Weiterentwicklung der Unsicherheitsanalyse für eine PSA

Ansätze zur Berücksichtigung von Modellunsicherheiten

SR 2547

GRS - A - 3412

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Weiterentwicklung der Unsicherheitsanalyse für eine PSA

Ansätze zur Berücksichtigung von Modellunsicherheiten

M. Kloos

J. Peschke

März 2008

Auftrags-Nr.: 857166

Anmerkung:

Das diesem Bericht zu Grunde liegende FE-Vorhaben SR 2547 wurde im Auftrag des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit durchgeführt. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Auftragnehmer.
Der Bericht gibt die Auffassung und Meinung des Auftragnehmers wieder und muss nicht mit der Meinung des Auftraggebers übereinstimmen.

GRS - A - 3412

Kurzfassung

Ziel des Vorhabens SR 2547 ist die Weiterentwicklung von PSA Methoden im Hinblick aufsichtlicher Fragestellungen, insbesondere im Rahmen von Sicherheitsbeurteilungen von Kernkraftwerken vorgelegter PSA und deren Begutachtung. Arbeitspunkt 2 des Vorhabens beabsichtigt, die Unsicherheitsanalyse in einer PSA weiter zu entwickeln.

Die bislang praktizierte Unsicherheitsanalyse für eine PSA beschränkt sich in der Regel auf die Quantifizierung der Unsicherheiten in den Häufigkeiten für die auslösenden Ereignisse und in den Zuverlässigkeitskenngrößen. D.h. sie berücksichtigt lediglich die Unsicherheiten in den Eingabedaten für die Fehlerbaum- und Ereignisbaumanalysen. Weitere Unsicherheitsquellen, wie z. B. Parameter- und Modellunsicherheiten aus den Störfallsimulationen mit Thermohydraulik-Modellen, werden im Allgemeinen nicht berücksichtigt, obwohl nicht auszuschließen ist, dass auch sie die PSA-Ergebnisse und ihre Unsicherheiten erheblich beeinflussen können.

Notwendig für eine Weiterentwicklung zu einer umfassenderen Unsicherheitsanalyse einer PSA ist eine systematische Berücksichtigung möglichst aller relevanten Unsicherheitsquellen. Als ein erster Schritt zur Erreichung dieses Ziels werden in diesem Projekt verschiedene Unsicherheitsquellen identifiziert und diskutiert, die neben den unsicheren Eingangsdaten für die Fehlerbaum- und Ereignisbaumanalysen als relevant in Betracht zu ziehen sind. Insbesondere wird auf das Thema der Modellunsicherheiten Bezug genommen, die bisher in PSA's nicht berücksichtigt werden und deren Einfluss auf PSA-Ergebnisse deshalb nicht quantifiziert werden kann.

Um zusätzliche relevante Unsicherheitsquellen (incl. Modellunsicherheiten) identifizieren zu können, wird in diesem Projekt systematisch untersucht, welche Annahmen den in einer PSA verwendeten Modellen (z. B. Fehler – und Ereignisbaummodelle, Modelle zur Quantifizierung menschlicher Handlungen etc.) zugrunde liegen. In diesem Zusammenhang wird beschrieben, welche Vereinfachungen in den Annahmen stecken und welche Konsequenzen sich aus den vereinfachenden Annahmen in Bezug auf die Diskrepanz zwischen Modellergebnis und Realität ergeben können. Eine Quantifizierung, welchen Einfluss vereinfachende Modellannahmen auf die Modellergebnisse haben können, fand bisher nicht statt. In diesem Projekt werden erstmals Verfahren

vorgeschlagen, die für ausgewählte Fragestellungen eine Abschätzung des Einflusses vereinfachender Annahmen auf die Modellergebnisse prinzipiell ermöglichen.

Für die im Rahmen von Störfallanalysen eingesetzten Rechencodes erfolgt eine Beschreibung der verschiedenen Quellen von Modellunsicherheiten sowie der bekannten Methoden zur Quantifizierung von Modellunsicherheiten. Es wird versucht, den in einer PSA zu berücksichtigenden Modellunsicherheiten die geeigneten Methoden zur Quantifizierung zuzuordnen.

Die in diesem Arbeitspunkt durchgeführten Arbeiten bilden einen ersten Schritt für eine umfassende Unsicherheitsanalyse. Sie identifizieren und beschreiben mögliche zusätzliche Quellen von Unsicherheiten, die in einer PSA bisher nicht berücksichtigt werden, und liefern Vorschläge und erste Methodenkonzepte, wie Modellunsicherheiten berücksichtigt und deren Einfluss auf PSA-Ergebnisse quantifiziert werden können.

Summary

Objective of the project SR 2547 is the further development of PSA methods with respect to regulatory control issues in the framework of PSAs and PSA reviews of nuclear power plants. Working point 2 of the project particularly aims to further develop the uncertainty analysis in a PSA.

Up to now the uncertainty analysis of a PSA is generally restricted to the quantification of uncertainties in initiating event frequencies and in reliability parameters. This means that only uncertainties regarding the input data of the fault-tree and event-tree analyses are considered. Other sources of uncertainties, like e.g. parameter- and model uncertainties in thermodynamics codes used for accident simulations are generally not taken into account, although it is well known that they might have significant influence on PSA results.

For the development of a more extensive uncertainty analysis, a systematic consideration of potential relevant sources of uncertainties is necessary. As a first step in this direction, additional sources of uncertainties, which might be relevant beside the input data of the fault-tree and event-tree analyses, are identified and discussed. The work in this project particularly focused on model uncertainties which are usually not considered in a PSA.

In order to identify additional relevant sources of uncertainties (including model uncertainties), the assumptions of the well known PSA models (e.g. fault-tree and event-tree models, models for human factors etc.) are systematically examined. In this context the simplifications of the model assumptions and their consequences, which might influence the divergence between model results and reality, are discussed. A quantification of the influence of simplified model assumptions on the results has not yet been performed. Therefore, the work in this project also aims to propose methods which would principally allow an assessment of the influence of simplified model assumptions.

For the deterministic codes which are used for the accident simulations in a PSA, different sources of model uncertainties and methods for their quantification are described. Methods for model uncertainty quantification are also presented for other model uncertainties which may arise in a PSA.

The achievements of this work represent a first step towards an improvement of the uncertainty analysis in a PSA. Sources of uncertainties are identified which have not yet been considered. Proposals are offered how to consider relevant sources of uncertainties in order to quantify their influence on PSA-results.

Inhaltsverzeichnis

1 Einleitung

Im Rahmen einer PSA werden unterschiedliche Modelle eingesetzt, um das Sicherheitskonzept eines Kernkraftwerks probabilistisch bewerten zu können. Die probabilistische Bewertung liefert Angaben zu Systemschadens- und Kernschadens-Häufigkeiten (PSA Stufe 1) sowie zu den Häufigkeiten von Anlagenschadenszuständen (PSA Stufe 2).

Zu den wichtigsten Modellen, die in einer PSA eingesetzt werden, gehören

- die Ereignisbaum-Modelle der Stufen 1 und 2, die Ereignisabläufe beschreiben und probabilistisch bewerten, die zu einem Schadenszustand führen können:
  - Ereignisabläufe der Stufe 1: Abläufe von Erfolgen/Misserfolgen bei der Anforderung von Sicherheitsfunktionen und präventiven Notfallmaßnahmen,
  - Ereignisabläufe der Stufe 2: Abläufe von unterschiedlichen Auswirkungen physikalisch/chemischer Phänomene in Kombination mit Erfolgen/Misserfolgen bei der Anforderung von Sicherheitsfunktionen und Notfallmaßnahmen,
- die Fehlerbaum-Modelle der Stufe 1, die Ausfallwahrscheinlichkeiten von angeforderten Funktionen der Sicherheits-, ATWS- und Notstandssysteme berechnen,
- die Modelle zur Bewertung von Personalhandlungen,
- die Wahrscheinlichkeitsmodelle zur Bewertung der Zuverlässigkeit von Komponenten und Teilsystemen, von menschlichen Fehlern, GVA-Ereignissen, usw.
- die Thermohydraulikmodelle zur Bestimmung der Mindestanforderungen an die Funktionen der Sicherheits-, ATWS- und Notstandssysteme sowie an die Notfallmaßnahmen,
- die Modelle zur Beurteilung der Festigkeit von Strukturen, wie z. B. des Reaktordruckbehälters, Druck führender Leitungen, des Sicherheitsbehälters, usw.
- die Modelle zur Ermittlung der Lasteinträge in den Reaktordruckbehälter oder in den Sicherheitsbehälter aus verschiedenen physikalisch/chemischen Prozessen wie z. B. Wasserstoffverbrennung oder Dampfexplosion
- Modelle zur Einbeziehung von brandspezifischen Ereignissen.

Wie genau die Ergebnisse der einzelnen Modelle die Realität wiedergeben ist unsicher. Die Unsicherheit in den Modellergebnissen hat verschiedene Ursachen (/GAL 93/)):

1. Unsicherheit aufgrund des konzeptionellen Modells: Wenn der abzubildende (komplexe) Zusammenhang nicht vollständig bekannt ist, können Modellannahmen ungenau, unvollständig oder sogar ungeeignet sein.

2. Unsicherheit aufgrund des mathematischen Modells: Um einen Zusammenhang mit Hilfe mathematischer Gleichungen darstellen zu können, sind i. A. zusätzliche Näherungen und Vereinfachungen notwendig, die einen Einfluss auf die Unsicherheit des Modellergebnisses haben.

3. Unsicherheit aufgrund des numerischen Modells: Hier sind Codierungsfehler, Diskretisierungen von mathematischen Gleichungen und sonstige rechentechnische Einschränkungen in Betracht zu ziehen. Z. B. können Lücken bei der Modellerstellung bewusst in Kauf genommen werden, um den rechentechnischen Aufwand in Grenzen zu halten. Unsicherheit besteht dann darüber, ob mit dem vereinfachten Modell noch hinreichend genaue Ergebnisse erzielbar sind.

4. Unsicherheit aufgrund der verwendeten Modellparameter und Daten: Wenn Modellparameter und Eingangsdaten (z. B. Anfangs- und Randbedingungen) für eine Modellanwendung nicht eindeutig zu bestimmen sind und geschätzt werden müssen, sind sie als unsicher zu betrachten. Eingangsdaten können je nach Fragestellung der Modellanwendung entweder fest aber ungenau bekannt sein (epistemische Unsicherheit) oder inhärent unsicher aufgrund stochastischer Variabilität (aleatorische Unsicherheit).

   Wenn Messergebnisse zu entsprechenden Modellrechnungen vorliegen, werden im Allgemeinen Korrekturterme (additiver Term, Korrekturfaktor) angewendet, um das Modellergebnis den Messergebnissen entsprechend zu modifizieren. Die Korrekturterme sind als unsicher zu betrachten, wenn die Messergebnisse streuen.

   Nicht selten werden Eingangsdaten aus Modellanwendungen abgeleitet und sind dadurch bereits mit einer Unsicherheit behaftet. Sind Modellparameter oder Daten aus Messungen abgeleitet, so müssen Messfehler berücksichtigt werden.

   Häufig sind mit Modellparametern keine physikalischen Einheiten verbunden, d.h. sie sind weder messbar noch exakt quantifizierbar. Diese „abstrakten“ Parameter dienen als Näherung eines unbekannten Zusammenhangs in Form einer Konstanten und müssen geschätzt werden. Aufgrund der Schätzung dieser Konstanten

kann es nicht nur einen einzigen "wahren" Wert geben, sondern die Schätzung der Parameter wird immer mit einer Unsicherheit verbunden sein. Beispiele sind Ausfallraten, Ablagerungsgeschwindigkeiten, Transferfaktoren, etc.

Die Unsicherheitsquellen 1-3 werden allgemein als Modellunsicherheit bezeichnet. Unsicherheitsquelle 4 ist als Parameter- bzw. Datenunsicherheit bekannt. Auf die Unterschiede zwischen Parameterunsicherheit und Modellunsicherheit wird in /HOF 94/ detailliert eingegangen. Je weniger Modelle durch Experimente abgesichert sind und je weiter die zur Validierung eventuell durchgeführten Experimente von den für die PSA maßgeblichen Bedingungen entfernt sind, desto größer ist die Modellunsicherheit.

