Unfallzahl sinkt und somit das wahrgenommene Risiko, die Vorsichtsmaßnahmen werden wieder verringert.

Fazit: Ein dauerhafter Erfolg kann nur durch Maßnahmen (Tab. 38) zur Senkung der Risikobereitschaft (d.h. des akzeptierten Risikos RA) erzielt werden (WILDE 1978, S.141).

MASSNAHME	BEISPIELE
(1) Den erwarteten Nutzen von riskantem Verhalten herabsetzen	• Keine Akkord bei gefährlichen Arbeiten geben • Fernfahrern keine Prämie für frühes Eintreffen am Ziel gewähren
(2) Die erwarteten Kosten von vorsichtigem Verhalten herabsetzen	• durch gleitende Arbeitszeit, wodurch Vorsicht auf der Fahrt zum Betrieb nicht bestraft wird • durch bequeme, gut handhabbare Sicherheitsgurte
(3) Den erwarteten Nutzen von vorsichtigem Verhalten heraufsetzen	• Prämien für das Tragen von Schutzausrüstung • Prämien für Unfallfreiheit
(4) Die erwarteten Kosten von riskantem Verhalten heraufsetzen	• höhere Versicherungsprämien für Fahrer mit Unfällen

Tab. 38. Maßnahmen zur Senkung der Risikobereitschaft (WILDE 1978)

Schlußfolgerungen aus dem Risikovergleich RW-RA

Allgemein

Ein Bestandteil der Theorie der Risikokompensation ist der bei der Entscheidungsfindung angenommene Vergleich zwischen dem wahrgenommenen Risiko RW und dem akzeptierten Risiko RA:

$RW > RA$: Erhöhung der Vorsichtsmaßnahmen,

$RW < RA$: Verringerung der Vorsichtsmaßnahmen.

Das hier untersuchte Fehlverhalten läßt sich über eine Diskretisierung der Variable Vorsichtsmaßnahmenumfang V definieren: Unterschreitung des Umfangs an Vorsichtsmaßnahmen V' , der lt. Vorschrift einzuhalten ist. Für die Fehlverhaltenswahrscheinlichkeit p gilt demnach:

$$p = w(V < V')$$

Diese Gleichung ist geeignet, um auf der Basis empirischer Daten p zu schätzen. Zur Vorhersage von p auf der Basis des akzeptierten Risikos RA gilt:

$$p = w(RW \leq RA) = w(RA - RW \geq 0),$$

wobei RA u.a. auch von den vorgeschriebenen Vorsichtsmaßnahmen V' , d.h. von den Kosten vorsichtigen Verhaltens (Tab. 38), abhängt. Mit RA und RW als Zufallsgrößen (aufgrund individueller Unterschiede in der Risikobereitschaft und -wahrnehmung) erhält man:

$$p = \int_{UGR}^{OGR} g(R) F(R) dR$$

mit

$g(R)$ = Verteilungsdichte des akzeptierten Risikos,

$F(R)$ = Verteilungsfunktion des wahrgenommenen Risikos,

UGR = Untergrenze des Definitionsbereichs für das Risiko,

OGR = Obergrenze des Definitionsbereichs für das Risiko.

Mit Hilfe des Thurstone-Modells Fall V (vgl. COOMBS u.a. 1975), läßt sich - bei bekannter Fehlverhaltenswahrscheinlichkeit p - der Erwartungswert (oder Mittelwert) der Differenz zwischen dem wahrgenommen und akzeptiertem Risiko auf einer Intervallskala abbilden. Dabei wird für das akzeptierte Risiko vorausgesetzt, daß alle Mittelwerte mit konstanter Standardabweichung DRA normalverteilt sind. Für das wahrgenommene Risiko wird die gleiche Voraussetzung getroffen. Weiter wird vorausgesetzt, daß die Standardabweichung DRW des wahrgenommenen Risikos von der Standardabweichung DRA des akzeptierten Risikos unabhängig ist. Für die Risikodifferenz (Mittelwert) gilt:

$$ERA - ERW = z(p) [(DRA)^2 + (DRW)^2]^{0.5}$$

mit

$z(p) = \Phi^{-1}(p)$ = inverse Funktion der Standardnormalverteilung,

ERA = Mittelwert des akzeptierten Risikos,

ERW = Mittelwert des wahrgenommenen Risikos.

Aufgrund der o.g. Voraussetzung ist der Faktor hinter $z(p)$ für alle Differenzen gleich. Er kann daher gleich 1 gesetzt werden; denn die Einheit einer Intervallskala ist frei wählbar.

Beispiel 1: Fiktive Situationen, reale Verhaltenswahrscheinlichkeiten

Die o.g. Skalierungsmethode wird nun am Beispiel der Ergebnisse der 15. Runde des ersten Farmerspiels (Tab. 37 auf Seite 121) erläutert.

Es gilt:

$$ERW = ERA - z(p) \text{ (Thurstone Fall V)}$$

mit

p = Anteil der Vpn, die sich GEGEN die Versicherung entschieden.

Da jede Versicherung den gleichen Preis (500 \$) kostete, ist der Mittelwert (ERA) des akzeptierten Risikos in allen Situationen gleich. ERA kann daher gleich 0 gesetzt werden, denn der Nullpunkt einer Intervallskala ist frei wählbar; daraus folgt:

$$ERW = - z(p).$$

Man erhält somit folgenden Skalenwerte der im Farmerspiel wahrgenommen Risikomittelwerte:

Skalenwert→	0	0.44	0.71	0.95
Verlustrisiko →	0.002x247500\$	0.01x49500\$	0.10x4950\$ 0.25x1980\$	0.05x9900\$

Der Skala ist zu entnehmen, daß z.B. das Risiko 0.25x1980\$ um 0.71 Einheiten höher bewertet wurde als das Risiko 0.002x247500\$. In der ersten Runde lag diese Skalenwertdifferenz bei 1.02 Einheiten.

Diese Ergebnisse können jedoch nicht verallgemeinert werden. Tab. 39 zeigt, daß selbst in klar definierten Spielsituationen widersprüchliche Ergebnisse zum Risikoverhalten vorliegen.

VERSUCH → (GE = Geldeinheit) STUDIE ↓	(I) (A) 0.5x1000 GE Verlustrisiko ODER (B) 500 GE sicherer Verlust	(II) (A) 0.001x5000 GE Verlustrisiko ODER (B) 5 GE sicherer Verlust
(1) Kahneman&Tversky (1979), p.273 + 281	68 Vpn: 69 % für A 31 % für B	72 Vpn: 17 % für A 83 % für B
(2) Slovic u.a. (1977), p.246	36 Vpn: 47 % für A 53 % für B	36 Vpn: 72 % für A 28 % für B

Tab. 39. Widersprüchliche Ergebnisse zum Risikoverhalten in Spielsituationen

In Studie 1 tendierten die Vpn zu Risiken mit hoher Eintrittswahrscheinlichkeit und mieden Risiken mit kleiner Eintrittswahrscheinlichkeit. Diese Ergebnisse erklären KAHNEMAN&TVERSKY (1979) mit der subjektiven Gewichtsfunktion (p.283) von Wahrscheinlichkeiten: Kleine Wahrscheinlichkeiten werden (im Vergleich zu ihren wahren bekannten Zahlenwerten) zu hoch bewertet, hohe Wahrscheinlichkeiten werden zu niedrig bewertet. Insgesamt werden die Eintrittswahrscheinlichkeiten der möglichen Ausgänge so bewertet, daß ihre Summe kleiner als 1 ist ("subcertainty").

In Studie 2 entschied sich eine knappe Mehrheit gegen das Risiko mit hoher Eintrittswahrscheinlichkeit (I), aber eine deutliche Mehrheit für das Risiko mit kleiner Eintrittswahrscheinlichkeit (II). Das Ergebnis aus Versuch II erklären SLOVIC u.a. (1977, p.254) mit der Schwellenwerttheorie: Risiken mit Eintrittswahrscheinlichkeiten, die unterhalb einer gewissen Grenze liegen, werden vernachlässigt.

Die Ergebnisse zu Versuch I sind auch mit der Form der Verlustfunktion erklärbar. Ist diese Funktion konvex, dann werden Verschlechterungen im Bereich hohe Verluste (hier von 500 GE auf 1000 GE) höher bewertet als Verschlechterungen im Bereich kleiner Verluste. Ist diese Funktion konkav, dann werden Verschlechterungen im Bereich hohe Verluste niedriger bewertet als Verschlechterungen im Bereich kleiner Verluste.

Das Vorliegen verschiedener Phänomene menschlichen Entscheidungsverhaltens ("subcertainty", Schwellentheorie, Konvexität, Konkavität) hat also zur Folge, daß selbst in klar definierten Spielsituationen keine eindeutigen Vorhersagen zum Risikoverhalten gemacht werden können.

Beispiel 2: Reale Situationen, fiktive Verhaltenswahrscheinlichkeiten

Das oben erläuterte Thurstone-Modell (Fall V) hat den Vorteil, das auch verbal formulierte Risiken - zu denen keine Zahlenwerte über Verlustwahrscheinlichkeiten und -höhen bekannt sind - auf einer Skala abgebildet werden können. In Tab. 40 wurde eine solche Skalierung für reale KKW-Situationen (in der Terminologie der Theorie der Risikokompensation) durchgeführt.

TÄTIGKEIT: Vom Wartenpersonal durchzuführende Prozedur			
RISIKO: Unterlassung (Vergessen) eines wichtigen Schritts			
VORGESCHRIEBENE VORSICHTSMASSNAHME: Benutzung der für die Tätigkeit vorgesehenen schriftlichen Unterlage			
FEHLVERHALTEN: Nichtbenutzen der schriftliche Unterlage			
FALL 1: Normalbetrieb, kein besonderer Anreiz zu Fehlverhalten $p_1 = 0.01$ (MDN) $= w(RA'' - RW'' \geq 0)$ $\rightarrow ERW'' - ERA'' = z(p_1)$ $= 2.33$	FALL 2: Störfall, kein besonderer Anreiz zu Fehlverhalten $p_2 = 0.005$ (MDN) $= w(RA'' - RW' \geq 0)$ $\rightarrow ERW' - ERA' = z(p_2)$ $= 2.58$	FALL 3: Normalbetrieb, besonderer Anreiz (z.B. Termindruck) zu Fehlverhalten $p_3 = 2 \cdot 0.01$ (MDN) $= w(RA' - RW'' \geq 0)$ $\rightarrow ERW'' - ERA' = z(p_3)$ $= 2.05$	
↓ INTERVALLSKALA (mit ERA'' = 0) ↓			
Akzeptiertes Risiko für das Nichtbenutzen der schriftl. Unterlage (ERA'') ↓	Akzeptiertes Risiko für das Nichtbenutzen der schriftl. Unterlage, wenn besonderer Anreiz (ERA') ↓	Wahrgenommenes Risiko eines Unterlassungsfehlers im Normabetrieb (ERW'') ↓	Wahrgenommenes Risiko eines Unterlassungsfehlers im Störfall (ERW') ↓
0	0.25	2.33	2.58
1	1.64	98.5	161.1
↑ VERHÄLTNISSKALA (s. Text)			

Tab. 40. Beispiel für eine Skalierung verbal formulierter Risiken:
Verhaltenswahrscheinlichkeiten aus SWAIN (1983, p.20-22);
Faktor 2 (PSF, FALL 3) aus WILLIAMS (1988, EPC21).

Außerdem wurden - auf der Grundlage des probabilistischen Entscheidungsmodells von LUCE (1959) - die Risiken auf einer Verhältnisskala abgebildet. Nach dem Modell von LUCE gilt für die Wahrscheinlichkeit von Fehlverhalten:

$$p = w(RW \geq RA) = 1/(1 + ERW^*/ERA^*) = 1/\{1 + \exp[k (ERW - ERA)]\}$$

mit

$$ERA^* = \exp(k ERA)$$

= Verhältnisskalenwert des akzeptierten Risikos (Mittelwert),

$$ERW^* = \exp(k ERW)$$

= Verhältnisskalenwert des wahrgenommenen Risikos (Mittelwert).

In LUCE (1959) wurde gezeigt, daß sich eine gute Übereinstimmung ergibt, wenn man die über das Thurstone-Modell berechneten Intervallskalenwerte für ERA und ERW in die o.g. Gleichung einsetzt. Der zur Bestimmung von ERA* und ERW* benötigte Wert k ergibt sich also, indem man die o.g. Gleichung nach k auflöst,

$$k = [\ln(1/p - 1)]/(ERW - ERA),$$

und für einen bekannten Fall, z.B. Fall 1 (Tab. 40), die über das Thurstone-Modell berechneten Skalenwerte einsetzt:

$$k = [\ln(1/0.01 - 1)]/(2.33 - 0) = 1.97.$$

Zur Schätzung der Fehlverhaltenwahrscheinlichkeit p_4 eines 4. Falls, z.B. besonderer Anreiz für das Nichtbenutzen der schriftlichen Unterlage ($RA' = 0.28$) und Risiko für Unterlassungsfehler im Störfall ($RW' = 2.58$), ergeben sich nun folgende Möglichkeiten:

1. Die PRA-übliche Methode. Direkte Anwendung von $PSF = 2$ (Tab. 40, Fall 3) auf die Wahrscheinlichkeit in Fall 2:

$$p_4 = 2 \cdot p_2 = 2 \cdot 0.005 = 0.01.$$

2. Anwendung des Thurstone-Modells:

$$p_4 = \Phi(ERA' - ERW') = \Phi(-2.3) = 0.01.$$

3. Anwendung des Luce-Modells:

$$p_4 = 1/(1 + ERW^*/ERA^*) = 1/(1 + 161.2/1.74) = 0.011.$$

Generell gilt, daß die Abweichung von der PRA-üblichen Methode umso größer ist, je näher die zu modifizierende Wahrscheinlichkeit bei 1 liegt. Insgesamt zeigt die PRA-übliche Methode eine gute Übereinstimmung zu den methodisch korrekten Ver-

fahren nach Luce oder Thurstone. Abweichungen sind durch die hohen Unsicherheitsfaktoren (mindestens 3), die in einer PRA für Wahrscheinlichkeiten menschlicher Fehler angesetzt werden (SWAIN 1983, p.7-13), erfaßt.

Wegen fehlender Daten wird hier (Abschnitt 5.2.3) ein Modell verwendet, daß auf die in einer PRA üblichen direkten Modifizierungen mit Faktoren (PSFs), beruht. Auch die Datenvielfalt in Tab. 40 ist nur vorgetäuscht. Allenfalls die Wahrscheinlichkeit für Fall 1 beruht auf empirischen Daten.

Fazit: Die Theorie der Risikokompensation (in Verbindung mit dem Thurstone-Modell) liefert einen geeigneten Ansatz zur Auswertung von auf empirischen Daten beruhenden Fehlverhaltenswahrscheinlichkeiten. Mit Hilfe der dadurch gewonnenen Risikoskala lassen sich dann auch Fehlverhaltenswahrscheinlichkeiten berechnen, für die keine empirischen Daten verfügbar sind.

Schlußfolgerungen aus der Risikokompensation

Die Risikokompensation, d.h. die Anpassung der Vorsichtsmaßnahmen an das wahrgenommene Risiko, ist der dynamische Bestandteil der Theorie von WILDE (1978) über das Verhalten in gefährlichen Situationen. Zu den sich daraus ergebenden Folgen für die Wirksamkeit technisch-organisatorischer Maßnahmen zur Erhöhung der Sicherheit schreibt UNDEUTSCH (1985, S.138):

„Nie kann auf diesem Wege erreicht werden, daß sicherheitswidriges Verhalten unmöglich oder unter allen Umständen schadlos bleibt. Es ist nicht einmal selten, daß mit technisch-organisatorischen Maßnahmen erreichte Sicherheitsgewinne durch daraufhin nachlassende Sorgfalt seitens des in das System einbezogenen Menschen ganz oder teilweise wieder aufgezehrt“ werden.

D.h. auch in Systemen mit weitgehender Automatisierung, hervorragenden ergonomischen Verhältnissen und sehr guter Arbeitsorganisation kann es aufgrund menschlicher Risikobereitschaft zu Schadensereignissen kommen. Deshalb haben die in Tab. 38 auf Seite 123 genannten Maßnahmen zur Senkung der Risikobereitschaft eine hohe Bedeutung.

5.2.3 Methodische Empfehlung zur Quantifizierung von Fehlverhalten

"Blame and guilt tend to be associated with errors, and therefore many erroneous actions are not reported because of the likelihood of punitive actions against the operator." (EMBREY u.a. 1984, Vol.I, p.2)

Das Zitat trifft insbesondere auf Fehlverhalten im Sinne einer bewußten Risikoan-nahme zu. Die Aussicht auf empirische Daten, die eine direkte Ableitung von situa-tionsspezifischen Wahrscheinlichkeiten zu solchem Fehlverhalten erlauben, ist also gering. Deshalb wird hier ein Modell vorgeschlagen, das auf Extrapolationen zu vor-handenen Daten beruht. Zu dem Modell wurde ein benutzerfreundliches EDV-Programm erstellt.

Die Extrapolationen erfolgen auf der Grundlage von subjektiven (vom Anwender ein-zugebenden) Schätzungen über den "Grad des Vorhandenseins" von Einflußfaktoren (s. Abschnitt 5.2.3.2). Die Modellparameter sind voreingestellt und werden zusammen mit der Ergebnswahrscheinlichkeit ausgedruckt. Die Schätzungen (Abschnitt 5.2.3.3), mit denen die Modellparameter berechnet wurden, werden ebenfalls mit ausge-druckt. Diese Schätzungen können ohne großen Aufwand vom Benutzer geändert werden.

5.2.3.1 Theoretische Grundlage: SLIM

Wegen unzureichender Wahrscheinlichkeitsdaten zu Fehlverhalten wird hier ein auf n Einflußfaktoren (PSFs) basierendes Extrapolationsmodell (Abb. 20) angewendet:

$$p = p_o \prod_{i=1}^n F_i = p_o \prod_{i=1}^n K_i^{x_i} \quad (1)$$

mit

$0 \leq x_i \leq 1$,

$K_i > 1$,

p_o = Basiswahrscheinlichkeit (kleinster Wert),

K_i = maximaler Faktor von PSF i ,

x_i = Grad des Vorhandenseins von PSF i .

Die Skalierung eines Faktors F_i erfolgt geometrisch über die Beziehung

$$F_i = K_i^{x_i} \quad (2)$$

Der Grad x_i des Vorhandenseins kann Werte zwischen 0 ("nicht vorhanden") bis 1 ("total vorhanden") annehmen. Für $x_i=0$ ist daher $F_i=1$ (d.h. keine Erhöhung). Für $x_i=1$ ist $F_i=K_i$ (d.h. maximale Erhöhung).

Die Bestimmung von p_o (Abschnitt 5.2.3.3) erfolgt auf der Basis der auf industriellen Erfahrungen basierenden Wahrscheinlichkeit

$$p' = 0.01 < 5 > \text{ (d.h. MDN = 0.01, UF = 5)}$$

für das gelegentliche Ignorieren von Vorschriften (SWAIN 1980, p.19-11). Die Auswahl der PSFs erfolgt in Abschnitt 5.2.3.2.

Das oben skizzierte Vorgehen basiert auf dem Modell SLIM-MAUD (EMBREY u.a. 1984; EMBREY 1983). Nach der in EMBREY (1983, p.15) angesetzten Modellgleichung hängt die logarithmierte Fehlerwahrscheinlichkeit p linear von einem Zuverlässigkeitsindex SLI ab:

$$\log p = C + D \text{ SLI} \quad (3)$$

$$\text{SLI} = \sum_{i=1}^n (y_i w_i) \quad (4)$$

$$\sum_{i=1}^n w_i = 1$$

mit

$$0 \leq y_i \leq 1,$$

$$0 \leq w_i \leq 1,$$

$$0 \leq \text{SLI} \leq 1,$$

n = Anzahl der Einflußfaktoren (PSFs),

y_i = Skalenwert von PSF i bzgl. Zuverlässigkeitserhöhung,

w_i = Wichtungsfaktor von PSF i .

SLI ist ein Maß für eine aus den einzelnen PSFs zusammengefaßte Expertenmeinung über die erfolgreiche Durchführung der betrachteten Aufgabe (EMBREY u.a. 1984, Vol.I, p.3).

Das Modell läßt sich, mit

$x_i = 1 - y_i =$ Skalenwert bzgl. Zuverlässigkeitsminderung,

ebenfalls in ein loglineares Modell mit einem Fehlerindex FLI als Einflußgröße überführen:

$$\log p = A + B \text{ FLI} \quad (5)$$

$$\text{FLI} = \sum_{i=1}^n (w_i x_i) \quad (6)$$

mit

$$0 \leq \text{FLI} \leq 1,$$

$$A = C + D,$$

$$B = -D.$$

Das Modell in Gleichung 1 läßt durch Logarithmieren in das o.g. FLI-Modell (Gleichung 5) überführen:

$$\begin{aligned} \log p &= \log \left(p_o \prod_{i=1}^n K_i^{x_i} \right) \\ &= \log p_o + \sum_{i=1}^n (x_i \log K_i) \\ &= \log p_o + \sum_{i=1}^n (\log K_i) \sum_{i=1}^n \frac{x_i \log K_i}{\sum_{i=1}^n (\log K_i)} \\ &= A + B \sum_{i=1}^n (x_i w_i) \\ &= A + B \text{ FLI} \end{aligned}$$

mit

$$B = \sum_{i=1}^n (\log K_i) \quad (7)$$

$$w_i = \frac{\log K_i}{\sum_{i=1}^n (\log K_i)} \quad (8)$$

$$A = \log p_o \quad (9)$$

Das hier verwendete PSF-Modell ist also eine umgeformte Version des Modells SLIM. FLI kann als ein Maß für die aus den einzelnen PSFs zusammengefaßte Expertenmeinung über das Auftreten des betrachteten Fehlers interpretiert werden.

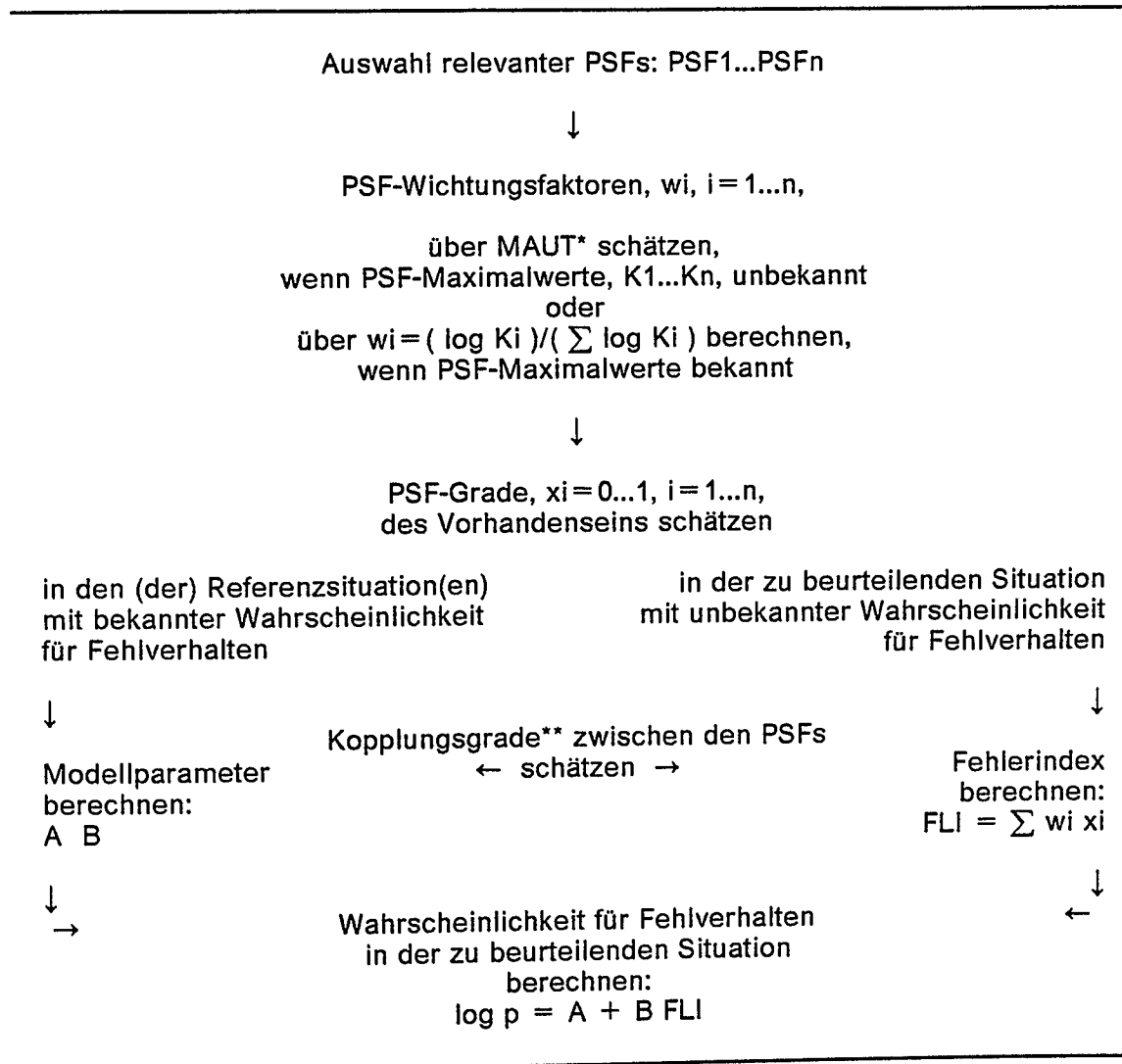


Abb. 20. PSF-Extrapolationsmodell:

* Multi-Attribute Utility Theory (Bestandteil von SLIM-MAUD),
 ** kein Bestandteil von SLIM-MAUD, wird hier nur andiskutiert.

5.2.3.2 Berücksichtigte Einflußfaktoren (PSFs)

Hier wurden nur Einflußfaktoren mit bekanntem Maximalfaktor K_i berücksichtigt. Dies hat den Vorteil, daß die aufwendige Schätzung der Wichtungsfaktoren (über MAUT) entfallen konnte (s. Abb. 20). Das Ergebnis der hier durchgeführten Literaturdurch-

sicht über Einflußfaktoren für Fehlverhalten (im Sinne einer bewußten Risikoan-
nahme) ist in Tab. 41 zusammengestellt.

Fak- tor	Zitat	Interpretation
2	An incentive to use other more dangerous procedures*	(x1) Besonderer Anreiz zu Fehlverhalten: x1 = 1, wenn richtiges Verhalten nicht nur lästig ist, sondern durch Fehlverhalten besondere Unannehmlichkeiten (wie z.B. längere Ab- schaltpausen) vermieden werden können. x1 = 0, wenn durch Fehlverhalten - abgesehen von geringfügigen Vorzügen (wie z.B. Bequem- lichkeit) - keine besondere Vorteile erzielt werden können.
2.5	A conflict between immediate and long term objectives*	(x2) Zielkonflikt: x2 = 1, wenn es irgendeinen (auch geringfügigen) An- reiz für Fehlverhalten gibt. x2 = 0, wenn praktisch überhaupt keinen Anreiz für Fehlverhalten gibt. Wenn x2 = 0, dann ist ein anderes Modell zu verwenden.
12.5	Personal safety affected**	(x3) Möglicher Schaden vernachlässigbar klein: x3 = 1, wenn Fehlverhalten zwar zu einem Fehler füh- ren kann (z.B. Unterlassung eines Aufgabenteils einer ohne Checkliste durchgeführten Proze- dur), dieser Fehler aber nur eine geringfügige Sicherheitsbedeutung hat. $0 < x3 \leq 0.5$, wenn durch Fehlverhalten ein schwerwie- gender Schaden mit erhöhter Wahrschein- lichkeit auftreten kann. x3 = 0, wenn durch Fehlverhalten ein schwerwie- gender Schaden praktisch erst ermöglicht wird.

