Gesellschaft für Reaktorsicherheit (GRS) mbH

GRS-Bericht

Programmsystem RALLY – Zur probabilistischen Sicherheitsbeurteilung großer technischer Systeme

Wolfgang Güldner, Heinz Polke, Heinz Spindler und Gerhard Zipf

GRS-44 (März 1982)

Glockengasse 2 · 5000 Köln 1 · Telefon (02 21) 20 68–1 · Telex 8 881 807 grs d

Anmerkung:

Dieser Bericht ist von der GRS im Auftrag des Bundesministers des Innern erstellt worden. Er ist inhaltsgleich mit dem Auftragsbericht GRS-A-639 (September 1981). Die darin enthaltenen Arbeitsergebnisse müssen nicht mit der Auffassung des Auftraggebers übereinstimmen.

Vorwort

Im Rahmen des Vorhabens SR 122, A.1.1, wurde von der Gesellschaft für Reaktorsicherheit das Programmsystem RALLY (GE 81, GE 80) zur Berechnung von Zuverlässigkeitskenngrößen großer und vermaschter technischer Systeme entwickelt.

Während die wichtigsten der einzelnen Programme des Programmsystems GRS-intern bereits ausführlich dokumentiert sind, soll in diesem Bericht eine zusammenfassende Darstellung der Aufgaben und der Möglichkeiten des gesamten Programmsystems erfolgen. Vor allem die Anwendbarkeit der Programme für die probabilistische Sicherheitsbeurteilung kerntechnischer Anlagen soll dargestellt werden.

Dieser Bericht gliedert sich in drei Teile. Nach einem Überblick über die einzelnen Programme des Programmsystems werden die Anwendungsmöglichkeiten von RALLY

- in wissenschaftlichen Untersuchungen,
- in Genehmigungsverfahren kerntechnischer Einrichtungen,
- bei der Aufsicht über kerntechnische Einrichtungen und
- im Rahmen allgemeiner administrativer Überprüfungen

diskutiert. Nach der Beschreibung der Möglichkeiten, die RALLY bietet, erfolgt abschließend ein Kapitel über die mit RALLY bereits durchgeführten Analysen im Genehmigungsverfahren und bei Risikostudien.

Kurzfassung

Dieser Bericht beschreibt das Programmsystem RALLY zur Berechnung von Zuverlässigkeitskenngrößen großer und vermaschter Systeme. Neben einer kurzen Erläuterung der einzelnen Programme werden die Anwendungsmöglichkeiten des Programmsystems aufgezeigt und die wichtigsten der mit RALLY bereits durchgeführten Analysen diskutiert.

Abstract

This report describes the program system RALLY to compute the reliability of large and intermeshed technical systems. In addition to a short explanation of the different programs, the possible applications of the program system RALLY are demonstrated. Finally, the most important studies carried out so far on RALLY are discussed.

INHALT

Seite

BILDER

1. EINLEITUNG

Zur Beurteilung der Sicherheit von Kernkraftwerken und in neuester Zeit auch für andere großtechnische Anlagen werden - wegen der oft weitreichenden Folgen eines Störfalls - immer häufiger Zuverlässigkeitsanalysen benötigt. Damit lassen sich umfassende Informationen über das Zustandekommen von Systemausfällen gewinnen. Quantitative Ergebnisse dieser Analysen sind für Systeme, die bei Anforderung funktionieren müssen, die mittlere Nichtverfügbarkeit $M_s(t)$ und für Betriebssysteme die Ausfallwahrscheinlichkeit $Q_s(t)$ bzw. Ausfallhäufigkeit $H_s(t)$. Neben dieser rein quantitativen Bewertung ist die Schwachstellen- und Sensitivitätsanalyse eines Systems eine weitere wichtige Aufgabe von Zuverlässigkeitsuntersuchungen.

Da für die verschiedenartigen Systeme meist statistische Daten aus der Betriebserfahrung zur Beschreibung der Zuverlässigkeit fehlen, für Komponenten aber vorhanden sind, kann unter Berücksichtigung der systemtechnischen Verknüpfung der Komponenten die Zuverlässigkeit des Systems ermittelt werden. Die Systeme müssen dazu so weit unterteilt werden, daß aus den Daten der Betriebserfahrung über das Ausfallverhalten der Untersysteme bzw. Komponenten auf das Systemverhalten hochgerechnet werden kann. Diese Unterteilung führt allerdings zu großen und vermaschten Systemdarstellungen, die mittels Fehlerbäumen beschrieben werden können. Ein Fehlerbaum ist dabei die graphische Darstellung der logischen Zusammenhänge der verschiedenen Komponenten und Untersysteme in bezug auf einen vorgegebenen, meist unerwünschten Ausgangszustand, wie z.B. ein ausgefallenes System (siehe Abschnitt 3.1).

Die quantitative Auswertung der Fehlerbäume, eine Schwachstellenanalyse und die Berechnung der verschiedenen Zuverlässigkeitskenngrößen sind bei großen Systemen nur mit EDV-Anlagen möglich. Zu diesem Zweck wurde von der GRS das Programmsystem RALLY entwickelt.

2. BESCHREIBUNG DER EINZELNEN PROGRAMME DES PROGRAMMSYSTEMS RALLY

Nach einer kurzen Beschreibung des Gesamtsystems von RALLY erfolgt in diesem Kapitel eine Diskussion der einzelnen Programme des Programmsystems. Anwendungsmöglichkeiten und Algorithmen werden kurz aufgezeigt. Bild 1 zeigt einen Überblick über RALLY und veranschaulicht den Datenfluß zwischen den verschiedenen Programmen.

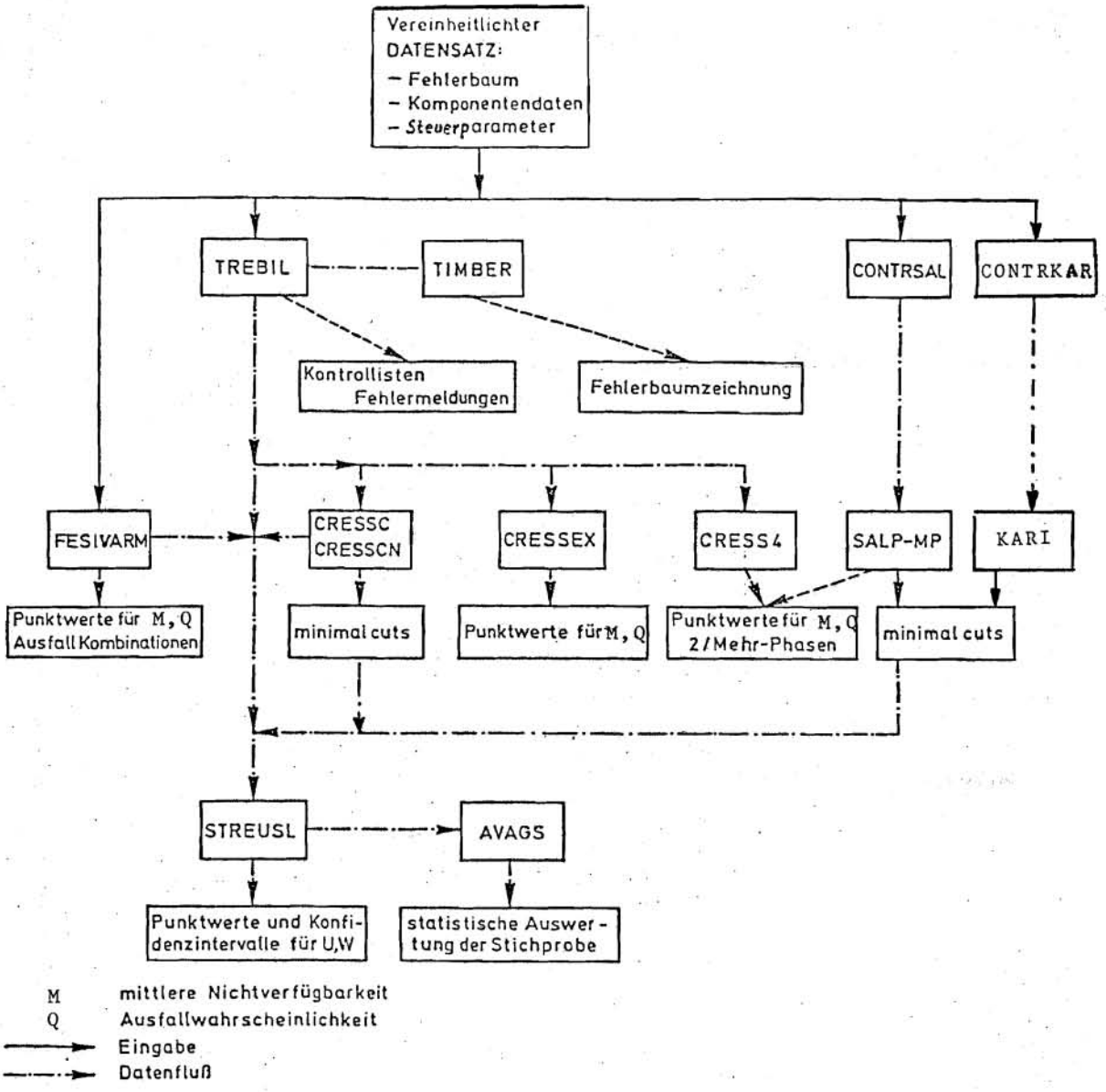

Bild 1:
Schematische Darstellung des Programmsystems RALLY

Für das gesamte Programmsystem ist nur ein leicht zu erstellender Datensatz erforderlich. Die Informationen für die verschiedenen Programme werden automatisch selektiert und aufbereitet, d.h., ein Eingreifen des Anwenders im weiteren Programmablauf ist nicht erforderlich.

