Gesellschaft für Reaktorsicherheit

Deutsche Risikostudie Kernkraftwerke

Fachband 2

Zuverlässigkeitsanalyse

Verlag TÜV Rheinland

Gesellschaft für Reaktorsicherheit

Deutsche Risikostudie Kernkraftwerke

Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko

Fachband 2

Zuverlässigkeitsanalyse

Studie im Auftrage des Bundesministeriums für Forschung und Technologie

Verlag TÜV Rheinland

Die Autoren dieses Fachbandes 2 "Zuverlässigkeitsanalyse" der Deutschen Risikostudie - Kernkraftwerke sind:

Wilhelm Dietlmeier
Stefan Goßner
Wolfgang Güldner
Helmut Hörtner
Joachim von Linden
Wolfgang Preischl
Günther Reichart
Heinz Spindler
Gerhard Volmer
Gerhard Zipf

Alle Autoren sind Mitarbeiter der Gesellschaft für Reaktorsicherheit (GRS) mbH.

Redaktion:

H.-P. Butz, H.-J. Danzmann, L.F. Franzen, H. de Groot-Böhlhoff, K. Kotthoff, M. Straßenmeyer

ISBN 3-88585-013-3
Herausgeber: Der Bundesminister für Forschung und Technologie

Verlegerische Betreuung und Gesamtherstellung: Verlag TÜV Rheinland GmbH, Köln
Printed in Germany 1981

Vorwort

Im Frühjahr 1976 hatte der Bundesminister für Forschung und Technologie (BMFT) die "Deutsche Risikostudie - Kernkraftwerke" bei der Gesellschaft für Reaktorsicherheit (GRS) mbH in Auftrag gegeben. Unter der wissenschaftlichen Leitung ihres Geschäftsführers, Prof. Dr. A. Birkhofer, wurden die zugehörigen Arbeiten zusammen mit weiteren technisch-wissenschaftlichen Organisationen durchgeführt und die Ergebnisse im Augsut 1979 vorgelegt. Ziel dieser Studie war es, das durch Störfälle in Kernkraftwerken verursachte Risiko unter Berücksichtigung deutscher Verhältnisse in Anlehnung an die amerikanische Reaktorsicherheitsstudie WASH-1400 zu ermitteln.

Die Studie gliedert sich in zwei Arbeitsphasen. Die erste Phase ist abgeschlossen. Die Ergebnisse sind in einer allgemein verständlichen Kurzfassung, herausgegeben vom BMFT, vom 15. August 1979 und in einem Hauptband, erschienen im Verlag TÜV Rheinland, ebenfalls 1979, dokumentiert. Ergänzend zu diesen Veröffentlichungen werden die für die Studie im einzelnen durchgeführten Untersuchungen und ihre Ergebnisse in einer Reihe von Fachbänden zusammengestellt, die im Laufe des Jahres 1980 erscheinen: F1 - Ereignisablaufanalyse, F2 - Zuverlässigkeitsanalyse, F3 - Zuverlässigkeitsdaten und Betriebserfahrungen, F4 - Einwirkungen von außen (einschließlich anlageninterner Brände), F5 - Untersuchung von Kernschmelzunfällen, F6 - Ermittlung der Spaltproduktfreisetzung, F7 - Ergebnisse der anlagentechnischen Untersuchungen, F8 - Unfallfolgenrechnungen und Risikoergebnisse.

Der hier vorliegende Fachband 2 ergänzt zusammen mit dem Fachband 3 (Zuverlässigkeitsdaten und Betriebserfahrungen) die Abschnitte 4.5, 4.6, 5.1, 5.2 und 6.6 des Hauptbandes. Er behandelt detailliert die Methoden der Zuverlässigkeitsanalyse, den Aufbau und die Wirkungsweise sicherheitstechnisch wichtiger Systeme sowie die Funktionsprüfungen an diesen Systemen. Aufbauend auf diesem Material werden Durchführung und Ergebnisse der Zuverlässigkeitsanalyse für die anlageninternen Störfälle dargestellt. Untersucht werden die Kühlmittelverluststörfälle und die Transienten, die zu Transientenstörfällen führen können. Den Ab-

schluß bilden Zuverlässigkeitsanalysen des Reaktorschnellabschaltsystems und des Sicherheitsbehälterabschlusses. Das umfangreiche Material ist in Hauptteil (F2/I) und Anhänge (F2/II), in denen Schaltpläne, Gesamt- und Teilfehlerbäume sowie Funktionselemente zusammengestellt sind, gegliedert. Der Fachband verdeutlicht den Stand, den die Zuverlässigkeitsanalyse in der Kerntechnik erreicht hat.

Garching, im August 1980

Gesellschaft für Reaktorsicherheit
(GRS) mbH

KURZFASSUNG

Aufbauend auf die im Fachband 1 dokumentierte Ereignisablaufanalyse werden im vorliegenden Fachband die Versagenswahrscheinlichkeiten der zur Beherrschung der auslösenden Ereignisse benötigten Systemfunktionen ermittelt. Die zu dieser Bewertung der Ereignisabläufe erforderlichen Zuverlässigkeitsuntersuchungen werden weitgehend mit Hilfe der Fehlerbaumanalyse durchgeführt. Die Methoden der Zuverlässigkeitsanalyse, der Aufbau und die Wirkungsweise sicherheitstechnisch wichtiger Systeme sowie die Funktionsprüfungen an diesen Systemen werden detailliert behandelt. Die umfangreiche Dokumentation der für die anlageninternen Störfälle durchgeführten Zuverlässigkeitsanalysen macht es erforderlich, eine Zweiteilung des Fachbandes 2 vorzunehmen.

ABSTRACT

Based on the event tree analysis as documented in the appendix 1, the failure probabilities of the system functions required to control the initiating events are evaluated in this appendix 2. The reliability investigations necessary for the evaluation of the event sequences are performed mostly by means of the fault tree analysis. The methods of the reliability analysis, the composition and function of the systems important to safety and the functional tests performed on these systems are dealt with in detail. The comprehensive documentation of the reliability analyses as performed for the internal events necessitated a division of this appendix 2 into two volumes.

INHALT

BILDER

TABELLEN

1. ZUSAMMENFASSUNG

Für die Ermittlung der zur Störfallbeherrschung benötigten Systeme wird eine Ereignisablaufanalyse durchgeführt, in der, ausgehend von einem definierten auslösenden Ereignis (z.B. Bruch einer Rohrleitung), über den Erfolg oder das Versagen dann notwendiger Gegenmaßnahmen (Systemfunktionen) die verschiedenen Auswirkungen dieses Ereignisses erfaßt werden. Aufgabe der Zuverlässigkeitsanalyse ist die Bestimmung der Versagenswahrscheinlichkeiten der zur Störfallbeherrschung benötigten Systemfunktionen. Die hierzu erforderlichen Zuverlässigkeitsuntersuchungen werden weitgehend mit Hilfe der Fehlerbaumanalyse durchgeführt. Das unerwünschte Ereignis (die Spitze des Fehlerbaums) bildet der Ausfall der laut Ereignisablaufdiagramm geforderten Systemfunktionen (z.B. Notkühlung fällt bei Anforderung aus). Es werden alle Kombinationen von Komponentenausfällen gesucht, die zu einem Versagen der Notkühlung, also dem Eintreten des unerwünschten Ereignisses führen. Die Anwendung der Fehlerbaumanalyse ist vor allem auch deshalb notwendig, weil Erfahrungswerte für die Zuverlässigkeit von Systemen meist fehlen, für die verschiedenen Komponenten aber vorhanden sind.

Die Systeme, die für die im Ereignisablaufdiagramm definierten Systemfunktionen notwendig sind, bestehen aus redundanten Komponenten oder Teilsystemen (Strängen). Das heißt, daß mehr Stränge vorhanden sind, als für die Erfüllung dieser Funktion erforderlich wären. Bei der Definition des unerwünschten Ereignisses ist es daher von großer Bedeutung, wie viele redundante Stränge für die Erfüllung der sicherheitstechnischen Aufgabe notwendig sind. Man spricht hier von Mindestanforderungen. Diese hängen sowohl vom auslösenden Ereignis als auch vom weiteren Ereignisablauf ab. In den hier beschriebenen Untersuchungen werden die Mindestanforderungen zugrunde gelegt, die im Genehmigungsverfahren festgeschrieben sind. Darüber hinaus wird generell davon ausgegangen, daß die adäquate Systemauslegung im Genehmigungsverfahren geprüft wurde.

Die Fehlerbäume sind so aufgebaut, daß sie das gesamte Zusammenwirken von leittechnischen Systemen (z.B. Reaktorschutzsystem),

Energieversorgung (z.B. Notstromsystem) und verfahrenstechnischen Systemen (z.B. Not- und Nachkühlsystem) enthalten. So ist es möglich, Ausfälle, die durch das Zusammenwirken verschiedener Systeme entstehen, zu identifizieren und entsprechend zu berücksichtigen.

Die Eingangsdaten zur quantitativen Auswertung der Fehlerbaumanalyse sind die für die unterschiedlichen Ausfallarten der Komponenten maßgeblichen Ausfallraten oder Ausfallwahrscheinlichkeiten pro Anforderung sowie die Streuung dieser Daten, der zeitliche Abstand der Funktionsprüfungen und die Nichtverfügbarkeit aufgrund der Instandhaltung. Vor allem durch die Berücksichtigung der regelmäßigen Funktionsprüfungen an den verschiedenen Teilsystemen und Komponenten ist es möglich, die Berechnung der Zuverlässigkeit der Systeme den im Betrieb vorliegenden Bedingungen gut anzupassen.

Für die numerische Auswertung der Fehlerbäume wird das Programmsystem RALLY eingesetzt. Dieses besteht im wesentlichen aus einem Simulationsprogramm zur Ermittlung der Erwartungswerte von Versagenswahrscheinlichkeiten und aus einem analytisch-simulativen Programm zur Ermittlung der Streuung der Ergebnisse aufgrund der Streuung der Ausfallraten.

Die auslösenden Ereignisse sind im Fachband 1 zusammengestellt. Dort findet sich auch eine ausführliche Beschreibung der durchgeführten Ereignisablaufanalysen. Die quantitative Bewertung der Ereignisabläufe für die anlageninternen Störfälle ist im vorliegenden Fachband enthalten. Störfälle durch Einwirkungen von außen (anlagenexterne Störfälle) sind in Fachband 4 dargelegt. Zusammenstellung und Diskussion der in die Zuverlässigkeitsuntersuchungen eingehenden Daten sind in Fachband 3 zu finden.

Alle anlageninternen Störfälle, die zu einer Überhitzung des Reaktorkerns führen können, lassen sich in zwei Gruppen einteilen:

- Störfälle, die durch einen Verlust von Hauptkühlmittel ausgelöst werden,

- Störfälle, bei denen die Leistung im Kern erhöht oder die Wärmeabfuhr aus dem Kern beeinträchtigt wird, ohne daß Hauptkühlmittel verlorengeht.

Die erste Gruppe wird als Kühlmittelverluststörfälle, die zweite Gruppe als Transientenstörfälle bezeichnet. In diese zwei Gruppen unterteilt, sind sie auch im vorliegenden Fachband diskutiert (Kapitel 6 und 7). Dabei ist zu berücksichtigen, daß sich bei Erstellung der Ereignisablaufdiagramme eine zweckmäßige Unterteilung am Entscheidungspunkt "Kernschmelzen" ergibt. Die in den genannten zwei Kapiteln bewerteten Ereignisabläufe gehen bis an diesen Entscheidungspunkt. Zur Bestimmung der Freisetzung radioaktiver Stoffe infolge Kernschmelzens werden die Versagensarten des Sicherheitsbehälters untersucht und entsprechend einer für die Berechnung der Freisetzungsraten zweckmäßigen Form kategorisiert. In den Untersuchungen werden, u.a. geordnet nach abnehmendem Leckquerschnitt, sechs verschiedene Versagensarten des Sicherheitsbehälters α, β_1, β_2, β_3, η und δ definiert. Diese Versagensarten werden mit den Ereignisabläufen verknüpft, die bis zum obengenannten Entscheidungspunkt führen. So ergeben sich die Freisetzungswahrscheinlichkeiten aus dem Sicherheitsbehälter entsprechend der jeweils betrachteten Versagensart (Kapitel 9).

Für die im folgenden diskutierten wichtigsten Ergebnisse der Zuverlässigkeitsanalysen ist zu beachten, daß die für den Ausfall der erforderlichen Systemfunktionen angegebenen Werte bedingte Wahrscheinlichkeiten darstellen, d.h. jeweils davon ausgegangen wird, daß das auslösende Ereignis eingetreten ist. Der Beitrag zur Häufigkeit des unbeherrschten Störfalls (Kernschmelzen) ergibt sich somit durch Multiplikation mit der Häufigkeit des entsprechenden auslösenden Ereignisses. Für die Bestimmung der Häufigkeiten von Spaltproduktfreisetzungen aus dem Reaktorgebäude sind darüber hinaus die Versagensmöglichkeiten für den Sicherheitsbehälter und die zugehörigen Wahrscheinlichkeiten zu berücksichtigen.

Für das große und mittlere Leck in einer Hauptkühlmittelleitung ergeben sich bedingte Versagenswahrscheinlichkeiten der erforderlichen Systemfunktionen zu $1{,}7 \cdot 10^{-3}$ bzw. $2{,}3 \cdot 10^{-3}$. Da die

zur Störfallbeherrschung notwendigen Sicherheitssysteme automatisch in Betrieb genommen werden, spielt menschliches Fehlverhalten nur im Zusammenhang mit der Kalibrierung von Meßkanälen eine Rolle. 73 % des Ergebnisses werden von unabhängigen Ausfällen der Hardware verursacht. Von "common mode"-Ausfällen (CMA) der Hardware sind Ausfälle der Nachkühlpumpen während der Langzeit-Notnachkühlung zu nennen. Beim kleinen Leck in einer Hauptkühlmittelleitung erhält man eine bedingte Versagenswahrscheinlichkeit der erforderlichen Systemfunktionen von $2{,}1 \cdot 10^{-2}$. Hier ergeben fehlerhafte Handmaßnahmen zur Vorbereitung des Abfahrens mit ca. 78 % den größten Beitrag. Weitere Handmaßnahmen sind demgegenüber von untergeordneter Bedeutung. So machen CMA durch Fehlkalibrierung von Meßkanälen nur etwa 3 % des Beitrags aus.

Tritt ein Notstromfall ein und versagt die Notspeisewasserversorgung aufgrund von unabhängigen Ausfällen oder CMA der Notstromdiesel, so ist es möglich, durch Handmaßnahmen das Notstandssystem in Betrieb zu nehmen. Dadurch kann eine Notspeisewasserversorgung vom Block A aus hergestellt werden. CMA der Hardware allein liefern somit keinen Beitrag. Menschliches Fehlverhalten allein spielt ebenfalls keine Rolle, da im Notstromfall normalerweise alle Maßnahmen automatisch erfolgen. Ausfälle durch Fehlkalibrierung sind im Notstromfall vernachlässigbar. Die bedingte Versagenswahrscheinlichkeit der beim Notstromfall erforderlichen Systemfunktionen wurde zu $1{,}3 \cdot 10^{-4}$ ermittelt.

Beim kleinen Leck am Druckhalter als Folge des Notstromfalls ergibt sich die bedingte Versagenswahrscheinlichkeit der Systemfunktionen zu $2{,}6 \cdot 10^{-2}$. Dabei führen CMA der Hardware nur in Verbindung mit unabhängigen Ausfällen zum nichtbeherrschten Störfall. Dasselbe gilt für menschliches Fehlverhalten.

Bei den ATWS[1])-Störfällen spielt die Versagenswahrscheinlichkeit der Druckhalterventile die zentrale Rolle. Kommt es zu einem ATWS-Störfall als Folge des "Ausfalls der Hauptspeisewasserver-

---

[1]) Anticipated Transients Without Scram = zu erwartende Transienten ohne Reaktorschnellabschaltung

sorgung", so müssen die drei Druckhalterventile mit dem größten Ventilquerschnitt öffnen, um einen ausreichenden Druckabbau im Primärsystem zu erreichen. Für das Nichtöffnen eines dieser Ventile ergibt sich eine Wahrscheinlichkeit von $1{,}2 \cdot 10^{-1}$. Da andererseits bei allen ATWS-Störfällen in der Regel alle vier Druckhalterventile öffnen, ist es nach entsprechender Druckabsenkung notwendig, daß sie wieder schließen, um weiteren Kühlmittelverlust und damit den Störfall "kleines Leck am Druckhalter" zu verhindern. Die Wahrscheinlichkeit für das Nichtschließen eines der vier genannten Ventile wurde mit $2{,}5 \cdot 10^{-2}$ abgeschätzt.

Für das Versagen sowohl der oben genannten zur Störfallbeherrschung benötigten Systeme als auch des Sicherheitsbehälters sind im allgemeinen gemeinsame Komponenten von Bedeutung. So fällt bei der Versagensart β_1 des Sicherheitsbehälters meist auch die zur Beherrschung von Kühlmittelverluststörfällen benötigte Notkühlung aus. Dieses Versagen des Sicherheitsbehälters wird vor allem durch den Ausfall von Schweißnähten verursacht. Für die Versagensarten β_2 bis η des Sicherheitsbehälters spielt bei einem nicht beherrschten Kühlmittelverluststörfall der Ausfall von Reaktorschutzsignalen aufgrund von Kurzschlüssen eine Rolle, beim Notstromfall und beim kleinen Leck am Druckhalter als Folge des Notstromfalls sind darüber hinaus "common mode"-Ausfälle der Notstromdiesel in Verbindung mit menschlichem Fehlverhalten bzw.Ausfällen der Hardware von Bedeutung.

Abschließend sei wiederholt, daß die Häufigkeit des Kernschmelzens sowohl durch die Wahrscheinlichkeit für das Versagen der Systemfunktionen als auch durch die Häufigkeit der Anforderung (Eintreten des auslösenden Ereignisses) bestimmt wird. Berücksichtigt man das, so liefern der Reihe nach die folgenden Störfälle den größten Beitrag zum Kernschmelzen: kleines Leck in einer Hauptkühlmittelleitung, Notstromfall, kleines Leck am Druckhalter beim Notstromfall. Im Vergleich dazu spielen die anderen Störfälle (und der Ausfall der dann geforderten Systemfunktionen) eine eher untergeordnete Rolle (Fachbände 1 und 7).

2. EINLEITUNG

In einer Risikoanalyse sind die Häufigkeiten von Ereignisabläufen zu ermitteln. Ausgehend von einem auslösenden Ereignis wird das Funktionieren oder Versagen der angeforderten sicherheitstechnisch wichtigen Systeme berücksichtigt. Hierzu sind die Eintrittshäufigkeiten des auslösenden Ereignisses und die Versagenswahrscheinlichkeiten der zur Störfallbeherrschung benötigten Systeme zu bestimmen. Zur Ermittlung der Versagenswahrscheinlichkeiten sind Zuverlässigkeitsuntersuchungen erforderlich, da die Betriebserfahrungen gewöhnlich nicht ausreichen, um daraus direkt die Zuverlässigkeit der Systeme beurteilen zu können.

Zuverlässigkeitsanalysen sind damit eine entscheidende Voraussetzung zur Durchführung von Risikoanalysen. Sie sind ein verhältnismäßig neues Arbeitsgebiet, erstmals in großem Umfang in der Luft- und Raumfahrt angewendet, aber auch schon in der Reaktorsicherheit seit mehr als einem Jahrzehnt in zunehmendem Maße eingesetzt. Für die Zuverlässigkeitsanalyse großer technischer Systeme sind Grundlagen und Anwendungsbeispiele nur unzureichend in deutscher Sprache dokumentiert. Mit der Deutschen Risikostudie Kernkraftwerke liegt ein in dieser Art wichtiges Anwendungsbeispiel vor, so daß es angebracht schien, die Grundlagen, die verwendeten Methoden, die vorhandenen Daten und die durchgeführten Untersuchungen so zu dokumentieren, daß eine ausreichende Nachvollziehbarkeit der Analyse gewährleistet ist.

Anders als für die Systeme und deren Funktionen sind im allgemeinen ausreichende Erfahrungen über die Zuverlässigkeit der Komponenten bzw. für deren Funktionen vorhanden. Daraus läßt sich bei genauer Kenntnis des Systemaufbaus die Systemzuverlässigkeit ermitteln. Zwei Zuverlässigkeitskenngrößen sind hier zu unterscheiden, die Nichtverfügbarkeit und die Ausfallwahrscheinlichkeit. Die verwendeten Zuverlässigkeitskenngrößen für die Komponentenfunktionen sind die Ausfallrate und die Ausfallwahrscheinlichkeit pro Anforderung. Komponenten sind dabei nicht nur Bauteile, sondern auch Verfahrensvorschriften und Personen, die in den Betrieb eingreifen. Jeder Komponentenfunktion wird dabei ein Funktionselement zugeordnet, das die Zustände "intakt" oder

"ausgefallen" annehmen kann. Bei "common mode"-Ausfällen (CMA) kann darüber hinaus einer bestimmten Funktion von mehreren redundanten Komponenten ein einziges Funktionselement zugewiesen werden.

Für die Untersuchung großer Systeme hat sich die Fehlerbaumanalyse bewährt, bei der das unerwünschte Ereignis, das ist der Ausfall der zur Störfallbeherrschung erforderlichen Systemfunktionen, vorgegeben und nach allen Ausfallkombinationen von Funktionselementen gesucht wird, die zu diesem Ereignis führen. Die quantitative Auswertung der Fehlerbäume erfolgt mit EDV-Anlagen. Für die vorliegende Studie wird das Programmsystem RALLY, das speziell zur Behandlung komplexer und vermaschter Systeme entwickelt worden ist, eingesetzt. Dazu gehört das Daten- und Fehlerbaumaufbereitungsprogramm TREBIL, dessen Aufgabe eine Datenaufbereitung für die verschiedenen verwendeten Programme des Programmsystems ist. Die Bestimmung des Erwartungswertes der Ausfallwahrscheinlichkeit und der mittleren Nichtverfügbarkeit erfolgt mit dem Programm CRESSEX, die Berechnung der Streubreiten der Ergebnisse mit STREUSL. Zur Beschreibung der Streubreiten der Zuverlässigkeitskenngrößen können zwar grundsätzlich verschiedene Arten von Verteilungsfunktionen verwendet werden, doch eignet sich die verwendete logarithmische Normalverteilung für die in der vorliegenden Studie gestellten Aufgaben besonders gut.

Neben den unabhängigen Funktionsausfällen von Komponenten ist mit dem Auftreten voneinander abhängiger Funktionsausfälle zu rechnen. Betreffen sie redundante Komponenten, Teilsysteme oder Systeme, spricht man von "common mode"-Ausfällen. Ursache hierfür können Fehler bei der Planung und Herstellung oder solche während des Betriebes sein, wobei sich diese Kategorien noch weiter unterteilen lassen. Zu den Gegenmaßnahmen zählen Verwendung erprobter Konstruktionen und Standardisierung, Nutzung der Möglichkeiten von Redundanz und Diversität, räumliche Trennung, qualitätssichernde Maßnahmen bei Planung, Herstellung und Betrieb, regelmäßige Funktionsprüfungen, um nur die wichtigsten zu nennen. Aus der Betriebserfahrung können höchstens CMA-Wahrscheinlichkeiten der Hardware abgeleitet werden. Darüber hinaus

stehen zur Bewertung solcher CMA verschiedene Methoden zur Verfügung, von denen allerdings die Beta-Faktor-Methode wegen des unterschiedlichen Systemaufbaus in deutschen Kernkraftwerken und der unterschiedlichen Vorgehensweise in der vorliegenden Studie nicht zur Anwendung kommt. Im Hinblick auf menschliches Fehlverhalten muß über die Wahrscheinlichkeitsaussagen für einzelne Handlungen hinaus eine Aussage über die Größe der Abhängigkeit von Ausfällen aufgrund von Fehlhandlungen erhalten werden. Dazu wird wie in der amerikanischen Reaktorsicherheitsstudie WASH-1400 die Methode der Kopplung von Ausfällen verwendet.

Menschliche Fehlhandlungen können sich im bestimmungsgemäßen Betrieb, z.B. bei betrieblichen Schalthandlungen zur Eingrenzung kleiner Störungen und bei Instandhaltungsmaßnahmen auswirken. Handlungen des Betriebspersonals sind auch bei Störfällen erforderlich, doch ist die Auslegung so auf automatische Schutzaktionen abgestellt, daß mindestens 30 Minuten ab Störfalleintritt für Handeingriffe zur Verfügung stehen. In der vorliegenden Studie werden wie in WASH-1400 nur geplante Handeingriffe bewertet. Ungeplante Eingriffe, die sich sowohl negativ wie positiv auswirken können, werden nicht quantifiziert.

Nach allgemeinen Vorbemerkungen werden im Kapitel 3 die Fehlerbaumanalyse, die zugehörigen Rechenprogramme, die Zuverlässigkeitskenngrößen, die logarithmische Normalverteilung, die CMA und das menschliche Fehlverhalten detailliert behandelt. Kapitel 4 bringt die Systembeschreibungen für die Referenzanlage und Kapitel 5 einen Abriß der in diesem Zusammenhang wichtigen Funktionsprüfungen. Die im einzelnen durchgefürten Zuverlässigkeitsanalysen für Kühlmittelverluststörfälle (Kapitel 6) und für Transienten (Kapitel 7) werden ergänzt durch die in Kapitel 8 enthaltene Zuverlässigkeitsanalyse für die Reaktorschnellabschaltung und durch die in Kapitel 9 durchgeführte Zuverlässigkeitsanalyse für den Sicherheitsbehälterabschluß. Wegen des umfangreichen Materials erwies es sich als notwendig, eine Zweiteilung vorzunehmen. Der Hauptteil (F2/I) wird durch Anhänge (F2/II) ergänzt, in denen sich die zugehörigen Schaltpläne, Gesamt- und Teilfehlerbäume sowie die in den Fehlerbäumen verwendeten Daten der Funktionselemente befinden.

3. METHODEN DER ZUVERLÄSSIGKEITSANALYSE

3.1 Allgemeines

3.1.1 Vorgehen in der Zuverlässigkeitsanalyse

Das übergeordnete Ziel von Zuverlässigkeitsanalysen ist die quantitative Bewertung der Güte eines technischen Systems. Erfahrungswerte über die Zuverlässigkeit von Systemen fehlen meist, sind für Komponenten aber vorhanden. Daher wird die Zuverlässigkeit des Systems aus den entsprechenden Zuverlässigkeitsdaten der Komponenten ermittelt, wobei die Verknüpfung der Komponenten entsprechend berücksichtigt wird. Die Komponenten haben in der Regel verschiedene Funktionen, z.B. Ein- oder Ausschalten eines Aggregats. Es ist daher jeweils festzustellen, der Ausfall welcher Komponentenfunktion zum Systemausfall beiträgt. Aus diesem Grunde spricht man anstelle von Komponentenausfall häufig auch vom Ausfall einer Funktion (oder eines Funktionselements). Ähnliches gilt für die Verwendung des Begriffs Funktion im Zusammenhang mit den Systemen.

Neben dem Aufbau des Systems ist in der Zuverlässigkeitsanalyse auch dessen Betriebsweise zu berücksichtigen. So werden z.B. Notstromerzeugungsanlagen erst bei Bedarf zugeschaltet, während bestimmte Kühlwasserversorgungen ständig in Betrieb sind.

Wird eine Systemfunktion zu einem gewissen Zeitpunkt, nämlich bei Anforderung, benötigt, so bezeichnet man die Versagenswahrscheinlichkeit zu diesem Zeitpunkt als Nichtverfügbarkeit. Ist hingegen die Systemfunktion über eine bestimmte Zeitspanne aufrechtzuerhalten, spricht man von Ausfallwahrscheinlichkeit.

3.1.2 Zuverlässigkeitskenngrößen

Die zu erwartenden Eintrittshäufigkeiten der auslösenden Ereignisse werden generell anhand von Beobachtungen abgeleitet: Entweder werden Schätzwerte dieser Häufigkeit direkt aus den Be-

triebserfahrungen gewonnen (z.B. für das Eintreten von Rohrleitungslecks) oder das auslösende Ereignis wird in Unterereignisse zerlegt, für die Betriebserfahrungen vorliegen (z.B. beim Notstromfall). Die Anzahl der beobachteten Ereignisse einer Art kann auf die Zeiteinheit "Jahr" bezogen werden. Die zugehörige Häufigkeit stellt einen Mittelwert dar, mit dem der Eintritt eines Ereignisses pro Jahr zu erwarten ist. Die Häufigkeit kann also durchaus größer als 1 sein und ist nicht mit der Wahrscheinlichkeit eines Ereignisses zu verwechseln, die definitionsgemäß zwischen 0 und 1 liegt.

Die Wahrscheinlichkeiten für das Versagen der Systemfunktionen werden mit Hilfe einer Zuverlässigkeitsanalyse ermittelt, in der vom Ausfall der Komponentenfunktionen auf den Ausfall der Systemfunktionen hochgerechnet wird. Komponenten im Sinne der Zuverlässigkeitsanalyse sind dabei nicht nur Bauteile, sondern auch Verfahrensvorschriften und Personen, die in den Betrieb eingreifen. Dabei wird jeder Funktion einer Komponente der zu untersuchenden Systeme ein unabhängiges Funktionselement zugeordnet /F2, 3-1 und -2/. Darüber hinaus kann auch, zur Beschreibung von "common mode"-Ausfällen (CMA), einer bestimmten Funktion von mehreren redundanten Komponenten ein einziges Funktionselement zugeordnet werden.

Das Ausfallverhalten eines Funktionselementes läßt sich auf eine der beiden folgenden Arten beschreiben (Fachband 3):

- durch eine Ausfallrate λ

  Unter der Ausfallrate wird die relative Abnahme des Bestandes an noch nicht ausgefallenen Funktionselementen verstanden, die pro Zeiteinheit eintritt.

- durch eine Ausfallwahrscheinlichkeit pro Anforderung p

  Unter der Ausfallwahrscheinlichkeit pro Anforderung wird die Wahrscheinlichkeit verstanden, daß bei Anforderung des Funktionselementes ein Ausfall vorliegt (die Komponentenfunktion also in dem vor der Anforderung liegenden Zeitraum ausgefallen ist oder spätestens zum Anforderungszeitpunkt ausfällt).

Beide Größen sind ihrem Wesen nach Erfahrungswerte. Sie werden

also durch die statistischen Auswertungen von Beobachtungen ermittelt, die beim betrieblichen Einsatz entsprechender Einrichtungen (oder in geringerem Umfang in Laborversuchen) gemacht werden.

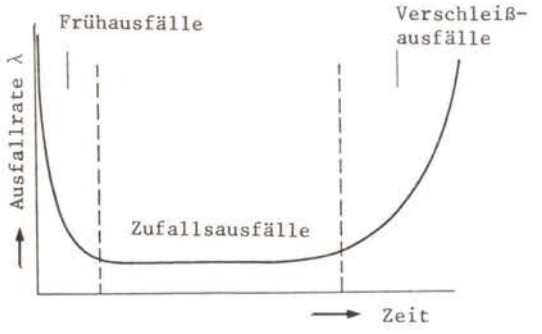


Bild F2, 3-1:
Zeitverhalten der Ausfallrate

In der Regel findet man ein Zeitverhalten der Ausfallrate λ, das man als "Badewannenkurve" bezeichnet (Bild F2, 3-1). Zu Anfang des betrieblichen Einsatzes besteht die Möglichkeit von sogenannten Frühausfällen: Fehler, z.B. aus der Fertigung, die trotz Qualitätssicherung und Inbetriebnahmeprüfungen nicht entdeckt wurden, können zu einer erhöhten Ausfallrate führen. Die Zahl der fehlerhaften Komponenten nimmt mit fortschreitender Zeit ständig ab, bis nur noch Komponenten des üblichen Qualitätsniveaus übrigbleiben. Am Ende der Lebensdauer der Komponenten kann die Ausfallrate infolge von Verschleißausfällen und Alterung zunehmen. Während des wesentlichen Teiles der Einsatzzeit wird das Ausfallverhalten jedoch nicht von einer derartigen systematischen Ausfallursache bestimmt, es kann mit einer konstanten Ausfallrate gerechnet werden. Man spricht von Zufallsausfällen. Es liegt dann eine Exponentialverteilung vor, d.h., die Verteilungsfunktion der Ausfallwahrscheinlichkeit $q(t)$ einer Komponentenfunktion in Abhängigkeit von der Einsatzzeit t ist durch

$$q(t) = 1 - \exp(-\lambda t) \qquad (3.1)$$

gegeben.

Obwohl bei Kernkraftwerken dem Auftreten von Früh- und Verschleißausfällen durch Verwendung betriebsbewährter Komponenten, Qualitätskontrollen und Wiederholungsprüfungen entgegengewirkt wird, ist eine Zeitabhängigkeit über die gesamte Einsatzzeit nicht auszuschließen. Aus den Betriebserfahrungen erhält man dann Mittelwerte für die Ausfallraten bzw. Ausfallwahrscheinlichkeiten. Diese konstanten Werte werden in den Zuverlässigkeitsanalysen verwendet.

Von den beiden Darstellungsarten (durch eine Ausfallrate oder eine Ausfallwahrscheinlichkeit pro Anforderung) für das Ausfallverhalten der Komponenten wird im allgemeinen die Beschreibung durch eine Ausfallrate verwendet. Wird eine solche Komponente regelmäßig im Zeitabstand T überprüft, so kann die Ausfallwahrscheinlichkeit pro Anforderung p der Komponente zum Zeitpunkt T durch

$$p = 1 - \exp(-\lambda T)$$
$$p \cong \lambda T \quad (\text{für } \lambda T << 1) \qquad (3.2)$$

beschrieben werden. Diese Wahrscheinlichkeit p kann auch für Zeiten $t < T$ als pessimistische Abschätzung verwendet werden.

Eine Beschreibung durch eine konstante Ausfallwahrscheinlichkeit pro Anforderung ist auch dann zu wählen, wenn das Versagen erst als Folge der Anforderung hervorgerufen wird, wie z.B. bei menschlichen Eingriffen.

Die Daten zur Beschreibung des Ausfallverhaltens der unterschiedlichen Funktionselemente sind im Fachband 3 zusammengestellt. Es sind in erster Linie Daten für unabhängige Ausfälle der Komponenten. Da für die CMA nur in beschränktem Umfang Daten vorliegen, sind eigene Zuverlässigkeitsanalysen notwendig, um den Einfluß von CMA abzuschätzen (Abschnitt 3.3). Eine besondere Stellung nimmt das menschliche Fehlverhalten ein, bei dem Zuverlässigkeitsabschätzungen für unterschiedliche Handlungen erforderlich sind, die als Funktionselemente in die Fehlerbaumanalysen eingehen (Abschnitt 3.4).

Bisher wurde nur das Ausfallverhalten der Funktionselemente behandelt. Es ist jedoch zu berücksichtigen, daß auch eine Instandhaltung /F2, 3-3 und -4/ der Komponenten gegeben ist. Unter dem Begriff "Instandhaltung" sind zusammengefaßt:

- Instandsetzung, d.h. die Reparatur ausgefallener Komponenten,
- Wartung, das sind regelmäßig vorbeugende Maßnahmen,
- Inspektionen, z.B. regelmäßige Funktionsprüfungen.

Vom Ausfall bis zum Abschluß der Instandsetzung ist ein Funktionselement als ausgefallen anzusehen. Dabei wird folgendes in Rechnung gesetzt:

- Häufigkeit der Funktionsanforderungen bzw. zeitlicher Abstand zwischen den regelmäßigen Funktionsprüfungen (Inspektionen) und deren Staffelung bei nicht selbstmeldenden Ausfällen; im allgemeinen sind zumindest jährliche Funktionsprüfungen (beim Brennelementwechsel) vorgesehen;
- sofortige Instandsetzung, sobald ein Ausfall erkannt wird;
- Einstufung eines Funktionselements als neuwertig nach erfolgreich durchgeführter Instandhaltung.

Nicht selbstmeldend ist der Ausfall eines Funktionselements dann, wenn er im Moment des Auftretens nicht zwangsläufig gemeldet wird.

Sind für die Systemfunktionen verschiedene Funktionen einer Komponente wichtig, so sind die zugehörigen unterschiedlichen Ausfallarten der Komponente zu berücksichtigen, d.h., in die Fehlerbaumanalyse gehen unterschiedliche Funktionselement-Ausfälle einer Komponente ein. Diese Ausfälle werden näherungsweise als voneinander unabhängig betrachtet.

Neben den Instandsetzungen einer Komponente aufgrund des untersuchten Funktionselement-Ausfalls ist noch mit Instandsetzungen der Komponente aufgrund von anderen, z.B. ungefährlichen Ausfällen und mit Wartungen zu rechnen. Während solcher Instandsetzungen und Wartungen kann es nötig sein, die Komponente vorübergehend auszubauen oder freizuschalten, so daß sie dann auch die untersuchte Funktion nicht mehr ausführen kann. Werden die-

se Instandsetzungs- und Wartungsarbeiten, die eine Außerbetriebnahme der Komponente erforderlich machen, während des Leistungsbetriebs der Anlage durchgeführt, so können sie von Einfluß auf die Systemfunktion sein. Alle Instandsetzungs- und Wartungsarbeiten an einer Komponente werden daher gemeinsam berücksichtigt (Abschnitt 3.5).

Außerdem kann während der Funktionsprüfungen der Sicherheitssysteme der getestete Teil für eine andere als die überprüfte Funktion ausgefallen sein. Wegen der hier anzusetzenden kurzen Zeitspannen kann dieser Einfluß aber vernachlässigt werden (Abschnitt 5.1).

3.2 Die Methode der Fehlerbaumanalyse

3.2.1 Allgemeines

Für die Untersuchung großer Systeme hat sich die Fehlerbaumanalyse bewährt, bei der man das unerwünschte Ereignis, den sogenannten TOP des Fehlerbaums, vorgibt und nach allen Ursachen sucht, die zu diesem Ereignis führen /F2, 3-1, -2 und -5/. Dabei ergibt sich eine Vielzahl von Ausfallkombinationen jeweils mehrerer Funktionselemente, die zum Ausfall von Teilsystemen führen. Der Ausfall eines Teilsystems kann entweder direkt oder in Kombination mit Ausfällen anderer Teilsysteme das unerwünschte Ereignis zur Folge haben.

Bild F2, 3-2 zeigt einen Ausschnitt aus einem Teilfehlerbaum, in dem der Ausfall eines Notstromdieselaggregats bei Anforderung im Notstromfall behandelt wird. Der Ausfall von Funktionselementen wird dabei durch Kreise dargestellt. So bedeutet z.B. der Kreis mit der Inschrift "1 VE31 S002 ön" den Ausfall der Funktion ÖFFNEN der Armatur 1 VE31 S002 (primäres Versagen der Armatur). Außerdem sind in Bild F2, 3-2 Überträge aus anderen Teilsystemen dargestellt, wie z.B. der Übertrag aus dem Teilfehlerbaum des Reaktorschutzsystems für den Ausfall des Notstromsignals. Ausgangspunkt für diesen Ausschnitt aus einem Gesamtfehlerbaum für einen bestimmten Störfall war, daß es für die Funk-

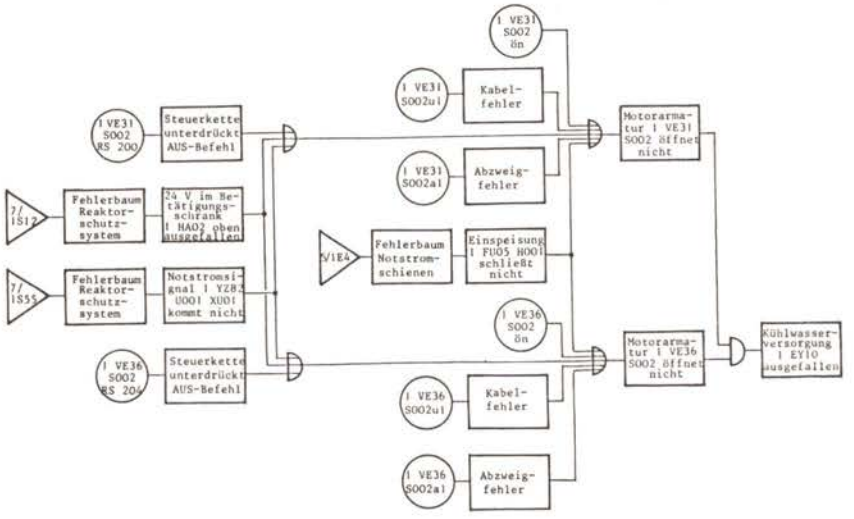


Bild F2, 3-2:
Ausschnitt aus einem Fehlerbaum

tion der Kühlwasserversorgung des untersuchten Notstromdieselaggregats notwendig ist, daß eine der beiden betrachteten Motorarmaturen öffnet. Dies bedeutet im Fehlerbaum, daß die Kühlwasserversorgung dann ausfällt, wenn die Armatur 1 VE31 S002 und die Armatur 1 VE36 S002 nicht öffnen (logische UND-Verknüpfung). Dabei gibt es jeweils mehrere Möglichkeiten, die zum Versagen einer Armatur führen können (logische ODER-Verknüpfung). Man erkennt, daß es Ausfallursachen gibt, die zum Versagen beider Armaturen führen. Dementsprechend könnten die logischen Verknüpfungen vereinfacht werden. Bei umfangreichen, vermaschten Systemen sind solche Abhängigkeiten aber nicht mehr ohne weiteres erkennbar. Aus diesem Grunde ist es bei der Erstellung von Fehlerbäumen unerläßlich, konsequent vorzugehen und alle Ausfallursachen zu betrachten.

Die bei der Fehlerbaumanalyse verwendeten Sinnbilder sind in Bild F2, 3-3 zusammengestellt. Außer den im obigen Beispiel be-

reits besprochenen UND- sowie ODER-Verknüpfungen findet man in Fehlerbäumen auch noch SEKUNDÄR-Verknüpfungen (Folge-Verknüpfungen). Bei den Rechnungen werden diese Verknüpfungen mit Hilfe einer UND-Verknüpfung und entsprechender Bewertung der Eingänge erfaßt. Statt "Verknüpfung" wird im folgenden auch der Begriff "Gatter" verwendet.

Ziel der Fehlerbaumanalyse ist die qualitative und quantitative Auswertung des Fehlerbaums. Dabei sind die Zuverlässigkeitskenngrößen

- mittlere Nichtverfügbarkeit und
- Ausfallwahrscheinlichkeit

für die untersuchte Funktion des Systems von Interesse /F2, 3-5 und -6/.

Die mittlere Nichtverfügbarkeit m errechnet sich durch zeitliche Mittelung aus der zeitabhängigen Nichtverfügbarkeit u(t)

$$m = \frac{1}{T}\int_0^T u(t)dt = \frac{\text{mittlere Ausfallzeit}}{\text{Betrachtungszeit T}} \qquad (3.3)$$

Die zeitabhängige Nichtverfügbarkeit u(t) einer Systemfunktion zum Zeitpunkt t ist als die Wahrscheinlichkeit definiert, daß diese Funktion zum Zeitpunkt t nicht vorhanden ist. Da die zeitabhängige Nichtverfügbarkeit eine periodische Funktion ist, wird als Betrachtungszeit T die Periodendauer gewählt. Die Periodendauer beträgt im allgemeinen ein Jahr.

Zur Bezeichnung der mittleren Nichtverfügbarkeit wird in diesem Kapitel auch M verwendet. Der Großbuchstabe M wird gewählt, wenn die mittlere Nichtverfügbarkeit eine Zufallsgröße in Abhängigkeit von den Verteilungen der Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung ist (Abschnitt 3.2.4).

Für Zuverlässigkeitsanalysen in der Kernkraftwerkstechnik sind häufig die mittleren Nichtverfügbarkeiten der Systemfunktionen relevant. Diese Funktionen müssen nämlich bei Anforderung zum

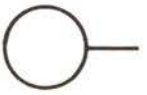
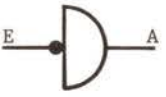
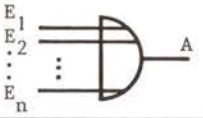
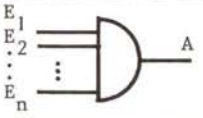
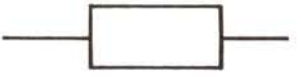
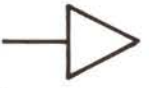
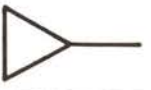
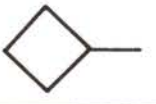
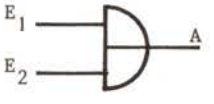
Benennung und Bildzeichen		Bemerkungen
Standardeingang		Das Bildzeichen steht für einen Funktionselementausfall, wenn primäres Versagen möglich ist.
NICHT-Verknüpfung		Die NICHT-Verknüpfung steht für die Negation. Ist der Eingang E der Verknüpfung "0", so ist der Ausgang A "1" und umgekehrt.
ODER-Verknüpfung		Die ODER-Verknüpfung steht für die logische Vereinigung. Der Ausgang A ist "1", wenn mindestens einer der Eingänge E_i "1" ist.
UND-Verknüpfung		Die UND-Verknüpfung steht für den logischen Durchschnitt. Der Ausgang A ist "1", wenn alle Eingänge $E_1,\ldots,E_n$ "1" sind.
Kommentar		Beschreibungen von Eingängen bzw. Ausgängen von Verknüpfungen werden in Rechtecke eingetragen.
Übertragungsausgang		Mit einem Übertragungsbildzeichen wird der Fehlerbaum abgebrochen bzw. an anderer Stelle fortgesetzt.
Übertragungseingang		
Sekundäreingang		Das Bildzeichen wird als ein Eingang der SEKUNDÄR-Verknüpfung verwendet.
SEKUNDÄR-Verknüpfung		Die SEKUNDÄR-Verknüpfung steht für das Entstehen eines Sekundärausfalls aus einem Primärausfall. Ändert sich E_1 von "0" nach "1", so wird mit einer durch den Sekundäreingang E_2 angegebenen Wahrscheinlichkeit und Dauer der Ausgangszustand A der Verknüpfung von "0" nach "1" geändert.

Bild F2, 3-3:
Darstellung der wichtigsten Sinnbilder der Fehlerbaumanalyse

Zeitpunkt eines Störfalls verfügbar sein, wobei davon ausgegangen werden kann, daß die Störfälle zu jedem beliebigen Zeitpunkt des Betrachtungszeitraums mit gleicher Wahrscheinlichkeit eintreten.

Die Ausfallwahrscheinlichkeit q(t) einer Systemfunktion ist definiert als die Wahrscheinlichkeit, daß diese Funktion innerhalb der Zeitspanne [0,t] ausfällt.

Bei der Fehlerbaumanalyse werden jedem Funktionselement nur die Zustände "ausgefallen" bzw. "intakt" zugeordnet. Zwischenzustände, wie z.B. Pumpe fördert nur 50 %, werden nicht betrachtet.

Die Auswertung des Fehlerbaums kann mit Hilfe der Booleschen Algebra durchgeführt werden /F2, 3-8/. Dazu wird der Zustand des Systems als ein Boolescher Ausdruck dargestellt, in dem die Funktionselemente mit Booleschen Variablen identifiziert werden, die die Werte "0" für nicht ausgefallen und "1" für ausgefallen annehmen.

Zusammenfassend kann über die Fehlerbaummethode folgendes gesagt werden:

- Sie ermöglicht durch graphische Darstellung eine übersichtliche Behandlung auch von komplexen Systemen. Dies ist für Zuverlässigkeitsuntersuchungen zur Risikoermittlung von Kernkraftwerken von nicht zu unterschätzender Bedeutung, da gewöhnlich sehr umfangreiche Systeme betrachtet werden müssen.
- Sie ermöglicht auch die Behandlung von spezifischen Problemen, wie z.B. die Behandlung von Folgeausfällen, CMA usw.
- Sie ist ein vollständiges Verfahren, d.h., aufgrund der deduktiven Vorhergehensweise liefert sie bei konsequenter Anwendung alle Ereigniskombinationen, die zum unerwünschten Ereignis führen. Grenzen sind nicht vom Verfahren her gesetzt, sondern nur von der Kenntnis und Sorgfalt des Anwenders sowie von der Aufgabenstellung. Man wird bei umfangreichen Systemen solche Ereigniskombination von vornherein nicht berücksichtigen, deren Eintrittswahrscheinlichkeit gegenüber anderen Ereigniskombinationen als vernachlässigbar abgeschätzt werden kann.

- Sie liefert nicht nur quantitative Ergebnisse, sondern auch qualitative, z.B. ermöglicht sie eine imfangreiche Schwachstellenanalyse.

Aus diesem Grund wurden für die Risikostudie die Zuverlässigkeitsuntersuchungen im allgemeinen als Fehlerbaumanalysen durchgeführt.

Die quantitative Auswertung von Fehlerbäumen ist für komplexe Systeme nur mit Hilfe von EDV-Anlagen möglich. Bei den verwendeten Rechenprogrammen können grundsätzlich

- simulative Verfahren und
- analytische Verfahren

unterschieden werden. Für die simulativen Verfahren ist auch der Begriff "Monte-Carlo-Simulation" gebräuchlich.

3.2.2 Simulative und analytische Verfahren

3.2.2.1 M o n t e - C a r l o - S i m u l a t i o n

Hier handelt es sich um ein Verfahren /F2, 3-9 bis -11/, bei dem zuerst ein dem gegebenen Problem angepaßtes statisches Modell aufgestellt wird und dann die verschiedenen Zufallsgrößen mit Hilfe von Zufallszahlengeneratoren simuliert werden. Im folgenden wird die Monte-Carlo-Simulation anhand der Berechnung der mittleren Nichtverfügbarkeit mit dem Problem CRESSEX /F2, 3-12 bis -14/ erklärt:

Entsprechend der exponentialverteilten Ausfallwahrscheinlichkeit der Komponentenfunktion (Abschnitt 3.1.2) werden in CRESSEX zuerst mit Hilfe eines Zufallszahlengenerators Komponentenausfallzeitpunkte erzeugt bzw. ausgespielt. Anschließend wurde überprüft, ob die Ausfallzeitpunkte innerhalb des Betrachtungszeitraums liegen. Die Anzahl der Ausfälle einer Komponentenfunktion während dieser Zeit ist abhängig von der Ausfallrate λ der Exponentialverteilung $1 - \exp(-\lambda t)$. Nach dem Ausspielen der Ausfallzeitpunkte wird, unter Berücksichtigung von Funktionsprüfungen und Instandsetzungszeiten, mit Hilfe des Fehlerbaums

festgestellt, ob ein Ausfall der Systemfunktion vorliegt. Ist dies der Fall, wird Ausfall- und Wiederherstellungszeitpunkt der Funktion berechnet. Die Differenz zwischen beiden Zeiten ist die Ausfalldauer T_i der betrachteten Systemfunktion in diesem Spiel i. Wegen der meist großen Zuverlässigkeit der Komponenten und wegen des redundanten Systemaufbaus wird natürlich bei der Mehrzahl der Spiele kein solcher Ausfall der Systemfunktion registriert.

Jedes Spiel simuliert also das Ausfallverhalten des realen Systems während der Betrachtungszeit. Die Zahl der ermittelten Systemausfälle hängt damit von der Zuverlässigkeit des realen Systems ab. Schließlich werden die Ausfallzeiträume T_i addiert und durch die Anzahl der Spiele N, multipliziert mit der Betrachtungszeit T, dividiert. Man erhält so die mittlere Nichtverfügbarkeit m der Systemfunktion:

$$m = \frac{1}{N \cdot T} \cdot \sum_{i=1}^{N} T_i \qquad (3.4)$$

Entsprechend der obigen Vorgehensweise ist bei der Monte-Carlo-Simulation das Ergebnis selbst wieder eine Zufallsgröße. Folglich ist es nicht möglich, die mittlere Nichtverfügbarkeit exakt zu bestimmen, sondern es lassen sich "nur" Vertrauensintervalle für m ermitteln. Die Größe des Vertrauensintervalls ist abhängig von der Anzahl der Ausfälle. Bei sehr zuverlässigen Systemen kann daher die gewünschte Genauigkeit oft nur mit hohem Rechenaufwand (Kosten) erreicht werden.

Durch den Einsatz varianzreduzierender Methoden (importance sampling) /F2, 3-10 und -11/ können in manchen Fällen auch noch Systeme mit großer Zuverlässigkeit mittels Monte-Carlo-Simulation untersucht werden. Varianzreduzierende Methoden verlangen vom Anwender sowohl gute Systemkenntnis als auch genaue Kenntnis des verwendeten Verfahrens.

3.2.2.2 Analytische Verfahren

Im Gegensatz zur Monte-Carlo-Simulation sind die Ergebnisse aus den analytischen Rechenverfahren /F2, 3-15/ feste Größen, die keinen Zufallsschwankungen aus dem Rechenverfahren ausgesetzt sind.

Grundlage für analytische Verfahren zur Berechnung von Zuverlässigkeitskenngrößen ist immer die Strukturfunktion /F2, 3-16 bis -18/. Definiert ist die Strukturfunktion $S(\bar{y})$ wie folgt:

$$S(\bar{y}) = S(y_1,\ldots,y_n)$$

$$= \begin{cases} 1 \\ 0 \end{cases} \text{ falls das unerwünschte Ereignis} \begin{cases} \text{eintritt} \\ \text{nicht eintritt} \end{cases}$$

mit

$$y_\mu = \begin{cases} 1 \\ 0 \end{cases} \text{ falls das } \mu\text{-te Primärereignis} \begin{cases} \text{eintritt} \\ \text{nicht eintritt} \end{cases}$$

Primärereignisse sind die Funktionselement-Ausfälle. Die Boolesche Variable y_μ heißt Zustandsvariable des Funktionselements μ und $\bar{y} = (y_1,\ldots,y_n)$ heißt Zustandsvektor der Systemfunktion. Es gibt verschiedene Möglichkeiten der Darstellung und der Ermittlung der Strukturfunktion. Der für große und komplexe Systeme am besten geeignete Weg ist die Ermittlung einer approximierten Strukturfunktion mit Hilfe der minimalen Schnittmengen (minimal cuts). Eine minimale Schnittmenge ist eine minimale Kombination von Funktionselementen, deren Ausfall zum Systemausfall führt. Die minimalen Schnittmengen können mit Hilfe des Fehlerbaums, unter Verwendung der Booleschen Algebra /F2, 3-5, -19 und -20/, oder durch Simulation, wie sie in den Programmen CRESSC und CRESSEX durchgeführt wird, gewonnen werden.

Mit Hilfe der Darstellung der Systemfunktion durch minimale Schnittmengen kann eine gute Näherung der zeitabhängigen Nichtverfügbarkeit u(t) ermittelt werden. Die mittlere Nichtverfügbarkeit erhält man dann durch Integration über die zeitabhängige Nichtverfügbarkeit.

3.2.2.3 Vergleich von simulativen und analytischen Verfahren

Simulative und analytische Verfahren haben spezifische Vor- und Nachteile.

Bei der Simulation können mit geringem mathematischen Aufwand auch sehr große und vermaschte Systeme analysiert werden. Folgeausfälle, Ausfälle gemeinsamer Ursache (CMA), Berücksichtigung von kalten Reserven, Strategien für Funktionsprüfungen und Instandsetzungen können vergleichsweise einfach berücksichtigt werden. Größter Nachteil ist die bereits angesprochene enorme Zunahme der Rechenzeit bei der Analyse sehr zuverlässiger Systeme. Beim Einsatz varianzreduzierender Methoden ist andererseits große Vorsicht geboten.

Bei der analytischen Berechnungsweise spielt hinsichtlich des Rechenaufwandes der Wert der Systemzuverlässigkeit keine Rolle. Hier können jedoch Schwierigkeiten bei sehr großen und sicherheitstechnisch ausgewogenen Systemen auftreten. Die Anzahl der minimalen Schnittmengen, die nötig ist, um eine gute Approximation der Strukturfunktion zu erhalten, kann dann sehr groß werden. Ferner können spezielle Probleme, wie z.B. kalte Reserven, oft nur vereinfacht berücksichtigt werden.

Zusammenfassend kann gesagt werden, daß simulative Verfahren beigroßen und vermaschten Systemen mit nicht zu kleiner Nichtverfügbarkeit bzw. Ausfallwahrscheinlichkeit günstig eingesetzt werden können. Analytischen Methoden ist der Vorzug zu geben, wenn das tatsächliche Systemverhalten hinreichend genau analytisch beschrieben werden kann.

3.2.3 Verwendete Programme zur Fehlerbaumanalyse

3.2.3.1 Allgemeines

Für diese Studie wird zur Berechnung der Zuverlässigkeitskenngrößen der Systeme das Programmsystem RALLY verwendet. Dieses

Programmpaket ist speziell zur Behandlung komplexer und vermaschter Systeme entwickelt worden. Bild F2, 3-4 zeigt eine schematische Darstellung von RALLY, die vor allem die spezifischen Aufgaben der verschiedenen Programme des Systems sowie den Datenfluß zwischen diesen verdeutlicht. Die einzelnen Teile von RALLY werden im folgenden kurz beschrieben.

- Die Basis ist das Daten- und Fehlerbaumaufbereitungsprogramm TREBIL. Es benötigt als Eingabe die logische Struktur des Fehlerbaums sowie Daten über die Komponentenfunktionen (Ausfallraten, Abstände zwischen den Funktionsprüfungen usw.). Mittels dieser Information werden Kontrollisten angelegt, die dem Anwender die Überprüfung des Fehlerbaums erleichtern. Weiterhin wird der Fehlerbaum auf logische Korrektheit untersucht, eventuelle Fehlermeldungen werden ausgedruckt. Wesentlichste Aufgabe von TREBIL ist eine Fehlerbaumoptimierung sowie eine spezifische Datenaufbereitung für die verschiedenen Programme des Programmsystems.
- Das Programm TIMBER zeichnet die Fehlerbäume und ermöglicht so eine Überprüfung der eingegebenen Systemlogik.
- Das Simulationsprogramm CRESSEX /F2, 3-12 bis -14/ bestimmt die Ausfallwahrscheinlichkeit und mittlere Nichtverfügbarkeit der gegebenen Systemfunktion und ermöglicht zusätzlich noch eine Schwachstellenanalyse.
- Das simulativ-analytische Programm STREUSL /F2, 3-21 und -22/ berechnet Erwartungswert und Streuung (Vertrauensintervall) der mittleren Nichtverfügbarkeit bzw. der Ausfallwahrscheinlichkeit der betrachteten Systemfunktion in Abhängigkeit von der Streuung der Ausfallraten bzw. der Ausfallwahrscheinlichkeiten pro Anforderung.
- Das Programm CRESSC ermittelt auf simulative Art die wichtigsten minimalen Schnittmengen des zu untersuchenden Systems und ermöglicht damit die Erstellung einer approximierten Systemfunktion für das Programm STREUSL.

  Zur Bewertung bestimmter Ereignisabläufe benötigt man nur solche minimalen Schnittmengen, die zwar zum Ausfall der untersuchten Systemfunktionen (zum TOP) führen, aber unter der Be-

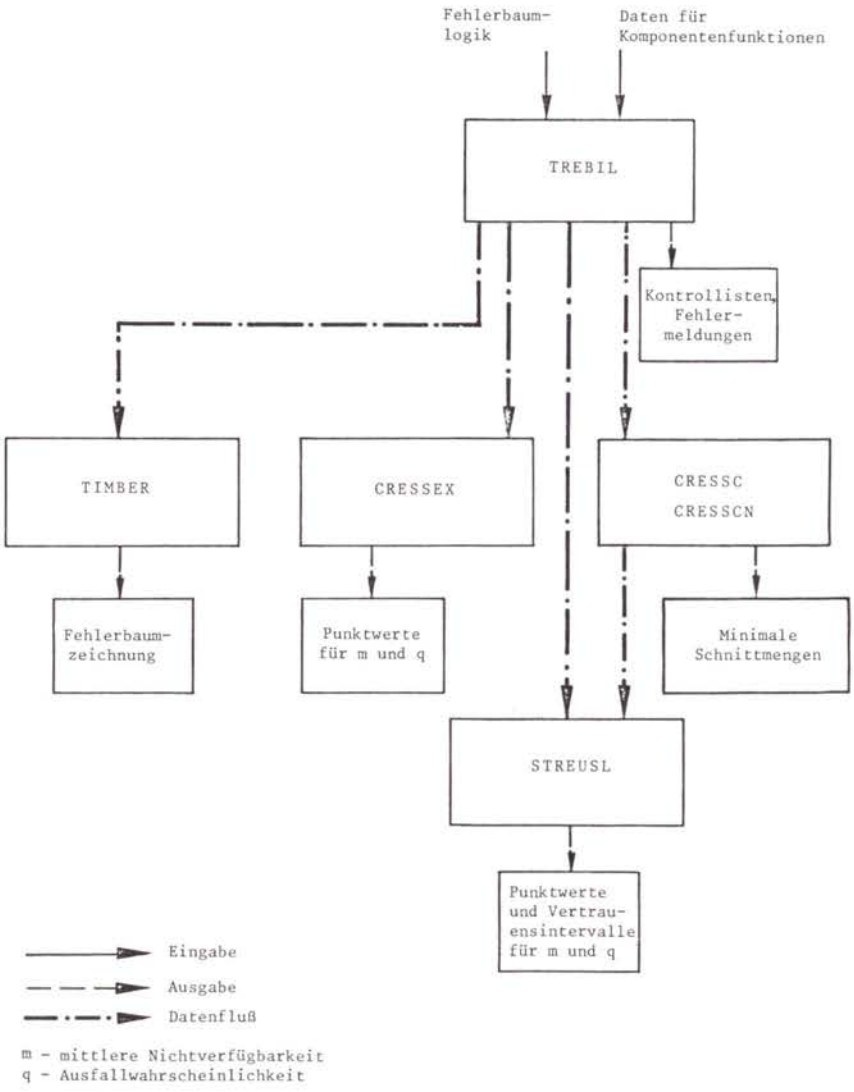


Bild F2, 3-4:
Schematische Darstellung des verwendeten Programmsystems

dingung, daß eine oder mehrere andere Systemfunktionen nicht ausgefallen sind. Dazu wird das Programm CRESSCN verwendet.

Im folgenden sollen die einzelnen Programme, soweit nötig, noch ausführlicher beschrieben werden.

3.2.3.2 Fehlerbaum-Aufbereitungsprogramm TREBIL

TREBIL ist eine Abwandlung bzw. Weiterentwicklung des gleichnamigen Programmes aus dem Programmpaket PREP & KITT /F2, 3-23/. Im wesentlichen hat das Programm folgende Aufgaben:

- Umsetzen der Eingabe

Die bei der Systemanalyse erstellten Fehlerbäume werden in folgender Form eingegeben:

- Gattername, Gattertyp (UND, ODER),
- Eingänge des Gatters (Gatter- bzw.Funktionselementnamen).

Die Reihenfolge der Eingabe der einzelnen Gatter ist beliebig.

Das Programm TREBIL setzt diese Eingabe in Boolesche Logik um, wobei die einzelnen Gatter entsprechend sortiert werden. Daraus wird ein Unterprogramm LOGIDR erstellt, das in CRESSEX und CRESSC(N) Verwendung findet.

Die Funktionselementdaten (z.B. Ausfallraten, Abstände zwischen den Funktionsprüfungen) werden entsprechend der ausgegebenen Fehlerbaumlogik sortiert und zu einem Datensatz zusammengefaßt. Dieser Datensatz dient als Eingabe für die Programme CRESSEX, CRESSC(N) und STREUSL.

- Überprüfung der Eingabe

TREBIL stellt fest, ob in einem Fehlerbaum Zirkularitäten (Rückkopplungen) vorhanden sind. Außerdem werden sogenannte

"cross-reference"-Listen ausgedruckt, die im wesentlichen folgende Zuordnungen festhalten:

- Gattername - Eingänge des Gatters,
- Gatter- bzw. Funktionselementname - Gatter, in die diese eingehen, und
- alphabetisch sortierte Namen der Funktionselemente - Funktionselementdaten.

- Vereinfachung der Fehlerbäume

Um mit RALLY Systeme mit einer großen Anzahl (> 500) von Komponenten noch mit vertretbarem Aufwand an Rechenzeit und Speicherplatz rechnen zu können, ist es in manchen Fällen nötig, die Fehlerbäume etwas zu vereinfachen. So können mehrere Komponenten, deren Funktionen in ein ODER-Gatter eingehen, zu einer Ersatzkomponente zusammengefaßt werden. Voraussetzung für diese Zusammenfassung ist, daß die Funktionsausfälle in kein weiteres Gatter einmünden und die Komponenten zu den gleichen Zeitpunkten Funktionsprüfungen unterzogen werden.

Sind λ die konstanten, logarithmisch normalverteilten Ausfallraten der Komponenten (Abschnitt 3.2.4) eines aus n Komponenten bestehenden Seriensystems, so gilt für die Ausfallwahrscheinlichkeit q(t) dieses Seriensystems bis zum Zeitpunkt t:

$$q(t) = 1 - \exp(-(\lambda_1+\lambda_2+\ldots+\lambda_n)t)$$
$$= 1 - \exp(-\lambda_E \cdot t) \qquad (3.5)$$

wobei λ_E die Ersatzausfallrate der Ersatzkomponente ist. Zur Berechnung von λ_E muß folglich die Summe von n logarithmischen Normalverteilungen berechnet werden (Abschnitt 3.2.5.3).

Analog lassen sich auch Komponenten, denen eine Ausfallwahrscheinlichkeit pro Anforderung zugeordnet ist, zu einer Ersatzkomponente zusammenfassen.

3.2.3.3 Fehlerbaum-Plotprogramm TIMBER

Das Plotprogramm TIMBER dient zur Dokumentation und erleichtert dem Anwender die Überprüfung des eingegebenen Fehlerbaums. Die Eingabe der Fehlerbaumlogik ist deshalb identisch mit derjenigen für TREBIL.

Die Zeichnung eines Fehlerbaums mittels des Programms TIMBER ist abhängig von der Reihenfolge der Eingabe der Funktionselemente und Gatter, da TIMBER die graphische Struktur eines Fehlerbaums nicht optimiert. Auf eine Optimierung wurde absichtlich verzichtet, da sonst bei komplexen Fehlerbäumen eine Überprüfung der Eingabe nur noch schwer möglich ist. Bei den Zeichnungen durch TIMBER werden die in Bild F2, 3-2 aufgeführten Bildzeichen verwendet. Durch Steuerparameter können für die Funktionselemente wahlweise Kommentare oder die verwendeten Zuverlässigkeitskenngrößen in die Kommentarkästen eingeschoben werden (Fachband 2/II).

3.2.3.4 Fehlerbaum-Rechenprogramm CRESSEX

Das Simulationsprogramm CRESSEX ermöglicht die Berechnung der Ausfallwahrscheinlichkeit und mittleren Nichtverfügbarkeit für komplexe technische Systeme /F2, 3-12 bis -14/. Das Programm simuliert für die vorgegebene Systemfunktion das Ausfallverhalten der einzelnen Funktionselemente ohne varianzreduzierende Methoden. Dabei können berücksichtigt werden:

- verschiedene Strategien bei der Durchführung von Funktionsprüfungen (z.B. zeitlich versetzte Funktionsprüfungen von redundanten Komponenten /F2, 3-24 und -25/);
- Ausfallverhalten der Komponentenfunktionen, die entweder durch eine konstante Ausfallrate oder durch eine konstante Ausfallwahrscheinlichkeit pro Anforderung beschrieben werden;
- Erkennungszeitpunkt eines Komponentenausfalls (selbstmelden-

der, d.h. sofort erkannter Ausfall oder erst bei der Funktionsprüfung erkannter Ausfall);
- konstante Instandsetzungszeiten der Komponenten.

Der Simulationsvorgang wird sehr oft wiederholt. Die in den Spielen vom Zufall abhängigen Zwischenergebnisse, wie z.B.

- Eintreten eines Systemausfalls,
- Ausfalldauer der Systemfunktion,
- am Ausfall beteiligte Komponentenfunktionen,

werden gespeichert und am Ende der Rechnung statistisch ausgewertet. Für die Erwartungswerte $\bar{q}$ und $\bar{m}$ der Ausfallwahrscheinlichkeit q und der mittleren Nichtverfügbarkeit m und für die zugehörigen Streuungen $D^2(q)$ und $D^2(m)$ berechnen sich folgende Schätzwerte:

$$\bar{q} = \frac{N_1}{N} \qquad D^2(q) = \frac{\bar{q}\cdot(1-\bar{q})}{N-1} \tag{3.6}$$

$$\bar{m} = \frac{\sum_{i=1}^{N} T_i}{N\cdot T} \qquad D^2(m) = \frac{1}{(N-1)} \sum_{i=1}^{N} (m_i-\bar{m})^2 \qquad m_i = \frac{T_i}{T} \tag{3.7}$$

Dabei ist N Anzahl der Spiele, T_i Ausfalldauer im i-ten Spiel, N_1 Anzahl der Systemausfälle (nur Erstausfälle), T Betrachtungszeit, m_i Nichtverfügbarkeit im i-ten Spiel.

Mit Hilfe der Streuungen $D^2(q)$ und $D^2(m)$ ist es möglich, die Genauigkeit der Erwartungswerte $\bar{q}$ und $\bar{m}$ abzuschätzen.

Neben der Berechnung der Erwartungswerte für die Ausfallwahrscheinlichkeit und die mittlere Nichtverfügbarkeit werden in CRESSEX noch zusätzlich die Komponentenfunktionen nach

- der Anzahl der Ausfälle und
- dem Beitrag zur mittleren Nichtverfügbarkeit

geordnet und die bei der Simulation aufgetretenen minimalen Schnittmengen ausgegeben. Diese Informationen können dann zur Schwachstellenanalyse herangezogen werden.

3.2.3.5 S t r e u b r e i t e n - R e c h e n p r o g r a m m S T R E U S L

Das Programm CRESSEX berechnet für die mittlere Nichtverfügbarkeit einer Systemfunktion nur einen Punktwert, d.h., statistische Unsicherheiten in den Eingabedaten werden nicht berücksichtigt. Bei der Bestimmung der Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung treten jedoch Unsicherheiten auf, die man mittels Verteilungsfunktionen (meist logarithmische Normalverteilungen /F2, 3-26/) beschreibt (Fachband 3).

Während im Programm CRESSEX nur Punktwerte, z.B. die Erwartungswerte der entsprechenden Verteilungen berücksichtigt werden, berechnet STREUSL /F2, 3-21 und -22/ Verteilungen und Vertrauensbereiche für die Nichtverfügbarkeit bzw. Ausfallwahrscheinlichkeit der betrachteten Systemfunktion in Abhängigkeit von den Verteilungen der Eingangsparameter (Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung).

In STREUSL behandelbare Verteilungen für die Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderungen sind:

- Normalverteilung,
- logarithmische Normalverteilung,
- Uniform- und logarithmische Uniformverteilung,
- Betaverteilung,
- χ^2-Verteilung.

Um Mißverständnissen vorzubeugen, sei nochmals erwähnt, daß bei einer Komponentenfunktion, deren Ausfallverhalten durch eine konstante Ausfallrate beschrieben wird, nur diese Ausfallrate λ eine der oben angeführten Verteilungen besitzt. Die Ausfallwahrscheinlichkeit der Komponentenfunktion (Lebensdauerverteilung) selbst besitzt immer die Verteilung $q(t) = 1 - \exp(-\lambda t)$.

Die Berechnung der mittleren Nichtverfügbarkeit bzw. Ausfallwahrscheinlichkeit der Systemfunktion in Abhängigkeit der Verteilungen für die Eingabedaten erfolgt im Programm STREUSL in einem simulativen und einem analytischen Teil. Im simulativen Teil wird in jedem Spiel aufgrund der Verteilungen der Para-

meter eine Kombination von Werten für die Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung der Funktionselemente ausgespielt. Mittels dieser Kombination wird dann die Nichtverfügbarkeit der untersuchten Systemfunktion analytisch berechnet. Grundlage für die analytische Berechnung ist die Approximation der Strukturfunktion /F2, 3-16 bis -18/ des betrachteten Systems mit Hilfe der minimalen Schnittmengen. Diese minimalen Schnittmengen können mit den Programmen CRESSEX, CRESSC oder CRESSCN gewonnen werden.

Mit Hilfe der Strukturfunktion und der pro Spiel ermittelten Werte für die Eingangsparameter erhält man in STREUSL eine Stichprobe (der Probenumfang sollte ≧ 100 sein) von mittleren Nichtverfügbarkeiten bzw. Ausfallwahrscheinlichkeiten, die dann im letzten Abschnitt des Programms mittels verschiedener Methoden ausgewertet werden, und zwar:

- Berechnung von Median, Erwartungswert und Streuung der Verteilung und Ermittlung der Dichtefunktion (Bild F2, 3-5),
- Auswertung mittels "order statistics" /F2, 3-27/ (Vertrauensintervalle für verschiedene Fraktilen),
- Auswertung mittels approximierender Verteilungsfunktionen (Bild F2, 3-5) (z.B. Normalverteilung, logarithmische Normalverteilung).

Zur Untersuchung von CMA bietet STREUSL noch die Möglichkeit der Ausfallraten-Kopplung. Dabei wird für die redundanten Komponentenfunktionen, die im Ausfallverhalten gekoppelt werden sollen, nur eine Zufallszahl für die Ausfallrate bzw. Ausfallwahrscheinlichkeit pro Anforderung je Spiel ausgespielt (Abschnitt 3.3.5.6).

3.2.3.6 Programme zur Ermittlung von minimalen Schnittmengen

- Programm CRESSC

Das Programm CRESSC ermittelt auf simulativer Basis die wichtigsten minimalen Schnittmengen (Beitrag zur mittleren Nichtverfüg-

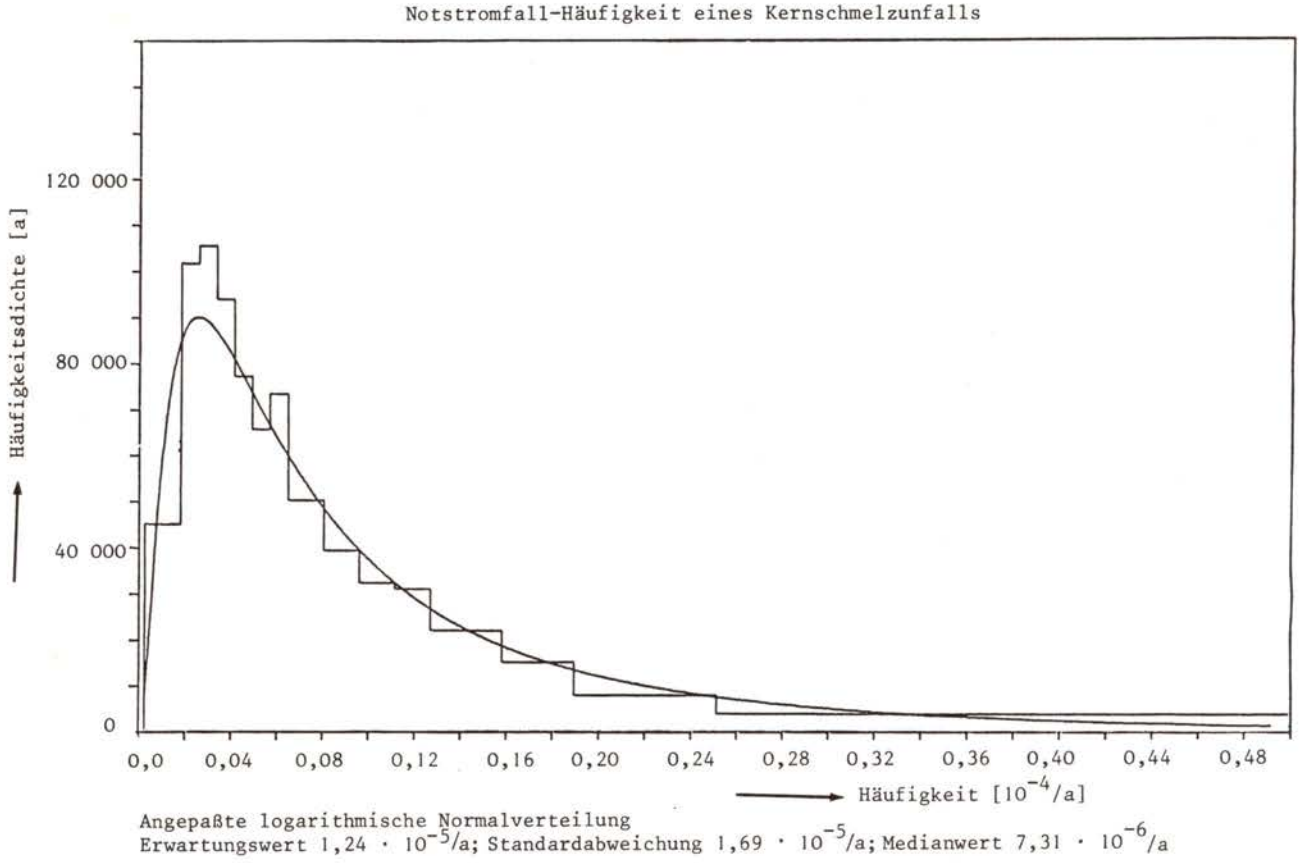


Bild F2, 3-5:

Histogramm und approximierte logarithmische Normalverteilung, erstellt vom Streubreitenrechenprogramm STREUSL

barkeit bzw. Ausfallwahrscheinlichkeit) einer Systemfunktion und ermöglicht damit die Erstellung einer approximierten Strukturfunktion, die für das Programm STREUSL verwendet wird.

Analog wie bei CRESSEX wird entsprechend dem Ausfallverhalten der Funktionselemente das Ausfallgeschehen der Systemfunktion simuliert. Da die Aufgabe des Programms nur die Ermittlung der wichtigsten minimalen Schnittmengen ist (und nicht die Berechnung von Zuverlässigkeitskenngrößen), kann auf die Berechnung von Ausfallzeitpunkt, Ausfalldauer usw. verzichtet werden, was im Vergleich zu CRESSEX zu einer wesentlichen Verkürzung der Rechenzeit führt. Ferner wird, um genügend Systemausfälle zu erhalten, der Betrachtungszeitraum vom Programm so gesteuert, daß ungefähr bei jedem zweiten Spiel ein Systemausfall auftritt. Da die Simulation das wirkliche Ausfallgeschehen des Systems widerspiegelt, ist anzunehmen, daß diejenigen minimalen Schnittmengen, die den größten Beitrag zur Ausfallwahrscheinlichkeit bzw. mittleren Nichtverfügbarkeit liefern, sehr bald eintreten werden. Am Ende eines Rechenlaufs werden die ermittelten minimalen Schnittmengen ihrer "Größe" (d.h. ihrem Beitrag zur mittleren Nichtverfügbarkeit oder Ausfallwahrscheinlichkeit) nach geordnet. Zur Approximation der Strukturfunktion für das Programm STREUSL genügen meist die ersten 1000-2000 der so errechneten minimalen Schnittmengen. Man muß allerdings, um wirklich die wichtigsten 1000-2000 zu erhalten, zunächst wesentlich mehr minimale Schnittmengen erzeugen.

- Programm CRESSCN

Das Programm CRESSCN dient zur Ermittlung bestimmter minimaler Schnittmengen von Systemfunktionen, wie im folgenden erläutert wird. Zur Berechnung der Ausfallwahrscheinlichkeit bzw. mittleren Nichtverfügbarkeit bestimmter Ereignisabläufe im Ereignisablaufdiagramm (Fachband 1) benötigt man nur solche minimalen Schnittmengen, die zwar zum Ausfall der untersuchten Systemfunktion führen, aber nur unter der Bedingung, daß andere Systemfunktionen nicht ausgefallen sind (z.B. Ausfall der ND-EINSPEISUNG FÜR SUMPF-UMWÄLZBETRIEB unter der Bedingung, daß die ND-EINSPEI-

SUNGEN FÜR FLUTEN intakt sind). Bei der weiteren Berechnung werden die Wahrscheinlichkeiten, daß diese Systemfunktionen nicht ausgefallen sind, nicht mehr berücksichtigt, d.h. = 1 gesetzt. Somit kommt es zu einer Erhöhung der berechneten mittleren Nichtverfügbarkeit bzw. Ausfallwahrscheinlichkeit der untersuchten Systemfunktion. Diese Konservativität ist jedoch gering, wenn die Wahrscheinlichkeiten, daß die anderen Systemfunktionen nicht ausgefallen sind, nahe bei 1 liegen.

Der verwendete Algorithmus entspricht CRESSC, nur muß bei jedem Ausfall der Systemfunktion mit Hilfe des Fehlerbaums überprüft werden, ob die entsprechenden anderen Systemfunktionen nicht ausgefallen sind. Nur Ausfallkombinationen, bei denen diese Bedingung erfüllt ist, werden zur Ermittlung der minimalen Schnittmengen verwendet. Minimale Schnittmengen, die unvereinbare Ereignisse enthalten, müssen also eliminiert werden.

Neben dieser simulativen Ermittlung gibt es noch Möglichkeit der analytischen Berechnung der minimalen Schnittmengen der Systemfunktionen mit Hilfe der Booleschen Gleichungen des Fehlerbaums. Die analytischen Methoden erfordern jedoch bei großen Systemen, vor allem bei nicht optimaler Programmierung, sehr viel Speicherplatz und Rechenzeit /F2, 3-19/.

3.2.4 Berechnung der Ausfallwahrscheinlichkeit und mittleren Nichtverfügbarkeit mit den Erwartungswerten

In dieser Studie werden die Ausfallraten λ_i bzw. Ausfallwahrscheinlichkeiten pro Anforderung p_j für die Funktionselemente als (meist logarithmisch normalverteilte) Zufallsgrößen Λ_i bzw. P_j betrachtet. Die mittlere Nichtverfügbarkeit M der Systemfunktion (Analoges gilt auch für die Ausfallwahrscheinlichkeit) ist folglich eine Funktion dieser Zufallsgrößen Λ_i bzw. P_j und des Beobachtungszeitraumes T:

$$
\begin{aligned}
M &= M(T,\Lambda_1,\ldots,\Lambda_k,P_1,\ldots,P_l) \\
&= M(T,\theta) \\
&= \frac{1}{T}\int_0^T u_s(t,\theta)dt
\end{aligned}
\tag{3.8}
$$

mit

$$\theta = (\Lambda_1,\ldots,\Lambda_k,P_1,\ldots,P_l)$$

wobei $u_s(t,\theta)$ die zeitabhängige Nichtverfügbarkeit des Systems zum Zeitpunkt t als Funktion von θ ist. $M(T,\theta)$ ist also eine eindimensionale Zufallsgröße und besitzt damit selbst eine Verteilung. Bei der Berechnung eines Punktwertes für M werden die Erwartungswerte $E(\Lambda_i)$ bzw. $E(P_j)$ verwendet. Der Erwartungswert ist deshalb zu verwenden, weil sich nur bei ihm die Beträge der Unter- bzw. Überschätzung, gewichtet mit den Wahrscheinlichkeiten ihres Zutreffens, die Waage halten. Ferner gilt, daß M, berechnet mit $E(\Lambda_i)$ und $E(P_j)$, in erster Näherung gleich ist dem Erwartungswert der mittleren Nichtverfügbarkeiten E(M), d.h.

$$
\begin{aligned}
E(M) = E(M(T,\theta)) &= E\left(\frac{1}{T}\int_0^T u_s(t,\theta)dt\right) \\
&\cong \frac{1}{T}\int_0^T u_s(t,E(\theta))dt \;=\; M(T,E(\theta))
\end{aligned}
\tag{3.9}
$$

Berechnet man also die mittlere Nichtverfügbarkeit des Systems mit den Erwartungswerten $E(\Lambda_i)$ und $E(P_j)$, so erhält man meist eine sehr gute Approximation des Erwartungswertes der mittleren Nichtverfügbarkeit. Die Abweichung

$$E(M(T,\theta)) - M(T,E(\theta)) \tag{3.10}$$

ist meistens im Bereich der Ungenauigkeit der Eingabedaten, wird allerdings um so größer, je schlechter bei den Komponenten mit einer zeitabhängigen Nichtverfügbarkeit die Approximation $1 - \exp(-\lambda T) \cong \lambda T$ ist. Verwendet man dagegen die Mediane

zur Berechnung der mittleren Nichtverfügbarkeit, so ist der so berechnete Wert

$$M(T,\theta_{50\ \%}) \qquad (3.11)$$

schwer zu bewerten, denn $M(T,\theta_{50\ \%})$ ist im allgemeinen weder gleich dem Median von M noch eine Näherung für den Erwartungswert E(M). Eine analoge Betrachtungsweise ist auch für die Ausfallwahrscheinlichkeit $Q(T,\theta)$ möglich.

3.2.5 Die logarithmische Normalverteilung

3.2.5.1 A l l g e m e i n e s

Zur Beschreibung der Zuverlässigkeitskenngrößen als Zufallsvariable können grundsätzlich verschiedene Arten von Verteilungsfunktionen verwendet werden. Während z.B. die Normalverteilung ein gutes Mittel ist, um Bandbreiten zu beschreiben, die innerhalb einer Größenordnung liegen, können dagegen mit der logarithmischen Normalverteilung auf einfache Weise Daten beschrieben werden, die sich um größere Faktoren unterscheiden.

In der Risikostudie werden generell logarithmische Normalverteilungen verwendet, nachdem die Daten meistens große Bandbreiten besitzen. Diese Vorgehensweise entspricht derjenigen in WASH-1400. Da die logarithmische Normalverteilung für die Ermittlung der interessierenden Häufigkeiten von großer Bedeutung ist, wird im folgenden sowohl auf die Eigenschaften als auch auf die wichtigsten Rechenregeln eingegangen.

Die logarithmische Normalverteilung besitzt folgende Eigenschaften:

- Sie ordnet Werten ≤ 0 die Wahrscheinlichkeit 0 zu. Damit berücksichtigt sie die Tatsache, daß die Werte aller hier interessierenden Größen positiv sind.
- Da sie zwei Parameter besitzt, paßt sie sich vielen empirischen Verteilungen recht gut an.

- Sie ist das geeignete Zufallsgesetz für Größen, die selbst Produkt vieler Zufallsgrößen sind.
- Der Erwartungswert einer logarithmischen Normalverteilung ist größer als ihr Median. Dadurch kommt die Eigenschaft zum Ausdruck, Bereiche hoher Werte stärker zu berücksichtigen, als eine Normalverteilung mit gleichen 5-%- und 50-%-Fraktilen.

Definiert ist die logarithmische Normalverteilung wie folgt: Eine Zufallsgröße Y heißt "logarithmisch normalverteilt", wenn die Zufallsgröße X = ln Y normalverteilt ist. Sie ist durch Erwartungswert und Streuung eindeutig bestimmt.

Durch die Abbildung Y = exp(X) werden die P-%-Fraktilen von X auf die P-%-Fraktilen von Y abgebildet, d.h.

$$y_{P\ \%} = \exp(x_{P\ \%}) \tag{3.12}$$

Ist X eine normalverteilte Zufallsgröße mit Erwartungswert ln ξ und Streuung σ^2, d.h. $X \sim N(\ln \xi, \sigma)$, dann gilt für Y = exp(X):

$$\frac{y_{95}}{y_{50}} = \frac{\exp(x_{95})}{\exp(x_{50})} = \exp(x_{95} - x_{50})$$

$$= \exp(\sigma \cdot u_{95} + \ln\xi - \ln\xi) = \exp(\sigma \cdot u_{95}) \tag{3.13}$$

wobei hier u_{95} der 95-%-Wert der (0,1) Normalverteilung ist. Bei den 5-%-, 50-%- und 95-%-Fraktilen wurde das %-Zeichen weggelassen, um eine übersichtlichere Schreibweise zu ermöglichen. Folglich gilt:

$$\frac{y_{95}}{y_{50}} = \exp(1{,}6449 \cdot \sigma) \tag{3.14}$$

Analog folgt:

$$\frac{y_{50}}{y_{5}} = \exp(1{,}6449 \cdot \sigma) \tag{3.15}$$

Die Größe exp(1,6449 · σ) nennt man auch den Unsicherheitsfaktor oder Streufaktor (K) der logarithmischen Normalverteilung Y.

Genauer müßte man $K = K_{95}$ schreiben, denn man kann analog statt u_{95} allgemein $u_{P\,\%}$ nehmen und erhält damit die P-%-Fraktile der logarithmischen Normalverteilung durch

$$y_{P\,\%} = y_{50} \cdot K_{P\,\%} \qquad (3.16)$$

Im folgenden soll jedoch unter dem Streufaktor K stets der Wert $\exp(1{,}6449 \cdot \sigma) = K_{95}$ verstanden werden.

Durch den Median y_{50} und den Streufaktor K ist die logarithmische Normalverteilung ebenfalls eindeutig bestimmt. Zusätzlich kann mit Hilfe von y_{50} und K sofort das 90-%ige Vertrauensintervall $[y_{50}/K;\ y_{50} \cdot K]$ der Verteilung angegeben werden.

Setzt man $X = \ln Y$ als $N(\ln \xi, \sigma)$ normalverteilt voraus, dann ergibt sich für die Dichtefunktion f(y) eine logarithmisch normalverteilte Zufallsgröße:

$$f(y) = \begin{cases} \frac{1}{\sqrt{2\pi}} \cdot \frac{1}{\sigma \cdot y} \exp\left(-\frac{(\ln y - \ln \xi)^2}{2\sigma^2}\right) & \text{für } y > 0 \\ 0 & \text{für } y \leq 0 \end{cases} \qquad (3.17)$$

Die logarithmische Normalverteilung ist eine unsymmetrische Verteilung:

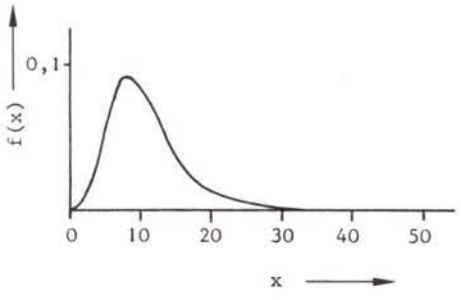


Bild F2, 3-6:
Logarithmische Normalverteilung
mit $\xi = 10$, $\sigma = 0{,}2$

Für die Zeichnung logarithmisch normalverteilter Größen ist es günstig, Wahrscheinlichkeitspapier mit logarithmischer Teilung

der Abszisse zu verwenden. Die Verteilungsfunktion der logarithmischen Normalverteilung ist dann eine Gerade. Man kann daher mit Hilfe des Wahrscheinlichkeitspapiers mit logarithmisch geteilter Abszisse feststellen, ob eine Größe Y, für die eine Anzahl von Beobachtungen y_i (i=1,..., n) vorliegt, angenähert logarithmisch normalverteilt ist. Die eingetragenen Punkte der empirischen Verteilungsfunktion müssen dann näherungsweise auf einer Geraden liegen /F2, 3-28/.

Ferner läßt sich aus dem Wahrscheinlichkeitspapier sofort Median und Streufaktor der Verteilung ablesen.

Die logarithmische Normalverteilung läßt sich sowohl durch Erwartungswert und Streuung als auch durch Median und Streufaktor eindeutig beschreiben. Für die einzelnen Größen gelten dabei folgende Zusammenhänge:

- Sind y_{50} der Median und K der Unsicherheitsfaktor einer logarithmischen Normalverteilung Y, so gilt für den Erwartungswert E(Y) und die Streuung $D^2(Y)$:

$$E(Y) = y_{50} \cdot \exp(\sigma^2/2) \qquad \sigma = \ln K/1{,}6449 \tag{3.18}$$

$$\begin{aligned} D^2(Y) &= (y_{50})^2 \cdot \exp(\sigma^2) \cdot (\exp(\sigma^2)-1) \\ &= (E(Y))^2 \cdot (\exp(\sigma^2)-1) \end{aligned} \tag{3.19}$$

- Sind E(Y) und $D^2(Y)$ Erwartungswert und Streuung einer logarithmisch normalverteilten Zufallsgröße Y, so gilt für den Median y_{50} und den Unsicherheitsfaktor K:

$$y_{50} = \frac{(E(Y))^2}{\sqrt{(E(Y))^2 + D^2(Y)}} \tag{3.20}$$

$$K = \exp(1{,}6449 \cdot \sigma) \qquad \sigma = \sqrt{\ln \left(\frac{D^2(Y)}{(E(Y))^2} + 1 \right)} \tag{3.21}$$

3.2.5.2 Produkt logarithmisch normalverteilter Zufallsgrößen

Sind X_1 und X_2 zwei unabhängige logarithmisch normalverteilte Zufallsgrößen, bestimmt durch Median ξ_μ und Streufaktor K_μ, $\mu = 1,2$, dann gilt

$$\ln (X_\mu) \text{ ist } N(\ln \xi_\mu, \sigma_\mu) \text{ normalverteilt,}$$

mit

$$\sigma_\mu = \ln K_\mu / 1{,}6449 \tag{3.22}$$

Wenn $Y = X_1 \cdot X_2$ ist, dann gilt $\ln Y = \ln X_1 + \ln X_2$:

$$\ln Y \text{ ist } N(\ln(\xi_1 \cdot \xi_2), \sqrt{\sigma_1^2 + \sigma_2^2}) \text{ normalverteilt} \tag{3.23}$$

$$y_{50} = \xi_1 \cdot \xi_2 \text{ (Produkt der Mediane)} \tag{3.24}$$

Für den Erwartungswert E(Y) gilt:

$$E(Y) = E(X_1) \cdot E(X_2) \tag{3.25}$$

Aus

$$\sigma_y = \sqrt{\sigma_1^2 + \sigma_2^2} \qquad K_y = \exp(1{,}6449 \cdot \sigma_y) \tag{3.26}$$

folgt:

$$K_y = \exp(\sqrt{(\ln K_1)^2 + (\ln K_2)^2}) \tag{3.27}$$

Analog folgt für das Produkt n logarithmisch normalverteilter Zufallsgrößen

$$y_{50} = \xi_1 \cdot \xi_2 \cdot \ldots \cdot \xi_n \tag{3.28}$$

$$K_y = \exp(\sqrt{(\ln K_1)^2 + (\ln K_2)^2 + \ldots (\ln K_n)^2}) \tag{3.29}$$

3.2.5.3 Summe logarithmisch normalverteilter Zufallsgrößen

Zur Zusammenfassung von Komponenten zu Ersatzkomponenten im Programm TREBIL ist es nötig, die Summe logarithmisch normalverteilter Zufallsgrößen zu berechnen.

- Summe zweier logarithmisch normalverteilter Zufallsgrößen

Sind X_1 und X_2 zwei unabhängige logarithmisch normalverteilte Zufallsgrößen, bestimmt durch Median ξ_μ und Streufaktor K_μ, $\mu = 1,2$, dann gilt für $Y = X_1+X_2$:

$$E(Y) = E(X_1) + E(X_2) \qquad (3.30)$$

$$D^2(Y) = D^2(X_1) + D^2(X_2) \qquad (3.31)$$

($E(X_\mu)$ und $D^2(X_\mu)$, $\mu = 1,2$, lassen sich mit den Formeln (3.18) und (3.19) berechnen.)

Die Zufallsgröße Y ist nicht logarithmisch normalverteilt. Sie kann jedoch sehr gut durch eine logarithmische Normalverteilung angenähert werden, sofern die Mediane von ungefähr gleicher Größenordnung sind. Dieses Ergebnis folgt aus zahlreichen Monte-Carlo-Simulationen und anschließenden Approximationen der ausgespielten Werte durch eine logarithmische Normalverteilung.

Wie das folgende Beispiel 1 zeigt, ist der Fehler (Ungenauigkeit) durch die Annahme, Y sei logarithmisch normalverteilt, relativ klein. Aufgrund der Näherung einer angenommenen logarithmischen Normalverteilung der Eingabedaten und der Ungenauigkeit der Eingabedaten ist die Annahme, Y sei logarithmisch normalverteilt, durchaus vertretbar.

Nimmt man also an, $E(Y)$ und $D^2(Y)$ sind Erwartungswert und Streuung einer logarithmischen Normalverteilung, dann kann man Median und Streufaktor mit Hilfe der Formeln (3.20) und (3.21) ermitteln.

Beispiel 1:

X_1 und X_2 seien zwei unabhängig logarithmisch normalverteilte Zufallsgrößen, bestimmt durch Median $\xi_\mu = 1$ und Streufaktor $K_\mu = 3$ ($\mu = 1,2$) und $Y = X_1 + X_2$, dann gilt:

$$E(X_\mu) = 1,25 \qquad D^2(X_\mu) = 0,878 \qquad (3.32)$$

$$E(Y) = 2,5 \qquad D^2(Y) = 1,76 \qquad (3.33)$$

Unter der Annahme, Y sei logarithmisch normalverteilt, ist diese Zufallsvariable durch ihren Erwartungswert = 2,5 und die Streuung = 1,76 eindeutig bestimmt. Aus den Formeln (3.18) bis (3.21) errechnet sich

Median	= 2,20
Streufaktor	= 2,26

Damit ergeben sich die Grenzen des 90%igen Vertrauensintervalls zu

$$y_5 = 0,973 \qquad y_{95} = 4,97$$

Für die tatsächliche Verteilung betragen die Schätzwerte der Monte-Carlo-Simulation bei 1000 Spielen:

Erwartungswert	2,45
Streuung	1,64
Median	2,17
5-%-Fraktile	0,97
95-%-Fraktile	4,91
Streufaktor	2,24

Der Streufaktor K von Y ist etwas kleiner als der Streufaktor von X_1 oder X_2. Dies heißt aber nicht, daß die Streuung von Y kleiner ist als die Streuung von X_1 oder X_2, denn der Unsicherheitsfaktor (K) ist ein relatives Maß, bezogen auf den Median. Da sich aber der Median ungefähr verdoppelt hat, hat sich auch das 90-%-Intervall von Y und damit die Streuung, im Vergleich zu X_1 oder X_2, vergrößert. Auch bei größeren Streufaktoren ($K \leq 10$) hat die Monte-Carlo-Simulation gezeigt, daß die Summe zweier logarithmisch normalverteilter Zufallsgrößen wieder annähernd logarithmisch normalverteilt ist, wenn die Mediane ungefähr gleich groß sind.

- Summe mehrerer logarithmisch normalverteilter Zufallsgrößen

Es sei

$$Y_n = \sum_{\mu=1}^{n} X_\mu$$

wobei X_μ unabhängige logarithmisch normalverteilte Zufallsgrößen sind, mit dem Median ξ_μ und dem Streufaktor K_μ, $\mu = 1,\ldots, n$.

Nach dem zentralen Grenzwertsatz ist die Summe von unabhängigen Zufallsgrößen unter sehr schwachen Voraussetzungen (die bei der logarithmischen Normalverteilung erfüllt sind) für $n \to \infty$ normalverteilt. Da die logarithmische Normalverteilung keine symmetrische Verteilung ist, vollzieht sich dieser Übergang zur Normalverteilung nur sehr langsam. Wie das folgende Beispiel (mit Monte-Carlo-Simulation gerechnet) zeigt, ist für $n = 10$, $K_\mu = 3$, $\xi_\mu = 1$ ($\mu = 1,\ldots, 10$) Y_{10} noch fast logarithmisch normalverteilt.

Die Hypothese, Y_{10} sei normalverteilt, mit

$$E(Y) = \sum_{\mu=1}^{10} E(X_\mu) \qquad D^2(Y) = \sum_{\mu=1}^{10} D^2(X_\mu) \qquad (3.34)$$

kann mit einer Aussagesicherheit von 90 % (Kolmogorov-Test) abgelehnt werden.

Das folgende Beispiel und viele weitere Monte-Carlo-Simulationen zeigen, daß bei nicht zu großen n und nicht zu großen Streufaktoren K_μ die Annahme, daß Y_n logarithmisch normalverteilt ist, durchaus vertretbar ist. Die Ungenauigkeit wird um so größer, je größer n ist und je größer die Streufaktoren K_μ sind.

Beispiel 2:

Als Beispiel seien $X_1,\ldots,X_{10}$ voneinander unabhängige logarithmisch normalverteilte Zufallsgrößen gewählt, bestimmt durch den Median $\xi_\mu = 1$ und den Streufaktor $K_\mu = 3$, $\mu = 1,\ldots,10$. Für

$$Y_{10} = \sum_{\mu=1}^{10} X_\mu$$

gilt dann:

$$E(X\mu) = 1{,}25 \qquad D^2(X_\mu) = 0{,}878$$
$$E(Y) = 12{,}5 \qquad D^2(Y) = 8{,}78$$

Unter der Annahme, Y sei logarithmisch normalverteilt, ergeben sich daraus:

Erwartungswert	12,5
Streuung	8,77
Median	12,16
Streufaktor	1,47

Aus Median und Streufaktor können die 5-%- und 95-%-Fraktile berechnet werden:

$$y_5 = 8{,}27 \qquad y_{95} = 17{,}88$$

Für die tatsächliche Verteilung betragen demgegenüber die Schätzwerte der Monte-Carlo-Simulation bei 1000 Spielen:

Erwartungswert	12,5
Streuung	8,82
Median	12,2
5-%-Fraktile	8,14
95-%-Fraktile	18,0
Streufaktor	1,49

3.2.5.4 Berechnung der Verteilungen für die mittlere und starke Kopplung

Zur Beschreibung der mittleren Kopplung Y_m und der starken Kopplung Y_s von Ausfällen (Abschnitt 3.3.5.2) sind die folgenden Verteilungen zu ermitteln:

$$Y_m = X_1 \sqrt{X_2} \text{ bzw. } Y_s = X_1 \sqrt[4]{X_2} \qquad (3.35)$$

wobei X_1 und X_2 logarithmisch normalverteilte Zufallsgrößen sind.

Aus $Y_m = X_1\sqrt{X_2}$ folgt $\ln Y_m = \ln X_1 + \frac{1}{2} \ln X_2$. Sind nun $\ln X_1 \sim N(\mu_1, \sigma_1^2)$ und $\ln X_2 \sim N(\mu_2, \sigma_2^2)$ normalverteilte Zufallsgrößen mit Erwartungswert μ_1 bzw. μ_2, und der Streuung σ_1^2 bzw. σ_2^2, so gilt:

$$\ln Y_m \sim N(\mu_1 + \tfrac{1}{2}\mu_2,\ \sigma_1^2 + \tfrac{1}{4}\sigma_2^2) \qquad (3.36)$$

$\ln Y_m$ ist also normalverteilt mit Erwartungswert $\mu_1 + \frac{1}{2}\mu_2$ und der Streuung $\sigma_1^2 + \frac{1}{4}\sigma_2^2$.

Analog folgt für Y_s:

$$\ln Y_s \sim N(\mu_1 + \frac{1}{4}\mu_2,\ \sigma_1^2 + \frac{1}{16}\sigma_2^2) \qquad (3.37)$$

Wie aus (3.36) und (3.37) zu entnehmen, sind Y_m bzw. Y_s logarithmisch normalverteilte Zufallsgrößen. Sind nun ξ_i Median und K_i Streufaktor der logarithmischen Normalverteilung X_i (i=1,2), so folgt für die

- mittlere Kopplung Y_m:

Y_m ist logarithmisch normalverteilt mit

Median

$$\xi_m = \xi_1 \sqrt{\xi_2} \qquad (3.38)$$

und Streufaktor

$$K_m = \exp(\sqrt{(\ln K_1)^2 + \tfrac{1}{4}(\ln K_2)^2}) \qquad (3.39)$$

- starke Kopplung Y_s:

Y_s ist logarithmisch normalverteilt mit

Median

$$\xi_s = \xi_1 \cdot \sqrt[4]{\xi_2} \qquad (3.40)$$

und Streufaktor

$$K_s = \exp(\sqrt{(\ln K_1)^2 + \tfrac{1}{16}(\ln K_2)^2}) \qquad (3.41)$$

3.2.6 Bestimmung von Ausfallwahrscheinlichkeiten pro Anforderung und Ausfallraten aus der Betriebserfahrung

Sind für die Bestimmung der Ausfallrate λ bzw. Ausfallwahrscheinlichkeiten pro Anforderung p keine Literaturdaten vorhanden, so muß die Betriebserfahrung über die entsprechenden Komponentenfunktionen zur Bestimmung der Zuverlässigkeitskenngrößen

herangezogen werden. Meist handelt es sich dabei um Komponentenfunktionen, für die nur wenige oder null Ausfälle registriert worden sind. In diesen Fällen werden zur Bestimmung von λ und p die folgenden Methoden angewandt.

- Ausfallwahrscheinlichkeiten pro Anforderung

Bei einem Versuch trete das Ereignis A ($\hat{=}$ Ausfall bei Anforderung) mit der unbekannten Wahrscheinlichkeit p auf. Tritt nun bei n-maliger Durchführung des Versuches genau m-mal das Ereignis A ein, dann ergeben sich für p die folgenden P-%-Vertrauensintervalle /F2, 3-28/:

$$0 \leq p \leq \frac{(m+1)\ a}{(m+1)\ a+n-m} \qquad a = F_{P\ \%}^{(2m+2,\ 2n-2m)} \tag{3.42}$$

wobei:

m $\hat{=}$ Anzahl der Ausfälle
n $\hat{=}$ Anzahl der Durchführungen (Anforderungen)
a $\hat{=}$ P-%-Fraktile der F-Verteilung
mit den Freiheitsgraden (2m+2, 2n-2m)

Durch Transformation $\bar{m} = 2m+2$, $\bar{n} = 2n-2m$ erhält man aus (3.42):

$$0 \leq p \leq Y_{P\ \%} \qquad Y_{P\ \%} = \frac{\bar{m}\ F_{P\ \%}^{\bar{m},\ \bar{n}}}{\bar{n}+\bar{m}\ F_{P\ \%}^{\bar{m},\ \bar{n}}} \tag{3.43}$$

Die rechte Seite von (3.43) ist also die P-%-Fraktile einer Betaverteilung mit (m+1, n-1) Freiheitsgraden.

Die obere Grenze für die Ausfallwahrscheinlichkeit pro Anforderung p, mit einer Aussagesicherheit von P %, ist folglich die P-%-Fraktile einer Betaverteilung mit (m+1, n-1) Freiheitsgraden ($\bar{m} = 2m+2$, $\bar{n} = 2n-2m$ und m $\hat{=}$ Anzahl der Ausfälle, n $\hat{=}$ Anzahl der Anforderungen).

Benötigt man nun für die Ausfallwahrscheinlichkeit pro Anforderung p eine Verteilungsfunktion F(p), so ist es naheliegend, die

obere Grenze des P-%-Vertrauensintervalls ($Y_{P\ \%}$) als P-%-Fraktile der Verteilung F(p) zu betrachten, d.h., p wird als Zufallsvariable P behandelt und P besitzt eine (m+1, n-1)-Betaverteilung.

Für den Erwartungswert der Betaverteilung von P gilt:

$$E(P) = \frac{\bar{m}}{\bar{n}+\bar{m}} = \frac{m+1}{n+1} \qquad (3.44)$$

Der Erwartungswert E(P) ist zwar ungleich dem unverzerrten Schätzwert $\frac{m}{n}$ für die Ausfallwahrscheinlichkeit pro Anforderung p, aber wegen der meist beschränkten Anzahl von Beobachtungen wird pessimistisch davon ausgegangen, daß bei der nächsten Anforderung ein Ausfall auftreten wird.

Für größere m und n ist:

$$\frac{m+1}{n+1} \cong \frac{m}{n} \qquad (3.45)$$

Für die Streuung von P gilt:

$$D^2(P) = \frac{2\bar{m}\,\bar{n}}{(\bar{m}+\bar{n})^2\,(\bar{m}+\bar{n}+2)} = \frac{(m+1)\,(n-m)}{(n+1)^2\,(n+2)} \qquad (3.46)$$

wobei

$m \triangleq$ Anzahl der Ausfälle

$n \triangleq$ Anzahl der Anforderungen

Die Fraktilen der Betaverteilung P lassen sich unmittelbar aus den Fraktilen der zugeordneten F-Verteilung wie folgt berechnen:

$$\text{P-\%-Fraktile von F(p)} = \frac{(m+1)\ a}{(m+1)\ a+n-m}$$

mit: (3.47)

$$a = F_{P\ \%}^{(2m+2,\ 2n-2m)}$$

Beispiel:

Es sei die Anzahl der Ausfälle m = 3, die Anzahl der Anforderungen n = 100. Dann gilt:

$$E(P) = \frac{4}{101} = 3{,}96 \cdot 10^{-2}$$

$$D(P) = 1{,}9 \cdot 10^{-2}$$

$$P_{50} = 3{,}66 \cdot 10^{-2}$$

Man kann eine Verteilung für die Ausfallwahrscheinlichkeit pro Anforderung F(p) auch mit Hilfe eines Bayes'schen Ansatzes gewinnen. Die Anwendbarkeit der allgemeinen Bayes-Methode ist mit der Schwierigkeit verbunden, daß man eine, die gemeinsame Meinung der Experten wiedergebende Apriori-Verteilung benötigt. Nimmt man jedoch als Apriori-Verteilung die Gleichverteilung (d.h. es liegt keine Expertenschätzung vor), so ergibt sich für eine große Anzahl n der Anforderungen eine sehr gute Übereinstimmung mit der zuvor beschriebenen Methode.

Anmerkung: Im Fachband 3 wird die Ausfallwahrscheinlichkeit pro Anforderung p bei null beobachteten Ausfällen (m = 0) mit Hilfe der χ^2-Verteilung berechnet. Bei einer Null-Ausfall-Statistik (m = 0) ergeben sich jedoch im Vergleich zur obigen Methode keine nennenswerten Unterschiede.

- Ausfallraten

Ist X eine Komponentenfunktion mit der Lebensdauerverteilung $1 - \exp(-\lambda t)$, wobei die Komponente nach dem Ausfall sofort durch eine neue gleichartige Komponente ersetzt wird, dann ist die Anzahl der Ausfälle N(t) der Komponente X im Intervall [0,t] poissonverteilt mit dem Parameter λt, d.h.

$$P(N(t)=\mu) = \frac{(\lambda t)^{\mu}}{\mu!} \exp(-\lambda t) \qquad \mu = 0,1,2,... \qquad (3.48)$$

und

$$H(t) = E(N(t)) = \lambda t \qquad (3.49)$$

Die zu erwartende Anzahl der Erneuerungen H(t) bis zum Zeitpunkt t ist gleich λt. Ein unverzerrter Schätzwert für die Ausfallrate λ ist folglich

$$\lambda = \frac{m}{t} \qquad (3.50)$$

mit m $\hat{=}$ Anzahl der Ausfälle, t $\hat{=}$ Beobachtungszeitraum.

Bei der Bestimmung von Vertrauensintervallen für λ geht man wie folgt vor:

Ist X eine zufällige Größe, die einer Poissonverteilung mit dem unbekannten Parameter a ($a = \lambda t$) genügt, und nimmt X den Wert m

(Anzahl der Ausfälle) an, so erhält man ein P-%-Vertrauensintervall für a durch

$$0 \leq a \leq y \qquad y = \frac{1}{2}\,\chi^2_{2(m+1)}(P\,\%) \tag{3.51}$$

und entsprechend

$$0 \leq \lambda \leq y \qquad y = \frac{1}{2t}\,\chi^2_{2(m+1)}(P\,\%) \tag{3.52}$$

d.h. mit einer Aussagesicherheit von P % liegt der Wert λ im Intervall [0,y].

Die obere Grenze für λ ist folglich eine χ^2-verteilte Zufallsgröße mit 2(m+1) Freiheitsgraden multipliziert mit einem konstanten Faktor 1/2t (Gamma-Verteilung).

Benötigt man für die Ausfallrate λ eine Verteilungsfunktion $F(\lambda)$, so ist es (analog wie bei der Ausfallwahrscheinlichkeit pro Anforderung p) naheliegend, die obere Grenze des P-%-Vertrauensintervalls für λ als P-%-Fraktile der Verteilungsfunktion $F(\lambda)$ zu betrachten. Die Ausfallrate λ ist folglich eine Zufallsgröße Λ und besitzt eine χ^2-Verteilung mit 2(m+1) Freiheitsgraden multipliziert mit 1/2t.

Für den Erwartungswert von Λ gilt:

$$E(\Lambda) = \frac{m+1}{t} \tag{3.53}$$

Dieser Wert ist ungleich dem unverzerrten Schätzwert $(\frac{m}{t})$ für Λ. Man geht aber hier pessimistisch davon aus, daß unmittelbar nach dem beobachteten Zeitraum t ein Ausfall erfolgt.

Für die Standardabweichung von Λ gilt:

$$D(\Lambda) = \frac{\sqrt{m+1}}{t} \tag{3.54}$$

und für die Fraktilen:

$$\lambda_{P\,\%} = \frac{1}{2t}\,\chi^2_{2(m+1)}(P\,\%)$$

Beispiel:

Es sei die Anzahl der Ausfälle m = 3, der beobachtete Zeitraum t = 100 Jahre. Dann gilt:

$$E(\Lambda) = \frac{4}{100} = 4 \cdot 10^{-2}/a$$
$$D(\Lambda) = 2 \cdot 10^{-2}/a$$
$$\lambda_{50} = 3{,}7 \cdot 10^{-2}/a$$

Anmerkung:

Die hier geschilderte Methode zur Bestimmung von Verteilungen für die Ausfallwahrscheinlichkeit P und Ausfallrate Λ mit Hilfe von Daten aus der Betriebserfahrung besitzt folgende Vorteile:

- Die resultierenden Verteilungen (Beta-, χ^2-Verteilung) sind verhältnismäßig einfach zu handhaben.
- Kenngrößen wie Erwartungswert, Varianz und Fraktile sind einfach zu berechnen.
- χ^2- und F-Verteilung liegen tabelliert vor.
- χ^2- und Beta-Verteilung sind einfach zu simulieren.

3.3 "Common mode"-Ausfälle

3.3.1 Arten

Außer mit den vorher besprochenen unabhängigen Funktionsausfällen von Komponenten ist mit dem Auftreten voneinander abhängiger Funktionsausfälle zu rechnen.

Im folgenden wird zwischen "common mode"-Ereignissen und "common mode"-Ausfällen unterschieden. Unter "common mode"-Ereignissen werden voneinander abhängige Funktionsausfälle von mehreren Komponenten, Teilsystemen oder Systemen verstanden, die auf eine einzelne Ursache zurückzuführen sind. Komponenten sind Bauteile (Hardware), Verfahrensvorschriften (Software) und Personen. Besonders unangenehm können diese "common mode"-Ereignisse sein, wenn sie redundante Komponenten, Teilsysteme oder Systeme betreffen und gleichzeitig oder in einem eng begrenzten Zeitintervall auftreten, so daß die ausgefallenen Zustände gleichzeitig vorliegen. Es wird dann von "common mode"-Aus-

fällen (CMA), d.h. gemeinsam verursachten Ausfällen, gesprochen. Folgende Arten von CMA können unterschieden werden (Bild F2, 3-7):

- Funktionsausfälle von zwei oder mehr ähnlichen oder baugleichen redundanten Komponenten, Teilsystemen oder Systemen aufgrund einer gemeinsamen Ursache. Sie werden als CMA im engeren Sinn oder "common cause failures" bezeichnet.
- Funktionsausfälle von zwei oder mehr redundanten Komponenten, Teilsystemen oder Systemen, die als Folge eines einzigen Funktionsausfalls auftreten. Sie werden als Folgeausfälle oder Sekundärausfälle oder "causal failures" bezeichnet.
- Funktionsausfälle von zwei oder mehr redundanten Komponenten, Teilsystemen oder Systemen, die sich aufgrund von funktionellen Abhängigkeiten, d.h. unmittelbar aus dem Systemaufbau ergeben. So können beispielsweise funktionelle Abhängigkeiten von einem gemeinsamen Hilfssystem, von einer gemeinsamen Ansteuerung oder von einer menschlichen Fehlhandlung bestehen. Diese Ausfälle werden in der vorliegenden Studie bereits durch die detaillierte Fehlerbaumanalyse erfaßt und daher nicht besonders ausgewiesen.

3.3.2 Ursachen

3.3.2.1 A l l g e m e i n e s

Zum Erkennen, zur Bewertung und zur Verringerung des Einflusses von CMA auf die Zuverlässigkeit der Systemfunktionen ist eine geeignete Klassifizierung dieser Ausfälle hilfreich. In der Literatur wird am häufigsten nach der Ursache der CMA klassifiziert, wobei die durchgeführten Unterteilungen weitgehend übereinstimmen /F2, 3-29/. Demnach lassen sich zwei Hauptkategorien von CMA unterscheiden, nämlich solche aufgrund von Fehlern bei der Planung und Herstellung und solche aufgrund von Fehlern, die während des Betriebs entstehen (Bild F2, 3-7). Jede dieser Kategorien kann weiter unterteilt werden.

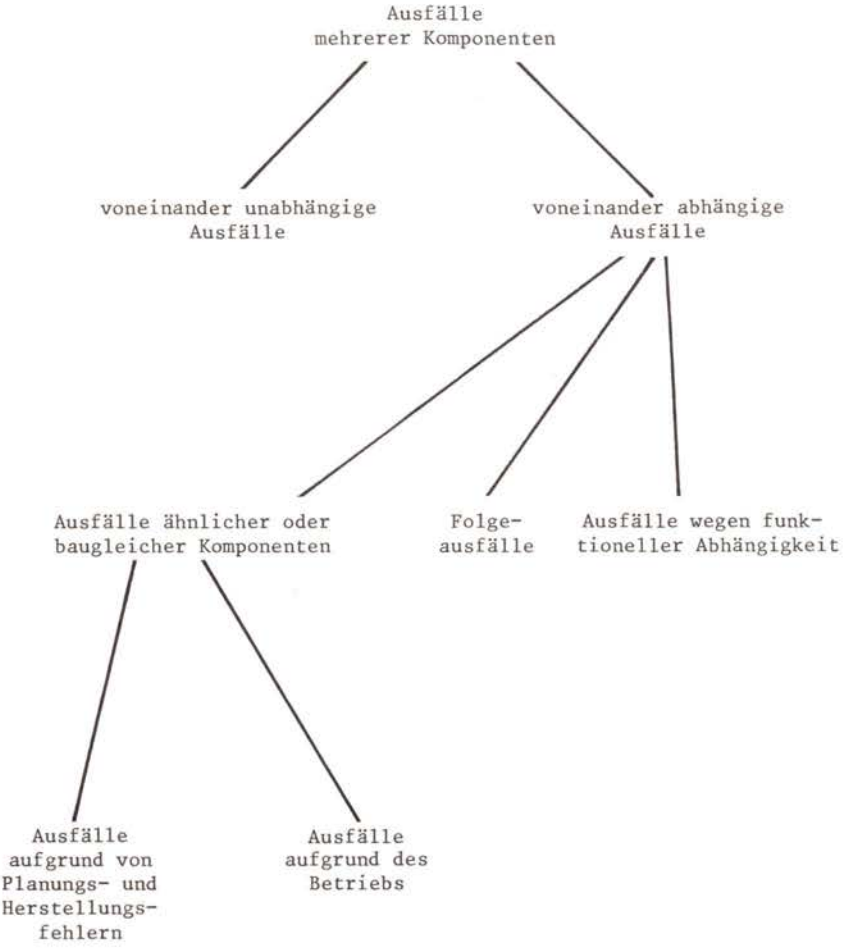


Bild F2, 3-7:

Arten von Ausfällen mehrerer Komponenten

3.3.2.2 Planung und Herstellung

- Planungsfehler

- Funktionelle Fehleinschätzungen

  Hierzu gehören funktionelle Mängel der Systeme aufgrund einer Fehleinschätzung des Verlaufs von Prozeßvariablen oder aufgrund einer unzureichenden Instrumentierung zur Erfassung der Prozeßvariablen. Aufgrund dieser Ursachen könnte eine Detektierung des Störfalls verhindert werden. Darüber hinaus ist es möglich, daß durch eine Fehleinschätzung der Prozeßvariablen eine unzureichende Wirksamkeit der Gegenmaßnahmen bedingt wird. Solche Fehleinschätzungen lassen sich nicht mit letzter Sicherheit vermeiden, da manche Vorgänge nicht experimentell, sondern nur durch Analysen im voraus ermittelt werden können.

- Auslegungsfehler und Konstruktionsfehler

  Zu den Planungsfehlern gehören auch falsche Auslegungen und Konstruktionsfehler, falsch festgelegte bzw. unzureichende schriftliche Handlungsanweisungen im Betriebshandbuch, in ihrer Tragweite falsch eingeschätzte gegenseitige elektrische oder mechanische Abhängigkeiten. Zu diesem Punkt sind auch nicht erkannte gemeinsame Abhängigkeiten von menschlichem Fehlverhalten und Umgebungseinflüssen zu rechnen. So gehört die nicht erkannte oder ungenügend berücksichtigte Beeinträchtigung von Komponenten der Sicherheitssysteme aufgrund von Umgebungseinflüssen nach einem Störfall hierher.

- Herstellungsfehler

Zu dieser Gruppe zählen Fehler, die bei der Fertigung (einschließlich Qualitätssicherung), der Installation bzw. Montage auf der Baustelle oder der Inbetriebsetzung entstehen.

3.3.2.3 B e t r i e b

- Bedienungsfehler, Instandhaltungsfehler

Das Fehlverhalten des Betriebspersonals kann eine Ursache für CMA darstellen. Grundsätzlich sind menschliche Fehlhandlungen im bestimmungsgemäßen Betrieb der Anlage und bei Störfällen zu unterscheiden. In die zuletzt genannte Kategorie fallen alle Handmaßnahmen, die laut Betriebshandbuch zur Störfallbeherrschung zu ergreifen sind. Zur ersten Kategorie gehören unzureichende oder fehlerhaft durchgeführte Instandhaltungen (z.B. Fehljustierungen).

- Extreme Umgebungsbedingungen und extreme Betriebsbedingungen

Extremwerte der Umgebungsbedingungen oder der Betriebsbedingungen können dauernd oder zeitweise nach einem Störfall auftreten. Solche Umgebungsbedingungen haben oft auch bei richtiger Auslegung der Komponenten größere Ausfallraten zur Folge. Sie können im ungünstigsten Fall einen plötzlichen Folgeausfall von redundanten Komponenten bewirken. Das kann dann eintreten, wenn die Umgebungsbedingungen eine Beanspruchung jenseits der Auslegungsgrenzen bewirken, wie das bei manchen Komponenten von Betriebssystemen der Fall ist, die von vornherein nicht für Störfallbedingungen ausgelegt werden. Hierher gehören auch Folgeausfälle an den Sicherheitssystemen bei extremen Störfallabläufen, die im Genehmigungsverfahren nicht zugrunde gelegt werden, im Rahmen einer Risikostudie aber zu bewerten sind. Typische Umgebungsbedingungen, die CMA nach sich ziehen können, sind durch erhöhte Werte von Temperatur, Feuchtigkeit oder Druck, durch starke Erschütterung oder durch eine korrosive Atmosphäre gegeben.

- Mechanische Einwirkungen aus benachbarten Systemen und Einwirkungen von außen

Zu Folgeausfällen kann es bei mechanischen Einwirkungen aus benachbarten Systemen kommen, z.B. aufgrund von Bruchstücken,

schlagenden Rohrleitungen und Strahlkräften. Mögliche Einwirkungen von außen sind Brand, Überflutung, Blitzschlag, Sturm, Erdbeben, Explosion, Flugzeugabsturz usw. Diese Einwirkungen von außen werden im Fachband 4 gesondert diskutiert.

3.3.3 Gegenmaßnahmen

Für die Sicherheitssysteme von Kernkraftwerken wird eine Vielzahl von Maßnahmen gegen den Ausfall der für diese Systeme wichtigen Komponentenfunktionen getroffen. Die meisten dieser Maßnahmen, die natürlich seit den Anfängen der Kernkraftwerkstechnik ständig erweitert und verfeinert wurden, richten sich primär gegen unabhängige Ausfälle. Nahezu alle dieser Maßnahmen sind auch gegen CMA, jedoch in unterschiedlichem Maße, wirksam. Im folgenden soll ein kurzer Überblick über die in Kernkraftwerken getroffenen Maßnahmen gegeben werden.

- Erprobte Konstruktion und Standardisierung

Durch den Einsatz von erprobten oder standardisierten Komponenten, d.h. durch das Vermeiden von unnötigen Neuerungen, lassen sich langjährige Betriebserfahrungen nutzen, so daß Auslegungsfehler oder Konstruktionsfehler mit hoher Wahrscheinlichkeit erkannt und ausgemerzt werden. Ein weiterer Vorteil dieser Maßnahme besteht darin, daß Fehler bei der Instandhaltung ebenfalls unwahrscheinlicher werden.

- Redundanz

Unter Redundanz versteht man, daß mehr Komponenten oder Teilsysteme vorhanden sind, als zur Erfüllung der gewünschten Systemfunktion benötigt werden. Analog kann auch von personeller Redundanz gesprochen werden. Darunter versteht man den Einsatz von mehr Personen zur Durchführung einer Handmaßnahme, als dafür notwendig sind.

Redundanz ist sehr wirksam gegenüber Einzelausfällen und auch gegenüber einer Reihe von CMA. Viele "common mode"-Ursachen führen ja nicht zum gleichzeitigen Ausfall gleichartiger Komponenten, sondern nur zu einer Häufung von Ausfällen in einem Zeitraum. In diesen Fällen wird durch den redundanten Aufbau erreicht, daß das Gesamtsystem nicht bereits beim ersten auftretenden Ausfall versagt. Ist dieser Ausfall selbstmeldend oder erfolgt eine regelmäßige Funktionsprüfung, so kann mit hoher Wahrscheinlichkeit vor einem weiteren Ausfall nicht nur die Komponente repariert oder ersetzt, sondern auch die Ursache für den Ausfall erkannt werden.

- Diversität

Unter Diversität versteht man, daß die zur Erzielung einer bestimmten Systemfunktion vorhandenen redundanten Komponenten oder Teilsysteme eine unterschiedliche Bauart oder Wirkungsweise besitzen (gerätetechnische bzw. funktionelle Diversität).

Die gerätetechnische Diversität läuft dem Wunsch nach Standardisierung zuwider und erschwert die Instandhaltung. Für manche Funktionen sind diversitäre Komponenten vergleichbarer Qualität nicht erhältlich. Aus diesen Gründen wird vom Prinzip der gerätetechnischen Diversität nur begrenzt Gebrauch gemacht.

Diversität wird vor allem im Reaktorschutzsystem angewandt. So wird in der KTA-Regel 3501 /F2, 3-30/ gefordert, daß für jeden vom Reaktorschutzsystem zu erfassenden Störfall mindestens zwei physikalisch unterschiedliche Anregekriterien herangezogen werden. Die Verwendung physikalisch unterschiedlicher Prozeßvariablen zur Störfallerfassung, d.h. funktionelle Diversität, schließt im allgemeinen die gerätetechnische Diversität im Bereich der Meßfühler ein. Unterschiedliche Meßfühler erfordern unterschiedliche Instandhaltungsmaßnahmen (z.B. Funktionsprüfungen), so daß CMA aller Meßkanäle unwahrscheinlicher werden.

Ähnlich wie bei der Diversität von Bauteilen kann auch von personeller Diversität gesprochen werden, d.h. Einsatz ver-

schiedener Personen für die gleichartigen Aufgaben, z.B. für die Durchführung von Funktionsprüfungen an redundanten Teilsystemen (Qualitätssicherung während des Betriebes).

- Räumliche Trennung

Eine räumliche Trennung von redundanten Komponenten oder Teilsystemen ist vor allem gegen Ursachen von CMA wirksam, die von außerhalb des Systems herrühren.

Es ist zu unterscheiden, ob redundante Komponenten und Systemstränge nur durch einen Mindestabstand separiert oder ob sie in voneinander getrennten und geschützten Räumen untergebracht sind. Voneinander getrennte Räume bewirken einen weitergehenden Schutz gegenüber mechanischen und elektrischen Einwirkungen aus benachbarten Systemen und Einwirkungen von außen, sind jedoch nicht immer durchführbar.

- Einrichtungen zur Ausfallerkennung

Durch eine schnelle Ausfallerkennung kann die Verfügbarkeit von in Bereitschaft befindlichen Systemen erhöht werden. Eine Möglichkeit ist die Installation von Einrichtungen, durch die eine ständige Überwachung von Komponenten möglich wird, so daß Ausfälle selbstmeldend werden. Ist ein System so ausgelegt, daß Ausfälle von Komponenten oder Teilsystemen vom System selbst erkannt und gemeldet werden, so spricht man von Selbstüberwachung. Dieses Prinzip wird weitgehend im Reaktorschutzsystem angewandt.

- Regelmäßige Funktionsprüfungen

Eine weitere Möglichkeit zur schnelleren Fehlererkennung ist die regelmäßige Durchführung von Funktionsprüfungen der sicherheitsrelevanten Komponenten, Teilsysteme und Systeme. Durch ausreichend kurze Prüfintervalle kann eine Erhöhung der Verfügbarkeit von in Bereitschaft befindlichen Systemen erreicht werden.

- Ausnutzung der sicheren Ausfallrichtung

Mit dieser Maßnahme kann erreicht werden, daß geeignet konstruierte Systeme bei Ausfällen zugehöriger Komponenten in ihrer Funktion nicht beeinträchtigt werden ("fail safe"-Prinzip).

Für manche Signale des Reaktorschutzsystems, z.B. für die Reaktorschnellabschaltung, ist eine solche sichere Ausfallrichtung gegeben. Die Steuerstäbe zur Reaktorschnellabschaltung werden durch Elektromagnete gehalten. Bei Ausfall der Stromversorgung der Elektromagnete fallen die Steuerstäbe in den Reaktorkern ein und schalten den Reaktor ab.

- Entkopplung zwischen Sicherheitssystemen und Betriebssystemen

Mit einer solchen Entkopplung kann eine Rückwirkung von Betriebssystemen auf die Verfügbarkeit der Funktionen von Sicherheitssystemen verhindert werden. Insbesondere kann dadurch ausgeschlossen werden, daß aufgrund des Ausfalls von Komponenten der Betriebssysteme sicherheitstechnische Maßnahmen erforderlich sind, zu deren Durchführung gerade diese Komponenten benötigt werden. Die Folge einer solchen Entkopplung kann jedoch sein, daß mit einer größeren Ausfallerkennungszeit bei sicherheitstechnisch wichtigen Komponenten zu rechnen ist. Die Ausfälle dieser Komponenten werden dann nicht durch ein Betriebsversagen erkannt, sondern gegebenenfalls erst bei der nächsten Funktionsprüfung.

- Einfacher Systemaufbau

Bei einem komplexen, unübersichtlichen Systemaufbau besteht eine höhere Wahrscheinlichkeit, daß Zusammenhänge nicht erkannt und dadurch CMA bewirkt werden.

- Qualitätssicherung bei Planung, Herstellung und Inbetriebnahme

Eine ständige Überwachung von Bauteilen, Teilsystemen und Systemen, ausgehend von der Spezifikation über die Fertigung bis zur Inbetriebnahme des Kernkraftwerks, vermindert die Wahrscheinlichkeit von CMA. Zu den qualitätssichernden Maßnahmen gehören die Prüfungen im Herstellerwerk sowie die im Rahmen des Genehmigungsverfahrens durchgeführten Untersuchungen und Überprüfungen. Insbesondere sind Eignungsprüfung, Qualitätskontrolle zur Aufdeckung von Fertigungsfehlern und die ausreichende Erprobung während der Inbetriebnahme des Kernkraftwerks zu nennen. Durch detaillierte Zuverlässigkeitsanalysen der konzipierten Systeme können Schwachstellen im Systemaufbau und gemeinsame Abhängigkeiten erkannt und beseitigt werden.

- Qualitätssicherung während des Betriebes

Solche qualitätssichernden Maßnahmen gehören zu den wirkungsvollsten, insbesondere gegen CMA, die aufgrund des Betriebes auftreten können. Im folgenden sollen einige dieser Maßnahmen aufgelistet werden:

- gründliche Ausbildung und fortlaufende Schulung des Personals;
- ausführliches und leicht verständliches Betriebshandbuch, in dem alle notwendigen Maßnahmen für den Normalbetrieb, den anomalen Betrieb und für Störfälle vorgeschrieben sind;
- Zutritt zu den einzelnen Anlagenteilen nur für jeweils autorisiertes Personal;
- sorgfältige Instandhaltung von sicherheitstechnisch wichtigen Komponenten;
- Funktionsprüfung nach Durchführung von Instandhaltungen;
- sorgfältige Dokumentation der durchgeführten Instandhaltungen;
- personelle Redundanz und Diversität bei der Durchführung von Instandhaltungen: Durchführung der Instandhaltungsmaßnahmen an einer Komponente bzw. einem Teilsystem durch mehrere Personen der Betriebsmannschaft und Durchführung der entspre-

chenden Maßnahmen an den redundanten Komponenten oder Teilsystemen durch jeweils andere Schichten des Betriebspersonals.[1])

- Auswertung der Betriebserfahrungen

Die Betriebserfahrungen zeigen, daß auch bei erfahrenen Konstrukteuren und erfahrenem Betriebspersonal menschliches Fehlverhalten nicht ausgeschlossen werden kann. Eine systematische Erfassung und Auswertung aller aufgetretenen CMA, aber auch aller anderen erkennbaren "common mode"-Ereignisse, ist daher für eine weitere Verbesserung der sicherheitstechnisch wichtigen Systeme von großer Bedeutung.

3.3.4 Allgemeines zur Bewertung

Zur systematischen Erfassung der CMA ist die in Abschnitt 3.3.2 getroffene Unterscheidung nach Ursachen hilfreich. Zur Quantifizierung ist zusätzlich eine Unterteilung der CMA nach der Art ihrer Entdeckung wichtig. Dabei ist zu differenzieren zwischen CMA,

- die nur bei einem Störfall auftreten oder entdeckt werden,
- die bei regelmäßigen Funktionsanforderungen (im Rahmen von Funktionsprüfungen oder anderen regelmäßigen Systemanforderungen) entdeckt werden,
- die selbstmeldend sind.

Die Betriebserfahrung liefert in erster Linie Daten für die beiden zuletzt angeführten Arten von CMA, die während des bestimmungsgemäßen Betriebs entdeckt werden. Die nur bei einem Störfall auftretenden oder entdeckbaren CMA können im wesentlichen nur analytisch ermittelt werden.

---

[1]) Für die Referenzanlage der vorliegenden Studie ist personelle Diversität bei der Durchführung von Funktionsprüfungen gegeben (Abschnitt 3.3.6).

Die Quantifizierung aufgrund der Betriebserfahrung erweist sich aber auch für die während des bestimmungsgemäßen Betriebs entdeckbaren CMA als schwierig, da Beobachtungen in geringerem Maß dafür heranziehbar sind als für unabhängige Ausfälle. Die Gründe hierfür sind:

- Nur ein Teil der Komponentenausfälle sind CMA. In den meisten Literaturstellen werden Werte $\lesssim$ 10 % angegeben. Damit ist die Betriebserfahrung statistisch schlechter auswertbar.
- Die Ursachen aufgetretener Ausfälle, die als CMA erkannt werden und einen großen Einfluß auf die Systemzuverlässigkeit haben, werden behoben und in derselben Weise, nur mit reduzierter Wahrscheinlichkeit, wieder auftreten.

In der vorliegenden Studie werden CMA baugleicher (oder ähnlicher) Komponenten nur dann quantifiziert, wenn solche Ausfälle oder zumindest ähnliche CMA aus der Betriebserfahrung bekannt sind. Voraussetzung für eine zahlenmäßige Bewertung ist also, daß entsprechende Ereignisse schon aufgetreten sind. Ausfälle von funktionell oder gerätetechnisch weitgehend diversitären Komponenten werden als unabhängige Ausfälle der Komponenten in Rechnung gesetzt.

Darüber hinaus werden potentielle Quellen von CMA diskutiert. Solche sind gegeben, wenn:

- Verknüpfungen zwischen redundanten Teilsystemen (Strängen) von Sicherheitssystemen oder zwischen Betriebs- und Sicherheitssystemen vorhanden sind, die sich erst bei Störfällen auswirken,
- eine räumliche Trennung der Teilsysteme (Stränge) nicht möglich ist,
- die Teilsysteme (Stränge) mehrere Funktionen zu erfüllen haben,
- die Anforderungen sowohl beim Betrieb der Anlage als auch bei Funktionsprüfungen die Betriebsbedingungen bei Störfällen nur begrenzt wiedergeben,
- bei Störfällen andere Umgebungsbedingungen vorliegen als beim bestimmungsgemäßen Betrieb.

In der vorliegenden Studie wird davon ausgegangen, daß Planungs- und Herstellungsfehler derart, daß Komponenten den Beanspruchungen unter Störfallbedingungen grundsätzlich nicht gewachsen sind, obwohl sie dafür ausgelegt wurden, keine dominante Rolle spielen. Entsprechende Überprüfungen der Komponenten sind eine Hauptaufgabe im Rahmen des Genehmigungsverfahrens. Dort werden z.B. die Auslegungen der Komponenten für die Belastungen unter Störfallbedingungen anhand der Auslegungsstörfälle eingehend untersucht.

Für die in dieser Studie durchgeführte Quantifizierung der CMA ist die im Abschnitt 3.3.1 durchgeführte Unterscheidung der CMA maßgebend:

- Zur Bewertung der CMA von ähnlichen, vor allem aber baugleichen Komponenten oder Teilsystemen muß in erster Linie die Betriebserfahrung herangezogen werden. Ist dies nicht möglich, so kann versucht werden, den Einfluß dieser CMA mit Hilfe von Modellen abzuschätzen. Ein Überblick über diese Modelle wird im nächsten Abschnitt gegeben.

- Folgeausfälle können durch den zu analysierenden Störfall selbst verursacht werden. Beispielsweise können durch einen Kühlmittelverluststörfall Folgeausfälle durch extreme Umgebungsbedingungen und durch mechanische Belastungen hervorgerufen werden.

  Folgeausfälle, die aufgrund des Störfalls selbst oder aufgrund eines anderen Ausfalls auftreten können, werden in ihrer Wahrscheinlichkeit abgeschätzt und in den Fehlerbaumanalysen entsprechend berücksichtigt. Der Einfluß der Folgeausfälle wird dann mit den Fehlerbaumanalysen ebenfalls erfaßt und braucht nicht besonders ausgewiesen werden.