Während die Unsicherheitsquellen 1 und 4 für alle Modelle der PSA berücksichtigt werden sollten, sind die Unsicherheitsquellen 2 und 3 im Allgemeinen nur für die komplexen Modelle, wie z. B. die zur Thermohydraulik oder Strukturzuverlässigkeit, in Betracht zu ziehen.

Die Berücksichtigung von Unsicherheiten in den einzelnen Modellen der PSA hat im Allgemeinen Konsequenzen für diejenigen Modelle, die in der Analysekette nachfolgen. Zum Beispiel könnte aus der Berücksichtigung von Unsicherheiten in den thermohydraulischen Untersuchungen zu den Mindestanforderungen an das Niederdruck-Fluten des Notkühlsystems folgen, dass mit subjektiver Wahrscheinlichkeit p_1 einer von vier redundanten Strängen zur Beherrschung des Störfalls ausreicht und mit subjektiver Wahrscheinlichkeit $q_1=1-p_1$ zwei von vier Strängen erforderlich sind. Es müssen also zwei alternative Ereignisbaummodelle für die Unsicherheitsanalyse bereitgestellt werden (/PAR 82/). Ein Modell beinhaltet die Anforderung von mindestens einem von vier Strängen, ein anderes Modell beinhaltet am selben Verzweigungspunkt des Ereignisbaums die Anforderung von mindestens zwei der vier Stränge. Abhängig von den Mindestanforderungen an das Niederdruck-Fluten des Notkühlsystems ist auch ein anderes Fehlerbaummodell (ein Fehlerbaum mit dem TOP-Ereignis: Ausfall von mindestens einem von vier Strängen, ein anderer Fehlerbaum mit dem TOP-Ereignis: Ausfall von mindestens zwei der vier Stränge) notwendig. Somit sind unterschiedliche TOP-Ereignis-Wahrscheinlichkeiten möglich, die sich schließlich auf die Unsicherheit in den PSA-Ergebnissen auswirken.

Die Unsicherheitsanalyse für die PSA-Ergebnisse ist gegenwärtig nur auf den Einfluss der Unsicherheiten in den Eingangsdaten für die Fehlerbaum– und Ereignisbaumanalysen beschränkt. Das schließt die Berücksichtigung der Unsicherheiten bzgl. der Ver-

sagenswahrscheinlichkeiten für Personalhandlungen und die Unsicherheiten bei der Schätzung von GVA-Wahrscheinlichkeiten ein. Der Einfluss von Modellunsicherheiten auf die PSA-Ergebnisse, z. B. Unsicherheiten in den Ergebnissen von Thermohydraulik-Modellanwendungen, wurde bislang nicht berücksichtigt obwohl bekannt ist, dass diese erheblich sein können. Dies entspricht nicht dem Stand von Wissenschaft und Technik.

Die Gründe für die Vernachlässigung sind einerseits in der zum Teil komplizierten Spezifikation und Abgrenzung von Modellunsicherheiten zu suchen und zum anderen darin, dass sich ein erheblicher Mehraufwand bei der Durchführung einer PSA ergeben kann. Insbesondere dann, wenn mehrere alternative Modellstrukturen zu entwickeln und in die Unsicherheitsanalyse einer PSA zu integrieren sind. Trotz dieser Schwierigkeiten wird immer mehr auf die Notwendigkeit und Wichtigkeit zur Berücksichtigung von Modellunsicherheiten hingewiesen. Ergebnisunsicherheiten, die sich lediglich aus Parameterunsicherheiten ergeben, berücksichtigen nicht die Auswirkungen, die z. B. alternative Modelle auf die Ergebnisse haben, oder welche Auswirkungen Unsicherheiten aus deterministischen Rechenmodellen auf die weiteren Modelle in der PSA Analysekette haben können. Dadurch können sich möglicherweise signifikante Unterschiede in den Aussagen der Unsicherheitsanalyse ergeben.

Die bisherige, einschlägige Literatur besteht überwiegend aus allgemeinen und mehr theoretischen Beschreibungen von Modellunsicherheiten. Im Rahmen dieses Projekts soll ein erster Schritt in Richtung einer systematischen Betrachtung von Modellunsicherheiten im Rahmen einer PSA begonnen werden. Dazu werden verschiedene Unsicherheitsquellen, die im Rahmen einer PSA auftreten können und bisher nicht berücksichtigt wurden, identifiziert und beschrieben. Wo möglich, werden erste Ideen zur methodischen Berücksichtigung der Modellunsicherheiten diskutiert. Hier sind insbesondere Unsicherheiten zu nennen, die aus der Anwendung von Thermohydraulik-Modellen im Rahmen von Störfallanalysen resultieren.

Auf der Basis der von der GRS im Rahmen des BMU Vorhabens SR 2414 für den Leistungsbetrieb eines Siedewasserreaktors erstellten PSA SWR 69 wird anhand von Beispielen gezeigt, welche Unsicherheiten einen potentiell wichtigen Einfluss haben können. Zusätzlich erfolgt eine Beschreibung der bekannten Methoden zur Quantifizierung von Modellunsicherheiten. Wo möglich, werden für die zu berücksichtigenden Modellunsicherheiten geeignete Methode zur Quantifizierung vorgeschlagen.

Ziel des Arbeitspunktes 2 im Vorhaben SR 2547 ist eine Weiterentwicklung der Unsicherheitsanalyse im Rahmen einer PSA. Aufgrund des begrenzten Projektrahmens und der Komplexität des Themas, kann die Bearbeitung dieses Arbeitspunktes keinen Anspruch auf Vollständigkeit haben. Vielmehr ist die Arbeit lediglich als erster Schritt in die Richtung zu betrachten, Teilaspekte einer PSA realistischer zu modellieren, um den Einfluss der bisher allgemein akzeptierten Vereinfachungen in einer PSA auf die Modellergebnisse quantifizieren und beurteilen zu können.

An dieser Stelle soll insbesondere betont werden, dass die nachfolgenden Ausführungen lediglich dazu dienen, mögliche Quellen von Unsicherheiten in einer PSA zu beschreiben sowie Vorschläge und Ansatzpunkte zur Berücksichtigung und Quantifizierung verschiedener Quellen von Modellunsicherheiten zu liefern. Sie stellen keine Kritik an bisher durchgeführten PSA-Analysen dar und insbesondere nicht an der PSA, die hier zu Beispielzwecken herangezogen wird.

2 Unsicherheit in den Fehlerbaum- und Ereignisbaum-Modellergebnissen

Zwei wesentliche Methoden einer PSA, die sich seit der WASH 1400- Studie /NUR 75/ als Stand von Wissenschaft und Technik etabliert haben, sind die Fehler- und die Ereignisbaumanalyse. Im Folgenden werden sowohl für die Fehlerbaumanalyse (in Abschnitt 2.1) als auch für die Ereignisbaumanalyse (in Abschnitt 2.2.) zunächst die den Modellen zugrundeliegenden Annahmen sowie die allgemein üblichen Vorgehensweisen beschrieben. Danach wird aufgezeigt, welche Vereinfachungen in den Annahmen stecken und welche Konsequenzen sich aus den vereinfachenden Annahmen in Bezug auf die Diskrepanz zwischen Modell und Realität ergeben. Des Weiteren wird diskutiert, welche Konsequenzen vereinfachte Modellierungen im Vergleich zu realistischeren Modellierungen auf die Modellergebnisse haben können. Verfahren werden vorgeschlagen, um den Einfluss der vereinfachenden Annahmen auf die Modellergebnisse abschätzen zu können.

2.1 Fehlerbaumanalyse

Die Fehlerbaumanalyse ist eine systematische Methode, um die Wahrscheinlichkeit für den Ausfall eines Systems in Abhängigkeit vom Ausfallverhalten seiner Komponenten zu ermitteln. Die Ergebnisse der Fehlerbaumberechnung im Rahmen einer PSA zielen darauf ab, die Nichtverfügbarkeit einer geforderten Systemfunktion zu ermitteln und diese als Verzweigungswahrscheinlichkeit an den entsprechenden Verzweigungspunkten eines Ereignisablaufs bereitzustellen. Darüber hinaus stellt das Ergebnis einer Fehlerbaumanalyse eine Beurteilungsgrundlage für die analysierte Systemfunktion dar.

Die wesentlichen Kenngrößen, die als Eingabe in das Fehlerbaummodell eingehen, sind /FAK 05/:

- Ausfallwahrscheinlichkeit (pro Anforderung) p,
- Ausfallrate λ [1/h] ,
- Zeitspanne zwischen zwei wiederkehrenden Funktionsprüfungen T_I [h].

Vereinzelt können zusätzlich noch die

- Reparaturzeit T_R [h],
- Zeit bis zu ersten Funktionsprüfung T_F [h] und
- die geforderte Betriebsdauer [h]

als Eingabegrößen in den Fehlerbaum eingehen.

2.1.1 Annahmen der Fehlerbaumanalyse

Eine generelle Annahme der Fehlerbaumanalyse ist, dass die Ausfallrate λ , die als Zuverlässigkeitskenngröße für eine Komponente bzgl. einer Zeiteinheit angegeben wird, als konstant über die Betriebszeit der Komponente vorausgesetzt wird. Diese Annahme hat verschiedene Konsequenzen zur Folge, die eine problemlose Anwendung der Fehlerbaumanalyse erst ermöglichen. Diese Konsequenzen sind:

1. Das Ausfallverhalten der Komponente folgt einer Exponentialverteilung mit dem Parameter λ. Die Ausfallwahrscheinlichkeit bzw. Zuverlässigkeit einer Komponente kann für ein gegebenes Zeitintervall t somit über eine Exponentialverteilung durch $q(t) = 1- \exp(-\lambda t)$ bzw. $R(t) = \exp(-\lambda t)$ ermittelt werden.

2. Das Ausfallverhalten der Komponente ist unabhängig vom Alter der Komponente, d.h. die Komponente altert nicht. Formal wird dies durch folgende Beziehung gezeigt: Seien t_1 und t_2 zwei Zeitintervalle. Die Wahrscheinlichkeit der Komponente, die Zeitdauer $t_1 + t_2$ zu überleben, unter der Bedingung, dass sie das Zeitintervall t_1 bereits überlebt hat ist

$$P(T > t_1 + t_2 \mid T > t_1) = \frac{\exp(-\lambda \cdot (t_1 + t_2))}{\exp(-\lambda \cdot t_1)} = \exp(-\lambda \cdot t_2) . \qquad (1)$$

   D.h., die bedingte Wahrscheinlichkeit der Komponente, die Zeitspanne $t_1 + t_2$ zu überleben ist unabhängig vom Alter bzw. der bisherigen Betriebszeit t_1 der Komponente.

3. Bereitschaftskomponenten („stand-by“-Komponenten) werden in regelmäßigen Zeitabständen auf ihre Funktionsfähigkeit überprüft (Testintervalle). Die Annahme

einer Exponentialverteilung für die Fehlerbaumanalyse bedeutet, dass eine Komponente nach erfolgreicher Funktionsprüfung, Wartung oder Instandsetzung (Reparatur) als neuwertig und fehlerfrei (″as good as new″) betrachtet wird.

Aus (3) wird deutlich, dass nach Durchführung der Funktionsprüfung einer Komponente, die im Falle von erkannten Schädigungen eine Instandsetzung zur Folge hat, die Komponente gemäß der für die Fehlerbaumanalyse geltenden Annahmen als neuwertig und fehlerfrei betrachtet wird. Es wird somit vorausgesetzt, dass Wartungen und Instandhaltungsarbeiten absolut zuverlässig durchgeführt werden. Außerdem wird angenommen, dass die regelmäßigen Funktionsprüfungen keinen Einfluss auf das Ausfallverhalten einer Komponente haben.