Basis dieses Systems ist das Daten- und Fehlerbaumaufbereitungsprogramm TREBIL. Wesentlichste Aufgabe von TREBIL ist neben der Überprüfung der Eingabedaten die Umsetzung der Fehlerbaumlogik in ein Boolesches Gleichungssystem sowie die Erstellung der Datensätze für die Nachfolgeprogramme.

Die nachgeschalteten Programme lassen sich hinsichtlich der methodischen Behandlung der Zuverlässigkeitsanalyse in zwei Klassen einteilen.

- Direkte Simulation

Bei den Simulationsprogrammen nach der Monte-Carlo-Methode wird das Ausfallverhalten der Komponenten (und damit des Systems) mit Hilfe von Zufallszahlengeneratoren simuliert. Bei der Simulation können mit geringem mathematischen Aufwand auch sehr große und vermaschte Systeme analysiert werden. Folgeausfälle, Ausfälle gemeinsamer Ursachen (Common-Mode-Ausfälle = CMA), Berücksichtigung von kalten Reserven, Funktionsprüfungen und Instandsetzungen können verhältnismäßig einfach berücksichtigt werden. Der Nachteil von Simulationsprogrammen ist die enorme Zunahme der Rechenzeit bei der Analyse sehr zuverlässiger Systeme, da die Genauigkeit der Ergebnisse abhängig ist von der Anzahl der simulierten Ausfälle. Durch den Einsatz varianzreduzierender Methoden können in manchen Fällen auch noch Systeme mit hoher Zuverlässigkeit durch Simulation berechnet werden. Varianzreduzierende Methoden erfordern aber vom Anwender eine genaue Kenntnis des verwendeten Verfahrens.

- Weg über die minimalen Schnittmengen

Neben der Monte-Carlo-Simulation hat sich zur Ermittlung von Zuverlässigkeitskenngrößen großer vermaschter Systeme der Weg über die minimalen Schnittmengen (auch Minimalschnitte oder "minimal cut" genannt) bewährt. Eine minimale Schnittmenge ist dabei eine minimale Kombination von Komponenten, deren Ausfall zum Systemausfall führt. Die Methode der Minimalschnitte gliedert sich in zwei Schritte:

- das Auffinden der Minimalschnitte einer gegebenen Struktur (Fehlerbaum) sowie
- die anschließende Berechnung der Zuverlässigkeitskenngrößen des Systems mit Hilfe dieser Schnittmengen.

Sind C_1, C_2,...C_n die minimalen Schnittmengen einer Systemfunktion, so gilt z.B. für die mittlere Nichtverfügbarkeit $M_s(t)$ des Systems

$$M_s(t) = \frac{1}{t} \int_0^t U_s(t')dt' = \frac{1}{t} \int_0^t \sum_{i=1}^{n} U_{C_i}(t')dt'$$

$$\text{mit } U_{C_i}(t) = \prod_{j \in C_i} U_j(t)$$

wobei $U_s(t)$ (d.h. $U_{C_i}(t)$; $U_j(t)$) die Nichtverfügbarkeit des Systems (d.h. der minimalen Schnittmenge C_i; der Komponente j) zur Zeit t bezeichnet. Ebenfalls mit Hilfe der minimalen Schnittmengen läßt sich auch die Ausfallhäufigkeit des Systems berechnen.

Im Gegensatz zur Monte-Carlo-Simulation spielt bei der Methode der Minimalschnitte der Wert der Systemzuverlässigkeit hinsichtlich der erzielbaren Genauigkeit der Ergebnisse keine Rolle. Der Nachteil dieser Methode ist, daß spezielle Teststrategien, Common-Mode-Ausfälle oder kalte Redundanzen oft nur vereinfacht berücksichtigt werden können. Ferner können bei großen Systemen auch Schwierigkeiten bei der Ermittlung der wichtigsten minimalen Schnittmengen auftreten, denn große Systeme be-

sitzen oft mehrere Millionen minimaler Schnittmengen. In der Regel bestimmen jedoch 1000-2000 Minimalschnitte das Ergebnis.

Im Programmsystem RALLY können die wesentlichen minimalen Schnittmengen berechnet werden

- simulativ mit den Programmen CRESSC und CRESSCN,
- analytisch, durch Auflösen der Booleschen Struktur des Fehlerbaums, mit den Programmen SALP-MP und KARI.

Um zusätzlich die Streuung der Komponentendaten, die sich bei der Auswertung der Betriebserfahrung ergibt, berücksichtigen zu können, wurde das simulativ-analytische Programm STREUSL geschaffen.

Die Berechnung für Mehrphasensysteme, denen für jede Phase ein eigener Fehlerbaum zugrunde liegt, ist mit den Programmen CRESS4 und SALP-MP möglich.

Im folgenden sollen die einzelnen Programme ausführlicher beschrieben werden.

2.1 Fehlerbaum-Aufbereitungsprogramm TREBIL

TREBIL benötigt als Eingabe Informationen über die logische Struktur des zu untersuchenden Systems sowie quantitative Angaben (Ausfallrate, Testintervall usw.) über die Systemkomponenten. Mittels dieser Information werden Kontrollisten angelegt, die die Überprüfung des Fehlerbaums erleichtern. Weiterhin wird der Fehlerbaum, soweit möglich, auf Korrektheit untersucht und eventuell Fehlermeldungen ausgedruckt. Wesentlichste Aufgabe von TREBIL ist jedoch eine Fehlerbaumoptimierung sowie eine spezifische Datenaufbereitung für die anderen Programme des Programmsystems. Dazu werden unter anderem die einzelnen logischen Verknüpfungen der eingegebenen Fehlerbäume in Boolesche Ausdrücke umgewandelt und für die Simulationsprogramme (wie z.B. CRESSEX) zu einer Booleschen Subroutine zusammengefaßt.

2.2 Fehlerbaum-Plotprogramm TIMBER

Das Plotprogramm TIMBER dient zur Dokumentation und ermöglicht dem Anwender die optische Überprüfung des eingegebenen Fehlerbaums. Die Zeichnung eines Fehlerbaums ist abhängig von der Eingabe der Komponenten- und Gatterreihenfolge, da TIMBER die logische Struktur eines Fehlerbaums nicht optimiert. Auf eine Optimierung wurde absichtlich verzichtet, da bei komplexen Fehlerbäumen eine Überprüfung der Eingabe nach einer Fehlerbaumoptimierung nur noch schwer möglich ist. Durch Steuerparameter können für die Komponenten wahlweise Kommentare oder Zuverlässigkeitskenngrößen in die Kommentarkästen eingeschoben werden. Bild 2 zeigt den Plot eines Fehlerbaumes durch das Programm TIMBER.

2.3 Fehlerbaum-Rechenprogramm CRESSEX

Das Simulationsprogramm CRESSEX ermöglicht die Berechnung der Ausfallwahrscheinlichkeit und mittleren Nichtverfügbarkeit für komplexe technische Systeme. 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),
- Ausfallverhalten der Komponentenfunktionen, die entweder durch eine konstante Ausfallrate oder durch eine konstante Ausfallwahrscheinlichkeit pro Anforderung beschrieben werden,
- Erkennungszeitpunkt eines Komponentenausfalls (selbstmeldender, d.h. sofort erkannter Ausfall oder erst bei der Funktionsprüfung erkannter Ausfall) und
- konstante Instandsetzungszeiten der Komponenten.