- Abhängigkeiten von gemeinsamen Komponenten, Teilsystemen oder Systemen werden durch die Fehlerbaumanalyse automatisch richtig erfaßt (Abschnitt 3.3.1). In den sehr detaillierten Fehlerbaumanalysen werden nämlich die notwendigen Energieversorgungen, Hilfsmedienversorgungen, Kühlungen und Ansteuerungen der Komponenten berücksichtigt. Der Einfluß von gemeinsamen Komponenten wird daher nicht besonders ausgewiesen.

3.3.5 Modelle zur Bewertung

3.3.5.1 Obere Grenzwerte für die Wahrscheinlichkeiten

Eine der ersten Fragen, die man sich bei der Berücksichtigung von CMA gleichartiger Komponenten oder Teilsysteme in der Zuverlässigkeitsanalyse stellt, ist die nach dem möglichen Einfluß der CMA auf die Nichtverfügbarkeit bzw. die Ausfallwahrscheinlichkeit der untersuchten Systemfunktion. Mit Hilfe der in WASH-1400 beschriebenen einfachen Abschätzung kann man leicht einen oberen Grenzwert für die Wahrscheinlichkeit von CMA solcher Betrachtungseinheiten angeben. Falls sich durch diese Maximaleinschätzung die Wahrscheinlichkeit für das Versagen der Systemfunktion nicht merkbar erhöht, brauchen keine weiteren Untersuchungen zur Quantifizierung der entsprechenden CMA durchgeführt zu werden.

Die Wahrscheinlichkeit für den gemeinsamen Ausfall von zwei Betrachtungseinheiten 1 und 2, d.h. für das Eintreten eines Ausfalls e_1 und eines Ausfalls e_2, ist

$$\begin{aligned} W(e_1 \wedge e_2) &= W(e_1) \cdot W(e_2/e_1) \\ &= W(e_2) \cdot W(e_1/e_2) \end{aligned} \qquad (3.55)$$

wobei

$W(e_i)$ $\triangleq$ unbedingte Wahrscheinlichkeit für das Eintreten von e_i,

$W(e_i/e_j)$ $\triangleq$ bedingte Wahrscheinlichkeit für das Eintreten von e_i, unter der Bedingung, daß e_j eintritt.

Falls e_1 und e_2 voneinander abhängig sind, haben jeweils die unbedingte Wahrscheinlichkeit $W(e_i)$ und die bedingte Wahrscheinlichkeit $W(e_i/e_j)$ unterschiedliche Werte. Da Wahrscheinlichkeiten immer ≤ 1 sind, gilt

$$W(e_1 \wedge e_2) \leq W(e_1) \qquad (3.56)$$

$$W(e_1 \wedge e_2) \leq W(e_2) \qquad (3.57)$$

Als oberen Grenzwert W_{OG} erhält man daraus die kleinere der beiden Wahrscheinlichkeiten

$$W(e_1 \wedge e_2) \leq \text{Min}[W(e_1), W(e_2)] = W_{OG} \qquad (3.58)$$

Wird nach der Wahrscheinlichkeit des gemeinsamen Ausfalls von drei Betrachtungseinheiten gefragt, so erhält man auf die gleiche Weise folgende obere Grenzwerte:

$$W(e_1 \wedge e_2 \wedge e_3) \leq \text{Min}[W(e_1), W(e_2), W(e_3)] \qquad (3.59)$$

$$W(e_1 \wedge e_2 \wedge e_3) \leq \text{Min}[W(e_1 \wedge e_2), W(e_1 \wedge e_3), W(e_2 \wedge e_3)] \qquad (3.60)$$

Beziehung (3.60) ergibt sich aus den obigen Betrachtungen, wenn man die Doppelausfälle jeweils als Einzelereignisse ansieht.

3.3.5.2 Kopplung von Ausfällen

Aus der Betriebserfahrung können höchstens Wahrscheinlichkeiten für das Eintreten von CMA an mehreren gleich aufgebauten und gleich eingesetzten Komponenten abgeleitet werden (Abschnitt 3.3.4). Im Hinblick auf menschliches Fehlverhalten können Wahrscheinlichkeitsaussagen meist nur für einzelne Handlungen gewonnen werden. In vielen Fällen werden aber Aussagen über die Wahrscheinlichkeit benötigt, mit der der gleiche Operator mehrere gleichartige Aktionen, Bedienungen, Instandhaltungsarbeiten falsch ausführt oder CMA gleichzeitig in mehreren Teilsystemen (z.B. Meßkanalgruppen) vorliegen. Zur Beantwortung dieser Fragen muß versucht werden, eine Aussage über die Größe der Abhängigkeit der Ausfälle zu erhalten. Dazu wird eine Kopplung zwischen den Ausfällen angenommen und der jeweils vorliegende Grad der Kopplung abgeschätzt. In WASH-1400 werden folgende Kopplungsarten unterschieden:

- keine Kopplung (no coupling),
- mittlere Kopplung (loose coupling),
- starke Kopplung (tight coupling),
- vollständige Kopplung (complete coupling).

- Keine Kopplung

Unter "keine Kopplung" versteht man Unabhängigkeit der Ausfälle. Diese wird nach WASH-1400 für menschliche Fehlhandlungen immer dann erwartet, wenn sich die durchzuführenden Aufgaben nicht ähnlich sind oder wenn die Durchführung dieser Aufgaben räumlich und zeitlich weitgehend getrennt erfolgt. Zu den Handlungen, die sich nicht ähnlich sind und für die deshalb keine Kopplung erwartet wird, werden auch die Durchführung einer Maßnahme und die anschließende Kontrolle durch eine andere Person gerechnet.

In WASH-1400 wird davon ausgegangen, daß ein unterer Grenzwert von 10^{-5} für die Wahrscheinlichkeit menschlicher Fehlhandlungen nicht unterschritten werden kann. Selbst bei vielen Möglichkeiten für das Entdecken einer Fehlhandlung oder bei sehr hoher personeller Redundanz muß immer mit einer Restwahrscheinlichkeit für menschliches Versagen gerechnet werden. Dies ist u.a. damit begründet, daß bei einer Vielzahl von beteiligten Personen der Informationsaustausch schlechter wird und die Beteiligten sich teilweise aufeinander verlassen /F2, 3-32/. Aus diesen Gründen wird davon ausgegangen, daß für die fälschliche Ausführung eines Arbeitsganges bzw. einer Aktion auch bei Einsatz hoher personeller Redundanz ein Wert unter 10^{-5} nicht oder nur sehr schwer erreicht werden kann.

Ausfälle von gleichartigen Bauteilen (d.h. der Hardware) wurden in WASH-1400 grundsätzlich als unabhängig angesetzt, ausgenommen sind Ausfälle der Steuerstäbe für die Reaktorschnellabschaltung, Ausfälle aufgrund einer Überlastung der Dieselaggregate und Folgeausfälle. CMA redundanter Bauteile wurden sonst nur aufgrund von menschlichen Fehlhandlungen während des Betriebs der Anlage berücksichtigt.

- Mittlere Kopplung

In Abschnitt 3.3.5.1 wurde gezeigt, wie man einen oberen Grenzwert für die Wahrscheinlichkeit des Ausfalls der untersuchten

Systemfunktion erhält bei Berücksichtigung von CMA mehrerer Komponenten bzw. Teilsysteme. Ein unterer Grenzwert für die Wahrscheinlichkeit von CMA ist durch die Wahrscheinlichkeit von unabhängigen Ausfällen gegeben. Bei zwei Komponenten oder Teilsystemen bedeutet das:

oberer Grenzwert:

$$W_{OG} = \text{Min}[W(e_1),\ W(e_2)] \tag{3.61}$$

unterer Grenzwert:

$$W_{UG} = W(e_1) \cdot W(e_2) \tag{3.62}$$

Diese Grenzen definieren einen Bereich, in dem die tatsächliche Wahrscheinlichkeit für den CMA liegt. In WASH-1400 wird als Näherung angenommen, daß die Wahrscheinlichkeit zwischen diesen beiden Grenzen logarithmisch normalverteilt ist. Entsprechend Abschnitt 3.2 ist der Medianwert dann durch das geometrische Mittel zwischen oberer und unterer Grenze gegeben:

$$W = \sqrt{W_{OG} \cdot W_{UG}} \tag{3.63}$$

Für zwei Betrachtungseinheiten 1 und 2 mit $W(e_1) \leq W(e_2)$ gilt

$$W = \sqrt{W^2(e_1) \cdot W(e_2)} \tag{3.64}$$

Diese "mittlere Kopplung", in WASH-1400 auch als "square-root bounding"-Modell bezeichnet, kann nur als erste Näherung für die Wahrscheinlichkeit von CMA angesehen werden, die dann verwendet wird, wenn keine weiteren Informationen vorliegen. Die Anwendung dieser Näherung erscheint insbesondere für höher redundante Systeme und bei sehr zuverlässigen Komponenten problematisch, da dann unter Umständen über viele Größenordnungen zu mitteln ist.

Die mittlere Kopplung wird in WASH-1400 für Fehlhandlungen der Betriebsmannschaft zugrunde gelegt, wenn zwei sehr ähnliche Handlungen durch das gleiche Personal durchzuführen sind, wie

- Fehlkalibrierung von zwei Meßkanalgruppen des Reaktorschutzsystems,

- Durchführung von zwei gleichartigen Handmaßnahmen bei Funktionsprüfungen.

So wird die mittlere Kopplung in WASH-1400 zur Abschätzung der Wahrscheinlichkeit für eine gleichzeitig falsche Stellung von zwei redundanten Handarmaturen verwendet, wenn beide Armaturen bei einer Funktionsprüfung betätigt werden müssen. Außerdem wird mit dieser Methode in WASH-1400 die Wahrscheinlichkeit für den Ausfall des mechanischen Systems zur Reaktorschnellabschaltung abgeschätzt.

In /F2, 3-33/ wird der Begriff der mittleren Kopplung etwas abgeändert interpretiert. Dort wird eine mittlere Kopplung in den Fällen erwartet, in denen

- verschiedene Personen dieselbe Aufgabe durchführen, aber räumlich oder zeitlich versetzt, oder
- eine bestimmte Person eine Aufgabe nach einer längeren Zeitunterbrechung (ca. 24 Stunden) nochmals durchführt.

In der vorliegenden Studie wird eine mittlere Kopplung zwischen menschlichen Fehlhandlungen immer dann angesetzt, wenn vom gleichen Personal Kalibrierungen an zwei vom physikalischen Meßprinzip gleichartigen Meßkanalgruppen für unterschiedliche Prozeßvariable durchgeführt werden. Einen derartigen Fall stellen zum Beispiel aufeinanderfolgende Justierarbeiten an den Meßkanalgruppen zur Erfassung des Druckhalter-Wasserstandes und zur Erfasssung des Kühlmitteldruckes dar. Bei vom physikalischen Meßprinzip verschiedenartigen Meßkanalgruppen ist eine derartige Abhängigkeit aus folgenden Gründen nicht zu erwarten: Zur Überprüfung und Justierung von Druck- bzw. Temperatur-Meßumformern werden unterschiedliche Meßgeräte eingesetzt. Ebenso kann ein fälschliches Absperren von Wirkdruckleitungen nur bei den Meßarten Druck bzw. Differenzdruck auftreten. Eine denkbare Fehljustierung der Grenzsignalgeber aufgrund eines defekten Meßgerätes ist über eine Vielzahl von unterschiedlichen Meßkanalgruppen hinweg sehr unwahrscheinlich.

Sind mehr als zwei vom physikalischen Meßprinzip gleichartige Meßkanalgruppen zur Auslösung eines Reaktorschutzsignals vor-

handen, so ist die Wahrscheinlichkeit der Fehlkalibrierung aller Meßkanalgruppen als deutlich geringer einzuschätzen. Eine solche Abhängigkeit der menschlichen Fehlhandlungen könnte etwa durch eine "leichte Kopplung" beschrieben werden. Wie weiter unten ausgeführt wird, kann der Einfluß einer solchen Kopplung aber vernachlässigt werden. Entsprechende CMA mehrerer Meßkanalgruppen wären bei der Auslösung der Reaktorschnellabschaltung zu bewerten. Sie spielen dort gegenüber Ausfällen des Relaisteils keine dominierende Rolle.

- Starke Kopplung

Eine "starke Kopplung" von Ausfällen wird in WASH-1400 für redundante Komponenten unter extremen Umgebungsbedingungen berücksichtigt (für Pumpen, die innerhalb des Sicherheitsbehälters installiert und damit nach Kühlmittelverluststörfällen extremen Bedingungen ausgesetzt sind). Eine solche Kopplung wird auch für die Bewertung gleichartiger Handmaßnahmen zugrunde gelegt, wie sie für die Justierung von redundanten Meßkanälen innerhalb einer Meßkanalgruppe notwendig sind. Dabei wird von einer Ausfallwahrscheinlichkeit von 10^{-2} pro Anforderung für menschliches Fehlverhalten bei der Kalibrierung eines Meßkanals ausgegangen. Für eine zweite identische Aktion (Kalibrierung des zweiten Meßkanals) wird unter der Bedingung, daß schon die erste Aktion falsch ausgeführt wurde, eine Wahrscheinlichkeit von 10^{-1} für eine Fehlhandlung angesetzt. Das kann so interpretiert werden, daß bei der Kalibrierung des zweiten Meßkanals dem Bedienungsmann in 90 % aller Fälle auffällt, daß sein Prüfgerät fehlerhaft ist oder falsch eingesetzt wird. Es wird angenommen, daß die bedingte Wahrscheinlichkeit für das Fehlkalibrieren des dritten Meßkanals gleich 1 ist. Damit ergibt sich für CMA einer Meßkanalgruppe aufgrund von Fehlkalibrierung eine Wahrscheinlichkeit von 10^{-3}. Die starke Kopplung wurde in WASH-1400 auch bei der Abschätzung der oberen Grenze für CMA von Steuerstäben angewandt. (Bei diesen wird ein weiterer Faktor 0,1 in Rechnung gestellt. Dieser soll näherungsweise den Bruchteil der "common mode"-Ereignisse berücksichtigen, der zu einem vollständigen Ausfall der betrachteten Komponentenfunktion führt (Abschnitt 3.3.6.4.2)).

In /F2, 3-33 und -34/ wird abweichend davon für "starke Kopplung" von menschlichem Fehlverhalten (high dependence) eine logarithmische Normalverteilung angesetzt, deren Medianwert zwischen denjenigen für "vollständige Kopplung" und "mittlere Kopplung" liegt; die mit diesen Kopplungen berechneten Wahrscheinlichkeiten werden als 95-%- und 5-%-Vertrauensgrenzen herangezogen. Diese Methode hat den Vorteil einer gleichmäßigen Aufteilung der logarithmischen Wahrscheinlichkeitsskala zwischen "keine Kopplung" und "vollständige Kopplung"; sie liefert bei Wahrscheinlichkeiten für einzelne Ausfälle > 10^{-4}, was in den vorliegenden Fällen zutrifft, gegenüber der oben geschilderten Vorgehensweise größere Wahrscheinlichkeiten von CMA.

Diese zuletzt erläuterte Vorgehensweise wird für die vorliegende Studie übernommen. In ihr wird, abweichend von WASH-1400, eine "starke Kopplung" auch in Fällen angesetzt, in denen Justierarbeiten an mehreren Meßkanalgruppen zur Erfassung der gleichen Prozeßvariablen durchgeführt werden, beispielsweise für die Fehljustierung der vier Meßkanalgruppen zur Erfassung der Flutbehälter-Wasserstände. Diese Vorgehensweise ist pessimistisch, zumal die Meßkanalgruppen räumlich getrennt sind. Eine Fehlkalibrierung von mehr als einer Meßkanalgruppe wird mit hoher Wahrscheinlichkeit bemerkt werden.

- Vollständige Kopplung

Unter "vollständige Kopplung" versteht man vollständige Abhängigkeit zwischen den Ausfällen. So ist bei "vollständige Kopplung" von menschlichem Fehlverhalten die bedingte Wahrscheinlichkeit, daß mehrere gleichartige Handlungen nicht oder falsch ausgeführt werden, gleich 1, wenn schon die erste Aktion nicht oder falsch ausgeführt wird. Die Wahrscheinlichkeit für CMA ist dann durch den in Abschnitt 3.3.5.1 diskutierten oberen Grenzwert gegeben.

Als Beispiel wird in WASH-1400 der Fall angeführt, daß ein einzelner Schritt in einer Betriebsanweisung die Durchführung mehrerer Aktionen erfordert, z.B. die Betätigung von zwei Ventilen.

Die beiden Armaturen werden dann durch den Operator als eine Einheit betrachtet: Wird ein Ventil betätigt, so wird auch das andere betätigt; vergißt der Operator die Betätigung des einen Ventils, so wird das auch für das andere zutreffen.

Eine "vollständige Kopplung" von Hardware-Ausfällen wird in WASH-1400 bei einer Überflutung von redundanten Pumpen (Folgeausfall) angesetzt. In der vorliegenden Studie wird eine "vollständige Kopplung" der Ausfälle von Bauteilen dann berücksichtigt, wenn gleichartige Komponenten Betriebs- oder Umgebungsbedingungen ausgesetzt sind, für die sie nicht ausgelegt sind: Kommt es zum Ausfall einer Komponente aufgrund dieser Bedingungen, so ist auch ein Ausfall der anderen gleichartigen Komponenten zu erwarten.

- Leichte Kopplung

In /F2, 3-34/ wird der Begriff "leichte Abhängigkeit" als eine zusätzliche Abstufung des Grades an wechselseitiger Abhängigkeit mehrerer Handlungen eingeführt. Dafür wird eine logarithmische Normalverteilung angesetzt, deren Medianwert zwischen denjenigen für "mittlere Kopplung" und "keine Kopplung" liegt; die entsprechenden Wahrscheinlichkeiten werden als 95-%- und 5-%-Vertrauensgrenzen herangezogen. Diese "leichte Abhängigkeit" wird Handlungen zugemessen, die offensichtlich nicht völlig unabhängig sind, so zum Beispiel für mehrere verschiedenartige Handlungen, die von der gleichen Person ausgeführt werden. In der vorliegenden Studie wurde diese Art der Kopplung nicht verwendet, zumal der Einfluß leicht gekoppelter Handlungen auf die Ergebnisse vernachlässigbar ist.

3.3.5.3 Ausfallwahrscheinlichkeit pro Anforderung und Ausfallrate

Die Wahrscheinlichkeit für den gemeinsamen Ausfall von zwei baugleichen (ähnlichen) Komponenten oder Teilsystemen, d.h. für

das Eintreten eines Ausfalls e_1 und eines Ausfalls e_2, kann man nach WASH-1400 auch folgendermaßen darstellen:

$$W(e_1 \wedge e_2) = \sum_M W(e_1 \wedge e_2/M) \cdot W(M) \qquad (3.65)$$

Dabei bezeichnet M die unterschiedlichen, einander ausschließenden Mechanismen oder Bedingungen (Ursachen) für das Eintreten der Ausfälle e_1 und e_2.

Bezeichnet M_o die Bedingungen, unter denen unabhängige Ausfälle e_1 und e_2 vorliegen, und $M \neq M_o$ die unterschiedlichen Bedingungen (Ursachen) für CMA, so gilt:

$$W(e_1 \wedge e_2) = W(e_1) \cdot W(e_2) \cdot W(M_o) + \sum_{M \neq M_o} W(e_1 \wedge e_2/M) \cdot W(M) \qquad (3.66)$$

Näherungsweise kann meist $W(M_o) \cong 1$ gesetzt werden.

Ein häufig verwendeter Ansatz ist, die Ursachen von CMA, ebenso wie die Ursachen für unabhängige Ausfälle, zusammenzufassen:

$$W(e_1 \wedge e_2) = W(e_1) \cdot W(e_2) \cdot W(M_o) + W(e_1 \wedge e_2/M) \cdot W(M) \qquad (3.67)$$

M beschreibt jetzt die Gesamtheit der Bedingungen für das Auftreten von CMA. W(M) ist die Wahrscheinlichkeit für das Eintreten irgendeiner der Bedingungen.

Wenn eine "vollständige Kopplung" zwischen den Ausfällen bei Eintreten von M unterstellt wird, so gilt

$$W(e_1 \wedge e_2/M) = 1 \qquad (3.68)$$

Dem liegt die pessimistische Annahme zugrunde, daß jeweils alle redundanten Betrachtungseinheiten ausfallen und das zum gleichen Zeitpunkt. Die Wahrscheinlichkeit für das Eintreten von CMA ist dann durch W(M) gegeben.

Werden solche CMA durch Bedingungen beim Betrieb bewirkt, so steigt die Wahrscheinlichkeit der CMA mit der Betriebszeit. Ähnlich wie bei unabhängigen Ausfällen kann dann die Wahrscheinlichkeit für das Eintreten von CMA durch eine (konstante) Ausfallrate λ_{CMA} beschrieben werden: $W(M) = \exp(-\lambda_{CMA} \cdot t)$

Solche CMA können z.B. durch Instandhaltungsfehler oder durch ständig vorliegende ungünstige Bedingungen verursacht werden.

Liegt die Ursache der CMA in der Planung und Herstellung, so ist die Beschreibung der CMA mit Hilfe einer konstanten Ausfallwahrscheinlichkeit pro Anforderung

$$W(M) = p_{CMA} \tag{3.69}$$

möglich. Damit können CMA behandelt werden, die inhärent zum Zeitpunkt der Inbetriebnahme bereits vorliegen und zum sofortigen Ausfall bei Anforderung führen.

3.3.5.4 B e t a - F a k t o r - M e t h o d e

In /F2, 3-35/ wird erstmals davon ausgegangen, daß CMA wie unabhängige Funktionsausfälle näherungsweise durch eine konstante Ausfallrate beschrieben werden können. Im HTGR AIPA Status Report /F2, 3-36/ wird darüber hinaus die Annahme getroffen, daß für eine bestimmte Funktion der redundanten Komponenten das Verhältnis ß zwischen den CMA und allen Ausfällen im Durchschnitt nur vom Komponententyp abhängt.

Die Methode wird in /F2, 3-36 und -37/ zunächst anhand eines aus 2 redundanten Komponenten aufgebauten Systems entwickelt. Zwei Typen von Komponentenausfällen werden unterschieden:

Typ 1: Komponentenausfall, der vollkommen unabhängig ist vom Funktionieren oder dem Ausfall der anderen Komponenten des Systems, und
Typ 2: Mehrfachausfall, der durch ein einziges (gemeinsames) Ereignis verursacht wird (common cause failure).

Dementsprechend kann die Ausfallrate einer Komponente aus zwei voneinander unabhängigen Ausdrücken zusammengesetzt werden, der Ausfallrate für Ausfälle des Typs 1 und der Ausfallrate für Ausfälle des Typs 2:

$$\lambda = \lambda_1 + \lambda_2 \tag{3.70}$$

Es wird vorausgesetzt, daß beim Auftreten eines Ausfalls vom Typ 2 alle redundanten Komponenten gleichzeitig ausfallen. Diese Annahme ist pessimistisch und dürfte um so weniger zutreffen, je höher der Redundanzgrad des betrachteten Systems ist (Abschnitt 3.3.5.5).

Zur Behandlung von Ausfällen des Typs 2 wird ein Faktor ß eingeführt, der als bedingte Wahrscheinlichkeit dafür definiert wird, daß ein Ausfall des Typs 2 stattfindet, wenn ein Komponentenausfall vorliegt

$$ß = \frac{\lambda_2}{\lambda} \tag{3.71}$$

Interessiert bei einem redundanten System die durch Ausfälle des Typs 2 verursachte Ausfallwahrscheinlichkeit q_2 zum Zeitpunkt t, wobei vorausgesetzt wird, daß das System zum Zeitpunkt t = 0 funktionsfähig ist, so ergibt sich diese in erster Näherung zu

$$q_2 = \beta\lambda t \tag{3.72}$$

Die entsprechenden exakten Formeln für die Überlebenswahrscheinlichkeit r von 1v2-, 2v3- und 1v3-Systemen lauten nach /F2, 3-36/:

$$r_{1v2} = 2\exp(-\lambda t) - \exp[-(2-ß)\lambda t] \tag{3.73}$$

$$r_{2v3} = 3\exp[-(2-ß)\lambda t] - 2\exp[-(3-2ß)\lambda t] \tag{3.74}$$

$$r_{1v3} = \exp[-(3-2ß)\lambda t] - 3\exp[-(2-ß)\lambda t] + 3\exp(-\lambda t) \tag{3.75}$$

Der Faktor ß wird in /F2, 3-36/ auch auf Komponenten mit einer Ausfallwahrscheinlichkeit pro Anforderung angewendet, wobei sich

die Nichtverfügbarkeit des betrachteten redundanten Systems analog zur oben genannten Ausfallwahrscheinlichkeit q_2 errechnet.

Ausfälle des Typs 1 werden weiter in folgende Kategorien unterteilt:

Typ 1a: Ausfall, der als unabhängiger Ausfall auftritt und keine weiteren Ausfälle nach sich zieht (independent failure), und
Typ 1b: Ausfall, der als unabhängiger Ausfall auftritt, jedoch weitere Ausfälle nach sich zieht (causal failure).

Zur Behandlung von Ausfällen des Typs 1b wird ein Faktor γ eingeführt, der als bedingte Wahrscheinlichkeit dafür definiert ist, daß ein Komponentenausfall einen Folgeausfall verursacht, unter der Bedingung, daß die Komponente selbst ausgefallen ist und kein Ausfall des Typs 2 (common cause failure) vorliegt:

$$\gamma = \frac{\lambda_{1b}}{\lambda_{1a} + \lambda_{1b}} \qquad (3.76)$$

mit

$$\lambda = \lambda_{1a} + \lambda_{1b} + \lambda_2$$

Für die Überlebenswahrscheinlichkeit eines 1v2-Systems wird in /F2, 3-36/ folgende Näherungsformel abgeleitet:

$$r_{1v2} = 2(1-\gamma)\exp(-\lambda t) - (1-2\gamma)\exp[-(2-\beta)\lambda t] \qquad (3.77)$$

Zur Aufteilung von CMA in die Typen 1b und 2 ist zu bemerken, daß CMA des Typs 1b (Folgeausfälle) in den Fehlerbäumen mit Hilfe von Folgeausfall- oder Sekundär-Verknüpfungen (Abschnitt 3.2, Bild F2, 3-3) dargestellt werden. Es ist evident, daß die Wahrscheinlichkeit von Folgeausfällen sehr vom Anlagenkonzept und dem Systemaufbau abhängt. Die Angabe eines allgemeingültigen γ-Faktors ist damit wohl nicht möglich.

Die Beta-Faktor-Methode geht davon aus, daß bei Auftreten von CMA alle redundanten Komponenten praktisch gleichzeitig ausfallen. Das wird durch eine in /F2, 3-36/ durchgeführte Aus-

wertung von in den USA gewonnener nuklearer Betriebserfahrung gestützt, mit deren Hilfe Vertrauensgrenzen für ein logarithmisch normalverteiltes ß ermittelt werden. Danach stellt ein Erwartungswert ß = 0,1 für alle Typen von Komponenten und alle Ausfallarten eine gute Näherung dar.

Nach Tabelle II, 4-4 aus /F2, 3-36/ werden im Mittel mehr als die Hälfte der "common cause"-Ausfälle durch Fehler in der Planung und mehr als ein Viertel durch menschliche Fehlhandlungen (Fehler des Operators und Wartungsfehler) bedingt. "Common cause"-Ausfälle aufgrund von Fehlern bei der Herstellung sind hingegen überhaupt noch nicht beobachtet worden. Was unter den erwähnten Arten von Fehlern jeweils zu verstehen ist, wird in Tabelle II, 4-2 aus /F2, 3-36/ aufgezeigt. Es wird argumentiert, daß die Mehrzahl der Planungsfehler und der menschlichen Fehlhandlungen in einem gleichzeitigen oder nahezu gleichzeitigen Ausfall der gleichartigen redundanten Teile resultieren würde. Für die anderen Ursachen, die den Rest der Beiträge zur Wahrscheinlichkeit der "common cause"-Ausfälle liefern, läge allerdings eine ziemlich schwache Kopplung der Ausfälle vor, die z.B. nur zu einem Anwachsen der unabhängigen Ausfallraten führen würde (Abschnitt 3.3.5.6).

Eine genaue Durchsicht der Tabelle II, 4-2 aus /F2, 3-36/, die aufgrund der Betriebserfahrung in den USA erstellt wurde, zeigt für die Ursachen von "common cause"-Ausfällen folgendes:

Die aufgetretenen Planungsfehler waren:

- unvorhergesehene Stellen von Einzelausfällen in redundant aufgebauten Systemen,
- elektrische oder mechanische Abhängigkeit von einem gemeinsamen Element,
- mangelhafte räumliche Trennung redundanter Einheiten,
- Abhängigkeit von Elementen, deren Ausfall oder Fehlverhalten eine Schutzaktion nötig macht,
- gemeinsamer Fehler durch fehlerhafte Vorhersage des Systemverhaltens,
- unvorhergesehene Abhängigkeit zwischen Systemen untereinander,

- mangelhafte räumliche Trennung zwischen Systemen,
- gemeinsamer Fehler durch fehlerhafte Vorhersage des Anlagenverhaltens.

Die menschlichen Fehlhandlungen, die "common cause"-Ausfälle nach sich zogen, waren

- Fehljustierungen,
- Wartungs- und Instandsetzungsfehler,
- mangelhafte Aufzeichnungen und Unterlagen,
- ungeeignete Handlungen des Operators.

Die oben genannten funktionellen Abhängigkeiten aufgrund von Planungsfehlern wurden in der vorliegenden Studie bereits im Rahmen der Fehlerbaumanalyse berücksichtigt. Deshalb war es im Gegensatz zu /F2, 3-36/ nicht notwendig, diese Abhängigkeiten mit Hilfe der Beta-Faktor-Methode abzuschätzen. Außerdem ist zu berücksichtigen, daß die redundanten Stränge der Sicherheitssysteme weitgehend räumlich getrennt aufgebaut sind.

Gemeinsame Ausfälle aufgrund einer fehlerhaften Vorhersage des Anlagen- bzw. Systemverhaltens können unseres Erachtens durch die während des bestimmungsgemäßen Betriebs gewonnene Betriebserfahrung kaum erfaßt werden.

Bei der Beurteilung des menschliches Fehlverhaltens in der deutschen Referenzanlage ist zu bedenken, daß bei Justierarbeiten immer personelle Redundanz vorliegt und gleichzeitig diversitäre Meßgeräte eingesetzt werden. Über alle Justierarbeiten, aber auch über andere Instandhaltungsarbeiten werden detaillierte Aufzeichnungen geführt. Liegen nach Instandhaltungsarbeiten Fehlstellungen von Motorarmaturen in Sicherheitssystemen vor, so werden diese bei Anforderung der Systeme durch Kontrollbefehle korrigiert. Funktionsprüfungen der redundanten Stränge werden außerdem wöchentlich versetzt von unterschiedlichen Schichten des Kraftwerkspersonals durchgeführt. Die meisten der zur Beherrschung von Störfällen geforderten Systeme und Komponenten werden automatisch in Betrieb genommen, Handlungen des Personals sind nur in wenigen Fällen erforderlich.

Aus den dargelegten Gründen ist ein vergleichbarer Beitrag zu den "common cause"-Ausfällen bei der deutschen Referenzanlage nicht zu erwarten. Die Beta-Faktor-Methode wird daher nicht als geeignetes Hilfsmittel zur Bewertung der "common cause"-Ausfälle angesehen, denn sie liefert unter Zugrundelegung eines Erwartungswertes des ß-Faktors von 0,1 meist viel zu pessimistische Ergebnisse.

3.3.5.5 Spezialisiertes Marshall-Olkin-Modell

Mit diesem von Vesely entwickelten Verfahren /F2, 3-38/, das eine Spezialisierung des Modells ("multivariate exponential model") von Marshall und Olkin darstellt, lassen sich "common mode"-Ausfallraten in Abhängigkeit von der Anzahl der gleichzeitig ausgefallenen gleichartigen Komponenten berechnen. Es wird also zwischen dem gleichzeitigen Ausfall von 2, von 3, von 4 usw. Komponenten, allgemein von x Komponenten, unterschieden. Dem Verfahren liegen folgende Annahmen zugrunde:

- Die Zeiträume bis zum Eintritt von CMA mit x Komponenten sind exponential verteilt, d.h. die Ausfallraten λ_x sind konstant.
- Die Komponenten sind reparierbar, wobei die Instandsetzungszeiten gegenüber dem Kehrwert der Ausfallraten vernachlässigbar sind.
- Die Ausfallraten λ_x für CMA mit x bestimmten Komponenten hängen nur von der Anzahl x ab, nicht dagegen von den speziellen Komponenten, d.h., alle Komponenten sind als gleichwertig anzusehen.
- Bei Vorliegen eines CMA ist jede Komponente mit der gleichen Wahrscheinlichkeit p ausgefallen, d.h. mit dieser Wahrscheinlichkeit am CMA beteiligt.

Zur Bestimmung der λ_x für x bestimmte Komponenten bzw. zur Bestimmung der Λ_x für x beliebige Komponenten müssen aus der Betriebserfahrung zwei Größen gewonnen werden:

- die Summen-Ausfallrate λ_{CMA} für CMA mit einer festgelegten Mindestanzahl von beteiligten Komponenten und

- die bedingte Wahrscheinlichkeit p, daß bei Auftreten eines CMA eine bestimmte Komponente ausfällt.

Während p ein Maß für die Stärke der Kopplung der Komponenten untereinander darstellt, ist λ_{CMA} ein Maß für die Häufigkeit von CMA. Die Abschätzung der beiden Größen λ_{CMA} und p kann nach /F2, 3-38/ mit Hilfe folgender Beziehungen erfolgen:

$$\lambda_{CMA} = \frac{N_{X1}}{T} \tag{3.78}$$

mit

T ≙ Beobachtungszeitraum

N_{X1} ≙ Anzahl der CMA mit dem gleichzeitigen Ausfall von X1 und mehr Komponenten im Beobachtungszeitraum T

und

$$p_x = \frac{\binom{m}{x} p^x (1-p)^{m-x}}{C} \tag{3.79}$$

$$C = \sum_{x=x1}^{m} \binom{m}{x} p^x (1-p)^{m-x} \tag{3.80}$$

mit

p_x ≙ bedingte Wahrscheinlichkeit, daß bei Auftreten eines CMA genau x Komponenten ausfallen

C ≙ Normierungsfaktor

m ≙ Anzahl der Komponenten

p wird durch Maximierung des folgenden Ausdruckes der Wahrscheinlichkeit P bestimmt (Multinomialverteilung):

$$P(N_{X1} = n_{X1},\ldots,N_m = n_m) = \frac{n!}{n_{X1}!\ldots n_m!} p_{X1}^{n_{X1}} \ldots p_m^{n_m} \tag{3.81}$$

mit

$N_{X1}\ldots N_m$ ≙ poissonverteilte Zufallsgröße für die Anzahl der CMA mit X1...m ausgefallenen Komponenten

$n_{X1 \cdots n_m}$ ≙ Anzahl der beobachteten CMA mit X1...m ausgefallenen Komponenten im Beobachtungszeitraum T

n ≙ Anzahl der CMA mit mehr als X1 ausgefallenen Komponenten

Während also für die Schätzung von λ_{CMA} zunächst nur die Anzahl aller beobachteten CMA benötigt wird, ist für die Bestimmung von p zusätzlich die Kenntnis der Anzahl der von den insgesamt vorhandenen Komponenten jeweils am CMA beteiligten Komponenten notwendig.

Das beschriebene Verfahren wird als eine der alternativen Methoden zur Abschätzung der Nichtverfügbarkeit des mechanischen Systems zur Reaktorschnellabschaltung aufgrund von CMA verwendet.

3.3.5.6 A u s f a l l r a t e n - K o p p l u n g

Die Beschreibung einer leichten Art der Abhängigkeit zwischen den Ausfällen von Komponenten kann nach WASH-1400 durch eine "Ausfallratenkopplung" der Komponentenfunktionen berücksichtigt werden. Diese Art der Kopplung kann bei Streubreitenrechnungen (Abschnitt 3.2.3.5) zur Anwendung kommen und darf nicht mit der "Kopplung von Ausfällen" nach Abschnitt 3.3.5.2 verwechselt werden. Die Ausfallratenkopplung führt nicht zu gleichzeitigen, sondern zu zeitlich versetzten Ausfällen der Komponenten. Anders als in Abschnitt 3.3.5.3 werden in der Beziehung

$$W(e_1 \wedge e_2) = W(e_1) \cdot W(e_2) \cdot W(M_o) + W(e_1 \wedge e_2/M) \cdot W(M) \qquad (3.82)$$

für den zweiten Term, der die CMA beschreibt, unabhängige Ausfälle der einzelnen Komponenten mit veränderten Wahrscheinlichkeiten angesetzt:

$$W(e_1 \wedge e_2/M) = W(e_1/M) \cdot W(e_2/M) \qquad (3.83)$$

Für die Zeitspanne nach Eintreten der Bedingung M sind dann veränderte Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung zu berücksichtigen.

Mit einer solchen Vorgehensweise können z.B. gemeinsame Fertigung, Frühausfälle, Verschleiß- und Korrosionsausfälle, Materialermüdung, gewisse Wartungsfehler sowie Ausfälle aufgrund erschwerter Umgebungsbedingungen behandelt werden, indem für das in Frage kommende Zeitintervall erhöhte Ausfallraten zugrunde gelegt werden.

Gemeinsame Einflüsse während Planung und Herstellung von gleichartigen Komponenten, aber auch bei der Funktionsprüfung, Wartung oder Instandsetzung können nicht nur größere Werte der Ausfallraten nach sich ziehen. So können z.B. überdurchschnittliche Qualitätssicherung oder höhere Anforderungen an die Wartung niedrigere Ausfallraten zur Folge haben. Jedenfalls bedingen diese gemeinsamen Einflüsse eine gewisse Abhängigkeit zwischen den Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung gleichartiger Komponenten.

Diese Abhängigkeit kann in den Zuverlässigkeitsuntersuchungen durch eine Kopplung der Ausfallraten bzw. der Ausfallwahrscheinlichkeiten pro Anforderung behandelt werden. Die Werte dieser Parameter für die einzelnen gleichartigen Komponenten werden mit Hilfe des Rechenprogramms dann nicht unabhängig voneinander ausgespielt, sondern gemeinsam variiert. Bei dieser Ausfallraten-Kopplung wird also in jedem Simulationsspiel nur jeweils ein Wert der Ausfallraten für die Funktionsausfälle aller gleichartigen Komponenten verwendet.

3.3.6 Durchgeführte Bewertung

3.3.6.1 A l l g e m e i n e s

CMA aufgrund funktioneller Abhängigkeiten werden in der vorliegenden Studie, wie bereits erwähnt, mit den Fehlerbaumanalysen automatisch richtig erfaßt und daher, anders als in WASH-1400,

nicht besonders ausgewiesen. Die in WASH-1400 aufgrund solcher Abhängigkeiten ermittelten Beiträge zu CMA sind jedoch gering, da dort die Systemfunktionen so festgelegt wurden, daß die entsprechenden Systeme nur wenige gemeinsame Komponenten enthalten (z.B. wurde die Energieversorgung als eine separate Systemfunktion definiert). Diese Vorgehensweise bei der Definition der Systemfunktionen war in der vorliegenden Studie nicht zweckmäßig: Da die einzelnen Stränge der Sicherheitssysteme in der Referenzanlage weitgehend getrennt aufgebaut sind, hätte das vor allem die Ermittlung der Wahrscheinlichkeiten für den Ausfall der verschiedenen Systemfunktionen erschwert. Die Systemfunktionen wurden daher hier unter anderen Gesichtspunkten festgelegt (Fachband 1). In der vorliegenden Studie wird für alle zur Beherrschung eines Störfalls erforderlichen Systemfunktionen ein einziger Gesamtfehlerbaum erstellt. Damit wird sichergestellt, daß die Abhängigkeiten zwischen mehreren Systemfunktionen immer richtig berücksichtigt werden.

Bei CMA ähnlicher, vor allem aber baugleicher Komponenten oder Teilsysteme, die während des bestimmungsgemäßen Betriebes entdeckt werden, sind Hardware-Ausfälle und Ausfälle aufgrund menschlichen Fehlverhaltens zu unterscheiden. Die Wahrscheinlichkeiten dieser CMA können auf der Basis von Betriebserfahrung mit Hilfe von Modellen abgeschätzt werden. Wie im Abschnitt 3.3.5.2 erläutert wurde, liefert die Kopplung von Ausfällen nur eine erste Näherung.

In der vorliegenden Studie wird für die Bewertung von CMA aufgrund menschlicher Fehlhandlungen die von Swain gegenüber WASH-1400 modifizierte Methode der Kopplung von Ausfällen herangezogen, sofern diese Ausfälle mehrere Meßkanalgruppen betreffen. Auch bei der Bewertung von Hardware-Ausfällen mehrerer Meßkanalgruppen wird nicht immer eine Unabhängigkeit der CMA zugrunde gelegt. Aufgrund ingenieurmäßiger Abschätzung wird davon ausgegangen, daß CMA von gerätetechnisch gleichartigen Meßumformern mehrerer Meßkanalgruppen mit einer um zumindest eine Größenordnung geringeren Wahrscheinlichkeit als CMA in einer Meßkanalgruppe auftreten werden.

Nach Abschnitt 3.3.5.4 kann die Beta-Faktor-Methode im Rahmen der in dieser Studie durchgeführten Zuverlässigkeitsmethode kaum verwendet werden, da sie meist viel zu pessimistische Ergebnisse liefert. Die Beta-Faktor-Methode wird nur zur Abschätzung der Wahrscheinlichkeit von CMA der Steuerstäbe zur Reaktorschnellabschaltung herangezogen. Hier wird auch das Marshall-Olkin-Modell eingesetzt.

Im übrigen werden CMA von Komponenten im Rahmen der vorliegenden Studie nur dann durch eine CMA-Rate λ_{CMA} oder eine CMA-Wahrscheinlichkeit p_{CMA} pro Anforderung quantifiziert, wenn zu diesen Ausfällen Hinweise aus der Betriebserfahrung vorliegen. Voraussetzung für eine zahlenmäßige Bewertung ist, daß entsprechende CMA oder zumindest ähnliche "common mode"-Ereignisse aufgetreten sind. Bewertet wird dabei im allgemeinen nur die in der Bundesrepublik Deutschland gewonnene Betriebserfahrung, über die meist detailierte Informationen vorhanden sind. Aus dieser Betriebserfahrung sind "common mode"-Ereignisse für die Meßwerterfassung und für Abschlußrelais, für Notstromdiesel und für Pumpen im Langzeitbetrieb bekannt.

Seit Jahren wird in den USA und auch international /F2, 3-29/ eine systematische Erfassung und Dokumentation der aufgetretenen CMA angestrebt, um alle Erfahrungen aus der Kraftwerkstechnik zu nutzen. Allerdings werden in den verschiedenen Ländern teilweise sehr unterschiedlich aufgebaute Komponenten und Systeme eingesetzt, über die meist nur unzureichende Informationen veröffentlicht sind. Außerdem unterscheiden sich die Instandhaltungsmaßnahmen. Diese haben einen erheblichen Einfluß auf die frühzeitige Entdeckung und Beseitigung von "common mode"-Ursachen, können aber andererseits auch selbst zu CMA führen. Die Gewinnung und Verwendung quantitativer Daten von international aufgetretenen CMA ist daher nur in Ausnahmefällen möglich (insbesondere bei Relais).

Denkbare CMA bei Anforderung oder kurzzeitigem Betrieb baugleicher Komponenten, die während des bestimmungsgemäßen Betriebs entdeckt würden, bisher aber noch nie aufgetreten sind, werden

nur qualitativ behandelt. Solche CMA sind jedoch für die meisten Komponenten aus folgenden Gründen sehr unwahrscheinlich:

- Auch bei einer gemeinsamen Ausfallursache streuen die Ausfallzeitpunkte meist erheblich.
- Funktionsprüfungen erfolgen meist in kurzen Abständen (vierwöchentlich), und zwar zeitlich versetzt für die einzelnen redundanten Teilsysteme (Stränge), durch unterschiedliche Schichten des Betriebspersonals. Vorliegende Ausfälle werden damit kurzfristig entdeckt.
- Zumindest bei den baugleichen Pumpen liegen meist erhebliche Unterschiede in den Betriebszeiten vor, so daß auch dadurch deutliche Streuungen der Ausfallzeitpunkte zu erwarten sind.

Darüber hinaus werden bei schwerwiegenden Schäden an einer Komponente, die auf das Vorliegen einer "common mode"-Ursache hindeuten, auch die der redundanten Komponenten untersucht. Ein Beispiel dazu ist der Bruch der Welle einer Nachkühlpumpe (Abschnitt 3.3.6.2.2).

Diese Aussagen gelten meist nicht für die Funktionen von Komponenten, die nur halbjährlich oder jährlich überprüft werden. Dies sind vor allem (Abschnitt 5.2):

- die Notstromdiesel, die zwar monatlich überprüft, bei denen aber Vollastprüfungen nur halbjährlich durchgeführt werden,
- die Meßwerterfassung des Reaktorschutzsystems,
- die Druckhalter-Abblaseventile und Sicherheitsventile sowie die Frischdampf-Sicherheitsventile,
- ein Teil der Rückschlagventile im Not- und Nachkühlsystem,
- einige Abschlußrelais im Reaktorschutzsystem,
- Schütze und Steuerstäbe zur Reaktorschnellabschaltung.

Die für die Reaktorschnellabschaltung benötigten Komponenten werden aber, außer bei den jährlichen Funktionsprüfungen, auch bei betrieblichen Anforderungen getestet. CMA wurden dabei nur bei den Abschlußrelais beobachtet. Wegen der besonderen Bedeutung der Reaktorschnellabschaltung für die Beherrschung von Störfällen wird jedoch versucht, auch die anderen denkbaren Möglichkeiten von CMA zu quantifizieren (Abschnitt 3.3.6.5). Bei den Abschlußrelais der Referenzanlage ist zu berücksichtigen,

daß gerätetechnisch diversitär aufgebaute Relaisarten eingesetzt werden.

CMA von Sicherheitsventilen oder Abblaseventilen liefern nur dann einen maßgeblichen Beitrag zur Nichtverfügbarkeit der Sicherheitssysteme, wenn sie alle redundanten Ventile betreffen. Aus der weltweiten Betriebserfahrung sind zwar gemeinsame Ausfälle mehrerer solcher Ventile bekannt, CMA, die alle redundanten Ventile betreffen, sind demgegenüber aber erheblich unwahrscheinlicher und noch nie aufgetreten. Ein dominanter Beitrag zur Nichtverfügbarkeit der Systemfunktionen ist daher nicht zu erwarten.

Über CMA von Rückschlagventilen, durch die ein Öffnen verhindert wird, sind keine Betriebserfahrungen bekannt.

CMA von Notstromdieseln und CMA im Reaktorschutzsystem werden in den Abschnitten 3.3.6.3 bzw. 3.3.6.4 diskutiert.

Außer der Auswertung und Berücksichtigung der Betriebserfahrung der CMA in den Zuverlässigkeitsanalysen wird der Einfluß gezeigt, den eine Ausfallraten-Kopplung aller im wesentlichen baugleichen Komponenten auf die Ergebnisse der Zuverlässigkeitsanalyse und insbesondere auf die Vertrauensbereiche dieser Ergebnisse hat.

Bei CMA, die nur bei einem Störfall auftreten oder entdeckt werden, ist zwischen Folgeausfällen und CMA baugleicher (oder ähnlicher) Komponenten zu differenzieren. Denkbare Folgeausfälle werden in ihrer Wahrscheinlichkeit abgeschätzt. Gemeinsame Ausfälle baugleicher Komponenten, die nur bei einem Störfall auftreten oder entdeckt werden, sind dann möglich, wenn die Anforderungen sowohl beim Betrieb als auch bei Funktionsprüfungen nicht repräsentativ für die Anforderungen von Komponenten oder Systemen unter Störfallbedingungen sind. In diesem Zusammenhang sei darauf verwiesen, daß die Studie davon ausgeht, daß diese Frage im Rahmen des Genehmigungsverfahrens beachtet wird und somit derartige CMA keine dominante Rolle spielen.

3.3.6.2 Verfahrenstechnik

3.3.6.2.1 Allgemeines

Von besonderer Wichtigkeit für die Funktion der verfahrenstechnischen Systeme sind Pumpen und Armaturen mit Stellantrieben. Daher werden im folgenden CMA dieser Komponenten eingehend diskutiert.

Ein CMA ist aufgrund mechanischer Schäden und aufgrund einer Überlastung der Antriebe möglich. Aufgrund mechanischer Schäden ist ein gleichzeitiger Ausfall der Pumpen bei Anforderung und bei gegebenenfalls mehreren Stunden Betriebszeit sehr unwahrscheinlich. Auf CMA von Pumpen im Langzeitbetrieb wird in Abschnitt 3.3.6.2.2 eingegangen. Für die Pumpenantriebe ist zu beachten, ob nach Kühlmittelverluststörfällen oder Transienten Betriebszeiten von mehreren Stunden auftreten und ob ähnliche durchgehende Betriebszeiten während des bestimmungsgemäßen Betriebs vorliegen. Andernfalls sind Ausfälle aufgrund mangelhafter Kühlung denkbar oder aufgrund zu niedrig eingestellter Überstromauslöser (Abschnitt 6.1.2.3.2). Die Betriebszeiten der Pumpen werden bei den jeweiligen Fehlerbäumen in Abschnitt 6.1.2.2 diskutiert.

Ähnlich wie bei Pumpen ist bei Stellantrieben eine Überlastung der Antriebe nicht auszuschließen (Abschnitt 3.3.6.2.3).

CMA von Armaturen aufgrund von falschen Stellungen nach Instandhaltungen sind von untergeordneter Bedeutung. Nach Wartungs- und Instandsetzungsarbeiten erfolgen nämlich Funktionsprüfungen. Die regelmäßigen Funktionsprüfungen werden für unterschiedliche Teilsysteme (Stränge) durch unterschiedliche Schichten des Betriebspersonals durchgeführt (personelle Diversität). Liegen trotzdem Fehlstellungen von Motorarmaturen in Sicherheitssystemen vor, so werden diese bei Anforderung der Systeme durch Kontrollbefehle korrigiert.

3.3.6.2.2 Pumpen

Während aus der Betriebserfahrung keine CMA von Pumpen bei Anforderung bekannt sind, ist für Pumpen im Langzeitbetrieb zumindest ein "common mode"-Ereignis aufgetreten, das allerdings nicht zu einem CMA führte. Aufgrund dieses besonderen Vorkommnisses ist eine Bewertung von entsprechenden CMA möglich.

Im folgenden werden CMA der Nachkühlpumpen im Langzeitbetrieb nach Kühlmittelverluststörfällen quantifiziert. CMA anderer Pumpen in den zur Nachwärmeabfuhr benötigten Systemen spielen demgegenüber eine untergeordnete Rolle. Die Gründe dafür sind:

- Nach den Kühlmittelverluststörfällen "großes Leck" und "mittleres Leck" ist wegen der Aktivitätsfreisetzung in den Sicherheitsbehälter eine LANGZEIT-NOTNACHKÜHLUNG, d.h. eine langfristige Nachwärmeabfuhr über Not- und Nachkühlsystem, nuklearen Zwischenkühlkreis und nukleares Nebenkühlwasser, aufrechtzuerhalten. Im Rahmen der durchgeführten Analysen wird von einem halben Jahr ausgegangen.
- Die Durchführung von provisorischen Maßnahmen bei drohendem oder sogar eingetretenem Ausfall der im Ringraum installierten Pumpen des Not- und Nachkühlsystem oder des nuklearen Zwischenkühlkreises ist, wegen der Aktivität im Sicherheitsbehälter, die erste Zeit nach Störfalleintritt kaum möglich.
- Im nuklearen Zwischenkühlkreis sind nur in jeweils zwei der vier Stränge die Pumpen konstruktionsgleich. In zwei Strängen stehen sogar je zwei Pumpen zur Verfügung, wenn nicht gleichzeitig ein Notstromfall vorliegt.
- Die Pumpen des Not- und Nachkühlsystems, das sind die Nachkühlpumpen, werden durch den Kontakt mit Sumpfwasser kontaminiert. Dadurch sind die Bedingungen für die Instandsetzung erheblich ungünstiger als bei den anderen Pumpen.

CMA von Nachkühlpumpen im Langzeitbetrieb sind aufgrund eines zum Anforderungszeitpunkt noch nicht entdeckten Planungs- oder Herstellungsfehlers möglich. Das Auftreten eines derartigen Fehlers ist an den Nachkühlpumpen der deutschen DWR-Anlage Biblis A

beobachtet worden /F2, 3-39/: Eine von vier vorhandenen Pumpen fiel am 7.5.1976 nach 1480 Stunden Betriebszeit mit Wellenbruch aus, die übrigen Aggregate zeigten bei der daraufhin durchgeführten Untersuchung Schäden an der Welle, die eine sofortige Instandsetzung und konstruktive Änderung veranlaßten. Die Angaben zur Schadensursache und zu den getroffenen Maßnahmen deuten auf vorzeitigen Verschleiß, verursacht durch einen Konstruktionsfehler oder falsche Betriebsweise, hin. Damit kann auf das Vorliegen einer "common mode"-Ursache, nämlich eines systematischen Fehlers geschlossen werden, der eine erhöhte Ausfallwahrscheinlichkeit für das Versagen der Pumpen während des Betriebs zur Folge hat.

Die vier Nachkühlpumpen der Anlage Biblis A hatten zur Zeit der Fehlerentdeckung, nach ca. 20 Monaten Betriebsdauer der Anlage, folgende Betriebszeiten aufzuweisen:

- Aggregat 1: 1480 h (Ausfall)
- Aggregat 2: 2310 h (Instandsetzung veranlaßt)
- Aggregat 3: 2047 h (Instandsetzung veranlaßt)
- Aggregat 4: 1684 h (Instandsetzung veranlaßt)

Für eine pessimistische modellmäßige Darstellung des Ausfallverhaltens der Pumpen wird unterstellt, daß die Aggregate 2 bis 4 unmittelbar nach der Kontrolle, die ihre Schadhaftigkeit zeigte, ebenfalls ausgefallen wären. Dann berechnet sich die mittlere Lebensdauer zu $MTBF_{CMA}$ = 1880 h bei einer Standardabweichung von σ_{CMA} = 370 h. Zur Beschreibung eines so stark um die mittlere Lebensdauer konzentrierten Ausfallverhaltens ist die Normalverteilung gut geeignet. Unter Zugrundelegung dieser Verteilung ergibt sich $\lambda_{CMA}(t)$ für das Betriebsversagen einer Nachkühlpumpe bei Vorliegen eines systematischen Fehlers wie folgt:

$$\lambda_{CMA}(t) = \frac{\exp\left(-\frac{(t-MTBF_{CMA})^2}{2\cdot\sigma^2_{CMA}}\right)}{\int_t^\infty \exp\left(-\frac{(t'-MTBF_{CMA})^2}{2\cdot\sigma^2_{CMA}}\right)dt'} \qquad (3.84)$$

Für die Berechnung der Ausfallwahrscheinlichkeit einer Nachkühlpumpe im Langzeitbetrieb nach einem Kühlmittelverluststörfall sind zwei Teilbeträge zu beachten:

- Für das Betriebsversagen aufgrund von Zufallsausfällen nach Kühlmittelverluststörfällen, bei normalen Umgebungsbedingungen (wie sie im Ringraum der Referenzanlage vorliegen) gibt WASH-1400 in Tab. III, 4-1 den Wert

$$\lambda_{50} = 3 \cdot 10^{-4}/h \qquad K = 10$$

  an. Dieser Wert liegt höher als der Wert der Zufallsausfälle bei normalen Betriebsbedingungen, was die erschwerten Betriebsbedingungen nach einem Kühlmittelverluststörfall (verunreinigtes Fördermedium) berücksichtigt.

- Für das Betriebsversagen infolge CMA ist $\lambda_{CMA}(t)$, wie oben angegeben, zu berücksichtigen.

Die gesamte Ausfallrate für eine Nachkühlpumpe ist dann:

$$\lambda_{ges}(t) = \lambda_{CMA}(t) + \lambda \qquad (3.85)$$

Die zugehörige Ausfallwahrscheinlichkeit findet man in Bild F2, 3-8. Damit ergibt sich eine Zeitabhängigkeit der Ausfallwahrscheinlichkeit für ein in Betrieb befindliches Pumpenaggregat, wie sie in Bild F2, 3-9 dargestellt ist.

Die zur Instandsetzung oder zum Austausch einer ausgefallenen Nachkühlpumpe benötigte Zeit wird mit 2 Wochen abgeschätzt. Unter Berücksichtigung der Ersatzteilbeschaffung und der Montagearbeiten bei ungünstigen radiologischen Bedingungen wird diese Instandsetzungszeit als realistisch angesehen. Als pessimistische Abschätzung für die benötigte Instandsetzungszeit werden alternativ 6 Wochen berücksichtigt.

Es werden zwei unterschiedliche Fahrstrategien für die Nachkühlpumpen untersucht:

- Fahrstrategie A
  Alle zu einem Zeitpunkt verfügbaren Redundanzen sind in Be-

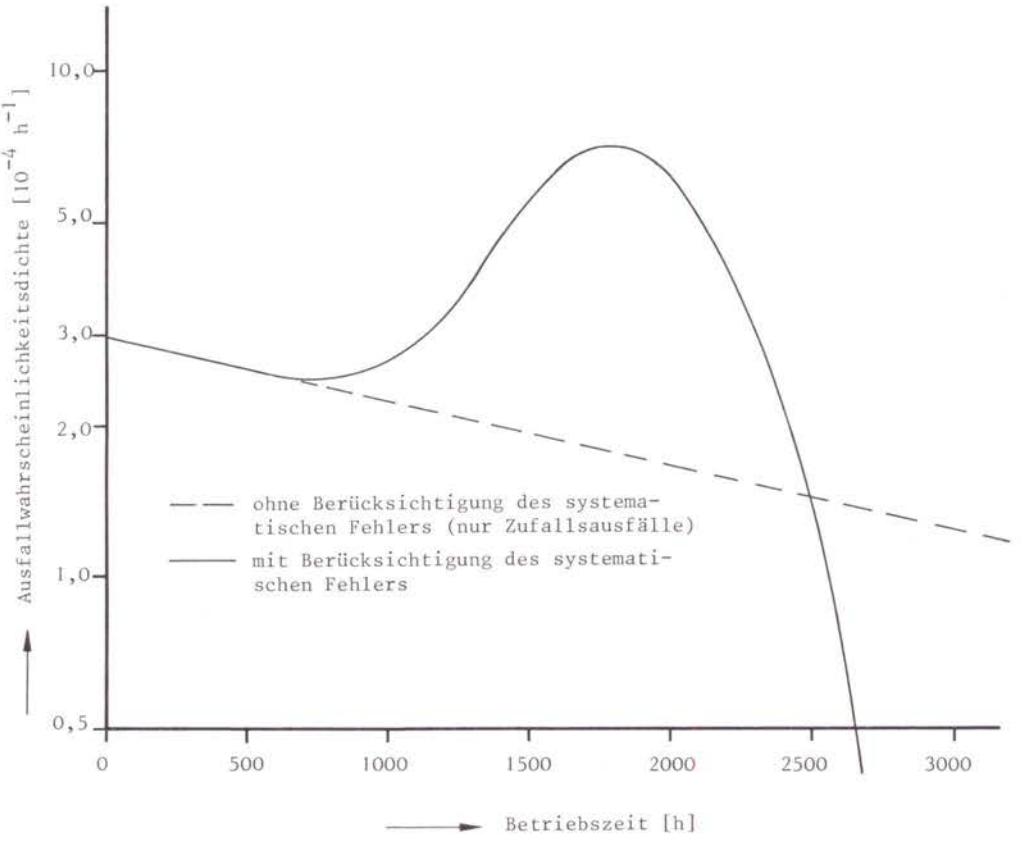


Bild F2, 3-8:

Gesamte Ausfallwahrscheinlichkeitsdichte für das Betriebsversagen einer Nachkühlpumpe (erschwerte Betriebsbedingungen)

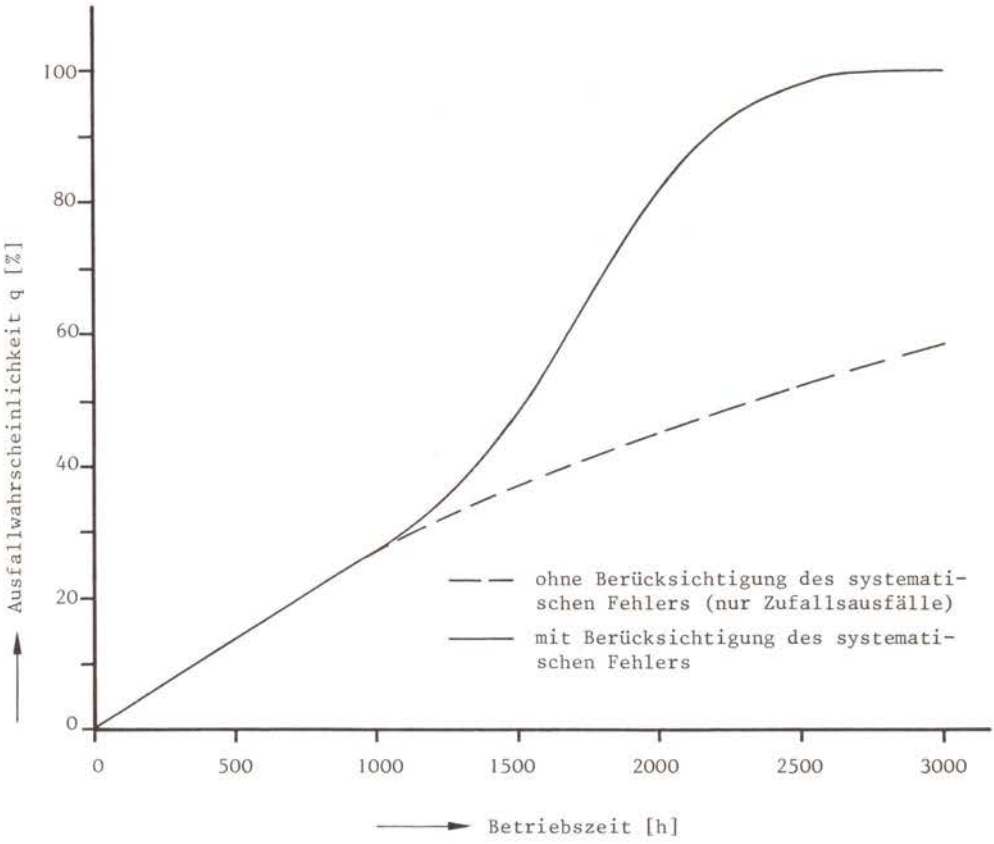


Bild F2, 3-9:

Gesamte Ausfallwahrscheinlichkeit für das Betriebsversagen einer Nachkühlpumpe (erschwerte Betriebsbedingungen)

trieb. Dies ist der bei "großes Leck" und "mittleres Leck" zu erwartende Ablauf, da die anstehenden Reaktorschutzsignale ein Ausschalten der Nachkühlpumpen verhindern.

- Fahrstrategie B
  Bis zum Ausfall der ersten Pumpe bleiben wie oben alle verfügbaren Redundanzen in Betrieb. Unmittelbar nach diesem Ausfall - der das Vorhandensein des systematischen Fehlers offenbart - wird nur die minimal zur Wärmeabfuhr erforderliche Zahl an Redundanzen gefahren, mit Reserve der übrigen. Diese Fahrstrategie stellt die günstigst mögliche dar.

Zur langfristigen Nachwärmeabfuhr nach einem Kühlmittelverluststörfall sind 1v4-Stränge des Not- und Nachkühlsystems erforderlich. Für die Ermittlung der Ausfallwahrscheinlichkeit des 1v4-Systems der Nachkühlpumpen wurde ein Simulationsprogramm eingesetzt.

Bei Strategie A und zwei Wochen Instandhaltungszeit pro Aggregat ergibt sich eine Ausfallwahrscheinlichkeit von $7 \cdot 10^{-3}$ für das System der Nachkühlpumpen und damit für die langfristige Nachwärmeabfuhr, wobei alle Ausfälle in den ersten 14 Wochen der Anforderungszeit liegen (Bild F2, 3-10). Bei Fahrstrategie B verschiebt sich im wesentlichen nur der durchschnittliche Ausfallzeitpunkt zu etwas späteren Zeiten hin, die Ausfallwahrscheinlichkeit ist mit $6{,}6 \cdot 10^{-3}$ nur unwesentlich geringer. Auch hier liegen alle Ausfälle in den ersten 4 Monaten. Bei Strategie A und sechs Wochen Instandsetzungszeit liegt die Ausfallwahrscheinlichkeit bei $9 \cdot 10^{-2}$, bei Strategie B nur noch bei $4{,}7 \cdot 10^{-2}$. Erst bei längerer Instandsetzungszeit ist also Strategie B deutlich besser als Strategie A. Auch in diesen Fällen ergibt sich für die zeitliche Verteilung der Ausfälle das gleiche Bild: Nach ca. 4 Monaten werden keine Systemausfälle mehr beobachtet. Eine Verlängerung der Betriebszeit der LANGZEIT-NOTNACHKÜHLUNG über sechs Monate hinaus ist daher ohne Einfluß auf die Ergebnisse.

Tritt ein Kühlmittelverluststörfall während der ersten drei Anlagenbetriebsjahre ein, so ist die über diese Zeitspanne gemit-

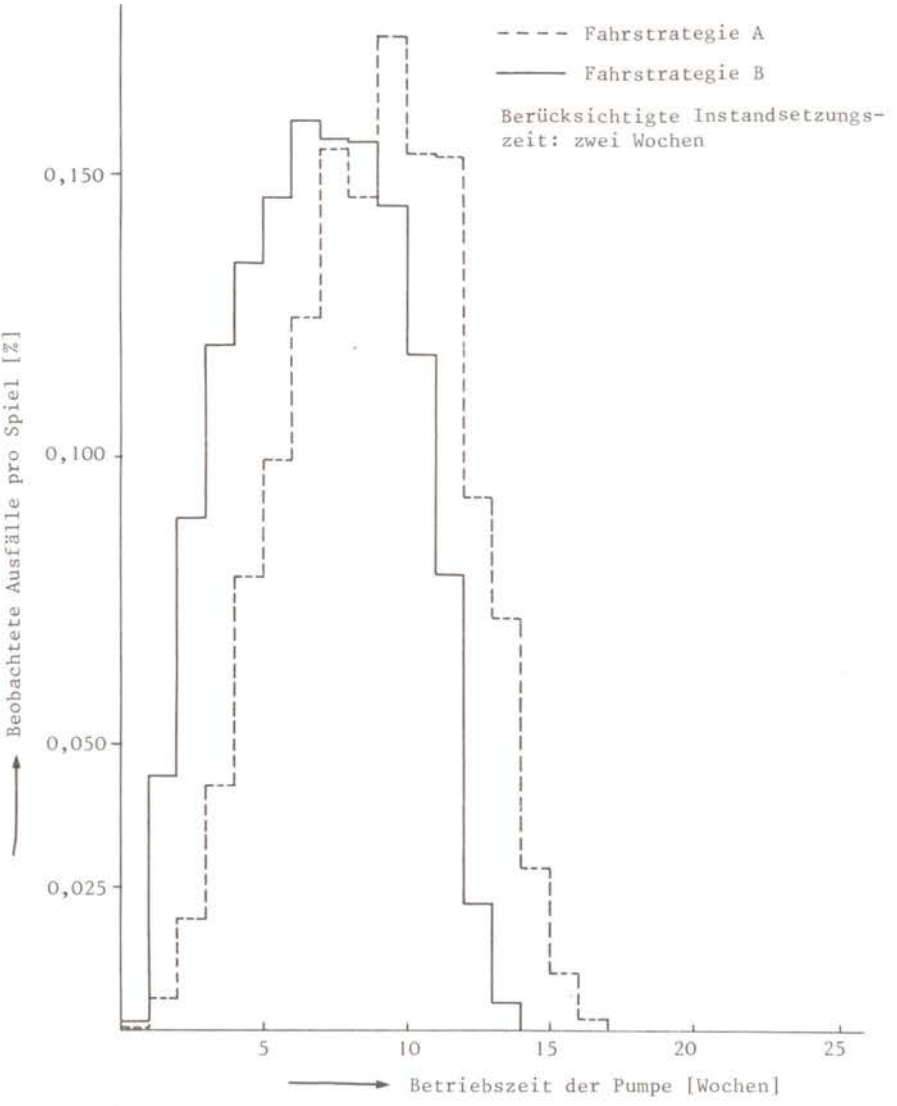


Bild F2, 3-10:

Zeitliche Ausfallverteilung der Nachkühlpumpen nach Anforderung, bei Vorliegen eines systematischen Fehlers

telte Wahrscheinlichkeit für eine Erkennung des systematischen Fehlers vor Eintritt des Störfalls $6 \cdot 10^{-1}$. Bei Eintritt des Kühlmittelverluststörfalls nach mehr als 3 Anlagenbetriebsjahren ist die Wahrscheinlichkeit praktisch gleich 1, daß der vorliegende systematische Fehler erkannt und beseitigt ist. Die beiden Werte wurden durch Simulation ermittelt. Bei einer Anlagenbetriebszeit von insgesamt 40 Jahren ist somit die Wahrscheinlichkeit, daß ein vorliegender systematischer Fehler noch nicht beseitigt ist, etwa 0,1. Die Wahrscheinlichkeit, daß die Nachkühlpumpen eines Kernkraftwerkes einen solchen systematischen Fehler aufweisen, läßt sich aus der deutschen Betriebserfahrung mit 9 Kernkraftwerken zu ebenfalls ca. 0,1 abschätzen. Insgesamt erhält man damit als Ausfallwahrscheinlichkeit für die Nachkühlpumpen bei der LANGZEIT-NOTNACHKÜHLUNG

bei 2 Wochen Instandsetzungszeit:

$$q_{50} = 0{,}1 \cdot 0{,}1 \cdot 7 \cdot 10^{-3} = 7 \cdot 10^{-5}$$

bei 6 Wochen Instandsetzungszeit:

$$q_{50} = 0{,}1 \cdot 0{,}1 \cdot 9 \cdot 10^{-2} = 9 \cdot 10^{-4}$$

Dabei wurde die ungünstigere Fahrweise (Fahrstrategie A) zugrunde gelegt.

Der zuerst angegebene Wert basiert auf einer realistischen Schätzung der Instandsetzungszeit und wird daher als realistische Schätzung für den Median der Ausfallwahrscheinlichkeit angesehen. Aufgrund der sehr pessimistischen Abschätzung der Instandsetzungszeit mit 6 Wochen kann der zuletzt angeführte Wert als oberer Grenzwert für die Ausfallwahrscheinlichkeit interpretiert werden. Damit erhält man

$$q_{50} = 7 \cdot 10^{-5} \qquad K = 13$$

Als Erwartungswert ergibt sich daraus

$$\bar{q} = 2{,}4 \cdot 10^{-4}$$

Diese Ausfallwahrscheinlichkeiten wurden unter den Annahmen ermittelt, daß in der Anlage Biblis A die schadhaften Nachkühlpumpen unmittelbar nach der Inspektion ausgefallen wären und daß die Nachkühlpumpen in der Referenzanlage ähnlich gestaffelte Betriebszeiten haben wie die in Biblis A. Beide Annahmen sind pessimistisch. Dabei ist zu beachten, daß als Folgerung aus dem besonderen Vorkommnis in Biblis A die Betriebszeiten der Nachkühlpumpen noch stärker als vorher gespreizt werden.

3.3.6.2.3 Stellantriebe

Im Gegensatz zu pneumatischen und hydraulischen Antrieben, bei denen Stellkraft und Stellmoment durch den Druck des Betriebsmittels begrenzt sind und in den Endlagen von mechanischen Anschlägen im Stellglied oder Antrieb aufgenommen werden können, muß bei elektrischen Stellantrieben der Motor in der Endlage drehmoment- oder wegabhängig abgeschaltet werden. Dies ist notwendig, weil das Schwungmoment zu unkontrollierbaren Stellkräften führen könnte und der Motor im Stillstand nicht an Spannung liegen darf.

Bei den elektromotorischen Antrieben wird für den drehmoment- oder wegabhängigen Abschaltvorgang heute fast ausschließlich das Verschiebeschneckenprinzip angewandt. Der Antriebsmotor treibt dabei eine Schnecke an, die wiederum über das Schneckenrad und, falls erforderlich, über ein Getriebe auf den Antrieb wirkt. Dabei ist die Schnecke auf ihrer Welle verschiebbar angeordnet und wird durch Federn in der Mittellage gehalten. Wird nun bei laufendem Antrieb die Abtriebsseite gebremst, so wird sich die Schnecke auf dem Schneckenrad weiterdrehen und auf der Schneckenwelle axial verschieben. Dieser Verschiebeweg wird über einen Endschalter erfaßt, dessen Signal die Abschaltung des Antriebsmotors auslöst. Die Schnecke kann sich nur gegen die Kraft der Haltefedern verschieben. Federkonstante und Vorspannung der Federn sind somit ein unmittelbares Maß für das Drehmoment an der Abtriebsseite des Stellantriebs.

Die benötigten Drehmomente für die Betätigung der Armaturen wurden für die Referenzanlage von den Armaturenherstellern ermittelt. Verluste durch Reibung und Druckwiderstände wurden mit einem Sicherheitszuschlag von ca. 20 % berücksichtigt. Die benötigten Drehmomente sind identisch mit den Abschaltmomenten, auf die die Drehmoment-Endschalter eingestellt wurden.

Beim Verfahren von Armaturen, insbesondere beim Öffnen, können jedoch Anfahr-Drehmomente erreicht bzw. benötigt werden, die die eingestellten Abschaltmomente übertreffen und damit den Motor abschalten. Zu hohe Anfahr-Drehmomente werden im allgemeinen durch ein Verklemmen der Ventilkegel oder Schieber in ihren Sitzen hervorgerufen. Um trotzdem ein Auffahren dieser Armaturen sicherzustellen, wird ihr drehmomentabhängiger Endschalter so lange überbrückt, bis ein zusätzlich installierter wegabhängiger Endschalter durch das Auffahren der Armatur von der Stellung ZU auf die Stellung NICHT ZU umgeschaltet wird. Für den weiteren Stellweg ist die drehmomentabhängige Abschaltung wieder wirksam. Eine Überlastung der Antriebsmotoren bei der Drehmomentschalterüberbrückung ist im allgemeinen nicht zu erwarten, da die Motoren meist für wesentlich höhere Leistungen ausgelegt sind.

Falls der Antriebsmotor eines Stellantriebs wesentlich überlastet wird, so spricht der Überstromauslöser in der Schaltanlage an. Die Überstromauslöser für Stellantriebe werden auf 1,5fachen Motornennstrom eingestellt. Näheres hierzu kann Abschnitt 6.1.2.3 entnommen werden.

Eine falsche Einstellung der Abschaltgrenzwerte muß grundsätzlich unterstellt werden. Die Wahrscheinlichkeit, daß bei der Ersteinstellung durch das Lieferwerk ein falscher Abschaltwert eingestellt wird, ist gering im Vergleich zur Wahrscheinlichkeit einer fehlerhaften Berechnung der Abschaltgrenzwerte /F2, 3-40/. Zur Vermeidung derartiger CMA von Stellantrieben werden regelmäßige Funktionsprüfungen der Armaturen durchgeführt. Dabei ist auch darauf zu achten, daß für die Armaturen die Betriebs- und Umgebungsbedingungen vorliegen, die im wesentlichen denen bei Anforderung der Sicherheitssysteme zur Beherrschung eines Kühlmittelverluststörfalls oder einer Transiente entsprechen.

Im Rahmen der Zuverlässigkeitsanalyse wurden daher die wichtigsten bei Kühlmittelverluststörfällen und Transienten zu verfahrenden Armaturen auf die Tauglichkeit ihrer Funktionsprüfung hin untersucht. Es wurde außerdem überprüft, ob Betriebszustände auftreten können, für die die Armaturen nicht ausgelegt sind. Die Beschreibung dazu folgt im Abschnitt 6.1.2.2 bei den jeweiligen Fehlerbäumen.

3.3.6.3 Elektrische Energieversorgung

Im Bereich der elektrischen Energieversorgung ist eine quantitative Aussage aufgrund der Betriebserfahrung derzeit nur für Notstromdiesel möglich. Einzelheiten hierzu können dem Fachband 3 entnommen werden.

Außer CMA der Notstromdiesel könnten CMA der 24-V- und 220-V-Gleichstromversorgung bei Anforderung im Notstromfall (als Störfallfolge oder auslösendes Ereignis) von Einfluß sein: Beide Gleichstromversorgungen werden sowohl für den Start der Notstromdiesel als auch für den Gebäudeabschluß benötigt. Es kann jedoch davon ausgegangen werden, daß die Wahrscheinlichkeit für den CMA der Batterien erheblich niedriger ist als diejenige für den CMA der Notstromdiesel. Unter dieser Annahme beeinflussen vollständige Ausfälle der Gleichstromversorgungen aus folgenden Gründen die Ergebnisse nicht wesentlich:

- Eine Netzrückschaltung ist beim Ausfall aller Notstromdiesel nicht möglich (Abschnitt 6.1.2.3). Dadurch führt im Notstromfall ein CMA der Notstromdiesel zu den gleichen Konsequenzen im Hinblick auf den nicht beherrschten Störfall wie ein CMA von Batterien.
- Der für das Risiko wichtige Gebäudeabschluß der Lüftungsleitungen (Freisetzungskategorie 2) wird auch bei einem CMA der Batterien ausgelöst.

3.3.6.4 L e i t t e c h n i k

3.3.6.4.1 Allgemeines

Die Leittechnik eines Kernkraftwerkes umfaßt alle Meß-, Regel- und Steuereinrichtungen, die Meldeanlagen sowie die Einrichtungen zur Anzeige, Registrierung und Protokollierung von Prozeßgrößen. Das Reaktorschutzsystem ist somit ein Teilsystem der Leittechnik. Wegen der überragenden sicherheitstechnischen Bedeutung des Reaktorschutzsystems wird dieses gesondert in den Abschnitten 3.3.6.4.2 bis 3.3.6.4.4 behandelt.

Für die anderen Geräte, die sogenannte "betriebliche Leittechnik" werden im allgemeinen keine CMA von ähnlichen oder baugleichen Komponenten berücksichtigt (eine Ausnahme bildet aufgrund ihrer besonderen Bedeutung die Kühlmitteldruckregelung). Einerseits sind nämlich viele Geräte der betrieblichen Leittechnik ständig oder zumindest häufig in Betrieb, so daß CMA entdeckt würden. Andererseits werden die sicherheitstechnischen Auswirkungen derartiger CMA durch das Reaktorschutzsystem begrenzt.

Folgeausfälle der betrieblichen Leittechnik aufgrund der im Störfall herrschenden Umgebungsbedingungen sind, soweit sie die Beherrschung des Störfalls ungünstig beeinflussen, in der Fehlerbaumanalyse berücksichtigt.

Funktionelle Abhängigkeiten können ebenfalls zum gleichzeitigen Versagen redundanter Komponenten führen, z.B. aufgrund einer fehlerhaft aufgebauten Steuerung. Diese Abhängigkeiten werden durch die detaillierte Fehlerbaumanalyse richtig erfaßt.

CMA in der Leittechnik sind nur bei Meßfühlern und elektromechanischen Geräten (Relais) aufgetreten. Für die elektronischen Geräte der Leittechnik in Kraftwerken sind solche Ausfälle bisher nicht bekannt und werden daher nicht berücksichtigt.

3.3.6.4.2 Ursachen

- Fehler aufgrund von Planung oder Herstellung

Bei Reaktorschutzsystemen in deutschen Kernkraftwerken sind einige derartige Fehler aufgetreten, die jedoch nur in einem Fall dazu führten, daß gleichzeitig ein Ausfall mehrerer zueinander redundanter Komponenten oder Teilsysteme vorlag. Beispiele für derartige Fehler sind nach /F2, 3-41/ das Verwechseln von bar und bar_{abs} bei der Auslegung, ein ungenügendes Aushärten von Korrosionsschutzlacken an Relais, Verformungen an Mikroschaltergehäusen durch Erwärmung bei Ruhestrombetrieb oder Korrosion von Komponenten (von Federn der Meßbereichsplatten von Bartonzellen).

- Fehler aufgrund des Betriebes

Eine Reihe von "common mode"-Ursachen, die während des Betriebes der Anlage denkbar sind, kann aus der deutschen Betriebserfahrung nachgewiesen werden /F2, 3-39/. In einigen Fällen war zwar nicht das Reaktorschutzsystem, sondern andere leittechnische Systeme davon betroffen, jedoch wären CMA im Reaktorschutzsystem aufgrund der gleichen Ursachen möglich gewesen. So sind z.B. Ausfälle von Neutronenflußmeßkammern aufgrund schlechter Lötanschlüsse oder Ausfälle von Druckmeßkanälen durch Fehlbedienung bei Prüfarbeiten aufgetreten.

3.3.6.4.3 Gegenmaßnahmen

Die KTA-Regel 3501 /F2, 3-30/ fordert in Punkt 4 für Reaktorschutzsysteme, daß diese so auszulegen, auszuführen und zu betreiben sind, daß versagensauslösende Ereignisse sowohl innerhalb des Reaktorschutzsystems als auch außerhalb oder innerhalb der Reaktoranlage die notwendigen Schutzaktionen im Bedarfsfall nicht verhindern. Als versagensauslösendes Ereignis innerhalb des Reaktorschutzsystems sind unter anderem in Betracht zu ziehen:

- systematische Ausfälle, wie mehrere gleichzeitig oder kurzfristig aufeinanderfolgende Ausfälle in den Untersystemen des Reaktorschutzsystems, die eine gemeinsame Ursache im System selbst haben (z.B. durch Fertigungsfehler, Auslegungsfehler, Drift);
- Fehler bei der Bedienung und Wartung des Reaktorschutzsystems durch das Personal.

Um den KTA-Regeln oder Anforderungen im Rahmen des Genehmigungsverfahrens zu genügen, ist in den Reaktorschutzsystemen der deutschen Kernkraftwerke eine Vielzahl von Maßnahmen gegen unabhängige Ausfälle und CMA getroffen worden. Diese Maßnahmen sind ausführlich bereits im Abschnitt 3.3.3 beschrieben. Im folgenden werden sie für das Reaktorschutzsystem diskutiert:

- Erprobte Konstruktion und Standardisierung

Das Reaktorschutzsystem der untersuchten Anlage ist weitgehend aus betriebsbewährten Steuerungssystemen und Komponenten aufgebaut. Allerdings wurden in einigen Einzelfällen Bausteine eingesetzt, über die kaum Erfahrung vorlag. Für diese Bausteine waren im Rahmen des Genehmigungsverfahrens eigene Zuverlässigkeitsnachweise zu führen.

- Redundanz

Die Anwendung des Redundanzprinzips im Reaktorschutzsystem bedeutet, daß die Signalbildung mehrfach entsprechend der Zahl der verfahrenstechnischen Redundanzen erfolgt. Dabei ist die gesamte Kette zur Bildung der Ausgangssignale von der Meßwerterfassung über die Grenzsignalbildung, logische Verknüpfung und Wertung ebenfalls mehrfach (redundant) aufgebaut.

- Diversität

Im Reaktorschutzsystem muß zwischen Gerätediversität und Diversität der Anregekriterien unterschieden werden. Diversität der Anregekriterien ist eine der wichtigsten Maßnahmen gegen CMA im Reaktorschutzsystem. In der KTA-Regel 3501 wird daher gefordert, daß für jeden vom Reaktorschutzsystem zu beherrschenden Störfall mindestens zwei unterschiedliche Anregekriterien (z.B. Temperatur und Druck) herangezogen werden müssen. Die Verwendung solcher unterschiedlichen Prozeßvariablen zur Störfallerfassung schließt zumindest im Bereich der Meßfühler die gerätetechnische Diversität ein. Völlige gerätetechnische Diversität ist aus einer Reihe von Gründen schwer zu realisieren. Im untersuchten Reaktorschutzsystem wurde dieses Prinzip bei den Meßfühlern und den Ausgangsrelais verwirklicht.

- Räumliche Trennung

Das Prinzip der räumlichen Trennung ist bei den Geräteschränken des Analog-, Logik- und Relaisteils verwirklicht. Bei den Meßfühlern und Meßumformern ist dies jedoch aufgrund der Anordnung der verfahrenstechnischen Komponenten nicht immer möglich.

- Einrichtungen zur Fehlererkennung und periodische Funktionsprüfungen

Auch diese Prinzipien werden im untersuchten Reaktorschutzsystem angewandt. So überwachen in der Meßwerterfassung Vergleicher die einzelnen Meßkanäle und Referenzspannungen für die Grenzwertbildung auf Abweichungen von den anderen Kanälen der gleichen Anregekanalgruppe. Dies ist zwar gegen gleichzeitig und gleichsinnig auftretende CMA unwirksam, jedoch ist deren Auftreten ziemlich unwahrscheinlich. Weiterhin wird auch das Ansprechen von Sicherungen in den Betätigungsschränken auf der Warte gemeldet. Derartige selbstmeldende Ausfälle während des bestimmungsgemäßen Betriebes wurden in der Zuverlässigkeitsanalyse vernachlässigt. Als selbstmeldend wird dabei ein Ausfall

bezeichnet, der durch eine Einzel- oder Sammelmeldung gemeldet oder durch die Fehlauslösung einer Aktion sofort entdeckt wird. Die meisten Reaktorschutzsignale werden in der Referenzanlage in vierwöchigem Turnus, redundanzmäßig je eine Woche versetzt, getestet. Die Meßwerterfassung, Grenzsignalbildung und Vergleicherfunktion werden einmal jährlich geprüft. Die Wirksamkeit beider Maßnahmen wurde durch die bisherige Betriebserfahrung bestätigt.

- Ausnutzung der sicheren Ausfallrichtung

Für viele Signale des untersuchten Reaktorschutzsystems ist eine sichere Ausfallrichtung gegeben. Für Teilsysteme des Reaktorschutzsystems, bei denen Ausfälle zu nicht eindeutig sicherheitsgerichteten Aktionen führen, wird ein besonderer Aufwand im Hinblick auf räumliche und redundanzmäßige Trennung getrieben, so ist zum Beispiel der gesicherte Teil des Reaktorschutzsystems in unterschiedlichen Quadranten des Ringraumes untergebracht. Konstruktiv wird eine sichere Ausfallrichtung durch Anwendung des Ruhestromprinzips und der "fail safe"-Technik erreicht.

- Qualitätssicherung während der Planung, Herstellung und Inbetriebnahme

Da es sich beim untersuchten Reaktorschutzsystem um ein betriebsbewährtes System handelt, wurden Eignungsprüfungen nur an solchen Bausteinen (z.B. Langzeitstufen) durchgeführt, die erstmalig zum Einsatz kommen. Die sonstigen Maßnahmen entsprachen dem üblichen Standard des Genehmigungsverfahrens.

- Qualitätssicherung während des Betriebs

Das Prüfhandbuch gewährleistet eine gründliche Überprüfung der Hardware des Reaktorschutzsystems. Die Prüfanweisungen für die Reaktorschutzsignale zeigten unseres Erachtens nicht in allen

Punkten das wünschenswerte Maß an Klarheit, Übersichtlichkeit und leichter Kontrollierbarkeit. Dies wurde bei der Bewertung von Handmaßnahmen entsprechend berücksichtigt.

- Auswertung der Betriebserfahrung

Der Betreiber registriert die Ausfälle im Reaktorschutzsystem und wertet sie selbst aus. Soweit sicherheitstechnisch bedeutsame Vorkommnisse auftreten, werden die Genehmigungsbehörde und gegebenenfalls weitere Stellen (BMI, GRS, RSK) unterrichtet.

3.3.6.4.4 Quantitative Bewertung

Aus der Betriebserfahrung Aussagen über CMA zu gewinnen, ist schwierig. Gründe dafür sind die geringe Wahrscheinlichkeit von CMA und die mangelnde Vollständigkeit der Erfassung der Ausfälle. Die Vollständigkeit der Erfassung ist besonders bei weit zurückliegenden Ereignissen etwas problematisch. Ein zusätzliches Problem besteht in der Vergleichbarkeit der Systeme, da statistische Auswertungen nur dann sinnvoll sind, wenn sie sich auf vergleichbare Komponenten beziehen. So können Betriebserfahrungen mit Druckschaltern nicht auf Differenzdruckmeßumformer übertragen werden. Ferner ist es kaum möglich, die Betriebserfahrung zu "common mode"-Ereignissen in einzelnen Meßkanälen für Aussagen über CMA von Meßkanalgruppen auszuwerten. In der vorliegenden Arbeit wurde für die Steuerebene (speziell Relaisteil) des Reaktorschutzsystems zum Teil auch auf "Weltbetriebserfahrung" /F2, 3-42/ zurückgegriffen, da unseres Erachtens bei Relaissystemen im wesentlichen vergleichbare Relaistypen verwendet werden.

Das Reaktorschutzsystem der Referenzanlage besteht aus den drei Teilsystemen Anregeebene, Logikebene und Steuerebene (Abschnitte 4.4.1.1 und 4.4.1.2):

- In der Anregeebene wird jedes Anregekriterium durch mindestens drei redundante Meßkanäle überwacht, die eine Meßkanalgruppe bilden. Ein Meßkanal besteht aus Fühler und Meßumfor-

mer, Impedanzwandler und Trennverstärker sowie dem Grenzsignalgeber mit angeschlossenem Vergleicher. Zwischen Impedanzwandler und Trennverstärker kann eine Signalverzweigung für andere Grenzsignale vorhanden sein. Sofern aus mehreren Prozeßvariablen in Rechenschaltungen nicht direkt meßbare Anregekriterien ermittelt werden müssen, sind diese Rechenschaltungen nach den Impedanzwandlern eingefügt.

- In der Logikebene werden die Ausgangssignale der Grenzsignalgeber jeder Meßkanalgruppe einer Majoritätsentscheidung (2v3- oder 2v4-Auswahl) unterworfen und zu einer Schaltanregung verarbeitet. Zusätzlich werden, falls erforderlich, die verschiedenen Anregekriterien logisch verknüpft. Majoritätsentscheidung und logische Verknüpfung erfolgen gleichzeitig in drei parallelen Kanälen. Im Logikteil werden dynamische Signale verarbeitet. Der Logikteil wird von Ausgabegeräten abgeschlossen, die aus den dynamischen Signalen eine statische Gleichspannung erzeugen. Aufgrund der dynamischen Arbeitsweise ist dieses Teilsystem besonders zuverlässig. Für dieses Teilsystem sind keine CMA bekannt und nur sehr schwer vorstellbar. Der Ausfall der Logikebene wurde folglich im weiteren nicht berücksichtigt.

- In der Steuerebene werden Relais in Ruhestromschaltung von den Ausgabegeräten des Logikteils mit Spannung versorgt (Relaisteil). Ein Ausbleiben der Gleichspannung am Ausgabegerät führt zum Abfallen der Relais, über deren Kontakte dann statische Ausgangssignale geschaltet werden. Diese Ausgangssignale steuern entweder das 6-Kontaktsystem der Reaktorschnellabschaltung oder die Betätigungsebene anderer Sicherheitseinrichtungen an. In der Betätigungsebene werden diese Signale zur Bildung der "EIN"- und "AUS"-Befehle für die Schaltgeräte der einzelnen Komponenten verwendet. Durch spezielle Baugruppen wird der Vorrang der Reaktorschutzsignale vor allen anderen Signalen sichergestellt. Zeitverzögerte Reaktorschutzsignale werden mittels Zeitstufen gebildet, die in den Schränken des Reaktorschutzsystems untergebracht sind.

- Anregeebene

Bei der Auswertung von Betriebserfahrungen über CMA wurden nur solche Ausfälle berücksichtigt, die den Ausfall einer Meßkanalgruppe verursachen.

Es muß unterschieden werden nach CMA in der Hardware (Meßfühler, Meßumformer, Impedanzwandler etc.) und CMA aufgrund menschlicher Fehlhandlungen (z.B. Fehljustierungen an Grenzsignalgebern). Die Auswertung der deutschen Betriebserfahrung erstreckte sich auf die folgenden Kernkraftwerke mit Leichtwasserreaktoren:

Versuchsatomkraftwerk Kahl	SWR
Kernkraftwerk Lingen	SWR
Kernkraftwerk Gundremmingen	SWR
Kernkraftwerk Würgassen	SWR
Kernkraftwerk Brunsbüttel	SWR
Kernkraftwerk Obrigheim	DWR
Kernkraftwerk Stade	DWR
Kernkraftwerk Biblis, Blöcke A und B	DWR
Gemeinschaftskernkraftwerk Neckarwestheim	DWR

Die Auswertung lieferte keinen Nachweis von CMA in der Hardware der Anregeebene des Reaktorschutzsystems. Jedoch ist sowohl ein CMA einer Meßkanalgruppe aus zwei Meßkanälen der betrieblichen Instrumentierung (14.9.1976, Gundremmingen) als auch ein CMA aufgrund menschlichen Fehlverhaltens im Reaktorschutzsystem (12.12.1975, Gundremmingen) bekannt. Der erste Ausfall trat aufgrund des Hängenbleibens von Bartonzellen auf. Der CMA in der Hardware wäre prinzipiell auch im Reaktorschutzsystem möglich gewesen, ist dort allerdings noch nicht aufgetreten. Die Bewertung entsprechender CMA im Reaktorschutzsystem wird daher aufgrund einer Null-Ausfall-Statistik vorgenommen. Der Ausfall aufgrund menschlichen Fehlverhaltens wurde durch ein fälschlich geschlossenes Erstabsperrventil verursacht. Erstabsperrventile in den Meßleitungen (Wirkdruckleitungen) sind für die redundanten Meßkanäle in einer Meßkanalgruppe zur Druck- bzw. Differenzdruckmessung gemeinsam.

Beide CMA betrafen Differenzdruck-Meßkanäle. Für Druck- bzw. Differenzdruck-Meßkanalgruppen wurden im Reaktorschutzsystem ca. $1 \cdot 10^7$ Betriebsstunden abgeschätzt, die durch eine genauere Überprüfung bestätigt werden konnten. Unter der Voraussetzung, daß das Ausfallverhalten durch eine konstante Ausfallrate beschrieben werden kann, ergeben sich bei m beobachteten Ausfällen mit Hilfe der χ^2-Verteilung (Abschnitt 3.2.6) Erwartungswert, Medianwert und obere Grenze für die Ausfallraten zu

$$\bar{\lambda}_{CMA} = \frac{m+1}{T} = 10^{-7}/h$$

$$\lambda_{CMA\ 95} = \frac{1}{2T} \chi^2_{2m+2;0,95} = 3 \cdot 10^{-7}/h$$

$$\lambda_{CMA\ 50} = \frac{1}{2T} \chi^2_{2m+2;0,5} = 7 \cdot 10^{-8}/h$$

Zur Erleichterung der weiteren Rechnungen wurde die χ^2-Verteilung durch eine logarithmische Normalverteilung mit dem Unsicherheitsfaktor K = 4 approximiert.

Bei einer Funktionsprüfung pro Jahr läßt sich daraus eine mittlere Nichtverfügbarkeit von

$$\bar{m}_{CMA} = 5 \cdot 10^{-4}$$

$$m_{CMA\ 50} = 3{,}1 \cdot 10^{-4}/K = 4$$

angeben. Dieser Wert bezieht sich nur auf CMA in der Hardware der Anregeebene.

Für die anderen im Reaktorschutzsystem vorkommenden Meßarten wurde untersucht, ob dieser Wert ebenfalls als Schätzwert verwendet werden kann.

Bei Temperaturmessungen kann der für die Druck- und Differenzdruckmessungen ermittelte Wert als eher pessimistisch eingeschätzt werden. Eine Auswertung von Betriebserfahrungen war für die in der Referenzanlage eingesetzte spezielle Schaltungsart nicht möglich, da die Betriebszeit zu gering ist. Die bisherige

Erfahrung mit Temperaturmessungen im Reaktorschutzsystem weist jedoch keine gleichzeitigen oder gleichartigen Ausfälle mehrerer Meßkanäle nach.

Die Drehzahlmessungen arbeiten nach einem dynamischen Meßprinzip, d.h., es wird eine Wechselspannung mit drehzahlabhängiger Frequenz erzeugt, die in ein der Drehzahl proportionales Gleichstromsignal umgeformt wird. CMA der Fühler derart, daß trotz Stillstandes des Aggregates eine Drehzahl simuliert wird, sind nicht vorstellbar. Für die Elektronik der Meßumformer dürfte der bei Druck- bzw. Differenzdruckmessungen gefundene Wert für CMA einen eher pessimistischen Schätzwert darstellen, da CMA von elektronischen Bausteinen bisher aus der Kernkraftwerks-Betriebserfahrung nicht nachweisbar sind.

Die Neutronenfluß- und Aktivitätsmessungen haben für die untersuchten Störfälle nur geringe Bedeutung. Diese Messungen unterliegen in ihrer Schaltung und ihrem Aufbau sehr spezifischen Problemen (z.B. Hochspannungsversorgung) und können daher mit den übrigen Messungen nicht verglichen werden. Es wurde in den Analysen pessimistisch davon ausgegangen, daß von diesen Meßstellen keine Anregung von Reaktorschutzsignalen erfolgt.

Mögliche CMA der Spannungsmessungen zur Bildung der Notstromsignale können quantitativ gegen die Wahrscheinlichkeit von CMA der Notstromdiesel vernachlässigt werden. CMA der Spannungsmessungen an den Steuerstabschienen spielen in den untersuchten Störfällen keine Rolle (Kapitel 8) und wurden daher nicht berücksichtigt.

CMA in der Hardware mehrerer gerätetechnisch gleichartiger Meßkanalgruppen (z.B. zur Druckmessung) werden durch einen Faktor von 0,1 berücksichtigt. Dieser Faktor ergibt sich aus der groben Abschätzung, daß 10 % aller Ausfallursachen, die zum CMA einer Meßkanalgruppe führen, auch einen CMA aller übrigen gleichartigen Meßkanalgruppen bewirken.

Für CMA aufgrund menschlicher Fehlhandlungen wird weitgehend die Vorgehensweise von WASH-1400 übernommen (Abschnitt 3.3.5.2). CMA

aufgrund menschlicher Fehlhandlungen können z.B. durch fälschliches Absperren von Wirkdruckleitungen oder Fehljustierungen an Grenzsignalgebern auftreten. Wie bereits erwähnt, liefert die Auswertung der deutschen Kernkraftwerks-Betriebserfahrung einen Ausfall einer Meßkanalgruppe im Reaktorschutzsystem aufgrund des CMA zweier Differenzdruckmeßkanäle /F2, 3-39/.

Für die quantitative Auswertung der deutschen Betriebserfahrung wurde eine Betriebszeit aller Anregekanalgruppen des Reaktorschutzsystems von rund $2 \cdot 10^7$ h abgeschätzt, diese Zeit umfaßt sowohl Anlagen mit Siedewasser- als auch mit Druckwasserreaktoren. Eine inzwischen durchgeführte Ermittlung der Betriebszeit hat diese Annahme als pessimistisch bestätigt, da die tatsächliche Betriebszeit größer ist. Die Prüf- und Justierarbeiten werden einmal jährlich während des Brennelementwechsels vorgenommen. Es wird davon ausgegangen, daß durchgeführte Fehlhandlungen während des darauffolgenden Leistungsbetriebes nicht entdeckt werden, sondern erst bei den Funktionsprüfungen im Rahmen des nächsten Brennelementwechsels.

Unter den genannten Voraussetzungen lassen sich unter Zugrundelegung einer Betaverteilung (Abschnitt 3.2.6) Erwartungswert, Medianwert und obere Grenze für eine konstante Wahrscheinlichkeit von CMA ermitteln (Gleichungen 3.42 und 3.44):

$$\bar{p}_{CMA} = \frac{m+1}{n+1} = 1 \cdot 10^{-3}$$

$$p_{CMA\ 50} = \frac{(m+1)\ F_{50}^{2(m+1),2(n-m)}}{n-m+(m+1)\ F_{50}^{2(m+1),2(n-m)}} = 0{,}8 \cdot 10^{-3}$$

$$p_{CMA\ 95} = \frac{(m+1)\ F_{95}^{2(m+1),2(n-m)}}{n-m+(m+1)\ F_{95}^{2(m+1),2(n-m)}} = 2{,}4 \cdot 10^{-3}$$

$$n = \frac{2 \cdot 10^7}{8760} = 2\ 280 \text{ Anforderungen}$$

Zur Erleichterung der weiteren Rechnung wurde die Betaverteilung durch eine logarithmische Normalverteilung mit dem Unsicherheitsfaktor K = 3 approximiert. Der ermittelte Wert zeigt

eine sehr gute Übereinstimmung zu WASH-1400; dort wird die Fehljustierung einer Meßkanalgruppe mit $p_{50} = 1 \cdot 10^{-3}/K = 3$ bewertet.

Es ist zu beachten, daß bei den Justierarbeiten an unterschiedlichen Meßkanalgruppen meist keine Unabhängigkeit zwischen den einzelnen menschlichen Handlungen angesetzt werden darf (WASH-1400, App. III, Section 6.1). Entsprechend den Abschnitten 3.3.5.2 und 3.4.2.5 werden die Grade der Abhängigkeit der einzelnen Handlungen voneinander durch unterschiedliche "Kopplungsarten" angenähert.

Es wird unterschieden zwischen "keine Kopplung" (no coupling), "mittlere Kopplung" (loose coupling), "starke Kopplung" (tight coupling) und "vollständige Kopplung" (complete coupling). Für die "mittlere Kopplung" wird in Übereinstimmung mit WASH-1400 eine logarithmische Normalverteilung zwischen "keine Kopplung" und "vollständige Kopplung" angesetzt. Für die Ermittlung des Wertes für "starke Kopplung" wird in der vorliegenden Studie der Weg nach /F2, 3-33 und 3-34/ beschritten, d.h., es wird eine logarithmische Normalverteilung zwischen den Werten für "vollständige Kopplung" und "mittlere Kopplung" angesetzt. Dies ist im allgemeinen gegenüber der Vorgehensweise in WASH-1400, in der ein Kopplungsfaktor von 0,1 verwendet wird, pessimistisch (Abschnitt 3.3.5.2).

Die Berechnung der verschiedenen Kopplungswerte ergab:

mittlere Kopplung

$$\bar{p}_{CMA} = 3{,}2 \cdot 10^{-5}$$

$$p_{CMA\ 50} = 2{,}5 \cdot 10^{-5}/K = 3{,}5$$

starke Kopplung

$$\bar{p}_{CMA} = 1{,}8 \cdot 10^{-4}$$

$$p_{CMA\ 50} = 1{,}5 \cdot 10^{-4}/K = 3$$

- Steuerebene

Bei der Auswertung von Betriebserfahrungen zu CMA in der Steuerebene werden nur solche Ausfälle berücksichtigt, die den vollständigen Ausfall der Steuerebene einer Redundanz oder den Ausfall identischer Steuerketten mehrerer Redundanzen verursachen. Die Steuerebene umfaßt die Relais zur Bildung der Reaktorschutzsignale, die Zeitstufen der verzögerten Signale, Vorrangbausteine und die Betätigungsbausteine. Bisher wurde nur ein CMA der Relais festgestellt. Für die angeführten elektronischen Bausteine sind derartige Ausfälle nicht bekannt, sie wurden daher in der "comron mode"-Bewertung nicht berücksichtigt.

Die Steuerebene für die Reaktorschnellabschaltung besteht aus den Auslöserelais, den Auslöseschützen des 6-Kontaktsystems und den Hilfsschützen. Hier wird nur der CMA der Relais und der Schütze des 6-Kontaktsystems diskutiert, entsprechende Ausfälle der Hilfsschütze werden im Rahmen der "common mode"-Bewertung der Stabbetätigung behandelt.

Die bisher vorliegende deutsche Betriebserfahrung führt aufgrund des relativ kleinen Beobachtungszeitraums und bei einem CMA von Relais am Beginn der Beobachtungszeit (29.7.1965, Kahl) zu sehr pessimistischen Werten, d.h., die Wahrscheinlichkeit für CMA der Relais wird zweifellos überschätzt. Für die Zuverlässigkeitsbewertung der Reaktorschnellabschaltung wurde jedoch wegen deren hohen sicherheitstechnischen Bedeutung diese sehr pessimistische Abschätzung übernommen.

Die Schütze des 6-Kontaktsystems sind aus zwei zueinander diversitären Gerätetypen aufgebaut. CMA von Schützen sind bisher aus der deutschen Kernkraftwerks-Betriebserfahrung nicht bekannt, sie wurden daher nicht quantifiziert.

Für die Zuverlässigkeitsbewertung der Auslösung sonstiger Reaktorschutzsignale ist aufgrund des andersartigen Aufbaus des Relaissystems folgendes zu beachten: Die Relais zur Bildung der Auslösesignale sind jeweils innerhalb einer von vier Redundanzen vom gleichen Typ, jedoch sind die Relais zweier Redundanzen

zueinander diversitär. Diese Relais sind zudem in jeder Redundanz noch auf mehrere Schränke verteilt untergebracht, so daß die Möglichkeit einer gleichartigen und gleichzeitigen Beeinflussung ihrer Funktion reduziert ist. Im Gegensatz dazu sind die zwei Auslöserelais der Reaktorschnellabschaltung innerhalb einer Redundanz zueinander diversitär, aber im gleichen Schrank montiert, so daß sie jeweils den gleichen Umgebungsbedingungen unterliegen. Diese beiden untereinander diversitären Auslöserelais der Reaktorschnellabschaltung sind in drei Redundanzen vorhanden und in redundanzmäßig getrennten Schränken aufgebaut.

Aus den genannten Gründen erschien es daher vernünftig, für die Zuverlässigkeitsbewertung des Relaisteils der Reaktorschutzsignale eine etwas abgeänderte Vorgehensweise zu wählen.

Für die Bewertung der Wahrscheinlichkeit eines CMA des Relaisteils zur Reaktorschnellabschaltung (Auslöserelais und Auslöseschütze des 6-Kontaktsystems) wird auf die deutsche Betriebserfahrung zurückgegriffen. Es wurde eine Betriebszeit für Relaisteile zur Reaktorschnellabschaltung von ca. 85 Jahren ermittelt. Bei im Mittel 6 bis 7 Reaktorschnellabschaltungen pro Jahr und monatlichem Test der Auslöserelais ergeben sich etwa 18 Anforderungen pro Jahr. Unter Zugrundelegung einer Betaverteilung und eines Ausfalls lassen sich folgende Werte ermitteln:

$$\bar{p}_{CMA} = 1{,}3 \cdot 10^{-3}$$

$$p_{CMA\ 50} = 1{,}1 \cdot 10^{-3}$$

$$p_{CMA\ 95} = 3{,}1 \cdot 10^{-3}$$

$$n = 85 \cdot 18 = 1\ 530 \text{ Anforderungen}$$

Zur leichteren Weiterrechnung wurde die Betaverteilung durch eine logarithmische Normalverteilung mit dem Unsicherheitsfaktor K = 3 approximiert.

Der beobachtete Ausfall betraf nur einen Relaistyp. CMA der beiden zueinander diversitären Relaistypen der Reaktorschnellabschaltung sind voneinander unabhängig und haben somit eine Wahr-

scheinlichkeit von

$$\bar{p}_{CMA} = 1{,}8 \cdot 10^{-6}$$
$$p_{CMA\ 50} = 1{,}2 \cdot 10^{-6}/K = 4{,}5$$

Wie bereits erwähnt, unterscheidet sich der Aufbau des Relaisteils der Reaktorschutzsignale in einigen Punkten wesentlich von dem für die Reaktorschnellabschaltung. Es wurde angenommen, daß wegen der unterschiedlichen räumlichen Unterbringung und der Aufteilung auf mehrere Schränke nur in ca. 10 % der CMA von Relais einer Redundanz auch die Relais der dazu nicht diversitären Redundanz betroffen sein werden. Aus der oben ermittelten Wahrscheinlichkeit von $1{,}3 \cdot 10^{-3}$ ergibt sich

$$\bar{p}_{CMA} = 1{,}3 \cdot 10^{-4}$$
$$p_{CMA\ 50} = 1{,}1 \cdot 10^{-4}/K = 3$$

Die Weltbetriebserfahrung an etwa vergleichbaren Relaissystemen zur Auslösung der Reaktorschnellabschaltung weist bei einer Betriebszeit der betrachteten Anlagen von ca. 660 Jahren (Stand: Dezember 1977) einen Ausfall (VAK-Kahl) aus /F2, 3-42/. Daraus läßt sich ein Wert von $\bar{p}_{CMA} \cong 1{,}3 \cdot 10^{-4}$ ableiten.

Für den gleichzeitigen Ausfall der diversitären Relaistypen ergibt sich damit ein Erwartungswert von

$$\bar{p}_{CMA} = 1{,}8 \cdot 10^{-8}$$
$$p_{CMA\ 50} = 1{,}2 \cdot 10^{-8}/K = 4{,}5$$

Das Versagen des Relaisteils liefert daher quantitativ keinen Beitrag zur Nichtverfügbarkeit der untersuchten Reaktorschutzsignale.

3.3.6.5 Mechanisches System zur Reaktorschnellabschaltung

3.3.6.5.1 Ursachen

Wegen der sehr hohen Redundanz des mechanischen Systems und der besonders hohen Zuverlässigkeit der Steuerstäbe muß grundsätzlich von einem dominanten Einfluß der CMA auf die Nichtverfügbarkeit ausgegangen werden. Eine qualitative Analyse des mechanischen Systems zeigt allerdings, daß in der Referenzanlage erkennbare Schwachstellen hinsichtlich CMA nicht vorliegen. Außerdem hat die ca. 20jährige Betriebserfahrung mit konstruktiv weitgehend gleichen Steuerstäben keine Planungsfehler an den Steuerstäben aufgezeigt.

Um Herstellungsfehler zu erkennen, werden umfangreiche Funktionsprüfungen vor und während der Inbetriebnahme durchgeführt. Die jährlichen Wiederholungsprüfungen vor und nach dem Brennelementwechsel, die auch Einzelstabfallzeitmessungen enthalten, gewährleisten das Erkennen von Mängeln, die als Langzeiteffekte während des bestimmungsgemäßen Betriebs entstehen oder die beim Aus- und Einbau der Stäbe auftreten können.

Extreme Umgebungsbedingungen für das mechanische System durch erhöhte Staudrücke beim Kühlmittelverluststörfall "doppelendiger Bruch einer Hauptkühlmittelleitung" führen nach einer für das Kernkraftwerk Unterweser durchgeführten Untersuchung bei nur einem Stab zu geringfügigen Staudrucküberschreitungen, so daß für diesen Störfall und alle anderen Kühlmittelverluststörfälle CMA mit 7 oder mehr Stäben (Ausfallkriterium, Abschnitt 8.2) vernachlässigt werden können. Dieses Ergebnis kann auf die Referenzanlage übertragen werden. Ebenso läßt sich das Auftreten von wesentlich erhöhten Temperaturen im Bereich der Stabantriebe mit der Folge von unerwünschten Spaltverengungen wegen der redundanten Anregungen der Reaktorschnellabschaltung über die Kühlmitteltemperatur ausschließen. Merkliche Materialaufdickung im Bereich der Passungen aufgrund von Korrosion wird wegen der verschwindend geringen Korrosionsrate der verwendeten Chromschicht an diesen Teilen ebenfalls als nicht relevant für CMA angesehen.

3.3.6.5.2 Quantitative Bewertung

Aus der Betriebserfahrung mit Steuerstäben, die hinsichtlich des Konstruktionsprinzips (Bauart Westinghouse) denen der Referenzanlage entsprechen, sind CMA bei Anforderung der Reaktorschnellabschaltung nicht bekannt. Dagegen wurde nach /F2, 3-43/ in amerikanischen Kernkraftwerken mit Druckwasserreaktoren ein CMA mit Steuerstäben der Herstellerfirma Combustion Engineering beobachtet: Am 29.8.1972 fielen im amerikanischen Kernkraftwerk Palisades 1 bei einer Reaktorschnellabschaltung 4 Stäbe nicht bis mindestens 96 % ein, wobei es sich jedoch um Steuerstäbe einer veralteten Bauart handelte. Bei der Ermittlung von Ausfallraten wird daher in /F2, 3-43/ dieser CMA nicht berücksichtigt. Folgende Ereignisse aufgrund einer gemeinsamen Ursache, die jedoch nicht zu CMA bei Anforderung der Reaktorschnellabschaltung führten, sind aus der Betriebserfahrung mit Steuerstäben der Bauart Westinghouse in KWU-Druckwasserreaktoren bekannt:

- Kernkraftwerk Stade

Fallzeitverlängerung mehrerer Steuerstäbe am 3.11.1972 bei einer Inspektion (5 1/2 Monate nach Übernahme) und am 13.7.1973 beim 1. Brennelementwechsel.

Bei der Prüfung der Steuerstabantriebe zeigten sich bei einigen Steuerstäben unregelmäßige und gegenüber den ursprünglichen Fallzeiten verlängerte Fallzeiten. Bei den Messungen wurde jeweils nur 1 Steuerstab eingeworfen. Bei Einwurf der gesamten Bank traten auch bei niedrigen Kühlmitteltemperaturen keine wesentlichen Unregelmäßigkeiten auf. Daher wurden diese Ereignisse auch nicht zur Bewertung von CMA bei Anforderung der Reaktorschnellabschaltung herangezogen. Die Fallzeiten bei den Einzelstabmessungen wiesen eine starke Abhängigkeit von der Strömung (Bereich Austrittsstutzen), der Zahl der ausgeführten Schritte und der Temperatur auf. Wesentliche Fallzeitüberschreitungen traten bei einer Kühlmitteltemperatur von 115 °C, bei 100 % Durchsatz und bei Stäben hoher Schrittzahl auf. Durchgeführte Untersuchungen führten zu konstruktiven Änderungen an den Steu-

erstabführungseinsätzen. Nach Auswechseln der Steuerstabführungseinsätze ergaben die Fallzeitmessungen einwandfreie Werte.

- Kernkraftwerk Biblis, Block A

Fehler am Klinkenmechanismus von Steuerstäben mit Stabfehleinfällen am 17.10.1975 während des Leistungsbetriebs und am 28.5.1976 beim 1. Brennelementwechsel.

Neben Fehlern in der Ansteuerung der Stäbe traten ab einer Schalthäufigkeit von ca. 300 000 Schritten Störungen am Klinkenmechanismus auf. Bei 15 untersuchten Antrieben (D-Bänke und 3 willkürlich herausgegriffene Steuerstäbe) wurden 4 gebrochene Hubankerfedern gefunden. Als Ursache wird Ermüdungskorrosion angegeben. Als Unterschied zu anderen Anlagen konnte festgestellt werden, daß

- der Drahtlieferant gewechselt wurde und
- die Federn für Block A einer bestimmten Wärmebehandlungscharge zuzuordnen sind.

Die Federn haben keine sicherheitstechnische Funktion und sind nur zur Einhaltung des Taktes erforderlich.

- Kernkraftwerk Biblis, Block A

Ausfall des Hilfsschützes für die Greifspule eines Steuerstabantriebes am 3.1.1977 bei den neutronenphysikalischen Versuchen.

Beim Fahren der Steuerstäbe bei unterkritischem Reaktor ließ sich der Steuerstab 44 nicht mehr verfahren. Als Ursache stellte sich der Ausfall des Hilfsschützes der Greifspule heraus: Klemmen des Ankers der Spule infolge Schrumpfung des Spulengehäuses wegen Übertemperatur, diese entstand durch fehlerhafte Vorwiderstände. Bei Anforderung der Reaktorschnellabschaltung wäre dieser Stab nicht eingefallen. Vorwiderstände sind jedoch in der Referenzanlage nicht vorhanden.

Die beschriebenen Ereignisse führten in keinem Fall zu einem CMA des mechanischen Systems zur Reaktorschnellabschaltung. Auch sonst sind entsprechende Ausfälle weder aus der Betriebserfahrung in der Bundesrepublik Deutschland noch aus der Weltbetriebserfahrung mit Druckwasserreaktoren bekannt, wenn von dem oben genannten Ausfall im Kernkraftwerk Palisades 1 mit veralteten Steuerstäben abgesehen wird. Für die Bewertung der Zuverlässigkeit des mechanischen Systems zur Reaktorschnellabschaltung mit Hilfe der Null-Ausfall-Statistik ist die vorliegende Weltbetriebserfahrung allerdings nicht ausreichend. Mit nur ca. 10^6 Reaktorstunden /F2, 3-43/ (nur Druckwasserreaktoren, nicht gezählt solche mit veralteten Steuerstäben) und null Ausfällen des mechanischen Systems erhält man eine CMA-Rate von $\bar{\lambda}_{CMA} = 10^{-6}/h$, die um den Faktor 5 höher liegt als die Ausfallrate für den einzelnen Steuerstab, ermittelt aus Betriebserfahrungen mit Steuerstäben in KWU-Druckwasserreaktoren ($\bar{\lambda} = 2 \cdot 10^{-7}/h$, Fachband 3).

Es müßte bei Anwendung der Null-Ausfall-Statistik unterstellt werden, daß bei Auftreten von CMA mit der genannten Ausfallrate $\bar{\lambda}_{CMA} = 10^{-6}/h$ jeweils entweder 7 bestimmte oder mindestens 8 beliebige Steuerstäbe gleichzeitig betroffen sind (Ausfallkriterien, Abschnitt 8.2). Insgesamt wird daher die Bewertung der CMA des mechanischen Systems zur Reaktorschnellabschaltung mit Hilfe der Null-Ausfall-Statistik bei der vorliegenden Betriebserfahrung für ungeeignet gehalten. Statt dessen wird versucht, eine erste Abschätzung mit Hilfe verschiedener Modelle bzw. Annahmen durchzuführen.

Wird angenommen, daß sich, bezogen auf den einzelnen Steuerstab, ein Verhältnis f der Ausfallraten für CMA und für unabhängige Ausfälle angeben läßt und daß bei Vorliegen eines CMA jeweils alle Komponenten betroffen sind (vollständige Kopplung, Abschnitt 3.3.5.2), so ergibt sich die Ausfallrate für CMA des mechanischen Systems zur Reaktorschnellabschaltung aus:

$$\bar{\lambda}_{CMA} = \bar{\lambda} \cdot f \qquad (3.86)$$

Für den Faktor f wird der Wert 10^{-2} abgeschätzt, wobei entsprechende Angaben aus WASH-1400 verwendet werden. Dort wird zur

Ermittlung der CMA-Wahrscheinlichkeit von Steuerstäben ein Wert aus der Betriebserfahrung verwendet. Danach sind bei etwa 10 % aller Ausfälle die Funktionen mehrerer Komponenten eingeschränkt, bei 10 % davon sind mehrere Komponenten gleichzeitig ausgefallen. In WASH-1400 werden diese Erfahrungswerte zur Ermittlung einer oberen Grenze der Wahrscheinlichkeit dafür, daß 3 bestimmte Steuerstäbe durch einen CMA gleichzeitig ausfallen, verwendet. Diese obere Grenze ergibt sich aus dem Produkt der Ausfallwahrscheinlichkeit des einzelnen Steuerstabes mit dem Faktor 10^{-2} (starke Kopplung, Abschnitt 3.3.5.2).

Mit dem in der vorliegenden Studie ermittelten Wert der Ausfallrate für den einzelnen Steuerstab einschließlich Hilfsschütze (Fachband 3) erhält man unter der pessimistischen Annahme, daß alle Steuerstäbe gleichzeitig ausfallen:

$$\bar{\lambda}_{CMA} = \bar{\lambda} \cdot 10^{-2} = 2 \cdot 10^{-9}/h$$

mit

$\bar{\lambda}$ ≙ Ausfallrate des einzelnen Steuerstabes einschließlich Hilfsschütze (Abschnitt 8.2)

$= 2 \cdot 10^{-7}/h$

Unter Zugrundelegung einer mittleren Zeitdauer zwischen zwei Reaktorschnellabschaltungen von $\bar{t} = 1{,}3 \cdot 10^{3}$ h (Abschnitt 8.2) führt dies zu einer Nichtverfügbarkeit des mechanischen Systems zur Reaktorschnellabschaltung aufgrund von CMA von

$$\bar{u}(\bar{t}) = 2 \cdot 10^{-9} \cdot 1{,}3 \cdot 10^{3} \cong 3 \cdot 10^{-6}$$

Die Vorgehensweise entspricht der Beta-Faktor-Methode (Abschnitt 3.3.5.4), wobei jedoch entsprechend den Angaben in WASH-1400 ein zusätzlicher Faktor 10 verwendet wird, der das Verhältnis von "common mode"-Ereignissen zu CMA angibt.

Der ermittelte Wert kann nur als eine erste Abschätzung angesehen werden, da sowohl für die Anwendung dieser Methode als auch für den Wert des β-Faktors die Betriebserfahrung mit Steuerstäben keine ausreichende Begründung liefert. So sind weder CMA

des mechanischen Systems mit gleichzeitigem Ausfall aller Komponenten beobachtet worden, noch liegen der Ermittlung des Beta-Faktors Ausfälle von Steuerstäben zugrunde.

Zwei weitere Möglichkeiten zur Berechnung der CMA-Wahrscheinlichkeit des mechanischen Systems zur Reaktorschnellabschaltung werden in /F2, 3-44/ angegeben. Sie bestätigen recht gut den oben ermittelten Wert von $3 \cdot 10^{-6}$.

Eine der alternativen Berechnungen geht davon aus, daß bei Vorliegen eines Steuerstabausfalles ein zweiter benachbarter Steuerstab mit der Wahrscheinlichkeit 10^{-2} gleichzeitig ausfällt. Der Wert deckt sich mit der 1-%-Angabe in WASH-1400, wenn bei den 1 % beobachteten CMA vorwiegend zwei Komponenten ausgefallen waren. Weiterhin wird unterstellt, daß bei Vorliegen eines Ausfalls von gleichzeitig zwei Steuerstäben ein dritter benachbarter Steuerstab mit der Wahrscheinlichkeit 10^{-2} ausfällt. Bei Verwendung dieser Werte und der zusätzlichen pessimistischen Annahme, daß bei Vorliegen eines Ausfalls von gleichzeitig drei Steuerstäben mindestens 5 weitere Steuerstäbe mit der Wahrscheinlichkeit 1 ausfallen, ergibt sich für die Referenzanlage die Nichtverfügbarkeit des mechanischen Systems zur Reaktorschnellabschaltung zu $\bar{u}(\bar{t}) = 2 \cdot 10^{-6}$.

Die andere alternative Berechnung in /F2, 3-44/ geht von folgender Interpretation der 1-%-Angabe aus: In 1 % der Betriebszeit liegen Umgebungsbedingungen vor, die bei Ausfall eines Steuerstabes sehr wahrscheinlich auch zum Ausfall aller anderen Steuerstäbe führen (Abschnitt 3.3.5.3). Mit dieser Annahme erhält man für die Nichtverfügbarkeit des mechanischen Systems zur Reaktorschnellabschaltung $\bar{u}(\bar{t}) = 3 \cdot 10^{-6}$.

In WASH-1400 wird zur Ermittlung der Wahrscheinlichkeit von CMA des mechanischen Systems zur Reaktorschnellabschaltung das "square-root-bounding"-Modell verwendet ("mittlere Kopplung" in Abschnitt 3.3.5.2). Da sich mit den Ausfallkriterien der Referenzanlage eine Mittelung zwischen den oberen und unteren Grenzwerten über mindestens 25 Zehnerpotenzen ergäbe, wird dieses Modell hier nicht verwendet.

Die Anwendung eines differenzierten Verfahrens, wie es von Vesely entwickelt wurde (Abschnitt 3.3.5.5), ist bei der vorliegenden Betriebserfahrung mit vergleichbaren Steuerstäben - nämlich 0 beobachte CMA - fragwürdig. Die nach dem spezialisierten Marshall-Olkin-Modell ermittelten Werte der Nichtverfügbarkeit liegen etwa um den Faktor 50 höher als der ermittelte Wert von $3 \cdot 10^{-6}$, wenn die amerikanische Betriebserfahrung mit Berücksichtigtung des CMA im Kernkraftwerk Palisades 1 zugrunde gelegt wird. Bei einem CMA mit vier ausgefallenen von insgesamt 45 Steuerstäben ergibt sich für die Parameter p und $\bar{\lambda}_{CMA}$:

$$p \cong 0{,}08$$

$$\bar{\lambda}_{CMA} \cong 1 \cdot 10^{-6}$$

Dies ergibt mit $\bar{t} = 1{,}3 \cdot 10^{3}$ h für die Nichtverfügbarkeit des mechanischen Systems bei Anforderung den Wert $1{,}5 \cdot 10^{-4}$. Dieser Wert, dem die Ausfallkriterien der Referenzanlage zugrunde liegen (Abschnitt 8.2), ist nur um den Faktor 2 kleiner als der Wert, der für die Ausfallwahrscheinlichkeit des Einzelstabes ermittelt wurde. Dies entspricht einem ß-Faktor von 0,5, der als sehr pessimistisch zu beurteilen ist.

3.4 Menschliches Fehlverhalten

3.4.1 Allgemeines

Menschliche Eingriffe sind während des bestimmungsgemäßen Betriebes eines Kernkraftwerkes bei betrieblichen Schalthandlungen (Normalbetrieb), zur Eingrenzung kleiner Störungen (anomaler Betrieb) sowie bei Instandhaltung (Wartung, Instandsetzung, Inspektion) durchzuführen. Weiterhin sind menschliche Handlungen auch bei Störfällen notwendig. Es ist jedoch ein Auslegungsprinzip der Sicherheitseinrichtungen in deutschen Kernkraftwerken, daß Schutzaktionen im allgemeinen automatisch, d.h. ohne Eingriff der Betriebsmannschaft durchgeführt werden. In Ausnahmefällen sind Handeingriffe nötig, für die jedoch eine Zeit von mindestens 30 Minuten ab Störfalleintritt zur Verfügung stehen

muß. In die Kraftwerkswarte werden bei einem Störfall Informationen über den Zustand der Anlage und die Folge der ablaufenden Schutzmaßnahmen übermittelt, die es dem Wartenpersonal ermöglichen, den Zustand der Anlage und den Ereignisablauf zu überwachen, ohne selbst handeln zu müssen.

Menschliche Eingriffe wären unmittelbar nach Störfalleintritt nur erforderlich, falls automatisch gesteuerte Systeme nicht in gewünschter Weise arbeiten würden. Wie bereits vorher erwähnt, müssen je nach Störfall erste Schalthandlungen 30 Minuten nach Störfalleintritt erfolgt sein. Für viele Handeingriffe steht jedoch erheblich mehr Zeit zur Verfügung.

In den Zuverlässigkeitsanalysen sind diese menschlichen Eingriffe zu bewerten. Da menschliche Handlungen kaum in ein starres Schema gepreßt werden können, muß man sich hier mit Abschätzungen behelfen. Eine solche pauschale Bewertung reicht jedoch in vielen Fällen aus, da man sich bemüht, den Einfluß menschlichen Fehlverhaltens durch Auslegung und Betriebsweise gering zu halten. Soweit möglich, wird bei der Ermittlung der Wahrscheinlichkeiten für menschliche Fehlhandlungen wie in WASH-1400 vorgegangen, unter Verwendung der im zugehörigen App. III zusammengestellten Datenbasis. Für einige spezielle Probleme wird außerdem eine Methode verwendet, die in /F2, 3-36/ beschrieben ist.

In der vorliegenden Studie werden in Übereinstimmung mit WASH-1400 nur geplante Handeingriffe bewertet. Darunter werden Handlungen verstanden, die entweder gemäß schriftlicher Anweisungen (Betriebshandbuch) durchgeführt oder während des bestimmungsgemäßen Betriebes geübt werden (z.B. Rücksetzen des $\Delta p/\Delta t$-Signals YZ60), sowie Handlungen, auf die eine eindeutige Gefahrmeldung (z.B. Notgefahrmeldung) hinweist. Als ungeplant werden Handlungen angesehen, wenn die Notwendigkeit der Durchführung auch bei Vorhandensein solcher Meldungen nur durch Überlegung erkannt werden kann.

Es wird vorausgesetzt, daß ungeplante Handeingriffe nicht vorgenommen werden. Ungeplante Handeingriffe, die sich sowohl in ne-

gativer wie in positiver Richtung auswirken können, werden daher nicht quantifiziert.

In den folgenden Abschnitten werden die in der vorliegenden Studie angewandten Methoden zur Bewertung menschlicher Fehlhandlungen erläutert. Die wesentlichen Charakteristika der deutschen Wartentechnik sowie organisatorische und administrative Aspekte der Referenzanlage werden dargestellt, soweit diese Einfluß auf die Bewertung menschlicher Fehlhandlung haben.

3.4.2 Einflüsse auf die Zuverlässigkeit menschlicher Handlungen

Bei der Bewertung menschlicher Zuverlässigkeit ist zu unterscheiden zwischen Fehlern, die durch Einflüsse verursacht werden, die in der Person des Operators liegen (human caused errors), und solchen, die von der Arbeitssituation bedingt sind (situation caused errors). Der weitaus größere Teil menschlicher Fehlhandlungen wird dabei von den zuletzt genannten Faktoren beeinflußt. In WASH-1400 wurde versucht, die wichtigsten Einflußgrößen auf die Zuverlässigkeit menschlicher Handlungen zu berücksichtigen. In der vorliegenden Studie wird die gleiche Vorgehensweise verwendet.

Außerdem wurde in WASH-1400 ein Korrekturfaktor, der sogenannte Fehlerentdeckungsfaktor (recovery factor) berücksichtigt, wenn der Informationsfluß so gestaltet ist, daß nach einem fehlerhaften Eingriff des Operators entsprechende Rückmeldungen (Anzeigen, Meldungen) auf diesen Irrtum hinweisen, oder wenn eine personelle Redundanz bei der Entscheidung und Durchführung der Maßnahme vorhanden war. In der vorliegenden Studie wird auch hier wie in WASH-1400 verfahren.

3.4.2.1 P s y c h i s c h e r S t r e ß

Wie in WASH-1400 und in /F2, 3-34/ ausführlicher dargestellt, ergibt sich qualitativ folgender Zusammenhang zwischen der Höhe

der psychischen Belastung und der Zuverlässigkeit menschlicher Handlungen:

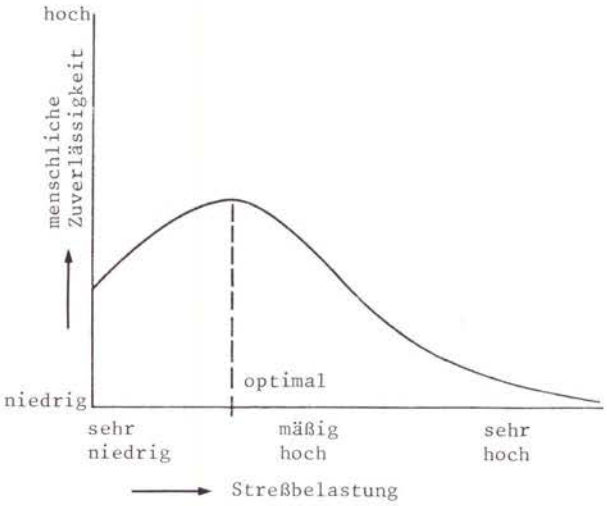


Bild F2, 3-11:

Zusammenhang zwischen psychischem Streß und menschlicher Zuverlässigkeit

Wie aus der Kurve zu ersehen ist, wird eine optimale Zuverlässigkeit bei einer mäßigen Streßbelastung erreicht, die aber doch so hoch ist, daß die Aufmerksamkeit des Operators voll in Anspruch genommen wird. Niedrigere Streßbelastungen verschlechtern die Zuverlässigkeit, da uninteressante und wenig fordernde Aufgaben ein Nachlassen der Aufmerksamkeit zur Folge haben. Zu hohe Streßbelastungen verschlechtern ebenfalls die Zuverlässigkeit. Dies kann zu einem Übersehen von Erfordernissen bis hin zu völliger Konfusion der Bedienungsmannschaft führen. Gründe hierfür können in zunehmender Unruhe oder Unsicherheit des Personals liegen.

Eine sehr niedrige Streßbelastung liegt z.B. bei routinemäßigen Kontrollgängen vor. Dem können Fehlerwahrscheinlichkeiten von 0,5 oder höher zugeordnet werden (Tabelle F2, 3-1). Für spezielle Überwachungsaufgaben liegt die Fehlerwahrscheinlichkeit bei 0,1.

Bezüglich der Streßbelastung optimale menschliche Zuverlässigkeiten werden den Routinetätigkeiten in der Warte während des bestimmungsgemäßen Betriebes der Anlage sowie den Arbeiten bei Wartung, Instandsetzung und Funktionsprüfungen zugeordnet. Dabei wird davon ausgegangen, daß bei diesen Tätigkeiten eine mäßige Streßbelastung zu erwarten ist, die ausreichend hoch ist, um eine zuverlässige Durchführung der Arbeiten zu begünstigen.

Ein sehr hoher Streß und damit hohe Wahrscheinlichkeiten für menschliche Fehlhandlungen liegen z.B. kurz nach einem Kühlmittelverluststörfall vor. Es wird eine Fehlerwahrscheinlichkeit von 1 unmittelbar nach einem Kühlmittelverluststörfall ("großes Leck") verwendet. Für 5 Minuten nach Störfalleintritt wird diese Wahrscheinlichkeit zu 0,9 abgeschätzt, nach 30 Minuten zu 0,1 und nach mehreren Stunden zu 0,01 (Tabelle F2, 3-2). Dabei wird unterstellt, daß die Anlage durch geeignete automatische und menschliche Eingriffe während des Störfallablaufs unter Kontrolle gebracht wird, d.h., daß sich die Anlagensituation mit zunehmender Zeit bessert und damit die Streßbelastung langsam abklingt.

In WASH-1400 wird eine Besonderheit bezüglich der Streßbelastung beschrieben. Wenn ein Operator eine Maßnahme innerhalb einer sehr beschränkten Zeitspanne durchzuführen hat und diese Maßnahme falsch ausführt bzw. sich nicht der gewünschte Effekt einstellt, wird eine doppelt so hohe Fehlerwahrscheinlichkeit für die darauffolgende Handlung des Operators angesetzt usw. Bei mehreren nacheinander durchgeführten Versuchen wird auf diese Weise schließlich eine Fehlerwahrscheinlichkeit von 1 erreicht. Die entsprechende Person ist dann zu keiner richtigen Handlung mehr fähig.

Durch verfügbare personelle Redundanz, d.h. durch Überprüfung der von einem Operator durchgeführten Aufgabe durch eine andere Person, können nicht beliebig niedrige Fehlerwahrscheinlichkeiten erreicht werden. Wahrscheinlichkeiten unter 10^{-5} sind nur für sehr einfache menschliche Tätigkeiten erzielbar und werden folglich für komplizierte Handlungsabläufe nicht verwendet.

3.4.2.2 Ergonomische Gestaltung der Warte

Erhöhte menschliche Fehlerwahrscheinlichkeiten sind in solchen Fällen anzuwenden, in denen die Anordnung, Kennzeichnung oder das Design der zu bedienenden Steuerungseinrichtungen bzw. der abzulesenden Melde- und Anzeigeeinrichtungen einen Irrtum begünstigen. Zu unterstellen sind solche Einflüsse, wenn zum Beispiel Stereotypen verletzt werden, die Kennzeichnung leicht verwechselt werden kann oder Anzeigen oder Meldungen schlecht ablesbar bzw. ungeeignet sind.

Unter Stereotyp wird hier die zu erwartende Reaktion eines Menschen auf einen äußeren Reiz verstanden. So ist zum Beispiel ein grünes Licht (wie bei einer Verkehrsampel) mit der Erwartung von Sicherheit, Gefahrlosigkeit usw. verbunden. Bei Elektrogeräten wird bei Drehung des Reglerknopfes nach rechts ein "mehr", "stärker", "lauter" erwartet (Bewegungsstereotyp). Bei Gruppierungen von Anzeigenelementen und Betätigungseinrichtungen wird erwartet, daß Elemente gleicher relativer Lage zusammengehören (Lagestereotyp), so z.B. Anzeigen in der Mitte der Gruppierung zu Betätigungen in der Mitte der Gruppierung. Diesen Erwartungen muß bei der ergonomischen Gestaltung einer Warte Rechnung getragen werden /F2, 3-45/. Grundsätzlich läßt sich zwar auch die Bedienung einer andersartigen Anordnung trainieren, jedoch ist immer damit zu rechnen, daß unter hohem Streß die natürlichen Verhaltensweisen dominieren.

Nach WASH-1400 sind hohe Irrtumswahrscheinlichkeiten vor allem für ähnliche Betätigungs- und Anzeigefelder anzusetzen, die ohne Kennzeichnung durch Fließschemata nahe beieinander liegen. In der Warte der Referenzanlage der vorliegenden Studie sind jedoch durchweg übersichtliche Fließschemata vorhanden. Aus diesen ist die Bedeutung der einzelnen Komponenten der Anlage gut zu erkennen, aufgrund der Bezeichnung sind die einzelnen redundanten Stränge im allgemeinen leicht zu unterscheiden. Es muß folglich davon ausgegangen werden, daß die Wahrscheinlichkeiten für die Verwechslung von Komponenten sehr gering sind und keinen Einfluß auf die Störfallbeherrschung haben.

Im weiteren werden einige Aspekte der Gestaltung der Warte der Referenzanlage näher erläutert. Bild F2, 3-12 gibt einen Überblick über die Anordnung der wichtigsten Einrichtungen in der Warte der Referenzanlage.