Wenn auch gegen die letzte Annahme bisher nicht viel eingewendet werden kann, zeigen jedoch Erfahrungen, dass insbesondere die Annahme bzgl. der Wartung und Instandhaltungsarbeiten von Komponenten als zu optimistisch betrachtet werden muss. Eine realistischere Annahme wäre, dass Wartungen und Instandhaltungsarbeiten, wenn sie nach einem Funktionstest als notwendig erachtet werden, mit gewissen Wahrscheinlichkeiten zu einem erhöhten Ausfallverhalten der jeweiligen Komponenten führen können.

Eine realitätsnahe Modellierung durch einen Fehlerbaum wäre relativ schwierig, da hier zeitliche Aspekte zu berücksichtigen sind, die aufgrund der statischen Struktur des Fehlerbaummodells nicht angemessen berücksichtigt werden können. Die zeitlichen Aspekte beziehen sich auf die zufälligen Zeitpunkte, wann die Wartungs- bzw. Instandhaltungsarbeiten einer Komponente durchgeführt werden und dass mit einer gewissen Wahrscheinlichkeit die Ausfallrate nach diesen Arbeiten erhöht ist. D.h., wenn Instandsetzungsarbeiten eine Erhöhung der Ausfallrate zur Folge haben, so können sich für die Zuverlässigkeit des Systems Unterschiede daraus ergeben, je nachdem ob die Erhöhung der Ausfallrate ziemlich früh im Lebensdauerzyklus einer Komponente oder erst relativ spät eintritt. Diese und ähnliche Zeiteffekte können unter Verwendung der konventionellen Methodik entweder gar nicht und wenn, dann nur sehr grob und vereinfacht z. B. durch die konservative Annahme der erhöhten Ausfallrate berücksichtigt werden.

Eine weitere Vereinfachung der Fehlerbaumanalyse ist, dass nur 2 Komponentenzustände bzw. Systemfunktionen betrachtet werden, und zwar

- Komponente intakt (bzw. Systemfunktion verfügbar) oder
- Komponente ausgefallen (bzw. Systemfunktion nicht verfügbar).

Mögliche Zwischenzustände werden entsprechend festgelegter Ausfallkriterien der jeweiligen Komponente einem der beiden Zustände zugeordnet. D.h., Schädigungen von Komponenten, die nur eine gewisse Beeinträchtigung der Funktionsfähigkeit und keinen kompletten Ausfall der Komponente bedeuten (z. B. Pumpe fördert nur mit einem verringerten Durchsatz) und die möglicherweise nur eine eingeschränkte Funktion des Systems zur Folge haben, werden in einem Fehlerbaum nicht berücksichtigt.

Insgesamt stellt sich die Frage, welchen Einfluss die oben genannten vereinfachenden Annahmen, die der Fehlerbaumanalyse zugrunde liegen, auf die Nichtverfügbarkeiten der analysierten Systeme haben.

Folgendes einfache Beispiel soll als eine weitere Veranschaulichung der Diskrepanz zwischen der Modellierung in einem Fehlerbaum und den realen Verhältnissen dienen. Dieses Beispiel stellt insbesondere bestehende Wechselwirkungen und zeitliche Einflüsse heraus, die in einer konventionellen Fehlerbaummodellierung nicht angemessen berücksichtigt werden können.

In der PSA zu KKP1 /LIN 06/ heißt es beispielsweise:

„ … Für die Bespeisung des RDB mit den Steuerstabantriebs-Pumpen (RS) werden zwei unterschiedliche Systemfunktionen verwendet.

Die Füllstandshaltung mit RS ist ausgefallen, wenn

a) die Notwendigkeit einer Bespeisung des RDB mit RS nicht rechtzeitig (innerhalb von 4 h) erkannt wird oder die Handmaßnahmen zur Durchsatzerhöhung der Pumpen nicht durchgeführt werden,

b) beide RS-Pumpen ausfallen, d. h.

- *die vor Eintritt des auslösenden Ereignisses in Betrieb befindliche Pumpe RS11D102 nicht wieder startet bzw. im Betrieb ausfällt (Anforderungszeit 24 h) oder die Schmierölversorgung versagt und*
- *die Umschaltautomatik ausfällt oder die Pumpe RS21D102 nicht startet bzw. im Betrieb ausfällt (Anforderungszeit 24 h) oder die Schmierölversorgung versagt. … "*

Im Fall (a) werden für die Fehlerbaumanalyse die Wahrscheinlichkeiten bestimmt, dass die Notwendigkeit einer Bespeisung des RDB nicht innerhalb von 4 Stunden erkannt wird (Diagnosefehler) und dass die Handmaßnahmen zur Durchsatzerhöhung der Pumpen nicht durchgeführt werden (Auslassungsfehler). Diese Wahrscheinlichkeiten gehen als Zuverlässigkeitskenngrößen der jeweiligen Basisereignisse in den Fehlerbaum ein und werden gemäß der entsprechenden Logik (in diesem Fall durch ein Oder-Gatter) verknüpft. Dies entspricht der Addition der beiden Wahrscheinlichkeiten.

Ein Faktor, der in der Realität einen wesentlichen Einfluss auf Prozessabläufe hat, ist der Zeitfaktor. In der konventionellen Fehler- und Ereignisbaumanalyse kann der Zeitfaktor jedoch nur unzureichend berücksichtigt werden. Im obigen Beispiel hängt der Erfolg der Handmaßnahme zur Durchsatzerhöhung der Pumpen von verschiedenen zeitlichen Einflüssen ab. Einmal vom Zeitpunkt, wann die Notwendigkeit der Bespeisung des RDB mit den RS-Pumpen nach Eintritt des auslösenden Ereignisses erkannt wird. Und zum anderen von der Zeitdauer, wie lange die menschlichen Handlungen zur Durchsatzerhöhung der Pumpen benötigen. D.h. auch wenn die Diagnose innerhalb der ersten 4 h korrekt durchgeführt wird und die Handmaßnahme nicht unterlassen und korrekt durchgeführt wird, können mit gewissen Wahrscheinlichkeiten Situationen eintreten, die auch bei funktionierenden technischen Bedingungen eine Bespeisung des RDB mit den Steuerstabantriebs-Pumpen (RS) nicht ermöglichen. Diese Situationen können z. B. dann auftreten, wenn die Notwendigkeit zur Bespeisung des RDB erst relativ spät erkannt wird und die Ausführung der Handmaßnahmen nach der erst spät getroffenen Diagnose aufgrund von stochastischen Einflussfaktoren relativ lange dauert. Die Ausführungszeiten von Handmaßnahmen und die Zeitdauer, in denen eine Diagnose gestellt wird, sind stochastische Größen, deren Berücksichtigung in der Analyse den beschriebenen Effekt haben könnte.

Derartige Situationen können in einer Fehlerbaumanalyse prinzipiell nicht angemessen berücksichtigt und quantifiziert werden. Obwohl man ansonsten die Konservativität der Abschätzungen in einer PSA betont, begnügt man sich in diesem Fall mit der Annah-

me, dass die Wahrscheinlichkeit der beschriebenen Situation vernachlässigbar klein ist. Ob diese Annahme gerechtfertigt ist, bleibt unsicher, solange diesbezüglich keine Quantifizierung möglich ist.

Die Modellierung im Fall (b) berücksichtigt nicht die Möglichkeit, dass bei gleichzeitigem Funktionieren beider Pumpen, eine bzw. beide eine verminderte Leistung zeigen können und damit eine verminderte Bespeisung des RDB erfolgt. Die Leistungsfähigkeit der Pumpen könnte wiederum vom gegebenen Zustand abhängen, in dem sich das System zur Zeit der Anforderung befindet. Z. B. könnte die Leistungsfähigkeit der Pumpen abnehmen, wenn der Druck oder die Temperatur über einen gewissen Schwellenwert angestiegen ist. Um zu untersuchen, ob und in welchem Ausmaß der RDB mit den geschädigten Pumpen erfolgreich bespeist werden kann und wie sich eine verminderte Leistungsfähigkeit der Pumpen auf die Bespeisung des RDB auswirkt, muss der physikalische Prozess in Wechselwirkung mit dem stochastischen Verhalten der Komponenten berücksichtigt werden.

Außerdem würde eine realistischere Modellierung berücksichtigen, zu welchem Zeitpunkt eine in Betrieb befindliche Pumpe ausfällt und welchen Einfluss der Ausfallzeitpunkt auf das Prozessverhalten hat.

2.1.2 Abhängigkeit der Komponenten-Nichtverfügbarkeit vom Anforderungszeitpunkt des Systems

In diesem Abschnitt wird eine weitere Vereinfachung in der Fehlerbaummodellierung angesprochen. Ziel der Fehlerbaumanalyse ist die Ermittlung der Wahrscheinlichkeit, dass ein System bei seiner Anforderung seine Funktion nicht erfüllt (weil das System entweder in dem vor der Anforderung liegenden Zeitraum ausgefallen ist oder spätestens zum Anforderungszeitpunkt ausfällt). Diese Wahrscheinlichkeit wird auch als Nichtverfügbarkeit u des Systems bezeichnet (/FAK 05/).

Die logische Verknüpfung zwischen den Ausfällen von Komponenten und dem Ausfall des Systems wird über die Strukturfunktion beschrieben, die aus einer Summe von Minimalschnitten besteht. Als Minimalschnitt („minimal cut set“) eines Systems bezeichnet man eine Kombination von Komponenten, deren gemeinsamer Ausfall einen Systemausfall zur Folge hat.

Um die Nichtverfügbarkeit eines Systems zu ermitteln, müssen für alle Komponenten, die das System beschreiben und die im Fehlerbaum modelliert sind, entsprechende Nichtverfügbarkeiten (Zuverlässigkeitskenngrößen) ermittelt werden, die jeweils das stochastische Ausfallverhalten der entsprechenden Komponenten beschreiben. Dies sind im Falle unabhängiger Komponenten:

- die Ausfallwahrscheinlichkeit p pro Anforderung und
- die Ausfallrate λ pro Zeiteinheit.

Die Ausfallwahrscheinlichkeit p pro Anforderung ist die Nichtverfügbarkeit einer Komponente bei ihrer Anforderung und kann somit direkt in den Fehlerbaum eingehen. Das Standard-Wahrscheinlichkeitsmodell zur Ermittlung der Ausfallwahrscheinlichkeit pro Anforderung basiert auf der Annahme einer Binomialverteilung für die Anzahl der Ausfälle. Die Binomialverteilung impliziert die folgenden Annahmen:

1. Bei jeder Anforderung tritt ein Ausfall mit der Wahrscheinlichkeit p ein. p ist für alle Anforderungen identisch.
2. Ausfälle zu unterschiedlichen Anforderungszeitpunkten sind statistisch unabhängig, d.h. die Ausfallwahrscheinlichkeit p wird nicht beeinflusst durch das Komponentenverhalten zu früheren Anforderungszeitpunkten.
3. Die Anzahl der Ausfälle bezieht sich auf eine feste vorgegebene Anzahl von Anforderungen.

Liegt für eine Komponente die Ausfallrate λ vor, so muss die Nichtverfügbarkeit der Komponente erst ermittelt werden. Die Ausfallrate λ ist keine Ausfallwahrscheinlichkeit, sondern sie ist der Parameter einer Exponentialverteilung E(λ), die das stochastische Ausfallverhalten der Komponente über die Zeit modelliert. Über die Exponentialverteilung E(λ) = 1-exp(-$\lambda\Delta$t)kann die Wahrscheinlichkeit berechnet werden, dass eine Komponente mit der Ausfallrate λ in einem gewissen Zeitintervall ($\Delta t = t_2 - t_1$) $t_2 \geq t_1$ ausfällt. Verschiedene Eigenschaften der Exponentialverteilung wurden bereits in Abschnitt 2.1.1 diskutiert.