Tab. 41. Einflußfaktoren zur Quantifizierung von Fehlverhalten: (wird fortgesetzt)

Faktor	Zitat	Interpretation
2	If an operator is assigned as a checker of a maintainer use one-half the HEPs of an operator checking another operator ... the operator-checker is likely to take more care when checking the work of a maintainer**	(x4) Kleine Wahrscheinlichkeit für Mißerfolg: $x_4 = 1$, wenn gute Erfolgschancen trotz Fehlverhalten. $x_4 = 0$, wenn sehr geringe Erfolgschancen bei Fehlverhalten.
4	A mismatch between perceived and real risk*	(x5) Risikounterschätzung: $x_5 = 1$, wenn z.B. Interviews ergeben, daß das Personal sehr optimistische Erwartungen über den Eintritt und das Ausmaß von Ereignisabläufen hat: "Wieso kann das System ausfallen, wir haben doch 2 Pumpen". $0.5 < x_5 < 1$, wenn die Wahrscheinlichkeit für den Mißerfolg bei Fehlverhalten zeitabhängig ist.*** $x_5 = 0$, wenn Interviews ergeben, daß eine realistische Risikoeinschätzung vorhanden ist.
9	A means of suppressing or over-riding information or features which is too easily accessible*	(x6) Fehlverhalten zu einfach, fehlende Hindernisse: $x_6 = 1$, wenn Fehlverhalten passiv (kein aktiver Eingriff) und Fehlverhalten als Fehlinterpretation erklärbar $0.5 < x_6 < 1$, wenn Fehlverhalten passiv, aber nicht ohne weiteres als Fehlinterpretation erklärbar. $x_6 = 0$, wenn Fehlverhalten mit einem aktiven Eingriff ins System (z.B. Überbrücken eines Schutzsignals) verbunden ist.
6	A need to unlearn a technique and apply one which requires the application of an opposing philosophy*	(x7) Richtiges Verhalten ist ungewöhnlich, Fehlverhalten manchmal richtig: $x_7 = 1$, wenn ein Systemzustandsziel (z.B. Öffnen des Primärkreises während feed + bleed) richtigen Verhaltens einem normalen Systemzustandsziel (z.B. Primärkreisintegrität) widerspricht. $x_7 = 0$, wenn durch richtiges Verhalten kein Widerspruch zu normalen Systemzustandszielen entsteht.
* WILLIAMS (1988), ** SWAIN (1980, p.13-12ff), *** vgl. HAAS&BOTT (1982)		
Tab. 41 (Fortsetzung)		

Die Auswahl der PSFs x_1 bis x_5 ist mit dem "klassischen" entscheidungstheoretischen Ansatz begründbar (EDVARDS 1968). Denn sie beziehen sich auf die Ausgänge (Kosten und Nutzen sowie deren Eintrittserwartungen) falschen (sicherheitswidrigen) und richtigen (sicherheitsgerechten) Verhaltens. Zahlreiche Autoren (z.B. zusammenfassend in HOYOS 1980, S.126ff) gehen davon aus, daß das Entschei-

ungsverhalten in Risikosituationen von dem Abwägen positiver und negativer Anreize möglicher Handlungsfolgen sowie deren Eintrittserwartungen abhängt.

Die PSFs x6 FEHLVERHALTEN ZU EINFACH und x7 RICHTIGES VERHALTEN UNGEWÖHNLICH stellen eine Erweiterung dieses Ansatzes dar. Sie beziehen sich nicht auf die Handlungsfolgen, sondern auf die Art der Verhaltensweise selber. Der zusammengefaßte Effekt dieser PSFs kann als Index FEHLVERHALTEN NAHELIEGEND interpretiert werden. Diese PSFs bewirken, daß konfliktbedingtes Fehlverhalten noch als Fehlinterpretation ausgelegt werden kann. So war z.B. das während des Störfalls im DWR Davis-Besse (Abschnitt 2) aufgetretene Fehlverhalten "Nichteinleiten von feed + bleed" einfach durchführbar, weil es praktisch im "Nichtstun" bezüglich feed + bleed bestand. Außerdem entsprach es der Gewohnheit, weil feed + bleed im Widerspruch zu dem normalerweise angestrebtem Handlungsziel "Integrität des Primärkreises" steht.

Für den Modifizierungsfaktor eines PSFs mit dem Maximalfaktor K gilt:

$$F = K^x \quad (10)$$

Die Maximalfaktoren sind in Tab. 41 aufgelistet. Der Skalenwert x ist der "Grad des Vorhandenseins" des betrachteten PSFs; x ist situationsspezifisch zu schätzen. Im Rahmen einer PRA ist es üblich, Wertebereiche zu diskretisieren (z.B. SWAIN 1983, p.6-9). Hier wird folgende Diskretisierung verwendet:

- x = 0 für NICHT,
- x = 0.25 für SCHWACH,
- x = 0.50 für MITTEL oder KEINE AHNUNG,
- x = 0.75 für STARK und
- x = 1.0 für TOTAL.

Bei der Schätzung KEINE AHNUNG wird die Unsicherheit mit doppelter Standardabweichung berücksichtigt (s. Abschnitt 5.2.3.4).

Abb. 21 enthält die Eingabedatei des hier erstellten Rechenprogramms. Vom Benutzer wird verlangt, daß er zu jedem PSF eine Schätzung abgibt. Es empfiehlt sich, diese Schätzungen unter Zurhilfenahme von Tab. 41 durchzuführen. Außerdem können Beschreibungen zu dem betrachteten Fehlverhalten sowie dessen Vor- und Nachteile angegeben werden.

Aus den in der Tab. 41 genannten Maximalfaktoren erhält man (unter Anwendung von Gleichung 8 in Abschnitt 5.2.3.1) folgende Parameter des FLI-Modell in Gleichung 5 (Tab. 42).

(x1)	(x2)	(x3)	(x4)	(x5)	(x6)	(x7)
Besonderer Anreiz zu Fehlverhalten	Zielkonflikt	Möglicher Schaden gering	Wahrsch. für Schaden gering	Risiko wird unterschätzt	Fehlverhalten zu einfach	Richtiges Verhalten ungewöhnlich
w1=0.068	w2=0.089	w3=0.248	w4=0.068	w5=0.14	w6=0.215	w7=0.176

Tab. 42. PSF-Wichtungsfaktoren

SITUATION: .

FEHLVERHALTEN: .

VORTEIL: .

NACHTEIL: .

. MEDIAN DER WAHRSCH. FÜR FEHLVERHALTEN

. UNSICHERHEITSFAKTOR (BEZUGLICH 90%-INTERVALL)

FRAGE: WELCHER GRAD DES ZUTREFFENS? (LINKS EINTRAGEN!)

(.=KEINE AHNUNG, 0=NICHT, 25=SCHWACH, 50=MITTEL, 75=STARK, 100=TOTAL)

- . _____ PERSONAL SIEHT BESONDEREN ANREIZ ZU FEHLVERHALTEN (X1)
- . _____ KONFLIKT ZWISCHEN KURZ- UND LANGFRISTIGEN ZIELEN (X2)
- . _____ MÖGLICHER SCHADEN VERNACHLÄSSIGBAR KLEIN (X3)
- . _____ WAHRSCH. FÜR MÖGLICHEN SCHADEN VERNACHLÄSSIGBAR KLEIN (X4)
- . _____ PERSONAL UNTERSCHÄTZT VORHANDENES RISIKO (X5)
- . _____ FEHLVERHALTEN ZU EINFACH DURCHFÜHRBAR, KEINE HINDERNISSE (X6)
- . _____ RICHTIGES VERHALTEN UNGEWÖHNLICH, FEHLVERH. MANCHMAL RICHTIG (X7)

Abb. 21. PSF-Eingabedatei für die betrachtete Konfliktsituation oder die bekannte Referenzsituation:

Eingaben für die Referenzsituation werden zur Kalibrierung (Abschnitt 5.2.3.3) benötigt. Hierbei sind auch MDN und UF der Wahrscheinlichkeit für Fehlverhalten anzugeben.

5.2.3.3 Kalibrierung

Die Bestimmung der Modellparameter A und B in Gleichung 5 bzw. C und D in Gleichung 3 wird in der Methodenbeschreibung von SLIM Kalibrierung genannt (EMBREY u.a. 1984, Vol.II, p.12ff). Hier wird von Gleichung 5,

$$\log p = A + B \text{ FLI},$$

ausgegangen. Nach der Methodenschreibung sind zur Berechnung von A und B mindestens zwei bekannte Referenzwahrscheinlichkeiten (p_1, p_2) nötig. Zu diesen Wahrscheinlichkeiten werden die PSF-Grade ($x_i, i = 1 \dots n$) der n berücksichtigten PSFs geschätzt, und aus diesen Schätzungen werden über Gleichung 6 die Fehlerindizes FLI1 und FLI2 berechnet. Man erhält somit zu jeder Wahrscheinlichkeit einen Fehlerindex: (FLI1, p_1) und (FLI2, p_2). Diese beiden Punkte erlauben eine eindeutige Bestimmung von A und B:

$$\log p_1 = A + B \text{ FLI1} \quad (11)$$

$$\log p_2 = A + B \text{ FLI2} \quad (12)$$

$$\rightarrow B = [\log(p_1/p_2)]/(\text{FLI1} - \text{FLI2}) \quad (13)$$

$$\rightarrow A = \log p_1 - B \text{ FLI1} \quad (14)$$

In dem hier verwendeten Modell sind die Maximalfaktoren ($K_i, i = 1 \dots 7$) der 7 berücksichtigten PSFs bekannt (Tab. 41 auf Seite 134). B läßt sich also direkt über Gleichung 7 (Abschnitt 5.2.3.1) berechnen (hier über den dekadischen Logarithmus "lg" zur Basis 10):

$$B = \sum_{i=1}^7 (\lg K_i) = \lg\left(\prod_{i=1}^7 K_i\right) = \lg(2 \cdot 2.5 \cdot 12.5 \cdot 2 \cdot 4 \cdot 9 \cdot 6) = 4.43$$

Zur Berechnung von A wird demnach nur noch eine Referenzwahrscheinlichkeit benötigt. Hier wird der Median der auf industriellen Erfahrungen beruhenden Wahrscheinlichkeit $0.01 < 5 >$ (SWAIN 1983, p.19-11) für das gelegentliche Ignorieren von Vorschriften verwendet. Zu diesem Referenzdatum wurden folgende PSF-Grade geschätzt (Tab. 43).

P S F	GRAD DES ZUTREFFENS
(x1) besonderer Anreiz zu Fehlverhalten	nicht →x1=0
(x2) Zielkonflikt	total →x2=1
(x3) Schadenshöhe gering	stark →x3=0.75
(x4) Schadenswahrsch. gering	keine Ahnung →x4=0.5
(x5) Risikounterschätzung	schwach →x5=0.25
(x6) Fehlverhalten zu einfach	stark →x6=0.75
(x7) richtiges Verhalten ungewöhnlich	schwach →x7=0.25

Tab. 43. Geschätzte PSF-Grade für das gelegentliche Ignorieren von Vorschriften im industriellen Alltag (Kalibrierung für MDN=0.01):

Nähere PSF-Beschreibungen in Tab. 41 auf Seite 134

Aus diesen Schätzungen erhält man folgenden Fehlerindex (Wichtungsfaktoren aus Tab. 42 auf Seite 137):

$$\text{FLI} = .068 \cdot 0 + .089 \cdot 1 + .248 \cdot .75 + .068 \cdot .5 + .136 \cdot .25 + .215 \cdot .75 + .176 \cdot .25 \\ \simeq 0.548$$

Für den Parameter A gilt (Gleichung 14):

$$A = \lg p - B \text{ FLI} = \lg 0.01 - 4.43 \cdot 0.548 \simeq -4.43$$

Für die kleinste Basiswahrscheinlichkeit in Gleichung 1 gilt:

$$p_o = 10^A \simeq 3.7\text{E-}5 \text{ (ein rein theoretischer Wert)}$$

Das FLI-Modell lautet demnach:

$$\lg p = -4.43 + 4.43 \text{ FLI} \quad (15)$$

mit

$$\text{FLI} = 0.068 x_1 + 0.089 x_2 + 0.248 x_3 + 0.068 x_4 + 0.136 x_5 + 0.215 x_6 + 0.176 x_7$$

x1 = besonderer Anreiz zu Fehlverhalten,

x2 = Zielkonflikt,

x3 = Schadenshöhe gering,

x4 = Schadenswahrsch. gering,

x5 = Risikounterschätzung,

x6 = Fehlverhalten zu einfach,

x7 = richtiges Verhalten ungewöhnlich.

Es ist Zufall, daß hier die Parameter A und B den gleichen Betrag haben. Die Gleichheit der Beträge bedeutet, daß für den ungünstigsten Wert, FLI = 1, des Fehlerindizes die Fehlerwahrscheinlichkeit p genau 1 ist. Ist $|A| > B$, dann ist p auch für FLI = 1 kleiner als 1. Ist $|A| < B$, dann erreicht p bereits 1, obwohl FLI noch unterhalb 1 liegt.

Zu diesem Modell wurde ein Konsistenztest durchgeführt. In SWAIN (1980, p.19-11) wird eine zweite, auf empirischen Daten beruhende Wahrscheinlichkeit genannt:

$p = 0.5 < 5 >$ für das nicht richtige Benutzen einer Checkliste.

Beispiel: Die Liste wird nicht während der Arbeit ausgefüllt, sondern hinterher. Vorteil: Keine Unterbrechung des Arbeitsflusses durch lästige Schreibarbeit. Nachteil: Die Liste verliert ihre eigentliche Kontrollfunktion.

Zu dieser Wahrscheinlichkeit wurden folgende PSF-Skalenwerte geschätzt (Tab. 44):

P S F	GRAD DES ZUTREFFENS
(x1) besonderer Anreiz zu Fehlverhalten	mittel $\rightarrow x1 = 0.50$
(x2) Zielkonflikt	total $\rightarrow x2 = 1$
(x3) Schadenshöhe gering	total $\rightarrow x3 = 1.0$
(x4) Schadenswahrsch. gering	total $\rightarrow x4 = 1.0$
(x5) Risikounterschätzung	total $\rightarrow x5 = 1.0$
(x6) Fehlverhalten zu einfach	total $\rightarrow x6 = 1.0$
(x7) richtiges Verhalten ungewöhnlich	stark $\rightarrow x7 = 0.75$

Tab. 44. Geschätzte PSF-Grade für das nicht richtige Benutzen einer Checkliste (Kalibrierung für MDN=0.5):

Nähere PSF-Beschreibungen in Tab. 41 auf Seite 134

Durch Einsetzen dieser Werte in das FLI-Modell (Gleichung 15) erhält man
FLI = 0.937 und

eine Wahrscheinlichkeit von 0.53.

Eine erstaunlich gute Übereinstimmung mit dem Originalwert: MDN = 0.5.

Meine subjektiven Schätzungen sind also zu den beiden in SWAIN (1983) genannten empirischen Wahrscheinlichkeiten (0.01 und 0.5) regelwidrigen Verhaltens konsistent. Ein weitergehender Konstistenztest, der die subjektiven Schätzungen mehrerer

PRA-Durchführer umfaßt, wurde hier nicht durchgeführt. Deshalb ist es notwendig, daß sich ein PRA-Team vor der Anwendung des Modells über die Schätzungen zur Kalibrierung einigt. Da zu dem Modell ein benutzerfreundliches Rechenprogramm existiert, sind Änderungen der hier voreingestellten Kalibrierungsannahmen (Tab. 43 auf Seite 139) einfach durchführbar. Es ist auch möglich, eine andere Referenzwahrscheinlichkeit zu verwenden (vgl. Abb. 21).

Falls mehr als zwei Referenzwahrscheinlichkeiten regelwidrigen Verhaltens bekannt sind, dann empfiehlt es sich, die Modellparameter A und B per Regression von FLI auf $\log p$ zu berechnen. Dadurch kann sich der aus den PSF-Maximalwerten (K_i , $i = 1 \dots n$) bestimmte Wert für B ändern:

$$B = \sum_{i=1}^n (\log K_i)$$

- (1) Ist der per Regression bestimmte Wert B' kleiner als B, dann ist der gemeinsamer Effekt aller Maximalfaktoren kleiner als deren Produkt $\prod K_i$ (für $i = 1 \dots n$).
- (2) Ist $B' > B$, dann ist der gemeinsame Effekt aller Maximalfaktoren größer als deren Produkt.

Der erste Fall deutet daraufhin, daß im Modell insgesamt negative Abhängigkeiten zwischen den PSFs überwiegen, der zweite Fall deutet auf ein Übergewicht positiver Abhängigkeiten hin. Auf das Vorliegen solcher Abhängigkeiten wird im Abschnitt 5.2.3.5 näher eingegangen.

5.2.3.4 Unsicherheiten

Alle Punktwerte von Faktoren und Wahrscheinlichkeiten werden als Mediane interpretiert. Es wird sowohl die Unsicherheit jedes einzelnen Faktors, $F_i = K^{x_i}$, als auch die Unsicherheit der Basiswahrscheinlichkeit p_0 berücksichtigt. Die Unsicherheit des Faktors F_i wird über x quantifiziert. Aufgrund des Abstands 0.25 zur benachbarten Kategorie wird subjektiv ein 90%-Unsicherheitsintervall von $x_i \pm 0.25$ angenommen. Wenn die Schätzung KEINE AHNUNG lautet, dann wird 0.5 ± 0.5 verwendet. Für den Unsicherheitsfaktor U_{F_i} von F_i gilt also:

$$U_{F_i} = K_i^{0.50}, \text{ für } x_i = \text{KEINE AHNUNG}, \quad (16)$$

$$U_{F_i} = K_i^{0.25}, \text{ sonst.}$$

mit

K_i = Maximalfaktor (Tab. 41).

Beispiel. Aus den Schätzungen in Tab. 43 auf Seite 139 und aus dem Median ($MDN' = 0.01$) der Referenzwahrscheinlichkeit ($0.01 < 5 >$) wurde der Median der Basiswahrscheinlichkeit wie folgt berechnet:

$$MDN_o = (.01) / (2^0 2.5^1 12.5^{.75} 2^5 4^{.25} 9^{.75} 6^{.25}) = 3.7E-5$$

Die Referenzwahrscheinlichkeit ($MDN' = 0.01$, $UF' = 5$) wird (so wie in SWAIN 1983) als lognormalverteilt angenommen. Alle Faktoren (F_i , $i = 1 \dots 7$) werden hier ebenfalls als lognormalverteilte Größen angenommen, deren Unsicherheitsfaktoren (UF_i , $i = 1 \dots 7$) sich über Gleichung 16 berechnen lassen. Demnach gilt für den Unsicherheitsfaktor von p_o :

$$UF_o = \exp\{ [(\ln UF')^2 + (\ln UF_F)^2]^{0.5} \} \simeq 7$$

mit

$$UF_F = \sum_{i=1}^7 (\ln UF_i)^2$$

UF_i = Unsicherheitsfaktor von PSF i (Gleichung 16),

$UF' = 5$ = Unsicherheitsfaktor der Referenzwahrscheinlichkeit.

Die Konstante des FLI-Modells (Gleichung 15),

$$A = \lg p_o = -4.43,$$

hat demnach folgende Unsicherheit:

$$\Delta A = \pm \lg 7 \simeq \pm 0.85.$$

Aufgrund der hier vorgenommenen Kalibrierung hat also die logarithmierte Fehlverhaltenswahrscheinlichkeit ($\lg p$) eine Unsicherheit von mindestens ± 0.85 . Diese Unsicherheit erhöht sich noch durch die Schätzungen zu den PSF-Graden (x_i , $i = 1 \dots 7$)

der aktuellen Konfliktsituation, für die p bestimmt werden soll. Auch die Unsicherheiten aufgrund der dieser Schätzungen werden in dem Modell berücksichtigt.

Auf weitere Unsicherheiten, die über die Schätzunsicherheiten hinausgehen, wird im nächsten Abschnitt näher eingegangen.

5.2.3.5 Kritik

Die hier vorgeschlagene Methode ist in vielen Punkten kritisierbar:

1. Wie wirken sich evtl. vorhandene Abhängigkeiten zwischen den PSFs aus?
2. Welche Unsicherheiten entstehen aufgrund der willkürlich festgelegten geometrischen Skalierung?
3. Ist die Liste der berücksichtigten PSFs vollständig?
4. Ist die kombinierte Verwendung auf unterschiedlichen Quellen basierenden PSFs zulässig?
5. Sind die vorgenommenen Extrapolationen zulässig?
6. Inwiefern sind die PSFs auf die Referenzwahrscheinlichkeit anwendbar?
7. Wie zuverlässig und konsistent sind die Schätzungen zu den PSFs?

Hier wird auf den ersten drei Kritikpunkte näher eingegangen.

Die Frage der kombinierten Verwendung (Punkt 4) betrifft in erster Linie das Problem der Abhängigkeiten (Punkt 1). Weitere Erörterungen werden hier nicht durchgeführt, weil sie den grundsätzlichen Modellansatz SLIM betreffen.

Die Unsicherheiten (Punkte 5 und 6) aufgrund der hier vorgenommen Extrapolationen, ausgehend von der hier ausgewählten Referenzwahrscheinlichkeit, können erst quantifiziert werden, wenn man das Modell anhand weiterer bekannter Referenzwahrscheinlichkeiten überprüft. Hierzu wurde im Abschnitt 5.2.3.3 (Tab. 44 auf Seite 140) ein Konsistenztest durchgeführt, der aufgrund meiner subjektiven Schätzungen zu einer weiteren Referenzwahrscheinlichkeit die Gültigkeit der Modellparameter bestätigte. Die an einer Referenzwahrscheinlichkeit festgestellte Gültigkeit darf jedoch nicht verallgemeinert werden.

Außerdem ist nicht geklärt, ob auch die subjektiven Schätzungen anderer Modellanwender die Gültigkeit bestätigen werden. Dieser Punkt betrifft die Zuverlässigkeit der Schätzungen zu den PSFs: Wie unterscheiden sich die Schätzung verschiedener PRA-Durchführer zu der gleichen Konfliktsituation? Wie unterscheiden sich die Schätzungen eines PRA-Durchführers zu verschiedenen Zeitpunkten? Die Kritik, daß hierzu keine Untersuchungen durchgeführt wurden ist berechtigt. Es daher zu empfehlen, daß - falls aus Zeitgründen keine aufwendigen Expertenbefragungen durchgeführt werden können - sich ein PRA-Team, das das Modell anwendet, die Schätzungen zu den PSFs diskutiert und mit evtl. zuvor durchgeführten Schätzungen vergleicht.

Abhängigkeiten

Die Vernachlässigung von Abhängigkeiten kann zur Unter- oder Überschätzung der Zuverlässigkeit führen - je nachdem, ob positive oder negative Abhängigkeit vorliegt.

Positive Abhängigkeit

Eine Unterschätzung würde sich z.B. aufgrund einer Abhängigkeit zwischen x1 BESONDERER ANREIZ ZU FEHLVERHALTEN und x3 MÖGLICHER SCHADEN KLEIN ergeben: Ein Operateur, der im Fehlverhalten einen besonderen Anreiz sieht, wird auch die mögliche Schadenshöhe unterbewerten. Eine solche Abhängigkeit ließe sich z.B. durch folgendes Modell integrieren:

$$x3(x1) = x3 + (1 - x3) \beta x1 \quad (17)$$

mit

$$0 \leq \beta \leq 1,$$

β = Kopplungsgrad zwischen x1 und x3,

x3 = unabhängiger Grad von PSF 3,

x3(x1) = von x1 abhängiger Grad des PSF 3.

Beispiel. Durch Fehlverhalten wird ein schwerer Schaden erst ermöglicht; zu x3 MÖGLICHER SCHADEN KLEIN kann also die Schätzung NICHT, d.h. $x3=0$, abgegeben werden. Andererseits kann durch Fehlverhalten ein hoher wirtschaftlicher Verlust vermieden werden; x1 BESONDERER ANREIZ ZU FEHLVERHALTEN kann also auf TOTAL, d.h. $x1=1$, gesetzt werden.

Bei unabhängiger Modellierung ergibt sich folgender zusammengefaßter Modifizierungsfaktor dieser beiden PSFs:

$$F(x_1, x_3) = (K_1)^{x_1} (K_3)^{x_3} = 2^1 12.5^0 = 2.$$

mit

$K_1 = 2$ = Maximalfaktor von PSF 1,

$K_3 = 12.5$ = Maximalfaktor von PSF 3 (Tab. 41).

Angenommen zwischen den beiden PSFs besteht eine positive Abhängigkeit mit dem Kopplungsgrad $\beta = 0.25$. Für den von x_1 abhängigen Grad des PSFs MÖGLICHER SCHADEN KLEIN erhält man dann:

$$x_3(x_1) = 0 + (1 - 0) 0.25 \cdot 1 = 0.25.$$

Man erhält einen zusammengefaßten Effekt, der ca. um den Faktor 2 höher ist als bei unabhängiger Modellierung:

$$F[x_1, x_3(x_1)] = (K_1)^{x_1} (K_3)^{x_3(x_1)} = 2^1 12.5^{0.25} = 3.8.$$

Negative Abhängigkeit

Eine Überschätzung würde sich z.B. aus folgender Abhängigkeit zwischen x_1 BESONDERER ANREIZ ZU FEHLVERHALTEN und x_7 RICHTIGES VERHALTEN UNGEWÖHNLICH ergeben: Der Operateur sieht einen besonderen Anreiz zu Fehlverhalten (x_1), weil richtiges Verhalten dem gewohnheitsmäßigem Empfinden widerspricht (x_7). D.h., x_1 ist in x_7 schon enthalten und muß nicht separat berücksichtigt werden.

Quantifizierungsvorschlag:

$$x_1(x_7) = x_1 - x_1 \beta x_7 \tag{18}$$

Hier gibt β an, inwieweit x_1 schon in x_7 enthalten ist.

Beispiel. Für den PSF ANREIZ ZU FEHLVERHALTEN wird die Schätzung STARK (d.h. $x_1 = 0.75$) abgegeben, für den PSF RICHTIGES VERHALTEN UNGEWÖHNLICH die Schätzung TOTAL ($x_7 = 1$). Bei unabhängiger Modellierung erhält man einen gemeinsamen Faktor von

$$F(x_1, x_7) = (K_1)^{x_1} (K_7)^{x_7} = 2^{0.75} 6^1 = 10.1.$$

Es wird nun angenommen, daß zwischen den PSFs x_1 und x_7 eine negative Abhängigkeit mit dem Kopplungsgrad $\beta=0.5$ besteht. Man erhält somit für x_1 in Abhängigkeit von x_7 :

$$x_1(x_7) = 0.75 - 0.75 \cdot 0.5 \cdot 1 = 0.375.$$

Der gemeinsame Modifizierungsfaktor ist bei abhängiger Modellierung ca. um den Faktor 1.3 geringer als bei unabhängiger Modellierung:

$$F[x_1(x_7), x_7] = (K_1)^{x_1(x_7)} (K_7)^{x_7} = 2^{0.375} 6^1 = 7.8$$

Das häufige Auftreten negativer Abhängigkeiten mit hohen Kopplungsgraden würde daraufhin deuten, daß das PSF-Modell "überbelegt" ist, d.h., es gibt PSFs, die praktisch das gleiche aussagen. Dieser Punkt ist zu beachten, wenn man das Modell um einen neuen PSF erweitern möchte.

Skalierung

Die hier getroffene Entscheidung für eine geometrische Skalierung,

$$F = K^x, 0 \leq x \leq 1,$$

des Modifizierungsfaktors F eines PSFs mit dem Maximalfaktor K ist willkürlich. Diese Skalierung wurde deshalb gewählt, damit eine Kohärenz zu der Methode SLIM (s. Abschnitt 5.2.3.1) vorhanden ist.

In WILLIAMS (1988) wird z.B. eine arithmetische Skalierung vorgeschlagen:

$$F = 1 + (K - 1) x$$

Tab. 45 ist zu entnehmen, daß die Unterschiede zwischen den beiden Verfahren umso größer sind, je höher der Maximalfaktor K ist: Für hohe K -Werte liefert die arithmetische Skalierung ca. um den Faktor 2 höhere Modifizierungsfaktoren.

Maximalfaktor → PSF-Grad ↓	K = 2	K = 2	K = 10	K = 10
x	K^x	$1 + (K - 1) x$	K^x	$1 + (K - 1) x$
0	1	1	1	1
0.25	1.19	1.25	1.78	3.25
0.50	1.41	1.50	3.16	5.50
0.75	1.68	1.75	5.62	7.75
1.0	2	2	10	10

Tab. 45. Vergleich zwischen geometrischer und arithmetischer PSF-Skalierung:

Bei geometrischer Skalierung ist der Quotient zwischen zwei Faktoren konstant, bei arithmetischer die Differenz.

Vollständigkeit, Erweiterbarkeit

Das Problem der Vollständigkeit betrifft die Frage, ob alle PSFs, die einen wesentlichen Einfluß auf das Auftreten von Fehlverhalten haben, berücksichtigt sind. Zu diesem Problem wird hier ein konstruktiver Vorschlag gemacht. Es wird ein aus der "Multiattribute Utility Theory" (MAUT) (vgl. z.B. VON WINTERFELDT & EDWARDS 1986) ableitbares Verfahren vorgestellt, mit dem das PSF-Modell,

$$FLI = w_1 x_1 + w_2 x_2 + w_3 x_3 + w_4 x_4 + w_5 x_5 + w_6 x_6 + w_7 x_7,$$

um einen neuen PSF x^* , dessen Gewicht w^* unbekannt ist, erweitert werden kann. Dieses Verfahren ist in Tab. 46 skizziert.