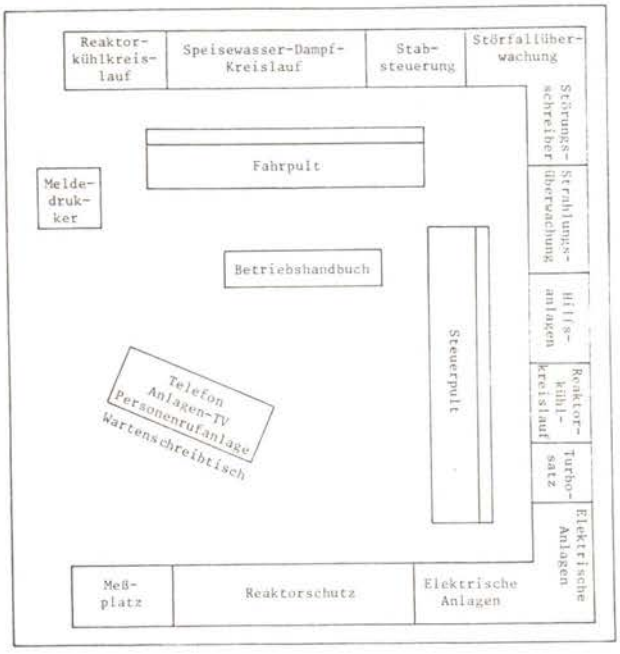
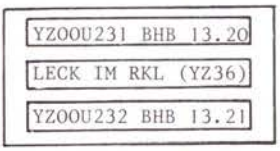


Bild F2, 3-12:
Anordnung der wichtigsten Einrichtungen in der Kraftwerkswarte der Referenzanlage

Die wesentlichsten Einrichtungen sind das Fahrpult (Hauptleitstand), das Steuerpult (Nebenleitstand) sowie die Wandtafel. Das Fahrpult enthält die für den Normalbetrieb der Anlage nötigen Steuerungs-, Melde- und Anzeigeeinrichtungen sowie die Meldeeinrichtung der Gefahrmeldeanlage. Das Steuerpult enthält Steuerungs-, Melde- und Anzeigeeinrichtungen, die vor allem beim An- und Abfahren der Anlage sowie bei Störungen in Teilsystemen benötigt werden. Die Wandtafel enthält im wesentlichen die Anzeiger und Schreiber für die wichtigen Betriebsparameter sowie für Störfälle, ferner für die Strahlungsüberwachung. Weiterhin sind die Anzeigen und Rückmeldungen der Stabsteuerung sowie die

Reaktorschutztafel dort untergebracht. Die elektrischen Anlagen werden ebenfalls von dieser Wandtafel aus gesteuert und überwacht. In der Nähe des Schichtleiter-Büros, das unmittelbar an den eigentlichen Wartenraum angrenzt, steht der Wartenschreibtisch mit Kommunikationseinrichtungen und den Bedienungselementen für die Anlagen-Fernseheinrichtung. Fahrpult und Steuerpult sind in der sogenannten Kompaktwartentechnik ausgeführt.

Das Rastermaß der dort eingesetzten Tischfelder und Anzeigen beträgt im allgemeinen 48 x 24 mm oder 48 x 48 mm. In die Wandtafel sind die Anzeige- und Schreibgeräte eingesetzt, die im allgemeinen eine Größe von 288 x 288 mm oder 144 x 144 mm besitzen. Einige schematische Darstellungen von Tischfeldern (Bild F2, 3-13 bis -15) sollen die wesentlichen Gestaltungsmerkmale des Fahr- und Steuerpultes aufzeigen.



Meldeschlitze

Bei anstehender Meldung leuchtet der entsprechende Meldeschlitz mit Blinklicht auf. Auf das Fenster des Meldeschlitzes ist das Anlagenkennzeichen oder der Meldetext aufgedruckt.

Bild F2, 3-13:
Gefahrmeldetischfeld

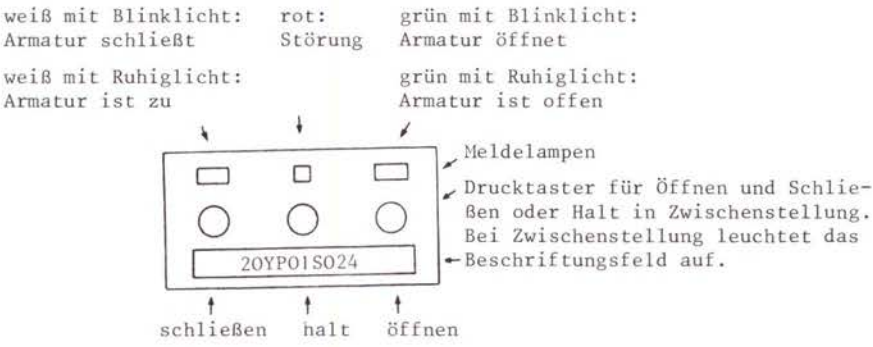


Bild F2, 3-14:
Betätigungstischfeld

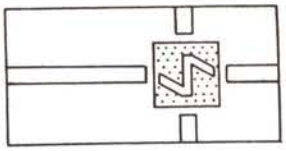


Bild F2, 3-15:
Tischfeld mit Fließbild
(Beispiel für einen Wärmetauscher)

In der Konzeption der Warte für die Referenzanlage sind wesentliche ergonomische Gesichtspunkte berücksichtigt, wenn auch einige Schwachstellen zu erkennen sind.

Ungünstig erscheint die Anzeige einiger wichtiger Meßgrößen, die von den Betätigungstischfeldern am Fahrpult aus beeinflußt werden (z.B. Betätigung der Regelventile für die Frischdampfabgabe), aber nicht vom Fahrpult aus abzulesen sind oder auf ungeeigneten Instrumenten aufgezeichnet werden (z.B. 12fach-Punktdrucker für die Frischdampftemperatur).

An einigen Stellen sind die Betätigungstischfelder so nahe beieinander angeordnet, daß eine rasche Orientierung erschwert ist. Die Stellung einiger sicherheitstechnisch wichtiger Rückschlagarmaturen wird in ungünstiger Weise nur über Stellungsmeldelampen im Tischfeld angezeigt, ohne besondere Warnung bei Fehlstellung.

Generell können die hohe Pultbelegungsdichte und die große Informationsfülle die Zuverlässigkeit des Bedienungspersonals besonders bei Störungen beeinträchtigen, da sie eine rasche Orientierung erschweren und höhere Wahrscheinlichkeiten für das Übersehen von Meldungen bedingen. Für die Phase B der Risikostudie ist eine vertiefte Untersuchung der Wartengestaltung der Referenzanlage vorgesehen.

3.4.2.3 Aufgabenstellung und Ausbildung des Schichtpersonals

In WASH-1400 wurden der Ausbildungsstand und die Erfahrung des in der Kraftwerkswarte anwesenden Schichtpersonals als auffallend gut bewertet, soweit es sich um Kenntnisse über den bestimmungsgemäßen Betrieb der Anlage handelt. Dementsprechend konnten hohe menschliche Zuverlässigkeiten für dieses Wartenpersonal angesetzt werden.

Die Ausbildung des Wartenpersonals schließt ein Simulatortraining ein. Da jedoch ein solch simulatives Störfalltraining in der jeweiligen Anlage kaum durchführbar ist und die Diskussion mit dem Wartenpersonal gewisse Unsicherheiten über die richtige Reaktion auf Störfallsituationen erkennen ließ, wurde in WASH-1400 eine relativ hohe Fehlerwahrscheinlichkeit für die menschlichen Eingriffe angesetzt, die kurzfristig nach einem Störfalleintritt vorgenommen werden. Diese Wertung wurde für die vorliegende Studie übernommen.

Die Ausbildung des Wartenpersonals in deutschen Kernkraftwerken wird in /F2, 3-46 bis -48/ geregelt. Der Schichtleiter und die Reaktorfahrer werden in regelmäßigen Abständen an einem Kraftwerkssimulator geschult, wobei einige wesentliche Störfallabläufe simuliert werden. Die Besetzung der Warte und die Zusammensetzung des Wartenpersonals differieren etwas zwischen deutschen und amerikanischen Anlagen. Zusammensetzung und Personalstärke der regulären Schicht sowie Aufgabenstellung und Ausbildung des Personals lassen sich für die Referenzanlage wie folgt angeben:

- 1 Schichtleiter

Der Schichtleiter ist verantwortlich für die Koordinierung aller Bedienungsmaßnahmen des Kraftwerksbetriebes einer Blockanlage mit den zugehörigen Nebenanlagen im Normalbetrieb ebenso wie im Störfall. Er entscheidet auch über mögliche Freischaltmaßnahmen im Rahmen des Wartungs- und Instandsetzungsprogrammes. Die Qualifikation als Schichtleiter muß in einer speziellen Schichtleiterprüfung nachgewiesen werden.

- 1 Reaktorfahrer für das Fahrpult

Dieser Reaktorfahrer kontrolliert den Blockbetrieb, das nukleare Dampferzeugungssystem (Reaktorkühlkreislauf) und alle hierzu erforderlichen Hilfssysteme. Er überwacht die Warnmeldeanlage für den gesamten Kraftwerksblock. Im Rahmen der Festlegungen des Betriebshandbuches und des Fahrprogrammes bedient er die obengenannten Anlagenteile eigenverantwortlich. Es besteht Informationspflicht gegenüber dem Schichtleiter.

- 1 Reaktorfahrer für das Steuerpult

Dieser Reaktorfahrer kontrolliert den Speisewasser-Dampf-Kreislauf und die Blocknebenanlagen. In Abstimmung mit dem Reaktorfahrer des Fahrpultes bedient er die ihm zugewiesenen Anlagenbereiche nach Betriebshandbuch eigenverantwortlich. Es besteht Informationspflicht gegenüber dem Schichtleiter.

- 1 Reaktorfahrer für organisatorische Aufgaben

Neben diesen drei speziell ausgebildeten und geprüften Fachkräften wird ein weiterer Reaktorfahrer im Tagdienst eingesetzt. Er entlastet die anderen Reaktorfahrer bei Durchführung von Funktionsprüfungen nach Maßgabe des Prüfhandbuchs. Dieser Reaktorfahrer schreibt auch die Arbeitsaufträge für alle Instandhaltungsmaßnahmen, die vom Schichtpersonal veranlaßt werden. Er formuliert die Freischaltmaßnahmen für die Durchführung von Wartungs- und Instandsetzungsarbeiten nach Maßgabe des Betriebshandbuches und der Unfallverhütungsvorschriften eigenverantwortlich.

- 2 Schichtelektriker

Die Schichtelektriker werden für die Bedienung der Telefon- und Personensuchanlage sowie für die Maßnahmen zur Eigenbedarfsversorgung auf Anweisung des Schichtleiters eingesetzt. Weiterhin übernehmen sie Betriebsrundgänge in den elektrotechnischen Anlagen, die Durchführung von Freischaltmaßnahmen und die Bedienung vor Ort auf Anweisung. Einer von beiden befindet sich jeweils auf der Warte.

- 2 Schichtschlosser

Die Schichtschlosser werden bei Rundgängen für die Durchführung von Freischaltmaßnahmen und die Bedienung vor Ort auf Anweisung eingesetzt.

Die Minimalbesetzung einer Schichtgruppe besteht somit aus 1 Schichtleiter, 2 Reaktorfahrern, 2 Schichtelektrikern und 2 Schichtschlossern, wobei mindestens ein, meist aber beide Reaktorfahrer Schichtleiterqualifikation besitzen. Die Entscheidungsbefugnis bei Stör- und Schadensfällen sowie das Verhalten der Schichtgruppe ist bei der untersuchten Anlage wie folgt organisiert:

Die Kriterien der Schadensfälle nach Betriebshandbuch (die Schadensfälle werden im Genehmigungsverfahren begutachtet und festgelegt) sind als festverdrahtete Warnmeldungen im Fahrpult mit Hinweis auf den entsprechenden Abschnitt des Betriebshandbuches installiert. Die Reaktorfahrer können im Rahmen ihrer Entscheidungsbefugnis anhand des Betriebshandbuches die notwendigen Maßnahmen durchführen oder veranlassen. Werden Betriebszustände erreicht, bei denen die Kriterien für eine Reaktorschnellabschaltung überschritten werden, ist der Reaktorfahrer verpflichtet, die Abschaltung von Hand auszulösen. Ergibt sich anhand der Anlageninstrumentierung ein anderer Zustand, als er in den Unterlagen des Betriebshandbuches für die Störfälle fixiert ist, so entscheidet der verantwortliche Schichtleiter über die notwendigen Maßnahmen. Der Schichtleiter hat Anweisung, schwerwiegende Eingriffe in den Betriebsablauf und alle besonderen Vorkommnisse seinen Vorgesetzten unverzüglich zu melden und sich über das weitere Vorgehen abzustimmen. Ist eine Abstimmung aus zeitlichen Gründen nicht möglich, trifft er alle unaufschiebbaren Entscheidungen, um einen eventuellen Schaden so gering wie möglich zu halten. Handmaßnahmen in der Warte werden von dem zuständigen Reaktorfahrer in Abstimmung mit dem zweiten Reaktorfahrer und dem Schichtleiter durchgeführt.

3.4.2.4 Schriftliche Anweisungen

In WASH-1400 werden im allgemeinen geringere Fehlerwahrscheinlichkeiten für Handlungen angesetzt, für die schriftliche Anweisungen vorhanden sind. In einem solchen Fall wird die Wahrscheinlichkeit dafür abgeschätzt, daß die vorhandenen schriftlichen Anweisungen tatsächlich benutzt werden oder sich das Bedienungspersonal eher auf sein Gedächtnis verläßt.

Bei der Bewertung der Qualität schriftlicher Anweisungen sind nach WASH-1400 Kriterien wie gute Lesbarkeit und Übersichtlichkeit, bei Störfallanweisungen außerdem übersichtliche und leicht zugängliche Aufbewahrung, Aktualisierung und Klarheit der Anweisung zu berücksichtigen.

Für die Referenzanalge werden sowohl die Logikfahnen des Betriebshandbuches als auch die des Prüfhandbuches berücksichtigt. Die Logikfahnen des Betriebshandbuches liegen den Bewertungen der Handmaßnahmen zur Beherrschung von Störfällen und Schadensfällen zugrunde. Die laut Prüfhandbuch durchzuführenden wiederkehrenden Prüfungen werden in Kapitel 5 behandelt.

3.4.2.5 Kopplung menschlicher Handlungen

Ein wichtiger Einflußfaktor bei der Bewertung menschlicher Zuverlässigkeit ist die Abhängigkeit menschlicher Handlungen untereinander, die in WASH-1400 als Kopplung bezeichnet wird. Bei menschlichen Handlungen lassen sich zwei Arten von Abhängigkeiten, nämlich direkte und indirekte, feststellen.

- Direkte Abhängigkeit menschlicher Handlungen ist dann gegeben, wenn eine Abhängigkeit unter den Handlungen selbst besteht. Ein Beispiel dazu sind ähnliche Aufgaben, die durch den gleichen Operator nacheinander durchgeführt werden (Bedienung von 2 unmittelbar aufeinanderfolgend zu betätigenden Komponenten).
- Indirekte Abhängigkeit liegt vor, wenn eine Abhängigkeit zwischen mehreren Handlungen und einem diese gemeinsam beein-

flussenden Faktor gegeben ist. Ein solcher Faktor wäre z.B. ein falsch eingestelltes oder falsch justiertes Meßgerät, mit dem die Kalibrierung von Meßkanälen erfolgt.

Unabhängigkeit der Handlungen ist zu erwarten, wenn die Handlungen unterschiedlich sind oder wenn sie voneinander räumlich und zeitlich getrennt durchgeführt werden.

Der Grad der Abhängigkeit der menschlichen Handlungen voneinander kann jedem Wert zwischen Unabhängigkeit und vollständiger Abhängigkeit annehmen.

Für die quantitative Bewertung ist jedoch eine Beschränkung auf einige Punkte dieses Bereiches sinnvoll und ausreichend. In WASH-1400 werden dazu vier Grade von Kopplungen unterschieden. Dies sind:

- keine Kopplung:
  Unabhängigkeit der einzelnen Handlungen voneinander,
- mittlere Kopplung:
  geringe Abhänigkeit der einzelnen Handlungen voneinander oder von einem gemeinsamen Faktor,
- starke Kopplung:
  starke Abhängigkeiten der einzelnen Handlungen voneinander oder einem gemeisamen Faktor,
- vollständige Kopplung:
  vollständige Abhänigkeit der einzelnen Handlungen voneinander oder von einem gemeinsamen Faktor.

Die Vorgehensweise dieser Studie bei der Berwertung gekoppelter Handlungen ist bereits im Abschnitt 3.3.5.2 beschrieben.

3.4.2.6 Rückkopplung durch Anzeigen und Meldungen

Die Wahrscheinlichkeiten menschlicher Fehlhandlungen werden verringert, wenn Rückkopplungen durch Anzeigen und Meldungen gegeben sind, die die Entdeckung und Beherrschung eines begangenen

Fehlers wahrscheinlich machen. Dies wird nach WASH-1400 durch Multiplikation der Fehlerwahrscheinlichkeit für die Handlung selbst mit einem Fehlerentdeckungsfaktor (recovery factor) berücksichtigt. Ein Fehlerentdeckungsfaktor ist insbesondere dann zu beachten, wenn der Operator unmittelbar nach einer Fehlhandlung durch eine Meldung gewarnt wird, so daß der Fehler bemerkt und korrigiert werden kann. Für die Fehlhandlungen, die eine langsame Änderung von Prozeßgrößen zur Folge haben und an Geräten der Wandtafel angezeigt werden, sind nach WASH-1400 höhere Fehlerentdeckungsfaktoren (z.B. 0,5) anzusetzen, d.h., die Wahrscheinlichkeit, den Fehler zu entdecken, ist entsprechend geringer.

Ein anderes Beispiel für Fehlerentdeckungsfaktoren liegt vor, wenn eine Armatur fälschlich in einer geschlossenen Stellung belassen wird und eine oft kontrollierte Anzeige (z.B. für Druck oder Durchfluß) daraufhin eine gravierende Abweichung vom Normalzustand aufweist.

3.4.2.7 Personelle Redundanz

Eine weitere Möglichkeit für die Fehlerentdeckung ist durch personelle Redundanz gegeben. Unter personeller Redundanz wird verstanden, daß bei der Entscheidung und/oder bei der Durchführung einer Maßnahme mehrere Personen mit ausreichender Qualifikation beteiligt sind; dabei kann sich die Tätigkeit der redundanten Person(en) auf reine Kontrolltätigkeit beschränken.

Nach WASH-1400 wird zwischen hohen und niedrigen Graden personeller Redundanz unterschieden. Von völliger (hoher) Redundanz wird dann gesprochen, wenn die Durchführung der Handlung unabhängig von ihrer Überprüfung ist. Ein niedriger Grad an personeller Redundanz wird in den Fällen angenommen, bei denen ein hoher Grad von Abhängigkeit zwischen Durchführung der Handlung und ihrer Kontrolle besteht. Generell werden in WASH-1400 relativ hohe Grade personeller Redundanz für Justierungsarbeiten, niedrigere für einfachere Aufgaben, wie das Verfahren von Armaturen von Hand, und sehr niedrige für reine Wartungsarbeiten

angesetzt. Im letzten Fall können jedoch Funktionsprüfungen im Anschluß an die Wartung eine zuverlässige Fehlerentdeckung bewirken. In der vorliegenden Studie werden diese Bewertungsmaßstäbe aus WASH-1400 übernommen.

Insbesondere wird für die Bewertung menschlicher Handlungen nach Störfalleintritt davon ausgegangen, daß für die Ausführung von Handlungen am Fahrpult bzw. Steuerpult grundsätzlich der entsprechende Reaktorfahrer zur Verfügung steht. Eine vollständige personelle Redundanz ist in der Person des Schichtleiters vorhanden, gegenüber dem Informationspflicht besteht. Weist eine Vielzahl von Meldungen und Anzeigen auf die Notwendigkeit der Durchführung von Handeingriffen hin, so ist eine zusätzliche personelle Redundanz durch den zweiten Reaktorfahrer gegeben. Von einer solchen personellen Redundanz ist auch bei übergreifenden Aktionen auszugehen, deren Konsequenzen sowohl vom Fahrpult als auch vom Steuerpult ersichtlich sind.

3.4.3 Basisdaten

Die Vorgehensweise in der vorliegenden Studie zur Bewertung menschlicher Fehlhandlungen lehnt sich eng an die Vorgehensweise von WASH-1400 an. Das der Bewertung zugrunde liegende Datenmaterial wird weitgehend von dort übernommen, lediglich in einigen speziellen Fällen wird auf die Vorgehensweise in der HTGR AIPA-Studie /F2, 3-36/ zurückgegriffen. Im folgenden werden die Daten, die die Grundlage der Bewertungen waren, und das in /F2, 3-36/ verwendete Bewertungsmodell dargestellt.

In WASH-1400 wird versucht, die Aussageunsicherheiten durch ungleiche Arbeitsleistung, Erfahrung und Ausbildung verschiedener Personen der Bedienungsmannschaft sowie Unterschiede in den Randbedingungen bei der Durchführung einer Arbeit usw. durch Annahme einer Verteilung für die Daten zu erfassen. Aus der vorliegenden Betriebserfahrung ist eine schiefe Wahrscheinlichkeitsdichteverteilung zu erkennen. Im Hinblick auf die verlangten Genauigkeiten und die Unempfindlichkeit der Gesamtergebnis-

se gegenüber der speziellen Form der Verteilung wird in WASH-1400 die logarithmische Normalverteilung als geeignete Näherung angesetzt.

In WASH-1400 sind die für menschliche Fehlhandlungen zugrunde gelegten Unsicherheitsfaktoren nicht dokumentiert. In der vorliegenden Studie wird für die Basisdaten zu menschlichen Fehlhandlungen ein Unsicherheitsfaktor 3 angesetzt, wie dies in WASH-1400 generell für sonstige Basisdaten der Fall ist. Für zusammengesetzte Fehlerwahrscheinlichkeiten werden die resultierenden Unsicherheitsfaktoren entsprechend den Rechengesetzen für logarithmisch normalverteilte Zufallsgrößen ermittelt.

Nach Abschluß der Untersuchungen für die vorliegende Studie sind in /F2, 3-49/ folgende Werte der in WASH-1400 verwendeten Unsicherheitsfaktoren ausgewiesen worden:

Fehlerwahrscheinlichkeit p_{50}	Unsicherheitsfaktor K
Normale Arbeitsbedingungen:	
$1 > p_{50} \geq 10^{-3}$	3
$10^{-4} > p_{50}$	10
$10^{-3} > p_{50} \geq 10^{-4}$:	
- Einzelhandlungen	3
- zusammengesetzte Fehlerwahrscheinlichkeiten für mehrfache Handlungen	10
Hohe Streßbelastungen	10

Tab. F2, 3-1:
In WASH-1400 verwendete Unsicherheitsfaktoren der Wahrscheinlichkeiten für menschliche Fehlhandlungen

In der Tabelle F2, 3-2 sind die Medianwerte der Fehlerwahrscheinlichkeiten zusammengestellt, die für die vorliegende Studie von Bedeutung sind. Die Werte sind WASH-1400, App. III entnommen.

In WASH-1400 wurden die in Tabelle F2, 3-2 angegebenen Basisdaten modifiziert, wenn spezielle Einflüsse auf die bewerteten Aufgaben zu berücksichtigen waren. Soweit nichts anderes ange-

Operator-Handlung	Wahrscheinlichkeit
Fehlhandlung innerhalb der ersten 60 Sekunden nach dem Beginn einer extremen Streßsituation, z.B. bei einem großen Leck in einer Hauptkühlmittelleitung	1
Fehlhandlung 5 Minuten nach Eintritt einer extremen Streßsituation	0,9
Fehlhandlung 30 Minuten nach Eintritt einer extremen Streßsituation	10^{-1}
Fehlhandlung mehrere Stunden nach Eintritt einer extremen Streßsituation	10^{-2}
Fehlhandlung allgemein (z.B. falsche Ablesung einer Anzeige und deshalb Betätigung eines falschen Schalters)	$3 \cdot 10^{-3}$
Unterlassungsfehler allgemein, wobei in der Warte keine Anzeige über den Zustand der nichtbetätigten Komponente vorhanden ist (z.B. Fehler, ein von Hand zu betätigendes Prüfventil nach Abschluß von Wartungsarbeiten wieder in die für den Betrieb richtige Stellung zu bringen)	10^{-2}
Unterlassungsfehler derart, daß während eines Arbeitsablaufs eine Handlung trotz schriftlicher Anweisungen vergessen wird; dies gilt nicht, wenn es am Ende des Arbeitsablaufs geschieht, wie im vorherigen Fall	$3 \cdot 10^{-3}$
Nichtentdeckung eines vorausgehenden Fehlers bei einer Kontrolle oder bei einem Kontrollrundgang Anmerkung: Bei ständiger Meldung des Fehlers auf einer Meldeeinrichtung trifft diese hohe Fehlerwahrscheinlichkeit nicht zu.	10^{-1}
Nichtentdeckung einer falschen Armaturenstellung u.ä. bei einem Kontrollrundgang in der Anlage, falls für die Kontrolle keine Checkliste verwendet wird	0,5
Fehlhandlung allgemein bei sehr hoher Streßbelastung, wenn schnell gefährliche Handlungen durchzuführen sind	0,2...0,3
Wiederholte Fehlhandlung unter extrem hohem Zeitdruck; bei jedem der n Versuche, die ursprüngliche Fehlhandlung zu korrigieren, verdoppelt sich die vorhergehende Fehlerwahrscheinlichkeit Anmerkung: Die Fehlhandlungswahrscheinlichkeit verdoppelt sich so lange, bis die Fehlerwahrscheinlichkeit p=1 erreicht oder die verfügbare Zeit abgelaufen ist.	$p=2^{(n-1)}p_o$

Tab. F2, 3-2:

Medianwerte der Wahrscheinlichkeiten für menschliche Fehlhandlungen nach WASH-1400

geben ist, beinhalten die Wahrscheinlichkeiten keinen unangemessenen Zeitdruck und keine Streßbelastungen aufgrund von Störfällen.

In /F2, 3-36/ wird bei der Ermittlung der Wahrscheinlichkeit für menschliches Fehlverhalten die zur Verfügung stehende Zeit und die für den Eingriff erforderliche Zeit berücksichtigt. Dies ist wichtig für die Bewertung menschlichen Fehlverhaltens bei Handmaßnahmen, für die erhebliche Zeit durch das Personal benötigt wird.

Zur Berechnung der Wahrscheinlichkeit p, mit der innerhalb der zur Verfügung stehenden Zeit t die erforderliche Handlung nicht erfolgt, wird eine Exponentialverteilung zugrunde gelegt. Ist MTOR die Zeit, die im Mittel zur Durchführung der Handlung erforderlich ist (Mean Time of Operator Response), so gilt

$$p(t) = \exp(-t/MTOR) \qquad (3.87)$$

Durch Erhöhung von MTOR gegenüber der bei Versuchen benötigten Zeit (z.B. um 10 %) kann nach /F2, 3-36/ auf einfache Weise berücksichtigt werden, daß das Personal bei einem Störfall erhöhtem Streß unterliegt.

In /F2, 3-36/ wird vorgeschlagen, für die Zeit MTOR eine logarithmische Normalverteilung zugrunde zu legen, wodurch die Streuung der Wahrscheinlichkeit p berücksichtigt werden kann. Diese Vorgehensweise wird auch in der vorliegenden Studie angewandt.

So wurden aus der Betriebserfahrung der Anlage Biblis 13 Werte für die zur Inbetriebnahme des Notstandssystems benötigten Zeiten ermittelt. Wie Bild F2, 3-16 zeigt, können diese Zeiten sehr gut als logarithmisch normalverteilt betrachtet werden. Als mittlere Zeit zur Inbetriebnahme des Notstandssystems wurden 16 Minuten ermittelt. Der Medianwert ergibt sich ebenfalls zu 16 Minuten und der Unsicherheitsfaktor zu 1,3. Die Wahrscheinlichkeiten p(t) werden wieder durch eine logarithmische Normalverteilung approximiert.

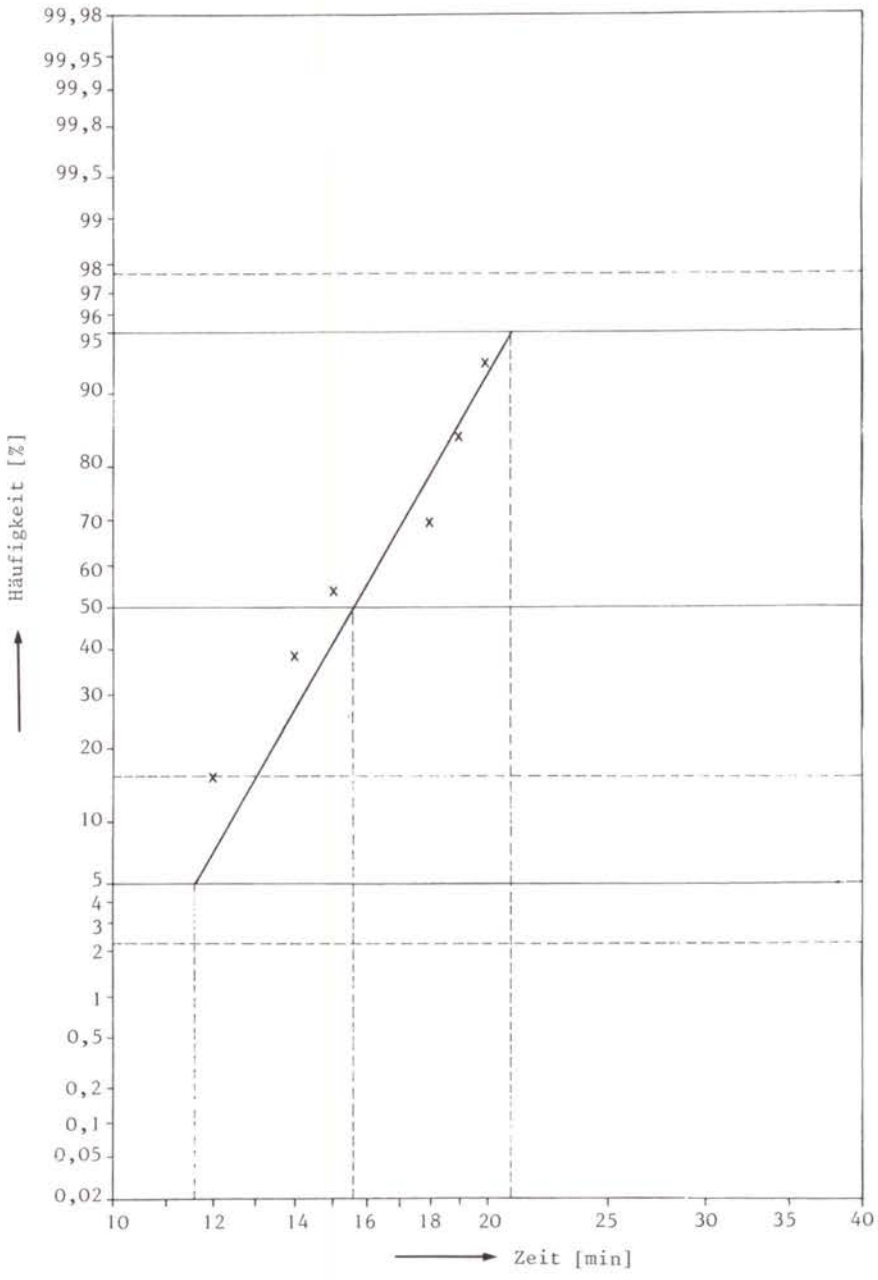


Bild F2, 3-16:

Zur Inbetriebnahme des Notstandssystems der Referenzanlage benötigte Zeiten

3.4.4 Durchgeführte Bewertung

Bei der Bewertung menschlichen Fehlverhaltens während des bestimmungsgemäßen Betriebes wird entsprechend WASH-1400 vorgegangen. Im Abschnitt 3.5 wird aber darauf hingewiesen, daß Fehler bei der Instandhaltung (Wartung, Instandsetzung, Inspektion) im allgemeinen von untergeordneter Bedeutung sind. Außerdem wird in allen Sicherheitssystemen der Einfluß menschlichen Fehlverhaltens bei Funktionsprüfungen oder anderen betrieblichen Systemanforderungen mit Hilfe von Kontrollbefehlen reduziert: Wird ein Sicherheitssystem durch Reaktorschutzsignale angefordert, so werden die wichtigsten Armaturen, die mit einem Motorantrieb ausgerüstet sind, nochmals gesteuert und gegebenenfalls in die richtige Stellung verfahren.

Auch bei der Bewertung der nach Störfällen oder Störungen durchgeführten Handmaßnahmen wird wie in WASH-1400 vorgegangen. So werden generell nur geplante Handmaßnahmen bewertet. Nicht geplante menschliche Handlungen, wie z.B. Maßnahmen, die bei Störungen in der Leittechnik oder von Schaltgeräten der elektrischen Energieversorgung dazu dienen können, verfahrenstechnische Komponenten in Betrieb zu nehmen, werden für Zeiträume unter 10 Stunden nicht berücksichtigt.

Wie in WASH-1400 wird in der vorliegenden Studie davon ausgegangen, daß nach einem Zeitraum von 10 Stunden auch umfangreichere Maßnahmen durchgeführt werden können.

Nach WASH-1400 kann erst für Zeitspannen $\geq$ 10 Stunden mit Eingriffen des Bedienungspersonals in Bereichen außerhalb der Kraftwerkswarte (z.B. in örtlichen Leitständen oder der Schaltanlage) gerechnet werden. Derartige Eingriffe sind in der Referenzanlage zum Teil auch während des bestimmungsmäßigen Betriebes der Anlage üblich und für bestimmte Störfälle vorgesehen. Dafür ist immer fachkundiges Wartenpersonal (Schichtelektriker und Schichtschlosser) zugegen. Geplante Handmaßnahmen außerhalb der Warte werden demnach in der vorliegenden Studie auch für Zeitspannen $<$ 10 Stunden nach Störfall- bzw. Störungseintritt berücksichtigt.

Bei der Bewertung menschlichen Fehlverhaltens werden grundsätzlich drei Punkte quantifiziert:

- das Erkennen, welche Maßnahmen durchzuführen sind;
- die benötigte Zeit, um die Maßnahmen durchzuführen;
  Sie wird nur bei Handmaßnahmen berücksichtigt, die erhebliche Zeit erfordern, insbesondere durch Begehung des Ringraums. Fehler beim Erkennen oder bei der Ausführung der Maßnahmen sind demgegenüber meist vernachlässigbar.
- die Ausführung der Maßnahmen;
  Fehlhandlungen bei der Ausführung werden nur bei schwierigen oder komplizierten Handlungen bewertet. Beispiele dazu sind das Einzeichnen des Abfahrgradienten für die Frischdampftemperatur auf einem Schreiberstreifen oder das gezielte Auffahren der Frischdampf-Umleitventile bzw. Abblaseregelventile. Die Wahrscheinlichkeit für das Betätigen einer falschen Taste wird aufgrund der ergonomischen Gestaltung der Warte, insbesondere aufgrund der vorhandenen Fließbilder (Abschnitt 3.4.2.2) als sehr gering eingeschätzt und folglich nicht berücksichtigt.

Bei der Bewertung des ersten und letzten Punktes wird auf die Vorgehensweise von WASH-1400 zurückgegriffen. Die in Abschnitt 3.4.2 erläuterten Einflüsse werden berücksichtigt. Die Bewertung des zweiten Punktes folgt der Vorgehensweise in /F2, 3-36/; bei der Wahrscheinlichkeitsverteilung für die benötigten Zeiten MTOR wird auf die Betriebserfahrung im Kernkraftwerk Biblis zurückgegriffen.

3.5 Instandhaltung

Außer der Nichtverfügbarkeit von Systemfunktionen aufgrund von Komponentenausfällen (Ausfall von notwendigen Komponentenfunktionen bei Anforderung) ist auch die Nichtverfügbarkeit durch Instandhaltung (Instandsetzung, Wartung und Inspektion) zu berücksichtigen. Die Nichtverfügbarkeit durch Inspektionen, insbesondere Funktionsprüfungen, spielt gegenüber der Nichtverfügbarkeit aufgrund von Instandsetzung und Wartung keine Rolle (Abschnitt 5.1).

Zur Ermittlung der Nichtverfügbarkeit durch Instandsetzung und Wartung wird auf die Betriebserfahrung im Kernkraftwerk Biblis zurückgegriffen. Grundlage der Auswertung sind die aufgetretenen Ausfallzeiten durch Instandhaltung für die Teilstränge des Not- und Nachkühlsystems für folgende Systemfunktionen:

- HD-Einspeisungen,
- Druckspeicher-Einspeisungen,
- ND-Einspeisungen,
- Nachkühlung,
- Gebäudesprühung.

Die Beobachtungen beziehen sich auf einen Zeitraum von 27 Monaten und folgende Komponenten (einschließlich komponentenspezifischer Steuerung und Energieversorgung):

- 20 Pumpen,
- 36 Motorarmaturen,
- 28 Sicherheitsventile.

Mit Hilfe der bekannten Daten für die Ausfallzeiten t, der Betrachtungszeit T und der Anzahl n der jeweils vorhandenen Komponenten läßt sich für Pumpen, Motorarmaturen und Sicherheitsventile eine Schätzung des Erwartungswerts $\bar{m}$ und der Varianz D^2 der Nichtverfügbarkeiten durch Instandsetzung und Wartung durchführen:

$$\bar{m} = \frac{1}{n \cdot T} \cdot \Sigma\, t \qquad (3.88)$$

Dabei geht man davon aus, daß für eine Komponentenart die Ausfallrate zeitlich konstant ist sowie die Ausfallzeiten voneinander unabhängig sind und die gleiche Verteilung besitzen. Die Summation erstreckt sich jeweils über sämtliche aufgetretenen Ausfallzeiten einer Komponentenart. Die hier betrachteten Ausfallzeiten beinhalten nicht die Zeit bis zur Fehlerentdeckung.

$$D^2(\bar{m}) = \frac{1}{(n \cdot T)^2} \cdot \Sigma\, t^2 \qquad (3.89)$$

Setzt man für die Nichtverfügbarkeit durch Instandsetzung und Wartung eine logarithmische Normalverteilung an, so ergaben

sich der Schätzwert für den Medianwert m_{50} und der Unsicherheitsfaktor K folgendermaßen:

$$m_{50} = \frac{\bar{m}^2}{\sqrt{D^2(\bar{m}) + \bar{m}^2}} \qquad (3.90)$$

$$\sigma = \sqrt{\ln(D^2(\bar{m})/\bar{m}^2 + 1)} \qquad (3.91)$$

$$K = \exp\,(1{,}6449 \cdot \sigma) \qquad (3.92)$$

Mit den Daten aus der Betriebserfahrung für die Nichtverfügbarkeit von Pumpen, Motorarmaturen und Sicherheitsventilen aufgrund von Instandhaltung ergeben sich folgende Werte:

Komponentenart	n	Σ t	m_{50}	K
Pumpe	20	372,0 h	$1 \cdot 10^{-3}$	2
Motorarmatur	36	139,5 h	$2 \cdot 10^{-4}$	2
Sicherheitsventil	28	230,5 h	$4 \cdot 10^{-4}$	2

In den Fehlerbäumen wird bei den einzelnen Systemteilsträngen entsprechend der Anzahl der vorhandenen Komponenten eine Ersatz-Nichtverfügbarkeit zur Berücksichtigung der Instandhaltung eingeführt.

Bei der Abschätzung des Einflusses dieser Instandsetzungs- und Wartungsarbeiten auf die Nichtverfügbarkeiten der Systemfunktionen ist zu berücksichtigen, daß sie überall dort keine Rolle spielen, wo die Summe der sich auf diese Weise ergebenden Ausfallzeiten des Funktionselements klein gegenüber den insgesamt zu berücksichtigenden Ausfallzeiten des Funktionselements ist.

Ferner ist zu beachten, daß die Anlage abgefahren werden muß, wenn aufgrund der durchzuführenden Instandhaltungen das Einzelfehlerkriterium nicht mehr erfüllt ist /F2, 3-50/. Somit ist bei Leistungsbetrieb der Anlage eine gleichzeitige Instandsetzung oder Wartung von redundanten Strängen auszuschließen. Pessimistisch wird diese Bedingung für die Instandsetzung der Funktionselemente nicht berücksichtigt.

Weiterhin ist es möglich, daß Instandsetzungen von Funktionselementen falsch ausgeführt werden oder daß nach einer Instandsetzung das betroffene Teilsystem nicht wieder in den Ausgangszustand versetzt wird (z.B. der Schieber zur Freischaltung einer Pumpe nicht wieder geöffnet wird). Es besteht jedoch die Vorschrift, daß nach jeder Instandsetzung das betroffene Teilsystem einer Funktionsprüfung zu unterziehen ist.

In WASH-1400 werden für Fehlhandlungen bei Instandsetzungen oder Funktionsprüfungen Wahrscheinlichkeiten von $3 \cdot 10^{-3}$ bis 10^{-2} angegeben. Für die vorliegende Studie wurde diese Bewertung übernommen, damit ergibt sich im allgemeinen ein vernachlässigbar geringer Einfluß auf das Ergebnis für die Systemfunktion. Diese Aussage gilt auch für das Übersehen von aufgetretenen Ausfällen bei den regelmäßig durchzuführenden Funktionsprüfungen (Abschnitt 5.1).

4. SYSTEMBESCHREIBUNGEN

4.1 Allgemeines

In den folgenden Abschnitten werden für die Referenzanlage die verfahrenstechnischen Systeme, die Systeme zur elektrischen Energieversorgung und der Leittechnik nur so weit beschrieben, wie es für die nachfolgende Zuverlässigkeitsanalyse erforderlich ist. Die Systembeschreibungen beziehen sich auf den Stand der Systeme, der bei Durchführung der in dieser Studie dargestellten Untersuchungen vorlag. Seit Abschluß der Zuverlässigkeitsanalyse wurde eine Reihe von systemtechnischen Änderungen durchgeführt. Darauf wird im folgenden nicht eingegangen.

4.2 Verfahrenstechnische Systeme

4.2.1 Not- und Nachkühlsystem

Der Aufbau des Not- und Nachkühlsystems, über das nach einem Kühlmittelverluststörfall sowohl die Einspeisung von Borwasser in den Reaktordruckbehälter als auch die Umwälzung und Kühlung von Sumpfwasser erfolgt, ist dem Schaltplan 1 (Anhang 1) zu entnehmen. Es besteht aus vier getrennten Strängen, von denen jeder einen Druckspeicher sowie die Komponenten zur Hochdruck(HD)- und zur Niederdruck(ND)-Einspeisung aus den beiden miteinander direkt verbundenen Flutbehältern enthält.

Für die Funktion der einzelnen Druckspeicher und Flutbehälter ist es notwendig, daß diese

- die vorgesehenen Wassermengen mit der vorgesehenen Borkonzentration von mindestens 2200 ppm Bor enthalten, wobei
- die Wassermengen in den Druckspeichern unter einem Stickstoff-Überdruck von 25 bar

stehen müssen. Um das sicherzustellen, werden die Wasserstände in jedem der Flutbehälter-Paare sowie die Wasserstände und Drükke in den einzelnen Druckspeichern mittels je einer "betrieblichen" Messung überwacht. Das heißt, bei Unter- bzw. Überschrei-

ten von folgenden Grenzwerten erhält man optische und akustische Störungsmeldungen in der Kraftwerkswarte (am Beispiel des Stranges der Redundanz 1):

- Niveaumessung 20 TH10 L002 an den Flutbehältern 20 TH10 B001/2
  Störungsmeldung bei Wasserstand ≧ 10,75 m
  ≦ 10,45 m
- Niveaumessung 20 TH16 L002 am Druckspeicher 20 TH16 B001
  Störungsmeldung bei Wasserstand ≧ 10,6 m
  ≦ 10,0 m
- Druckmessung 20 TH16 P002 am Druckspeicher 20 TH16 B001
  Störungsmeldung bei Überdruck ≧ 26,5 bar
  ≦ 23,5 bar

Die Analogwerte dieser Messungen werden in der Kraftwerkswarte auf dem Wartenpult angezeigt. Zusätzlich werden an jedem Flutbehälter noch drei unabhängige Messungen der Wasserstände zur Bildung der Sumpfsignale YZ41-44 vorgenommen. Für die Flutbehälter 20 TH10 B001/2 sind das die Niveaumessungen 21 TH10 L051, 22 TH10 L052 und 24 TH10 L053. Die Analogwerte dieser Messungen werden in der Kraftwerkswarte auf der Reaktorschutztafel angezeigt.

Für jeden der vier Druckspeicher gibt es noch eine unabhängige Messung des Stickstoffdruckes, z.B. durch 21 TH16 P051, zur Bildung der ND-Einspeisesignale YZ38. Dazu werden jeweils drei Messungen zyklisch vertauscht in 2v3-Verknüpfungen verarbeitet. Dadurch findet ein mehrfacher Vergleich, also eine weitere ständige Überwachung dieser Drücke statt. Die Analogwerte dieser Messungen werden ebenfalls auf der Reaktorschutztafel in der Warte angezeigt.

Es gibt ferner noch örtliche Druck- und Wasserstandsmessungen an den Behältern, z.B. die Druckmessung 20 TH16 P001 und die Niveaumessung 20 TH16 L001 am Druckspeicher 20 TH16 B001.

Bei Verlust oder Zufuhr sowohl von Stickstoff als auch von Wasser spricht zuerst der Druckgrenzwert an. Bei den Störungsmeldungen DRUCK DRUCKSPEICHER TIEF und DRUCK DRUCKSPEICHER HOCH ist

daher laut Betriebshandbuch auch eine Überprüfung des Wasserstandes und gegebenenfalls ein Ergänzen des Borwassers vor einem Nachspeisen von Stickstoff erforderlich. Stickstoff wird aus dem Schutzgassystem TP3, und zwar durch Handbedienung einer Armatur vor Ort nachgespeist. Borwasser wird mit der HD-Sicherheitseinspeisepumpe der entsprechenden Redundanz des Not- und Nachkühlsystems durch Nachspeisen aus den Flutbehältern über eine gesonderte Fülleitung ergänzt.

Innerhalb des Sicherheitsbehälters sind die vier getrennten Stränge des Not- und Nachkühlsystems entsprechend der Anordnung der vier Hauptkühlkreisläufe in vier unterschiedlichen Quadranten des Reaktorgebäudes angeordnet. Die Druckspeicher befinden sich dabei außerhalb des Beton-Trümmerschutzes, sie sind also gegen Folgeschäden beim Bruch einer Hauptkühlmittelleitung geschützt. Um innerhalb des Beton-Trümmerschutzes eine Beschädigung eines Stranges des Not- und Nachkühlsystems durch das Versagen eines anderen Hauptkühlkreislaufes zu verhindern, wurde zwischen den jeweils unmittelbar benachbarten Hauptkühlkreisläufen eine Trennwand gezogen, die für alle bei einem Kühlmittelverluststörfall auftretenden Belastungen ausgelegt ist. Im Schutz dieser Trennwand wurden dann die kalte und die heiße Einspeiseleitung des jeweiligen Stranges des Not- und Nachkühlsystems verlegt. Diese Trennwände haben keine vollständige räumliche Trennung zweier benachbarter Hauptkühlkreisläufe zur Folge, sie bilden insbesondere keine räumliche Trennung der benachbarten Dampferzeuger, die jedoch gemeinsam durch Betonwände teilweise geschützt werden.

Um die heiße/kalte Einspeiseleitung eines Stranges des Not- und Nachkühlsystems gegen die Folgeschäden beim Bruch des heißen/kalten Abschnittes der zugehörigen Hauptkühlmittelleitung zu schützen, wurden für die Einspeiseleitungen zusätzlich Stahlkonstruktionen installiert, die die Wahrscheinlichkeit eines Folgeausfalles herabsetzen sollen. Aus diesem Grund wurden auch die innerhalb der Stahlhülle befindlichen Armaturen eines Stranges in einer durch eine Betonzwischenwand vom zugehörigen Hauptkühlkreislauf weitgehend geschützten Armaturenkammer angeordnet.

Um bei Brüchen der heißen/kalten Einspeiseleitung eines Stranges im Bereich der Anschlußstutzen der Hauptkühlmittelleitung Folgeschäden an der jeweils anderen Einspeiseleitung dieses Stranges zu verhindern, wurden an diesen Ausschlag- und Verdrehsicherungen installiert.

Die im Ringraum befindlichen Komponenten des Not- und Nachkühlsystems sind nach Redundanzen getrennt in unterschiedlichen Ringraumsegmenten aufgestellt. Zu diesen Komponenten gehören die Flutbehälter, die HD-Sicherheitseinspeisepumpen, die zur ND-Einspeisung dienenden Nachkühlpumpen, die Nachwärmekühler, die Flutbehälter- und Sumpfarmaturen. Um Brüche der Sumpfsaugleitungen bei Kühlmittelverluststörfällen zu verhindern, sind diese Leitungen nach der Stahlhüllendurchführung bis zu den Absperrarmaturen TH01 (02/03/04) S001 als Doppelrohre mit Dichtheitsüberwachung ausgeführt. Überwacht wird dabei der Stickstoffdruck im Zwischenraum der Doppelrohre.

Bei Kühlmittelverluststörfällen sprechen die Druckspeicher-Einspeisungen selbsttätig an, die HD- und die ND-Einspeisungen aus den Flutbehältern werden durch die HD- bzw. ND-Einspeisesignale YZ36 und YZ38 gestartet. Diese Reaktorschutzsignale, auf deren Bildung im Schaltplan 15 eingegangen wird, bewirken in den vier getrennten Strängen des Not- und Nachkühlsystems das Starten der HD-Sicherheitseinspeisepumpen bzw. der Nachkühlpumpen.

Die HD-Sicherheitseinspeisepumpen sind mehrstufige Pumpen. Sie besitzen Stopfbuchsdichtungen und Gleitlager. Alle Pumpenlager sind druckölgeschmiert, jede Pumpe hat eine eigene Ölversorgung. So besitzt (am Beispiel des Stranges der Redundanz 1) die Pumpe 21 TH15 D001 den Ölbehälter 20 TH15 B001, zwei redundante Zahnrad-Ölpumpen, einen Ölfilter 20 TH15 N001 und einen Ölkühler. Der Ölstand des Ölbehälters wird über einen Niveau-Wächter überwacht, bei Unterschreiten eines Minimalwertes wird eine Meldung ausgegeben. Die Motoren der HD-Sicherheitseinspeisepumpen besitzen eine Luft-Wasser-Kühlung. Die Motoren, Stopfbuchsen und Ölkühler werden vom nuklearen Zwischenkühlkreis aus mit Kühlwasser versorgt. Die luftgekühlten Motoren der Ölpumpen sind für Umgebungstemperaturen bis zu 40 °C ausgelegt. Bei Anstehen der Ge-

bäudeabschlußsignale für lufttechnische Anlagen YZ32[1]) oder beim Notstromfall ist die Kühlung der Raumluft durch die Umluftanlage notwendig.

Die Nachkühlpumpen besitzen zur Wellenabdichtung doppelte Gleitringdichtungen. Die Gleitringdichtungen aller Nachkühlpumpen werden über zwei getrennte Stränge des Deionatnetzes mit Sperrwasser beaufschlagt. Bei Ausfall der Sperrwasserversorgung, deren Pumpen beim Störfall durch die Notkühlvorbereitungssignale YZ31[1]) gestartet werden, wird die Aktivitätsabgabe an die Umgebung erhöht. Die Nachkühlpumpen können jedoch im Notfall ohne Sperrwasserversorgung betrieben werden. Die Nachkühlpumpen haben Wälzlager mit Ölschmierung, die zugehörigen Ölvorratsbehälter sind an den Pumpen angebracht. Wie die HD-Sicherheitseinspeisepumpen besitzen auch die Nachkühlpumpen Luft-Wasser-Kühlung. Ebenso wird die Motorluft-, Sperrwasser- und Ölkühlung über den nuklearen Zwischenkühlkreis mit Kühlwasser versorgt.

Alle Armaturen des Not- und Nachkühlsystems mit Motorantrieb oder Mediumsteuerung befinden sich normalerweise bereits in den richtigen Stellungen für den Einspeisebetrieb aus den Flutbehältern (im folgenden kurz als Fluten bezeichnet), eine Ausnahme bilden die regelmäßigen Funktionsprüfungen, bei denen die Armaturen verfahren werden. Die Fehlstellungen der Armaturen werden durch die Sammelmeldung NOTKÜHLBEREITSCHAFT GESTÖRT sofort gemeldet. Außerdem ergehen an die Armaturen mit Motorantrieb durch den Reaktorschutz die Stellung kontrollierende Befehle. So werden durch die Notkühlvorbereitungssignale YZ31 an die Armaturen der Redundanz 1 folgende Befehle ausgegeben:

21	TH16	S001	AUF	21 TH10 S009	ZU
21	TH16	S002	AUF	21 TH12 S001	AUF
21	TH51	S001	ZU	21 TH12 S005	ZU
21	TH51	S002	ZU	21 TH12 S007	ZU
21	TH10	S007	AUF	21 TH12 S009	ZU
21	TH10	S008	ZU		

[1]) Dieses Signal ist wie alle anderen Reaktorschutzsignale in vier Redundanzen vorhanden, es wird jedoch hier nur eine gemeinsame YZ-Nummer verwendet.

Analoges gilt für die Redundanzen 2 bis 4. Durch die Notkühlvorbereitungssignale YZ31 erhalten außerdem die Armaturen in den Leitungen des Reinigungssystems, hinter der Reduzierstation sowie in der Reaktorbecken-Flutleitung die Stellung kontrollierende ZU-Befehle:

21 TH10 S010 ZU
22 TH20 S010 ZU

23 TA35 S005 ZU

21 TH17 S007 ZU
23 TH37 S007 ZU

Für das Not- und Nachkühlsystem sind außer den Notkühlvorbereitungssignalen YZ31, den HD- und den ND-Einspeisesignalen YZ36 und YZ38 noch die Flutsignale YZ45 bis YZ48 wichtig. Durch diese Flutsignale erhalten die motorbetätigten Flutbehälterarmaturen die Stellung kontrollierende AUF-Befehle und die Sumpfarmaturen ebensolche ZU-Befehle. Für die Redundanz 1 bedeutet das:

21 TH10 S001 AUF
21 TH10 S002 AUF
21 TH01 S001 ZU

Ferner ergehen an die Schieber in den Gebäudesprühleitungen und an die Armaturen in den Prüfleitungen zur Kontrolle ZU-Befehle.

Ist ein Flutbehälter bis auf die Sprühreserve entleert, so werden anstelle der Flutsignale YZ45-48 die entsprechenden Sumpfsignale YZ41 bis YZ44 ausgegeben. Dadurch werden in diesem Strang des Not- und Nachkühlsystems die redundanten, diversitären Flutbehälterarmaturen sowie die Sumpfarmaturen betätigt, der Strang wird auf Sumpf-Umwälzbetrieb umgeschaltet. Für die Redundanz 1 ergehen durch das Sumpfsignal YZ41 folgende Befehle:

21 TH10 S001 ZU (unverzögert)
21 TH10 S002 ZU (unverzögert)
21 TH01 S001 AUF (verzögert)

Das Sumpfwasser wird beim Sumpf-Umwälzbetrieb in den Nachwärmekühlern durch den nuklearen Zwischenkühlkreis gekühlt.

Die Eintrittsstutzen der vier Sumpfleitungen befinden sich in vier getrennten Sumpfkammern. Diese Kammern sind bis auf die Eintrittsöffnung allseits von Betonwänden umgeben. Die Eintrittsöffnungen sind mit Sieben der Maschenweite 8 x 8 mm versehen. Außerdem sind die Sumpfkammern der Stränge 1 und 2 sowie 3 und 4 durch Siebe miteinander verbunden.

Bevor das herabfließende Wasser die Sumpfkammern erreicht, passiert es eine waagerechte Gitterrostbühne mit einer Maschenweite von 4 x 4 cm. Die gesamte Siebfläche der waagerechten Gitter beträgt ca. 160 m^2.

4.2.2 Nuklearer Zwischenkühlkreis

Der nukleare Zwischenkühlkreis ist ein Teil der Kühlkette zur Abfuhr der Wärme aus den Kühlstellen der nuklearen Hilfs- und Nebenanlagen. Die dort aufgenommene Wärme wird an das Nebenkühlwasser abgegeben. Der nukleare Zwischenkühlkreis soll bei Auftreten von Leckagen an den nuklearen Kühlstellen eine unmittelbare Freisetzung von Aktivitäten verhindern.

Bei Kühlmittelverluststörfällen dient der nukleare Zwischenkühlkreis zur Kühlung der HD-Sicherheitseinspeisepumpen-Aggregate und deren Ölversorgung, der Nachkühlpumpen-Aggregate und deren Sperrwasserversorgung, der von Sumpfwasser durchflossenen Nachwärmekühler sowie des Brennelement-Beckenkühlers.

Bei kleinen Lecks in einer Hauptkühlmittelleitung, im Notstromfall und beim Ausfall der Hauptspeisewasserversorgung hat der nukleare Zwischenkühlkreis außerdem die Aufgabe, die Motorluft-, Öl- und Stopfbuchsen-Kühlung der im Hilfsanlagengebäude aufgestellten Notspeisewasser-Pumpen der Redundanzen 3 und 4 zu übernehmen.

Bei einem Kühlmittelverluststörfall ist eine Kühlung des nuklearen Zwischenkühlkreises durch das Nebenkühlwassersystem erst bei Sumpfbetrieb notwendig, wenn die über die Nachwärmekühler anfallende Wärme abgeführt werden muß.

Der in Schaltplan 2 (Anhang 1) dargestellte nukleare Zwischenkühlkreis ist aus vier getrennten Strängen aufgebaut, die den entsprechenden Redundanzen des Not- und Nachkühlsystems zugeordnet sind. Die vier Stränge sind wie jene des Not- und Nachkühlsystems in unterschiedlichen Ringraumsegmenten angeordnet. Von den Strängen 1 und 3, die mit je 2 nuklearen Zwischenkühlpumpen ausgestattet sind, werden beim bestimmungsgemäßen Betrieb zusätzlich die beim Störfall nicht relevanten Kühlstellen innerhalb der Stahlhülle und im Reaktor-Hilfsanlagengebäude über eine Ringleitung versorgt. Bei Leistungsbetrieb ist einer dieser Stränge in Betrieb; der zweite sowie die Stränge 2 und 4 des nuklearen Zwischenkühlkreises befinden sich in Bereitschaft.

Die nuklearen Zwischenkühlpumpen besitzen für ihre ölgeschmierten Wälzlager keine externe Versorgung mit Schmiermittel. Die Pumpen und ihre Antriebsmotoren benötigen keine Kühlwasserversorgung.

Die Motoren mit Kühlung durch Raumluft sind für eine maximale Raumlufttemperatur von 40 °C ausgelegt. Beträgt die Motorbelastung nur 82 % der Nennleistung, so können die angesprochenen Motoren auch noch bei einer Raumlufttemperatur von 60 °C betrieben werden.

In jedem der vier Stränge des nuklearen Zwischenkühlkreises ist eine Pumpe notstromgesichert. Bei Kühlmittelverluststörfällen werden diese Pumpen von den Notstromvorbereitungssignalen YZ81 gestartet, wobei die folgenden Befehle ausgegeben werden:

21 TF11 D001 EIN
22 TF21 D001 EIN
23 TF31 D001 EIN
24 TF41 D001 EIN

Durch die Notkühlvorbereitungssignale YZ31 ergehen an die Absperrarmaturen der Stränge 1 und 3 zur Ringleitung folgende Befehle:

21 TF50 S001 ZU
22 TF50 S002 ZU

23 TF50 S003 ZU
24 TF50 S004 ZU

Falls die Ringleitung nicht abgetrennt werden kann, müssen die entsprechenden Stränge des nuklearen Zwischenkühlkreises als ausgefallen betrachtet werden.

Durch die Gebäudeabschlußsignale für die Hauptkühlmittelpumpen YZ34 werden die Verbraucher innerhalb der Stahlhülle durch doppelte Gebäudeabschlußarmaturen zusätzlich abgetrennt. Dazu ergehen folgende Befehle:

23 TF60 S001 ZU
24 TF60 S002 ZU
23 TF60 S069 ZU
24 TF60 S070 ZU

In den Strängen 1 und 3 werden außerdem durch die entsprechenden Notkühlvorbereitungssignale die parallel geschalteten Absperrarmaturen der Nachwärmekühler geöffnet:

21 TF10 S004 AUF
21 TF10 S014 AUF
23 TF30 S004 AUF
23 TF30 S014 AUF

Beim Notstromfall werden 2 der 4 Zwischenkühlpumpen betrieblich gestartet. Es sind dies die Zwischenkühlpumpen 23 TF31 D001 und 24 TF41 D001. Die Pumpe 21 TF11 D001 steht über eine automatische Störumschaltung in Bereitschaft, unter der Annahme, daß der Strang 3 Betriebsstrang war. An die Pumpen 23 TF31 D001 bzw. 24 TF41 D001 ergehen als Startbefehle die nullredundanten Notstromsignale YZ84 und YZ85.

Die Wärmeabfuhr aus den einzelnen Strängen des nuklearen Zwischenkühlkreises an das Nebenkühlwassersystem geht über die Zwischenkühler. Alle Armaturen in den Umgehungsleitungen der Zwischenkühler erhalten ZU-Befehle, obwohl diese laut Betriebshandbuch in den außer Betrieb befindlichen Strängen des nuklearen Zwischenkühlkreises bereits geschlossen sein sollen. Bei dem in Betrieb befindlichen Strang des nuklearen Zwischenkühl-

kreises (Strang 1 oder 3) ist bei niedrigen Flußwassertemperaturen (im Winter) die Armatur in der Umgehungsleitung hingegen geöffnet, um das Zwischenkühlwasser nicht zu stark abzukühlen und Schwitzwasserbildung zu vermeiden. Durch die Notkühlvorbereitungssignale YZ31 werden folgende Befehle ausgegeben:

21 TF10 S048 ZU
22 TF20 S048 ZU
23 TF30 S048 ZU
24 TF40 S048 ZU

Ebenso soll laut Betriebshandbuch in dem Strang 1 oder 3 des nuklearen Zwischenkühlkreises, der bei Leistungsbetrieb gerade außer Betrieb ist, die Absperrarmatur zum Brennelement-Beckenkühler geschlossen sein. Beim vor dem Störfall in Betrieb befindlichen Strang ergeht bei Ausfall einer der beiden Zwischenkühlpumpen ein ZU-Befehl an die Absperrarmatur zum Brennelement-Beckenkühler. Falls dann die Beckenkühlung nicht abgeschaltet wird, ist eine ausreichende Kühlwasserversorgung der Nachwärmekühler und gegebenenfalls der Notspeisewasser-Pumpe 23 RL06 D001 in der ersten Zeit nach einem Kühlmittelverluststörfall nicht gewährleistet.

In jedem der Stränge des nuklearen Zwischenkühlkreises sind zwei miteinander verbundene Ausgleichsbehälter vorhanden. Bei Absinken des Wasserstandes in den Behältern wird das Deionatzulaufventil automatisch geöffnet und so aus dem Deionatsystem 4,5 m^3/h Wasser nachgespeist. Diese Deionatzuspeisung ist notstromgesichert. Durch Öffnen eines Handventils vor Ort kann zusätzlich Nachspeisen bis zu 20 m^3/h erfolgen.

4.2.3 Nukleares Nebenkühlwassersystem

Über das nukleare Nebenkühlwassersystem wird die Wärme abgeführt, die bei Normalbetrieb oder bei Störfällen in den nuklearen Zwischenkühlern, den Kühlern der Notstromdiesel und den Kühlern der großen und kleinen Kältemaschinen anfällt.

Das nukleare Nebenkühlwassersystem ist saugseitig aus vier getrennten Strängen aufgebaut (Schaltplan 3, Anhang 1). In jedem

der Stränge wird von den Nebenkühlpumpen über Grob- und Feinrechen sowie über Siebbandmaschinen mechanisch gereinigtes Flußwasser angesaugt. Für eine ausreichende Kühlwasserversorgung sind den Kühlern der Notstromdiesel und den Kühlern der Kältemaschinen zusätzliche Druckerhöhungspumpen vorgeschaltet. Hinter den Kühlern werden die Stränge 1 und 2 sowie die Stränge 3 und 4 zu je einer Rücklaufsammelleitung zusammengefaßt. Das Nebenkühlwasser fließt über diese Leitungen in ein Nebenkühlwasser-Sammelbecken und wird dort in den Fluß zurückgeleitet.

Die Nebenkühlwasserpumpen sind paarweise in getrennten Räumen des Reinigungs- bzw. Pumpenbauwerks angeordnet. Die Rohrleitungen des nuklearen Nebenkühlwassersystems sind von dort bis zu den Kühlern ebenfalls paarweise getrennt verlegt, so daß nie mehr als zwei Stränge zusammentreffen. Die nuklearen Zwischenkühler sind im Ringraum räumlich getrennt angeordnet, die Dieselkühler bilden eine Baueinheit mit den in getrennten Räumen des Schaltanlagengebäudes installierten Notstromdieseln. Die kleinen Kältemaschinen sind ebenfalls in getrennten Räumen des Schaltanlagengebäudes aufgestellt.

Bei Leistungsbetrieb des Kernkraftwerks ist Strang 1 oder 3 des Nebenkühlwassersystems in Betrieb, da von diesen die Betriebsstränge des nuklearen Zwischenkühlkreises versorgt werden. Von den Strängen 2 oder 4 des Nebenkühlwassersystems werden bei Leistungsbetrieb die großen Kältemaschinen versorgt, so daß sich auch einer dieser beiden Stränge in Betrieb befindet.

Die Antriebe für die Grob- und Feinrechen sowie für die Siebbandmaschinen laufen nur, wenn durch die entsprechende Reinigungsstraße Wasser angesaugt wird. Die Antriebe werden nicht mit Notstrom versorgt. Falls es aufgrund des Ausfalls der Antriebe zu einer starken Verschmutzung einer Siebbandmaschine kommt, öffnet deren Notauslaßklappe. Es fließt dann das verschmutzte Wasser den Nebenkühlwasserpumpen zu.

Die Nebenkühlwasserpumpen und ihre Antriebsmotoren benötigen keine Kühlwasserversorgung. Zur Schmierung der Gleitlager besitzt Pumpenaggregat zwei Fettpumpen, von denen eine zum Anfah-

ren und zum Betrieb ausreicht. Eine Nebenkühlwasserpumpe kann bei Ausfall von zwei Fettpumpen noch etwa eine halbe Stunde ohne Beschädigung der Gleitlager weiterbetrieben werden.

Die Druckerhöhungspumpen und ihre Antriebsmotoren benötigen keine Kühlwasserversorgung und keine Schmierpumpen zur Versorgung der Gleitlager.

Bei Kühlmittelverluststörfällen werden in jedem der vier Stränge die Nebenkühlwasserpumpe, die beiden zugehörigen Fettpumpen sowie die Druckerhöhungspumpe für die kleinen Kältemaschinen gestartet. Dazu werden durch das Notstromvorbereitungssignal YZ81 für die Redundanz 1 folgende Befehle ausgegeben:

21 VE10 D001 EIN
21 VE10 D002 EIN
21 VE10 D003 EIN
21 VE12 D001 EIN

Außerdem ergehen durch das Notstromvorbereitungssignal noch an die Regelventile der kleinen Kältemaschinen AUF-Befehle, um eine ausreichende Kühlwasserversorgung der kleinen Kältemaschinen zu gewährleisten:

21 VE12 S004 AUF
22 VE22 S004 AUF
23 VE32 S004 AUF
24 VE42 S004 AUF

Im Notstromfall werden in jedem der vier Stränge von getrennten Teilsteuerungen die Nebenkühlwasserpumpe, die beiden zugehörigen Fettpumpen sowie die Druckerhöhungspumpe für die kleinen Kältemaschinen durch die nullredundanten Notstromsignale YZ82-85 bzw. durch die Rückmeldung NEBENKÜHLWASSERPUMPE EIN gestartet.

Zur Kühlung der im Notstromfall angeforderten Notstromdiesel werden die Druckerhöhungspumpen 20 EY10 D005 usw. benötigt, die mit den Dieseln fest gekoppelt sind. Ferner müssen die bei Leistungsbetrieb des Kernkraftwerks in geschlossener Stellung befindlichen parallelen Absperrarmaturen vor den Dieselkühlern geöffnet

werden. Dazu ergehen innerhalb der ersten Dieselbelastungsstufe durch die negierten Notstromsignale YZ82-85 folgende Befehle:

21 VE14 S001 AUF
21 VE14 S010 AUF
22 VE24 S001 AUF
22 VE24 S010 AUF
23 VE34 S001 AUF
23 VE34 S010 AUF
24 VE44 S001 AUF
24 VE44 S010 AUF

4.2.4 Druckhaltesystem

Das Druckhaltesystem (Schaltplan 4, Anhang 1) dient dazu, den für den Reaktorkühlkreislauf erforderlichen Betriebsdruck zu erzeugen und Druckänderungen, die aufgrund von Volumenschwankungen des Kühlmittels bei Laständerungen auftreten, auszugleichen. Diese Aufgabe erfüllt im wesentlichen der Druckhalter 20 YP01 B001, der dazu mit einer Sprühung und einer Heizung ausgestattet ist. Der Druckhalter ist über die Volumenausgleichsleitung an die heiße Hauptkühlmittelleitung des Hauptkühlkreislaufs 2 angeschlossen.

Über je 2 am Druckhalter angeschlossene Abblase- und Sicherheitsventile wird bei Störungen der Kühlmitteldruck begrenzt. Die Ansprechdrücke der Abblase- und Sicherheitsventile sind gestaffelt, beginnend mit einem Absolutdruck von 161 bar (1. Ablaseventil) bis zum Auslegungsdruck des Systems von 173 bar (2. Sicherheitsventil). Der über diese Ventile abgegebene Dampf wird in den Druckhalter-Abblasetank 20 YP01 B002 geleitet. Der Abblasetank, der durch den nuklearen Zwischenkühlkreis gekühlt wird, kann durch Kondensation die Dampfmenge aufnehmen, die dem 1,1fachen Dampfvolumen des Druckhalters bei Regelwasserstand entspricht. Dadurch gelangt bei Ansprechen der Abblase- oder Sicherheitsventile normalerweise kein Dampf aus dem Reaktorkühlkreislauf in den Sicherheitsbehälter. Vier Berstscheiben des Abblasetanks sind in der Lage, den bei Abblasen von Dampf aus dem

Druckhalter maximal möglichen Durchsatz der Druckhalter-Sicherheitsventile ohne Überschreitung des Auslegungsdruckes des Ablasetanks in den Sicherheitsbehälter abzuführen.

Die beiden eigenmedium-betätigten Abblaseventile 20 YP01 S025 und 20 YP01 S021 können mit Hilfe je eines magnetbetätigten Steuerventils (20 YP01 S125, 22 YP01 S121) geöffnet bzw. geschlossen werden. Die Abblaseventile arbeiten nach dem Belastungsprinzip, d.h., sie öffnen nach Aufbringen der Belastung durch den Steuerdampf. Zum Öffnen der als Steuerventile verwendeten Magnetventile 20 YP01 S125 und 20 YP02 S121 ist deren elektrische Energieversorgung notwendig. Bei Ausfall der Energieversorgung schließen diese Ventile durch Federkraft und damit auch die Abblaseventile. In den Steuerleitungen befindet sich außerdem je ein motorbetätigtes Steuer-Absperrventil (20 YP01 S050 und 20 YP01 S049), das bei normalem Leistungsbetrieb geöffnet ist und das neben den Steuerventilen zum Schließen der Steuerleitungen herangezogen werden kann. Jedem Abblaseventil ist ein Absperrventil (20 YP01 S024, 20 YP01 S020) vorgeschaltet, mit dessen Hilfe beim Probebetrieb die erforderlichen Ablasemengen eingestellt wurden und das eine zusätzliche Abschieberung der betreffenden Abblaseleitung ermöglicht. Die zuletzt genannten Ventile sind an notstromgesicherte Schienen angeschlossen.

Die Abblaseventile werden von der Kühlmitteldruckregelung angesteuert. Diese Regelung ist aus drei redundanten Strängen aufgebaut. Der Kühlmitteldruck wird in jedem der vier Hauptkühlkreisläufe einmal gemessen. Zur Regelung werden allerdings nur drei Meßkanäle verwendet, der vierte befindet sich in Reserve und läßt sich als Ersatz für einen ausgefallenen Meßkanal zuschalten. Die Meßumformer sind in einem innerhalb des Sicherheitsbehälters befindlichen Meßumformerraum untergebracht. Die drei analogen Meßwerte werden jeweils in einem Analog-Digital-Umsetzer digitalisiert und in dem nachgeschalteten Code-Umsetzer umgewandelt.

Die drei aktiven Meßkanäle werden durch gegenseitigen Vergleich sowohl der analogen als auch der digitalen Meßsignale überwacht.

Die Ausgangssignale einer der drei Code-Umsetzer werden zur Ziffernanzeige in der Warte herangezogen. Die Schaltsignale jedes Regelstranges werden aus der Verknüpfung der Ausgangssignale des Code-Umsetzers gebildet. Die Ansteuerung der beiden Abblaseventile erfolgt jeweils über eine 2v3-Auswahl der entsprechenden Schaltsignale der drei Regelungsstränge und über einen Speicher. Der Speicher wird gesetzt und damit über das Steuerventil das entsprechende Abblaseventil geöffnet, wenn ein Druck von 161 bar (1. Abblaseventil) oder ein Druck von 163 bar (2. Abblaseventil) erreicht wird. Das Löschen des Speichers und damit das Schließen der Ventile erfolgt bei Unterschreitung des Ansprechdrucks um 2 bar.

Die zwei eigenmedium-betätigten Sicherheitsventile 20 YP01 S010 und 20 YP02 S011 arbeiten nach dem Entlastungsprinzip, d.h., sie öffnen nach Wegnahme der Belastung des Ventilkolbens durch den Steuerdampf. Die Steuerung jedes Hauptventils erfolgt über zwei Steuerstränge. In jedem Steuerstrang sind zwei parallel angeordnete Steuerventile, bestehend aus Impulsventil und Steuerrückschlagventil, den entsprechenden Impuls- bzw. Steuerleitungen zugeordnet. Jedes Steuerventil besitzt ein vor- und nachgeschaltetes Hand-Absperrventil; die Absperrventile sind mechanisch so verriegelt, daß je Steuerstrang jeweils ein Steuerventil wirksam ist. Pro Hauptventil sind damit immer zwei Steuerventile betriebsbereit. Zur Erhöhung der Dichtkraft und zur besseren Einhaltung der Öffnungs- und Schließdrücke sind die Steuerventile (genau: die Impulsventile) mit einer magnetischen Zusatzbelastung ausgerüstet, die für beide Sicherheitsventile gleichzeitig bei Erreichen des höchstzulässigen Betriebsdrucks von 173 bar am Hauptkühlmittel-Druckstutzen weggeschaltet wird. Dieser Druck entspricht dem Ansprechdruck des 1. Sicherheitsventils von 166 bar. Der Grenzwert wird von Meßstellen des Reaktorschutzsystems abgeleitet. Ohne diesen Abwurf der Zusatzbelastung öffnen die Steuer- bzw. Hauptventile bei einem Druck, der ca. 20 % über dem Ansprechdruck liegt.

Eine ausreichende Diversität zwischen Abblase- und Sicherheitsventilen ist durch die unterschiedlichen Funktionsprinzipien und Bauarten sowohl der Hauptventile als auch der Steuereinrichtungen gegeben.

4.2.5 Volumenregelsystem

Das Volumenregelsystem hat die Aufgaben,

- den Reaktorkühlkreislauf mit Borwasser zu füllen,
- dem Reaktorkühlkreislauf laufend Hauptkühlmittel zur Reinigung zu entnehmen und dieses danach dem Reaktorkühlkreislauf wieder zuzuführen,
- die Volumenänderungen des Hauptkühlmittels auszugleichen,
- die zur chemischen Reaktivitätsregelung erforderlichen Borsäure- und Deionatmengen einzuspeisen,
- kleine Leckagen im Reaktorkühlsystem auszugleichen,
- die Hochdruck-Wellendichtungen der Hauptkühlmittelpumpen mit Sperrwasser zu versorgen,
- die Hilfssprühung im Druckhalter zu ermöglichen,
- den Reaktorkühlkreislauf bei wiederkehrenden Prüfungen abzudrücken.

Der Aufbau dieses Systems ist im einzelnen dem Schaltplan 5 (Anhang 1) zu entnehmen. Vereinfacht läßt sich das System folgendermaßen beschreiben: Dem Reaktorkühlkreislauf wird die Kühlmittelmenge vor der Hauptkühlmittelpumpe des Hauptkühlkreislaufs 2 entnommen und dem Rekuperativ-Wärmetauscher zugeführt. Bei einem Betriebsdruck von 155 bar wird das Kühlmittel zunächst von 295 °C auf 115 °C und anschließend in den HD-Kühlern auf 50 °C abgekühlt. Der maximale betriebliche Durchsatz beträgt 70 t/h. Nach den HD-Reduzierstationen wird das Kühlmittel außerhalb des Sicherheitsbehälters aufbereitet und dem Volumenausgleichsbehälter zugeführt. Der Systemdruck liegt hier bei 4 bar.

Die HD-Förderpumpen saugen aus dem Volumenausgleichsbehälter an. An die Ansaugleitung sind die Einspeiseleitungen für die Deionat-Borsäure-Dosierung angeschlossen. Von der Sammelleitung hinter den HD-Förderpumpen wird in den Rekuperativ-Wärmetauscher und über ein Dreiwegeventil in die vier Hauptkühlkreisläufe zurückgefördert. Über das Dreiwegeventil kann auch eine Hilfssprühung des Druckhalters vorgenommen werden. Die Sperrwasserleitung zur Versorgung der Hauptkühlmittelpumpen zweigt von der Sammelleitung hinter den HD-Förderpumpen ab.

Auf ein eventuelles Leck im Volumenregelsystem wird das Wartenpersonal durch mehrere Meldungen hingewiesen:

- Volumenausgleichsbehälter-Wasserstand tief,
- Leckageergänzung mit maximal 70 t/h und
- Entnahmemenge aus dem Reaktorkühlkreislauf tief.

Folgende Absperreinrichtungen sind im Volumenregelsystem vorhanden:

22 TA00 S001	Entnahmeschieber vor dem Rekuperativ-Wärmetauscher
23 TA30 S001 22 TA30 S025 22 TA40 S002 23 TA40 S001	Gebäudeabschlußarmaturen
22 TA50 S015 23 TA50 S016	Gebäudeabschlußarmaturen in den Sperrwasserleitungen für die Hauptkühlmittelpumpen
22 TA41 S007 22 TA42 S007	Druckschieber nach den HD-Förderpumpen

Bei einem Leck im Volumenregelsystem oder einer Fehlfunktion der Druckhalter-Wasserstandsregelung wird die Notgefahrmeldung DRUCKHALTER-WASSERSTAND GESTÖRT ausgelöst, sofern ein Wasserstand > 8,55 m bzw. < 3,48 m erreicht wird. Bei einem Druckhalterwasserstand < 2,85 m wird der Entnahmeschieber 22 TA00 S001 vor dem Rekuperativ-Wärmetauscher vom Reaktorschutzsignal YZ37 automatisch zugefahren. Die Druckschieber 20 TA41/42 S007 hinter den HD-Förderpumpen schließen bei einem Systemdruck im Reaktorkühlkreislauf < 120 bar.

Die Gebäudeabschlußarmaturen können von Hand zugefahren werden. Die Gebäudeabschlußsignale für das Volumenregelsystem YZ35, aufgrund dessen diese Ventile automatisch schließen würden, stehen an, wenn zumindest zwei der drei folgenden Bedingun-

gen erfüllt sind:

- Druckhalter-Wasserstand < 2,85 m,
- Druck im Reaktorkühlkreislauf < 110 bar,
- Druck in den Anlagen- oder Betriebsräumen des Sicherheitsbehälters > 30 mbar.

Die Gebäudeabschlußarmatur 23 TA40 S001 wird außerdem zugefahren, wenn es in der von den HD-Förderpumpen zum Rekuperativ-Wärmetauscher führenden Leitung zu einem Temperaturanstieg auf 100 °C kommt. Steigt wegen einer fehlerhaft arbeitenden Regelung die Kühlmitteltemperatur in der HD-Reduzierstation, so werden ebenfalls Absperrmaßnahmen eingeleitet, und zwar folgende Armaturen geschlossen:

20 TA30 S032	bei T_1 > 65 °C
20 TA21 S005	
20 TA22 S005	
20 TA21 S002	bei T_2 > 80 °C
20 TA22 S002	

Fehler in der HD-Reduzierstation könnten steigenden Leitungsdruck nach der Reduzierstation bedeuten und damit zu einer Drucküberlastung der nachfolgenden Rohrleitung führen. Deshalb werden ab einem Druck > 12 bar die hinter der Reduzierstation liegenden Ventile

20 TA21 S005
20 TA22 S005

automatisch zugefahren.

4.2.6 Hauptspeisewassersystem

Das Hauptspeisewassersystem hat die Aufgabe, bei Leistungsbetrieb des Kraftwerks die vier Dampferzeuger mit Speisewasser zu versorgen. Es beinhaltet die Hauptspeisewasser-Pumpen, die zuge-

hörigen Rohrleitungen zwischen dem Speisewasserbehälter und den Dampferzeugern sowie die dort installierten Armaturen (Schaltplan 6, Anhang 1). Im Normalbetrieb werden die Dampferzeuger durch die beiden Hauptspeisewasser-Pumpen 21 RL01 D001 und 22 RL02 D001 mit Speisewasser versorgt. Bei Ausfall einer der beiden Pumpen wird automatisch auf die Reservepumpe 23 RL03 D001 umgeschaltet.

Alle drei Pumpenaggregate sind konstruktiv gleich und für eine Nenn-Fördermenge von 3580 t/h bei einem Pumpendruck von 76,7 bar ausgelegt. Im Gegensatz zu den beiden Betriebsaggregaten fördert die Reservepumpe jedoch nicht durch die Hochdruck-Vorwärmer, was ein Absinken der Speisewasser-Endtemperatur um ca. 15 °C bewirkt und damit zu einer geringfügigen Abnahme der Generatorleistung führt. Hinter den beiden HD-Vorwärmern sind die drei Pumpenstränge vermascht, die sich dann in vier zu den einzelnen Dampferzeugern führende Hauptspeisewasserleitungen aufteilen. Durch die damit verbundene Vermischung des Hauptspeisewassers erreicht man eine gleiche Einspeisetemperatur in die vier Dampferzeuger. Zur Regelung des Hauptspeisewasser-Durchsatzes befinden sich in jeder der vier Hauptspeisewasserleitungen je ein Hauptspeisewasser-Regelventil (z.B. 20 RL11 S001), ein Schwachlast-Speisewasser-Regelventil (z.B. 24 RL12 S001) sowie die zugehörigen Absperrarmaturen.

Die Hauptspeisewasserregelung besitzt in jedem Strang zwei getrennte Regelkreise für die Betriebsbereiche "Hauptlast" und "Schwachlast". Dabei kommt die Hauptspeisewasserregelung "Hauptlast" bei einer Reaktorleistung von mehr als 25 % zum Einsatz, die Schwachlastregelung bei niedrigerer Reaktorleistung. Regelgröße beider Regelkreise ist der Dampferzeuger-Wasserstand, als weitere Einflußgrößen werden der Speisewasserdurchsatz und die abströmende Frischdampfmenge berücksichtigt. Beide Regelkreise verfügen über gemeinsame Meßwerterfassung und Sollwertgeber, haben jedoch eigene Regler und Stellglieder. Die Regelung kann von der Automatik SPEISEWASSERFÖRDERUNG oder von Hand ein- und abgeschaltet werden.

4.2.7 Notspeisewassersystem

Das Notspeisewassersystem 21 RL04 bis 24 RL07 (Schaltplan 7, Anhang 1) entspricht in seinem Gesamtkonzept dem viersträngigen Aufbau des Reaktorkühlkreislaufs. Es hat die Aufgabe, in allen Fällen, in denen das Hauptspeisewassersystem nicht zur Verfügung steht, Speisewasser in die Sekundärseite der Dampferzeuger zu fördern.

Jede der vier Notspeisewasser-Pumpen ist für eine Nennfördermenge von 110 t/h bei einem Pumpendruck von 92 bar ausgelegt. Dieser Pumpendruck ist erforderlich, um gegen den Ansprechdruck der Sicherheitsventile von 82,5 bar zuzüglich den Druckverlusten im System von 5,4 bar und der geodätischen Förderhöhe von 2 bar in die Dampferzeuger fördern zu können. Die Leitungen des Notspeisewassersystem sind saugseitig für 13 bar und 200 °C, druckseitig für 140 bar und 200 °C ausgelegt. Jede Notspeisewasser-Pumpe fördert das Wasser in separate Leitungsstränge, die über eigene Notspeisewasser-Regelventile verfügen. Stellantriebe für Regelventile sind für Aussetzbetrieb ausgelegt, und zwar für 600 Schaltungen pro Stunde bei 20 % Einschaltdauer.

Die Notspeisewasser-Regelung hat die Aufgabe, bei Ausfall oder Abschaltung der Hauptspeisewasserversorgung einen Mindestwasserstand in den Dampferzeugern zu halten und so ein Ausdampfen der Dampferzeuger zu verhindern. Die Notspeisewasser-Regelung ist strangweise getrennt aufgebaut. Regelgröße ist jeweils der Dampferzeuger-Wasserstand.

Um einen gleichzeitigen Ausfall mehrerer Stränge des Notspeisewassersystems zu verhindern, sind jeweils zwei Einspeiseleitungen zu den Dampferzeugern räumlich getrennt verlegt. Demgemäß sind auch die Notspeisewasser-Pumpen paarweise räumlich getrennt aufgestellt. Die Pumpen 21 RL04 D001 und 22 RL05 D001 stehen im Verbindungstrakt unterhalb der Deionatbehälter, die Pumpen 23 RL06 D001 und 24 RL07 D001 im Hilfsanlagengebäude. Die Druckleitungen der beiden Notspeisewasser-Pumpen im Hilfsanlagengebäude und der beiden Notspeisewasser-Pumpen im Verbindungstrakt

laufen im Abstand von jeweils 1-2 m nebeneinander bis zum Reaktorgebäude und werden von da aus getrennt zu den einzelnen Dampferzeugern geführt.

Bei den vier Notspeisewasser-Pumpen handelt es sich um mehrstufige Pumpen, die durch einen Elektromotor angetrieben werden. Jedes Pumpenaggregat besitzt eine Hilfsölpumpe, die bereits vor dem Anlaufen der Notspeisewasser-Pumpe gestartet wird und für den nötigen Öldruck sorgt. Die für den Betrieb der Notspeisewasser-Pumpen erforderlichen Hilfsaggregate werden je nach Aufstellungsort der Pumpen durch verschiedene Systeme gekühlt. Bei den im Hilfsanlagengebäude aufgestellten Pumpen der Redundanzen 3 und 4 werden die Motorluft-, Öl- und Stopfbuchsenkühlung durch den nuklearen Zwischenkühlkreislauf TF gewährleistet. Da der Verbindungstrakt nicht zum Kontrollbereich zählt, können die beiden dort aufgestellten Pumpen nicht von diesem System versorgt werden. Die Wärmeabfuhr aus den Motorkühlern dieser Pumpen wird daher vom Kaltwassersystem UZ 50/60 übernommen. Die Stopfbuchsen- und Ölkühlung läuft über den konventionellen Zwischenkühlkreis VG. Da dieses System nicht notstromgesichert ist, wird bei Eintritt des Notstromfalls auf das Deionatsystem RY umgeschaltet und von diesem die Kühlung übernommen.

In dem Notspeisewassersystem befinden sich alle Armaturen mit Motorantrieb oder Mediumsteuerung normalerweise bereits in der richtigen Stellung für den Einspeisebetrieb. Eine Ausnahme bilden die regelmäßigen Funktionsprüfungen, bei denen die Armaturen verfahren werden. An alle Armaturen mit Motorantrieb ergehen, nach Absinken des Wasserstandes in einem der vier Dampferzeuger auf 6,5 m, durch das Reaktorschutzsystem die Stellung kontrollierende Befehle. Für den Strang 21 RL04 (kurz: Strang 1) bedeutet das:

- Durch das Speisewassersignal YZ50 erhält der Notspeise-Pumpensaugschieber den Befehl 21 RL04 S019 AUF.
- Durch das Notspeisesignal YZ52 ergehen bei Absinken des Wasserstands im Dampferzeuger YB01 die Befehle

  Notspeise-Druckschieber 21 RL04 S005 AUF
  Notspeise-Regelventil 24 RL13 S003 AUF

Analoges gilt für die Stränge 2 bis 4.

Druckseitig ist zwischen den vier Notspeisewasser-Strängen eine Sammelleitung installiert. Diese ist jedoch im Normalbetrieb durch die vier Absperrschieber

21 RL04 S015
22 RL05 S015
23 RL06 S015
24 RL07 S015

geschlossen. Zweck dieser Verbindungsleitung ist es, auch bei Betrieb von weniger als vier Notspeisewasser-Pumpen die Möglichkeit zu haben, gleichmäßig in alle vier Dampferzeuger einspeisen zu können. Dazu sollen die Trennschieber nach Störfalleintritt von Hand verfahren werden. Diese Möglichkeit besteht aber nur, wenn die Notspeisezuschaltsignale YZ51, die bei einem Dampferzeuger-Wasserstand < 6,50 m ausgelöst werden, nicht anstehen. Von diesen Signalen erhalten die 4 Trennschieber nämlich einen Schließbefehl.

Die Förderung von Speisewasser zu einem Dampferzeuger mit gebrochener Speisewasserleitung wird, je nach Strang, durch die Absperrsignale YZ56 bis YZ59 verhindert. Für den Strang 1 werden dadurch folgende Befehle ausgegeben:

Notspeisewasser-Regelventil	24 RL13 S003	ZU
Notspeisewasser-Druckschieber	21 RL04 S005	ZU
Deionatschieber	21 RL04 S018	ZU

Das Absperrsignal für einen Strang wird gebildet durch eine UND-Verknüpfung des Grenzwertes

- Dampferzeuger-Wasserstand < 6,50 m für den betreffenden Strang

mit dem Grenzwert

- Differenz der Absolutdrücke zu zwei nicht benachbarten Speisewasserleitungen > 7 bar

oder mit dem Grenzwert

- Differenz der Durchsätze zu zwei nicht benachbarten Speisewasserleitungen > 20 t/h.

Ebenso wie die Hauptspeisewasser-Pumpen saugen auch die Notspeisewasser-Pumpen aus dem Speisewasserbehälter 20 RF50 B001 an. Sie verfügen nur über eine gemeinsame Saugleitung für alle vier Pumpen. Sie wird erst am Aufstellungsort der einzelnen Pumpen in separate Stränge aufgeteilt.

Beim normalen An- und Abfahren der Anlage sowie bei Störungen, bei denen die sekundärseitige Hauptwärmesenke zur Verfügung steht, wird die dem Speisewasserbehälter entnommene Wassermenge durch Nachspeisen von kaltem Kondensat (30 °C - 40 °C) ersetzt. Die Temperatur im Speisewasserbehälter sinkt auf 130 °C, der Druck auf 2 bar ab. Dieser Betriebszustand wird von der Stützdampf-Regelung aufrechterhalten.

Steht die sekundärseitige Wärmesenke dagegen nicht zur Verfügung, z.B. durch Ansprechen des Kondensatorschutzes im Notstromfall, so sind bei einer Anforderung des Notspeisewassersystems zwei Fälle zu unterscheiden:

- Speisewasserbehälter intakt, geregelter Wasserstand im Speisewasserbehälter (320 t) und in den Deionatbehältern (600 - 680 t).

Die vier Notspeisewasser-Pumpen und deren Hilfsölpumpen werden bei Ausfall aller 3 Hauptspeisewasser-Pumpen durch die Meldung LETZTE HAUPTSPEISEWASSER-PUMPE AUSGEFALLEN mittels einer betrieblichen Verriegelung gestartet. Laufen nicht alle Notspeisewasser-Pumpen an und werden die Trennschieber in der Notspeise-Sammelleitung nicht von Hand geöffnet, so ergehen nach ca. 7 Minuten durch die Notspeisezuschaltsignale YZ51 - ausgelöst durch den Dampferzeuger-Wasserstand < 6,5 m - erneute Startbefehle an alle Notspeisewasser- und Hilfsölpumpen. Die Trennschieber erhalten von diesen Reaktorschutzsignalen einen Schließbefehl.

Die einzelnen Notspeisewasser-Pumpen saugen, sofern die zugehörigen Notspeisewasser-Stränge nicht vom Reaktorschutzsystem abgesperrt wurden, das zunächst noch warme Speisewasser aus dem Speisewasserbehälter an. Ein Beheizen des Speisewasserbehälters

ist nur noch vorübergehend möglich. Das entnommene Speisewasser wird durch Einspeisen von kaltem Deionat ersetzt.

Sind mindestens zwei Stränge des Notspeisewassersystems intakt, so daß die Anlage abgefahren werden kann, so benötigen die Notspeisewasser-Pumpen ca. 500 t Wasser bis zur Übernahme der Wärmeabfuhr aus dem Reaktorkühlkreislauf durch das Not- und Nachkühlsystem. Bei Funktion nur eines Stranges des Notspeisewassersystems reicht die im Block B gespeicherte Speisewasser- und Deionatmenge von ca. 900 t für ca. 15 Stunden, um die Anlage auf Druck und Temperatur zu halten. Bei Ausfall des Speisewasserbehälters (siehe unten) steht für 10 Stunden ausreichend Deionat zur Verfügung.

- Direktes Ansaugen der Notspeisewasser-Pumpen aus den Deionatbehältern, geregelter Wasserstand in den Deionatbehältern (600 - 680 t)

Die Notspeisewasser-Pumpen müssen in allen Fällen, in denen der Wasserstand im Speisewasserbehälter auf den Abschaltgrenzwert von 0,2 m absinkt, auf direktes Ansaugen aus den Deionatbehältern umgeschaltet werden. Dieses Absinken des Wasserstandes kann seine Ursache in einem Leck im Speisewasserbehälter oder in einer Speisewasserleitung haben oder, falls die Notspeisewasser-Pumpen bis zu diesem Zeitpunkt bereits aus dem Speisewasserbehälter ansaugten, in einer ungenügenden Deionateinspeisung aus den Deionatbehältern.

In jedem Falle werden bei Erreichen des erwähnten Abschaltgrenzwertes von den Deionatsignalen YZ62-65 die Saugschieber RL04-07 S019 in der Leitung zum Speisewasserbehälter zugefahren, während die Deionatsaugschieber RL04-07 S018 die Stellung kontrollierende AUF-Befehle erhalten. Außerdem ergehen von den Deionatzuschaltsignalen YZ61 an die Armaturen 24 RY10 S002 und 22 RY10 S001 in der Deionatleitung zum Speisewasserbehälter ZU-Befehle. Die Notspeisewasser-Pumpen saugen somit direkt aus den Deionatbehältern, in denen sich eine Mindestreserve von 500 t befindet, kaltes Deionat an.

Herrscht zum Zeitpunkt des Umschaltens auf direkte Deionatversorgung im Speisewasserbehälter ein größerer Druck als 2 bar, so muß zunächst kaltes Deionat in die Saugleitung der Notspeisewasser-Pumpen eingespritzt werden. Dies ist notwendig, da sich in der Saugleitung noch 180 °C warmes Speisewasser befindet, das unter einem Druck von ca. 10 bar steht und nach dem Schließen des Notspeisewasser-Saugschiebers auszudampfen beginnt. Somit können die Rückschlagklappen RL04-07 S011 in den Saugleitungen zu den Deionatbehältern nicht öffnen, da der Druck in Schließrichtung größer ist als in Öffnungsrichtung (ca. 2,5 bar Zulaufdruck von den Deionatbehältern).

In den Notspeisewassersträngen RL04 und RL05 erfolgt das Einspritzen von kaltem Deionat mit den Deionat- und Druckerhöhungspumpen, in den anderen beiden Strängen mit den Einspritzpumpen 23 RL06 D003 und 24 RL07 D003.

Die EIN-Befehle an diese Pumpen werden durch die Deionatzuschaltsignale YZ61 ausgegeben. Von diesen Signalen erhalten außerdem die vier Einspritzventile 21 RY23 S004, 22 RY23 S003, 23 RL06 S033 und 24 RL07 S033 AUF-Befehle. Nach erfolgtem Druckausgleich und Öffnen der Rückschlagklappen RL04-07 S011 sind für die weitere Deionatversorgung der Notspeisewasser-Pumpen keine zusätzlichen Pumpen nötig.

4.2.8 Deionatsystem

Das Deionatsystem (Schaltplan 8, Anhang 1) dient im wesentlichen zur Speicherung von Wasser für Störungen, bei denen der Wasservorrat des Speisewasserbehälters nicht zur Verfügung steht. Außerdem werden vom Deionatsystem einige Systeme der Hilfs- und Nebenanlagen und des Sekundärkreises versorgt. Der Deionatvorrat wird in den beiden Deionatbehältern 20 RY00 B001/2 gespeichert, die untereinander verbunden sind. Da der Block B über keine Vollentsalzungsanlage verfügt, erfolgt die Versorgung der Deionatbehälter mittels der Zubringerpumpen 20 RY31/32 D001 aus den Deionatbehältern des Blocks A. Die Pumpen werden durch eine Automatik so ein- und ausgeschaltet, daß sich die gespeicherte Deionatmenge in jedem Behälter zwischen 308 m^3 und 384 m^3 bewegt. Sinkt der Wasserstand

in den Deionatbehältern, so wird bei Füllständen von 290 m^3, 283 m^3 und 259 m^3 jeweils eine Meldung auf die Warte gegeben. Bei Unterschreiten des Mindestwasserstands von 259 m^3 muß die Anlage abgefahren werden.

Die Deionatverbraucher werden durch drei Gruppen von jeweils zwei Pumpen versorgt:

- Deionatpumpen 20 RY21/22 D001

Die Deionatpumpen sind einstufige Pumpen mit Antrieb durch einen Elektromotor. Sie verfügen über tauchölgeschmierte Wälzlager und benötigen für ihren Betrieb keine weiteren Hilfsaggregate. Die Nennfördermenge beträgt 110 t/h bei einem Pumpendruck von 5,7 bar. Benötigt werden die Deionatpumpen für die Einspeisung in den Speisewasserbehälter, in den Kondensator sowie in die einzelnen Verbraucher der konventionellen Hilfs- und Nebenanlagen. Während im Normalbetrieb die einzuspeisenden Deionatmengen sehr gering sind (ca. 10 t/h), werden bei Kühlmittelverluststörfällen, bei denen zusätzlich ein Notstromfall vorliegt, oder bei Ausfall der Hauptspeisewasserversorgung bis zu 220 t/h gefördert.

- Deionat-Druckerhöhungspumpen 20 RY11/12 D001

Die Deionatdruckerhöhungspumpen entsprechen in ihrer Konzeption den Deionatpumpen. Sie sind für eine Fördermenge von 30 t/h bei einem Pumpendruck von 4,4 bar ausgelegt. Die Druckerhöhungspumpen werden in Verbindung mit den Deionatpumpen zur Einspeisung von Deionat in den Speisewasserbehälter benötigt, jedoch nur dann, wenn im Speisewasserbehälter ein Druck von mehr als 4,9 bar herrscht. Außerdem werden die Druckerhöhungspumpen gegebenenfalls zum Einspritzen von Deionat in die Saugleitungen der Notspeisestränge RL04 und RL05 benötigt.

- Sperrwasserpumpen 20 RY41/42 D001

Die Sperrwasserpumpen entsprechen in ihrer Konzeption ebenfalls den Deionatpumpen. Sie sind für eine Fördermenge von 2 t/h bei einem Druck von 9,1 bar ausgelegt. Ihre Aufgabe ist es, alle sicherheitstechnisch wichtigen Pumpen, die mit einer Gleitringdichtung versehen sind (wie z.B. die Nachkühlpumpen), mit Sperrwasser zu versorgen.

Alle Pumpen des Deionatsystems sind paarweise räumlich getrennt im Zwischentrakt aufgestellt. Die Leitungen des Deionatsystems sind zum größten Teil nur einsträngig ausgeführt. Der zwischen den Deionat-Druckerhöhungspumpen und dem Speisewasserbehälter liegende Abschnitt ist für einen Überdruck von 20 bar, der übrige Bereich für einen Überdruck von 10 bar ausgelegt.

Die Ansteuerung der Deionat- und Druckerhöhungspumpen unterscheidet sich je nach Betriebszustand und Anforderung. Im Normalbetrieb des Kraftwerks läuft ständig eine Deionatpumpe. Über eine Störumschaltung wird bei Ausfall dieser Pumpe automatisch die andere Deionatpumpe in Betrieb genommen.

Im Notstromfall ergeht durch eines der nullredundanten Notstromsignale ein EIN-Befehl an eine Deionatpumpe. Die zweite Deionatpumpe sowie die Druckerhöhungspumpen müssen laut Betriebshandbuch von Hand zugeschaltet werden. Die Druckerhöhungspumpen erhalten jedoch zusätzlich bei Unterschreiten des Speisewasserbehälter-Wasserstands von 1,75 m einen EIN-Befehl.

Beim Umschalten der Notspeisewasser-Pumpen auf direkte Deionatversorgung erhalten beide Deionat- und Druckerhöhungspumpen EIN-Befehle durch die nullredundanten Deionatzuschaltsignale YZ61. Diese Signale werden bei Absinken des Wasserstandes im Speisewasserbehälter auf einen Wert von < 0,2 m ausgegeben. Beide Druckerhöhungspumpen werden nach Unterschreiten eines Druckes von 5 bar im Speisewasserbehälter über eine Druckmessung abgeschaltet.

Im Deionatsystem werden die meisten Armaturen mit Motorantrieb von Reaktorschutzsignalen angesteuert. So geben die Deionatzuschaltsignale YZ61 die folgenden Befehle aus:

Zulauf Speisewasserbehälter	22 RY10 S001	ZU
	24 RY10 S002	ZU
Einspritzventile	21 RY23 S004	AUF
	22 RY23 S003	AUF
	23 RL06 S033	AUF
	24 RL07 S033	AUF

Von den Deionatsignalen YZ62 bis YZ65 werden in den Notspeisewasser-Saugleitungen die Saugschieber angesteuert. Für den Strang 21 RL04 werden folgende Befehle ausgegeben:

Deionatzulauf zur Notspeisewasser-Pumpe	21 RL04 S018	AUF
Notspeisewasser-Saugschieber	21 RL04 S019	ZU

An die Saugschieber in den Deionatleitungen ergehen außerdem durch die Notspeisezuschaltsignale YZ51 AUF-Befehle. Folgende Armaturen erhalten von den Notstromvorbereitungssignalen YZ81 einen ZU-Befehl:

- die Trennschieber 23 RY00 S004 und 24 RY00 S003 in der Verbindungsleitung der Deionatbehälter sowie
- die Armaturen 22 RY20 S004 und 21 RY20 S002 in der Deionatleitung zum Kondensator.

4.2.9 Notstandssystem

Das Notstandssystem (Schaltplan 9, Anhang 1) wurde eingerichtet, um die Anlage bei Zerstörungen in größeren Bereichen, wie sie bei Einwirkungen von außen unterstellt werden, in einen sicheren Zustand überführen zu können. Dazu muß das Notstandssystem die Wärmeabfuhr des abgeschalteten Reaktors übernehmen. Im Falle der Referenzanlage, die zur 2-Block-Anlage des Kernkraftwerks Biblis gehört, kann von Block A aus, selbst wenn bei diesem der Notstromfall gegeben ist, noch die Abfuhr der Nachzerfallswärme des Blocks B sichergestellt werden. Dementsprechend ist das Notstandssystem so aufgebaut, daß bei Funktion von 3 der 4 Notspeisewasser-Stränge des "Notstromblocks" dieser bis zur Übernahme der Wärmeabfuhr durch das Nachkühlsystem abgefahren werden kann, während der "Notstandsblock" ca. 10 Stunden im Zustand unterkritisch heiß gehalten wird.

Zur Abfuhr der Nachzerfallswärme des "Notstandsblocks" muß Speisewasser in die Sekundärseite der Dampferzeuger gefördert werden. Dies geschieht über eine gemeinsame Notstands-Einspeiseleitung, die vom Ringraum eines Blocks über einen unter der Erde verlegten Rohrkanal zum Ringraum des anderen Blocks führt. Maximal

zwei Notspeisewasser-Pumpen fördern Speisewasser zu zwei Dampferzeugern des anderen Blocks. Um eine möglichst gleichmäßige Temperaturverteilung und Durchmischung des Bors im Kern zu erreichen, wird die Notstandseinspeisung in zwei diagonal gegenüberliegende Dampferzeuger vorgenommen. Befindet sich der Block B im Notstand, so sind das die Dampferzeuger 20 YB01/03 B001.

Zur Notstand-Speisewasserförderung werden im Block A die elektrisch betriebenen Notspeisewasser-Pumpen 12 RL05 D001 und 14 RL06 D001 herangezogen. Ein entsprechender Betrieb beider Pumpen ist jedoch nach dem Betriebshandbuch nur dann zulässig, wenn sich die beiden turbinengetriebenen Notspeisewasser-Pumpen 11 RL04 D001 und 13 RL 07 D001 im betriebsbereiten Zustand befinden. Die Verwendung dieser Pumpen zur Notstands-Speisewasserförderung ist nicht vorgesehen.

Vor der Zusammenführung zur gemeinsamen Leitung befindet sich in den beiden Notspeisewasser-Rohrleitungsabzweigen des Blocks A jeweils eine Handabsperrarmatur 10 RX10 S001/2, die im Normalbetrieb geschlossen ist und im Notstandsfall vor Ort von Hand geöffnet werden muß. Ebenso ist in jeder Notstands-Einspeiseleitung vor den Dampferzeugern eine Absperrarmatur. Diese Stellventile 22 RX20 S005 und 23 RX20 S006 sind jedoch von der Notstandstafel des Blocks A aus steuerbar. Zusätzlich zu diesen Stellventilen befinden sich in den Einspeiseleitungen noch die Rückschlagklappen 20 RX20 S003 und 20 RX20 S004.

Die Dampferzeuger-Wasserstände werden von Hand von der Notstandstafel des nicht im Notstand befindlichen Blocks A aus geregelt. Auf der Notstandstafel wird zu diesem Zweck der Speisewasserdruck und der Wasserstand in den beiden Dampferzeugern angezeigt.

Das Notstandssystem kann auch dann zur Notspeisewasser-Versorgung eines Blockes herangezogen werden, wenn in ihm die Speisewasser- und Notspeisewasser-Versorgung ausgefallen ist, aber kein Störfall "Notstand" vorliegt.

4.2.10 Frischdampfsystem

Entsprechend dem Notspeisewassersystem ist auch das Frischdampfsystem viersträngig aufgebaut (Schaltplan 10, Anhang 1), wobei jeweils 2 Frischdampfleitungen von den Dampferzeugern bis zu den Frischdampf-Schnellschlußschiebern räumlich getrennt verlegt sind. Der Frischdampf (FD) am Dampferzeugeraustritt hat bei Vollast der Anlage einen Druck von 54 bar. Die anfallende Frischdampfmenge beträgt dabei insgesamt 7159 t/h. Ein Druckausgleich in allen Leitungen und damit gleiche Frischdampfdrücke vor den kombinierten Schnellschluß-Regelventilen der Turbine werden durch eine Ausgleichsleitung, den Frischdampfsammler, ermöglicht. In jeder Frischdampfleitung befinden sich vor dem Abzweig zum Frischdampfsammler ein Sicherheitsventil 20 RA01-04 S001 und ein Frischdampf-Schnellschlußschieber 20 RA01-04 S002.

Die hilfsgesteuerten, eigenmediumbetätigten Sicherheitsventile, bestehend aus je einem Hauptventil, 3 federbelasteten Steuerventilen mit pneumatischer Zusatzbelastung und einem Steuergerät, sprechen bei einem Druck von 82,5 bar an und sind in der Lage, die bei Vollast erzeugte Frischdampfmenge in die Atmosphäre abzublasen. Erfolgt eine Reaktorschnellabschaltung, so kann die durch die Nachwärme erzeugte Frischdampfmenge über 1v4 FD-Sicherheitsventile abgegeben werden.

Zum Öffnen der Hauptventile müssen jeweils mindestens 1v3 Steuerventile ansprechen. Die Hauptventile öffnen dabei durch Beaufschlagung des Ventilkolbens mit Steuerdampf (Belastungsprinzip). Die auf die Kolben der Steuerventile wirkende pneumatische Zusatzbelastung dient der Erhöhung der Dichtkraft der Steuerkegel und der Einhaltung genauer Öffnungs- und Schließdrücke. Das Weg- bzw. Zuschalten der Zusatzbelastung wird durch den Frischdampfdruck über ein Steuergerät gesteuert, das hinsichtlich Wegschalten 3fach redundant aufgebaut ist. Wird beim Ansprechdruck der FD-Sicherheitsventile die Zusatzbelastung nicht weggeschaltet, so öffnen die Steuer- und damit auch die Hauptventile bei einem Frischdampfdruck, der ca. 20 % über dem normalen Ansprechdruck liegt. Umgekehrt schließen Steuer- und Hauptventile verzögert,

wenn die Zusatzbelastung nicht aufgebaut werden kann. Für Instandhaltungsmaßnahmen kann jeweils ein Steuerventil außer Betrieb genommen werden. Durch eine mechanische Verriegelungsschiene wird gewährleistet, daß immer mindestens zwei Steuerventile betriebsbereit sind.

Die Frischdampf-Schnellschlußschieber 20 RA01-04 S002 haben die Aufgabe, bei schnellen Druckabsenkungen im Speisewasser-Dampf-Kreislauf, z.B. bei Rohrleitungsbrüchen oder Fehlansprechen eines Sicherheitsventils, die Frischdampfleitungen in maximal 5 Sekunden abzuschiebern und damit auch untereinander zu trennen. Die Schieber werden durch vom Eigenmedium angetriebene Kolben betätigt. Bei einem Schnellschluß wird der im ungestörten Leistungsbetrieb von beiden Seiten mit Frischdampf beaufschlagte Kolben auf seiner Unterseite druckentlastet und bewegt sich durch den entstandenen Druckunterschied in Schließrichtung. Die Druckentlastung wird durch das Öffnen von zwei redundanten Magnetventilen, die von den Reaktorschutzsignalen YZ60 angesteuert werden, erreicht. Die zusätzliche Möglichkeit, die Frischdampf-Schnellschlußschieber durch den Motorantrieb zu schließen, ist im Notstromfall nicht vorhanden, da diese Antriebe an nicht notstromgesicherte Schienen angeschlossen sind.

Zum Abfahren der Anlage muß der Frischdampfdruck geregelt abgesenkt werden. Der Frischdampf wird dazu über die Frischdampf-Umleiteinrichtung direkt in den Kondensator abgegeben. Die Frischdampf-Umleiteinrichtung besteht im wesentlichen aus kombinierten Umleitregelventilen und Umleitschnellschlußschiebern. Steht die Umleiteinrichtung nach Turbinenschnellabschaltung oder der Kondensator nicht zur Verfügung, z.B. bei Ansprechen des Kondensatorschutzes im Notstromfall, so muß die beim Abfahren anfallende Dampfmenge mit den Abblaseregelventilen über Dach abgeblasen werden. Diese Ventile (22 RA11 S001 und 24 RA12 S001) stehen über vier Leitungsstränge, in denen sich je ein Absperrschieber befindet, mit den Frischdampfleitungen in Verbindung. Sie sind in der Lage, bei vollständig offener Stellung und bei einem Druck von 82,5 bar vor dem Ventil, zusammen 2560 t/h abzublasen. Abblaseventile und Absperrschieber sind im Leistungsbetrieb geschlossen. Beim Abfahren mit dem bei Kühlmittelverluststörfällen

("kleines Leck") erforderlichen Abfahrgradienten von 100 °C/h müssen die Umleitregelventile bzw. bei Abblasen über Dach die Abblaseregelventile und die Absperrschieber von Hand gefahren werden. Ohne Handeingriffe wird bei funktionierendem Kondensator der Frischdampfdruck entsprechend dem Teillastdiagramm auf ca. 76,5 bar gehalten. Steht dagegen der Kondensator nicht zur Verfügung, so wird der Frischdampfdruck durch die Sicherheitsventile auf 82,5 bar begrenzt.

4.2.11 Kaltwassersystem

Das Kaltwassersystem UZ50 bis UZ90 (Schaltplan 11, Anhang 1) hat die Aufgabe, sicherheitstechnisch wichtige Komponenten, wie die vier Notstromdiesel, die zugehörigen Transformatoren sowie die Antriebe von zwei der vier Notspeisewasser-Pumpen mit Kühlwasser zu versorgen. Das Teilsystem UZ70 dient speziell der Versorgung des Abgassystems TS. Aus Sicherheitsgründen kann dieses System zusätzlich von den Kaltwassersträngen UZ50 und UZ90 mit Kühlwasser versorgt werden. Die übrigen Anlagen des Kaltwassersystems (UZ01 und UZ02) sind nur für die betriebliche Verfügbarkeit der Anlage von Bedeutung.

Das Kaltwassersystem UZ50/60/80/90 ist wie die anderen Sicherheitssysteme viersträngig aufgebaut. Die erforderliche Kälteleistung wird durch vier gleichgroße Turbokaltwassersätze 20 UZ50/60/80/90 D011 mit einer Leistung von je 1,15 Gcal/h erbracht. Die Vorlauftemperatur des Wassers beträgt 6 °C, die Rücklauftemperatur in Abhängigkeit vom Leistungsbedarf bis 12 °C. Alle vier Kältemaschinen sind im Verbindungstrakt aufgestellt, wobei jeweils zwei Anlagen in einem Raum untergebracht sind.

Jede der Maschinen verfügt über drei Ölpumpen, die vom Kompressor direkt angetrieben werden, sowie eine elektrische Hilfsölpumpe, die sicherstellt, daß beim Anfahren alle Schmierstellen mit Öl versorgt werden. Die Antriebsmotoren und die Kondensatoren werden vom nuklearen Nebenkühlwassersystem gekühlt. Die Temperatur des Kondensatorkühlmediums wird im Winter auf mindestens

15 °C begrenzt. Den Kältemaschinen sind die Kaltwasserpumpen 20 UZ50/60/80/90 D001 zugeordnet. Sie übernehmen die Kaltwasserförderung.

Zwei der vier Kaltwassersätze sind ständig in Betrieb. Die beiden anderen werden durch "Vorkühlung" mittels UZ10 betriebsbereit gehalten.

Im Notstromfall werden in jeder der vier Redundanzen des Kaltwassersystems der Turbokaltwassersatz, die Kaltwasserumwälzpumpe und die zugehörige Hilfsölpumpe mittels einer betrieblichen Teilsteuerung durch die nullredundanten Notstromsignale YZ82 bis YZ85 gestartet.

Bei Störfällen, bei denen das Notstromvorbereitungssignal YZ81 ausgelöst wird, ergehen in der ersten Redundanz an diese Komponenten folgende Befehle:

21 UZ50 D001 EIN
21 UZ50 D011 EIN
21 UZ50 D012 EIN

Zur Inbetriebnahme der Kaltwassersysteme UZ50 bis UZ90 müssen keine Motorarmaturen verfahren werden.

4.2.12 Lüftungsanlagen

Eine Aufgabe der lufttechnischen Anlagen (Schaltplan 12, Anhang 1) im Kernkraftwerk ist es, bei Störfällen in wichtigen Räumen die Einhaltung bestimmter Raumlufttemperaturen zu gewährleisten, d.h. im allgemeinen ein Ansteigen über zulässige Werte zu verhindern.

Es werden im folgenden nur die Lüftungsanlagen im nuklearen und konventionellen Bereich untersucht, deren Ausfall zum Versagen von zur Störfallbeherrschung benötigten Komponenten durch Überschreiten der Auslegungstemperatur führen kann.

- Umluftanlage Notstromdiesel

In jedem der vier Dieselräume ist eine Umluftanlage, bestehend aus einem Kühler und einem Ventilator, angeordnet.

Über diese Anlage wird die bei Betrieb des Dieselmotors an die Raumluft abgegebene Wärme an das Kaltwassersystem der jeweiligen Redundanz abgeführt. Die Stromversorgung erfolgt von einer notstromgesicherten Schiene der entsprechenden Redundanz.

Die Anlagen werden sowohl über Raumthermostate als auch über die Meldung DIESELGENERATOR EIN eingeschaltet, ferner erhalten bei Ausgabe der Notstromvorbereitungssignale YZ81 alle Ventilatoren einen EIN-Befehl.

Bei Ausfall des Kaltwassersystems in einer Redundanz kann durch Öffnen der Türen zu den benachbarten Dieselräumen ein Überschreiten kritischer Temperaturen verhindert werden, wenn die Umluftanlagen in anderen Dieselräumen intakt sind. Werden die Türen nicht - oder nicht rechtzeitig - geöffnet, oder fällt mehr als eine Umluftanlage aus, so ist nach kurzer Zeit mit einem Ausfall der nicht ausreichend gekühlten Dieselaggregate zu rechnen. Bei der Analyse wurde das Öffnen der Türen nicht berücksichtigt.

- Umluftanlage in den Räumen der nuklearen Zwischenkühlpumpen

In den Räumen der nuklearen Zwischenkühlpumpen sind neben diesen auch noch die HD-Sicherheitseinspeisepumpen und die Gebäudesprühpumpen aufgestellt. Im Normalbetrieb werden die Räume durch die Zu- und Fortluftanlage belüftet. Im Notstromfall und bei Gebäudeabschluß, wenn diese Frischluftkühlung ausfällt, sind bei Betrieb der Komponenten Umluftkühlanlagen in den vier Räumen zur Kühlung vorgesehen. Jede Anlage besteht aus einem Ventilator mit vorgeschaltetem Kühler. Die Wärme wird an den Zwischenkühlstrang der entsprechenden Redundanz abgeführt. Die Einschaltung der Ventilatoren erfolgt über Raumthermostate und außerdem von den Notstromvorbereitungssignalen der entsprechen-

den Redundanz. Auch bei der Versorgung der Ventilatorantriebe mit elektrischer Energie liegt diese Trennung nach Redundanzen vor.

Die einzelnen Räume sind nach oben und zum Ringraum hin offen, so daß sie lüftungstechnisch miteinander in Verbindung stehen. Bei Versagen einer der Anlagen könnte die Kühlung dieses Raumes durch die Anlagen der Nachbarräume übernommen werden.

Wie neuere Detailuntersuchungen des Herstellers über die Kühlung der Zwischenkühlpumpe ergaben, ist die Umluftanlage zur Sicherstellung der Funktion des Motors nicht erforderlich. Es wurde unterstellt, daß die Umluftanlage jedoch bei Betrieb der HD-Sicherheitseinspeisepumpe benötigt wird.

4.2.13 Gebäudeabschluß

Bei Kernkraftwerken mit Druckwasserreaktor stellen der Sicherheitsbehälter und die Stahlbetonhülle den äußeren Sicherheitseinschluß dar.

Der Sicherheitsbehälter ist als druckfeste und gasdichte Stahlkugel mit einem Durchmesser von 56 m ausgebildet. Er umschließt den gesamten Primärkreis einschließlich der Dampferzeuger. Im unteren Bereich ist die Stahlhülle in die Fundamentplatte und das daran anschließende kalottenförmig ausgebildete Stahlbetonringbauwerk eingebettet. Oberhalb eines Durchmessers von ca. 45 m steht die Stahlhülle freitragend.

Die Stahlbetonhülle von 100 cm Wandstärke schützt die Anlage gegen Einwirkungen von außen. Sie ist im unteren und mittleren Bereich zylinderförmig ausgebildet und folgt im oberen Bereich mit einem Abstand von ca. 1,5 m der Kugelform der Sicherheitshülle. Sie ist nur gegen geringfügige Druckdifferenzen ausgelegt und nicht absolut dicht. Der Raum zwischen dem Sicherheitsbehälter und der Stahlbetonhülle wird als Ringraum bezeichnet. Im Sicherheitsbehälter sind u.a. das gesamte Reaktorkühl- und Druckhalte-

system, Teile der unmittelbar damit im Zusammenhang stehenden nuklearen Hilfsanlagen und das Brennelementbecken angeordnet. Der Innenraum des Sicherheitsbehälters ist in die bei Betrieb des Reaktors nicht begehbaren Anlagenräume und in die bedingt begehbaren bzw. begehbaren Betriebsräume unterteilt.

Im Ringraum sind u.a. wesentliche Teile des Not- und Nachkühlsystems einschließlich der Borwasserbehälter, das Gebäudesprühsystem, das Beckenkühlsystem, der Kühler und Umwälzpumpen des nuklearen Zwischenkühlsystems, die HD-Förderpumpen des Volumenregelsystems und die Ölversorgung der Hauptkühlmittelpumpen aufgestellt.

Während des Reaktorbetriebs ist das Betreten des Sicherheitsbehälters nur über die Personenschleuse oder die Materialschleuse möglich. Die Notschleuse, die in der Nähe der Materialschleuse angeordnet ist, soll bei Störfällen einen möglichst kurzen Fluchtweg aus dem Sicherheitsbehälter sicherstellen.

Zum Betrieb der Systeme im Innern muß durch die Stahlhülle eine Reihe von Rohrleitungen, Lüftungsleitungen und Kabeln geführt werden. Die Rohrdurchführungen sind mit der Stahlhülle verschweißt. Die Durchführungsstutzen der Lüftungsleitungen haben Flansche, auf die die Absperrklappen aufgesetzt sind. Die Leitungs-, Steuer- und Meßkabel werden durch spezielle Kabeldurchführungselemente geführt, die auf die Stahlhülle geflanscht und mit einer Ringdichtung abgedichtet sind. Der Bemessung der Stahlhülle und der Durchdringungen mit den zugehörigen Abschlußorganen wurden die Unfallbedingungen beim Auslegungsstörfall (5,7 bar Druck und 143°C Temperatur des Sattdampf-Luftgemisches im Sicherheitsbehälters) zugrunde gelegt. Die maximal zulässige Leckrate des Sicherheitsbehälters beträgt 0,25 Vol.-%/Tag, bezogen auf den Auslegungsdruck und das freie Volumen des Sicherheitsbehälters.

Im Normalbetrieb wird gegenüber dem Atmosphärendruck im Ringraum ein Unterdruck von 10 mm WS, in den Betriebsräumen ein Unterdruck von 15 mm WS, in den bedingt begehbaren Räumen ein Unterdruck von 20 mm WS und in den Anlagenräumen ein Unterdruck von

25 mm WS aufrechterhalten. Aufgrund dieses Druckgefälles verlaufen eventuelle Leckagen stets von außen nach innen und können kontrolliert über Filter abgegeben werden. Außerdem können so zusammen mit der Drucküberwachung im Sicherheitsbehälter größere Leckagen vom Ringraum in den Sicherheitsbehälter erkannt werden.

Bei Störfällen ist es Aufgabe des Sicherheitsbehälters, Aktivitäten, die möglicherweise in das Innere des Sicherheitsbehälters freigesetzt werden, zurückzuhalten und dadurch die Freisetzung in die Umgebung des Kraftwerkes zu verhindern. Um einen Abschluß des Sicherheitsbehälters zu gewährleisten, sind alle Rohrleitungen, die durch die Stahlhülle führen, mit Absperrarmaturen versehen. Bei Eintritt eines Störfalls erhalten die Absperrarmaturen aller Rohrleitungen, die zur Beherrschung des Störfalls nicht benötigt werden, Schließbefehle vom Reaktorschutzsystem, wenn zwei der drei folgenden Kriterien anstehen:

- Druckhalter-Wasserstand < 2,85 m,
- Differenzdruck Anlagenräume gegen Atmosphäre > 30 mbar
  oder Differenzdruck Betriebsräume gegen Atmosphäre > 30 mbar,
- Reaktorkühlkreislaufdruck < 110 bar.

Die Signale zum Abschluß des Reaktorkühlkreislaufes YZ37 werden allein vom Druckhalter-Wasserstand in einer 2v4-Wertung abgeleitet.

Aufgrund der zulässigen Leckrate des Sicherheitsbehälters kann es bei Störfällen zu einer geringfügigen Freisetzung von radioaktiven Stoffen kommen.

Zur weiteren Verringerung dieser Freisetzung sind das Leckabsaugesystem und die Ringraumabsaugung vorgesehen. Mit dem Leckabsaugesystem, das für die spezifizierte Leckrate des Sicherheitsbehälters von 0,25 Vol.-%/Tag ausgelegt ist, werden mögliche Leckagen an einer Reihe wichtiger Durchführungen (Schleusendichtungen, temperatur- und druckbeanspruchte Rohrleitungen) erfaßt und in den Sicherheitsbehälter zurückgepumpt. Dadurch wird die effektive Leckrate des Sicherheitsbehälters gesenkt.

Die Ringraumabsaugung hat die Aufgabe, geringe Leckagen aus dem Sicherheitsbehälter, die nicht durch das Leckabsaugesystem zurückgefördert werden, zu erfassen und kontrolliert über Filter und Kamin abzugeben. Dazu werden auf Anregung aus dem Reaktorschutz die Zu- und Abluftklappen der Ringraumlüftung geschlossen und mit den Ventilatoren der Absauganlage im Ringraum ein Unterdruck gegenüber der Außenatmosphäre aufgebaut. Die abgesaugte Luft wird nach Filterung durch Aerosol- und Jodfilter über den Kamin abgegeben.

Im Rahmen der Zuverlässigkeitsanalyse des Gebäudeabschlusses sind die Möglichkeiten von Leckagen des Sicherheitsbehälters bei Störfällen und Unfällen zu untersuchen. Solche Leckagen können an den Durchdringungen der Stahlkugel wie auch an der Stahlkugel selbst auftreten. Für die Untersuchungen ist es zweckmäßig, zu unterscheiden zwischen Leckagen, die bei Versagen passiver Komponenten auftreten, und Leckagen, die bei Versagen aktiver Komponenten auftreten. Unter passiven Komponenten werden dabei die Stahlkugel, die Schweißnähte und Dichtungen der Durchführungen, die Schleusen usw. zusammengefaßt. Hierauf wird im folgenden Punkt "passive Komponenten" näher eingegangen.

Unter "aktiven Komponenten" werden die Gebäudeabschlußarmaturen der Rohrleitungen, die durch die Stahlkugel führen, verstanden. Die entsprechenden Systeme werden im Punkt "Systeme mit aktiven Gebäudeabschlußarmaturen" im einzelnen beschrieben.

- Passive Komponenten

- Rohrleitungsdurchführungen

  Für Rohrleitungsdurchführungen sind Stutzen in den Sicherheitsbehälter eingeschweißt. Leitungen, die im Durchführungsstutzen ihren Festpunkt haben, sind in den Stutzendeckel fest eingeschweißt. Bei Rohrleitungen, die temperaturbedingte Bewegungen gegenüber dem Sicherheitsbehälter ausführen können, wird die Verbindung zwischen Rohrleitung und Stutzen mit einem Stahlkompensator bzw. durch eine Balgkonstruktion herge-

stellt. Die entsprechenden Abkammerungen werden vom Leckabsaugesystem abgesaugt.

Die Durchführungsstutzen der Lüftungsleitungen haben Flansche, auf die die Abschlußklappen aufgesetzt sind. Die Räume zwischen den Abschlußklappen werden im Störfall vom Leckabsaugesystem abgesaugt.

- Kabeldurchführungen

  Die Leitungs-, Steuer- und Meßkabel sind mit speziellen Kabeldurchführungselementen durch die Stahlhülle geführt. Diese Durchführungselemente sind auf das Material der Stahlhülle geflanscht und mit einer Metallringdichtung abgedichtet. Die Leitungen selbst sind gegen das Metall durch Druckglas-Einschmelzung abgedichtet und isoliert. Bei einem Druckaufbau im Sicherheitsbehälter wirken die Druckkräfte zusätzlich als Dichtkräfte auf den Dichtring.

- Reservedurchführungen

  Zum Nachrüsten oder Erweitern von Systemen im Sicherheitsbehälter sind Reservedurchführungen vorhanden. Für Rohrleitungen sind Stutzen in den Sicherheitsbehälter eingeschweißt und auf der Innenseite mit einem geschweißten oder - bei Lüftungsleitungen - geschraubten Deckel verschlossen. Nicht benutzte Kabeldurchführungen sind durch Blindflansche verschlossen.

- Schleusen

  Zum Materialtransport und für den Zutritt von Personen sind in die Stahlhülle Schleusen eingeschweißt. Die Abdichtung der Schleusentore besteht aus zwei Dichtringen im Schleusentor, die beim Schließen des Tores gegen die Dichtfläche am Schleusenkörper gepreßt werden. Der Ringspalt zwischen den beiden Dichtungen ist an das Leckabsaugesystem angeschlossen. Da die beiden Tore einer Schleuse in den Innenraum des Sicherheitsbehälters hinein öffnen, wirken bei einem Druckaufbau im Sicherheitsbehälter die Druckkräfte zusätzlich als Dichtkräfte.

Die Materialschleuse führt vom Innern des Sicherheitsbehälters in den Ringraum vor das Hauptportal. Bei Schleusvorgängen ist immer ein Tor geschlossen, bei Normalbetrieb sind beide Tore geschlossen. Die Materialschleuse ist in die Abdeckung einer größeren Montageöffnung eingelassen, die im Bedarfsfall dem Auswechseln von Großkomponenten dient.

Die Personenschleuse führt in das Hilfsanlagengebäude. Über Ausgleichsventile ist beim Schleusvorgang eine Anpassung des Druckes im Schleuseninnenraum an den Druck im Hilfsanlagengebäude bzw. im Sicherheitsbehälter möglich. Außer bei Schleusvorgängen sind die innere Tür und das entsprechende Druckausgleichsventil stets geöffnet. Dadurch herrschen auch bei Störfällen mit einem Druckaufbau im Sicherheitsbehälter im Innenraum der Schleuse die gleichen Druckverhältnisse wie im Sicherheitsbehälter.

Die Notschleuse führt in den Ringraum. Ihre Türen werden von Hand betätigt. Um jederzeit ein Verlassen des Sicherheitsbehälters sicherzustellen, erfolgt der Betrieb der Innentür wie bei der Personenschleuse. Es sind ebenfalls Druckausgleichsventile eingebaut.

Im Rahmen der Risikostudie werden die Innentüren der Personen- und Notschleuse als offen angenommen.

- Systeme mit aktiven Gebäudeabschlußarmaturen

- Lüftung

Die Lüftungsanlagen des Kontrollbereiches haben folgende Aufgaben:

- Einhaltung vorgegebener Raumlufttemperaturen und -feuchtigkeiten,
- Einhaltung vorgegebener Unterdrücke,
- Schutz des Personals vor Strahlenbelastung durch radioaktiv verunreinigte Luft und Begrenzung der Abgabe von radioaktiven Stoffen mit der Fortluft aus dem Kamin in die Kraftwerksumgebung.

Im folgenden werden von den umfangreichen Anlagen nur die behandelt, die mit Leitungen durch die Stahlhülle führen. Es sind dies folgende Leitungen:

- Unterdruckhaltung
  Zuluft
  Abluft
- Spülluft
  Zuluft
  Abluft

- Luftaktivitätsmessung

Bei Normalbetrieb werden den Betriebsräumen im Sicherheitsbehälter über die Unterdruckhaltung ca. 1000 m^3/h Luft zugeführt. Diese Luftmenge strömt aus den Betriebsräumen in die Anlagenräume und in die beschränkt begehbaren Räume und wird von dort durch die Abluftleitungen abgesaugt. Durch Regelung der Zu- und Abluftmengen in den einzelnen Raumbereichen werden die zuvor aufgeführten Drücke und Druckdifferenzen eingehalten.

Sollen die bedingt begehbaren Räume vor einem Betreten belüftet werden, so kann durch Öffnen der Einströmöffnungen (von Hand) die aus den Betriebsräumen angesaugte Luftmenge vergrößert werden. Zusätzlich kann die Förderleistung der Unterdruckhaltung durch Zuschalten der Reserveventilatoren erhöht werden.

Die Zuluft- und die Abluftleitung der Unterdruckhaltung werden als Stahlrohre mit einem Auslegungsdruck von 10 bar durch den Ringraum geführt. In diesen Leitungen befinden sich je 3 Abschlußklappen (1 innerhalb des Sicherheitsbehälters und 2 außerhalb). Je eine der außerhalb des Sicherheitsbehälters angeordneten Abschlußklappen wird durch einen Motorantrieb betätigt. Bei den übrigen Abschlußklappen handelt es sich um Schnellschlußklappen, die pneumatisch in Offenstellung gehalten und durch ein Fallgewicht geschlossen werden. Bei Störfällen erhalten alle Klappen durch die Reaktorschutzsignale Gebäudeabschluß für lufttechnische Anlagen YZ32 einen ZU-Befehl.

Bevor die Anlagenräume im Sicherheitsbehälter nach dem Abschalten des Reaktors betreten werden dürfen, muß zuerst eine Spülung durch Frischluft vorgenommen werden. Dazu wird die Zuluftmenge durch Öffnen der Spül-Zuluftleitungen erhöht. Die Spül-Abluft wird gefiltert über den Kamin abgegeben.

Im Normalbetrieb sind je 2 Schnellschlußklappen in den Spülluftleitungen geschlossen. Die Stellung wird in der Warte angezeigt. Die Klappen erhalten zusätzlich einen Schließbefehl bei Ausgabe der Reaktorschutzsignale YZ32. Ein Öffnen der Klappen ist ohne weitere Maßnahmen erst möglich, wenn Druck und Temperatur im Primärkreis unterhalb bestimmter Werte liegen.

Die Lüftungskanäle der Unterdruckhalter und der Spülluft sind zwischen den Sicherheitsbehälter-Absperrarmaturen gasdicht geschweißt und mit einem Auslegungsdruck von 10 bar ausgeführt.

Die Lüftungsklappen sind so ausgelegt, daß sich in geschlossener Stellung ein gas- und druckdichter Abschluß der Lüftungsleitungen ergibt. Zusätzlich wird der Raum zwischen den geschlossenen Klappen vom Leckabsaugesystem abgesaugt.

Zu den Aufgaben der lufttechnischen Anlagen gehört auch die Messung der Luftaktivität. Mit zwei Ventilatoren wird über insgesamt 7 Meßluftstränge aus Räumen im Sicherheitsbehälter, im Ringraum, im Hilfsanlagengebäude und aus dem Kamin Luft angesaugt und über Meßstrecken geleitet. Drei der sieben Stränge führen durch den Sicherheitsbehälter in Anlagenräume, in begehbare und bedingt begehbare Betriebsräume. Jede dieser Meßleitungen ist durch zwei hintereinander liegende Armaturen absperrbar, die von den Reaktorschutzsignalen Gebäudeabschluß für lufttechnische Anlagen YZ32 einen Schließbefehl erhalten. Die weiteren Stränge der Luftaktivitätsmeßanlage bleiben weiterhin in Betrieb. Bis auf die Durchführungen durch den Sicherheitsbehälter einschließlich der Absperrarmaturen sind alle Leitungen der Aktivitätsmeßanlage als Kunststoffschläuche ausgeführt.

Die elektrische Energieversorgung der genannten Abschlußarmaturen der Lüftungsanlage erfolgt notstromgesichert. Mindestens eine der hintereinander liegenden Abschlußarmaturen ist

dabei den unterbrechungsfrei versorgten Schienen zugeordnet. Die Schnellschlußklappen in der Zu- und Abluftleitung der Unterdruckhaltung sowie in den Spülluftleitungen sind darüber hinaus so konzipiert, daß sie bei Ausfall ihrer elektrischen Energieversorgung automatisch geschlossen werden.

- Volumenregelsystem

  Das Volumenregelsystem wird im einzelnen in Abschnitt 4.2.5 behandelt. Hier soll nur kurz auf die für den Gebäudeabschluß wesentlichen Betriebsarten des Volumenregelsystems und die zahlreichen Verbindungen zu anderen Systemen eingegangen werden.

  Das dem Hauptkühlkreislauf entnommene Kühlmittel wird so abgekühlt und im Druck reduziert, daß beim Eintritt in den Volumenausgleichsbehälter dessen Auslegungswerte (6 bar, 100 °C) nicht überschritten werden. Zur Druckabsicherung ist ein Sicherheitsventil mit einem Ansprechdruck von 6 bar eingebaut. Abhängig vom Niveau im Volumenausgleichsbehälter werden die Armaturen zur Kühlmittellagerung geöffnet und Kühlmittel zurückgegeben bzw. entnommen. Die Kühlmittellagerbehälter sind auf einen Druck von 3 bar ausgelegt.

  Die HD-Förderpumpen speisen nach Bedarf Kühlmittel über den Rekuperativ-Wärmetauscher in den Kühlkreislauf ein. Eine zweite Einspeiseleitung führt direkt in zwei Hauptkühlkreisläufe. Sie wird bei Ausfall des Einspeisewegs über den Rekuperativ-Wärmetauscher benutzt.

  Die Entnahme- und Einspeiseleitungen können durch je zwei Armaturen abgesperrt werden. Die Armaturen sind unmittelbar hinter den Durchführungen des Sicherheitsbehälters außenliegend eingebaut. Bei Anstehen der Reaktorschutzsignale Gebäudeabschluß für das Volumenregelsystem YZ35 erhalten die Armaturen einen Schließbefehl.

- Gebäudeentwässerungssystem

  Die Gebäudeentwässerung hat die Aufgabe, alles frei in den Sicherheitsbehälter ausfließende Wasser in Sümpfen zu sammeln und von dort in die Abwasseraufbereitung abzuführen. Aus den

Pumpensümpfen wird das Wasser von den Sumpfpumpen in die Abwassersammelbehälter gefördert. Die Pumpen werden durch Schwimmerschalter ein- und ausgeschaltet.

Die Leitungen des Gebäudeentwässerungssystems und die entsprechenden Leitungen des Abwassersystems bestehen - bis auf ein Stück im Durchtritt durch die Stahlhülle - aus Polypropylen. Dieses Material kann Belastungen von 1-3 bar Überdruck und einer Temperatur von ca. 120 °C mehrere Tage standhalten.