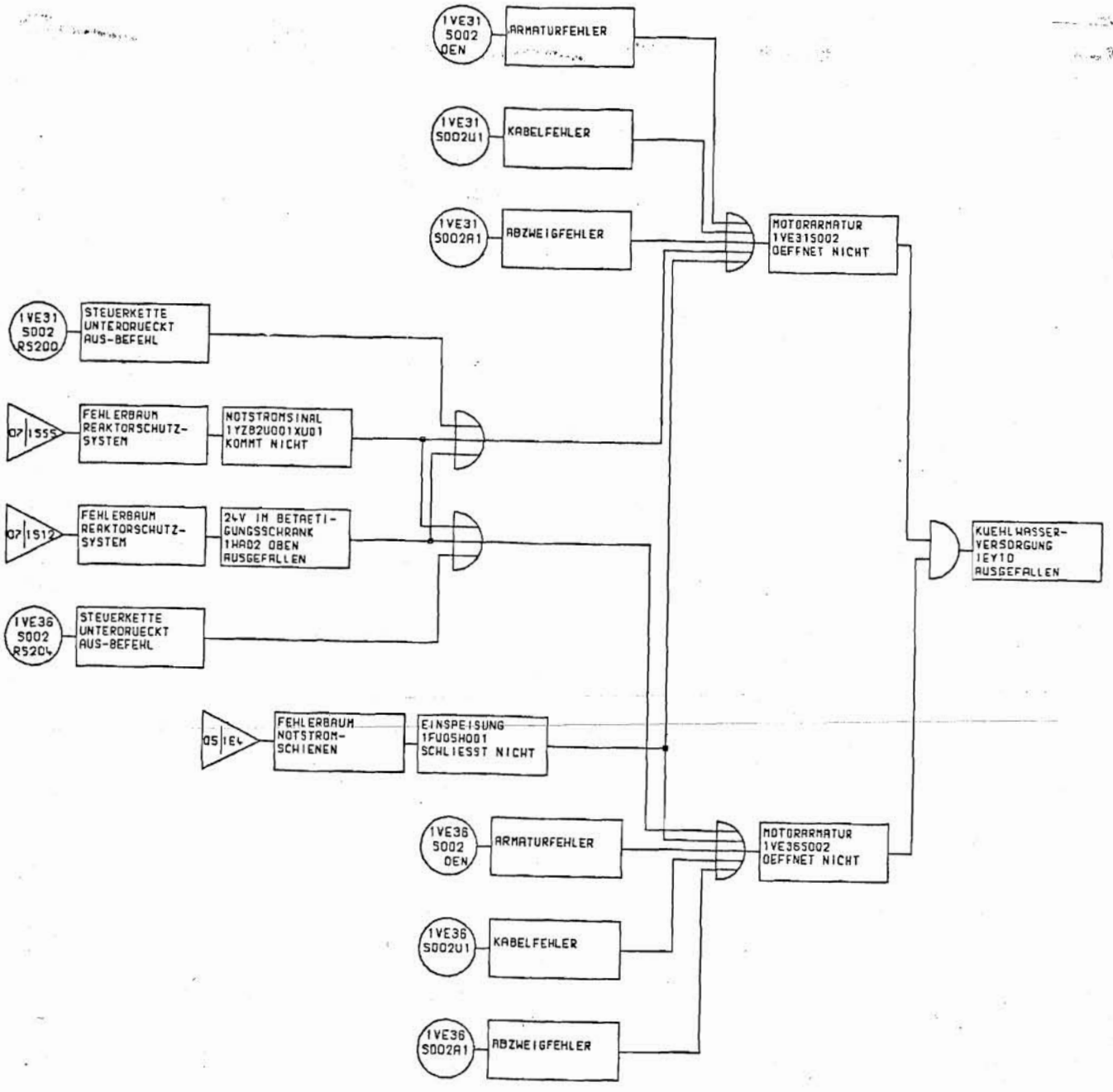

Bild 2:
Plot eines Fehlerbaumes mit dem Programm TIMBER

Der Simulationsvorgang wird sehr oft wiederholt. Die in den einzelnen Spielen vom Zufall abhängigen Zwischenergebnisse, wie z.B. Eintreten eines Systemausfalls, Ausfalldauer der Systemfunktion, am Ausfall beteiligte Komponenten, werden gespeichert und am Ende der Rechnung statistisch ausgewertet. Berechnet werden die Schätzwerte der Ausfallwahrscheinlichkeit

$Q_s(t)$, der Ausfallhäufigkeit $H_s(t)$ und der mittleren Nichtverfügbarkeit $M_s(t)$ sowie deren Varianzen (Varianz in Abhängigkeit von der Anzahl der Spiele bzw. simulierter Totzeiten).

$$H_s(t) = \frac{\text{Anzahl der Systemausfälle in } [0,t]}{\text{Anzahl der Spiele}}$$

$$Q_s(t) = \frac{\text{Anzahl der Systemerstausfälle in } [0,t]}{\text{Anzahl der Spiele}}$$

$$M_s(t) = \frac{\text{Summe der Systemausfalldauer}}{\text{Anzahl der Spiele} \cdot t}$$

$t \hat{=}$ Betrachtungszeitraum

Darüber hinaus werden in CRESSEX noch zusätzlich die Komponenten nach der Anzahl der Ausfälle und deren Beitrag zur mittleren Nichtverfügbarkeit angeordnet und die bei der Simulation aufgetretenen minimalen Schnittmengen ausgegeben. Diese Informationen können dann zur Schwachstellenanalyse herangezogen werden.

Gleichzeitig lassen sich auch Zuverlässigkeitskenngrößen für ausgewählte Untersysteme berechnen, um somit deren Beitrag zu den Systemkenngrößen abschätzen zu können.

2.4 Fehlerbaum-Rechenprogramm FESIVARM

Das Programm FESIVARM bestimmt die Ausfallwahrscheinlichkeit und mittlere Nichtverfügbarkeit auf simulative Art mit "importance sampling". Durch Eingabe eines Wichtungsfaktors läßt sich die Anzahl der Ausfälle erhöhen, was zu einer Reduzierung der Rechenzeit bei vorgegebener gewünschter Genauigkeit führt. Auf diese Weise können meist auch noch sehr zuverlässige Systeme simulativ behandelt werden. Darüber hinaus ermöglicht das Programm, anhand der Ausfallkombinationen des Systems eine Schwachstellen- und Sensitivitätstabelle zu erstellen. Die weiteren Eigenschaften sind ähnlich denen des Programms CRESSEX.

Bedingt durch eine andersartige Behandlung der logischen Struktur des Fehlerbaumes sind jedoch die Verknüpfungsmöglichkeiten erweitert. So lassen sich auch NOT- oder RESERVE-Verknüpfungen mit kalten oder warmen Standby-Komponenten und nicht-perfektem Umschalter behandeln.

2.5 Programme zur simulativen Ermittlung von minimalen Schnittmengen - CRESSC, CRESSCN

- Programm CRESSC

Das Programm CRESSC ermittelt auf simulativer Basis für das Programm STREUSL die wichtigsten minimalen Schnittmengen eines Systems.

Analog 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 Berücksichtigung von Ausfallzeitpunkt, Ausfalldauer usw. verzichtet werden, was im Vergleich zu CRESSEX zu einer wesentlichen Verkürzung der Rechenzeit führt. Ferner wird, um bei der Simulation genügend Systemausfälle zu erhalten, der Betrachtungszeitraum vom Programm so gesteuert, daß ungefähr bei jedem zweiten Spiel ein Systemausfall auftritt. Die Auswertung der minimalen Schnittmengen erfolgt durch Integration im Programm STREUSL.

- Programm CRESSCN

Das Programm CRESSCN dient zur Ermittlung minimaler Schnittmengen von Systemfunktionen, die NOT-Verknüpfungen enthalten. Der Algorithmus entspricht CRESSC, nur müssen minimale Schnittmengen, die unvereinbare Ereignisse enthalten, eliminiert werden.

2.6 Programm zur analytischen Ermittlung von minimalen Schnittmengen - SALP-MP

Das analytische Programm SALP-MP (As et al. 80) wurde von JRC ISPRA übernommen. In diesem Programm werden alle minimalen Schnittmengen ermittelt, deren Beitrag zur Nichtverfügbarkeit größer als eine frei wählbare Schranke ist. Das dabei verwendete Verfahren gestattet es darüber hinaus, Fehlerabschätzungen über die nichtberücksichtigten minimalen Schnittmengen zu machen. Die Einbeziehung des vollständigen Satzes der minimalen Schnittmengen ist somit nur eine Frage der Rechenzeit.

Das Programm berechnet die Zuverlässigkeitskenngrößen für den Betrachtungszeitraum und für interessierende Zwischenzeiten und gibt die Ergebnisse geordnet nach Beiträgen zur Nichtverfügbarkeit aus.

SALP-MP erlaubt auch die Behandlung von Mehr-Phasen-Systemen. Darunter sind Systeme zu verstehen, deren Konfiguration, d.h. in diesem Fall deren Fehlerbäume sich während aufeinanderfolgender festgelegter Zeitpunkte ändern. Hier interessiert vor allem die Ausfallwahrscheinlichkeit, jedoch wird wie im einphasigen Fall auch die Nichtverfügbarkeit für alle angegebenen Zeitpunkte berechnet und für alle Phasen ausgegeben.

Zur Verwendung des Programms SALP-MP muß das Programm CONTRSAL vorgeschaltet werden. Seine wesentlichste Aufgabe ist es, aus einer speziellen Ausgabe von TREBIL eine für SALP-MP geeignete Datenstruktur zu erzeugen.

2.7 Programm zur analytischen Ermittlung von minimalen Schnittmengen - KARI

Analog dem Programm SALP-MP werden im Programm KARI (Ca, Ri 75) alle minimalen Schnittmengen ermittelt, deren Beitrag zur Nichtverfügbarkeit (bzw. Ausfallhäufigkeit) größer als eine frei wählbare Schranke ε ist. Wie im Programm SALP-MP

kann der Fehler, der durch das Abschneiden von minimalen Schnittmengen entsteht, konservativ abgeschätzt werden. Beide Programme (KARI und SALP-MP) unterscheiden sich im wesentlichen in der Art der Fehlerbaumbehandlung zur Bestimmung der Minimalschnitte. Der im Programm KARI implementierte Algorithmus ist in (Ca, Ri 75) beschrieben.