Während des ungestörten Leistungsbetriebs befinden sich die meisten Sicherheitssysteme in Bereitschaftsstellung („stand-by“-Zustand). Da eine Störung in einem Bereitschaftssystem nicht zwangsläufig entdeckt wird, werden wiederkehrende Prüfungen bzgl. der Komponenten des Systems durchgeführt, um die Funktionsfähigkeit des Sys-

tems sicherzustellen. Die wiederkehrenden Prüfungen werden in regelmäßigen Zeitabständen und nach einer Prozedur durchgeführt, die im Prüfhandbuch festgelegt ist. Die zeitlichen Abstände, in denen die wiederkehrenden Prüfungen stattfinden, werden durch das Testintervall T_I spezifiziert. Unter Verwendung des gegebenen Testintervalls T_I und der Annahme, dass nach Durchführung einer Funktionsprüfung bzw. Instandsetzung (falls erforderlich) die Komponente wieder als neuwertig und fehlerfrei betrachtet wird, wird in der Regel von folgender Überlegung bei der Berechnung der Nichtverfügbarkeit einer Komponente mit der Ausfallrate λ ausgegangen.

Unmittelbar nach einem Funktionstest, ist die Komponente so gut wie neu und praktisch am Beginn ihrer Lebenszeit t_0. Der nächste Funktionstest erfolgt in einem Zeitabstand von T_I zum Zeitpunkt $t_1 = t_0 + T_I$. Die Nichtverfügbarkeit einer Komponente zum Zeitpunkt t wird berechnet durch $u(t) = 1-\exp(-\lambda(t - t_0))$ mit $t_0 < t \leq t_1$. Da die Komponente zu jedem beliebigen Zeitpunkt zwischen t_0 und t_1 zufällig angefordert werden kann, muss für den Fehlerbaum festgelegt werden, bzgl. welchen Zeitpunkts t die Nichtverfügbarkeit der Komponente zu ermitteln ist. Im Allgemeinen wird die mittlere Nichtverfügbarkeit im Fehlerbaum verwendet. Die mittlere Nichtverfügbarkeit einer Komponente über das Testintervall TI = t1 - t0 wird berechnet durch:

$$\bar{u}(T_I) = \frac{1}{T_I}\int_0^{T_I} 1-\exp(-\lambda T_I)\ dt = 1 - \frac{1}{\lambda \cdot T_I}(1-\exp(-\lambda \cdot T_I)) \qquad (1)$$

Wenn $\lambda \cdot T_I << 1$ (d.h. wesentlich kleiner als 1) ist, kann die mittlere Nichtverfügbarkeit durch $\bar{u}(T_I) \approx \frac{\lambda \cdot T_I}{2}$ approximiert werden. Dies entspricht in etwa der Nichtverfügbarkeit einer Komponente zu einem Anforderungszeit, der in der Mitte des Testintervalls bei $\frac{t_1 - t_0}{2} = T_I / 2$ liegt.

Grundsätzlich werden die mittleren Nicht-Verfügbarkeiten aller Komponenten bestimmt, die zur Beschreibung des Systems in das Fehlerbaum-Modell eingehen. D.h., für jede Komponente, deren Ausfallverhalten durch eine Ausfallrate λ gegeben ist, wird die mittlere Nichtverfügbarkeit in Abhängigkeit ihres Testintervalls und ihrer Ausfallrate gemäß

Gleichung (1) oder durch ihre Approximation $\bar{u}(T_I) \approx \frac{\lambda \cdot T_I}{2}$ bestimmt. Die Nichtverfügbarkeit des Systems ist dann eine Funktion der mittleren Nichtverfügbarkeiten der das System beschreibenden Komponenten.

Tatsächlich entspricht dies jedoch nicht ganz den realen Gegebenheiten. In Wirklichkeit ist die Nichtverfügbarkeit einer Komponente, deren Ausfallverhalten durch eine Ausfallrate pro Zeiteinheit spezifiziert wird, abhängig von dem Zeitpunkt, wann das System bzw. die Komponente angefordert wird. Geht man davon aus, dass Komponenten im Allgemeinen unterschiedliche Testintervalle haben, so impliziert die Abhängigkeit der Komponenten-Nichtverfügbarkeit vom Anforderungszeitpunkt, dass für einige Komponenten der Anforderungszeitpunkt am Ende ihres Testintervalls liegt und für andere Komponenten am Anfang ihres Testintervalls. Eine Abschätzung darüber, ob die mittlere Nichtverfügbarkeit des Systems, die sich als Funktion der mittleren Nichtverfügbarkeiten der das System beschreibenden Komponenten ergibt, eine gute Annäherung der tatsächlichen Verhältnisse darstellt, kann nur erfolgen, indem die Nichtverfügbarkeit der Systemkomponenten als zeitabhängige Größe explizit berücksichtigt wird.

2.1.2.1 Anwendungsbeispiel

Zur Veranschaulichung, welchen Einfluss die vereinfachende Fehlerbaummodellierung auf das Ergebnis der Nichtverfügbarkeit eines Systems haben kann, soll folgendes Beispiel dienen:

Aus dem in Abschnitt 2.1.1 aufgeführten Zitat aus der PSA zu KKP 1 /LIN 06/ ist ein Ausfall der RDB-Bespeisung mit den Steuerstabantriebs-Pumpen (RS) dann gegeben, wenn beide RS-Pumpen ausfallen. Die beiden RS-Pumpen sind nicht verfügbar, wenn:

- die vor Eintritt des auslösenden Ereignisses in Betrieb befindliche Pumpe RS11D102 nicht wieder startet oder
- im Betrieb innerhalb einer Anforderungszeit von 24 h ausfällt oder
- die Schmierölversorgung versagt

und

- die Umschaltautomatik ausfällt oder
- die Pumpe RS21D102 nicht startet oder
- im Betrieb innerhalb einer Anforderungszeit von 24 h ausfällt oder
- die Schmierölversorgung versagt.

Folgende Zuverlässigkeitskenngrößen seien für die oben genannten Ereignisse gegeben (zu Demonstrationszwecken werden hier nur fiktive Werte verwendet):

Ausfallrate der in Betrieb befindlichen Pumpe RS11D102: $\lambda_{1,Betrieb}$ = 8,91 E-06 / h

Ausfallrate der in Betrieb befindlichen Pumpe RS21D102: $\lambda_{2,Betrieb}$ = 8,91 E-06 / h

Pumpe RS11D102 startet nicht: $\lambda_{1,start}$ = 2,13 E-05 / h $T_{I,1start}$ = 336 h

Pumpe RS21D102 startet nicht: $\lambda_{2,start}$ = 2,13 E-05 / h $T_{I,2start}$ = 336 h

Umschaltautomatik fällt aus: $\lambda_{Schalter}$ = 1,0 E-05 / h $T_{I,Schalter}$ = 672 h

Schmierölversorgung fällt aus: $\lambda_{Öl}$ = 4,4 E-06 / h $T_{I,Öl}$ = 4.380 h.

Die beiden redundanten Pumpen werden wöchentlich versetzt getestet, so dass für jede Pumpe ein Testintervall von 2 Wochen $T_{I,1} = T_{I,2}$ = 336 h gegeben ist. Die Umschaltautomatik wird monatlich und die Schmierölversorgung halbjährlich getestet.

In der Fehlerbaumanalyse wird üblicherweise die mittlere Nichtverfügbarkeit für die jeweiligen Komponenten nach Gleichung (1) bzw. über deren Approximation $\bar{u}(T_I) \approx \frac{\lambda \cdot T_I}{2}$ bestimmt. Da für die Komponenten die Bedingung $\lambda \cdot T_I$ << 1 gegeben ist, werden für das Beispiel die mittleren Nichtverfügbarkeiten über die Approximation abgeschätzt. Damit ergeben sich für die Komponenten die folgenden mittleren Nichtverfügbarkeiten:

Mittlere Nichtverfügbarkeit der Pumpen wegen Startversagen:

$p_{1,start} = p_{2,start}$ ~ 3,58 E-03

Mittlere Nichtverfügbarkeit der Umschaltautomatik : $p_{schalter}$ ~ 3,36 E-03

Mittlere Nichtverfügbarkeit der Schmierölversorgung : $p_{Öl}$ ~ 9,6 E-03

Wahrscheinlichkeit, dass Pumpe RS11D102 bzw. RS21D102 innerhalb von 24 h ausfallen, wenn sie in Betrieb sind: $p_{1,Betrieb} = p_{2,Betrieb}$ ~ 2,14 E-04

Unter der Annahme, dass bei Anforderung der RDB-Bespeisung mit den Steuerstabantriebs-Pumpen die Pumpe RS11D102 bereits läuft, berechnet sich nach obiger Beschreibung und den gegebenen Zuverlässigkeitskenngrößen die Wahrscheinlichkeit dass beide RS Pumpen ausfallen durch:

P(beide RS-Pumpen ausgefallen)

$= (p_{1,Betrieb} + p_{Öl}) * (p_{schalter} + p_{2,start} + p_{2,Betrieb} + p_{Öl})$

= (2,14 E-04 + 9,6 E-03) * (3,36 E-03 + 3,58 E-03 + 2,14 E-04 + 9,6 E-03)

= 9,814 E-03 * 1,675 E-02

= 1,644 E-04 (3)

Die mittleren Nichtverfügbarkeiten wurden hier gemäß der allgemeinen Vorgehensweise in einer Fehlerbaumanalyse so bestimmt, als würden die jeweiligen Komponenten jeweils in der Hälfte ihres Testintervalls angefordert.

In den folgenden Ausführungen soll beschrieben werden, worin die Vereinfachung in der Fehlerbaum-Modellierung besteht und es soll gezeigt werden, welchen Einfluss diese Vereinfachungen auf das Ergebnis der System-Nichtverfügbarkeit haben können. Die Nichtverfügbarkeit einer Komponente zum Zeitpunkt t wird berechnet durch $u(t) = 1-\exp(-\lambda t)$.

Der Zeitpunkt, wann ein System und damit die zu dem System gehörenden Komponenten angefordert werden, ist zufällig. Durch den zufälligen Anforderungszeitpunkt des Systems, durch die Zeitabhängigkeit der Nichtverfügbarkeit und durch die unterschiedlichen Testintervalle der Komponenten, die außerdem zum Teil durch ein versetztes Testen charakterisiert sein können, ergeben sich im Allgemeinen Nichtverfügbarkeiten für die einzelnen Komponenten und für das System, die durch die übliche Vorgehensweise der Fehlerbaumanalyse nur unzureichend abgeschätzt werden können. Zur Veranschaulichung sind in **Abb. 2-1** die Testintervalle der jeweiligen Komponenten sowie verschiedene Anforderungszeitpunkte des Systems im Verhältnis zu den jeweiligen Testintervallen dargestellt. Es ist zu beachten, dass die beiden RS-Pumpen jeweils im Abstand von 2 Wochen, jedoch wöchentlich versetzt getestet werden. Die wöchentlich versetzten Testzeitpunkte der beiden Pumpen ist in Abb.2-1

durch die Angaben P1 und P2 gekennzeichnet, zu denen jeweils Pumpe 1 und Pumpe 2 getestet werden.