1. Schätzen, an welchem Rang der Reihenfolge der unbekannte Maximalfaktor K^* des neuen PSF liegt:

$$\begin{array}{c} K^* \\ \downarrow \\ ? \\ K_1 \leq K_2 \leq \dots \leq K_n \end{array}$$

2. Indifferenzschätzung und Berechnung von K^*

- a. $K^* < K_j \leq K_n$, $1 \leq j \leq n$
(K^* ist kleiner als der größte Maximalfaktor K_n ; K_j ist der kleinste Maximalfaktor, der oberhalb K^* liegt):

- x_j so schätzen, daß gilt:

$$[(x^*=0) \rightarrow (x^*=1)] \sim [(x_j=0) \rightarrow (x_j=?)]$$

- Aus x_j folgt:

$$w^*/w_j = x_j$$

Aus

$$w_i = (\log K_j) / [\sum (\log K_i) + \log K^*] \text{ und } w^* = (\log K^*) / [\sum (\log K_i) + \log K^*], i=1\dots n, \text{ folgt:}$$

$$w^*/w_j = (\log K^*) / (\log K_j) = x_j$$

$$\rightarrow \log K^* = x_j \log K_j$$

- b. $K^* > K_n$:

- x^* so schätzen, daß gilt:

$$[(x_n=0) \rightarrow (x_n=1)] \sim [(x^*=0) \rightarrow (x^*=?)]$$

- Aus x^* folgt:

$$w_n/w^* = x^*$$

Aus

$$w_n = (\log K_n) / [\sum (\log K_i) + \log K^*] \text{ und } w^* = (\log K^*) / [\sum (\log K_i) + \log K^*], i=1\dots n, \text{ folgt:}$$

$$w_n/w^* = (\log K_n) / (\log K^*) = x^*$$

$$\rightarrow \log K^* = (\log K_n) / x^*$$

3. Gewichte für das FLI-Modell, $\log p = A + B \text{ FLI}$, berechnen (für $i=1\dots n$):

$$w^* = (\log K^*) / [\sum (\log K_i) + \log K^*]$$

$$w_i = (\log K_i) / [\sum (\log K_i) + \log K^*]$$

Tab. 46. Erweiterung eines PSF-Modells mit den Maximalfaktoren $K_1\dots K_n$ um einen neuen PSF mit dem unbekannten Maximalfaktor K^* :

$$0 \leq w_i, w^* \leq 1; 0 \leq x_i, x^* \leq 1; K_i, K^* > 1$$

Das in der Tabelle beschriebene Verfahren wird hier kurz an einem Beispiel erläutert. Folgender, zu den PSFs in Tab. 41 auf Seite 134 neu hinzukommender PSF wird betrachtet:

(x*) KEINE KRITIK BEI FEHLVERHALTEN MIT SCHADLOSEM AUSGANG.

Das Nichtvorhandensein ($x^* = 0$) des PSFs bedeutet, daß die Vorgesetzten regelwidriges Verhalten immer kritisieren, auch dann wenn keine ernsthaften Folgen aufgetreten sind. Zur Einbeziehung von x^* ist die Schätzung des Maximalfaktors erforderlich. Hierzu werden die Maximalfaktoren (K_i , $i=1\dots n$) der bislang berücksichtigten PSFs der Größe nach geordnet, und es wird geschätzt, welchen Platz der Maximalfaktor K^* des neuen PSF in dieser Reihenfolge einnimmt.

Schätzergebnis: K^* liegt unterhalb des Maximalfaktors, $K_5=4$, des PSFs x_5 RISIKOÜBERSCHÄTZUNG; K_5 ist der kleinste Faktor, der oberhalb K^* liegt.

Nun ist folgendes, nicht triviales Schätzproblem zu lösen:

Die Erhöhung des PSF-Grades x^* KEINE KRITIK von
 $x^* = 0$ (NICHT VORHANDEN) auf $x^* = 1$ (TOTAL VORHANDEN)

hat bewirkt eine multiplikative Erhöhung der Wahrscheinlichkeit für Fehlverhalten.

Frage: Auf welchen Wert, ausgehend von $x_5 = 0$ (NICHT VORHANDEN), muß sich der PSF-Grad x_5 RISIKOÜBERSCHÄTZUNG erhöhen, damit man die gleiche multiplikative Erhöhung der Wahrscheinlichkeit für Fehlverhalten erhält?

Antwort: Von $x_5 = 0$ auf $x_5 = 0.75$.

$$\rightarrow w^*/w_5 = (\ln K^*)/(\ln K_5) = 0.75$$

$$\rightarrow K^* = \exp(0.75 \ln 4) \simeq 2.8$$

Der neue PSF KEINE KRITIK hätte demnach den Maximalfaktor 2.8.

Durch die Einbeziehung eines neuen PSFs ergibt sich eine Tendenz zur Erhöhung der Wahrscheinlichkeit für Fehlverhalten, wenn dieser PSF mit einem kleinen Grad in der für Kalibrierung verwendeten Referenzwahrscheinlichkeit enthalten ist.

Das o.g. Schätzbeispiel hat gezeigt, daß die Erweiterung des Modells ohne bekannte PSF-Daten sehr hohe Anforderungen an das Beurteilungsvermögen eines PRA-Teams stellt.

Fazit

Ein mit dem hier vorgeschlagenen Modell berechneter Punktwert (MDN) ist mit hohen Unsicherheiten verbunden. Er sollte deshalb nur in Verbindung mit dem ebenfalls berechneten Unsicherheitsfaktor (UF) angegeben werden. Dieser UF beträgt - aufgrund der Unsicherheiten, die mit der Berechnung der Basiswahrscheinlichkeit verbunden waren (Abschnitt 5.2.3.3) - mindestens 7. Angenommen, mit dem Modell wird ein Punktwert von 0.1 berechnet. Das Mindestausmaß des 90%-Unsicherheitsintervalls beträgt dann $<0.014, 0.7>$ - ein Bereich, der nach dem alltäglichen Empfinden sowohl seltene als auch häufige Ereignisse umfaßt.

In dem UF 7 ist auch der UF 5 der zur Kalibrierung verwendeten Referenzwahrscheinlichkeit 0.01 (MDN) (SWAIN 1983) für das gelegentliche Ignorieren von Vorschriften enthalten. Dieser UF basiert nicht auf fehlerspezifischen empirischen Daten, sondern - wie alle Unsicherheitsfaktoren in SWAIN (1983) - auf subjektiven Schätzungen. Diese Schätzungen beruhen auf konservativen Schlußfolgerungen aus Untersuchungen (z.B. WECHSLER 1952) zur Variabilität menschlicher Leistungen (SWAIN 1983, ch.7). In SWAIN (1983, p.7-9f) wird die Expertenmeinung geäußert, daß die aus diesen Untersuchungen abgeleiteten Unsicherheitsfaktoren so hoch sind, daß folgende Variabilitätsursachen erfaßt werden (Tab. 47):

- | |
|---|
| <ol style="list-style-type: none">1. Der Mangel an brauchbaren Daten, die in einer menschlichen Zuverlässigkeitsanalyse für KKW-spezifische Aufgaben benötigt werden.2. Die Ungenauigkeit von Modellen, die vorgeben, menschliches Verhalten in verschiedenen Situationen und unter verschiedenen Bedingungen zu beschreiben.3. Die unzureichende Identifizierung aller, die Durchführung einer Aufgabe beeinflussenden Faktoren, ihrer Zusammenhänge und ihrer Auswirkungen.4. Begrenzte Erfahrung und mangelndes Wissen des Durchführers einer menschlichen Zuverlässigkeitsanalyse.5. Die Variabilität in der Aufgabendurchführung, von Individuum zu Individuum, von Tag zu Tag ... |
|---|

Tab. 47. Variabilitätsursachen, die durch die Unsicherheitsfaktoren des Swain-Handbuchs erfaßt werden sollen: Übersetzt aus SWAIN (1983, p. 7-9f)

Die Frage, inwieweit die tatsächlich vorhandenen Unsicherheiten des hier verwendeten Modells, durch die berechneten Unsicherheiten abgedeckt sind, kann hier wegen fehlender empirischer Daten nur qualitativ diskutiert werden. Eine Argumentation mit den Punkten 2 bis 4 in Tab. 47 wäre zu einfach.

Die Unsicherheiten aufgrund der Schätzungen (Abschnitt 5.2.3.2) zu den PSF-Skalenwerten NICHT, LEICHT, MITTEL, STARK und TOTAL liegen im PRA-üblichen Rahmen. Auch die Vorgehensweise gemäß SWAIN (1983) verlangt vom PRA-Team Schätzungen zu Variablen mit relativ unscharf definierten Ausprägungen, z.B.

- Stressniveau: ZU GERING, OPTIMAL, MITTELHOCH oder EXTREM HOCH (ch. 17) oder
- Kopplungsgrad: NICHT, LEICHT, MITTEL, HOCH oder TOTAL (ch. 10).

Die Unsicherheit aufgrund der Auswahl der PSFs sowie der Annahme, daß ihre Maximalfaktoren auf die hier verwendete Referenzwahrscheinlichkeit 0.01 (MDN) anwendbar sind, könnte meines Erachtens über die PRA-üblichen Unsicherheiten hinausgehen. Diese Unsicherheit betrifft die Frage der Validität (Gültigkeit) der Parameter (A,B,w1,...,w7) des FLI-Modells (Gleichung 5). Wegen fehlender Wahrscheinlichkeitsdaten konnte hier kein Validitätstest durchgeführt werden.

Das hier vorgeschlagene Modell erhebt deshalb nicht den Anspruch einer genauen Wahrscheinlichkeitsvorhersage für Fehlverhalten (bewußte Risikoannahme) in Situationen mit Zielkonflikt. Mit dem Modell kann jedoch ein Wert berechnet werden, der nach der subjektiven Meinung des Modellanwenders in einer angemessenen Relation zu der auf empirischen Daten beruhenden Wahrscheinlichkeit 0.01 (MDN) für das gelegentliche Ignorieren von Vorschriften steht. Das Modell stellt somit eine Alternative zur generellen Verwendung von 0.01 dar. Situationsspezifische Gegebenheiten (PSFs) werden zumindest tendenziell berücksichtigt.

5.3 Durch Ähnlichkeiten verursachte Erwartungsfehler

5.3.1 Problembeschreibung

Ähnlichkeiten werden hier immer dann unterstellt, wenn sich unterschiedliche Situationen nur in einem kritischen Detail unterscheiden (s. Abschnitt 4.3.2). Ein Teilsignal kann eine Erwartung auslösen, die zu einer falschen Entscheidung führt, weil das übrige Informationsangebot gar nicht mehr oder nur noch flüchtig genutzt wird (vgl. HACKER 1980, S.347ff). Die hier betrachteten Erwartungsfehler beziehen sich auf im Störfall anzuwendende Diagnoseregeln der Form
WENN Situation A, DANN Reaktion B.
Ein auftretender Erwartungsfehler kann dazu führen,

- daß - obwohl die Situation A vorhanden ist - die Reaktion B nicht ausgeführt wird, weil ein Reiz auftritt, der dem Nichtvorhandensein der Situation A ähnlich ist, oder
- daß - obwohl die Situation A nicht vorhanden ist - die Reaktion B ausgeführt wird, weil ein Reiz auftritt, der dem Vorhandensein der Situation A ähnelt.

Solche Fehler können zu ungeplanten Handlungen führen.

Beispiel HTR-500, NWA-Ausfall wegen Gebläseschaden. Das Nichtwahrnehmen der Situation BEIDE WÄRMETAUSCHER BESPEIST (vgl. Schritt 9 in Tab. 15 auf Seite 55) kann dazu führen, daß die Anwendbarkeit der Gegenmaßnahme NATURKONVEKTION nicht erkannt wird. Die ungeplante Handlung würde dann in dem Nichtnutzen einer verfügbaren Maßnahme zur Wiederherstellung der NWA bestehen. Da jeder Strang der Wärmetauscherbespeisung auf 2x100% ausgelegt ist, ist die Anwendbarkeit der NATURKONVEKTION auch dann noch gegeben, wenn eine Pumpe in der Wärmesenke ausfällt. Ein solcher Ausfall könnte allerdings ein Diagnoseproblem verursachen. Denn die Situation EINE PUMPE AUSGEFALLEN ist der Situation EIN WÄRMETAUSCHER NICHT BESPEIST ähnlich. Der von dem Pumpenausfall ausgehenden Reiz könnte dazu führen, daß die Operateure sich auf die Diagnose NATURKONVEKTION NICHT ANWENDBAR festlegen und das weitere Informationsangebot (bezüglich der Anwendbarkeit) garnicht mehr oder nur flüchtig nutzen.

Beispiel TMI-2 (s. Tab. 32 auf Seite 108). Hier war die Ähnlichkeit der tatsächlich vorhandenen Situation zu der Situation, die ein Ausschalten der Hochdruckeinspeisepumpen erfordert, besonders stark: Die falsche Stellungsanzeige des Ablaseventils am Druckhalter könnte die Erwartung KEIN KÜHLMITTELVERLUST ausgelöst haben, der aufgrund einer Blasenbildung steigenden Füllstand im Druckhalter die Erwartung AUSREICHEND WASSER IM PRIMÄRKREIS.

Im Prinzip sind Wahrnehmungsfehler zum WENN-Teil von Diagnoseregeln anhand von Tab. 48 quantifizierbar. Problematisch ist die Verwendung von Wahrscheinlichkeiten in Situationen, die aufgrund von Ähnlichkeitsbetrachtungen (Abschnitt 4.3.2) als Diagnoseprobleme identifiziert wurden. Dieses Problem wird hier diskutiert, und es wird ein als erste Näherung zu betrachtendes Quantifizierungsverfahren vorgeschlagen.

QUANTITATIVE INFORMATIONEN WAHRNEHMEN	
1) Druckaufzeichner mit vielen Parametern	0.05 < 5 >
2) Graphische Darstellung	0.01 < 3 >
3) Blattschreiber	0.006 < 3 >
4) Analoganzeige	0.003 < 3 >
5) Digitalanzeige (< 5 Stellen)	0.001 < 3 >
QUALITATIVE INFORMATIONEN WAHRNEHMEN	
6) Blattschreiber ohne Grenzwertlinien	0.006 < 3 >
7) Blattschreiber mit Grenzwertlinien	0.002 < 3 >
8) Analoganzeige ohne Grenzwertlinien	0.003 < 3 >
9) Analoganzeige mit Grenzwertlinien	0.001 < 3 >
10) Anzeigelampe richtig interpretieren	≈0
11) Anzeigelampe richtig interpretieren unter Stress	0.001 < 3 >

Tab. 48. Fehlerwahrscheinlichkeiten (MDN<UF>) für das gezielte (nicht zufällige) Beobachten von Anzeigen: Quelle: SWAIN (1983, p.20-26f)

5.3.2 Versuch einer Einordnung in ein Klassifizierungsschema

Klassifizierungsansätze menschlicher Fehler lassen sich wie folgt untergliedern (vgl. REASON 1990, p.11f):

- **WAS/WOBEI:**
Der auf das Verhalten und den Handlungszusammenhang gerichtete Ansatz ("behavioral level" und "contextual level"): Was wird falsch gemacht und wobei? Fast alle verfügbaren Wahrscheinlichkeiten zu menschlichen Fehlern werden diesem Ansatz entsprechend klassifiziert (vgl. Anhang E).
- **WIE/WARUM:**
Der auf die Fehlerentstehung gerichtete Ansatz ("conceptual level"): Wie oder warum wird etwas falsch gemacht? Mit welchem kognitiven Mechanismus oder mit welcher kognitiver Struktur ist der Fehler begründbar?

Die WAS/WOBEI-Klassifizierung zur Ermittlung von Fehlwahrscheinlichkeiten bildet den Schwerpunkt bei der praktischen Durchführung einer PRA. Dies wird von psychologischer Seite kritisiert (z.B. zusammenfassend in APOSTOLAKIS u.a. 1988). In

der Psychologie wird der Schwerpunkt auf die WIE/WARUM-Klassifizierung gelegt (z.B. REASON 1990). Lt. EMBREY&REASON (1986, p.300) riskiert man bei dem Verzicht auf eine WIE/WARUM-Klassifizierung die Verwendung falscher Fehlerwahrscheinlichkeiten ("mixing apples with pears").

Der hier betrachtete Erwartungsfehler (aufgrund von Ähnlichkeiten bei der Anwendung von WENN-DANN-Regeln) kann der Kategorie "Diagnosefehler" oder "Wahrnehmungsfehler" zugeordnet werden. Diese Kategorien sind sehr weit gefaßt. Hier wird unterstellt, daß sich bei dem Vorliegen von Ähnlichkeiten über erwartungsgebundenes Verhalten die Wahrnehmungsfehlerwahrscheinlichkeiten in Tab. 48 auf Seite 153 ändern. Dies ist auch der in HACKER (1980) verwendeten WIE/WARUM-Klassifizierung zu entnehmen (Tab. 49 auf Seite 157): Unter dem Oberbegriff FEHLENDE bzw. FALSCHER NUTZUNG OBJEKTIV VORHANDENER INFORMATIONEN bildet der Erwartungsfehler eine Sonderkategorie.

Eine noch mehr in Detail gehende WIE/WARUM-Klassifizierung wird von REASON (1990) vorgeschlagen (Tab. 50 auf Seite 158). Die Klassifizierung von HACKER orientiert sich an der Systematik von SURRY (Tab. 31 auf Seite 107), die von REASON an dem Modell von RASMUSSEN (Abb. 9 auf Seite 35).

Der hier betrachtete Erwartungsfehler (aufgrund von Ähnlichkeiten bei der Anwendung von WENN-DANN-Regeln) kann verschiedenen Fehlerarten in Tab. 50 zugeordnet werden. Zunächst kann er der Kategorie 1a (Unterlassung einer Überprüfung) in Tab. 50 zugeordnet werden.

Beispiel HTR-500 (s. Abschnitt 5.3.1). Nach der Wahrnehmung der Situation EINE PUMPE AUSGEFALLEN unterläßt der Operateur die Überprüfung des Durchsatzes der beiden Wärmetauscher, weil die Situation eine Ähnlichkeit zu der Situation EIN WÄRMETAUSCHER NICHT BESPEIST aufweist.

Beispiel TMI-2 (s. Abschnitt 5.3.1): Nichtbeachtung der Temperatur am Abblasestrang des Entlastungsventils am Druckhalter. Die Temperatur deutete darauf hin, daß sich das Ventil noch in Offenstellung befand. In einer früheren Veröffentlichung (EMBREY&REASON 1986) ordnete REASON den Fehler eindeutig der Kategorie SKILL-BASED SLIP zu. In REASON (1990, p.55) wird die Kategorie RULE-BASED MISTAKE ebenfalls als zutreffend eingestuft.

Auf den hier betrachteten Erwartungsfehler trifft auch die Kategorie 2a1 in Tab. 50 zu: Regelbasierte Fehlentscheidung wegen falscher Anwendung einer richtigen Regel, weil erstmalig eine Situation auftritt, in der die Regel nicht gilt.

Beispiel HTR-500. Die Regel

WENN EINE PUMPE AUSGEFALLEN, DANN EIN WÄRMETAUSCHER NICHT BESPEIST
gilt im Normalbetrieb, weil dann nur eine Pumpe pro Wärmetauscher in Betrieb ist.
In der Ausnahmesituation NWA-ANFORDERUNG IM STÖRFALL gilt diese Regel nicht.

Beispiel TMI-2. Die Regel

WENN FÜLLSTANDSANZEIGE IM DRUCKHALTER AUF HOHEM NIVEAU, DANN AUS-
REICHEND WASSER IM PRIMÄRKREIS
gilt nicht in der Ausnahmesituation, in der sich eine Dampfblase im Druckhalter ge-
bildet hat.

Eine weitere Zuordnungsmöglichkeit ergibt sich aufgrund der Fehlerart 3j4 in Tab. 50: Wissensbasierte Fehlentscheidung in komplexen Diagnoseproblemen, weil in Ursachenketten (Ereignissequenzen) und nicht in Ursachennetzen (Ereignisbäumen) gedacht wird.

Beispiel HTR-500. Es wird nicht bedacht, daß es auch Situationen mit Pumpenausfall geben kann, in denen beide Wärmetauscher ausreichend (mit 100% NWA-Kapazität) bespeist werden.

Beispiel TMI-2. Es wird nicht bedacht, daß es auch Situationen geben kann, in denen trotz hohem Druckhalterniveau zu wenig Wasser im Primärkreis ist.

Je genauer man also die kognitiven Mechanismen der Fehlerentstehung unterteilt, desto weniger eindeutig wird die Einordnung des hier betrachteten Erwartungsfehlers (aufgrund von Ähnlichkeiten bei der Anwendung von WENN/DANN-Regeln).

Zur Erinnerung: Der hier betrachtete Erwartungsfehler beschränkt sich auf die Wahrnehmung der Anwendungsbedingung (d.h. des WENN-Teils) einer solchen Regel. Tab. 48 auf Seite 153 enthält die Fehlerwahrscheinlichkeiten einiger Wahrnehmungsaufgaben. Der Informationsgehalt der Tabelle in Bezug auf die kognitiven Mechanismen bei der Fehlerentstehung ist praktisch gleich null: Man kann der Tabelle nur entnehmen, (1) was für ein Fehler gemeint ist (z.B. Nichtbemerken einer Grenzwertüberschreitung) und (2) wobei er auftritt (z.B. beim Ablesen einer

Analoganzeige mit Grenzwertlinien), nicht aber die kognitiven Mechanismen der Fehlerentstehung. Hier wird die subjektive Annahme getroffen, daß zu den Fehlern in Tab. 48 vorwiegend solche kognitiven Mechanismen (z.B. Ablenkung oder Überschreiten der aktuellen Kapazität der Informationsaufnahme) beitragen, die nach dem Klassifizierungsschema von HACKER (Tab. 49 auf Seite 157) unter die Kategorie 2a1 fallen: Übersehen aktuell angebotener handlungsrelevanter Informationen. Weiter wird angenommen, daß sich die Fehlerwahrscheinlichkeiten in Tab. 48 erhöhen, wenn der unter die Kategorie 2a4 fallende kognitive Mechanismus ERWARTUNGS-
GEBUNDENES VERHALTEN BEI ÄHNLICHKEITEN als zusätzliche Fehlerursache hinzukommt. Um ein "Gefühl" über das Ausmaß solcher Erhöhungen zu bekommen, werden im nächsten Abschnitt einige quantitative Effekte von Erwartungen diskutiert.

1. Objektives Fehlen erforderlicher Informationen
2. Nutzungsmängel objektiv vorhandener Informationen
 - a. Fehlende Nutzung
 - 1) Übersehen
 - 2) Vergessen/Versäumen
 - 3) Übergehen (als beabsichtigtes Nichtnutzen)
 - 4) Redundanzbedingte Informationsreduktion
(Stereotypisierungsfehler, Erwartungsfehler 1. Art*¹)
 - b. Falsches Nutzen vorhandener Informationen
 - 1) falsches Orientieren
 - a) Fehlidentifikation
("Sinnestäuschung", Erwartungsfehler 2. Art*²)
 - b) Erinnerungstäuschung
 - c) Fehlbeurteilung
 - 2) falsches Entwerfen von Aktionsprogrammen
 - a) Bewegungsprogramme mit räumlich und/oder zeitlich falschen Parametern
 - b) Fehlkalkül (Verrechnen, Verplanen)
 - 3) unzutreffende Bedingungseinordnung von Aktionsprogrammen
 - a) zeitliche Fehleinordnung (Zeitfehler)*³
 - b) räumliche Fehleinordnung*³
 - c) Verwechseln*³

Tab. 49. Klassifizierung von Fehlhandlungen nach HACKER (1980, S.344-348):

* Anmerkungen zu Tab. 49

1. "Erwartungsgebundes (einstellungs- und hypothesengebundenes Verhalten), welches bei unerwarteten Bedingungswechsel zum Erwartungsfehler führt. Dabei handelt es sich um einen Erwartungsfehler, der entsteht, weil das objektiv vorhandene Informationsangebot *nicht* genutzt, sondern eine Hypothese ungeprüft beibehalten wird." (S.347)
2. "Nicht jede unrichtige Wahrnehmung muß auf eine Sinnestäuschung ... zurückgehen. Fehlidentifikationen entstehen unter umgebungs- oder subjektbedingten erschwerten Wahrnehmungsbedingungen dadurch, daß die Identifikation an einem eingeschränkten Signalelement ansetzt und darüberhinaus sogar Fehlendes ergänzt, wobei objektiv ähnliche und nur durch ein kritisches Detail unterschiedene Einwirkungen nicht unterschieden werden können (sogenannte Ähnlichkeitsfehler bei WEIMER)." (S.348f)
3. "unter gegebenen Bedingungen im Sinne von Populationsstereotypen". (S.348)

Eine ausführliche Diskussion der einzelnen Fehlerarten würde über den Rahmen der hier vorliegenden Arbeit hinausgehen.

1. Skill-based performance
 - a. Inattention (omitted checks)
 - 1) Double-capture slips
 - 2) Omissions following interruptions
 - 3) Reduced intentionality
 - 4) Perceptual confusion
 - 5) Interference errors
 - b. Overattention
 - 1) Omissions
 - 2) Repetitions
 - 3) Reversals
2. Rule-based performance
 - a. Misapplication of good rules
 - 1) First exceptions
 - 2) Countersigns and nonsigns
 - 3) Informational overload
 - 4) Rule strength
 - 5) General rules
 - 6) Redundancy
 - 7) Rigidity
 - b. Application of bad rules
 - 1) Encoding deficiencies
 - 2) Action deficiencies
 - a) Wrong rules
 - b) Inelegant rules
 - c) Inadvisable rules
3. Knowledge-based performance
 - a. Selectivity
 - b. Workspace limitations
 - c. Out of sight out of mind
 - d. Confirmation bias
 - e. Overconfidence
 - f. Biased reviewing
 - g. Illusory correlations
 - h. Halo effects
 - i. Problems with causality
 - j. Problems with complexity
 - 1) Problem with delayed feedback
 - 2) Insufficient consideration of processes in time
 - 3) Difficulties with exponential developments
 - 4) Thinking in causal series not causal nets
 - 5) Thematic vagabounding
 - 6) Encysting

Tab. 50. Summarizing the Main Headings for Failure Modes at Each of the Three Performance Levels (REASON 1990, p.69):

Eine ausführliche Diskussion der einzelnen Fehlerarten würde über den Rahmen der hier vorliegenden Arbeit hinausgehen ("thematic vagabounding").

5.3.3 Beispiele für quantitative Effekte von Erwartungen

Die hier vorgestellten quantitativen Effekte (Abschnitte 5.3.3.1 bis 5.3.3.3) beziehen sich auf Erwartungen, die nicht durch Ähnlichkeiten verursacht werden. Es handelt sich um Erwartungen, die dem dem allgemeinen gewohnheitsmäßigen Empfinden entsprechen. Diese Effekte können unter dem Begriff "Stereotypisierungsfehler" der Kategorie 2a4 in Tab. 49 auf Seite 157 zugeordnet werden.

5.3.3.1 Beispiel 1: Drehschalter betätigen

Die Aufgabe BETÄTIGUNG EINES DREHSCHALTERS wird angefordert. Die Wahrscheinlichkeit (MDN) für die Verwechslung der Drehrichtung hängt lt. SWAIN (1983, p.13-6) u.a. davon ab, ob die die Funktionsweise des Schalters den allgemeinen Erwartungen (z.B. links drehen für AUF und rechts drehen für ZU) des Bedieners entspricht:

- 0.0005 Kein Widerspruch zur allgemeinen Erwartung
- 0.05 Widerspruch zur allgemeinen Erwartung

5.3.3.2 Beispiel 2: Grenzwertüberschreitung bemerken

Die Wahrscheinlichkeit (MDN) für das Nichtbemerken einer Grenzwertüberschreitung auf einem Analoganzeigegerät mit (gut erkennbarer) Grenzwertlinie ist zu schätzen. Lt. SWAIN (1983, p.11-16,11-29) hängt diese Wahrscheinlichkeit von der Erwartung des Operators ab, ob überhaupt eine Grenzwertüberschreitung vorhanden ist:

- 0.001 Eine Prozedur enthält die Anweisung, die Einhaltung des Grenzwerts zu kontrollieren. Der Operator führt diese Anweisung aus.
(Hohe Erwartung für eine etwaige Grenzwertüberschreitung.)
- 0.05 Routinemäßige Schichtübernahme. Erster Wartenrundgang.
(Geringe Erwartung für eine etwaige Grenzwertüberschreitung.)
- 0.9 Letzter Wartenrundgang nach Schichtübernahme.
(Sehr geringe Erwartung für eine etwaige Grenzwertüberschreitung.)

5.3.3.3 Beispiel 3: Schriftliche Registrierung

In einem Experiment (WEHNER&MEHL 1986) erhielten 30 Vpn (Studenten) die Anweisung für folgenden Handlungsablauf:

- (A) Aus einer Schale soll - passend zu einem vorgegebenen Legemuster - eine Kugel entnommen werden.
- (B) Die Kugel soll in einen Trichter geworfen werden, der in einen Apparat (black box) führt.
- (C) An dem Apparat ist ein Hebel nach rechts zu bewegen und
- (D) ein zweiter Hebel nach links.
- (E) Die dann aus dem Apparat rollende Kugel ist aufzufangen und
- (F) auf eine Legemuster zu plazieren.

Nach kurzer Übung wurde folgende Zusatzaufgabe eingeführt:

- (Z) Die Farbe der Kugel per Bleistift auf einen Zettel registrieren.

Als Fehler wurde das Nichtdurchführen oder das nachträgliche Durchführen der Zusatzaufgabe Z gewertet. In Abhängigkeit vom Rangplatz der Zusatzaufgabe im Handlungsablauf (s.o.) ergaben sich folgende Fehlerwahrscheinlichkeiten:

- 5.3 % Rangplatz frei wählbar.
(Alle Vpn entschieden sich dafür, die Zusatzaufgabe nach Handlung F durchzuführen.)
- 10.4 % Rangplatz zwischen Handlung B und C vorgegeben.
- 3.1 % Rangplatz zwischen Handlung C und D vorgegeben.