2.8 Programm CRESS4 (Zweiphasen-Rechenprogramm)

Das Zweiphasenprogramm CRESS4 berechnet die Ausfallwahrscheinlichkeit eines Systems, das nach Anforderung (Standby-Phase) über einen vorgegebenen Zeitraum seine Funktion aufrechterhalten muß (Langzeitphase). Die beiden Phasen können durch unterschiedliche Fehlerbäume (z.B. geänderte Wirksamkeitsbedingungen) und durch unterschiedliche Ausfalldaten (z.B. Startversagen bei Anforderung und Betriebsversagen in der Durchhaltephase) beschrieben werden. Falls gleiche Komponenten in beiden Phasen wirksam sind, werden deren simulierte Ausfälle in der ersten Phase (Ermittlung der Systemnichtverfügbarkeit) mit in die zweite Phase übernommen.

2.9 Streubreiten-Rechenprogramm STREUSL

Die bisher aufgezählten Programme berechnen nur Punktwerte der Zuverlässigkeitskenngrößen, d.h., statistische Unsicherheiten bzw. Streuungen in den Eingabedaten werden nicht berücksichtigt. Bei der Bestimmung repräsentativer Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung treten jedoch Unsicherheiten auf, die man mittels Verteilungsfunktionen (meist logarithmische Normalverteilungen) beschreibt.

Im Programm STREUSL werden die Erwartungswerte, Verteilungen und Vertrauensbereiche für die Nichtverfügbarkeit bzw. Ausfallwahrscheinlichkeit der betrachteten Systemfunktion in Abhängigkeit von den Verteilungen der Eingangsparameter (Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung) berechnet.

Dabei können folgende Verteilungen behandelt werden: Normal- und logarithmische Normal-, Uniform- und logarithmische Uniform-, Beta- und χ^2-Verteilung.

Die Berechnung der mittleren Nichtverfügbarkeit bzw. Ausfallhäufigkeit des Systems in Abhängigkeit der Verteilungen für die Eingabedaten erfolgt im Programm STREUSL in einem simulativen und einem analytischen Teil. Im simulativen Teil wird aufgrund der Verteilungen der Parameter eine Kombination von Werten für die Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung der Funktionselemente ausgespielt. Mittels dieser Kombination wird dann die Nichtverfügbarkeit bzw. Ausfallhäufigkeit der untersuchten Systemfunktion analytisch berechnet. Grundlage für die analytische Berechnung des Systems sind die minimalen Schnittmengen.

Dieser Vorgang - Ausspielen der Zufallszahlen und Berechnung der Zuverlässigkeitskenngrößen, auch Spiel genannt -, kann nun oft wiederholt werden. Auf dieses Weise erhält man in STREUSL eine Stichprobe (der Probenumfang sollte ≥ 200 sein) von mittleren Nichtverfügbarkeiten bzw. Ausfallhäufigkeiten, die dann im letzten Abschnitt des Programms mittels verschiedener statistischer Methoden ausgewertet werden, und zwar

- Berechnung von Median, Erwartungswert und Streuung der Verteilung und Ermittlung der Dichtefunktion,
- Auswertung mittels "order statistics" (Vertrauensintervalle für vorgegebene Fraktilen) und
- Auswertung mittels approximierender Verteilungsfunktionen (AVAGS).

Zur Untersuchung von Common-Mode-Ausfällen bietet STREUSL noch die Möglichkeit der Ausfallraten-Kopplung. Dabei kann für die redundanten Komponentenfunktionen das Ausfallverhalten gekoppelt werden, d.h., pro Spiel wird für die gekoppelten Komponenten nur eine Zufallszahl für die Ausfallrate bzw. Ausfallwahrscheinlichkeit pro Anforderung ausgespielt.

2.10 Programm AVAGS zur Approximation einer gegebenen Stichprobe durch verschiedene Verteilungen

Das Programm AVAGS erlaubt die Approximation einer gegebenen Stichprobe durch verschiedene Verteilungen (Normal-, Lognormal-, Johnson-SL-, Beta-, χ^2-, Weibull-, Extrem-1-, Gamma- und Exponentialverteilung). Zusätzlich werden die Momente (Erwartungswert, Streuung, Schiefe, Exzeß) und das Histogramm der Stichprobe berechnet. Entwickelt wurde AVAGS für das Streubreiten-Rechenprogramm STREUSL zur Auswertung der Stichprobe von mittleren Nichtverfügbarkeiten oder Ausfallhäufigkeiten (Bild 3).

Ferner bietet AVAGS die Möglichkeit, Komponentendaten aus der Literatur oder der Betriebserfahrung statistisch auszuwerten. Diese Ergebnisse können dann als Eingabedaten für die anderen Programme von RALLY verwendet werden.

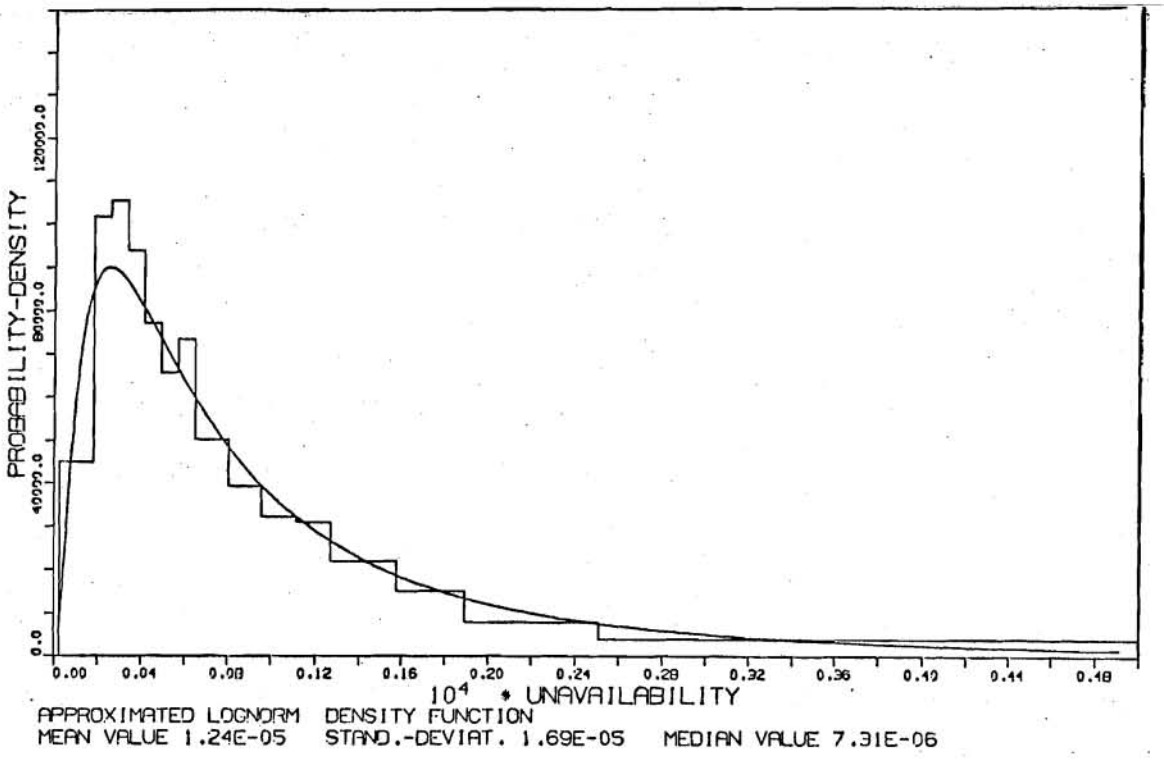

Bild 3:

Plot der Bestapproximation einer Stichprobe, erzeugt durch das Programm AVAGS

3. ZWECK UND ANWENDUNGSMÖGLICHKEITEN DES PROGRAMMSYSTEMS RALLY

Nach Vorstellung der einzelnen Programme des Programmsystems RALLY sollen in diesem Kapitel Zweck und Anwendungsmöglichkeiten des Programmsystem ausführlich diskutiert werden. Da RALLY vor allem zur Berechnung von Fehlerbaum- und Ereignisablaufanalysen konzipiert wurde, folgt zuerst ein Abschnitt zu diesem Themenkreis.

3.1 Ereignisablauf- und Fehlerbaumanalyse

In der Ereignisablaufanalyse werden, ausgehend von einem definierten auslösenden Ereignis (z.B. Bruch einer Hauptkühlmittelleitung) über den Erfolg oder das Versagen dann notwendiger Gegenmaßnahmen (Systemfunktionen), die verschiedenen möglichen Auswirkungen dieses Ereignisses erfaßt. Je nach Umfang der erforderlichen Gegenmaßnahmen ergibt sich somit eine unterschiedliche Zahl möglicher Ereignisabläufe, die in sogenannten Ereignisablaufdiagrammen zusammengefaßt werden.

Als auslösendes Ereignis wird in Bild 4 ein Leck in einer Hauptkühlmittelleitung angenommen. Dies führt zur Reaktorschnellabschaltung, die vom Reaktorschutzsystem ausgelöst wird. Abhängig vom Erfolg oder Versagen dieser Sicherheitsmaßnahme ergeben sich zwei Ereignisabläufe. Im weiteren Verlauf greifen die Systeme zur Notkühlung und Nachwärmeabfuhr automatisch ein, so daß weitere Verzweigungspunkte entstehen. Im obigen Beispiel sind also acht verschiedene Ereignisabläufe zu untersuchen.