Die vier Abwassersammelbehälter, die im Hilfsanlagengebäude stehen, haben einen Inhalt von je 50 m^3 und sind auf einen Überdruck von 0,5 bar ausgelegt. Das Erreichen des maximalen Füllstandes wird auf der Warte gemeldet, gleichzeitig läuft das Abwasser in den jeweils nächsten Behälter über. Erst wenn alle vier Behälter gefüllt sind, läuft das Abwasser in den als dichte Wanne ausgebildeten unteren Teil des Raumes. Die Wanne kann nochmals 50 m^3 aufnehmen.

Die Sammelleitung von den Sümpfen innerhalb des Sicherheitsbehälters hat eine Nennweite von 100 mm. Sie ist im Normalbetrieb offen und durch zwei hintereinander geschaltete Armaturen unmittelbar nach Durchgang durch die Stahlhülle absperrbar. Die Armaturen erhalten von den Reaktorschutzsignalen Gebäudeabschluß allgemein YZ33 einen Schließbefehl.

Zusätzlich zu den Gebäudeabschlußarmaturen kann die Sammelleitung der Gebäudeentwässerung durch eine Motorarmatur unmittelbar vor den Abwassersammelbehältern von der Warte aus ferngesteuert abgesperrt werden. Diese Armatur ist an eine nicht notstromgesicherte Schiene angeschlossen.

- Abgassystem

Die Abgasanlage hat die Aufgabe, in allen Komponenten, in denen Wasserstoff oder Spaltgase auftreten können, einen Unterdruck zu halten, die anfallenden aktiven Gase nach ausreichender Abklingzeit kontrolliert abzuführen sowie den Wasserstoffgehalt im System zu begrenzen. An den Unterdruckteil, in dem durch einen Kompressor ein Druck von 0,8 bar gehalten wird, sind sämtliche Komponenten der Hilfs- und Nebenanlagen angeschlossen, in denen aus dem Hauptkühlmittel Spaltgase und

Wasserstoff ausgasen können (Druckhalter-Abblasetank, Kühlmittelspeicher, Volumenausgleichsbehälter, Borsäurebehälter usw.). Der abgesaugte Gasstrom wird durch eine Rekombinatoranlage und eine Verzögerungsstrecke geleitet und anschließend je nach anfallender Gasmenge über eine Reduzierstation wieder in den Unterdruckteil zurückgeführt bzw. teilweise über Kamin abgegeben. Im Normalbetrieb kann das System weitgehend geschlossen betrieben werden, da der überwiegend anfallende Wasserstoff im Rekombinator verbrannt wird, d.h. die Abgaben über den Kamin sind gering. Steigt jedoch der Druck am Ende der Verzögerungsstrecke, wird die Kaminabgabe automatisch erhöht und die Rückführung in den Unterdruckteil vermindert.

Innerhalb des Sicherheitsbehälters wird der Druckhalter-Abblasetank vom Abgassystem gespült. In der Zu- und Ableitung sind je zwei Absperrarmaturen angeordnet, die von den Reaktorschutzsignalen Gebäudeabschluß allgemein YZ33 einen Schließbefehl erhalten.

- Gebäudesprühsystem

Das Gebäudesprühsystem hat bei einem Störfall mit Kühlmittelverlust die Aufgabe, radioaktive Spaltprodukte (vor allem Jod) aus der Sicherheitsbehälteratmosphäre auszuwaschen. Es kann von Hand eingeschaltet werden, wenn der Druck im Sicherheitsbehälter über 1,5 bar liegt und das Notkühlsystem auf Sumpfbetrieb umgeschaltet ist. Dazu werden die beiden Sicherheitsbehälter-Absperrarmaturen in jeder Sprühleitung, die normal geschlossen sind, geöffnet und die Pumpen eingeschaltet. Jedem Borwasser-Flutbehälter ist eine Sprühpumpe zugeordnet, je zwei Pumpen speisen in eine Sprühleitung.

Bei Absinken des Sprühdruckes unter 1 bar werden die Pumpen abgeschaltet und die Gebäudeabschlußarmaturen in den Sprühleitungen geschlossen. Der Druck von 1 bar zum Abschalten der Pumpe wird auch dann erreicht, wenn im Sicherheitsbehälter der volle Störfalldruck herrscht.

Der effektive Querschnitt der Sprühleitung wird nicht durch die Nennweite der Rohrleitung bzw. der Armaturen bestimmt, sondern durch die Sprühdüsen im Sicherheitsbehälter. Es läßt

sich abschätzen, daß er etwa 10 cm^2 beträgt, das entspricht einem effektiven Rohrdurchmesser von ca. 35 mm.

- Elektrische Energieversorgung und Ansteuerung der aktiven Gebäudeabschlußarmaturen

  Die Gebäudeabschlußarmaturen werden - bis auf einige Lüftungsklappen - durch Motorantrieb geschlossen. Diese Motoren werden von notstromdieselgesicherten bzw. von unterbrechungslos versorgten Schienen mit elektrischer Energie versorgt. Mindestens eine von zwei hintereinander liegenden Abschlußarmaturen ist dabei unterbrechungslos versorgten Schienen zugeordnet.

  Folgende Signale werden zum Schließen der Absperreinrichtungen des Sicherheitsbehälters vom Reaktorschutz ausgegeben:

  · Mit den Gebäudeabschlußsignalen für die lufttechnischen Anlagen YZ32 werden die Absperrklappen der nuklearen Lüftungsanlagen geschlossen.

  · Von den allgemeinen Gebäudeabschlußsignalen YZ33 werden die Sicherheitsbehälter-Absperrschieber der nuklearen Hilfssysteme geschlossen.

  · Mit den Signalen YZ35 und YZ37 erhalten die Gebäudeabsperrarmaturen des Volumenregelsystems und des Reaktorkühlkreislaufs einen Schließbefehl.

  Die Meßwerterfassung und -verarbeitung zur Bildung dieser Reaktorschutzsignale wird in Abschnitt 4.4.1 behandelt. Sie ist bei den Signalen YZ35 bis auf die Abschlußglieder völlig identisch mit den Notkühlvorbereitungssignalen YZ31. Mit Ausnahme einer Handüberbrückung gilt dies auch für die Signale YZ32, YZ33 und YZ34.

  Ob und nach welcher Zeit die physikalischen Bedingungen für das Ansprechen der Reaktorschutz-Grenzwerte zur Ausgabe der Gebäudeabschlußsignale vorliegen, wird bei den Abläufen der jeweiligen Störfälle behandelt.

4.3 Elektrische Energieversorgung

4.3.1 Generator und Eigenbedarfsanlage

Bei Leistungsbetrieb des Kraftwerks speist der Turbogenerator über die Generatorableitung 20 AP04 die beiden Maschinentransformatoren (Schaltplan 13, Anhang 1). Der Maschinentransformator 20 AT01 ist an die 220-kV-Ebene des Verbundnetzes angeschlossen, der Maschinentransformator 20 AT02 an die 380-kV-Ebene (zweigeteilter Hauptnetzanschluß).

Die für den Eigenbedarf des Kraftwerks benötigte elektrische Energie wird über einen Abzweig in der Generatorableitung und über zwei Eigenbedarfstransformatoren 20 BT01 und 20 BT02 den vier 10-kV-Blockschienen 20 BA, 20 BB, 20 BC und 20 BD zugeführt. Außerdem besteht die Möglichkeit, die 10-kV-Blockschienen der Blöcke A und B zu verbinden. Diese Verbindungen sind für eine Leistung von jeweils 3 MW ausgelegt. An jede 10-kV-Blockschiene ist über eine Kabelverbindung mit zwei Leistungsschaltern eine 10-kV-Notstromschiene angeschlossen.

Falls die Turbine abgeschaltet wird, geht der Generator nach einigen Sekunden in Motorbetrieb über und durch den Rückleistungsschutz wird mit einer Zeitverzögerung von 2 Sekunden der Generatorschalter 20 AP03 H001 geöffnet. Dadurch kann die Eigenbedarfsversorgung unterbrechungslos durch das Verbundnetz übernommen werden. Wenn diese Übernahme nicht gelingt oder die Versorgung durch das Netz ausfällt, liegt ein Notstromfall vor.

4.3.2 Notstromanlagen

Die für die Sicherheit eines Kraftwerks wichtigen Verbraucher sind an Notstromanlagen anzuschließen. Dies müssen insbesondere die Verbraucher sein, die erforderlich sind, um den Reaktor sicher abzuschalten, im abgeschalteten Zustand zu halten, die Nachwärme abzuführen und eine unzulässige Freisetzung radioaktiver Stoffe zu verhindern.

Schaltplan 14, (Anhang 1) zeigt den Aufbau der Notstromanlagen. Die 10-kV-Notstromschienen 21 BU, 22 BV, 23 BW, 24 BX werden normalerweise von der Eigenbedarfsanlage aus versorgt. Bei Anstehen der Notstromsignale YZ82-85 (Abschnitt 4.4) werden die Verbindungen zwischen den 10-kV-Blockschienen und den 10-kV-Notstromschienen sowie die Einspeiseschalter der 380-V-Notstromschienen geöffnet, und die Notstromdiesel 21 EY10 bis 24 EY40 übernehmen nach ihrem Hochlauf die Versorgung der zugeordneten Notstromschienen entsprechend dem Notstromzuschaltprogramm.

An jede 10-kV-Notstromschiene sind über Transformatoren zwei 380-V-Notstromschienen angeschlossen. Eine der beiden 380-V-Schienen einer Redundanz, z.B. 21 FU, ist nicht kuppelbar, d.h., sie kann nur von der zugehörigen 10-kV-Schiene 21 BU aus versorgt werden. Die andere 380-V-Schiene einer Redundanz ist kuppelbar. Eine Kupplung ist zwischen den Schienen 21 EU und 24 EX möglich sowie zwischen den Schienen 22 EV und 23 EW. Der Kuppelschalter wird geschlossen, wenn der Einspeiseschalter einer kuppelbaren Schiene nicht schließt und keine Schalterfallmeldung des Einspeiseschalters ansteht. Die Schalterfallmeldung wird abgefragt, um eine Überlastung der nicht ausgefallenen Schiene zu verhindern. Von den kuppelbaren 380-V-Schienen 22 EV bzw. 24 EX wird die Schiene 20 ES versorgt, wobei beim Ausfall einer der beiden kuppelbaren Notstromschienen automatisch auf die andere umgeschaltet wird.

Über Gleichrichter werden durch jeweils zwei nicht kuppelbare 380-V-Notstromschienen die batteriegepufferten 220-V-Gleichstromschienen 20 EA und 20 EB redundant versorgt. Entsprechendes gilt für die ebenfalls batteriegepufferten 24-V-Gleichstromschienen 20 FJ und 20 FH. Außerdem sind noch weitere Schienen vorhanden, die von den genannten Gleichstromschienen gespeist werden. An die 220-V-Gleichstromschienen sind auch die rotierenden Umformer für die unterbrechungslose Drehstromversorgung angeschlossen. Es sind drei unterbrechungslose 380-V-Drehstromschienen - 20 EM, 20 EN, 20 EP - vorhanden, denen je ein Umformer zugeordnet ist. Ein vierter Umformer dient als Reserve.

Wenn nur zwei der vier 24-V-Batterien zur Verfügung stehen, ergibt sich ohne Nachladung durch die Gleichrichter eine Versorgungszeit von ca. 1 1/2 Stunden, bei vier funktionsfähigen 24-V-Batterien kann von der doppelten Entladezeit ausgegangen werden. Bei nur zwei zur Verfügung stehenden 220-V-Batterien können die von den Umformern versorgten Gebäudeabschlußarmaturen bis ca. 50 Minuten nach Ausfall aller Gleichrichtereinspeisungen geschlossen werden. Bei Funktion aller vier 220-V-Batterien beträgt die entsprechende Zeit ca. 3 Stunden.

Die Notstandsschienen 21 FR10, 22 FR20, 23 FR30, 24 FR40 werden normalerweise von der entsprechenden nicht kuppelbaren 380-V-Notstromschiene versorgt. Fällt diese Einspeisung aus, so wird mit einer Zeitverzögerung von 50 Sekunden automatisch auf die unterbrechungslose Drehstromschiene 10 ES des Blocks A umgeschaltet.

Die Umschaltung der genannten Notstandsschienen auf Versorgung vom stützenden Block A wird auf der Notstandstafel in Block A gemeldet. Die Umschaltung und damit die Meldung ist verzögert, um ein mehrmaliges Ansprechen bei Testbetrieb zu unterbinden. Ausfälle der Notstromversorgung und damit auch ein CMA der Dieselanlage werden direkt zur Betriebsmannschaft des ungestörten Blockes gemeldet.

Bei den Notstandsschienen 20 FR80 und 20 FR90, die normalerweise an die gesicherten Drehstromschienen 20 EN bzw. 20 EP angeschlossen sind, wird diese Umschaltung auf die Schiene 10 ES des Blocks A mit einer Zeitverzögerung von 1 Sekunde ausgeführt.

Die Gleichstromversorgung für das Notstandssystem erfolgt über die batteriegepufferten 24-V-Schienen 20 FS10 und 20 FS20. Die Gleichrichter dieser Schienen werden aus den Notstandsschienen 21 FR10 bis 24 FR40 gespeist.

Die vier Redundanzen der Notstromanlagen sind grundsätzlich jeweils voneinander räumlich getrennt. Die Notstromdiesel sind in getrennten Räumen des Schaltanlagengebäudes aufgestellt. Das gleiche gilt für die vier Redundanzen der Notstromschaltanlagen,

wobei sich die Redundanzen 1 und 4 in einem anderen Stockwerk des Schaltanlagengebäudes befinden als die Redundanzen 2 und 3. Die Kabeltrassen für die vier Redundanzen sind in unterschiedlichen Räumen verlegt oder voneinander abgemauert bzw. geschottet.

4.3.3 Zuordnung der Verbraucher zu den Sammelschienen

Sicherheitstechnisch wichtige Verbraucher, für die eine kurzzeitige Unterbrechung der Energieversorgung zulässig ist, sind je nach ihrer Leistungsaufnahme an die 10-kV- oder 380-V-Notstromschienen angeschlossen.

Die 220-V-Gleichstromschienen sind für die Steuerspannungsversorgung der Leistungsschalter erforderlich, die 24-V-Gleichstromschienen für die elektronische Steuerung. Jede Schaltanlage bzw. jede Gruppe von Steuerschränken ist an zwei redundante Gleichstromschienen angeschlossen, wobei die beiden Einspeisungen jeweils über Dioden entkoppelt werden. An die unterbrechungslosen 380-V-Drehstromschienen sind die Verbraucher angeschlossen, für die eine kurzzeitige Unterbrechung der Energieversorgung nicht zulässig ist oder für die eine besonders zuverlässige Stromversorgung erforderlich ist.

4.3.4 Verbraucherabzweige

Die einzelnen Verbraucher sind über Abzweige an die Sammelschienen angeschlossen. Die Verbraucherabzweige sind in Einschubtechnik ausgeführt, wobei jeder Abzweig aus einem Einschub besteht. Dieser beinhaltet das Hauptschaltgerät sowie die zu dessen Betätigung notwendigen Hilfsgeräte (220-V-Steuerung). Die mechanischen Schaltgeräte eines Abzweiges werden über Koppelschütze angesteuert. Die Koppelschütze werden zu den Verbraucherabzweigen gezählt.

Die Abzweige für Kühlwasserpumpen besitzen einen Leistungsschalter als Hauptschaltgerät. Die verschiedenen Schienen unterein-

ander sind ebenfalls über Leistungsschalter verbunden. Hilfsantriebe wie Fettpressen oder Ölpumpen werden über Abzweige mit einem Schütz als Hauptschaltgerät versorgt. Bei den Einschüben für Motorarmaturen mit einer Leistungsaufnahme bis zu 7,5 kW werden die Hauptschaltgeräte direkt durch die Simatic-Steuerung betätigt.

Die 10-kV-Abzweige sind mit Leistungsschaltern mit Motorantrieb ausgestattet. Der Motorantrieb betätigt den Leistungsschalter nicht direkt, sondern spannt die Federkraftspeicher für das Ein- und Ausschalten. Die Federkraftspeicher werden beide nach jedem Ausschalten des Leistungsschalters gespannt. Sowohl für den Motorantrieb als auch zur Auslösung des Leistungsschalters wird die 220-V-Steuerspannung (Gleichstrom) benötigt. Der Leistungsschalter ist durch ein Hilfsschütz gegen fälschliches Schließen verriegelt. Wenn dieses Hilfsschütz nach einem Ausschalten des Leistungsschalters fälschlicherweise nicht abfällt, kann dieser nicht wieder geschlossen werden. Das gleiche gilt für das AUS-Koppelschütz.

Das Schließen eines Niederspannungs-Leistungsschalters geschieht durch einen Elektromotor. Beim Schließen wird gleichzeitig der Federkraftspeicher für das Öffnen vorgespannt. Zum Ansteuern des Elektromotors ist außer dem EIN-Koppelschütz noch ein weiteres Schütz notwendig. Wenn eines der beiden Schütze nicht schließt, wird der Leistungsschalter nicht geschlossen. Der Leistungsschalter kann auch dann nicht geschlossen werden, wenn ein Schaden am Motor oder am Antrieb vorliegt. Falls der Motor beim Erreichen der Endstellung des Leistungsschalters wegen eines Fehlers am Steuerschütz nicht ausgeschaltet wird, so schaltet der zugehörige Sicherungsautomat ab. Dieser Fehler ist unkritisch, da er gemeldet wird und der Leistungsschalter trotzdem geschlossen wird.

4.3.5 Kurzschlußschutz

Sämtliche elektrischen Verbraucher einschließlich der Sammelschienen sind gegen Kurzschlußströme abgesichert. Bei den Hilfs-

antrieben und den Antrieben für Motorarmaturen sind hierfür Schmelzsicherungen eingesetzt. Für mehrere Verbraucherabzweige dieser Art ist zusätzlich eine gemeinsame Gruppensicherung vorhanden. Bei den Verbraucherabzweigen für Pumpenmotoren bis 150 kW sind ebenfalls Schmelzsicherungen eingebaut, bei höheren Nennleistungen der Motoren ist ein elektromagnetischer Kurzschlußauslöser vorhanden, bei dessen Ansprechen der Leistungsschalter des Abzweiges öffnet.

Die Einspeiseschalter der 380-V- und 10-kV-Sammelschienen besitzen kurzverzögerte elektromagnetische Kurzschlußauslöser. Dadurch wird erreicht, daß bei einem Kurzschluß in einem Verbraucher nur der zugehörige Kurzschlußschutz anspricht, nicht jedoch der Einspeiseschalter der Sammelschiene öffnet. Letzteres geschieht jedoch dann, wenn der Kurzschlußschutz eines Verbrauchers bei Anforderung nicht oder nicht schnell genug anspricht (verschleppter Kurzschluß).

Die Auslösezeiten der Kurzschlußauslöser der Sammelschienen für 380 V und 10 kV sind gestaffelt. Das gleiche gilt für die Einspeiseschalter und den Kuppelschalter eines Paares kuppelbarer 380-V-Drehstromschienen. Für die Schienen 21 EU und 24 EX liegen die Auslösezeiten folgendermaßen:

Einspeiseschalter:	0,35	Sekunden
Kuppelschalter :	0,2	Sekunden

Entsprechendes gilt für die Schienen 22 EV und 23 EW.

4.3.6 Notstromdiesel

Eine Diesel-Notstromerzeugungsanlage (Notstromdiesel) besteht aus einem Diesel-Aggregat und den Hilfssystemen. Zum Start bzw. Betrieb eines Notstromdiesels sind folgende äußeren Systeme erforderlich:

- Raumbelüftung,
- äußerer Kühlkreislauf,

- Stromversorgung der Hilfsantriebe und der Leittechnik,
- Reaktorschutzsystem.

Die folgende Beschreibung bezieht sich auf den Notstromdiesel 21 EY10 D001.

- Dieselaggregat

Die eingesetzten Dieselmotoren können dauernd eine Leistung von 3383 kW bei 1500 U/min (Leistung B nach DIN 6270) abgeben. Motoren dieser Baureihe sind in größerer Stückzahl für Schiffs- und Lokomotivantriebe im Einsatz.

Die Generatoren mit einer Scheinleistung von 3900 kVA sind Drehstrom-Konstantspannungs-Synchron-Generatoren. Der jedem Generator zugeordnete Entregungsschalter wird nur bei Störungen des Notstromaggregats betätigt und erhält außerdem zur Kontrolle einen AUS-Befehl vom Notstromsignal YZ82. Zur Auferregung wird die Erregerwicklung jedes Notstromgenerators während des Startvorganges kurzzeitig an die 220-V-Gleichstromversorgung geschaltet.

Der interne Kühlwasserkreislauf des Dieselmotors wird über einen Wärmetauscher aus dem Nebenkühlwassersystem rückgekühlt. Es wird davon ausgegangen, daß ein Versagen dieser Rückkühlung kurzzeitig zu einem Ausfall des Dieselmotors führt.

Durch die Vorheizung wird das Wasser des internen Kühlkreislaufs des Dieselmotors auf einer Temperatur zwischen 45 °C und 55 °C gehalten.

Beim Ausfall der Vorheizung während der Bereitschaftsphase wird eine Notgefahrmeldung abgegeben. Bei Erreichen der Zünddrehzahl wird die Vorheizung abgeschaltet. Der laufende Dieselmotor wird bei eingeschalteter Vorheizung nicht beschädigt.

Die Abstrahlungswärme der Dieselmotoren und die Verlustleistung der Generatoren werden über eine Umluftanlage und das Kaltwassersystem an das Nebenkühlwassersystem abgeführt.

- Kraftstoff- und Ölversorgung

Jedem Dieselmotor ist ein Kraftstoff-Betriebsbehälter zugeordnet. Unterschreiten des minimalen Füllstandes im Betriebsbehälter löst eine Notgefahrmeldung aus. Mit dem Inhalt des gefüllten Tagesbehälters kann ein Diesel drei bis vier Stunden betrieben werden.

Zur Inbetriebnahme des Dieselmotors brauchen innerhalb der Kraftstoffversorgung keine motorgetriebenen Armaturen oder Pumpen betätigt zu werden. In der Leitung vom Betriebsbehälter zum Dieselmotor befindet sich ein handbetätigtes Absperrventil, das bei Arbeiten am Dieselmotor ein Leerlaufen der Kraftstoffleitung verhindert. Dieses Ventil ist in Offenstellung zu verriegeln.

Der Abstellmagnet sperrt bei Erregung die Kraftstoffzufuhr. Nach dem Abstellen des Diesels wird der Abstellmagnet zeitverzögert entregt, eine falsche Stellung wird am entsprechenden Tischfeld gemeldet. Außerdem erhält der Abstellmagnet durch das Notstromsignal YZ82 einen vorrangigen Kontrollbefehl.

Der Dieselmotor besitzt eine elektrisch getriebene Dauervorschmierpumpe. Zu niedriger Schmieröldruck während der Bereitschaftsphase führt zu einer Notgefahrmeldung. Die Dauervorschmierpumpe wird bei Erreichen der Zünddrehzahl abgeschaltet. Die elektrisch getriebene Anlaßvorschmierpumpe dient als zusätzliche Sicherheit, um den Betriebsöldruck schneller zu erreichen.

- Anlaßeinrichtung

Zum Starten des Dieselmotors wird durch das Anlaßventil 21 EY10 S001 (Magnetventil) Druckluft auf 8 der 16 Zylinder geschaltet. Die Betätigungsspule des Anlaßventils ist über ein Schütz an die 220-V-Gleichstromversorgung des Dieselschranks angeschlossen.

Die Druckluft wird den für jeden Diesel vorhandenen zwei parallelgeschalteten Flaschen entnommen. Der Druck in den Flaschen

wird ständig überwacht; Unterschreiten des Wertes von 28 bar in einer der Flaschen löst eine Notgefahrmeldung aus. Zur Aufrechterhaltung des Drucks in den Flaschen sind zwei elektrisch getriebene Kompressoren vorhanden, an die über Rückschlagventile jeweils vier Druckluftflaschen angeschlossen sind. Jeder Kompressor versorgt dabei eine Druckluftflasche aller Diesel. Beim Unterschreiten eines Druckes von 35 bar in einer der angeschlossenen Flaschen wird ein Kompressor automatisch gestartet und bei einem Druck von 40 bar in allen zugehörigen Flaschen wieder abgeschaltet. Die Handabsperrarmaturen an den Druckluftflaschen sind in Offenstellung zu verriegeln. Zur Entwässerung ist an jedem Kompressor ein automatisches Ablaßventil angebaut. Darüber hinaus ist in der Leitung von den Druckluftflaschen zum Dieselmotor an der tiefsten Stelle ein Entwässerungsventil angebracht.

- Ansaugluft- und Abgasanlage

Es wird vorausgesetzt, daß die Ansaugluft- und Abgasanlage die Zuverlässigkeit des Notstromaggregates nicht beeinflußt.

- Gleichstromversorgung

Zum Anlassen eines Dieselaggregates ist die 24-V-Gleichstromversorgung für die elektronische Steuerung und das Reaktorschutzsystem erforderlich sowie die 220-V-Gleichstromversorgung im Dieselschrank zur Betätigung des Startventils. Dabei stehen für die Gleichstromversorgungen nur die Batterien zur Verfügung.

Die 220-V-Gleichstromversorgung im Dieselschrank wird diodenentkoppelt aus den Schienen 20 EA und 20 EB gespeist. Vor den Dioden wird die Spannung beider Einspeisungen ständig überwacht. Der Ausfall einer der beiden Einspeisungen führt zu einer Notgefahrmeldung. Eine praktische Bedeutung für den Ausfall der 220-V-Gleichstromversorgung des Startventils haben deshalb nur Ausfälle von Klemmverbindungen innerhalb des Dieselschranks.

4.3.7 Zuschaltung des Notstromdiesels und der Verbraucher

Die Notstromdiesel gehen in Betrieb, sobald die Spannung an den Notstromschienen länger als 1 Sekunde 80 % des Nennwerts unterschreitet. Die zum Start benötigten Hilfssysteme werden durch die Notstromsignale YZ82 bis YZ85 angesteuert. Sechs Sekunden nach Eintritt des Notstromfalls schließen die Einspeiseschalter der Generatoren.

Bei Spannungswiederkehr werden die notstromgesicherten Verbraucher gemäß dem Notstromzuschaltprogramm zugeschaltet. Ein gleichzeitiges Zuschalten aller Verbraucher führt zu einer Überlastung der Notstromdiesel. Das Notstromzuschaltprogramm läuft deshalb in sieben zeitlich aufeinanderfolgenden, als Dieselbelastungsstufen (DB) bezeichneten Schritten ab.

Nach drei Sekunden schließen zunächst die Einspeiseschalter zu den Schienen FU, FV, FW und FX (DB 1). 380-V-Drehstromverbraucher, insbesonders durchlaufende Antriebe, werden durch die Drehstromüberwachungsstufe Ü 26 wieder auf diese Schienen geschaltet.

Die Nebenkühlwasserpumpen erhalten nach 7 Sekunden und die nuklearen Zwischenkühlpumpen nach 11 Sekunden einen EIN-Befehl (DB 2 und 2a).

Nach 14 Sekunden starten, falls durch das Reaktorschutzsystem angefordert (Leck im Notstromfall), die Nachkühl- oder die Sicherheitseinspeisepumpen (DB 3).

Stehen die Notspeisezuschaltsignale YZ51 an, so werden die Notspeisepumpen nach 19 Sekunden gestartet (DB 4). In DB 5 und 6 (nach 33 bzw. 36 Sekunden) schließen die Einspeiseschalter zu den Schienen EU, EV, EW, EX.

Die Kältemaschinen werden nach 38 Sekunden von den nullredundanten Notstromsignalen eingeschaltet (DB 7).

Eine unzulässige Änderung der Betriebsparameter (Öldruck, Überdrehzahl, Überstrom) führt zur Beschädigung des Notstromdiesels. Falls kein Notspeisesignal und kein Flutsignal ansteht, wird dann eine Störabschaltung ausgelöst.

4.4 Leittechnische Systeme

4.4.1 Reaktorschutzsystem

Die leittechnischen Systeme einer Kernkraftwerksanlage bestehen aus der Betriebsinstrumentierung (Regelung, betriebliche Steuerung, Überwachungs- und Meldeanlagen) und dem Reaktorschutzsystem.

Das Reaktorschutzsystem hat die Aufgabe, den sicheren Zustand der Kraftwerksanlage zu überwachen. Wenn die dazu erfaßten Prozeßgrößen vorgegebene Grenzwerte über- bzw. unterschreiten, werden durch das Reaktorschutzsystem Gegenmaßnahmen eingeleitet (Schaltplan 15, Anhang 1)[1]). Durch die ausgelösten Reaktorschutzsignale werden vor allem die erforderlichen Sicherheitssysteme automatisch gesteuert.

Das Reaktorschutzsystem ist für den "gesicherten Bereich" und den "nicht gesicherten Bereich" getrennt aufgebaut. Als gesicherter Bereich wird der Teil der Anlage bezeichnet, der durch Einwirkungen von außen (z.B. Flugzeugabsturz, Druckwelle) nicht zerstört werden kann.

Dieser besonders geschützte Teil des Reaktorschutzsystems befindet sich im Ringraum. Seine Aufgabe ist es, bei einer Zerstörung von Frischdampfleitungen oder von Anschlußleitungen an den Reaktorkühlkreislauf durch Einwirkung von außen den Abschluß der beschädigten Leitungen sicherzustellen. Außerdem sind in diesem Teilsystem auch die Einrichtungen untergebracht, die bei einer

---

[1]) Alle im Schaltplan 15 und im folgenden aufgeführten Druckgrenzwerte sind als Drücke, gemessen gegen Atmosphäre, zu verstehen.

Zerstörung der Warte des Blockes B das Abfahren des Blockes mit Hilfe der Notstandstafel in Block A ermöglichen (Vorrangschaltungen, Ausblendung von Meßwerten zu den Anzeigen auf der Notstandstafel in Block A).

Zerstörungen im nicht gesicherten Bereich dürfen keine Rückwirkungen auf den gesicherten Bereich haben. Für Reaktorschutzmeßstellen, deren Analogsignale in beiden Bereichen benötigt werden, wird z.B. das vom Meßumformer kommende Signal zunächst in den gesicherten Bereich geführt und von dort wird über rückwirkungsfreie Trennverstärker das Signal zur Weiterverarbeitung in den nicht gesicherten Teil des Reaktorschutzsystems ausgeblendet.

Innerhalb des Reaktorschutzsystems unterscheidet man zwischen Anregeebene, Logikebene und Steuerebene (Bild F2, 4-1).

4.4.1.1 A n r e g e e b e n e

In der Anregeebene (Meßwerterfassung, Meßwertverarbeitung) wird jedes Anregekriterium durch mindestens drei redundante Meßkanäle, die eine Meßkanalgruppe bilden, überwacht.

Die Geräte und Kabel bzw. Wirkdruckleitungen unterschiedlicher Redundanzen sind entweder in verschiedenen Räumen oder zumindest in genügendem Abstand voneinander untergebracht. Die Meßkanäle werden nur für die Funktion innerhalb des Reaktorschutzes und nicht für betriebliche Aufgaben verwendet. Die zur Anzeige an der Reaktorschutztafel ausgeblendeten Meßsignale sind über Trennverstärker rückwirkungsfrei entkoppelt. Damit die Meßwerterfassung auch bei Kühlmittelverluststörfällen noch einwandfrei erfolgt, sind die Meßumformer, die diese Störfälle erfassen sollen, entweder außerhalb des Sicherheitsbehälters angeordnet oder, falls sie sich innerhalb des Sicherheitsbehälters befinden, besonders geschützt untergebracht.

Den prinzipiellen Aufbau eines Meßkanals zeigt Bild F2, 4-2 am Beispiel der Kühlmitteldruckmessung. Der Meßkanal besteht aus Fühler und Meßumformer, I/U-Wandler (Impedanzwandler) und U/U-

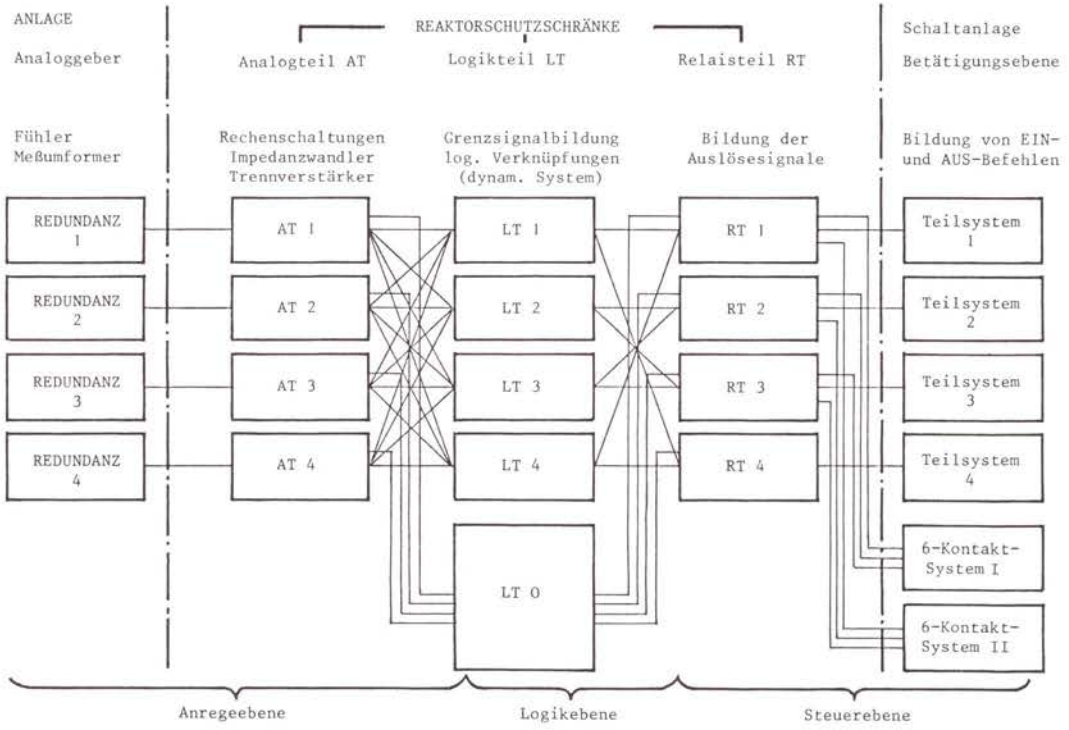


Bild F2, 4-1:
Prinzipieller Aufbau des Reaktorschutzsystems

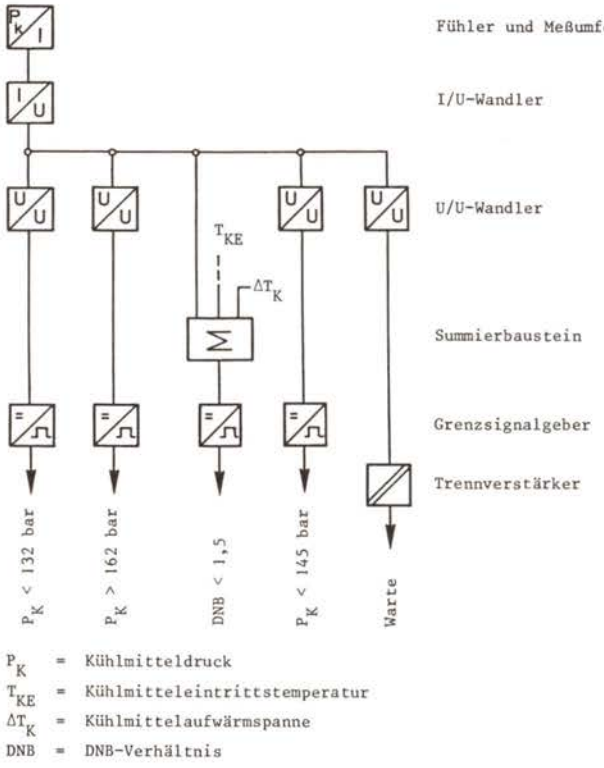


Bild F2, 4-2:
Prinzipieller Aufbau eines Meßkanals am Beispiel der Kühlmitteldruckmessung

Wandler (Trennverstärker) sowie dem Grenzsignalgeber (Grenzwertmelder) mit angeschlossenem Vergleicher (I = Strom, U = Spannung). Die durch analoge Stromsignale erfaßten Anregekriterien (Meßfühler und Meßumformer) werden in vier räumlich voneinander getrennten Schränken (AT1-AT4) des sogenannten Analogteils in analoge Spannungssignale umgeformt und anschließend direkt auf die der Logikebene zugerechneten Grenzsignalgeber geführt. Wenn ein solches Spannungssignal den vorgegebenen Grenzwert über- bzw. unterschreitet, wird ein Grenzsignal gebildet.

Ausfälle eines Meßkanals, die zu einer Veränderung der Spannung des Meßsignals oder der im Grenzsignalgeber eingestellten Referenzspannung führen, werden durch Vergleich der Signale von redundanten Meßkanälen detektiert sowie optisch und akustisch zur Meldung gebracht.

Zwischen I/U- und U/U-Wandler kann, wie in dem gezeigten Beispiel, eine Signalverzweigung für andere Grenzwerte vorhanden sein. Sofern aus mehreren Prozeßvariablen in Rechenschaltungen nicht direkt meßbare Anregekriterien ermittelt werden, sind diese Rechenschaltungen zwischen den jeweiligen I/U- bzw. U/U-Wandlern und dem Grenzsignalgeber eingefügt. Die Grenzsignalgeber stellen die Nahtstelle zwischen dem Analogteil und dem Logikteil dar; sie verarbeiten statische Analogsignale zu dynamischen Binärsignalen.

4.4.1.2 Logikebene und Steuerebene

In der Logikebene oder dem Logikteil (LT) werden die Ausgangssignale der Grenzsignalgeber jeder Meßkanalgruppe einer Majoritätsentscheidung (2v3- oder 2v4-Auswahl) unterworfen und zu einer Abschaltanregung verarbeitet. Zusätzlich werden die verschiedenen Anregekriterien logisch miteinander verknüpft (UND- und ODER-Verknüpfung). Im Relaisteil (RT) werden daraus schließlich die Auslösesignale gebildet. Innerhalb des LT wird unterschieden zwischen eindeutig sicherheitsgerichteten und nicht eindeutig sicherheitsgerichteten Auslösungen. So ist z.B. das Fehlansprechen eines Sumpfsignals nicht eindeutig sicherheitsgerichtet, da bei anstehendem Sumpfsignal die Armaturen zwischen Borwasser-Flutbehälter und Nachkühlpumpe geschlossen werden. Im Bedarfsfall ist dann eine Einspeisung aus diesem Behälter nicht möglich. Die Signalverarbeitung für eindeutig sicherheitsgerichtete Auslösungen (z.B. Reaktorschnellabschaltung) erfolgt in den Schrankgruppen LT0. Im Gegensatz zu den Schränken LT/RT1-LT/RT4, in denen die Signalverarbeitung für nicht eindeutig sicherheitsgerichtete Auslösungen vorgenommen wird, ist hier die konsequente räumliche Trennung der Redundanzen 1 - 4 nicht verwirklicht.

Zur Bildung einiger Reaktorschutzsignale ist es erforderlich, eine Schaltkette aus der Schrankgruppe LT0 mit einer Schaltkette der Schrankgruppen LT/RT1-LT/RT4 zu verknüpfen. Hierzu wird das dynamische Signal in LT0 zunächst in ein statisches umgewandelt, nach LT/RT1-LT/RT4 übertragen und dort durch eine Binärsignaleingabestufe wiederum in ein dynamisches Signal umgewandelt. Den prinzipiellen Aufbau des LT zeigt Bild F2, 4-3 am Beispiel der Reaktorschnellabschaltung.

Jedem Logikkanal ist ein treibender Taktgeber zugeordnet, der sowohl die Auswahlschaltungen als auch jeweils einen Grenzsignalgeber jeder Meßkanalgruppe mit dem erforderlichen Rechtecktakt (Einstellimpulse bzw. Auslöseimpulse) versorgt. Für die Meßkanalgruppen mit vier Meßkanälen ist ein vierter Taktgeber vorhanden. Die vier Taktgeber arbeiten synchron. Die Majoritätsentscheidungen werden von gepulsten Magnetkern-Transistorschaltungen ausgeführt (Baugruppen der Baureihe Simatic-N). Der LT arbeitet in der Weise, daß einem Wegfall des dynamischen Rechtecksignals eine Anregung der Reaktorschnellabschaltung entspricht ("fail safe"-Prinzip).

Bei einer 2v3-Verknüpfung wird ein Ausfall zunächst nur erkannt, wenn hierfür besondere Meldeorgane vorgesehen sind; Ausfälle im Meßkanal bis zum Eingang des Grenzsignalgebers werden durch den statischen Ausgang des Grenzsignalgebers oder über die Vergleicher gemeldet. Ausfälle der dynamischen Ausgangsstufe des Grenzsignalgebers bis zum Kettenglied (Auswahlschaltung) können nicht ohne weiteres erkannt werden, da die 2v3- bzw. 2v4-Bedingung erst bei Auftreten eines zweiten Fehlers erfüllt wird. Die Verfügbarkeit wäre durch diese Fehlauslösung nicht mehr gewährleistet.

Aus diesem Grund wird die Schrankgruppe LT0 mit Impulssperrsignalverteilern ausgerüstet. Der Impulssperrsignalverteiler blokkiert in bestimmtem Rhythmus (alle 256 Impulse) nacheinander im 1., 2., 3. und 4. Teilsystem die Einstellimpulse. Fehlen z.B. infolge eines Ausfalls die Einstellimpulse eines Grenzsignalgebers in einem Teilsystem, so ist bei Sperren des Einstellimpulses in einem anderen Teilsystem die 2v3- bzw. 2v4-Funktion kurz-

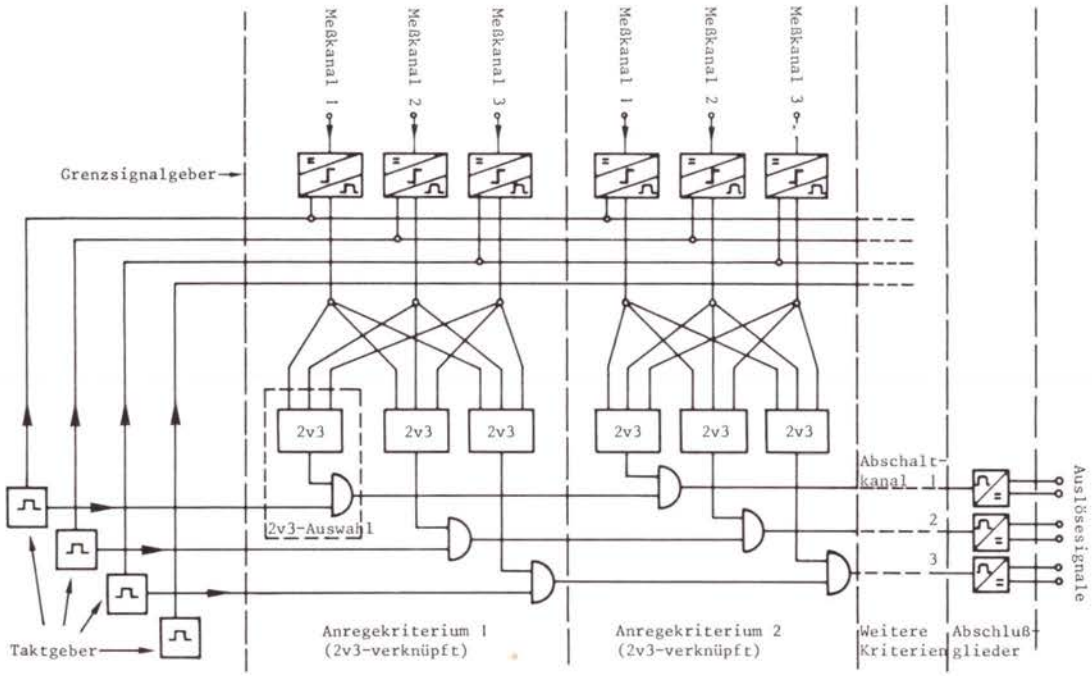


Bild F2, 4-3:
Prinzipieller Aufbau des Logikteils am Beispiel der Reaktorschnellabschaltung

zeitig erfüllt und die Spannung am Ausgang der Abschlußglieder ist kurzzeitig unterbrochen. Damit sprechen die dort angeschlossenen Meldeeinheiten an.

In einigen Fällen ist es erforderlich, die Funktion des Reaktorschutzsystems in Abhängigkeit vom Betriebszustand zu ändern. Hierzu sind im dynamischen LT drei von Hand zu betätigende Schutzüberbrückungen eingebaut. Es sind dies:

- Anfahrüberbrückung,
- Überbrückung Druckhalterwasserstand < 2,85 m,
- Überbrückung der Notkühlvorbereitungssignale.

Diese Schutzüberbrückungen können nur durchgeführt werden, wenn die jeweils notwendige Freigabe erfüllt ist. (So können z.B. die Notkühlvorbereitungssignale nur überbrückt werden, wenn die Anregung für diese Signale ansteht und der Druckhalterwasserstand über 3,15 m liegt.) Ist eine Schutzüberbrückung durchgeführt, dann wird sie automatisch wieder aufgehoben, wenn die Freigabe nicht mehr erfüllt ist.

Am Ende jedes Abschaltkanals befindet sich ein Ausgabegerät, das sogenannte Abschlußglied, das aus dem dynamischen Logiksignal eine statische Gleichspannung erzeugt. Bei Ausfall des Rechtecksignals verschwindet die Gleichspannung. Die Abschlußglieder stellen die Nahtstelle zwischen dem LT und dem RT dar. Die Gleichspannung wird zu einem Abschlußrelais geführt, das nach dem Ruheprinzip arbeitet. Die Kontakte der Abschlußrelais bilden die Auslösesignale, die in der Betätigungsebene die notwendigen Schalthandlungen auslösen (Bild F2, 4-4). Des weiteren können im RT Reaktorschutzsignale verzögert oder logisch miteinander verknüpft werden. An jedem Ausgangsrelais sind noch weitere an ein anderes Versorgungspotential P0 angeschlossene Kontakte vorhanden. Sie werden für Meldeaufgaben (Ansteuerung von Meldelampen auf der Reaktorschutztafel) und zur Bildung der null-redundanten Reaktorschutzsignale (Reaktorschutzsignale dieser Redundanz haben nur Betriebsfunktion) verwendet. Fehler in der Steuerebene des Reaktorschutzsystems werden durch Funktionsprüfung festgestellt.

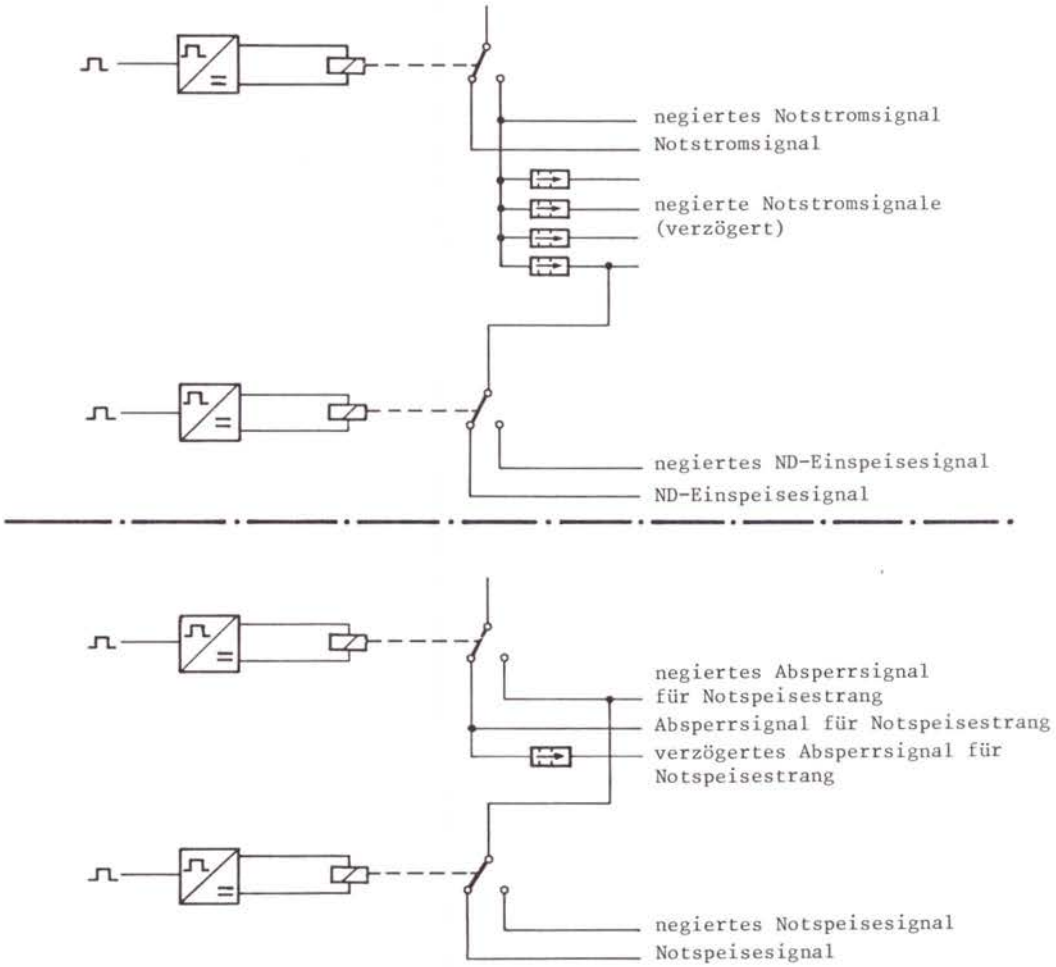
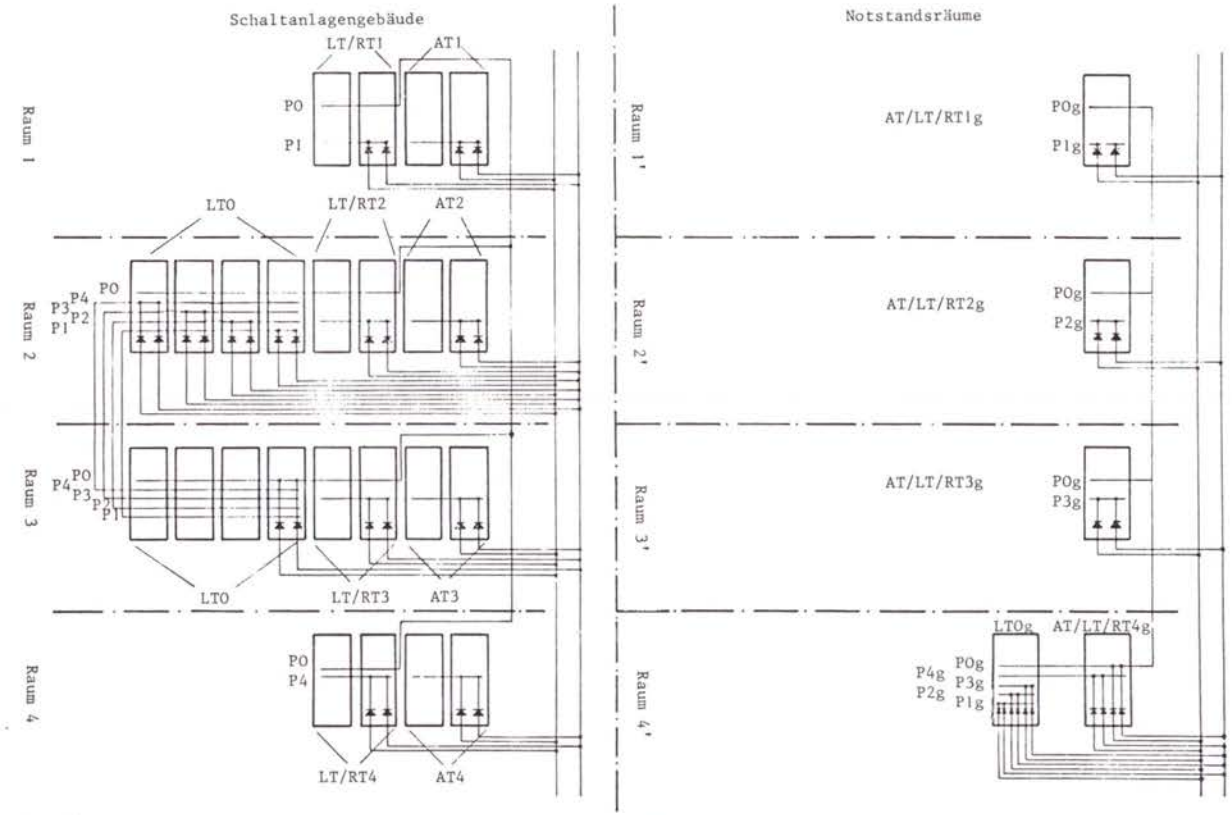


Bild F2, 4-4:
Beispiel zum Aufbau des Relaisteils

In der Betätigungsebene werden die Auslösesignale über spezielle Bausteine an die zu betätigenden Komponenten ausgegeben. Der Vorrang der Reaktorschutzsignale vor betrieblichen Signalen, wie Handsignalen und Signalen der betrieblichen Automatiken oder des Aggregateschutzes, wird über einen dem jeweiligen Betätigungsbaustein vorgeschalteten Vorrangbaustein sichergestellt. Die betrieblichen Signale können nur wirksam werden, wenn sie vom Reaktorschutzsystem freigegeben werden (diese Freigabe wird häufig durch das negierte Reaktorschutzsignal gegeben). Das Ansprechen des Kurzschluß- bzw. Überlastschutzes in den Verbraucherabzweigen kann durch die Reaktorschutzsignale nicht überbrückt werden.

Wie bereits beschrieben, sind die im Reaktorschutzsystem verwendeten Baugruppen (mit Ausnahme der Fühler zur Meßwerterfassung, der Meßumformer und der Anzeigegeräte) in Schränken untergebracht. Die Aufteilung der einzelnen Ebenen des Reaktorschutzsystems auf diese Schränke sowie deren Spannungsversorgung und räumliche Aufteilung ist Bild F2, 4-5 zu entnehmen. Die Schränke sind zu Schrankgruppen von zwei bis vier Schränken zusammengefaßt. Jede Schrankgruppe besitzt eine gemeinsame Stromversorgung, die von zwei redundanten 24-V-Schienen über Entkopplungsdioden gespeist wird. Die einzelnen Schrankgruppen sowie die Schränke selbst sind getrennt abgesichert. Ein Ansprechen dieser Sicherung wird optisch und akustisch gemeldet. Im Rahmen der vorliegenden Analyse wird davon ausgegangen, daß die Absicherungen der Potentiale in den Reaktorschutzschränken eine genügende Selektivität gegen die vorgelagerten Absicherungen aufweisen.

Den Einrichtungen, die das Reaktorschutzsystem selbst und die anderen Komponenten der Sicherheitssysteme überwachen, kommt eine besondere Bedeutung zu, da sofort entdeckte Ausfälle bei der Zuverlässigkeitsanalyse in der Regel vernachlässigt werden können. Für die ständige Überwachung von sicherheitstechnisch wichtigen Komponenten, die sich hinsichtlich der geforderten Funktionen in Bereitschaft befinden, gibt es optische und akustische Sammelmeldungen, z.B. die Notgefahrmeldungen DIESEL-STEUERUNG GESTÖRT und NOTSTROMDIESEL GESTÖRT. Außer Notgefahrmeldungen gibt es noch eine Vielzahl von Einzelmeldungen und Stellungsmeldungen.



P1-4/P1-4g = redundante Stromversorgung im ungesicherten/gesicherten Bereich
PO/POg = null-redundante Stromversorgung im ungesicherten/gesicherten Bereich

Bild F2, 4-5:

Anordnung und Stromversorgung der Reaktorschutzschränke

In der Kraftwerkswarte befindet sich eine Reaktorschutztafel, die einen Überblick über den Zustand des Reaktorschutzsystems gibt. Dort wird ein Ansprechen von Grenzsignalgebern und von Vergleichern sowie eine Schutzüberbrückung von Reaktorschutzsignalen angezeigt. Ebenso werden bei anstehenden Reaktorschutzsignalen die Signale selbst angezeigt. In welcher Stellung sich die angesteuerten verfahrenstechnischen und starkstromtechnischen Komponenten der Sicherheitssysteme befinden, ist aus den Anzeigen der Tischfelder der Wartenpulte zu ersehen.

4.4.2 Steuerung

Aufbau und Organisation der leittechnischen Einrichtungen zeigt Bild F2, 4-6. Die leittechnische Gesamtanlage ist funktionell gegliedert in

- Geräte und Geber in der Anlage,
- Anlagenkoppeleinrichtungen oder Betätigungsebene,
- automatische Einrichtungen und
- Leitstand.

Die einzelnen Aufgabenbereiche werden im folgenden erläutert. Die Anlagenkoppeleinrichtung bzw. Betätigungsebene enthält die Befehlsverarbeitung und Signalverknüpfung für Befehle von Hand und von der Automatik sowie für die Signale von Schutzverriegelungen oder vom Reaktorschutzsystem. Außerdem übernimmt die Betätigungsebene die Überwachung der Antriebe in der Anlage bezüglich der Schaltstellung und Richtigkeit der Rückmeldesignale. Jedes elektrisch anzusteuernde Stellglied (Schieber, Ventile, Pumpen usw.) wird zu diesem Zweck mit einem ihm zugeordneten Betätigungsbaustein ausgerüstet. Der Vorrang der Reaktorschutzsignale vor betrieblichen Signalen wird über einen den Betätigungsbausteinen vorgeschalteten Vorrangbaustein sichergestellt (Abschnitt 4.4.1.2).

Die Betätigungsebene ist die unterste Steuerebene. Von hier aus werden entweder direkt oder über Koppelrelais die zur Betätigung der Stellglieder eingesetzten Leistungsschütze in der Schaltanlage angesteuert. Die Baugruppen zur Aufbereitung der analogen

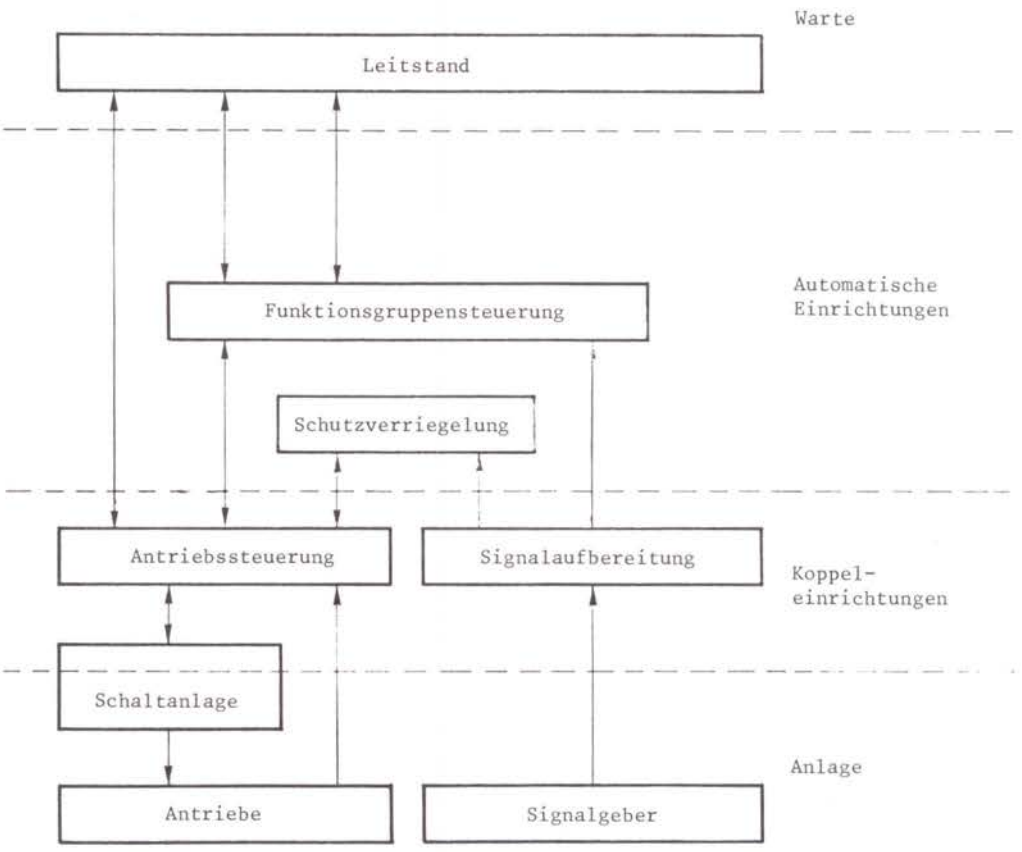


Bild F2, 4-6:
Hierarchie der Kraftwerkssteuerung

oder binären Signale aus der Anlage werden ebenfalls der Betätigungsebene zugerechnet.

Der Betätigungsebene übergeordnet sind die automatischen Einrichtungen, d.h. die Funktionsgruppensteuerung und die Schutzverriegelung. Jede Funktionsgruppe umfaßt meist mehrere, zum Teil gleichartige Aggregate, z.B. drei Speisewasserpumpen, die als Untergruppen einer Funktionsgruppe betrachtet werden können.

Demgemäß unterteilt man die Funktionsgruppensteuerung in entsprechend viele Untergruppensteuerungen. Die Untergruppensteuerungen enthalten die Schaltfolgelogik und haben die Aufgabe, die ihnen zugeordneten Untergruppen in den gewünschten Betriebs zu bringen oder stillzusetzen. Ihr wesentliches Kennzeichen ist ein Schrittablauf. Vor jedem Programmschritt wird abgefragt, ob der Schrittbefehl an die Anlage zulässig ist. Nach jedem Programmschritt wird abgefragt, ob die entsprechenden Befehle ausgeführt wurden. Die Untergruppensteuerungen stellen die unterste Entscheidungsebene und den Schwerpunkt der Funktionsgruppensteuerung dar. Die nächsthöhere Entscheidungsebene innerhalb der Funktionsgruppensteuerung ist die Gruppensteuerung, die die Einsatzlogik enthält. Sie bestimmt den Einsatz der ihr unterlagerten Untergruppensteuerungen und entscheidet durch Abfragen des Anlagenzustandes (Rückmeldungen von der Signalaufbereitung und der Antriebssteuerung), zu welchem Zeitpunkt welche Untergruppen in Betrieb zu nehmen oder stillzusetzen sind. Außerdem enthält die Gruppensteuerung die Störumschaltlogik, die bei gestörtem Betrieb einer Untergruppe den Einsatz einer in Reserve stehenden gleichartigen Untergruppe veranlaßt.

Die Schutzverriegelung soll eine Gefährdung von Personal sowie Schäden in der Anlage verhindern. Sie ist daher nicht abschaltbar und sowohl bei Einzelsteuerung der Stellglieder von Hand als auch bei automatischem Betrieb wirksam. Zu beachten ist, daß Befehle der Schutzverriegelung, falls sie über die Vorrangbausteine geführt werden, ebenfalls die Freigabe durch das Reaktorschutzsystem benötigen.

Alle im Bereich der Automatiken und der Koppeleinrichtungen eingesetzten elektronischen Geräte sind der Baureihe Simatic-P entnommen. Die Baugruppen sind in Schränken untergebracht (Verriegelungs-, Betätigungsschränke usw.). Diese Schränke werden über abgesicherte Doppeleinspeisungen mit Spannung aus der Gleichstromanlage versorgt. Die Spannungsverteilung an die Baugruppen ist für Verriegelungs- und Betätigungsschränke unterschiedlich abgesichert. So sind die Verriegelungsschränke zeilenweise abgesichert, bei den Betätigungsschränken besitzt dagegen jeder Baustein eine eigene Stromüberwachung.

An oberster Stelle der hierarchisch aufgebauten Kraftwerksteuerung steht der Leitstand in der Warte (Abschnitt 3.4.2.2). Auf dem Fahrpult sind die Betätigungsfelder und Anzeigegeräte der Gruppen- und Untergruppensteuerungen sowie der Regelungen untergebracht, die zum An- oder Abfahren der Anlage oder zum Leistungsbetrieb der Anlage benötigt werden. Zusätzlich sind auf diesem Pult die Betätigungsfelder sowie Anzeiger wichtiger Aggregate untergebracht, die nicht von Automatiken gesteuert werden.

Im Aufsatz des Fahrpultes sind die Anzeiger wichtiger Prozeßvariabler sowie die Meldefelder von Meldungen hoher Priorität untergebracht. Im Aufsatz des Fahrpultes sind auch Datensichtgeräte integriert, auf denen die von der Prozeßrechneranlage kommenden Meldungen angezeigt werden. Vor dem Fahrpult befinden sich in der Wartenwandtafel weitere Anzeige- und Registriergeräte, die für das An- und Abfahren sowie den Leistungsbetrieb benötigt werden. Außerdem ist dort auch die sogenannte Anweisungstafel untergebracht, von der in einigen wichtigen Störfällen Hinweise auf die durchzuführenden Maßnahmen (mit Angabe des entsprechenden Logikschemas des Betriebshandbuches) automatisch gegeben werden.

Um 90° versetzt dazu sind auf dem Steuerpult die Betätigungsfelder und Anzeigen der Komponenten untergebracht, die nur bei Störung ihrer Automatik einzeln gesteuert werden müssen oder die vom Blockbetrieb unabhängig sind. Im Pultaufsatz des Steuerpultes befinden sich analog zum Fahrpult ebenfalls Anzeigegeräte und Meldefelder für Meldungen niedrigerer Priorität. Auf der vor dem Steuerpult befindlichen Wandtafel und der daran anschließenden Wandtafel sind weitere Anzeige- und Registriergeräte wichtiger Prozeßvariabler angebracht. In diesen Wandtafeln sind auch die Reaktorschutz-Wandtafel und die Eigenbedarfstafel integriert. Weiterhin sind die Strahlungsüberwachung, die Unfallfolgeinstrumentierung und Störungsschreiber auf der Wandtafel untergebracht. Neben dem Fahrpult steht der Meldedrucker, an dem alle Prozeßrechnermeldungen ausgedruckt werden.

4.4.3 Melde- und Überwachungseinrichtungen

Um den Betriebszustand der Anlage jederzeit zu kontrollieren und Störungen vor dem Eintritt größerer Schäden rechtzeitig zu erkennen, so daß notwendige Gegenmaßnahmen getroffen werden können, ist in der untersuchten Anlage eine Reihe von Melde- und Überwachungseinrichtungen installiert. Im allgemeinen werden Meldungen bezüglich ihrer Aussage nach

- Warnmeldungen
- Fehlermeldungen
- Zustandsmeldungen

} Gefahrmeldungen

unterschieden. Die Gefahrmeldungen werden je nach ihrer Dringlichkeit oder sicherheitstechnischen Bedeutung in Prioritätsklassen eingeteilt. Dabei besitzen die sogenannten Notgefahrmeldungen die höchste Priorität.

- Warnmeldungen

Diese Meldungen werden ausgegeben, wenn ein Abweichen einer Größe vom Sollzustand auftritt. Ein Überschreiten des zugehörigen Grenzwertes führt noch nicht zum Ansprechen einer Schutzeinrichtung. Jedoch kann die Zeit, die für Gegenmaßnahmen zur Verfügung steht, sehr knapp sein. So steht bei der Meldung LAGERTEMPERATUR ZU HOCH bei einem laufenden Aggregat meist nur wenig Zeit für eine Gegenmaßnahme (Aus- bzw. Umschalten) zur Verfügung. In einigen Fällen werden daher gestaffelte Grenzwerte festgelegt, bei denen der erste Ansprechwert einen Hinweis auf einen sich abzeichnenden gefährlichen Trend liefert, z.B. die Meldung ÖLBEHÄLTER, ÖLSTAND TIEF. Die entsprechende nächste Meldung würde dann lauten: ÖLBEHÄLTER, ÖLSTAND ZU TIEF.

- Fehlermeldungen

Fehlermeldungen weisen darauf hin, daß eine Einrichtung aufgrund eines Fehlers gestört bzw. ausgefallen ist oder daß die entsprechenden Schutzeinrichtungen angesprochen haben. So weist die

Meldung VAKUUMSCHUTZ auf das Ansprechen einer Schutzeinrichtung an der Turbine hin, die Meldung LETZTE HAUPTSPEISEWASSERPUMPE AUSGEFALLEN weist auf den vollständigen Ausfall der Hauptspeisewasserversorgung hin.

- Zustandsmeldungen

Eine Zustandsmeldung dient dazu, dem Bedienungspersonal in der Warte eine Information darüber zu geben, in welchem Betriebszustand sich die Einrichtungen des Kraftwerkes befinden, unabhängig davon, ob dieser Zustand von Hand, durch Automatiken oder Schutzeinrichtungen herbeigeführt wurde. So werden zum Beispiel Rückmeldungen wie EIN bzw. AUS von Schaltgeräten oder AUF bzw. ZU von Stellantrieben am jeweiligen Betätigungstischfeld gemeldet. Die Meldung AGGREGATESCHUTZ KÄLTEMASCHINE HAT ANGESPROCHEN zeigt den Betriebszustand nach Ansprechen einer Schutzeinrichtung an. Zusammen mit einer eventuell vorher aufgetretenen Warnmeldung, z.B. ÖLDRUCK ZU TIEF, kann die Störungsquelle rasch lokalisiert werden und es können geeignete Maßnahmen zur Instandsetzung eingeleitet werden.

Dieses Meldekonzept gewährleistet für den bestimmungsgemäßen Betrieb der Anlage eine rasche und umfassende Information der Bedienungsmannschaft. Bei Störfällen jedoch könnte eine Überforderung des Personals auftreten. Deshalb wurde durch Einführung von Prioritätsklassen für die Meldungen versucht, eine Reduzierung des "Meldeschwalls" zu erreichen. So werden die für die Erkennung des Störfalls wichtigen Meldungen als sogenannte Notgefahrmeldungen (Prioritätsklasse I) auf einer im Fahrpult integrierten Meldeanlage optisch (Blinklicht) und akustisch (Hupe) gemeldet. Meldungen niedrigerer Priorität (Prioritätsklasse II) werden über Prozeßrechner am Meldedrucker und über im Pult integrierte Datensichtgeräte ausgegeben. Das Eintreffen einer Meldung wird ebenfalls akustisch (Gong) und optisch (letzte Meldung am Datensichtgerät blinkt) angezeigt. Bei Auftreten eines "Meldeschwalls" werden die Meldungen der Prioritätsklasse II automatisch unterdrückt.

4.5 System zur Reaktorschnellabschaltung

4.5.1 Reaktorschutzsystem zur Reaktorschnellabschaltung

4.5.1.1 Anregeebene

Jedes Anregekriterium für die Reaktorschnellabschaltung (RESA) wird durch mindestens drei redundante Meßkanäle, die eine Meßkanalgruppe bilden, überwacht. Ein Meßkanal besteht aus Fühler und Meßumformer, I/U- und U/U-Wandler (I = Strom, U = Spannung), sowie den Grenzsignalgebern mit angeschlossenem Vergleicher. Zwischen I/U- und U/U-Wandler kann, wie in dem gezeigten Beispiel, eine Signalverzweigung für andere Grenzwerte vorhanden sein. Sofern aus mehreren Prozeßvariablen in Rechenschaltungen nicht direkt meßbare Anregekriterien ermittelt werden müssen, sind diese Rechenschaltungen zwischen den jeweiligen I/U- bzw. U/U-Wandlern und dem Grenzsignalgeber eingefügt. Der prinzipielle Aufbau eines Meßkanals ist bereits in Abschnitt 4.4.1.1 dargestellt.

Insgesamt werden in der Zuverlässigkeitsanalyse der vorliegenden Studie folgende Meßkanäle quantitativ berücksichtigt:

- 4 Meßkanalgruppen aus je 3 Meßkanälen zur Überwachung der Drehzahl der vier Hauptkühlmittelpumpen,
- 1 Meßkanalgruppe aus 4 Meßkanälen für die Kühlmitteleintrittstemperatur zur Errechnung der DNB-Verhältnisse für die vier Kühlkreisläufe sowie zur Errechnung der mittleren Kühlmitteltemperatur,
- 4 Meßkanalgruppen aus je 3 Meßkanälen für die Aufwärmspanne zur Errechnung der DNB-Verhältnisse für die vier Kühlkreisläufe sowie davon 4 mal je 1 Meßkanal zur Errechnung der mittleren Kühlmitteltemperatur,
- 1 Meßkanalgruppe aus 4 Meßkanälen für den Kühlmitteldruck zur Errechnung der DNB-Verhältnisse in den 4 Kühlkreisläufen, davon 3 Meßkanäle für die Kühlmitteldruckgrenzwerte,
- 1 Meßkanalgruppe aus 3 Meßkanälen für den Druckhalter-Wasserstand. Hierzu erfolgt eine Analogsignalaufbereitung im gesicherten Bereich und wird über Trennverstärker in den ungesicherten Bereich ausgekoppelt,

- 1 Meßkanalgruppe aus 3 Meßkanälen für den Anlagenraumdruck,
- 1 Meßkanalgruppe aus 3 Meßkanälen für den Betriebsraumdruck,
- 4 Meßkanalgruppen aus je 3 Meßkanälen für die Dampferzeuger-Wasserstände und
- 4 Meßkanalgruppen aus je 3 Meßkanälen für den Druck in den Speisewasserleitungen.

Nicht betrachtet werden die Meßkanäle für folgende Prozeß- bzw. Sicherheitsvariablen:

- Reaktorleistung,
- Neutronenfluß,
- N-16-Aktivität hinter den Dampferzeugern und
- Frischdampfsammler-Druck.

Durch Vergleicher am Ende der analogen Meßwertverarbeitung werden Abweichungen in einzelnen Meßkanälen entdeckt und zur Meldung gebracht. Diese Überwachung bezieht sich auch auf die eingestellten Referenzspannungen in den Grenzsignalgebern. Die Grenzsignalgeber dienen zur Überwachung von Überschreitungen vorgegebener Grenzen durch die gemessenen Prozeßvariablen. Die Grenzsignalgeber stellen die Nahtstelle dar zwischen dem Analogteil und dem Logikteil; sie verarbeiten statische Analogsignale zu dynamischen Binärsignalen.

4.5.1.2 L o g i k e b e n e

In der Logikebene werden die Ausgangssignale der Grenzsignalgeber jeder Meßkanalgruppe einer Majoritätsentscheidung (2v3- oder 2v4-Auswahl) unterworfen und zu einer Abschaltanregung verarbeitet. Zusätzlich werden die verschiedenen Anregekriterien logisch miteinander verknüpft (UND- und ODER-Verknüpfung). Die Majoritätsentscheidungen werden von gepulsten Magnetkern-Transistor-Schaltungen ausgeführt, die ODER-Verknüpfung der verschiedenen Anregekriterien durch Reihenschaltung der entsprechenden Auswahlschaltungen.

Majoritätsentscheidung und logische Verknüpfung werden gleichzeitig in drei parallelen Abschaltkanälen herbeigeführt. Jedem

Abschaltkanal ist ein treibender Taktgeber zugeordnet, der sowohl die Auswahlschaltungen des Abschaltkanals als auch jeweils einen Grenzwertmelder jeder Meßkanalgruppe mit dem erforderlichen Rechtecktakt versorgt. Für die Meßkanalgruppen mit vier Meßkanälen ist ein vierter Taktgeber vorhanden. Die vier Taktgeber arbeiten synchron. Das Logiksystem arbeitet in der Weise, daß einem Wegfall des dynamischen Rechtecksignals eine Anregung der Reaktorschnellabschaltung entspricht ("fail safe"-Prinzip).

Durch die Majoritätsentscheidungen und logische Verknüpfungen werden folgende in dieser Untersuchung berücksichtigte Anregekriterien für die Reaktorschnellabschaltung gewonnen[1]):

- Drehzahl von 3v4-Hauptkühlmittelpumpen < 93 %
  (3v4 aus 4 x 2v3)
- DNB-Verhältnis in einem Kühlkanal < 1,5
  (1v4 aus 4 x 2v3)
- Kühlmitteldruck > 162 bar (2v3)
- Druckhalterniveau > 9,56 m (2v3)
- Druckhalterniveau < 2,85 m (2v3) und Kühlmitteldruck
  < 145 bar (2v3)
- Anlagenraumdruck > 30 mbar (2v3)
- Betriebsraumdruck >30 mbar (2v3)
- Wasserstand in einem Dampferzeuger < 6,5 m
  (1v4 aus 4 x 2v3)
- Mittlere Kühlmitteltemperatur > 311 °C
  (2v4 aus 3 x 2v3, zyklisch vertauscht)
- Wasserstand in zwei Dampferzeugern < 8,85 m
  (2v4 aus 4 x 2v3)
- Druck in einer Speisewasserleitung > 78 bar
  (1v4 aus 4 x 2v3)

Die zugehörigen 2v3-Kettenglieder sind in der hier dargestellten Reihenfolge der Anregekriterien hintereinandergeschaltet. Vor den Kettengliedern für das Anregekriterium "Hauptkühlmittelpumpendrehzahl < 93 %" sind die Kettenglieder für die anfahrverriegelten Neutronenflußgrenzwerte angeordnet. Zwischen den Kettengliedern der Anregekriterien "Hauptkühlmittelpumpendrehzahl < 93 %" und "DNB-Verhältnis < 1,5" befinden sich die Kettenglieder für

---

[1]) Vgl. Fußnote, S. 198

das über die Reaktorleistung verriegelte Anregekriterium "Drehzahl von 1 oder 2 Hauptkühlmittelpumpen < 65 %" sowie für die aus der Reaktorleistung abgeleiteten Anregungen. Die Kettenglieder für das Anregekriterium aufgrund der "N-16-Aktivität hinter einem Dampferzeuger" sind hinter den Kettengliedern für das Anregekriterium "Wasserstand in zwei Dampferzeugern < 8,85 m" untergebracht.

Am Ende jedes Abschaltkanals befindet sich ein Ausgabegerät, das sogenannte Abschlußglied, das aus dem dynamischen Logiksignal eine statische Gleichspannung erzeugt. Bei Ausfall des Rechtecksignals verschwindet die Gleichspannung. Die Abschlußglieder stellen die Nahtstelle zwischen dem Logikteil und dem Relaisteil dar. Eine Darstellung des Funktionsprinzips des Logikteils findet sich bereits in Abschnitt 4.4.1.2.

4.5.1.3 S t e u e r e b e n e

Die drei Ausgabegeräte der drei Abschaltkanäle versorgen je zwei parallel geschaltete Relais, also insgesamt sechs Relais.

Jedes Relais schaltet einen Abschaltschütz. Mit den Kontakten von je drei Schützen wird eine 2v3-Auswahl der Ausgangssignale der Ausgabegeräte gebildet. Über zwei solche 2v3-Auswahlschaltungen werden die Hilfsschütze der Hub-, Halte- und Greifspulen der Steuerstäbe mit Strom versorgt (Bild F2, 4-7 und -8).

Relais und Schütze arbeiten nach dem Ruhestromprinzip. Bei Relais und Abschaltschützen (nicht bei den Hilfsschützen) ist gerätetechnische Diversität vorhanden, um "common mode"-Einflüssen zu begegnen.

4.5.2 Mechanisches System zur Reaktorschnellabschaltung

Der mechanische Teil des Systems zur Reaktorschnellabschaltung besteht aus 61 gleichartigen Steuerstäben und den entsprechenden Führungen. Jeder Steuerstab setzt sich aus einem Steuerelement und einer Antriebseinheit zusammen.

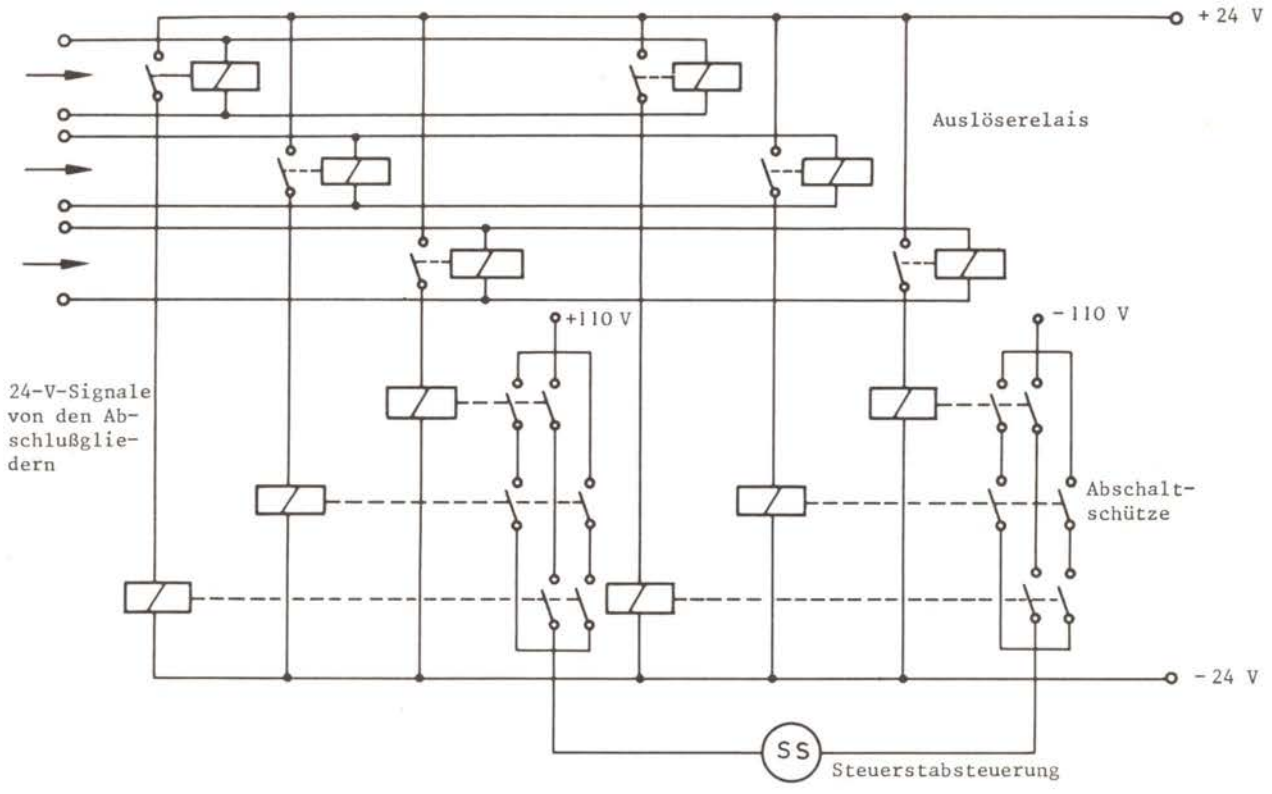


Bild F2, 4-7:
Relaisteil des Systems zur Reaktorschnellabschaltung

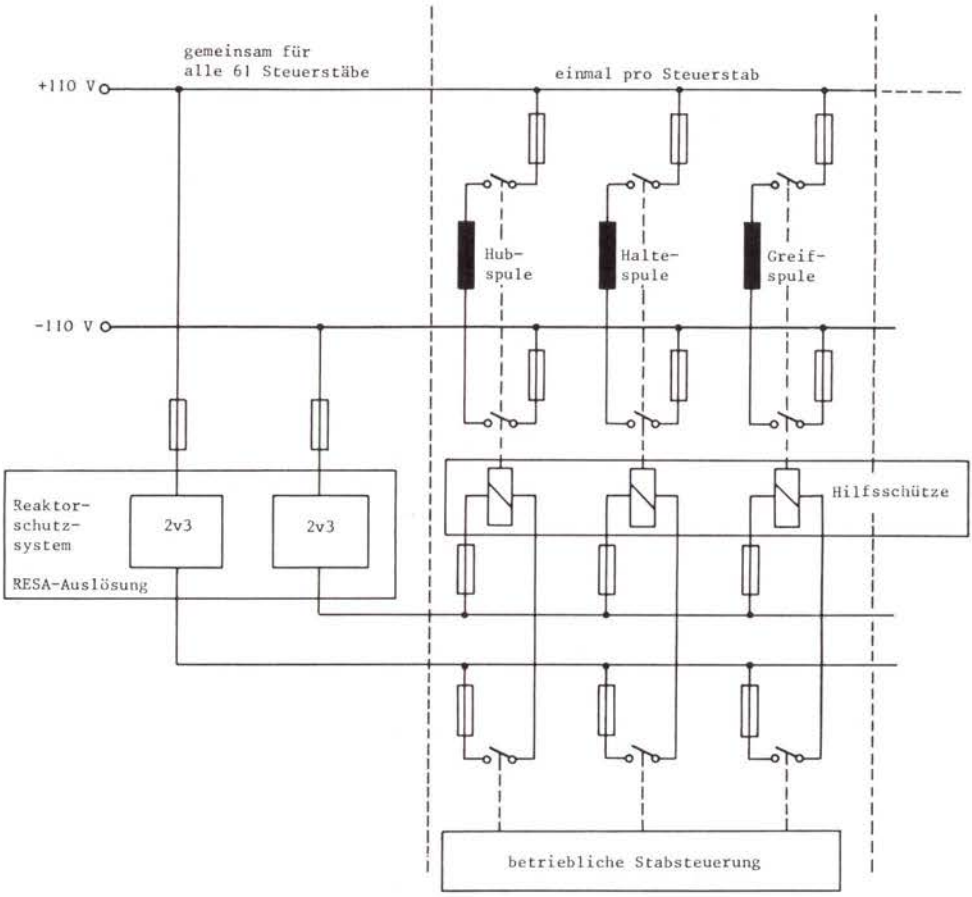
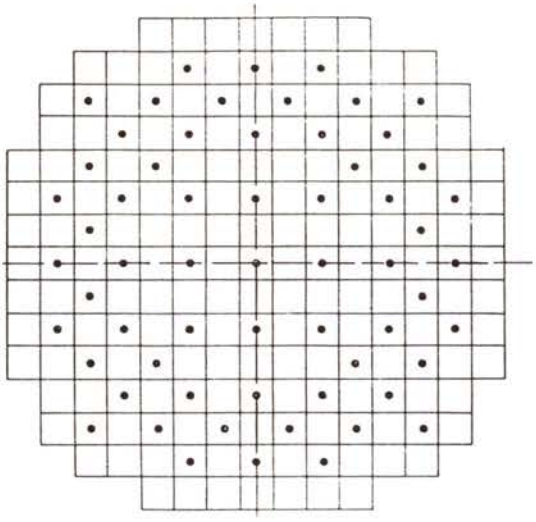


Bild F2, 4-8:
Prinzipielle Darstellung der Steuerstabsteuerung und der Auslösung der Reaktorschnellabschaltung

Die Steuerelemente werden von den in Bild F2, 4-9 bezeichneten Brennelementen aufgenommen und sind untereinander durch den Druckbehälterdeckel mit den Steuerstabstutzen, durch das obere Kerngerüst mit den Steuerstabführungseinsätzen und durch das untere Kerngerüst konstruktiv verbunden. Die gemeinsame Umgebung aller Stäbe stellt das Hauptkühlmittel dar. Durch Abdeckungen der Führungseinsätze werden die Steuerstäbe gegen Querströmung



• 61 Steuerstabpositionen

Bild F2, 4-9:
Querschnitt des Reaktorkerns

geschützt. Die außerhalb des Druckbehälterdeckels liegenden Steuerstabantriebe werden durch Druckkörper gegenüber der Atmosphäre dicht abgeschlossen. Für diese Druckkörper gelten die Auslegungsbestimmungen des Reaktordruckbehälters.

Das einzelne Steuerelement besteht aus 20 Fingern, die an ihrem oberen Ende mit einer spinnenartigen Tragekonstruktion (Spinne) verschraubt sind. Diese Spinne nimmt über eine Kupplung die Antriebsstange auf, die mit dem Steuerstabantrieb verbunden ist. Das Ein- und Ausfahren der Steuerstäbe erfolgt schrittweise durch Senken bzw. Heben der Antriebsstange. Bei einem Senkschritt fällt der Stab aufgrund seiner Schwerkraft um ca. 10 mm, bei einem Hubschritt wird der Stab durch eine Magnetspule (Hubspule) um die gleiche Länge angezogen.

Beide Bewegungen werden mit Hilfe eines magnetischen Klinkenschritthebers ausgeführt, dessen beide Klinken, Greif- und Halteklinke, bei jedem Auf- oder Abwärtsschritt abwechselnd in die gerillte Antriebsstange gedrückt werden. Jeder Klinke ist dazu eine Arbeitsspule und eine Spreizfeder zugeordnet. Die Klinke ist im Eingriff, wenn die zugehörige Spule stromdurchflossen ist, sie wird bei Stromunterbrechung durch die Spreizfeder außer Eingriff gebracht.

Eine Reaktorschnellabschaltung erfolgt durch die Stromunterbrechung in den Halte-, Greif- und Hubspulen aller Steuerstäbe, so daß alle Stäbe frei in den Kern fallen. Die Fallbewegung wird dabei durch besondere Ausbildung der Stabführungsrohre im unteren Teil gedämpft. Die mittlere Fallzeit bei Schnellabschaltung aus der obersten Stabstellung beträgt ca. 2 Sekunden.

5. FUNKTIONSPRÜFUNGEN

5.1 Allgemeines

Jede Komponente der sicherheitstechnisch wichtigen Systeme eines Kernkraftwerks hat eine oder mehrere Funktionen zu erfüllen. Entsprechend dieser Funktionen können der Komponente Funktionselemente zugeordnet werden. Während des normalen Leistungsbetriebes der Anlage befindet sich die Komponente für eine dieser Funktionen entweder in Betrieb oder in Bereitschaft.

Bei den Komponenten, die während des Leistungsbetriebes bereits die bei einem Kühlmittelverluststörfall oder einer Transiente geforderte Funktion ausüben, wird ein Versagen dieser Funktion, also ein Ausfall des zugehörigen Funktionselementes, sofort entdeckt. Derartige Komponenten sind z.B. die in Betrieb befindlichen Pumpen des nuklearen Zwischenkühlkreislaufes oder des Nebenkühlwassersystems. Keine solche Komponenten sind jedoch z.B. die Einspeiseschalter zur Stromversorgung dieser Pumpen, falls ein Notstromfall eintritt, da diese Schalter dann betätigt werden müssen.

Bei den sicherheitstechnisch wichtigen Komponenten, die während des Leistungsbetriebes des Kraftwerks nicht die bei einem Kühlmittelverluststörfall oder einer Transiente geforderten Funktionen ausüben, sind wiederkehrende Prüfungen durchzuführen. Durch diese regelmäßigen Funktionsprüfungen soll eine hohe Verfügbarkeit der Komponenten für die geforderten Funktionen gewährleistet werden. Die Prüfanweisungen sind im sogenannten Prüfhandbuch, das ein Teil des Betriebshandbuches ist, schriftlich fixiert. Art und Umfang sowie die Zeitabstände der durchzuführenden Funktionsprüfungen werden im Genehmigungsverfahren festgelegt. Die Ergebnisse der Prüfungen müssen dokumentiert werden. Die administrative Organisation des Prüfablaufes und die Art der Dokumentation der Ergebnisse liegen zum Teil im Ermessen des Anlagenbetreibers.

Wenn bei der Prüfung der Ausfall eines Funktionselementes festgestellt wird, erfolgt eine Instandsetzung der Komponente. Nach

Beendigung der Instandsetzung wird die entsprechende Funktion überprüft. Aufgrund von menschlichen Fehlhandlungen ist es möglich, daß der Ausfall einer Funktion bei der Funktionsprüfung nicht entdeckt wird oder daß bei Armaturen eine Fehlstellung nach der Funktionsprüfung vorliegt, d.h., daß die Armatur in einer falschen Stellung belassen bzw. in eine falsche Stellung gefahren wird. In den Zuverlässigkeitsanalysen werden diese menschlichen Fehlhandlungen bei Funktionsprüfungen grundsätzlich berücksichtigt.

Aufgrund von Abschätzungen, die mit den in Abschnitt 3.4.3 genannten Basisdaten für menschliche Fehlhandlungen (z.B. Auslassungsfehler während eines Arbeitsablaufes) durchgeführt werden, ergeben sich im allgemeinen vernachlässigbare Beiträge zur Nichtverfügbarkeit der Systemfunktionen (Abschnitt 3.5). Dies gilt insbesondere für kontrollverriegelte Armaturen des Not- und Nachkühlsystems, sofern bei Fehlstellung die Notgefahrmeldung NOTKÜHLBEREITSCHAFT GESTÖRT ausgegeben wird (Abschnitt 6.1.2.2). Fehlstellungen von Regelventilen werden nicht berücksichtigt, da die Regler im allgemeinen ständig in Betrieb sind, die Stellung des Regelventils, die Regelabweichung und die zu regelnde Prozeßgröße am Wartenpult angezeigt werden. Die zu regelnde Prozeßgröße wird zusätzlich durch Grenzsignalgeber überwacht. Wo für falsch durchgeführte Funktionsprüfungen höhere als die in Abschnitt 3.4.3 angeführten Wahrscheinlichkeiten angesetzt werden oder wo der Einfluß menschlicher Fehlhandlungen bei Funktionsprüfungen nicht von vornherein vernachlässigbar ist, werden die entsprechenden Ausfallkombinationen in den Fehlerbäumen näherungsweise berücksichtigt.

Außerdem ist zu beachten, daß es während der regelmäßig durchzuführenden Funktionsprüfungen der Sicherheitssysteme Zeiträume geben kann, in denen der getestete Strang nicht funktionsfähig ist. Die Funktion der hier untersuchten Systeme wird jedoch in der Regel über die Ausgabe der entsprechenden Reaktorschutzsignale geprüft. Die angesteuerten Komponenten werden vor Ausgabe der Reaktorschutzsignale in die Zustände gebracht, in denen sie sich bei einem Störfall nicht befinden sollen (laufende Pumpen werden abgeschaltet, Armaturen und Schalter in die fal-

sche Stellung gebracht). Sollte während dieses Zeitraums ein Störfall eintreten, also eine Ansteuerung dieser Komponenten durch das Reaktorschutzsystem erfolgen, so werden die Reaktorschutzsignale vorrangig behandelt und betriebliche Befehle unterdrückt. Das System ist also während dieses Teils der Funktionsprüfung voll funktionsfähig. Anschließend wird bei vorhandener Prüffreigabe für wenige Sekunden das jeweilige Reaktorschutzsignal ausgegeben. Nur in den Fällen, in denen das zur Prüfung ausgegebene Reaktorschutzsignal die Ausgabe eines anderen Reaktorschutzsignals verhindert (z.B. wird bei Ausgabe des Sumpfsignals das Flutsignal unterdrückt), ist ein bestimmter Teil des Systems aufgrund der Funktionsprüfung für wenige Sekunden funktionsunfähig. Der Einfluß dieser äußerst geringen Ausfallzeit auf die Nichtverfügbarkeit des Stranges kann aber vernachlässigt werden.

Der Sicherheitsbehälter und seine Abschlußorgane werden während der Herstellung umfangreichen Prüfungen unterworfen /F2, 5-1 bis -4/:

Nach Abschluß des Zusammenbaus des Sicherheitsbehälters einschließlich Schleusen, Kabel- und Rohrdurchführungen wird eine Druckprobe mit Luft durchgeführt. Die Druckprüfung wird nach einem Druck-Zeit-Diagramm gefahren, dabei beträgt der maximale Druck (Prüfdruck) das 1,1fache des Auslegungsdrucks multipliziert mit einem Faktor, der sich aus dem Verhältnis des Mindestdehngrenzwertes des Behälterwerkstoffes bei Umgebungstemperatur zu dem bei Auslegungstemperatur ergibt. Während der Druckprüfung werden Dichtheitsprüfungen an allen Dichtflächen durchgeführt. Getrennt von dieser Druckprüfung wird die Leckratenerstprüfung vorgenommen /F2, 5-5/. Dabei wird geprüft, ob der Sicherheitsbehälter ausreichend dicht ist, d.h. ob die obere Vertrauensgrenze der Leckrate kleiner oder gleich dem Wert der zulässigen Leckrate ist. Die Leckrate wird bei zwei Druckstufen bestimmt, bei 0,5 bar Überdruck und bei Auslegungsdruck.

Auch beim Betrieb des Kernkraftwerkes werden regelmäßig wiederkehrende Prüfungen vorgenommen /F2, 5-4/. So erfolgt eine Dichtheitsprüfung an den Schleusen und den Absperrklappen.

Die Bestimmung der Leckrate des Sicherheitsbehälters wird alle vier Jahre im Rahmen des Brennelementwechsels nach Abschluß aller Arbeiten an den Sicherheitsbehälterdurchführungen wiederholt. Dabei beträgt der Prüfüberdruck 0,5 bar. Unter Heranziehung der Meßergebnisse bei der Leckratenerstprüfung wird die Leckrate bei Auslegungsdruck ermittelt.

5.2 Vorgehen bei den Funktionsprüfungen

Die Funktionsprüfungen werden für die Komponenten des Reaktorschutzsystems folgendermaßen durchgeführt:

- Funktionsprüfungen der Anregeebene

Die Meßkanäle für die Zünddrehzahl der Diesel werden überprüft durch eine tatsächliche Veränderung der Meßgröße im Rahmen der vierwöchentlichen Funktionsprüfungen der Notstromdiesel (siehe unten). Die anderen Meßkanäle werden durch Simulation der Meßgrößen überprüft, z.B. durch Abdrücken der Bartonzellen. Zusätzlich werden die Meßkanäle ständig über Vergleicherbausteine überwacht, wobei auch die Referenzspannungen der Grenzsignalgeber ständig mitüberwacht werden. Dadurch werden solche Ausfälle entdeckt, die zu einer Veränderung eines einzelnen Meßsignals oder zu einer Veränderung der Referenzspannung eines Grenzsignalgebers führen. Weichen 2 Meßkanäle um mehr als 4 % voneinander ab, wird von den Vergleichern eine Notgefahrmeldung ausgelöst.

Die Grenzsignalgeber bilden die Schnittstelle zwischen der Anregeebene und der Logikebene.

- Funktionsprüfungen der Logikebene

Die Logikebene ist in "fail-safe"-Technik aufgebaut. Durch die dynamische Arbeitsweise werden auftretende Ausfälle sofort entdeckt; eine Ausnahme davon bilden nichtselbstmeldende gefährli-

che Ausfälle der Grenzsignalgeber /F2, 5-6/ oder der Binärsignaleingabe oder im Logikteil zur Bildung des Sumpfsignals. Diese Ausfälle werden aber bei den jährlichen Funktionsprüfungen der Logikebene entdeckt.

- Funktionsprüfungen der Steuerebene

Bei den regelmäßigen Funktionsprüfungen des Relaisteils, der logischen Verknüpfungen in Relaistechnik sowie der Zeitstufen werden durch Unterbrechen der Spannungsversorgung für die Abschlußglieder des dynamischen Teils die entsprechenden Reaktorschutzsignale ausgegeben. Durch dieses Prüfverfahren werden die Funktionen der ausgelösten Reaktorschutzsignale ab Abschlußglied, der angesteuerten Komponenten der Verfahrenstechnik und der elektrischen Energieversorgung überprüft.

In den verfahrenstechnischen Systemen werden dazu die bei Störfällen kontrollbetätigten Motorarmaturen vor Durchführung der Funktionsprüfungen verfahren. Diese Armaturen werden dann durch Simulation der beim Störfall anstehenden Reaktorschutzsignale wieder in Bereitschaftsstellung gebracht. Laufende Pumpen werden vor Simulation der entsprechenden Reaktorschutzsignale außer Betrieb genommen.

Bei den vierwöchentlichen Funktionsprüfungen der Notstromdiesel wird vor dem Öffnen des Einspeiseschalters einer 10-kV-Notstromschiene die nukleare Zwischenkühlpumpe sowie die Nebenkühlwasserpumpe der zugehörigen Redundanz gestartet. Außerdem werden die EIN-Tasten der Nachkühlpumpe bzw. HD-Sicherheitseinspeisepumpe sowie der Notspeisewasserpumpe bis zum automatischen Zuschalten dieser Pumpen betätigt. Dadurch wird das Notstromzuschaltprogramm vollständig getestet. Nach dem Wartungsplan des Motorherstellers ist der monatliche Probelauf der Notstromdiesel zwei Stunden lang durchzuführen.

Außerdem werden vom Reaktorschutz getrennte Funktionsprüfungen der elektrischen Energieversorgung und der Verfahrenstechnik vorgenommen. So werden im halbjährlichen Abstand die Notstromdiesel mit dem Netz synchronisiert und mit Vollast betrieben.

Bei den Batterien der Gleichstromversorgungen werden folgende Funktionsprüfungen durchgeführt:

- Kontrolle des Wasserstandes beim täglichen Rundgang,
- Messung der Säuredichte, Zellenspannung und Wassertemperatur an zwei bzw. vier Zellen jeder Batterie monatlich,
- wie oben, jedoch an allen Zellen jährlich und
- Kapazitätsprüfung durch Entladen der Batterie alle 5 - 6 Jahre.

Im Rahmen der jährlichen Funktionsprüfungen der Frischdampf-Sicherheitsventile werden die Komponenten im ausgebauten Zustand einer Sichtkontrolle unterworfen und auch die Reibungskräfte am Hauptventil gemessen. Außerdem wird die Funktion der Steuer- und Hauptventile durch Wegnahme der Zusatzbelastung mittels Handeingriffes noch vor Erreichen des Ansprechdrucks überprüft.

Die jährlichen Funktionsprüfungen der Druckhalter-Sicherheitsventile einschließlich der Steuerventile werden bei einem auf 100 bar reduzierten Systemdruck durchgeführt, wobei die Einrichtungen zur magnetischen Zusatzbelastung bei dem jeweils zu prüfenden Steuerventil demontiert und durch einen Meßhebel mit Zusatzgewichten ersetzt werden.

5.3 Zeitabstand zwischen den Funktionsprüfungen

Die Funktionsprüfungen werden im allgemeinen im Abstand von vier Wochen durchgeführt, die für die einzelnen Redundanzen zeitlich versetzt sind (jede Woche wird eine andere Redundanz überprüft). Ausnahmen davon bilden folgende jährlich durchgeführte Prüfungen:

- Anregeebene des Reaktorschutzssystems,
- Logikteil des Reaktorschutzsystems,
- Steuerstäbe mit den zur Reaktorschnellabschaltung notwendigen Funktionen,
- Gebäudeabschluß für den Reaktorkühlkreislauf und das Volumenregelsystem,
- Verriegelungen und Meldungen, mit Ausnahme der Notstromanlage,

- Kuppelschalter zwischen den kuppelbaren 380-V-Notstromschienen und Umschaltautomatiken der vom Block A aus versorgbaren Notstromschienen,
- mechanische Verriegelung von Armaturen,
- Prüfung der Durchflußmengen und des kF-Wertes der Nachwärmekühler sowie von sicherheitstechnisch wichtigen Kühlern im Nebenkühlwasser,
- Druckhalter-Sicherheits- und Abblaseventile,
- Frischdampf-Sicherheitsventile,
- Rückschlagklappen im Deionatsystem,
- letzte Rückschlagarmaturen, die das Not- und Nachkühlsystem vom Reaktorkühlkreislauf trennen (z.B. 20 TH11 S002, 20 TH12 S006) und
- letzte Rückschlagarmaturen vor den Dampferzeugern in den Einspeiseleitungen des Haupt- und Notspeisewassersystems (z.B. 20 RL10 S001, 20 RL13 S001).

Das Prüfen auf Öffnen dieser Rückschlagarmaturen kann ebenso wie das Prüfen der Meßkanäle, des Logikteils und der genannten Gebäudeabschlüsse nur nach Abfahren der Anlage durchgeführt werden. Dementsprechend sind jährliche Funktionsprüfungen in Verbindung mit dem Brennelementwechsel vorgesehen.

Das Prüfen auf inneren Bruch der Zweitabsperrarmaturen, die das Not- und Nachkühlsystem vom Reaktorkühlkreislauf trennen (z.B. der Rückschlagarmatur 20 TH11 S001), findet im Rahmen der wiederkehrenden Druckprobe des gesamten Reaktorkühlkreislaufs alle 8 Jahre statt.

Sicherheitsventile zur Druckabsicherung bestimmter Rohrleitungsabschnitte des Not- und Nachkühlsystems (z.B. 20 TH12 S008) werden alle 4 Jahre überprüft.

Die Überprüfung des Öffnens der Druckspeicher-Rückschlagventile sowie der Borkonzentration in den Druckspeichern geschieht im Abstand von 6 Monaten, die Borkonzentration in den Flutbehältern wird vierwöchentlich überprüft.

Die Umschaltung von einem auf den anderen Brennelement-Beckenkühlkreis wird einschließlich der Absperrarmaturen im nuklearen

Zwischenkühlkreis zum Beckenkühler in vierteljährlichem Abstand überprüft.

Das Notstandssystem wird jährlich überprüft. Dazu wird der Block B von der Warte des Blocks A aus abgefahren. Zusätzlich wird zweimal jährlich eine Alarmübung ohne Abfahren der Anlage durchgeführt. Es wird dabei lediglich die erforderliche Vorbereitungszeit für die notwendigen Handmaßnahmen ermittelt.

Nicht geprobt wird die Herstellung eines Rohwasseranschlusses. Es erfolgt aber im Anschluß an die Überprüfung des Notstandssystems eine Sichtkontrolle der Schläuche und Kuppelwerkzeuge für die Verbindung Feuerlöschsystem - Notspeisewassersystem.

Die an den Grenzsignalgebern des Reaktorschutzsystems eingestellten Referenzspannungen werden in vierteljährlichem Abstand überprüft.

Eine Funktionsprüfung der Meßkanäle und Meldeeinrichtungen ist für die "betrieblichen" Messungen des Drucks[1]) und des Wasserstands in den Druckspeichern, des Wasserstands in den Flutbehältern[1]) und des Wasserstands in dem Speisewasserbehälter[1]) nicht vorgesehen. Die Überprüfung der Analogwert-Anzeigen für die Flutbehälter-Wasserstände fällt aber zwangsläufig jährlich mit dem Brennelementwechsel zusammen. Die Meßkanäle und die Störungsmeldungen für die Messungen in den Druckspeichern sowie im Speisewasserbehälter werden bei den nach UVV /F2, 5-7/ vorgeschriebenen vierjährlichen inneren Prüfungen der Druckbehälter auf nichtselbstmeldende Ausfälle getestet. Es wurde davon ausgegangen, daß bei einem Nachfüllen von Stickstoff, zumindest aber einmal jährlich, die beiden vorhandenen Anzeigegeräte für den Wasserstand in den Druckspeichern auf Übereinstimmung geprüft werden.

Bei den Meßkanälen für den Wasserstand im Speisewasserbehälter wird davon ausgegangen, daß sie mindestens einmal jährlich zur

---

[1]) Diese "betrieblichen" Messungen sind zusätzlich zu den Reaktorschutzmessungen vorhanden.

Nachspeisung des Deionats in den Speisewasserbehälter betrieblich angefordert werden.

An Schleusen und an den Absperrklappen der Lüftungsleitungen wird jährlich eine Dichtheitsprüfung vorgenommen. Bei Durchführungen mit Abkammerungen befindet sich im Raum zwischen Rohrleitung und Durchführung ein Stickstoffpolster mit einer Druckanzeige. Der Stickstoffdruck wird mindestens einmal jährlich auf außergewöhnliche Abweichungen kontrolliert. Die Bestimmung der Leckrate des Sicherheitsbehälters wird alle 4 Jahre wiederholt.

Vollastprüfungen der Notstromdiesel werden in halbjährlichem Abstand durchgeführt. Die Überstromauslöser, die Verriegelungen und die Meldungen der Notstromanlagen werden, sofern sie nicht bei den vierwöchentlichen Funktionsprüfungen angefordert werden, im Abstand von 4 Jahren geprüft.

Eine Funktionsprüfung der Kühlmitteldruckregelung im Hinblick auf eine Ansteuerung der Druckhalter-Abblaseventile (Steuerventil, Steuer-Absperrventil und Abblase-Absperrventil) ist nicht vorgesehen.

Die Einrichtungen für die Stellungsmeldung der Rückschlagventile im Not- und Nachkühlsystem werden nicht überprüft. Ebenfalls keine Funktionsprüfung erfolgt für das Schließen der Rückschlagklappen nach den Hauptspeisewasserpumpen (20 RL01-03 S005). In solchen Fällen werden zur Abschätzung des Einflusses auf die Nichtverfügbarkeit als Zeitabstand zwischen den Funktionsprüfungen 10 Jahre angesetzt.

Generell wird davon ausgegangen, daß die Funktionen von Komponenten, für die keine Prüfungen vorgesehen sind, im Mittel alle 10 Jahre getestet werden. Ursache für solche Prüfungen können betriebliche Anforderungen sein oder Schwierigkeiten in der Ersatzteilbeschaffung für elektronische Komponenten, die dann erneuert werden.

Diese Vorgehensweise ist im Vergleich zu WASH-1400 pessimistisch. Dort wird in entsprechenden Fällen eine mittlere Aus-

fallentdeckungszeit von 6 Jahren angesetzt. Diese Zeitspanne ergibt sich als geometrisches Mittel der minimalen Ausfallentdekkungszeit von einem Jahr und der maximalen von 40 Jahren (WASH-1400, App. II, p. II-123 oder p. II-211).

6. ZUVERLÄSSIGKEITSANALYSE FÜR KÜHLMITTELVERLUSTSTÖRFÄLLE

6.1 Lecks in einer Hauptkühlmittelleitung

6.1.1 Annahmen und Voraussetzungen

Es wird vorausgesetzt, daß den untersuchten Kühlmittelverluststörfällen "großes Leck", "mittleres Leck" oder "kleines Leck" in einer Hauptkühlmittelleitung ein ungestörter Leistungsbetrieb, und zwar Vollastbetrieb vorausgeht, denn damit ergeben sich die größten Anforderungen an die Systemfunktionen.

Der Kühlmittelverluststörfall kann entweder im kalten oder im heißen Teil eines Hauptkühlkreislaufs auftreten. Für die durchgeführten Zuverlässigkeitsanalysen wird im folgenden der Bruch einer kalten Hauptkühlmittelleitung zugrunde gelegt. Der Bruch einer heißen Leitung führt im wesentlichen zu den gleichen Systemanforderungen. Für die numerische Auswertung wird der Eintritt des Lecks in Strang 1 unterstellt.

Es wird ferner davon ausgegangen, daß vor dem Störfall der Strang 3 des nuklearen Zwischenkühlkreislaufs, die Stränge 2 und 3 des nuklearen Nebenkühlwassersystems, die Teilsysteme UZ60 und UZ90 des Kaltwassersystems sowie eine der beiden Deionatpumpen in Betrieb waren (Abschnitte 4.2.2, 4.2.3, 4.2.8 und 4.2.11). Der Einfluß dieser Annahmen auf die Ergebnisse ist gering.

Zur Ausgangssituation bei Störfalleintritt wird weiterhin folgendes vorausgesetzt:

- Zum Zeitpunkt des Störfalleintritts sind entsprechend dem geregelten Wasserstand im Speisewasserbehälter ca. 320 t an Speisewasservorrat vorhanden. In den Deionatbehältern befinden sich entsprechend dem minimalen betrieblichen Soll-Wasserstand 600 t Deionat.
- Schäden an den Dampferzeugerrohren liegen nicht in einem solchen Ausmaß vor, daß der Störfallablauf beeinflußt wird.

Die Systemfunktionen zur Herstellung der Unterkritikalität und

zur Nachwärmeabfuhr sind (Fachband 1):

- Reaktorschnellabschaltung,
- Meßwerterfassung für die Notkühlvorbereitungssignale,
- Hochdruck-Einspeisungen,
- Druckspeicher-Einspeisungen,
- Niederdruck-Einspeisungen für Fluten,
- Niederdruck-Einspeisungen für Sumpf-Umwälzbetrieb,

  } Notkühlung

- Sicherheitsbehälter-Integrität für die Notkühlung,
- Hauptspeisewasserversorgung und Frischdampfabgabe,
- Notspeisewasserversorgung und Frischdampfabgabe und
- Langzeit-Notnachkühlung.

Für Lecks über 1000 cm^2 muß keine REAKTORSCHNELLABSCHALTUNG ausgelöst werden. Bei Versagen der Reaktorschnellabschaltung bewirkt der Verlust des Kühlmittels eine rasche Abschaltung des Reaktors über physikalische Effekte. Für Lecks unter 1000 cm^2 Querschnitt wird pessimistisch davon ausgegangen, daß die REAKTORSCHNELLABSCHALTUNG erforderlich ist. Dadurch wird die Anlage in den Zustand "unterkritisch heiß" übergeführt. Eine im Genehmigungsverfahren überprüfte Auslegungsbedingung ist, daß dieser unterkritische Zustand auch beim Abkühlen der Anlage aufrechterhalten wird. Dazu wird im Rahmen der Notkühlung boriertes Wasser aus den Borwasser-Flutbehältern und den Druckspeichern in die Hauptkühlmittelleitungen eingespeist. Unter dem Begriff Notkühlung werden dabei die HD-EINSPEISUNGEN, die DRUCKSPEICHEREINSPEISUNGEN und die ND-EINSPEISUNGEN FÜR FLUTEN sowie die ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB zusammengefaßt.

Bei Erreichen der Grenzwerte aus der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE werden die Notkühlung und der Abschluß der Durchführungen durch den Sicherheitsbehälter (der Gebäudeabschluß) automatisch eingeleitet.

Die Ausfallkriterien für die Systemfunktionen zur Nachwärmeabfuhr werden von den Mindestanforderungen abgeleitet (Tabelle F2, 6-1). Eine Systemfunktion gilt für die Analyse als vollständig ausgefallen, wenn weniger Teilsysteme zur Verfügung stehen, als im Genehmigungsverfahren zugrunde gelegt wurde.

Kühlmittelverlust-störfall	Bruchquerschnitt (cm^2)	Systemfunktionen					
		Hochdruck-Einspeisungen	Druckspeicher-Einspeisungen	Niederdruck-Einspeisungen für Fluten	Niederdruck-Einspeisungen für Sumpf-Umwälzbetrieb	Speisewasserversorgung (a) Hauptspeisewasser (b) Notspeisewasser	Langzeit-Notnachkühlung
großes Leck	> 400	-	heiß 3v4 kalt 2v4	heiß 2v4 kalt 1v4	heiß 2v4	-	heiß 1v4
mittleres Leck	80 - 400	2v4	heiß 2v4 kalt 2v4	heiß 2v4 kalt 1v4	heiß 2v4	-	heiß 1v4
kleines Leck	2 - 80	2v4	-	heiß 2v4 kalt 1v4	heiß 2v4	(a) 1v4[1]) oder (b) 2v4[2])	-
sehr kleines Leck	< 2	-	-	-	-	(a) 1v4[1]) oder (b) 1v4[2])	-

[1]) Einspeisungen über die Hauptspeisewasserleitungen in die Dampferzeuger
[2]) Einspeisungen über das Notspeisewassersystem in die Dampferzeuger
1v4, 2v4, 3v4 ≙ von 4 vorhandenen redundanten Teilsystemen sind 1, 2 bzw. 3 erforderlich

Tab. F2, 6-1:

Mindestanforderungen an die Systemfunktionen zur Nachwärmeabfuhr bei Lecks in einer kalten Hauptkühlmittelleitung

Bei einem großen Leck werden die HD-EINSPEISUNGEN nicht benötigt. Wenn kein Notstromfall vorliegt, werden die HD-Sicherheitseinspeisepumpen jedoch in jedem Fall gestartet. Um in den Zuverlässigkeitsuntersuchungen für große Lecks in einer Hauptkühlmittelleitung nicht unterscheiden zu müssen, in welchem Anfangszustand sich das Not- und Nachkühlsystem befindet, wird pessimistisch angenommen, daß immer die HD-EINSPEISUNGEN vor den ND-EINSPEISUNGEN FÜR FLUTEN stattfinden. Die Betriebszeit der HD-EINSPEISUNGEN und folglich der HD-Sicherheitseinspeisungen hängt von der Größe des Lecks ab. Die Betriebszeit nimmt mit kleiner werdender Leckgröße zu, beim Kühlmittelverluststörfall "kleines Leck in einer Hauptkühlmittelleitung" ist eine Betriebszeit von 2 Stunden zu erwarten. Die ND-EINSPEISUNGEN FÜR FLUTEN sind so lange aufrechtzuerhalten, bis die Flutbehälter entleert sind. Die ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB in mindestens 2 heiße Hauptkühlmittelleitungen sind bis etwa 5 Stunden nach Störfalleintritt notwendig.

Wichtig für die Aufrechterhaltung der Notkühlung ist, daß es zu keinem größeren Verlust von Dampf oder Wasser aus dem Sicherheitsbehälter kommt. Das heißt, die SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG muß gewahrt werden. Wegen der Kontamination des Sicherheitsbehälters nach einem großen oder mittleren Leck ist davon auszugehen, daß unter Umständen für mehrere Monate keine Arbeiten im Sicherheitsbehälter durchgeführt werden können. Während dieser Zeitspanne ist es daher nicht möglich, die Brennelemente aus dem Reaktordruckbehälter auszulagern, so daß eine LANGZEIT-NOTNACHKÜHLUNG durch mindestens eine in Sumpf-Umwälzbetrieb arbeitende ND-Einspeisung aufrechterhalten werden muß. In den Analysen wird von einem halben Jahr ausgegangen. Bis zu dieser Betriebszeit wird die Ausfallwahrscheinlichkeit der Systemfunktion durch "common mode"-Ausfälle (CMA) der Nachkühlpumpen bestimmt (Abschnitt 3.3.6.2.1). Nach einem halben Jahr kann etwa einen Tag auf die Notkühlung verzichtet werden, so daß dann zumindest provisorische Maßnahmen ergriffen werden können.

Bei einem kleinen Leck in einer Hauptkühlmittelleitung ist zusätzlich zur Notkühlung die Wärmeabfuhr über den Speisewasser-Dampf-Kreislauf erforderlich. Hierfür stehen grundsätzlich die

Systemfunktionen HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE sowie NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE zur Verfügung. Dabei wird von folgenden Anforderungen ausgegangen:

- Die Anlage ist abzufahren, wobei spätestens 60 Minuten nach Störfalleintritt mit dem Abfahren begonnen werden muß und ein Abfahrgradient von 100 °C/h einzuhalten ist. Ein zu spätes Abfahren oder ein zu niedriger Abfahrgradient kann aufgrund der Pumpenkennlinie der HD-Sicherheitseinspeisepumpen bzw. wegen des begrenzten Wasserinhalts der Flutbehälter zu einer unzulässigen Wasserspiegelabsenkung im Kern führen. Ein zu hoher Abfahrgradient kann dagegen das Reaktorschutzsignal YZ60 auslösen, das zur vorübergehenden Unterbrechung des Abfahrvorgangs führt. Für die Bewertung der Handmaßnahmen "Einleiten des Abfahrens" und "Einzeichnen des Abfahrgradienten 100 °C/h" wird pessimistisch davon ausgegangen, daß diese Handmaßnahmen innerhalb 30 Minuten nach Störfalleintritt durchgeführt werden (Abschnitte 6.1.4 und 6.1.2.2.15).
- Zum Abfahren über die Abblaseregelventile, d.h. bei Ausfall der Frischdampf-Umleiteinrichtung, ist die Funktion der beiden Abblaseregelventile erforderlich.

Bei der Bewertung der HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE sowie der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE ist zu berücksichtigen, daß die Meßumformer für die Hauptspeisewasser-Regelung und für die Notspeisewasser-Regelung nicht für die bei Kühlmittelverluststörfällen herrschenden Umgebungsbedingungen ausgelegt sind. Die Hauptspeisewasserversorgung wird daher als nicht verfügbar gewertet. Die Notspeisewasser-Regelventile werden hingegen durch Reaktorschutzsignale aufgefahren, wenn in einem der Dampferzeuger der Wasserstand unzulässig absinkt. Bei einem fälschlichen Zu-Befehl durch die Notspeisewasser-Regelung ist ein dauerndes Auf- und Zufahren der Regelventile nicht auszuschließen. Eine solche Betriebsweise entspricht nicht der Auslegungsgrundlage der Motorantriebe von Regelventilen, weshalb möglicherweise ein Auslösen des Motorschutzes erfolgt. Dabei wird die Sammelstörmeldung "Steuerkopf Störung" auf der Warte ausgegeben und der Regler automatisch auf Handbetrieb umgeschaltet. Folglich tritt auch unter ungünstigen Annahmen kein Ausfall der Notspeisewasserversorgung auf.

Die Einspeisungen durch das Notspeisewassersystem sind so lange aufrechtzuerhalten, bis die Nachwärmeabfuhr vollständig durch die ND-EINSPEISUNGEN übernommen wird. Dazu ist bei kleinen Lecks eine Überbrückung der Notkühlvorbereitungssignale und ein Auffahren der letzten Rückschlagarmatur in der heißen Einspeiseleitung eines funktionsfähigen Nachkühlstranges notwendig, der wie beim normalen Nachkühlen zu betreiben ist. Die Meßwerterfassung der Verriegelung dieser Armatur ist jedoch nicht für die bei Kühlmittelverluststörfällen herrschenden Umgebungsbedingungen ausgelegt. Aus diesem Grunde wurde davon ausgegangen, daß eine NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE für etwa 10 Stunden aufrechterhalten werden muß. Während dieses Zeitraums können geeignete Maßnahmen erfolgen, um die Verriegelung unwirksam zu machen.

6.1.2 Fehlerbaumbeschreibungen

6.1.2.1 G e s a m t f e h l e r b ä u m e

6.1.2.1.1 Allgemeines

Für die zu analysierenden Kühlmittelverluststörfälle "großes, mittleres und kleines Leck" in einer Hauptkühlmittelleitung liegen drei unterschiedliche Gesamtfehlerbäume vor (Anhang 2). Wegen der Anforderungen an die Speisewasserversorgung und Frischdampfabgabe beim kleinen Leck ist der Gesamtfehlerbaum in die Teile A und B untergliedert. Teil A enthält die Verknüpfungen der Ausfälle des Not- und Nachkühlsystems, Teil B die des Speisewasser-Dampf-Kreislaufs.

Die Gesamtfehlerbäume (Anhang 2) stellen im wesentlichen die Umsetzung der Ereignisablaufdiagramme (Fachband 1) unter Berücksichtigung der Mindestanforderungen an die Systemfunktionen (Tabelle F2, 6-1) dar. Das unerwünschte Ereignis des Fehlerbaumes (auch als TOP bezeichnet) bildet der "Systemausfall bei Anforderung". Der Ausfall der Systemfunktion REAKTORSCHNELLABSCHALTUNG ist in den Gesamtfehlerbäumen nicht enthalten, da hierzu eine gesonderte Zuverlässigkeitsanalyse vorliegt (Kapitel 8). Die

Ausfälle von Teilsystemfunktionen (z.B. HD-Einspeisung durch Strang 1) sind im allgemeinen als Überträge aus Teilfehlerbäumen dargestellt. In den Gesamtfehlerbäumen werden dabei insgesamt die Überträge folgender Teilfehlerbäume verknüpft (Anhang 3):

Fehlerbaum 1:	Deionatsystem (nur für das kleine Leck relevant)
Fehlerbäume 2 bis 5:	Notspeisewassersystem (nur für das kleine Leck relevant)
Fehlerbaum 6:	Notstandssystem (nur für das kleine Leck relevant)
Fehlerbaum 10:	Frischdampfsystem (nur für das kleine Leck relevant)
Fehlerbaum 15:	Reaktorschutzsystem
Fehlerbaum 17:	Not- und Nachkühlsystem, HD-Einspeisungen (nur für das mittlere und kleine Leck relevant)
Fehlerbaum 18:	Not- und Nachkühlsystem, ND-Einspeisungen
Fehlerbaum 19:	Not- und Nachkühlsystem, Druckspeicher-Einspeisungen (nur für das große und mittlere Leck relevant).

Die oben genannten Teilfehlerbäume enthalten ihrerseits Überträge aus dem Fehlerbaum 15 (Reaktorschutzsystem) und weiteren Teilfehlerbäumen, die die Ausfälle von Funktionen des nuklearen Zwischenkühlkreises, des nuklearen Nebenkühlwassersystems, des Kaltwassersystems und der elektrischen Energieversorgung im Notstromfall berücksichtigen.

Alle Teilfehlerbäume sind so aufgebaut, daß sie gemeinsam für alle analysierten Kühlmittelverluststörfälle und zum größten Teil auch für die Transientenstörfälle verwendet werden können.

Der Ausfall der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE (Übertrag aus Fehlerbaum 15) wird in Abschnitt 6.1.2.4.2 näher erläutert. Der Ausfall dieser Funktion ist in den Ausfallkombinationen für die einzelnen Notkühlvorbereitungssignale und damit für die entsprechenden Notkühlsysteme nicht enthalten.

Die Gesamtfehlerbäume enthalten zusätzlich die Ausfallkombinationen für das Versagen der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG. Der Austritt von Wasser oder Dampf aus dem Sicherheitsbehälter könnte nämlich zum Ausfall der Notkühlung führen. Die Ursachen sind:

- Ausfall von Komponenten im Ringraum aufgrund von Temperatur, Feuchte oder Druck oder wegen Flutung des Ringraums,
- Verlust von Sumpfwasser,
- Ausfall der Nachkühlpumpen aufgrund von Kavitation.

Es sind dabei folgende sechs Pfade für den Ausfall der Notkühlung zu unterscheiden:

- Ausfall der Notkühlung bei Versagen von Komponenten aufgrund von Leckagen aus dem Sicherheitsbehälter in den Ringraum

Bei Leckagen aus dem Sicherheitsbehälter in den Ringraum tritt eine erhöhte Beanspruchung der im Ringraum befindlichen und zur Störfallbeherrschung erforderlichen Komponenten auf. Bei großen Leckagen aus dem Sicherheitsbehälters in den Ringraum wird mit einem Versagen von Komponenten im Ringraum aufgrund von Temperatur, Feuchte oder Druck gerechnet. Das Versagen von Schweißnähten und Dichtungen mit einem solchen Leckquerschnitt wird im Gesamtfehlerbaum zum "Ausfall der Notkühlung aufgrund von Leckagen aus dem Sicherheitsbehälter in den Ringraum" zusammengefaßt. Ein Versagen des Abschlusses der Lüftungsleitungen der Unterdruckhaltung führt nicht zu Leckagen in den Ringraum, da Zu- und Fortluftleitung als druckfeste Stahlrohre durch den Ringraum geführt werden (Abschnitt 4.2.13).

- Ausfall des Not- und Nachkühlsystems bei Bruch der Nachkühlsaugleitung

Es ist nicht auszuschließen, daß Folgeschäden an der Nachkühlsaugleitung bei einem Bruch des Pumpenbogens der Hauptkühlmittelleitung auftreten. Beim Bruch der Nachkühlsaugleitung als Störfallfolge führt eine fälschlich offene Flutbehälter-Rückschlagklappe dazu, daß Dampf aus dem Sicherheitsbehälter in die

Flutbehälter und, ggf. nach einer Beschädigung der Flutbehälter, in den Ringraum strömt. In der Phase A der Risikostudie wird der Bruch der Nachkühlsaugleitung als Folgeausfall des Kühlmittelverluststörfalles mit der Wahrscheinlichkeit Null bewertet (Abschnitte 6.1.2.2.1 und 6.1.2.2.18).

- Ausfall des Not- und Nachkühlsystems bei offener Sumpfarmatur für Fluten

Bei einer während des Flutbetriebs fälschlich offenen Sumpfarmatur und einer fälschlich offenen Flutbehälter-Rückschlagklappe wird das vorhandene Sumpfwasser über die Flutbehälter in den Ringraum gedrückt (Abschnitt 6.1.2.2.18).

- Ausfall des Not- und Nachkühlsystems bei offenen Flutbehälterarmaturen für Sumpf-Umwälzbetrieb

Schließen bei Umschaltung auf Sumpfbetrieb die beiden Motorarmaturen in einer Flutbehälterleitung nicht, während die Sumpfarmatur öffnet, so kann das wie bei fälschlich offener Sumpfarmatur zum Ausfall der Notkühlung führen (Abschnitt 6.1.2.2.18).

- Ausfall des Not- und Nachkühlsystems bei Rückströmung durch einen HD-Einspeisestrang

Zum Ausfall der Notkühlung kann es auch kommen, wenn im Anschluß an die HD-EINSPEISUNGEN eine Rückströmung von Wasser durch einen HD-Einspeisestrang in die entsprechenden Flutbehälter erfolgt und das Wasser nicht mehr zurückgefördert werden kann (Abschnitt 6.1.2.2.18).

- Ausfall des Not- und Nachkühlsystems für Sumpf-Umwälzbetrieb bei Kavitation der Nachkühlpumpen

Um einen Ausfall der Nachkühlpumpen infolge Kavitation nach Umschaltung auf Sumpfbetrieb zu verhindern, ist bei bestimmten

Leckquerschnitten in einer Hauptkühlmittelleitung möglicherweise ein Überdruck im Sicherheitsbehälter erforderlich. Bei einer großen Leckage des Sicherheitsbehälters ist ein solcher Überdruck nicht vorhanden. Bei einem Ausfall des Gebäudeabschlusses für die Lüftungsleitungen könnte dies zum Ausfall der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG führen. Die Wahrscheinlichkeit für ein solches Versagen des Gebäudeabschlusses ist aber gegenüber den anderen Beiträgen vernachlässigbar gering.

Im folgenden wird kurz auf Ausfälle der anderen Systemfunktionen bei den einzelnen Störfällen eingegangen, wobei großes und mittleres Leck zusammengefaßt werden.

6.1.2.1.2 Großes und mittleres Leck

Die Verknüpfungen für die Systemfunktionen HD-EINSPEISUNGEN, DRUCKSPEICHER-EINSPEISUNGEN, ND-EINSPEISUNGEN FÜR FLUTEN und ND-EINSPEISUNGEN FÜR SUMPFUMWÄLZBETRIEB basieren auf den in Tabelle F2, 6-1 zusammengestellten Mindestanforderungen an diese Funktionen. Bei Nichterfüllen einer Mindestanforderung gilt die entsprechende Systemfunktion als ausgefallen (Abschnitt 6.1.1). Beispielsweise entspricht die Mindestanforderung an die HD-EINSPEISUNGEN für das mittlere Leck, nämlich 2 von 4 Teilsystemen (ein Teilsystem entspricht einem Einspeisestrang) müssen funktionieren, einer 3v4-Verknüpfung im Fehlerbaum. Dies bedeutet, bei Ausfall von (mindestens) 3 Einspeisesträngen ist die Systemfunktion ausgefallen.

Beim großen und mittleren Leck ist eine LANGZEIT-NOTNACHKÜHLUNG erforderlich, d.h. mindestens ein ND-Einspeisestrang für Sumpf-Umwälzbetrieb muß für etwa 6 Monate in Betrieb gehalten werden. In Abschnitt 3.3.6.2.2 wird die Ausfallwahrscheinlichkeit der Nachkühlpumpen während der Langzeit-Notnachkühlung zu $2 \cdot 10^{-4}$ abgeschätzt. Dieser Wert beinhaltet sowohl CMA als auch unabhängige Ausfälle. Wegen der erheblich günstigeren Bedingungen für Reparaturmaßnahmen können die Ausfälle der anderen Pumpen der Nachkühlketten vernachlässigt werden. Ausfälle von Armaturen spielen ebenfalls keine Rolle.

Die Wahrscheinlichkeit dafür, daß innerhalb der Zeitspanne der Langzeit-Notnachkühlung ein Notstromfall eintritt, beträgt $8 \cdot 10^{-2}$. Dieser Wert ergibt sich aus dem Ausfall eines Eigenbedarfstransformators und dem Ausfall beider Netzeinspeisungen (Abschnitt 7.1). Mit einer Wahrscheinlichkeit für den CMA der Notstromdiesel von $1,5 \cdot 10^{-3}$ (Anforderung und 2,5 Stunden Betrieb) erhält man eine Wahrscheinlichkeit von $1,2 \cdot 10^{-4}$ für einen Ausfall der gesamten Energieversorgung während der Langzeit-Notnachkühlung. Berücksichtigt man, daß im Mittel für mehrere Stunden die Nachwärmeabfuhr unterbrochen werden darf, so kann davon ausgegangen werden, daß CMA der Notstromdiesel keinen wesentlichen Beitrag zum Ergebnis für die Langzeit-Notnachkühlung liefern.

6.1.2.1.3 Kleines Leck

Teil A des Gesamtfehlerbaums für das kleine Leck in einer Hauptkühlmittelleitung enthält, entsprechend den Mindestanforderungen nach Tabelle F2, 6-1, neben den Verknüpfungen für die Systemfunktionen zur Notkühlung zusätzlich den Ausfall der Systemfunktionen für die Speisewasserversorgung und Frischdampfabgabe. Die Verknüpfungen für diese Systemfunktionen sind in Teil B des Gesamtfehlerbaums dargestellt. In diesem Teil des Gesamtfehlerbaums sind die vier grundsätzlichen Möglichkeiten zum sekundärseitigen Abfahren enthalten:

- Abfahren mit dem Hauptspeisewassersystem und der Frischdampf-Umleiteinrichtung,
- Abfahren mit dem Hauptspeisewassersystem und den Abblaseregelventilen (Abblasen über Dach),
- Abfahren mit dem Notspeisewassersystem bzw. Notstandssystem und der Frischdampf-Umleiteinrichtung und
- Abfahren mit dem Notspeisewassersystem bzw. Notstandssystem und den Abblaseregelventilen (Abblasen über Dach).

Aufgrund der Annahme, daß das Hauptspeisewassersystem nicht zur Verfügung steht (Abschnitt 6.1.1), erhält die entsprechende Verknüpfung in der numerischen Auswertung den Wert 1, d.h., die Sy-

stemfunktion HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE gilt als ausgefallen. Die Möglichkeit, bei Bedarf gleichzeitig über die Frischdampf-Umleiteinrichtung und die Abblaseregelventile abzufahren, wird in der Analyse nicht berücksichtigt.

Es ist zu beachten, daß die zum Abfahren erforderlichen Handmaßnahmen nicht oder fehlerhaft durchgeführt werden können. Diese Möglichkeiten sind in einem Übertrag aus Fehlerbaum 10 (Frischdampfsystem) unter "zu spätes Abfahren oder Abfahren mit falschem Abfahrgradienten" zusammengefaßt.

Bei ausgefallener HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE sind für eine erfolgreiche NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE mindestens zwei Einspeisungen durch das Notspeisewassersystem bzw. Notstandssystem erforderlich. Damit ergibt sich insgesamt eine 5v6-Verknüpfung für den Ausfall der Speisewasserversorgung: Es sind 4 Einspeisungen durch das Notspeisewassersystem und 2 Einspeisungen (Redundanz 1 und 3) durch das Notstandssystem vorhanden. In der numerischen Auswertung wird allerdings das Notstandssystem als zum Abfahren nicht einsetzbar betrachtet (Abschnitt 6.1.2.2.11, Fehlerbaum 6), so daß die Speisewasserversorgung beim Versagen von mindestens 3 von 4 Notspeisewassersträngen ausfällt. Steht die Frischdampf-Umleiteinrichtung zum Abfahren nicht zur Verfügung (Übertrag aus Fehlerbaum 10), so muß der Dampf über Dach abgeblasen werden. Ein Notspeisewasserstrang fällt auch dann aus, wenn keine Nachspeisung aus den Deionatbehältern, entweder direkt oder über den Speisewasserbehälter, zustande kommt (Überträge aus den Fehlerbäumen 1 B bis 1 E).

Die festgelegten Mindestanforderungen für die Speisewasserversorgung beziehen sich auch auf die Frischdampfleitungen, d.h. von den zwei bespeisten Dampferzeugern, die zum Abfahren erforderlich sind, muß der Frischdampf über die zugehörigen Frischdampfleitungen abgeführt werden können. Die entsprechenden Ausfallkombinationen sind in Überträgen aus Fehlerbaum 10 zusammengefaßt. Dabei wird unterschieden, ob das Abfahren über die Frischdampf-Umleiteinrichtung oder, bei deren Ausfall, über die

Abblaseregelventile erfolgt. In einem Fall wird der Frischdampf über die Frischdampf-Schnellschlußschieber, im anderen über die Absperrschieber in den Abfahrleitungen geführt. Der Frischdampf muß schließlich über die Frischdampf-Umleiteinrichtung bzw. über die Abblaseregelventile abgegeben werden können. Die entsprechenden Ausfälle sind wieder durch Überträge aus Fehlerbaum 10 dargestellt.

In der numerischen Auswertung der Fehlerbäume wird die Hauptspeisewasserversorgung wegen des Folgeausfalls der Meßumformer für die Regelung (Wahrscheinlichkeit $W_{13} = 1$) als ausgefallen betrachtet (Abschnitt 6.1.2.2.1). Die im Fehlerbaum dargestellten zusätzlichen Ausfallkombinationen haben deshalb nur formale Bedeutung. Die Hauptspeisewasserversorgung steht nämlich auch dann nicht zur Verfügung, wenn

- der Notstromfall (NSF) vorliegt, oder
- die Funktionsgruppensteuerung (FGS) für die Schwachlastregelung ausfällt, oder
- 1v4 Einspeisungen in die Dampferzeuger (HS1 bis HS4) ausfallen, oder
- bei Ausfall der Frischdampf-Umleiteinrichtung keine Deionatnachspeisung in den Speisewasserbehälter zustande kommt.

Die Funktionselemente HS1 bis HS4 enthalten die Regelarmaturen in den einzelnen Strängen einschließlich elektrischer Energieversorgung und Regelung, wobei die Ausfallarten "Regelarmatur öffnet nicht" bzw. "schließt fälschlich" unterstellt werden. Die Kombination 1v4 ergibt sich daraus, daß die Hauptspeisewasserversorgung durch die Auslösung des Notspeisezuschaltsignals (Kriterium Dampferzeugerwasserstand < 6,5 m) bei Ausfall von bereits einer Einspeisung außer Betrieb genommen wird. Für die Frischdampfstränge führt dagegen entsprechend den Mindestanforderungen nur der Ausfall aller vier Redundanzen zum Ausfall der Frischdampfabgabe.