Die in den Beispielen 1 und 2 genannten quantitativen Effekte basieren auf Expertenschätzungen der Autoren des SWAIN-Handbuchs, der Effekt in Beispiel 3 auf empirischen Daten. Das Beispiel 3 zeigt, daß Einflüsse auf Fehlerwahrscheinlichkeiten nicht immer vorhersehbar sind. Der Unterschied (ca. Faktor 2) zwischen den Fehlerwahrscheinlichkeiten 10.4% (Registrierung zwischen B und C) und 5.3% (Registrierung am Ende) war vorhersehbar. Denn die Durchführung einer Schreibaufgabe nach Abschluß einer manuellen Tätigkeit entspricht eher den Erwartungen als die Durchführung mitten im Handlungsablauf. Diese Aussage widerspricht jedoch der geringen Fehlerwahrscheinlichkeit 3.1% für die Registrierung zwischen den Schritten C und D.

Zu diesem Ergebnis (3.1%) wird von WEHNER&MEHL (1986, S.238) folgende Interpretation genannt:

"Gerade die hohe funktionale Beziehung zwischen den beiden Hebeln einerseits und die hierzu inkompatibel wirkende Instruktion zur Bearbeitung der Erweiterungsauf-

gabe andererseits führen zum Aufbrechen der bestehenden oder zur Verhinderung einer sich bildenden Handlungsganzheit.“

Meines Erachtens ist auch folgende Erklärung plausibel: Die Anweisung REGISTRIERUNG ZWISCHEN ZWEI HEBELBETÄTIGUNGEN ist einfacher (zu behalten) als z.B. die Anweisung REGISTRIERUNG ZWISCHEN DEM EINWERFEN IN DEN TRICHTER UND DER BETÄTIGUNG DES ERSTEN HEBELS.

5.3.4 Quantifizierungsvorschlag

Wegen nicht verfügbarer Daten kann hier kein Verfahren genannt werden, daß die Berechnung der Wahrscheinlichkeit eines Erwartungsfehlers (Systemzustandsfehlidentifizierung aufgrund einer Ähnlichkeit bei der Anwendung einer WENN-DANN-Regel) erlaubt. Stattdessen werden hier drei Orientierungswerte (Tab. 51 auf Seite 163) genannt, die eine grobe Schätzung der Wahrscheinlichkeit erlauben.

Der erste Wert ist die Wahrscheinlichkeit für das Nichtbemerken einer Information, die dem Operateur optisch auf einer Anzeige signalisiert wird. Die entsprechenden Wahrscheinlichkeiten sind Tab. 48 auf Seite 153 zu entnehmen. Dabei ist zu beachten, daß in der Wahrscheinlichkeit $0.001 < 3 >$ für das nicht richtige Interpretieren eines Signals einer Anzeigelampe schon Stress enthalten ist.

Als zweiter Orientierungswert wird hier die Wahrscheinlichkeit $0.1 < 5 >$ vorgeschlagen. Dieser Wert (SWAIN 1983, p.11-11) gilt für den Fehler, daß der Operateur nicht bemerkt, daß von einer Anzeige ein falsches Signal ausgeht (z.B. weil der Zeiger "hängt"), obwohl die falsche Anzeige durch Kontrolle anderer Anzeigen zu bemerken ist. Dieser Wert 0.1 ist unter erhöhten Stressbedingungen noch zu modifizieren (Anhang F).

In SWAIN (1983, p.11-11) wird zu diesem Fehler die Ursache "perceptual tunneling" genannt: Der Operateur handelt gemäß der zuerst wahrgenommenen Fehlinformation und versäumt es einen sog. "cross-check" durchzuführen. Der kognitive Mechanismus "perceptual tunneling" kann also der Kategorie ERWARTUNGSFEHLER zugeordnet werden (vgl. Fußnote 1 zu Tab. 49 auf Seite 157): Die falsche Anzeige löst eine Erwartung in Richtung Systemzustandsfehlidentifizierung aus, die bewirken kann, daß das weitere Informationsangebot nicht mehr genutzt wird.

Die Wahrscheinlichkeit 1.0 wird hier als dritter Orientierungswert empfohlen. Dieser Wert kann verwendet werden, wenn "TMI-ähnliche" Verhältnisse vorliegen (vgl. Tab. 32 auf Seite 108): Die zur Systemzustandsidentifizierung relevante Anzeige (TMI: Stellungsanzeige der Abblaseventils) zeigt falsch an und es gibt ein weiteres Signal (TMI: Druckhalterpegelstand hoch), das dem der Falschanzeige entsprechendem Zustand sehr ähnlich ist. Dieser Wert (1.0) ist nicht überpessimistisch. Denn wenn man die o.g. Wahrscheinlichkeit $0.1 < 5 >$ für das Versäumen eines "cross-check" mit dem Stressfaktor 2 (Anhang F) modifiziert, dann erhält man eine Wahrscheinlichkeit von $0.2 < 5 >$, deren 95%-Obergrenze gleich 1.0 ist.

Die hier vorgeschlagene Methode besteht also darin, daß unter Verwendung von Tab. 51 die Wahrscheinlichkeit eines Erwartungsfehlers durch eine "vorsichtige" Interpolation zwischen den angegebenen Orientierungswerten geschätzt wird. Dabei sind - neben dem für die Systemzustandsidentifizierung relevanten Signal - auch andere Signale, die zum Zustandekommen von Ähnlichkeiten beitragen können, zu berücksichtigen.

Beispiel HTR-500, Schritt 3 in Tab. 15 auf Seite 55: Nach NWA-Ausfall ist der Zustand BEIDE WÄRMETAUSCHER BESPEIST zu identifizieren. Es wird angenommen, daß dieser Zustand anhand einer Anzeigelampe identifizierbar ist, d.h. $p_0 = 0.001 < 3 >$ (Item 11 in Tab. 48 auf Seite 153). Unter der Bedingung, daß die Lampe falsch anzeigt und der Annahme eines Stressfaktors von 2 erhält man einen Median von 0.2 für das Nichtidentifizieren des richtigen Zustands (Tab. 51). Im Abschnitt 4 wurde das Auftreten des Signals EINE PUMPE AUSGEFALLEN als Diagnoseproblem identifiziert, weil es dem Zustand BEIDE WÄRMETAUSCHER BESPEIST unähnlich ist. Durch Interpolation zwischen den o.g. Werten 0.001 und 0.2 wurde hier (unter Verwendung von Tab. 51) geschätzt, daß bei Auftreten des Signals EINE PUMPE AUSGEFALLEN das (richtig anzeigende) Signal BEIDE WÄRMETAUSCHER BESPEIST mit der Wahrscheinlichkeit 0.05 (MDN) nicht wahrgenommen wird. Da dieser Wert für einen Operateur gilt, verringert er sich noch aufgrund personeller Redundanz.

Für PRA-Durchführer, die sich bei Interpolationen zwischen den Orientierungswerten "unsicher" fühlen, stellt das Abhängigkeitsmodell von SWAIN (s. Anhang G) eine brauchbare Alternative dar. Das Abhängigkeitsproblem kann wie folgt definiert werden: Wie ändert sich die Wahrscheinlichkeit p_0 einer Systemzustandsfehlidentifizierung unter der Bedingung, daß eine Ähnlichkeit zum falschen Zustand oder eine Unähnlichkeit zum richtigen Zustand vorhanden ist? Zu dieser Abhängigkeit kann dann ein Kopplungsgrad (zwischen Ähnlichkeit und Fehlidentifizierung) geschätzt werden,

und über diesen Kopplungsgrad ist dann - mit p_0 aus Tab. 51 als unabhängiger Wahrscheinlichkeit - die bedingte Wahrscheinlichkeit für eine Fehlidentifizierung (aufgrund eines Ähnlichkeitsbedingten Erwartungsfehlers) zu berechnen. In Situationen mit nicht optimalem Stressniveau ist - dem SWAIN-Modell entsprechend - die Stressmodifizierung (Anhang F) vor Anwendung des Abhängigkeitsmodells (Anhang G) vorzunehmen.

Informationsdarbietung	Wahrsch.*
Relevantes Signal (für die Systemzustandsidentifizierung) wird RICHTIG angezeigt. KEINE weiteren Signale, die dem richtigen Systemzustand unähnlich sind oder die einem falschen Systemzustand ähnlich sind.	p_0^{**}
Relevantes Signal (für die Systemzustandsidentifizierung) wird RICHTIG angezeigt. Ein weiteres Signal tritt auf, das dem richtigen Systemzustand ETWAS UNÄHNLICH ist oder das dem falschen Systemzustand ETWAS ÄHNLICH ist.	?
Relevantes Signal (für die Systemzustandsidentifizierung) wird RICHTIG angezeigt. Ein weiteres Signal tritt auf, das dem richtigen Systemzustand SEHR UNÄHNLICH ist oder das dem falschen Systemzustand SEHR ÄHNLICH ist.	?
Relevantes Signal (für die Systemzustandsidentifizierung) wird FALSCH angezeigt. Anzeige ist durch Kontrolle anderer Anzeigen ("cross check") als falsch identifizierbar. KEINE weiteren Signale, die dem richtigen Systemzustand unähnlich sind oder die einem falschen Systemzustand ähnlich sind.	$0.1 < 5 >$
Relevantes Signal (für die Systemzustandsidentifizierung) wird FALSCH angezeigt. Anzeige ist durch Kontrolle anderer Anzeigen ("cross check") als falsch identifizierbar. Ein weiteres Signal tritt auf, das dem richtigen Systemzustand ETWAS UNÄHNLICH ist oder das dem falschen Systemzustand ETWAS ÄHNLICH ist.	?
TMI-ähnliche Verhältnisse (Tab. 32 auf Seite 108): Relevantes Signal (für die Systemzustandsidentifizierung) wird FALSCH angezeigt. Anzeige ist durch Kontrolle anderer Anzeigen ("cross check") als falsch identifizierbar. Ein weiteres Signal tritt auf, das dem richtigen Systemzustand SEHR UNÄHNLICH ist oder das dem falschen Systemzustand SEHR ÄHNLICH ist.	1.0

Tab. 51. Orientierungswerte zur Schätzung der Wahrscheinlichkeit einer falschen Identifizierung des Systemzustands (Erwartungsfehler):

* Gilt für einen Operateur bei optimalem Stress.

** Basiswert (z.B. aus Tab. 48 auf Seite 153).

Hier noch eine abschließende Bemerkung zu der in Tab. 51 skizzierten Methode. In vielen Fällen ist - wegen hoher meßtechnischer Zuverlässigkeit - der Fall einer falschen Anzeige vernachlässigbar. Die gesuchte Fehlerwahrscheinlichkeit wird sich

also ca. zwischen 0.001 und 0.1 bewegen. Aber auch dieser Bereich umfaßt noch zwei Größenordnungen. Da innerhalb dieses Bereichs kein weiterer Orientierungswert angegeben werden konnte, enthalten die darin liegenden Schätzungen ein hohes Maß an Unsicherheit. Die absoluten Schätzwerte sollten deshalb nicht überbewertet werden, weil sie (aufgrund fehlender Anhaltspunkte) nur erste, auf subjektiven Einschätzungen beruhende Näherungen sein können. Wichtig ist der qualitative Trend: Das Erkennen eines Diagnoseproblems wird dadurch zum Ausdruck gebracht, daß man eine in Richtung 0.1 liegende Wahrscheinlichkeit verwendet.

5.4 Anwendungsbeispiel HTR-500

5.4.1 Überblick

Im Abschnitt 3 wurde - ohne Berücksichtigung ungeplanter Handlungen aufgrund von Konflikten oder aufgrund von ähnlichkeitsbedingten Diagnoseproblemen - für die NWA des HTR-500 eine Ausfallwahrscheinlichkeit von $3.4E-4 < 2.8 >$ berechnet. Hier geht es um die Frage, auf welchen Wert sich diese Wahrscheinlichkeit erhöht, wenn man die o.g. ungeplanten Handlungen in die Analyse mit einbezieht.

Im Abschnitt 5.4 werden die in den Abschnitten 5.2 und 5.3 vorgestellten Quantifizierungsansätze zu den im Abschnitt 4 identifizierten Rückwirkungen auf die NWA-Zuverlässigkeit des HTR-500 angewendet. Die Berechnung der Wahrscheinlichkeiten der zusätzlich berücksichtigten Fehler erfolgt im Abschnitt 5.4.2. Im Abschnitt 5.4.3 werden die Rückwirkungen auf die NWA-Zuverlässigkeit vor Beginn etwaiger Gegenmaßnahmen einbezogen. Die Rückwirkungen auf die Zuverlässigkeit der Gegenmaßnahmen werden im Abschnitt 5.4.4 quantifiziert. Im Abschnitt 5.4.5 erfolgt einer Zusammenfassung der quantitativen Effekte.

5.4.2 Neue Fehlerwahrscheinlichkeiten

Die im Abschnitt 4 als signifikant eingestuften Rückwirkungen (in Form von ungeplanten Handlungen aufgrund von Konflikten oder Diagnoseproblemen) sind in Tab. 52 auf Seite 166 zusammengefaßt. Tab. 53 auf Seite 167 enthält die Schätzungen, die zur Berechnung der Fehlverhaltenwahrscheinlichkeiten in Konfliktsituationen führten. Dabei wurde das mit der Methode SLIM (EMBREY u.a. 1984) verwandte FLI-Modell (Gleichung 15 in Abschnitt 5.2.3.3) angesetzt. Die Parameter des Modells basieren auf den in Tab. 41 auf Seite 134 genannten Einflußfaktoren (PSFs) und den in Tab. 43 auf Seite 139 genannten Kalibrierungsannahmen zu der

Referenzwahrscheinlichkeit $0.01 < 5 >$ für das gelegentliche Ignorieren von Vorschriften.

Für die drei Konfliktsituationen wurden folgende Wahrscheinlichkeiten (MDN < UF >) berechnet:

$0.034 < 9.2 >$ (FN) Nichteinleiten der Naturkonvektion

$0.0015 < 12.1 >$ (FG) Voreilige Entscheidung für Gebläsehandstart

$0.0021 < 12.1 >$ (FQ) Entscheidung für unnötige Querverbindung bei NWA-Betrieb mit einem Kreislauf

Das verwendete Modell ist mit erheblichen Unsicherheiten (s. Abschnitt 5.2.3.5) verbunden. Es kann derzeit nicht gesagt werden, ob diese Unsicherheiten durch die o.g. Streufaktoren erfaßt werden.

Für die beiden Erwartungsfehler in Tab. 52,

(W5) Nichtbemerken, daß Wärmesenke noch nicht hochgefahren,
und

(W9P) Nichtbemerken, daß beide Wärmetauscher bespeist,

wurde unter Zurhilfenahme von Tab. 51 auf Seite 163 eine Wahrscheinlichkeit von $0.05 < 3 >$ geschätzt. Den Ausgangswert dieser Schätzung bildete die Wahrscheinlichkeit $0.001 < 3 >$ für das nicht richtige Interpretieren einer Anzeigelampe unter Stress (Item 11 in Tab. 48 auf Seite 153). Der MDN 0.05 reduziert sich noch aufgrund personeller Redundanz. Unter der Annahme einer mittleren Kopplung (MD) gilt für den zweiten Operateur eine Wahrscheinlichkeit von $0.16 < 3.2 >$ (vgl. Anhang G).

1. Rückwirkungen auf die ohne Berücksichtigung von Gegenmaßnahmen berechnete NWA-Ausfallwahrscheinlichkeit $2.4E-3$.
 - FG Aktives Fehlverhalten (Situation 3 in Tab. 28 auf Seite 96): Frühzeitige (innerhalb 3 min nach Ausfall der Hauptkühlung) Entscheidung für einen Handstart der NWA-Gebläse.
 $p = 1.5E-3 < 12.1 > *$
 Denkbare Motive: Möglichst schnelle Störfallbeherrschung, frühzeitige Gewißheit über das Funktionieren der NWA.
 Risiko: Gebläseschaden, wenn nicht bemerkt wird, daß das Zwischenkühlwassersystem noch nicht hochgefahren ist.
 - W5 Erwartungsfehler (s. Abschnitt 4.3.2): Nichtbemerken, daß das Zwischenkühlwassersystem (ZKS) noch nicht hochgefahren ist, unter der Bedingung, daß das Nukleare Nebenkühlwassersystem (NNK) gerade hochgefahren ist.
 $p = 5.0E-2 < 3 > **$
 Diagnoseproblem: Der Reiz NNK HOCHGEFAHREN könnte die Erwartung ZKS HOCHGEFAHREN auslösen.
 - FQ Aktives Fehlverhalten (Situation 4 in Tab. 28 auf Seite 96): Entscheidung für Querverbindung (zur Wiederherstellung des ausgefallenen Kreislaufs), wenn NWA-Betrieb mit einem Kreislauf.
 $p = 2.1E-3 < 12.1 > *$
 Denkbare Motiv: Schnelle Wiederherstellung eine NWA mit zwei Kreisläufen.
 Risiko: Fehlhandlung während Querverbindung könnte zum Ausfall des noch funktionierenden Kreislaufs führen.
2. Rückwirkungen auf die Versagenswahrscheinlichkeit $0.14 < 2.8 >$ der Gegenmaßnahmen nach NWA-Ausfall.
 - FN Passives Fehlverhalten (Situation 1 in Tab. 28 auf Seite 96): Nichteinleiten der Naturkonvektion.
 $p = 3.4E-2 < 9.2 > *$
 Motiv: Bevorzugung einer aktiven NWA.
 Risiko: Herstellen einer aktiven NWA ist mit einem erhöhten Zeitbedarf verbunden.
 - W9P Erwartungsfehler (s. Abschnitt 4.3.2): Nichtbemerken, daß beide Wärmetauscher bespeist, wenn Pumpenausfall in der Wärmesenke.
 $p = 5.0E-2 < 3 > **$
 Diagnoseproblem: Der Reiz EINE PUMPE AUSGEFALLEN könnte die Erwartung EIN WÄRMETAUSCHER NICHT BESPEIST auslösen.

Tab. 52. HTR-500. Berücksichtigte ungeplante Handlungen aufgrund von Konflikten und Diagnoseproblemen:

- * Mit Schätzungen aus Tab. 53 über Gleichung 15 (Abschnitt 5.2.3.3) berechnet.
- ** Direkt mit Hilfe von Tab. 51 auf Seite 163 geschätzt, $p_0 = 0.001 < 3 >$ (Item 11 aus Tab. 48 auf Seite 153).

Fehlverhalten → PSF ↓	(FN) Nichteinleiten der Naturkonvektion (Situation 1 in Tab. 28)	(FQ) Entscheidung für Querverbindung (zur Wiederherstel- lung des ausgefal- lenen Kreislaufs), wenn NWA-Betrieb mit einem Kreislauf. (Situation 4 in Tab. 28)	(FG) Frühzeitige (innerhalb 3 min nach Ausfall der Hauptkühlung) Ent- scheidung für einen Handstart der NWA-Gebläse. (Si- tuation 3 in Tab. 28)
(x1) Besonderer An- reiz zu Fehlver- halten	total ($x1 = 1 \pm 0.25$)	nicht ($x1 = 0 \pm 0.25$)	mittel ($x1 = 0.5 \pm 0.25$)
(x2) Zielkonflikt	total ($x2 = 1 \pm 0.25$)	total ($x2 = 1 \pm 0.25$)	total ($x2 = 1 \pm 0.25$)
(x3) Möglicher Schaden klein	schwach ($x3 = 0.25 \pm 0.25$)	nicht ($x3 = 0 \pm 0.25$)	nicht ($x3 = 0 \pm 0.25$)
(x4) Wahrschein- lichkeit für Schaden klein	nicht ($x4 = 0 \pm 0.25$)	stark ($x4 = 0.75 \pm 0.25$)	stark ($x4 = 0.75 \pm 0.25$)
(x5) Risiko wird unterschätzt	stark ($x5 = 0.75 \pm 0.25$)	keine Ahnung ($x5 = 0.5 \pm 0.5$)	keine Ahnung ($x5 = 0.5 \pm 0.5$)
(x6) Fehlverhalten zu einfach, keine Hindernisse	total ($x6 = 1 \pm 0.25$)	keine Ahnung ($x6 = 0.5 \pm 0.5$)	keine Ahnung ($x6 = 0.5 \pm 0.5$)
(x7) Richtiges Ver- halten ungewöhn- lich, Fehlverhalten manchmal richtig	stark ($x7 = 0.75 \pm 0.25$)	schwach ($x7 = 0.25 \pm 0.25$)	schwach ($x7 = 0.25 \pm 0.25$)

Tab. 53. HTR-500. Geschätzte PSF-Grade zu (ungeplantem) Fehlverhalten in drei signifikanten Konfliktsituationen:

Nähere PSF-Beschreibungen in Tab. 41 auf Seite 134

5.4.3 Modifizierung der NWA-Zuverlässigkeit ohne Gegenmaßnahmen

Im Abschnitt 3 wurde für die NWA des HTR-500 eine Ausfallwahrscheinlichkeit von $2.4E-3$ berechnet. In diesem Wert sind menschlichen Gegenmaßnahmen nicht enthalten. Die Fehler FG, FQ und W5 (Tab. 52) betreffen die Zuverlässigkeit der NWA vor Anforderung etwaiger Gegenmaßnahmen. Durch ihre Einbeziehung erhöht sich die Ausfallwahrscheinlichkeit geringfügig von $2.4E-3$ auf $2.5E-3$. Der Wert $2.4E-3$ enthält (direkt) nur technische Ursachen. Die Wahrscheinlichkeiten solcher Ursachen wurden - entsprechend der im Abschnitt 3.3.1 beschriebenen Methode - nur als Punktwerte (ohne Streufaktoren) berücksichtigt. Wahrscheinlichkeiten menschlicher Fehler wurden mit Unsicherheiten berücksichtigt. Da menschliche Fehler zur Erhöhung des Werts $2.4E-3$ beigetragen haben, ergeben sich für den neuen Wert, $EW = 2.5E-3$, folgende Verteilungsparameter:

MDN = $2.47E-3$, UF = 1.3.

Das daraus resultierende Unsicherheitsintervall $< 1.9E-3, 3.2E-3 >$ enthält den Wert $2.4E-3$ ohne Berücksichtigung ungeplanter Eingriffe mit ausreichender Sicherheit. Die Erhöhung liegt also im Rahmen der durch die Einbeziehung menschlicher Fehler entstehenden Unsicherheiten.

In Abb. 22 ist die Berechnung des neuen Wertes ($2.5E-3$) dokumentiert. Drei Beiträge tragen zur Erhöhung der Wahrscheinlichkeit $2.4E-3$ für das Versagen der NWA vor Anforderung etwaiger Gegenmaßnahmen bei. Zwei Beiträge aufgrund der voreiligen Entscheidung (FG) für einen Handstart der Gebläse, ein Beitrag aufgrund der unnötigen Entscheidung (FQ) für eine Querverbindung.

Für die Entscheidung FG, $p = 1.5E-3 < 12.1 >$, werden zwei Korrekturwahrscheinlichkeiten angenommen: Zwei Operateure können bemerken, daß das Zwischenkühlwassersystem (ZKS) noch nicht hochgefahren ist (Schritt 5 des in Tab. 15 auf Seite 55 angenommenen Handlungsablaufs).

Als Fehler für das Nichtbemerken werden folgende zwei Ursachen betrachtet:

(U5) Unterlassung: $p = 0.02 < 5 >$

(Anhang E: ID=3.111; Anhang F: PSF=2 wegen mitterem Stress bei regelbasiertem Verhalten).

(W5) Wahrnehmungsfehler: $p = 0.05 < 3 >$

(Tab. 52 auf Seite 166)

Aufgrund personeller Redundanz durch einen zweiten Operateur ($_2$) bei mittlerer Kopplung (vgl. Anhang G) ergeben sich zu den o.g. Fehlern die Korrekturwahrscheinlichkeiten $0.16 < 3.2 >$ (U5₂) und $0.19 < 2.8 >$ (W5₂).

Das ZKS ist ca. 3 min nach Ausfall der Hauptkühlung verfügbar (vgl. Tab. 10 auf Seite 49). Die Wahrscheinlichkeit, daß die etwaige Ausführung der Entscheidung FG - nach dem nicht bemerkt wird, daß das ZKS noch nicht hochgefahren ist - vor Hochfahren des ZKS beginnt, wird hier gleich 1 gesetzt.

Der Beitrag aufgrund der Entscheidung FQ (unnötige Querverbindung) reduziert sich durch folgende Wahrscheinlichkeiten:

- $w(TQ) \approx 2 \cdot 5.4E-3 \approx 0.011$,
die Wahrscheinlichkeit, daß es zu einem NWA-Betrieb mit nur einem Kreislauf kommt, derart, daß ein Übergang per Querverbindung zu einem NWA-Betrieb mit zwei Kreisläufen möglich ist. Hauptbeitrag zu $w(TQ)$ liefert das Ereignis AUSFALL 1v2 GEBLÄSEKÜHLPUMPEN ($5.4E-3$ pro Pumpe). Da die Wärmetauscherbespeisung mit zwei Pumpen pro Strang überdimensioniert ist (s. Abb. 12 auf Seite 48) könnte dann eine dieser Pumpen das noch nicht angeforderte Gebläse kühlen.
- $w(Q) = 0.042 < 2.6 >$,
die Wahrscheinlichkeit, daß während einer ungeplanten Querverbindung ein Operateurfehler auftritt, der zum Ausfall des noch funktionierenden NWA-Kreislaufs führt. Wegen fehlender Systemunterlagen wurde hier die Wahrscheinlichkeit für das Versagen der Querverbindung aufgrund von Operateurfehlern außerhalb der Warte angesetzt (s. Abschnitt 3.3.3.3).

Abb. 22 ist zu entnehmen, daß die ungeplante Querverbindung (FQ) nur einen geringen Beitrag zur Erhöhung der Ausfallwahrscheinlichkeit von $2.4E-3$ auf $2.5E-3$ liefert. Den Hauptbeitrag der Erhöhung liefert der ungeplante Gebläsehandstart (FG).

QUANTIFIZIERUNGSPROBLEM

FEHLER: NWA-AUSFALL OHNE GEGENMASSNAHMEN,
MIT AKTIVEN EINGRIFFEN VOR NWA-START

1) KONTROLLAUSDRUCK DER EINGABEDATEN

CUT_SET	FEHLER1	MDN1	UF1	FEHLER2	MDN2	UF2	FEHLER3	MDN3	UF3	FEHLER4	MDN4	UF4
1	NWA_T	0.0024	1		.	.		.	.		.	.
2	U5	0.0200	5	U5_2	0.1600	3.2	FG	0.0015	12.1		.	.
3	W5	0.0500	3	W5_2	0.1900	2.8	FG	0.0015	12.1		.	.
4	TQ	0.0110	1	FQ	0.0021	12.1	Q	0.0420	2.6		.	.

2) CUT SETS SORTIERT NACH GROESSE (EW) UND AUFSUMMIERT

FEHLER1	FEHLER2	FEHLER3	FEHLER4	EW	EW_SUM	MDN_SUM	UF_SUM
NWA_T				.0024000	.0024000	.0024000	1.00000
W5	W5_2	FG		.0000683	.0024683	.0024478	1.23690
U5	U5_2	FG		.0000314	.0024997	.0024714	1.28148
TQ	FQ	Q		.0000036	.0025033	.0024751	1.28121

3) ERGEBNISWAHRSCHEINLICHKEIT, WENN CUT SETS NICHT EXKLUSIV

MDN	UF	EW	VAR	STD	UG	OG
0.002474	1.28	0.002503	0.000000	0.000379	.0019316	.0031708

Abb. 22. HTR-500. NWA-Ausfallwahrscheinlichkeit ohne Gegenmaßnahmen, aber mit ungeplanten Handlungen: Erläuterungen im Text von Abschnitt 5.4.3

5.4.4 Modifizierung der Zuverlässigkeit der Gegenmaßnahmen

Der Ausfall der NWA fordert Gegenmaßnahmen ("Accident Management") an, die vom Personal durchzuführen sind. Diese Gegenmaßnahmen (Naturkonvektion, Querverbindung und Reparatur) wurden im Abschnitt 3 analysiert. Für ihr Versagen in Bezug auf das Hauptziel NWA AUSREICHEND wurde eine Wahrscheinlichkeit von $0.14 < 2.8 >$ berechnet.

Die zusätzlichen Fehler (Tab. 52 auf Seite 166),

(FN) Nichteinleiten der Naturkonvektion und

(W9P) Nichtbemerken, daß beide Wärmetauscher bespeist, wenn Pumpenausfall in der Wärmesenke,

betreffen die Gegenmaßnahme Naturkonvektion. Ohne diese Fehler liegt die Wahrscheinlichkeit für ihr Versagen aufgrund von Operateurfehler bei $0.13 < 4.3 >$. Die

Einbeziehung der o.g. Fehler FN und W9P bewirkt, daß sich dieser Wert auf $0.18 < 4.3 >$ erhöht - eine Erhöhung, die durch das 90%-Unsicherheitsintervall $< 0.03, 0.56 >$ des alten Werts gut abgedeckt ist.