Nach Erstellung der Ereignisablaufdiagramme erfolgt die quantitative Bewertung durch Ermittlung der Eintrittshäufigkeit des auslösenden Ereignisses sowie der Wahrscheinlichkeit für das Versagen der benötigten Systemfunktionen mit Hilfe von RALLY. Eventuelle Abhängigkeiten zwischen den einzelnen Systemen müssen dabei berücksichtigt werden.

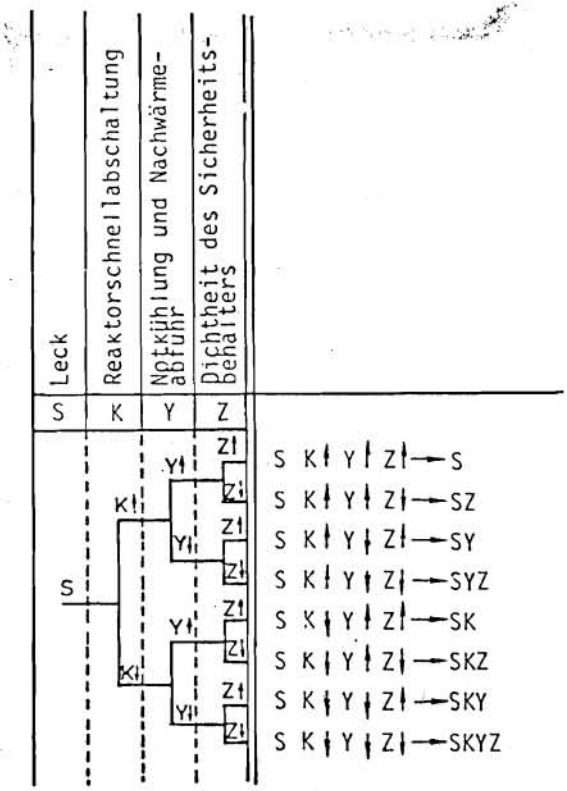

Bild 4:

Vereinfachtes Ereignisablauf-diagramm für einen Kühlmit-telverluststörfall

Zur Auflösung der erläuterten Ereignisabläufe bis auf Komponentenebene verwendet man meist die Fehlerbaumanalyse. Ausgangspunkt dieser Methode ist die Definition des zu untersuchenden (meist unerwünschten) Systemzustands (z.B. Ausfall der Notkühlung und Nachwärmeabfuhr). Ausgehend von diesem "TOP-Ereignis" werden systematisch alle Ereigniskombinationen ermittelt, die zum unerwünschten Ereignis führen (siehe Bild 2). Die Beschreibung dieser Kombinationen erfolgt durch eine graphische Darstellung, den Fehlerbaum, wobei die Ereignisse durch die Operanden UND, ODER und NICHT verknüpft werden.

Bei der Verknüpfung zwischen Ereignisablauf- und Fehlerbaummethode müssen, wie schon erwähnt, Abhängigkeiten zwischen dem auslösenden Ereignis und/oder den verschiedenen störfallbeherr-

schenden Systemen mitberücksichtigt werden. Nur bei statistischer Unabhängigkeit der einzelnen Systeme kann die Eintrittshäufigkeit eines Ereignisablaufpfades einfach durch Multiplikation der entsprechenden Wahrscheinlichkeiten ermittelt werden. Bei Abhängigkeit im Ausfallgeschehen muß der gesamte Ereignisablaufpfad, oft einschließlich des auslösenden Ereignisses, berechnet werden. Dies bedeutet, daß z.B. in Bild 4 bei Abhängigkeiten nicht die Ereignisse S, K, Y und Z getrennt gerechnet werden können, sondern für jeden Ereignisablaufpfad ein eigener Fehlerbaum aufgestellt werden muß.

3.2 Risiko- und Zuverlässigkeitsanalysen

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.

Das übergeordnete Ziel von Zuverlässigkeitsanalysen ist die quantitative Bewertung der Güte eines technischen Systems. Dabei 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, welcher Ausfall der 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.

Zur Beschreibung der oben angesprochenen Güte eines technischen Systems wird bei Systemen, die bei Anforderung funktionieren müssen, die mittlere Nichtverfügbarkeit $M_s(t)$ und für Betriebssysteme die Ausfallhäufigkeit $H_s(t)$ bzw. Ausfallwahrscheinlichkeit $Q_s(t)$ verwendet. Ist der Zeitpunkt der Anforderung eines Systems gleichverteilt im Intervall [0,t], so ist die mittlere Nichtverfügbarkeit gleich der Wahrscheinlichkeit, daß das System bei Anforderung versagt. Während die Ausfallhäufigkeit die zu erwartende Anzahl von Ausfällen im Intervall [0,t] angibt und eventuell auch größer 1 sein kann, ist die Ausfallwahrscheinlichkeit $Q_s(t)$ gleich der Wahrscheinlichkeit, daß das System im Intervall [0,t] mindestens einmal ausfällt, d.h. $Q_s(t) \leqq 1$.

Punktwerte für diese Zuverlässigkeitskenngröße können simulativ mit den Programmen CRESSEX oder FESIVARM oder analytisch mit dem Programm STREUSL ermittelt werden. Mit FESIVARM können durch die Möglichkeit des "importance sampling" auch noch sehr zuverlässige Systeme simulativ berechnet werden. Interessiert die Verteilung von $M_s(t)$ oder $H_s(t)$ in Abhängigkeit von den Verteilungen der Eingabedaten (Ausfallraten, Ausfallwahrscheinlichkeit pro Anforderung), so kann das Programm STREUSL verwendet werden.

Neben dieser rein quantitativen Bedeutung ist die Schwachstellenanalyse eines Systems eine weitere wichtige Aufgabe von Zuverlässigkeitsuntersuchungen. So können anhand des Ausdrucks der Programme CRESSEX und FESIVARM die Komponenten identifiziert werden, die den größten Beitrag zur mittleren Nichtverfügbarkeit bzw. Ausfallhäufigkeit und damit den größten Risikobeitrag liefern. Auch die minimalen Schnittmengen (kritische Mengen), erzeugt von den Programmen CRESSC, CRESSCN, SALP-MP oder KARI, geben eine gute Möglichkeit zur Schwachstellenanaly-

se. Ordnet man die minimalen Schnittmengen eines Systems gemäß ihren Beiträgen zur mittleren Nichtverfügbarkeit bzw. Ausfallhäufigkeit des Systems, so können die wichtigsten kritischen Mengen (Schwachstellen) erkannt werden. Durch Systemänderung oder Verbesserung der Komponente einer solchen wesentlichen kritischen Menge kann das System oft entscheidend verbessert werden (zur Behandlung von Common-Mode-Ausfällen, Ausfallratenkopplung siehe Abschnitt 3.10).

3.3 Genehmigungsverfahren

Nach den Sicherheitskriterien für Kernkraftwerke des BMI, den Leitlinien für Druckwasserreaktoren der RSK und nach den Weisungsbeschlüssen der TÜV-Leitstelle Kerntechnik sind im Genehmigungsverfahren für bestimmte Systeme Zuverlässigkeitsuntersuchungen erforderlich (siehe Abschnitt 4.2). Vor allem die Ausgewogenheit der Systeme ist nachzuweisen, d.h., dominierende Schwachstellen sollen erkannt und beseitigt werden.

Eine wesentliche Hilfe, solche Schwachstellen zu erkennen, bietet das Programmsystem RALLY. So können z.B. Fehlerbäume mit dem Programm TIMBER (siehe Bild 2) sehr übersichtlich geplottet werden. Anhand dieser Zeichnungen können schon oft kritische Pfade, die zum TOP (unerwünschtes Ereignis) führen, erkannt werden. Neben der rein optischen Kontrolle des Systems kann mit den im vorigen Abschnitt bereits erwähnten Programmen eine Schwachstellenanalyse des untersuchten Systems durchgeführt werden. Auch können anhand der Ergebnisse der einzelnen Programme Abschalt- und Teststrategien bei Komponenten und Systemen bestimmt werden (siehe Abschnitt 3.4).

3.4 Vergleich von Systemen

Für die Auslegung (Aufbau) eines Systems kann meist zwischen verschiedenen Möglichkeiten gewählt werden. So wird z.B. ein redundantes System entweder strangweise aufgebaut, wobei die

einzelnen Stränge voneinander unabhängig sind, oder es können, mit dem Ziel die Zuverlässigkeit des Systems zu erhöhen, zwischen den einzelnen Strängen Vermaschungen vorgesehen sein. Zum Vergleich solcher verschiedener Aufbaumöglichkeiten von Systemen kann das Programmsystem RALLY verwendet werden. Mit RALLY ist es möglich, Zuverlässigkeitskenngrößen verschiedener Entwürfe zu bewerten und zu vergleichen. Dabei können auch Schwachstellen gefunden werden. Gerade die Problematik zwischen vermaschten und entmaschten Systemen ist bei größeren Systemen ohne EDV-Programme meist kaum zu entscheiden.

Auch die Auswirkung verschiedener Teststrategien auf die Ausfallwahrscheinlichkeit oder mittlere Nichtverfügbarkeit kann mittels RALLY beurteilt werden. Die Ergebnisse können dann z.B. bei Standby-Systemen zu Entscheidungen herangezogen werden, in welchen Zeitabständen bestimmte Komponenten zu testen sind oder welche Funktionsausfälle eventuell selbstmeldend auszuführen sind.