6.1.2.2 Teilfehlerbäume der verfahrenstechnischen Systeme

6.1.2.2.1 Allgemeines

Zur Beherrschung der Kühlmittelverluststörfälle "großes, mittleres und kleines Leck" in einer Hauptkühlmittelleitung liegen folgende Teilfehlerbäume der verfahrenstechnischen Systeme vor (Anhang 3):

Fehlerbaum 1 A: Deionatsystem,
Einspeisung in den Speisewasserbehälter,
Fehlerbaum 1 B: Deionatsystem,
Einspeisung in den Notspeisewasser-Strang 1 (RL04),
Fehlerbaum 1 C: Deionatsystem,
Einspeisung in den Notspeisewasser-Strang 2 (RL05),
Fehlerbaum 1 D: Deionatsystem,
Einspeisung in den Notspeisewasser-Strang 3 (RL06),
Fehlerbaum 1 E: Deionatsystem,
Einspeisung in den Notspeisewasser-Strang 4 (RL07),
Fehlerbaum 2 : Notspeisewassersystem, Strang 1,
Fehlerbaum 3 : Notspeisewassersystem, Strang 2,
Fehlerbaum 4 : Notspeisewassersystem, Strang 3,
Fehlerbaum 5 : Notspeisewassersystem, Strang 4,
Fehlerbaum 6 : Notstandssystem,
Fehlerbaum 7 A: Nuklearer Zwischenkühlkreis, Stränge 1 und 2,
Fehlerbaum 7 B: Nuklearer Zwischenkühlkreis, Stränge 3 und 4,
Fehlerbaum 8 : Kaltwassersystem,
Fehlerbaum 9 A: Nukleares Nebenkühlwassersystem,
Stränge 1 und 2,
Fehlerbaum 9 B: Nukleares Nebenkühlwassersystem,
Stränge 3 und 4,
Fehlerbaum 10 A: Frischdampfsystem, Strang 1,
Fehlerbaum 10 B: Frischdampfsystem, Strang 2,
Fehlerbaum 10 C: Frischdampfsystem, Strang 3,

Fehlerbaum 10 D: Frischdampfsystem, Strang 4,
Fehlerbaum 16 A: Lüftungsanlagen,
Fehlerbaum 17 A: Not- und Nachkühlsystem,
HD-Einspeisungen, Stränge 1 und 2,
Fehlerbaum 17 B: Not- und Nachkühlsystem,
HD-Einspeisungen, Stränge 3 und 4,
Fehlerbaum 18 A: Not- und Nachkühlsystem,
ND-Einspeisung, Strang 1,
Fehlerbaum 18 B: Not- und Nachkühlsystem,
ND-Einspeisung, Strang 2,
Fehlerbaum 18 C: Not- und Nachkühlsystem,
ND-Einspeisung, Strang 3,
Fehlerbaum 18 D: Not- und Nachkühlsystem,
ND-Einspeisung, Strang 4,
Fehlerbaum 19 : Not- und Nachkühlsystem,
Druckspeicher-Einspeisungen.

Die Teilfehlerbäume für die verfahrenstechnischen Systeme sind aus Gründen der Übersichtlichkeit in die drei Ebenen Verfahrenstechnik, Energieversorgung und Steuerung (von rechts nach links) unterteilt. Der Ausfall einer aktiven verfahrenstechnischen Komponente wird im allgemeinen als ODER-Verknüpfung folgender Funktionselemente dargestellt (Beispiel aus Teilfehlerbaum 17 A: "Ausfall der Ölpumpe 21 TH15 D002"):

- Ausfall der Komponente selbst (z.B. "Ölpumpe 21 TH15 D002 startet nicht")

  Bei Pumpen werden grundsätzlich die Ausfallarten "Pumpe startet nicht" und "Pumpe fördert nicht" berücksichtigt. War die Pumpe vor Störfalleintritt in Betrieb, so kann die Ausfallart "Pumpe startet nicht" entweder nicht auftreten (Pumpe läuft ohne Unterbrechung weiter), oder vernachlässigt werden (mittlere Nichtverfügbarkeit der Pumpe wegen kurzer Zeitspanne zwischen Abschalten der Pumpe und Wiederstart vernachlässigbar). Je nach der zugrunde gelegten Betriebszeit der Pumpe im Störfall kann auch die Ausfallart "Pumpe fördert nicht" gegenüber dem Startversagen vernachlässigt werden. Bei Armaturen werden je nach Anforderung die Ausfallarten "öffnet nicht",

"schließt nicht", "regelt nicht" sowie "schaltet nicht um" (bei den Dreiwegeventilen im Not- und Nachkühlsystem) berücksichtigt. Bei Armaturen mit Motorantrieb ist jeweils der Ausfall des Antriebs mit enthalten.

- Ausfall des zugehörigen Verbraucherabzweiges der elektrischen Energieversorgung, bei Armaturen und bestimmten Pumpen einschließlich Gruppensicherung (z.B. "Abzweig- oder Kabelausfall", "Ausfall der Gruppensicherung")

  Die Verbraucherabzweige von Pumpen, die vor Störfalleintritt in Betrieb waren und ohne Unterbrechung weiterlaufen, brauchen nicht berücksichtigt zu werden.

- Ausfall der Sammelschiene der elektrischen Energieversorgung (z.B. "Ausfall der Schiene 21 FU")

  Die Ausfälle der Sammelschienen werden durch Überträge aus den Teilfehlerbäumen 13 A und 13 B beschrieben. Bei Kühlmittelverluststörfällen, bei denen kein Notstromfall eintritt, spielen diese Sammelschienen jedoch keine Rolle (Abschnitt 6.1.2.3.2).

- Ausfall der Steuerkette (z.B. "Steuerkette unterdrückt EIN-Befehl")

- Ausfall der Steuerung durch betriebliche Automatiken, Reaktorschutzsignale (z.B. "HD-Einspeisesignal 21 YZ36 U001 XU01 kommt nicht") oder durch nicht erfolgende oder fehlerhafte Handmaßnahmen

  Die Ausfälle von Reaktorschutzsignalen werden durch Überträge aus den Fehlerbäumen 15 A bis 15 D dargestellt. Das gleiche gilt für den Ausfall der 24-V-Versorgung in den Betätigungsschränken (z.B. "24 V im Betätigungsschrank 21 HA03 ausgefallen"). Betriebliche Signale oder Befehle von Hand können bei den meisten Komponenten nur wirksam werden, wenn sie vom Reaktorschutzsystem freigegeben werden. Zum Ausfall von Reaktorschutzsignalen kommt es vor allem durch Fehler, die auch gleichzeitig zum Ausfall des Freigabesignals führen (Kurzschlüsse). Wird eine Komponente im Störfall zunächst durch

ein Reaktorschutzsignal angefordert, so wird daher bei dessen Ausfall pessimistisch angenommen, daß dies zum Ausfall der gesamten Ansteuerung führt. Der Ausfall der Ansteuerung kann in der Regel vernachlässigt werden, wenn das Reaktorschutzsignal zeitverzögert zu einer eventuell vorhandenen betrieblichen Ansteuerung ansteht, da nun beide Befehle zueinander redundant sind (Doppelausfall).

- Speziell für Pumpen: Ausfälle der Ölversorgung oder der Kühlung (Umluft oder Kühlwasser)

  Diese Ausfälle werden durch Überträge aus den Fehlerbäumen 7 (Nuklearer Zwischenkühlkreis), 9 (Nukleares Nebenkühlwassersystem) und 16 (Lüftungsanlagen) beschrieben.

In den Beschreibungen der einzelnen Teilfehlerbäume wird bei der Behandlung der Komponentenausfälle auf die Verbraucherabzweige, Sammelschienen und Steuerketten im allgemeinen nicht mehr eingegangen.

Sind in den Teilfehlerbäumen, die auch für den "Notstromfall" (Kapitel 7) verwendet werden, Ausfallkombinationen enthalten, die nur für die Kühlmittelverluststörfälle Gültigkeit haben, so werden diese Ausfallkombinationen mit dem Funktionselement "KMV" (Kühlmittelverluststörfall) UND-verknüpft. In der numerischen Auswertung erhält dann das Funktionselement "KMV" bei den Fehlerbaumrechnungen für die Kühlmittelverluststörfälle die Wahrscheinlichkeit KMV = 1, beim "Notstromfall" dagegen die Wahrscheinlichkeit KMV = 0 (z.T. wird statt "KMV" auch "LOCA" verwendet, beide Funktionselemente haben die gleiche Bedeutung). Ausfallkombinationen, die nur bei den Kühlmittelverluststörfällen mit Eintritt des Notstromfalls oder beim "Notstromfall" gelten, werden mit dem Funktionselement "NSF" (Notstromfall) UND-verknüpft. Bei der numerischen Auswertung der Fehlerbäume für das große, mittlere und kleine Leck in einer Hauptkühlmittelleitung wird für NSF ein Median der Wahrscheinlichkeit von $NSF = 3 \cdot 10^{-3}$ eingesetzt (Abschnitt 6.1.2.3.2), bei den Rechnungen für den "Notstromfall" und das "kleine Leck am Druckhalter beim Notstromfall" dagegen die Wahrscheinlichkeit NSF = 1.

Beim "großen" und "mittleren Leck in einer Hauptkühlmittelleitung" erreichen die Einspeisungen durch den Strang des Not- und Nachkühlsystems, der zur gebrochenen Hauptkühlmittelleitung führt, den Reaktorkern nicht und sind damit als ausgefallen zu betrachten. Diese Ausfälle werden in den Fehlerbäumen durch die Funktionselemente LOCA 1 bis LOCA 4 berücksichtigt. Für das unterstellte Leck in der kalten Hauptkühlmittelleitung 1 (Abschnitt 6.1.1) ist daher bei den Rechnungen für das große und mittlere Leck LOCA 1 = 1 und LOCA 2 bis LOCA 4 = 0 zu setzen. Beim kleinen Leck in einer Hauptkühlmittelleitung wird hingegen LOCA 1 bis LOCA 4 = 0 gesetzt.

Beim Not- und Nachkühlsystem befinden sich normalerweise sämtliche Motorarmaturen in der für die HD-EINSPEISUNGEN und die ND-EINSPEISUNGEN FÜR FLUTEN richtigen Stellung. Ebenso sind die meisten Motorarmaturen der in Bereitschaft befindlichen Stränge des nuklearen Zwischenkühlkreises und des nuklearen Nebenkühlwassersystems in der für die Störfallbereitschaft richtigen Stellung. Diese Armaturen erhalten außerdem nach Erkennen des Störfalls durch das Reaktorschutzsystem noch einen diese Stellung kontrollierenden Befehl. Nach einer am Ende dieses Abschnitts durchgeführten Abschätzung von Ersatzausfallraten für kontrollverriegelte Motorarmaturen, deren Fehlstellung gemeldet wird, können deren Ausfälle vernachlässigt werden und sind deshalb in den Fehlerbäumen nicht enthalten.

Rohrleitungsausfälle sowie Versagen von anderen Bauteilen der verfahrenstechnischen Systeme, wie Kühler oder Armaturen aufgrund von Leckage oder Blockage des Durchflusses, werden bei der Erstellung der Fehlerbäume von Bereitschaftssystemen bzw. Bereitschaftskomponenten grundsätzlich berücksichtigt. Dort können latent solche Ausfälle vorliegen, die erst bei Inbetriebnahme des Systems bemerkt werden. Ein Ausfall von Rohrleitungen ist jedoch wesentlich seltener zu erwarten als ein Ausfall von zu betätigenden Komponenten und spielt daher bei der numerischen Auswertung der Fehlerbäume keine Rolle.

Dies gilt insbesondere auch für den vollständigen Bruch von Rohrleitungen im Not- und Nachkühlsystem, der innerhalb kurzer

Zeit den Verlust eines Großteils des Sumpfwassers in den Ringraum zur Folge haben und ein Eingreifen des Wartenpersonals unmöglich machen würde. Jede der Ansaugleitungen aus dem Reaktorgebäudesumpf ist nämlich als doppelwandige Rohrleitung ausgeführt; das Doppelrohr wird außerdem mit Stickstoff gefüllt und auf Dichtheit überwacht. Die für die ND-EINSPEISUNGEN wichtigen Rohrleitungen des Not- und Nachkühlsystems sind für einen Druck von 40 bzw. 50 bar ausgelegt, während sie nach dem Störfall nur bei Drücken von wenigen bar betrieben werden. Bei großen Leckagen der Einspeiseleitungen zwischen dem Druckspeicher und dem Reaktorkühlkreislauf handelt es sich um sofort entdeckte und reparierte Ausfälle.

- Folgeausfälle

Im Rahmen des Genehmigungsverfahrens wurden die bei verschiedenen Bruchlagen im Reaktorkühlkreislauf auftretenden Belastungen untersucht. Eine nochmalige Überprüfung der Auslegung war nicht Aufgabe der vorliegenden Studie (Abschnitt 3.3.4). Unterlagen aus dem Genehmigungsverfahren, nach denen Folgeschäden am Reaktorkühlkreislauf selbst auftreten könnten, liegen nicht vor. Entsprechende Folgeausfälle werden daher nicht unterstellt.

In den Fehlerbäumen werden die berücksichtigten Folgeausfälle durch Sekundäreingänge beschrieben. Die bei der Analyse der Systemfunktionen zur Beherrschung der Kühlmittelverluststörfälle berücksichtigten Sekundäreingänge sind in der Tabelle F2, 6-2 zusammengestellt. Sie werden im folgenden zusammenfassend behandelt.

Der Bruch der heißen Einspeiseleitung, die zum gebrochenen Hauptkühlkreislauf führt, ist als Störfallfolge durch Strahlkräfte oder durch die gebrochene Hauptkühlmittelleitung selbst denkbar (W_1): Ohne die in der Referenzanlage gegen Strahlkräfte ausgelegte Trennwand zwischen Dampferzeugerraum und TH-Armaturenkammer wurde im Genehmigungsverfahren davon ausgegangen, daß mit einer Wahrscheinlichkeit von $W_1 = 0,1$ beim Bruch der Hauptkühlmittelleitung mit einem Folgeausfall an der heißen Einspei-

Art des Folgeausfalls	Bezeichnung der Wahrscheinlichkeit	Wahrscheinlichkeit (Median/Streufaktor) bei einem			Fehlerbaum
		großen	mittleren Leck	kleinen	
Bruch der heißen Einspeiseleitung zum gebrochenen Hauptkühlkreislauf	W_1	0,01 K=10	0,01 K=10	0	17,18,19
Folgeausfall der heißen Druckspeicher-Einspeisung zum gebrochenen Hauptkühlkreislauf	W_2	0	1	-	19
Bruch von Rohrleitungen des nuklearen Zwischenkühlkreises innerhalb der Stahlhülle	W_3	1	1	1	7
Bruch der Nachkühlsaugleitung zum gebrochenen Hauptkühlkreislauf	W_5	0	0	0	18
Folgeausfall der Motorarmaturen zur Rückschaltung auf Flutbetrieb	W_6	1	1	1	18
Folgeausfall der betrieblichen Notspeisewasser-Regelung durch Dampfabgabe in den Sicherheitsbehälter	W_8	-	-	1	2,3,4,5
Folgeausfall der Hauptspeisewasser-Regelung durch Dampfabgabe in den Sicherheitsbehälter	W_{13}	-	-	1	Gesamtfehlerbaum

Tab. F2, 6-2:

Folgeausfälle bei einem Leck in einer Hauptkühlmittelleitung

seleitung zu rechnen ist. Aufgrund der verbesserten Schutzkonstruktionen, die einen derartigen Folgeschaden sehr unwahrscheinlich machen, wird die Wahrscheinlichkeit mit W_1 = 0,01 (Unsicherheitsfaktor K = 10) angesetzt.

Unter dem Folgeausfall der heißen Druckspeicher-Einspeisung zum gebrochenen Hauptkühlkreislauf wird die Entleerung des Druckspeichers über den kalten Strang verstanden, bevor eine heiße Einspeisung aufgrund des herrschenden Gegendrucks stattfindet (W_2). Bei großen Lecks findet eine derartige Entleerung nicht statt, entsprechend ist dafür eine Wahrscheinlichkeit 0 einzusetzen, bei einem mittleren Leck hingegen die Wahrscheinlichkeit 1 anzusetzen, da eine weitgehende Entleerung vor der Einspeisung stattfindet. Beim kleinen Leck werden die Druckspeicher-Einspeisungen nicht benötigt (Tabelle F2, 6-1).

Der Bruch von Rohrleitungen des nuklearen Zwischenkühlkreises innerhalb der Stahlhülle ist durch Beschädigung der Kühlwasserleitungen möglich, die zur Hauptkühlmittelpumpe des gebrochenen Kreislaufs führen (W_3). Dafür wird pessimistisch die Wahrscheinlichkeit 1 angesetzt.

Die für 40 bar ausgelegte Nachkühlsaugleitung TH12 Z01 ist zwischen Zweitabsperrung zum Primärkreis 20TH12 S003 und Durchführung durch die Stahlhülle teilweise ungeschützt vom Pumpenbogen der entsprechenden Hauptkühlmittelpumpe verlegt. Bei einem Leck im Pumpenbogen ist damit eine Beschädigung der angeführten Leitung möglich (W_5). Um beurteilen zu können, ob eine solche Beschädigung stattfindet, ist die Wirkung der Strahlkräfte auf die Nachkühlsaugleitung bei verschiedenen Rißlagen für Längs- und Rundrisse abzuschätzen. Eine erste Untersuchung hat gezeigt, daß ein Folgeausfall der Nachkühlsaugleitung als sehr unwahrscheinlich einzuschätzen ist. Bis zur Durchführung weitergehender Analysen wird eine Wahrscheinlichkeit von W_5 = 0 angesetzt.

Nach erfolgten HD-Einspeisungen kann es bei den ND-Einspeisungen für Sumpf-Umwälzbetrieb zu einer Rückströmung von Sumpfwasser durch einen HD-Einspeisestrang in die zugehörigen Flutbehälter kommen, wenn die entsprechenden Armaturen in diesem Strang

nicht schließen. Eine Rückförderung des Wassers aus den Flutbehältern ist dann möglich, wenn die Rückschaltung der entsprechenden ND-Einspeisung auf Fluten erfolgt. In diesem Fall wird nach Absinken des Flutbehälter-Wasserstandes erneut das Sumpfsignal ausgegeben. Als Folge davon steigt der Wasserstand wieder an. Es kommt somit zu einem häufigen Hin- und Herschalten zwischen Flut- und Sumpf-Umwälzbetrieb. Langfristig ist daher ein Ausfall dieser Rückschaltung aufgrund von Armatur-Ausfällen möglich. Es wird dafür pessimistisch von einer Wahrscheinlichkeit $W_6 = 1$ ausgegangen.

Die Meßumformer der Hauptspeisewasser- und Notspeisewasser-Regelungen sind nicht für die bei Kühlmittelverluststörfällen innerhalb des Sicherheitsbehälters herrschenden Umgebungsbedingungen ausgelegt. Es wird deshalb bei Kühlmittelverluststörfällen pessimistisch davon ausgegangen, daß aufgrund der Dampfabgabe in den Sicherheitsbehälter diese Meßwertumformer den auftretenden Temperaturen und der Feuchtigkeit nicht gewachsen sind. Für den Ausfall der betrieblichen Notspeisewasser-Regelung (W_8) und der Hauptspeisewasserregelung (W_{13}) wird daher die Wahrscheinlichkeit 1 angesetzt.

Eine Blockierung der Sumpfansaugung oder des Durchflusses im Nachwärmekühler eines Stranges als Störfallfolge wird bei den CMA des Teilfehlerbaums 18 behandelt.

Folgeausfälle sind auch durch Schwungradbruch oder durch das Nichtabschalten von Hauptkühlmittelpumpen denkbar. Darauf wird in den folgenden beiden Punkten detailliert eingegangen.

- Schwungradbruch

Beim Bruch der Hauptkühlmittelleitung zwischen Hauptkühlmittelpumpe und Einspeisestutzen in den Reaktordruckbehälter werden durch den ausströmenden Dampf das Pumpenlaufrad und damit der Rotor des Elektromotors und das Pumpenschwungrad beschleunigt. Als gefährdetster Teil ist das Schwungrad anzusehen. Bei Versagen der Schwungrad-Abwurfvorrichtung muß pessimistisch davon

ausgegangen werden, daß durch die entstehende Überdrehzahl ein Bersten des Schwungrades auftritt. Eines von zwei Bruchstücken würde nach Berücksichtigung der räumlichen Anordnung mit der Wahrscheinlichkeit 0,18 den zum gleichen Reaktorkühlkreislauf gehörenden Dampferzeuger treffen und mit der halben Wahrscheinlichkeit 0,09 den Dampferzeuger des benachbarten Reaktorkühlkreislaufs, so daß ein zweiter Reaktorkühlkreislauf beschädigt würde. Dadurch könnte ein nicht mehr beherrschbarer Kühlmittelverluststörfall hervorgerufen werden.

Entsprechend dem Verhältnis der Rohrleitungslängen der Hauptkühlmittelleitung kann die Wahrscheinlichkeit, daß es sich beim Störfall "großes Leck in einer Hauptkühlmittelleitung" um einen Bruch in dem für das Schwungradbersten maßgebenden Teil der kalten Hauptkühlmittelleitung handelt, zu 0,32 angesetzt werden. Wenn nicht die Rohrleitungslängen maßgebend sind, sondern die Anzahl der Schweißnähte, so erhält man eine Wahrscheinlichkeit von 0,37, also praktisch den gleichen Wert. Unterstellt man, daß die Abwurfeinrichtung in 1 % der Anforderungsfälle versagt, so ergibt sich für einen durch die Sicherheitssysteme nicht beherrschten Störfall "großes Leck" aufgrund des Schwungradbruchs eine Wahrscheinlichkeit von

$$0{,}09 \cdot 0{,}32 \cdot 10^{-2} = 3 \cdot 10^{-4}$$

Diese Nichtverfügbarkeit liegt dann bereits unter der mit Hilfe der Fehlerbaumanalyse ermittelten Wahrscheinlichkeit für das nicht beherrschte "große Leck".

Bei diesem Wert ist nicht berücksichtigt, daß es nicht bei jedem Kühlmittelverluststörfall zum Hochlaufen der Pumpe kommt. So wird z.B. bei Vorliegen eines 2F-Bruchquerschnitts durch das anstehende Druckgefälle ein Moment erzeugt werden, das die Bogenzahnkupplung nicht verkraftet. Damit sind die Schwungmassen von Elektromotor und Schwungrad nicht mehr aktiv. Es kommt somit nur zu einem Hochlaufen und Blockieren des Laufrades.

Ein Bersten des Schwungrades ist bei Drehzahlen von etwa 5000 U/min zu erwarten. Die installierte Schwungrad-Abwurfeinrichtung

soll ein Lösen des Schwungrades bei 2400 U/min sicherstellen. Als Streuband wurde von den Gutachtern eine Drehzahl von ± 150 U/min festgesetzt. Anhand einer Fehlerrechnung konnte nachgewiesen werden, daß sich die Abwurfdrehzahl in einem wesentlich engeren Bereich (± 60 U/min) theoretisch vorhersagen läßt. Diese Aussage konnte auch in einem Versuch /F2, 6-1/ nachgewiesen werden, bei dem die Abwurfdrehzahl nahezu exakt vorhergesagt wurde.

Unter diesen Voraussetzungen kann davon ausgegangen werden, daß ein Versagen des Schwungrades infolge Hochlaufens des Pumpenaggregates praktisch ausgeschlossen werden kann.

- Keine Abschaltung von Hauptkühlmittelpumpen

Die Wirksamkeitsuntersuchungen zur Notkühlung wurden unter der Voraussetzung durchgeführt, daß die Hauptkühlmittelpumpen zum Zeitpunkt des Störfalls oder kurzzeitig später abgeschaltet werden. Zuverlässigkeitsuntersuchungen des Abschaltverhaltens der Hauptkühlmittelpumpen zeigen jedoch, daß ein Weiterlaufen von Pumpen nach Eintritt eines Kühlmittelverluststörfalls nicht auszuschließen ist. Untersuchungsergebnisse aus Druckentlastungsrechnungen sowie Kernaufheizrechnungen bezüglich der Wirksamkeit der Kernnotkühlung bei laufenden Hauptkühlmittelpumpen lassen erkennen, daß es beim 2F- und 1F-Bruch in einem kalten Strang zu einer höheren, bei kleineren Bruchgrößen dagegen zu einer niedrigeren Kernaufheizung kommt. Im Vergleich zum Pumpenauslauf, wie er für die Mindestanforderungen an die Notkühlung entsprechend Tabelle F2, 6-1 angenommen wurde, führt das Durchlaufen der Pumpen also bei sehr großen Lecks im kalten Strang einer Hauptkühlmittelleitung zu einer Gefährdung des Kerns.

Die Abschaltung der Hauptkühlmittelpumpen erfolgt

- durch das Gebäudeabschlußsignal für die Hauptkühlmittelpumpen,
- durch den Pumpenschutz und
- im Notstromfall durch Spannungsausfall an den 10-kV-Normalnetzschienen 0 BA, 0 BB, 0 BC, 0 BD.

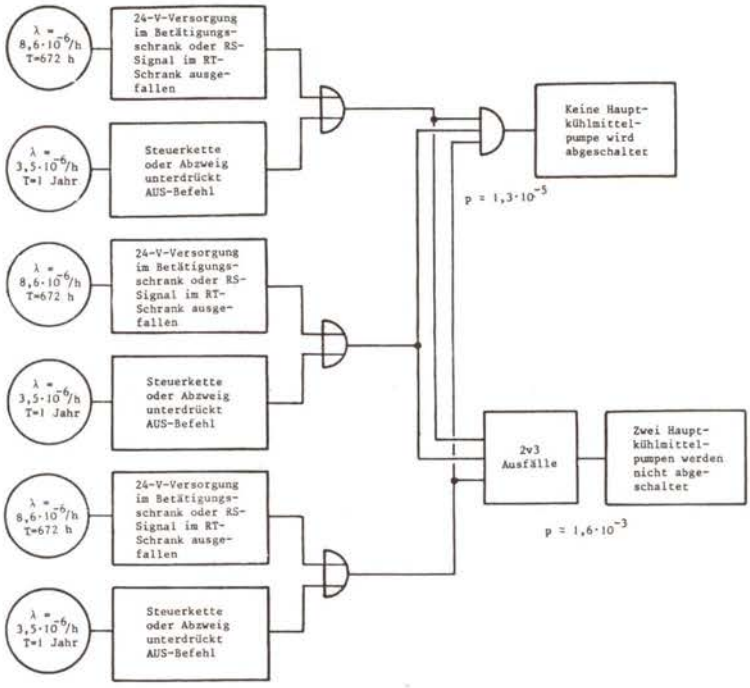


Bild F2, 6-1:

Fehlerbaum für das Versagen der Abschaltung der Hauptkühlmittelpumpen (Erwartungswerte)

Die Abschaltung würde auch durch einen Notstromfall, der als Folge des Kühlmittelverluststörfalls eintritt, ausgelöst werden. Ein solcher Notstromfall ist aber sehr unwahrscheinlich und würde möglicherweise zeitverzögert eintreten. Eine Abschaltung der Hauptkühlmittelpumpen durch einen Notstromfall wird daher nicht berücksichtigt. Die Ausfälle, die zum Versagen der Abschaltung der Hauptkühlmittelpumpen führen, sind aus dem Fehlerbaum in Bild F2, 6-1 ersichtlich. Dabei werden nur die Ausfälle berücksichtigt, die einen nicht zu vernachlässigenden Beitrag zum Gesamtergebnis liefern. Es sind dies der Ausfall der Steuerkette, der 24-V-Versorgung im Betätigungsschrank und der Ausfall der Ansteuerung durch das Gebäudeabschlußsignal aufgrund von Kurzschlüssen im Relaisteilschrank.

Die Abschaltung durch den Pumpenschutz kann bei einem Kurzschluß im Relaisteilschrank nicht erfolgen, da hierdurch auch das erforderliche Freigabesignal ausfällt.

Bei den oben erwähnten thermohydraulischen Untersuchungen wurden unter der Voraussetzung, daß alle drei zu den intakten Hauptkühlkreisläufen gehörenden Hauptkühlmittelpumpen nach Störfalleintritt weiterlaufen, beim 2F- und 1F-Bruch Kühlmitteltemperaturen von über 1 200 °C ermittelt (Fachband 1).

Würde bereits der Ausfall der Abschaltung von zwei der drei zu den intakten Hauptkühlkreisläufen gehörenden Hauptkühlmittelpumpen zu solchen Kühlmitteltemperaturen und damit zu veränderten Wirksamkeitsbedingungen der Notkühlung führen, so hätte man diese mit einer Wahrscheinlichkeit von

$$\bar{p} \cong 1{,}6 \cdot 10^{-3}$$

in Rechnung zu stellen. Aufgrund der durchgeführten Untersuchungen sind veränderte Wirksamkeitsbedingungen zu berücksichtigen, wenn keine der drei Hauptkühlmittelpumpen abgeschaltet wird. Dafür ergibt sich eine zu vernachlässigende Wahrscheinlichkeit von

$$\bar{p} \cong 1{,}3 \cdot 10^{-5}$$

Die Zeitabstände T zwischen den Funktionsprüfungen sind im Fehlerbaum eingetragen.

- Berücksichtigung der Instandhaltung

In den Teilfehlerbäumen der Bereitschaftssysteme werden die mittleren Nichtverfügbarkeiten der einzelnen Stränge aufgrund von Instandhaltungsmaßnahmen (Wartung, Instandsetzung) durch Ersatzkomponenten berücksichtigt (zur Ermittlung der entsprechenden Ausfallwahrscheinlichkeiten pro Anforderung siehe Abschnitt 3.5 und Fachband 3). Pro Strang eines verfahrenstechnischen Systems wird eine Ersatzkomponente eingeführt (z.B. für Notspeisewasserstrang RL04: "I RL04"), die die während des Leistungsbetriebes reparierbaren verfahrenstechnischen Komponenten dieser Redundanz enthält. Bei der Bildung dieser Ersatzkomponen-

ten werden auch solche Pumpen, Armaturen und Sicherheitsventile berücksichtigt, die im Störfall nicht benötigt werden und somit im Fehlerbaum nicht auftreten, während ihrer Wartung eine Bereitschaftsfunktion des Stranges jedoch nicht ermöglichen. Durch die Art der Verknüpfung in den Teilfehlerbäumen sind im Ergebnis für Kernschmelzen Doppel- und Mehrfachausfälle aufgrund von Instandhaltung enthalten. Nach /F2, 6-2/ ist jedoch die Anlage bei Ausfall von zwei Strängen des Not- und Nachkühlsystems abzufahren, d.h. Instandhaltungsvorgänge an zwei Strängen sind nur bei abgefahrener Anlage zulässig. Die vereinfachte Behandlung im Fehlerbaum spielt bei der numerischen Auswertung keine Rolle.

- Ersatzausfallrate einer kontrollverriegelten Armatur mit Motorantrieb

Die Ersatzausfallraten kontrollverriegelter Armaturen, die nur zum Zeitpunkt des Störfalls einen die Stellung kontrollierenden Befehl erhalten, aber nicht zu einem späteren Zeitpunkt durch einen anderen Reaktorschutzbefehl angesteuert werden, lassen sich mit Hilfe des im folgenden beschriebenen Fehlerbaumes abschätzen. Dieser gilt nur für solche Armaturen, bei denen neben den sonst üblichen Stellungsmeldelampen im Tischfeld eine Notgefahrmeldung vorhanden ist. Die Notgefahrmeldung spricht an, wenn sich die Armatur während des Normalbetriebs des Kraftwerks in der falschen Stellung befindet. Zur Abschätzung der eingetragenen Ausfallraten λ und Wahrscheinlichkeiten p genügt es, sich auf den Versagensfall zu beziehen, der die größte Ausfallwahrscheinlichkeit liefert. Aus diesem Grunde wurde der Fehlerbaum für eine Armatur aufgestellt, die sich normalerweise in geöffnetem Zustand befindet. Bei der eingesetzten SIMATIC-P-Steuerung sind die Ausfallraten für die unterschiedlichen Ausfallarten der Steuerkette einer normalerweise geschlossenen Armatur kleiner als die einer normalerweise geöffneten Armatur. Die Ausfallraten der Armatur für die Ausfallarten "öffnet nicht" und "schließt nicht" sind gleich groß. Ebenso sind die Wahrscheinlichkeiten eines falschen Handbefehls für Öffnen oder Schließen ungefähr gleich groß. Bei Ansteuerung des Betätigungsbausteins über den Vorrangbaustein ergibt sich die Ausfallrate aus "fälschlichem

Befehl durch Ausfälle im Betätigungsbaustein mit Vorrang" und aus Fehlern in der Verdrahtung zwischen Vorrang- und Betätigungsbaustein ("mit Vorrang" heißt hier, daß der fälschliche ZU-Befehl im Betätigungsbaustein vorrangig behandelt wird und ein Öffnen durch den Kontrollbefehl nicht mehr möglich ist). Für die Abschätzung der Ausfallwahrscheinlichkeit der 380-V-Sammelschiene wurde pessimistisch angenommen, daß die betrachtete Armatur von einer nicht kuppelbaren Schiene versorgt wird.

Als obere Schranke für die Ersatzausfallwahrscheinlichkeit einer Motorarmatur, die zum Zeitpunkt des Störfalls einen die Stellung kontrollierenden Befehl erhält, ergibt sich demnach $2 \cdot 10^{-5}$ (Bild F2, 6-2).

Wenn der Ausfall der kontrollverriegelten Motorarmatur mit dem Ausfall einer beim Störfall betätigten Motorarmatur oder Pumpe der gleichen Redundanz im Fehlerbaum logisch ODER-verknüpft ist, so braucht der Ausfall der 380-V-Sammelschiene der Energieversorgung nicht berücksichtigt zu werden. Falls darüber hinaus der Ausfall der betrachteten kontrollverriegelten Motorarmatur mit dem Versagen einer vom gleichen Reaktorschutzsignal angesteuerten Komponente im Fehlerbaum logisch ODER-verknüpft ist, braucht bei der Ermittlung der Ersatzausfallrate der kontrollverriegelten Motorarmatur auch der Ausfall des Reaktorschutzsignals nicht berücksichtigt zu werden. Die entsprechende Ersatzausfallwahrscheinlichkeit ist in diesem Fall kleiner als $1{,}8 \cdot 10^{-5}$ (siehe die in Klammern eingetragenen Werte im Fehlerbaum).

Hieraus läßt sich ableiten, daß kontrollverriegelte Motorarmaturen im Fehlerbaum für die ND-Einspeisungen durch das Not- und Nachkühlsystem nicht berücksichtigt zu werden brauchen. Dort ist nämlich der Ausfall einer solchen Armatur stets mit einer im Störfall zu betätigenden Pumpe oder Armatur der gleichen Redundanz logisch ODER-verknüpft. Die entsprechende Ersatzausfallwahrscheinlichkeit ist also in diesem Fall kleiner als $2 \cdot 10^{-5}$, was gegenüber einer Ausfallwahrscheinlichkeit von ca. $4 \cdot 10^{-3}$ für eine zu betätigende Motorarmatur bzw. $5 \cdot 10^{-3}$ für eine zu startende Pumpe vernachlässigbar ist. Zugrunde gelegt wird jeweils ein Zeitabstand von vier Wochen zwischen den Funktionsprüfungen.

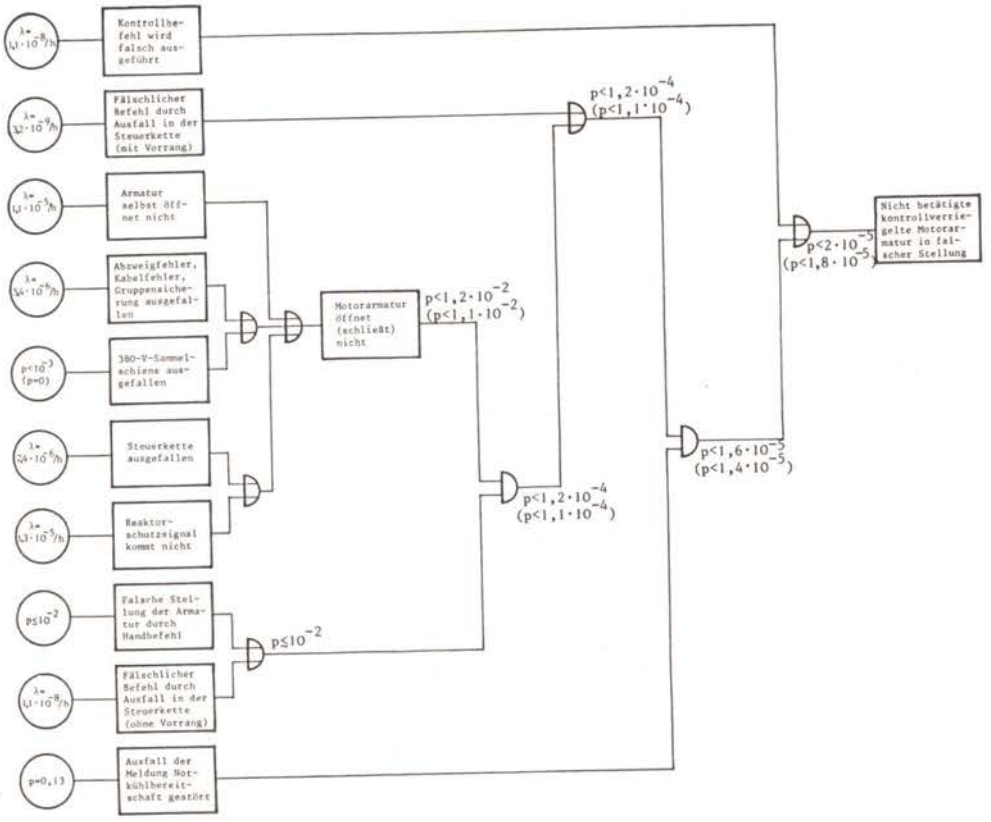


Bild F2, 6-2:

Fehlerbaum für den Ausfall einer nicht betätigten Motorarmatur, die nur durch einen Kontrollbefehl angesteuert wird (Erwartungswerte)

Im Fehlerbaum für die Druckspeichereinspeisungen durch das Not- und Nachkühlsystem wäre für jede der Druckspeichereinspeisungen auch eine kontrollverriegelte Motorarmatur einschließlich Energieversorgung zu berücksichtigen. Die entsprechenden Ersatzausfallwahrscheinlichkeiten betragen ca. 1 % der in dieser Untersuchung verwendeten Ausfallwahrscheinlichkeiten für die jährlich getesteten Rückschlagarmaturen der heißen bzw. kalten Druckspeichereinspeisungen. Im Fehlerbaum für die Druckspeichereinspeisungen können daher die kontrollverriegelten Motorarmaturen vernachlässigt werden.

6.1.2.2.2 Fehlerbaum 1 A: Deionatsystem, Einspeisung in den Speisewasserbehälter

Die Deionatförderung in den Speisewasserbehälter fällt aus, wenn

- die Leitung von den Deionatbehältern zum Speisewasserbehälter nicht freigeschaltet wird,
- beide Deionat- oder beide Druckerhöhungspumpen nicht starten oder deren Pumpenrückschlagklappen nicht öffnen, wobei das Starten der Pumpen automatisch durch einen Niveauschalter oder durch einen Handbefehl erfolgt,
- die Pumpenrückschlagklappen der nicht in Betrieb befindlichen Pumpen nicht schließen,
- die Rückschlagklappe 20 RY10 S005 nicht schließt,
- der Druckschalter 20 RF50 P001 im Speisewasserbehälter zu früh anspricht und die Druckerhöhungspumpen abschaltet und
- die Deionatleitung zum Kondensator nicht abgesperrt wird.

Zum Freischalten der Deionatleitung zum Speisewasserbehälter müssen drei Armaturen öffnen:

- der Absperrschieber 22 RY10 S001, der sich bereits bei normalem Leistungsbetrieb des Kraftwerks in AUF-Stellung befinden sollte,
- die Regelarmatur 24 RY10 S002, die durch den Niveauschalter 20 RF50 L003 aufgefahren wird oder von Hand geöffnet werden muß und
- die Rückschlagklappe 20 RY10 S001.

Die genannten Handmaßnahmen sind im Fehlerbaum zu einem Funktionselement (L 451 OP RY10/11) zusammengefaßt: "Kein EIN-Befehl von Hand für Deionatpumpen oder Druckerhöhungspumpen bzw. kein AUF-Befehl von Hand für die Armaturen im Deionatzulauf zum Speisewasserbehälter bei Kühlmittelverluststörfällen" (Kurzform im Fehlerbaum: Keine Inbetriebnahme Deionatförderung bei Kühlmittelverluststörfällen). Sie sind ca. 30 Minuten nach Störfalleintritt durchzuführen, wobei für die Bewertung berücksichtigt wurde, daß zwar dazu im Betriebshandbuch keinerlei Hinweise vorliegen, jedoch eine Prozeßrechnermeldung und eine Notgefahrmeldung auf die Notwendigkeit der Deionateinspeisung hinweisen.

Die Handmaßnahme L 451 OP RY10/11 wird mit dem Ereignis Kühlmittelverluststörfall (KMV) UND-verknüpft, wobei für die Rechnung zum kleinen Leck in einer Hauptkühlmittelleitung die Wahrscheinlichkeit für KMV gleich 1 ist. Wegen der unterschiedlichen Bewertung der genannten Handmaßnahme beim "Notstromfall" wird dafür das Funktionselement L 449 OP RY10/11 eingeführt und mit dem Funktionselement NSF (Notstromfall) UND-verknüpft.

Ein Ausfall der Deionatpumpen 20 RY21/22 D001 sowie der Deionat-Druckerhöhungspumpen 20 RY11/12 D001 durch Fehler in der Steuerebene liegt vor, wenn der EIN-Befehl durch die jeweilige Steuerkette unterdrückt wird oder der Niveauschalter 20 RF50 L003 im Speisewasserbehälter nicht anspricht und gleichzeitig kein Startbefehl per Hand ausgegeben wird (Handmaßnahme L 451 OP RY10/11). Diese Ansteuerung wird zur Vereinfachung des Fehlerbaums direkt ins TOP des Fehlerbaums 1 A (Anhang 3) geführt.

Zum unmittelbaren Ausfall der Deionatförderung in den Speisewasserbehälter kann der Druckfühler 20 RF50 P001 führen. Dieser Druckschalter kann so ausfallen, daß er zu früh anspricht und die Druckerhöhungspumpen abschaltet. Da die Deionatpumpen nur über eine Förderhöhe von 7,8 bar verfügen, sind sie dann nicht mehr in der Lage, gegen den im Speisewasserbehälter herrschenden Druck zu fördern.

Die den beiden Deionat-Druckerhöhungspumpen parallel geschaltete Rückschlagklappe 20 RY10 S005 hat zweierlei Funktionen zu erfüllen: Sie muß bei Betrieb der Druckerhöhungspumpen schließen, um eine Kurzschlußströmung zu verhindern. Nach deren Abschalten muß sie öffnen, um das Einspeisen mit den Deionatpumpen zu ermöglichen. Ein Versagen dieser Rückschlagklappe führt somit ebenfalls zum Ausfall der Deionateinspeisung.

Das Kondensatorregelventil 21 RY20 S002 oder der Absperrschieber 24 RY20 S004 muß laut Betriebshandbuch beim Freischalten der Deionatleitung zum Speisewasserbehälter geschlossen werden, da andernfalls die Deionatpumpen nur in den Kondensator fördern. Im Kühlmittelverluststörfall erhalten diese Armaturen vom Reaktorschutzsystem einen Schließbefehl. Bei Ausfall der Reaktor-

schutzsignale YZ81 kann diese Leitung nicht abgesperrt werden. Schließbefehle von Hand können nicht mehr gegeben werden, da die Freigabe durch das Reaktorschutzsystem fehlt.

6.1.2.2.3 Fehlerbaum 1 B: Deionatsystem, Einspeisung in den Notspeisewasser-Strang 1 (RL04)

Wird kein Deionat in den Speisewasserbehälter gefördert, so muß auf direktes Ansaugen aus den Deionatbehältern umgeschaltet werden. Die Speisewasserversorgung durch das Deionatsystem über den Notspeisewasserstrang RL04 fällt daher aus, wenn sowohl die Deionatförderung in den Speisewasserbehälter (Übertrag aus Fehlerbaum 1 A, Anhang 3) als auch die Direkteinspeisung in den Notspeisewasserstrang versagt.

Ausgehend von einem Druck im Speisewasserbehälter von 10,2 bar bei Eintritt des Störfalls, sinkt der Druck ohne Einspeisung von kaltem Deionat im Speisewasserbehälter nur sehr langsam, so daß bei Erreichen seines minimalen Wasserstandes immer noch ein Druck von mehr als 2 bar herrscht. Damit ist bei der Umschaltung auf direkte Deionatversorgung eine zusätzliche Deionateinspritzung in die Notspeisewasser-Saugleitung notwendig.

Um diese Deionateinspritzung zu ermöglichen, ist es notwendig, die Deionatleitungen zum Speisewasserbehälter und zum Kondensator abzusperren. Die Armaturen in der Leitung zum Speisewasserbehälter erhalten dazu von den Deionatzuschaltsignalen YZ61 ZU-Befehle. Die Ausfallkombinationen, die zum Nichtabsperren der Leitung zum Kondensator führen, entsprechen denen im Fehlerbaum 1 A. Das Schließen jeweils einer Armatur in einer Leitung ist dabei ausreichend.

Die Deionateinspritzung in die Notspeisewasserstränge RL04 und RL05 fällt außerdem aus, wenn

- nicht mindestens je eine Deionatpumpe und eine Druckerhöhungspumpe starten und deren Pumpenrückschlagklappen öffnen,
- die Pumpenrückschlagklappen der nicht in Betrieb befindlichen Pumpen nicht schließen,

- die Rückschlagklappe 20 RY10 S005 nicht schließt und damit eine Kurzschlußströmung entsteht.

Neben diesen Ausfallkombinationen führt auch noch das Versagen der folgenden Komponenten (speziell im Strang RL04) zum Ausfall der Deionatversorgung:

- Das Einspritzventil 21 RY23 S004 oder die Rückschlagklappe 20 RY23 S006 öffnet nicht,
- der Deionatsaugschieber 21 RL04 S018 oder die Rückschlagklappe 20 RL04 S011 öffnet nicht - der Notspeisesaugschieber 21 RL04 S019 und die Rückschlagklappe 20 RL04 S002 schließen nicht.

Für die Ansteuerung der Deionatpumpen gilt das im Fehlerbaum 1 A Gesagte. Zusätzlich wird noch ein EIN-Befehl von null-redundanten Deionatzuschaltsignalen gegeben, so daß wegen der Notwendigkeit von Doppelausfällen der Ausfall des EIN-Befehls nicht berücksichtigt zu werden braucht. Ein fälschliches Ansprechen des Druckfühlers 20 RF50 P001 führt somit auch in diesem Fall zur Abschaltung der Druckerhöhungspumpen und damit zum Ausfall der Deionateinspritzung in den Redundanzen 1 und 2 des Notspeisewassersystems.

Im Gegensatz dazu werden die Einspritzventile sowie die Deionat- und Notspeisesaugschieber von Deionatzuschalt- bzw. Deionatsignalen in Reaktorschutzqualität angesteuert.

Nicht im Fehlerbaum berücksichtigt wurde, da ihr Beitrag zur Nichtverfügbarkeit der Notspeisewasserversorgung und Frischdampfabgabe zu vernachlässigen ist, die Ausfallkombination: gleichzeitiges Nichtschließen des Notspeise-Saugschiebers 21 RL04 S019 und der Rückschlagklappe 20 RL04 S011 nach Ausgabe der Deionatsignale YZ62. Bei einem derartigen Versagen würde Wasser aus dem Speisewasserbehälter in die Deionatbehälter strömen, wobei aufgrund des hohen Speisewasserbehälter-Betriebsdrucks mit einem Bersten der Deionatbehälter zu rechnen ist. Der gleiche Störfall ist auch bei jeder Auslösung der Notspeisezuschaltsignale YZ51 möglich, von denen alle Notspeise- und Deionatsaugschieber einen AUF-Befehl erhalten. Um die Wahrscheinlichkeit für einen derar-

tigen Störfall gering zu halten, wurde die Rückschlagklappe 20 RL04 S011 mit einer Stellungsmeldung auf dem Wartenpult ausgerüstet. Vor jeder Funktionsprüfung der Notspeisezuschaltsignale YZ51 wird die Rückschlagklappe auf sicheres Schließen und (mittels einer Temperaturmeßstelle) auf Dichtheit überprüft.

Rohrleitungsbrüche im Deionatsystem werden durch die Warnmeldung "Deionatbehälter RY00 B001/2 TIEF 1" auf der Warte angezeigt, sobald der Wasserstand in den Deionatbehältern von 15 m auf 13,7 m gesunken ist. Gegenüber der Notabfahrreserve sind zu diesem Zeitpunkt noch 74 t gespeichert. Ist trotz Inbetriebnahme beider Deionat-Zubringerpumpen 20 RY31/32 D001 der normale Betriebswasserstand nicht mehr zu erreichen, so ist nach dem entsprechenden Logikschema des Betriebshandbuches, das für ein Leck im Deionatsystem oder im Sekundärkreislauf heranzuziehen ist, die Anlage unverzüglich abzufahren.

Bei Brüchen von Deionatleitungen in den Deionatbehälterräumen ist ein Überfluten der Räume im Verbindungstrakt, in denen alle Deionatpumpen und die Notspeisewasserpumpen RL04/05 D001 aufgestellt sind, nicht möglich, da dieser Raum als Wanne ausgebildet ist und nur oben über einen Einstieg verfügt. Reißt dagegen eine Deionatsaugleitung unmittelbar vor den Deionatpumpen, so entsteht ein Leck, das von der Warte aus nicht absperrbar ist. In diesem Fall würde der gesamte Inhalt beider Deionatbehälter (mindestens 500 t) ausfließen. Noch vor Ausgabe der eingangs erwähnten Warnmeldung "Deionatbehälter TIEF" erscheint auf der Warte die Warnmeldung "Sumpf Verbindungstrakt HOCH". Die Sumpfpumpe 20 UL91 D001 ist zu diesem Zeitpunkt bereits in Betrieb. Um das Auslaufen der Deionatbehälter zu verhindern, muß das Betriebspersonal versuchen, Handarmaturen in den Deionatsaugleitungen zuzufahren. Dazu ist es unter Umständen notwendig, bis zum Boden der "Deionatbehälter-Wanne" hinunterzusteigen und eine dort befindliche Armatur zu schließen.

Werden vom Betriebspersonal die entsprechenden Handmaßnahmen nicht oder erst zu spät durchgeführt, so ist mit Folgeausfällen aller Deionatpumpen, der Notspeisewasser-Pumpen RL04/05 D001 sowie der Druckerhöhungspumpen VE23/43 D001 zu rechnen. Für ein

sekundärseitiges Abfahren stünden damit nur noch die Redundanzen 3 und 4 sowie das Notstandssystem zur Verfügung.

Da der Rohrleitungsabschnitt, in dem derartige Leckagen möglich sind, jedoch nur sehr kurz ist und außerdem für einen Druck von 12 bar ausgelegt ist, aber nur mit einem Druck von etwa 2 bar belastet wird, ist die Wahrscheinlichkeit für diesen Störfall vernachlässigbar gering.

6.1.2.2.4 Fehlerbaum 1 C: Deionatsystem, Einspeisung in den Notspeisewasser-Strang 2 (RL05)

Die Ausfallkombinationen, die zum Versagen der direkten Deionatversorgung des Notspeisewasserstranges RL05 führen, entsprechen denen des Notspeisewasserstranges RL04.

6.1.2.2.5 Fehlerbaum 1 D: Deionatsystem, Einspeisung in den Notspeisewasser-Strang 3 (RL06)

Das Ansaugen von kaltem Deionat durch die Notspeisewasserpumpe 23 RL06 D001 mißlingt, wenn

- der Deionatsaugschieber 23 RL06 S018 oder die Rückschlagklappe 20 RL06 S011 nicht öffnet,
- der Saugschieber 23 RL06 S019 und die Rückschlagklappe 20 RL06 S002 nicht schließen,
- das Einspritzventil 23 RL06 S033 nicht öffnet,
- die Einspritzpumpe 23 RL06 D003 nicht startet oder deren Rückschlagventil 20 RL06 S032 nicht öffnet.

Einspritzpumpe und Einspritzventil werden vom Deionatzuschaltsignal angesteuert, die beiden Saugschieber vom Deionatsignal.

6.1.2.2.6 Fehlerbaum 1 E: Deionatsystem, Einspeisung in den Notspeisewasser-Strang 4 (RL07)

Die Ausfallkombinationen dieses Fehlerbaums entsprechen denen des Fehlerbaums 1 D (Anhang 3).

6.1.2.2.7 Fehlerbaum 2: Notspeisewassersystem, Strang 1 (RL04)

Da die vier zur Norspeisewasserversorgung der Dampferzeuger vorgesehenen Stränge in ihren wesentlichen Komponenten redundant aufgebaut sind, werden die Fehlerbäume im Detail nur für die erste Redundanz, d.h. für den Notspeisewasserstrang RL04 beschrieben. Bei den anderen drei Notspeisewassersträngen werden nur die Abweichungen gegenüber Strang RL04 aufgeführt.

Der Ausfall der Speisewasserversorgung des Dampferzeugers über den Notspeisewasserstrang RL04 kann hervorgerufen werden durch

- falsche Armaturenstellung in der Notspeisewasser-Saugleitung,
- falsche Armaturenstellung in der Notspeisewasser-Druckleitung und
- einen Ausfall der Notspeisewasser-Pumpe.

- Ausfall der Notspeisewasserförderung durch falsche Armaturenstellung in der Notspeisewasser-Saugleitung

Für das Ansaugen der Notspeisewasser-Pumpen aus dem Speisewasserbehälter ist es erforderlich, daß der Saugschieber 21 RL04 S019 und die nachgeschaltete Rückschlagklappe 20 RL04 S002 offen sind. Ein Ausfall liegt somit bei einem Nichtöffnen der Rückschlagklappe oder einer falschen Stellung des kontrollverriegelten Saugschiebers vor. Falsche Armaturenstellungen nach Funktionsprüfungen werden bei den kontrollverriegelten Armaturen des Notspeisewassersystems grundsätzlich berücksichtigt. Im Gegensatz zum Not- und Nachkühlsystem existiert hier nämlich keine Meldung, die auf eine gestörte "Notspeisebereitschaft" hindeutet.

Ist eine der beiden Armaturen geschlossen, so erfolgt bei einem Dampferzeuger-Wasserstand < 6,50 m die Auslösung der Reaktorschutzsignale YZ56 und damit die Absperrung des Stranges. Somit ist auch eine Umschaltung auf direkte Deionatversorgung für diesen Strang nicht mehr möglich. Die Absperrung erfolgt aber nur, wenn in dem Strang RL06 oder RL07 ein größerer Durchfluß oder Druck als Strang RL04 vorhanden ist. Bei der Aufstellung des Fehlerbaums wurde davon ausgegangen, daß diese Bedingung erfüllt ist.

- Ausfall der Notspeisewasserförderung durch falsche Armaturenstellung in der Notspeisewasser-Druckleitung

Die beiden einzigen motorbetätigten Armaturen in der Druckleitung, nämlich der Druckschieber 21 RL04 S005 und das Regelventil 24 RL13 S003, befinden sich bereits im Normalbetrieb der Anlage in offener Stellung. Der Druckschieber erhält bei Anforderung des Systems zusätzlich einen Kontrollbefehl zum Öffnen. Ein Ausfall liegt somit vor, wenn diese Armatur sich vor Anforderung in der falschen Stellung befindet und aufgrund eines Versagens der Armatur selbst, eines Ausfalls der Energieversorgung oder der Steuerung nicht öffnet.

Beim Notspeisewasser-Regelventil besteht die Möglichkeit, daß aufgrund eines Ausfalls des zugehörigen Differenzdruck-Meßumformers die Armatur bei Anforderung wieder zugefahren wird. Nach Absinken des Dampferzeugerwasserstands unter 6,50 m erhält das Regelventil vom Notspeisesignal wieder einen AUF-Befehl. Ein Ausfall dieses Differenzdruck-Meßumformers ist denkbar bei Dampfabgabe in den Sicherheitsbehälter. Für das kleine Leck in einer Hauptkühlmittelleitung wird die Wahrscheinlichkeit dafür $W_8 = 1$ angesetzt. Um eine Speisewasserförderung zu ermöglichen, müssen außerdem das Pumpenrückschlagventil 20 RL04 S004 und die Rückschlagklappe 20 RL13 S001 öffnen. Letztere wird im Normalbetrieb von dem im Dampferzeuger herrschenden Druck geschlossen gehalten und muß bei Notspeisebetrieb somit gegen dessen Druck öffnen. Eine Überprüfung dieser Rückschlagklappe ist nur bei abgeschaltetem Reaktor möglich.

Da die Schließzeit der Hauptspeisewasser-Regelventile ca. 70 Sekunden beträgt, müssen die Dampferzeuger-Rückschlagklappe 20 RL10 S001 oder die Pumpen-Rückschlagklappen 20 RL01 S005 und 20 RL02 S005 nach Auslaufen der Hauptspeisewasserpumpen sicher schließen. Andernfalls setzt eine kurzzeitige Rückströmung vom Dampferzeuger zum Speisewasserbehälter ein, was zur Abschieberung des betreffenden Notspeisewasserstrangs führt.

Nicht berücksichtigt wird in diesem Fehlerbaum die druckseitige Ausgleichsleitung mit ihren Absperrschiebern. Die Schieber soll-

ten im Normalbetrieb geschlossen sein. Werden im Störfall die Notspeisezuschaltsignale YZ51 ausgelöst, so erhalten sie nochmals einen Schließbefehl. Da Lecks in den Leitungen des Notspeisewassersystems nicht unterstellt bzw. sofort bemerkt werden, ist ein Speisewasserverlust aufgrund eines fälschlichen Öffnens eines oder aller Absperrschieber nicht zu befürchten.

- Ausfall der Notspeisewasser-Pumpe 21 RL04 D001

Der Ausfall der Notspeisewasser-Pumpe 21 RL04 D001 kann hervorgerufen werden durch

- den Ausfall der Stopfbuchsen- und Ölkühlung,
- den Ausfall der Motorkühlung,
- den Ausfall der Notspeisewasser-Pumpe selbst oder deren Hilfsölpumpe,
- den Ausfall der Energieversorgung und
- den Ausfall der Ansteuerung.

Zur Stopfbuchsen- und Ölkühlung muß bei Eintritt des Notstromfalls auf das Deionatsystem zurückgegriffen werden. Dazu ist das Schließen der Rückschlagklappe 20 VG72 S005 und das Öffnen des Absperrschiebers 21 VG72 S001 notwendig. Da die erforderliche Deionatmenge nur 2,4 m^3/h beträgt, genügt zur Versorgung der Kühler eine von zwei Deionatpumpen. Bezüglich der Ansteuerung der Deionatpumpen wird wie im Fehlerbaum 1 A (Anhang 3) verfahren, d.h., es wird nur die zugehörige Steuerkette berücksichtigt.

Die Kühlung der Motorluft wird vom Kaltwassersystem UZ50 übernommen (Übertrag aus Fehlerbaum 8, Anhang 3). Die Wärmeabfuhr aus diesem System übernimmt das nukleare Nebenkühlwassersystem VE10 (Übertrag aus Fehlerbaum 9 A, Anhang 3). Während im Notstromfall zunächst die betriebliche Ansteuerung zur Verfügung steht, werden im Kühlmittelverluststörfall die Motorarmaturen und Pumpen nur von Reaktorschutzsignalen angesteuert. Der Ausfall der Reaktorschutzsignale kann bei diesem Störfall daher nicht vernachlässigt werden. Die Notspeisewasser-Pumpen sind auch während des bestimmungsgemäßen Betriebes jeweils mehrere

Stunden lang im Einsatz, wenn nach einer Abschaltung des Reaktors die Anlage im Zustand unterkritisch heiß gehalten oder die Anlage abgefahren wird.

Bei der Funktionsprüfung saugt die Notspeisewasser-Pumpe aus dem Speisewasserbehälter an und fördert über ein Freilaufrückschlagventil und eine nachgeschaltete Drossel im Mindestmengenbetrieb (22 t/h bei einem Pumpendruck von 115 bar) in den Speisewasserbehälter zurück. Es besteht im Prüfhandbuch keine Anweisung zu kontrollieren, ob der bei der Funktionsprüfung gefahrene Betriebspunkt auf der Kennlinie der Notspeisewasser-Pumpe liegt. Das Starten der Pumpen wird vom Betriebspersonal vor Ort überwacht.

Rohrleitungsbrüche im Notspeisewassersystem werden vom Reaktorschutzsystem erkannt. Während des normalen Leistungsbetriebes hätte ein Leck in einer Notspeisewasserleitung das Leerlaufen des Speisewasserbehälters, das Abschalten der Hauptspeisewasser-Pumpen sowie die Inbetriebnahme der direkten Deionatansaugung durch die Notspeisewasser-Pumpen zur Folge. Der defekte Notspeisewasser-Strang wird zur Vermeidung von weiterem Deionatverlust vom zugehörigen Absperrsignal abgeschiebert. Folgeausfälle aufgrund des ausströmenden Wasser-Dampf-Gemisches sind wegen des langen Rohrleitungssystems im Maschinenhaus, im Verbindungstrakt, im Hilfsanlagengebäude und im Reaktorgebäude denkbar.

6.1.2.2.8 Fehlerbaum 3: Notspeisewassersystem, Strang 2 (RL05)

Dieser Fehlerbaum entspricht in seinen Ausfallkombinationen dem des Notspeisewasserstrangs RL04. Das Kaltwassersystem UZ60, das für die Kühlung der Motorluft der Notspeisewasser-Pumpe 22 RL05 D001 verantwortlich ist, sowie der nukleare Nebenkühlwasserstrang VE20, der für die Kondensatorkühlung der Kältemaschine zuständig ist, werden als bei Eintritt des Störfalls in Betrieb befindliche Systeme behandelt.

6.1.2.2.9 Fehlerbaum 4: Notspeisewassersystem, Strang 3 (RL06)

Die Ausfälle aufgrund falscher Armaturenstellungen in der Notspeisesaugleitung und Notspeisedruckleitung entsprechen denen im Fehlerbaum des Notspeisewasserstrangs 21 RL04. Unterschiede ergeben sich jedoch bei der Kühlung der Notspeisewasser-Pumpe 23 RL06 D001

Ein Ausfall der Stopfbuchsen-, Öl- und Motorkühlung der Notspeisewasser-Pumpe 23 RL06 D001 liegt vor bei einem Versagen des nuklearen Zwischenkühlstranges 3 oder des Nebenkühlwasserstranges 3. Beide Stränge befinden sich zum Zeitpunkt des Störfalls in Betrieb (Überträge aus Fehlerbaum 7 B und 9 B, Anhang 3).

6.1.2.2.10 Fehlerbaum 5: Notspeisewassersystem, Strang 4 (RL07)

Die Ausfallkombinationen des Fehlerbaums für den Notspeisewasserstrang 24 RL07 entsprechen denen des Fehlerbaums 4 (Anhang 3). Lediglich bei der Kühlung der Notspeisewasser-Pumpe 24 RL07 D001 ergeben sich Unterschiede, da es sich bei den dafür maßgebenden nuklearen Zwischen- und Nebenkühlwassersträngen 4 um Bereitschaftssysteme handelt.

6.1.2.2.11 Fehlerbaum 6: Notstandssystem

Beim Störfall "Kleines Leck in einer Hauptkühlmittelleitung" wird unterstellt, daß das rechtzeitige Abfahren der Anlage (mit 100°C/h) mit Hilfe des Notstandssystems von Block A aus nicht möglich ist, da laut Betriebshandbuch zunächst Block A abzufahren ist. Der Ausfall der entsprechenden Handmaßnahme (L562 OP RX10/20 C) wird daher mit der Wahrscheinlichkeit 1 bewertet. Damit gilt das Notstandssystem für diesen Störfall als ausgefallen.

6.1.2.2.12 Fehlerbaum 7: Nuklearer Zwischenkühlkreis

Die Stränge 1 und 2 des nuklearen Zwischenkühlkreises werden in Fehlerbaum 7 A, die Stränge 3 und 4 in Fehlerbaum 7 B behandelt (Anhang 3).

Der Ausfall der Stränge 1 bis 4 führt zum Ausfall der entsprechenden Stränge der HD- und ND-Einspeisungen (vgl. Fehlerbäume 17 und 18, Anhang 3), bei den Strängen 3 und 4 sind zusätzlich die entsprechenden Redundanzen des Notspeisewassersystems betroffen (Fehlerbäume 4 und 5, Anhang 3). Während zur HD-Einspeisung, zum Fluten und zur Notspeisewasserversorgung die Kühlung der entsprechenden Pumpen durch den nuklearen Zwischenkühlkreis sichergestellt werden muß, ist für den Sumpf-Umwälzbetrieb zusätzlich die Wärmeabfuhr über den Nachwärmekühler erforderlich.

Die Zwischenkühlpumpen sind beim Abfahren der Anlage langfristig im Einsatz. Im Leistungsbetrieb ist immer der Strang 1 oder der Strang 3 in Betrieb.

Aufgrund der getroffenen Annahmen (Abschnitt 6.1.1) befindet sich von diesen beiden Strängen des nuklearen Zwischenkühlkreises, die Kühlstellen im Reaktor-Hilfsanlagengebäude versorgen können, Strang 1 in Reserve und Strang 3 in Betrieb.

In Strang 3 werden daher Rohrleitungsausfälle, soweit sie nicht als Störfallfolge auftreten, nicht berücksichtigt, weil bei diesem Strang größere Leckagen bemerkt werden. Im nuklearen Zwischenkühlkreis werden Leckagen über 100 l/h entdeckt, während durch das Deionatsystem 4,5 m^3/h ($\hat{=}$ 4 500 l/h) nachgespeist werden können. Eine nicht entdeckte Blockage der zur Störfallbeherrschung wichtigen Kühler

- der HD-Sicherheitseinspeisepumpe,
- der Nachkühlpumpe und
- des Nachwärmekühlers

ist dagegen in allen Strängen des nuklearen Zwischenkühlkreislaufs grundsätzlich möglich, da über diese Kühler bei ungestörtem Leistungsbetrieb keine Wärme abgeführt wird. In der numerischen Auswertung der Fehlerbäume sind jedoch die Ausfälle von passiven Komponenten gegenüber den Ausfällen von zu betätigenden Komponenten zu vernachlässigen.

Untersucht wurde auch die Möglichkeit eines TF-Rohrleitungsbruches im Ringraum: Der Wasserinhalt eines Stranges des nuklearen

Zwischenkühlkreislaufs beträgt etwa 266 m^3. Diese Wassermenge würde zwar alle vier Ringraum-Quadranten überfluten, die Sockelhöhe der Pumpen (Nachkühlpumpen, Sicherheitseinspeisepumpen, Beckenkühlpumpen, Zwischenkühlpumpen) wird jedoch nicht erreicht. Somit sind Folgeschäden an anderen Systemen nicht zu erwarten.

Je nach Größe der Leckage werden bei Brüchen im TF-System folgende Warnmeldungen auf der Warte ausgegeben:

- "Pumpensumpf-Ringraumquadrant HOCH",
- "Aerosolaktivität Ringraum > max",
- "Aktivität Abluft Ringraum > max".

Von diesen Meldungen werden folgende Notgefahrmeldungen abgeleitet:

- "Niveau Pumpensumpf > max",
- "Abluft-Aktivität Ringraum".

Das Wartenpersonal wird bei Lecks im Betriebsstrang des TF-Systems durch das Betriebshandbuch angewiesen, auf einen in Bereitschaft stehenden Strang umzuschalten. Die Zwischenkühlpumpen und die nach Störfalleintritt zu schließenden Beckenkühlarmaturen unterliegen bei den Funktionsprüfungen den gleichen Bedingungen wie im Störfall.

- Ausfall Zwischenkühlstrang 1

Außer den in Abschnitt 6.1.2.2 angesprochenen Ausfällen passiver Komponenten kann der Zwischenkühlstrang 1 für die HD-Einspeisung und für Fluten ausfallen, weil

- die nukleare Zwischenkühlpumpe 21 TF11 D001 nicht startet oder während des Störfalls versagt, oder
- die zugehörige Pumpenrückschlagklappe 20 TF11 S002 nicht öffnet, oder
- die Pumpenrückschlagklappe 20 TF12 S002 der zweiten, durch Reaktorschutzsignale nicht angesteuerten nuklearen Zwischenkühlpumpe 20 TF21 D001 nicht schließt, so daß über diese Pumpe eine Kurzschlußströmung erfolgt, oder

- beide Absperrarmaturen 21 TF50 S001 und 22 TF50 S002 zu den Hilfsanlagen fälschlich offen sind.

Ursache für den Ausfall der Absperrung der Hilfsanlagen kann sein, daß der nukleare Zwischenkühlstrang 1 einmal seit der letzten Funktionsprüfung Betriebsstrang war bzw. beim Test von Strang 3 in Betrieb genommen wurde. Durch betriebliche Automatiken wird beim Abschalten des Strangs an die Absperrarmaturen zwar ein ZU-Befehl gegeben, die Ausführung des Befehls wird jedoch nicht überprüft. Für die Absperrungen der Hilfsanlagen mit den Armaturen 21 TF50 S001 und 22 TF50 S002 wurde im Fehlerbaum der Ausfall der Ansteuerung nicht berücksichtigt, da die Armaturen sowohl bei Abschaltung beider Betriebspumpen in Strang 1 über die betriebliche Automatik als auch beim Störfall durch die Notkühlvorbereitungssignale YZ31 zugefahren werden und somit nur Doppelausfälle zum Versagen der Ansteuerung der Armaturen führen können.

Ein Ausfall des Stranges 1 liegt dann vor, wenn beide Absperrarmaturen 21 TF50 S001 und 22 TF50 S002 zu den Hilfsanlagen nicht geschlossen sind und somit die Ringleitung nicht abgetrennt ist. Außerdem ist der Strang 1 dann ausgefallen, wenn die gebrochenen Kühlwasserleitungen der Hauptkühlmittelpumpe im Vorlauf oder Rücklauf nicht abgetrennt sind (Bruch von Rohrleitungen innerhalb der Stahlhülle als Störfallfolge, siehe W_3 in Tabelle F2, 6-2).

Die Absperrarmatur 20 TF10 S012 für den Brennelement-Beckenkühler wird bei Abschaltung des Stranges laut Anweisung im Betriebshandbuch zugefahren. An die Armatur ergeht außerdem beim Störfall ein ZU-Befehl durch eine betriebliche Automatik. Das Versagen der Armatur wird daher vernachlässigt.

Eine fälschlich offene Armatur in der Umgehungsleitung des nuklearen Zwischenkühlers hat eine verminderte Wärmeabfuhr an das nukleare Nebenkühlwasser zur Folge. Diese Armatur wird jedoch bei Abschaltung des Stranges laut Anweisung im Betriebshandbuch zugefahren. An die Armatur ergeht außerdem beim Störfall ein Kontrollbefehl, so daß diese Armatur nicht berücksichtigt zu werden braucht.

Der Strang 1 fällt für Sumpfbetrieb zusätzlich dann aus, wenn beide Absperrarmaturen 21 TF10 S004 und 21 TF10 S014 des Nachkühlers nicht öffnen.

Da die Nichtverfügbarkeit beider Absperrarmaturen des Nachkühlers gegenüber der Nichtverfügbarkeit einer Reservepumpe vernachlässigt werden kann, wurde im Fehlerbaum der Einfachheit und Übersichtlichkeit halber nicht zwischen dem Ausfall eines Zwischenkühlstranges für Fluten und für Sumpfbetrieb unterschieden. Die Nichtverfügbarkeit des nuklearen Zwischenkühlkreises für Fluten wird dadurch leicht überschätzt.

- Ausfall Zwischenkühlstrang 2 oder 4

Ein Ausfall des Stranges 2 oder 4 des nuklearen Zwischenkühlkreises (wie erwähnt, haben diese Stränge keine betrieblichen Funktionen) kann außer den vorher angesprochenen Ausfällen nicht betätigter, d.h. passiver Komponenten durch den Ausfall der Zwischenkühlpumpe herbeigeführt werden. Eine fälschlich offene Armatur in der Umgehungsleitung des nuklearen Zwischenkühlers wird wie beim Zwischenkühlstrang 1 vernachlässigt.

- Ausfall Zwischenkühlstrang 3

Für den vor Störfalleintritt in Betrieb befindlichen Strang 3 liegt ein Versagen für Fluten bzw. zur Kühlung der Notspeisepumpe 23 RL06 D001 dann vor, wenn neben den oben angesprochenen Ausfällen passiver Komponenten

- die laufende nukleare Zwischenkühlumpe 23 TF31 D001 während des Störfalls versagt,
- die beiden Absperrarmaturen 23 TF50 S003 und 24 TF50 S004 zu den Hilfsanlagen nicht schließen (siehe Strang 1),
- bei Eintritt des Notstromfalls die Ansteuerung oder die Energieversorgung der nuklearen Zwischenkühlpumpe 23 TF31 D001 ausfällt,
- bei Eintritt des Notstromfalls die Pumpenrückschlagklappe 20 TF32 S002 der zweiten, nicht notstromgesicherten nuklearen

Zwischenkühlpumpe 20 TF32 D001 nicht schließt, so daß über diese Pumpe eine Kurzschlußströmung erfolgt und

- bei Eintritt des Notstromfalls die Absperrarmatur 20 TF30 S012 für den Brennelement-Beckenkühler nicht schließt.

An die Absperrarmatur 20 TF30 S012 für den Brennelement-Beckenkühler ergeht durch betriebliche Automation ein ZU-Befehl, wenn eine der beiden nuklearen Zwischenkühlpumpen ausfällt und eine Nachkühler-Absperrarmatur öffnet. Wenn im Notstromfall die Armatur nicht schließt, ist der nukleare Zwischenkühlstrang wegen verminderten Durchsatzes durch alle zur Störfallbeherrschung wichtigen Kühler ausgefallen.

Die Armatur 23 TF30 S048 in der Umgehungsleitung des nuklearen Zwischenkühlers wird durch das Notkühlvorbereitungssignal zugefahren. Diese Armatur ist nur bei niedrigen Flußwassertemperaturen geöffnet, um die Vorlauftemperatur des nuklearen Zwischenkühlstranges nicht zu tief absinken zu lassen. In diesem Fall weist die Kapazität der Kühlkette jedoch eine erhebliche Reserve auf. Eine ausreichende Wärmeabfuhr ist daher auch sichergestellt, wenn der Bypass nicht geschlossen ist.

Der Strang 3 fällt für Sumpfbetrieb dann aus, wenn beide Absperrarmaturen 23 TF30 S004 und 23 TF30 S014 des Nachkühlers nicht öffnen. Auch hier wurde wie bei Strang 1 wegen der geringen Unterschiede der Nichtverfügbarkeit zwischen dem Ausfall des Zwischenkühlstranges für Fluten und für Sumpfbetrieb nicht unterschieden.

6.1.2.2.13 Fehlerbaum 8: Kaltwassersystem

Bei der Aufstellung des Fehlerbaums für das Kaltwassersystem wurde davon ausgegangen, daß sich die Stränge UZ60 und UZ90 vor Eintritt des Störfalls bereits in Betrieb befinden. Die Stränge UZ50 und UZ80 wurden als in Bereitschaft stehende Systeme behandelt.

Der Ausfall eines Kaltwasserstranges liegt immer dann vor, wenn

- ein Turbokaltwassersatz versagt,
- dessen Hilfsölpumpe nicht startet oder
- die Kaltwasserumwälzpumpe ausfällt.

Die Kältemaschinen und Umwälzpumpen in den Betriebssträngen UZ60 und UZ90 werden als laufende Aggregate in Rechnung gesetzt. Ein Startversagen wird dabei nicht unterstellt. Die zum Kaltwassersatz gehörige Hilfsölpumpe erhält jedoch bei jedem Ein- und Ausschalten des Verdichters - also auch nach Eintritt des Notstromfalls - einen EIN-Befehl. Sie wird nach wenigen Minuten wieder abgeschaltet. Für diese Komponente wird daher in den Betriebssträngen ein Startversagen berücksichtigt.

Die Ansteuerung des UZ-Systems wird vernachlässigt, da dieses System von einer betrieblichen Steuerung und, wenn diese ausgefallen ist, auch vom Reaktorschutzsystem in Betrieb genommen wird. Für die Pumpen in diesem System gilt auch darüber hinaus, daß sie auch noch (nach Abschalten der Notspeisepumpen über den Pumpenschutz) entweder in der Warte oder in den Schaltanlagen eingeschaltet werden können.

Berücksichtigt wurde jedoch in Form einer Ersatzausfallrate:

- das fälschliche Ansprechen des Aggregateschutzes,
- der Ausfall der Leistungsregelung des Verdichters,
- der Ausfall der Steuerspannung,
- der Ausfall der Einschaltfreigabe und
- das Unterdrücken des EIN-Befehls durch die Einschaltverzögerung.

Folgeschäden an anderen Redundanzen des Kaltwassersystems oder an anderen Systemen sind bei Rohrleitungsbrüchen im Kaltwassersystem nicht zu befürchten.

Jeder Strang des Kaltwassersystems (Wasserinhalt ca. 25 m^3) verfügt über einen Ausgleichsbehälter, der den Betriebsdruck konstant auf 4 bar halten soll. Geringfügige Leckagemengen werden durch Nachspeisen aus den Deionatsystem ersetzt. Große Leckagen

hingegen würden zu einem Druckabfall im Ausgleichsbehälter und damit zur Auslösung einer Warnmeldung führen. Außerdem würde ein derartiges Leck von den Strömungswächtern im Vorlaufstrang der Kältemaschinen registriert; dadurch würde mit einer Zeitverzögerung von 10 Sekunden die betreffende Kaltwasser-Umwälzpumpe abgeschaltet werden. Alle an einem UZ-Strang hängenden Verbraucher können gegebenenfalls einzeln abgeschiebert werden.

6.1.2.2.14 Fehlerbaum 9: Nukleares Nebenkühlwassersystem

Beim bestimmungsgemäßen Betrieb sind immer der Strang 1 oder 3 und der Strang 2 oder 4 des nuklearen Nebenkühlwassers im Einsatz. Im Rahmen der vorliegenden Analyse wird davon ausgegangen, daß die Pumpen der Stränge 2 und 3 vor Störfalleintritt laufen (Abschnitt 6.1.1).

Die während des Störfalls zu betätigenden Komponenten des nuklearen Nebenkühlwassersystems fallen durch die Steuerung aus, wenn die entsprechende Steuerkette, die 24-V-Versorgung im oberen Teil des Betätigungsschrankes HA05 oder das Reaktorschutzsignal ausfallen. Für die vor Störfalleintritt laufenden Pumpen der Stränge 2 und 3 ist der Ausfall der Steuerung nur dann relevant, wenn während des Störfalls der Notstromfall eintritt und die Pumpen nach Spannungsrückkehr wieder anlaufen müssen.

In den Strängen 2 und 3 des nuklearen Nebenkühlwassersystems, die sich zum Zeitpunkt des Störfalls in Betrieb befinden, sind Rohrleitungsausfälle sowie Blockagen von Kühlern dann in Rechnung zu stellen, wenn sie bei den in Betrieb nicht durchflossenen Dieselkühlern auftreten. Eine Blockage ist auch bei dem nuklearen Zwischenkühler denkbar, der bei Leistungsbetrieb des Kraftwerks keine Wärme abzuführen hat.

- Ausfall Nebenkühlwasser-Strang 1 oder 4

Bei den Strängen 1 und 4 des nuklearen Nebenkühlwassersystems, die in Bereitschaft sind, ist ein Bruch von Rohrleitungen oder

eine Blockage von Kühlern grundsätzlich zu berücksichtigen. In der numerischen Auswertung der Fehlerbäume können jedoch diese Ausfälle passiver Komponenten gegenüber den Ausfällen von zu betätigenden Komponenten vernachlässigt werden.

Der in Bereitschaft befindliche Strang 1 des nuklearen Nebenkühlwassers kann außerdem ausfallen, weil

- die nukleare Nebenkühlwasserpumpe 21 VE10 D001 oder
- die zugehörige Betriebs-Fettpumpe 21 VE10 D003 nicht startet oder im Betrieb ausfällt und die Anfahr-Reserve-Fettpumpe 21 VE10 D002 nicht startet oder
- die Pumpenrückschlagklappe 20 VE10 S004 nicht öffnet.

Entsprechendes gilt für den Strang 4.

Aus rechentechnischen Gründen ist im Fehlerbaum der Ausfall der den genannten Komponenten zugeordneten Energieversorgungsschiene (nur im Notstromfall relevant) nicht jeweils bei den Komponenten berücksichtigt, sondern gesondert in den TOP geführt.

- Ausfall Nebenkühlwasser-Strang 2 oder 3

Bei den Betriebssträngen kann ein Ausfall der Nebenkühlwasserpumpe oder der Betriebs-Fettpumpe während des Betriebes eintreten, im Notstromfall dagegen durch Ausfall der Energieversorgung oder der Ansteuerung.

- Ausfall der Dieselkühlung im Notstromfall

Wenn nach Störfalleintritt kein Notstromfall vorliegt, ist für die HD-Einspeisungen und die ND-Einspeisungen aus den Flutbehältern eine Kühlung der Stränge des nuklearen Zwischenkühlkreises durch das nukleare Nebenkühlwasser nicht erforderlich (Abschnitt 4.2.2). Beim Notstromfall werden die Notstromdiesel gestartet. Es müssen dann zur Kühlwasserversorgung der einzelnen Diesel die entsprechenden Nebenkühlstränge funktionieren und mindestens eine der beiden Absperrarmaturen vor den Dieselkühlern (z.B. Strang 1: 21 VE14 S001 oder 21 VE14 S010) öffnen.

- Ausfall der Kühlung der kleinen Kältemaschinen

Zur Kühlung der kleinen Kältemaschinen ist neben der oben behandelten Funktion der entsprechenden Nebenkühlwasser-Stränge die Inbetriebnahme der zu den Kältemaschinenkühlern gehörigen Druckerhöhungspumpen und das Öffnen der Regelventile notwendig. Bei Außerbetriebnahme einer kleinen Kältemaschine wird durch Abschalten der Druckerhöhungspumpe das Regelventil automatisch aufgefahren. Da beim Störfall durch das Notstromvorbereitungssignal nochmals zur Kontrolle ein AUF-Befehl ausgegeben und die Stellung des Ventils in der Warte analog angezeigt wird, braucht bei den in Bereitschaft befindlichen Strängen des nuklearen Nebenkühlwassers der Ausfall des Regelventils nicht berücksichtigt zu werden. Bei einem in Bereitschaft befindlichen Strang kann ein Ausfall der Druckerhöhungspumpe auftreten, weil diese nicht startet oder während des Störfalls versagt.

Bei einem zum Zeitpunkt des Störfalls in Betrieb befindlichen Strang des nuklearen Nebenkühlwassers kann die Druckerhöhungspumpe der kleinen Kältemaschine nur im Notstromfall versagen. Hingegen muß, um eine ausreichende Kühlwasserversorgung sicherzustellen, das Regelventil der Kältemaschine vollständig aufgefahren werden.

- Rohrleitungsbrüche

Rohrleitungsbrüche im nuklearen Nebenkühlwassersystem können in folgenden Gebäudeteilen auftreten:

- Ringraum,
- Verbindungstrakt,
- Schaltanlagengebäude (Dieselräume) oder
- Pumpenhaus.

Die zur Beherrschung derartiger Leckstörfälle notwendigen Maßnahmen sind im Logikschema "Leck im VE-System" des Betriebshandbuches aufgeführt. Es gibt allerdings keine spezielle Meldung auf der Warte, die das Betriebspersonal definitiv auffordert, dieses Logikschema zur Hand zu nehmen und die darin angegebenen

Gegenmaßnahmen einzuleiten. Das Betriebspersonal wird im allgemeinen auf derartige Leckagen nur durch ständiges Laufen einzelner Sumpfpumpen oder durch das Anstehen von Meldungen hingewiesen. Im einzelnen werden in den verschiedenen Anlagenteilen außerdem folgende Warnmeldungen ausgegeben:

- Ringraum

Bei Leckagen im Ringraum erfolgt bei einem Wasserstand von 0,15 m zunächst die Sammelgefahrenmeldung "Pumpensumpf HOCH". Bei Erreichen einer Sumpf-Wasserstandshöhe von 0,5 m werden für jeden Quadranten eigene Warnmeldungen "Pumpensumpf Ringraumquadrant HOCH" ausgegeben.

Von diesen Meldungen wird die Notgefahrmeldung "Niveau Pumpensumpf > max" abgeleitet. Die den vier Ringraumquadranten zugeordneten Sumpfpumpen 20 TZ21-24 D001 befinden sich bereits vor Ausgabe dieser Meldungen in Betrieb. Das Einschalten dieser Pumpen wird über die Prozeßrechneranlage gemeldet.

Das Betriebshandbuch sieht bei Anstehen dieser Meldungen als erste Maßnahme eine Überprüfung der Rohrleitungen im Ringraum auf Leckagen vor.

Aufgrund der großen Fördermengen der Nebenkühlwasserpumpen (2 000 bis 3 000 m^3/h) ist bei doppelendigen Brüchen von Rohrleitungen des Nebenkühlwassersystems im Ringraum bereits nach ca. 1 Minute mit dem Übertreten von Wasser in die benachbarten Ringraum-Quadranten zu rechnen. Damit wird es in vielen Fällen schwierig sein, von der Warte aus festzustellen, in welcher Redundanz des Systems eine Leckage auftrat.

Das Betriebspersonal muß bei einem derartigen Leck schnell Gegenmaßnahmen ergreifen, d.h. den gestörten Strang abschalten und gegebenenfalls einen in Bereitschaft befindlichen Strang in Betrieb nehmen. Es muß außerdem dafür sorgen, daß dieser Strang nicht mehr automatisch in Betrieb genommen werden kann. Bereits ca. 10 Minuten nach Störfalleintritt kann nämlich im ungünstig-

sten Fall der gesamte Ringraum bis zur Sockelhöhe der dort aufgestellten Pumpen geflutet sein. Bei einem weiteren Ansteigen der Wasserhöhe muß mit Folgeschäden an den Nachkühlpumpen, den HD-Sicherheitseinspeisepumpen, den HD-Förderpumpen und Abdrückpumpen des Volumenregelsystems, den Beckenkühl- und Beckenreinigungspumpen sowie den nuklearen Zwischenkühlpumpen gerechnet werden. Die Wahrscheinlichkeit für einen derartigen Störfall muß jedoch als äußerst gering eingestuft werden, zumal die im Ringraum verlegten Rohrleitungen des Nebenkühlwassersystems im Vergleich zur Gesamtrohrlänge des Systems sehr kurz sind. Außerdem ist ein plötzlicher Abriß bei den auftretenden geringen Spannungen in den Rohrleitungen des nuklearen Nebenkühlwassersystems besonders unwahrscheinlich, d.h., es ist mit einem Leck vor Bruch zu rechnen.

- Verbindungstrakt

Bei Leckagen des Nebenkühlwassersystems im Verbindungstrakt steht in der Warte die Warnmeldung "Sumpf Verbindungstrakt HOCH" an. Das selbsttätige Einschalten der zugehörigen Sumpfpumpe 20 UL91 D001 wird über die Prozeßrechneranlage gemeldet.

Das Betriebspersonal muß daraufhin vor Ort die Rohrleitungen des Verbindungstraktes auf Leckagen überprüfen. Es ist von der Warte aus weder erkennbar, welches der im Verbindungstrakt installierten Systeme (RY, RL, UZ, VE) die Leckage verursacht hat, noch in welcher Redundanz der Schaden liegt.

Ein Rohrleitungsbruch eines Nebenkühlwasser-Stranges ist im Verbindungstrakt auf den Gebäudehöhen von - 6 m bis + 15 m möglich. Die Ausströmrate beträgt dort maximal ca. 200 m^3/h. Das auslaufende Wasser wird über das Treppenhaus nach unten strömen und sich auf der Gebäudeebene - 6 m sammeln. Wird vom Betriebspersonal der schadhafte Strang nicht - wie es das Betriebshandbuch vorsieht - abgeschaltet und ein entsprechender Reservestrang eingeschaltet, so ist nach ca. 45 Minuten mit Folgeschäden an den Notspeisewasserpumpen der Redundanzen 1 und 2 sowie an allen Deionatpumpen zu rechnen.

- Dieselräume

Bei Leckagen eines Nebenkühlwasser-Stranges in den Räumen der Notstromaggregate erscheint auf der Warte die Warnmeldung "Sumpf Schaltanlagengebäude HOCH". Außerdem wird das Laufen der zugehörigen Sumpfpumpe 20 UL90 D001 angezeigt. Das Betriebshandbuch sieht daraufhin eine Überprüfung der Rohrleitungen im Schaltanlagengebäude vor. Bei Vorliegen eines Lecks an einem Dieselkühler müssen die Dieselkühler-Absperrarmaturen geschlossen werden. In der ersten Redundanz wären dies die Motorarmaturen 20 VE14 S001/S010 und die Handarmatur 20 VE14 S005. Es muß dafür gesorgt werden, daß ein automatisches Auffahren der Motorarmaturen und ein Starten des Diesels verhindert wird. Folgeschäden an anderen Aggregaten sind kurzzeitig nicht zu befürchten.

- Pumpenhaus

Die nuklearen Nebenkühlwasserpumpen sind im Pumpenhaus paarweise räumlich getrennt aufgestellt. Jeder Raum verfügt über eine eigene Sumpfpumpe, außerdem wird das Überschreiten des Sumpfwasserstand-Grenzwertes für jeden Raum getrennt auf der Warte angezeigt. Je eine Sumpfpumpe und eine entsprechende Meldung "Niveau Sumpf NKW-Pumpe > max" sind den Redundanzen 1 und 2 bzw. den Redundanzen 3 und 4 zugeordnet.

Bei Rohrleitungsbrüchen in den Nebenkühlwasser-Pumpenräumen zwischen Pumpe und erstem Druckschieber muß der vor der Pumpe angeordnete Plattenschieber von Hand geschlossen werden, da ansonsten - auch nach Abschalten der Pumpe - der Raum überflutet werden kann. Leckagen im Pumpenhaus sind im Betriebshandbuch nicht berücksichtigt. Handmaßnahmen werden vom ständig besetzten örtlichen Leitstand im Pumpenhaus durchgeführt.

Werden bei einem Leck im Nebenkühlwasser-Pumpenhaus keine Gegenmaßnahmen getroffen, so ist mit dem Ausfall einer weiteren nuklearen Nebenkühlwasserpumpe und einer konventionellen Nebenkühlwasserpumpe zu rechnen.

- Verstopfung des Einlaufbauwerks

Die Gefahr einer Verstopfung des VE-Einlaufbauwerks aufgrund von Gras- oder Laubanfall wird aus den folgenden Gründen nicht berücksichtigt: Verschmutzungsprobleme treten nach bisherigen Erfahrungen nur bei steigendem Rheinpegel (Hochwasser) auf. Eine manuelle Reinigung der Grob- und Feinrechen war in der Referenzanlage bisher auch bei verstärktem Schmutzanfall nicht notwendig. Dagegen mußte am Schmutzabwurf Personal eingesetzt werden, da in Extremfällen die vorhandene Fördereinrichtung überlastet war. Die Rechenroste bei den Grob- und Feinrechen sind so gestaltet, daß es auch bei einem Stau zu keiner Durchbiegung und damit zu einer Verschlechterung der Reinigungswirkung kommen kann. Auch im Notstromfall, wenn die Siebbandmaschinen nicht in Betrieb sind, ist mit keiner Verstopfung des Einlaufbauwerks zu rechnen. Nach Ausfall der Hauptkühlwasser- und konventionellen Nebenkühlwasser-Versorgung werden aus dem Rhein nur noch ca. 1 500 m^3/h Wasser entnommen. Dies hat zur Folge, daß einerseits die Siebe nicht mehr voll belastet werden und andererseits die Strömungsgeschwindigkeit im Entnahmekanal so weit absinkt, daß größere Verunreinigungen im allgemeinen von der Strömung nicht mehr mitgetragen werden. Auch nach einem eventuellen Öffnen der Notauslaßklappen ist eine Beschädigung von Pumpenlaufrädern aufgrund der den Siebbandmaschinen vorgeschalteten Feinrechen mit einer Spaltbreite von 12 mm nicht zu erwarten.

Der zur Förderung des benötigten Kühlwasserdurchsatzes erforderliche Mindestwasserstand vor den Nebenkühlwasserpumpen wird auf der Warte mittels einer Fernanzeige und durch Gefahrenmeldungen bei Unterschreiten eines gewissen Mindestwasserstandes überwacht. Für die Kühlwasserreinigung sind pro Reinigungsstraße Sammelmeldungen vorhanden, die u.a. bei einem großen einseitigen Überstau an der Siebbandmaschine oder an der Grobrechen- und Feinrechenanlage gebildet werden. Eine Sammelmeldung für die gesamte Reinigungsanlage erfolgt als Notgefahrmeldung.

Am örtlichen Leitstand, der im Kühlwasser-Pumpenbauwerk untergebracht ist, wird angezeigt, an welcher Komponente der Reinigungsstraße eine Störung vorliegt. An diesem örtlichen Steuerschrank, der regelmäßig überwacht wird, können die einzelnen

Wasserstandsdifferenzen von Siebband, Feinrechen und Grobrechen abgelesen werden. Außerdem werden hier auftretende Staus einzeln gemeldet.

Auf der Warte kann außerdem noch die Differenz zwischen dem Rheinniveau und dem Wasserstand vor den Nebenkühlwasserpumpen abgelesen werden. Bei Überschreiten eines bestimmten Differenzbetrages wird eine Gefahrmeldung ausgelöst.

6.1.2.2.15 Fehlerbaum 10: Frischdampfsystem

Die Ausfälle im Frischdampfsystem sind folgendermaßen zusammengefaßt (Überträge, die in den Gesamtfehlerbaum führen):

- zu spätes Abfahren oder Abfahren mit falschem Abfahrgradienten (Fehlerbaum 10 A, Anhang 3),
- Ausfall des Abfahrens über Frischdampf-Umleiteinrichtung (Fehlerbaum 10 A, Anhang 3),
- Ausfall des Abfahrens über Abblaseregelventile (Fehlerbaum 10 A, Anhang 3),
- Ausfall der Frischdampfabgabe über Strang 1 und Frischdampf-Schnellschlußschieber (Fehlerbaum 10 A, Strang 2 bis 4 in Fehlerbaum 10 B bis 10 D, Anhang 3) und
- Ausfall der Frischdampfabgabe über Strang 1 und Abfahrleitung (Fehlerbaum 10 A, Strang 2 bis 4 in Fehlerbaum 10 B bis 10 D Anhang 3).

Eine Reihe von Meldungen und Anzeigen an der Reaktorschutztafel läßt das Vorliegen eines Kühlmittelverluststörfalls (kleines Leck) leicht erkennen. Dem Wartenpersonal ist zwar bekannt, daß bei kleinen Lecks ein Abfahren mit dem Speisewasser-Dampf-Kreislauf einzuleiten ist. Allerdings gibt es eine entsprechende Notgefahrmeldung und die Meldung "Abfahren mit RL-System" auf der Anweisungstafel nur, wenn der Wasserstand im Druckhalter einen Wert von > 3,15 m hat.

Bei einem Druck im Reaktorkühlkreislauf ≦ 35 bar wird statt der genannten Meldungen eine andere Notgefahrmeldung und die Meldung

auf der Anweisungstafel "Abfahren mit TH-System" ausgelöst. Im Unterschied dazu wird im entsprechenden Logikschema des Betriebshandbuches aber richtigerweise darauf hingewiesen, daß das Abfahren mittels TH-System erst bei einem Druck von ≦ 10 bar eingeleitet werden soll.

Da die Druckmeßumformer für die Verriegelung der letzten Rückschlagarmaturen in den heißen Einspeiseleitungen der Nachkühlstränge nicht für die Umgebungsbedingungen nach Kühlmittelverluststörfällen ausgelegt sind, können diese Stränge ohne Eingriffe in die Verriegelungen nicht auf normales Nachkühlen umgeschaltet werden (Abschnitt 6.1.1). Es wird daher davon ausgegangen, daß die Wärmeabfuhr über die NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE auch nach Abfahren der Anlage aufrechterhalten werden muß.

Ist der Druckhalter-Wasserstand < 2,85 m, so werden bei Absenken des Drucks im Reaktorkühlkreislauf auf 10 bar die ND-Einspeisesignale YZ38 und als Folge die Δp/Δt-Signale YZ60 ausgelöst. Dadurch wird die Frischdampfabgabe vorübergehend unterbunden. Nach 15 Minuten kann die Wärmeabfuhr über die Abblaseregelventile wieder in Betrieb genommen werden. Außerdem können nach Rücksetzen der Δp/Δt-Signale im Ringraum die Frischdampfschieber wieder geöffnet und die Frischdampf-Umleiteinrichtung wieder in Betrieb genommen werden.

- Zu spätes Abfahren oder Abfahren mit falschem Abfahrgradienten

Beim kleinen Leck in einer Hauptkühlmittelleitung muß spätestens 60 Minuten nach Störfalleintritt mit dem sekundärseitigen Abfahren begonnen werden, wobei ein Abfahrgradient von 100 °C/h einzuhalten ist (Abschnitt 6.1.1). Demnach liegt ein Ausfall der geregelten Frischdampfabgabe vor, wenn das Abfahren entweder zu spät eingeleitet wird, unzulässige Verzögerungen auftreten oder der Gradient falsch gewählt wird. Für das Einleiten des Abfahrens wird eine Zeitspanne von 30 Minuten zugrunde gelegt. Damit wird pessimistisch unterstellt, daß das Abfahren später als 30 Minuten nach Störfallmeldung nicht mehr eingeleitet wird. Unter

Berücksichtigung der zwei möglichen Ausgangssituationen: Frischdampf-Umleiteinrichtung intakt oder Frischdampf-Umleiteinrichtung steht nicht zur Verfügung, sind im Funktionselement L 582 OP RA11/12 "Kein Einleiten des Abfahrens innerhalb von 30 Minuten" die Ausfälle folgender Handmaßnahmen zusammengefaßt:

Frischdampf-Umleiteinrichtung intakt:

- H/R-Umschaltung auf Stellung HAND (H/R ≙ HAND/REGELUNG)
- 1v3 Frischdampf-Umleitventile von Hand langsam AUF

Frischdampf-Umleiteinrichtung steht nicht zur Verfügung (Abblasen über Frischdampf-Sicherheitsventile):

- H/R-Umschaltung auf Stellung HAND
- Absperrschieber in Abfahrleitungen von Hand AUF
- 1v2 Abblaseregelventile von Hand langsam AUF.

Zum Ausfall der geregelten Frischdampfabgabe führt auch das Abfahren mit einem unzulässigen Abfahrgradienten. Laut Betriebshandbuch ist der Frischdampfdruck entsprechend einem Temperaturgradienten von 100 °C/h abzusenken. Dazu muß der Gradient auf einem Schreiber eingetragen werden, auf dem die Frischdampftemperatur aufgezeichnet wird. Nach dieser Vorgabe sind dann die Frischdampf-Umleitventile bzw. die Abblaseregelventile zu fahren. Der Ausfall der genannten Handmaßnahmen wird in dem Funktionselement L 583 OP RA11/12 C "Abfahren mit falschem Abfahrgradienten innerhalb 30 Minuten" zusammengefaßt. Es wird dabei unterstellt, daß der Gradient innerhalb 30 Minuten nach Störfalleintritt einzuzeichnen ist. Bei der Bewertung der Handmaßnahme spielt das Einzeichnen der Sollgeraden gegenüber dem Regeln der Ventile entsprechend der Temperatur/Zeit-Vorgabe die dominante Rolle (Abschnitt 6.1.4).

In diesem Zusammenhang ist darauf hinzuweisen, daß in der Warte nur ein Schreiber für die Frischdampftemperatur vorhanden ist, der zum geregelten Abfahren nach Kühlmittelverluststörfällen eingesetzt werden kann. Dieser zeichnet die Frischdampftemperatur auf, die vor einem der Turbinenschnellschlußventile gemessen wird. Wird nicht über die FD-Umleiteinrichtung abgefahren, müssen die Anzeigen der Frischdampftemperatur herangezogen werden,

deren Meßstellen vor den FD-Schnellschlußschiebern liegen. Das Wartenpersonal muß dann selbst ein Temperatur/Zeit-Diagramm erstellen.

Schließlich soll noch erwähnt werden, daß der Frischdampftemperaturschreiber kein Linienschreiber ist, sondern ein 12fach-Punktdrucker. Es handelt sich hier also um eine unübersichtliche und ungenaue Anzeige. Das Gerät ist noch dazu in der Wartentafel vor dem Steuerpult untergebracht, während die Betätigung der Frischdampf-Umleiteinrichtung und der Abblaseregelventile vom Fahrpult aus erfolgt.

Gesondert behandelt wird das zu schnelle Auffahren der Frischdampf-Umleitventile bzw. der Abblaseregelventile. Die dadurch verursachte Druckabsenkung im Frischdampfsystem führt zum Ansprechen der Reaktorschutzsignale YZ60 ($\Delta p/\Delta t$-Signale zur Leckerkennung im Frischdampfsystem, Abschnitt 4.4), wodurch sowohl die Frischdampf-Schnellschlußschieber als auch die Frischdampf-Abblaseeinrichtung automatisch geschlossen werden. Ein Öffnen der Armaturen der Frischdampf-Abblaseeinrichtung zum Fortsetzen des Abfahrens ist dann frühestens nach 15 Minuten möglich. Zum Öffnen der Frischdampf-Schnellschlußschieber ist die Rücksetzung der Absperrsignale YZ60 im Ringraum notwendig; das ist nach 15 bis 20 Minuten möglich. Bei abgesperrtem Frischdampfsystem kann eine Frischdampfabgabe nur über die Frischdampf-Sicherheitsventile bei ca. 83 bar erfolgen.

Bei der Aufstellung der Ausfallkombinationen, die im Zusammenhang mit der ungewollten Auslösung der $\Delta p/\Delta t$-Signale stehen und die zum Ausfall des Frischdampfsystems führen, wird davon ausgegangen, daß spätestens 60 Minuten nach Störfalleintritt mit dem Abfahren (mit 100 °C/h) begonnen werden muß. Bei einem tatsächlichen Abfahrbeginn zwischen 20 und 30 Minuten nach Störfalleintritt können demnach höchstens zwei Auslösungen der $\Delta p/\Delta t$-Signale durch zu schnelles Auffahren der Armaturen zugelassen werden, um gerade noch in der Zeit zu bleiben. Zum Ausfall des Frischdampfsystems führt daher die Ausfallkombination: dreimal zu schnelles Auffahren der Frischdampf-Umleitventile bzw. der Abblaseregelventile. Dabei wird angenommen, daß die Rücksetzung des Absperrsignals nach einer Fehlauslösung so schnell wie

möglich durchgeführt wird. Die dritte Fehlauslösung kann frühestens nach ca. 1 Stunde erfolgen.

Es wird davon ausgegangen, daß nach Fehlauslösung des Absperrsignals zunächst über die Abblaseregelventile (über Dach) weiter abgefahren wird. Gelingt dann nach der ersten Fehlauslösung des Absperrsignals die Fortsetzung des Abfahrens über die Abblaseregelventile nicht, so führt bereits eine weitere Fehlauslösung zum Ausfall des Frischdampfsystems. Durch die in diesem Fall erforderliche Zeit für die Rücksetzung des Absperrsignals (zum Öffnen der Frischdampf-Schnellschlußschieber) wird bei dem zugrunde gelegten Abfahrbeginn (20 bis 30 Minuten nach Störfalleintritt) der Abfahrvorgang unzulässig lange verzögert. Im Fehlerbaum ist dieser Fall durch folgende Ausfallkombination dargestellt:

- zu schnelles Auffahren der Frischdampf-Umleitventile (bewirkt erste Auslösung des Absperrsignals) UND
- Ausfall der Fortsetzung des Abfahrens über Abblaseregelventile durch Ausfall beider Abblaseregelventile ODER durch Ausfall der Abfahrleitungen zu diesen Ventilen UND
- nochmaliges zu schnelles Auffahren der Frischdampf-Umleitventile (bewirkt zweite Auslösung des Absperrsignals).

Weiterhin führt der Ausfall der Rücksetzung der Absperrsignale innerhalb von ca. 40 Minuten nach Auslösung in Verbindung mit dem Versagen des Abfahrens über die Abblaseregelventile zum Ausfall des Frischdampfsystems, so daß sich folgende Verknüpfung ergibt:

- zu schnelles Auffahren der Frischdampf-Umleitventile (bewirkt erste Auslösung des Absperrsignals) UND
- Ausfall der Fortsetzung des Abfahrens über Abblaseregelventile (siehe oben) UND
- kein Rücksetzen des Absperrsignals innerhalb von ca. 40 Minuten nach Auslösung.

- Ausfall des Abfahrens über Frischdampf-Umleiteinrichtung

Tritt beim Kühlmittelverluststörfall zusätzlich der Notstromfall ein, so spricht der Kondensatorschutz an. Ein Abfahren über die

Frischdampf-Umleiteinrichtung ist dann nicht mehr möglich. Die Komponentenausfälle, die zusätzlich zum Ausfall des Abfahrens über die Umleiteinrichtung führen, sind im Fehlerbaum im Funktionselement "Ausfall der Frischdampf-Umleiteinrichtung" zusammengefaßt. Sie umfassen Ausfälle bei den Frischdampf-Umleitventilen und dem Kondensator.

- Ausfall des Abfahrens über Abblaseregelventile

Zum Abfahren über die Abblaseeinrichtung sind im Störfall "Kleines Leck in einer Hauptkühlmittelleitung" beide Abblaseregelventile (22 RA11 S001, 24 RA12 S001) erforderlich (Abschnitt 6.1.1), d.h., der Ausfall eines der Ventile führt zum Ausfall des Abfahrens über die Abblaseeinrichtung. Die Energieversorgung der Ventile läuft über die unterbrechungslose Notstromschiene 22 FR82 J bzw. 24 FR92 J. Der Ausfall dieser Schienen im Notstromfall kann gegenüber den Armaturen vernachlässigt werden und ist im Fehlerbaum nicht enthalten.

- Ausfall der Frischdampfabgabe über Frischdampfstrang 1 und Frischdampfschieber

Da sich die Frischdampf-Schnellschlußschieber im normalen Leistungsbetrieb in Offenstellung befinden, ist der Ausfall der Frischdampfabgabe über die einzelnen Stränge nur nach einer Systemauftrennung durch fälschliches Auslösen der $\Delta p/\Delta t$-Signale zu betrachten. Ein Ausfall von Strang 1 liegt dann vor, wenn

- die Frischdampf-Umleitventile zu schnell aufgefahren werden UND
- das Frischdampf-Sicherheitsventil in Strang 1 nicht schließt ODER
- die Frischdampf-Umleitventile zu schnell aufgefahren werden UND
- der Frischdampf-Schnellschlußschieber 20 RA01 S002 in Strang 1 nicht öffnet UND
- eine Verbindung über die Abfahrleitung von Strang 1 und einen der übrigen drei Frischdampfstränge nicht zustande kommt.

Der Ausfall des hydraulisch betätigten Frischdampf-Schnellschlußschiebers liegt vor, wenn eines von sechs Steuerventilen oder der elektromotorische Antrieb des Schnellschlußschiebers ausfällt. Die Funktion des Elektroantriebs 20 RA01-04 S802 ist erforderlich, weil die Betätigung der Steuerventile 20 RA01-04 S302 und 20 RA01-04 S502 zum Öffnen des Schiebers nur möglich ist, wenn vorher (nach dem Schnellschluß) der Antrieb in die Geschlossen-Stellung gefahren ist (Freigabe-Bedingung). Kann nach Auslösung der Absperrsignale YZ60 zunächst über die Abblaseregelventile weiter abgefahren werden, so steht zur Rücksetzung des Absperrsignals und Wiederinbetriebnahme der Frischdampf-Umleiteinrichtung (Öffnen der Frischdampf-Schnellschlußschieber und der Frischdampf-Umleitventile) mehr als eine Stunde zur Verfügung. Bei Ausfall des Frischdampf-Schnellschlußschiebers in Strang 1 besteht die Möglichkeit, eine Verbindung über die Abfahrleitung von Strang 1 zu einem der übrigen Frischdampfstränge herzustellen. Ein Ausfall dieser Verbindung liegt vor, wenn der Absperrschieber in der Abfahrleitung von Strang 1 oder wenn Absperrschieber bzw. Schnellschlußschieber der Stränge 2, 3 und 4 nicht aufgefahren werden können.

Da nach der ersten Auslösung der $\Delta p/\Delta t$-Signale der Frischdampfdruck bis zum Ansprechen der Sicherheitsventile ansteigt, liegt der Ausfall eines Frischdampfstranges auch dann vor, wenn das entsprechende Sicherheitsventil nicht schließt. Die Ausfallkombination 1v4 Frischdampf-Sicherheitsventilen schließt nicht UND fälschliches Öffnen des entsprechenden Absperrschiebers oder Frischdampf-Schnellschlußschiebers wird gegenüber der Handmaßnahme "Nochmaliges zu schnelles Auffahren der Frischdampf-Umleiteinrichtung oder der Abblaseregelventile" vernachlässigt.

- Ausfall der Frischdampfabgabe über Frischdampfstrang 1 und Abfahrleitung

Steht die Frischdampf-Umleiteinrichtung beim Einleiten des Abfahrens nicht zur Verfügung, so erfolgt die Frischdampfabgabe über die Abfahrleitungen der Frischdampfstränge. Es kommt in diesem

Fall zum Ansprechen der Frischdampf-Sicherheitsventile. Schließt 1v4 Sicherheitsventilen nicht, so werden u.a. die Absperrsignale YZ60 ausgelöst. Die Auslösung der $\Delta p/\Delta t$-Signale erfolgt außerdem bei zu schnellem Auffahren der Abblaseregelventile.

Nur bei voneinander getrennten Frischdampfsträngen (d.h. bei geschlossenen Frischdampf-Schnellschlußschiebern) führt allein der Ausfall des Absperrschiebers in Strang 1 zum Ausfall der Frischdampfabgabe über Strang 1. Bei offenen Frischdampf-Schnellschlußschiebern ist dagegen eine Verbindung über den Frischdampfsammler und die Abfahrleitungen der übrigen Frischdampfstränge möglich. Die entsprechende Ausfallkombination für diesen Fall (3v4 Absperrschieber in den Abfahrleitungen öffnen nicht) wird gegenüber dem Ausfall der Abblaseregelventile vernachlässigt.

Die Funktionsprüfungen der Abblaseabsperrschieber und Abblaseregelventile werden bei Leistungsbetrieb des Kraftwerks durchgeführt. Die Armaturen sind für Frischdampfdrücke von 82 bar ausgelegt. Im Frischdampfsystem sind jedoch Störfälle denkbar, bei denen der Frischdampfdruck auf über 100 bar ansteigt. Eine Drehmomentschalter-Überbrückung zum Auffahren der Armaturen ist aus folgenden Gründen weder bei den Abblase-Absperrschiebern noch bei den Regelventilen vorhanden:

- Als Absperrarmaturen sind Schieber eingesetzt, bei denen die Schieberplatte wegabhängig auf- und zugefahren wird.
- Bei den Regelventilen wurde festgestellt, daß zum Auffahren der Ventilkegel nur ca. 33 % des zum Schließen benötigten Drehmoments aufgewendet werden müssen. Ein Ansprechen der Drehmoment-Schalter ist somit nicht zu befürchten. Der Antrieb der Regelventile ist so dimensioniert, daß der Kegel auch bei einem FD-Druck von ca. 100 bar aus dem Sitz gefahren werden kann.

Die in den Fehlerbäumen 10 B, C und D dargestellten Ausfallverknüpfungen für die Redundanzen 2, 3 und 4 des Frischdampfsystems entsprechen denen der Redundanz 1.

6.1.2.2.16 Fehlerbaum 16: Lüftungsanlagen

Während des Leistungsbetriebs des Kernkraftwerks sind die Umluftanlagen in Bereitschaft. Die Belüftung und Klimatisierung erfolgt dann über separate Lüftungsanlagen. Eine Einschaltung der Umluftanlagen über die Raumthermostate ist daher bei Normalbetrieb nicht zu erwarten.

Die Funktion der Anlagen wird bei Tests der entsprechenden Reaktorschutzsignale geprüft. Die Kühler werden dauernd vom Kühlwasser durchströmt, so daß hier unerkannte Ausfälle nicht zu unterstellen sind.

Aus rechenprogrammtechnischen Gründen sind die Ausfälle der Energieversorgungsschienen (nur im Notstromfall relevant) in den Ausfallkombinationen der Umluftkühlung für die Diesel nicht enthalten.

In den betrachteten Störfällen wird die zu den Reaktorschutzsignalen YZ81 redundante betriebliche Ansteuerung nicht berücksichtigt, da bei Ausfall der Reaktorschutzsignale die Freigabe durch das Reaktorschutzsystem fehlt.

6.1.2.2.17 Fehlerbaum 17: Not- und Nachkühlsystem, Hochdruck-Einspeisungen

Der Ausfall der Hochdruck-(HD-)Einspeisung durch einen Strang des Not- und Nachkühlsystems ist durch

- das Versagen von Rohrleitungen oder Flutbehältern,
- den Ausfall der HD-Sicherheitseinspeisepumpe oder
- den Ausfall von Armaturen

möglich. Dabei ist zu beachten, daß sämtliche Rückschlagarmaturen sowohl in der kalten als auch in der heißen Einspeiseleitung öffnen müssen. Falls eine Rückschlagarmatur nahezu dicht bleibt, schaltet das Dreiwegeventil - bei Absinken des Druckes im Reaktorkühlkreislauf - zu der Einspeiseleitung mit der geschlossenen Armatur um, da sich dort der höhere Druck aufbaut.

Die zugehörige HD-Sicherheitseinspeisepumpe fördert dann nur über die Mindestmengenleitung in den Flutbehälter zurück.

Der Ausfall der Umschaltfunktion des Dreiwegeventils in Strang 1 des HD-Systems führt beim mittleren Leck in einer Hauptkühlmittelleitung zum Versagen der HD-Einspeisung durch diesen Strang, da in diesem Fall die Einspeisung in die gebrochene kalte Hauptkühlmittelleitung vorgenommen wurde (Abschnitt 6.1.1 und Abschnitt 6.1.2.2.1)

Der Ausfall von passiven Komponenten, wie Bruch von Rohrleitungen oder Versagen von Flutbehältern, wird gegenüber den zu betätigenden Komponenten bei der numerischen Auswertung der Fehlerbäume vernachlässigt. Dagegen ist für das große und mittlere Leck der Folgeausfall der heißen Einspeiseleitung, die zum gebrochenen Hauptkühlkreislauf führt, in Rechnung zu stellen (Tabelle F2, 6-2).

Der Ausfall einer HD-Sicherheitseinspeisepumpe kann eintreten durch

- den Ausfall der Pumpe selbst,
- den Ausfall der elektrischen Energieversorgung,
- den Ausfall der Ansteuerung durch den Reaktorschutz,
- den Ausfall der Ölversorgung der Pumpe,
- den Ausfall der Umluftkühlung und
- den Ausfall der Kühlwasserversorgung der Pumpe durch den nuklearen Zwischenkühlkreis.

Ein Einschalten der in Bereitschaft befindlichen Pumpen durch das Reaktorschutzsystem wird verhindert, wenn die Steuerkette (bestehend aus Vorrang- und Betätigungsbaustein, Endschalter und zugehöriger Verdrahtung) oder die HD-Einspeisesignale YZ36 ausgefallen sind bzw. die Stromversorgung im Betätigungsschrank unterbrochen ist. Bei Ausfall der unverzögerten HD-Einspeisesignale werden die zur HD-Pumpe gehörigen Ölpumpen nicht eingeschaltet, was seinerseits den Ausfall der HD-Pumpe selbst zur Folge hat. Der Ausfall der verzögerten Reaktorschutzsignale führt direkt zum Ausfall der angesteuerten HD-Pumpe. Das Anstehen von AUS-Befehlen der betrieblichen Steuerung, z.B. über den

Aggregateschutz, wird über die HD-Einspeisesignale (keine Freigabe für betriebliche Steuerung) verriegelt. Das fälschliche Anstehen des AUS-Befehls vom ND-Einspeise- oder Notstromsignal ist selbstmeldend und wird daher auch nicht berücksichtigt.

Nach Anweisung des für den betrachteten Störfall relevanten Logikschemas des Betriebshandbuches sollen nach Erreichen einer Temperatur im Reaktorkühlkreislauf < 150°C bei einem Druckhalterwasserstand > 3,15 m die Notkühlvorbereitungssignale überbrückt und die HD-Sicherheitseinspeisepumpen abgeschaltet werden. Bei einem Wasserstand ≦ 2,85 m werden diese Pumpen über das Reaktorschutzsystem jedoch wieder eingeschaltet. Ein häufiges Ein- und Ausschalten der HD-Sicherheitseinspeisepumpen könnte längerfristig zum Ausfall dieser Pumpen durch Ansprechen der Überstromauslöser führen.

Vom Wartenpersonal ist der Druckhalter-Wasserstand zu beobachten (Anweisung im Betriebshandbuch) und durch geeignete Maßnahmen (Zu- bzw. Abschalten einer geeigneten Zahl von HD-Sicherheitseinspeisepumpen) zu halten. Im Logikschema wird zur Beobachtung des Druckhalter-Wasserstandes auf eine Anzeige (YP01 L004) verwiesen, deren zugehörige Meßwerterfassung nicht für die Umgebungsbedingungen nach Kühlmittelverluststörfällen ausgelegt ist. Für das Reaktorschutzsystem ist jedoch eine entsprechend ausgelegte Meßwerterfassung mit Anzeige auf der Reaktorschutztafel vorhanden, auf die das Wartenpersonal bei Ausfall der erstgenannten Meßstelle zurückgreifen kann.

Hier muß darauf hingewiesen werden, daß eine Überbrückung der Notkühlvorbereitungssignale mittels eines Schlüsselschalters dann vorgenommen werden soll, wenn der Druckhalter-Wasserstand > 3,15 m und die Temperatur im Reaktorkühlkreislauf ≦ 150°C sind. Dieser Zusammenhang wird richtig im Betriebshandbuch wiedergegeben. Bei der Bildung der Notgefahrmeldung wird jedoch die Temperatur im Reaktorkühlkreislauf nicht abgefragt. Von dieser Notgefahrmeldung wird auch die Meldung auf der Anweisungstafel "Leck im RKL, Überbrückung YZ31/35/36/38" abgeleitet.

Für die vorliegende Studie wird davon ausgegangen, daß eine Abschaltung der HD-Sicherheitseinspeisepumpen und eine damit ver-

bundene Überbrückung der Notkühlvorbereitungssignale nicht erforderlich sind.

Die HD-Sicherheitseinspeisepumpen werden während der Funktionsprüfungen bei zwei Betriebspunkten der Pumpenkennlinie getestet. Die Pumpen unterliegen dabei den gleichen Beanspruchungen wie bei einem Störfall. Die Dauer der Funktionsprüfungen der HD-Sicherheitseinspeisungen ist allerdings sehr kurz, bei "kleinen Lecks" sind hingegen zwei Stunden Betriebszeit zu erwarten. Bei "kleinen Lecks am Druckhalter" können die Betriebszeiten auch erheblich länger sein.

Bei bestimmten Querschnitten von kleinen Lecks im Reaktorkühlkreislauf ist eine Überspeisung des Lecks möglich. Je nach Leckquerschnitt und Anzahl der funktionierenden HD-Einspeisungen stellt sich dann ein bestimmter Druck im Reaktorkühlkreislauf ein, der trotz sekundärseitigem Abfahren nicht abgesenkt werden kann, solange die HD-Einspeisungen laufen. Dagegen wird durch das sekundärseitige Abfahren und die Einspeisung von Borwasser mit einer Temperatur von 25 °C aus den Flutbehältern die Kühlmitteltemperatur abgesenkt. Als Folge des unter hohem Druck eingespeisten kalten Wassers ist eine Unterschreitung der Sprödbruchübergangstemperatur denkbar. Eine Rechnung zeigt jedoch, daß unter Zugrundelegung des während der HD-Einspeisungen maximal möglichen Druckes im Reaktorkühlkreislauf von 110 bar (Nullförderhöhe der HD-Sicherheitseinspeisungen) die kritischen Temperaturwerte nicht erreicht werden. Die Werte gehen von 40 Betriebsjahren der Anlage aus.

6.1.2.2.18 Fehlerbaum 18: Not- und Nachkühlsystem, Niederdruck-Einspeisungen

Unabhängige Ausfälle von Rohrleitungen werden wie bei den Hochdruck-Einspeisungen grundsätzlich berücksichtigt. Beim Bruch von Rohrleitungen, Armaturen oder des Nachwärmekühlers (primär) brauchen die Rohrleitungen zwischen dem Druckspeicher und dem Reaktorkühlkreis nicht in Rechnung gesetzt werden, da deren Versagen (zum Unterschied von Rissen in den übrigen angesprochenen

Komponenten) sofort entdeckt wird. Ebenso wird das Versagen eines Flutbehälters oder der anschließenden Rohrleitungen sofort erkannt, es spielt daher nur eine untergeordnete Rolle. Folgeausfälle von Einspeiseleitungen sind in Tabelle F2, 6-2 erfaßt. Für die im Fehlerbaum eingetragene Blockierung der Sumpfansaugung oder des Nachwärmekühlers spielen höchstens CMA eine Rolle; unabhängige Ausfälle können im Vergleich zu denen der zu betätigenden Komponenten des Not- und Nachkühlsystems vernachlässigt werden.

Ein zu geringer Wasserstand in einem Flutbehälter führt zum Ausfall des entsprechenden Stranges des Kernnot- und Nachkühlsystems für Fluten.

Der Wasserstand wird daher über Differenzdruckmessungen, z.B. 20 TH10 L002, verfolgt und auf der Warte angezeigt. Durch Grenzsignalgeber wird auf der Warte eine Störungsmeldung bei zu hohem oder zu niedrigem Wasserstand ausgegeben. Eine Funktionsprüfung der Meßwerterfassung der Störungsmeldungen ist zwar nicht vorgeschrieben (Abschnitt 5.2), der Wasserstand wird aber jährlich beim Fluten des Reaktorbeckens zum Brennelement-Wechsel überprüft. Ein nicht selbstmeldender gefährlicher Ausfall der Messung 20 TH10 L002 wird dadurch bemerkt, daß für den Flutbehälter noch zusätzlich drei Wasserstandsanzeigen auf der Reaktorschutztafel der Warte vorhanden sind, die aus den zur Bildung von Reaktorschutzsignalen notwendigen Messungen abgeleitet werden. Ferner gibt es für jeden Flutbehälter eine örtliche Niveauanzeige, die von Zeit zu Zeit überprüft wird. Ein außerhalb des Toleranzbereiches liegender Wasserstand in den Flutbehältern kann daher nur bei Vielfachausfällen auftreten und wird deshalb vernachlässigt.

Das in den Flutbehältern gelagerte Deionat muß mindestens 2200 ppm Bor enthalten. Diese Konzentration kann unterschritten werden durch

- Ansteigen des Wasserstandes in den Flutbehältern durch Leckagen aus dem Reaktorkühlkreislauf,
- Auskristallisation von Bor oder
- Nachfüllen von Deionat mit zu niedriger Borkonzentration.

Bei zu hohem Flutbehälterwasserstand wird, wie bereits beschrieben, eine Störmeldung auf der Warte ausgegeben. Laut Betriebshandbuch ist dann neben einer Absenkung des Wasserstandes auch eine Überprüfung der Borkonzentration vorzunehmen. Eine Auskristallisation von Bor ist nicht zu befürchten, da die Lösung einen genügend großen Abstand zu ihrem Sättigungspunkt aufweist. Durch die vorgeschriebene vierwöchentliche Funktionsprüfung (Probeentnahme mit chemischer Analyse im Labor) wird eine Abnahme der Borkonzentration, z.B. durch Nachfüllen von Deionat mit zu niedrigem Borgehalt, erkannt. Damit wird die Möglichkeit einer unbemerkt zu niedrigen Borkonzentration gegenüber anderen Ausfällen in diesem System vernachlässigbar.

Für die Nachkühlpumpen ist, ähnlich wie nach Kühlmittelverluststörfällen, ein langfristiger Einsatz beim bestimmungsgemäßen Betrieb während des Abfahrens der Anlage in den Zustand "unterkritisch kalt" notwendig.

Ausfälle von laufenden Nachkühlpumpen bei Kühlmittelverluststörfällen sollen durch Funktionsprüfungen vermieden werden, bei denen die Pumpen unter störfallähnlichen Bedingungen getestet werden. Bei den Nachkühlpumpen ist dies jedoch nicht in vollem Umfang möglich. Die Nachkühlpumpen saugen bei den Funktionsprüfungen ausschließlich aus den Flutbehältern an und fördern ca. 100 t/h in die Einspeisestränge des Not- und Nachkühlsystems. Eine Überprüfung des bei Kühlmittelverluststörfällen notwendigen Umschaltvorgangs auf Sumpfbetrieb ist nicht möglich. Im Störfall tritt dabei eine Temperaturänderung des Fördermediums von ca. 60 bis 70 °C ein. Die Pumpen laufen für ca. 20 Sekunden in Kavitation.

Unter pessimistischen Randbedingungen durchgeführte Rechnungen haben ergeben, daß bei bestimmten Leckquerschnitten in einer Hauptkühlmittelleitung außerdem ein längerfristiger Kavitationsbetrieb eintreten kann. Voraussetzung ist dabei, daß nur die Mindestanforderungen an die Notkühlung erfüllt sind, d.h. nur 2v4 ND-Einspeisungen funktionieren. Versuche haben aber gezeigt, daß auch bei mehrstündigem Kavitationsbetrieb keine Schäden an den Nachkühlpumpen zu erwarten sind.

Bei "kleinen Lecks" fällt der Kühlmitteldruck unter Umständen nur sehr langsam ab, Schäden an den Nachkühlpumpen sind auch hierdurch nicht zu erwarten. Pumpentests haben nämlich ergeben, daß weder ein 24stündiger Betrieb mit der Mindestmenge von 20 t/h noch ein 30minütiger Betrieb bei Nullförderhöhe an Welle oder Laufrad Schäden hervorrufen.

Bei einer Sumpfwasserverschmutzung ist nicht mit einem kurzfristigen Ausfall der Nachkühlpumpen zu rechnen. Das Einsetzen von Gitterrosten mit einer Maschenweite von 8 x 8 mm am Eintritt zu den Sumpfkammern verhindert zum einen eine übermäßig grobkörnige Verschmutzung des Sumpfwassers, andererseits haben Versuche bewiesen, daß z.B. Betonsplitter mit einer Körnung von 15 mm von der Pumpe zerrieben wurden, ohne Schäden an ihr zu hinterlassen. Unter solch ungünstigen Betriebsbedingungen sind jedoch erhöhte Ausfallraten der Pumpen anzusetzen (Abschnitt 3.3.6.2.2).

Eine Blockage des Gebäudesumpfes ist ebenfalls nicht zu erwarten. Unter der Annahme, daß sich das gesamte anfallende Isoliermaterial in der an den Hauptkühlmittelleitungen vorhandenen Stärke von 120 mm gleichmäßig über die Gitterfläche ausbreitet, wird eine Fläche von ca. 75 m^2 bedeckt, so daß 90 m^2 der waagerechten Gitter frei bleiben. Werden beim Bruch einer Hauptkühlmittelleitung durch die Auswirkungen der Strahlkräfte auch Folgeschäden am Beton unterstellt, so muß davon ausgegangen werden, daß derartige Abplatzungen oder Auswaschungen nur eng begrenzt auftreten und somit die anfallenden Mengen sehr gering sind. Die vollständige Integrität der waagerechten Gitter kann aufgrund der herabfallenden Bruchstücke zwar nicht sichergestellt werden, ihre Siebwirkung bleibt jedoch weitgehend erhalten.

Im folgenden soll auf die im Fehlerbaum 18 eingetragenen Ausfallkombinationen eingegangen werden. Dabei wird auf die Redundanz 1 Bezug genommen. Abgesehen von der numerischen Behandlung von Leitungsbrüchen als Störfallfolge gilt Entsprechendes für die Redundanzen 2, 3 und 4.

- Ausfall der kalten ND-Einspeisung durch Nachkühlstrang 1 für Fluten

Hier ist das Nichtöffnen der Rückschlagarmaturen 20 TH11 S001 und 20 TH11 S002, über die die kalte Einspeisung erfolgt, zu berücksichtigen. Falls vor der ND-Einspeisung die HD-Einspeisung angefordert wird, ist ein Ausfall der kalten ND-Einspeisung auch dadurch möglich, daß die Armaturen im HD-Einspeisestrang nicht mehr schließen. Die Nachkühlpumpe saugt dann aus dem Flutbehälter an und fördert über diese Leitung einen Teil wieder in den Flutbehälter zurück, so daß nicht mehr die gesamte geförderte Menge in den Reaktordruckbehälter eingespeist wird. (Nach einer Abschätzung gehen dadurch allerdings nur etwa 10 % der Fördermenge verloren.)

Außerdem geht hier, wie auch beim "Ausfall der heißen Einspeisung für Fluten und Sumpfbetrieb", ein Versagen der Komponentenfunktionen ein, ohne die weder eine kalte noch eine heiße Einspeisung möglich ist. Es sind dies neben den Ausfällen passiver Komponenten der Ausfall der Nachkühlpumpe 21 TH10 D001 und das Versagen der Flutbehälter-Rückschlagklappe 20 TH10 S035; öffnet nämlich diese Armatur bei Flutbetrieb nicht, so wird der Flutbehälter nicht entleert und die Umschaltung auf Sumpfbetrieb unterbleibt.

Zum Betrieb der Nachkühlpumpen ist deren Kühlung über den entsprechenden Strang des nuklearen Zwischenkühlkreises erforderlich. Die Nachkühlpumpen können nicht anlaufen, wenn die Steuerkette den EIN-Befehl unterdrückt oder wenn die ND-Einspeisesignale nicht ausgegeben werden. Die zu den Reaktorschutzsignalen redundante Handzuschaltung der Pumpe wird als ausgefallen betrachtet, da der Ausfall der ND-Einspeisesignale vorwiegend durch Kurzschlüsse verursacht wird (Abschnitt 6.1.2.2.1) und damit auch keine Freigabe für Handbefehle vorhanden ist.

Das fälschliche Anstehen des Notstromsignals würde zwar auch das Einschalten der Pumpe verhindern, dieser Ausfall ist aber selbstmeldend und kann daher vernachlässigt werden. Ist die 24-

V-Versorgung für den oberen Teil des Betätigungsschranks 21 HA03 ausgefallen, so kann die Nachkühlpumpe nicht gestartet werden.

Ferner sind die Funktionselement-Ausfälle zu berücksichtigen, die einen "Ausfall der ND-Einspeisung durch den Nachkühlstrang 1 nur für Fluten" zur Folge haben (siehe unten).

- Ausfall der heißen ND-Einspeisung durch Nachkühlstrang 1 für Fluten und Sumpfbetrieb

Darunter fällt das Versagen der Komponenten, ohne die eine entsprechende ND-Einspeisung nicht möglich ist. Wie beim Ausfall der kalten ND-Einspeisung für Fluten geht auch hier ein Versagen der Komponenten ein, ohne die überhaupt keine Einspeisung erfolgt. Zusätzlich ist zu beachten, daß ein Bruch der Nachkühlsaugleitung im Strang 1 als Störfallfolge zu einem Ausfall der Nachkühlpumpe infolge Kavitation führt. Ein Ausfall der heißen Einspeisung erfolgt darüber hinaus bei einem Bruch der heißen Einspeiseleitung als Störfallfolge oder bei Nichtöffnen der Rückschlagarmatur 21 TH12 S006 oder 21 TH12 S001 in der heißen Einspeiseleitung des Nachkühlstranges. Falls vor der ND-Einspeisung die HD-Einspeisung angefordert wurde, kann es zum Ausfall der heißen ND-Einspeisung auch dadurch kommen, daß die Armaturen für die HD-Einspeisung nicht mehr schließen; es wird dann nicht die gesamte durch die Nachkühlpumpe geförderte Menge in den Reaktordruckbehälter eingespeist.

- Ausfall der ND-Einspeisung durch Nachkühlstrang 1 nur für Fluten

Während die kontrollverriegelten Armaturen, die nach dem Störfall keinen weiteren Befehl erhalten, nach einer Abschätzung (Abschnitt 6.1.2.2.1) vernachlässigt werden können, ist dies bei den Armaturen nicht möglich, die sowohl kontrollverriegelt sind als auch zu einem späteren Zeitpunkt betätigt werden. Dies trifft für alle Armaturen zu, die sowohl von den Flut- als auch von den Sumpfsignalen angesteuert werden. Ein fälschlicherweise

anstehendes Sumpfsignal YZ41 bewirkt hier ein fälschliches Verfahren der Flutbehälter-Armaturen 21 TH10 S001 und 21 TH10 S002. So ist es möglich, daß diese Motorarmaturen zum Zeitpunkt des Störfalls durch ein vor der Entleerung des Flutbehälters fälschlich bereits anstehendes Signal unbeabsichtigt schließen. Das hat einen Ausfall des Stranges nur für Fluten zur Folge (Borwasser aus dem Flutbehälter wird nicht eingespeist), denn bei diesem Ausfall wird durch das Sumpfsignal gleichzeitig die Sumpfarmatur geöffnet.

Bei der Auswirkung dieser vorzeitigen Umschaltung auf Sumpfbetrieb sind bezüglich der Nachkühlpumpe zwei Fälle zu unterscheiden:

- Ist die Ansaugöffnung der TH-Saugleitung im Sumpf bereits geflutet, so ist ein kavitationsfreier Betrieb der Nachkühlpumpe gewährleistet, wenn von drei laufenden Nachkühlpumpen ausgegangen wird. Bei Einspeisung mit nur zwei Nachkühlpumpen ergeben sich einerseits höhere Sumpfwassertemperaturen, andererseits steigt aufgrund der höheren Verdampfungsrate auch der Druck im Sicherheitsbehälter. Beide Effekte kompensieren sich teilweise, so daß nicht mit einer Gefährdung der Nachkühlpumpen durch Kavitation zu rechnen ist.
- Ist die Ansaugöffnung im Gebäudesumpf zum Zeitpunkt der Umschaltung noch nicht geflutet, so saugt die entsprechende Nachkühlpumpe ein Dampf-Luft-Gemisch an, es tritt Kavitation ein. Bei Erfüllung der Mindestanforderungen an die Notkühlung liegen solche Betriebsbedingungen nur für kurze Zeit vor, nämlich bis durch die beiden verfügbaren ND-Einspeisungen für Fluten die Ansaugöffnungen im Sumpf geflutet sind. Aufgrund von Versuchen kann davon ausgegangen werden, daß die Nachkühlpumpe in dem vorzeitig umgeschalteten Strang für Sumpf-Umwälzbetrieb verfügbar ist.

Ein Ausfall des Nachkühlstranges nur für Fluten ist auch dadurch möglich, daß die Sumpfarmatur 21 TH01 S001 unbeabsichtigt öffnet.

Ausfälle von Sumpf- und Flutbehälterarmaturen bei Kühlmittelverluststörfällen aufgrund von unterdimensionierten Stellantrieben sind nicht zu erwarten. Bei den monatlich durchzuführenden Funk-

tionsprüfungen müssen zum Verfahren der Armaturen in etwa die gleichen Drehmomente aufgewendet werden wie beim Störfall. Um ein fälschliches Ansprechen der Drehmomentschalter bei Umschalten auf Sumpfbetrieb zu verhindern, sind die Sumpfarmaturen zum Auffahren mit einer Drehmomentschalter-Überbrückung ausgerüstet. Die redundanten Flutbehälterarmaturen sind diversitär ausgeführt. Die Armaturen TH10-40 S001 werden in Schließrichtung drehmomentabhängig abgeschaltet, die Armaturen TH10-40 S002 dagegen wegabhängig. Eine Drehmomentschalter-Überbrückung ist bei den Armaturen in Schließrichtung nicht vorhanden.

- Ausfall der heißen ND-Einspeisung durch Nachkühlstrang 1 für Sumpfbetrieb

Beim "Ausfall der heißen ND-Einspeisung durch Nachkühlstrang 1 für Sumpfbetrieb" ist zusätzlich zum Ausfall der heißen Einspeisung für Fluten und Sumpfbetrieb zu berücksichtigen, daß die Sumpfarmatur 21 TH01 S001 bei Umschaltung auf Sumpfbetrieb nicht öffnet. Wie bei der Ansteuerung der Nachkühlpumpen wird die zum Reaktorschutzsignal redundante Handzuschaltung bei Kühlmittelverluststörfällen als ausgefallen betrachtet.

Der Ausfall der Nachkühlpumpen ist für Sumpfbetrieb noch zusätzlich dadurch möglich, daß die Pumpen fälschlich aus bereits leeren Flutbehältern Luft ansaugen und dadurch ausfallen. Dies kann der Fall sein, wenn bei überbrückten ND-Einspeisesignalen die Nachkühlpumpen nach Unterschreiten des Mindestwasserstandes in den Flutbehältern nicht ausgeschaltet bzw. die entsprechenden Armaturen nicht auf Sumpfbetrieb umgeschaltet werden und der Pumpenschutz nicht anspricht.

Weiterhin ist für Sumpfbetrieb der Ausfall des nuklearen Nebenkühlwasserstranges 1 zu berücksichtigen, da zusätzlich zur Verlustwärme der Pumpen die über die Nachwärmekühler anfallende Wärme abgeführt werden muß.