In Abb. 23 ist die Berechnung des erhöhten Werts ($0.18 < 4.3 >$) dokumentiert. Die Wahrscheinlichkeit, $0.034 < 9.2 >$ (FN in Tab. 52 auf Seite 166), für das (absichtliche) Nichteinleiten der Naturkonvektion liefert einen direkten Beitrag zum TOP. Dagegen reduziert sich der Beitrag der Wahrscheinlichkeit $0.05 < 3 >$ (W9P in Tab. 52) aufgrund folgender Korrekturfaktoren:

- $w(P) \simeq 0.12$,
Wahrscheinlichkeit, daß Pumpenausfall in der Wärmesenke, wenn NWA-Ausfall. Diese Wahrscheinlichkeit ergibt sich in etwa aus der Summe der Wahrscheinlichkeiten folgender Ereignisse:
 - Querverbindung möglich, wenn NWA-Ausfall ($p \simeq 0.1$, s. Abschnitt 3.3.3.3).
 - Ausfall 1v4 Pumpen der Wärmetauscherbespeisung ($p \simeq 4.5.4E-3$, s. Tab. 13 auf Seite 53).
- $w(W9P_2) = 0.19 < 2.8 >$ (mittlere Kopplung, s. Anhang G),
Wahrscheinlichkeit, daß auch der zweite Operateur nicht bemerkt, daß beide Wärmetauscher bespeist sind, wenn ein Pumpenausfall in der Wärmesenke vorliegt.

Aufgrund der erhöhten Operateurfehlerwahrscheinlichkeit $0.18 < 4.3 >$ der Naturkonvektion erhöht sich die gesamte Versagenswahrscheinlichkeit aller drei Gegenmaßnahmen von $0.14 < 2.8 >$ (s. Abb. 19 auf Seite 81) auf $0.18 < 3 >$.

In Abb. 24 ist die zu dem Wert $0.18 < 3 >$ (Output 2, letzte Zeile, "MDN_SUM", "UF_SUM") führende Rechnung dokumentiert. Anstelle von $0.13 < 4.3 >$ wie in Abb. 19 wurde in Abb. 24 für den Fehler N (Naturkonvektion versagt wegen Operateurfehler) der in Abb. 23 berechnete Wert $0.18 < 4.3 >$ verwendet.

Folgende drei Cutsets liefern den Hauptbeitrag zur modifizierten Versagenswahrscheinlichkeit $0.18 < 3 >$ ($EW = 0.22$) aller Gegenmaßnahmen:

1. $_QR\ N$ ($EW = 0.149$):

Querverbindung und Reparatur technisch unmöglich UND keine Naturkonvektion wegen Operateurfehler.

2. NQR (EW = 0.042):

Alle drei Gegenmaßnahmen technisch unmöglich..

3. _Q_ N R (EW = 0.02265):

Querverbindung technisch unmöglich, keine Naturkonvektion UND keine Reparatur wegen Operateurfehler.

Die Berechnung in Abb. 24 gilt für die in Tab. 22 auf Seite 79 berechnete Verteilung der technischen Möglichkeiten nach NWA-Ausfall. Diese Verteilung hängt von der Ausfallwahrscheinlichkeit $2.4E-3$ der NWA ohne Einbeziehung etwaiger Gegenmaßnahmen ab. In Abb. 22 auf Seite 170 wurde hierfür ein leicht erhöhter Wert von $2.5E-3$ berechnet. Dies führt zu einer Neuverteilung der technischen Möglichkeiten. So erhöht sich z.B. der Anteil der nicht reparierbaren Ausfälle geringfügig. Diese Änderungen können jedoch vernachlässigt werden. Die modifizierte NWA-Ausfallwahrscheinlichkeit unter Einbeziehung von Gegenmaßnahmen kann also aus dem Produkt folgender Wahrscheinlichkeiten berechnet werden:

$0.00247 < 1.3 >$ NWA-Ausfall ohne Gegenmaßnahmen

$0.18 < 3 >$ Gegenmaßnahmen versagen

Man erhält $4.4E-4 < 3.1 >$ (EW = $5.5E-4$) für das NWA-Versagen des HTR-500. Der Wert ohne Einbeziehung der im Abschnitt 4 identifizierten ungeplanten Handlungen beträgt $3.4E-4 < 2.8 >$ (EW = $4.1E-4$).

QUANTIFIZIERUNGSPROBLEM

FEHLER: KEINE NATURKONVEKTION WEGEN OPERATEURFEHLER,
MIT ZEITFEHLER (N_Z, N_S), MIT ERWARTUNGSFEHLER (W9P) UND FEHLVERHALTEN (FN)

1) KONTROLLAUSDRUCK DER EINGABEDATEN

CUT_SET	FEHLER1	MDN1	UF1	FEHLER2	MDN2	UF2	FEHLER3	MDN3	UF3	FEHLER4	MDN4	UF4
1	D1	0.0100	10.0		.	.		.	.		.	.
2	W9	0.0010	3.0	W9_2	0.15	3.3		.	.		.	.
3	W9P	0.0500	3.0	W9P_2	0.19	2.8	P	0.12	.		.	.
4	U10	0.0200	5.0	U10_2	0.16	3.2	U10_3	0.51	1.9		.	.
5	W10	0.0010	3.0	W10_2	0.15	3.3		.	.		.	.
6	FN	0.0340	9.2		.	.		.	.		.	.
7	U11N	0.0130	5.0	U11N_2	0.16	3.2	U11N_3	0.51	1.9	N_S	0.54	5
8	W11N	0.0007	3.0	W11N_2	0.15	3.3		.	.	N_S	0.54	5
9	V11N	0.0170	10.0	V11N_2	0.16	3.2		.	.	N_S	0.54	5
10	V12N	0.0250	10.0	V12N_2	0.16	3.2		.	.	N_S	0.54	5
11	U13N	0.0250	5.0	U13N_2	0.16	3.2	U13N_3	0.51	1.9	N_S	0.54	5
12	N_Z	0.0885	5.0		.	.		.	.		.	.

2) CUT SETS SORTIERT NACH GROESSE (EW) UND AUFSUMMIERT

FEHLER1	FEHLER2	FEHLER3	FEHLER4	EW	EW_SUM	MDN_SUM	UF_SUM
N_Z				0.14282	0.14282	0.08850	5.00000
FN				0.08447	0.22729	0.14834	4.57084
D1				0.02664	0.25393	0.17330	4.21170
V12N	V12N_2		N_S	0.01192	0.26585	0.18321	4.13492
V11N	V11N_2		N_S	0.00811	0.27395	0.19055	4.06206
U13N	U13N_2	U13N_3	N_S	0.00398	0.27793	0.19463	4.00898
U10	U10_2	U10_3		0.00365	0.28158	0.19846	3.95877
U11N	U11N_2	U11N_3	N_S	0.00207	0.28365	0.20062	3.93149
W9P	W9P_2	P		0.00173	0.28538	0.20246	3.90802
W9	W9_2			0.00024	0.28562	0.20272	3.90473
W10	W10_2			0.00024	0.28587	0.20298	3.90145
W11N	W11N_2		N_S	0.00015	0.28602	0.20313	3.89945

3) ERGEBNISWAHRSCHEINLICHKEIT, WENN CUT SETS NICHT EXKLUSIV

MDN	UF	EW	VAR	STD	UG	OG
0.176092	4.28	0.260343	0.080371	0.283499	0.041114	0.75422

Abb. 23. Naturkonvektion. Operateurfehler einschließlich ungeplanter Handlungen:
_2: 2. Operateur, _3: 3. Operateur, _S: späte Korrektur, _Z: Zeitüberschreitung;
weitere Erläuterungen in Tab. 18 auf Seite 59 und im Text von Abschnitt 5.4.4

QUANTIFIZIERUNGSPROBLEM

FEHLER: GEGENMASSNAHMEN ERFOLGLOS, FEHLER1: TECHNIK,
FEHLER2-4: PERSONAL, MIT FEHLVERHALTEN UND ERWARTUNGSFEHLER

1) KONTROLLAUSDRUCK DER EINGABEDATEN

CUT_SET	FEHLER1	MDN1	UF1	FEHLER2	MDN2	UF2	FEHLER3	MDN3	UF3	FEHLER4	MDN4	UF4
1	—	0.03700	1	N	0.18	4.3	Q	0.053	2.3	R	0.23	3.4
2	—R	0.05600	1	N	0.18	4.3	Q	0.053	2.3		.	.
3	—Q	0.28000	1	N	0.18	4.3		.	.	R	0.23	3.4
4	—QR	0.56000	1	N	0.18	4.3		.	.		.	.
5	N—	0.00270	1		.	.	Q	0.053	2.3	R	0.23	3.4
6	N_R10	0.00006	1		.	.	Q	0.053	2.3	R10	0.46	2.0
7	N_R	0.00420	1		.	.	Q	0.053	2.3		.	.
8	NQ—	0.02000	1		.	.		.	.	R	0.23	3.4
9	NQR10	0.00040	1		.	.		.	.	R10	0.46	3.4
10	NQR	0.04200	1		.	.		.	.		.	.

2) CUT SETS SORTIERT NACH GROESSE (EW) UND AUFSUMMIERT

FEHLER1	FEHLER2	FEHLER3	FEHLER4	EW	EW_SUM	MDN_SUM	UF_SUM
—QR	N			0.14934	0.14934	0.10080	4.30000
NQR				0.04200	0.19134	0.14556	3.37574
—Q—	N		R	0.02265	0.21399	0.16846	3.12021
NQ—			R	0.00607	0.22006	0.17502	3.04412
—R	N	Q		0.00090	0.22096	0.17600	3.03312
NQR10			R10	0.00029	0.22125	0.17632	3.02957
N_R		Q		0.00025	0.22150	0.17659	3.02649
—	N	Q	R	0.00018	0.22168	0.17679	3.02430
N—		Q	R	0.00005	0.22173	0.17684	3.02370
N_R10		Q	R10	0.00000	0.22174	0.17684	3.02368

Abb. 24. Gegenmaßnahmen. Menschliche und technische Fehler. Gesamtbewertung einschließlich ungeplanter Handlungen:
Erläuterungen im Text von Abschnitt 5.4.4

5.4.5 Ergebniszusammenfassung

Die hier neu berücksichtigten Fehler, bewußte Risikoannahme in Konfliktsituationen (Fehlverhalten) und Systemzustandfehlidentifikation aufgrund ähnlichkeitsbedingter Diagnoseprobleme (Erwartungsfehler), werden hier unter dem Begriff "ungeplante Handlungen" zusammengefaßt. Denn diese Fehler führen unmittelbar zur der Verfolgung nicht vorgesehener Strategien. Mit diesen Fehlern werden Ursachen ungeplanter Handlungen berücksichtigt, die nicht direkt durch die Fehlerwahrscheinlichkeiten des SWAIN-Handbuchs erfaßt werden.

Beispiel HTR-500. Mit SWAIN (1983) lassen sich z.B. für die ungeplante Handlung NICHT EINLEITEN DER NATURKONVEKTION (nach richtiger Diagnose für die Störfallprozedur) die Ursachen W9, U10 und W10 in Tab. 18 auf Seite 59 berücksichtigen. Hier wurden zusätzlich noch die Ursachen (W9P) NICHT BEMERKT, DASS BEIDE WÄRMETAUSCHER BESPEIST, WENN PUMPENAUSFALL IN DER WÄRMESENKE (Diagnoseproblem wegen Ähnlichkeit) und (FN) ABSICHTLICHES NICHT EINLEITEN DER NATURKONVEKTION (Entscheidungsproblem wegen Konflikt) berücksichtigt.

In Tab. 54 sind die Effekte menschlichen Verhaltens auf die Ausfallwahrscheinlichkeit der NWA zusammengefaßt. In horizontaler Richtung ist der Effekt aufgrund der Änderung von X=NEIN auf X=JA signifikant: Die Punktwerte für X=NEIN sind nicht in den Unsicherheitsintervallen für X=JA enthalten. Die Berücksichtigung menschlicher Gegenmaßnahmen trägt also signifikant zur Verringerung der Ausfallwahrscheinlichkeit bei. Dagegen sind die vertikalen Effekte (Tab. 54) nicht signifikant. Denn die Punktwerte für Y=NEIN sind in den Unsicherheitsintervallen für Y=JA enthalten. Die Einbeziehung von Konflikten und Ähnlichkeiten (als Ursachen ungeplanter Handlungen) trägt also nur unwesentlich zur Erhöhung der Ausfallwahrscheinlichkeit bei. Diese Aussage kann jedoch nicht auf die gesamte PRA des HTR-500 übertragen werden. Die Zuverlässigkeit der NWA ist zwar ein bedeutender, aber kein alles umfassender Bestandteil einer PRA.

(X) Gegenmaßnahmen berücksichtigt → (Y) Konflikte und Ähnlichkeiten berücksichtigt ↓	N E I N	J A
N E I N *	2.4E-3	4.1E-4 < 1.2E-4, 9.4E-4 >
J A	2.5E-3 < 1.9E-3, 3.2E-3 >	5.5E-4 < 1.4E-4, 1.4E-3 >

Tab. 54. HTR-500. Einflüsse menschlichen Verhaltens auf die Wahrscheinlichkeit des Versagens der NWA:

Erwartungswerte und 90%-Unsicherheitsintervalle aufgrund menschlicher Variationsursachen.

* Im Sinne von "weder ... noch".

5.5 Zusammenfassung von Abschnitt 5

Es wurden zwei Quantifizierungsansätze vorgeschlagen, die die Einbeziehung von Konflikten und Ähnlichkeiten (als Ursachen ungeplanter Handlungen) in eine probabilistische Risikoanalyse (PRA) erlauben. Aufgrund von Konflikten kann eine ungeplante Handlung als bewußte Risikoannahme (Fehlverhalten) auftreten, aufgrund von Ähnlichkeiten als erwartungsgebundene Systemzustandsfehlidentifizierung (Erwartungsfehler).

Die Einbeziehung dieser Fehler in die Zuverlässigkeitsanalyse der Nachwärmeabfuhr eines Hochtemperaturreaktorkonzepts (HTR-500) mittlerer Leistung ergab eine nicht signifikante Erhöhung der Auffallwahrscheinlichkeit von $4.1\text{E-}4$, mit $< 1.2\text{E-}4, 9.4\text{E-}4 >$ als 90%-Unsicherheitsintervall, auf $5.5\text{E-}4 < 1.4\text{E-}4, 1.4\text{E-}3 >$.

In den Unsicherheiten sind nur Variabilitätsursachen menschlicher Fehlerwahrscheinlichkeiten enthalten. Hauptbeitrag der Erhöhung liefern ungeplante Handlungen aufgrund von Konflikten.

Solches Fehlverhalten fällt in der psychologischen Sicherheitsforschung unter die Rubrik menschliches Risikoverhalten. Hierzu gibt es derzeit kein einheitliches Vorhersagemodell. Selbst einfache Entscheidungsexperimente mit klar definierten Anreizen (z.B. Geldgewinnen oder -verlusten) und Aussichten (z.B. bekannte Gewinn- bzw. Verlustwahrscheinlichkeiten) weisen widersprüchliche Ergebnisse auf.

Auf Verhältnisse im Kernkraftwerk übertragbare Wahrscheinlichkeiten zum Risikoverhalten sind selten. Deshalb wurde hier ein Modell entwickelt, daß auf Extrapolationen zu einer dem SWAIN-Handbuch zu entnehmenden Wahrscheinlichkeit 0.01 (Median) für das gelegentliche Ignorieren von Vorschriften basiert. Das Modell ist mit der Methode SLIM vergleichbar. Die Extrapolationen erfolgen multiplikativ über Einflußfaktoren (sog. PSFs), die sich sowohl auf die Folgen (Kosten/Nutzen) ungeplante Handlungen als auch deren "psychologische Nähe" (Einfachheit, der Gewohnheit entsprechend) beziehen.

Zur Schätzung von Erwartungsfehlerwahrscheinlichkeiten wurde hier ein Modell vorgeschlagen, daß auf direkten Wahrscheinlichkeitsschätzungen beruht. Es werden drei Orientierungswerte mit Situationsbeschreibungen gegeben. Mit diesen Situationsbeschreibungen ist die zu beurteilende Situation, in der der zu quantifizierende Erwartungsfehler auftreten könnte, zu vergleichen. Auf der Basis dieses Vergleichs ist dann

durch Interpolationen zwischen den Orientierungswerten die gesuchte Wahrscheinlichkeit zu schätzen.

Beide Quantifizierungsvorschläge zur Schätzung der Wahrscheinlichkeit ungeplanter Handlungen (aufgrund von Konflikten oder Ähnlichkeiten) enthalten erhebliche Unsicherheiten. Es kann derzeit nicht gesagt werden, ob diese Unsicherheiten durch die verwendeten Streufaktoren abgedeckt sind.

6. Zusammenfassung

Aktuelle Forschungsarbeiten zur Erhöhung der Realitätsnähe einer Mensch-Maschine-Systemanalyse (MMSA) konzentrieren sich auf Entscheidungsfehler des Personals, die zu ungeplanten Handlungen mit sicherheitsrelevanten Folgen führen können. Das Auftreten von Konflikten (zwischen Handlungsalternativen) oder Ähnlichkeiten (zwischen Systemzuständen) führt zu kritischen Situationen im Störfallablauf, in denen ungeplante Handlungen mit einer erhöhten Wahrscheinlichkeit zu erwarten sind. Aufgrund menschlicher Risikobereitschaft kann es in Konfliktsituationen, in denen die richtige Verhaltensweise mit negativen Nebeneffekten verbunden ist, zu Fehlentscheidungen kommen (z.B. Davis-Besse 1985). Ähnlichkeiten können Erwartungsfehler auslösen, die zu einer falschen Identifizierung des Systemzustands führen (z.B. TMI 1979).

In dieser Arbeit wurde eine Methode zur Einbeziehung solcher Fehler in eine probabilistische Risikoanalyse (PRA) vorgestellt und am Beispiel der Zuverlässigkeit der Nachwärmeabfuhr (NWA) des Konzeptes eines mittelgroßen Hochtemperaturreaktors (HTR-500) angewendet.

Es wurde gezeigt, daß solche kritische Situationen im Rahmen einer PRA identifizierbar sind, indem man nach Rückwirkungen untergeordneter Ziele auf das Hauptziel SICHERHEIT sucht. Für das hier analysierte Hauptziel, die Zuverlässigkeit der NWA des HTR-500, wurden fünf kritische Situationen identifiziert.

Die hier vorgeschlagene Methode zur Identifizierung möglicher Konflikte im Störfallablauf besteht darin, daß auf der Grundlage von vier Differenzierungskriterien mögliche Realisierungsalternativen des Hauptziels SICHERHEIT gebildet werden. Anhand verschiedener Checklisten werden die Alternativen auf mögliche Nachteile hin untersucht und bewertet. Unter der Annahme, daß sich das Personal - neben der Erreichung des Hauptziels SICHERHEIT - auch die Vermeidung dieser Nachteile zum Ziel setzt, sind Konflikte immer dann zu erwarten, wenn die Rangfolge der Alternativen bezüglich ihrer Nachteile nicht eindeutig ist.

Die hier vorgeschlagene Methode zur Identifizierung von Diagnoseproblemen aufgrund von Ähnlichkeiten basiert auf der Bildung von Erscheinungsformen des WENN-Teils von Regeln der Form
WENN Situation X, DANN Reaktion Y.

Zur Identifizierung von Diagnoseproblemen, die zum Nichtausführen des DANN-Teils führen können, werden verschiedene Erscheinungsformen gebildet, die den WENN-Teil erfüllen. Zu diesen Erscheinungsformen wird gefragt, wie "unähnlich" sie den WENN-Teil erfüllen; oder anders formuliert, ob sie Reize enthalten, die die Assoziation erwecken können, daß der WENN-Teil nicht erfüllt ist.

Zur Identifizierung von Diagnoseproblemen, die zum fälschlichen Ausführen des DANN-Teils führen können, werden zunächst Regeln mit widersprüchlichen DANN-Teilen identifiziert. Zu den WENN-Teilen werden verschiedene Erscheinungsformen gebildet und auf Ähnlichkeiten hin untersucht: Kann eine Situation, die die Reaktion Y erfordert, mit einer anderen Situation verwechselt werden, die die gegenteilige Reaktion erfordert?

Die Schätzung der Wahrscheinlichkeiten ungeplanter Handlungen in - aufgrund von Konflikten (Entscheidungsproblemen) oder Ähnlichkeiten (Diagnoseproblemen) - kritischen Situationen ist mit erheblichen Unsicherheiten verbunden. Die hier vorgeschlagenen Modelle nutzen Extra- und Interpolationen auf der Grundlage der wenigen Daten, die zu Entscheidungsfehlern von Operateuren verfügbar sind. Somit sind die damit ermittelten Wahrscheinlichkeiten als Werte zu interpretieren, die - nach der subjektiven Meinung des Modellanwenders - in angemessener Relation zu bekannten Wahrscheinlichkeiten vergleichbarer Fehler stehen.

Fehlverhalten in Konfliktsituationen fällt in der psychologischen Sicherheitsforschung unter die Rubrik menschliches Risikoverhalten. Hierzu gibt es derzeit kein einheitliches Vorhersagemodell. Selbst einfache Entscheidungsexperimente mit klar definierten Anreizen (z.B. Geldgewinnen oder -verlusten) und Aussichten (z.B. bekannte Gewinn- bzw. Verlustwahrscheinlichkeiten) weisen widersprüchliche Ergebnisse auf.

Auf Verhältnisse im Kernkraftwerk übertragbare Wahrscheinlichkeiten zum Risikoverhalten sind selten. Deshalb wurde hier ein Modell entwickelt, daß auf Extrapolationen zu der auf industriellen Erfahrungen basierenden Wahrscheinlichkeit 0.01 (Median) für das gelegentliche Ignorieren von Vorschriften basiert. Das Modell ist mit der Methode SLIM vergleichbar. Die Extrapolationen erfolgen multiplikativ über Einflußfaktoren (sog. PSFs), die sich sowohl auf die Folgen (Kosten/Nutzen) ungeplanter Handlungen als auch auf deren "psychologischen Nähe" (Einfachheit, der Gewohnheit entsprechend) beziehen.

Zur Schätzung der Wahrscheinlichkeit einer falschen Identifizierung des Systemszustands aufgrund von Ähnlichkeiten (Erwartungsfehler) wurde hier ein Modell vorge-

schlagen, daß auf direkten Wahrscheinlichkeitsschätzungen beruht. Das Modell besteht aus drei Orientierungswerten mit Situationsbeschreibungen. Mit diesen Situationsbeschreibungen ist die zu beurteilende Situation, in der der zu quantifizierende Erwartungsfehler auftreten könnte, zu vergleichen. Auf der Basis dieses Vergleichs ist dann durch Interpolationen zwischen den Orientierungswerten die gesuchte Wahrscheinlichkeit zu schätzen.

Beide Quantifizierungsvorschläge zur Schätzung der Wahrscheinlichkeit ungeplanter Handlungen (aufgrund von Konflikten oder Ähnlichkeiten) enthalten erhebliche Unsicherheiten. Es kann derzeit nicht gesagt werden, ob diese Unsicherheiten durch die verwendeten Streufaktoren abgedeckt sind.

Die Einbeziehung der hier identifizierten Rückwirkungen in die Zuverlässigkeitsanalyse der NWA des HTR-500 ergab eine nicht signifikante Erhöhung der Auffallwahrscheinlichkeit von

$4.1\text{E-}4$, mit $< 1.2\text{E-}4, 9.4\text{E-}4 >$ als 90%-Unsicherheitsintervall, auf $5.5\text{E-}4 < 1.4\text{E-}4, 1.4\text{E-}3 >$.

In den Unsicherheiten sind nur Variabilitätsursachen menschlicher Fehlerwahrscheinlichkeiten enthalten. Hauptbeitrag der Erhöhung liefern ungeplante Handlungen aufgrund von Konflikten.

Außerdem wurde für passive Entscheidungsfehler (Unterlassungen notwendiger Handlungen) ein völlig neuartige Modellansatz vorgestellt, der solche Fehler nicht über Wahrscheinlichkeiten, sondern über Verzögerungszeiten quantifiziert. Die praktische Durchführbarkeit dieses dynamischen Ansatzes wurde am Beispiel einer probabilistischen Analyse der konkreten Operateurmaßnahmen gezeigt, die während des Störfalls im Kernkraftwerk Davis-Besse (1985) angefordert wurden. Dieser Ansatz setzt jedoch die Verfügbarkeit situationsspezifischer Verzögerungszeiten voraus.

7. Schlußfolgerungen

Es wurde hier eine Methode vorgestellt, mit der sich im Rahmen einer probabilistischen Risikoanalyse (PRA) ungeplante Handlungen aufgrund von Konflikten und Ähnlichkeiten identifizieren und quantifizieren lassen. Die Anwendung auf die Analyse des Systems zur Nachwärmeabfuhr (NWA) eines mittelgroßen Hochtemperaturreaktorkonzepts (HTR-500) ergab keine signifikante Erhöhung der Ausfallwahrscheinlichkeit aufgrund ungeplanter Handlungen. Das Ergebnis bedeutet nicht, daß kein signifikanter Einfluß vorhanden ist, sondern nur, daß keiner nachweisbar ist! Die hohen Streufaktoren der verwendeten menschlichen Fehlerwahrscheinlichkeiten erschweren den Nachweis signifikanter Einflüsse. Wegen fehlender spezifischer Daten kann derzeit nicht auf diese hohen Streufaktoren verzichtet werden; denn die als Eingangsgrößen verwendeten Fehlerwahrscheinlichkeiten enthalten ein hohes Maß an Expertenmeinung. Man kann keine Ergebniswahrscheinlichkeit mit kleiner Unsicherheit erwarten, wenn die zur Berechnung erforderlichen Eingangsgrößen sehr "unscharf" definiert sind; z.B. die Definitionen der Kategorien "hohe Kopplung", "mittelhoher Stress" oder "stark vorhandene Risikounterschätzung".

Die hier näher erörterten Schlußfolgerungen der Ergebnisse dieser Arbeit gehen in zwei Zielrichtungen: (1) Erhöhung Sicherheit von Kernkraftwerken durch Senkung der menschlichen Risikobereitschaft und (2) Erhöhung der Realitätsnähe einer PRA durch methodische Weiterentwicklungen.

Senkung menschlicher Risikobereitschaft

Aufgrund der hier in die NWA-Analyse des HTR-500 einbezogenen ungeplanten Handlungen - von denen drei durch menschliche Risikobereitschaft erklärbar sind - erhöhte sich die Ausfallwahrscheinlichkeit nur geringfügig von

$4.1\text{E-}4$, 90%-Unsicherheitsintervall $< 1.2\text{E-}4, 9.4\text{E-}4 >$, auf

$5.5\text{E-}4 < 1.4\text{E-}4, 1.4\text{E-}3 >$.

Hauptbeitrag der Erhöhung lieferten ungeplante Handlungen in Konfliktsituationen aufgrund menschlicher Risikobereitschaft. Den Unsicherheitsintervallen ist zu entnehmen, daß ein signifikanter Beitrag menschlicher Risikobereitschaft nicht nachweisbar ist. Trotzdem haben m.E. Maßnahmen zur Senkung der Risikobereitschaft - und somit zur Senkung der der Wahrscheinlichkeit ungeplanter Handlungen - eine hohe Bedeutung für die Reaktorsicherheit. Denn zum einen ist das hier analysierte NWA-Problem nur ein Aspekt der Reaktorsicherheit, und zum anderen könnte das hier verwendete Modell zur Unterschätzung der Wahrscheinlichkeit ungeplanter

Handlungen tendieren oder es sind - trotz systematischer Suche - wichtige Situationen, in denen ungeplante Handlungen auftreten könnten, nicht erkannt worden.

WILDE (1978) sieht in dem Vorhandensein menschlicher Risikobereitschaft die wesentliche Ursache in der Entstehung von Unfällen. Er schlägt daher Maßnahmen vor, die folgende Zielpunkte haben:

- vorsichtiges Verhalten: erwarteten Nutzen heraufsetzen, erwartete Kosten senken,
- riskantes Verhalten: erwarteten Nutzen senken, erwartete Kosten heraufsetzen.

Zur praktischen Umsetzung dieser Zielvorgaben existieren verschiedene Vorschläge, die sich auf die Bereiche Arbeits- und Verkehrssicherheit konzentrieren (z.B. SKIBA 1979; ZINK 1985). Eine Überprüfung dieser Vorschläge auf Anwendbarkeit in einem Kernkraftwerk (KKW) sowie deren Umsetzung würde m.E. zur Erhöhung der Sicherheit beitragen. Tab. 55 enthält hierzu einige Anregungen.