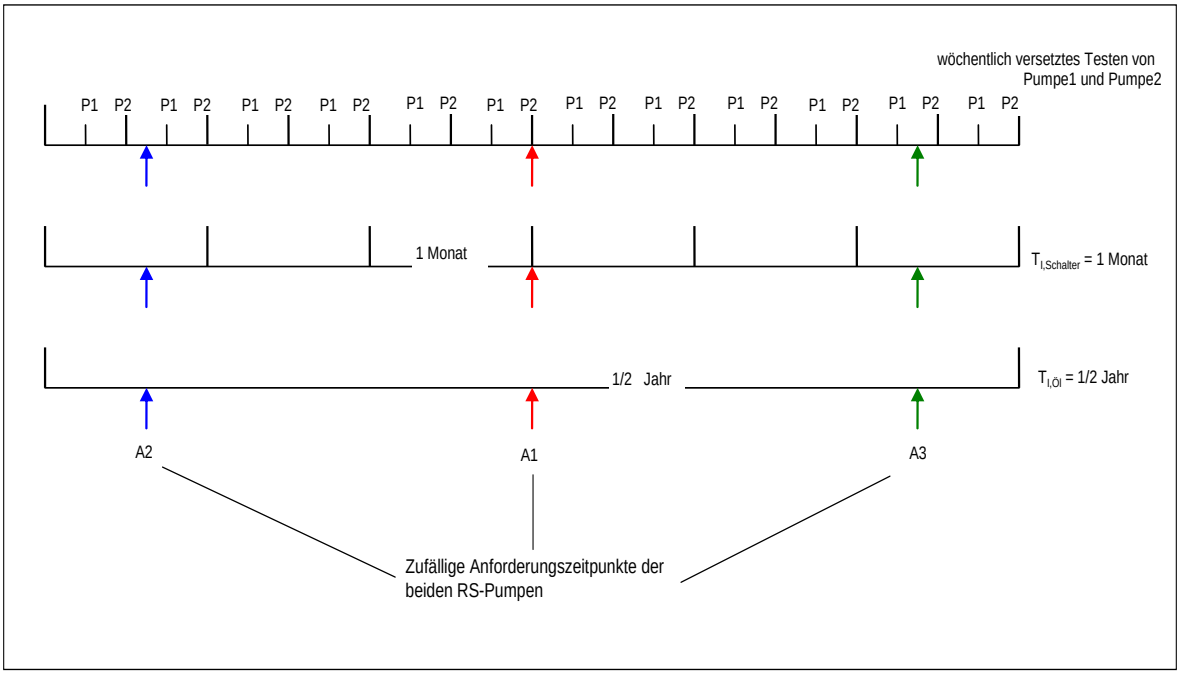

Abb. 2-1 Testintervalle der RS-Pumpen, der Umschaltautomatik und der Schmierölversorgung und zufällige Anforderungszeitpunkte des Systems

In Abb.2-1 tritt der Anforderungszeitpunkt A1 ungefähr nach einem Viertel Jahr ein und liegt in der Mitte des Testintervalls der Schmierölversorgung. Entsprechend der Schmierölversorgung liegt der zufällige Anforderungszeitpunkt A1 für die Pumpe 1 ebenfalls ungefähr in der Mitte des Testintervalls, so dass die Nichtverfügbarkeit der Pumpe 1 und der Schmierölversorgung für diesen Anforderungszeitpunkt der mittleren Nichtverfügbarkeit entsprechen würde. Der Anforderungszeitpunkt A1 fällt ungefähr mit dem Testzeitpunkt des Schalters und dem Testzeitpunkt der Pumpe 2 zusammen. D.h. wenn die Tests dieser beiden Komponenten gerade stattgefunden haben, so befinden sie sich zum Anforderungszeitpunkt A1 in einem fast neuwertigen Zustand und die Nichtverfügbarkeit wäre in diesem Falle für beide Komponenten sehr gering. Wenn die Tests noch nicht stattgefunden haben und gerade bevorstehen, wären die Nichtverfügbarkeiten für den Schalter und die Pumpe 2 nahe an ihren jeweiligen maximalen Nichtverfügbarkeiten.

Der Anforderungszeitpunkt A3 liegt ziemlich am Ende des Testintervalls $T_{I,Öl}$, so dass die Nichtverfügbarkeit der Schmierölversorgung für diesen Anforderungszeitpunkt auf jeden Fall größer als die mittlere Nichtverfügbarkeit $p_{Öl}$ wäre. In Abb.2-1 ist zu erkennen, dass die Nichtverfügbarkeit der Pumpe 2 für den Anforderungszeitpunkt A3 ebenfalls größer als ihre mittlere Nichtverfügbarkeit wäre, während die Nichtverfügbarkeiten des Schalters und der Pumpe 1 etwas geringer als ihre mittleren Nichtverfügbarkeiten wären.

Für den Anforderungszeitpunkt A2 wären die tatsächlichen Nichtverfügbarkeiten von Pumpe 1 und Schalter jeweils etwas größer und die von Pumpe 2 etwas kleiner als ihre jeweiligen mittleren Nichtverfügbarkeiten. Ein relativ großer Unterschied stellt sich für die Nichtverfügbarkeit der Schmierölversorgung ein, die für den Anforderungszeitpunkt A2 deutlich kleiner als ihre mittlere Nichtverfügbarkeit ist.

Die drei verschiedenen Anforderungszeitpunkte in dem relativ einfachen Beispiel zeigen bereits, dass für einen zufällig auftretenden Anforderungszeitpunkt des Systems die Nichtverfügbarkeit des Systems nicht der System-Nichtverfügbarkeit entspricht, die wie in der Fehlerbaumanalyse üblich, über die mittleren Nichtverfügbarkeiten der beteiligten Komponenten berechnet wird. Bei der praktizierten Vorgehensweise in der Fehlerbaumanalyse wird jedoch angenommen, dass die System-Nichtverfügbarkeit, die unabhängig vom Anforderungszeitpunkt des Systems über die mittleren Nichtverfügbarkeiten der Komponenten ermittelt werden, hinreichend genau approximiert wird.

Eine Quantifizierung des Einflusses der vereinfachenden Annahme der Fehlerbaum-Modellierung auf das Ergebnis der System-Nichtverfügbarkeit kann dadurch erfolgen, dass das Ergebnis des Fehlerbaum-Modells mit den Ergebnissen verglichen wird, die sich aus realitätsnäheren Modellierungen ergeben. Eine solche realitätsnähere Modellierung würde z. B. darin bestehen, die Abhängigkeit der Komponenten-Nichtverfügbarkeiten vom zufälligen Anforderungszeitpunkt des Systems und deren Auswirkung auf die System-Nichtverfügbarkeit explizit im Modell zu berücksichtigen.

Unter Verwendung des oben beschriebenen Beispiels soll im Folgenden untersucht werden, wie sich die Berücksichtigung des Anforderungszeitpunktes des Systems (T_{demand}) auf die Ausfallwahrscheinlichkeit (Nichtverfügbarkeit) des Systems auswirkt. In Abhängigkeit des Anforderungszeitpunktes T_{demand} wurden die entsprechenden Nich-

tverfügbarkeiten der Komponenten bzgl. ihrer Testintervalle T_I (s. Abb.2-1) berechnet durch

$$1. - \exp(-\lambda \cdot (T_{demand} \text{ Modulo } T_I)).$$

Da Pumpe 1 und Pumpe 2 wöchentlich versetzt getestet werden, wurde das Startversagen der Pumpe 1 durch

$1. - \exp(-\lambda_{1,start}((T_{demand} - 168) \text{ Modulo } T_{I,1start}))$ für $T_{demand} > 168$ berechnet.

Die Modulo-Berechnung wird verwendet um die Nichtverfügbarkeit beim Anforderungszeitpunkt in Bezug auf den Zeitpunkt des zuletzt durchgeführten Tests zu bestimmen. Wenn das System zufällig zum Zeitpunkt T_{demand} = 1494 h angefordert wird, ergeben sich beispielsweise folgende Nichtverfügbarkeiten für die jeweiligen Komponenten:

- Wahrscheinlichkeit, dass Pumpe RS11D102 (= Pumpe 1) bei T_{demand} = 1494 h nicht verfügbar ist unter Berücksichtigung des wöchentlich versetzten Testens zwischen den Pumpen:
  $1-\exp(-\lambda_{1,start} * ((1494 - 168) \text{ Modulo } 336)) = 1-\exp(- 2{,}13 \text{ E-05} *318) = 6{,}75 \text{ E-03}$
- Wahrscheinlichkeit, dass Pumpe RS21D102 (= Pumpe 2) bei 1.494 h nicht verfügbar ist:
  $1 - \exp(-\lambda_{2,start} * (1494 \text{ Modulo } 336)) = 1- \exp(- 2{,}13 \text{ E-05} *150) = 3{,}19 \text{ E-03}$
- Wahrscheinlichkeit, dass Umschaltautomatik ausgefallen ist :
  $1 - \exp(-\lambda_{Schalter} * (1494 \text{ h Modulo } 672 \text{ h})) = 1 – \exp(- 1{,}0 \text{ E-05} * 150) = 1{,}5 \text{ E-03}$
- Wahrscheinlichkeit, dass Schmierölversorgung ausgefallen ist :
  $1- \exp(- \lambda_{Öl} * (1494 \text{ h Modulo } 4380 \text{ h})) = 1 - \exp(- 4{,}4 \text{ E-06} * 1494) = 6{,}55 \text{ E-03}$

Gemäß der oben beschriebenen Ausfalllogik ergibt sich bei einem Anforderungszeitpunkt von T_{demand} = 1494 h eine Nichtverfügbarkeit des Systems von 7,75 E-05 (s. Abb. 2-2). Wenn das System zufällig zum Zeitpunk T_{demand} = 3962 h angefordert wird, beträgt die Nichtverfügbarkeit des Systems 5,1 E-04 (s. Abb. 2-2).

Mit dem in der Fehlerbaumanalyse üblichen Vorgehen würde sich eine mittlere Nichtverfügbarkeit des Systems von 1,644 E-04 ergeben.

In Abb. 2-2 ist die Nichtverfügbarkeit des Systems als Funktion der Zeit dargestellt. Die in der Abbildung dargestellte rote (gestrichelte) Linie weist die mittlere Nichtverfügbarkeit des Systems (1,644 E-04) aus, wie sie im Fehlerbaum ermittelt wird. Obwohl es

sich um ein relativ einfaches System handelt, ist aus **Abb. 2-2** zu erkennen, dass die Nichtverfügbarkeit des Systems in Abhängigkeit des Zeitpunktes, wann das System angefordert wird, sehr stark variiert und eine Abhängigkeitsstruktur aufweist, die durch das Ergebnis des Fehlerbaum-Modells (rote Linie) kaum zufriedenstellend erfasst wird.

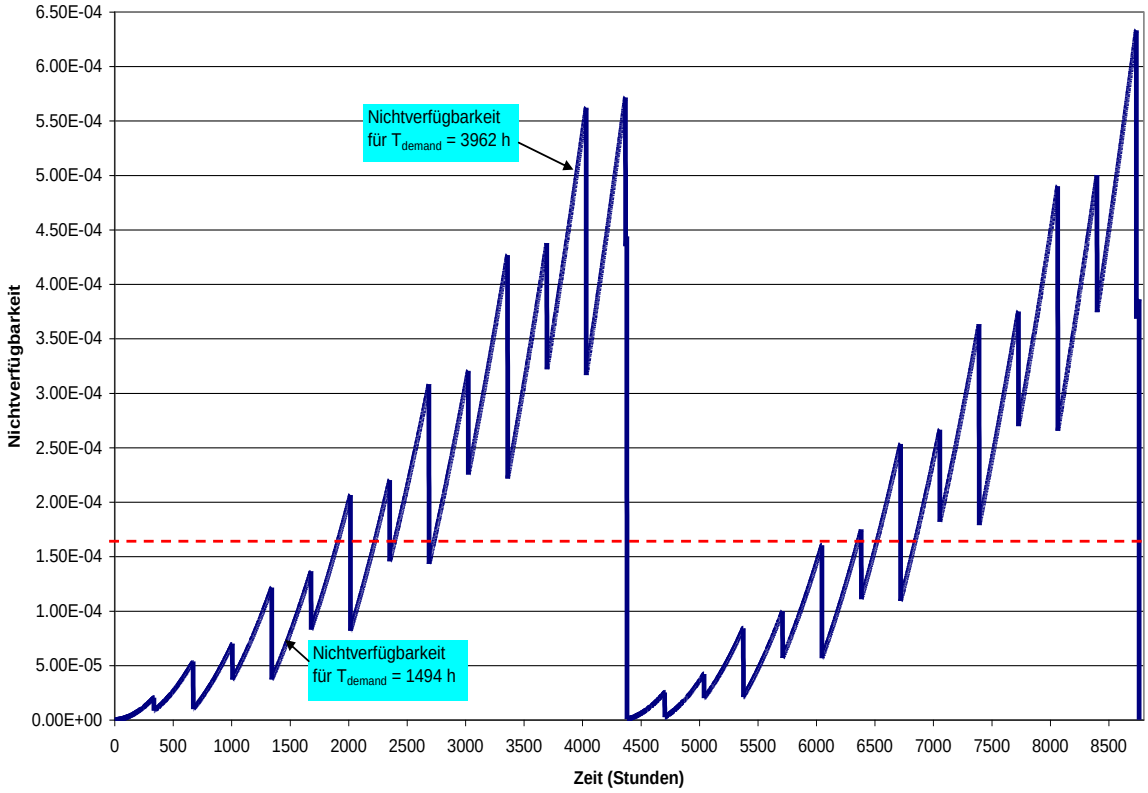

Abb. 2-2 Nichtverfügbarkeit des Systems als Funktion der Zeit

Aus Abbildung 2-2 wird deutlich, dass die durch das Fehlerbaum-Modell ermittelte Nichtverfügbarkeit des Systems nur eine sehr unvollständige und ungenaue Beschreibung der tatsächlichen Verhältnisse erlaubt. So lassen sich große Zeitbereiche angeben, in denen die Nichtverfügbarkeit des Systems ausschließlich kleiner (bzw. ausschließlich größer) ist als die durch das Fehlerbaum-Modell ermittelte Nichtverfügbarkeit des Systems. So sind beispielsweise in den Zeitbereichen von 1 h – 1900 h und 4381 h - 6350 h die Nichtverfügbarkeiten des Systems ausschließlich kleiner und zum großen Teil sogar erheblich kleiner als die durch die konventionell berechnete mittlere Nichtverfügbarkeit des Systems. In den Zeitbereichen von 2740 h – 4380 h und 6860 h – 8760 h sind die Nichtverfügbarkeiten ausschließlich größer und zu einem nicht unerheblichen Teil sogar mehr als um einen Faktor 2 größer die konventionell berechnete mittlere Nichtverfügbarkeit des Systems.