3.5 Berechnung von Importanzkenngrößen

Die Zuverlässigkeitsmerkmale eines Systems werden im allgemeinen durch die Komponenten unterschiedlich stark beeinflußt.

Allein durch ihre Anordnung in einem gegebenen System sind in der Regel einige Komponenten wichtiger im Hinblick auf ihr Funktionieren als andere. So ist im allgemeinen eine Komponente, die in Serie mit dem restlichen System geschaltet ist, wichtiger, als wenn sie parallel zu den restlichen Systemteilen stehen würde.

Ein weiterer wesentlicher Faktor, der die Bedeutung von Komponenten in einem System bestimmt, ist ihre Zuverlässigkeit. Die Frage nach der Wichtigkeit einer Systemkomponente kann, abhängig von der interessierenden Problemstellung, sehr unterschiedlich formuliert werden.

- Wie ändert sich das interessierende Systemzuverlässigkeitsmerkmal bei einer bestimmten Änderung eines relevanten Komponentenmerkmals? Eine Beantwortung dieser Fragestellung führt insbesondere zur Identifikation derjenigen Komponenten, deren zuverlässigkeitsmäßige Verbesserung sich am stärksten auf Systemebene auswirkt (Systemoptimierung, Identifikation von Systemschwachstellen).
- Der Systemausfall fällt stets mit dem Ausfall einer Systemkomponente zusammen. Die Wahrscheinlichkeit, daß eine Komponente den Systemausfall im obigen Sinne bewirkt, kann somit als ein weiteres Wichtungsmerkmal für die Komponente benutzt werden.
- Zur Fehlererkennung und -diagnose ist die Reihenfolge, in der die Bestandteile des Systems getestet werden, bedeutungsvoll. Speziell im Hinblick auf eine Minimierung der Instandsetzungszeit ist es nach einem Systemausfall wichtig, den Reparaturprozeß bei derjenigen Komponente zu beginnen, deren Erneuerung das System mit der größten Wahrscheinlichkeit in den funktionstüchtigen Zustand zurückbringt.

Neben dieser systemabhängigen Bewertung der Komponenten ist auch eine systemunabhängige Beurteilung der Komponenten oft von großem Nutzen. So gibt z.B. die Ausfallhäufigkeit interessante Informationen über die Anzahl der durchzuführenden Reparaturen und über die notwendige Bereitstellung von Ersatzkomponenten.

Zur teilweisen Beantwortung der gerade angesprochenen Fragestellungen kann das Programmsystem RALLY verwendet werden. So werden z.B. in den Programmen CRESSEX und FESIVARM die Komponenten, geordnet nach Anzahl der Ausfälle und Totzeiten bzw. Ausfallwahrscheinlichkeit und Nichtverfügbarkeit, ausgedruckt. Das Programm SALP-MP berechnet für diejenigen Komponenten, die am Ausfall des Systems beteiligt sind, deren Beiträge (Gewichte) zur Nichtverfügbarkeit des TOP. Über diese Gewichte läßt sich dann anhand der Variation der Komponentennichtverfügbarkeit das Ausmaß der Variation der Systemnichtverfügbarkeit

leicht abschätzen. Differenziertere Importanzkenngrößen erfordern darüber hinaus eine Weiterentwicklung einiger Programme im System RALLY.

3.6 Verknüpfung von Verteilungsfunktionen

In der Praxis tritt oft das Problem auf, die Verteilung einer Funktion Y von Zufallsgrößen $Y=f(X_1,X_2,\ldots,X_n)$ zu bestimmen. In vielen Fällen ist die Verteilungsfunktion F(y) von Y analytisch kaum zu berechnen, d.h., man ist auf simulative Methoden angewiesen.

Zur Ermittlung der Verteilung F(y) kann das Programm STREUSL verwendet werden. Der Algorithmus wurde zum Teil schon in Abschnitt 2.8 beschrieben. Zuerst werden aufgrund der Verteilungen von X_i, i=1,...,n mit Hilfe von Zufallszahlengeneratoren Werte x_i^k für X_i ausgespielt. Anschließend wird mit dieser Kombination von Werten die Funktion $y_k=f(x_1^k, x_2^k,\ldots,x_n^k)$ berechnet. Dieser Vorgang, Ausspielen der Zufallszahlen und Berechnung von $f(x_1^k,x_2^k,\ldots,x_n^k)$, wird nun sooft wie möglich wiederholt. Auf diese Weise erhält man dann eine Stichprobe $y_1,y_2,\ldots,y_n$ von Y, die mit dem Programm AVAGS (siehe Abschnitt 2.9) statistisch ausgewertet werden kann.

3.7 Störfallsimulator

Aufgabe eines (Störfall-)Simulators ist es, die Wechselwirkung der physikalischen Abläufe mit der Funktion oder dem Ausfall der Komponenten in geeigneter Weise auf einer Rechnerstruktur abzubilden. Die Realisierung eines solchen Konzeptes hängt entscheidend von der Definition des Simulationsumfanges ab.

Diese Definition wird stufenweise über die Festlegung von Störungs- und Störfallklassen, die man simulieren will, Systemfunktionen und Systeme, die dabei relevant sind, und Teilsysteme, Komponenten und Operateureingriffe, die zum Ablauf und

zur Beherrschung der Störung oder des Störfalls beitragen, vorgenommen. Eine systematische Methode dafür bietet sich durch Zuverlässigkeitsanalysen mit Hilfe der Fehlerbaummethode an. Da die Fehlerbäume z.B. in der deutschen Risikostudie bis zur Komponentenebene aufgelöst sind, können anhand der Ergebnisse von Berechnungen mit dem Programmsystem RALLY Komponenten, Teilsysteme oder Systeme in Klassen eingeteilt werden, die ihrer Bedeutung bei der Beherrschung von Störfällen entsprechen.

Durch die Verbindung dieser Informationen mit den allgemeinen simulationstechnischen Anforderungen für Normalbetrieb und Störungen kann dann der Simulationsumfang eindeutig festgelegt werden.

3.8 Aufsicht über kerntechnische Einrichtungen

Bei der Wahrnehmung ihrer Aufgaben während des Betriebes eines Kernkraftwerkes kann die Kontrollbehörde weitere Begutachtungen anfordern, wenn dies infolge der Betriebserfahrung oder angesichts des Fortschrittes bei der Reaktorsicherheitstechnologie erforderlich erscheint. Eine solche Begutachtung kann zu Änderungen in Systemfunktionen oder in Betriebsverfügungen führen; der Grad der Veränderung/Verbesserung muß quantifizierbar offenkundig werden.

Das Programmsystem RALLY ist geeignet, Nachanalysen bei Änderungen von Vorschriften und Regeln, bei Änderungen im System oder in der Betriebsweise (z.B. geänderte Test- oder Reparaturstrategie) sowie Nachanalysen von aufgetretenen Betriebsstörungen bzw. Störfällen durchzuführen und Systemvergleiche im Rahmen von "backfitting"-Maßnahmen anzustellen.

3.9 Kopplung RALLY mit Datenbank

Aussagen über Streuungen und Kenngrößen in Zuverlässigkeitsanalysen sind sicherheitstechnisch von Bedeutung. Für Begut-

achtungsfälle ist die Wahl geeigneter Bewertungskennzahlen (Median, Erwartungswert) derzeit Ansatzpunkt heftiger Diskussion. Die Angabe der Verteilungsfunktion der Zuverlässigkeitskenngrößen liefert in diesem Zusammenhang ein größeres Maß an Information.

Für solche Fälle wurde das Programm STREUSL entwickelt, das eine Stichprobe der Zuverlässigkeitskenngrößen liefert unter Berücksichtigung der Verteilungen der Basisdaten. Die Anpassung verschiedener Verteilungsfunktionen an die Stichprobe bzw. deren Kenngrößen (Median, Streufaktor, Erwartungswert, Streuung, Schiefe, Exzeß usw.) läßt sich mit dem Programm AVAGS durchführen.

Darüber hinaus kann AVAGS auch zur Ermittlung von Verteilungen für Ausfallraten und -wahrscheinlichkeiten pro Anforderung aus Literaturdaten verwendet werden. Ebenso können Komponentendaten, die aus der Betriebserfahrung stammen, mit Hilfe dieses Programms statistisch ausgewertet werden.

Eine Kopplung des Programmsystems RALLY bzw. Teile davon mit einer Datenbank, in der Anlagen- und Schadensdaten von Kernkraftwerken gespeichert sind, kann somit einen erleichterten Zugang zu neuesten Erkenntnissen bezüglich der Betriebserfahrung ermöglichen.

Die Verbindung der Fehlerbaummethode mit einer Datenbank kann auch im wissenschaftlich-technischen Bereich zu einer wesentlichen Erweiterung der interessierenden Fragestellungen führen: So könnte systematisch eine im Betrieb erkannte Schwachstelle (wie ungeeignetes Material, Konstruktionsfehler) dahingehend überprüft werden, welche weiteren Komponenten des gleichen Typs oder Werkstoffs etc. vom gleichen Ausfallmechanismus betroffen sein können. Ferner ließen sich diejenigen Komponenten ermitteln, die von besonderer sicherheits- und systemtechnischer Bedeutung sind. Ebenso kann bei einem aufgetretenen Ausfall gefragt werden, mit welchen weiteren Ausfallkombinationen zu rechnen ist und mit welcher Wahrscheinlichkeit ein bestimmtes unerwünschtes Ereignis eintritt.