Ziel → Ebene ↓	VORSICHTIGES VERHALTEN: erwarteten Nutzen erhöhen, erwartete Kosten senken	RISKANTES VERHALTEN: erwarteten Nutzen senken, erwartete Kosten erhöhen
BEHÖRDLICH	• Nach kritischen Vorfällen: keine unnötigen Abschaltpausen, zügige Abwicklung der zur Wiederinbetriebnahme erforderlichen Untersuchungen. • Öffentlich loben (z.B. in der Presse), wenn bekannt wird, daß eine kritische Situation durch vorschriftsmäßiges Verhalten beherrscht wurde. • Evtl. vorhandene innerbetriebliche Maßnahmen (s.u.) zur Senkung der Risikobereitschaft öffentlich loben.	Wenn Verstöße gegen Sicherheitsbestimmungen aufgetreten sind: • Gründliche Untersuchung. • Durchführung innerbetrieblicher Maßnahmen zur Senkung der Risikobereitschaft anordnen.
TECHNISCH, ORGANISATORISCH	• Nachteilige Nebeneffekte vorsichtigen Verhaltens - wenn möglich - beseitigen. • Vorschriften so gestalten, daß sie einfach und einsichtig sind.	• Mechanische Hindernisse gegen aktive Eingriffe. • Formale Hindernisse gegen passives Fehlverhalten: Die Prozedur so gestalten, daß der Operateur die Notwendigkeit einer erforderlichen Maßnahme schriftlich protokollieren muß. Nachteil: Zeitverlust.
PERSONELL	• Lob, wenn vorsichtiges Verhalten beobachtet wird. • Keine Kritik, wenn vorsichtiges Verhalten unnötigerweise auftritt. • Den Operateuren klar machen, daß vorsichtiges Verhalten dem Ansehen der Kernenergie nutzt.	• Riskantes Verhalten immer kritisieren - auch wenn es schadlos bleibt. • Den Operateuren klar machen, daß auch bei schadlosem Verlauf einer riskanten Verhaltensweise mit einer längeren Abschaltpause (aufgrund behördlicher Auflagen) zu rechnen ist. • Den Operateuren klar machen, daß riskantes Verhalten dem Ansehen der Kernenergie schadet.

Tab. 55. Vorschläge zur Senkung der Risikobereitschaft von Operateuren:

Um einen langfristigen Erfolg zu erzielen, sind die Maßnahmen auf der personellen Ebene in regelmäßigen Abständen zu wiederholen.

Methodische Weiterentwicklungen

Die Einbeziehung ungeplanter Handlungen in eine PRA trägt zur Erhöhung ihrer Realitätsnähe bei. Dabei treten zwei Hauptschwierigkeiten auf: (1) die Identifizierung und (2) die Quantifizierung ungeplanter Handlungen.

Jede Methode zur Identifizierung von kritischen Situationen, in denen ungeplante Handlungen auftreten könnten, ist mit dem Problem der Vollständigkeit verbunden: Sind alle kritischen Situationen identifiziert worden? Diese Unsicherheit ist nie vollständig beseitigbar. Sie ist aber reduzierbar. Die hier erarbeitete Systematik zur Identifizierung von Situationen, in denen Konflikte oder Ähnlichkeiten zum Auftreten ungeplanter Handlungen führen könnten, ist ein erster Schritt in diese Richtung. Erweiterungen zu den in der Systematik vorgeschlagenen Checklisten zur Identifizierung von Zielen, die der Sicherheit untergeordnet sind, könnten die o.g. Unsicherheit noch weiter reduzieren.

Auch Befragungen von Operateuren liefern wertvolle Informationen. Man wird erstaunt sein, wenn man die vom Operateur genannten Handlungsziele mit den Handlungszielen vergleicht, die man ihm in der Analyse unterstellt hat.

Beispiel. Unter meiner Mitarbeit wird derzeit eine PSA für den Forschungsreaktor FRJ-2 erstellt. Wir, das PSA-Team, sind davon ausgegangen, daß das Personal nach einem Kühlmittelverlust als erstes die Leichtwassereinspeisung vorbereitet, für den Fall, daß die Kühlung mit Schwerwasser versagt. Eine Befragung ergab, daß folgende zwei Handlungsziele als erstes verfolgt werden: Ausschaltung des durch den Kühlmittelverlust ausgelösten akustischen Huptons (Reaktorunfallalarm) und Bergung von Personen, die sich evtl. noch in der Reaktorhalle befinden.

Die Quantifizierung menschlichen Verhaltens über die Verwendung von Fehlerwahrscheinlichkeiten ist in erster Linie ein Datenproblem. Wegen des Mangels situationsspezifischer Fehlerwahrscheinlichkeiten tritt das Datenproblem in nahezu jeder PRA auf. Es hängt vom individuellen Standpunkt ab, auf welchem situationsspezifischen Niveau man verfügbare Fehlerwahrscheinlichkeiten für aussagekräftig hält: Aus praktischer Sicht (eines PRA-Durchführers) wird man sich mit einem Niveau zufrieden geben, dem die Informationen "Was wurde falsch gemacht und wobei?" zu entnehmen sind. Aus psychologischer Sicht wird man weiter nach dem "Wie?" und "Warum?" fragen. Die Überbetonung der praktischen Sichtweise kann dazu führen, daß gewisse kognitive Mechanismen, wie z.B. Risikobereitschaft in Konfliktsituationen, nicht berücksichtigt werden. Die Überbetonung der psychologischen Sicht-

weise bedeutet, daß - mit den derzeit verfügbaren Fehlerdaten - keine PRA unter Einbeziehung menschlichen Verhaltens durchgeführt werden kann. Ein vernünftiger Ausweg aus diesem Dilemma liegt darin, daß man wichtige kognitive Mechanismen der Fehlerentstehung über Expertenschätzungen quantifiziert und hohe Streufaktoren verwendet. Dieser Weg entspricht der Grundkonzeption des SWAIN-Handbuchs.

Die Quantifizierung, d.h. die Schätzung von Wahrscheinlichkeiten, ist insbesondere für ungeplante Handlungen aufgrund menschlicher Risikobereitschaft in Konfliktsituationen ein schwieriges Problem. Da solches Fehlverhalten mit Schuldzuweisungen verbunden ist, ist die Aussicht auf situationsspezifische Fehlerdaten gering. Methoden, wie z.B. SLIM, die nach Einflußgrößen (PSFs) strukturierte Expertenschätzungen benutzen, kommt daher eine hohe Bedeutung zu. In der Weiterentwicklung solcher Methoden liegen m.E. ein aussichtsreicher Weg zur Einbeziehung wichtiger kognitiver Mechanismen, wie z.B. menschliche Risikobereitschaft, in eine PRA. Die Berücksichtigung von Abhängigkeiten zwischen den PSFs über den hier vorgeschlagenen Ansatz (Abschnitt 5.2.3.5, Gleichungen 17 und 18) stellt z.B. eine mögliche Weiterentwicklung dar. PRA-Durchführer, die Expertenschätzungen ablehnen, sollten bedenken, daß auch die Nichteinbeziehung bestimmter kognitiver Mechanismen, eine Expertenmeinung ist. Außerdem steht eine ablehnende Haltung gegenüber der Verwendung von Expertenschätzungen im Widerspruch zu der Verwendung der Datentabellen des SWAIN-Handbuchs. Dem Kapitel 6 des Handbuchs von 1983 ist zu entnehmen, daß nur wenige der tabellierten Fehlerwahrscheinlichkeiten mit empirischen Daten begründbar sind; die meisten Fehlerwahrscheinlichkeiten sind also Expertenschätzungen der Autoren des Handbuchs (häufiges Zitat: "we estimate ...").

Ein vielversprechender Ansatz zur Reduktion des Bedarfs an Expertenschätzungen bei Quantifizierung menschlicher Risikobereitschaft in Konfliktsituationen liegt in dem hier vorgestellten dynamischen Modell. Die Anwendbarkeit beschränkt sich auf passives Fehlverhalten: Unterlassung einer notwendigen geplanten Handlung. Mit diesem Modell wurde ein Teil des Handlungsablaufs zur Wiederherstellung der Nachwärmeabfuhr nach Ausfall der Dampferzeugerbespeisung im Kernkraftwerk Davis-Besse (1985) modelliert. Aufgrund dieser Modellierung war es möglich, Konflikte über geschätzte Zeitverzögerungen bei der Durchführung der kritischen Schritte des Handlungsablaufs einzubeziehen und die daraus resultierende erhöhte Wahrscheinlichkeit für die nicht rechtzeitige Durchführung des gesamten Handlungsablaufs zu berechnen. Bei dieser Vorgehensweise wird also Risikobereitschaft nicht über eine Fehlerwahrscheinlichkeit, sondern über eine Zeitverzögerung quantifiziert. Dadurch entstehen Vorteile bei der Datenbeschaffung; denn situationsspezifische

Zeitverzögerungen sind empirisch (Betriebserfahrung) und experimentell (Simulator) einfacher zu erheben als Fehler pro Gelegenheit. Aufgrund der "unscharfen" Fehlerdefinition bei der Modellierung von Konflikten über Zeitverzögerungen reduziert sich das Problem der Schuldzuweisung bei der Datenbeschaffung. Dem Operateur wird nicht unterstellt, daß er die Durchführung der geplanten Handlung regelwidrig unterläßt (binäre Logik), sondern daß er mit deren Durchführung "etwas" abwartet ("fuzzy logic"):

"Nun, das ist ein ganz schön drastischer Schritt und ich wollte warten bis ich -- nun, ich wollte es nicht frühzeitig tun. Ich wollte bis zu dem Punkt warten, an dem die Prozedur es vorschreibt."

(Aussage des Schichtleiters im KKW Davis-Besse zu seiner Entscheidung in Bezug auf das Einleiten der primärseitigen Kühlung; siehe Abschnitt 2).

8. Literaturverzeichnis

Apostolakis,G.E. / Kafka,P. / Mancini,G. (1988): "Summary of Panel Discussion at the International Seminar on Accident Sequence Modeling", Rel.Eng. & System Safety 22, p.1-3.

Becker,G.G. (1990): "Analysis of Human Behavior During NPP Incidents: A Case Study", IAEA-SM-315/39, International Symposium on Balancing Automation and Human Action in Nuclear Power Plants, IAEA & OECD Nuclear Energy Agency, München.

Bley,D.C. / Buttemer,D.R. / Stetkar,J.W. (1988): "Light Water Reactor Sequence Timing: its Significance to Probabilistic Safety Assessment Modeling", Rel.Eng. & System Safety 22, p.27-60.

Blindert,H.-P. (1988): "Untersuchungen zur passiven Nachwärmeabfuhr mittels Naturkonvektion im Primärkreislauf des Hochtemperatur-Reaktors am Beispiel des HTR-500", Interner Bericht, KFA-ISF-IB-3/88, Jülich.

Bubb,H. (1988): "System Ergonomics as an Approach to Improve Human Reliability", Nuclear Engineering and Design 110, p.233-245.

Bubb,H. (1990): "Zuverlässigkeit in technischen Systemen", in: Hoyos/Zimolong (1990).

Burkardt,F. (1985): "Unfallschwerpunktbezogene Verhaltensmodifikation", in: C.Graf Hoyos/G.Wenninger (Hg.): "Gefahrenbewußtsein und sicheres Handeln", Bericht Nr. 13, Lehrstuhl für Psychologie der Technischen Universität München, 1985.

Carnino,A. / Nicolet,J.-L. / Wanner,J.C. (1990): "Man and Risk. Technological and Human Risk Prevention", New York u. Basel: Dekker
(aus der Reihe "Occupational Safety and Health", Hg.: A.L.Kling).

Coombs,C.H. / Dawes,R.M. / Tversky,A. (1975): "Mathematische Psychologie", Weinheim und Basel: Beltz.

Dunn,J.G. (1972): "Subjective and Objective Risk Distribution", Occupational Psychology 46, p.183-187
(zit.n. Hoyos 1980, S.113).

Edwards,W. (1968): "Information Processing, Decision Making and Highway Safety", in: J.O'Day (Ed.): "Driver Behavior: Cause and Effect", Washington. D.C.: Insurance Institute for Highway Safety
(zit.n. Hoyos 1980, S.126).

Embrey,D.E. (1983): "The Use of Performance Shaping Factors and Quantified Expert Judgement in the Evaluation of Human Reliability: An Initial Appraisal", NUREG/CR-2986, Washington, D.C.

Embrey,D.E. / Humphreys,P.C. / Rosa,E.A. / Kirwan,B. / Rea,K. (1984): "SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement.

Vol.I: Overview of SLIM-MAUD.

Vol.II: Detailed Analysis of the Technical Issues",
NUREG/CR-3518, Washington, D.C.

Embrey,D.E. / Reason,J.T. (1986): "The Application of Cognitive Models to the Evaluation and Prediction of Human Reliability", Proceedings of the Internat. Topical Meeting on "Advances in Human Factors in Nuclear Power Systems", Knoxville, Tennessee.

Fell,J.C. (1976): "A Motor Vehicle Accident Causal System", Human Factors 18, p.85-94
(zit.n. Hoyos 1980, S.106).

Gertman,D.I. / Haney,L.N. / Jenkins,J.P. / Blackman,H.S. (1985): "Operational Decisionmaking and Action Selection Under Psychological Stress in Nuclear Power Plants", NUREG/CR-4040, Washington, D.C.

Gertman,D.I. / Blackman,H.S. / Haney,L.N. / Seidler,K.S. / Hahn,H.A. (1992): "INTENT: A Method for Estimating Human Error Probabilities for Decisionbased Errors", Rel.Eng. & System Safety 35, p.127-136.

Ghertman,F. / Dietz,P. (1985): "Human Error Data Collection Analysis Program Undertaken since 1982 by Electricite de France with INPO", ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications. San Francisco. Proceedings, Vol.2, Paper 89.

GRS (1979): "Deutsche Risikostudie Kernkraftwerke. Hauptband", Hg.: BMFT, Köln: Vlg. TÜV Rheinland.

GRS (1980): "Deutsche Risikostudie Kernkraftwerke. Fachband 3: Zuverlässigkeitskenngrößen und Betriebserfahrungen", Hg.: BMFT, Köln: Vlg. TÜV Rheinland.

GRS (1990): "Deutsche Risikostudie Kernkraftwerke, Phase B", Hg.: BMFT, Köln: Vlg. TÜV Rheinland.

Haas,P.M. / Bott,T.F. (1982): "Criteria for Safety Related Plant Operator Actions: A Preliminary Assessment of Available Data", Rel.Eng. 3, p.59-72.

Hacker,W. (1980): "Allgemeine Arbeits- und Ingenieurpsychologie", Berlin: VEB Deutscher Vlg. der Wissenschaften.

Hacker,W. (1986): "Arbeitspsychologie", Bern u.a.: Huber.

Häcker,H. (1980): "Persönlichkeit", in: R.Asanger/G.Wenninger (Hg.): "Handwörterbuch der Psychologie", S.324-330, Weinheim u. Basel: Beltz, 1980.

Hall,R.E. / Fragola,J. / Wreathall,J. (1982): "Post Event Human Decision Errors: Operating Action Tree / Time Reliability Correlation", NUREG/CR-3010, Washington, D.C.

Hannaman,G.W. / Worledge, D.H. (1988): "Some Developments in Human Reliability Analysis Approaches and Tools", Rel.Eng. & System Safety 22, p.235-257.

Hannaman,G.W. / Spurgin,A.J. / Lukic,Y.D. (1984): "Human Cognitive Reliability Model for PRA Analysis", Draft Report, NUS-4531, EPRI-RP-2170-3, Palo Alto, CA.

Hennings,W. (1987): "Methodik umfassender probabilistischer Sicherheitsanalysen für zukünftige HTR-Anlagenkonzepte. Ein Statusbericht. Band 1: Ereignisabläufe, Systemzuverlässigkeiten und Freisetzungshäufigkeiten", Jül-Spez-388/Bd.1, Jülich.

Hirschberg,S. (1990) (Hg.): "Dependencies, Human Interactions and Uncertainties in Probabilistic Safety Assessment", Final Report of the NKA Project RAS 470, Västerås, Sweden: ABB Atom AB Library, Prepared by: ABB Atom, Sweden, Risø National Laboratory, Denmark, Studsvik AB, Sweden, Technical Research Centre of Finland.

Holzkamp,K. (1988): "Thermohydraulische Untersuchungen zum Primärkreis eines HTR's für die Nachwärmeabfuhr mit Naturumlauf am Beispiel des HTR-500", Jül-2187, Jülich.

Hoyos,C.Graf (1980): "Psychologische Unfall- und Sicherheitsforschung", Stuttgart u.a.: Kohlhammer.

Hoyos,C.Graf / Zimolong,B. (1988): "Occupational Safety and Accident Prevention: Behavioral Strategies and Methods", Amsterdam u.a.: Elsevier (Vol.11 der Reihe "Advances in Human Factors/Ergonomics").

Hoyos,C.Graf / Zimolong,B. (1990) (Hg.): "Ingenieurpsychologie", in: C.F.Graumann u.a. (Hg.): "Enzyklopädie der Psychologie", Themenbereich D, Serie III, Bd.2, Göttingen u.a.: Vlg. für Psychologie Hogrefe, 1990.

HRB (1983): "HTR-500. Kernkraftwerk mit Hochtemperaturreaktor 500 MWel. Anlagen- und Sicherheitskonzept", Mannheim.

ISF (1984): "Sicherheitstechnische Untersuchungen zum Störfallverhalten des HTR-500. Ergänzungsband mit vertiefenden Einzelbeiträgen zum Bericht Jül-Spez-220", Jül-Spez-240, Jülich,
"Vorwort", J.Fassbender,
Kap.I. "System- und Ereignisablaufanalyse, Systemzuverlässigkeiten", S.3-52, J.Mertens, H.G. Mohr,
Kap.II. "Corethermodynamik", S.53-120, W.Jahn, M.Haben, W.Rehm,
Kap.III. "Verhalten von Komponenten des Primärkreises beim Coreaufheizstörfall", S.121-160, J.Altes,
Kap.IV. "Reaktivitätsverhalten des HTR-500", S.129-149, R.Nabbi,

Kap.V. "Graphitkorrosion durch Wasserdampf aus zersetztem Beton des Reaktor-druckbehälters bei unbegrenzter Coreaufheizung", S.151-160, W.Katscher, R.Moormann, R.Finken,
 Kap.VI. "Freisetzung von Spaltprodukten aus dem Core und aus dem Reaktordruck-behälter des HTR-500", S.161-186, K.Verfondern,
 Kap.VII. "RSG-Verhalten und Quellterme", S.187-198, G.Breitbach, P.H.David, K.Schwarzer,
 Kap.VIII. "Unfallfolgen und Risiko", S.199-217, W.Kröger, G.Degen.

ISF / GRS (1981): "Sicherheitsstudie für HTR-Konzepte unter deutschen Standortbe-dingungen", Jül-Spez-136/Bd.1, Jülich.

Jung,C.G. (1921): "Psychologie der Typen", Zürich: Rascher.

Kahneman,D. / Tversky,A. (1979): "Prospect Theory: An Analysis of Decision Under Risk", Econometrica 47, p.263-291.

Kirchner,U. (1991): "Der Hochtemperaturreaktor. Konflikte, Interessen, Entschei-dungen", Frankfurt a.M. u. New York: Campus.

Kröger,W. / Chakraborty,S. (1989): "Tschernobyl und weltweite Konsequenzen", Köln: Vlg. TÜV Rheinland.

Kugeler,K. / Schulten,R. (1989): "Hochtemperaturreaktortechnik", Heidelberg: Springer.

Lewis,H.W. u.a. (1978): "Risk Assessment Review Group Report to the USNRC", NUREG/CR-0400, Washington, D.C.

Luce,R.D. (1959): "Individual Choice Behavior", New York, Reprress: Westport, Conn.: Greenwood Press.

Marbe,K. (1926): "Praktische Psychologie der Unfälle und Betriebsschäden", Mün-chen und Berlin: Oldenbourg
 (zit.n. Hacker 1980, S.355).

Marek,J. / Sten,T. (1977): "Traffic Environment and the Driver", Springfield, Illinois: Thomas
 (zit.n. Hoyos 1980, S.175).

Mittenecker,E. (1972): "Methoden und Ergebnisse der psychologischen Unfallfor-schung", Wien: Deuticke
 (zit.n. Hoyos 1980, S.117).

Miller,G.A. / Galanter,E. / Pibram,K.-H. (1960): "Plans in the Structur of Behavior", New York: Holt, Rinehart & Winston.

NRC (1983): "PRA Procedures Guide. Final Report", Vol.1, NUREG/CR-2300, Washington, D.C.

NRC (1985): "Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985", NUREG-1154, Washington, D.C.

NRC (1987): "Reactor Risk Reference Document. Vol.1: Main Report. Draft for Comment", NUREG-1150, Washington, D.C.

Peters,G.A. (1966): "Human Error, Analysis, and Control", A.S.S.E. Journal XI, p.9-15 (zit.n. Hoyos 1980, S.103).

Peters,O.H. / Meyna,A. (1985) (Hg.): "Handbuch der Sicherheitstechnik", Bd.1&2, München und Wien: Carl Hanser.

Potash,L.M. / Stewart,M. / Dietz,P.E. / Lewis,C.M. / Dougherty,E.M. jr. (1981): "Experience in Integrating the Operator Contribution in the PRA of Actual Operating Plants", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, PM Session VI-A, Port Chester, N.Y.

PRA-Leitfaden: s. NRC (1983).

Radl,G.W. / Tietze,A. (1976): "Zur systematischen Bewertung der Sicherheit bei ergonomischen Fragestellungen", in: "Praktische Anwendung der Ergonomie in industriellen Prozessen", ZFU-Kolloquium des TÜV Rheinland, S.85-116, Köln: Vlg. TÜV Rheinland.

Rasmussen,J. (1979): "On the Stucture of Knowledge - A Morphology of Mental Models in a Man-Machine Context", Risø-M-2192, Risø National Laboratory, Roskilde.

Rasmussen,J. (1983): "Skills, Rules, Knowledge, Signals, Signs, and Symbols, and other other Distinctions in Human Performance Models", IEEE Transactions on Systems, Man, and Cybernetics, 13, p.266-275 (zit. n. Hoyos/Zimolong 1988, p.114).

Rasmussen,J. (1988): "Human Error Mechanisms in Complex Work Environments", Rel.Eng. & System Safety 22, p.155-167.

Reason,J. (1988): "Modelling the Basic Error Tendencies of Human Operators", Rel.Eng. & System Safety 22, p.137-153.

Reason,J. (1990): "Human Error", Cambridge u.a.: Cambridge University Press.

Reer,B.: "Dynamische Analysemethode für Operateurhandlungen (DAO)", Interner Bericht, Jülich (in Vorbereitung).

Rehhahn,H. (1973): "Ergebnisse einer Fehlverhaltensuntersuchung zur Verbesserung der Arbeitssicherheit", Arbeit und Leben, Nr. 3, S.44-47.

Rehhahn,H. (1973p): Persönliche Mitteilung an R.Skiba
(zit. in Skiba 1979, S.310).

Reinartz,S.J. / Reinartz,G. / Heyden,W. / Liere,B. (1986): "Verhalten des Kernkraftwerk-Wartenpersonals. Band I: Schlußbericht", Köln: Vlg. TÜV Rheinland.

Ryan,Th.A. / Smith,P.C. (1954): "Principles of Industrial Psychology", New York: Ronald Press
(zit.n. Hoyos 1980).

Sabri,Z.A. / Husseiny,A.A. / Casto,W. (1981): "Assessment of Human Contribution to Significant Trends Based on LWR Past Operating Experience", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, PM Session VI-A, Port Chester, N.Y.

Schaarschmidt,U. (1971): "Zur eignungsdiagnostischen Valenz von Komponenten des Entscheidungsverhaltens bei Arbeiten mit Risikoanteil", in: F.Klix (Hg.): "Psychologie in der sozialistischen Industrie", Berlin: VEB Deutscher Vlg. der Wissenschaften
(zit.n. Hoyos 1980, S.127).

Shealy,J.E. (1975): "Risk Taking in Skilled Task Performance: Effects of Control and Need for Achievement", Phil. Dissertation, University of N.Y. at Buffalo
(zit.n. Hoyos 1980, S.130).

Skiba,R. (1979): "Taschenbuch Arbeitssicherheit", 4. Aufl., Bielefeld: E.Schmidt.

Slovic,P. / Fischhoff,B. / Lichtenstein,S. / Corrigan,B. / Combs,B. (1977): "Preference for Insuring Against Probable Small Losses: Insurance Implications", Journal of Risk and Insurance 44, p.237-258.

Smidt,D. (1979): "Reaktorsicherheitstechnik", Berlin u.a.: Springer.

Stampelos,J.G. / Apostolakis,G. (1985): "A Methodology for the Analysis of Dynamic Human Actions", ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications. San Francisco. Proceedings, Vol.2, Paper 93.

Surry,J. (1969): "Industrial Accident Research: A Human Engineering Appraisal", Toronto: Labour Safety Concil Ontario, Ministry of Labour
(zit.n. Hoyos 1980, S.84).

Swain (1980): s. Swain/Guttman (1980).

Swain (1983): s. Swain/Guttman (1983).

Swain,A.D. (1989): "Comparative Evaluation of Methods for Human Reliability Analysis", GRS-71, Köln u. Garching: GRS.

Swain-Handbuch: s. Swain/Guttmann.

Swain,A.D. / Guttmann,H.E. (1980): "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Draft Report", NUREG/CR-1278, Washington, D.C.

Swain,A.D. / Guttmann,H.E. (1983): "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report", NUREG/CR-1278, Washington, D.C.

Swain,A.D. / Weston,L.M. (1988): "An Approach to the Diagnosis and Misdiagnosis of Abnormal Conditions in Post-Accident Sequences in Complex Man-Machine Systems", in: L.P.Goodstein/H.Anderson/S.Olson (Hg.): "Task, Errors and Mental Models", London u. New York: Taylor & Francis, 1988.

UKAEA (1987): "The Chernobyl Accident and its Consequences", United Kingdom Atomic Energy Authority, London: H.M.S.O.
(zit.n. Reason 1990, p.213).

Undeutsch,U. (1985): "Sicherheitspsychologie", in: Peters/Meyna (1985, Bd.2, S.130-156).

von Klebelsberg,D. (1977): "Das Modell der subjektiven und objektiven Sicherheit", Schweizerische Zeitschrift für Psychologie und ihre Anwendungen, 36, S.285-294.

von Winterfeldt,D. / Edwards,W. (1986): "Decision Analysis And Behavioral Research", Camebridge u.a.: Camebridge University Press.

Wakefield,D.J. (1988): "Application of the Human Cognitive Reliability Model and Confusion Matrix Approach in a Probabilistic Risk Assessment", Rel.Eng. & System Safety 22, p.295-312.

Wakefield,D.J. / Adams,C.D. (1987): "Quantification of Dynamic Errors in the TMI-1 PRA", in: ENS/SNS (Hg.): "Probabilistic Safety Assessment and Risk Management. PSA'87", Köln: Vlg. TÜV Rheinland, 1987.

WASH-1400 (1975): "Reactor Safety Study. An Assessment of Accidents Risks in U.S. Comercial Nuclear Power Plants", NUREG-75/014, Washington, D.C.

Wechsler,D. (1952): "Range of Human Capacities", Baltimore: Williams & Wilkins Co.
(zit.n. Swain 1983, ch.7).

Wehner,T. / Mehl,K. (1986): "Über das Verhältnis von Handlungsteilen zum Handlungsganzen - Der Fehler als Indikator unterschiedlicher Bindungsstärken in 'Automatismen'", Zeitschrift für Psychologie 194, S.231-245.

Weimer,H. (1925): "Psychologie der Fehler", Leipzig: Klinckhardt.

Wilde,G.J.S. (1978): "Theorie der Risikokompensation der Unfallverursachung und praktische Folgerungen für die Unfallverhütung", Hefte zur Unfallheilkunde, Heft 130, S.134-156.

Williams,J.C. (1988): "A Data-Based Method For Assessing And Reducing Human Error to Improve Operational Performance", in: "Proceedings of the IEEE conference on Human Factors and Power Plants", Monterey, CA, p.436-450.

Woods,D.D. / Roth,E. / Pople,H. jr. (1987): "Cognitive Environment Simulations: An Artificial Intelligence System for Human Performance Assessment. Vol.2: Modeling Human Intention Formation", NUREG/CR-4862, Washington, D.C.

Woods,D.D. / Roth,E. (1987): "Cognitive Environment Simulations: An Artificial Intelligence System for Human Performance Assessment. Vol.3: Cognitive Reliability Analysis Technique", NUREG/CR-4862, Washington, D.C.

Woods,D.D. / Roth,E. / Pople,H. jr. (1988): "Modeling Human Intention Formation for Human Reliability Assessment", Rel.Eng. & System Safety 22, p.169-200.

Woods,D.D. / Roth,E. / Pople,H. jr. (1990): "The Cognitive Environment Simulation as Tool for Modeling Human Performance", Main Report, NUREG/CR-5213, Vol.2, Washington, D.C.

Zimolong,B. (1990): "Fehler und Zuverlässigkeit", in: Hoyos/Zimolong (1990).

Zink,K.J. (1985): "Verhaltensorientierte Maßnahmen zur Förderung der Arbeitssicherheit", in: Peters/Meyna (1985, Bd.2, S.202-224).