Die mittlere Nichtverfügbarkeit des Beispielsystems beträgt 1,95 E-04 im Vergleich zum Wert 1,644 E-04, der in der konventionellen Fehlerbaumanalyse berechnet wird. D.h., die konventionelle Berechnung führt zu einer Unterschätzung von ca. 20 % der tatsächlichen mittleren Nichtverfügbarkeit des Systems. Das Anwendungsbeispiel soll deutlich machen, dass durch die Verwendung der mittleren Nichtverfügbarkeiten wesentliche Abhängigkeiten und Eigenschaften des Systems nicht berücksichtigt werden und erhebliche Fehleinschätzungen möglich sind, die sich schließlich auch auf das PSA-Ergebnis auswirken können.

Zur Quantifizierung, mit welcher Wahrscheinlichkeit die durch die konventionelle Berechnung ermittelte mittlere Nichtverfügbarkeit des Systems (1,644 E-04) über- bzw. unterschritten wird, zeigt **Abb. 2-3** die kumulierten Wahrscheinlichkeiten für die Nichtverfügbarkeiten, die sich über einen Zeitraum von einem Jahr für das Beispielsystem ergeben.

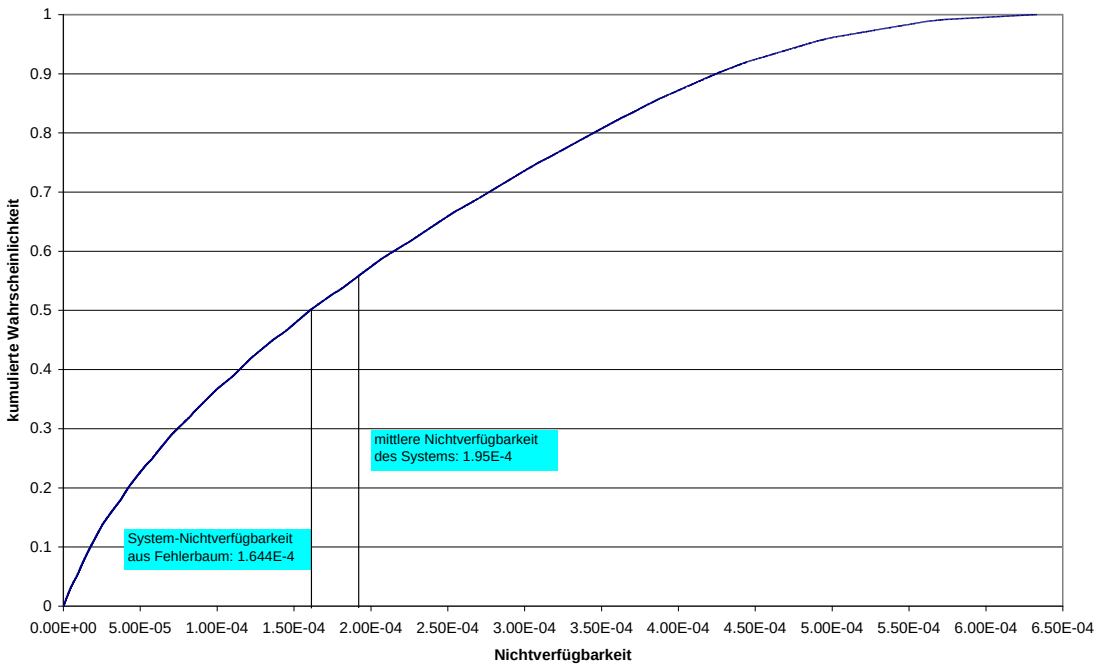

Abb. 2-3 Verteilung der Nichtverfügbarkeit des Systems

Aus der Verteilung der System-Nichtverfügbarkeiten in Abb. 2-3 können verschiedene Aussagen abgeleitet werden, die einen ungefähren Eindruck von der Größenordnung des Fehlers geben, der bzgl. des Beispielsystems gemacht wird, wenn die Zeitabhängigkeit der Nichtverfügbarkeit nicht berücksichtigt wird.

Lediglich 35 % der Nichtverfügbarkeiten des System, die sich im Verlauf eines Jahres ergeben, liegen innerhalb eines Genauigkeitsbereichs von +/- 50 % der konventionell berechneten Nichtverfügbarkeit von 1,644 E-04. Der Anteil der System-Nichtverfügbarkeiten, der größer als das 1,5-fache (bzw. 2-fache) des Schätzwertes aus der Fehlerbaumberechnung sind, beträgt ca. 34 % (bzw. ca. 22 %). Der Anteil der System-Nichtverfügbarkeiten, der kleiner als das 2-fache (bzw. 4-fache) des Schätzwertes der Fehlerbaumanalyse ist, beträgt ca. 30,6 % (bzw. ca. 18 %).

Das Anwendungsbeispiel hat gezeigt, dass durch die Abhängigkeit der System-Nichtverfügbarkeit vom zufälligen Anforderungszeitpunkt des Systems eine erhebliche Variation bzgl. der System-Nichtverfügbarkeit existiert, die bisher nicht berücksichtigt wird. Die Kenntnis dieser Variation wäre jedoch wichtig, um Aussagen darüber machen zu können, welchen Einfluss die Variation der zeitabhängigen System-Nichtverfügbarkeiten auf das PSA-Ergebnis hat.

Ein Vergleich mit Analysen, die den Zeitfaktor explizit berücksichtigen, kann Aufschluss darüber geben, wie das Ergebnis der konventionellen Analyse, die auf einer vereinfachten Modellierung ohne Berücksichtigung der Zeitabhängigkeit basiert, einzuordnen und (mit einem Korrekturterm) zu korrigieren ist, um ein realistischeres Ergebnis zu erhalten.

2.1.3 Vorschlag eines methodischen Verfahrens zur Quantifizierung des Einflusses vereinfachender Annahmen in Fehlerbaumanalysen auf PSA-Ergebnisse.

Generell kann die Qualität eines probabilistischen Ergebnisses im Wesentlichen nur durch die Qualität des zugrundeliegenden Modells, aus dem die Wahrscheinlichkeitswerte hervorgehen, abgeschätzt werden. Deshalb ist davon auszugehen, dass die Ergebnisse probabilistischer Modelle umso glaubwürdiger sind, je genauer die realen Gegebenheiten durch das zugrundeliegende Modell abgebildet werden können.

Aus den diskutierten Beispielen in Abschnitt 2.1.1 und 2.1.2 wird deutlich, dass aufgrund der den Fehlerbaummodellen zugrunde liegenden vereinfachenden Annahmen wichtige Aspekte der realen Gegebenheiten – wie z. B. zeitliche Abhängigkeiten der Nichtverfügbarkeit der Komponenten vom Anforderungszeitpunkt des Systems - nicht modelliert werden können. Diese versucht man teilweise durch mehr oder weniger gro-

be Abschätzungen und Vereinfachungen – z. B. mittlere Nichtverfügbarkeiten - in den Fehlerbaum einzubinden. Andere Aspekte, wie z. B. Alterungsprozesse oder Wechselwirkungsprozesse von menschlichen Eingriffen und Systemverhalten, werden nicht modelliert.

Die Berücksichtigung der Kenntnisstandunsicherheit bzgl. der in einen Fehlerbaum eingehenden Zuverlässigkeitskenngrößen ist mittlerweile Stand von Wissenschaft und Technik. Aber nicht nur die Kenntnisstandunsicherheiten bzgl. der Zuverlässigkeitskenngrößen tragen zur Unsicherheit in PSA-Ergebnissen bei. Unsicherheiten in PSA-Ergebnissen können sich zusätzlich auch durch unterschiedliche Modellformulierungen ergeben, in denen beispielsweise zusätzliche Einflussfaktoren berücksichtigt oder wichtige Abhängigkeiten und gegenseitige Wechselwirkungsprozesse genauer modelliert werden.

Die in Abschnitt 2.1.1 und 2.1.2 diskutierten Beispiele haben verdeutlicht, dass in einem realen System komplexe Wechselwirkungen im zeitlichen Verlauf stattfinden, in denen sich der System- und Prozesszustand auf stochastische Größen und umgekehrt stochastische Ereignisse Einfluss auf den weiteren Prozessverlauf haben können. Entsprechend müssten für eine möglichst realistische Modellierung menschliche Handlungsabläufe als dynamische Prozesse betrachtet werden, die sich in gegenseitiger Abhängigkeit von technischen Komponenten, physikalischen Prozessgrößen und stochastischen Ereignissen im zeitlichen Verlauf entwickeln. Mit den konventionellen Methoden der PSA ist eine solche Modellierung nicht möglich. Seit jüngster Zeit stehen Methoden zur Verfügung (z. B. die in der GRS entwickelte Methode MCDET /HOF 01/ und das Crew-Modul /PES 06/), mit denen diese komplexen dynamischen Wechselwirkungen realitätsnah modelliert werden können.

Die Frage, welche Auswirkungen genauere bzw. verfeinerte Modellierungen auf die Ergebnisse einer PSA haben, konnte bisher nicht beantwortet werden. Mit den Entwicklungen fortschrittlicher Methoden wären solche Untersuchungen und Analysen grundsätzlich möglich.

Ein systematischer Ansatz zu einer möglichen Quantifizierung dieses Einflusses könnte aus folgendem Vorgehen bestehen:

1. Auswahl relevanter Teilsysteme, die bereits durch einen Fehlerbaum im Rahmen einer PSA modelliert worden sind.

2. Berücksichtigung relevanter Einflussgrößen, die im Fehlerbaum nicht oder nur vereinfacht dargestellt werden (z. B. Zeitabhängigkeit der Nichtverfügbarkeiten, Wechselwirkungen zwischen menschlichem Handeln und Systemverhalten etc.)

3. Modellierung der spezifizierten zusätzlichen Einflussgrößen unter Verwendung der neu entwickelten Methoden zur dynamischen PSA.

4. Vergleich und Diskussion der Ergebnisse, die sich aus der konventionellen Fehlerbaummodellierung und aus den Methoden zur dynamischen PSA ergeben.

Zeigt sich in dem Vergleich, dass der Einfluss der unterschiedlichen Modellierungen erheblich sein kann, so wäre zu untersuchen, ob eine Weiterentwicklung der bestehenden Fehlerbaummethode (z. B. Kopplung von Fehlerbaum und Markov-Prozessen) den Anforderungen einer realistischeren Modellierung entsprechen kann oder ob dynamische Methoden für bestimmte Fragestellungen die konventionellen Methoden ergänzen sollten. Zumindest könnten derartige Vergleichsrechnungen einen ersten Hinweis darauf geben, welchen Einfluss die vereinfachten Annahmen des Fehlerbaummodells auf die Schätzung der Systemzuverlässigkeiten haben.