3.10 Berücksichtigung von Common-Mode-Ausfällen und Human Error

Von besonderem Interesse sind die als 'CMA' bezeichneten Ausfälle aufgrund gemeinsamer Ursache, da sie letztlich für die untere Grenze der Zuverlässigkeitskenngrößen von Systemen verantwortlich sind: So ist bei jedem System letzten Endes mit dem Auftreten voneinander abhängiger Funktionsausfälle zu rechnen, sei es wegen funktioneller Abhängigkeit, als Folge eines einzigen Funktionsausfalls oder aufgrund gemeinsamer Ursache bei redundanten Komponenten. Besondere Beachtung verdienen dabei Ereignisse, die zugleich oder in einem eng begrenzten Zeitintervall auftreten, so daß ausgefallene Zustände wegen begrenzter Ausfallentdeckungszeit gleichzeitig vorliegen.

Die Berücksichtigung solcher Abhängigkeiten - auch was den Grad der Abhängigkeit angeht - wird modellhaft erfaßt ("Kopplung von Ausfällen") und kann dann im Fehlerbaum als unabhängige Komponente behandelt werden. Die Behandlung von Common-Mode-Ausfällen in RALLY ist damit keinen weiteren Einschränkungen unterlegen.

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 Art der Abhängigkeit kann in den Zuverlässigkeitsuntersuchungen durch eine Kopplung der Ausfallraten bzw. der Ausfallwahrscheinlichkeiten pro Anforderung behandelt werden. Sie kommt bei Streubreitenrechnungen zur Anwendung und führt nicht zu gleichzeitigen, sondern zu zeitlich versetzten Ausfällen der Komponenten. Die Werte der Ausfallraten solcher gleichartiger

Komponenten werden im Rechenprogramm STREUSL 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 gleichartiger Komponenten verwendet.

Das Programmsystem gestattet darüber hinaus auch die Erfassung des Einflusses menschlichen Fehlverhaltens. Fehlhandlungen bei Wartungs- oder Justierungsarbeiten, bei Prüfmaßnahmen oder bei der Ausführung von Handlungen gemäß den Störfallogiken des Betriebshandbuches können im Fehlerbaum erfaßt werden. Sie werden dann wie jede andere Komponentenfunktion behandelt. Dabei ist jedoch bei der Interpretation der Ergebnisse solcher Zuverlässigkeitsanalysen zu bedenken, daß man sich bei den Basisdaten mit groben Abschätzungen behelfen muß, da menschliche Handlungen nur schwer quantifizierbar als Ausfallwahrscheinlichkeiten einzustufen sind. Darüber hinaus muß bei der Bewertung menschlicher Zuverlässigkeit als wichtiger Einflußfaktor die Abhängigkeit menschlicher Handlungen untereinander Berücksichtigung finden. Dies kann wiederum nur modellhaft geschehen. Die Vorgehensweise - und damit die Behandlung im Programmsystem RALLY - ist dann die gleiche wie bei den Common-Mode-Ausfällen.

Obwohl also in den meisten Fällen nur eine pauschale Bewertung aufgrund der Unsicherheit bei den Basisdaten erreicht werden kann, kann die Berücksichtigung menschlicher Handlungen dazu benutzt werden, den Einfluß derartiger Handlungen auf Störfallablauf und -beherrschung zu ermitteln sowie eventuelle Überforderungen des Personals zu erkennen. Nach eingetretenen Störfällen kann überprüft werden, an welchen Stellen ein Operatoreingriff erforderlich war und wie das reale Operatorverhalten mit dem theoretisch geforderten Verhalten übereinstimmt, um gegebenenfalls systematisch die betroffenen schriftlichen Anweisungen zu korrigieren.

4. BEREITS ERFOLGTE ANWENDUNGEN DES PROGRAMMSYSTEMS RALLY

Nach der Diskussion der Möglichkeiten, die RALLY bietet, sollen in diesem Kapitel die mit RALLY bereits durchgeführten Analysen beschrieben werden.

4.1 Anwendung von RALLY bei Risikostudien

Einen Einsatzschwerpunkt für das Programmsystem RALLY bildete die Deutsche Risikostudie Kernkraftwerke (GE 79). Eine der wesentlichen Aufgaben war dabei, Ereignisabläufe für die Störfälle 'großes Leck', 'mittleres Leck', 'kleines Leck', 'Notstromfall' und 'Druckhalterleck beim Notstromfall' zu quantifizieren. Durch die Vereinheitlichung der Datensätze für alle Programme im Programmsystem RALLY war es möglich, in einem einzigen Rechenlauf pro Programm die Nichtverfügbarkeit der angeforderten Systemfunktionen bei einem vorgegebenen einleitenden Ereignis zu berechnen. Für diese Fälle zeigte sich ganz deutlich, daß die hier eingesetzten simulativen Programme diese sehr großen, komplexen Systeme, im Gegensatz zu analytischen Programmen, in vernünftiger Rechenzeit bearbeiten konnten.

Zusätzlich war auch die Aufgabe gestellt, für die bedingten Störfallwahrscheinlichkeiten Streubreiten aufgrund der Streuungen der Eingangsdaten zu berechnen. Dabei mußten mit dem Programm CRESSC die minimalen Schnittmengen (minimal cuts) ermittelt werden. Anhand dieser 'minimal cuts' und der Verteilung der Komponentenausfallraten wurde dann im Programm STREUSL die Streuung des Gesamtergebnisses berechnet, wobei zur Kontrolle die Erwartungswerte aus STREUSL und CRESSEX auf Übereinstimmung geprüft wurden.

Um die Abhängigkeit von Ausfällen gleichartiger Komponenten im selben System, aber unterschiedlicher Redundanz, zu berücksichtigen, wurde mit dem Programm STREUSL ein Rechenlauf mit sogenannter "Ausfallratenkopplung" durchgeführt. Mit dieser Vorgehensweise können z.B. Abhängigkeiten durch gemeinsame Ferti-

gung, Korrosionsausfälle, gewisse Wartungsfehler sowie Ausfälle aufgrund erschwerter Umgebungsbedingungen behandelt werden. Als Beispiel für den Rechenlauf mit "Ausfallratenkopplung" wurde der Ereignisablauf Notstromfall gewählt, wobei jeweils gleichartige Hardware-Ausfälle, wie Startversagen Pumpe, Startversagen Notstromdiesel oder Öffnungsversagen Motorarmatur, zu Kopplungsgruppen zusammengefaßt wurden.

Der Rechenlauf ergab, daß sich Erwartungswert und Streubreite des ursprünglichen Ergebnisses nicht wesentlich erhöhten. Bei der Durchsicht der minimalen Schnittmengen (minimal cuts) ließ sich feststellen, daß Kombinationen gleichartiger Komponentenausfälle das Ergebnis nicht bestimmen, sondern vielmehr der Einfluß des Common-Mode-Ausfalls der Notstromdiesel und des menschlichen Fehlverhaltens (Inbetriebnahme des Notstandsystems) dominiert.

Ein weiterer Schritt in der Risikostudie war die Verknüpfung der System-Fehlerbäume mit den Fehlerbäumen für das Versagen des Sicherheitsbehälter-Abschlusses, um die verschiedenen Freisetzungspfade zu ermitteln und quantitativ zu bewerten. Mit dem Programmsystem RALLY wurden die Freisetzungshäufigkeiten nach Kernschmelzen für die Kategorien $ß_1$ (große Leckage, z.B. durch Versagen des Lüftungsabschlusses bzw. der Schweißnähte am Sicherheitsbehälter), $ß_2$ (mittlere Leckage, z.B. durch Versagen des Gebäudeentwässerungs-Abschlusses), $ß_3$ (kleine Leckage, z.B. durch Versagen des aktiven Abschlusses von Meßleitungen im Lüftungssystem) und η (Versagen der Ringraumabsaugung) berechnet. Diese Ergebnisse bildeten die Grundlage für die nachfolgenden Ausbreitungsrechnungen und Unfallfolgenbetrachtungen.

Neben der Bestimmung der Kollektiv- und Individualrisiken aufgrund von denkbaren Unfällen in Kernkraftwerken war die Ermittlung von Schwachstellen und die Erarbeitung von Vorschlägen zu Systemverbesserungen ein wichtiges "Produkt" der deutschen Risikostudie, an dem das Programmsystem RALLY wesentlich beteiligt war. So resultierte zum Beispiel aus den Berechnungen die

Beobachtung, daß beim mittleren Leck in einer Hauptkühlmittelleitung die Nichtverfügbarkeit der unbedingt erforderlichen Hochdruckeinspeisung zu 33 % durch den Ausfall des Dreiwegeventils im gebrochenen Strang bestimmt wird. Ein weiteres Beispiel läßt sich beim Notstromfall anführen, wo der Common-Mode-Ausfall der Notstromdiesel mit 80 % zur Nichtverfügbarkeit der Systemfunktion "Notspeisewasserversorgung und Frischdampfabgabe" beiträgt. Unter anderem als Folge des letzteren Ergebnisses wurde bereits im August 1978 die Möglichkeit einer Netzrückschaltung in der Referenzanlage Biblis B geschaffen. Diese Systemverbesserung bewirkt bereits eine Verminderung der Häufigkeit eines Kernschmelzunfalls als Folge eines Notstromfalls um etwa 10^{-5}/a. Insgesamt ergab sich eine Reihe von Systemverbesserungen, wie zum Beispiel GAU-Festigkeit von Meßumformern für die Speisewasserregelung oder Teilautomatisierung des 100°C/h-Abfahrens bei "kleinen Lecks", die in der Referenzanlage bereits durchgeführt wurden.