Anhang A: BMFT-Forschungsvorhaben zur Erweiterung der PRA-Zielsetzung. Kurzbeschreibung

Das Vorhaben erweitert systematisch die Methodik probabilistischer Sicherheits/Risikoanalysen (PSA/PRA), mit denen in den nächsten Jahren aktuelle HTR-Konzepte planungsbegleitend auf homogene Sicherheitskonzepte und ausreichend kleines Risiko überprüft werden sollen. Dazu wird der radiologisch orientierte Bewertungsansatz durch weitere Aspekte ergänzt:

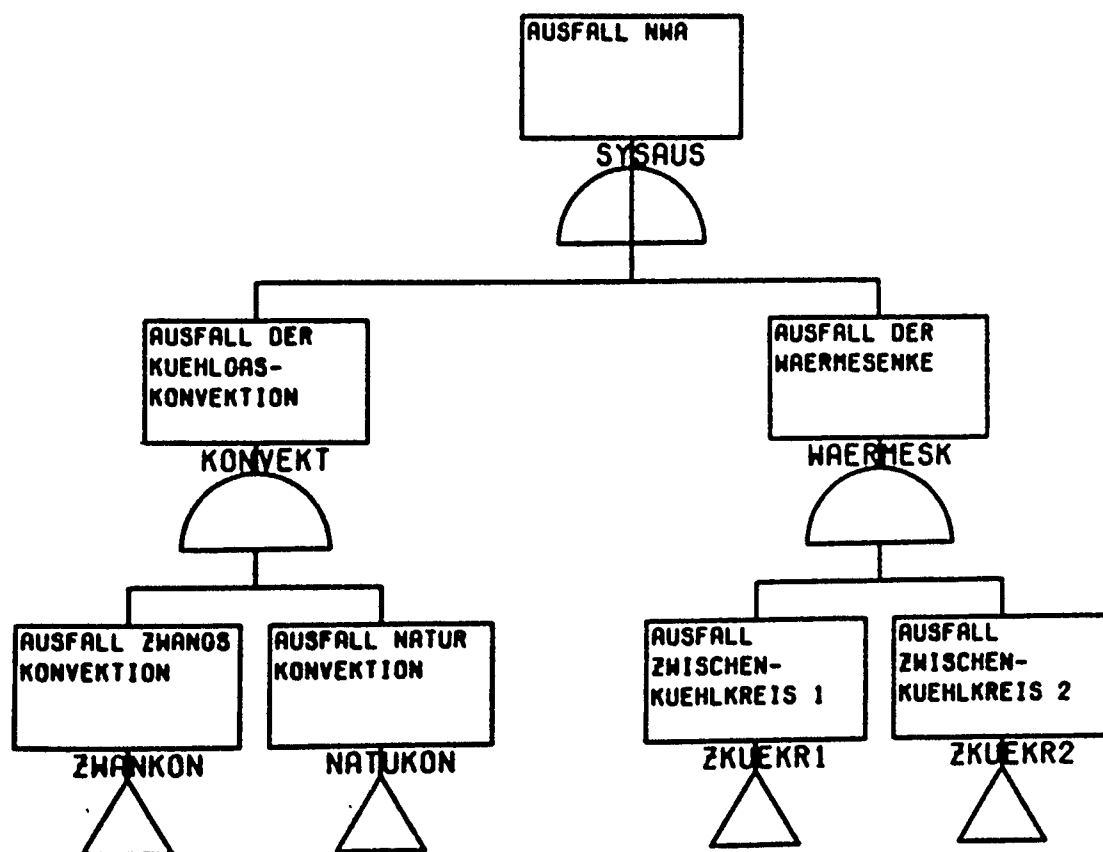
1. Einbeziehung potentieller Konflikte zwischen den Zielen "Anlagenverfügbarkeit - Anlagen/Komponentenschonung - Vermeidung radiologischer Freisetzungen" bei Entscheidungen des Personals.
2. Erweiterung der Ereignisablaufdiagramme um daraus resultierende neue Abfragen und Teilfunktionen; Analyse von Störungen, die durch betriebsorientierte Personalhandlungen zu Störfällen führen können.
3. Erweiterung der Versagensmodelle für Komponenten um Belastungen aufgrund der Zielkonflikte.

Das Vorhaben sichert die Aussagen 'klassischer' PSA/PRA-Analysen ab, verbessert den Vollständigkeitsnachweis und schafft Voraussetzungen zur Quantifizierung des Risikos eines störungs/störfallbedingten Anlagenverlustes.

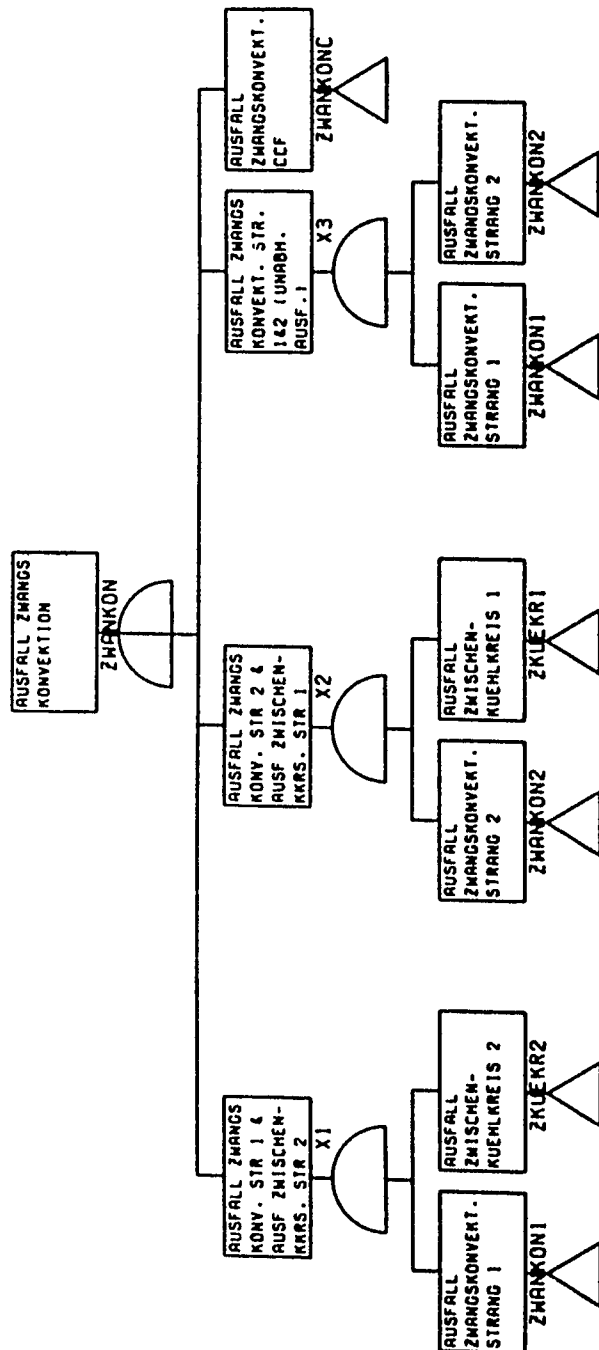
(Kennziffer 03 THA 202)

Anhang B: HTR-500. NWA-System. Fehlerbäume aus ISF (1984)

Hauptfehlerbaum: Ausfall NWA

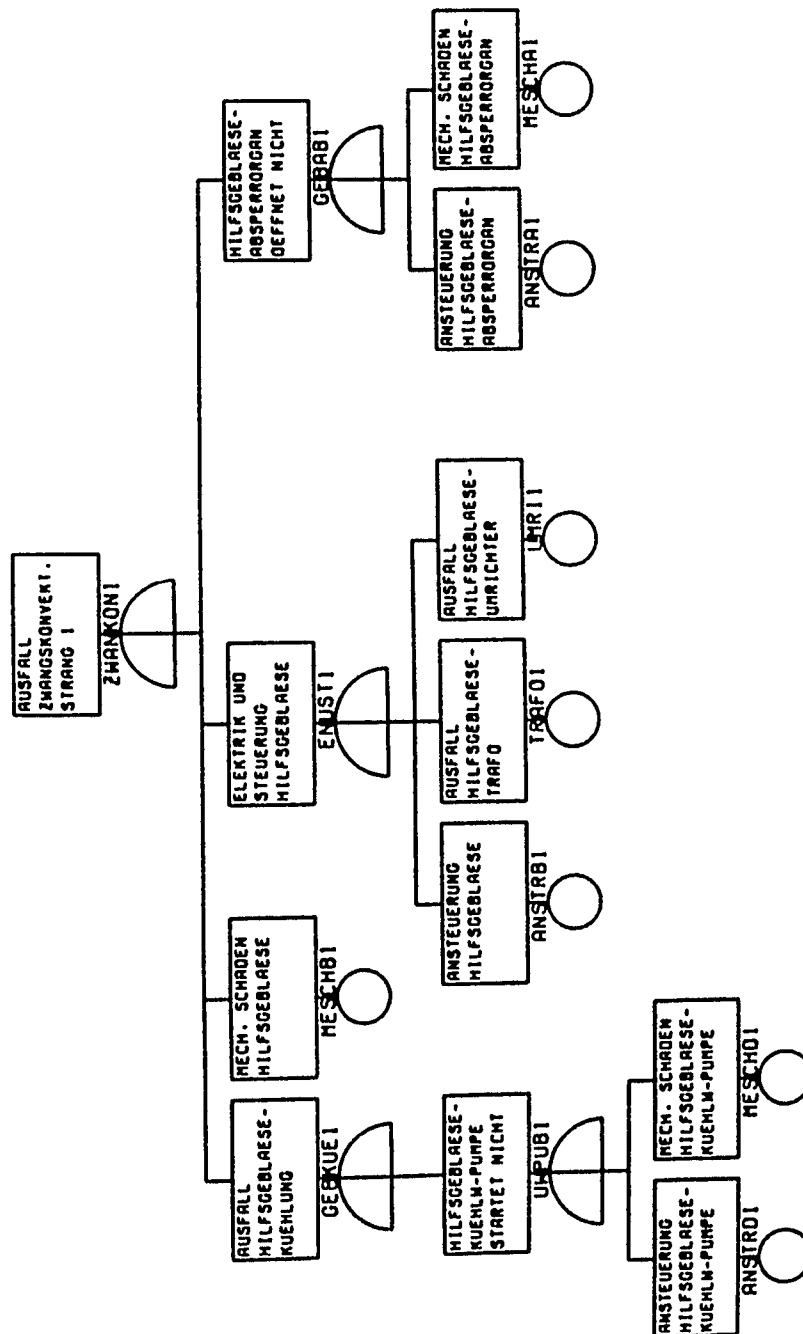


Unterfehlerbaum 1: Ausfall Zwangskonvektion

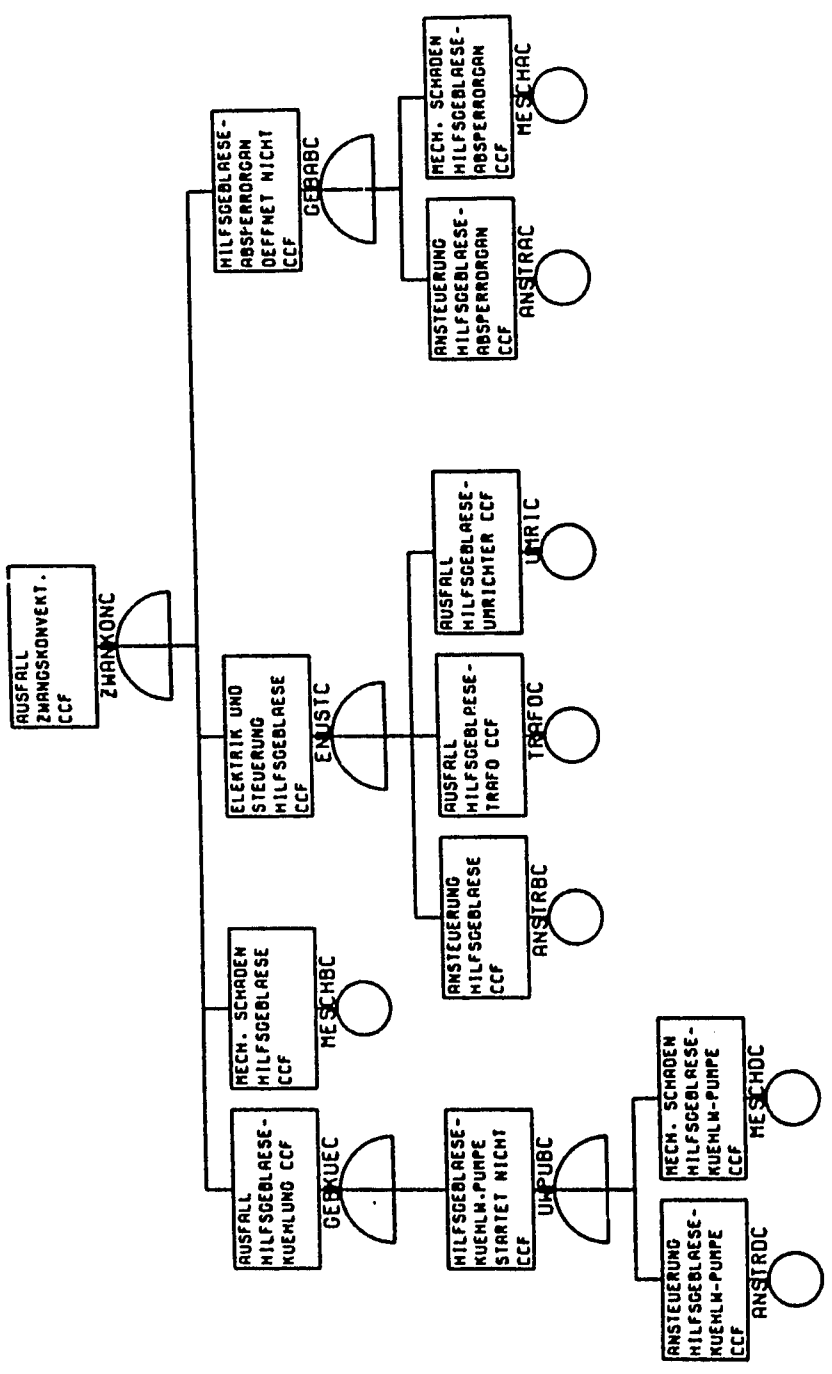


Unterfehlerbaum 1.1: Ausfall Zwangskonvektion Strang 1

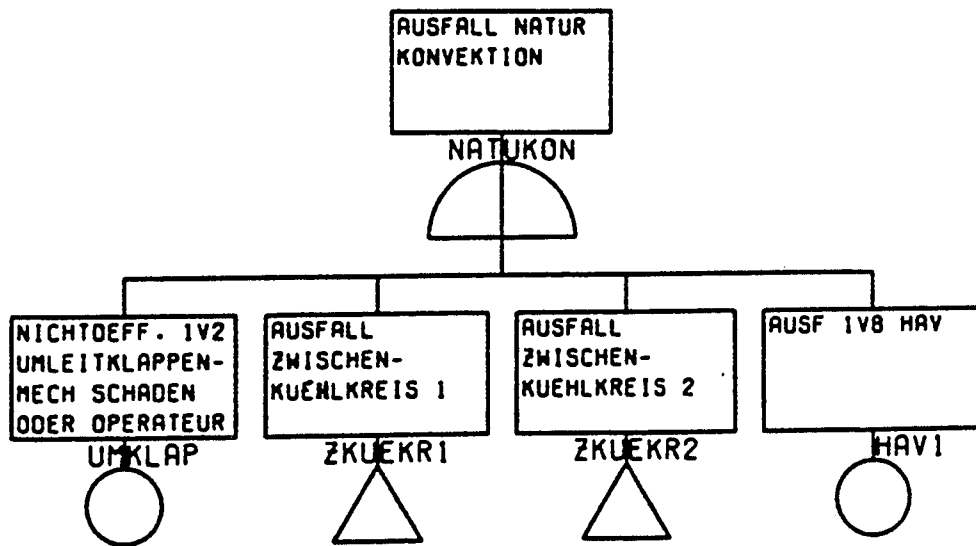
Für Strang 2 gilt eine dem entsprechende Struktur.



Unterfehlerbaum 1.2: Ausfall Zwangskonvektion CCF

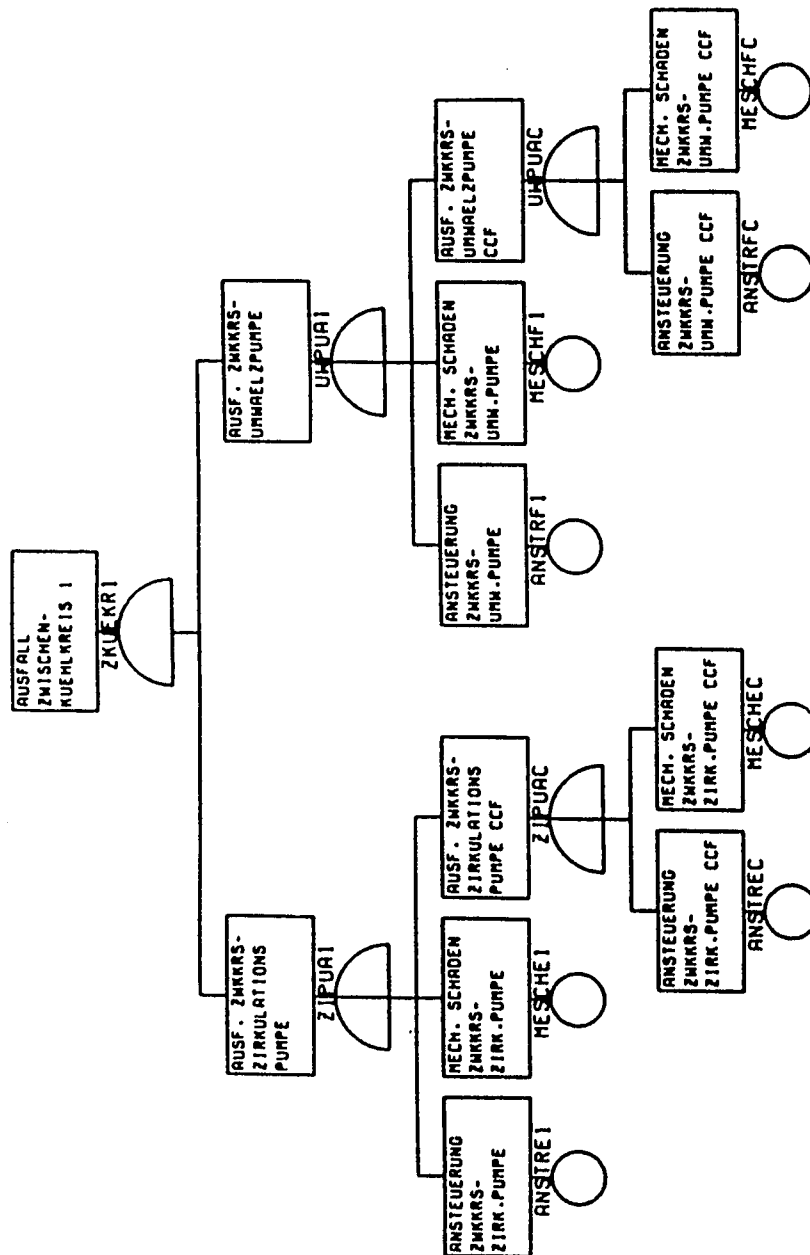


Unterfehlerbaum 2: Ausfall Naturkonvektion



Unterfehlerbaum 2.1 und 1.3: Ausfall Zwischenkühlkreislauf 1

Der Fehlerbaum wird als Eingang für die Unterfehlerbäume 1 und 2 verwendet.
Für Kreislauf 2 gilt eine dem entsprechende Struktur.



Anhang C: HTR-500. Passive NWA per Naturkonvektion. Hypothetische Prozedur

ANWENDUNGSZEITRAUM: Innerhalb der ersten 30 min nach NWA-Ausfall

ANWENDUNGSFALL:

- beide NWA-Wärmetauscher gekühlt UND alle 8 Hauptabsperrrklappen geschlossen
ABER
- aktive Kühlgasumwälzung (per Gebläse) ausgefallen

MASSNAHMEN:

- Überprüfen, ob beide Absperrrorgane der NWA-Gebläse geschlossen.
Ggfs. schließen.
- Verriegelung der Bypassorgane an den NWA-Gebläsen aufheben.
- Beide Bypassorgane öffnen.
- Überprüfen, ob die normale Strömungsrichtung im Primärkreis beibehalten wird.

Anhang D: HTR-500. Querverbindung zur Gebläsekühlung. Hypothetische Prozedur

ANWENDUNGSFALL:

Ausfall

Gebläsekühlung Strang 1 UND Kühlgasumwälzung Strang 2

ODER

Gebläsekühlung Strang 2 UND Kühlgasumwälzung Strang 1

MASSNAHMEN (vgl. Abb. 25):

- Aktive Komponenten im AUSGEFALLENEN Gebläsekühlstrang außer Betrieb nehmen.
- Pumpenisolationsarmatur (A-Pi) und Wärmetauscherisolationsarmatur (A-Wi) (vor Ort) im AUSGEFALLENEN Strang schließen.
- Pumpenquerverbindungsarmatur (A-Pq) und Wärmetauscherquerverbindungsarmatur (A-Wq) (vor Ort) im FUNKTIONIERENDEN Strang öffnen.
- Pumpenisolationsarmatur (A-Pi) und Wärmetauscherisolationsarmatur (A-Wi) (vor Ort) im FUNKTIONIERENDEN Strang schließen.
- Überprüfen, ob Bypassorgan am noch nicht angeforderten NWA-Gebläse geschlossen. Ggfs. schließen.
- NWA-Gebläse starten

STRANG 1

STRANG 2

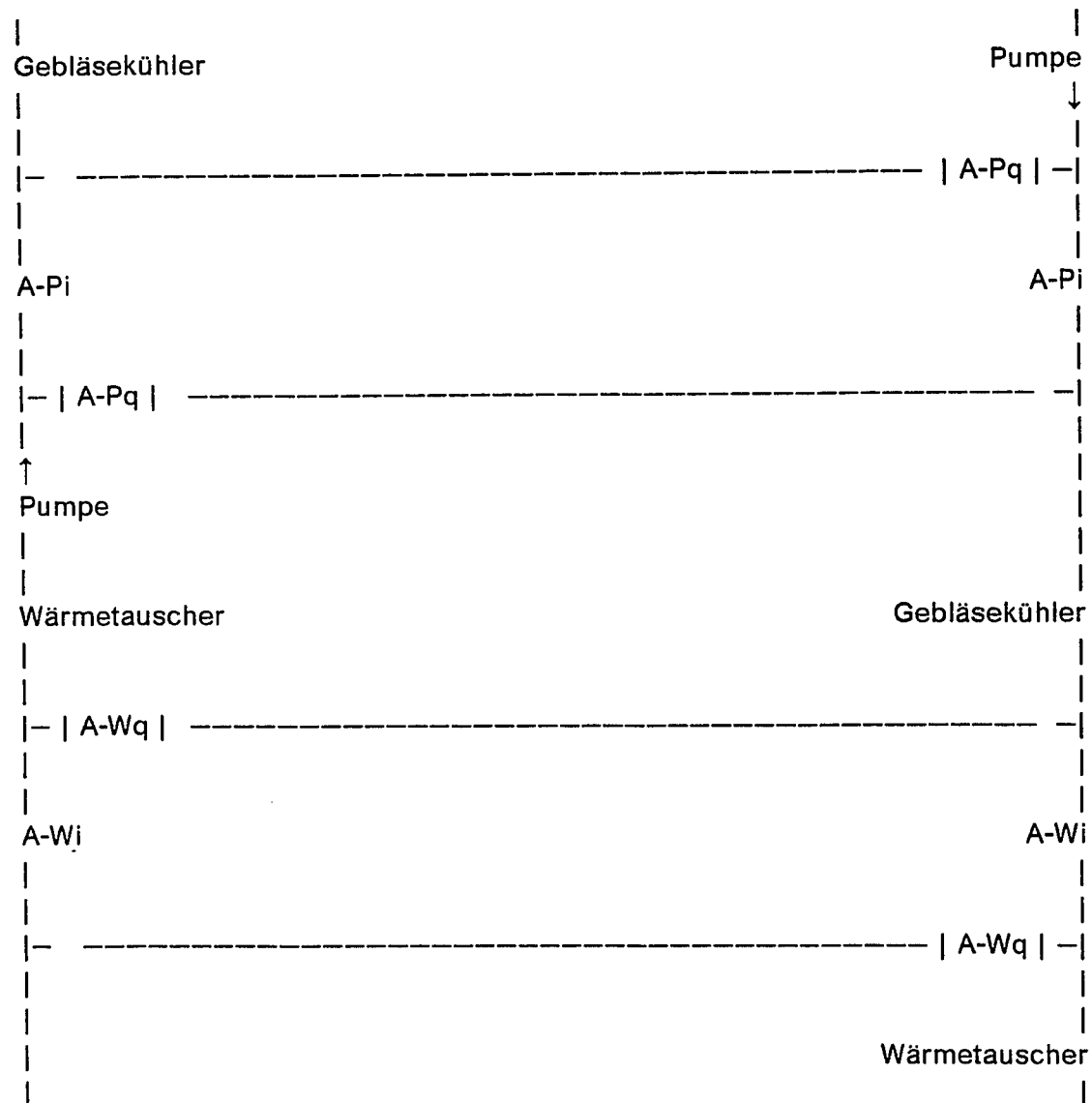


Abb. 25. Gebläsekühlung mit hypothetischer Querverbindungsmöglichkeit

Anhang E: Basisfehlerwahrscheinlichkeiten

In der folgende Tabelle sind fast alle wesentlichen Basisfehlerwahrscheinlichkeiten aus dem SWAIN-Handbuch (1983) zusammengefaßt. Weitere Fehlerwahrscheinlichkeiten können z.B. Tab. 57 entnommen werden.