Mit dem Ziel der Weiterentwicklung der Unsicherheitsanalyse, kann eine generelle Abschätzung der Unsicherheiten aus der Fehlerbaummodellierung nur durch Erfahrungswerte aus solchen Vergleichsrechnungen gewonnen werden. Bisher konnten solche Untersuchungen aufgrund Mangels der entsprechenden Methoden nicht durchgeführt werden. Mit der Entwicklung fortschrittlicher Methoden sind diesbezügliche Untersuchungen möglich geworden und können dazu beitragen, wesentliche Erkenntnisse auf dem Gebiet der Unsicherheitsanalyse zu erhalten.

Es sei an dieser Stelle ausdrücklich betont, dass sich die konventionellen PSA-Methoden der Fehler und Ereignisbaumanalyse als sehr nützlich und praktikabel erwiesen haben. Es wird hier keineswegs die Meinung vertreten, dass diese bewährten Methoden durch dynamische Analysen vollständig ersetzt werden könnten. Allerdings sollten fortschrittliche dynamische Methoden verstärkt eingesetzt werden, um gewisse Teilbereiche einer PSA, bei denen die konventionellen Methoden offensichtlich an ihre Grenzen stoßen, zu modellieren. Mit dem Einsatz dieser Methoden könnten erste Erfahrungen und Aussagen darüber gewonnen werden, welchen Einfluss vereinfachte Modellierungen und grobe Abschätzungen auf PSA-Ergebnisse haben können.

2.2 Ereignisbaumanalyse

Über eine Ereignisbaumanalyse sind diejenigen Ereignisabläufe zu untersuchen, die sich ausgehend vom auslösenden Ereignis in Abhängigkeit von der Verfügbarkeit (Funktion/Ausfall) der zur Beherrschung des Störfalls erforderlichen Systemfunktionen ergeben. Die unterschiedlichen Ereignisabläufe werden in Form von Ereignisablaufdiagrammen dargestellt. Aus den Kombinationen der möglichen Zustände der angeforderten Systemfunktionen (Funktion/Ausfall) ergeben sich ausgehend vom auslösenden Ereignis die verschiedenen Zweige des Ereignisablaufdiagramms.

Zur Ermittlung von Systemschadenszuständen werden diejenigen Systemfunktionen in den Ereignisabläufen ermittelt, die zur Beherrschung des Ereignisablaufs vorgesehen sind und angefordert werden. Grundlage dieser Ermittlung sind die Anregekriterien für die Betriebssysteme, für Begrenzungseinrichtungen, für das Reaktorschutzsystem sowie die Kriterien vorgesehener Handmaßnahmen.

Zur Weiterführung der Ereignisabläufe vom Systemschadenszustand zum Kernschadenszustand werden die präventiven Notfall-Systemfunktionen des anlageninternen Notfallschutzes berücksichtigt, die entsprechend dem jeweils vorliegenden Anlagenzustand gemäß Notfallhandbuch (NHB) zur Überführung in einen sicheren Anlagenzustand vorgesehen sind. Neben technischen Auslegungsreserven, zusätzlichen Einrichtungen und Personalhandlungen können hierzu auch Reparaturmaßnahmen zur Wiederherstellung ausgefallener Systemfunktionen einbezogen werden. Grundlagen dazu sind

- die im NHB festgelegten anlageninternen Notfallmaßnahmen mit den jeweiligen fest gelegten Vorbereitungs- und Einleitungskriterien,
- die Kriterien für die zu berücksichtigenden Reparaturmaßnahmen sowie
- die bei den einzelnen Ereignisabläufen vorliegenden systemtechnischen und physikalischen Zustände.

2.2.1 Unsicherheiten in den Ergebnissen aus Störfallsimulationen

Für die im Ereignisbaum und entsprechend im Fehlerbaum zu berücksichtigenden Systemfunktionen und präventiven Notfall-Systemfunktionen sind die jeweiligen Mindestanforderungen zu bestimmen. Die Mindestanforderungen sind vom jeweils vorliegenden Ereignisablauf abhängig und betreffen

- die Anzahl der erforderlichen Systeme bzw. Teilsysteme sowie
- deren Anforderungszeitpunkte und Einsatzzeiten

die zur Beherrschung des Störfalls notwendig sind.

Ferner sind die Zeiten zu ermitteln, die für die Durchführung von Handmaßnahmen zur Verfügung stehen. Die Zeiten sind vom jeweiligen Betriebszustand und von den jeweils vorherrschenden Prozessbedingungen abhängig.

Mindestanforderungen für Systemfunktionen bzw. die zur Verfügung stehende Zeit für menschliche Maßnahmen werden anhand von Störfallsimulationen mit entsprechenden Thermohydraulik-Codes ermittelt. In der GRS wird dazu der ATHLET-Code verwendet. Bisher wurden Störfallsimulationen lediglich als Punktwertrechnungen durchgeführt. D.h., alle Eingabeparameter des Thermohydraulik-Codes wurden durch einen festen Wert spezifiziert, was zur Folge hat, dass man auch nur einen bestimmten Punktwert als Ergebnis erhält. Unsicherheiten in Eingabeparametern, die sich durch das Thermohydraulikmodell fortpflanzen und zu Unsicherheiten in den Ergebnissen führen, wurden bisher nicht berücksichtigt. Weitere Unsicherheiten in den Thermohydraulik-Codes sind die sogenannten Modellunsicherheiten, d.h. die Unsicherheiten bzgl. der verwendeten Sub-Modelle. Auf die Problematik von Parameter- und Modell-Unsicherheiten in Thermohydraulik-Codes und ihre Auswirkung auf die PSA-Ergebnisse wird in Kapitel 4 ausführlich eingegangen.

Generell muss davon ausgegangen werden, dass die in Störfallsimulationen ermittelten Mindestanforderungen für Systemfunktionen mit Unsicherheiten behaftet sind. Dies wird beispielsweise durch die Aussage in /LIN 06/ bzgl. des mittleren Lecks innerhalb des Sicherheitsbehälters deutlich:

„…. Die automatische Druckentlastung ist ausreichend wirksam, wenn eins von sieben S/E-Ventilen öffnet. (Basis-PSA: zwei von sieben S/E-Ventilen). Die Bespeisung mit RS (Systemfunktion RS) bei Ereignisabläufen mit Ausfall des Durchdringungsabschlusses in einer der Frischdampfleitungen RA11-41 wird im Unterschied zur Basis-PSA als wirksam erachtet (in der Basis-PSA wird RS mit der Wahrscheinlichkeit P = 1 als ausgefallen bzw. nicht wirksam unterstellt). Der Ausfall der Rückförderung des Wassers vom SHB-Sumpf in die Kondensationskammer (Systemfunktionen X, X1) führt nach den Ergebnissen der thermohydraulischen Rechnungen der GRS nicht ohne weiteres zum Gefährdungs- bzw. Kernschadenszustand. Die Modellierung in der Basis-PSA wird als pessimistisch erachtet, wurde jedoch aufgrund der geringen numerischen Relevanz für das Gesamtergebnis nicht modifiziert."

Allein aus diesem Textabschnitt, der beispielhaft für viele andere ist, wird deutlich, dass in Abhängigkeit von Thermohydraulik-Rechenergebnissen und unterschiedlichen Experteneinschätzungen die Ereignisbaum-Modellierung in einer PSA unter anderen Annahmen und Voraussetzungen erfolgen kann. Die in der Basis-PSA zugrunde gelegten Mindestanforderungen an die Systemfunktionen wurden von der Firma Siemens mit dem Rechenprogramm SAFE ermittelt, das nach Einschätzung der GRS zu pessimistischen Ergebnissen für die maximal erreichten Hüllrohrtemperaturen führt. Für die in /LIN 06/ beschriebene PSA wurden die entsprechenden Berechnungen mit dem ATHLET-Code durchgeführt.

Generell sollten in den Störfallsimulationen die potentiell wichtigen Parameter- und Modell-Unsicherheiten in dem verwendeten Thermohydraulik-Code berücksichtigt werden. Die Unsicherheiten, die sich bzgl. der ermittelten Mindestanforderungen ergeben, sind im weiteren Vorgehen der PSA konsistent in der Fehler- und Ereignisbaummodellierung zu berücksichtigen (siehe Kapitel 4).

2.2.2 Unsicherheiten bzgl. der Vollständigkeit des zugrundeliegenden Modells (Completeness Uncertainty)

Ein weiterer Gesichtspunkt, der im Rahmen der Ereignisablaufanalyse einer PSA der Stufe 1 (und insbesondere der Stufe 2) hinsichtlich Modellunsicherheiten zu diskutieren ist, bezieht sich auf die Frage, wie genau bzw. realitätsnah die in einer Anlage ablaufenden komplexen, dynamischen Prozesse mit den herkömmlichen Methoden modelliert werden können und wie die damit berechneten PSA-Ergebnisse zu bewerten sind.

Die Ereignisbaum-Analyse für die Stufe 1 einer PSA geht von einer Abfolge von Systemfunktionen und menschlichen Eingriffen aus, die zur Beherrschung eines Unfalls angefordert werden. Das stochastische Verhalten von Systemfunktionen bzw. menschlicher Handlungen wird in der Regel durch 2 Ereignisausprägungen beschrieben. Dies sind Verfügbarkeit bzw. Nichtverfügbarkeit bei Anforderung von Systemfunktionen und erfolgreiche bzw. nicht erfolgreiche Durchführung menschlicher Handlungen.

Der Einfluss des Zeitfaktors bei funktionalen Abhängigkeiten (z. B. wie lange funktionieren erfolgreich gestartete Systemkomponenten bis sie infolge des Einflusses sich verändernder Belastungen ausfallen), oder die zeitlichen Abhängigkeiten bei der Durchführung menschlicher Handlungen, bleiben in der Regel unberücksichtigt. Auch wird im Allgemeinen nicht in Betracht gezogen, dass Systemfunktionen, die bei ihrer Anforderung verfügbar sind, im Laufe ihrer Betriebszeit aufgrund zufälliger Einflüsse nur noch eingeschränkt ihre Funktion erfüllen oder sogar ausfallen können. Sowohl die eingeschränkte Funktionsfähigkeit als auch der zufällige Ausfall einer erfolgreich angeforderten Systemfunktion können den Ereignisablauf gravierend verändern und die Häufigkeiten von Schadenszuständen entsprechend erhöhen.

Die Modellierung der Ablaufmöglichkeiten eines Unfallszenarios durch einen Ereignisbaum ist prinzipiell statischer Natur. D.h., die Analysten geben die zu betrachtenden Ereignisse in ihrer Reihenfolge ohne Angabe von Zeitpunkten und zeitlichen Abständen vor. Die Analyse erfolgt damit entlang einer sogenannten Wirkungslinie ohne Zeitachse. Daraus ergeben sich mehr oder weniger einschneidende Einschränkungen hinsichtlich der Berücksichtigung der im zeitlichen Ablauf stattfindenden Wechselwirkungen zwischen der Dynamik des Anlagenverhaltens, der Dynamik der Personalhandlungen und den zufälligen Einflussfaktoren. Eine realitätsnahe Modellierung dieser Wechselwirkungen ist mit der konventionellen Ereignisbaumanalyse nicht möglich.

Gegenwärtig beschränkt sich die Charakterisierung und Bewertung bei den vielen möglichen Ereignisabläufen auf ein sehr grobes Raster in der Zeit (z. B. Spannungswiederkehr früher oder später als 2 h nach einem Station-Black-Out oder **früh**, **spät** oder **vor**, **nach**), im Ort (z. B. **oben**, **unten**), im Betrag (z. B. **klein**, **mittel**, **groß**), etc. Für die diskreten Klassen des Rasters wird dabei jeweils ein repräsentativer Wert spezifiziert, der dann zusammen mit den anderen Werten die Randbedingungen definiert, unter denen die Unfallabläufe durchgeführt werden. Als Konsequenz ergibt sich daraus, dass z. B. die Zeit, die in vielen realen Prozessen ein wesentlicher Einflussfaktor

ist, in der konventionellen Ereignisbaumanalyse - wenn überhaupt -, nur sehr grob und ungenau berücksichtigt werden kann.