Bei der risikoorientierten HTR-Sicherheitsstudie (KE, GE 81) beschränkte sich die GRS-Mitarbeit, hinsichtlich der Zuverlässigkeitsanalyse unter Einsatz von RALLY, auf die Untersuchung des Ereignisablaufs "Notstromfall". Die Quantifizierung des auf ein 1160-MW-Hochtemperaturreaktor-Konzept bezogenen Ereignisablaufs erfolgte analog zu der Vorgehensweise in der DWR-Studie, das heißt, daß die beim "Notstromfall" angeforderten Sicherheits- und Hilfssysteme mittels Fehlerbaummethode analysiert und anschließend deren Zuverlässigkeit mit den Programmen CRESSEX, CRESSC und STREUSL bewertet wurden. Die daraus resultierenden Verteilungen der Nichtverfügbarkeiten, bezogen auf die einzelnen Ereignisabläufe, wurden mit den Versagensmöglichkeiten des Gebäudeabschlusses gekoppelt, um die Häufigkeiten der Freisetzungen (eingeteilt in Klassen) aufgrund des einleitenden Ereignisses "Notstromfall" zu ermitteln.

Eine weitere GRS-Studie ist die risikoorientierte Analyse zum SNR-300. Da die Untersuchungen erst vor einigen Wochen begonnen haben, liegen noch keine Ergebnisse vor. Es besteht die

Absicht, das Programmsystem RALLY entsprechend den Anwendungen bei den oben beschriebenen Studien einzusetzen.

4.2 Anwendung von RALLY im Genehmigungsverfahren

Entsprechend den BMI-Kriterien (BU 77) sind für die Überprüfung der Ausgewogenheit des Sicherheitskonzepts - in Ergänzung zur Gesamtbeurteilung der Sicherheit des Kernkraftwerkes aufgrund deterministischer Methoden - die Zuverlässigkeiten sicherheitstechnisch wichtiger Systeme und Anlagenteile mit Hilfe probabilistischer Methoden zu bestimmen, soweit dies nach dem Stand von Wissenschaft und Technik mit der erforderlichen Genauigkeit möglich ist.

Die Überprüfung der Sicherheit von kleineren Systemen bzw. Systemteilen mit Hilfe probabilistischer Methoden im Rahmen von Genehmigungsverfahren ist häufig durch Handabschätzungen auf der Grundlage der erstellten Fehlerbäume möglich. Ein Beispiel hierfür ist die bei der GRS durchgeführte Zuverlässigkeitsuntersuchung der Hosenbeineinspeisungen von Notstromschienen des SNR-300.

Bei umfangreichen Systemen mit verschiedenen Abständen zwischen den Funktionsprüfungen für die Komponenten ist eine zahlenmäßige Ermittlung der Zuverlässigkeitskenngrößen (mittlere Nichtverfügbarkeit, Ausfallwahrscheinlichkeit) nur mit Hilfe von Rechenprogrammen möglich. Hierbei werden bei Rechnungen für Genehmigungsverfahren von der GRS normalerweise die Programme TREBIL, TIMBER und CRESSEX verwendet.

Im Rahmen des Genehmigungsverfahrens für den SNR-300 wurde für die Nachwärmeabfuhr eine probabilistische Untersuchung unter Verwendung des Programmsystems RALLY durchgeführt. Dabei erfolgte für die beiden diversitären Systeme (strangspezifisches Nachwärmeabfuhrsystem, Tauchkühlsystem) sowohl eine Berechnung der Nichtverfügbarkeit bei Anforderung als auch der Ausfallwahrscheinlichkeit während der anschließenden Langzeitphase. Für die Langzeitphase kam dabei das Programm CRESS4 zum Einsatz.

Die Rechnungen zeigten unter anderem, daß es günstig ist, während der Langzeitphase nicht den automatischen Start des Tauchkühlsystems abzuwarten, sondern schon unmittelbar nach einem Ausfall des strangspezifischen Nachwärmeabfuhrsystems das Tauchkühlsystem manuell in Betrieb zu nehmen, ohne dabei das Notumwälzsystem anzufordern.

Für das Kernkraftwerk Grafenrheinfeld wurden Zuverlässigkeitsuntersuchungen für das "große Leck" und das "kleine Leck" im Primärkreis durchgeführt. Bei diesen Untersuchungen wurde vor allem auf folgende Punkte Wert gelegt:

- Schwachstellensuche,
- Parameterrechnungen,
- Einfluß von Testintervallen,
- Einfluß von Teilsystemen auf das Gesamtergebnis,
- Vergleich mit den Ergebnissen der deutschen Risikostudie und
- Einfluß von Instandhaltungszeiten.

Für die Behandlung des letzten Punktes wurden Parameteruntersuchungen durchgeführt, um den Einfluß zusätzlicher Prüfungen an allen Redundanzen berücksichtigen zu können. Solche zusätzlichen Prüfungen können durchgeführt werden, wenn Komponentenausfälle festgestellt werden oder wenn Wartungsarbeiten anstehen. Zur Berechnung des Einflusses zusätzlicher Prüfungen mußte das Programm CRESSEX modifiziert werden, was durch relativ geringen Aufwand möglich war.

Entsprechende Fragestellungen, wie die für die Anlage Grafenrheinfeld genannten, sind auch für das Kernkraftwerk Gundremmingen (KRB II) für die einleitenden Ereignisse "Notstromfall" und "Frischdampfleitungsbruch" zu behandeln.

Zusätzlich zu den obigen Aufgaben wurde für das Kernkraftwerk Grafenrheinfeld die Wahrscheinlichkeit für den Ausfall der Überdrehzahlsicherheits- und Schutzeinrichtungen des Turbosatzes berechnet. Wegen der geringen Versagenswahrscheinlichkeit des Systems war ein Einsatz des Simulationsprogramms CRESSEX in diesem Fall nicht zweckmäßig. Deshalb wurde mit

Hilfe des Programms CRESSC die approximierte Systemfunktion (minimal cuts) ermittelt und mit STREUSL der Punktwert des Ergebnisses berechnet.

Bei den Untersuchungen über die Zuverlässigkeit des Notkühlsystems für das Kernkraftwerk Krümmel waren im Gegensatz zu den bisher aufgeführten Aufgaben im Rahmen von Genehmigungsverfahren keine mittleren, sondern maximale Nichtverfügbarkeiten zu ermitteln. Hierfür wurde das Programm FESIVAR eingesetzt, das darüber hinaus eine Berechnung maximaler Nichtverfügbarkeiten erlaubt.

4.3 Benutzer des Programmsystems

Das Programmsystem RALLY wird auch außerhalb der GRS zur Zuverlässigkeitsbeurteilung von Systemen eingesetzt. Folgenden Instituten und Firmen wurde das Programmsystem, oder zumindest Teile davon, überlassen:

- Bayer AG, Leverkusen,
- BBR (Babcock-Brown Boveri Reaktor GmbH),
- CNEN - Brasilien,
- Dornier-System, Friedrichshafen,
- KFA Jülich,
- KWU (Kraftwerk Union AG),
- TÜV Bayern,
- TÜV Rheinland.

Interessenten des Programmsystems werden gebeten, sich an die GRS, Bereich Datenverarbeitung, zu wenden.

Schrifttum

(As et al. 80) Astolfi, M., C.A. Clarotti, S. Contini und F.R. Picchia:
SALP-MP, A Computer Program for Fault Tree Analysis of Complex Systems and Phased Missions
P.E.R. 389, 1980 - JRC Ispra Establishment

(BU 77) Der Bundesminister des Innern:
Sicherheitskriterien für Kernkraftwerke
Bundesanzeiger Nr. 206 vom 3. Nov. 1977

(Ca, Ri 75) Camarinopoulos, L., und G. Richter:
KARI - ein neues analytisches Programm zur Berechnung von Zuverlässigkeitsmerkmalen technischer Systeme
Angewandte Informatik 12/75

(GE 79) Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke
- Hauptband -
Hrsg.: Der Bundesminister für Forschung und Technologie, Bonn,
Verlag TÜV-Rheinland, Köln, 1979
ISBN 3-921059-67-4

(GE 80) Gesellschaft für Reaktorsicherheit:
GRS-Jahresbericht 1980

(GE 81) Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke,
Fachband 2: Zuverlässigkeitsanalyse
Hrsg.: Der Bundesminister für Forschung und Technologie, Bonn,
Verlag TÜV-Rheinland, Köln, 1981
ISBN 3-88585-013-3

(KE, GE 81) Kernforschungsanlage Jülich und
Gesellschaft für Reaktorsicherheit:
Sicherheitsstudie für HTR-Konzepte unter
deutschen Standortbedingungen
Jül-Spez-136/Bd.1, Dez. 1981
ISSN 0343-7639