- Ausfall des Not- und Nachkühlsystems beim Bruch der Nachkühlsaugleitung im Strang 1

Falls die Nachkühlsaugleitung beschädigt wird, führt eine zum Zeitpunkt des Störfalls fälschlich offene Flutbehälter-Rückschlagklappe 20 TH10 S035 zum Ausfall des Not- und Nachkühlsystems.

Eine fälschlich offene, d.h. eine in Offenstellung verklemmte Flutbehälter-Rückschlagklappe ist aus folgenden Gründen möglich:

- Die Rückschlagklappe hat bei der letzten Funktionsprüfung nicht geschlossen und die zugehörige Stellungsmeldung am Wartenpult wurde übersehen bzw. nicht überprüft. Laut Prüfablauf für die Reaktorschutzsignale YZ36/38 wird am Ende der Funktionsprüfung die Störfallbereitschaft des entsprechenden Nachkühlstrangs geprüft, wobei allerdings nur auf ein anderes Logikschema des Betriebshandbuches verwiesen wird. Eine besondere Überprüfung der Stellung der Rückschlagklappe ist nicht vorgesehen.
- Die Rückschlagklappe ist ständig fälschlich offen, dies kann aber nicht entdeckt werden, weil die Meldeeinrichtung hierzu ausgefallen ist und nicht überprüft wird, ob auch bei offener Rückschlagklappe fälschlicherweise die Meldung "Rückschlagklappe geschlossen" ansteht.

- Ausfall des Not- und Nachkühlsystems bei offener Sumpfarmatur im Strang 1 für Fluten

Eine zum Zeitpunkt des Störfalls fälschlich offene Rückschlagklappe führt auch zum Ausfall des Not- und Nachkühlsystems, wenn zusätzlich die Sumpfarmatur 21 TH01 S001 unbeabsichtigt öffnet sowie die Flutbehälter-Armaturen 21 TH10 S001 und 21 TH10 S002 nicht schließen.

Durch den nach dem Auslegungsstörfall in der Stahlhülle herrschenden Druck wird dann das im Reaktorgebäude befindliche Sumpfwasser über die Flutbehälter in den Ringraum gedrückt.

Ursache kann sein, daß bei anstehenden Flutsignalen die Sumpfarmatur fälschlicherweise aufgefahren wird. Dies ist dadurch möglich, daß bei einem Ausfall in der Steuerkette ein die Stellung kontrollierender ZU-Befehl die Armatur auffährt. Eine weitere Ursache kann sein, daß statt der Flut- fälschlicherweise die Sumpfsignale ausgegeben werden und gleichzeitig die beiden Flutbehälter-Armaturen 21 TH10 S001 und 21 TH10 S002 ausgefallen sind, also nicht mehr schließen.

- Ausfall des Not- und Nachkühlsystems bei offener Rückschlagklappe und offenen Flutbehälterarmaturen im Strang 1 für Sumpfbetrieb

Zusätzlich zu dem bisher diskutierten Fall der fälschlich offenen Flutbehälter-Rückschlagklappe 20 TH10 S035 besteht die Möglichkeit, daß die Rückschlagklappe bei Flutbetrieb öffnet und bei Umschaltung auf Sumpfbetrieb nicht mehr schließt. Fallen bei der Umschaltung auf Sumpfbetrieb außer der Flutbehälter-Rückschlagklappe die Motorarmaturen 21 TH10 S001 und 21 TH10 S002 in der Flutbehälterleitung aus, während die Sumpfarmatur 21 TH01 S001 öffnet, so wird das Sumpfwasser durch den im Sicherheitsbehälter herrschenden Druck in die Flutbehälter zurückgedrückt. Bei Überschreitung des minimalen Flutbehälterwasserstandes wird durch die Flutsignale die Rückschaltung auf Flutbetrieb ausgelöst. Ist eine Rückschaltung nicht mehr möglich, weil die Sumpfarmatur nicht wieder schließt, so führt dies ebenfalls zum Ausfall des gesamten Not- und Nachkühlsystems.

- Ausfall des Not- und Nachkühlsystems bei Rückströmung durch den HD-Einspeisestrang 1

Nach erfolgter HD-Einspeisung kann es zum Ausfall der Schließfunktion der Rückschlagarmaturen im HD-Einspeisestrang kommen. Zum Ausfall des gesamten Not- und Nachkühlsystems führt eine dann stattfindende Rückströmung durch den HD-Einspeisestrang in die zugehörigen Flutbehälter, wenn das Wasser von dort nicht mehr zurückgefördert werden kann. Ursache kann entweder das Versagen der Nachkühlpumpe einschließlich deren Kühlung sein oder

der Ausfall der Rückschaltung auf Flutbetrieb (Tabelle F2, 6-2 und zugehörige Erläuterungen). Genaugenommen wären diese beiden Möglichkeiten im Gesamtfehlerbaum zu differenzieren, da sie zu einem unterschiedlichen Zeitpunkt zum Versagen der Notkühlung führen.

Für ein fälschlich offenes Rückschlagventil 20 TH15 S005 gilt das bei der Flutbehälter-Rückschlagklappe Gesagte. Auf diese Weise sind auch fälschlich offene Rückschlagarmaturen 20 TH15 S009 und 20 TH15 S010 möglich. Da diese Ausfälle aber durch die Druckmessung 20 TH15 P003 (Anzeige auf der Warte) entdeckt werden können und daher wesentlich unwahrscheinlicher sind, werden sie im Fehlerbaum vernachlässigt.

Bei Versagen der Schließfunktion der Rückschlagklappen wird das rückströmende Wasser zunächst in den Flutbehältern aufgefangen. Dadurch wird Zeit gewonnen, so daß durch Handeingriff der Schieber 20 TH15 S001 zugefahren werden kann. Ein Austritt des Wassers in den übrigen Ringraum wird so verhindert. Wird der Schieber nicht zugefahren, so kann es langfristig zu einer Überflutung des Ringraumes kommen. Dann ist wie beim Bruch von TH-Rohrleitungen im Ringraum während der ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB vorzugehen (siehe unten). Aufgrund der vorgesehenen Außerbetriebnahme der Notkühlpumpe schließen in diesem Strang des Not- und Nachkühlsystems die letzten Rückschlagarmaturen zum Reaktorkühlkreislauf, wodurch eine weitere Rückströmung durch den HD-Einspeisestrang unterbunden wird.

Ausfälle des Not- und Nachkühlsystems aufgrund einer Rückströmung durch die Nachkühlsaugleitung oder durch den ND-Einspeisestrang bei gleichzeitigem Ausfall der Nachkühlpumpe haben eine wesentlich geringere Wahrscheinlichkeit als die hier diskutierten Ausfälle und spielen demnach keine Rolle.

- Rückschlagarmaturen im Not- und Nachkühlsystem

Die Funktion der Rückschlagarmaturen im Not- und Nachkühlsystem an den Einspeisestellen zum Reaktorkühlkreislauf wird entsprechend dem Prüfhandbuch nur einmal jährlich - beim Brennele-

mentwechsel - getestet. Die Prüfung, der die Rückschlagventile dabei unterzogen werden, kann nicht als repräsentativ für Kühlmittelverluststörfälle angesehen werden. Ein CMA dieser Rückschlagventile ist aber aus folgenden Gründen trotzdem nicht zu erwarten:

- Das Konstruktionsprinzip dieser Rückschlagventile ist bewährt.
- Während des Betriebes herrschen an den Rückschlagventilen ständig die gleichen Betriebszustände, so daß keine Veränderungen an den für die Gängigkeit der Armaturen maßgebenden Teilen auftreten.
- Aufgrund der gewählten Wasserchemie können korrosive Angriffe auf das Ventilgehäuse ausgeschlossen werden.
- Zumindest die Rückschlagventile in der kalten Einspeiseleitung werden außerdem bei jedem An- und Abfahrvorgang auf einwandfreie Funktion geprüft, d.h. im Mittel etwa dreimal pro Jahr.

- Bruch von TH-Rohrleitungen während der HD-Einspeisungen oder der ND-Einspeisungen für Flutbetrieb

Leckagen des TH-Systems im Bereich des Ringraumes haben das Auslaufen eines Flutbehälterpaares zur Folge. Das Betriebspersonal kann dies anhand folgender Kriterien erkennen:

- Ausgabe der Warnmeldung "Pumpensumpf Ringraumquadrant hoch",
- Ausgabe der Notgefahrmeldung "Niveau Pumpensumpf > max" und
- Ausgabe von Warnmeldungen über sinkendes Flutbehälterniveau.

Da das Auslaufen der Flutbehälter vermutlich sehr rasch erfolgt, sind Eingriffe des Betriebspersonals bis zum Umschalten auf Sumpf-Umwälzbetrieb nicht zu erwarten. Die im Ringraum aufgestellten Pumpen sind durch das ausströmende Wasser jedoch nicht gefährdet, da der Wasserinhalt eines Flutbehälterpaares (Netto-Inhalt 316 m^3) nicht ausreicht, um die 40 cm hohen Sockel, auf denen die Aggregate montiert sind, zu überfluten.

Die Wahrscheinlichkeit für ein Leck in den Rohrleitungen des Not- und Nachkühlsystems im Ringraum ist sehr gering, da die

Leitungen nur sehr wenig belastet werden. Sofern das Betriebspersonal nach dem Umschalten auf Sumpf-Umwälzbetrieb entsprechend der Logikfahne des Betriebshandbuches "Bruch im TH-System" rasch eingreift, sind Folgeschäden an anderen im Ringraum aufgestellten Komponenten auch dann nicht zu erwarten.

- Bruch von TH-Rohrleitungen im Ringraum während der ND-Einspeisungen für Sumpf-Umwälzbetrieb

Der Bruch einer Rohrleitung eines Stranges des Not- und Nachkühlsystems zwischen der Sumpfdurchführung und der hinter dem Nachwärmekühler liegenden Durchführung der Einspeiseleitung durch die Stahlhülle kann bei Sumpf-Umwälzbetrieb zum Ausfall des gesamten TH-Systems führen. In diesem Fall würde aufgrund des nach dem Störfall vorhandenen erhöhten Druckes innerhalb der Stahlhülle das gesamte Wasser des Reaktorgebäudesumpfes in den Ringraum gedrückt werden und somit zur Kühlung des Reaktorkerns nicht mehr zur Verfügung stehen.

Für das Betriebspersonal ist ein derartiges Leck anhand folgender Kriterien erkennbar:

- Ausgabe der Warnmeldung "Pumpensumpf Ringraumquadrant hoch",
- Sinken des Sumpfniveaus TH00 L001,
- Schließen der Rückschlagklappen TH11(21/31/41) S001 und TH12 (22/32/42) S001 (Rückmeldung),
- Anzeige anomaler Betriebswerte bezüglich Druck und Durchfluß in einem Nachkühlstrang.

Von der zuerst genannten Warnmeldung wird die Notgefahrmeldung "Niveau Pumpensumpf > max" abgeleitet.

Das Betriebspersonal hat entsprechend der Logikfahne des Betriebshandbuches "Bruch im TH-System" den Betätigungsbaustein der Sumpfarmatur im defekten Notkühlstrang zu ziehen und die Sumpfarmatur mittels eines Prüfadapters zuzufahren. Anschließend muß die Nachkühlpumpe ebenfalls durch Ziehen des Betätigungsbausteins außer Betrieb genommen werden.

Die Wahrscheinlichkeit für das Auftreten eines derartigen Leckstörfalls während des Sumpf-Umwälzbetriebes wurde als vernachlässigbar gering abgeschätzt.

Falls für das Entstehen eines Rohrleitungsrisses das halbe Zeitintervall zwischen zwei Funktionsprüfungen angesetzt wird, obwohl die Rohrleitung zwischen den Funktionsprüfungen nicht durch Innendruck belastet wird, so erhält man eine pessimistische Abschätzung für die Wahrscheinlichkeit eines Risses, der bei der Inbetriebnahme des Systems zum Bruch der Leitung führt. Unter Verwendung einer mittleren Rohrleitungsausfallrate von $\lambda = 8{,}7 \cdot 10^{-9}/h$ (Fachband 3) ergibt sich eine Wahrscheinlichkeit von

$$\bar{p} = 4 \cdot 8{,}7 \cdot 10^{-9} \cdot 336 \cong 10^{-5}$$

für einen Rohrleitungsbruch in einem der vier Not- und Nachkühlstränge.

Es ist außerdem noch zu berücksichtigen, daß dem Sumpfbetrieb in den meisten Fällen ein Flutbetrieb vorausgeht. Ein Leck in diesem Leitungsabschnitt des Not- und Nachkühlsystems würde somit schon vor dem Umschalten auf Sumpfumwälzbetrieb entdeckt. Die Ansaugleitung aus dem Reaktorgebäudesumpf ist bis zur Sumpfarmatur im übrigen als doppelwandige Rohrleitung ausgeführt und wird auf Dichtheit überprüft. Die übrigen Rohrleitungen sind für 40 bar ausgelegt, während sie nach einem Störfall nur bei wenigen bar betrieben werden.

- Ausfall des Not- und Nachkühlsystems im Langzeitbetrieb aufgrund eines Rohrleitungsbruches im Brennelement-Beckenkühlsystem

Bei Rohrleitungsbrüchen im Bereich des Beckenkühlsystems TG wird nach Unterschreiten eines Wasserstand-Grenzwertes im Brennelementbecken (Inhalt ca. 1 380 m^3) auf dem örtlichen Leitstand die Warnmeldung "BE-Becken TIEF" ausgegeben. Von dieser Meldung wird die Notgefahrmeldung "Brennelementbecken gestört" abgeleitet.

Beim Anstehen dieser Meldung schreibt das Betriebshandbuch allerdings keine Überprüfung auf eine Leckage, sondern Inbetriebnahme der Nachspeisung aus dem Deionatsystem vor. Erst durch das ständige Laufen bestimmter Sumpfpumpen und der Ausgabe entsprechender Sumpfniveau-Meldungen wird das Betriebspersonal veranlaßt, nach möglichen Lecks zu suchen:

So wird bei Brüchen innerhalb der Stahlhülle ständig die Sumpfpumpe 20 TZ14 D001 laufen, bei Leckagen im Ringraum im Bereich des Stranges TG02 die Sumpfpumpe 20 TZ23 D001, im Bereich des Stranges TG01 die Sumpfpumpe 20 TZ24 D001 oder 20 TZ25 D001.

In allen Rohrleitungen des TG-Systems befindet sich unmittelbar nach der Stahlhüllendurchführung je eine Motorarmatur, die im Falle einer Leckage von der Warte aus geschlossen werden kann. Unterbleibt dies, so kann je nach Lage der Bruchstelle ein großer Teil des Brennelementbecken-Inhalts in den Ringraum ausfließen und somit den Ausfall des Not- und Nachkühlsystems und der nuklearen Zwischenkühlkreise verursachen. Unter Berücksichtigung der Tatsache, daß das Beckenkühlsystem ständig in Betrieb ist, ist die Wahrscheinlichkeit, daß es während der LANGZEIT-NOTNACHKÜHLUNG zu einem unentdeckten Rohrleitungsbruch mit Überflutung des Ringraumes kommt, sehr gering.

6.1.2.2.19 Fehlerbaum 19: Not- und Nachkühlsystem, Druckspeicher-Einspeisungen

Der Ausfall einer Druckspeicher-Einspeisung ist durch

- den Ausfall des zugehörigen Druckspeichers,
- den Ausfall der zu dem Druckspeicher führenden Rohrleitungen bzw.
- den Ausfall in diesen Rohrleitungen installierten Armaturen

möglich. Darüber hinaus ist ein Ausfall der Druckspeicher-Einspeisung als Störfallfolge zu berücksichtigen (Abschnitt 6.1.2.2.1).

Der Ausfall eines Druckspeichers kann, außer durch festigkeitsmäßiges Versagen des Behälters, durch einen außerhalb des Tole-

ranzbereiches liegenden Druck des Stickstoffpolsters oder durch einen außerhalb der Toleranzen liegenden Wasserstand erfolgen.

Das Fehlen des erforderlichen Drucks in einem Druckspeicher wird durch eine Druckmessung, z.B. 20 TH16 P002, gemeldet. Der gemessene Druck wird nicht nur auf der Warte angezeigt; durch Grenzsignalmelder wird außerdem auf der Warte eine Störungsmeldung bei zu hohem oder zu niedrigem Druck ausgegeben (Abschnitt 4.2.1). Für jeden Druckspeicher gibt es durch eine weitere Meßstelle eine davon unabhängige Messung des Gasdruckes zur Bildung von Reaktorschutzsignalen. Die entsprechenden Meßwerte werden auf der Reaktorschutztafel der Warte angezeigt. Liegt einer der hier gemessenen Drücke außerhalb der Toleranz, werden von der oben erwähnten Störungsmeldung unabhängige Meldungen auf die Reaktorschutztafel übertragen. Aufgrund dieser redundanten Meldungen und Anzeigen sowie der zusätzlich noch vorhandenen örtlichen Druckanzeige an jedem Druckspeicher kann das Fehlen des erforderlichen Stickstoffdruckes gegenüber dem im folgenden diskutierten zu niedrigen Wasserstand vernachlässigt werden.

Ein zu hoher Wasserstand in einem Druckspeicher kann durch Nachspeisen von Borwasser hervorgerufen werden; ein solches Nachspeisen folgt auf die Meldung eines zu niedrigen Wasserstandes auf der Warte. Auch eine langsam driftende Wasserstandsmessung kann einen zu hohen oder zu niedrigen Wasserstand zur Folge haben; dies wird nur durch die Kontrolle der Anzeige vor Ort entdeckt. Es wird davon ausgegangen, daß die Ausfallrate für Driften der Bartonzelle klein gegenüber derjenigen für "Hängenbleiben" der Bartonzelle ist. Da die Konsequenzen die gleichen sind, wird nur die Anzeige eines unveränderlichen Wasserstandes weiter diskutiert.

Ein zu niedriger Wasserstand in einem Druckspeicher kann durch geringfügige Leckagen des Druckspeichers, seiner Hilfssysteme oder der Anschlußleitungen seiner Instrumentierung, aber auch durch die regelmäßigen Funktionsprüfungen der Rückschlagwirkung der absperrbaren Rückschlagarmaturen an den Druckspeichern hervorgerufen werden.

Eine sehr wahrscheinliche Ursache für einen zu hohen oder zu niedrigen Wasserstand ist die Leckage der letzten Rückschlagarmaturen in den Einspeiseleitungen bzw. in den ND- und HD-Einspeisesträngen des Not- und Nachkühlsystems. Ein dadurch hervorgerufener zu niedriger Wasserstand wird nur dann nicht sofort entdeckt, wenn das Meßwerk der Bartonzelle hängenbleibt. Ein gleichzeitiger Ausfall der Grenzsignalgeber für minimalen Wasserstand und der Analoganzeige auf der Warte wird demgegenüber vernachlässigt. Außerdem muß noch die Druckmessung des Reaktorschutzsystems ausgefallen sein, oder beim Nachspeisen von Stickstoff in den Druckspeicher muß die örtliche Wasserstandsmessung nicht abgelesen worden bzw. der betreffende Meßkanal nicht funktionsfähig sein. Nicht berücksichtigt wird die Möglichkeit, daß die Borkonzentration im Druckspeicher unbemerkt zu niedrig ist, da, wie bereits für die Flutbehälter diskutiert (Abschnitt 6.1.2.2.18), einerseits das Personal bei Störungen in diesem System auf mögliche Konzentrationsabnahmen hingewiesen und andererseits im Rahmen der regelmäßigen Funktionsprüfungen auch der Borgehalt kontrolliert wird.

Ein Ausfall der Armaturen in den zu dem Druckspeicher führenden Rohrleitungen ist außer durch Bruch auch infolge Nichtöffnens bei Anforderung möglich.

Im Fehlerbaum 19 ist der Bruch oder das Leck des Druckspeichers zusammen mit dem der anschließenden Rohrleitungen eingetragen. Da diese Systemteile unter Druck stehen, werden während des Kraftwerksbetriebs solche Ausfälle sofort erkannt und repariert. Eine sofortige Reparatur ist schon deswegen erforderlich, weil das Kernkraftwerk laut Genehmigungsverfahren mit verminderter Leistung gefahren werden muß, wenn ein Druckspeicher länger als ca. 10 Stunden nicht einsatzbereit ist. Bei der Auswertung der Fehlerbäume spielen diese Ausfälle während des Leistungsbetriebs des Kraftwerks keine Rolle. Jedoch ist der Ausfall der Einspeiseleitungen als Störfallfolge zu berücksichtigen (Abschnitt 6.1.2.2.1).

Im Unterschied zu der im folgenden diskutierten Vernachlässigung von Armaturen mit Kontrollansteuerung ist ein Nichtöffnen zu be-

rücksichtigen, wenn diese als Rückschlagarmaturen ausgebildet sind. Rückschlagarmaturen mit Motorantrieb werden wie Rückschlagarmaturen ohne Antrieb in Rechnung gesetzt. Da die Druckspeicher selbsttätig einspeisen, spielt ein Ausfall von elektrischer Energie oder der Steuerung zum Zeitpunkt des Störfalls keine Rolle.

Erfolgt bei Störfällen eine Hochdruck-Einspeisung, kann es zu einem Druckanstieg in einem der Druckspeicher kommen, wenn die entsprechende Druckspeicher-Rückschlagarmatur nicht dicht schließt. Es muß dann mit einem Überdruckversagen des Druckspeichers gerechnet werden, wenn der Druck erheblich über 40 bar ansteigt. Bei diesem Druck, der dem 1,3fachen Auslegungsdruck entspricht, werden die Wiederholungsdruckprüfungen der Druckspeicher durchgeführt. Ein Druckanstieg über den Auslegungsdruck der Druckspeicher (31 bar) ist jedoch nur bei zusätzlichem Versagen einer weiteren Armatur möglich, wobei zwei Fälle zu unterscheiden sind:

- Ausfall des Öffnens des Druckspeicher-Sicherheitsventils (Ansprechdruck = 31 bar), wenn die Leckrate der Druckspeicher-Rückschlagarmatur kleiner ist als der zum Umschalten des Dreiwegeventils im HD-Einspeisestrang notwendige Mindestdurchsatz;
- Ausfall der Umschaltfunktion des Dreiwegeventils im HD-Einspeisestrang, wenn die Leckrate der Druckspeicher-Rückschlagarmatur größer ist als der zum Umschalten notwendige Mindestdurchsatz.

Eine Untersuchung ergibt, daß die Leckrate mindestens ca. 5 t/h betragen muß, damit es bei einem Kühlmittelverluststörfall zum Ansteigen des Druckes über 40 bar kommen kann. Dabei wird vom ungünstigsten Fall, dem Kühlmittelverluststörfall "kleines Leck", ausgegangen, weil dort der hohe Druck am längsten ansteht. Auf mögliche Leckagen an den Druckspeicher-Rückschlagarmaturen wird das Wartenpersonal durch die Anzeige des Druckspeicher-Wasserstands auf der Warte und durch die Ausgabe von Prozeßrechnermeldungen bei Über- oder Unterschreitung von Wasserstands- oder Druckgrenzwerten hingewiesen. So wird regelmäßig beim Schicht-

wechsel der Druckspeicher-Wasserstand abgelesen und protokolliert. Voraussetzung zur rechtzeitigen Erkennung von Leckagen ist jedoch, daß es aufgrund der Druckverhältnisse in den Leitungsstücken des Not- und Nachkühlsystems zwischen Erst- und Zweitabsperrung der Hauptkühlkreisläufe zu einer merkbaren Einspeisung in die Druckspeicher oder umgekehrt zu einem merkbaren Ausströmen aus den Druckspeichern kommt.

Eine Einspeisung während des normalen Leistungsbetriebes ist möglich, wenn zusätzlich zur Undichtheit der Druckspeicher-Rückschlagarmatur eine Leckage der entsprechenden Erstabsperrung vorliegt. Die dafür verwendeten Armaturen schließen - wie die Betriebserfahrung zeigt - nie "völlig dicht", allerdings liegen zur Größe der Leckrate keine Untersuchungen vor.

Zur Einspeisung kann es auch während der monatlichen Prüfung der HD-Einspeisesignale kommen. Nach einer Abschätzung wird im ungünstigsten Fall (der Druckspeicher-Druck liegt zu Beginn der Prüfung am unteren Grenzwert) der obere Grenzwert bei einer Leckrate von ca. 30 t/h nach ca. 3 Minuten, bei einer Leckrate von 5 t/h nach ca. 18 Minuten ansprechen. Mit der Größe der Leckrate erhöht sich auch die Umschaltzeit des Dreiwegeventils. Dies würde man bei jeder Prüfung feststellen, weil die Umschaltzeit gemessen wird.

Mit einer Ausströmung aus den Druckspeichern und folglich mit einer Absenkung des Druckspeicher-Wasserstandes und -druckes bei undichten Druckspeicher-Rückschlagarmaturen ist bei der Prüfung der ND-Einspeisesignale zu rechnen.

Um die Möglichkeiten einer Fehlererkennung von relevanten Undichtheiten der Druckspeicher-Rückschlagarmaturen beurteilen zu können, sind noch weitere Untersuchungen erforderlich, insbesondere werden aus der Betriebserfahrung Aussagen zu den Leckraten der Rückschlagarmaturen benötigt.

Gefährliche Druckstöße in den Einspeiseleitungen des Not- und Nachkühlsystems oder im Reaktorkühlkreislauf, die durch Ausströmen von Stickstoff aus den Druckspeichern nach einer Druckspei-

cher-Einspeisung denkbar sind, werden nicht erwartet. Die Druckspeicher sind so ausgelegt, daß nach Ende der Druckspeicher-Einspeisung noch eine Wasservorlage vorhanden ist und somit bis zu diesem Zeitpunkt keine größeren Mengen Stickstoff ausströmen. Erst beim Sumpf-Umwälzbetrieb, wenn der Druck im Sicherheitsbehälter so weit abgesunken ist, daß der Förderdruck der Nachkühlpumpen die Druckspeicher-Rückschlagarmaturen nicht mehr geschlossen halten kann, ist mit dem Ausströmen von Stickstoff zu rechnen. Eine Abschätzung zeigt, daß die dabei auftretenden Druckstöße bzw. Kräfte im Vergleich zu denen, die bei den Druckspeicher-Einspeiseversuchen während der Inbetriebsetzung auftreten, vernachlässigbar sind.

Das Ausströmen von Stickstoff aus den Druckspeichern könnte jedoch zu einer Beeinträchtigung des Naturumlaufs in den Hauptkühlkreisläufen führen, wenn sich das Gas in den U-Rohren der Dampferzeuger sammelt. Als Folge wäre eine Verschlechterung der für die kleinen Lecks notwendigen Wärmeabfuhr über die Dampferzeuger möglich. Eine Untersuchung zeigt, daß die aus dem Hauptkühlmittel und aus den Borwasservorräten des Not- und Nachkühlsystems desorbierten Gase sich unter der Kalotte des Reaktordruckbehälters sammeln und einen Teil dieses Volumens einnehmen. Das zusätzliche Einströmen von Stickstoff aus den Druckspeichern ist deshalb zu verhindern. Daher werden laut Betriebshandbuch bei Lecks mit Auslösung des HD-Einspeisesignals, nach Überbrükkung der Notkühlvorbereitungssignale die Stellantriebe der Druckspeicher-Rückschlagarmaturen bei einem Druck im Reaktorkühlkreislauf von < 35 bar von Hand zugefahren. Beim Versagen der Absperrung kommt es nach der erwähnten Untersuchung jedoch erst bei einem Druck im Reaktorkühlkreislauf < 7 bar zur Ausströmung des Stickstoffs. Bei diesen Drücken soll die Wärmeabfuhr bereits über das Not- und Nachkühlsystem gehen. Zu dem Problemkreis sind außerdem experimentelle Untersuchungen geplant.

6.1.2.3 Teilfehlerbäume für die elektrische Energieversorgung

6.1.2.3.1 Allgemeines

Für die Beherrschung von Kühlmittelverluststörfällen werden keine Verbraucher benötigt, die an die Blockschienen angeschlossen sind. Es ist deshalb bei den Fehlerbäumen für die elektrische Energieversorgung nur der Ausfall von Notstromschienen zu betrachten.

6.1.2.3.2 Fehlerbaum 13: Notstromschienen

Die Notstromschienen werden normalerweise von der Eigenbedarfsanlage aus versorgt. Deshalb ist ein Ausfall von Notstromschienen nur dann relevant, wenn zusätzlich zum Kühlmittelverluststörfall ein Notstromfall eintritt (in den Fehlerbäumen durch das Funktionselement NSF berücksichtigt).

Zum Zeitpunkt des Kühlmittelverluststörfalls oder im Verlauf der darauffolgenden Minuten kann als Folge des Kraftwerksausfalls die Einspeisung der Eigenbedarfsleistung aus dem Verbundnetz versagen, weil die Leistung (Wirk- und Blindleistung) des ausgefallenen Kraftwerks im Verbundnetz fehlt. Die Wahrscheinlichkeit hierfür wird mit einem Medianwert von $3 \cdot 10^{-3}$ und einem Unsicherheitsfaktor 3 abgeschätzt (Abschnitt 7.1, Turbinenschnellabschaltung). Außerdem führt ein Nichtöffnen des Generatorschalters zum Notstromfall. Für die Wahrscheinlichkeit eines Notstromfalls bei Eintritt des Kühlmittelverluststörfalls oder kurze Zeit darauf ergibt sich ein Medianwert von insgesamt $4 \cdot 10^{-3}$ mit einem Unsicherheitsfaktor 3 für das 90-%-Vertrauensintervall.

Die Wahrscheinlichkeit dafür, daß während der Notkühlung ein statistischer Netzausfall auftritt, d.h. ein zufälliger Ausfall des Verbundnetzes, der ursächlich nichts mit dem Ausfall des untersuchten Kraftwerks zu tun hat, ist sehr gering und wird deshalb nicht betrachtet.

Bei Anforderung infolge des Notstromfalls fällt eine der 10-kV-Notstromschienen 21 BU, 22 BV, 23 BW, 24 BX aus, wenn die Notstromeinspeisung durch den zugehörigen Diesel ausfällt. Zum Betrieb eines Dieselaggregats sind Hilfssysteme notwendig, die von der redundanzmäßig zugeordneten nicht kuppelbaren 380-V-Notstromschiene versorgt werden. Aus diesem Grunde führt im Notstromfall ein Ausfall z.B. der Schiene 21 FU zu einem Folgeausfall der Schiene 21 BU. Umgekehrt führt ein Ausfall z.B. der Schiene 21 BU zu einem Ausfall der Schiene 21 FU, da die Schiene 21 FU von 21 BU aus versorgt wird. Daraus folgt, daß die einander zugeordneten 10-kV-Notstromschienen und nicht kuppelbaren 380-V-Notstromschienen stets gemeinsam ausfallen. Die Schiene 21 FU fällt bei Anforderung im Notstromfall aus, wenn

- die Notstromeinspeisung durch den Notstromdiesel 21 EY10 D001 ausfällt,
- der Einspeiseschalter 21 FU04 G der Schiene 21 FU nicht schließt,
- die Steuerkette für den Einspeiseschalter den EIN-Befehl unterdrückt oder
- das Signal "Notstrom nicht" 21 YZ82 U001XU61 nicht ausgegeben wird.

Entsprechendes gilt für die Redundanzen 2 bis 4.

Das Versagen der beiden Schalter zwischen einer 10-kV-Notstromschiene und der zugehörigen Blockschiene im Notstromfall kann gegenüber den Einzelausfällen von Schaltern vernachlässigt werden. Der Ausfall des entsprechenden Signals führt zu einem Startversagen der Notstromdiesel, so daß es im Fehlerbaum der Notstromschienen nicht mehr berücksichtigt werden muß.

Für durchlaufende Antriebe (Pumpen) ist im Notstromfall außer dem Ausfall der Sammelschienen bei Anforderung auch das Betriebsversagen der Notstromeinspeisungen zu berücksichtigen, wobei die gesamte Laufzeit der Notstromdiesel in Rechnung zu setzen ist. Bei Stellantrieben, die nicht unmittelbar nach Störfalleintritt betätigt werden, wird pessimistisch ebenfalls die gesamte Diesellaufzeit berücksichtigt.

Eine kuppelbare 380-V-Notstromschiene, z.B. 21 EU, fällt aus, wenn ihre Notstromeinspeisung ausfällt und keine Versorgung von der zweiten Schiene des kuppelbaren Paares möglich ist. Für die Notstromeinspeisung einer kuppelbaren Notstromschiene gilt Entsprechendes wie für die nicht kuppelbaren Schienen. Eine Versorgung von der zweiten Schiene des Paares ist nicht möglich, wenn deren Notstromeinspeisung ausgefallen ist oder wenn der Kuppelschalter nicht schließt. Ein Ausfall der Kupplung erfolgt bei

- Ausfall des Kuppelschalters,
- fälschlich anstehender Schalterfallmeldung eines Einspeiseschalters,
- Ausfall des angeforderten Teils der Zuschaltautomatik,
- Ausfall der 24-V-Versorgung im Verriegelungsschrank.

Ebenso wie bei den nicht kuppelbaren Notstromschienen ist auch hier zwischen einem Ausfall bei Anforderung und einem Ausfall während der Betriebszeit der Notstromdiesel zu unterscheiden.

Ein Ausfall eines kuppelbaren Schienenpaares ist durch einen Schließbefehl für einen Einspeiseschalter während des Schließens des Kuppelschalters möglich. Der Grund hierfür ist, daß Leistungsschalter einen Schaltbefehl auch dann zu Ende führen, wenn während des Schaltvorgangs der Befehl durch eine Verriegelung unwirksam wird. Eine Verriegelung zwischen Einspeise- und Kuppelschalter ist daher wirkungslos, wenn beide Schalter gleichzeitig oder annähernd gleichzeitig EIN-Befehle erhalten. Dadurch kann es grundsätzlich zu Fehlschaltungen zwischen zwei kuppelbaren 380-V-Notstromschienen kommen. Die Wahrscheinlichkeit dafür, daß dies nach Eintritt eines Störfalls vorkommt, kann jedoch vernachlässigt werden.

Um definierte Voraussetzungen zu haben, wurde für den Fehlerbaum der Schiene 20 ES davon ausgegangen, daß vor Störfalleintritt die Einspeisung von der Schiene 24 EX aus geschieht (Schalter 20 ES04 H001). Wenn unter dieser Voraussetzung im Notstromfall der Schalter 20 ES04 H001 nicht schließt, ist die Schiene 20 ES ausgefallen, da grundsätzlich mögliche, aber ungeplante Handmaßnahmen nicht berücksichtigt werden. Ein Ausfall der Schiene

20 ES tritt ebenfalls ein, wenn die Schienen 24 EX und 22 EV ausfallen. Der Ausfall einer der beiden Schienen 24 EX oder 22 EV gemeinsam mit dem Ausfall der Umschaltautomatik der Schiene 20 ES wird im Fehlerbaum vernachlässigt.

Die Notstandsschiene 21 FR10 fällt aus, wenn die Schienen 21 BU und 21 FU ausfallen und die Automatik nicht auf die unterbrechungslose Schiene 10 ES des Blocks A umschaltet. Entsprechendes gilt für die Notstandsschienen 22 FR20, 23 FR30, 24 FR40.

Verschleppte Kurzschlüsse werden sofort entdeckt, wenn sie von Komponenten verursacht werden, die während des Normalbetriebs des Kraftwerks eingeschaltet sind. Diese Art von verschleppten Kurzschlüssen kann genauso vernachlässigt werden wie die anderen sofort entdeckten und innerhalb kurzer Zeit reparierten Komponentenausfälle. Ein verschleppter Kurzschluß kann jedoch auch dadurch entstehen, daß beim Störfall eine Bereitschaftskomponente eingeschaltet wird, bei der ein nichtentdeckter Kurzschluß vorliegt. Wenn man berücksichtigt, daß ein solcher Kurzschluß einer Komponente bei den regelmäßigen Funktionsprüfungen entdeckt wird und außerdem noch ein übergeordneter Schalter versagen muß, kann auch diese Art von verschleppten Kurzschlüssen vernachlässigt werden.

Im Notstromfall muß während der Hochlaufzeit der Notstromdiesel die Versorgung der 220-V- und 24-V-Gleichstromanlagen durch die Batterien übernommen werden. Da die Verbraucher jeweils diodenentkoppelt aus zwei Gleichstromschienen gespeist werden, genügt es, wenn bei jeder der beiden Gleichstromanlagen zwei der vier vorhandenen 50-%-Batterien funktionieren. Unter der Voraussetzung, daß der größte Teil der Ausfälle von Batterien sofort oder bei den monatlichen und jährlichen Prüfungen entdeckt wird, kann der Ausfall der Gleichstromversorgung von Verbrauchern aufgrund unabhängiger Ausfälle von Batterien vernachlässigt werden. Allerdings ist hier anzumerken, daß keine Funktionsprüfungen durchgeführt werden, bei denen die Batterien den gleichen Belastungen unterworfen sind wie bei einem Kühlmittelverluststörfall mit Notstromfall. Wegen des redundanten Aufbaus können Ausfälle der Einspeisungen der Gleichstromverbraucher vernachlässigt werden.

Die rotierenden Umformer der gesicherten Drehstromschienen sind ständig in Betrieb. Wegen des vorhandenen Reserveumformers braucht beim Ausfall eines Umformers eine gesicherte Drehstromschiene nur kurzzeitig über die Verbindung zu der entsprechenden Notstromschiene versorgt werden. Ein Ausfall von gesicherten Drehstromschienen aufgrund unabhängiger Ausfälle von Funktionselementen kann daher im Fehlerbaum vernachlässigt werden.

Im folgenden wird auf denkbare CMA eingegangen, die quantitativ jedoch nicht bewertet werden, da Hinweise auf entsprechende CMA aus der Betriebserfahrung nicht vorliegen.

- Unterspannung an den Sammelschienen

Ein Kühlmittelverluststörfall führt zu einer Turbinenschnellabschaltung. Als Folge der Turbinenschnellabschaltung bzw. der Abtrennung des Generators vom Netz muß mit einer Spannungsabsenkung an den Block- und Notstromschienen gerechnet werden. Es ist denkbar, daß die Spannung an den 10-kV-Notstromschienen für einige Zeit bis auf etwas mehr als 80 % der Nennspannung absinkt. In diesem Fall würden die Notstromdiesel nicht durch das Notstromsignal starten.

Für die Dimensionierung der Pumpenmotoren wurde unter anderem gefordert, daß sie bei folgenden Klemmenspannungen noch sicher anlaufen:

- 10-kV-Motoren: 85 % der Nennspannung
- Niederspannungsmotoren: 80 % der Nennspannung

Für die Klemmenspannung eines Motors ist außer der Sammelschienenspannung auch der Spannungsabfall über das Anschlußkabel zu berücksichtigen. Die Kabel für 10-kV-Motoren sind entsprechend der Kurzschlußbelastung ausgelegt, wohingegen bei den Niederspannungsverbrauchern bei Motornennstrom ein Spannungsabfall über das Kabel von 5 % der Nennspannung zugelassen wird.

Da der Anlaufstrom der für Pumpen verwendeten Drehstrommotoren mit Kurzschlußläufer normalerweise ein Mehrfaches des Nennstroms ist, könnten bei einer Sammelschienenspannung von etwas über 80 %

der Nennspannung bei Niederspannungsmotoren Anlaufschwierigkeiten auftreten.

Bei Stellantrieben liegt eine ähnliche Problematik wie bei Pumpenmotoren vor, wobei sich jedoch wegen der begrenzten Zahl von Stellantriebstypen zum Großteil eine erhebliche Überdimensionierung in bezug auf das bei Nennspannung tatsächlich erreichbare Motormoment ergibt.

- CMA von Verbraucherabzweigen

In den Schaltanlagen wird eine begrenzte Anzahl von Abzweigtypen eingesetzt, so daß redundante Verbraucher normalerweise über den gleichen Abzweigtyp versorgt werden. Bei Abzweigen für Stellantriebe werden standardmäßig, soweit es sich nicht um Sonderkonstruktionen handelt, zwei Typen eingesetzt, und zwar für Stellantriebe bis zu einer Motornennleistung von 7,5 kW bzw. 15 kW. Das kann bei Stellantrieben zur Folge haben, daß diversitäre Armaturen über den gleichen Abzweigtyp versorgt werden (z.B. die Flutbehälter-Absperrarmaturen TH10 S001 und TH10 S002). Es ist jedoch anzumerken, daß bei unterschiedlicher Leistungsaufnahme unterschiedliche Belastungen der Abzweige stattfinden.

Bei Verbrauchern, die während des bestimmungsgemäßen Betriebs nicht unter Störfallbedingungen belastet werden (Leistungsaufnahme, Betriebszeit bei Pumpen), besteht prinzipiell die Möglichkeit eines CMA aufgrund zu niedrig eingestellter thermischer Überstromauslöser.

Nach VDE 0660 gelten für thermische Überstromauslöser normalerweise folgende Werte:

Ansprechstrom als Vielfaches des Einstellstroms	Verzögerungszeit
1,05	> 2 Stunden
1,20	< 2 Stunden
1,50	< 2 Minuten
6,00	> 2 Sekunden

Daraus folgt, daß eine geringfügig zu niedrige Einstellung des Auslösewertes erst mit einer erheblichen Zeitverzögerung zur Abschaltung führt und daher bei den Funktionsprüfungen nicht ohne weiteres entdeckt wird.

Bei Abzweigen für Pumpenmotoren (Motorabzweige) wird die Einstellung der thermischen Überstromauslöser grundsätzlich auf 1fachen Nennstrom vorgenommen. Die Überstromauslöser für Stellantriebe werden auf 1,5fachen Motornennstrom eingestellt.

Bei 0,4-kV-Verbraucherabzweigen für eine Leistung bis 150 kW wird der Kurzschlußschutz von Schmelzsicherungen übernommen. Innerhalb gewisser Grenzen (Sicherungsunterteile) besteht die Möglichkeit, daß zu kleine Schmelzsicherungen eingesetzt werden. Um dies zu verhindern, sind auf sämtlichen Abzweigen Aufkleber mit den Nennwerten der zu verwendenden Sicherungen angebracht.

6.1.2.3.3 Fehlerbaum 14: Notstromdiesel

Die Komponenten der Dieseleinspeisungen sind bezüglich der beim Notstromfall geforderten Funktionen während des Normalbetriebs des Kraftwerks in Bereitschaft. Von diesen Komponenten brauchen jedoch diejenigen nicht berücksichtigt zu werden, die einer ständigen Überwachung unterliegen. Ihr Ausfall wird, wie bei den Betriebskomponenten, sofort entdeckt.

Bei den Notstromeinspeisungen ist zu unterscheiden zwischen dem Ausfall bei Anforderung und dem Betriebsversagen. Die für das Betriebsversagen maßgebliche Laufzeit wird logarithmisch normalverteilt angesetzt mit einem Medianwert von 2 Stunden und einem Unsicherheitsfaktor von 3. Dabei wird vorausgesetzt, daß bei einem länger andauernden Notstromfall die Verbindungen zu den 10-kV-Normalnetzschienen des Blocks A hergestellt werden, woraufhin die Diesel abgeschaltet werden können.

Zum Ausfall einer Notstromeinspeisung bei Anforderung kommt es, wenn

- der Notstromdiesel nicht startet,
- das Notstromsignal für den Startbefehl nicht kommt,
- der Einspeiseschalter 21 BU02 nicht schließt oder
- die Dieselkühlung durch das Nebenkühlwassersystem ausfällt.

Für das Betriebsversagen einer Notstromeinspeisung ist außer dem Betriebsversagen des Notstromdiesels auch der Ausfall der Raumluftkühlung (Kaltwassersystem, Umluftkühlung) zu berücksichtigen.

Beim Start- oder Betriebsversagen eines Notstromdiesels war die Wiederversorgung der zugehörigen 10-kV-Notstromschiene über die Eigenbedarfsanlage (Netzrückschaltung) ursprünglich nur durch Eingriffe in das Reaktorschutzsystem möglich. Eine Netzrückschaltung bei ausgefallenen Notstromdieseln wird deshalb in den Fehlerbäumen nicht berücksichtigt. Infolge einer nachträglich durchgeführten Systemänderung ist jetzt eine Netzrückschaltung auch bei ausgefallenen Dieseln möglich. Die Netzrückschaltung ist allerdings noch nicht in die Logikfahnen des Betriebshandbuches aufgenommen, so daß sie als nicht geplante Handmaßnahme zu bewerten ist (vgl. Abschnitt 3.4.1). Unterlagen über regelmäßige Funktionsprüfungen der zur Netzrückschaltung benötigten Komponenten liegen ebenfalls noch nicht vor.

6.1.2.4 Teilfehlerbäume für das Reaktorschutzsystem

6.1.2.4.1 Fehlerbaum 15: Reaktorschutzsystem

Dieser Fehlerbaum beschreibt Ausfälle, die innerhalb des Reaktorschutzsystems oder in den Schränken der Antriebssteuerebene auftreten können. Er enthält nur Komponenten, die nicht eindeutig einem Teilsystem der Verfahrenstechnik oder der Energieversorgung zuzuordnen sind.

- Unterdrückung von Reaktorschutzsignalen

Die Teilfehlerbäume für die Unterdrückung der Reaktorschutzsignale nur einer Redundanzgruppe beziehen sich auf Ausfälle in

der Meßwerterfassung, im dynamisch arbeitenden Logikteil und im Relaisteil der logischen Verknüpfungen des Reaktorschutzsystems. In der Meßwerterfassung tragen nur CMA merklich zum Ergebnis bei (Abschnitt 3.3.6.4.4). Alle anderen denkbaren Ausfälle in diesem Teil des Reaktorschutzsystems, deren Eintrittswahrscheinlichkeiten nicht vernachlässigbar klein sind, werden über Vergleicher sofort erkannt, sind also selbstmeldend. Aufgrund der kurzen Instandsetzungszeiten können selbstmeldende Ausfälle vernachlässigt werden. Eine Ausnahme bildet die Meßwerterfassung zur Bildung der Sumpfsignale. Das Versagen von 2v3 Druckfühlern zur Messung des Wasserstandes in den Borwasser-Flutbehältern (fälschliche Ausgabe eines konstanten Meßwertes) wird erst bei der jährlichen Funktionsprüfung bemerkt, da sich die Wasserstände während des Betriebs der Anlage nur geringfügig ändern.

Die meisten im dynamisch arbeitenden Logikteil möglichen Ausfallarten sind im Fehlerbaum ebenfalls nicht enthalten, da diese Ausfälle selbstmeldend sind. Mögliche nicht selbstmeldende Ausfälle innerhalb der Schränke LT0, LT1-4 (z.B. Kurzschlüsse vom Eingang zum Ausgang der 2v3 Kettenglieder) spielen wegen der geringen Wahrscheinlichkeit ihres Auftretens quantitativ keine Rolle. Einen nicht zu vernachlässigenden Beitrag liefert dagegen die zur Bildung einiger Reaktorschutzsignale erforderliche Binärsignalübertragung von der Schrankgruppe LT0 zu den Schrankgruppen LT1-4. Zur Unterdrückung dieser Signale kommt es, wenn die betreffenden Binärsignaleingabestufen so ausfallen, daß sie ohne anstehendes Eingangssignal weiterhin Impulse ausgeben. Im Relaisteil des Reaktorschutzsystems werden vier Ausfälle, die zur Signalunterdrückung führen, unterstellt. Es sind dies:

- Versagen des Abschlußrelais,
- Ausfall der positiven Spannung im RT-Schrank durch Kurzschluß in den Steuerleitungen der Reaktorschutzsignale,
- CMA der Abschlußrelais der Redundanzen 1 und 2 bzw. 3 und 4

und bei verzögerten Signalen

- Verzögerungsstufe gibt kein Signal aus.

Ein Spannungsausfall in den Reaktorschutzschränken 21-24 IK21 oder 21-24 IK22 hat den Ausfall aller Signale, die in dem jeweils

betroffenen Schrank gebildet werden, zur Folge. Die entsprechende Ausfallkombination ist daher in allen Verknüpfungen enthalten, die zur Unterdrückung dieser Reaktorschutzsignale führen.

Zum Ausfall der Schrankspannung können Fehler in den von den Reaktorschutzsignalen angesteuerten Zeitstufen und Betätigungsbausteinen führen (Abschnitt 6.1.3.2.2). Ein Kurzschluß in diesen Bausteinen wird erst entdeckt, wenn die betroffenen Bausteine angesteuert werden, d.h. bei einer Funktionsprüfung oder im Störfall. Bei Eintritt eines Kühlmittelverluststörfalles oder eines Notstromfalles werden vom Reaktorschutzsystem zum Teil unterschiedliche Signale ausgegeben. Gemeinsam sind nur die Signale YZ11 (RESA) und YZ71 (TUSA). Im Übertrag "Ausfall des Reaktorschutzsignals im RT-Schrank 21-24 IK21" werden deshalb solche Anteile, die nur einem auslösenden Ereignis zuzuordnen sind, mit der Eintrittswahrscheinlichkeit dieses Ereignisses logisch UND-verknüpft. So ist im Kühlmittelverluststörfall das Funktionselement KMV = 1 und das Funktionselement NSF = 0 zu setzen.

- Reaktorschutzsignale kommen fälschlich

Das fälschliche Ansprechen des gepulsten Logikkanals zur Bildung des Sumpfsignals führt zur Ausgabe des Sumpfsignals, wenn gleichzeitig noch das Notkühlvorbereitungssignal ansteht. Dies ist aber nur bei Anforderung oder bei der Funktionsprüfung der Fall. Der Ausfall ist dann nicht selbstmeldend, wenn 2v3 Grenzwertmelder so ansprechen, daß ihr Ausfall nicht über den Meldeausgang gemeldet wird. Die Eintrittswahrscheinlichkeit dieses Mehrfachausfalles ist jedoch sehr gering und kann gegen die Einzelausfälle, die ebenfalls eine Fehlanregung bewirken, vernachlässigt werden. Es sind dies ein Fehlansprechen des Abschlußglieds oder des Ausgaberelais sowie Ausfälle, die zur Unterdrükkung des Takts im Logikteil führen.

- Ausfall der Betätigungsschränke

Zum Ausfall des gesamten Betätigungsschrankes kommt es, wenn die für beide Schrankhälften gemeinsame Masse unterbrochen ist. Der

Ausfall einer Schrankhälfte kann darüber hinaus durch die Unterbrechung des negativen Potentials verursacht werden. Es werden nur die nicht selbstmeldenden Ausfälle der Schränke in den Teilfehlerbäumen berücksichtigt.

6.1.2.4.2 "Common mode"-Ausfälle von Reaktorschutzsignalen

Da CMA in der Anregeebene mehrere Meßkanalgruppen und die der Auslöserelais mehrere Reaktorschutzsignale betreffen können, ist ihr Einfluß in den Zuverlässigkeitsanalysen nicht zu vernachlässigen. In diesem Abschnitt werden nur CMA der Meßkanalgruppen diskutiert, die einen Einfluß auf die Zuverlässigkeit der Notkühlung, der sekundärseitigen Wärmeabfuhr oder der Integrität des Sicherheitsbehälters haben können. CMA, die zu einem Versagen der Auslösung der Reaktorschnellabschaltung führen können, werden im Abschnitt 8.1 gesondert behandelt. CMA des Relaisteils sind in den Fehlerbäumen berücksichtigt und werden hier nicht weiter erörtert (Abschnitt 3.3.6.4.4).

Die folgenden Reaktorschutzsignale sind für die untersuchten Systemfunktionen von Bedeutung:

- Notkühlvorbereitungssignale
  einschließlich der Anregung durch den Kühlmitteldruck,
- Notkühlvorbereitungssignale
  ohne Anregung durch den Kühlmitteldruck (Notstromfall),
- HD-Einspeisesignale (zu frühes Ansprechen der ND-Signale),
- ND-Einspeisesignale,
- Flutsignale,
- Sumpfsignale,
- Reaktorkühlkreislaufabschlußsignale,
- Notspeisezuschaltsignale,
- Notspeisesignale,
- Deionatzuschaltsignale,
- Deionatsignale,
- Speisewassersignale,
- Notstromvorbereitungssignale und
- Notstromsignale.

- CMA der Notkühlvorbereitungssignale

Die Notkühlvorbereitungssignale werden aus einer dreifachen ODER-Verknüpfung der folgenden jeweils paarweise UND-verknüpften Anregekriterien gebildet:

- Kühlmitteldruck < 110 bar,
- Druckhalter-Wasserstand < 2,85 m und
- Differenzdruck der Anlagen- oder Betriebsräume gegen Atmosphäre > 30 mbar.

Den wesentlichen Beitrag zur Nichtverfügbarkeit dieser Signale liefert der CMA der Meßkanalgruppe des Kühlmitteldruckes und der Meßkanalgruppe für den Druckhalter-Wasserstand aufgrund menschlicher Fehlhandlungen. Für den gemeinsamen Ausfall beider Meßkanalgruppen wurde eine "mittlere Kopplung" (Abschnitt 3.3.5.2) angesetzt, damit ergibt sich ein Wert von

$$\bar{p}_{CMA} = 3{,}2 \cdot 10^{-5} \quad (p_{CMA\ 50} = 2{,}5 \cdot 10^{-5}/K = 3{,}5)$$

für den CMA der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE.

Für Fälle, bei denen es nicht zum Absinken des Kühlmitteldruckes kommt (z.B. Notstromfall), errechnet sich ein Wert von

$$\bar{p}_{CMA} = 1{,}7 \cdot 10^{-3} \quad (p_{CMA\ 50} = 1{,}4 \cdot 10^{-3}/K = 3)$$

Den Hauptbeitrag zu diesem Ergebnis (ca. 60 %) liefern hier CMA aufgrund menschlicher Fehlhandlungen bei der Meßkanalgruppe zur Erfassung des Druckhalter-Wasserstandes. Für die Meßkanalgruppen der Differenzdrücke zwischen Anlagen- bzw. Betriebsräumen gegen Atmosphäre wurde eine "starke Kopplung" angesetzt.

- CMA der HD-Einspeisesignale

Die Anregung der HD-Einspeisesignale (YZ36) erfolgt durch eine UND-Verknüpfung der Notkühlvorbereitungssignale mit dem Krite-

rium "Kein ND-Einspeisesignal". Zum Ausfall dieses Signals führt also entweder der CMA der Notkühlvorbereitungssignale oder das fälschliche Anstehen (zu frühe Anstehen) der ND-Einspeisesignale. Der Ausfall der Notkühlvorbereitungssignale führt für sich bereits zum Systemausfall und braucht daher nicht nochmals berücksichtigt zu werden. Im folgenden wird deshalb nur das zu frühe Ansprechen der ND-Einspeisesignale bewertet, das bei Kühlmittelverluststörfällen mit einer kleinen bis mittleren Leckgröße zu berücksichtigen ist.

Die ND-Einspeisesignale YZ38 werden aus der ODER-Verknüpfung von "Druckhalter-Wasserstand < 2,85 m" und "Anlagen- bzw. Betriebsraumdruck gegen Atmosphäre > 30 mbar" sowie aus der ODER-Verknüpfung "Reaktorkühlkreislaufdruck < 10 bar" und "Druckspeicherdruck < 10 bar" gebildet, die ihrerseits wieder UND-verknüpft sind. Die Meßkanalgruppen zur Erfassung des Druckspeicherdruckes und des Reaktorkühlkreislaufdruckes sind jeweils vierfach in 2v3-Verknüpfung aufgebaut.

Die Wahrscheinlichkeit eines CMA errechnet sich zu

$$\bar{p}_{CMA} = 4{,}1 \cdot 10^{-4} \quad (p_{CMA\ 50} = 3{,}8 \cdot 10^{-4}/K = 2)$$

Den maßgeblichen Einfluß (ca. 88 %) liefern auch hier CMA aufgrund menschlichen Fehlverhaltens, wobei für die Meßkanalgruppen des Druckspeicher- bzw. Reaktorkühlkreislaufdruckes eine "starke Kopplung" angesetzt wurde.

- CMA der ND-Einspeisesignale

Der Aufbau der Anregung dieser Signale wurde bereits beim CMA der HD-Einspeisesignale beschrieben. Die Wahrscheinlichkeit eines CMA dieser Signale liegt um zwei Größenordnungen niedriger als die für den Ausfall der Notkühlvorbereitungssignale. Dieser Ausfall konnte daher quantitativ in den Analysen vernachlässigt werden.

- CMA der Flutsignale

Die Flutsignale YZ45-YZ48 werden aus einer UND-Verknüpfung der Notkühlvorbereitungssignale mit der negierten Anregung über die Kriterien "Flutbehälter-Wasserstand < 1,15 m" gebildet. Der Ausfall der Notkühlvorbereitungssignale führt bereits allein zum Systemausfall und braucht daher hier nicht berücksichtigt zu werden. CMA in der Hardware der Meßkanalgruppen zur Erfassung der Flutbehälter-Wasserstände oder Ausfälle aufgrund menschlicher Fehlhandlungen in diesen Meßkanalgruppen können vernachlässigt werden, da unbemerkte Ausfälle, die einen zu niedrigen Wasserstand (< 1,15 m) vortäuschen, in mehreren Meßkanalgruppen wegen des Vorhandenseins von separaten Anzeigen in der Warte nicht zu erwarten sind. Dabei ist zu berücksichtigen, daß mindestens 3 Flutbehälter-Wasserstandsmeßkanalgruppen ausfallen müßten, da zur Störfallbeherrschung 2 intakte Not- und Nachkühlstränge ausreichen.

Aus den genannten Gründen erscheint der CMA der Flutsignale aufgrund von CMA der Meßkanalgruppen vernachlässigbar. Mögliche Ausfälle der Signale über CMA des Relaisteils sind in den Fehlerbäumen berücksichtigt.

- CMA der Sumpfsignale

Die Sumpfsignale, die die Umschaltung der Not- bzw. Nachkühlsysteme auf Ansaugen aus dem Gebäudesumpf bewirken, werden aus einer UND-Verknüpfung der Anregungen aufgrund der Grenzwerte "Flutbehälter-Wasserstand < 1,15 m" und dem Notkühlvorbereitungssignal gebildet. Da jedoch der Ausfall des Notkühlvorbereitungssignals allein bereits vor Umschalten auf Sumpfbetrieb zum Systemausfall führt, ist für den Ausfall der Umschaltung auf Sumpfbetrieb nur die Anregung über die Flutbehälter-Wasserstandsmessung zu berücksichtigen. Die Meßkanalgruppen zur Erfassung des Flutbehälter-Wasserstandes sind vierfach vorhanden und jeweils in 2v3-Verknüpfung aufgebaut. Die Wahrscheinlichkeit für den CMA der Sumpfsignale ergibt sich zu:

$$\bar{p}_{CMA} = 2{,}3 \cdot 10^{-4} \quad (p_{CMA\ 50} = 1{,}9 \cdot 10^{-4}/K = 3).$$

Den wesentlichen Einfluß (78 %) auf das Ergebnis liefern auch hier CMA aufgrund menschlicher Fehlhandlungen. Für die CMA in den Meßkanalgruppen zur Erfassung der Flutbehälter-Wasserstände wurde eine "starke Kopplung" unterstellt. Im Gegensatz zu den Ausfallmöglichkeiten der Flutsignale wird hier ein fälschliches Absperren von Wirkdruckleitungen nicht bemerkt.

- CMA der Reaktorkühlkreislaufsabschlußsignale

Die Reaktorkühlkreislaufabschlußsignale YZ37 werden vom Kriterium "Wasserstand des Druckhalters < 2,85 m" angeregt. Diese Meßkanalgruppe wird je Redundanz in 2v3-Verknüpfung ausgewertet. Damit errechnet sich die Wahrscheinlichkeit eines CMA dieser Signale für eine Redundanz zu:

$$\bar{p}_{CMA} = 1{,}5 \cdot 10^{-3} \quad (p_{CMA\ 50} = 1{,}2 \cdot 10^{-3}/K = 2{,}5)$$

Das Ergebnis wird zu 67 % durch Ausfälle aufgrund menschlichen Fehlverhaltens bestimmt.

- CMA der Notspeisezuschaltsignale

Die Notspeisezuschaltsignale YZ51 werden aus einer ODER-Verknüpfung der vier Dampferzeuger-Wasserstandsmeßkanalgruppen gebildet, die ihrerseits in 2v3-Verknüpfung aufgebaut sind. Die Wahrscheinlichkeit für den Ausfall der Notspeisezuschaltsignale ergibt sich zu:

$$\bar{p}_{CMA} = 2{,}3 \cdot 10^{-4} \quad (p_{CMA\ 50} = 1{,}9 \cdot 10^{-4}/K = 3)$$

Das Ergebnis wird im wesentlichen durch Ausfälle aufgrund menschlicher Fehlhandlungen bestimmt, für die eine starke Kopplung berücksichtigt wurde.

- CMA der Notspeisesignale

Die Notspeisesignale YZ52-YZ55 für die Dampferzeuger YB01-YB04 werden aus einer 2v4-Verknüpfung der Messungen des jeweiligen Dampferzeuger-Wasserstandes gebildet. Für Ausfälle aufgrund menschlicher Fehlhandlungen wird eine starke Kopplung angesetzt. Damit ergibt sich ein Wert von

$$\bar{p}_{CMA} = 2{,}3 \cdot 10^{-4} \quad (p_{CMA\ 50} = 1{,}9 \cdot 10^{-4}/K = 3)$$

Dieses Ergebnis wird im wesentlichen durch Ausfälle aufgrund menschlicher Fehlhandlungen bestimmt. Der Ausfall des Notspeisesignals für einen bestimmten Notspeisestrang errechnet sich zu:

$$\bar{p}_{CMA} = 1{,}5 \cdot 10^{-3} \quad (p_{CMA\ 50} = 1{,}2 \cdot 10^{-3}/K = 2{,}5)$$

- CMA der Deionatzuschaltsignale

Die Deionatzuschaltsignale YZ61 werden von der Meßkanalgruppe zur Erfassung des Wasserstandes im Speisewasserbehälter angeregt. Diese Meßkanalgruppe wird in 2v4-Verknüpfung ausgewertet. Die Wahrscheinlichkeit eines CMA errechnet sich zu:

$$\bar{p}_{CMA} = 1{,}5 \cdot 10^{-3} \quad (p_{CMA\ 50} = 1{,}2 \cdot 10^{-3}/K = 2{,}5)$$

Dieser Wert wird überwiegend durch Ausfälle aufgrund menschlicher Fehlhandlungen bestimmt.

- CMA der Deionatsignale

Die Deionatsignale YZ62 bis YZ64 für die vier Notspeisestränge werden aus UND-Verknüpfungen der Deionatzuschaltsignale mit den negierten Absperrsignalen der entsprechenden Notspeisestränge gebildet. Die Wahrscheinlichkeit eines CMA dieser Signale entspricht in erster Näherung dem Wert für die Deionatzuschaltsignale. Dieser Wert wurde auch den Fehlerbaumanalysen zugrunde gelegt.

- CMA der Speisewassersignale

Die Speisewassersignale YZ50 werden aus einer UND-Verknüpfung von Notspeisezuschaltsignalen und den negierten Deionatzuschaltsignalen gebildet. Zum Ausfall der Signale führt also der Ausfall der Notspeisezuschaltsignale oder das zu frühe Ansprechen der Deionatzuschaltsignale. Dabei führt der Ausfall der Notspeisezuschaltsignale allein zum Ausfall des Notspeisewassersystems und braucht daher nicht berücksichtigt zu werden. Das zu frühe Ansprechen der Deionatzuschaltsignale bewirkt, daß die Notspeisewasserpumpen auf Ansaugen aus den Deionatbehältern umgeschaltet werden, dies führt jedoch zu keinen gravierenden Auswirkungen. Für einige Störfälle könnte in diesem Fall der zur Verfügung stehende Wasservorrat für das sekundärseitige Abfahren eingeschränkt werden.

- CMA der Notstromvorbereitungssignale

Die Notstromvorbereitungssignale YZ81 werden aus einer ODER-Verknüpfung der Notkühlvorbereitungssignale und der Notspeisezuschaltsignale gebildet. Diese ODER-Verknüpfung erfolgt in der Logikebene des Reaktorschutzsystems. Werden die Notkühlvorbereitungssignale oder die Notspeisezuschaltsignale im Störfall benötigt, so führt bereits der CMA dieser Signale allein zum Systemausfall. Diese CMA brauchen hier nicht nochmals berücksichtigt zu werden. CMA des Relaisteils für die Notstromvorbereitungssignale sind im Fehlerbaum dagegen berücksichtigt.

- CMA der Notstromsignale

Die Notstromsignale YZ82 bis YZ85 werden durch eine Spannung an der jeweiligen Notstromschiene < 80% der Nennspannung angeregt. Der CMA der Notstromsignale kann gegenüber der Wahrscheinlichkeit eines CMA der Notstromdiesel vernachlässigt werden.

6.1.3 Bewertung der leittechnischen Komponenten

6.1.3.1 Ersatzausfallraten für leittechnische Komponenten

Die leittechnischen Systeme der untersuchten Anlage enthalten eine Vielzahl von Bauelementen, die im wesentlichen in diskreter Schaltungstechnik aufgebaut sind. Damit sind die Fehlermöglichkeiten, die zum Ausfall einer bestimmten, gewünschten Systemfunktion führen können, entsprechend zahlreich und deren Darstellung in den Teilfehlerbäumen aus Gründen der Übersichtlichkeit nicht zweckmäßig.

Die Analyse dieser Systeme wird deshalb getrennt durchgeführt. In den Fehlerbäumen werden lediglich die Ergebnisse dieser Untersuchungen, hier als "Ersatzausfallraten der Leittechnik" bezeichnet, verwendet. Die Ersatzausfallraten fassen die Einzelausfallraten von Bauelementen oder Geräten in Teilsystemen zusammen.

Die folgenden Abschnitte beschreiben die Analysemethode und die dabei zugrunde gelegten Voraussetzungen. Einzelne Teilsysteme (z.B. die Steuerkette) werden ausführlich erläutert. Die im Abschnitt 6.1.3.2.5 aufgeführte Liste der Ersatzausfallraten gibt eine Übersicht über alle weiteren untersuchten Teilsysteme sowie eine kurze Beschreibung der Ausfallart und der hierzu beitragenden Bauelementausfälle.

- Basisdaten

Grundlage für die hier durchgeführten Berechnungen sind die im Fachband 3 aufgelisteten Baugruppen- bzw. Einzelausfallraten. Sie sind aus Betriebserfahrung, durch Literaturrecherchen oder Ausfalleffektanalysen gewonnen worden. Letztere gelten besonders für die in Steuerketten, Teilsteuerungen und Verriegelungen eingesetzten Bausteine der Baureihe Simatic-P (UND-, ODER-Gatter, Vorrang-, Betätigungsbausteine usw.).

Des weiteren sind nach /F2, 6-3 und -4/ Korrekturfaktoren zu berücksichtigen, die verschiedenen Umgebungseinflüssen und Belastungen Rechnung tragen.

Für Komponenten, die außerhalb der Sicherheitshülle in Räumen mit kontrollierter Atmosphäre vibrationsfrei (in Schränken) installiert sind, wird ein Belastungsfaktor von 0,5 in Rechnung gesetzt. Für die Temperaturbelastung von elektronischen Bausteinen wird ein Faktor von 1,3 berücksichtigt, was einer Umgebungstemperatur von 40 °C entspricht. Bei Bausteinen der Simatic-P-Baureihe wird zusätzlich noch die Unterbelastung der Bauelemente durch einen Faktor von 0,2 mit einbezogen, womit eine Belastung mit 40 % der Nennleistung berücksichtigt wird. Bei den Bausteinen der Simatic-N-Baureihe und der Meßwerterfassung wird eine Belastung mit 60 % der Nennlast und damit ein Faktor von 0,3 in Rechnung gesetzt.

- Voraussetzungen

Die Zuverlässigkeitsanalysen an leittechnischen Systemen sind mit Hilfe der Fehlerbaummethode durchgeführt worden. Bei ihr wird gezielt nach jenen Fehlern bzw. Ausfällen gesucht, die zu einem bestimmten, vorher definierten unerwünschten Verhalten, z.B. an einem Geräteausgang, führen.

Beginnend an dem entsprechenden Ausgang, werden nach und nach alle Signalwege rückwärts in die Schaltung hinein verfolgt und daraufhin untersucht, über welche Wege und von welchen Ausfällen das betrachtete unerwünschte Verhalten verursacht werden kann.

Diese Methode läßt sich im allgemeinen nur theoretisch und nicht experimentell durchführen. Ihr Vorteil liegt darin, daß jene Fehler, die nicht zu dem definierten Ausfallverhalten führen, nicht weiter betrachtet werden müssen. Ebenso sind, ohne daß dabei größere Fehler gemacht werden, folgende Vereinfachungen zulässig:

- Ausfälle, die bei ihrem Auftreten sofort gemeldet werden, können in der Regel vernachlässigt werden. Dies gilt besonders dann, wenn

$$\lambda_s \cdot \tau << \lambda_F \cdot T$$

mit

λ_s ≙ Ausfallrate für die selbstmeldenden Ausfälle,

λ_F ≙ Ausfallrate der erst bei den Funktionsprüfungen entdeckbaren Ausfälle,

τ ≙ mittlere Instandsetzungszeit,

T ≙ Zeit zwischen zwei aufeinanderfolgenden Funktionsprüfungen;

- Mehrfachausfälle, die nur zum Ausfall eines der redundanten Untersysteme oder Stränge führen, können meist gegenüber Einzelausfällen mit gleicher Wirkung vernachlässigt werden. Dies gilt besonders dann, wenn

$$\lambda_{d1} \cdot \lambda_{d2} \cdot T_1 \cdot T_d << \lambda_e \cdot T_e$$

mit

λ_{d1} ≙ Ausfallrate des ersten Ausfalls eines Doppelausfalls,

λ_{d2} ≙ Ausfallrate des zweiten Ausfalls eines Doppelausfalls,

T_1 ≙ Fehlerentdeckungszeit, wenn nur ein Ausfall vorliegt,

T_d ≙ Fehlerentdeckungszeit der Doppelausfälle ,

λ_e ≙ Ausfallrate der möglichen Einzelausfälle,

T_e ≙ Ausfallentdeckungszeit der Einzelausfälle, wobei T_e häufig gleich T_d ist.

Die Gesamtausfallrate erhält man unter diesen Voraussetzungen durch Addition aller Einzelausfallraten.

6.1.3.2 Ausfallverhalten und Beschreibung einzelner Teilsysteme

6.1.3.2.1 Steuerkette

Unter dem Begriff der Steuerkette wird hier der Teil eines leittechnischen Systems in Kraftwerken zusammengefaßt, der zur Ansteuerung von Komponenten der Betätigungsebene (Antriebe, Stellglieder usw.) benötigt wird. Die Steuerkette umfaßt die Betätigungsbausteine (ggf. die Vorrangbausteine), die Endschalter und sämtliche Kabel, Lötstellen und Klemmen, die die einzelnen Elemente bis hin zum Koppelschütz in der Schaltanlage verbinden.

Die eingesetzten Schaltkreise sind weitgehend standardisiert. So werden z.B. im Sicherheitssystem von Druckwasserreaktoren mehrere hundert Antriebe betätigt und überwacht. Hinsichtlich der Ansteuerung müssen jedoch nur 2 unterschiedliche Arten von Steuerketten betrachtet werden:

- Steuerketten für Pumpen, Schütze oder Leistungsschalter und
- Steuerketten für Motorarmaturen.

Die Befehlskanäle für den EIN- bzw. ZU-Befehl und den AUS- bzw. AUF-Befehl unterscheiden sich. Für die interessierende Ausfallrichtung - Befehl wird unterdrückt - ergeben sich demnach vier verschiedene Fälle:

Steuerkette für Pumpen, Schütze, Leistungsschalter unterdrückt

- EIN-Befehl ($\lambda_{ges} = 0,7/3$)
- AUS-Befehl ($\lambda_{ges} = 0,6/3$)

Steuerkette für Motorarmaturen unterdrückt

- AUF-Befehl ($\lambda_{ges} = 1,9/3$)
- ZU-Befehl ($\lambda_{ges} = 1,8/3$)

6.1.3.2.2 Ausfälle der Stromversorgung und der Signalpotentiale

Die Baugruppen der Verriegelungsebene, Betätigungsebene oder des Reaktorschutzsystems sind in Schränken untergebracht. Jeder einzelne Schrank bezieht seine Versorgungsspannung von einer Schleifenleitung, die doppelt eingespeist, über Dioden entkoppelt durch die Schränke einer Schrankgruppe geführt wird. In den Schränken werden die von der Schleifenleitung abgegriffenen Ströme aufgeteilt und den angeschlossenen Bausteinen zugeführt.

- Ausfall der positiven Spannung in den Relaisteilschränken des Reaktorschutzsystems

Die Ausgabe von Reaktorschutzsignalen erfolgt im Relaisteil des Reaktorschutzsystems. Dabei wird die positive Spannung in den Relaisteilschränken (je nach Redundanz P1 bis P4) durch Relais auf die entsprechenden Steuerleitungen geschaltet. Angeschlossen daran ist eine von Signal zu Signal unterschiedliche Anzahl von Bausteinen bzw. Steuerketten.

Gibt es auf dem Weg zwischen Ausgaberelais und angeschlossenem Baustein einen Masseschluß, so spricht die Schranksicherung an. Die Potentiale sind nicht, wie in den Verriegelungsschränken, zeilenweise abgesichert. Durch einen Kurzschluß, z.B. in einem der angesteuerten Betätigungsbausteine, fallen also das betreffende Potential und damit alle in diesem Schrank vom gleichen Potential gebildeten Signale aus.

Die Spannungsausfälle werden für die einzelnen Störfälle getrennt untersucht:

- Kurzschlüsse bei Ausgabe der Reaktorschutzsignale zur Notkühlung,
- Kurzschlüsse bei Ausgabe der Notstromsignale,
- Kurzschlüsse bei Ausgabe der Reaktorschutzsignale zur Notspeisung und
- Kurzschlüsse bei Ausgabe der Reaktorschutzsignale des gesicherten Bereichs.

Des weiteren wird unterschieden nach

- Ausfällen durch Fehler in den Zeitstufen von verzögerten Reaktorschutzsignalen und
- Ausfällen durch Fehler innerhalb der angesteuerten Steuerketten.

Den Beitrag einer Zeitstufe bzw. Steuerkette hinsichtlich der Ausfallrichtung "verursacht Kurzschluß" liefert die Ausfalleffektanalyse. Aus der Zahl der im Einzelfall angeforderten Bausteine wird die jeweilige Ersatzausfallrate bestimmt.

- 24-V-Ausfall in den Verriegelungsschränken

In den Verriegelungsschränken sitzen die zum Aufbau einer Teilsteuerung oder Verriegelung benötigten Simatic-P-Bausteine (Speicher, UND-, ODER-Gatter usw.).

Ausfälle der Potentiale P, N oder M werden über die Überwachungsstufe Y3 der betroffenen Schrankzeile gemeldet. Nicht selbstmeldende Ausfälle der 24-V-Versorgung treten dagegen bei Ausfall der Überwachungsstufe auf.

Zu dieser Ausfallrate müssen noch Anteile hinzugerechnet werden, die die möglichen Kurzschlüsse in den versorgten Gattern und in den angesteuerten Bausteinen, einschließlich der bis zu diesen Bausteinen gehenden Verkabelung, repräsentieren. Ein Kurzschluß in diesem Bereich wird erst entdeckt, wenn die betroffenen Bausteine angesteuert werden, d.h. bei einer vollständigen Funktionsprüfung oder beim Störfall.

- 24-V-Ausfall in den Betätigungsschränken

In diesen Schränken werden die Betätigungsbausteine untergebracht und mit Spannung versorgt.

Jeder Betätigungsbaustein besitzt eine eigene Stromüberwachung.

Kurzschlüsse im Baustein selbst führen hier nicht zum Ausfall der Versorgungsspannung.

Nicht selbstmeldend sind Fehler, die zum Ausfall des M-Potentials führen (Unterbrechung von Kabeln, Löt- und Klemmverbindungen).

Der Ausfall einer Schrankhälfte kann darüber hinaus durch die Unterbrechung des negativen Potentials verursacht werden.

6.1.3.2.3 Ausfall von einzelnen Reaktorschutzsignalen

Ein Teil der denkbaren Ausfälle im Logik- oder Relaisteil des Reaktorschutzsystems führt zur Unterdrückung einzelner Reaktorschutzsignale.

Da aufgrund der kurzen Instandsetzungszeiten selbstmeldende Fehler in der Regel vernachlässigbar sind, werden die im dynamisch arbeitenden Logikteil möglichen Ausfallarten nicht berücksichtigt. Mögliche nicht selbstmeldende Fehler im Logikteil (z.B. Kurzschlüsse vom Eingang zum Ausgang der 2v3-Kettenglieder) spielen wegen der geringen Wahrscheinlichkeit ihres Auftretens quantitativ keine Rolle, sie wurden daher vernachlässigt.

An Ausfällen, die zur Unterdrückung eines Signals im Relaisteil führen, wird entweder das Kleben des Ausgabekontaktes des zugehörigen Abschlußrelais oder - bei verzögerten Signalen - die Unterdrückung eines Signals in der entsprechenden Verzögerungsstufe berücksichtigt.

6.1.3.2.4 Unterdrückung von Stellbefehlen durch Ausfälle in Teilsteuerungen oder Verriegelungen

Einige Komponenten (z.B. Deionatpumpen) werden im Störfall zunächst durch eine Teilsteuerung (nicht durch das Reaktorschutzsystem) angefordert. Diese Teilsteuerungen beinhalten einen Teil der automatischen Betriebsweise einer Funktionsgruppe oder eines

Aggregats innerhalb dieser Funktionsgruppe. Sie sind ausschließlich in Verknüpfungstechnik, d.h. mit logischen Verknüpfungen, Speichern und Zeitfunktionen, ohne schrittweisen Ablauf, ausgeführt. Die Stellbefehle werden durch Verarbeitung der aus der Anlage kommenden Rückmeldungen gebildet. Im Unterschied zu Verriegelungen sind Teilsteuerungen von Hand abschaltbar.

Verriegelungen werden im wesentlichen wie Teilsteuerungen aufgebaut. Sie verknüpfen jedoch bereits vorhandene EIN- bzw. AUS-Befehle mit Kriterien, die zum Schutz der Anlage oder des Aggregats dienen.

Zum Ausfall eines Stellbefehls kommt es demnach dadurch, daß entweder die Bauelemente, aus denen die Verriegelungen und Teilsteuerungen aufgebaut sind, ausfallen (z.B. UND-Gatter unterdrückt EIN-Befehl) oder Signale aus der Anlage ausfallen (Versagen von Gebern und Endschaltern).

6.1.3.2.5 Zusammenstellung weiterer Teilsysteme

Die nachfolgende Liste gibt eine Übersicht über alle weiteren, durch Fehlerbaumanalyse untersuchten Teilsysteme. Sie enthält neben einer kurzen Beschreibung des unterstellten Systemausfalls die zur Ersatzausfallrate maßgeblich beitragenden Einzelausfälle.

Kennzeichnung	Ausfallbeschreibung	$\lambda_{50}[10^{-6}/h]$ /Streufaktor
L97 21 EU01 H001 L98 22 EV01 H001 L99 23 EW01 H001 L100 24 EX01 H001	Schalterfall von Einspeiseschalter kommt fälschlich (1 Betätigungsbaustein bildet fälschlich Schalterfallmeldung, 1 Relaiskontakt klebt)	0,3/K = 3
L103 20 EU06 U001 L104 20 EV06 U001	Angeforderter Teil der Zuschaltautomatik für die Kuppelschalter ausgefallen (3 Verzögerungsstu-	6,0/K = 3

Kennzeichnung	Ausfallbeschreibung	$\lambda_{50}[10^{-6}/h]$ /Streufaktor
	fen, 1 UND-Gatter geben fälschlich Signal aus; 1 Relais zieht nicht an, 2 Relaiskontakte kleben; 3 UND-, 2 ODER-Gatter, 2 Verzögerungsstufen, 2 Speicher unterdrücken Signal)	
L121 21 YZ01 K1U11 L122 22 YZ02 K2U11 L123 23 YZ03 K3U11 L124 24 YZ04 K4U11	Takt für Ansteuerung der Grenzsignalgeber des Sumpfsignals fällt aus (3 NOR-Gatter, 1 Impulsformer ausgefallen)	3,2/K = 3
L125 21 YZ41 U001 L126 22 YZ42 U002 L127 23 YZ43 U003 L128 24 YZ44 U004	Kanal des Logikteils für das Sumpfsignal ausgefallen (1 Abschlußglied oder eine 2v3-Auswahleinheit ausgefallen)	3,5/K = 3
L161 21 YZ82 U1X02 L162 22 YZ83 U2X02 L163 23 YZ84 U3X02 L164 24 YZ85 U4X02	Ausfall des Notstromsignals für Startbefehl (1 Verzögerungsstufe spricht nicht an, 1 Relais schließt nicht, 1 Verzögerungsstufe spricht fälschlich an, 1 Relaiskontakt klebt, 1 Relaiskontakt unterbricht)	1,1/K = 3
L285 20 TH16 L001 L286 20 TH26 L001 L287 20 TH36 L001 L288 20 TH46 L001	Örtliche Niveaumessung ausgefallen (1 Differenzdruckfühler mißt zu hohen Druck, analoges Druckanzeige gerät ausgefallen)	11,0/K = 3
L289 20 ES04 H001	Steuerung für Koppelschalter unterdrückt EIN-Befehl (2 Relaiskontakte kleben, 1 ODER-Gatter unterdrückt Signal, 1 UND-Gatter gibt fälschlich Signal aus)	1,8/K = 3

Kennzeichnung	Ausfallbeschreibung	$\lambda_{50}[10^{-6}/h]$ /Streufaktor
L329 20 RY21 D001 L330 20 RY22 D001	Steuerung für Deionatpumpe unterdrückt EIN-Befehl (1 Niveauschalter spricht nicht an, ODER-Gatter unterdrücken Signal, 24 V in einer Zeile des Verriegelungsschranks ausgefallen)	8,0/K = 10
L371 21 VG72 S001 L372 22 VG72 S002	Steuerung für Motorarmaturen der Ölkühler unterdrückt AUF-Befehl (4 Relaiskontakte kleben, 24 V in einer Zeile des Verriegelungsschranks ausgefallen, Steuerkette unterdrückt AUF-Befehl)	3,0/K = 10
L446 20 RY11 D001 L447 20 RY12 D001	Steuerung für Deionatdruckerhöhungspumpe unterdrückt EIN-Befehl (2 ODER-Gatter geben kein Signal aus, 24 V im Betätigungs- oder Verriegelungsschrank ausgefallen, 1 UND-, 1 ODER-Gatter, 1 analoge Zeitstufe geben fälschlich Signal aus, Steuerkette unterdrückt EIN-Befehl)	2,5/K = 3
L621 20 EY10 D1X01 L622 20 EY20 D1X01 L623 20 EY30 D1X01 L624 30 EY40 D1X01	Rückmeldung "Dieselgeneratorschalter ist EIN" ausgefallen (1 Relaiskontakt klebt, 1 ODER-Gatter gibt kein Signal aus)	0,4/K = 3
L626 20 TH10 U120 L627 20 TH20 U120 L628 20 TH30 U120 L629 20 TH40 U120	Pumpenschutz für Nachkühlpumpe spricht nicht an (1 ODER-, 1 UND-Gatter, 1 analoge Zeitstufe geben kein Signal aus; 1 Relais fällt durch Kurzschluß oder Unterbrechung aus)	2,0/K = 3

Kennzeichnung	Ausfallbeschreibung	$\lambda_{50}[10^{-6}/h]$ /Streufaktor
L778 20 TF30 S012	Schutzverriegelung für Absperrung vor Beckenkühler unterdrückt ZU-Befehl (2 ODER-, 1 UND-Gatter geben kein Signal aus, 1 Endschalter spricht nicht an, 24 V-Ausfall im Betätigungs-oder Verriegelungsschrank)	2,2/K = 3

6.1.4 Bewertung der Handmaßnahmen

Wie bereits im Abschnitt 3.4 ausführlich beschrieben, werden in der vorliegenden Studie in Übereinstimmung mit WASH-1400 nur geplante Handmaßnahmen bewertet. Im folgenden ist die Bewertung derjenigen Handmaßnahmen dargestellt, die sowohl bei Kühlmittelverluststörfällen allein als auch bei Transienten berücksichtigt werden. Handmaßnahmen, die nur in der Zuverlässigkeitsanalyse von Transienten eine Rolle spielen, sind dort gesondert erläutert.

L 344 OP RL04 S019	Notspeisewasser-Saugschieber wird in
L 345 OP RL05 S019	falscher Stellung belassen oder fälsch-
L 346 OP RL06 S019	lich zugefahren.
L 347 OP RL07 S019	$p_{50} = 1 \cdot 10^{-2}/K = 3$

Die Saugschieber werden zum Beispiel im Rahmen der Funktionsprüfung der Notspeisezuschalt- bzw. der Notspeisesignale (YZ51 bzw. YZ52) verfahren. Nach Anweisung des Betriebshandbuches sollen sie vor der Funktionsprüfung von Hand zugefahren werden, um dann von den Reaktorschutzsignalen aufgefahren zu werden. Im letzten Schritt der Prüfanweisung ist dann die offene Stellung des Saugschiebers zu kontrollieren.

Die Bewertung erfolgt in Anlehnung an WASH-1400. Dort werden Wahrscheinlichkeiten für das Nichtentdecken von Armaturenfehl-

stellungen zwischen $p_{50} = 3 \cdot 10^{-3}$ und 10^{-2} unter der Voraussetzung angegeben, daß keine Anzeigen der Armaturenstellungen in der Warte vorhanden sind. In der Warte der Referenzanlage erscheinen jedoch Stellungsmeldungen, so daß die durchgeführte Bewertung als pessimistische Abschätzung anzusehen ist.

L 348 21 RL04 S005	Notspeisewasser-Druckschieber wird in
L 349 22 RL05 S005	falscher Stellung belassen oder fälsch-
L 350 23 RL06 S005	lich zugefahren.
L 351 24 RL07 S005	$p_{50} = 1 \cdot 10^{-2}/K = 3$

Diese Armaturen werden auch zum Beispiel im Rahmen der Funktionsprüfung der Notspeisezuschalt- bzw. Notspeisesignale verfahren. Die Bewertung erfolgte in der gleichen Weise wie bei L 348 bis L 351.

L 397 OP TH10 FP	Bei Funktionsprüfungen wird die Stel-
L 398 OP TH20 FP	lungsmeldung der Flutbehälter-Rück-
L 399 OP TH30 FP	schlagklappe nicht beachtet.
L 400 OP TH40 FP	$p_{50} = 3 \cdot 10^{-2}/K = 3$

Die Funktion der Flutbehälter-Rückschlagklappen wird im Rahmen der Funktionsprüfung der Reaktorschutzsignale YZ36/38 geprüft. Am Ende des Prüfablaufes soll die Störfallbereitschaft des entsprechenden Nachkühlstranges kontrolliert werden, wobei allerdings nur auf ein anderes Logikschema des Betriebshandbuches verwiesen wird. Eine besondere Überprüfung der Stellung der Rückschlagklappe ist nicht vorgesehen. Damit muß in Betracht gezogen werden, daß die Stellungsmeldung einer nach Funktionsprüfung fälschlich nicht schließenden Rückschlagklappe am Steuerpult übersehen oder nicht überprüft wird.

In WASH-1400 werden für ein eher zufälliges Entdecken einer Armaturenfehlstellung Wahrscheinlichkeiten von $p_{50} = 10^{-2}$ bis 10^{-1} erwartet. Ebenso wie bei L 334 bis L 347 wird auch hier das Vorhandensein von Stellungsmeldungen in der Warte nicht berücksichtigt, so daß die Bewertung mit $p_{50} = 3 \cdot 10^{-2}$ als pessimistische Abschätzung gelten kann.

L 401 OP TH10 ME
L 402 OP TH20 ME
L 403 OP TH30 ME
L 404 OP TH40 ME

Bei Funktionsprüfungen wird das Nichtansprechen der Stellungsmeldungen der Flutbehälter-Rückschlagklappe nicht beachtet.
$p_{50} = 0,5/K = 3$

Diese Ausfallwahrscheinlichkeiten beziehen sich auf folgenden Fall: Die Rückschlagklappe ist ständig fälschlich offen, dies wird aber nicht entdeckt, weil der Ausfall der Meldeeinrichtung nicht bemerkt oder nicht überprüft wird, ob auch bei offener Rückschlagklappe fälschlicherweise die Meldung "Rückschlagklappe geschlossen" ansteht. Für beide Möglichkeiten wird eine Wahrscheinlichkeit von insgesamt $p_{50} = 0,5/K = 3$ abgeschätzt. Diese Bewertung berücksichtigt die Tatsache, daß der Fehler in einer nur sehr kurzen Zeitspanne während der Funktionsprüfung entdeckt werden kann.

L 409 OP TH15 FP
L 410 OP TH25 FP
L 411 OP TH35 FP
L 412 OP TH45 FP

Bei Funktionsprüfungen wird die Stellungsmeldung der Rückschlagklappe der HD-Sicherheitseinspeisepumpe nicht beachtet.
$p_{50} = 3 \cdot 10^{-2}/K = 3$

Der Operator-Fehler wird in gleicher Weise wie bei L 397 bis L 400 bewertet, auch hier sind keine speziellen Prüfhinweise vorhanden.

L 413 OP TH15 ME
L 414 OP TH25 ME
L 415 OP TH35 ME
L 416 OP TH45 ME

Bei Funktionsprüfungen wird das Nichtansprechen der Stellungsmeldung der Rückschlagklappe der HD-Sicherheitseinspeisepumpe nicht beachtet.
$p_{50} = 0,5/K = 3$

Die Fehlermöglichkeiten entsprechen denen bei der Funktionsprüfung der Flutbehälter-Rückschlagklappen, deshalb erfolgt die Bewertung in der gleichen Weise wie bei L 401 bis L 404.

L 449 OP RY10/11

Kein EIN-Befehl von Hand für Deionatpumpen oder Deionat-Druckerhöhungspumpen oder kein AUF-Befehl von Hand für Armaturen im Deio-

natzulauf zum Speisewasserbehälter beim Notstromfall
$p_{50} = 10^{-3}/K = 7$

Auf die Notwendigkeit dieser Maßnahmen wird in der entsprechenden Logikfahne des Betriebshandbuches hingewiesen, außerdem weisen Prozeßrechnermeldungen und eine Notgefahrmeldung auf den niedrigen Wasserstand im Speisewasserbehälter hin. Es wird für die Durchführung der Maßnahme personelle Redundanz in Form eines Reaktorfahrers und des Schichtleiters angesetzt. Außerdem werden die Notgefahrmeldung und die Prozeßrechnermeldungen mit einem Fehlerentdeckungsfaktor (recovery factor) von $p_{50} = 10^{-1}/K = 3$ berücksichtigt. Dabei wird davon ausgegangen, daß diese Meldungen wahrscheinlich nur vom Reaktorfahrer am Fahrpult beachtet werden.

Die Maßnahme ist frühestens 30 Minuten nach Störfalleintritt erforderlich, deshalb wird für die Handlung des Reaktorfahrers gemäß WASH-1400, App. III, eine Wahrscheinlichkeit von $p_{50} = 10^{-1}$ angesetzt. Die Berücksichtigung der personellen Redundanz ergibt das Quadrat dieses Wertes. Damit ergibt sich insgesamt $p_{50} = 10^{-3}/K = 7$.

L 451 OP RY10/11 — Kein EIN-Befehl von Hand für Deionatpumpen oder Deionat-Druckerhöhungspumpen oder kein AUF-Befehl von Hand für Armaturen im Deionatzulauf zum Speisewasserbehälter bei Kühlmittelverluststörfällen
$p_{50} = 10^{-1}/K = 3$

In den Logikfahnen des Betriebshandbuches für diese Störfälle werden für solche Maßnahmen keine Hinweise gegeben. Lediglich Prozeßrechnermeldungen sowie eine Notgefahrmeldung weisen auf den niedrigen Wasserstand im Speisewasserbehälter hin. Es wird keine personelle Redundanz angesetzt, da die Notgefahrmeldung und die Prozeßrechnermeldungen wahrscheinlich nur vom Reaktorfahrer am Fahrpult beachtet werden. Entsprechend zu WASH-1400 wird für Handmaßnahmen ca. 30 Minuten nach Störfalleintritt eine Fehlerwahrscheinlichkeit von $p_{50} = 10^{-1}$ angesetzt.

L 477 OP TF30 S012 Kein ZU-Befehl von Hand für Absperrarmaturen des Beckenkühlers
$p = 1$

Es gibt für die Notwendigkeit der Maßnahme keine direkten Hinweise. Außerdem steht für die Durchführung der Maßnahme wenig Zeit zur Verfügung, so daß bei der Meldung "Temperatur Ölkühler der Notspeisepumpe RL06 zu hoch" keine Zeit zur Suche der Ursache gegeben ist.

Die Maßnahme wird als nicht geplanter Handeingriff mit $p = 1$ bewertet. Ungeplante Handeingriffe werden auch in WASH-1400 nicht berücksichtigt.

L 478 OP RY10 S001 Absperrschieber wird fälschlich in ZU-Stellung gefahren oder nach Funktionsprüfung.
$p_{50} = 1 \cdot 10^{-2}/K = 3$

Diese Armatur wird im Rahmen der Funktionsprüfung der Deionatzuschaltsignale bzw. der Deionatsignale für die Notspeisestränge gefahren. Die Bewertung erfolgt in analoger Weise wie bei L 344 bis L 347.

L 530 OP YZ60 Kein Rücksetzen der Absperrsignale für Frischdampf- und Speisewasser-Kreislauf innerhalb von 40 Minuten nach Auslösung von YZ60
$p_{50} = 7 \cdot 10^{-2}/K = 3$

Die Bewertung lehnt sich an die Vorgehensweise in der AIPA-Studie an (Abschnitt 3.4.3). Es stehen etwa 40 Minuten Zeit für die Durchführung der Maßnahme zur Verfügung. Das Rücksetzen der Signale muß in den Reaktorschutzschränken des Notstandssystems im Ringraum der Anlage erfolgen. Für die Durchführung der Maßnahme werden im Mittel MTOR = 16 Minuten benötigt.

L 531 OPSF11-13 Nochmaliges zu schnelles Auffahren der FD-Umleitventile bzw. der Abblaseregelventile etwa 1 Stunde nach Störfalleintritt
$p_{50} = 3 \cdot 10^{-2}/K = 3$

Durch zu schnelles Auffahren der Ventile wurde bereits einmal YZ60 ausgelöst. Nach Rücksetzen des Reaktorschutzsignals werden die Armaturen mit größerer Vorsicht gefahren. Die Bewertung lehnt sich an WASH-1400 an. Es wird das geometrische Mittel aus der Wahrscheinlichkeit einer Fehlhandlung 30 Minuten nach Störfalleintritt ($p_{50} = 10^{-1}$) und mehrere Stunden nach Störfalleintritt ($p_{50} = 10^{-3}$) gebildet.

L 533 OP YZ60 — Kein Rücksetzen der Absperrsignale für Frischdampf- und Speisewasser-Kreislauf innerhalb von 1 Stunde nach Auslösung von YZ60
$p_{50} = 2 \cdot 10^{-2}/K = 3$

Die Bewertung wurde auf der Basis der AIPA-Studie (Abschnitt 3.4.3) unter der Annahme durchgeführt, daß nach fälschlichem zu schnellen Auffahren der Frischdampf-Umleiteinrichtung der Operator ca. eine Stunde mit mindestens einem Abblaseregelventil abfährt und danach wieder die Frischdampf-Umleiteinrichtung in Betrieb nimmt. Die Durchführung der Maßnahme muß in den Reaktorschränken des Notstandssystems im Ringraum erfolgen. Für die Durchführung der Maßnahme werden im Mittel MTOR = 16 Minuten benötigt.

L 534 OP SF11-13 — Zu schnelles Auffahren der FD-Umleitventile bzw. der Abblaseregelventile
$p_{50} = 10^{-1}/K = 3$

Das Auffahren der Umleitventile bzw. der Abblaseregelventile erfolgt ca. 30 Minuten nach Störfalleintritt. Das Auffahren der Armaturen erfolgt vom Betätigungstischfeld am Fahrpult in der Warte und wird von einem Reaktorfahrer durchgeführt. Nach WASH-1400 sind Handlungen ca. 30 Minuten nach Störfalleintritt mit $p_{50} = 10^{-1}$ zu bewerten.

L 535 OP SF11-13 — Nochmaliges zu schnelles Auffahren der FD-Umleitventile bzw. der Abblaseregelventile
$p_{50} = 10^{-1}/K = 3$

Im allgemeinen geht man bei der Bewertung menschlicher Zuverlässigkeit davon aus, daß bei hoher Streßbelastung Handlungen, die im ersten Versuch falsch durchgeführt wurden, bei den nächsten Versuchen mit höherer Wahrscheinlichkeit erneut falsch durchgeführt werden.

Im vorliegenden Fall erschien diese Vorgehensweise aus folgenden Gründen zu pessimistisch: Das zweite Auffahren wird sicherlich vom Schichtleiter überwacht werden. Dem Operator ist bekannt, daß die erste Auslösung von YZ60 durch zu schnelles Auffahren der Ventile verursacht worden war, er wird daher entsprechend vorsichtig die Ventile öffnen. Deshalb erschien die durchgeführte Bewertung gerechtfertigt.

L 562 OP RX10/20C — Kein Abfahren mittels Notstandssystem innerhalb von 30 Minuten nach Störfalleintritt (kleines Leck in einer Hauptkühlmittelleitung)
$p = 1$

Bei diesem Störfall steht nur wenig Zeit für das Einleiten des Abfahrens zur Verfügung. Um das Notstandssystem für das Abfahren einsetzen zu können, ist laut Betriebshandbuch notwendig, daß zuerst der Block A so weit abgefahren ist, daß dort die Nachwärmeabfuhr durch das Not- und Nachkühlsystem erfolgt. Dazu werden aber 2 bis 3 Stunden benötigt. Ein Abfahren über das Notstandssystem wird daher nicht berücksichtigt.

L 582 OP RA11/12 — Kein Einleiten des Abfahrens (kein AUF-Befehl von Hand für FD-Umleitventile bzw. für Abblase-Absperrschieber und Regelventile) innerhalb von ca. 30 Minuten nach Störfalleintritt (kleines Leck in einer Hauptkühlmittelleitung)
$p_{50} = 10^{-4}/K = 15$

Das Abfahren soll, entsprechend den Anweisungen im Betriebshandbuch, spätestens 30 Minuten nach Störfalleintritt eingeleitet

werden. Die Notwendigkeit des Abfahrens ist aufgrund verschiedener Meldungen für den Schichtleiter und die beiden Reaktorfahrer ersichtlich, daher wird eine entsprechende personelle Redundanz unterstellt. Bei Fehlhandlungen ist aufgrund einer Reihe von Anzeigen eine Fehlerentdeckung möglich. Die Bewertung wird in Anlehnung an WASH-1400 durchgeführt. Dort wird eine fehlerhafte Operatorhandlung ca. 30 Minuten nach Störfalleintritt mit $p_{50} = 10^{-1}$ und der Fehlerentdeckungsfaktor (recovery factor) pro Operator mit 0,5 bewertet. Unter der Beachtung der personellen Redundanz ergibt sich der obige Wert.

L 583 OP RA11/12C — Abfahren von Hand mit falschem Abfahrgradienten innerhalb von ca. 30 Minuten nach Störfalleintritt
$p_{50} = 10^{-2}/K = 5$

Bei diesem Störfall steht nur wenig Zeit zur Verfügung, deshalb wird eine relativ hohe Streßbelastung des Wartenpersonals erwartet und kein Fehlerentdeckungsfaktor berücksichtigt. Ein Reaktorfahrer zeichnet den Abfahrgradienten auf den Schreiberstreifen ein, die Kontrolle obliegt dem Schichtleiter (einfache personelle Redundanz).

L 615 OP TH01/10
L 616 OP TH02/20
L 617 OP TH03/30
L 618 OP TH04/40 — Keine Handumschaltung des Nachkühlstranges auf Sumpf-Umwälzbetrieb
$p_{50} = 10^{-4}/K = 5$

Die Notwendigkeit der Maßnahme ist dem Bedienungspersonal bekannt, die Maßnahme muß frühestens 2 Stunden nach Störfalleintritt ergriffen werden. Es wird eine einfache personelle Redundanz angesetzt (Durchführung der Maßnahme von einem Reaktorfahrer, Kontrolle durch den Schichtleiter). Damit ergibt sich $p_{50} = 10^{-4}/K = 5$.

L 620 OP RA11/12 — Kein Auffahren der Abblase-Absperrschieber von Hand und vor Ort innerhalb von 30 Minuten nach Störfalleintritt
$p = 1$

Prinzipiell besteht zwar die Möglichkeit, die Abblase-Absperrschieber bei Versagen der Ansteuerung von der Warte aus auch von Hand und vor Ort aufzufahren. Hierfür besteht aber keinerlei schriftliche Anweisung, daher wird dieser Handeingriff als ungeplant bewertet.

L 724 OP RA1-4 — Keine Betätigung von Hand und vor Ort der Steuerarmaturen zum Öffnen der FD-Schieber
$p = 1$

Die Begründung, diese Handmaßnahme als ungeplant zu bewerten, entspricht der Bewertung des Handeingriffs L 620.

L 741 OP RA1-4 — Keine Wiederinbetriebnahme der Frischdampf-Umleitstation nach Auslösung von YZ60
$p_{50} = 10^{-2}/K = 3$

Die Verriegelung der Frischdampf-Umleiteinrichtung und der Abblasestation bei Auslösung von YZ60 erfolgt unterschiedlich. Während sich die Abblasestation 15 Minuten nach Auslösung von YZ60 wieder von der Warte aus öffnen läßt, müssen für das Auffahren der Frischdampf-Umleiteinrichtung nach ca. 17 Minuten erst die Auslöserelais des Signals YZ60 zurückgesetzt werden. Die Bedienungsmannschaft hat zwar die Anweisung, nach Möglichkeit mit der Frischdampf-Umleiteinrichtung abzufahren, jedoch besteht eine gewisse Wahrscheinlichkeit, daß nach einem Auslösen von YZ60 und nach erfolgreichem weiteren Abfahren mit der Frischdampf-Abblaseeinrichtung die Frischdampf-Umleiteinrichtung nicht mehr in Betrieb genommen wird. Diese Wahrscheinlichkeit wird zu $p_{50} = 10^{-2}/K = 3$ abgeschätzt.

L 742 OP TH1-4 — Kein Handeingriff zur Verhinderung der Rückströmung in den Flutbehälter
$p_{50} = 10^{-2}/K = 5$

Bei einem großen Leck werden ca. 20 bis 30 Minuten nach Störfalleintritt die Nachkühlpumpen vom Ansaugen aus den Flutbehältern auf Sumpf-Umwälzbetrieb geschaltet. Der aufgrund einer Rückströmung wieder steigende Wasserstand in den Flutbehältern

hebt das Anregekriterium für den Sumpfbetrieb auf, so daß wieder Flutbetrieb gefahren wird. Dies wird sich bis zum eventuellen Ausfall der von den Reaktorschutzsignalen angesteuerten Armaturen wiederholen.

Es wird erwartet, daß der Operator den wieder steigenden Flutbehälterwasserstand und das wiederholte Anstehen der Flutsignale erkennt und Gegenmaßnahmen veranlaßt. Für das Erkennen der Notwendigkeit eines Handeingriffs wird personelle Redundanz in Form eines Reaktorfahrers und des Schichtleiters angesetzt. Nach WASH-1400 sind Handeingriffe ca. 20 bis 30 Minuten nach Störfalleintritt mit $p_{50} = 10^{-1}/K = 3$ zu bewerten. Die Berücksichtigung der personellen Redundanz führt zu einem Wert von $p_{50} = 10^{-2}/K = 5$.

Bei mittleren und kleinen Lecks ist diese Bewertung etwas pessimistisch, da die Umschaltung auf Sumpf-Umwälzbetrieb später erfolgt und die Rückströmung aufgrund der niedrigeren Druckverhältnisse langsamer verläuft. Das erneute Ansprechen der Grenzwerte des Flutbehälter-Wasserstandes wird in diesen Fällen bis ca. 2 Stunden nach Störfalleintritt auftreten, so daß für Handmaßnahmen bereits niedrigere Streßbelastungen zu erwarten sind.

6.1.5 Ergebnisse

6.1.5.1 Großes und mittleres Leck

Beim großen und mittleren Leck in einer Hauptkühlmittelleitung wird unterschieden zwischen den Systemfunktionen, die bei Anforderung durch einen entsprechenden Kühlmittelverluststörfall verfügbar sein müssen, und der LANGZEIT-NOTNACHKÜHLUNG.

Die Nichtverfügbarkeit der Systemfunktionen bei Anforderung ergibt sich aus den Fehlerbaumrechnungen. Für das "große Leck" beträgt der Erwartungswert der Nichtverfügbarkeit

$$\bar{m} = 1{,}5 \cdot 10^{-3}$$

und für das "mittlere Leck"

$$\bar{m} = 2{,}1 \cdot 10^{-3}$$

Unter Berücksichtigung der Unsicherheiten der Komponentendaten erhält man als Medianwerte $1{,}2 \cdot 10^{-3}$ bzw. $1{,}7 \cdot 10^{-3}$ sowie in beiden Fällen einen Streufaktor 3.

Im folgenden wird auf die Nichtverfügbarkeiten der einzelnen Systemfunktionen eingegangen, wie sie sich aus den Fehlerbäumen ergeben (Bild F2, 6-3, und -4). Anschließend wird erläutert, wie sich aus den Fehlerbäumen die Wahrscheinlichkeiten für die einzelnen Ereignisabläufe (Bild F2, 6-5 und -6) errechnen. Die Nichtverfügbarkeit der Reaktorschnellabschaltung wird in Kapitel 8 behandelt.

Für beide Störfälle wird die Nichtverfügbarkeit der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE durch CMA bestimmt und beträgt $3 \cdot 10^{-5}$. Den wesentlichen Beitrag hierzu liefern die CMA der Meßkanalgruppen der Kühlmitteldruck- und der Druckhalter-Wasserstandsmessung aufgrund menschlicher Fehlhandlungen (Abschnitt 6.1.2.4.2).

Entsprechend den Fehlerbäumen ergibt sich für die HD-EINSPEISUNGEN eine Nichtverfügbarkeit von $1{,}2 \cdot 10^{-3}$. Es besteht die Möglichkeit, daß die Grenzwerte der Kühlmitteldruckmessung die ND-EINSPEISUNGEN bei zu hohen Drücken auslösen. Dadurch werden die HD-EINSPEISUNGEN zu früh abgeschaltet. Die Wahrscheinlichkeit hierfür beträgt $4 \cdot 10^{-4}$. Ein weiterer wesentlicher Beitrag von $4 \cdot 10^{-4}$ zur Nichtverfügbarkeit der HD-EINSPEISUNGEN resultiert aus dem Ausfall des Dreiwegeventils an der gebrochenen Hauptkühlmittelleitung.

Die Nichtverfügbarkeit der DRUCKSPEICHER-EINSPEISUNGEN ergibt sich für das große Leck mit $7 \cdot 10^{-4}$ und für das mittlere Leck mit $2 \cdot 10^{-4}$. Der Unterschied zwischen diesen beiden Werten resultiert aus den unterschiedlichen Mindestanforderungen beim großen und beim mittleren Leck.

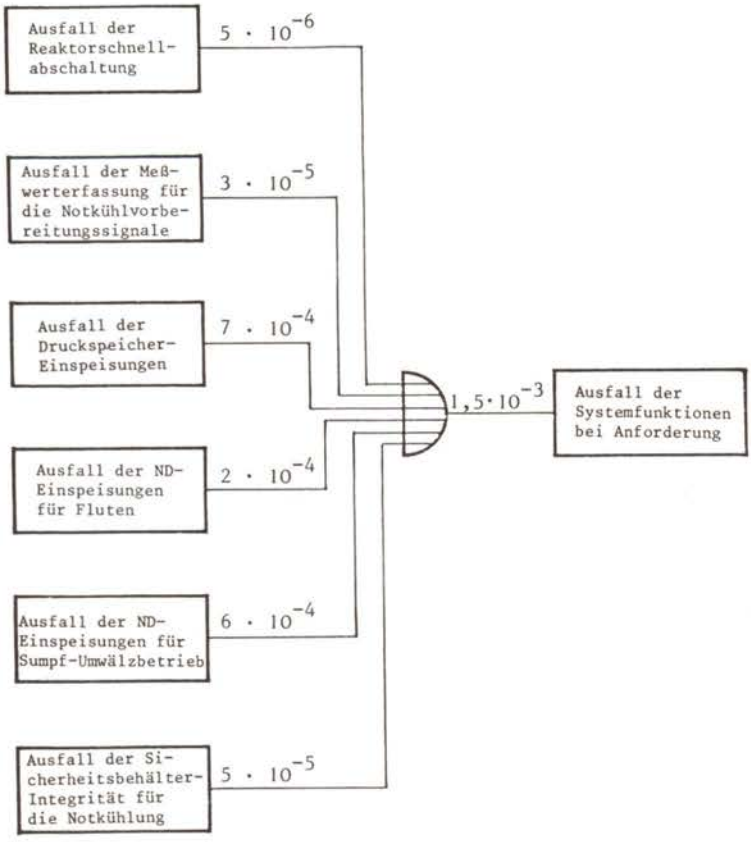


Bild F2, 6-3:

Mittlere Nichtverfügbarkeit der Systemfunktionen bei Anforderung durch ein "großes Leck"

Die Nichtverfügbarkeit der ND-EINSPEISUNGEN FÜR FLUTEN errechnet sich bei beiden Lecks zu $2 \cdot 10^{-4}$. Für die Nichtverfügbarkeit der ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB erhält man aufgrund der Fehlerbäume eine Nichtverfügbarkeit von $6 \cdot 10^{-4}$. Zu diesem Wert tragen Funktionselementausfälle nicht unerheblich bei, die bereits zum Ausfall der ND-EINSPEISUNGEN FÜR FLUTEN führen (z.B. der Ausfall der Nachkühlpumpen). Der Ausfall der Sumpfsignale infolge von CMA trägt mit $2{,}3 \cdot 10^{-4}$ bei.

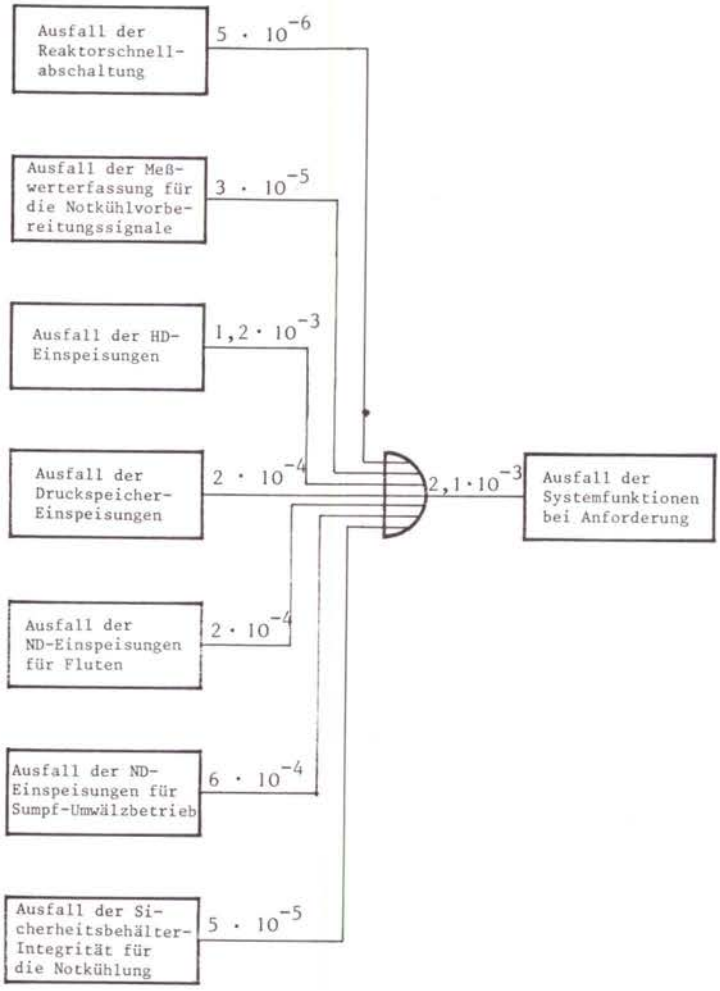


Bild F2, 6-4:
Mittlere Nichtverfügbarkeit der Systemfunktionen bei Anforderung durch ein "mittleres Leck"

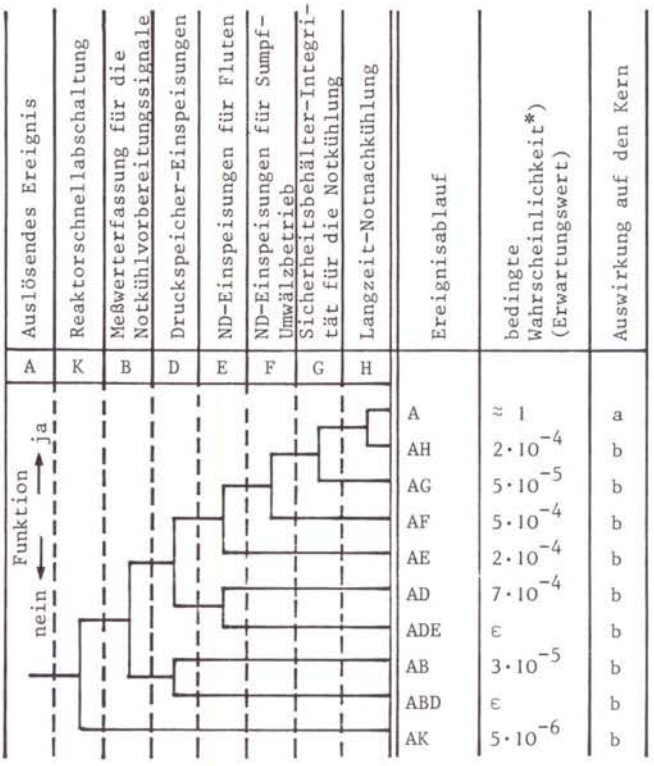
Für das Versagen der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOT-KÜHLUNG ergibt sich eine Wahrscheinlichkeit von $5 \cdot 10^{-5}$. Den Hauptbeitrag liefert das Versagen von Schweißnähten.

Die Ausfallwahrscheinlichkeit von $2 \cdot 10^{-4}$ für die LANGZEIT-NOT-NACHKÜHLUNG wird durch CMA bestimmt (Median $7 \cdot 10^{-5}$, Streufaktor 13).

Die Summe der Nichtverfügbarkeiten der einzelnen Systemfunktionen ist größer als die Nichtverfügbarkeit des Gesamtsystems. Der Grund dafür ist, daß bei unterschiedlichen Systemfunktionen teilweise gemeinsame Komponenten vorhanden sind. So führt zum Beispiel der Ausfall eines Stranges des nuklearen Zwischenkühlkreises zum Ausfall des entsprechenden Stranges der HD-EINSPEISUNGEN, der ND-EINSPEISUNGEN FÜR FLUTEN und der ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB. Die gemeinsamen Komponenten der einzelnen Systemfunktionen sind bei der Berechnung der Wahrscheinlichkeiten der einzelnen Ereignisabläufe entsprechend zu berücksichtigen. Im folgenden wird auf die Ermittlung der bedingten Wahrscheinlichkeiten der einzelnen Ereignisabläufe für das große Leck (Bild F2, 6-5) und das mittlere Leck (Bild F2, 6-6) eingegangen. Die Wahrscheinlichkeiten werden unter der Bedingung ermittelt, daß das auslösende Ereignis eingetreten ist. Mit ε werden in den Ereignisablaufdiagrammen vernachlässigbar kleine Wahrscheinlichkeiten bezeichnet (Hauptband, Abschnitt 5.2.1.2 und Fachband 1). Die Häufigkeiten der einzelnen Ereignisabläufe ergeben sich durch Multiplikation mit der Häufigkeit des auslösenden Ereignisses.

Die bedingte Wahrscheinlichkeit für den Ereignisablauf AK (großes Leck) bzw. S_1K (mittleres Leck) entspricht der Nichtverfügbarkeit der REAKTORSCHNELLABSCHALTUNG von $5 \cdot 10^{-6}$ (Kapitel 8).

Die MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE kann unabhängig von den anderen angeforderten Systemfunktionen betrachtet werden. Dadurch erhält man als bedingte Wahrscheinlichkeit für den Ereignisablauf AB bzw. S_1B die Nichtverfügbarkeit der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE. Die DRUCKSPEICHER-EINSPEISUNGEN sind unabhängig von der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE, wodurch sich für die Ereignisabläufe ABD und S_1BD eine vernachlässigbare Wahrscheinlichkeit ergibt.



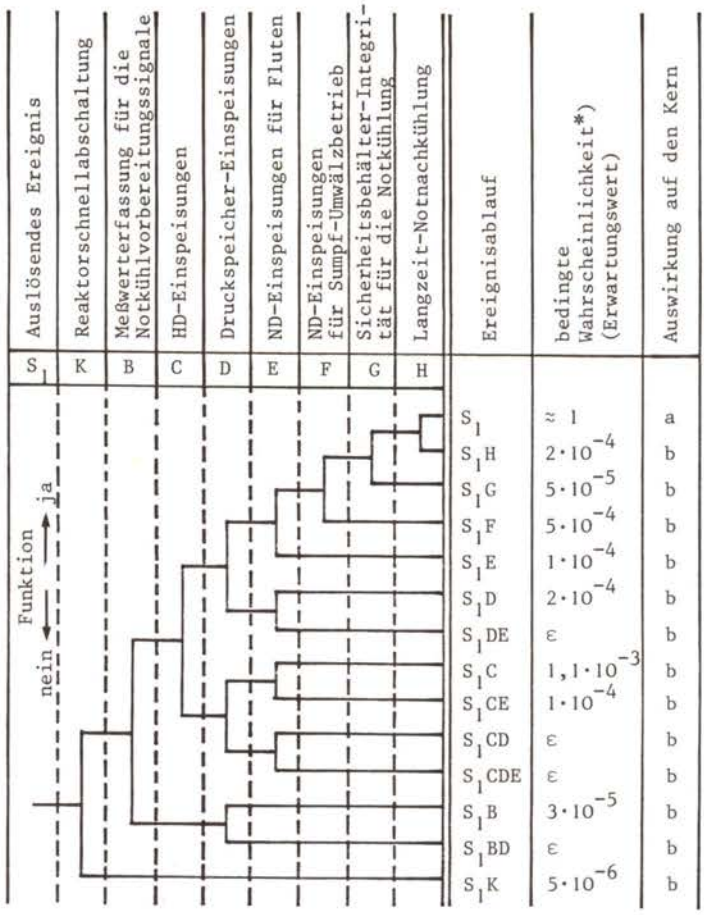
a kein Kernschmelzen
b Kernschmelzen

*) Wahrscheinlichkeit der einzelnen Ereignisabläufe unter der Bedingung, daß das auslösende Ereignis eingetreten ist.
Die Häufigkeit der einzelnen Ereignisabläufe ergibt sich durch Multiplikation mit der Häufigkeit h des auslösenden Ereignisses.

$$h(A) = 2{,}7 \cdot 10^{-4}/a \text{ (Erwartungswert)}$$

Bild F2, 6-5:

Ereignisablaufdiagramm "großes Leck"



a kein Kernschmelzen
b Kernschmelzen

*) Wahrscheinlichkeit der einzelnen Ereignisabläufe unter der Bedingung, daß das auslösende Ereignis eingetreten ist.
Die Häufigkeit der einzelnen Ereignisabläufe ergibt sich durch Multiplikation mit der Häufigkeit h des auslösenden Ereignisses.

$$h(S_1) = 8 \cdot 10^{-4}/a \text{ (Erwartungswert)}$$

Bild F2, 6-6:

Ereignisablaufdiagramm "mittleres Leck"

Die Wahrscheinlichkeit für den gemeinsamen Ausfall der HD-EINSPEISUNGEN und der DRUCKSPEICHER-EINSPEISUNGEN ist ebenfalls vernachlässigbar. D.h., die Wahrscheinlichkeiten für die Ereignisabläufe S_1CD und S_1CDE sind vernachlässigbar klein. Die Summe der bedingten Wahrscheinlichkeiten der Ereignisabläufe S_1C und S_1CE entspricht der Nichtverfügbarkeit der HD-EINSPEISUNGEN. Die bedingte Wahrscheinlichkeit für den Ereignisablauf S_1CE ergibt sich aus der logischen UND-Verknüpfung folgender Eingänge in den Gesamtfehlerbaum:

- Ausfall der HD-Einspeisungen und
- Ausfall der ND-Einspeisungen für Fluten.

Die Wahrscheinlichkeit für den gemeinsamen Ausfall der DRUCKSPEICHER-EINSPEISUNGEN und der ND-EINSPEISUNGEN FÜR FLUTEN ist vernachlässigbar, wodurch sich für die Ereignisabläufe ADE und S_1DE vernachlässigbare bedingte Wahrscheinlichkeiten ergeben. Die bedingten Wahrscheinlichkeiten der Ereignisabläufe AD bzw. S_1D entsprechen den Nichtverfügbarkeiten der Druckspeicher-Einspeisungen.

Für den Ereignisablauf AE entspricht die bedingte Wahrscheinlichkeit der Nichtverfügbarkeit der ND-EINSPEISUNG FÜR FLUTEN. Die Wahrscheinlichkeit für den Ausfall der ND-EINSPEISUNG FÜR FLUTEN unter der Bedingung, daß sowohl die HD-EINSPEISUNGEN als auch die DRUCKSPEICHER-EINSPEISUNGEN funktionieren (Ereignisablauf S_1E), erhält man als Differenz zwischen den ODER-Verknüpfungen A und B von Eingängen des Gesamtfehlerbaums.

- Verknüpfung A:
  Ausfall der HD-EINSPEISUNGEN
  Ausfall der DRUCKSPEICHER-EINSPEISUNGEN
  Ausfall der ND-EINSPEISUNGEN FÜR FLUTEN
- Verknüpfung B:
  Ausfall der HD-EINSPEISUNGEN
  Ausfall der DRUCKSPEICHER-EINSPEISUNGEN

Beim mittleren Leck erhält man die Wahrscheinlichkeit für den Ausfall der ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB unter der Bedingung, daß sowohl die HD-EINSPEISUNGEN als auch die DRUCK-

SPEICHER-EINSPEISUNGEN sowie die ND-EINSPEISUNGEN FÜR FLUTEN funktionieren (Ereignisablauf S_1F), indem man von der Nichtverfügbarkeit des Gesamtsystems die Nichtverfügbarkeit der ODER-Verknüpfung aller Eingänge des Gesamtfehlerbaums außer dem Ausfall der ND-EINSPEISUNG FÜR SUMPF-UMWÄLZBETRIEB subtrahiert. Analog ergibt sich die bedingte Wahrscheinlichkeit für den Ereignisablauf AF.

Die bedingte Wahrscheinlichkeit für den Ereignisablauf AG bzw. S_1G entspricht der Versagenswahrscheinlichkeit der SICHERHEITS-BEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG.

Die Ausfallwahrscheinlichkeit der LANGZEIT-NOTNACHKÜHLUNG entspricht der bedingten Wahrscheinlichkeit für den Ereignisablauf AH bzw. S_1H.

Die Versagenswahrscheinlichkeit der für die Beherrschung des großen bzw. mittleren Lecks erforderlichen Systemfunktionen setzt sich aus der Nichtverfügbarkeit der bei Störfalleintritt notwendigen Systemfunktionen und der Ausfallwahrscheinlichkeit der LANGZEIT-NOTNACHKÜHLUNG zusammen. Dadurch ergibt sich für das große Leck eine Versagenswahrscheinlichkeit von $1{,}7 \cdot 10^{-3}$ und für das mittlere Leck von $2{,}3 \cdot 10^{-3}$.

Der Anteil von "common mode"-Ausfällen der Hardware am Ergebnis beträgt beim großen Leck 15 %, beim mittleren Leck 11 %. Zu der Versagenswahrscheinlichkeit aufgrund von "common mode"-Ausfällen der Hardware trägt die LANGZEIT-NOTNACHKÜHLUNG mit $2 \cdot 10^{-4}$ bei und die Sumpfsignale mit einem Anteil von $5 \cdot 10^{-5}$.

Beim großen Leck erhält man einen Beitrag zum Ergebnis von 12 % und beim mittleren Leck einen Beitrag von 27 % aufgrund menschlichen Fehlverhaltens. Hierzu trägt bei beiden Störfällen ein Anteil von $1{,}8 \cdot 10^{-4}$ an der Nichtverfügbarkeit der Sumpfsignale sowie an der Nichtverfügbarkeit der Meßwerterfassung der Notkühlvorbereitungssignale bei. Beim mittleren Leck ist zusätzlich ein zu frühes Ansprechen der ND-Einspeisesignale zu berücksichtigen.

6.1.5.2 Kleines Leck in einer Hauptkühlmittelleitung

Für die mittlere Nichtverfügbarkeit der Systemfunktionen, die bei einem kleinen Leck in einer Hauptkühlmittelleitung erforderlich sind, ergibt sich aus den Fehlerbaumrechnungen der Erwartungswert

$$\bar{m} = 2{,}1 \cdot 10^{-2}$$

Unter Berücksichtigung der Unsicherheiten der Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung für die einzelnen Komponenten erhält man einen Medianwert von $1{,}5 \cdot 10^{-2}$ und einen Streufaktor von 4.

Das Ergebnis wird im wesentlichen von der Handmaßnahme "Abfahren mit 100 °C/h" mit der Ausfallwahrscheinlichkeit $\bar{p} = 1{,}6 \cdot 10^{-2}$ bestimmt. Die Handmaßnahmen insgesamt, ohne Beteiligung von Hardware-Ausfällen, jedoch einschließlich CMA durch Fehlkalibrierungen, tragen mit $1{,}8 \cdot 10^{-2}$ etwa 85 % zum Ergebnis bei. Unabhängige Hardware-Ausfälle mit einer Wahrscheinlichkeit von $2{,}7 \cdot 10^{-3}$ machen dagegen nur etwa 13 % aus. Darin sind auch Ausfälle aufgrund von Instandhaltungsmaßnahmen enthalten (2 bis 3 % vom Gesamtergebnis). Die CMA der Hardware sind mit knapp 1 % am Ergebnis nur unerheblich beteiligt.

Die mittleren Nichtverfügbarkeiten der einzelnen Systemfunktionen sind in Bild F2, 6-7 dargestellt. Es zeigt sich, daß die Summen der Einzelwerte etwa dem Gesamtwert entsprechen, das heißt, die vorhandenen Abhängigkeiten der Systeme untereinander (z.B. durch Reaktorschutzsignale, Energieversorgung, Kühlketten usw.) spielen zahlenmäßig keine Rolle.

Es folgt nun eine Diskussion der Beiträge der einzelnen Systemfunktionen, wobei zum Ausfall der REAKTORSCHNELLABSCHALTUNG auf Kapitel 8 verwiesen wird.

Der Hauptbeitrag zur Wahrscheinlichkeit des nicht beherrschten kleinen Lecks in einer Hauptkühlmittelleitung kommt vom Ausfall

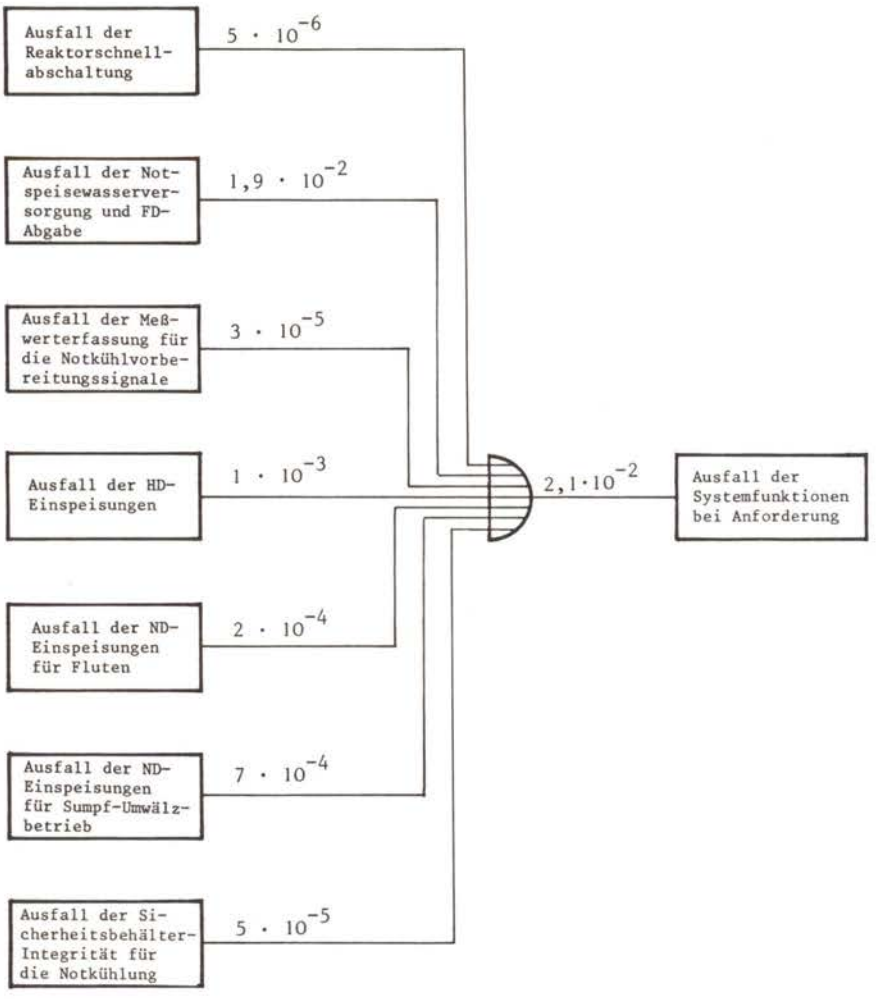


Bild F2, 6-7:
Mittlere Nichtverfügbarkeit der Systemfunktionen bei Anforderung durch ein "kleines Leck in einer Hauptkühlmittelleitung"

der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE mit $1,9 \cdot 10^{-2}$. Davon liefert mit $1,6 \cdot 10^{-2}$ der Ausfall der bereits genannten Handmaßnahme "Abfahren mit 100 °C/h" den größten Anteil. Bei der Bewertung wurde davon ausgegangen, daß das erforderliche Ein-

zeichnen des Gradienten von 100 °C/h innerhalb von etwa 30 Minuten nach Störfalleintritt vorgenommen wird (Abschnitt 6.1.4).

Weitere Anteile der Nichtverfügbarkeit aufgrund von Handeingriffen sind $6 \cdot 10^{-4}$ für dreimaliges zu schnelles Auffahren der Frischdampf-Umleiteinrichtung bzw. der Abblaseregelventile und $4 \cdot 10^{-4}$ für Nichteinleitung des Abfahrens innerhalb von etwa 30 Minuten nach Störfalleintritt. Der restliche Anteil von ca. $2 \cdot 10^{-3}$ geht im wesentlichen auf Hardware-Ausfälle des Notspeisewasser- und Frischdampfsystems zurück. Da beim kleinen Leck in einer Hauptkühlmittelleitung weder das Hauptspeisewassersystem noch das Notstandssystem zur Verfügung stehen (Abschnitt 6.1.2.1.3), liegt ein Systemausfall bei Versagen von 3v4 Notspeisewassersträngen vor.

Zum Ausfall der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGS-SIGNALE gilt auch das im Abschnitt 6.1.5.1 Gesagte. Die ermittelte Nichtverfügbarkeit von $3 \cdot 10^{-5}$ liefert keinen signifikanten Beitrag zur Wahrscheinlichkeit des nicht beherrschten Störfalls.

Mit einer Wahrscheinlichkeit von $1{,}1 \cdot 10^{-3}$, das sind etwa 5 % des Gesamtergebnisses, trägt der Ausfall der HD-EINSPEISUNGEN zum nicht beherrschten Störfall bei. Wie beim mittleren Leck ist ein zu frühes Umschalten auf die ND-EINSPEISUNGEN und damit ein Abschalten der HD-EINSPEISUNGEN möglich. Die Wahrscheinlichkeit dafür beträgt $4 \cdot 10^{-4}$ und wird durch CMA der Meßwerterfassung zur Bildung der ND-Einspeisesignale bestimmt, die ein zu frühes Umschalten auf die ND-EINSPEISUNGEN FÜR FLUTEN verursachen. Das Versagen der HD-EINSPEISUNGEN aufgrund unabhängiger Hardware-Ausfälle in 3v4 Strängen führt zu einer Nichtverfügbarkeit von etwa $7 \cdot 10^{-4}$.

Die Nichtverfügbarkeit der ND-EINSPEISUNGEN FÜR FLUTEN beträgt $2 \cdot 10^{-4}$. Der Wert wird im wesentlichen von unabhängigen Hardware-Ausfällen in 3v4 heißen Einspeisesträngen bestimmt.

Für ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB wurde eine Nichtverfügbarkeit von $7 \cdot 10^{-4}$ ermittelt. Etwa $5 \cdot 10^{-4}$ resultieren

aus unabhängigen Hardware-Ausfällen in 3v4 Einspeisesträngen. In starkem Maße sind wieder Ausfälle beteiligt, die sowohl zum Versagen der ND-EINSPEISUNGEN FÜR FLUTEN als auch der HD-EINSPEISUNGEN führen. Der Ausfall der Sumpfsignale durch CMA beträgt wie bei den großen und mittleren Lecks $2 \cdot 10^{-4}$.

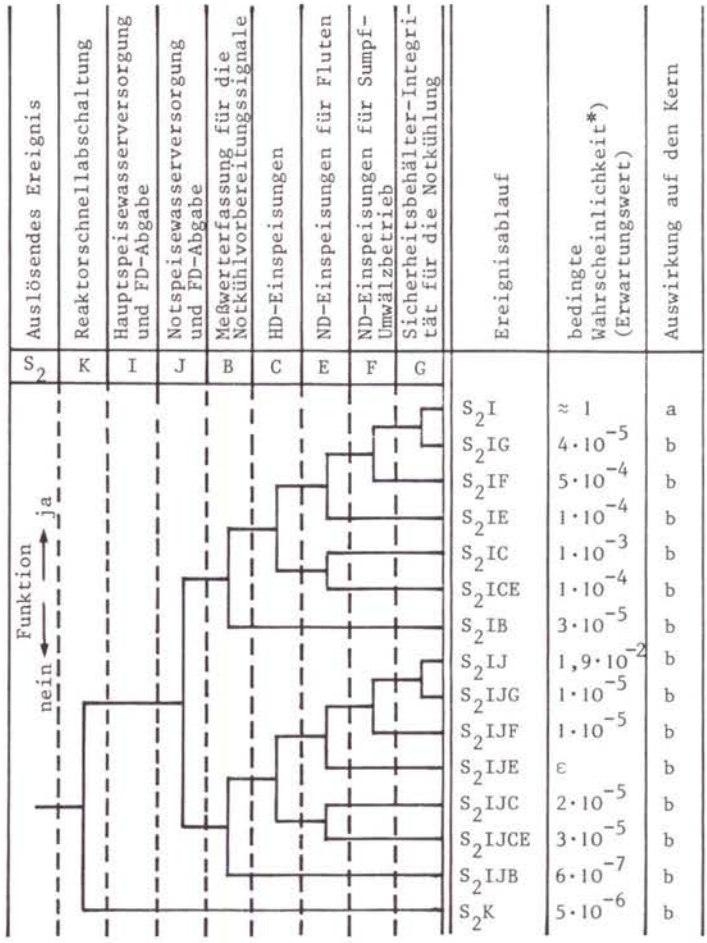
Entsprechend dem großen und mittleren Leck wird das Versagen der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG mit der Wahrscheinlichkeit von $5 \cdot 10^{-5}$ durch das Versagen der Schweißnähte bestimmt.

In Bild F2, 6-8 sind die bedingten Wahrscheinlichkeiten (Erwartungswerte) der einzelnen Ereignisabläufe beim kleinen Leck in einer Hauptkühlmittelleitung dargestellt. Die Wahrscheinlichkeiten sind unter der Bedingung ermittelt, daß das auslösende Ereignis, nämlich das kleine Leck in einer Hauptkühlmittelleitung, eingetreten ist. Es wird im folgenden auf die einzelnen Ereignisabläufe eingegangen. Dabei ist zu beachten, daß der Ausfall der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG G, der auch zum Ausfall der Systemfunktionen zur Notkühlung führt, in den entsprechenden Systemfunktionen C, E und F nicht enthalten ist. Bei allen Ereignisabläufen wird zudem der Ausfall der HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE I zugrunde gelegt.

Die bedingte Wahrscheinlichkeit für den Ereignisablauf S_2K entspricht der Nichtverfügbarkeit der REAKTORSCHNELLABSCHALTUNG.

Der Ausfall der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE kann als unabhängig vom Ausfall der anderen Systemfunktionen, insbesondere von der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE, betrachtet werden. Als bedingte Wahrscheinlichkeit für den Ereignisablauf S_2IJB erhält man dabei aus dem Produkt der Nichtverfügbarkeiten der beiden Systemfunktionen B und J den Wert $6 \cdot 10^{-7}$.

Beim Ereignisablauf S_2IJCE mit $3 \cdot 10^{-5}$ sind Abhängigkeiten zwischen den Systemfunktionen J, C und E vor allem bei gleichzeitigem Vorliegen des Notstromfalls gegeben: Ausfall von 10-kV-Notstromschienen oder CMA der Notstromdiesel. Weitere Abhängigkei-



*) Wahrscheinlichkeit der einzelnen Ereignisabläufe unter der Bedingung, daß das auslösende Ereignis eingetreten ist.
Die Häufigkeit der einzelnen Ereignisabläufe ergibt sich durch Multiplikation mit der Häufigkeit h des auslösenden Ereignisses.

$$h(S_2) = 2{,}7 \cdot 10^{-3}/a \text{ (Erwartungswert)}$$

Bild F2, 6-8:

Ereignisablaufdiagramm "kleines Leck in einer Hauptkühlmittelleitung"

ten bestehen durch die Reaktorschutzsignale (Kurzschlüsse bei Ausgabe der Reaktorschutzsignale zur Notkühlung) und durch den nuklearen Zwischenkühlkreis.