ID	BHEP < UF >	Fehler, Randbedingung(en)	Zitat ⁰
1.0001	1.0	1. Nicht richtige Diagnose* des Störfalls. 1 min verfügbar.	T.20-3(1)
1.0010	0.1 < 10 >	10 min verfügbar	T.20-3(2)
1.0020	0.01 < 10 >	20 min verfügbar	T.20-3(3)
1.0030	0.001 < 10 >	30 min verfügbar	T.20-3(4)
1.0060	0.0001 < 30 >	60 min verfügbar	T.20-3(5)
1.1500	0.00001 < 30 >	1500 min verfügbar	T.20-3(6)
		2. Wahrnehmungsfehler. 2.1 Quantitative Informationen (z.B. konkreter Meßwert).	
2.11	0.05 < 5 >	Druckaufzeichner mit vielen Parametern	T.20-10(4)
2.12	0.01 < 3 >	Graphische Darstellung	T.20-10(5)
2.13	0.006 < 3 >	Blattschreiber	T.20-10(3)
2.14	0.003 < 3 >	Analoganzeige	T.20-10(1)
2.15	0.001 < 3 >	Digitalanzeige mit weniger als 5 Stellen	T.20-10(2)
		2.2 Qualitative Informationen (z.B. Grenzwert-überschreitung).	
2.2111	0.006 < 3 >	Blattschreiber ohne Grenzwertlinien. Gezieltes Beobachten	T.20-11(6)
2.2112	0.3 < 5 >	Blattschreiber ohne Grenzwertlinien. Eher zufälliges Beobachten beim 1. Wartenrundgang nach Schichtübernahme	T.20-25(4a) T.20-20(3)
2.2121	0.002 < 3 >	Blattschreiber mit Grenzwertlinien. Gezieltes Beobachten	T.20-11(5)
2.2122	0.1 < 5 >	Blattschreiber mit Grenzwertlinien. Eher zufälliges Beobachten beim 1. Wartenrundgang nach Schichtübernahme	T.20-25(3a) T.20-20(3)
2.2211	0.003 < 3 >	Analoganzeige ohne Grenzwertlinien. Gezieltes Beobachten	T.20-11(4)
2.2212	0.15 < 5 >	Analoganzeige ohne Grenzwertlinien. Eher zufälliges Beobachten beim 1. Wartenrundgang nach Schichtübernahme	T.20-25(2a) T.20-20(3)
2.2221	0.001 < 3 >	Analoganzeige mit Grenzwertlinien. Gezieltes Beobachten	T.20-11(2)
2.2222	0.05 < 5 >	Analoganzeige mit Grenzwertlinien. Eher zufälliges Beobachten beim 1. Wartenrundgang nach Schichtübernahme	T.20-25(1a) T.20-20(3)
2.2301	0.001 < 3 >	Digitalanzeige. Gezieltes Beobachten	T.20-11(1)
2.2302	0.98 < 5 >	Digitalanzeige. Eher zufälliges Beobachten beim 1. Wartenrundgang nach Schichtübernahme	T.20-25(6a) T.20-20(3)
2.2401	≈ 0	Anzeigelampe nicht richtig interpretiert. Gezieltes Beobachten	T.20-11(7)

ID	BHEP < UF >	Fehler, Randbedingung(en)	Zitat ⁰
2.2402	0.99 < 5 >	Anzeigelampe nicht richtig interpretiert. Eher zufälliges Beobachten beim 1. Wartenrundgang nach Schichtübernahme	T.20-25(7a) T.20-20(3)
2.2403	0.001 < 3 >	Anzeigelampe nicht richtig interpretiert. Gezieltes Beobachten unter Stress	T.20-11(7)
2.2501	0.0001 < 10 >	Nicht reagiert auf 1. hörbaren Alarm	T.20-23(1)
2.2502	0.001 < 10 >	Nicht reagiert auf 2. hörbaren Alarm**	T.20-23(2)
2.2503	0.002 < 10 >	Nicht reagiert auf 3. hörbaren Alarm**	T.20-23(3)
2.2504	0.004 < 10 >	Nicht reagiert auf 4. hörbaren Alarm**	T.20-23(4)
2.2505	0.008 < 10 >	Nicht reagiert auf 5. hörbaren Alarm**	T.20-23(5)
2.2506	0.016 < 10 >	Nicht reagiert auf 6. hörbaren Alarm**	T.20-23(6)
2.2507	0.032 < 10 >	Nicht reagiert auf 7. hörbaren Alarm**	T.20-23(7)
2.2508	0.064 < 10 >	Nicht reagiert auf 8. hörbaren Alarm**	T.20-23(8)
2.2509	0.13 < 10 >	Nicht reagiert auf 9. hörbaren Alarm**	T.20-23(9)
2.2510	0.25 < 10 >	Nicht reagiert auf 10. hörbaren Alarm** und alle weiteren	T.20-23(10)
2.26	0.1 < 5 >	Falschanzeige nicht als falsch erkannt, obwohl sie durch Kontrolle ("cross check") anderer Anzeigen als falsch erkennbar ist	T.20-10(7)
3.111	0.01 < 3 >	3. Unterlassung eines Schritts (= Wahrnehmungseinheit). 3.1 Schriftliche Prozedur. Lang (> 10 Schritte). Checkliste: nicht vorhanden, falsch benutzt oder garnicht benutzt	T.20-7(4)
3.112	0.003 < 3 >	Lang (> 10 Schritte). Checkliste: vorhanden und richtig benutzt	T.20-7(2)
3.121	0.003 < 3 >	Kurz (≤ 10 Schritte). Checkliste: nicht vorhanden, falsch benutzt oder garnicht benutzt	T.20-7(3)
3.122	0.001 < 3 >	Kurz (≤ 10 Schritte). Checkliste: vorhanden und richtig benutzt	T.20-7(1)
3.13	0.05 < 5 >	Wenn vorgesehene schriftliche Unterlage nicht benutzt wird	T.20-7(5)
3.211	0.001 < 3 >	3.21 Mündliche Anweisung. Genau gehalten. 1. Schritt	T.20-8(1a)
3.212	0.003 < 3 >	2. Schritt	T.20-8(2a)
3.213	0.01 < 3 >	3. Schritt	T.20-8(3a)
3.214	0.03 < 5 >	4. Schritt	T.20-8(4a)
3.215	0.1 < 5 >	5. Schritt	T.20-8(5a)
3.221	0.001 < 3 >	3.22 Mündliche Anweisung. Ungenau gehalten. 1. Schritt	T.20-8(1b)
3.222	0.006 < 3 >	2. Schritt	T.20-8(2b)
3.223	0.02 < 3 >	3. Schritt	T.20-8(3b)
3.224	0.06 < 5 >	4. Schritt	T.20-8(4b)
3.225	0.2 < 5 >	5. Schritt	T.20-8(5b)

ID	BHEP <UF>	Fehler, Randbedingung(en)	Zitat ⁰
4.1112	0.001 <3>	4. Verwechslungsfehler. 4.1 Vor Ort nicht das richtige Ventil betätigt. 4.11 Klar und eindeutig gekennzeichnet. Abseits einer Gruppe benachbarter Ventile. Ähnlich bezüglich Größe, Gestalt UND Zustand (auf/zu)	T.20-13(1)
4.1121	0.003 <3>	Teil einer Gruppe benachbarter Ventile. Ähnlich bezüglich Größe, Gestalt ODER Zustand (auf/zu)	T.20-13(2)
4.1212	0.005 <3>	4.12 Unklar oder zweideutig gekennzeichnet. Abseits einer Gruppe benachbarter Ventile. Ähnlich bezüglich Größe, Gestalt UND Zustand (auf/zu)	T.20-13(3)
4.1221	0.008 <3>	Teil einer Gruppe benachbarter Ventile. Ähnlich bezüglich Größe, Gestalt ODER Zustand (auf/zu)	T.20-13(4)
4.1222	0.01 <3>	Teil einer Gruppe benachbarter Ventile. Ähnlich bezüglich Größe, Gestalt UND Zustand (auf/zu)	T.20-13(5)
4.211	0.003 <3>	4.21 Nicht den richtigen Schalter (auf einem Schaltpult) betätigt. Von benachbarten Schaltern nur durch Aufschrift unterscheidbar	T.20-12(1)
4.212	0.001 <3>	Benachbarte Schalter in funktionellen Gruppen angeordnet	T.20-12(2)
4.213	0.0005 <10>	Benachbarte Schalter in Flußdiagramm integriert	T.20-12(3)
4.221	0.005 <3>	4.22 Nicht den richtigen Trennschalter (Stromunterbrecher im Schaltschrank) betätigt. Benachbarte Trennschalter dicht angeordnet	T.20-12(11)
4.222	0.003 <3>	Benachbarte Trennschalter weniger dicht angeordnet. Gut beleuchtet	T.20-12(12)
4.311	0.0005 <10>	4.3 Drehschalter (mit mehr als 2 möglichen Positionen)*** nicht richtig positioniert. Funktionsweise entspricht gewohnheitsmäßigem Empfinden	T.20-12(5)
4.321	0.05 <5>	Funktionsweise widerspricht gewohnheitsmäßigem Empfinden	T.20-12(6)
4.322	0.5 <5>	Funktionsweise widerspricht gewohnheitsmäßigem Empfinden. Betätigung unter Stress	T.20-12(7)
4.41	≈ 0	4.4 Nicht die richtige Anzeigevorrichtung beobachtet. Benachbarten Anzeigevorrichtungen unähnlich	T.20-9(1)
4.421	0.0005 <10>	Benachbarten Anzeigevorrichtungen ähnlich. Unterscheidbar durch deutliche Begrenzungslinien	T.20-9(2)
4.422	0.001 <3>	Benachbarten Anzeigevorrichtungen ähnlich. In funktionellen Gruppen angeordnet	T.20-9(3)
4.423	0.003 <3>	Benachbarten Anzeigevorrichtungen ähnlich. Nur durch Aufschrift unterscheidbar	T.20-9(4)
5.1	0.01 <5>	5. Verhaltensfehler. Vorgeschriebene Verhaltensweise nicht eingehalten	T.20-6(1)
5.2	0.5 <5>	Checkliste nicht oder nicht richtig benutzt	T.20-6(8)

ID	BHEP < UF >	Fehler, Randbedingung(en)	Zitat ⁰
		5.3 Prozedur ohne Benutzung der vorgesehenen schriftlichen Unterlage durchgeführt.	
5.311	0.01 < 3 >	Tätigkeit des Wartenpersonals. Normalbetrieb	T.20-6(3)
5.312	0.005 < 10 >	Tätigkeit des Wartenpersonals. Störfall	T.20-6(4)
5.32	0.01 < 3 >	Arbeit an Ventilen	T.20-6(5)
5.33	0.05 < 5 >	Funktionstest, Kalibrierung	T.20-6(6)
5.34	0.3 < 5 >	Wartung	T.20-6(7)
		6. Fehlerkorrektur erfolglos.	
		6.1 Normalbetrieb (abhängige und unabhängige Fehler).	
6.111	0.1 < 5 >	Routinekontrolle. Mit schriftlicher Unterlage	T.20-22(1)
6.112	0.2 < 5 >	Routinekontrolle. Ohne schriftliche Unterlage	T.20-22(2)
6.12	0.5 < 5 >	2., zusätzliche Routinekontrolle	T.20-22(8)
6.13	0.05 < 5 >	Nicht alltägliche Kontrolle mit besonderer Aufmerksamkeit	T.20-22(3)
6.14	0.01 < 5 >	Mit aktiver Tätigkeit verbundene Kontrolle	T.20-22(4)
6.14	0.001 < 5 >	Nicht entdeckter Fehler = Lebensgefahr	T.20-22(9)
		6.2 Störfall (nur abhängige Fehler).	
6.21	0	Keine Abhängigkeit (ZD)	App.A
6.22	0.05 < 3 >	Leichte Abhängigkeit (LD)	App.A
6.23	0.15 < 3.3 >	Mittlere Abhängigkeit (MD)	App.A
6.24	0.5 < 2 >	Hohe Abhängigkeit (HD)	App.A
6.25	1.0 < 2 >	Totale Abhängigkeit (CD)	App.A

Tab. 56. Basisfehlerwahrscheinlichkeiten aus dem SWAIN-Handbuch (1983):

ID = Identifikations-Nr.

BHEP = Basisfehlerwahrscheinlichkeit (Median)

UF = Unsicherheitsfaktor

⁰ Aus SWAIN (1983).

* Für Zwischenwerte der verfügbaren Zeit T, $T(i) < T < T(i+1)$, läßt sich die BHEP über folgende Formel berechnen:

$$BHEP = BHEP(i) \cdot [T/T(i)]^{\{\ln [BHEP(i+1)]/BHEP(i)\} / \{\ln T(i+1)]/T(i)\}}$$

** Für den Fall, daß man den Rangplatz des betrachteten Alarms nicht kennt, empfiehlt SWAIN (1983) die Wahrnehmungsfehlerwahrscheinlichkeit für diesen Alarm aus dem arithmetischen Mittel der Wahrnehmungsfehlerwahrscheinlichkeiten aller auftretenden Alarme zu berechnen. Auch in diesem Fall empfiehlt SWAIN pauschal UF=10 zu verwenden.

*** Wenn nur 2 Positionen einstellbar sind, dann ist eine um den Faktor 5 reduzierte BHEP zu verwenden.

Tätigkeit	Gegenstand	Fehler	Fehler pro 10⁶ Arbeits- gänge
Betrachten	Plan	falsche Schalterbetätigung	1128
Ablesen	Anzeigeeinstrument	Fehler beim Ablesen	5000
Lesen	Anweisungen	fehlerhafte Vorgehensweise	64500
Verbinden	Schlauch	falsch verbunden	4700
Anschließen	Hydraulikleitungen	falsches Drehmoment aufgebracht	104
Anziehen	Muttern, Schrauben	nicht angezogen	4800
Anbringen	Muttern, Schrauben	nicht angebracht	600
Löten	Steckverbindungen	fehlerhafte Lötverbindungen	6460
Einlegen	Rundschnurring	nicht richtig eingelegt	66700
Montieren	Steckverbindungen	verbogene Steckerstifte	1500
Montieren	Steckverbindungen	vergessene Teile	1000
Schließen	Ventile	nicht richtig geschlossen	1800
Einstellen	mech. Verbindung	mangelhafte Einstellung	16700
Einsetzen	Lagerbuchse	falsche Größe eingesetzt	5000
Bearbeiten	Ventilanschlüsse	falsches Gewinde gebohrt	2083

Tab. 57. Repräsentative Raten menschlicher Fehler (nach PETERS 1966)

Anhang F: Berücksichtigung von Stress

1. Median (MDN) der neuen Fehlerwahrscheinlichkeit p bestimmen.
2. Neuen Unsicherheitsfaktor UF von MDN bestimmen.

Aufgabentyp → (Kenntnisbedarf) Stressniveau ↓	(A) SCHRITTWEISE (regelbasiert): Aufgabe kann durch einfache Anwendung einer Prozedur durchgeführt werden	(B) DYNAMISCH (wissensbasiert): ein nicht trivialer Denkvorgang ist erforderlich, Mensch-Maschine-Interaktionen sind von Bedeutung
(1) SEHR GERING: zu geringe Arbeitsbelastung (Unterforderung); z.B. bei der Überprüfung einer großen Anzahl gleichartiger Kriterien, die (fast) alle erfüllt sind	$MDN = 2 \cdot MDN_0$	
(2) OPTIMAL: Arbeitsbelastung gerade richtig; z.B. bei der Kalibrierung eines Grenzwertes oder beim Ablesen eines beleuchteten Textes auf einem Anzeigegerät	$MDN = MDN_0$ $UF = UF_0$ oder (wenn UF_0 unbekannt): $UF = 10 \mid MDN < 0.001$ $UF = 3 \mid 0.001 \leq MDN \leq 0.01$ $UF = 5 \mid MDN > 0.01$	$MDN = MDN_0$ $UF = 10 \mid MDN < 0.001$ $UF = 5 \mid MDN \geq 0.001$
(3) MITTELHOCH: eine Arbeitsbelastung, die die Kapazität des Leistungsvermögens erreicht hat oder gerade übersteigt; z.B. bei einer Transiente mit Reaktor- und Turbinenschnellabschaltung, bei einer unter Zeitdruck durchzuführenden Aufgabe während des An- oder Abfahrens der Anlage oder bei Arbeiten unter Schutzkleidung im strahlenbelasteten Bereich	$MDN = 2 \cdot MDN_0$ $UF = 10 \mid MDN < 0.001$ $UF = 5 \mid MDN \geq 0.001$	$MDN = 5 \cdot MDN_0$ $UF = 10$
(4) EXTREM HOCH: starkes emotionales Bedrohungserleben (Angst); z.B. nach einem großen Kühlmittelverlust	$MDN = 5 \cdot MDN_0$ $UF = 5$	$MDN = 0.25$ $UF = 5$

Tab. 58. Der Einfluß von Stress auf den Punktwert (MDN) und Streufaktor (UF) der Fehlerwahrscheinlichkeit eines erfahrenen Operators:

Erstellt nach SWAIN (1983, p. 18-5, 7-13).

MDN_0 = Median bei optimalem Stress und regelbasiertem Verhalten.

UF_0 = Streufaktor bei optimalem Stress und regelbasiertem Verhalten.

Anhang G: Berücksichtigung von Abhängigkeiten

Gegeben: Median MDN(ZD), Obergrenze OG(ZD) und Untergrenze UG(ZD) der unabhängigen Wahrscheinlichkeit für den Fehler B.

Gesucht: MDN, OG und UG der Wahrscheinlichkeit, für den Fehler B unter der Bedingung, daß zuvor der Fehler A aufgetreten ist.

Lösung: Lt. SWAIN (1983, p. 10-16ff, A-11f) hat die bedingte Wahrscheinlichkeit $w(B|A)$ in Abhängigkeit vom

Kopplungsgrad (LD: leicht, MD: mittel, HD: hoch, CD: total) zwischen A und B folgende Verteilungsparameter:

LD

$$\text{MDN(LD)} = [1 + 19 \text{MDN(ZD)}]/20$$

$$\text{OG(LD)} = \text{MAX} \{ \text{MDN(MD)}, \text{OG(ZD)} \}$$

$$\text{UG(LD)} = [\text{MDN(LD)}]^2 / \text{OG(LD)}$$

MD

$$\text{MDN(MD)} = [1 + 6 \text{MDN(ZD)}]/7$$

$$\text{OG(MD)} = \text{MAX} \{ \text{MDN(HD)}, \text{OG(ZD)} \}$$

$$\text{UG(MD)} = [\text{MDN(MD)}]^2 / \text{OG(MD)}$$

HD

$$\text{MDN(HD)} = [1 + \text{MDN(ZD)}]/2$$

$$\text{OG(HD)} = 1$$

$$\text{UG(HD)} = [\text{MDN(MD)}]^2$$

CD

$$\text{MDN(CD)} = 1$$

$$\text{OG(CD)} = 1$$

$$\text{UG(CD)} = \text{MDN(HD)}$$

Tab. 59. Abhängigkeitsmodell (SWAIN 1983):

Häufige Anwendungsfall: personelle Redundanz im Störfall.

Für personelle Redundanz unter Normalbedingungen empfiehlt SWAIN die im Anhang E unter 6.1 genannten Wahrscheinlichkeiten.

Falls $\text{MDN(ZD)} \leq 0.01$, dann können für $w(B|A)$ die in Anhang E unter ID=6.2 genannten Werte verwendet werden.

Anhang H: HTR-500. Weitere Konfliktsituationen

SITUATION	UNGEPLANTES VERHALTEN (bewußte Risikoannahme)	(+) VORTEILE UND (-) NACHTEILE UNGEPLANTEN VERHALTENS
Irgendein Störfall, für den ein automatisches Abfahren mit dem Hauptkühlsystem oder (nach erfolgter Schnellabschaltung) eine automatische NWA-Prozedur per Hauptkühlsystem vorgesehen ist. Die Abfahrprozedur bzw. die NWA-Prozedur per Hauptkühlsystem mißlingt. Ein automatischer Start des NWA-Systems steht bevor.	Maßnahmen mit dem Ziel, daß das Abfahren bzw. die NWA per Hauptkühlsystem doch noch gelingt.	(+) Schonende Abfahr- bzw. NWA-Prozedur (vgl. HRB 1983, S.94). (-) Die Maßnahmen könnten die Zuverlässigkeit der NWA beeinträchtigen.
Wassereinbruch wegen Leck am Dampferzeuger (DE). DE-Absperrung funktioniert. DE-Entlastungsleitung öffnet, schließt aber nicht wieder.	Absichtliches Hinauszögern der Handabspernung der DE-Entlastungsleitung.	(+) Keine Druckentlastung des Primärkreises ins Reaktorschutzgebäude (RSG). RSG ist somit für etwaige Reparaturen begehbar. (-) Ungefilterte Freisetzung in die Umgebung über offene Entlastungsleitung (vgl. ISF 1984, S.40).

Tab. 60. HTR-500. Weitere Konfliktsituationen

Anhang I: HTR-500. Weitere Diagnoseprobleme

DIAGNOSEPROBLEM	ERWARTUNGSFEHLER	UNGEPLANTE HANDLUNG
Kleines (0.5 kg/s) absperrbares Leck im Primärkreis. Abfahrprozedur per Hauptkühlsystem funktioniert. Absperrung des Primärkreises funktioniert nicht. Nach Druckabfall auf 40 bar (vgl. HRB 1983, S.141) werden folgende Systemreaktionen ausgelöst: RESA, Schließen der Hauptabsperrklappen (HAK) und Start des NWA-Systems.	Nichtbemerken, daß Druck unter 40 bar, z.B. weil man erwartet, daß die Systemreaktionen (RESA, HAK öffnen und NWA-Start) aufgrund des Versagens der Abfahrprozedur per Hauptkühlsystem ausgelöst worden sind.	Personal öffnet die HAK. Bei Reaktor unter Druck und funktionierender NWA ist der Zustand HAK GEÖFFNET richtig, damit die Rückwärtsdurchströmung der Hauptdampfzeuger durch heiße Gasstrahlen verhindert wird (vgl. HRB 1983, S.99). Bei druckentlastetem Reaktor kann dieser Zustand zu einer Beeinträchtigung der Kühlgasumwälzung führen, insbesondere dann, wenn nur ein NWA-Kreislauf funktioniert und die nachträgliche Absperrung des Primärkreis (bei ca. 30 bar) ebenfalls mißlingt.
Ausfall der Hauptkühlung. NWA versagt. Entlastungsventil des Primärkreises öffnet bei 55 bar, schließt aber nicht wieder, nachdem der Druck auf 50 bar abgefallen ist. Dem Personal gelingt die Reparatur des NWA-Systems, der Druck ist mittlerweile unter 40 bar.	Nichtbemerken, daß Druck unter 40 bar, z.B. weil man durch die Reparatur des NWA-System stark abgelenkt worden ist.	Personal öffnet die HAK. (s.o.)

Tab. 61. HTR-500. Weitere Diagnoseprobleme

Tabellenverzeichnis

Tab. 1.	Operateurfehler im Störfall, die Bestandteil der Datenbasis des SWAIN-Handbuchs sind	10
Tab. 2.	Basisfehlertypen nach REASON (1990)	14
Tab. 3.	Mögliche Komplikationsfaktoren (übersetzt aus WOODS u.a. 1990, p.44)	19
Tab. 4.	Der Störfall im KKW Davis-Besse. Die Zeit (min) bis zur Wiederherstellung der DE-Bespeisung	27
Tab. 5.	KKW Davis-Besse. NWA-Erfolgskriterien nach Ausfall der DE-Bespeisung	37
Tab. 6.	Zeitbedarfsanalyse für den Start einer Notspeisewasserpumpe	38
Tab. 7.	Zeitbedarfsanalyse für das Einleiten von feed + bleed	39
Tab. 8.	Zeitbedarfsanalyse für den Start der Elektro-Pumpe	39
Tab. 9.	HTR-500. Hauptauslegungsdaten bei 100% Last (HRB 1983, S.26)	46
Tab. 10.	Systemreaktionen nach Ausfall der Hauptkühlung	49
Tab. 11.	NWA-Daten bei Reaktor unter Druck (ISF 1984, Kap. II)	49
Tab. 12.	NWA-Ausfalldaten in ISF (1984)	51
Tab. 13.	Ausfallwahrscheinlichkeit der Zwangskonvektion (per Gebläse)	53
Tab. 14.	Beitrag der Wärmesenke zur NWA-Ausfallwahrscheinlichkeit	53
Tab. 15.	Hypothetischer Handlungsablauf nach Ausfall der Hauptkühlung	55
Tab. 16.	Naturkonvektion. Zeitbedarfsanalyse ohne zeitunabhängige Operateurfehler	57
Tab. 17.	Naturkonvektion. Zeitbedarfsanalyse, wenn zeitunabhängiger Operateurfehler	57
Tab. 18.	Naturkonvektion. Operateurfehler ohne recovery und ohne Zeitfehler	59
Tab. 19.	Querverbindung. Operateurfehler in der Warte ohne recovery	69
Tab. 20.	Zustandsvariablen nach NWA-Ausfall	71
Tab. 21.	HTR-500. Kernaufheizung. Belastungsannahmen	77
Tab. 22.	Wahrscheinlichkeiten technischer Möglichkeiten nach NWA-Ausfall	79
Tab. 23.	Verfahren zur Identifizierung von Nachteilen trotz Hauptzieleinhaltung	86
Tab. 24.	HTR-500. Nachteile (-) trotz ausreichender NWA	87
Tab. 25.	HTR-500. Wirtschaftlich bedeutsame Ereignisse nach Ausfall der Hauptkühlung	89
Tab. 26.	Verfahren zur Identifizierung von Konflikten	92
Tab. 27.	HTR-500. Nachteile erfolgreicher Gegenmaßnahmen nach NWA-Ausfall	93
Tab. 28.	HTR-500. Konfliktbedingte Rückwirkungen auf die NWA-Zuverlässigkeit nach Ausfall der Hauptkühlung	96
Tab. 29.	HTR-500. Beispiele für mögliche Zustandsbilder der NWA-Wärmesenke	100
Tab. 30.	Identifizierung von Situationen mit Zielkonflikt oder Diagnoseproblem	102
Tab. 31.	Modell zur Entstehung gefährlicher Situationen (SURRY 1966)	107
Tab. 32.	Reale Störfallbeispiele mit Fehlern in den Bereichen Diagnose und Risikoverhalten	108
Tab. 33.	Verteilung von 93 Fehlern des KKW-Personals (SABRI u.a. 1981)	109
Tab. 34.	Verwendung der Wahrscheinlichkeit 0.01 (MDN) regelwidrigen Verhaltens	112
Tab. 35.	An 24 Operateuren beobachtete Persönlichkeitsmerkmale	117
Tab. 36.	Leistungsbedürfnis, Kontrolle und Risikoverhalten (SHEALY 1975)	117
Tab. 37.	Anteil der 30 Vpn, die sich für 500 \$ versicherten (SLOVIC u.a. 1977)	121

Tab. 38. Maßnahmen zur Senkung der Risikobereitschaft (WILDE 1978)	123
Tab. 39. Widersprüchliche Ergebnisse zum Risikoverhalten in Spielsituationen	126
Tab. 40. Beispiel für eine Skalierung verbal formulierter Risiken	127
Tab. 41. Einflußfaktoren zur Quantifizierung von Fehlverhalten	134
Tab. 42. PSF-Wichtungsfaktoren	137
Tab. 43. Geschätzte PSF-Grade für das gelegentliche Ignorieren von Vorschriften im industriellen Alltag (Kalibrierung für MDN = 0.01)	139
Tab. 44. Geschätzte PSF-Grade für das nicht richtige Benutzen einer Checkliste (Kalibrierung für MDN = 0.5)	140
Tab. 45. Vergleich zwischen geometrischer und arithmetischer PSF-Skalierung	147
Tab. 46. Erweiterung eines PSF-Modells mit den Maximalfaktoren $K_1 \dots K_n$ um einen neuen PSF mit dem unbekannten Maximalfaktor K^*	148
Tab. 47. Variabilitätsursachen, die durch die Unsicherheitsfaktoren des Swain- Handbuchs erfaßt werden sollen	150
Tab. 48. Fehlerwahrscheinlichkeiten ($MDN < UF >$) für das gezielte (nicht zufäl- lige) Beobachten von Anzeigen	153
Tab. 49. Klassifizierung von Fehlhandlungen nach HACKER (1980, S.344-348) . .	157
Tab. 50. Summarizing the Main Headings for Failure Modes at Each of the Three Performance Levels (REASON 1990, p.69)	158
Tab. 51. Orientierungswerte zur Schätzung der Wahrscheinlichkeit einer falschen Identifizierung des Systemzustands (Erwartungsfehler)	163
Tab. 52. HTR-500. Berücksichtigte ungeplante Handlungen aufgrund von Kon- flikten und Diagnoseproblemen	166
Tab. 53. HTR-500. Geschätzte PSF-Grade zu (ungeplantem) Fehlverhalten in drei signifikanten Konfliktsituationen	167
Tab. 54. HTR-500. Einflüsse menschlichen Verhaltens auf die Wahrscheinlichkeit des Versagens der NWA	175
Tab. 55. Vorschläge zur Senkung der Risikobereitschaft von Operateuren	185
Tab. 56. Basisfehlerwahrscheinlichkeiten aus dem SWAIN-Handbuch (1983) . . .	209
Tab. 57. Repräsentative Raten menschlicher Fehler (nach PETERS 1966)	213
Tab. 58. Der Einfluß von Stress auf den Punktwert (MDN) und Streufaktor (UF) der Fehlerwahrscheinlichkeit eines erfahrenen Operateurs	215
Tab. 59. Abhängigkeitsmodell (SWAIN 1983)	217
Tab. 60. HTR-500. Weitere Konfliktsituationen	219
Tab. 61. HTR-500. Weitere Diagnoseprobleme	221

Abbildungsverzeichnis

Abb. 1.	Mögliche Schwerpunkte einer Mensch-Maschine-Systemanalyse	12
Abb. 2.	Performance Levels of Skilled Operators	13
Abb. 3.	A Summary of the Psychological Varieties of Unsafe Acts	15
Abb. 4.	Störfall im KKW Davis-Besse 1985. Sekundärseitige Maßnahmen	26
Abb. 5.	Dynamische Handlungsstruktur: Erst A, dann B	31
Abb. 6.	Dynamische Handlungsstruktur: A und B	32
Abb. 7.	Dynamische Handlungsstruktur: A oder B	32
Abb. 8.	Dynamische Handlungsstruktur: Erst A, dann B, aber B nicht vor TX	33
Abb. 9.	Leitermodell für das Operateurverhalten nach RASMUSSEN (1979), stark vereinfacht	35
Abb. 10.	Davis-Besse. Ereignisbaum für Gegenmaßnahmen nach NWA-Ausfall	41
Abb. 11.	HTR-500. Reaktordruckbehälter mit Einbauten (aus HRB 1983, S.29)	47
Abb. 12.	HTR-500. Anlagenübersicht (aus ISF 1984, S.7)	48
Abb. 13.	Naturkonvektion. Operateurfehler mit Korrektur, ohne Zeitfehler	63
Abb. 14.	Naturkonvektion. Operateurfehler mit Korrektur und Zeitfehler	64
Abb. 15.	Querverbindung. Operateurfehler mit Korrekturmöglichkeiten	70
Abb. 16.	Kernaufheizung ohne Wärmetauscherbespeisung, HAK geschlossen	74
Abb. 17.	Kernaufheizung ohne Wärmetauscherbespeisung, HAK nach 0.5 h geöffnet	75
Abb. 18.	Kernaufheizung ohne Zwangskonvektion, beide Wärmetauscher bespeist	76
Abb. 19.	Gegenmaßnahmen. Menschliche und technische Fehler. Gesamtbewertung	81
Abb. 20.	PSF-Extrapolationsmodell	133
Abb. 21.	PSF-Eingabedatei für die betrachtete Konfliktsituation oder die bekannte Referenzsituation	137
Abb. 22.	HTR-500. NWA-Ausfallwahrscheinlichkeit ohne Gegenmaßnahmen, aber mit ungeplanten Handlungen	170
Abb. 23.	Naturkonvektion. Operateurfehler einschließlich ungeplanter Handlungen	173
Abb. 24.	Gegenmaßnahmen. Menschliche und technische Fehler. Gesamtbewertung einschließlich ungeplanter Handlungen	174
Abb. 25.	Gebläsekühlung mit hypothetischer Querverbindungsmöglichkeit	208

Jül-2811

September 1993

ISSN 0944-2952