Der Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE und der HD-EINSPEISUNGEN bei funktionierenden ND-EINSPEISUNGEN FÜR FLUTEN (Ereignisablauf S_2IJC) ergibt eine bedingte Wahrscheinlichkeit von $2 \cdot 10^{-5}$. Hier spielen die Handmaßnahmen zum Abfahren eine wesentliche Rolle, vor allem in Verbindung mit dem Ausfall der HD-Einspeisesignale durch zu frühes Umschalten auf ND-Einspeisungen.

Der Ereignisablauf S_2IJE wird $< 10^{-5}$ abgeschätzt. Dies ergibt sich aus der Differenz der Wahrscheinlichkeiten für die UND-Verknüpfungen der Systemfunktionen J und E einerseits und J, C und E andererseits.

Zum Ereignisablauf S_2IJF trägt wesentlich der CMA der Sumpfsignale in Verbindung mit dem Ausfall von Handmaßnahmen, die beim Abfahren erforderlich sind, bei. Insgesamt ergibt sich für diesen Ereignisablauf eine bedingte Wahrscheinlichkeit von $1 \cdot 10^{-5}$.

Der Bruch von Schweißnähten, der zu einem Versagen der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG führt, bestimmt den Ereignisablauf S_2IJG. Die bedingte Wahrscheinlichkeit dafür beträgt $1 \cdot 10^{-5}$. Da als Folge dieses Ausfalls die Zwischenkühlpumpen (Aufstellung im Ringraum) und damit auch die Notspeisestränge 23 RL06 und 24 RL07 ausfallen, ist der Pfad S_2IJG erfüllt, wenn zusätzlich einer der beiden Notspeisestränge 21 RL04 oder 22 RL05 ausfällt. Die Wahrscheinlichkeit für einen solchen Ausfall beträgt 0,2.

Die bedingte Wahrscheinlichkeit $1{,}9 \cdot 10^{-2}$ für den Ereignisablauf S_2IJ entspricht der Nichtverfügbarkeit der Systemfunktion NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE. Dies folgt daraus, daß die bisher ermittelten Wahrscheinlichkeiten für die Pfade S_2IJB bis S_2IJG gegenüber dem Ausfall von J zu vernachlässigen sind.

Bei den folgenden Ereignisabläufen liegt kein Ausfall der Systemfunktion NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE vor.

Die bedingte Wahrscheinlichkeit für S_2ICE beträgt $1 \cdot 10^{-4}$. Dieser Wert der Nichtverfügbarkeit für Ausfall der HD-EINSPEISUNGEN und der ND-EINSPEISUNGEN FÜR FLUTEN ist wesentlich höher als das Produkt der entsprechenden Einzel-Nichtverfügbarkeiten, da zwischen den für die HD- und die ND-EINSPEISUNGEN erforderlichen Systemen starke Abhängigkeiten bestehen (Armaturen in den Einspeiseleitungen, Kühlkette, Reaktorschutzsignale).

Der Ereignisablauf S_2IC enthält nur den Ausfall der HD-EINSPEISUNGEN, aber keine weiteren Systemfunktionen. Für die bedingte Wahrscheinlichkeit des Ereignisablaufes ergibt sich näherungsweise der Wert der Nichtverfügbarkeit der HD-EINSPEISUNGEN, wobei der CMA für zu frühes Umschalten auf die ND-EINSPEISUNGEN mit $4 \cdot 10^{-4}$ einen wesentlichen Anteil hat.

Für den Ereignisablauf S_2IE mit Ausfall der ND-EINSPEISUNGEN FÜR FLUTEN bei sonst funktionierenden Systemfunktionen wird mit $1 \cdot 10^{-4}$ ein niedrigerer Wert ermittelt, als er der Nichtverfügbarkeit der Systemfunktion E entspricht. Hier spielen die Ausfallkombinationen eine Rolle, die gleichzeitig zum Versagen von HD-EINSPEISUNGEN und ND-EINSPEISUNGEN FÜR FLUTEN führen (Ereignisablauf S_2ICE) und damit in diesem Ereignisablauf nicht enthalten sind.

Abhängigkeiten bestehen auch zwischen den ND-EINSPEISUNGEN FÜR FLUTEN und den ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB. Die bedingte Wahrscheinlichkeit für den Ereignisablauf S_2IF ist daher geringer als die Nichtverfügbarkeit für Sumpf-Umwälzbetrieb. Es fallen die Ausfallkombinationen weg, die gleichzeitig zum Versagen der Systemfunktionen ND-EINSPEISUNGEN FÜR FLUTEN und ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB führen. Für S_2IF beträgt die bedingte Wahrscheinlichkeit $5 \cdot 10^{-4}$. Der CMA der Sumpfsignale mit $2 \cdot 10^{-4}$ hat hierbei einen starken Anteil.

Aus dem Ereignisablauf S_2IJG ergibt sich, daß bei Ausfall der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG G die Wahr-

scheinlichkeit für den gleichzeitigen Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE etwa 0,2 beträgt (siehe oben). Die Wahrscheinlichkeit, daß kein solcher Ausfall vorliegt, beträgt daher 0,8. Die Nichtverfügbarkeit der Systemfunktion G mit 0,8 multipliziert, ergibt dann die bedingte Wahrscheinlichkeit $4 \cdot 10^{-5}$ für den Ereignisablauf S_2IG.

Bei der Berechnung der bisher diskutierten Ergebnisse wurde vorausgesetzt, daß das Ausfallverhalten der einzelnen Funktionselemente der Fehlerbäume voneinander unabhängig ist. Nach Abschnitt 3.3.5.6 lassen sich viele Abhängigkeiten zwischen gleichartigen Funktionselementen durch eine "Ausfallraten-Kopplung" beschreiben. Deren Einfluß auf die Ergebnisse wurde anhand der beiden größten Beiträge zu nicht beherrschten Störfällen, nämlich für das "kleine Leck in einer Hauptkühlmittelleitung" und den "Notstromfall" überprüft. Wie bereits erwähnt, ist der Beitrag der Hardware zum nicht beherrschten "kleinen Leck" gering, der Hauptbeitrag kommt hier vom Abfahren mit falschem Abfahrgradient: Für das Mißlingen der Handmaßnahmen wurde ein Erwartungswert von $\bar{p} = 1{,}6 \cdot 10^{-2}$ ermittelt. Dabei wurde die Durchführung der Handmaßnahme von einem Reaktorfahrer und eine davon unabhängige Kontrolle von dem Schichtleiter angesetzt. Bei einer Ausfallraten-Kopplung erhöht sich der Erwartungswert auf $2{,}4 \cdot 10^{-2}$. Im Abschnitt 3.4.1 wurde allerdings darauf hingewiesen, daß in Anlehnung an WASH-1400 nur eine grobe Ermittlung der Wahrscheinlichkeiten für menschliches Fehlverhalten möglich ist. In diesem Rahmen stimmen die beiden Erwartungswerte überein.

6.2 Zuverlässigkeitsanalyse für Lecks über eine Anschlußleitung

6.2.1 Allgemeines

Der Reaktorkühlkreislauf ist über Anschlußleitungen mit verschiedenen Systemen verbunden, die für Leistungsbetrieb, zum An- und Abfahren und bei Störfällen erforderlich sind. Dazu gehören vor allem das Not- und Nachkühlsystem mit einer Nennweite der Anschlußleitungen von 250 mm und das Volumenregelsystem mit ei-

ner Nennweite der Anschlußleitungen von 50 und 100 mm. Wichtige Komponenten dieser Systeme sind außerhalb des Sicherheitsbehälters angeordnet.

Zwar sind die Anschlußleitungen an den Reaktorkühlkreislauf mit mindestens zwei hintereinandergeschalteten Absperrarmaturen versehen, es ist aber auch eine Zuverlässigkeitsanalyse zu prüfen, mit welcher Häufigkeit ein Kühlmittelverlust über die entsprechenden Anschlußleitungen eintreten kann. Bei einem Kühlmittelverlust könnte Hauptkühlmittel außerhalb des Sicherheitsbehälters austreten und sich deshalb nicht im Gebäudesumpf sammeln. Das Wasser stünde damit für die Notkühlung nicht mehr zur Verfügung. Außerdem ist zu berücksichtigen, daß bei einem Kühlmittelverlust in den Ringraum die dort angeordneten Komponenten zur Not- und Nachkühlung in Mitleidenschaft gezogen werden können.

Zur Eingrenzung der Untersuchungen ist folgendes zu beachten:

- Ein Rohrleitungsbruch in einer Anschlußleitung, der innerhalb des Sicherheitsbehälters auftritt, ist durch die Untersuchungen zum mittleren und kleinen Leck in einer Hauptkühlmittelleitung abgedeckt (Abschnitt 6.1). Bei bestimmten Bruchlagen sind zusätzliche Absperrmaßnahmen für diese Leitungen vorhanden.

- Rohrleitungsbrüche von Anschlußleitungen, die in den Ringraum führen, aber außer Betrieb (z.B. Entwässerungsleitungen) und innerhalb des Sicherheitsbehälters doppelt abgesperrt sind, brauchen gegenüber den nachfolgend besprochenen Leitungen nicht berücksichtigt zu werden.

- Rohrleitungen des Volumenregelsystems führen im Normalbetrieb im Bereich des Ringraumes Wasser mit einer Temperatur von ca. 50 °C, so daß sich aufgrund dieses Wassers bei einem Rohrbruch kein Dampf im Ringraum bildet. Bei einem Rohrleitungsbruch auf der Druckseite der HD-Förderpumpen kann zwar die geringe Menge heißen Kühlmittels, die sich im Rekuperativ-Wärmetauscher und den angrenzenden Rohrleitungen befindet, in den Ringraum ausströmen, bei funktionierenden letzten Rückschlag-

armaturen vor dem Reaktorkühlkreislauf kann sich aber auch dann keine nennenswerte Dampfatmosphäre bilden.

Bei einem Abriß der Rohrleitung zwischen den HD-Förderpumpen und der Stahlhülle und einem Ausfall der letzten Rückschlagarmaturen könnte es hingegen zu einem solchen Druckaufbau im Ringraum kommen, daß die Stahlhülle des Sicherheitsbehälters eingebeult würde. Die möglichen Folgen wären weiter zu untersuchen.

Bei einem Ausfall der letzten Rückschlagarmaturen ist zu unterscheiden, ob der Rohrleitungsbruch im Ringraum zwischen HD-Förderpumpen und Gebäudeabschlußarmaturen oder zwischen Gebäudeabschlußarmaturen und Stahlhülle stattfindet. Bei der zuletzt genannten Möglichkeit ist für den Bruch der Rohrleitung eine sehr geringe Eintrittshäufigkeit anzusetzen, da die in Frage kommenden Rohrleitungsstücke sehr kurz sind. Bei einem Bruch zwischen HD-Förderpumpen und Gebäudeabschlußarmaturen ist zu beachten, daß nach einem Absinken des Druckhalter-Wasserstandes und des Druckes im Reaktorkühlkreislauf alle Gebäudeabschlußarmaturen automatisch zugefahren werden (Abschnitt 4.2.5). Ein Leerlaufen des Reaktorkühlkreislaufes und ein daraus resultierender Kernschmelzunfall werden damit sehr unwahrscheinlich.

Eine großräumige Überflutung des Ringraumes aufgrund eines Rohrleitungsbruches im Volumenregelsystem hat ebenfalls eine kleine Eintrittshäufigkeit. Außerdem wäre eine Flutung des Ringraumes mit etwa 300 m^3 Wasser aufgrund der baulichen Ausführung beherrschbar. Dies hätte keinen Einfluß auf die Funktion der im Ringraum angeordneten Komponenten des Not- und Nachkühlsystems und des nuklearen Zwischenkühlkreises, da die Sockelhöhe der zugehörigen Pumpen nicht erreicht wird. Bei einer Ausströmrate aus dem Leck von 70 t/h würden ca. 4 Stunden Zeit für entsprechende Handmaßnahmen zur Verfügung stehen. Dabei wird das Wartenpersonal durch mehrere Meldungen auf ein Leck im Volumenregelsystem hingewiesen (Abschnitt 4.2.5).

- Ein Verlust von Hauptkühlmittel über das Volumenregelsystem wäre auch durch eine Fehlfunktion der Druckhalter-Wasserstandsregelung denkbar, so daß das Kühlmittelinventar im Re-

- Ausfall des konventionellen Nebenkühlwassersystems

Zum Leistungsbetrieb des Kraftwerks ist das konventionelle Nebenkühlwasser erforderlich. Ausfall dieses Systems führt zur Turbinenschnellabschaltung. Da das konventionelle Nebenkühlwasser auch zur Kühlung der Maschinentransformatoren erforderlich ist, führt sein Ausfall zum Notstromfall. Die Häufigkeit für den Ausfall des konventionellen Nebenkühlwassersystems wird mit 10^{-2}/a (Median $8 \cdot 10^{-3}$/a, K = 3) abgeschätzt. Die Zeitdauer eines solchen Notstromfalls richtet sich nach der Instandsetzungszeit der ausgefallenen Komponenten im konventionellen Nebenkühlwassersystem, wird in der Mehrzahl der Fälle jedoch mehr als eine Stunde betragen.

- Turbinenschnellabschaltung

Nach einer Turbinenschnellabschaltung wird der Generatorschalter geöffnet und der Generator entregt. Öffnet der Generatorschalter nicht, treten Schäden am Generator auf, die zum Ausfall der Eigenbedarfseinspeisung aus dem Verbundnetz führen. Da mit mehreren Turbinenschnellabschaltungen pro Jahr gerechnet werden muß, ergibt sich die Häufigkeit für einen Notstromfall nach Turbinenschnellabschaltung und Versagen des Generatorschalters direkt aus der Ausfallrate des Generatorschalters mit einem Erwartungswert von $8 \cdot 10^{-3}$/a. Es wird davon ausgegangen, daß bei einem Versagen des Generatorschalters dessen Ausbau erforderlich ist; die entsprechende Zeitdauer für den Notstromfall wird mit 24 Stunden geschätzt.

Der Ausfall eines großen Kraftwerksblocks stellt für das Verbundnetz eine erhebliche Störung dar. Deshalb muß damit gerechnet werden, daß nach einer Turbinenschnellabschaltung die Übernahme der Eigenbedarfsversorgung durch das Verbundnetz nicht in allen Fällen gelingt. Dies kann bei Trennung des Netzverbundes aufgrund von Kraftwerksausfall und anschließendem Ausfall des entsprechenden Teilnetzes zutreffen. Eine andere Möglichkeit ist eine zu geringe Spannung an den Eigenbedarfsschienen. Die Häufigkeit von Turbinenschnellabschaltungen wird aufgrund der Be-

triebserfahrung mit einem Medianwert von 7/a und einem Unsicherheitsfaktor 2 abgeschätzt, die Wahrscheinlichkeit dafür, daß die Übernahme der Eigenbedarfsversorgung durch das Verbundnetz nicht gelingt, mit einem Median von $3 \cdot 10^{-3}$ und einem Unsicherheitsfaktor 3. Dadurch ergibt sich die entsprechende Häufigkeit für den Notstromfall mit $3 \cdot 10^{-2}$/a. Anhaltspunkte für die Abschätzung der Wahrscheinlichkeit $3 \cdot 10^{-3}$ sind der in WASH-1400 verwendete Wert von 10^{-3} für den Netzausfall infolge Instabilität sowie die im Genehmigungsverfahren übliche Wahrscheinlichkeit von 10^{-2}. Die Dauer des Ausfalls der Eigenbedarfsversorgung kann von einigen Sekunden (kurzzeitiger Spannungseinbruch) bis zu mehreren Stunden betragen.

Insgesamt ergibt sich für den Notstromfall eine zu erwartende Häufigkeit von 0,1/a bzw. ein Median von 0,08/a mit einem Unsicherheitsfaktor 3. Bei der Mehrzahl der Notstromfälle ist eine Versorgung der Eigenbedarfsverbraucher innerhalb kurzer Zeit (etwa einer Stunde) nicht möglich, da beim Ausfall eines Eigenbedarfstransformators oder des Generatorschalters in jedem Fall, bei den anderen Ursachen des Notstromfalls zumindest teilweise mit längeren Instandsetzungszeiten zu rechnen ist. Die Verbindungen zwischen den 10-kV-Eigenbedarfsschienen der Blöcke A und B können zur Versorgung der zur Nachwärmeabfuhr einsetzbaren Hauptspeisewasser-Pumpen nicht herangezogen werden, da die übertragbare Leistung hierzu nicht ausreicht.

7.2 Notstromfall und kleines Leck am Druckhalter beim Notstromfall

7.2.1 Annahmen und Voraussetzungen

Bei der Analyse wird davon ausgegangen, daß den einleitenden, zum Notstromfall führenden Ereignissen ein ungestörter Leistungsbetrieb vorausgeht, und zwar ein Vollastbetrieb. Weiter wird vorausgesetzt, daß der Notstromfall nicht durch eine unzulässige Überspannung in der Gleichstromversorgung für die elektronische Steuerung hervorgerufen wird. Es ist grundsätzlich möglich, daß als Folge einer Turbinenschnellabschaltung über

längere Zeit an den 10-kV-Block- und Notstromschienen eine Unterspannung von maximal 20 % der Nennspannung auftritt; dies ist jedoch kein Notstromfall und wird folglich hier nicht behandelt.

In der Mehrzahl der Notstromfälle wird die Inbetriebnahme der Eigenbedarfsversorgung zwischen 24 und 72 Stunden dauern. Über die Verbindung der Blockschienen der Blöcke A und B kann vor Ablauf dieser Zeitspanne die Eigenbedarfsanlage teilweise versorgt werden. Dauert ein Notstromfall länger als 10 Stunden, so wird davon ausgegangen, daß innerhalb dieser Zeitspanne ein Rohwasseranschluß zur Förderung von Rheinwasser oder von Fremdwasser aus Tankfahrzeugen hergestellt werden kann. Die zur Versorgung der Deionatbehälter von Block B über die Vollentsalzungsanlage von Block A notwendigen Deionat-Zubringerpumpen sind nicht notstromversorgt.

Um für die vorliegende Analyse definierte Ausgangsbedingungen zu haben, wird davon ausgegangen, daß vor Eintritt des Notstromfalls der Strang 3 des nuklearen Zwischenkühlkreislaufs, die Stränge 2 und 3 des nuklearen Nebenkühlwassersystems sowie die Teilsysteme UZ60 und UZ90 des Kaltwassersystems in Betrieb waren. Weiterhin wurde vorausgesetzt:

- Zum Zeitpunkt des Eintritts des Notstromfalls sind entsprechend dem Regelwasserstand im Speisewasserbehälter ca. 320 t an Speisewasservorrat vorhanden. In den Deionatbehältern befinden sich entsprechend dem minimalen betrieblichen Soll-Wasserstand 600 t Deionat.
- Schäden an den Dampferzeugerheizrohren liegen nicht in einem solchen Ausmaß vor, daß der Ablauf des Notstromfalls beeinflußt wird.
- Die Trennschieber in der druckseitigen Notspeisesammelleitung sind bei Eintritt des Notstromfalls geschlossen. Dies entspricht dem Anlagenzustand, der bei Durchführung der Zuverlässigkeitsanalysen vorlag. Zu einem späteren Zeitpunkt wurde die Grundstellung der Trennschieber geändert. Der Einfluß dieser Änderung auf die ermittelten Zuverlässigkeiten ist unerheblich.

- Um die Wärmeabfuhr über einen Dampferzeuger sicherzustellen, muß nicht nur dessen Versorgung mit Speisewasser gegeben sein, sondern auch der zugehörige Frischdampfdruck entweder beim Ansprechdruck der Sicherheitsventile gehalten oder geregelt abgesenkt werden.

Falls die letzte Voraussetzung infolge eines nichtschließenden Sicherheitsventils nicht erfüllt wäre, würde die entsprechende Notspeisewasser-Pumpe im Kavitationsbetrieb fördern. Bei Ansaugen von Wasser, das eine Temperatur von etwa 20 °C hat, kommt es dadurch zu einem unruhigen Lauf der Pumpe und langfristig zu einem Materialabtrag am Laufzeug. Ein solcher Betrieb der Pumpe ist für mehrere Stunden möglich. Die Pumpen des Notspeisewasser- bzw. des Notstandssystems saugen beim Notstromfall jedoch aus dem zugehörigen Speisewasserbehälter an, dessen Wasservorrat sich zunächst auf einer Temperatur von 180 °C und einem Druck von 10 bar befindet. Dieses Speisewasser entspannt sich über den defekten Strang, so daß Dampf aus dem Speisewasserbehälter in den Dampfraum des Dampferzeugers und von dort direkt zum defekten Frischdampf-Sicherheitsventil strömt. Der Wasservorrat des Speisewasserbehälters geht somit teilweise verloren. Während dieser Zeitspanne wird durch die Notspeisewasser-Pumpe ein Wasser-Dampf-Gemisch gefördert, so daß ein Folgeausfall der Pumpe nicht auszuschließen ist.

Schließt ein Frischdampf-Sicherheitsventil nicht, so wird die Versorgung des entsprechenden Dampferzeugers vom Notspeisewassersystem durch Reaktorschutzsignale automatisch unterbunden. Außerdem werden die Frischdampfleitungen voneinander getrennt. Würde es zu einem Ausfall dieser sehr zuverlässigen automatischen Maßnahmen kommen, so müßte von einem Ausfall des Notspeisewassersystems ausgegangen werden. Falls nämlich die Notspeisewasser-Pumpe, die in einen Dampferzeuger mit fälschlich offenem Frischdampf-Sicherheitsventil fördert, nicht versagt, wird langfristig in den Dampferzeuger eingespeist. Die Verdampfungstemperatur des Wassers liegt (wegen des geringen Strömungswiderstandes im FD-Sicherheitsventil) nur wenig über 100°C. Der Reaktorkühlkreislauf wird dadurch abgekühlt, bis trotz erfolgter Reaktorschnellabschaltung der Reaktor wieder kritisch wird.

Das Notspeisewasser-Regelventil für den defekten Strang wird spätestens zu diesem Zeitpunkt durch die Regelung voll aufgefahren. Hingegen sind die Notspeisewasser-Regelventile der Stränge mit intakten Frischdampf-Sicherheitsventilen geschlossen, da eine Vermischung des in den einzelnen Dampferzeugern unterschiedlich stark abgekühlten Primärkühlmittels im Reaktordruckbehälter erfolgt. In den intakten Strängen wird dann die Verdampfungstemperatur des Notspeisewassers, die dem Ansprechdruck der Frischdampf-Sicherheitsventile entspricht, nicht mehr erreicht.

Aufgrund dieses Sachverhalts ist davon auszugehen, daß bei Einspeisung in einen defekten Strang mit dem Notspeisewassersystem die bei den geringen Gegendrücken maximal möglichen Mengen gefördert werden. Diese betragen entsprechend der Pumpenkennlinien etwa 220 t/h. Bei Einspeisung aus den Deionatbehältern (Mindestwassermenge 500 t, Regelwassermenge 600 bis 680 t) ist der Wasservorrat nach etwa 2 bis 3 Stunden verbraucht. Während dieser Zeitspanne kann mit Hilfe

- des Volumenregelsystems oder
- der HD-Einspeisungen

eine Unterkritikalität des Reaktors hergestellt werden. Im Anschluß daran kann das Notstandssystem zur Notspeisewasserversorgung herangezogen werden.

Wird mit dem Notstandssystem in einen Frischdampfstrang mit nicht schließendem Sicherheitsventil eingespeist, so geht die Analyse von einem Ausfall des Notstandssystems aus. Hier ist mit einem Folgeausfall aller Pumpen des Notstandssystems zu rechnen, da zunächst aus dem Speisewasserbehälter, Block A, gefördert wird. Tritt kein Pumpenausfall ein, so kann die in den Deionatbehältern von Block A gespeicherte Wassermenge, abzüglich des zur Auffüllung des Speisewasserbehälters von Block A benötigten Deionats, zur Einspeisung über das Notstandssystem herangezogen werden. Der gesamte Wasservorrat der Deionatbehälter ist bei Betrieb von zwei Pumpen (mit je 220 t/h) nach etwa 80 Minuten verbraucht. Zur Ergänzung des Wasservorrats in den Deionatbehältern ist vorgesehen, die Vollentsalzungsanlage in Betrieb zu nehmen.

Deren Kapazität von maximal 130 t/h ist jedoch nicht ausreichend. Es wird davon ausgegangen, daß die noch vorhandene Zeit nicht ausreicht, um einen Rohwasseranschluß (Fremd- oder Rheinwasseranschluß) herzustellen. Ein solcher Wasseranschluß muß nach Betriebshandbuch erst 6 bis 7 Stunden nach Eintritt des Notstandsfalls vorgenommen werden. Es ist auch zu beachten, daß mit dem Notstand in Block B immer ein Abfahren von Block A erforderlich wird, weil dort der Wasservorrat in den Deionatbehältern unter den für Leistungsbetrieb erforderlichen Mindestwasserstand absinkt.

Die zur Beherrschung des Notstromfalls erforderlichen Systemfunktionen sind im Fachband 1 zusammengestellt. Es sind dies:

- Reaktorschnellabschaltung,
- Notspeisewasserversorgung und Frischdampfabgabe,
- verzögerte Speisewasserversorgung und Frischdampfabgabe,
- Langzeit-Speisewasserversorgung und Frischdampfabgabe,
- Öffnen der Druckentlastung des Reaktorkühlkreislaufs und
- Schließen der Druckentlastung des Reaktorkühlkreislaufs.

Die Mindestanforderungen an diese Systemfunktionen sind unter der Voraussetzung, daß die Anlage im Zustand unterkritisch heiß gehalten wird und kein Leck im Frischdampfsystem vorliegt, in der Tabelle F2, 7-1 zusammengestellt. Die Anforderungszeitpunkte und -zeitspannen für die Systemfunktionen findet man in Bild F2, 7-2. Schließen nicht alle Frischdampf-Sicherheitsventile, so muß wegen der Trennung des Frischdampfsystems über die Reaktorschutzsignale YZ60 zumindest ein Dampferzeuger versorgt werden, dessen Frischdampf-Sicherheitsventil in Funktion ist.

Die für die Systemfunktionen notwendigen Schutzaktionen werden durch das Reaktorschutzsystem oder durch betriebliche Steuerungen eingeleitet.

Die REAKTORSCHNELLABSCHALTUNG wird ausgelöst, sobald die Drehzahl von mehr als zwei Hauptkühlmittelpumpen auf 93 % der Nenndrehzahl abgesunken ist (Kapitel 8). Dies geschieht innerhalb der ersten zwei Sekunden nach dem Ausfall der Eigenbedarfsver-

Transiente	Systemfunktionen		
	Öffnen der Druckentlastung des Reaktorkühlkreislaufs	Schließen der Druckentlastung des Reaktorkühlkreislaufs	Speisewasserversorgung (a) Hauptspeisewasser (b) Notspeisewasser (c) Verzögertes Speisewasser
Notstromfall mit Reaktorschnellabschaltung	-[1])	1v4 bzw. 2v4[2])	(a) 1v4[3]) oder (b) 1v4[4]) oder (c) 1v4[4])

[1]) Beim Notstromfall öffnet zwar in der Regel ein Druckhalterventil; dieses Öffnen ist jedoch nicht erforderlich, um ein Überdruckversagen des Reaktorkühlkreislaufs zu verhindern. Ein Öffnen der Druckentlastung des Reaktorkühlkreislaufs ist nur bei Ausfall der Speisewasserversorgungen (a) und (b) notwendig.

[2]) Schließen nicht alle Druckhalterventile, so mündet die Transiente in einen Kühlmittelverluststörfall.

[3]) Einspeisungen über die Hauptspeisewasserleitungen in die Dampferzeuger.

[4]) Einspeisungen über das Notspeisewassersystem in die Dampferzeuger. Zusätzlich sind 2 Einspeisungen über das Notstandssystem vorhanden. Insgesamt sind also 1v6 Einspeisungen erforderlich.

1v4, 2v4 usw. $\hat{=}$ von 3 vorhandenen redundanten Teilsystemen sind 1 bzw. 2 usw. erforderlich.

Tab. F2, 7-1:
Mindestanforderungen an die Systemfunktionen beim Notstromfall

sorgung. Versagt diese Auslösung der REAKTORSCHNELLABSCHALTUNG, so stehen weitere redundante Anregekriterien zur Verfügung. Bei Auslösung durch das zweite Anregekriterium, nämlich Kühlmitteldruck > 162 bar, treten gegenüber der Auslösung durch das erste Kriterium keine Unterschiede im weiteren Störfallablauf auf. Eine Reaktorschnellabschaltung durch ein erst später anstehendes Kriterium ist demgegenüber sehr unwahrscheinlich und braucht nicht berücksichtigt zu werden.

Ein Ausfall der REAKTORSCHNELLABSCHALTUNG wird in der vorliegenden Analyse nicht unterstellt. Alle Transientenstörfälle mit Ausfall der REAKTORSCHNELLABSCHALTUNG werden gemeinsam in Abschnitt 7.6 untersucht.

Bild F2, 7-2:

Anforderungszeitpunkte der Systemfunktionen beim "Notstromfall"

Nach Absinken der Spannung an den Notstromschienen unter 80 % der Nennspannung werden über die Notstromsignale des Reaktorschutzsystems die vier Notstromdiesel und die vier nuklearen Nebenkühlwasser-Pumpen gestartet.

Über das Signal "letzte Hauptspeisewasserpumpe ausgefallen" werden zur Sicherstellung der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE mittels einer betrieblichen Verriegelung die vier Stränge des Notspeisewassersystems in Betrieb genommen. Laufen nicht alle Notspeisewasser-Pumpen an, so müssen die Trennschieber in der Notspeisewasser-Sammelleitung von Hand geöffnet werden, da ansonsten die vier Dampferzeuger ungleich bespeist werden. Andernfalls werden etwa 7 Minuten nach Eintritt des Notstromfalls, bei Unterschreiten eines Wasserstandes von 6,50 m in einem der vier Dampferzeuger, über die Notspeisezuschaltsignale die vier Notspeisewasser-Pumpen gestartet und ihre Leitungen freigeschaltet, sofern kein Absperrsignal für den betreffenden Strang vorliegt. Dieses wird ausgegeben, wenn der Druck oder der Durchsatz in diesem Strang kleiner ist als in einem der beiden nicht benachbarten Stränge.

Wird im Speisewasserbehälter ein Wasserstand von 0,2 m erreicht (entspricht einem Wasservorrat von 60 t), so lösen die Deionatzuschaltsignale eine Umschaltung der Notspeisewasser-Pumpen auf direktes Ansaugen aus den Deionatbehältern aus.

Versagt die Einspeisung in die Dampferzeuger durch das Notspeisewassersystem, so kann von Hand noch das Notstandssystem in Betrieb genommen und damit in zwei Dampferzeuger gefördert werden.

Im Frischdampfsystem wird der Ansprechdruck der vier Frischdampf-Sicherheitsventile nach wenigen Minuten erreicht. Öffnet keines dieser Ventile, so stehen noch zwei Abblaseregelventile zur Verfügung. Diese sind durch Handbetätigung von der Warte aus aufzufahren. Versagt das Öffnen aller Frischdampf-Sicherheitsventile und blasen die Abblaseregelventile nicht ab, so werden etwa 15 Minuten nach Eintritt des Notstromfalls Drücke erreicht, bei denen mit einem Überdruckversagen zu rechnen ist. Ein Versa-

gen aller redundanten Sicherheitsventile aufgrund von "common mode"-Ausfällen (CMA) ist aus der Weltbetriebserfahrung nicht bekannt und wird daher im folgenden auch nicht unterstellt. Ein unabhängiger Ausfall aller vier Frischdampf-Sicherheitsventile ist äußerst unwahrscheinlich und kann in den Fehlerbäumen vernachlässigt werden.

Da sich die Ansprechdrücke der Frischdampf-Sicherheitsventile nicht unterscheiden, ist davon auszugehen, daß normalerweise alle Ventile öffnen. Schließt eine dieser Armaturen nicht, kommt es als Folge des Notstromfalls zum Störfall "Leck im Frischdampfsystem", wobei zusätzliche Reaktorschutzsignale ansprechen. Dadurch werden der zum Dampferzeuger mit dem defekten Sicherheitsventil führende Notspeisewasser-Strang abgeschiebert und das Frischdampfsystem in vier getrennte Stränge aufgeteilt. Dieser Störfall führt zu erhöhten Anforderungen an die Systemfunktionen: Bei der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE muß zur Wärmeabfuhr mittels eines Notspeisewasser-Stranges das zugehörige Frischdampf-Sicherheitsventil öffnen und schließen. Um die Integrität des Frischdampfsystems sicherzustellen, muß bei Nichtöffnen des Sicherheitsventils eines Stranges die Wärme über zwei intakte Notspeisewasser-Frischdampf-Stränge abgeführt werden. Ein Überdruckversagen ist andernfalls nach etwa 30 Minuten nicht mehr auszuschließen. Hierzu sind in der Phase B der Risikostudie noch besondere Festigkeitsuntersuchungen erforderlich. Im Rahmen der Phase A wird ein Überdruckversagen nicht unterstellt.

Im Reaktorkühlkreislauf steigt der Systemdruck ebenfalls bis zum Ansprechdruck der Druckhalterventile an. Diese Druckhalterventile werden im folgenden als Einrichtung zur Druckentlastung des Reaktorkühlkreislaufs bezeichnet. Auch bei funktionierender NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE wird es zum ÖFFNEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS kommen. Dies zeigen sowohl durchgeführte Dynamikuntersuchungen als auch die Betriebserfahrung. Dabei spricht nur das erste Druckhalter-Abblaseventil an. Ein Öffnen dieses Ventils, das nach wenigen Minuten stattfindet, ist nicht notwendig, um ein Überdruckversagen des Reaktorkühlkreislaufs zu verhindern. Nach dem Öffnen ist jedoch

ein SCHLIESSEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS erforderlich, um einen Kühlmittelverlust, d.h. ein kleines Leck am Druckhalter über das Ventil zu unterbinden.

Findet zunächst keine Notspeisewasserversorgung statt, so sind die Dampferzeuger frühestens 30 Minuten nach Eintritt des Notstromfalls ausgedampft[1]). Danach kommt es wieder zum ÖFFNEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS, und zwar werden jetzt die beiden Druckhalter-Abblaseventile ansprechen. Das Öffnen mindestens eines Ventils der vier Druckhalterventile ist erforderlich, um ein Überdruckversagen zu verhindern. Versagt das SCHLIESSEN DER DRUCKENTLASTUNG, so ist ein Kühlmittelverluststörfall die Folge.

Bis etwa 75 Minuten nach Eintritt des Notstromfalls muß eine VERZÖGERTE SPEISEWASSERVERSORGUNG UND FD-ABGABE hergestellt sein, um eine Überhitzung des Reaktorkerns zu verhindern[1]). Es ist zu berücksichtigen, daß bei Ausfall der sekundärseitigen Bespeisung der Dampferzeuger innerhalb des Sicherheitsbehälters Temperaturen und Feuchtigkeiten erreicht werden, die zu einem Versagen der Druckhalter-Abblaseventile, der zugehörigen Steuerventile sowie der jeweils redundanten Absperrarmaturen führen können. Ebenso ist mit einem Ausfall der magnetischen Zusatzbelastung für die Druckhalter-Sicherheitsventile und der Meßumformer für die Kühlmitteldruckregelung zu rechnen. Diese Komponenten sind nämlich nicht für derartige Umgebungsbedingungen ausgelegt. Eine durch die Umgebungsbedingungen verursachte Unterbrechung der Stromversorgung für die Armaturen wird zu einem Schließen der Abblase-Steuerventile und damit der Abblaseventile führen; dabei wird davon ausgegangen, daß die Schließfunktion des Steuerventils selbst sowie des Abblaseventils durch die Umgebungsbedingungen nicht beeinträchtigt wird. Zum Unterschied von der Ausfallrichtung des Steuerventils kann über die Ausfallrichtung der Meßumformer keine Aussage gemacht werden.

---

1) Bei der Abschätzung dieser Zeitspanne wurde die dem ANS-Standard entsprechende Nachzerfallsleistung mit einem Zuschlag von 20 % versehen.

Bei der LANGZEIT-SPEISEWASSERVERSORGUNG UND FD-ABGABE muß auf den im Deionatsystem gespeicherten Wasservorrat zurückgegriffen werden. Erfolgt keine Nachspeisung von Deionat in den Speisewasserbehälter, so ist dieser nach etwa 3 Stunden entleert. Mißlingt auch die Umschaltung der Notspeisewasser-Pumpen auf direkte Deionatversorgung und versagt die Einspeisung über das Notstandssystem, so sind die Dampferzeuger etwa 3 1/2 Stunden nach Störfalleintritt ausgedampft. Danach heizt sich der Reaktorkühlkreislauf bis zum ÖFFNEN DER DRUCKENTLASTUNG DES REAKTOR-KÜHLKREISLAUFS auf und dampft anschließend langsam aus. Frühestens etwa 4 Stunden nach Eintritt des Notstromfalls werden solche Zustände im Reaktorkühlkreislauf erreicht, daß eine Überhitzung des Reaktorkerns nicht mehr verhindert werden kann.

Das Betriebshandbuch verlangt zwar ein Abfahren 30 Minuten nach Eintritt des Notstromfalles, jedoch ist es auch bei Ausfall des Abfahrens möglich, den Reaktor im Zustand "unterkritisch heiß" zu halten, wobei sich die minimalen Systemanforderungen ergeben. Daher wird in der Analyse vereinfachend davon ausgegangen, daß die Anlage zunächst nicht abgefahren wird. Frühestens 10 Stunden nach Eintritt des Notstromfalles sind dann weitere Systemfunktionen erforderlich. Weiterhin wird davon ausgegangen, daß bis zu diesem Zeitpunkt, wenn notwendig, geeignete Maßnahmen ergriffen werden können, um diese Systemfunktionen sicherzustellen.

Für kleine Lecks am Druckhalter wird die gleiche Anzahl von mindestens erforderlichen Teilsystemen zugrunde gelegt, wie für kleine Lecks in einer Hauptkühlmittelleitung. Damit wird die Anzahl der für die einzelnen Systemfunktionen erforderlichen Teilsysteme, im Vergleich zu Lecks derselben Größe in einer Hauptkühlmittelleitung, möglicherweise überschätzt. Die Nachwärmeabfuhr wird hier nämlich durch günstigere thermodynamische Verhältnisse erleichtert. Berücksichtigt wird jedoch, daß die Nachwärmeabfuhr durch das Ausdampfen der Dampferzeuger und des Reaktorkühlkreislaufs für eine begrenzte Zeitspanne tolerierbar ist, d.h., daß eine verzögerte Inbetriebnahme der Speisewasserversorgung ausreicht.

Die NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE muß für "kleines Leck am Druckhalter" erneut betrachtet werden, obwohl sie bereits für den Notstromfall diskutiert wurde. Im Gegensatz zum Notstromfall, bei dem die Speisewasserversorgung spätestens nach etwa 75 Minuten erfolgen muß, stehen nämlich beim kleinen Leck am Druckhalter 2 bis 3 Stunden zur Verfügung. Nach dieser Zeitspanne ist außerdem das Abfahren der Anlage erforderlich, wobei für die NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE die gleichen Mindestanforderungen gelten wie für "kleines Leck in einer Hauptkühlmittelleitung". Allerdings stehen hier zusätzlich die beiden Stränge des Notstandssystems, also insgesamt 6 Stränge zur Verfügung. Für das Abblasen über Dach (die Frischdampf-Umleiteinrichtung ist wegen des Notstromfalls nicht verfügbar) ist die Funktion eines der beiden Abblaseregelventile ausreichend. Ebenso wie für "kleines Leck in einer Hauptkühlmittelleitung" muß mit einem Folgeausfall der Meßumformer für die Notspeisewasser-Regelung gerechnet werden, da diese nicht für die nach Kühlmittelverluststörfällen innerhalb der Stahlhülle herrschenden Umgebungsbedingungen ausgelegt sind. Sinkt danach der Wasserstand in den Dampferzeugern unzulässig ab, so werden die Notspeisewasser-Regelventile durch Reaktorschutzsignale aufgefahren. Bei einem fälschlichen ZU-Befehl durch die Notspeisewasser-Regelung ist ein dauerndes Auf- und Zufahren der Regelventile nicht auszuschließen. Eine solche Betriebsweise entspricht nicht der Auslegungsgrundlage der Motorantriebe von Regelventilen, weshalb möglicherweise ein Auslösen des Motorschutzes erfolgt. Dabei wird die Sammelstörmeldung "Steuerkopf-Störung" auf der Warte ausgegeben und der Regler auf Handbetrieb umgeschaltet, so daß kein Ausfall der Notspeisewasser-Regelventile auftritt. Selbst unter diesen ungünstigen Annahmen tritt also kein Ausfall der Notspeisewasserversorgung ein.

7.2.2 Fehlerbaumbeschreibungen

7.2.2.1 G e s a m t f e h l e r b ä u m e

7.2.2.1.1 Notstromfall

Der Gesamtfehlerbaum für den Notstromfall (Anhang 2) stellt im wesentlichen die Umsetzung der Ereignisablaufdiagramme (Fachband 1) unter Berücksichtigung der Mindestanforderungen an die Systemfunktionen (Tabelle F2, 7-1) dar. Es sind im Gesamtfehlerbaum die unerwünschten Ereignisse "Ausfall der Systemfunktionen bei Anforderung" und "kleines Leck am Druckhalter" eingezeichnet. Der Ausfall der REAKTORSCHNELLABSCHALTUNG ist im Gesamtfehlerbaum nicht enthalten, da hierzu eine gesonderte Zuverlässigkeitsanalyse vorliegt (Kapitel 8).

Ein nicht beherrschter Notstromfall liegt vor bei

- Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE und Ausfall der VERZÖGERTEN SPEISEWASSERVERSORGUNG UND FD-ABGABE,
- Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE und Ausfall des ÖFFNENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS,
- Ausfall der LANGZEIT-SPEISEWASSERVERSORGUNG UND FD-ABGABE.

Zum Störfall "kleines Leck am Druckhalter beim Notstromfall" führt

- der Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS beim Öffnen eines Stranges,
- der Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE und der Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS beim Öffnen von zwei Strängen.

Die Ausfälle der Teilsystemfunktionen (z.B. FD-Abgabe über Strang 1) sind als "Überträge" aus den Teilfehlerbäumen dargestellt: Im Gesamtfehlerbaum werden dabei insgesamt die Überträge folgender Teilfehlerbäume (Anhang 3) verknüpft:

Fehlerbaum 1:	Deionatsystem
Fehlerbäume 2 bis 5:	Notspeisewassersystem

Fehlerbaum 6:	Notstandssystem
Fehlerbaum 10:	Frischdampfsystem
Fehlerbaum 11:	Öffnen der Druckentlastung des Reaktorkühlkreislaufs
Fehlerbaum 12:	Schließen der Druckentlastung des Reaktorkühlkreislaufs.

Nachstehend wird kurz auf den Ausfall der folgenden Systemfunktionen eingegangen:

- Unverzögerte NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE

Ein Ausfall dieser Systemfunktion liegt vor, wenn alle vier vorhandenen Stränge zur NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE versagen. Es werden die Teilfehlerbäume verknüpft, die die Herstellung einer sekundärseitigen Wärmeabfuhr innerhalb von 30 Minuten nach Eintritt des Notstromfalls behandeln. Die in den Deionatbehältern gespeicherte Wassermenge wird dabei nicht berücksichtigt.

Ein Strang der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE fällt aus, wenn

- der entsprechende Dampferzeuger durch das Notspeisewassersystem oder durch das Notstandssystem nicht ausreichend mit Speisewasser versorgt wird oder
- eine Frischdampfabgabe über diesen Strang nicht möglich ist.

Bleibt ein Frischdampf-Sicherheitsventil fälschlich offen, so führt dies ebenfalls zum Ausfall der Notspeisewasserversorgung, falls der davon betroffene Strang nicht durch das Reaktorschutzsystem abgesperrt wird (die Absperrung wird hier aufgrund eines Druckvergleiches der Stränge ausgelöst). Diese Ausfallkombination kann jedoch aufgrund der geringen Ausfallwahrscheinlichkeit vernachlässigt werden.

- VERZÖGERTE SPEISEWASSERVERSORGUNG UND FD-ABGABE

Für diese Systemfunktionen werden die Teilfehlerbäume der zur sekundärseitigen Wärmeabfuhr notwendigen Systeme wie beim Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE verknüpft. Für die Inbetriebnahme des Notstandssystems wird jedoch im Gegensatz dazu die Zeitspanne zwischen 30 und 75 Minuten nach Eintritt des Notstromfalls betrachtet. Auch in diesem Fehlerbaum braucht die in den Deionatbehältern gespeicherte Wassermenge nicht berücksichtigt zu werden.

- LANGZEIT-SPEISEWASSERVERSORGUNG UND FD-ABGABE

Hier müssen die Teilfehlerbäume verknüpft werden, die die Aufrechterhaltung der sekundärseitigen Wärmeabfuhr in der Zeitspanne von ca. 3 bis 10 Stunden nach Eintritt des Notstromfalls behandeln. Ein Ausfall liegt vor, wenn keiner der vier Dampferzeuger ausreichend mit Speisewasser versorgt wird. Dies ist dann der Fall, wenn alle vier Notspeisewasser-Stränge ausgefallen sind und das Notstandssystem nicht in Betrieb genommen wird oder - falls es bereits in Betrieb war - ebenfalls ausgefallen ist.

Da die im Speisewasserbehälter bei Eintritt des Notstromfalls vorhandene Wassermenge bei Betrieb mit nur einer Notspeisewasser-Pumpe nach ca. 165 Minuten verbraucht ist, muß bei der LANGZEIT-SPEISEWASSERVERSORGUNG UND FD-ABGABE auf die im Deionatsystem gespeicherte Wassermenge zurückgegriffen werden. Ein Ausfall des Notspeisewassersystems liegt somit vor, wenn kein Deionat in den Speisewasserbehälter nachgespeist wird und die Umschaltung der Notspeisewasser-Pumpen auf direktes Ansaugen aus den Deionatbehältern mißlingt.

Nicht berücksichtigt werden in diesem Fehlerbaum erneute Ausfälle des Frischdampfsystems. Da die Frischdampf-Sicherheitsventile unmittelbar nach Störfalleintritt öffnen müssen, wird ein Ausfall dieser Ventile auch nur zu diesem Zeitpunkt unterstellt. Es wird also davon ausgegangen, daß es durch das wiederholte Ansprechen der Sicherheitsventile zu keinen Ausfällen kommt. Au-

ßerdem ist davon auszugehen, daß es dem Betriebspersonal im weiteren Verlauf gelingen wird, die Abblaseregelventile in Betrieb zu nehmen und den Frischdampfdruck abzusenken, so daß die Sicherheitsventile nicht mehr ansprechen.

Die Fehlerbäume für

- den Ausfall des ÖFFNENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS und
- den Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS

werden in den Abschnitten 7.2.2.2.9 und 7.2.2.2.10 beschrieben.

7.2.2.1.2 Kleines Leck am Druckhalter beim Notstromfall

Wie beim Gesamtfehlerbaum für "kleines Leck in einer Hauptkühlmittelleitung" (Anhang 2) liegt auch hier eine Aufteilung in die Verknüpfungen der Systemfunktionen zur Notkühlung (Teil A) und die Systemfunktionen zur Speisewasserversorgung und FD-Abgabe (Teil B) vor. Im TOP werden die Ausfälle von Systemfunktionen verknüpft, die zu einem unbeherrschten Störfall führen. Da für Lecks am Druckhalter die gleichen Mindestanforderungen an die Systemfunktionen zugrunde gelegt werden wie für Lecks in einer Hauptkühlmittelleitung, entsprechen die Verknüpfungen im Gesamtfehlerbaum für das kleine Leck am Druckhalter im wesentlichen denen für das kleine Leck in einer Hauptkühlmittelleitung (Abschnitt 6.1.2.1.3). Unterschiede in Teil A ergeben sich durch die Lage des Lecks:

- Da der Druckhalter über die Ausgleichsleitung an den "heißen" Strang der Hauptkühlmittelleitung angeschlossen ist, sind bei den Verknüpfungen für die ND-Einspeisungen "heiß" und "kalt" vertauscht, das bedeutet den Ausfall der Systemfunktion ND-EINSPEISUNG FÜR FLUTEN bei Versagen von 3v4 "kalten" oder 4v4 "heißen" Einspeisungen für Fluten.
- Die Verknüpfung "Ausfall des Not- und Nachkühlsystems bei Bruch der Nachkühlsaugleitung" entfällt, da als Folge eines nicht schließenden Druckhalterventils keine Beschädigung der Nachkühlsaugleitung auftreten kann.

Bei den Verknüpfungen in Teil B des Gesamtfehlerbaums für "kleines Leck am Druckhalter" ist berücksichtigt, daß der Notstromfall vorliegt, das heißt, es steht weder die HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE zur Verfügung, noch kann der Frischdampf über die Frischdampf-Umleiteinrichtung in den Kondensator abgegeben werden. Zum Versagen der zur Beherrschung des Störfalls erforderlichen NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE führt daher der Ausfall der geregelten FD-Abgabe über die Ablaseregelventile. Der Ausfall der Notspeisewasserversorgung ist als 5v6-Verknüpfung dargestellt, da von den vier Einspeisungen durch das Notspeisewassersystem und den zwei Einspeisungen durch das Notstandssystem mindestens zwei Einspeisungen funktionieren müssen. Die Ausfälle der zum Abfahren erforderlichen Handmaßnahmen bzw. fehlerhaft durchgeführte Handmaßnahmen sind unter "zu spätes Abfahren oder Abfahren mit falschem Abfahrgradient" zusammengefaßt.

Die Ausfälle von Teilsystemfunktionen (z.B. Ausfall des Notspeisestrangs 1) sind im allgemeinen als Überträge aus Teilfehlerbäumen dargestellt. Im Gesamtfehlerbaum (Anhang 2) werden dabei die gleichen Teilfehlerbäume wie bei den Lecks in einer Hauptkühlmittelleitung verknüpft (Abschnitt 6.1.2.1). Diese Teilfehlerbäume enthalten ihrerseits Überträge aus weiteren Teilfehlerbäumen (Anhang 3).

7.2.2.2 Teilfehlerbäume der verfahrenstechnischen Systeme

7.2.2.2.1 Allgemeines

Zur Beherrschung des Notstromfalls und des kleinen Lecks am Druckhalter beim Notstromfall liegen folgende Teilfehlerbäume der verfahrenstechnischen Systeme vor (Anhang 3):

Fehlerbaum 1 A: Deionatsystem,
Einspeisung in den Speisewasserbehälter

Fehlerbaum 1 B: Deionatsystem,
Einspeisung in den Notspeisewasser-Strang 1(RL04)

Fehlerbaum 1 C:	Deionatsystem, Einspeisung in den Notspeisewasser-Strang 2(RL05)
Fehlerbaum 1 D:	Deionatsystem, Einspeisung in den Notspeisewasser-Strang 3(RL06)
Fehlerbaum 1 E:	Deionatsystem, Einspeisung in den Notspeisewasser-Strang 4(RL07)
Fehlerbaum 2 :	Notspeisewassersystem, Strang 1
Fehlerbaum 3 :	Notspeisewassersystem, Strang 2
Fehlerbaum 4 :	Notspeisewassersystem, Strang 3
Fehlerbaum 5 :	Notspeisewassersystem, Strang 4
Fehlerbaum 6 :	Notstandssystem
Fehlerbaum 7 C:	Nuklearer Zwischenkühlkreis (Notstromfall)
Fehlerbaum 8 :	Kaltwassersystem
Fehlerbaum 9 C:	Nukleares Nebenkühlwassersystem, Stränge 1 und 2 (Notstromfall)
Fehlerbaum 9 D:	Nukleares Nebenkühlwassersystem, Stränge 3 und 4 (Notstromfall)
Fehlerbaum 10 E:	Frischdampfsystem, Stränge 1 und 2 (Notstromfall)
Fehlerbaum 10 F:	Frischdampfsystem, Stränge 3 und 4 (Notstromfall)
Fehlerbaum 11 :	Öffnen der Druckentlastung des Reaktorkühlkreislaufes
Fehlerbaum 12 A:	Schließen der Druckentlastung des Reaktorkühlkreislaufes (1 Abblasestrang)
Fehlerbaum 12 B:	Schließen der Druckentlastung des Reaktorkühlkreislaufes (2 Abblasestränge)
Fehlerbaum 16 A:	Lüftungsanlagen (Kühlmittelverluststörfälle)
Fehlerbaum 16 B:	Lüftungsanlagen (Notstromfall, ohne Leck am Druckhalter)
Fehlerbaum 17 A:	Not- und Nachkühlsystem, HD-Einspeisungen, Stränge 1 und 2
Fehlerbaum 17 B:	Not- und Nachkühlsystem, HD-Einspeisungen, Stränge 3 und 4

Fehlerbaum 18 A: Not- und Nachkühlsystem, ND-Einspeisung, Strang 1
Fehlerbaum 18 B: Not- und Nachkühlsystem, ND-Einspeisung, Strang 2
Fehlerbaum 18 C: Not- und Nachkühlsystem, ND-Einspeisung, Strang 3
Fehlerbaum 18 D: Not- und Nachkühlsystem, ND-Einspeisung, Strang 4

Mit Ausnahme der Fehlerbäume 11 und 12 werden diese Teilfehlerbäume bereits im Kapitel 6.1.2.2 bei den Kühlmittelverluststörfällen beschrieben. An dieser Stelle wird lediglich auf die Ausfallkombinationen eingegangen, die nur bei den Ereignisabläufen "Notstromfall" und "kleines Leck am Druckhalter beim Notstromfall" Gültigkeit besitzen. Das in den Teilfehlerbäumen verwendete Funktionselement "NSF" erhält bei beiden Abläufen den Wert p = 1, das Funktionselemet "KMV" wird bei den Ereignisabläufen "Notstromfall" mit p = 0 und bei den Ereignisabläufen "kleines Leck am Druckhalter beim Notstromfall" mit p = 1 bewertet (Abschnitt 6.1.2.2.1).

- Folgeausfälle

Folgeausfälle werden durch Sekundäreingänge in die Fehlerbäume beschrieben. Die bei der Analyse der Systemfunktionen zur Beherrschung des "Notstromfalls" und des "kleinen Lecks am Druckhalter beim Notstromfall" berücksichtigten Sekundäreingänge sind in der Tabelle F2, 7-2 zusammengestellt.

Die Absperrarmatur 20 TF30 S012 für den Brennelement-Beckenkühler sowie die Gebäudeabschlußarmaturen in der Ringleitung zu den Verbrauchern im Reaktorgebäude-Innenraum und im Reaktorhilfsanlagengebäude müssen im Notstromfall geschlossen sein, da im Notstromfall nur eine Zwischenkühlpumpe (im Strang 3) in Betrieb ist. Schließen im Notstromfall diese Armaturen nicht, so findet nur ein verminderter Durchsatz durch die zur Störfallbeherrschung wichtigen Kühler des Notspeisewasser-Pumpenaggregats

Art des Folgeausfalls	Bezeichnung der Wahrscheinlichkeit	Wahrscheinlichkeit	Fehlerbaum
Ausfall der Kühlung der Notspeisewasser-Pumpe durch den Strang 3 des nuklearen Zwischenkühlkreislaufes bei offenem Brennelement-Beckenkühler	W_7	0/1	7
Folgeausfall der Notspeisewasser-Regelung bei Dampfabgabe in den Sicherheitsbehälter	W_8	0/1	2,3,4,5
Überdruckversagen des Frischdampfsystems bei bestimmten Ausfallkombinationen	W_9	0	10
Folgeausfall einer Frischdampfleitung bei Überdruckversagen im benachbarten Strang	W_{10}	0	10
Folgeausfall der Druckhalter-Regelung bei Dampfabgabe in den Sicherheitsbehälter	W_{12}	1	12

Tab. F2, 7-2:

Folgeausfälle bei der Transiente "Notstromfall" und beim "kleinen Leck am Druckhalter beim Notstromfall"

23 RL06 D001 statt. Ein vom Betreiber durchgeführter Versuch unter diesen Bedingungen und bei durchschnittlichen Fördermengen durch die Kühler im Reaktorgebäude-Innenraum und Hilfsanlagengebäude ergab, daß im Kühler dieser Notspeisewasser-Pumpe der minimale Durchflußgrenzwert nicht erreicht wird. Unter den angegebenen Voraussetzungen ist die Kühlung also noch ausreichend. Dementsprechend wird die Wahrscheinlichkeit $W_7 = 0$ gesetzt. Beim Störfall "kleines Leck am Druckhalter beim Notstromfall" muß dieser Zwischenkühlstrang zusätzlich den Nachwärmekühler rückkühlen. Es wird daher unterstellt, daß für diesen Störfall die Kühlung der Notspeisewasser-Pumpe nicht mehr ausreichend ist. Somit wird $W_7 = 1$ angesetzt.

Bei Trennung des Frischdampfsystems in vier Teilstränge, hervorgerufen durch ein nicht schließendes FD-Sicherheitsventil, und bei Ausfall eines weiteren Notspeisewasser-Frischdampfstranges ist in einem Frischdampfstrang mit nicht öffnendem Sicherheitsventil und geschlossener Abblasestation mit Systemdrücken von über 110 bis 120 bar zu rechnen, für die das System nicht ausgelegt ist.

Erste Untersuchungen dazu haben ergeben, daß ein Überdruckversagen nicht zu erwarten ist, sofern an den Frischdampfleitungen bis dahin keine Materialfehler aufgetreten sind. In der vorliegenden Studie wird ein Überdruckversagen nicht unterstellt ($W_9 = 0$).

Eine aufgrund eines Überdruckversagens gebrochene Frischdampfleitung könnte die benachbarte Frischdampfleitung beschädigen. Das heißt, es müßte auch mit dem Bruch dieser Leitung gerechnet werden. Dieser Folgeausfall wird zunächst mit einer Wahrscheinlichkeit $W_{10} = 0$ bewertet.

Falls einige Minuten über die Druckhalterventile abgeblasen wird, sprechen die Berstscheiben des Abblasebehälters an, so daß im Anschluß daran Dampf in den Sicherheitsbehälter gelangt. Es wird pessimistisch davon ausgegangen, daß die Meßumformer der Kühlmitteldruckregelung diesen Temperaturen und Feuchtigkeiten innerhalb des Sicherheitsbehälters nicht standhalten und so ausfallen, daß vom Regler keine Schließbefehle ausgegeben werden.

Daher wird für $W_{12} = 1$ angesetzt. Diese Differenzdruck-Meßumformer werden bei Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE für das ÖFFNEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS und das SCHLIESSEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS benötigt, und zwar so lange, bis eine VERZÖGERTE SPEISEWASSERVERSORGUNG UND FD-ABGABE hergestellt ist.

Aus den gleichen Gründen muß bei Dampfabgabe in den Sicherheitsbehälter mit dem Ausfall der Meßumformer der Notspeisewasser-Regelung gerechnet werden. Für den Folgeausfall der Notspeisewas-

ser-Regelung wird beim Notstromfall ohne Leck am Druckhalter somit $W_8 = 0$, beim Notstromfall mit Leck am Druckhalter $W_8 = 1$ angesetzt.

Bei einem Ausfall der Schließfunktion der Druckhalterventile kann es langfristig zu einem Abblasen von Wasser über diese Ventile kommen. Ob Druckhalterventile bei einem Wasserabblasen ebenso zuverlässig arbeiten, wird gegenwärtig experimentell überprüft (Abschnitt 7.6.1). In der vorliegenden Studie wird aber die Möglichkeit nicht berücksichtigt, daß ein Druckhalter-Abblasestrang erst nach Störfalleintritt als offen erkannt und dann noch von Hand geschlossen wird. Es handelt sich hier nämlich um eine nicht geplante Handmaßnahme.

Bei Nichtschließen zweier Rückschlagklappen in einer Hauptspeisewasserleitung kommt es im Notstromfall zu einer vorübergehenden Rückströmung eines Wasser-Dampf-Gemisches aus einem Dampferzeuger in Richtung Speisewasserbehälter. Aufgrund der Temperaturdifferenz zwischen Dampferzeuger und Speisewasserbehälter ist dabei die Möglichkeit von Kondensationsschlägen in den Rohrleitungen zwischen Druckschieber und Speisewasserbehälter und im Speisewasserbehälter selbst in Betracht zu ziehen. Nach einer vorliegenden Untersuchung ist in den Rohrleitungen nicht mit Kondensationsschlägen zu rechnen, dagegen wird es im Speisewasserbehälter zeitweise zu Kondensationsschlägen kommen. Dabei ist jedoch nicht mit einer Beschädigung des Behälters zu rechnen. Ein Ausfall des Speisewasserbehälters wird somit nicht unterstellt.

7.2.2.2.2 Fehlerbaum 1: Deionatsystem

Im Notstromfall (NSF = 1, KMV = 0, Abschnitt 6.1.2.2.1) ist für die Inbetriebnahme der Deionatförderung in den Speisewasserbehälter die Handmaßnahme L 449 OP RY10/11 maßgebend. Bei der Bestimmung der Ausfallwahrscheinlichkeit dieser Handmaßnahme wurde berücksichtigt, daß das Betriebspersonal im Betriebshandbuch und aufgrund von Prozeßrechnermeldungen auf die Durchführung dieser Maßnahmen hingewiesen wird, diese Maßnahmen frühestens 30 Minu-

ten nach Eintritt des Notstromfalls durchgeführt werden müssen und dazu mehrfache personelle Redundanz vorhanden ist.

Für "kleines Leck am Druckhalter beim Notstromfall" (NSF = 1, KMV = 1) wird dagegen - wie bei den Kühlmittelverluststörfällen - die Handmaßnahme L 451 OP RY10/11 berücksichtigt.

7.2.2.2.3 Fehlerbäume 2 bis 5: Notspeisewassersystem

Bei den Fehlerbäumen der vier Redundanzen des Notspeisewassersystems ergeben sich für den Notstromfall gegenüber der Beschreibung dieser Fehlerbäume bei den Kühlmittelverluststörfällen folgende Abweichungen:

Da im Notstromfall ohne Leck am Druckhalter nicht mit einer Dampfabgabe in den Sicherheitsbehälter zu rechnen ist, wird für die Wahrscheinlichkeit des Ausfalls der Meßumformer der Notspeisewasser-Regelung W_8 = 0 angesetzt. Bei der Ansteuerung der Komponenten wurde davon ausgegangen, daß sie zunächst betrieblich erfolgt. Bei Ausfall der betrieblichen Ansteuerung ergehen außerdem durch das Reaktorschutzsystem Befehle an die Komponenten der Notspeisewasser-Stränge. Aus diesem Grund wird in den Fehlerbäumen beim Notstromfall nur der Ausfall der Steuerkette und der 24-V-Versorgung im Betätigungsschrank berücksichtigt.

7.2.2.2.4 Fehlerbaum 6: Notstandssystem

Zur Inbetriebnahme des Notstandssystems sind ausschließlich Handmaßnahmen notwendig. Fallen alle vier Stränge des Notspeisewassersystems bei Eintritt des Notstromfalls sofort aus, so müssen diese Maßnahmen bei der unverzögerten NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE spätestens 30 Minuten, bei der VERZÖGERTEN NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE spätestens 75 Minuten nach Eintritt des Notstromfalls durchgeführt worden sein. Bei der Ermittlung der Versagenswahrscheinlichkeiten dieser Handmaßnahmen wurde wie in der AIPA-Studie vorgegangen (Abschnitt 3.4.3). Für die Aktivierung des Notstandssystems durch

das Betriebspersonal wurde ein Zeitraum von ca. 16 Minuten angesetzt. Daraus ergab sich für die Inbetriebnahme des Notstandssystems innerhalb von 30 Minuten eine Ausfallwahrscheinlichkeit von $p_{50} = 2 \cdot 10^{-1}$, innerhalb der anschließenden 45 Minuten (verzögerte Inbetriebnahme) eine Ausfallwahrscheinlichkeit von $p_{50} = 6 \cdot 10^{-2}$.

Ein Ausfall des Notstandssystems liegt vor, wenn

- nicht mit mindestens einer Notspeisewasser-Pumpe des Kraftwerkblocks A über die gemeinsame Notstandsleitung in einen der beiden Dampferzeuger 20 YB01 B001 und 20 YB03 B001 eingespeist wird oder
- bei einem Ausfall der Schließfunktion eines FD-Sicherheitsventils fälschlicherweise das Stellventil im Notstandssystem vor dem betreffenden Dampferzeuger geöffnet wird.

Für die Wahrscheinlichkeit, daß vom Operator ein Stellventil fälschlich geöffnet wird, wird nach WASH-1400 p = 0,1 angesetzt. Es wurde davon ausgegangen, daß das Betriebspersonal sich noch in einer extremen Streßsituation befindet und die Anzeige des Frischdampfdruckes möglicherweise nicht beachtet.

Die Versorgung eines Dampferzeugers mit Speisewasser ist nicht möglich, wenn das Stellventil oder die nachgeschaltete Rückschlagklappe in der zugehörigen Notstands-Einspeiseleitung nicht geöffnet wird bzw. sich nicht öffnen läßt. Das Stellventil wird vorrangig von der Notstandstafel des Blocks A aus aufgefahren.

Ein Versagen der Notstands-Notspeisewasserversorgung aus dem Block A mittels der elektrisch betriebenen Notspeisewasserpumpen 12 RL05 D001 und 14 RL06 D001 kann hervorgerufen werden durch

- Nichtöffnen der Hand-Absperrarmatur 10 RX10 S001 bzw. 10 RX10 S002,
- Nichtschließen der Druckschieber 12 RL05 S005 bzw. 14 RL07 S005 (Handbefehl auf der Warte) und
- Ausfall der Notspeisewasserpumpen selbst. Dieser Ausfall kann auf einem Startversagen der Pumpen beruhen, er kann aber seine Ursache auch in einem Ausfall anderer Komponenten des Notspeisewassersystems von Block A haben.

Komponenten, die zum Notspeisewassersystem des Kraftwerkblocks A gehören, z.B. die Notspeisewasserpumpen und deren Druckschieber, werden zwar in dieser Beschreibung der Vollständigkeit halber einzeln erwähnt, wurden aber im Fehlerbaum strangweise in einer Ersatzausfallrate zusammengefaßt.

7.2.2.2.5 Fehlerbaum 7: Nuklearer Zwischenkühlkreis

Im Notstromfall ohne Leckstörfall werden vom nuklearen Zwischenkühlkreis nur die Stränge 3 und 4 zur Kühlung der Notspeisewasser-Pumpen benötigt. Alle sonstigen bei den Leckstörfällen beschriebenen Ausfallkombinationen und Überträge aus diesem Fehlerbaum brauchen somit nicht berücksichtigt zu werden.

An die Absperrarmatur 20 TF30 S012 für den Brennelement-Beckenkühler ergeht im Notstromfall durch eine betriebliche Automatik ein ZU-Befehl, wenn eine der beiden Nachkühler-Absperrarmaturen öffnet. Versagt im Notstromfall diese betriebliche Ansteuerung und wird auch kein Handbefehl zum Schließen dieser Armatur gegeben, so findet in diesem Zwischenkühlstrang nur ein verminderter Durchsatz durch die zur Beherrschung des Notstromfalls wichtigen Kühler statt. Die Wahrscheinlichkeit für den Ausfall der Notspeisewasser-Pumpe 23 RL06 D001 aufgrund unzureichender Kühlung wird mit $W_7 = 0$ angesetzt.

7.2.2.2.6 Fehlerbaum 8: Kaltwassersystem

Es ergeben sich keine Abweichungen gegenüber der Beschreibung bei den Kühlmittelverluststörfällen.

7.2.2.2.7 Fehlerbaum 9: Nukleares Nebenkühlwassersystem

Für das nukleare Nebenkühlwassersystem ergeben sich nur hinsichtlich der leittechnischen Ansteuerung Unterschiede zu dem bereits bei den Kühlmittelverluststörfällen beschriebenen Fehlerbäumen (Abschnitt 6.1.2.2.14). Im Notstromfall werden die zu

betätigenden Komponenten zunächst nicht durch das Reaktorschutzsystem, sondern durch die betriebliche Automatik angesteuert. Der Ausfall dieser beiden zueinander redundanten Ansteuerungen kann jedoch vernachlässigt werden.

7.2.2.2.8 Fehlerbaum 10: Frischdampfsystem

Ein Ausfall der Frischdampfabgabe über einen Frischdampfstrang liegt bei einem Ausfall der Schließfunktion des zugehörigen Sicherheitsventils vor. Mit einem Ausfall wäre auch beim Auftreten eines Überdruckversagens in einem Frischdampfstrang zu rechnen.

Zusätzlich liegt ein Ausfall eines Frischdampfstranges für das kleine Leck am Druckhalter beim Notstromfall vor, wenn die Frischdampfabgabe über diesen Strang, die zugehörige Abfahrleitung und die Abblaseregelventile nicht erfolgt. Die entsprechenden Ausfallkombinationen sind in den Überträgen "Ausfall der FD-Abgabe über Abfahrleitung, FD-Strang 1 (2,3,4)" zusammengefaßt.

Neben den Ausfällen einzelner Frischdampfstränge sind für das kleine Leck am Druckhalter zusätzlich die Ausfallkombinationen zu berücksichtigen, die strangunabhängig zum Versagen des Abfahrens über die Abblaseregelventile führen (Fehlerbaum 10 E):

- Zu spätes Abfahren oder Abfahren mit falschem Abfahrgradienten aufgrund menschlichen Fehlverhaltens (Abschnitt 7.2.4),
- Ausfall der geregelten Frischdampfabgabe über Abblaseregelventile, wenn beide Abblaseregelventile nicht geöffnet werden können (Abschnitt 7.2.1).

- Ausfall der Frischdampfabgabe durch Nichtschließen eines Sicherheitsventils

Die vier Frischdampfstränge sind durch eine Ausgleichsleitung untereinander verbunden. Bei Ausfall der Schließfunktion eines Sicherheitsventils wird mittels des Reaktorschutzsystems das Frischdampfsystem in vier getrennte Stränge aufgeteilt und der

zum entsprechenden Dampferzeuger gehörige Notspeisewasserstrang abgeschiebert. Ein nicht schließendes Frischdampf-Sicherheitsventil führt somit zum Ausfall des zugehörigen Notspeisewasserstranges. Besteht in diesem Notspeisewasser-Frischdampf-Strang auch eine Einspeisemöglichkeit durch das Notstandssystem, so gilt auch diese Speisewasserversorgung als ausgefallen.

Gegenüber dem Ausfall der Schließfunktion des FD-Sicherheitsventils in einem Frischdampfstrang kann folgende Ausfallkombination (Beispiel Strang 1) vernachlässigt werden, die ebenfalls zum Versagen eines Notspeisewasser-Frischdampf-Strangs führen würde:

- FD-Sicherheitsventil in Strang 2, 3 oder 4 schließt nicht (führt zur Aufteilung des Frischdampfsystems in vier getrennte Stränge) und
- FD-Sicherheitsventil in Strang 1 öffnet nicht (führt zum Ausfall der Frischdampfabgabe über Strang 1).

- Überdruckversagen in einem Frischdampfstrang

Zum Überdruckversagen in einem Frischdampfstrang könnte es kommen, wenn in diesem Strang das Frischdampf-Sicherheitsventil nicht öffnet und gleichzeitig noch folgende Ausfälle auftreten:

- Ausfall der Frischdampf-Abblaseeinrichtung,
- Ausfall der Schließfunktion eines Sicherheitsventils in einem anderen Frischdampfstrang (dies führt zur Trennung des Systems),
- Ausfall eines der beiden restlichen Notspeisewasser-Frischdampfstränge aufgrund eines weiteren Einzelfehlers.

Ein Ausfall der Frischdampf-Abblaseeinrichtung liegt vor, wenn

- der Abblase-Absperrschieber in der Leitung zum Frischdampfstrang mit nicht öffnendem Sicherheitsventil nicht aufgefahren wird oder
- vom Operator für keines der beiden Abblaseregelventile ein AUF-Befehl gegeben wird.

Beim Auftreten eines Überdruckversagens in einem Frischdampfstrang wären als Folgeausfälle Schäden am benachbarten Frischdampfstrang in Betracht zu ziehen, was zum Ausfall dieses Notspeisewasser-Frischdampf-Stranges führen würde. Die Wahrscheinlichkeit für das Auftreten eines Überdruckversagens wird mit $W_9 = 0$ angesetzt (Abschnitt 7.2.1 und 7.2.2.2.1).

- Ausfall des Abfahrens über FD-Strang 1

Es ist bei dieser Ausfallkombination das Versagen der Frischdampfabgabe über den Frischdampfstrang und die zugehörige Abfahrleitung gemeint. Unterschiede zur entsprechenden Ausfallkombination im Fehlerbaum 10 A für das kleine Leck in einer Hauptkühlmittelleitung (Abschnitt 6.1.2.2.15) ergeben sich durch die beim Notstromfall zusätzliche Möglichkeit des Überdruckversagens des Frischdampfstranges und durch die beim kleinen Leck am Druckhalter zur Verfügung stehende Zeitspanne von 2 bis 3 Stunden nach Störfalleintritt für die Handmaßnahme "Auffahren des Abblase-Absperrschiebers von Hand und vor Ort". In der numerischen Auswertung der Fehlerbäume wird jedoch einerseits der Ausfall dieser Handmaßnahme (L630 OP RA11/12 beim kleinen Leck am Druckhalter und L620 OP RA11/12 beim kleinen Leck in einer Hauptkühlmittelleitung) jeweils mit der Wahrscheinlichkeit 1 bewertet, andererseits der Eintritt des Überdruckversagens (W_9) mit der Wahrscheinlichkeit 0 angesetzt, so daß sich die genannten Unterschiede in den Ergebnissen nicht auswirken.

7.2.2.2.9 Fehlerbaum 11: Öffnen der Druckentlastung des Reaktorkühlkreislaufes

Ein Ausfall des ÖFFNENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS liegt vor, wenn sowohl beide Druckhalter-Abblaseventile als auch beide Druckhalter-Sicherheitsventile nicht öffnen.

Für das Öffnen eines Sicherheitsventils wird der Abwurf der magnetischen Zusatzbelastung nicht berücksichtigt, da auch bei de-

ren Ausfall ein Überdruckversagen des Reaktorkühlkreislaufs aus zuschließen ist. Im übrigen gilt die im Fehlerbaum 11 verwendete Ausfallrate für ein vollständiges Sicherheitsventilsystem, d.h. es sind Hauptventil, Steuerventile und Absperrarmaturen mit den entsprechenden Zuleitungen enthalten.

Der Ausfall eines Druckhalter-Abblaseventils ist gegeben, wenn das Abblaseventil selbst oder das zugehörige Steuerventil nicht öffnet.

Die Wahrscheinlichkeit eines CMA aller Druckhalterventile, genauer aller Steuerventile oder aller Hauptventile, wird als vernachlässigbar gering angesehen, da die Abblase- und Sicherheitsventile nach unterschiedlichen Funktionsprinzipien arbeiten und demnach auch unterschiedliche Bauarten aufweisen (Abschnitt 4.2.4). Diese Diversität gilt sowohl für die Steuereinrichtungen als auch für die Hauptventile.

Die Energieversorgung der Abblase-Steuerventile erfolgt über die Schiene 22 FR20. Ist diese Schiene ausgefallen, so läßt sich keines der beiden Abblaseventile öffnen.

Sind die Abblase-Absperrventile 20 YP01 S020 bzw. 20 YP01 S024 oder die Steuer-Absperrventile 20 YP01 S050 bzw. 20 YP01 S049 fälschlicherweise geschlossen, so kann über den entsprechenden Abblasestrang nicht abgeblasen werden. Im Normalbetrieb kann es zu diesem Ausfall nur kommen, wenn erstens die Verriegelung dieser Ventile so ausfällt, daß die Ventile nicht automatisch öffnen und zweitens das Wartenpersonal die Stellungsmeldung übersieht. Beim Störfall können diese Ventile nur dann fälschlicherweise geschlossen werden, wenn die Rückmeldung "Abblaseschieber AUF" fälschlicherweise ansteht und wenn durch einen zusätzlichen Ausfall die Ventile geschlossen werden. Da es im letztgenannten Fall nur aufgrund von Dreifachausfällen zum Versagen der beiden Abblaseventile kommen kann, werden die Ausfallkombinationen gegenüber den möglichen CMA der Meßwerterfassung für die Regelung oder den möglichen Doppelausfällen vernachlässigt. Das Steuerventil eines Abblaseventils kann nicht geöffnet werden, wenn die 2v3-Auswahleinheit, der von dieser angesteuerte

Speicher, das daran angeschlossene Schütz oder die Steuerkette ausfallen. Diese Komponentenausfälle sind in einem Funktionselementausfall zusammengefaßt.

Beide Steuerventile der Abblaseventile werden nicht geöffnet, wenn zwei der drei Stränge der Kühlmitteldruckregelung ausfallen. Da diese Regelung ein Betriebssystem ist und nicht nur die Abblaseventile, sondern auch die Heizung und Sprühung der Druckhalter ansteuert, ist ein großer Teil der auftretenden Ausfälle selbstmeldend und kann daher vernachlässigt werden. Nachteilig wirkt sich allerdings aus, daß der Ausfall von nur einem Strang der Regelung in vielen Fällen auch nicht bei den Funktionsprüfungen entdeckt wird, da die Ausgangssignale der Regelung in 2v3-Wertungsschaltungen verarbeitet werden. Auf diese Weise besteht die Möglichkeit, daß Einzelausfälle in der Betriebszeit der Anlage nicht oder erst bei Auftreten eines ähnlich wirkenden Ausfalls in einem anderen Strang der Regelung bemerkt werden.

Zum Ausfall eines Stranges der Regelung kommt es, wenn der Analog/Digital-Umsetzer bzw. der Code-Umsetzer so ausfällt, daß nur Drücke über den bei Normalbetrieb vorliegenden Druckwerten nicht umgesetzt werden. Da davon ausgegangen wurde, daß die Ziffernanzeige an den Code-Umsetzer des 2. Regelungsstranges angeschlossen ist, ist der Anteil der nicht selbstmeldenden Ausfälle für diese Funktionselemente niedriger angesetzt. Der Ausfall eines Stranges der Regelung ist auch möglich, wenn der Meßkanal dieses Stranges einen konstanten, unterhalb der Ansprechwerte der Abblaseventile liegenden Wert ausgibt. Ein solcher Ausfall führt aber, zusammen mit anderen ähnlich wirkenden Ausfällen in einem anderen Regelungsstrang, auch zum Versagen der übrigen Regelungsfunktionen und wird damit bei einer betrieblichen Anforderung dieser Funktionen sofort entdeckt. Bei einem Kurzschluß zwischen zwei Regelungssträngen kann ein falscher Wert in einem Regelungsstrang in den redundanten Strang übernommen werden. In diesem Zusammenhang wird nochmals darauf hingewiesen, daß die Ausfallraten der betrieblichen Steuer- und Regelungseinrichtungen in Anlehnung an die Betriebserfahrung mit ähnlichen Systemen abgeschätzt wurden. Diese Vorgehensweise wird als ausreichend angesehen, da alle diese Funktionselement-Ausfälle nur einen geringen Einfluß auf das Ergebnis haben.

7.2.2.2.10 Fehlerbaum 12 : Schließen der Druckentlastung des Reaktorkühlkreislaufes

Für den Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG DES REAKTOR-KÜHLKREISLAUFS werden (nach den in Abschnitt 7.2.1 getroffenen Voraussetzungen) zwei Fälle unterschieden:

- Ausfall des Schließens eines Druckhalter-Abblasestranges (bei funktionierender NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE),
- Ausfall des Schließens eines von zwei Druckhalter-Abblasesträngen (bei ausgefallener NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE).

Der Ausfall des Schließens eines Druckhalter-Abblasestranges liegt vor, wenn das Abblaseventil und das Abblaseabsperrventil dieses Stranges nicht schließen. Das Nichtschließen des Abblaseventils kann folgende Ursachen haben:

- Das Abblaseventil selbst schließt nicht.
- Das Steuerventil und das Steuer-Absperrventil schließen nicht.
- Der Schließbefehl durch die Druckhalter-Regelung, die Handbefehle und das Reaktorschutzsignal 22 YZ37 (Reaktorkühlkreisabschlußsignal) fallen aus.
- Die Energieversorgung für das Steuerabsperrventil fällt aus bei gleichzeitigem Versagen der Schließfunktion des Steuerventils.

Zum Ausfall der Schließfunktion des Abblase-Absperrventils tragen bei:

- Nichtschließen des Abblase-Absperrventils selbst,
- Ausfall der Energieversorgung des Abblase-Absperrventils,
- Ausfälle, die zum Unterdrücken des Schließbefehls durch die Steuerung führen.

Der Beitrag der Druckhalter-Sicherheitsventile zur Wahrscheinlichkeit des kleinen Lecks am Druckhalter ist nur für den Fall der VERZÖGERTEN NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE berücksichtigt worden. Nur in diesem Fall werden beide Abblasestränge in der Öffnungsfunktion angefordert und bei einem Versagen würde es dann zum Ansprechen des 1. Sicherheitsventils kommen.

Für den TOP des Fehlerbaumes "Druckentlastung des Reaktorkühlkreislaufes" wurden Ausfälle in der Meßwerterfassung, -verarbeitung und im gemeinsamen Teil der Regelung nicht unterstellt, da diese Ausfälle entweder über Vergleicher selbstmeldend sind oder bereits ein Versagen der vorher geforderten Öffnungsfunktion zur Folge gehabt hätten. CMA in der Meßwerterfassung, -verarbeitung und im gemeinsamen Teil der Regelung blieben nur dann unbemerkt, wenn sie sich nicht auf die Öffnungsfunktion auswirken würden. Bei dem hier vorliegenden Aufbau von Messung und Regelung kann dieser Einfluß vernachlässigt werden.

Für den Ausfall des Schließbefehls der Regelung wurden nur Ausfälle in der Ausgabe der Ausgangssignale berücksichtigt (2v3-Glieder, Speicher, NOR-Gatter, Leistungsverstärker, Relais).

Die verwendeten Ausfallraten sind im Fachband 3 der vorliegenden Studie enthalten. In einigen Einzelfällen wurden die Ausfallraten in Anlehnung an die Betriebserfahrung mit vergleichbaren Komponenten abgeschätzt. Die Handeingriffe wurden analog zur Vorgehensweise in WASH-1400 bewertet. Bei Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS und ausgefallener NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE (Fehlerbaum 12 B) wurde für den Ausfall der Kühlmitteldruckregelung die Wahrscheinlichkeit p = 1 angesetzt. Bei VERZÖGERTER NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE kommt es zu einer fortlaufenden Dampfabgabe in den Abblasetank. Dadurch sprechen nach wenigen Minuten dessen Berstscheiben an. Der dann aus dem Druckhalterabblasetank ausströmende Dampf kann in kurzer Zeit zum Ausfall der nicht für diese Umgebungsbedingungen ausgelegten Meßwerterfassung der Kühlmitteldruckregelung führen, ebenso zum Ausfall der Druckmessung am Abblasebehälter selbst.

Zum Ausfall des Reaktorschutzsignals 22 YZ37 (Reaktorkühlkreisabschlußsignal) tragen die CMA der Meßkanäle der Wasserstandsmessung am Druckhalter sowie der Ausfall des Abschlußrelais und der Stromversorgung bei.

Bei der Bewertung der Wahrscheinlichkeit eines Handeingriffs wegen fälschlich nicht schließender Abblaseventile muß zwischen

funktionierender und ausgefallener NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE unterschieden werden, da im ersten Fall nur der 1. Abblasestrang betroffen ist. Im zweiten Fall muß weiter unterschieden werden, ob das Reaktorschutzsignal YZ37 ausgefallen ist oder ob dieses Signal ausgegeben wird. Dabei ist zu beachten, daß die Abblasearmaturen bei sinkendem Druckhalterwasserstand bei einem Niveau < 2,85 m geschlossen werden, wonach der Druckhalterwasserstand wieder ansteigt und die Abblaseventile erneut öffnen usw. Das bedeutet, daß das Reaktorschutzsignal in diesem Fall intermittierend ausgegeben wird.

In den Fehlerbäumen wird bei Ausfall des Reaktorschutzsignals die Wahrscheinlichkeit des Handeingriffs mit p = 1 bewertet, da es sich um eine nicht geplante Handmaßnahme handelt. Für den Fall des fälschlichen Schließens der beiden Druckhalter-Abblasestränge bei intermittierend anstehendem Reaktorschutzsignal YZ37 wird eine Wahrscheinlichkeit von p = 0,5 eingesetzt.

Die Ausfallrate für das Unterdrücken des Schließbefehls durch die Verriegelung enthält diejenigen für den Ausfall der Bausteine der Verriegelungsebene (UND-Gatter, Zeitstufe) sowie der 24-V-Stromversorgung des Verriegelungsschrankes (Stromversorgungsstufen und Kurzschlüsse in der Verdrahtung).

Der Ausfall der 24-V-Versorgung der Betätigungsschränke muß nur für die Steuerabsperrarmatur und das Abblaseabsperrventil unterstellt werden, da das Abblasesteuerventil von einem anderen Betätigungsschrank aus angesteuert wird, wobei der Ausfall dann bereits ein Versagen der Öffnungsfunktion zur Folge gehabt hätte.

Die Ausfallart "Steuerventil bleibt in Zwischenstellung hängen", führt zum Ausfall auch des Steuer-Absperrventils, da dessen Verriegelung dann ein automatisches Zufahren verhindert. Ein zusätzlicher Ausfall in der Ansteuerung oder Stromversorgung des Abblase-Absperrventils oder der Ausfall des Ventils selbst führt zum Ausfall des jeweiligen Abblasestranges.

Zu einem kleinen Leck am Druckhalter über das 1. Druckhalter-Sicherheitsventil kann es dann kommen, wenn bei Versagen der

NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE entweder beide Abblasestränge nicht geöffnet haben oder wenn beide Abblasestränge fälschlich von Hand geschlossen wurden. Der Druck im Reaktorkühlkreislauf bzw. im Druckhalter steigt dann bis zum Ansprechdruck des 1. Sicherheitsventils an. Darüber hinaus ist mit einem Fehlansprechen der Sicherheitsventile zu rechnen, wenn die magnetische Zusatzbelastung dieser Ventile vorzeitig abgeworfen wird. Es wird pessimistisch angenommen, daß beim Störfall "Notstromfall" mit Versagen der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE ein derartiger Ausfall der magnetischen Zusatzbelastung eintritt (Abschnitt 7.2.1). Liegt der Ansprechdruck eines der Sicherheitsventile unter dem des 2. Druckhalter-Abblaseventils, z.B. aufgrund fehlerhafter Einstellung, so öffnet dieses Ventil. Der Ausfall des Schließens führt dann zum kleinen Leck. Eine Abschätzung zeigt, daß das Ergebnis für das kleine Leck am Druckhalter aufgrund dieser Ausfallkombination nur unwesentlich beeinflußt wird, auch wenn pessimistisch unterstellt wird, daß das 1. Druckhalter-Sicherheitsventil bei Ausfall der magnetischen Zusatzbelastung mit der Wahrscheinlichkeit 1 öffnet.

7.2.2.2.11 Fehlerbaum 16: Lüftungsanlagen

Beim "Notstromfall" ist die Umluftanlage für die Notstromdieselräume zu betrachten (Fehlerbaum 16 B). Abweichend zu den Kühlmittelverluststörfällen, liegt der Ausfall der Ansteuerung der Umluftkühlung für einen Notstromdiesel vor, wenn die Rückmeldung DIESELGENERATORSCHALTER EIN nicht ansteht.

Für ein "kleines Leck am Druckhalter beim Notstromfall" ist wie für ein "mittleres Leck in einer Hauptkühlmitteilleitung" und ein "kleines Leck in einer Hauptkühlmittelleitung" die Umluftanlage der HD-Sicherheitseinspeisepumpen erforderlich. Aus Gründen der Vereinfachung wird bei den Rechnungen für ein "kleines Leck am Druckhalter beim Notstromfall" der Fehlerbaum 16 A für die Kühlmittelverluststörfälle verwendet. Dieses Vorgehen ist bezüglich der Ansteuerung der Umluftkühlung für die Notstromdiesel pessimistisch, da ein Ausfall nur vorliegt, wenn sowohl die Rückmeldung DIESELGENERATORSCHALTER EIN als auch der EIN-Befehl durch

die Notstromvorbereitungssignale nicht ansteht. Im Fehlerbaum 16 A ist dagegen nur das Einschalten durch die Reaktorschutzsignale berücksichtigt.

7.2.2.2.12 Fehlerbäume 17 und 18: Not- und Nachkühlsystem

Die Fehlerbäume 17 und 18 werden nur für "kleines Leck am Druckhalter beim Notstromfall" benötigt. Es ergeben sich keine Abweichungen gegenüber der Beschreibung dieser Fehlerbäume für die Kühlmittelverluststörfälle (Abschnitte 6.1.2.2.17 und 6.1.2.2.18).

In der numerischen Auswertung werden wie beim "kleinen Leck in einer Hauptkühlmittelleitung" die Funktionselemente LOCA 1 bis LOCA 4 = 0 gesetzt.

7.2.2.3 Teilfehlerbäume für die elektrische Energieversorgung

Die Fehlerbäume 13 und 14 (Anhang 3) sind identisch mit denjenigen für die Kühlmittelverluststörfälle.

Bezüglich folgender CMA gelten bei den Transienten die gleichen Bedingungen wie bei den Kühlmittelverluststörfällen:

- CMA von Verbraucherabzweigen und
- Unterspannung an den Sammelschienen.

Zusätzlich ist bei den Transienten die Möglichkeit einer Überspannung auf sämtlichen Sammelschienen zu betrachten.

Bei einem Lastabwurf des Kraftwerks wird der Turbosatz auf Eigenbedarfsleistung abgefangen. Dabei wird der Erregerstrom des Hauptgenerators zuerst vermindert und danach hochgeregelt, bis die Nennspannung wieder erreicht ist. Dieser Regelvorgang ist mit einer transienten Spannungserhöhung verbunden, die vom Belastungszustand des Generators vor dem Lastabwurf abhängt. Als transiente Spannungserhöhungen wurden bei Lastabwurfversuchen folgende Werte gemessen:

Abwurf von 80 % Nennleistung auf Eigenbedarf:

$\Delta U_{Generator} = 23\ \%,\ \Delta U_{10\ kV} = 19{,}5\ \%$

Abwurf von 100 % Nennleistung auf Eigenbedarf:

$\Delta U_{Generator} = 19\ \%,\ \Delta U_{10\ kV} = 18{,}4\ \%$

Überspannungen in dieser Größenordnung dürften keine Schäden an den 10-kV- bzw. 0,4-kV-Drehstromverbrauchern verursachen. Die 24-V-Gleichstromverbraucher reagieren jedoch empfindlicher auf Spannungsveränderungen, weshalb die Ausgangsspannung der Gleichrichter überwacht wird. Die Überwachungsorgane der Gleichrichter schalten diese bei einer Ausgangsspannung von mehr als 31,7 V unverzögert ab, bei 30,5 V mit einer Verzögerungszeit von 0,4 Sekunden. Bei einem Lastabwurf von 100 % auf Eigenbedarf wurde am Ausgang eines Gleichrichters eine transiente Spannungserhöhung auf 31,5 V gemessen, d.h., der entsprechende Grenzwert wurde nur knapp unterschritten. Da der zeitliche Verlauf der Eingangsspannung des Gleichrichters bei einem Lastabwurf vom Belastungszustand des Generators abhängt, ist deshalb damit zu rechnen, daß bei einem Teil der Lastabwürfe die Gleichrichter abgeschaltet werden. Es kann jedoch davon ausgegangen werden, daß die bis zur Entladung der Batterien zur Verfügung stehende Zeit für eine Wiederinbetriebnahme der Gleichrichter ausreicht.

7.2.2.4 Teilfehlerbäume für das Reaktorschutzsystem

Zur Aufstellung der Teilfehlerbäume für die im Notstromfall vom Reaktorschutzsystem gebildeten Signale kann auf die bereits bei den Kühlmittelverluststörfällen diskutierten Ausfallursachen zurückgegriffen werden. Zusätzlich ist zu beachten, daß die Komponenten NSF und KMV im Teilfehlerbaum "Kurzschluß in den RT-Schränken 21-24 IK21" die Werte p = 1 bzw. p = 0 annehmen.

7.2.3 Bewertung der leittechnischen Komponenten

Die Berwertung der in den Fehlerbäumen verwendeten leittechnischen Komponenten erfolgt analog zu Abschnitt 6.1.3. Im folgen-

den wird lediglich auf die an dieser Stelle noch nicht beschriebenen Teilsysteme eingegangen.

Kennzeichnung	Ausfallbeschreibung	$\lambda_{50}[10^{-6}/h]$ bzw. p_{50} /Streufaktor
L494 22 YP01 S121 L495 22 YP01 S125	Speicher, 2v3-Auswahleinheit oder Steuerkette für Abblaseventil unterdrücken AUF-Befehl	$\lambda_{50} = 2,3$ K = 3
L503 CMA YP01	CMA der Meßkanäle der Kühlmitteldruck-Regelung	$p_{50} = 10^{-3}$ K = 3
L564 20 YP01 S050 L565 20 YP01 S024 L567 20 YP01 S020 L568 20 YP01 S049	Ausfall des Schließbefehls für die Abblase-Absperrventile durch die Verriegelung (1 Endschalter spricht nicht an, 1 UND-Gatter, 1 analoge Zeitstufe geben kein Signal aus, 24-V-Versorgungsspannung im Verriegelungsschrank ausgefallen)	$\lambda_{50} = 12$ K = 3

7.2.4 Bewertung der Handmaßnahmen

In diesem Abschnitt wird die Bewertung derjenigen Handmaßnahmen erläutert, denen nur in der Zuverlässigkeitsanalyse von Transienten Bedeutung zukommt.

L 485 OP RX10/20 — Keine verzögerte Inbetriebnahme des Notstandssystems innerhalb von etwa 30 bis 75 Minuten nach Eintritt des Notstromfalls.
$p_{50} = 6 \cdot 10^{-2}/K = 3$

Die Bewertung erfolgt auf Basis der Methode in der AIPA-Studie (Abschnitt 3.4.3). Für die Maßnahme stehen 45 Minuten zur Verfügung, im Mittel werden zur Inbetriebnahme des Notstandssystems 16 Minuten benötigt.

L 488 OP RX20 S005
L 489 OP RX20 S006

Stellventil wird beim Störfall und offenen FD-Sicherheitsventil fälschlich in AUF-Stellung gefahren oder in AUF-Stellung belassen.
$p_{50} = 10^{-1}/K = 3$

Störfälle, die eine Inbetriebnahme des Notstandssystems erfordern, stellen für die Betriebsmannschaft eine hohe Streßbelastung dar. Das Offenbleiben eines sekundärseitigen Sicherheitsventils wirkt störfallverschärfend, so daß man auch bei verzögerter Inbetriebnahme des Notstandssystems noch eine Handlung unter hoher Streßbelastung ansetzen muß. Gemäß WASH-1400 ist dafür eine Fehlerwahrscheinlichkeit von $p_{50} = 10^{-1}$ anzusetzen. Personelle Redundanz sowie ein Fehlerentdeckungsfaktor (recovery factor) werden dabei nicht berücksichtigt.

Das mögliche Offenbleiben eines sekundärseitigen Sicherheitsventils ist in der Logikfahne des Betriebshandbuches für die Inbetriebnahme des Notstandssystems nicht berücksichtigt. Dieser Anlagenzustand ist jedoch durch die Anzeigen an der Notstandstafel (Dampferzeugerwasserstand, Frischdampfdruck) sofort eindeutig erkennbar und läßt eine entsprechende Reaktion des Bedienungspersonals erwarten.

L 490 OP RX20

Kein Auffahren der Stellventile von Hand und vor Ort
$p = 1$

Das Auffahren der Stellventile von Hand und vor Ort ist nicht vorgesehen. Es wird daher als nicht geplanter Handeingriff mit $p = 1$ bewertet.

L 501 OP YP1 ST1/2

Kein ZU-Befehl für Druckhalter-Abblasestränge 1 und 2 bei Nichtschließen der Abblaseventile
$p = 1$

Es handelt sich um einen ungeplanten Handeingriff, der mit p_{50} = 1/K = 1 zu bewerten ist.

L 502 OP YP1 ST1 Kein ZU-Befehl für Druckhalter-Abblasestrang 1 bei Nichtschließen des Abblaseventils
p = 1

Die Bewertung entspricht der von L 501.

L 542 OP RA11/12 Kein AUF-Befehl von Hand für Abblase-Absperrschieber und Abblaseregelventile, um Überdruckversagen zu verhindern, innerhalb von ca. 15 Minuten nach Eintritt des Notstromfalls.
p_{50} = 0,1/K = 5

Die für die Durchführung der Maßnahme zur Verfügung stehende Zeit wurde wie folgt ermittelt: Nach einer Untersuchung wird in der Frischdampfleitung nach ca. 12 bis 15 Minuten ein Druck von 103 bar erreicht, sofern das Frischdampf-Sicherheitsventil nicht vorher öffnet. 30 Minuten nach Eintritt des Notstromfalls ist ein Überdruckversagen nicht mehr auszuschließen. Die drehmomentabhängigen Endschalter der Regelventilantriebe sind jedoch auf ein Nenndrehmoment eingestellt, das bei einem Druck von 103 bar in der Abblaseleitung erreicht wird.

Auf die Notwendigkeit einer sekundärseitigen Druckentlastung wird außer durch Gefahrmeldungen und eine Notgefahrmeldung sowie durch Anzeigen hingewiesen. Es wurde einfache personelle Redundanz für diese Maßnahme unterstellt, da unseres Erachtens ein Reaktorfahrer gemeinsam mit dem Schichtleiter diese Maßnahme durchführen wird, während der andere Reaktorfahrer mit der Beobachtung des Steuerpultes und der Geräte der Wartenwandtafel voll beansprucht ist. In Anlehnung an WASH-1400 ist für Handlungen ca. 15 Minuten nach Eintritt des Notstromfalls eine Fehlerwahrscheinlichkeit von etwa $p_{50} = 3 \cdot 10^{-1}$ anzusetzen. Die Berücksichtigung der personellen Redundanz liefert dann das obige Ergebnis.

L 544 OP RX10/20 Keine Inbetriebnahme des Notstandssystems innerhalb von 30 Minuten nach Eintritt des Notstromfalls

$p_{50} = 2 \cdot 10^{-1}/K = 2$

Die Bewertung lehnt sich an die Vorgehensweise in der AIPA-Studie an. Etwa 6 Minuten nach Eintritt des Notstromfalls werden als Mindestzeitspanne für das Erkennen und die Durchführung der Maßnahme berücksichtigt, so daß eine Exponentialverteilung nur für die restlichen 24 Minuten angesetzt wird.

L 561 OP RX10/20C Kein Abfahren mittels Notstandssystems innerhalb von 2 bis 3 Stunden nach Störfall-ein tritt (kleines Leck am Druckhalter)

$p_{50} = 10^{-3}/K = 7$

Spätestens beim Einleiten des Abfahrens wird das Personal im Block B die Notwendigkeit der Inbetriebnahme des Notstandssystems zum Abfahren erkennen. Dies ist ca. 30 Minuten nach Störfalleintritt der Fall. Für diese Maßnahme wird personelle Redundanz in Form des Schichtleiters und der beiden Reaktorfahrer angesetzt. Damit ergibt sich ein Wert von $p_{50} = 10^{-3}/K = 7$.

L 571 OP RX10/20 Keine Inbetriebnahme des Notstandssystems innerhalb von 2 bis 3 Stunden nach Störfall-eintritt (kleines Leck am Druckhalter)

$p_{50} = 5 \cdot 10^{-4}/K = 10$

Bei diesem Störfall steht relativ viel Zeit zur Durchführung der Maßnahme zur Verfügung. Die Bewertung lehnt sich an die AIPA-Studie an (MTOR = 16 Minuten).

L 580 OP RA11/12 Kein Einleiten des Abfahrens (kein AUF-Befehl von Hand für Abblase-Absperrschieber und Abblaseregelventile) innerhalb von 2 bis 3 Stunden nach Störfalleintritt (kleines Leck am Druckhalter)

$p_{50} = 10^{-5}/K = 12$

Das Abfahren soll entsprechend den Anweisungen des Betriebshandbuches spätestens 30 Minuten nach Störfalleintritt eingeleitet werden. Vom dynamischen Ablauf des Störfalles stünden ca. 2 bis 3 Stunden Zeit dafür zur Verfügung. Pessimistisch kann jedoch davon ausgegangen werden, daß im Falle des Nichterkennens der Notwendigkeit des Abfahrens innerhalb von 30 Minuten auch im weiteren Störfallverlauf die Notwendigkeit des Abfahrens nicht erkannt wird.

Es wird personelle Redundanz in Form des Schichtleiters und der beiden Reaktorfahrer angesetzt, da die Notwendigkeit des Abfahrens aufgrund verschiedener Meldungen für alle drei Personen ersichtlich ist. In Anlehnung an WASH-1400 ergibt sich für eine Handlung 30 Minuten nach Störfalleintritt bei entsprechender personeller Redundanz eine Fehlerwahrscheinlichkeit von

$$p_{50} = 10^{-3}/K = 7$$

Bei Fehlhandlung ist aufgrund einer Reihe von Anzeigen eine Fehlerentdeckung möglich. Außerdem weist eine nichtabschaltbare Notgefahrmeldung auf die entsprechende Logikfahne des Betriebshandbuches hin. Für das Nichtbeachten dieser Meldung ist personelle Redundanz anzusetzen, so daß sich dafür eine Wahrscheinlichkeit $p_{50} = 10^{-2}/K = 5$ ergibt. Berücksichtigt man pessimistisch keinen zusätzlichen Fehlerentdeckungsfaktor durch die Anzeigen, so erhält man insgesamt

$$p_{50} = 10^{-5}/K = 12$$

L 581 OP RA11/12C Abfahren mit falschem Abfahrgradienten innerhalb von 2 bis 3 Stunden nach Störfalleintritt (kleines Leck am Druckhalter)
$p_{50} = 10^{-5}/K = 7$

Der dynamische Ablauf des Störfalles erfordert ca. 2 bis 3 Stunden nach Störfalleintritt Abfahren der Anlage mit einem Abfahrgradienten von ca. 100 °C/h. Wird erst zu diesem Zeitpunkt und mit einem wesentlich kleineren Gradienten, d.h. zu langsam abgefahren, reicht der Wasservorrat nicht für das Abfahren der Anla-

ge aus. Die Bedeutung der Handlung ist der Bedienungsmannschaft bekannt. Die Maßnahme selbst, Einzeichnen des Abfahrgradienten auf Schreiberstreifen o.ä., ist relativ kompliziert. Es wird personelle Redundanz in Form des Schichtleiters und eines Reaktorfahrers angesetzt, da der andere Reaktorfahrer mit der Beobachtung von Anzeigen und Meldungen voll beschäftigt sein wird. Nach WASH-1400 sind Maßnahmen mehrere Stunden nach Störfalleintritt mit $p_{50} = 10^{-2}$ zu bewerten, damit ergibt sich unter Berücksichtigung der personellen Redundanz $p_{50} = 10^{-4}$.

Wegen der Bedeutung der Maßnahme ist eine häufige Kontrolle der Anzeige und des Schreiberstreifens notwendig. Außerdem ist die für eine gefährliche Auswirkung nötige, gravierende Abweichung vom Sollgradienten relativ leicht zu erkennen. Daher wird zusätzlich ein Fehlerentdeckungsfaktor (recovery factor) von $p_{50} = 10^{-1}$ berücksichtigt.

L 625 OP YP01 ST1/2 — Fälschlicher ZU-Befehl von Hand für Druckhalter-Abblasestränge 1 und 2 bei wiederholtem Ansprechen des Reaktorschutzsignals YZ37

Es handelt sich um eine nach dem Betriebshandbuch nicht geplante Handmaßnahme. Jedoch muß in diesem Fall bei wiederholtem Ansprechen des Reaktorschutzsignals YZ37 während des Störfalles davon ausgegangen werden, daß dieses Signal der höchsten Prioritätsklasse vom Wartenpersonal nicht ignoriert wird.

Dieses Signal ist so speziell mit dem Druckhaltesystem verknüpft, daß man mit hoher Wahrscheinlichkeit davon ausgehen kann, daß der Reaktorfahrer nach mehrmaligem Ansprechen des Signals das gesamte Druckhaltesystem kontrolliert, dabei ein Leck vermutet und die Abblaseleitungen fälschlich absperrt. Da eine genauere Bewertung nicht möglich ist, wird abgeschätzt, daß für die Hälfte aller Fälle eine Fehlbetätigung unterstellt wird, d.h.

$$p_{50} = 0,5/K = 3$$

L 630 OP RA11/12 Kein Auffahren der Abblase-Absperrschieber von Hand und vor Ort innerhalb 2 bis 3 Stunden nach Störfalleintritt
p = 1

Die Bewertung entspricht der Begründung bei der Handmaßnahme L 620 (Abschnitt 6.1.4).

7.2.5 Ergebnisse

7.2.5.1 N o t s t r o m f a l l

Die Wahrscheinlichkeit für das Versagen der Systemfunktionen, die zur Beherrschung des Notstromfalls erforderlich sind, wurde zu

$$\bar{m} = 1{,}3 \cdot 10^{-4}$$

ermittelt. Unter Berücksichtigung der Unsicherheiten der Komponentendaten ergibt sich ein Medianwert von $m_{50} = 9 \cdot 10^{-5}$ und ein Unsicherheitsfaktor K = 4 für den 90-%-Vertrauensbereich.

Durch Multiplikation mit der Häufigkeit des Notstromfalls ergibt sich für die Häufigkeit des nicht beherrschten Notstromfalls ein Medianwert $m_{50} = 7 \cdot 10^{-6}$ und ein Unsicherheitsfaktor K = 6 (siehe hierzu auch Bild F2, 3-5 in Abschnitt 3.2.3.5).

Im folgenden wird auf die Nichtverfügbarkeiten der einzelnen Systemfunktionen eingegangen, wie sie sich aus den Fehlerbäumen ergeben (Bild F2, 7-3). Außerdem werden diejenigen Verknüpfungen des Gesamtfehlerbaums behandelt, die zum "kleinen Leck am Druckhalter" und "ATWS-Störfall Notstromfall" führen (Abschnitt 7.5 und 7.6). Anhand der Verknüpfungen der Fehlerbäume wird erläutert, wie sich die bedingten Wahrscheinlichkeiten für die einzelnen Ereignisabläufe (Bild F2, 7-4) errechnen.

Die Versagenswahrscheinlichkeit der REAKTORSCHNELLABSCHALTUNG wird in Kapitel 8 zu $5 \cdot 10^{-6}$ ermittelt. Das Versagen der Reaktorschnellabschaltung führt zu einem ATWS-Störfall (Ereignisablauf T_1KI).

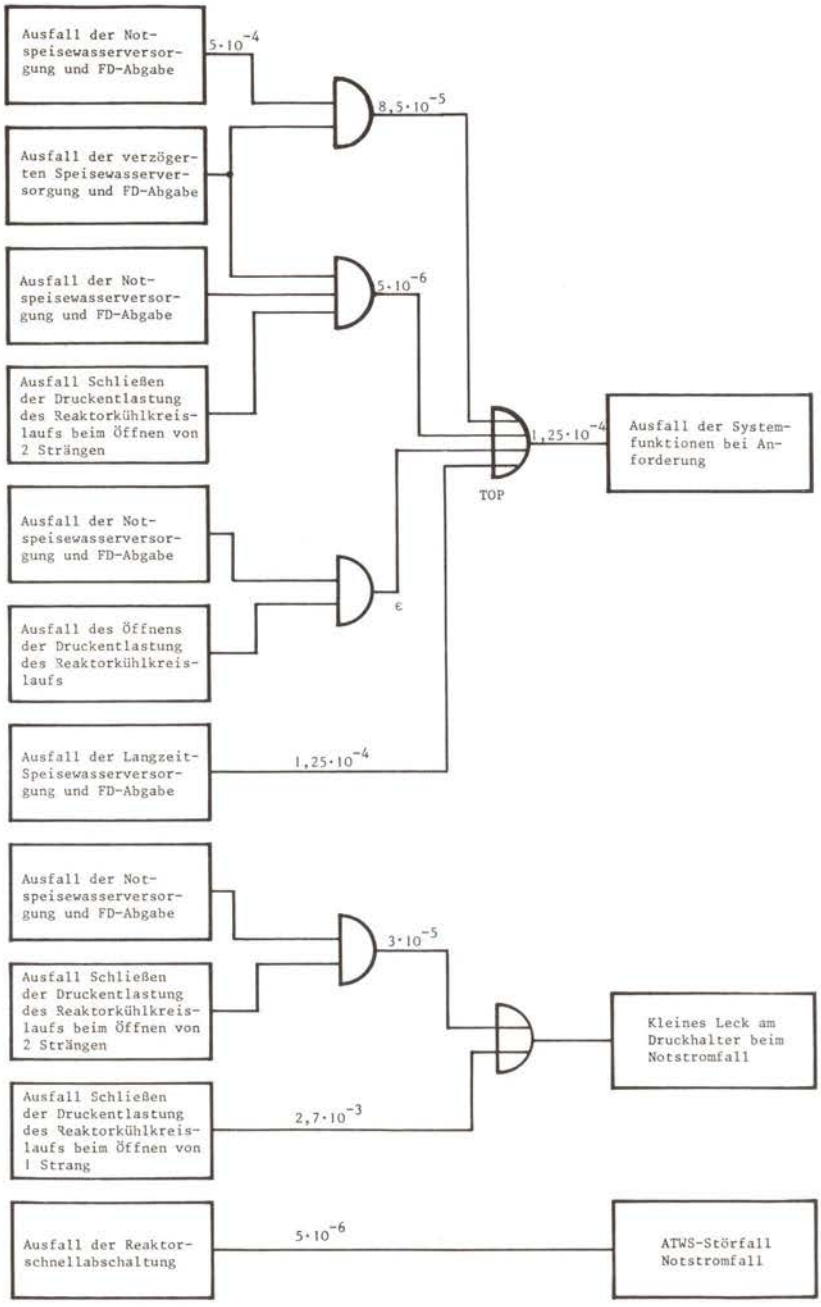
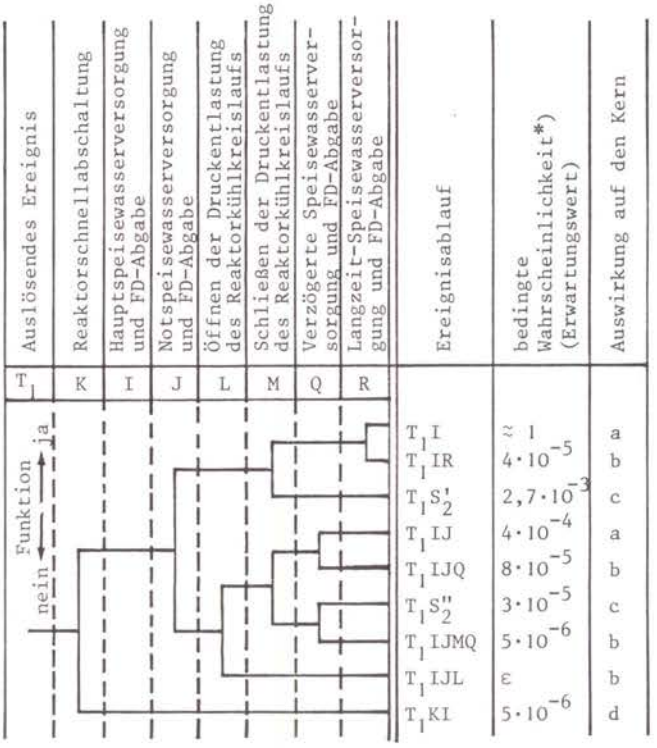


Bild F2, 7-3:

Mittlere Nichtverfügbarkeit der Systemfunktionen bei Anforderung durch einen "Notstromfall"



a kein Kernschmelzen
b Kernschmelzen
c Fortsetzung "kleines Leck am Druckhalter beim Notstromfall"
d Fortsetzung "ATWS-Störfälle"

*) Wahrscheinlichkeit der einzelnen Ereignisabläufe unter der Bedingung, daß das auslösende Ereignis eingetreten ist.
Die Häufigkeit der einzelnen Ereignisabläufe ergibt sich durch Multiplikation mit der Häufigkeit h des auslösenden Ereignisses.

$$h(T_1) = 0{,}1/a \text{ (Erwartungswert)}$$

Bild F2, 7-4:
Ereignisablaufdiagramm "Notstromfall"

Die Nichtverfügbarkeit der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE beträgt $5 \cdot 10^{-4}$. Von diesem Wert werden 80 % durch CMA der

Notstromdiesel verursacht. Wenn zusätzlich zur NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE auch die VERZÖGERTE SPEISEWASSERVERSORGUNG UND FD-ABGABE versagt, so führt dies zum nicht beherrschten Notstromfall. Die Nichtverfügbarkeit ergibt sich aus der UND-Verknüpfung beider Eingänge in den Gesamtfehlerbaum und beträgt $8{,}5 \cdot 10^{-5}$.

Für die logische UND-Verknüpfung folgender Eingänge in den Gesamtfehlerbaum erhält man eine Nichtverfügbarkeit von $5 \cdot 10^{-6}$:

- Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE,
- Ausfall der VERZÖGERTEN SPEISEWASSERVERSORGUNG UND FD-ABGABE,
- Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS beim Öffnen von zwei Strängen.

Diese Nichtverfügbarkeit entspricht der bedingten Wahrscheinlichkeit für den Ereignisablauf T_1IJMQ.

Die bedingte Wahrscheinlichkeit für den Ereignisablauf T_1IJQ ergibt sich aus der Differenz der beiden letztgenannten Nichtverfügbarkeiten mit $8{,}5 \cdot 10^{-5} - 0{,}5 \cdot 10^{-5} = 8 \cdot 10^{-5}$. Die Wahrscheinlichkeit für das Versagen der VERZÖGERTEN SPEISEWASSERVERSORGUNG UND FD-ABGABE unter der Bedingung, daß die NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE ausgefallen ist und das SCHLIESSEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS funktioniert, beträgt 0,16 ($8 \cdot 10^{-5}$ dividiert durch $5 \cdot 10^{-4}$). Ein Beitrag von $6 \cdot 10^{-2}$ zu diesem Wert resultiert aus der Wahrscheinlichkeit dafür, daß keine Inbetriebnahme des Notstandssystems von Hand innerhalb von 75 Minuten nach Störfalleintritt durchgeführt wird, unter der Bedingung, daß dies nicht bereits innerhalb der ersten 30 Minuten erfolgt ist. Der restliche Beitrag zu obiger Wahrscheinlichkeit für das Versagen der VERZÖGERTEN SPEISEWASSERVERSORGUNG UND FD-ABGABE bei Versagen der Notspeisewasserversorgung und FD-Abgabe ergibt sich durch Hardware-Ausfälle des Notstandssystems sowie Nichtschließen der FD-Sicherheitsventile in den Strängen 1 und 3.

Das gemeinsame Versagen der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE sowie des ÖFFNENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREIS-

LAUFS (Ereignisablauf T_1IJL) liefert keinen nennenswerten Beitrag zum Gesamtergebnis.

Für den Ereignisablauf T_1S_2'', d.h. den Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE und den Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS beim Öffnen von zwei Strängen ergibt sich eine bedingte Wahrscheinlichkeit von $3 \cdot 10^{-5}$. Dieser Ereignisablauf wird im Abschnitt 7.2.5.2 über "kleines Leck am Druckhalter beim Notstromfall" eingehend behandelt.

Die bedingte Wahrscheinlichkeit für den Ereignisablauf T_1IJ, bei dem der Notstromfall beherrscht ist, errechnet sich aus der Differenz zwischen der Nichtverfügbarkeit der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE sowie der Summe der bedingten Nichtverfügbarkeiten der Ereignisabläufe T_1IJQ bis T_1IJL:

$$5 \cdot 10^{-4} - (8 \cdot 10^{-5} + 3 \cdot 10^{-5} + 5 \cdot 10^{-6}) = 4 \cdot 10^{-4}$$

Entsprechend den Fehlerbäumen ergibt sich für den Ausfall der LANGZEIT-SPEISEWASSERVERSORGUNG UND FD-ABGABE eine Versagenswahrscheinlichkeit von $1{,}25 \cdot 10^{-4}$. Dies ist das Gesamtergebnis für den nicht beherrschten Notstromfall. Die bedingte Wahrscheinlichkeit für das Versagen der Systemfunktion der LANGZEIT-SPEISEWASSERVERSORGUNG UND FD-ABGABE (Ereignisablauf T_1IR) ergibt sich aus der Differenz zwischen dem Gesamtergebnis und der Wahrscheinlichkeit für das gemeinsame Versagen der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE sowie der verzögerten Speisewasserversorgung und FD-Abgabe mit $1{,}25 \cdot 10^{-4} - 8{,}5 \cdot 10^{-5} = 4 \cdot 10^{-5}$. Dieser Wert wird maßgeblich durch folgende Funktionselementausfälle bestimmt, von denen jeder zum Versagen der Notspeisestränge RL04 und RL05 im Langzeitbetrieb führt:

- Rückschlagklappe 20 RY10 S005 in der Deionatleitung zum Speisewasserbehälter schließt nicht,
- Druckfühler 20 RF50 P001 im Speisewasserbehälter spricht zu früh an.

Das SCHLIESSEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS kann als unabhängige Systemfunktion betrachtet werden, so daß

sich als bedingte Wahrscheinlichkeit für den Ereignisablauf T_1S_2' die Nichtverfügbarkeit der Verknüpfung "Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS beim Öffnen eines Stranges" mit $2{,}7 \cdot 10^{-3}$ (Median $2 \cdot 10^{-3}$, Streufaktor 4) ergibt. Der Ereignisablauf T_1S_2' beschreibt ein "kleines Leck am Druckhalter beim Notstromfall" (Abschnitt 7.2.2.1).

Zu einem Großteil der Wahrscheinlichkeit für das Versagen der Systemfunktionen, die zur Beherrschung des Notstromfalls erforderlich sind, tragen CMA von Notstromdieseln und menschliches Fehlverhalten bei. Weder CMA noch menschliche Fehlhandlungen führen allerdings nicht allein, sondern nur gemeinsam zu einem nicht beherrschten Störfall: Bei einem Versagen der Speisewasserversorgung aufgrund von CMA ist durch Handmaßnahmen eine Inbetriebnahme der Notspeisewasserversorgung vom Nachbarblock aus möglich, die ebenfalls ausfallen müßte. CMA durch Fehlkalibrieren von Meßkanälen spielen keine Rolle.

Die Wahrscheinlichkeit für den nicht beherrschten Notstromfall läßt sich folgendermaßen aufteilen:

- nur unabhängige Ausfälle der Hardware einschließlich Instandhaltung 26 %
- CMA der Notstromdiesel und unabhängige Ausfälle 29 %
- unabhängige Ausfälle und menschliches Fehlverhalten 27 %
- CMA der Notstromdiesel und menschliches Fehlverhalten 18 %

Um den Einfluß einer "Ausfallraten-Kopplung", wie in Abschnitt 3.3.5.6 beschrieben, zu ermitteln, wurden jeweils sämtliche gleichartige Funktionselement-Ausfälle der Hardware zu Gruppen zusammengefaßt (z.B. Startversagen Pumpe, Startversagen Diesel, Öffnungsversagen Motorarmaturen). Durch die Ausfallraten-Kopplung erhöht sich der Erwartungswert und die Streubreite des Ergebnisses nicht wesentlich. Bei der Durchsicht der minimalen Schnittmengen ergibt sich, daß Kombinationen gleichartiger Funktionselement-Ausfälle das Ergebnis nicht bestimmen, vielmehr der Einfluß der CMA der Notstromdiesel und des menschlichen Fehlverhaltens (Inbetriebnahme des Notstandssystems) dominiert.

7.2.5.2 Kleines Leck am Druckhalter beim Notstromfall

Für die mittlere Nichtverfügbarkeit der zur Beherrschung des kleinen Lecks am Druckhalter erforderlichen Systemfunktionen beträgt der Erwartungswert

$$\bar{m} = 2{,}6 \cdot 10^{-2}$$

Ein kleines Leck am Druckhalter liegt vor, wenn nach der beim Notstromfall erfolgenden Druckentlastung des Reaktorkühlkreislaufs die entsprechende Abblaseleitung nicht mehr abgesperrt werden kann. Es spielen dabei die zur Energieversorgung der Motorarmaturen notwendigen Notstromschienen eine Rolle, die andererseits auch die Nichtverfügbarkeit der zur Beherrschung des kleinen Lecks erforderlichen Systemfunktionen beeinflussen. Aufgrund dieser Abhängigkeit wird bei der numerischen Auswertung der Fehlerbäume stets die UND-Verknüpfung aus Eintritt des kleinen Lecks unter der Bedingung, daß der Notstromfall vorliegt, und Ausfall der Systemfunktionen gerechnet. Der so ermittelte Wert ist $7 \cdot 10^{-5}$ (Median $4 \cdot 10^{-5}$, Unsicherheitsfaktor 5). Dividiert man diesen Wert durch die bedingte Wahrscheinlichkeit für den Eintritt des kleinen Lecks, so führt das zur oben genannten Nichtverfügbarkeit der zur Beherrschung des Lecks erforderlichen Systemfunktionen.

Wie aus dem Ereignisablaufdiagramm für den "Notstromfall" hervorgeht (Bild F2, 7-4), führen zwei unterschiedliche Ereignisabläufe zu einem kleinen Leck am Druckhalter, nämlich T_1S_2' und T_1S_2''. Bei funktionierender NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE öffnet nur das 1. Druckhalter-Abblaseventil. Das Leck liegt dann vor, wenn nach erfolgter Druckentlastung die 1. Abblaseleitung nicht abgesperrt werden kann (T_1S_2'). Beim Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE J kommt es dagegen zum Ansprechen beider Druckhalter-Abblaseventile. Ein Leck tritt dann ein, wenn nach erfolgter Druckentlastung eine der beiden Abblaseleitungen nicht abgesperrt werden kann, wobei hier nur der Ablauf interessiert, bei dem die VERZÖGERTE SPEISEWASSERVERSORGUNG UND FD-ABGABE Q funktioniert (T_1S_2''). In beiden Fällen sind zwischen den

Systemfunktionen beim Notstromfall und dem Eintritt des kleinen Lecks zusätzliche Abhängigkeiten aufgrund der Notstromschienen gegeben. Die Ergebnisse für das nicht beherrschte kleine Leck werden zunächst getrennt für die Abläufe T_1S_2' und T_1S_2'' diskutiert.

Die bedingte Wahrscheinlichkeit für den Eintritt des kleinen Lecks am Druckhalter beim Ereignisablauf T_1S_2' ergibt sich zu $2,7 \cdot 10^{-3}$, wobei als Bedingung der Notstromfall zugrunde gelegt wird (Abschnitt 7.2.5.1). Als mittlere Nichtverfügbarkeit der zur Beherrschung dieses kleinen Lecks erforderlichen Systemfunktionen erhält man einen Erwartungswert von

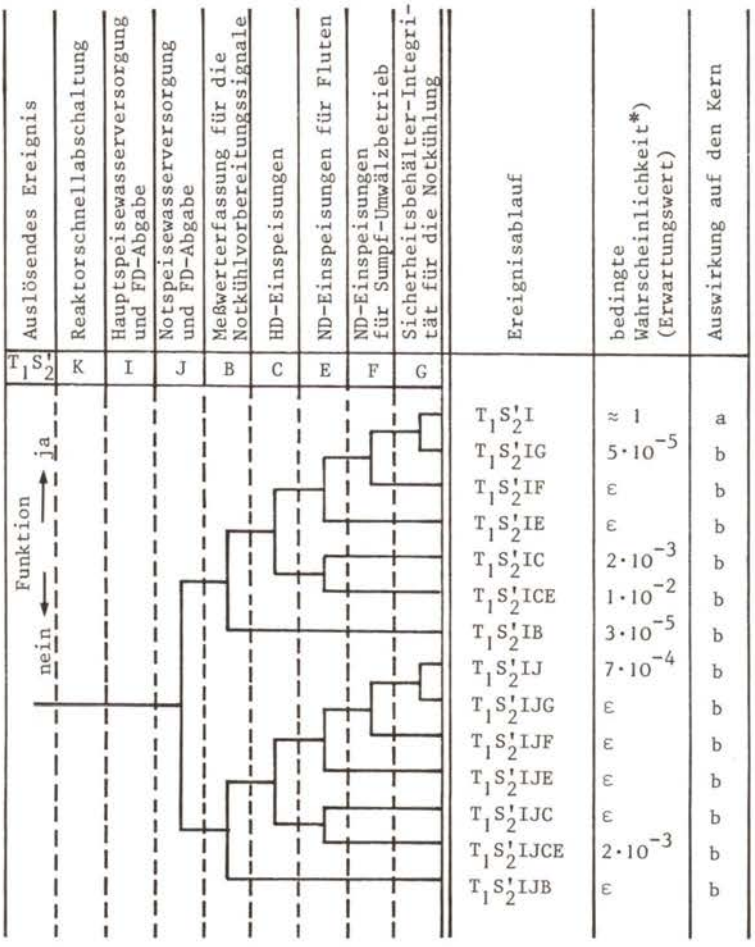
$$\bar{m} = 1,5 \cdot 10^{-2}$$

Dies entspricht einer bedingten Wahrscheinlichkeit von $4,1 \cdot 10^{-5}$ dafür, daß bei Vorliegen des Notstromfalls und funktionierender NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE ein kleines Leck eintritt und nicht beherrscht wird. Einen Beitrag von etwa 40 % zu diesem Wert liefern die Ausfallkombinationen, die ein Versagen aller vier Notstromdiesel aufgrund eines CMA enthalten. Es wird dabei zwischen dem Startversagen und dem Versagen während des Betriebs unterschieden. Während es in beiden Fällen zum Versagen der Notkühlung kommt, spielt für den Eintritt des kleinen Lecks der Ausfall durch Startversagen die entscheidende Rolle. Ein Leck liegt dann vor, wenn zusätzlich zum Startversagen ein Ausfall des Druckhalter-Abblaseventils oder des zugehörigen Steuerventils auftritt. Die redundanten Absperrarmaturen lassen sich in diesem Fall nicht mehr betätigen. Beim CMA der Diesel durch Betriebsversagen müssen dagegen zusätzlich mindestens zwei Ausfälle eintreten, damit es zum Eintritt des kleinen Lecks kommt: zum Beispiel Ausfall des Druckhalter-Abblaseventils oder der Steuerventile und zusätzlich Ausfall des Abblase-Absperrventils (einschließlich Ansteuerung). Die weiteren Beiträge zu T_1S_2' gehen im wesentlichen auf unabhängige Hardware-Ausfälle zurück, wobei neben dem Versagen des Druckhalter-Abblaseventils oder Steuerventils Ausfälle der Notstromschienen der Redundanz 1 und 4 (wodurch sich das zum Druckhalter-Abblaseventil redundante Abblase-Absperrventil nicht betätigen läßt) eine Rolle spielen.

Zum Versagen einer Systemfunktion muß dann zusätzlich mindestens ein Ausfall in der Redundanz 2 oder 3 vorliegen.

In Bild F2, 7-5 sind die bedingten Wahrscheinlichkeiten der dominanten Ereignisabläufe für T_1S_2' dargestellt. Bedingung ist jeweils, daß nach Eintritt des Notstromfalls die zur Beherrschung des Notstromfalls erforderliche NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE funktioniert und das Schließen der Druckentlastung des Reaktorkühlkreislaufs versagt. Zur Ermittlung dieser Werte wurden zunächst die Wahrscheinlichkeiten für die vollständigen Ereignisabläufe, ausgehend vom Notstromfall, ermittelt und dann durch die Wahrscheinlichkeit für den Eintritt des kleinen Lecks (wieder ausgehend vom Notstromfall) dividiert. Mit ε werden wieder vernachlässigbar kleine Wahrscheinlichkeiten der Ereignisabläufe bezeichnet (Hauptband, Abschnitt 5.2.2.4 und Fachband 1). Die folgende Diskussion der wesentlichen Ereignisabläufe bezieht sich sinnvollerweise nur auf die vollständigen Ereignisabläufe, d.h., im folgenden werden die bedingten Wahrscheinlichkeiten für die vollständigen Ereignisabläufe genannt.

Der Ereignisablauf T_1S_2' IJCE liefert mit $5 \cdot 10^{-6}$ etwa 13 % zu T_1S_2'. Neben dem Ausfall der Systemfunktionen HD-EINSPEISUNGEN und ND-EINSPEISUNGEN FÜR FLUTEN liegt bei diesem Ablauf auch ein Versagen der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE vor. Die Mindestanforderungen an diese Systemfunktionen sind: geregelte Wärmeabfuhr über 2v4 Dampferzeuger und 1v2 Abblaseregelventile (und die zugehörigen Abblasestränge). Bei allen Abläufen T_1S_2' ist andererseits die für die Beherrschung des Notstromfalls erforderliche Systemfunktion NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE vorausgesetzt. Hier sind die Mindestanforderungen geringer: Wärmeabfuhr über 1v4 Dampferzeuger und 1v4 FD-Sicherheitsventile. Beim Ereignisablauf T_1S_2'IJCE funktioniert also mindestens eine Einspeisung durch das Notspeisewasser- oder Notstandssystem, andererseits stehen zum Abfahren die erforderlichen zwei Einspeisungen (einschließlich der FD-Stränge) oder 1v2 FD-Abblasestränge nicht zur Verfügung. Die dominanten Ausfallkombinationen bei diesem Ereignisablauf enthalten das Startversagen der Notstromdiesel durch CMA (führt zum Ausfall der Systemfunktionen zur Notkühlung), den Ausfall des Druckhalter-Abblaseventils oder des



a kein Kernschmelzen
b Kernschmelzen

*) Wahrscheinlichkeit der einzelnen Ereignisabläufe unter der Bedingung, daß das auslösende Ereignis eingetreten ist.

Die Häufigkeit der einzelnen Ereignisabläufe ergibt sich durch Multiplikation mit der Häufigkeit h des auslösenden Ereignisses.

$$h(T_1S_2') = 2{,}7 \cdot 10^{-4}/a \text{ (Erwartungswert)}$$

Bild F2, 7-5:

Ereignisablaufdiagramm "kleines Leck am Druckhalter beim Notstromfall" T_1S_2'

zugehörigen Steuerventils (führt mit dem CMA der Diesel zum kleinen Leck) und den Ausfall einer der beiden Einspeisungen durch das Notstandssystem (führt mit dem CMA der Diesel zum Ausfall der Systemfunktion NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE).

Der Ereignisablauf $T_1S_2'IJ$ trägt mit $2 \cdot 10^{-6}$ etwa 5 % zu T_1S_2' bei. Für die Systemfunktion NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE gilt das oben Gesagte. Da hier weder die HD-EINSPEISUNGEN noch die ND-EINSPEISUNGEN ausgefallen sind, spielt der CMA der Notstromdiesel keine Rolle. Zu den Ausfällen, die zum kleinen Leck führen (im wesentlichen Ausfall des Druckhalter-Abblaseventils oder des zugehörigen Steuerventils und Ausfall des Abblase-Absperrventils bzw. Ausfalls der Notstromschienen 1 und 4), kommen noch Ausfälle im Notspeisewasser-, Deionat- oder Frischdampfsystem:

- Ausfall der Handeingriffe zum Abfahren,
- Mehrfachausfälle vorwiegend folgender Komponenten bzw. Teilsysteme:
  - FD-Sicherheitsventil (Redundanz 3) schließt nicht,
  - Druckmeßkanal 20 RF50 P001 im Deionatsystem spricht zu früh an,
  - Rückschlagklappe 20 RY10 S005 im Deionatsystem schließt nicht,
  - Motorarmatur OP RX20 S006 im Notstandssystem wird fälschlich aufgefahren,
  - Einspeisung in Dampferzeuger 1 oder 3 durch das Notstandssystem versagt.

Den dominanten Beitrag mit ca. 75 % zu T_1S_2' liefert der Ereignisablauf $T_1S_2'ICE$, bei dem die zur Beherrschung des kleinen Lecks erforderliche NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE funktioniert, jedoch die HD-EINSPEISUNGEN und ND-EINSPEISUNGEN ausgefallen sind. Die bedingte Wahrscheinlichkeit dafür beträgt $3 \cdot 10^{-5}$ und resultiert zu rund 60 % aus Versagenskombinationen mit dem CMA der Notstromdiesel, insbesondere aus

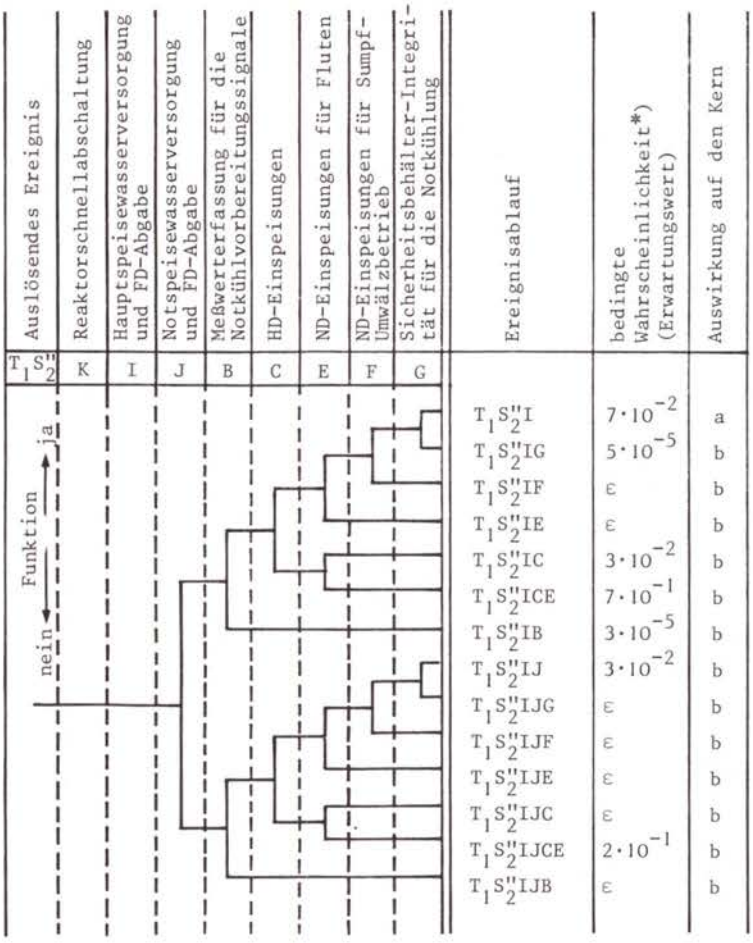
- Startversagen aller vier Notstromdiesel und Ausfall des Druckhalter-Abblaseventils oder des zugehörigen Steuerventils oder

- Betriebsversagen aller vier Notstromdiesel und Ausfall des Druckhalter-Abblaseventils oder Steuerventils und Ausfall des Abblase-Absperrventils.

Für den Ereignisablauf $T_1S_2'IC$ mit Eintritt des kleinen Lecks und Ausfall der HD-EINSPEISUNGEN bei sonst erfüllten Mindestanforderungen ergibt sich eine bedingte Wahrscheinlichkeit von $5 \cdot 10^{-6}$, was etwa 12 % von T_1S_2' entspricht. Die wesentlichen Versagenskombinationen enthalten den Ausfall des Druckhalter-Abblaseventils bzw. Steuerventils. Dazu kommt zum einen der Ausfall der Notstromschienen in den Redundanzen 1 und 4 und ein Ausfall in dem HD-Einspeisestrang 2 oder 3. Zum anderen führen die zusätzlichen Ausfälle des Abblase-Absperrventils, der Notstromschienen in zwei Redundanzen und eines HD-Einspeisestranges in einer weiteren Redundanz (nur Ausfälle der HD-Einspeisung, die nicht auch den Ausfall der ND-Einspeisung dieser Redundanz bewirken) zum Ereignisablauf $T_1S_2'IC$.

Der Ereignisablauf $T_1S_2'IG$ mit dem Ausfall der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG liefert zwar keinen signifikanten Beitrag zu T_1S_2', führt jedoch gleichzeitig mit dem Ausfall der Notkühlung zu einem Versagen des Sicherheitsbehälters. Die bedingte Wahrscheinlichkeit von $1{,}4 \cdot 10^{-7}$ wird von Ausfallkombinationen mit dem Versagen von Schweißnähten bestimmt. Der wesentliche Beitrag zum Eintritt des kleinen Lecks bei diesem Ereignisablauf kommt von Ausfällen des Druckhalter-Abblaseventils oder Steuerventils zusammen mit dem Versagen des Abblase-Absperrventils.

Bei den Ereignisabläufen T_1S_2'' (Bild F2, 7-4 und -6) liegt ein Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE entsprechend den Mindestanforderungen für den Notstromfall vor, d.h., es kann bis ca. 30 Minuten nach Eintritt des Notstromfalls keiner der 4 Notspeisewasser-Frischdampfstränge und auch keine Einspeisung durch das Notstandssystem in Betrieb genommen werden. Unter diesen Umständen kommt es zum Ansprechen beider Druckhalter-Abblaseventile. Aufgrund der Bewertung des Folgeausfalls der Kühlmitteldruckregelung mit der Wahrscheinlichkeit 1 steht als Schließbefehl für die Druckhalter-Armaturen lediglich das Reaktorschutzsignale YZ37 zur Verfügung. Von diesem Signal werden je-



a kein Kernschmelzen
b Kernschmelzen

*) Wahrscheinlichkeit der einzelnen Ereignisabläufe unter der Bedingung, daß das auslösende Ereignis eingetreten ist.

Die Häufigkeit der einzelnen Ereignisabläufe ergibt sich durch Multiplikation mit der Häufigkeit h des auslösenden Ereignisses.

$$h(T_1S_2'') = 3 \cdot 10^{-6}/a \text{ (Erwartungswert)}$$

Bild F2, 7-6:

Ereignisablaufdiagramm "kleines Leck am Druckhalter beim Notstromfall" T_1S_2''

doch nur die Abblase-Steuerventile, nicht dagegen die redundanten Steuerabsperr- bzw. Abblaseabsperr-Armaturen angesteuert. Ein Leck tritt also in diesem Fall ein, wenn eines der beiden DH-Abblaseventile oder eines der beiden zugehörigen Abblase-Steuerventile oder das Reaktorschutzsignal ausfällt. Zu einem Leck kann es auch kommen, wenn nach Ansprechen der Druckhalter-Abblaseventile eine fälschliche Absperrung der Abblasestränge von Hand erfolgt und das in diesem Fall ansprechende 1. Druckhalter-Sicherheitsventil nicht schließt. Diese Versagenskombination trägt etwa 10 % zum Eintritt des Lecks bei T_1S_2'' bei.

Da im weiteren Ereignisablauf die VERZÖGERTE SPEISEWASSERVERSORGUNG UND FD-ABGABE hergestellt werden kann, ist also bei T_1S_2'' mindestens ein Einspeisestrang des Notstandssystems in Betrieb. Als bedingte Wahrscheinlichkeit für das Versagen der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE (Bedingung: es liegt der Notstromfall vor), für Eintritt des Lecks und Funktionieren der VERZÖGERTEN SPEISEWASSERVERSORGUNG UND FD-ABGABE ergibt sich ein Erwartungswert von $3 \cdot 10^{-5}$ (Abschnitt 7.2.5.1). Für den Ausfall der Systemfunktionen zur Beherrschung des kleinen Lecks wurde unter der Bedingung, daß das Leck entsprechend T_1S_2'' vorliegt, eine Wahrscheinlichkeit von

$$\bar{m} = 0,93$$

ermittelt. Diese Werte entsprechen einer bedingten Wahrscheinlichkeit von $2,8 \cdot 10^{-5}$ für die Summe der Ereignisabläufe T_1S_2'' nach Bild F2, 7-6, d.h. dafür, daß bei Vorliegen des Notstromfalls ein kleines Leck entsprechend T_1S_2'' eintritt und nicht beherrscht wird. Die dominanten Ausfallkombinationen bei diesen Ereignisabläufen enthalten den CMA der Notstromdiesel und den Ausfall der Inbetriebnahme des Notstandssystems innerhalb 30 Minuten nach Eintritt des Notstromfalls. Beides zusammen führt zum Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE (bezüglich des Notstromfalls) und der Notkühlung (HD-EINSPEISUNGEN, ND-EINSPEISUNGEN). Zum Leck führt in den dominanten Ausfallkombinationen von T_1S_2'' das Versagen des Schließens eines der Druckhalter-Abblaseventile oder Abblase-Steuerventile oder der Ausfall des Reaktorschutzsignals YZ37.

Bei der Aufteilung der bedingten Wahrscheinlichkeit von $2{,}8 \cdot 10^{-5}$ auf die einzelnen Ereignisabläufe werden nur die Pfade mit relevanten Beiträgen berücksichtigt. So liefert der Ereignisablauf $T_1S_2''IJCE$ mit einer bedingten Wahrscheinlichkeit von $5 \cdot 10^{-6}$ einen Beitrag von ca. 18 % zu T_1S_2''. Neben dem CMA der Notstromdiesel und dem Ausfall einer der Druckhalterarmaturen bzw. des Reaktorschutzsignals YZ37 (siehe oben) ist bei diesem Pfad vor allem der zusätzliche Ausfall einer Einspeisung durch das Notstandssystem relevant.

Beim Ereignisablauf $T_1S_2''IJ$ funktionieren die HD-EINSPEISUNGEN und ND-EINSPEISUNGEN. Anstelle des CMA der Notstromdiesel führen hier vor allem Ausfälle der FD-Sicherheitsventile in Strang 1 oder 3 zusammen mit dem Ausfall von drei Notspeisewassersträngen zum Versagen der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE (bezüglich des Notstromfalls). Die bedingte Wahrscheinlichkeit für diesen Ereignisablauf wurde zu $1 \cdot 10^{-6}$ ermittelt, was etwa 4 % von T_1S_2'' entspricht.

Den Hauptbeitrag zu T_1S_2'' liefert mit über 70 % der Ereignisablauf $T_1S_2''ICE$ mit dem Versagen der Notkühlung, aber mit funktionierender NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE. Die bedingte Wahrscheinlichkeit dafür beträgt $2 \cdot 10^{-5}$. Die wesentlichen Ausfallkombinationen wurden bereits bei der Diskussion von T_1S_2'' genannt.

Das Versagen der HD-EINSPEISUNGEN bei funktionierenden ND-EINSPEISUNGEN wird durch den Ereignisablauf $T_1S_2''IC$ dargestellt, der mit $1 \cdot 10^{-6}$ etwa 4 % von T_1S_2'' ausmacht. Die wesentlichen Ausfallkombinationen enthalten das Versagen aller vier Notspeisewasserstränge, davon zwei aufgrund spezifischer Ausfälle im Notspeisewasser-Deionat-System (also beispielsweise durch den Ausfall von Notspeisewasserpumpen). Die zwei restlichen Notspeisewasserstränge versagen dabei durch Ausfall der Notstromschienen oder Hilfssysteme (z.B. des nuklearen Zwischenkühlkreises); diese Ausfälle führen auch zum Versagen der entsprechenden HD-Einspeisungen. Dazu kommt der Ausfall der Inbetriebnahme des Notstandssystems innerhalb 30 Minuten nach Eintritt des Notstrom-

falls und ein spezifischer Ausfall in einer weiteren Redundanz der HD-Einspeisungen, der nicht gleichzeitig zum Versagen der ND-Einspeisung dieser Redundanz führt.

Der Wert der bedingten Wahrscheinlichkeit für $T_1S_2''IG$ mit $2 \cdot 10^{-9}$ wird durch das Versagen der Schweißnähte des Sicherheitsbehälters bestimmt.

Als Summe aller Ereignisabläufe T_1S_2' und T_1S_2'' erhält man die Wahrscheinlichkeit $7 \cdot 10^{-5}$ für ein nicht beherrschtes kleines Leck am Druckhalter, unter der Bedingung, daß der Notstromfall vorliegt. Zusammengefaßt tragen dazu wesentlich der CMA der Notstromdiesel, der Ausfall der Inbetriebnahme des Notstandssystems innerhalb von 30 Minuten nach Eintritt des Notstromfalls, der Ausfall der Druckhalter-Abblaseventile oder Abblase-Steuerventile und der Ausfall von Notstromschienen bei.

Für die Ausfallarten unabhängige Ausfälle der Hardware einschließlich Instandhaltung (UA), "common mode"-Ausfälle der Hardware (CMA) und menschliches Fehlverhalten (M) einschließlich der "common mode"-Ausfälle durch Fehlkalibrierung von Meßkanälen ergibt sich folgende Aufteilung der bedingten Wahrscheinlichkeit von $7 \cdot 10^{-5}$:

UA	33 %
CMA	-
M	-
UA & CMA	26 %
UA & M	4 %
CMA & M	-
UA & CMA & M	37 %

Ausfallkombinationen, die "common mode"-Ausfälle enthalten, liefern demnach einen Beitrag von insgesamt 63 %, solche, bei denen menschliches Fehlverhalten beteiligt ist, insgesamt 41 %. Der Hauptbeitrag der "common mode"-Ausfälle kommt vom Versagen der Notstromdiesel, der maßgebliche Anteil am menschlichen Fehlverhalten geht auf den Ausfall der Inbetriebnahme des Notstandssystems innerhalb 30 Min. nach Eintritt des Notstromfalls zurück.

"Common mode"-Ausfälle oder menschliches Fehlverhalten für sich allein führen nicht zu einem unbeherrschten kleinen Leck. Bei T_1S_2' muß zum Eintritt des kleinen Lecks ein unabhängiger Hardware-Ausfall vorliegen, bei T_1S_2'' kann zwar das Leck durch einen "common mode"-Ausfall (Reaktorschutzsignal YZ37) auftreten, zum Versagen der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE (entsprechend "Notstromfall") muß dagegen auch immer menschliches Fehlverhalten vorliegen. Die Kombinationen aus "common mode"-Ausfällen und menschlichem Fehlverhalten spielen jedoch zahlenmäßig keine Rolle (< 1 %).

Das Bild F2, 7-7 zeigt die mittleren Nichtverfügbarkeiten der zur Beherrschung des kleinen Lecks am Druckhalter erforderlichen Systemfunktionen. Die Werte entsprechen den Wahrscheinlichkeiten für den Ausfall der Systemfunktion unter der Bedingung, daß, ausgehend vom Notstromfall, ein kleines Leck am Druckhalter vorliegt. Wegen der starken Abhängigkeit der Systemfunktionen untereinander ist die Summe der Einzelwahrscheinlichkeiten wesentlich höher als die Summenwahrscheinlichkeit. Die Abhängigkeit besteht vor allem in der Energieversorgung, wobei der CMA der Notstromdiesel eine wesentliche Rolle spielt.

7.3 Ausfall der Hauptspeisewasserversorgung

7.3.1 Allgemeines

Der Ausfall der Hauptspeisewasserversorgung bei Leistungsbetrieb des Kraftwerks kann verschiedene Ursachen haben. Insbesondere sind aus der deutschen Betriebserfahrung bekannt:

- Notstromfall,
- Auslösung des Pumpenschutzes der Hauptspeisewasserpumpen,
- Fehlauslösung des Pumpenschutzes der Hauptspeisewasserpumpen,
- Überlastung der Hauptspeisewasserpumpen mit Ansprechen der Überstromauslöser bei Nichtschließen der Rückschlagklappe in einer Hauptspeisewasserleitung,
- Außerbetriebnahme der Hauptspeisewasserversorgung durch menschliches Fehlverhalten und
- Auslösung oder Fehlauslösung der $\Delta p/\Delta t$-Signale YZ60.

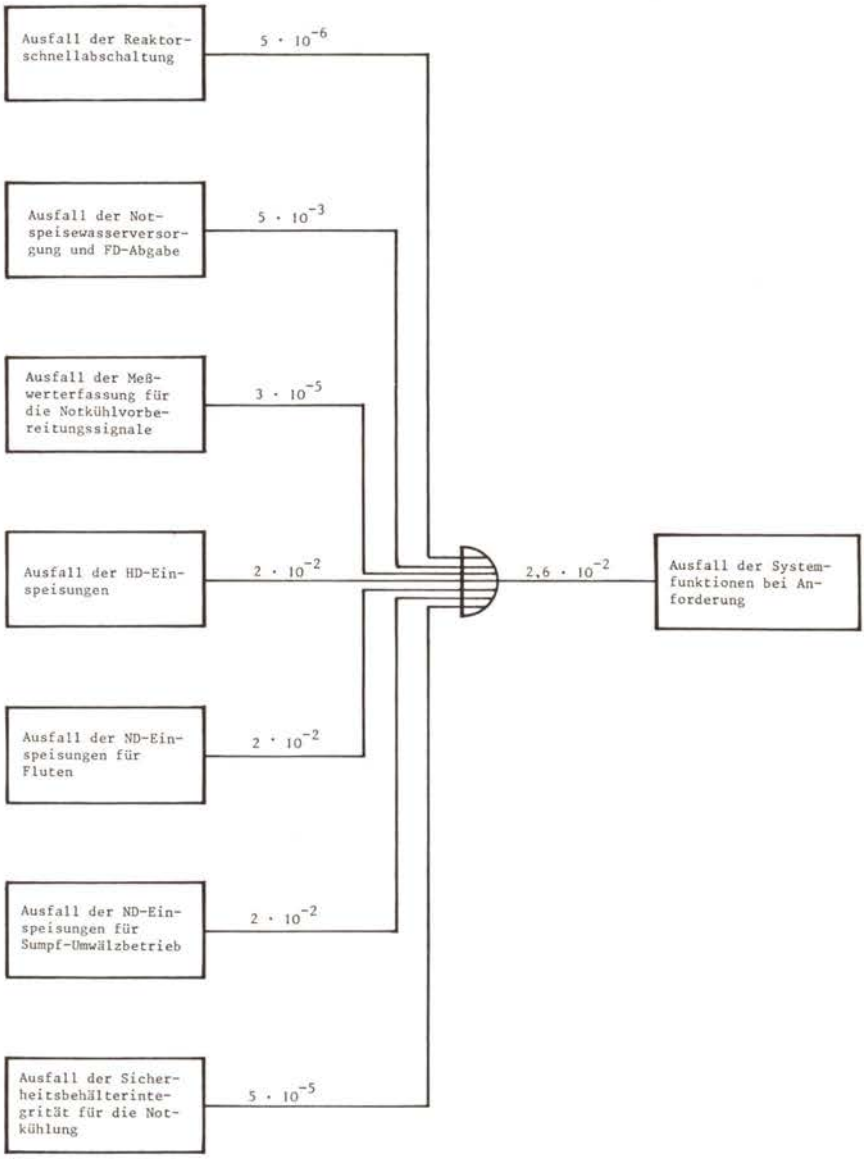


Bild F2, 7-7:

Mittlere Nichtverfügbarkeiten der Systemfunktionen bei Anforderung durch ein "kleines Leck am Druckhalter beim Notstromfall"

Ferner würde der Ausfall der Bespeisung eines Dampferzeugers über das Hauptlastregelventil zur vollständigen Abschaltung der Hauptspeisewasserversorgung aller Dampferzeuger führen.

Für die Zuverlässigkeitsanalyse muß unterschieden werden, ob die Ursache ein Notstromfall ist oder nicht. Der Notstromfall wird in Abschnitt 7.2 ausführlich diskutiert. Daher braucht hier nur der vollständige Ausfall der Hauptspeisewasserversorgung behandelt zu werden, der ohne Notstromfall eintritt. Die zugehörige mittlere Eintrittshäufigkeit wird aufgrund der deutschen Betriebserfahrung zu 0,8/a abgeschätzt.

Analog zum Notstromfall werden beim Ausfall der Hauptspeisewasserversorgung folgende Systemfunktionen betrachtet:

- Reaktorschnellabschaltung,
- Hauptspeisewasserversorgung und FD-Abgabe,
- Notspeisewasserversorgung und FD-Abgabe,
- Öffnen der Druckentlastung des Reaktorkühlkreislaufs,
- Schließen der Druckentlastung des Reaktorkühlkreislaufs,
- Verzögerte Speisewasserversorgung und FD-Abgabe und
- Langzeit-Speisewasserversorgung und FD-Abgabe.

Anders als beim Notstromfall wird hier die Systemfunktion HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE berücksichtigt. Während nämlich bei der Referenzanlage meist mit einer längeren Dauer des Notstromfalls zu rechnen ist (Abschnitt 7.1), konnte laut Betriebserfahrung die ausgefallene Hauptspeisewasserversorgung oft kurzfristig wieder in Betrieb genommen werden. Diese kurzfristige Wiederinbetriebnahme ist in der Hälfte aller Fälle zu erwarten. Sinkt hingegen in einem der vier Dampferzeuger der Wasserstand unter 6,5 m ab, so erhalten alle Druckschieber der Hauptspeisewasserpumpen vom Reaktorschutzsystem über die Notspeisezuschaltsignale einen Schließbefehl, und sämtliche betrieblichen Befehle (einschließlich möglicher Handbefehle) werden so lange unterdrückt, bis der Wasserstand in den Dampferzeugern wieder über 6,5 m angestiegen ist. Die Hauptspeisewasserversorgung kann anderenfalls nicht mehr zugeschaltet werden.

Beim Ausfall der Hauptspeisewasserversorgung ändern sich die Prozeßvariablen vergleichsweise langsam, daher wird auch die RE-

AKTORSCHNELLABSCHALTUNG später als beim Notstromfall ausgelöst. Folglich steht zur Abfuhr der Nachwärme wenig sekundärseitiger Wasservorrat in den Dampferzeugern zur Verfügung. Außerdem werden hier die Hauptkühlmittelpumpen nicht abgeschaltet, so daß auch die von diesen Pumpen in den Reaktorkühlkreislauf eingebrachte Wärme mit abgeführt werden muß. Steht auch die NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE zur Bespeisung der Dampferzeuger nicht zur Verfügung, so sind diese frühestens 15 Minuten nach Ausfall der Hauptspeisewasserversorgung sekundärseitig ausgetrocknet[1]). Danach öffnen die Druckhalterventile, über die nun die Nachwärme abgeführt wird. Bis etwa 45 Minuten nach Ausfall der Hauptspeisewasserversorgung muß eine VERZÖGERTE SPEISEWASSERVERSORGUNG UND FD-ABGABE hergestellt sein, um eine Überhitzung des Reaktorkerns zu vermeiden[1]). Dabei ist auch zu berücksichtigen, daß beim Ausfall der sekundärseitigen Bespeisung der Dampferzeuger innerhalb der Stahlhülle Temperaturen und Feuchtigkeiten erreicht werden, die zu einem Versagen der Druckhalter-Abblaseventile, der zugehörigen Steuerventile sowie der jeweils redundanten Absperrarmaturen führen können. Ebenso ist mit einem Ausfall der Meßumformer für die Kühlmitteldruckregelung zu rechnen. Diese Komponenten sind nicht für derartige Umgebungsbedingungen ausgelegt. Während eine durch die Umgebungsbedingungen verursachte Unterbrechung der Stromversorgung für diese Armaturen zu einem Schließen der Abblase-Steuerventile und damit der Abblaseventile führt, ist die Ausfallrichtung der Meßumformer nicht bekannt. Es wird pessimistisch davon ausgegangen, daß die Meßumformer so ausfallen, daß vom Regler keine Schließbefehle ausgegeben werden.

Die im Vergleich zum Notstromfall kürzeren Zeitspannen, die zur Inbetriebnahme des Notstandssystems zur Verfügung stehen, wirken sich ungünstig auf die Nichtverfügbarkeiten der Systemfunktionen zur Speisewasserversorgung aus. Andererseits steht zur Beherrschung der Störung die elektrische Eigenbedarfsversorgung zur Verfügung, was einen günstigen Einfluß auf die Nichtverfügbarkeiten der angeforderten Systemfunktionen hat. Im übrigen werden die Randbedingungen für die Zuverlässigkeitsanalysen wie im Notstromfall zugrunde gelegt.

---

[1]) vgl. Fußnote, S. 391

7.3.2 Ergebnisse

Für die Zuverlässigkeitsanalyse konnten grundsätzlich die gleichen Fehlerbäume wie für den Notstromfall herangezogen werden. Es mußte nur berücksichtigt werden, daß

- zur Energieversorgung auch die elektrische Eigenbedarfsanlage zur Verfügung steht,
- andere Zeitspannen anzusetzen sind und
- die Druckhalter-Abblaseventile im allgemeinen nicht öffnen.

Entsprechend der anderen zu berücksichtigenden Zeitspannen erfolgt eine neue Bewertung folgender Handmaßnahmen:

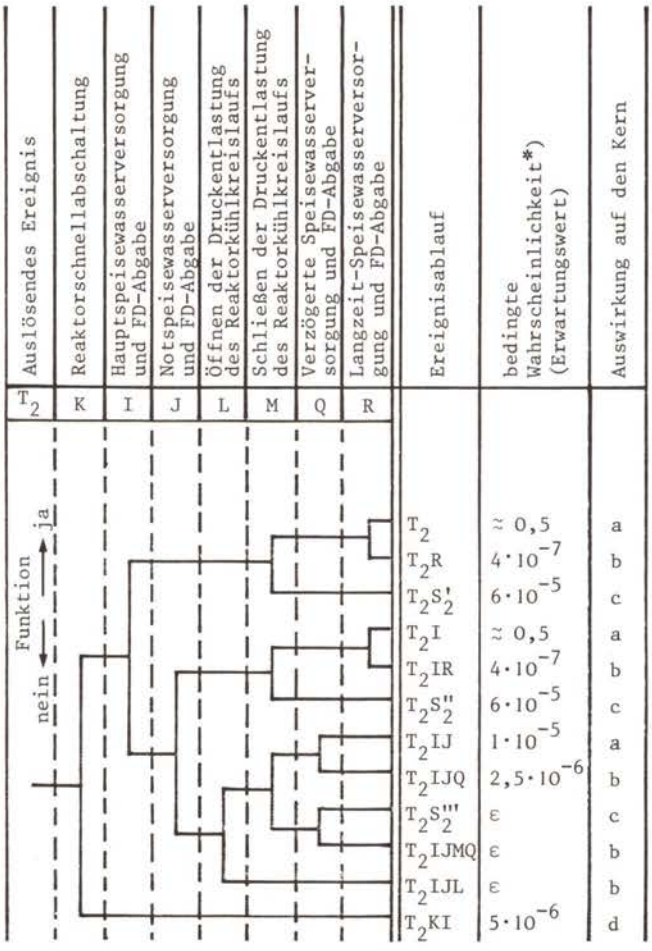
L 485 OP RX10/20 Keine verzögerte Inbetriebnahme des Notstandsystems innerhalb von etwa 15 bis 45 Minuten nach Ausfall der Hauptspeisewasserversorgung
$p_{50} = 2 \cdot 10^{-1}/K = 2$

L 544 OP RX10/20 Keine Inbetriebnahme des Notstandssystems innerhalb von 15 Minuten nach Ausfall der Hauptspeisewasserversorgung
$p_{50} = 6 \cdot 10^{-1}/K = 1$

Dabei wird wie beim Notstromfall eine Mindestzeitspanne, die für das Erkennen und die Durchführung der Maßnahme benötigt wird, von etwa 6 Minuten berücksichtigt.

Zu einem Ansprechen der Druckhalter-Abblaseventile kommt es, falls bei der als Folge der Reaktorschnellabschaltung stattfindenden Turbinenschnellabschaltung die Frischdampf-Umleiteinrichtung nicht öffnet oder die Dampferzeuger sekundärseitig austrocknen. Für das Nichtöffnen der Frischdampf-Umleiteinrichtung bei Eintreten einer Turbinenschnellabschaltung wurde ein Erwartungswert von $3{,}7 \cdot 10^{-2}$ verwendet, der aus der Betriebserfahrung gewonnen wurde.

Die Ereignisabläufe für den "Ausfall der Hauptspeisewasserversorgung" sind in Bild F2, 7-8 dargestellt. Dort sind auch die bedingten Wahrscheinlichkeiten für die einzelnen Ereignisabläufe



a kein Kernschmelzen
b Kernschmelzen
c Fortsetzung "kleines Leck am Druckhalter bei verschiedenen Transienten"
d Fortsetzung "ATWS-Störfälle"

*) Wahrscheinlichkeit der einzelnen Ereignisabläufe unter der Bedingung, daß das auslösende Ereignis eingetreten ist.
Die Häufigkeit der einzelnen Ereignisabläufe ergibt sich durch Multiplikation mit der Häufigkeit h des auslösenden Ereignisses.

$$h(T_2) = 0{,}8/a \text{ (Erwartungswert)}$$

Bild F2, 7-8:

Ereignisablaufdiagramm für den "Ausfall der Hauptspeisewasserversorgung"

eingetragen. Die Wahrscheinlichkeit für den Ausfall der Systemfunktionen, die zur Beherrschung dieser Störung erforderlich sind, wurde zu aufgerundet $4 \cdot 10^{-6}$ ermittelt. Die Ereignisabläufe T_2S_2 entsprechen denen für "kleines Leck am Druckhalter". Diese Kühlmittelverluststörfälle werden nicht wie beim Notstromfall einzeln diskutiert. Sie werden vielmehr gemeinsam mit entsprechenden Fällen als "kleines Leck am Druckhalter", das aus anderen Transienten resultieren kann, behandelt (Abschnitt 7.5).

7.4 Turbinenschnellabschaltung ohne Öffnen der Frischdampf-Umleiteinrichtung

Eine Turbinenschnellabschaltung ohne Öffnen der FD-Umleiteinrichtung, d.h. ein Ausfall der Hauptwärmesenke, kann verschiedene Ursachen haben:

- Notstromfall,
- Ausfall des Turbinenkondensators oder der zu seinem Betrieb erforderlichen Systeme,
- Turbinenschnellabschaltung und Ausfall der FD-Umleiteinrichtung bei Anforderung sowie
- Auslösung oder Fehlauslösung der $\Delta p/\Delta t$-Signale YZ60.

Der Notstromfall wird gesondert behandelt (Abschnitt 7.2). Ein Ausfall der Hauptspeisewasserversorgung, der gleichzeitig mit dem Ausfall der Hauptwärmesenke oder als Folge davon eintritt, braucht hier ebenfalls nicht diskutiert zu werden (Abschnitt 7.3). Es ist also nur zu untersuchen, mit welcher Wahrscheinlichkeit von der Systemfunkion HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE die Frischdampfabgabe versagt.

Im Frischdampfsystem wird der Ansprechdruck der vier Frischdampf-Sicherheitsventile nach wenigen Minuten erreicht. Öffnet keines dieser Ventile, so stehen noch zwei Abblaseregelventile zur Verfügung. Diese sind durch Handbetätigung von der Warte aus aufzufahren. Versagt das Öffnen aller Frischdampf-Sicherheitsventile und erfolgt kein Abblasen über die Abblaseregelventile, so werden etwa 15 Minuten nach Ausfall der Hauptwärmesenke Drücke erreicht, bei denen mit einem Überdruckversagen zu rechnen ist.

Ein Versagen aller redundanten Sicherheitsventile aufgrund von CMA ist aus der Weltbetriebserfahrung nicht bekannt und wird daher im folgenden auch nicht unterstellt. Ein unabhängiger Ausfall aller Frischdampf-Sicherheitsventile ist äußerst unwahrscheinlich.

Da sich die Ansprechdrücke der Frischdampf-Sicherheitsventile nicht unterscheiden, ist davon auszugehen, daß normalerweise alle Ventile öffnen. Schließt eine dieser Armaturen nicht, kommt es als Folge des Ausfalls der Hauptwärmesenke zum Störfall "Leck im Frischdampfsystem", wobei zusätzliche Reaktorschutzsignale ansprechen. Durch die YZ60-Signale werden die Hauptspeisewasserversorgung außer Betrieb genommen und das Frischdampfsystem in vier getrennte Stränge aufgeteilt. Ferner wird der zum Dampferzeuger mit dem defekten Sicherheitsventil führende Notspeisewasser-Strang abgeschiebert. Dieser Störfall führt zu erhöhten Anforderungen an die Systemfunktionen: Bei der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE muß zur Wärmeabfuhr mittels eines Notspeisewasser-Stranges das zugehörige Frischdampf-Sicherheitsventil öffnen und schließen. Um die Integrität des Frischdampfsystems sicherzustellen, muß bei Nichtöffnen des Sicherheitsventils eines Stranges die Wärmeabfuhr über zwei intakte Notspeisewasser-Frischdampf-Stränge erfolgen. Ein Überdruckversagen ist andernfalls nach etwa 30 Minuten nicht mehr auszuschließen. Hier sind in der Phase B der Risikostudie noch besondere Festigkeitsuntersuchungen erforderlich. Im Rahmen der Phase A wird ein Überdruckversagen nicht unterstellt.

Schließt keines der Frischdampf-Sicherheitsventile, so ist keine geregelte Frischdampfabgabe möglich. Denkbare CMA werden wie für das Öffnen dieser Ventile nicht bewertet. Unabhängige Ausfälle sind äußerst unwahrscheinlich.

Ein unabhängiger Ausfall des Öffnens oder des Schließens eines Sicherheitsventils ist mit einer Wahrscheinlichkeit von $1{,}7 \cdot 10^{-2}$ zu bewerten, so daß sich für den Ausfall aller vier Ventile und damit für den nicht beherrschten Ausfall der Hauptwärmesenke eine Wahrscheinlichkeit von etwa 10^{-7} ergibt (Median $3 \cdot 10^{-8}$, Unsicherheitsfaktor 12).

7.5 Kleines Leck am Druckhalter bei verschiedenen Transienten mit Reaktorschnellabschaltung

7.5.1 Allgemeines

Bei einigen Transienten steigt der Druck im Reaktorkühlkreislauf so weit an, daß Druckhalterventile öffnen. Die wichtigsten dieser Transienten sind:

- Notstromfall,
- Turbinenschnellabschaltung ohne Öffnen der FD-Umleiteinrichtung, sofern diese Turbinenschnellabschaltung nicht als Folge, sondern vor einer eventuellen Reaktorschnellabschaltung ausgelöst wird,
- Turbinenschnellabschaltung ohne Stabeinwurf,
- Ausfall aller Hauptkühlmittelpumpen,
- Ausfall der Kühlmitteldruck-Regelung,
- Fehlausfahren von Steuerstäben bei Teillastbetrieb und
- ATWS-Störfälle.

Daneben können andere Transienten ein Ansprechen von Druckhalterventilen bedingen, falls sie unmittelbar nach einer schnellen Leistungsänderung eintreten, die eine große Amplitude erreicht. Ein Öffnen von Druckhalterventilen ist auch möglich, wenn bei Transienten die dann angeforderten Regelungen nicht intakt sind oder die erste Anregung einer angeforderten Reaktorschnellabschaltung versagt.

Jedes der Druckhalterventile ist auf einen anderen Ansprechdruck eingestellt, die Druckhalter-Abblaseventile auf niedrigere Druckwerte als die Druckhalter-Sicherheitsventile. Der Anstieg des Kühlmitteldrucks wird bei zu erwartenden Transienten mit Reaktorschnellabschaltung durch das Öffnen von ein oder zwei Druckhalterventilen begrenzt, bei einem Großteil dieser Transienten öffnet sogar nur ein Druckhalter-Abblaseventil. Hingegen sprechen bei zu erwartenden Transienten mit Ausfall der Reaktorschnellabschaltung (ATWS-Störfällen) alle Druckhalterventile an. Die ATWS-Störfälle werden in Abschnitt 7.6 diskutiert.

Sinkt nach dem Öffnen der Druckhalterventile der Druck im Reaktorkühlkreislauf wieder ab, so sollen nach Unterschreiten der

jeweiligen Ansprechdrücke die Druckhalterventile wieder schließen. Schließt ein Druckhalter-Abblaseventil nicht, so sind redundante Absperrmaßnahmen vorgesehen. Versagen auch diese, so ist - entsprechend den Ventilquerschnitten - ein "kleines Leck am Druckhalter" die Folge. Ein solcher Kühlmittelverluststörfall liegt auch vor, wenn ein Druckhalter-Sicherheitsventil nach Unterschreiten seines Ansprechdrucks nicht schließt.

Bei den zu erwartenden Transienten, die bei der Referenzanlage zu einem Öffnen von Druckhalterventilen führen, ist grundsätzlich zwischen dem Notstromfall und den Transienten ohne Notstromfall zu unterscheiden. Der Notstromfall hat nämlich erheblichen Einfluß auf die Wahrscheinlichkeiten des Ausfalls der angeforderten Systemfunktionen. Kleine Lecks am Druckhalter, die durch Nichtschließen von Druckhalterventilen aus dem Notstromfall hervorgehen, werden im Abschnitt 7.2 eingehend diskutiert. Die Ergebnisse für "kleine Lecks am Druckhalter" als Folge aller übrigen Transienten mit Reaktorschnellabschaltung werden im nächsten Abschnitt behandelt.

7.5.2 Ergebnisse

Im Fachband 1 wird darauf hingewiesen, daß für ein Leck am Druckhalter die gleichen Mindestanforderungen zugrunde gelegt werden wie für ein entsprechendes Leck in einer Hauptkühlmittelleitung. Die Ergebnisse der Zuverlässigkeitsanalyse können daher weitgehend vom "kleinen Leck in einer Hauptkühlmittelleitung" übernommen werden. Die dort berücksichtigte Wahrscheinlichkeit für den Notstromfall als Störfallfolge hat keinen merkbaren Einfluß auf die ermittelten Ergebnisse. Zu berücksichtigen ist, daß hier

- das Abfahren der Anlage erst erheblich später als beim "kleinen Leck in einer Hauptkühlmittelleitung" erfolgen muß,
- in der Mehrzahl der Fälle auch das Notstandssystem zur NOT-SPEISEWASSERVERSORGUNG UND FD-ABGABE eingesetzt werden kann.

Aufgrund des ersten Punktes liefern die beim "kleinen Leck in einer Hauptkühlmittelleitung" dominierenden Handmaßnahmen hier

keinen Beitrag zum Ergebnis. Die beiden angeführten Punkte sind analog zum "kleinen Leck am Druckhalter beim Notstromfall". Eine Ausnahme bilden die "kleinen Lecks am Druckhalter", die bei Ausfall der Hauptspeisewasserversorgung auftreten. Hier muß gegebenenfalls das Abfahren früher eingeleitet werden, so daß das Notstandssystem zum Abfahren nicht mit eingesetzt werden darf. Laut Betriebshandbuch ist nämlich zuerst der Block A des Kernkraftwerks Biblis so weit abzufahren, bis die Nachwärmeabfuhr durch das Not- und Nachkühlsystem erfolgt.

Die Nichtverfügbarkeiten

- der HD-EINSPEISUNGEN (Ereignisabläufe TS_2IC, TS_2ICE) von $1{,}1 \cdot 10^{-3}$,
- der ND-EINSPEISUNGEN FÜR FLUTEN (Ereignisablauf TS_2IE) von $1 \cdot 10^{-4}$ und
- der ND-EINSPEISUNGEN FÜR SUMPF-UMWÄLZBETRIEB (Ereignisablauf TS_2IF) von $5 \cdot 10^{-4}$

ergeben zusammen einen Wert von $1{,}7 \cdot 10^{-3}$. Sie liefern damit den größten Beitrag zur Wahrscheinlichkeit des nicht beherrschten Störfalls. Die Nichtverfügbarkeit der Systeme zur NOTSPEISE-WASSERVERSORGUNG UND FD-ABGABE (Ereignisablauf TS_2IJ) liegt bei $2 \cdot 10^{-3}$, wenn das Notstandssystem nicht herangezogen wird. Unter Berücksichtigung des Notstandssystems ergibt sich damit eine bedingte Wahrscheinlichkeit von $\lesssim 5 \cdot 10^{-4}$ und damit insgesamt eine Wahrscheinlichkeit von $\cong 2 \cdot 10^{-3}$ für den nicht beherrschten Störfall.

7.6 Zuverlässigkeitsanalyse für ATWS-Störfälle

7.6.1 Allgemeines

Zur Reaktorschnellabschaltung aus Leistungsbetrieb kommt es in deutschen Kernkraftwerken mit Druckwasserreaktor mit einer mittleren Häufigkeit von 5/a. Würde die Reaktorschnellabschaltung versagen, so wären bei vielen der Transienten die Auswirkungen unkritisch. Die Druckentlastung des Reaktorkühlkreislaufs hätte dann die Aufgabe, einen möglichen Anstieg des Kühlmitteldrucks

zu begrenzen. Außerdem müßte dann ausreichend Wärme über den Speisewasser-Dampf-Kreislauf abgeführt werden.

Die Häufigkeit der ausgelösten Reaktorschnellabschaltungen liefert daher einen oberen Grenzwert für die Summe aller zu erwartenden Transienten, die das Eingreifen von Sicherheitssystemen erfordern. Versagt die Reaktorschnellabschaltung in einem solchen Anforderungsfall, so liegt ein "ATWS-Störfall"[1]) vor. Die zugrunde gelegten Mindestanforderungen an die Systemfunktionen sind, unterschieden nach auslösenden Ereignissen, der Tabelle F2, 7-3 zu entnehmen.

Transiente	Systemfunktionen		
	Öffnen der Druckentlastung des Reaktorkühlkreislaufs	Schließen der Druckentlastung des Reaktorkühlkreislaufs	Speisewasserversorgung (a) Hauptspeisewasser (b) Notspeisewasser (c) Verzögertes Speisewasser
ATWS-Störfall "Notstromfall"	2v3[1])	4v4	(b) 2v4[3])
ATWS-Störfall "Ausfall der Hauptspeisewasserversorgung"	3v3[1])	4v4	(b) 2v4[3])
Andere ATWS-Störfälle	2v3[1])	4v4	(a) 2v4[2])

[1]) Hier interessieren nur die 3 Druckhalterventile mit dem größeren Ventilquerschnitt.
[2]) Einspeisungen über die Hauptspeisewasserleitungen in die Dampferzeuger
[3]) Einspeisungen über das Notspeisewassersystem in die Dampferzeuger

2v4, 4v4 usw. ≙ von 4 vorhandenen redundanten Teilsystemen sind 2 bzw. 4 usw. erforderlich

Tab. F2, 7-3:
Mindestanforderungen an die Systemfunktionen bei ATWS-Störfällen

---

[1]) Anticipated Transients Without Scram = zu erwartende Transienten ohne Reaktorschnellabschaltung

Für den ATWS-Störfall "Notstromfall" (Ausfall der elektrischen Eigenbedarfsversorgung) wurden die Mindestanforderungen aus den Genehmigungsverfahren sowie aus /F2, 7-2 und -3/ übernommen.

Der größte Anstieg des Kühlmitteldrucks würde beim ATWS-Störfall "Ausfall der Hauptspeisewasserversorgung" erreicht. Für diesen in /F2, 7-2 und -3/ nicht untersuchten Störfall wird, wie in WASH-1400, davon ausgegangen, daß ein ausreichendes ÖFFNEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS nur dann erfolgt, wenn die drei Druckhalterventile mit dem größeren Ventilquerschnitt öffnen.

Die anderen ATWS-Störfälle können durch den ATWS-Störfall "Ausfall der Hauptwärmesenke (Turbinenschnellabschaltung ohne Öffnen der Frischdampf-Umleiteinrichtung) bei vorhandener elektrischer Eigenbedarfsversorgung" pessimistisch abgedeckt werden. Die hierfür in /F2, 7-2 und -3/ zugrunde gelegten Mindestanforderungen sind in der Tabelle F2, 7-3 angegeben. In diesen ATWS-Untersuchungen wird bezüglich der HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE davon ausgegangen, daß die Hauptspeisewasser-Regelung "Hauptlast" funktioniert, d.h. über die Hauptspeisewasser-Regelventile in die Dampferzeuger eingespeist wird.

Den Untersuchungen liegt dabei die Annahme zugrunde, daß die Auslösung der REAKTORSCHNELLABSCHALTUNG versagt. Versagt hingegen das mechanische System bei Auslösung der Reaktorschnellabschaltung, so wird die Stromversorgung der Steuerstäbe unterbrochen. Als Folge davon werden eine Turbinenschnellabschaltung ausgelöst sowie die Hauptspeisewasser-Regelventile geschlossen. Zeitverzögert wird die Hauptspeisewasser-Regelung "Schwachlast" in Betrieb genommen, d.h., die Schwachlastregelventile werden geöffnet. Die in Tabelle F2, 7-3 angeführten Mindestanforderungen an die SPEISEWASSERVERSORGUNG gelten auch unter dieser Voraussetzung.

Aufgrund des verzögerten Öffnens der Schwachlastregelventile sinkt der Wasserstand in den Dampferzeugern weiter ab. Wird in einem der vier Dampferzeuger der Wasserstand von 6,5 m unterschritten, so werden die Notspeisezuschaltsignale YZ51 ausge-

löst. Die Druckschieber aller Hauptspeisewasserpumpen werden dann geschlossen, so daß nur die NOTSPEISEWASSERVERSORGUNG zur Verfügung steht (Abschnitt 7.2.1). Im Rahmen der vorliegenden Studie wird davon ausgegangen, daß an die NOTSPEISEWASSERVERSORGUNG die gleichen Mindestanforderungen zu stellen sind wie an die HAUPTSPEISEWASSERVERSORGUNG. Hierzu sind weitergehende Untersuchungen erforderlich.

Da die NOTSPEISEWASSERVERSORGUNG bei ATWS-Störfällen praktisch sofort einzusetzen hat, kommt hierfür nur das Notspeisewassersystem in Frage. Zur Inbetriebnahme des Notstandssystems benötigt das Kraftwerkspersonal im Mittel 16 Minuten (Abschnitt 3.4). Aus diesem Grund ist auch eine VERZÖGERTE SPEISEWASSERVERSORGUNG nicht ausreichend.

Bei ATWS-Störfällen öffnen in der Regel alle vier Druckhalterventile. Sinkt der Kühlmitteldruck wieder ab, so ist ein SCHLIESSEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS, d.h. aller Druckhalterventile bzw. der redundanten Absperrarmaturen erforderlich. Andernfalls mündet der ATWS-Störfall in einen Kühlmittelverluststörfall "kleines Leck am Druckhalter". Für ein kleines Leck am Druckhalter werden die gleichen Mindestanforderungen zugrunde gelegt, wie für ein entsprechendes Leck in einer Hauptkühlmittelleitung. Analog zu WASH-1400 wird daher für ein solches Leck am Druckhalter die pessimistische Annahme getroffen, daß ein Ausfall der REAKTORSCHNELLABSCHALTUNG zum Kernschmelzen führt.

Während des Öffnens der Druckhalterventile gelangen Dampf und Wasser aus dem Druckhalter in den Abblasetank. Bei den ATWS-Störfällen "Notstromfall", "Ausfall der Hauptspeisewasserversorgung" und "Turbinenschnellabschaltung ohne Öffnen der Frischdampf-Umleiteinrichtung" kommt es dadurch bereits innerhalb einer bzw. weniger Minuten zum Ansprechen der Berstscheiben des Abblasetanks. Folglich strömen Wasser und Dampf aus dem Abblasebehälter in den Sicherheitsbehälter, wodurch der Druck und vor allem die Temperatur sowie die Feuchtigkeit in der Sicherheitsbehälter-Atmosphäre ansteigen. Das Öffnen der Druckhalterventile ist jedoch zeitlich begrenzt. Es ergeben sich meist Umgebungsbe-

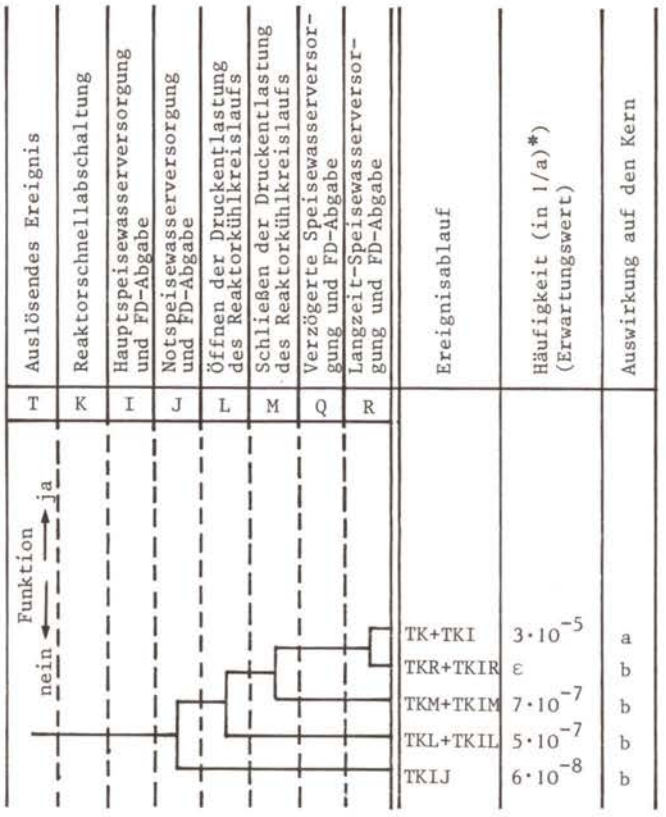
dingungen im Sicherheitsbehälter, die in etwa den Auslegungsbedingungen der Druckhalter-Abblaseventile, der Abblase-Steuerventile, der jeweils redundanten Absperrarmaturen, der Druckmeßumformer für die Kühlmitteldruckregelung und der Differenzdruckmeßumformer zur Wasserstandsmessung für die Speisewasserregelung entsprechen. Im Rahmen der vorliegenden Studie wird davon ausgegangen, daß aufgrund dieser bei ATWS-Störfällen herrschenden Umgebungsbedingungen kein Ausfall der angeführten Komponenten eintritt.

Bei ATWS-Störfällen findet nach dem Abblasen von Dampf über die Druckhalterventile ein Abblasen von Wasser statt. Dafür werden in der vorliegenden Studie die gleichen Zuverlässigkeitsdaten der Druckhalterventile zugrunde gelegt. In einem vom Bundesministerium für Forschung und Technologie geförderten Forschungsvorhaben wird gegenwärtig untersucht, ob die Druckhalter-Sicherheitsventile und deren Vorsteuerventile auch beim Wasserabblasen sowie beim Übergang von Dampf- auf Wasserabblasen ihre Aufgaben so zuverlässig wie beim Abblasen von Dampf erfüllen. Es ist zu prüfen, wieweit diese Versuchsergebnisse auch auf das Verhalten der Druckhalter-Abblaseventile übertragbar sind.

7.6.2 Ergebnisse

ATWS-Störfälle liefern wegen der hohen Zuverlässigkeit der Reaktorschnellabschaltung keinen wichtigen Beitrag zur Kernschmelzhäufigkeit: Die ermittelte Nichtverfügbarkeit dieser Systemfunktion liegt bei $5 \cdot 10^{-6}$. Durch Multiplikation mit der Häufigkeit von 5/a, mit der die Reaktorschnellabschaltung bei Leistungsbetrieb angefordert wird, ergibt sich eine obere Abschätzung für die Häufigkeit von ATWS-Störfällen, nämlich $3 \cdot 10^{-5}$/a. Zu einer Überhitzung des Kerns kann es bei solchen ATWS-Störfällen außerdem nur kommen, wenn weitere Ausfälle von angeforderten Teilsystemen vorliegen.

Für die Wahrscheinlichkeitsbewertung der Ereignisabläufe (Bild F2, 7-9) wurde der Einfachheit halber nicht unterschieden, ob den ATWS-Störfällen ein Ausfall des Reaktorschutzsystems oder



a kein Kernschmelzen
b Kernschmelzen

*) Häufigkeit der einzelnen Ereignisabläufe. Die Häufigkeit der auslösenden Ereignisse ist darin bereits enthalten.

Bild F2, 7-9:
Ereignisablaufdiagramm "ATWS-Störfälle"

des mechanischen Systems zur Reaktorschnellabschaltung zugrunde liegt. Im einen Fall ist die HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE verfügbar, im anderen Fall nicht, so daß nur die NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE zur Verfügung steht. Der zu-

letzt genannte ungünstigere Fall wurde den Wahrscheinlichkeitsabschätzungen zugrunde gelegt; der Einfluß auf die ermittelte Häufigkeit von nicht beherrschten Störfällen ist aber gering.

Die Wahrscheinlichkeiten für den Ausfall der einzelnen Systemfunktionen wurden meist für alle zu erwartenden Transienten T, die das Eingreifen von Sicherheitssystemen erfordern, gemeinsam bestimmt (Häufigkeit 5/a). Beim Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE ist jedoch zu unterscheiden, ob ein Notstromfall (Transiente T_1) vorliegt oder nicht (Häufigkeit des Notstromfalls 0,1/a). Die ermittelten Wahrscheinlichkeiten für den Ausfall der NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE betragen demnach $1 \cdot 10^{-2}$ bzw. $2 \cdot 10^{-3}$.

Eine weitere Ausnahme bildet das ÖFFNEN DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS. Wegen der anderen Mindestanforderungen ist hier der "Ausfall der Hauptspeisewasserversorgung" (Transiente T_2) getrennt zu untersuchen. Mit der Wahrscheinlichkeit für das Nichtöffnen eines Abblaseventils von $1{,}1 \cdot 10^{-1}$ und der Wahrscheinlichkeit für das Nichtöffnen eines Sicherheitsventils von $7 \cdot 10^{-3}$ ergibt sich die Wahrscheinlichkeit für das Nichtöffnen von

1v3 Druckhalterventilen	zu	$1{,}2 \cdot 10^{-1}$
2v3 Druckhalterventilen	zu	$1{,}5 \cdot 10^{-3}$

Die Transiente T_2 (Häufigkeit 0,8/a) liefert damit den Hauptbeitrag zu den Ereignisabläufen mit einem Ausfall des ÖFFNENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS.

Die Wahrscheinlichkeit für den Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS wurde zu $2{,}6 \cdot 10^{-3}$ bestimmt. Dabei wurde für das Nichtschließen eines Sicherheitsventils $1 \cdot 10^{-2}$ und für einen Abblasestrang $\hat{=}\ 3 \cdot 10^{-3}$ angesetzt.

Die bewerteten Ereignisabläufe für ATWS-Störfälle sind in Bild F2, 7-9 dargestellt. Die wichtigsten Beiträge zur ermittelten Häufigkeit von Kernschmelzunfällen kommen vom Ausfall des ÖFF-

NENS DER DRUCKENTLASTUNG DES REAKTORKÜHLKREISLAUFS und vom Ausfall des SCHLIESSENS DER DRUCKENTLASTUNG. Die ermittelten Beiträge sind unabhängig davon, ob die HAUPTSPEISEWASSERVERSORGUNG UND FD-ABGABE funktioniert oder nicht. Von einer weiteren Differenzierung der Ereignisabläufe konnte daher abgesehen werden. Für die Häufigkeit von nicht beherrschten ATWS-Störfällen erhält man insgesamt einen Erwartungswert von $1{,}3 \cdot 10^{-6}$/a (Median $8 \cdot 10^{-7}$/a, Unsicherheitsfaktor 5).

8. ZUVERLÄSSIGKEITSANALYSE DER REAKTORSCHNELLABSCHALTUNG

8.1 Reaktorschutzsystem zur Reaktorschnellabschaltung

8.1.1 Allgemeines

Der entsprechende Fehlerbaum des Reaktorschutzsystems ist im Anhang 4 (F2,II) dargestellt. Er setzt sich aus den Teilfehlerbäumen 1 bis 27 und dem Gesamtfehlerbaum 28 zusammen. Die Fehlerbäume mehrfach vorhandener, aber vom Aufbau her gleicher Teilsysteme sind nur jeweils einmal dargestellt.

Die Teilfehlerbäume 1 bis 19 berücksichtigen die Anregeebene, die Teilfehlerbäume 20 bis 25 die Logikebene und die Teilfehlerbäume 26 und 27 die Steuerebene (Relaisteil und Abschaltschütze). Für die Meßkanalgruppe zur Messung des Drucks in der Speisewasserleitung wurde kein eigener Fehlerbaum erstellt, da dieses Anregekriterium erst nach Erstellung der Fehlerbäume eingeführt wurde. Der Einfluß dieses Kriteriums auf die ermittelten Wahrscheinlichkeiten wurde abgeschätzt. "Common mode"-Ausfälle sind im Fehlerbaum nicht enthalten, sie werden getrennt bewertet.

8.1.2 Ergebnisse für Einzelanregungen

Zur Auswertung der Fehlerbaumanalysen wurde die mittlere Nichtverfügbarkeit aufgrund von unabhängigen Ausfällen der Hardware für jeweils ein einzelnes Anregekriterium, das zur Auslösung der Reaktorschnellabschaltung ausreicht, errechnet. Die Ergebnisse der Rechnungen sind in der Tabelle F2, 8-1 zusammengefaßt. In der Tabelle sind außerdem die durch "common mode"-Ausfälle der Hardware und aufgrund menschlichen Fehlverhaltens (Fehlkalibrierung von Meßkanälen) verursachten Nichtverfügbarkeiten angegeben. Die Nichtverfügbarkeiten aufgrund von Zufallsausfällen spielen gegenüber denjenigen aufgrund von "common mode"-Ausfällen keine Rolle.

Die Nichtverfügbarkeiten der Einzelanregungen aufgrund von unabhängigen Zufallsausfällen werden praktisch ausschließlich durch

Einzelanregung[1])	Erwartungswerte der mittleren Nichtverfügbarkeit infolge von	
	unabhängigen Ausfällen	"common mode"-Ausfällen
(1) Drehzahl von 3v4 Hauptkühlmittelpumpen < 93 %	10^{-8}	$2{,}3 \cdot 10^{-4}$
(2) DNB-Verhältnis < 1,5 (eine Anregung) (DNB vierfach als Anregekriterium vorhanden)	10^{-8}	$3{,}5 \cdot 10^{-3}$
(3) Kühlmitteldruck > 162 bar	10^{-5}	$1{,}5 \cdot 10^{-3}$
(4) Druckhalter-Wasserstand > 9,56 m	$2 \cdot 10^{-5}$	$1{,}5 \cdot 10^{-3}$
(5) Druckhalter-Wasserstand < 2,85 m UND Kühlmitteldruck < 145 bar	$3 \cdot 10^{-5}$	$3 \cdot 10^{-3}$
(6) Differenzdruck der Anlagenräume gegenüber Atmosphäre > 30 mbar	10^{-5}	$1{,}5 \cdot 10^{-3}$
(7) Differenzdruck der Betriebsräume gegenüber Atmosphäre > 30 mbar	10^{-5}	$1{,}5 \cdot 10^{-3}$
(8) Wasserstand in einem Dampferzeuger < 6,5 m	10^{-5}	$1{,}5 \cdot 10^{-3}$
(9) Mittlere Kühlmitteltemperatur > 311 °C	$1{,}5 \cdot 10^{-8}$	$1{,}5 \cdot 10^{-3}$
(10) Wasserstand in zwei Dampferzeugern < 8,85 m	10^{-8}	$2{,}3 \cdot 10^{-4}$
(11) Druck in der Speisewasserleitung > 78 bar	10^{-5}	$1{,}5 \cdot 10^{-3}$

[1]) Alle Druckgrenzwerte sind als Drücke, gemessen gegen Atmosphäre, zu verstehen.

Tab. F2, 8-1:

Nichtverfügbarkeit von Einzelanregungen aufgrund von unabhängigen Ausfällen und "common mode"-Ausfällen

Ausfälle der Meßkanäle beeinflußt. Die Nichtverfügbarkeiten von Logikteil und Relaisteil aufgrund solcher Ausfälle liegen deutlich niedriger (bei 10^{-10}).

Einige Anregekriterien sind nicht voneinander unabhängig, da zumindest teilweise dieselben Meßfühler und Meßkanäle verwendet werden. Dies trifft für die in der Tabelle F2, 8-1 unter (2) und (5), unter (2) und (9) sowie unter (8) und (10) genannten Anregekriterien zu.

8.1.3 Ergebnisse für einige auslösende Ereignisse

8.1.3.1 A l l g e m e i n e s

Zur Erkennung von Kühlmittelverluststörfällen und Transienten, die das Eingreifen von Sicherheitssystemen erfordern, sind praktisch immer mehrere Anregekriterien vorhanden. Die REAKTORSCHNELLABSCHALTUNG ist generell erst dann ausgefallen, wenn alle geeigneten Anregekriterien ausgefallen sind. Zur Ermittlung der Wahrscheinlichkeit für den Ausfall des Reaktorschutzsystems hinsichtlich der REAKTORSCHNELLABSCHALTUNG ist die Nichtverfügbarkeit der Meßkanalgruppen für die jeweils relevanten Anregekriterien und die Ausfallwahrscheinlichkeit des Relaisteils zu addieren.

Die Ausfallwahrscheinlichkeit pro Anforderung des Relaisteils der Reaktorschnellabschaltung aufgrund von CMA wurde in Abschnitt 3.3.6.4.4 zu

$$\bar{p}_{CMA} = 1{,}8 \cdot 10^{-6} \qquad (p_{CMA\ 50} = 1{,}2 \cdot 10^{-6}/K = 4{,}5)$$

ermittelt.

Im folgenden wird von den im Rahmen des Genehmigungsverfahrens berücksichtigten Anregekriterien ausgegangen. Für den Notstromfall werden abweichend hiervon nur die Drehzahl der Hauptkühlmittelpumpen und der Kühlmitteldruck berücksichtigt.

8.1.3.2 Leck in einer Hauptkühlmittelleitung

Anregekriterien:

- 1v4 DNB-Verhältnisse < 1,5 (Druck sinkt),
- Anlagenraumdruck > 30 mbar,
- Betriebsraumdruck > 30 mbar und
- Druckhalter-Wasserstand < 2,85 m und Kühlmitteldruck < 145 bar (gemeinsame Druckfühler für die Meßwerterfassung der DNB-Verhältnisse und des Kühlmitteldrucks).

Für die Bewertung der CMA der Meßkanalgruppen für Anlagen- bzw. Betriebsraumdruck wurde für die Ausfälle in der Hardware ein Faktor von 0,1 und für Ausfälle aufgrund menschlicher Fehlhandlungen eine "starke Kopplung" angesetzt (Abschnitt 3.3.6.4.4).

Zwischen den Meßkanalgruppen für DNB-Verhältnis und Druck im Reaktorkühlkreislauf wird für Hardware-Ausfälle eine "vollständige Kopplung" angesetzt, da dieselben Druckfühler verwendet werden. Zwischen Hardware-Ausfällen der DNB- bzw. Kühlmitteldruck-Meßkanäle einerseits und denen der Meßkanäle für die Raumdrücke andererseits wird keine Abhängigkeit berücksichtigt, da die Meßfühler diversitär sind. Die Wahrscheinlichkeit für diesen Ausfall wird durch den CMA des Relaisteils bestimmt und beträgt

$$\bar{p}_{CMA} = 1{,}8 \cdot 10^{-6} \qquad (p_{CMA\ 50} = 1{,}2 \cdot 10^{-6}/K = 4{,}5)$$

Sie gilt bei gleichen Anregekriterien auch für den Störfall "Leck am Druckhalter".

8.1.3.3 Notstromfall

Anregekriterien:

- 3v4 Hauptkühlmittelpumpen-Drehzahlen < 93 %,
- Kühlmitteldruck > 162 bar,
- Druckhalter-Wasserstand > 9,56 m,
- 2v4 Dampferzeuger-Wasserstände < 8,85 m,

- 1v4 Dampferzeuger-Wasserstände < 6,5 m,
- 1v4 DNB-Verhältnisse < 1,5,
- mittlere Kühlmitteltemperatur > 311 °C und
- 1v4 Drücke in den Speisewasserleitungen > 78 bar.

Berücksichtigt werden in der folgenden Abschätzung nur die ersten beiden Anregekriterien. Bei Auslösung der Reaktorschnellabschaltung durch das zweite Anregekriterium ergeben sich gegenüber einer unverzögerten Auslösung keine wesentlichen Unterschiede in den Systemanforderungen. Eine noch spätere Auslösung der Reaktorschnellabschaltung durch die weiteren Anregekriterien ist andererseits sehr unwahrscheinlich und ohne merkbaren Einfluß auf die Ergebnisse.

Bei den Ausfällen in der Hardware der Meßkanalgruppen für die Drehzahl der Hauptkühlmittelpumpen wird eine Abhängigkeit mit einem Faktor von 0,1 berücksichtigt. Für Ausfälle der gleichen Meßkanalgruppen aufgrund menschlicher Fehlhandlungen wird eine "starke Kopplung" unterstellt. Damit ergibt sich eine Ausfallwahrscheinlichkeit von:

$$\bar{p}_{CMA} = 2{,}1 \cdot 10^{-6} \qquad (p_{CMA\ 50} = 1{,}5 \cdot 10^{-6}/K = 4)$$

8.1.3.4 Turbinenschnellabschaltung und Ausfall der Frischdampf-Umleiteinrichtung

Anregekriterien:

- 1v4 Drücke in den Speisewasserleitungen > 78 bar,
- Kühlmitteldruck > 162 bar,
- Druckhalter-Wasserstand > 9,56 m,
- 2v4 Dampferzeuger-Wasserstände < 8,85 m und
- mittlere Kühlmitteltemperatur > 311 °C.

Es sind drei diversitäre Anregekriterien vorhanden. Für die Hardware der Messungen zur Erfassung des Druckes in den Speisewasserleitungen wird eine Kopplung mit dem Faktor 0,1 berücksichtigt. Es wird eine Kopplung von ca. 10 % aller CMA der Mes-

sungen des Kühlmitteldruckes bzw. des Druckes in den Speisewasserleitungen erwartet. Von den gleichen Bewertungen wird auch für die Hardware-CMA der Wasserstandsmessungen am Druckhalter bzw. an den Dampferzeugern ausgegangen. CMA aufgrund menschlicher Fehlhandlungen werden bei den Meßkanalgruppen zur Erfassung des Druckes in den Speisewasserleitungen und des Dampferzeuger-Wasserstandes durch "starke Kopplung" bewertet.

Die Wahrscheinlichkeit, daß die Auslösung der Reaktorschnellabschaltung versagt, wird allein durch den CMA des Relaisteils der Reaktorschnellabschaltung bestimmt. Es ergibt sich damit ein Wert von

$$\bar{p}_{CMA} = 1{,}8 \cdot 10^{-6} \qquad (p_{CMA\ 50} = 1{,}2 \cdot 10^{-6}/K = 4{,}5)$$

8.1.3.5 Ausfall der Hauptspeisewasserversorgung

Anregekriterien:

- 2v4 Dampferzeuger-Wasserstände < 8,85 m,
- 1v4 Dampferzeuger-Wasserstände < 6,5 m,
- Kühlmitteldruck > 162 bar,
- mittlere Kühlmitteltemperatur > 311 °C und
- Druckhalter-Wasserstand > 9,56 m.

Es sind also drei diversitäre Anregekriterien vorhanden. Dabei wird für die Hardware der Dampferzeuger-Wasserstandsmessungen eine Kopplung mit dem Faktor 0,1 berücksichtigt. Für Ausfälle aufgrund menschlicher Fehlhandlungen wird dagegen eine "starke Kopplung" angesetzt. Eine Kopplung von Ausfällen der Dampferzeuger- bzw. Druckhalter-Wasserstandsmessungen wird bei ca. 10 % aller CMA erwartet. Zur Wahrscheinlichkeit des Ausfalls der Anregung der Reaktorschnellabschaltung liefert bei dieser Störung nur der Ausfall des Relaisteils einen merklichen Beitrag. Damit ergibt sich ein Wert von

$$\bar{p}_{CMA} = 1{,}8 \cdot 10^{-6} \qquad (p_{CMA\ 50} = 1{,}2 \cdot 10^{-6}/K = 4{,}5)$$

8.1.3.6 Fehlfahren eines Frischdampfschiebers

Anregekriterien:

- Speisewasserdruck vor Dampferzeuger > 78 bar,
- Dampferzeuger-Wasserstand < 6,5 m,
- Kühlmitteldruck > 162 bar,
- Druckhalter-Wasserstand > 9,56 m und
- mittlere Kühlmitteltemperatur > 311 °C.

Es liegen hier drei diversitäre Anregekriterien vor. Zwischen den Hardware-CMA der diversitären Anregekriterien (Kühlmitteldruck-, Kühlmitteltemperatur- und Wasserstandsmessung) wird keine Abhängigkeit unterstellt. Bei Ausfällen aufgrund menschlicher Fehlhandlungen wird für Ausfälle der Speisewasserdruckmeßkanalgruppen und für die Meßkanalgruppen zur Erfassung der Dampferzeuger-Wasserstände eine "starke Kopplung" angesetzt.

Für die Hardware-Ausfälle der nichtdiversitären Anregekriterien wird eine gewisse Abhängigkeit mit einem Faktor von 0,1 berücksichtigt. Die Wahrscheinlichkeit eines CMA aller Anregekriterien ist auch hier gegenüber dem CMA des Relaisteiles vernachlässigbar. Somit erhält man

$$\bar{p}_{CMA} = 1{,}8 \cdot 10^{-6} \qquad (p_{CMA\ 50} = 1{,}2 \cdot 10^{-6}/K = 4{,}5)$$

8.1.3.7 Reaktivitätsstörfall

Anregekriterien:

- thermische Reaktorleistung > 108 %,
- kurzzeitkorrigierte Reaktorleistung, gleitender Grenzwert,
- mittlere Kühlmitteltemperatur > 311 °C,
- 1v4 DNB-Verhältnisse < 1,5,
- Kühlmitteldruck > 162 bar und
- Druckhalter-Wasserstand > 9,56 m.

Aufgrund der Vielzahl von diversitären Anregekriterien wird hier ebenfalls die Nichtverfügbarkeit der Auslösung der Reak-

torschnellabschaltung allein durch den Relaisteil bestimmt. Es ergibt sich also ein Wert von

$$\bar{p}_{CMA} = 1{,}8 \cdot 10^{-6} \qquad (p_{CMA\ 50} = 1{,}2 \cdot 10^{-6}/K = 4{,}5)$$

8.1.4 Zusammenfassung

Insgesamt zeigt sich, daß das Reaktorschutzsystem zur Auslösung einer Reaktorschnellabschaltung bei allen untersuchten Kühlmittelverluststörfällen und Transienten eine hohe Zuverlässigkeit aufweist. Die Wahrscheinlichkeit des Ausfalls der Anregeebene, der Logikebene und der Steuerebene aufgrund von CMA oder unabhängigen Ausfällen ist bei allen untersuchten auslösenden Ereignissen

$$\bar{p}_{CMA} \leq 2{,}1 \cdot 10^{-6}$$

Bei der Beurteilung dieses Ergebnisses sollte beachtet werden, daß für die Bewertung zum Teil sehr pessimistische Annahmen getroffen wurden.

8.2 Zuverlässigkeitsanalyse des mechanischen Systems zur Reaktorschnellabschaltung

Das mechanische System zur Reaktorschnellabschaltung gilt für die Systemfunktion REAKTORSCHNELLABSCHALTUNG als ausgefallen, wenn bei Anforderung ein bestimmter Wert der Kritikalität im Kern nicht unterschritten wird. Nach vorliegenden Rechnungen ist dies beim gleichzeitigen Ausfall von bestimmten Kombinationen von 7 Steuerstäben oder von beliebigen Kombinationen von mindestens 8 Steuerstäben der Fall, wobei für den Ausfall von genau 7 Steuerstäben insgesamt 16 Stabkombinationen zu zählen sind. Bei 8 und mehr ausgefallenen Stäben werden keine Einschränkungen bezüglich gefährlicher Kombinationen gemacht, d.h., es wird angenommen, daß jede mögliche Kombination von 8 oder mehr gleichzeitigen Stabausfällen zum Ausfall der REAKTORSCHNELLABSCHALTUNG führt.

Den Angaben liegen Rechnungen mit folgenden Annahmen zugrunde:

- frischer Kern bei Vollast-heiß und Xenongleichgewicht sowie
- Ausfall des Systems bei Anstieg des k_{eff}-Wertes auf k_{eff} = 0,9760 (Dopplereffekt 1,4 %, Unterkritikalität 1 %).

Ohne Berücksichtigung von 1 % Unterkritikalität ist ein weit höherer Grad der Redundanz gegeben: So ist die Funktion der REAKTORSCHNELLABSCHALTUNG noch erfüllt, wenn nur 12 Steuerstäbe einfallen, allerdings unter der Einschränkung, daß die Positionen der ausgefallenen Steuerstäbe über den Kernquerschnitt verteilt sind. In der vorliegenden Analyse wird jedoch pessimistisch von den oben genannten Kriterien ausgegangen.

Die Nichtverfügbarkeit für einen Ausfall des mechanischen Systems bei Anforderung aufgrund von unabhängigen Mehrfachausfällen ergibt sich aus:

$$\bar{u} = C_7 \cdot \bar{p}^7 + \sum_{i=8}^{61} C_i \cdot \bar{p}^i \qquad (8.1)$$

mit

$C_7 = 16$ Anzahl der Kombinationen mit genau 7 Steuerstäben, die zum Ausfall des mechanischen Systems führen

$\bar{p} = 3 \cdot 10^{-4}$ Ausfallwahrscheinlichkeit des Einzelstabes pro Anforderung (einschließlich Hilfsschütze)

zu

$$\bar{u} = 2 \cdot 10^{-19},$$

wobei das Ergebnis von den 8fachen Ausfällen bestimmt wird.

Der Ausfallwahrscheinlichkeit des Einzelstabes pro Anforderung $\bar{p} = 3 \cdot 10^{-4}$ liegt die Ausfallrate des Steuerstabs (einschließlich der Hilfsschütze) von $\bar{\lambda} = 2 \cdot 10^{-7}/h$ ($\lambda_{50} = 1,4 \cdot 10^{-7}/h$, K = 4) zugrunde (Fachband 3). Es wird davon ausgegangen, daß neben den jährlichen Funktionsprüfungen der Steuerstäbe auch jede betriebliche Reaktorschnellabschaltung als Funktionsprüfung bezüglich der vorliegenden Anforderungen angesehen werden kann.

Die Funktion "vollständiger, unverzögerter Stabeinfall" wird nach jeder betrieblichen Reaktorschnellabschaltung - geplant

oder ungeplant - überprüft. Dies geschieht durch Lampenanzeige auf der Warte und durch einen automatischen Rechnerausdruck. Der Rechner führt dazu zwei Abfragen zu verschiedenen Zeitpunkten durch: Zunächst werden alle Stäbe erfaßt, die ihre Endstellung nach 4 Sekunden noch nicht erreicht haben. Die zweite Abfrage nach 60 Sekunden registriert die Stäbe, die nach dieser Zeit nicht vollständig eingefallen sind, und gibt die Fallzeiten zwischen 4 und 60 Sekunden an. Die Stellungsmeldung erfolgt über Endschalter.

Der mittlere Zeitabstand zwischen zwei Reaktorschnellabschaltungen wurde aus der Betriebserfahrung der deutschen Kernkraftwerke mit Druckwasserreaktor ermittelt. Dabei wurde von mehreren aufeinanderfolgenden Reaktorschnellabschaltungen, die auf die gleiche Ursache zurückzuführen sind, jeweils nur die erste berücksichtigt. Als Erwartungswert der mittleren Zeitdauer zwischen zwei Anforderungen der Reaktorschnellabschaltungen erhält man:

$$\bar{t} = 1{,}8 \text{ Monate } (t_{50} = 1{,}3 \text{ Monate/K} = 4)$$

Dies führt mit der oben angegebenen Ausfallrate $\bar{\lambda} = 2 \cdot 10^{7}/h$ und der Beziehung

$$\bar{p} = \bar{\lambda} \cdot \bar{t}$$

näherungsweise zur Ausfallwahrscheinlichkeit des Einzelstabs pro Anforderung von

$$\bar{p} = 3 \cdot 10^{-4} \quad (p_{50} = 1{,}5 \cdot 10^{-4}/K = 7)$$

Dieser Wert wird auch zur Abschätzung der Nichtverfügbarkeit des mechanischen Systems aufgrund von CMA verwendet. Nach Abschnitt 3.3.6.5 erhält man

$$\bar{u}(\bar{t}) = 3 \cdot 10^{-6} \ (u_{50} = 1{,}4 \cdot 10^{-6}/K = 8)$$

mit

$$\bar{t} = 1{,}8 \text{ Monate}$$

Die Wahrscheinlichkeit für den Ausfall des mechanischen Systems aufgrund unabhängiger Mehrfachausfällen ist demgegenüber vernachlässigbar.

8.3 Zusammenfassung der Ergebnisse

Die Wahrscheinlichkeit für den Ausfall der Reaktorschnellabschaltung ergibt sich aus entsprechenden Wahrscheinlichkeiten für das Reaktorschutzsystem (einschließlich Relaisteil) und für das mechanische System (einschließlich Hilfsschütze). Der Beitrag des Reaktorschutzsystems ist je nach vorhandenen Anregekriterien etwas unterschiedlich. Für die Funktion der Reaktorschnellabschaltung ergibt sich im ungünstigsten Fall eine Nichtverfügbarkeit von

$$\bar{u}(\bar{t}) = 5 \cdot 10^{-6} \qquad \bar{t} = 1{,}8 \text{ Monate}$$

Der Median beträgt $3 \cdot 10^{-6}$ bei einem Streufaktor von 5. Diese Nichtverfügbarkeit setzt sich aus etwa gleich großen Beiträgen des Reaktorschutzsystems und des mechanischen Systems zusammen.

9. ZUVERLÄSSIGKEITSANALYSE FÜR DEN SICHERHEITSBEHÄLTER-ABSCHLUSS

9.1 Annahmen und Voraussetzungen

Gelangen bei einem Störfall radioaktive Stoffe aus dem Reaktorkern und dem Reaktorkühlkreislauf in den Sicherheitsbehälter, so stellt der Sicherheitsbehälter mit der umgebenden Stahlbetonhülle die letzte Sicherheitsbarriere dar. Bleibt diese Sicherheitsbarriere intakt, kommt es zu keiner nennenswerten Freisetzung von Spaltprodukten. Sollte sie jedoch versagen, so können radioaktive Spaltprodukte aus der Anlage in die Umgebung austreten.

Ein Versagen bzw. eine Undichtigkeit des Sicherheitsbehälters bei einem Störfall oder Unfall kann zwei prinzipiell unterschiedliche Ursachen haben. Zum einen ist es möglich, daß der Sicherheitsbehälter aufgrund von Fehlern im Anforderungsfall seine vorgesehene Funktion nicht erfüllt, d.h. nicht dicht schließt. Zum anderen ist es aber auch denkbar, daß der Sicherheitsbehälter im Verlauf eines Störfalls Belastungen unterworfen wird, für die er nicht ausgelegt ist. Überschreiten solche Belastungen die Versagensgrenzen des Sicherheitsbehälters, so wird er zwangsläufig beschädigt. Die Ausführungen im vorliegenden Fachband beziehen sich ausschließlich auf den ersten Komplex, das Versagen des Sicherheitsbehälterabschlusses. Das Versagen des Sicherheitsbehälters durch Überschreiten zulässiger Belastungen wird im Fachband 5 ausführlich diskutiert.

Entsprechend seiner Auslegung gilt der Sicherheitsbehälter als dicht, wenn seine Leckrate beim zugrunde gelegten Störfalldruck von 5,7 bar den Wert von 0,25 Vol.-% pro Tag nicht überschreitet. Wie in WASH-1400 wird in der vorliegenden Studie bei dichtem Sicherheitsbehälter pessimistisch nicht die Auslegungsleckrate, sondern das 10fache der Auslegungsleckrate unterstellt (Fachband 6).

Im Rahmen der hier durchgeführten Zuverlässigkeitsanalyse wird ein Versagen des Sicherheitsbehälterabschlusses angenommen, wenn die Leckrate des Sicherheitsbehälters - bezogen auf den Stör-

falldruck von 5,7 bar - größer als die 10fache Auslegungsleckrate ist. Dabei kann sich das Spektrum denkbarer Sicherheitsbehälterleckagen von kleinen Leckagen bis hin zum großflächigen Versagen der Stahlhülle erstrecken.

Bei Versagen des Sicherheitsbehälterabschlusses wird unterstellt, daß die Leckagen und eine eventuell damit verbundene Spaltproduktfreisetzung unmittelbar ins Freie gelangen. Eine mögliche Rückhaltewirkung von Sekundärabschirmung bzw. Ringraumabsaugung wird in einem solchen Fall nicht berücksichtigt.

Bei dichtem Sicherheitsbehälter in oben definiertem Sinn, d.h. bis zur 10fachen Auslegungsleckrate, kann die Ringraumabsaugung einen Unterdruck im Ringraum gegenüber der Außenatmosphäre aufrechterhalten (Fachband 5). In den Ringraum austretende Leckagen werden dabei gefiltert über den Kamin abgeführt. Bei einem Ausfall der Ringraumabsaugung wird unterstellt, daß die Leckagen unmittelbar ins Freie gelangen.

Die Leckabsaugung der Stahlhülle wird pessimistisch nicht berücksichtigt. Zum einen ist die Leckabsaugung der Stahlhülle nur für die Auslegungsleckrate der Stahlhülle bemessen, die im Vergleich zu den hier diskutierten Leckagen gering ist. Zum anderen werden von der Leckabsaugung nur einige Durchführungen erfaßt.

Bei den in der Zuverlässigkeitsanalyse zu untersuchenden Leckagemöglichkeiten wird zwischen Leckagen durch Versagen von aktiven oder passiven Komponenten unterschieden. Leckagen durch Versagen von aktiven Komponenten können über Rohrleitungen, die durch den Sicherheitsbehälter führen, auftreten, wenn die Absperrarmaturen dieser Rohrleitungen nicht schließen. Bei Versagen von passiven Komponenten, z.B. Schweißnähten und Dichtungen, ergeben sich Leckagen unmittelbar am Sicherheitsbehälter.

Versagt der Gebäudeabschluß von Rohrleitungen, so wird im allgemeinen pessimistisch der volle Rohrleitungsquerschnitt als Leckagequerschnitt unterstellt. Ausnahmen hiervon bilden Rohrleitungen, bei denen starke Einengungen des Querschnitts, z.B. durch Drosselstellen, vorhanden sind.

Beim Versagen von Dichtungen und Schweißnähten werden analog zu WASH-1400 folgende Leckquerschnitte unterstellt: Die Leckfläche bei Versagen einer Dichtung ergibt sich durch Multiplikation des Umfangs der Dichtung mit einer Spaltbreite von 1/16 inch ≙ 1,6 mm. Ein Versagen der Schweißnaht zwischen dem Stutzen einer Rohrdurchführung und der Stahlhülle führt zu einer Leckfläche, die 10 % des Stutzenquerschnitts beträgt. Versagt die Schweißnaht zwischen einem Reservestutzen und der Stahlhülle, so wird angenommen, daß der Reservestutzen - bedingt durch den Druckaufbau im Sicherheitsbehälter - aus der Stahlhülle herausgestoßen wird. Als Leckfläche muß in diesem Fall der volle Querschnitt des Stutzens angesetzt werden. Pessimistisch wird angenommen, daß alle Schweißnähte eines Stutzens an äußeren Stutzendurchmessern aufgebracht sind.

Für Systeme, die innerhalb des Sicherheitsbehälters geschlossen sind, d.h. keine Öffnung zum Reaktorkühlkreislauf bzw. zur Sicherheitsbehälter-Atmosphäre haben, werden keine Leckagen unterstellt. Entsprechendes gilt für Systeme, die außerhalb des Sicherheitsbehälters geschlossen und für einen Druck ausgelegt sind, der oberhalb des Auslegungsdruckes bzw. des Versagensdruckes des Sicherheitsbehälters liegt.

9.2 Fehlerbaumbeschreibungen

9.2.1 Allgemeines

Die verschiedenen Möglichkeiten von Leckagen aus dem Sicherheitsbehälter bei einem Störfall oder Unfall werden mit Hilfe der Fehlerbaumanalyse behandelt. Dabei hat es sich als zweckmäßig erwiesen, das Spektrum möglicher Leckagen in folgende drei Bereiche zu unterteilen:

- große Leckage des Sicherheitsbehälters, repräsentiert durch ein Leck mit einem Durchmesser von 300 mm,
- mittlere Leckage des Sicherheitsbehälters, repräsentiert durch ein Leck mit einem Durchmesser von 80 mm und
- kleine Leckage des Sicherheitsbehälters, repräsentiert durch ein Leck mit einem Durchmesser von 25 mm.

Mit diesen drei repräsentativen Lecks werden in der Studie alle möglichen Sicherheitsbehälterlecks abgedeckt. Die Zuordnung möglicher Leckagen zu den genannten Bereichen richtet sich bei Rohrleitungen im allgemeinen nach den Leitungsquerschnitten beim Durchtritt durch den Sicherheitsbehälter bzw. bei passiven Komponenten nach den äquivalenten Leckquerschnitten.

In den drei Bereichen sind folgende Systeme bzw. Komponenten zu betrachten:

- Große Leckage (Versagensart β_1):

  Lüftung:
  Unterdruckhaltung,
  Spülluft,

  Not- und Nachkühlsystem:
  HD-Einspeiseleitung,
  ND-Einspeiseleitung,
  Sumpfleitung,
  Nachkühlsaugleitung,

  Schweißnähte der:
  Schleusen,
  Stutzen und Reservestutzen für Rohrleitungen,

  Dichtungen der Materialschleuse.

- Mittlere Leckage (Versagensart β_2):

  Gebäudeentwässerung,

  Volumenregelsystem:
  Entnahmeleitung,
  Einspeiseleitung,

  Dichtungen:
  Personenschleuse,
  Notschleuse,

  Kabeldurchführungen.

- Kleine Leckage (Versagensart β_3):

  Leitungen des Abgassystems,

Leitungen zur Luftaktivitätsmessung,
Leitungen des Gebäudesprühsystems.

Bei dichtem Sicherheitsbehälter, d.h. im Rahmen der Zuverlässigkeitsanalyse bis zur zehnfachen Auslegungsleckage, wird ein möglicher Ausfall der Ringraumabsaugung (Versagensart η) analysiert.

Bei großen und mittleren Kühlmittelverluststörfällen, die von den Notkühlsystemen beherrscht werden, wird wie in WASH-1400 angenommen, daß eine Freisetzung von Spaltprodukten aus den Brennstoffhüllrohren in den Sicherheitsbehälter erfolgt. Hier ist deshalb die Möglichkeit einer Sicherheitsbehälter-Leckage zu untersuchen. In diesen Fällen wird vereinfachend nur ein Bereich von Sicherheitsbehälter-Leckagen betrachtet, der die mittlere und große Sicherheitsbehälter-Leckage umfaßt.

9.2.2 Große Leckage des Sicherheitsbehälters

Leckagen über die Lüftungsleitungen der Unterdruckhaltung werden im Fehlerbaum 20 A behandelt. Der Gebäudeabschluß der Lüftungsleitungen versagt, wenn entweder die Zuluft- oder die Abluftleitung nicht geschlossen wird. Der Abschluß einer Leitung fällt aus, wenn alle drei Gebäudeabschlußarmaturen nicht schließen bzw. die zugehörigen Gebäudeabschlußsignale ausfallen. Pessimistisch wird bei allen sechs Armaturen die Energieversorgung in Rechnung gesetzt.

Für die Schnellschlußklappen in den Leitungen der Unterdruckhaltung wird die gleiche Ausfallrate verwendet wie für Motorarmaturen, da zum Zeitpunkt der Rechnungen keine geeigneten Daten vorlagen. Die inzwischen verfügbare Betriebserfahrung zeigt, daß die Ausfallraten von Schnellschlußklappen in der gleichen Größenordnung liegen wie diejenigen von Motorarmaturen.

Die Spülluftleitungen werden im Fehlerbaum nicht berücksichtigt, da sie bei Normalbetrieb der Anlage geschlossen verriegelt sind. Leckagen aus dem Sicherheitsbehälter über das Not- und Nachkühlsystem (Ausfall der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOT-

KÜHLUNG) führen zum Ausfall des Not- und Nachkühlsystems und werden bei den Kühlmittelverluststörfällen behandelt (Abschnitt 6.1.2.1.1 bzw. 6.1.2.2.18).

Insgesamt werden in der Analyse rund 200 Schweißnähte von Schleusen, Stutzen und Reservestutzen berücksichtigt. In dieser Zahl sind pessimistisch auch einige Rohrleitungsstutzen enthalten, die einem Bereich mit geringerem Leckquerschnitt zuzuordnen wären. Entsprechend WASH-1400 beträgt die Ausfallwahrscheinlichkeit bei Anforderung für eine Schweißnaht $\bar{p} = 2{,}7 \cdot 10^{-7}$ (Median $p_{50} = 10^{-7}$, Unsicherheitsfaktor K = 10). Insgesamt ergibt sich für das Versagen einer der 200 Schweißnähte eine Ausfallwahrscheinlichkeit bei Anforderung von $\bar{p} \cong 5 \cdot 10^{-5}$ (Median $p_{50} = 5 \cdot 10^{-5}$, Unsicherheitsfaktor K = 1,1). Das entsprechende Funktionselement findet sich in den Gesamtfehlerbäumen für die Kühlmittelverluststörfälle, da ein Kühlmittelverluststörfall bei einer großen Leckage des Sicherheitsbehälters bei pessimistischer Betrachtung zum Kernschmelzen führt. Auf die Häufigkeit des nicht beherrschten Notstromfalls in Verbindung mit Versagen des Sicherheitsbehälterabschlusses hat das Versagen von Schweißnähten nur untergeordneten Einfluß.

Wie in WASH-1400 werden Fehler an der Stahlhülle, den Schweißnähten der Stahlhülle sowie an den Durchführungen selbst zu einem "Ausfall der Stahlhülle" zusammengefaßt. Entsprechend WASH-1400 ergibt sich hierfür eine Nichtverfügbarkeit bei Anforderung $\bar{p} = 5{,}5 \cdot 10^{-6}$ (Median $p_{50} = 6{,}5 \cdot 10^{-7}$, Unsicherheitsfaktor K = 30). Dieser Wert kann vernachlässigt werden.

Da beide Tore der Materialschleuse bei Normalbetrieb geschlossen sind, spielt das Versagen ihrer Schleusendichtungen keine Rolle (Ausfallwahrscheinlichkeit bei Anforderung $\bar{p} = 3 \cdot 10^{-5}$ pro Dichtung).

9.2.3 Mittlere Leckage des Sicherheitsbehälters

Leckagen über die Gebäudeentwässerung werden im Fehlerbaum 20 B behandelt. Die beiden Gebäudeabschlußarmaturen 23 TZ10 S001 und

22 TZ10 S002 erhalten durch das Reaktorschutzsystem einen ZU-Befehl. Schließen diese Armaturen nicht, so besteht eine Verbindung zwischen dem Inneren des Sicherheitsbehälters und den Abwassersammelbehältern.

Das Überschreiten des zulässigen Füllstandes in einem der Abwassersammelbehälter wird in der Warte gemeldet. Von der Warte aus kann die Leckage durch Zufahren der Motorarmatur vor dem Abwassersammelbehälter unterbunden werden. Da diese Motorarmaturen von der elektrischen Eigenbedarfsanlage aus versorgt werden, ist ein Schließen von der Warte aus nur möglich, wenn kein Notstromfall vorliegt. Bei den zu diesem Zeitpunkt herrschenden Drücken und Temperaturen des Sumpfwassers ist nicht mit einem Versagen der Kunststoff-Rohrleitungen zu rechnen. Die Wahrscheinlichkeit für das Nichtausführen der Handmaßnahme wird mit $\bar{p} = 0{,}3$ (Median $p_{50} = 0{,}1$, Unsicherheitsfaktor K = 10) angesetzt.

Leckagen aus dem Sicherheitsbehälter über das Volumenregelsystem können nur auftreten, wenn bei einem Störfall die Leitung zu den Kühlmittellagerbehältern geöffnet ist. Hierfür wird eine Wahrscheinlichkeit von 10^{-2} abgeschätzt. Leckagen über das Volumenregelsystem können dann gegenüber Leckagen über die Gebäudeentwässerung vernachlässigt werden.

Für die Dichtung der jeweils geschlossenen Tür der Personen- bzw. Notschleuse kann entsprechend WASH-1400 von einer Ausfallwahrscheinlichkeit bei Anforderung von $\bar{p} = 3 \cdot 10^{-5}$ (Median $p_{50} = 4 \cdot 10^{-6}$, Unsicherheitsfaktor K = 30) ausgegangen werden. Zieht man in Betracht, daß der Ausfall einer solchen Dichtung weder zum Versagen der Notkühlung führt, noch gemeinsame Komponenten (z.B. Reaktorschutzsignale) mit der Notkühlung vorhanden sind, so können Ausfälle der Dichtungen der genannten Schleusen vernachlässigt werden.

In der Analyse wird der Beitrag der Kabeldurchführungen und der entsprechenden Reservedurchführungen vernachlässigt. Die konstruktive Ausführung dieser Bauteile läßt ein Versagen bei einem Druckaufbau innerhalb des Sicherheitsbehälters nicht erwarten (Abschnitt 4.2.13).

9.2.4 Kleine Leckage des Sicherheitsbehälters

Leckagen über die Luftaktivitätsmessung und das Abgassystem werden im Fehlerbaum 20 C behandelt. Wenn beide Gebäudeabschlußarmaturen in einer der drei Leitungen zur Messung der Luftaktivität, die durch den Sicherheitsbehälter führen, nicht schließen, so liegt eine kleine Leckage des Sicherheitsbehälters vor. Entsprechendes gilt für die Zu- und Ableitung des Abgassystems.

Wird eine kleine Leckage beim Ausfall der Eigenbedarfsversorgung durch Ausfallkombinationen verursacht, die bereits zu einer mittleren Leckage (Versagensart β_2 bzw. Kategorie 3) führen, so sind diese Ausfallkombinationen bei der kleinen Leckage nicht mehr zu berücksichtigen.

Während des Leistungsbetriebs des Kraftwerks sind die Gebäudeabschlußarmaturen des Gebäudesprühsystems geschlossen. Sie bleiben bei einem Kühlmittelverluststörfall auch während des Flutbetriebs in dieser Stellung, so daß während dieser Zeit kein Versagen des Gebäudeabschlusses zu unterstellen ist.

Wenn das Not- und Nachkühlsystem auf Sumpfbetrieb umgeschaltet ist und der Druck im Sicherheitsbehälter über 1,5 bar liegt, wird das Gebäudesprühsystem von Hand in Betrieb genommen. Werden nach Beendigung des Sprühbetriebs die Gebäudeabschlußarmaturen nicht geschlossen, so ergibt sich eine Leckage aus dem Sicherheitsbehälter, wenn zusätzlich eine der Rückschlagklappen in den vier Druckleitungen der Pumpen nicht schließt. Für das Nichtschließen der Absperrarmaturen wird eine Wahrscheinlichkeit von 10^{-2} abgeschätzt. Die Leckage über das Gebäudesprühsystem kann dann vernachlässigt werden, da keine gemeinsamen Funktionselemente mit den zur Störfallbeherrschung erforderlichen Systemen vorhanden sind.

9.2.5 Ringraumabsaugung

Die Ringraumabsaugung wird im Fehlerbaum 20 D behandelt. Ein Ausfall der Ringraumabsaugung liegt dann vor, wenn der im Ringraum

erforderliche Unterdruck nicht gehalten werden kann. Dies ist der Fall, wenn mindestens drei der vier Gebläse versagen oder die Zu- bzw. Abluftleitung der Ringraumlüftung nicht abgeschlossen wird.

Für den Ausfall der Gebläse ist der CMA der Notstromdiesel beim Ausfall der Eigenbedarfsversorgung maßgeblich. Der Abschluß der Zuluftleitung der Ringraumlüftung versagt, wenn beide Lüftungsklappen offen bleiben. Entsprechendes gilt für die Abluftleitung.

9.3 Ergebnisse

9.3.1 Allgemeines

Bei der Zuverlässigkeitsanalyse des Sicherheitsbehälterabschlusses ist vor allem die Wahrscheinlichkeit von Interesse, mit der bei einem nicht beherrschten Störfall, d.h. bei Kernschmelzen, der Sicherheitsbehälterabschluß versagt. Das bedeutet, daß für jeden Störfall das TOP-Ereignis "Ausfall der Systemfunktionen" gemeinsam mit den Fehlerbäumen für das Versagen des Sicherheitsbehälterabschlusses für verschiedene Querschnitte zu behandeln ist (Versagensarten β_1, β_2, β_3, η). Dabei sind für jeden Kühlmittelverluststörfall bzw. jede Transiente folgende Ereignisse zu betrachten:

- Kernschmelzen und Leckage über Lüftungsleitungen (β_1, Freisetzungskategorie 2),
- Kernschmelzen und Leckage über das Gebäudeentwässerungssystem (β_2, Freisetzungskategorie 3),
- Kernschmelzen und Leckage über Leitungen NW25 (β_3, Freisetzungskategorie 4) und
- Kernschmelzen und Ausfall der Ringraumabsaugung (η, Freisetzungskategorie 5).

Im folgenden werden die Wahrscheinlichkeiten für den Eintritt der genannten Ereignisse unter der Bedingung, daß das auslösende Ereignis eingetreten ist, behandelt. Der Vollständigkeit halber wird für jeden Störfall bzw. jede Transiente auch die bedingte

Wahrscheinlichkeit für die Freisetzungskategorie 6 (Versagensart δ) angegeben.

9.3.2 Großes und mittleres Leck in einer Hauptkühlmittelleitung

Für das Versagen des Sicherheitsbehälterabschlusses beim nicht beherrschten großen bzw. mittleren Leck sind Ausfälle aller Reaktorschutzsignale von zwei Redundanzen von Bedeutung, da dann sowohl zwei Redundanzen der Gebäudeabschlußarmaturen als auch zwei Redundanzen der zur Störfallbeherrschung benötigten Systeme ausfallen. Für die Freisetzungskategorie 2 wird davon ausgegangen, daß die Notkühlung aufgrund von Leckagen in den Ringraum ausfällt. Die Ergebnisse für die einzelnen Freisetzungskategorien bei Versagen des Sicherheitsbehälterabschlusses sowie die Freisetzungskategorie 6 sind in Tabelle F2, 9-1 zusammengestellt. Im folgenden wird auf die dominierenden Beiträge zu den Ergebnissen eingegangen.

Beim Ausfall der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG beim großen Leck (Ereignisablauf AG des Ereignisablaufdiagrammes, Bild F2, 6-5) ist gleichzeitig auch der Pfad AG-β_1 der Kategorie 2 erfüllt. Andere Ausfälle spielen für AG-β_1 keine Rolle. Ebenso sind außer dem Ausfall der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE (Ereignisablauf AB) keine relevanten Beiträge zu AB-β_1 vorhanden. Entsprechendes gilt für die Ereignisabläufe S_1G-β_1 und S_1B-β_1 beim mittleren Leck (Bild F2, 6-6).

Für die Kategorien 3 und 4 ist der Ausfall der Reaktorschutzsignale der Redundanzen 2 und 3 von Bedeutung. Dadurch ist in der Kategorie 4 der Sicherheitsbehälterabschluß ausgefallen, in Kategorie 3 ist hierzu zusätzlich noch die Nichtausführung eines Handeingriffs erforderlich.

Durch den Ausfall der Reaktorschutzsignale der Redundanzen 2 und 3 stehen beim großen Leck die entsprechenden Redundanzen der ND-Einspeisung für Fluten nicht mehr zur Verfügung. Um den Ereignisablauf AE-β_2 bzw. AE-β_3 zu erfüllen, muß noch eine weitere

• Großes Leck	Freisetzungskategorien 2	3	4	5	6
$\bar{p}$ P_{50}/K	$8 \cdot 10^{-5}$ $8 \cdot 10^{-5}/2$	$5 \cdot 10^{-6}$ $1{,}6 \cdot 10^{-6}/13$	$4 \cdot 10^{-5}$ $3 \cdot 10^{-5}/3$	$3 \cdot 10^{-5}$ $2 \cdot 10^{-5}/3$	$1{,}6 \cdot 10^{-3}$ $1{,}3 \cdot 10^{-3}/3$
Prozentuale Beiträge	AG-β_1:60 % AB-β_1:40 %	AF-β_2:20 % AE-β_2:80 %	AF-β_3:30 % AE-β_3:70 %	AF-η:20 % AE-η:80 %	
• Mittleres Leck					
$\bar{p}$ P_{50}/K	$8 \cdot 10^{-5}$ $8 \cdot 10^{-5}/2$	$1 \cdot 10^{-5}$ $3 \cdot 10^{-6}/13$	$6 \cdot 10^{-5}$ $5 \cdot 10^{-5}/3$	$4 \cdot 10^{-5}$ $3 \cdot 10^{-5}/3$	$2{,}1 \cdot 10^{-3}$ $1{,}7 \cdot 10^{-3}/3$
Prozentuale Beiträge	S_1G-β_1:60 % S_1B-β_1:40 %	S_1F-β_2:12 % S_1E-β_2:6 % S_1C-β_2:42 % S_1CE-β_2:40 %	S_1F-β_3:17 % S_1E-β_3:8 % S_1C-β_3:45 % S_1CE-β_3:30 %	S_1F-η:9 % S_1E-η:5 % S_1C-η:40 % S_1CE-η:46 %	

Tab. F2, 9-1:

Prozentuale Beiträge der Ereignisabläufe mit Versagen des Gebäudeabschlusses beim "großen und mittleren Leck in einer Hauptkühlmittelleitung"

Erwartungswerte sowie Medianwerte und Unsicherheitsfaktoren für die bedingten Wahrscheinlichkeiten der Freisetzungskategorien 2 bis 6

Redundanz der Funktion ND-Einspeisung für Fluten ausfallen. Hierzu führt der Bruch der heißen Einspeiseleitung zum gebrochenen Hauptkühlkreislauf als Störfallfolge (Störfall wird im Strang 1 angenommen), zum Ausfall des Zwischenkühlstrangs 1 oder 4 sowie zum Ausfall des ND-Einspeisestranges 1 oder 4 für Fluten. Der Ausfall der Reaktorschutzsignale der Redundanzen 2 und 3 führt auch zum Ausfall der entsprechenden Stränge der ND-Einspeisung für Sumpf-Umwälzbetrieb. Fällt außerdem noch der Nebenkühlstrang 1 oder 4 oder die Sumpfumschaltung des Strangs 1 oder 4 aus, so liegt der Ereignisablauf AF-β_2 bzw. AF-β_3 vor.

Für die Ereignisabläufe S_1C-β_2 und S_1C-β_3 beim mittleren Leck ist der Ausfall des Dreiwegeventils 20 TH15 S006, der zum Aus-

fall des HD-Einspeisestranges führt, von großer Bedeutung. Der bereits beim großen Leck genannte Folgebruch oder der Ausfall des Zwischenkühlstranges 1 oder 4 führt zum Ausfall eines Stranges der HD-Einspeisung und liefert einen wesentlichen Beitrag zu den Ereignisabläufen $S_1CE\text{-}\beta_2$ und $S_1CE\text{-}\beta_3$.

Entsprechendes wie für die Kategorien 3 und 4 gilt auch für die Kategorie 5, wobei hier jedoch der Ausfall der Reaktorschutzsignale der Redundanzen 3 und 4 von Bedeutung ist. Die Ergebnisse für die Kategorie 6 unterscheiden sich nur unwesentlich von denjenigen für den nicht beherrschten Störfall.

Für die Wahrscheinlichkeit, daß bei einem beherrschten Störfall eine mittlere oder große Sicherheitsbehälterleckage vorliegt, wurde ein Wert von $2 \cdot 10^{-4}$, Unsicherheitsfaktor 2, ermittelt.

Ein solches Leck führt bei den Kühlmittelverluststörfällen "großes Leck" und "mittleres Leck", bei denen mit Hüllrohrschäden an den Brennelementen zu rechnen ist, zur Freisetzungskategorie 7. Liegen Leckagen des Sicherheitsbehälters bis zur 10fachen Auslegungsleckrate vor, so gehören zu diesen Kühlmittelverluststörfällen Aktivitätsfreisetzungen in der Freisetzungskategorie 8.

9.3.3 Kleines Leck in einer Hauptkühlmittelleitung

Die Ergebnisse der Gebäudeabschlußrechnungen für das kleine Leck in einer Hauptkühlmittelleitung sind in Tabelle F2, 9-2 dargestellt.

Für Kernschmelzen und Versagen des Sicherheitsbehälterabschlusses in der Freisetzungskategorie 2 (β_1, Lüftungsleitungen) wird eine bedingte Wahrscheinlichkeit von $8 \cdot 10^{-5}$ (Erwartungswert) ermittelt. Etwa 50 % dieses Wertes resultieren aus dem Ereignisablauf $S_2IG\text{-}\beta_1$ (Bild F2, 6-8), wobei der Bruch der Schweißnähte den maximalen Beitrag liefert. Der Ausfall von G bedingt β_1, so daß die Pfade S_2IG und $S_2IG\text{-}\beta_1$ identisch sind. Der Ereignisablauf $S_2IB\text{-}\beta_1$ trägt zur Kategorie 2 beim kleinen Leck etwa 40 % bei; der Ausfall von B bedingt β_1, so daß die Ereignisabläufe

• Kleines Leck	Freisetzungskategorien				
	2	3	4	5	6
$\bar{p}$	$8 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	$7 \cdot 10^{-5}$	$4 \cdot 10^{-5}$	$2 \cdot 10^{-2}$
p_{50}/K	$8 \cdot 10^{-5}/2$	$3 \cdot 10^{-6}/12$	$6 \cdot 10^{-5}/2{,}5$	$3 \cdot 10^{-5}/2{,}5$	$1{,}4 \cdot 10^{-2}/4{,}5$
Prozentuale Beiträge	$S_2IG\text{-}\beta_1$:50 % $S_2IB\text{-}\beta_1$:40 % $S_2IJG\text{-}\beta_1$:10 %	$S_2IF\text{-}\beta_2$:4 % $S_2IE\text{-}\beta_2$:5 % $S_2IC\text{-}\beta_2$:11 % $S_2ICE\text{-}\beta_2$:11 % $S_2IJ\text{-}\beta_2$:50 % $S_2IJF\text{-}\beta_2$:6 % $S_2IJCE\text{-}\beta_2$:13 %	$S_2IF\text{-}\beta_3$:6 % $S_2IE\text{-}\beta_3$:5 % $S_2IC\text{-}\beta_3$:11 % $S_2ICE\text{-}\beta_3$:9 % $S_2IJ\text{-}\beta_3$:50 % $S_2IJF\text{-}\beta_3$:6 % $S_2IJCE\text{-}\beta_3$:7 %	$S_2IJ\text{-}\eta$:58 % $S_2IJCE\text{-}\eta$:25 %	$S_2IF\text{-}\delta$:2 % $S_2IC\text{-}\delta$:5 % $S_2IJ\text{-}\delta$:93 %

Tab. F2, 9-2:

Prozentuale Beiträge der Ereignisabläufe mit Versagen des Sicherheitsbehälterabschlusses beim "kleinen Leck in einer Hauptkühlmittelleitung"

Erwartungswerte sowie Medianwerte und Unsicherheitsfaktoren für die bedingten Wahrscheinlichkeiten der Freisetzungskategorien 2 bis 6

S_2IB und $S_2IB\text{-}\beta_1$ identisch sind. Weitere 10 % gehen auf Ereignisablauf S_2IJG zurück, wieder mit dem Bruch der Schweißnähte als dominantem Beitrag.

Die bedingte Wahrscheinlichkeit für Kernschmelzen und gleichzeitiges Versagen des Sicherheitsbehälterabschlusses in der Freisetzungskategorie 3 (β_2, Gebäudeentwässerung) beträgt $1 \cdot 10^{-5}$. Im weitaus überwiegenden Teil der Ausfallkombinationen sind Ausfälle der Reaktorschutzsignale der Redundanzen 2 und 3 enthalten. Diese Ausfälle führen einerseits zum Versagen der Gebäudeabschlußarmatur in der entsprechenden Redundanz und haben andererseits in der Mehrzahl der Fälle auch den Ausfall des Notspeise-, HD- und ND-Einspeisestranges dieser Redundanz zur Folge. Zum Versagen des Sicherheitsbehälterabschlusses ist zusätzlich entweder die Nichtausführung einer Handmaßnahme oder der Ein-

tritt des Notstromfalls erforderlich. Der Ausfall des Handeingriffs spielt dabei gegenüber dem Notstromfall die dominante Rolle.

Mit etwa 50 % liefert der Ereignisablauf $S_2IJ\text{-}ß_2$ den größten Einzelbeitrag zur Kategorie $S_2\text{-}ß_2$. Neben den bereits genannten Ausfällen von Reaktorschutzsignalen der Redundanzen 2 und 3 und dem Versagen des Handeingriffs zum Schließen der Gebäudeabschlußarmaturen sind hier Ausfälle bei den Notspeisewassersträngen 1 oder 4 (ohne Hilfssysteme) relevant. Von Bedeutung bei diesem Ereignisablauf sind auch Kombinationen mit Ausfall der Handmaßnahme "Abfahren mit 100 °C/h" und Versagen des Gebäudeabschlusses durch den Ausfall beider Gebäudeabschlußarmaturen.

Die Ereignisabläufe S_2IF-, S_2IE-, S_2IC-, S_2ICE-, S_2IJF- und $S_2IJCE\text{-}ß_2$ tragen jeweils 4 bis 15 % zur bedingten Wahrscheinlichkeit von $S_2\text{-}ß_2$ bei.

Auch hier sind Ausfälle der Reaktorschutzsignale der Redundanzen 2 und 3 in starkem Maße beteiligt. Speziell beim Ereignisablauf $S_2IJCE\text{-}ß_2$ liefert der Eintritt des Notstromfalls einen wesentlichen Beitrag.

Für Kernschmelzen und gleichzeitiges Versagen des Sicherheitsbehälterabschlusses in der Freisetzungskategorie 4 wird beim kleinen Leck in einer Hauptkühlmittelleitung eine bedingte Wahrscheinlichkeit von $7 \cdot 10^{-5}$ ermittelt. Ähnlich wie in Kategorie 3 sind vor allem die Reaktorschutzsignale von Bedeutung, hier die Redundanzen 1, 2 und 3. Zum Versagen des Sicherheitsbehälterabschlusses genügt der Ausfall von jeweils zwei Gebäudeabschlußarmaturen in einer von fünf Lüftungs- bzw. Entwässerungsleitungen, wobei als Ursache sowohl der Ausfall der Armatur selbst als auch der Ausfall des entsprechenden Reaktorschutzsignals relevant sind.

Der Ereignisablauf $S_2IJ\text{-}ß_3$ liefert mit ca. 50 % den höchsten Beitrag zu $S_2\text{-}ß_3$. Die entscheidenden Ausfallkombinationen sind:

- Ausfall von Reaktorschutzsignalen der Redundanzen 1 und 2 oder 2 und 3 und zusätzlicher Ausfall eines Notspeisewasserstranges einer anderen Redundanz (3 oder 4 bzw. 1 oder 4),

- Ausfall der Handeingriffe zum Abfahren und Ausfall von zwei Gebäudeabschlußarmaturen (durch Ausfall der Armatur oder Ausfall der Reaktorschutzsignale),
- Ausfall des Reaktorschutzsignals der Redundanzen 1, 2 oder 3 und Ausfall einer Gebäudeabschlußarmatur (mechanischer Ausfall) sowie Ausfall von zwei Notspeisewassersträngen.

Die Ereignisabläufe S_2IF-, S_2IE-, S_2IC-, S_2ICE-, S_2IJF- und S_2IJCE-β_3 tragen mit jeweils 5 bis 11 % zum S_2-β_3 bei. Hier sind vor allem zu nennen:

- Ausfälle von Reaktorschutzsignalen der Redundanzen 1 und 2 bzw. 2 und 3 und das Versagen eines Stranges einer weiteren Redundanz bei der entsprechenden Systemfunktion.

Für Kernschmelzen und Versagen der Ringraumabsaugung (Freisetzungskategorie 5) ergibt sich eine bedingte Wahrscheinlichkeit von $4 \cdot 10^{-5}$. In dieser Kategorie sind vor allem die Reaktorschutzsignale der Redundanzen 3 und 4 maßgebend. So wird der Ereignisablauf S_2IJ-η mit ca. 58 % von S_2-η stark durch die Ausfälle dieser Reaktorschutzsignale mit zusätzlichem Ausfall des Notspeisewasserstranges der Redundanz 1 oder 2 bestimmt. Ebenfalls von Bedeutung sind die gleichzeitigen Ausfälle eines Reaktorschutzsignals (Redundanz 3 oder 4), einer Gebäudeabschluß-Armatur (Redundanz 3 oder 4) und zweier Notspeisewasserstränge der Redundanzen 1, 2 oder 4. Beim Ereignisablauf S_2IJCE-η, der etwa 25 % zu S_2-η liefert, spielt der Notstromfall in Verbindung mit dem CMA der Diesel die entscheidende Rolle.

Die Werte für die bedingten Wahrscheinlichkeiten in der Freisetzungskategorie 6 entsprechen im wesentlichen denen für Kernschmelzen (Abschnitt 6.1.5.2).

9.3.4 Notstromfall

Beim Notstromfall sind hier nur die Ereignisabläufe T_1IR, T_1IJQ und T_1IJMQ gemeinsam mit dem Versagen des Sicherheitsbehälterabschlusses zu betrachten (Tabelle F2, 9-3).

• Notstrom-fall	Freisetzungskategorien				
	2	3	4	5	6
$\bar{p}$	$2 \cdot 10^{-7}$	$1 \cdot 10^{-6}$	$3 \cdot 10^{-6}$	$7 \cdot 10^{-5}$	$5 \cdot 10^{-5}$
p_{50}/k	$1{,}2 \cdot 10^{-7}/6$	$6 \cdot 10^{-7}/7$	$1{,}3 \cdot 10^{-6}/8$	$3 \cdot 10^{-5}/9$	$4 \cdot 10^{-5}/4$
Prozentuale Beiträge	T_1IR-β_1:30 % T_1IJQ-β_1:66 % T_1IJMQ-β_1:4 %	T_1IR-β_2:10 % T_1IJQ-β_2:85 % T_1IJMQ-β_2:5 %	T_1IJQ-β_3:95 % T_1IJMQ-β_3:5 %	T_1IJQ-η:95 % T_1IJMQ-η:5 %	T_1IR-δ:75 % T_1IJQ-δ:25 %

Tab. F2, 9-3:

Prozentuale Beiträge der Ereignisabläufe mit Versagen des Sicherheitsbehälterabschlusses beim "Notstromfall"

Erwartungswerte sowie Medianwerte und Unsicherheitsfaktoren für die bedingten Wahrscheinlichkeiten der Freisetzungssetzungskategorien 2 bis 6

Für die Kategorie 2 liefern die genannten Ereignisabläufe gemeinsam mit dem CMA der Gebäudeabschlußsignale den Hauptbeitrag. Die Gebäudeabschlußsignale werden vom Notkühlvorbereitungssignal abgeleitet. Im Notstromfall kommt es nicht zum Ansprechen des Anregekriteriums Kühlmitteldruck < 110 bar; damit steht als Anregekriterium für die Gebäudeabschlußsignale nur die UND-Verknüpfung der Messung des Druckhalterwasserstandes < 2,85 m und der Messungen der Differenzdrücke der Anlagen- bzw. Betriebsräume gegen Atmosphäre < 30 mbar, die ihrerseits ODER-verknüpft sind, zur Verfügung. Insgesamt ergibt sich durch den CMA der Gebäudeabschlußsignale eine Nichtverfügbarkeit von $m_{50} = 1{,}4 \cdot 10^{-3}/K = 3$ für den Gebäudeabschluß der Lüftungsleitungen.

In den Kategorien 3 und 4 spielt der CMA der Notstromdiesel eine wichtige Rolle, was dazu führt, daß der Pfad T_1IR bedeutungslos ist. Bei einem CMA der Notstromdiesel ist der Notstromfall nicht beherrscht, wenn außerdem noch das Notstandssystem ausfällt. Den Hauptbeitrag zum Pfad T_1IJQ-β_2 liefert der zusätzliche Ausfall der Gebäudeabschlußarmatur der Redundanz 3 der Gebäudeentwässerung einschließlich Ansteuerung, Energieversorgung und Reaktorschutzsignal. Der Grund hierfür ist, daß der CMA der Notstrom-

diesel auch zum Ausfall der Gebäudeabschlußarmatur der Redundanz 2 wegen deren Energieversorgung führt. Entsprechendes gilt für die Kategorie 4, wozu hier mehrere Gebäudeabschlußarmaturen der Redundanz 3 beitragen.

Der CMA der Notstromdiesel führt in Kategorie 5 direkt zum Ausfall des Sicherheitsbehälterabschlusses, was zu einer relativ hohen Häufigkeit führt. Dementsprechend reduziert sich die Häufigkeit für die Kategorie 6.

9.3.5 Kleines Leck am Druckhalter beim Notstromfall

Die Erwartungswerte sowie Medianwerte und Unsicherheitsfaktoren für die bedingten Wahrscheinlichkeiten des nichtbeherrschten kleinen Lecks am Druckhalter mit Versagen des Sicherheitsbehälterabschlusses in den Freisetzungskategorien 2 bis 6 sind in Tabelle F2, 9-4 dargestellt. Bedingung ist, daß der Notstromfall eingetreten ist. Eine prozentuale Aufteilung dieser Werte auf die relevanten Ereignisabläufe ist in der gleichen Tabelle zu finden.

Für die Freisetzungskategorie 2 wird eine bedingte Wahrscheinlichkeit von $2 \cdot 10^{-7}$ ermittelt. Den Hauptbeitrag mit etwa 60 % von T_1S_2-β_1 liefert der Ereignisablauf $T_1S_2'IG$-β_1. Er ist identisch mit $T_1S_2'IG$, (Abschnitt 9.3.3), d.h. mit dem Versagen der SICHERHEITSBEHÄLTER-INTEGRITÄT FÜR DIE NOTKÜHLUNG. Da spielt das Versagen der Schweißnähte die dominante Rolle. Zum Eintritt des kleinen Lecks führt bei diesem Ereignisablauf vor allem der Ausfall des Druckhalter-Abblaseventils oder des Abblase-Steuerventils zusammen mit dem Ausfall des Abblase-Absperrventils. Der Ausfall der MESSWERTERFASSUNG FÜR DIE NOTKÜHLVORBEREITUNGSSIGNALE führt in Verbindung mit dem Eintritt des kleinen Lecks zum Ereignisablauf $T_1S_2'IB$-β_1 (identisch mit $T_1S_2'IB$, vgl. Abschnitt 9.3.3) und trägt etwa 34 % zu T_1S_2-β_1 bei. Hier sind im wesentlichen die CMA durch Fehlkalibrierung von Meßkanälen (menschliches Fehlverhalten), die Ausfälle des Druckhalter-Abblaseventils oder Abblase-Steuerventils und des Abblase-Absperrventils beteiligt.

• Kleines Leck am Druckhalter beim Notstromfall	Freisetzungskategorien				
	2	3	4	5	6
$\bar{p}$	$2 \cdot 10^{-7}$	$2 \cdot 10^{-6}$	$2 \cdot 10^{-6}$	$4 \cdot 10^{-5}$	$2 \cdot 10^{-5}$
für T_1S_2': P_{50}/K	$1{,}8 \cdot 10^{-7}/3{,}5$	$6 \cdot 10^{-7}/8$	$5 \cdot 10^{-7}/7$	$8 \cdot 10^{-6}/7$	$6 \cdot 10^{-6}/9$
für T_1S_2'': P_{50}/K	ε	$2 \cdot 10^{-7}/9$	$3 \cdot 10^{-7}/9$	$8 \cdot 10^{-6}/10$	$2 \cdot 10^{-7}/17$
Prozentuale Beiträge	$T_1S_2'IG\text{-}\beta_1$:60 %	$T_1S_2'IC\text{-}\beta_2$:6 %	$T_1S_2'ICE\text{-}\beta_3$:44 %	$T_1S_2'ICE\text{-}\eta$:38 %	$T_1S_2'IC\text{-}\delta$:20 %
	$T_1S_2'ICE\text{-}\beta_1$:4 %	$T_1S_2'ICE\text{-}\beta_2$:59 %	$T_1S_2'IJCE\text{-}\beta_3$:6 %	$T_1S_2'IJCE\text{-}\eta$:10 %	$T_1S_2'ICE\text{-}\delta$:50 %
	$T_1S_2'IB\text{-}\beta_1$:34 %	$T_1S_2'IJCE\text{-}\beta_2$:6 %			$T_1S_2'IJ\text{-}\delta$:10 %
	$T_1S_2''ICE\text{-}\beta_1$:2 %	$T_1S_2''ICE\text{-}\beta_2$:24 %	$T_1S_2''ICE\text{-}\beta_3$:39 %	$T_1S_2''ICE\text{-}\eta$:38 %	$T_1S_2''ICE\text{-}\delta$:5 %
		$T_1S_2''IJCE\text{-}\beta_2$:6 %	$T_1S_2''IJCE\text{-}\beta_3$:6 %	$T_1S_2''IJCE\text{-}\eta$:13 %	$T_1S_2''IJCE\text{-}\delta$:1 %

Tab. F2, 9-4:

Prozentuale Beiträge der Ereignisabläufe mit Versagen des Sicherheitsbehälterabschlusses beim "kleinen Leck am Druckhalter beim Notstromfall"

Erwartungswerte sowie Medianwerte und Unsicherheitsfaktoren für die bedingten Wahrscheinlichkeiten der Freisetzungskategorien 2 bis 6

Die Ereignisabläufe $T_1S_2'ICE\text{-}\beta_1$ und $T_1S_2''ICE\text{-}\beta_1$ ergeben zusammen etwa 6 % der Freisetzungskategorie 2. Die wesentlichen Ausfallkombinationen enthalten den CMA der Notstromdiesel (führt zum Versagen der HD-EINSPEISUNGEN und ND-EINSPEISUNGEN und der Klappen des Gebäudeabschlusses in der Redundanz 2), den Ausfall des Druckhalter-Abblaseventils oder des Abblase-Steuerventils (führt in Verbindung mit dem CMA der Diesel zum kleinen Leck) und Ausfälle von zwei Klappen des Gebäudeabschlusses der Redundanzen 1 und 3 oder 3 und 4. Zum Versagen der Klappen führen dabei vor allem Kurzschlüsse im Reaktorschutzsystem, Ausfälle der Klappen selbst oder Ausfälle der Gruppensicherungen, der Abzweige oder der Steuerketten.

Die bedingte Wahrscheinlichkeit für ein nichtbeherrschtes kleines Leck am Druckhalter und Versagen des Sicherheitsbehälterabschlusses in der Freisetzungskategorie 3 beträgt $2 \cdot 10^{-6}$. 59 % dieses Wertes gehen auf den Ereignisablauf $T_1S_2'ICE\text{-}\beta_2$ zurück. Zum Versagen des Sicherheitsbehälterabschlusses führt das Nichtschließen von zwei Motorarmaturen des Gebäudeentwässerungssystems. Neben dem Ausfall der Armaturen spielen vor allem die Ausfälle der Reaktorschutzsignale YZ33 in den Redundanzen 2 und 3 durch Kurzschlüsse und der Ausfall der Notstromschiene FV der Redundanz 2 eine Rolle, weil hiervon gleichzeitig die Systemfunktionen HD-EINSPEISUNGEN, ND-EINSPEISUNGEN und Schließen der Druckentlastung betroffen sind. Wesentliche Ausfallkombinationen für diesen Ereignisablauf sind damit:

- Ausfall des Druckhalter-Abblaseventils oder Abblase-Steuerventils und Ausfall des Abblase-Absperrventils (beides führt zum kleinen Leck) sowie Ausfall von zwei Notstromschienen (Redundanzen 2 und 1 oder 4) und Kurzschluß in der Redundanz 3 des Reaktorschutzsystems,
- Ausfall des Druckhalter-Abblaseventils oder Abblase-Steuerventils und Ausfall von drei Notstromschienen (Redundanzen 1, 2 und 4) sowie Ausfall des Reaktorschutzsignals oder der Gebäudeabschlußarmatur der Redundanz 3. Anstelle des Ausfalls der Notstromschienen der Redundanz 1 führt mit einem Beitrag gleicher Größenordnung der Ausfall des Kuppelschalters für die Notstromschienen 1 und 4 ebenfalls zu diesem Ereignisablauf.

Weiterhin spielt der CMA der Notstromdiesel in Verbindung mit dem Versagen des Druckhalter-Abblaseventils oder Abblase-Steuerventils und dem zusätzlichen Ausfall der Gebäudeabschluß-Armaturen oder des Reaktorschutzsignals der Redundanz 3 eine Rolle.

Der nächstniedrigere Beitrag mit etwa 24 % von T_1S_2-β_2 resultiert aus dem Ereignisablauf $T_1S_2''ICE$-β_2. Die bedingte Wahrscheinlichkeit dafür beträgt $4 \cdot 10^{-7}$ und setzt sich im wesentlichen aus minimalen Schnittmengen zusammen, die den CMA der Notstromdiesel und den Ausfall der kurzfristigen Inbetriebnahme des Notstandssystems enthalten. Dazu kommen die Ausfälle eines der beiden Druckhalter-Abblaseventile oder Abblase-Steuerventile oder des Reaktorschutzsignals YZ37 und der Ausfall der Gebäudeabschlußarmatur der Redundanz 3.

Die Ereignisabläufe $T_1S_2'IJCE$-β_2 und $T_1S_2''IJCE$-β_2 mit dem Versagen der Systemfunktion NOTSPEISEWASSERVERSORGUNG UND FD-ABGABE tragen jeweils etwa 6 % zur Freisetzungskategorie 3 bei. Als bedingte Wahrscheinlichkeit wird für beide Abläufe der gleiche Wert 10^{-7} ermittelt.

Von Bedeutung sind hier wieder der CMA der Notstromdiesel, Ausfall der kurzfristigen Inbetriebnahme des Notstandssystems, Ausfälle des Druckhalter-Abblaseventils oder der Abblase-Steuerventile und der Gebäudeabschlußarmatur der Redundanz 3. Dazu kommt der Ausfall einer der beiden Einspeisungen durch das Notstandssystem.

Beim Ereignisablauf $T_1S_2'IC$-β_2, der mit 10^{-7} ebenfalls 6 % zu T_1S_2-β_2 liefert, sind neben den Ausfällen, die zum Leck führen (Ausfall von zwei Druckhalter-Armaturen), vor allem der Ausfall der Notstromschiene FV der Redundanz 2, der Kurzschluß in Redundanz 3 des Reaktorschutzsystems und der Ausfall der HD-Einspeisung der Redundanz 1 oder 4 von Bedeutung.

Für die bedingte Wahrscheinlichkeit des unbeherrschten kleinen Lecks am Druckhalter mit Versagen des Sicherheitsbehälterabschlusses entsprechend der Freisetzungskategorie 4 ergibt sich $2 \cdot 10^{-6}$.

Der Hauptbeitrag mit etwa 44 % resultiert aus dem Ereignisablauf $T_1S_2'ICE-\beta_3$. Die dominanten Ausfallkombinationen enthalten dabei den CMA der Notstromdiesel und den Ausfall des Druckhalter-Abblaseventils oder Abblase-Steuerventils. Beides führt zum kleinen Leck, zum Versagen der HD-EINSPEISUNGEN und ND-EINSPEISUNGEN und zum Ausfall der Energieversorgung für die Gebäudeabschlußarmaturen. Es genügt dann der zusätzliche Ausfall einer redundanten Gebäudeabschlußarmatur, um diesen Ereignisablauf zu bewirken. Als bedingte Wahrscheinlichkeit wird dafür der Wert $8 \cdot 10^{-7}$ ermittelt.

In der gleichen Größenordnung, nämlich $7 \cdot 10^{-7}$, liegt die bedingte Wahrscheinlichkeit für den Ereignisablauf $T_1S_2''ICE-\beta_3$, die damit etwa 39 % von $T_1S_2-\beta_3$ ausmacht. Zum Unterschied von $T_1S_2'ICE-\beta_3$ enthalten die wesentlichen minimalen Schnittmengen einerseits den zusätzlichen Ausfall der Inbetriebnahme des Notstandssystems bis ca. 30 Minuten nach Eintritt des Notstromfalls, andererseits führt wie bei allen Abläufen T_1S_2'' der Ausfall eines der beiden Druckhalter-Abblaseventile oder eines der beiden zugehörigen Abblase-Steuerventile zum kleinen Leck. Mit jeweils ca. 6 % sind die Ereignisabläufe $T_1S_2'IJCE-\beta_3$ und $T_1S_2''IJCE-\beta_3$ beteiligt. Die bedingten Wahrscheinlichkeiten von jeweils $1 \cdot 10^{-7}$ sind hauptsächlich auf die oben genannten Ausfallkombinationen mit dem zusätzlichen Versagen eines der beiden Notstands-Einspeisungen zurückzuführen.

Als bedingte Wahrscheinlichkeit für die Ereignisabläufe $T_1S_2-\eta$ (Freisetzungskategorie 5) erhält man $4 \cdot 10^{-5}$. Bei dieser Freisetzungskategorie führt der CMA der Notstromdiesel allein zum Versagen des Sicherheitsbehälterabschlusses. Unabhängige Ausfälle von zwei Gebäudeabschlußarmaturen spielen dagegen eine geringere Rolle. Die Hauptbeiträge zu $T_1S_2-\eta$ stammen daher von den Ereignisabläufen $T_1S_2'ICE-\eta$ und $T_1S_2''ICE-\eta$ mit je 38 %, deren wesentliche Ausfallkombinationen den CMA der Notstromdiesel enthalten. Dazu kommt dann der Ausfall des ersten Druckhalter-Abblaseventils oder Abblase-Steuerventils bzw. eines der beiden Druckhalter-Abblaseventile oder der zugehörigen Abblase-Steuerventile und Ausfall der kurzfristigen Inbetriebnahme des Notstandssy-

stems. Bei den Ereignisabläufen T_1S_2'IJCE-η und T_1S_2''IJCE-η, die 10 und 13 % zu T_1S_2-η liefern, ist jeweils zusätzlich der Ausfall einer Einspeisung des Notstandssystems relevant.

10. SCHRIFTTUM

/F2, 3-1/ DIN 25 424 (Entwurf):
Fehlerbaumanalyse; Methode und Bildzeichen
Beuth-Verlag, Berlin, November 1974

/F2, 3-2/ DIN 25 424:
Fehlerbaumanalyse; Methode und Bildzeichen
Beuth-Verlag, Berlin, Juni 1977

/F2, 3-3/ DIN 31 051:
Instandhaltung; Begriffe (Blatt 1)
Beuth-Verlag, Berlin, Dezember 1974

/F2, 3-4/ Ergänzung zu DIN 31 051, Teil 10, Vornorm:
Instandhaltung; Begriffe
Beuth-Verlag, Berlin, Oktober 1977

/F2, 3-5/ Koslow, B.A., und J.A. Uschakow:
Handbuch zur Berechnung der Zuverlässigkeit
für Ingenieure
Carl Hanser Verlag, München-Wien, 1979

/F2, 3-6/ DIN 40 041 (Vornorm):
Zuverlässigkeit elektrischer Bauelemente; Begriffe
Beuth-Verlag, Berlin, Oktober 1967

/F2, 3-7/ DIN 40 042 (Vornorm):
Zuverlässigkeit elektrischer Geräte, Anlagen und
Systeme; Begriffe
Beuth-Verlag, Berlin, Juni 1970

/F2, 3-8/ VDI 4008, (Entwurf):
Boolesches Modell; (Blatt 2)
VDI-Verlag, Düsseldorf, März 1972

/F2, 3-9/ Anwendung von Monte-Carlo-Verfahren zur Ermittlung von Zuverlässigkeitsmerkmalen technischer Systeme
Hrsg.: Institut für Luft- und Raumfahrt, TU Berlin
ILR-Bericht 14, 1976

/F2, 3-10/ Camarinopoulos, L.:
Direkte und gewichtete Simulationsmethoden zur Zuverlässigkeitsuntersuchung technischer Systeme
Dissertation D 83, TU Berlin, April 1972

/F2, 3-11/ Schneider, C.:
Fehlerbaumanalyse von periodisch inspizierbaren Systemen mit Hilfe der Monte-Carlo-Methoden
Dissertation am Kernforschungszentrum Karlsruhe,
KfK 2628, 1978

/F2, 3-12/ Dressler, E.:
Theoretische Grundlagen zum Programmsystem SAFTL und CRESS zur Berechnung der Zuverlässigkeit von Systemen
MRR 164, September 1976

/F2, 3-13/ Daugherty, R., und L. Schlösser:
CRESSEX - Beschreibung eines Zuverlässigkeitsrechenprogramms zur Ermittlung wichtiger Kenngrößen von komplexen Systemen. Programmbeschreibung
MRR-P-23, September 1976

/F2, 3-14/ Dressler, E., und H. Lurz:
SAFTL und CRESS - Beschreibung zweier Programmsysteme zur Berechnung der Zuverlässigkeit von komplexen Systemen
MRR-P-21, Dezember 1975

/F2, 3-15/ Richter, G., und G. Memmert:
Berechnung von Zuverlässigkeitsdaten komplexer Systeme mit analytischen Methoden
TUBIK 28, Oktober 1973

/F2, 3-16/ VDI 4008:
Strukturfunktionen und ihre Anwendung
Blatt 7 (in Vorbereitung)
VDI-Verlag, Düsseldorf

/F2, 3-17/ Höfle-Isphording, U.:
Zuverlässigkeitsrechnung - Einführung in ihre Methoden
Springer Verlag, Berlin, Heidelberg, 1978

/F2, 3-18/ Gaede, K.W.:
Zuverlässigkeit, mathematische Modelle
Carl Hanser Verlag, München-Wien, 1977

/F2, 3-19/ Camarinopoulos, L., und E. Richter:
KARI - Ein neues analytisches Programm zur Berechnung von Zuverlässigkeitsmerkmalen technischer Systeme.
Angewandte Informatik 17 (1975) Nr. 12, S. 529/33

/F2, 3-20/ Fussell, J.B., E.B. Henry and N.H. Marshall:
MOCUS - A Computer Program to Obtain Minimal Sets from Fault Trees
ANCR-1156, March 1974

/F2, 3-21/ Schlösser, L.:
Theoretische Grundlagen zum Rechenprogramm STREUSL zur Ermittlung der Streuung in Zuverlässigkeitskenngrößen
GRS-20, Juli 1980

/F2, 3-22/ Schlösser, L.:
STREUSL - Ein Rechenprogramm zur Ermittlung der Streuung in Zuverlässigkeitskenngrößen aufgrund der Streuungen der Eingabedaten. Programmbeschreibung
GRS-19, Juli 1980

/F2, 3-23/ Vesely, W.E., and R.E. Narum:
PREP und KITT: Computer Codes for the Automatic Evaluation of a Fault Tree
IN-1349, August 1970

/F2, 3-24/ Dressler, E., und H. Spindler:
Die Nichtverfügbarkeit von Bereitschaftssystemen in Abhängigkeit von Teststrategie und Reparaturzeit
MRR 144, März 1975

/F2, 3-25/ Dressler, E., und H. Spindler:
Verbesserung der Nichtverfügbarkeit von Sicherheitssystemen durch zeitlich gestaffelte Prüfungen
atw 19 (1974) Nr. 3, S. 133

/F2, 3-26/ Schäfer, J.:
Unsicherheiten der Ausfallraten von Komponenten und der Eintrittswahrscheinlichkeit störfallauslösender Ereignisse
Abschlußbericht des Forschungsvorhabens BMFT-RS-228, Institut für Kerntechnik, TU Berlin, 1978

/F2, 3-27/ Gibbons, J.D.:
Non-Parametric Statistical Inference
McGraw-Hill Book Company, New York, San Francisco, Toronto, 1971

/F2, 3-28/ Heinhold, J., und K.W. Gaede:
Ingenieur-Statistik
R. Oldenbourg Verlag, München-Wien, 1972

/F2, 3-29/ Edwards, G.T., and I.A. Watson:
A Study of Common-Mode Failures
SRD R 146, July 1979

/F2, 3-30/ KTA 3501:
Reaktorschutzsystem und Überwachung von Sicherheitseinrichtungen
C. Heymanns Verlag, Köln, Fassung 3/1977

/F2, 3-31/ Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants WASH-1400 (NUREG-75/014), October 1975

/F2, 3-32/ Working Conditions for Nuclear Power Plant Operators. A Pilot Study. LUTAB-Report TA 875-R1, September 1976

/F2, 3-33/ Swain, A.D., and H.E. Guttmann: Human Reliability Analysis of Dependent Events Proceedings of the ANS Topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety Newport Beach, California, May 8-10, 1978

/F2, 3-34/ Swain, A.D., and H.E. Guttmann: Handbook of Human Reliability Analysis for Nuclear Power Plant Operations Sandia Laboratories, Draft, October 1977

/F2, 3-35/ Anticipated Transients Without Scram for Water-Cooled Power Reactors WASH-1270, September 1973

/F2, 3-36/ HTGR Accident Initiation and Progress Analysis Status Report GA-A13617, October 1975

/F2, 3-37/ Fleming, K.N., and P.H. Raabe: A Comparison of Three Methods for the Quantitative Analysis of Common Cause Failures Proceedings of the ANS-Topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety Newport Beach, California, May 8-10, 1978

/F2, 3-38/ Vesely, W.E.: Estimating Common Cause Failure Probabilities in Reliability and Risk Analyses: Marshall-Olkin Specializations

Proceedings of the International Conference on Nuclear Systems Reliability Engineering and Risk Assessment
Gatlinburg, Tennessee, June 20-24, 1977
edited by J.B. Fussell and G.R. Burdick
Society for Industrial and Applied Mathematics,
Philadelphia, 1977, p. 314/41

/F2, 3-39/ Zur friedlichen Nutzung der Kernenergie. Eine Dokumentation der Bundesregierung
Hrsg.: Der Bundesminister für Forschung und Technologie, 2., unveränderte Auflage, Bonn 1978

/F2, 3-40/ Berwerger, L.:
Stellantriebe mit gesteuerter Reibungskupplung verhindern Schäden - 2. Teil
VDI-Nachrichten Nr. 33 (1979), Nr. 24, S. 29

/F2, 3-41/ Das Reaktorschutzsystem als zentrale Sicherheitseinrichtung in Kernkraftwerken
Tagungsbericht, 8. IRS-Fachgespräch in Köln,
IRS-T-24, April 1973

/F2, 3-42/ Anticipated Transients Without Scram For Light Water Reactors
NUREG-0460, April 1978

/F2, 3-43/ Data Summaries of Licensee Event Reports of Control Rods and Drive Mechanisms at U.S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1978
NUREG/CR-1331 E, GG-EA-5079, February 1980

/F2, 3-44/ Vesely, W.E.:
Summary: WASH-1400 Bounding Approach, BWR Scram Rod Failure Analysis, Scram System Failure Probabilities, Conclusions
Unterlage für "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission" (Levis-Review-Group), Washington, 14.12.1977

/F2, 3-45/ Bohr, E.:
Ein Beitrag zur Wartengestaltung von Kernkraftwerken aus ergonomischer Sicht
VGB Kraftwerkstechnik 54 (1974), Nr.10, S. 657

/F2, 3-46/ Richtlinie für den Fachkundenachweis von Kraftwerkspersonal
Bekanntmachung des BMI vom 17.5.1979, GMBl 1979, S. 233

/F2, 3-47/ Richtlinie für den Inhalt der Fachkundeprüfung des verantwortlichen Schichtpersonals in Kernkraftwerken
Bekanntmachung des BMI vom 10.8.1978, GMBl 1978, S. 431

/F2, 3-48/ Richtlinie für Programme zur Erhaltung der Fachkunde des verantwortlichen Schichtpersonals in Kernkraftwerken
Bekanntmachung des BMI vom 17.5.1979, GMBl 1979, S. 238

/F2, 3-49/ Swain, A.D.:
Séminaire de la modélisation de la fiabilité humaine centrales nucléaire
Institut National des Sciences et Techniques Nucléaires, Saclay, 20-21 Septembre 1979

/F2, 3-50/ Einzelfehlerkonzept - Grundsätze zur Anwendung des Einzelfehlerkriteriums. Interpretation zu den Sicherheitskriterien für Kernkraftwerke
Bekanntmachung des BMI vom 26.10.1978, GMBl 1978, S. 631

/F2, 5-1/ KTA 3401.1:
Reaktorsicherheitsbehälter aus Stahl, Teil: Werkstoffe
Carl Heymanns Verlag, Köln, Fassung 10/79,

/F2, 5-2/ KTA 3401.2:
Reaktorsicherheitsbehälter aus Stahl, Teil: Auslegung, Konstruktion und Berechnung
Carl Heymanns Verlag, Köln, Fassung 10/79,

/F2, 5-3/ KTA 3401.3:
Reaktorsicherheitsbehälter aus Stahl, Teil: Herstellung
Carl Heymanns Verlag, Köln, Fassung 10/79

/F2, 5-4/ KTA 3401.4:
Reaktorsicherheitsbehälter aus Stahl, Teil: Betriebliche Überwachung
Carl Heymanns Verlag, Köln, Fassung 6/79

/F2, 5-5/ KTA 3401.5:
Integrale Leckratenprüfung des Sicherheitsbehälters mit der Absolutdruckmethode
Carl Heymanns Verlag, Köln, Fassung 2/79

/F2, 5-6/ Goßner, S.:
Theoretische Untersuchungen des Ausfallverhaltens eines dynamischen Grenzwertmelders
MRR 143, Februar 1975

/F2, 5-7/ Unfallverhütungsvorschrift, Druckbehälter (VBG 17) vom 1. April 1965, in der Fassung vom 1. April 1974

/F2, 6-1/ Sicherheitstechnisches Forschungsprogramm auf dem Gebiet LWR. Abschlußbericht
Förderungsvorhaben BMFT RS 168; Funktionsversuch zum Schwungradabfall; Kennwort: Schwungradabfall;
KWU-RE 23/014/76, Juni 1976

/F2, 6-2/ Einzelfehlerkonzept - Grundsätze zur Anwendung des Einzelfehlerkriteriums. Interpretationen zu den Sicherheitskriterien für Kernkraftwerke
Bekanntmachung des BMI vom 26.10.1978, GMBl 1978, S. 631

/F2, 6-3/ Otway, H.J., R.K. Lohrding and M.E. Battat:
A Risk Estimate for an Urban-Sited Reactor,
Nuclear Technology 12, (1971) No.2, p. 173

/F2, 6-4/ Green, A.E., and A.J. Bourne:
Safety Assessment with Reference to Automatic
Protective Systems for Nuclear Reactors
ASHB (S) R 117, UKAEA, 1966

/F2, 7-1/ KTA 3701.1:
Übergeordnete Anforderungen an die elektrische
Energieversorgung des Sicherheitssystems in Kern-
kraftwerken, Teil 1: Einblockanlagen
Carl Heymanns Verlag, Köln, Fassung 6/78

/F2, 7-2/ Forschungsprogramm Reaktorsicherheit, Abschlußbe-
richt, Kennwort: ATWS Studie, Teil 1: DWR
Förderungsvorhaben BMFT RS 153,
Kraftwerk Union RE 23/007/78, Reaktortechnik
Erlangen, April 1978

/F2, 7-3/ Ullrich, W., W. Frisch u.a.:
Untersuchungen von Betriebsstörungen bei Versagen
der Reaktorschnellabschaltung (ATWS) und anderer
ausgewählter Sicherheitseinrichtungen
Hrsg.: GRS, Köln
IRS-W-22 (September 1976)
MRR 163 (September 1976)

11. STICHWORTVERZEICHNIS