Die Einschränkungen in der herkömmlichen Ereignisablaufanalyse bergen die Gefahr in sich, dass

- wichtige Zusammenhänge unerkannt und damit unberücksichtigt bleiben;
- wichtige Abläufe, die sich gerade aus Details in Ort, Zeit, Betrag und Reihenfolge von Ereignissen ergeben, nicht erkannt werden;
- unrealistische Abläufe generiert werden, weil Bedingungen vom Experten nach subjektiver Einschätzung und unter vereinfachenden Annahmen vorgegeben werden müssen, die sich bei einer realitätsnahen Modellierung möglicherweise nicht ergeben würden.

In jüngster Zeit wird immer häufiger auf die Bedeutung der Wechselwirkungen zwischen Prozessgrößen, menschlichen Handlungen, technischen Komponenten und stochastischen Einflussfaktoren sowie auf den besonderen Einfluss zeitlicher Effekte bei der Analyse komplexer Systeme hingewiesen, z. B. /SIU 94/, /LAB 00/, /COJ 96/. Eine im Rahmen einer PSA durchgeführte zeitabhängige Analyse unter expliziter Berücksichtigung relevanter Dynamik-Stochastik Wechselwirkungen, wird auch als dynamische PSA bezeichnet. Andere Bezeichnungen, die man in diesem Zusammenhang in der einschlägigen Literatur findet, sind „probabilistische Dynamikanalyse“ (probabilistic dynamics analysis) oder „dynamische Zuverlässigkeitsanalyse“ (dynamic reliability analysis).

Fortschrittliche Methoden zur Durchführung einer probabilistischen Dynamikanalyse - z. B. die in der GRS entwickelte Methode MCDET (**M**onte **C**arlo **D**ynamic **E**vent **T**ree) /HOF 01/ in Verbindung mit dem Crew-Modul /PES 06/ - ermöglichen eine Analyse, die die Dynamik-Stochastik Wechselwirkungen im zeitlichen Verlauf realitätsnah berücksichtigt. Stochastischen Einflüssen unterworfen sind z. B. Umgebungsbedingungen, Auswirkungen von Phänomenen, das Ausfallverhalten von Komponenten und Systemen oder die Handlungen der Bedienmannschaft. Durch das in der GRS entwickelte Crew-Modul und dessen Kopplung an das Stochastik-Modul von MCDET kann der Handlungsablauf des Personals als eigener dynamischer Prozess analysiert werden, der sich im zeitlichen Ablauf parallel zur System- und Prozessdynamik entwickelt. Zusätzlich können die stochastischen Einflussfaktoren zeitnah berücksichtigt werden.

Bei der Anwendung der Methoden der probabilistischen Dynamikanalyse entwickeln sich die Unfallabläufe automatisch entlang der Zeitachse in Abhängigkeit von den Dynamik-Stochastik Wechselwirkungen. Diese Modellierung entspricht damit eher dem realen Entstehungsprozess eines Unfallablaufs als die in der konventionellen Ereignisbaumanalyse durch den Experten subjektiv festgelegte Reihenfolge der für den Unfallablauf wichtigen Ereignisse.

Im Gegensatz zu den Methoden der probabilistischen Dynamik erfolgt die klassische Fehler- und Ereignisbaum-Analyse ohne direkte Kopplung an die Prozess- und Systemdynamik, die mittels deterministischer Rechencodes simuliert wird. Wenige als abdeckend beurteilte Unfallsimulationen stellen die einzige Verbindung zur Prozess- und Systemdynamik her. Eine Folge davon ist, dass zum einen die Auswirkungen des Zufallgeschehens auf den Prozessverlauf nicht zeitnah und nur unvollständig erfasst werden, und zum anderen die unmittelbaren Auswirkungen der Prozess- und Systemdynamik sowohl auf das (zufällige) Ausfallverhalten technischer Komponenten als auch auf die Zuverlässigkeit menschlicher Handlungen nicht modelliert werden kann.

Das oftmals vorgetragene Argument, dass die im Rahmen einer PSA der Stufe 1 berücksichtigten Ereignisabläufe im wesentlichen nur durch die Verfügbarkeit von Systemfunktionen bestimmt werden und deshalb keine relevanten Wechselwirkungen zwischen Personalhandlungen und System- und Prozessdynamik auftreten, womit sich eine probabilistische Dynamikanalyse erübrigen würde, kann anhand einfacher Überlegungen widerlegt werden. In /LIN 06/ Abschnitt 4.2.2.7 wird beispielsweise folgende Situation zum Schließen der S/E-Ventile nach dem Öffnen (″DB3″) beschrieben:

„…Eine Rechnung zum „Ausfall Hauptwärmesenke“ zeigt, dass bei einem DDA der Frischdampfleitungen und Hilfsdampfleitung alle acht Entlastungsvorsteuerventile (EV1 bis EV3) und die zugehörigen S/E-Ventile einmal kurzzeitig öffnen (vgl. Rechnung Nr.20 in /STE 04/). In diesem Fall müssen also acht von acht Magnetvorsteuerventile und acht von acht S/E-Hauptventile schließen. Die Anforderungen an das Schließen der S/E-Ventile beim ″Notstromfall″ werden von der GRS analog zu denen ″beim Ausfall Hauptwärmesenke eingeschätzt….″

Angesichts dieser Aussage stellt sich die Frage, welche Druckverhältnisse sich in Abhängigkeit davon einstellen, ob und wie viele der geöffneten Ventile wieder schließen bzw. mit einer zufälligen zeitlichen Verzögerung schließen und welche Auswirkungen

dies auf den weiteren Prozessablauf hat. Es ist davon auszugehen, dass der Druck umso schneller sinkt, je mehr Ventile offen versagen bzw. erst mit einer zeitlichen Verzögerung wieder geschlossen werden können. Diese verschiedenen Druckverhältnisse können in ihrer zeitlichen Entwicklung wiederum Maßnahmen bewirken, z. B. menschliche Eingriffe, die dann früher oder später eingeleitet werden und die dementsprechend zu anderen Abläufen der Prozessdynamik und insgesamt zu anderen Störfall-Abläufen führen können.

Generell bewirken die einen Ereignisablauf beeinflussenden Zufallsereignisse, dass sich vielfältige unterschiedliche Prozessbedingungen zu zufälligen Zeitpunkten einstellen können. Das hat zur Folge, dass sich eine Vielzahl unterschiedlicher Störfall- bzw. Unfallabläufe gemäß ihrer jeweiligen Eintrittswahrscheinlichkeiten ergeben. Eine Bewertung von Schadenshäufigkeiten wird prinzipiell umso genauer und zuverlässiger, wenn möglichst viele Abläufe, die sich durch die Dynamik-Stochastik Wechselwirkungen ergeben, in der Analyse berücksichtigt werden und auf möglichst viele vereinfachende Annahmen verzichtet wird.

Fazit:

Die klassischen PSA-Methoden der Fehler- und Ereignisbaumanalyse und die Methoden der probabilistischen Dynamikanalyse sind unterschiedliche Modellierungsansätze zur Analyse von komplexen dynamischen Systemen. Die probabilistische Dynamikanalyse kann komplexe dynamische Prozess- und Systemabläufe ohne grobe vereinfachende Annahmen modellieren und simulieren. Bei der klassischen Fehler- und Ereignisbaumanalyse ist man gezwungen, eine Reihe verschiedener Vereinfachungen und grober Abschätzungen durchzuführen, deren Auswirkungen auf die Ergebnisse der PSA bisher nicht beurteilt werden konnten.

Durch die Anwendung sowohl konventioneller als auch dynamischer Methoden auf das gleiche System könnte erstmals eine quantitative Abschätzung der Modellunsicherheiten (completeness uncertainties) durchgeführt werden, die sich durch die notwendigen vereinfachenden Annahmen und relativ groben Abschätzungen im Rahmen der klassischen Fehler- und Ereignisbaumanalyse ergeben. Mit den neu entwickelten Methoden der probabilistischen Dynamikanalyse stehen somit erstmals Werkzeuge zur Verfügung, die eine Validierung der bisher verwendeten klassischen Methoden ermöglichen.

3 Unsicherheiten bei der Zuverlässigkeitsanalyse von Personalhandlungen

In der konventionellen PSA werden Personalhandlungen (Handmaßnahmen) als Basisereignisse in die Ereignis- und Fehlerbaum-Analysen eingebunden. Dabei werden diejenigen Personalhandlungen berücksichtigt, die für das zu analysierende System bzw. für den Unfallablauf als bedeutend eingestuft werden.

Die Bewertung der Zuverlässigkeit von Personalhandlungen macht überwiegend von so genannten HRA-Bäumen (HRA = **H**uman **R**eliability **A**nalysis) als Analysewerkzeug Gebrauch. Basis eines HRA-Baums ist eine Abfolge von Teilaufgaben (Handlungsschritten), die die Erfolgsaussichten der jeweiligen Handmaßnahme beeinflussen.

Für die Verzweigungspunkte des HRA-Baums müssen die entsprechenden Wahrscheinlichkeiten menschlicher Fehler (HEP - Human Error Probability) ermittelt werden. In der Literatur sind eine Vielzahl unterschiedlicher Verfahren zur Bestimmung der HEP vorgestellt worden, die jeweils mehr oder weniger Bedeutung bei der Durchführung einer PSA erlangt haben. Im Methodenband zur PSA /FAK 05/ werden die international bewährten HRA -Verfahren ASEP (Accident Sequence Evaluation Program) /SWA 87/ zur gröberen Abschätzung und THERP (Technique of Human Error Rate Prediction) /SWA 83/ zur feineren Abschätzung der Fehlerwahrscheinlichkeiten empfohlen.

Im Folgenden werden Quellen von Modellunsicherheiten bzgl. der Quantifizierung von Zuverlässigkeitskenngrößen menschlicher Handlungen diskutiert. Es werden Möglichkeiten besprochen, ob und ggf. wie die Modellunsicherheiten in einer PSA quantifiziert und berücksichtigt werden könnten. Zur Quantifizierung und Berücksichtigung von Modellunsicherheiten im Rahmen der menschlichen Zuverlässigkeitsanalyse liegen bisher keine Methoden und Untersuchungen vor. Deshalb dürfen die nachfolgenden Ausführungen dieses Kapitels lediglich als ein erster Versuch betrachtet werden, das Methodengerüst zur Berücksichtigung von Unsicherheiten im Rahmen der menschlichen Zuverlässigkeitsanalyse zu erweitern.

3.1 Unsicherheiten aufgrund alternativer Modelle zur Schätzung menschlicher Fehlerwahrscheinlichkeiten

Die erste Quelle, aus denen sich potentielle Modellunsicherheiten ergeben, besteht allein in der Existenz verschiedener Methoden mit denen Zuverlässigkeitskennwerte für Personalhandlungen ermittelt werden und dem Detaillierungsgrad, mit dem die menschlichen Handlungen modelliert werden.

Aufgrund praktischer Überlegungen (Zeit- und Kostenaufwand) werden Modellunsicherheiten, die sich anhand unterschiedlicher alternativer Modelle zur Ermittlung menschlicher Zuverlässigkeitskenngrößen ergeben, nicht berücksichtigt. Deshalb erscheinen insbesondere Bestrebungen begrüßenswert, deren Ziel darin besteht, eine Standardisierung der bestehenden HRA-Methoden herbeizuführen um vergleichbare Ergebnisse von Bewertungen der menschlichen Zuverlässigkeit zu erhalten, wenn es sich um ähnliche Handlungsabläufe in vergleichbaren Anlagen handelt. Eine solche Initiative wurde z. B. mit der im Jahr 2000 gegründeten EPRI HRA Users Group /JUL 06/ gestartet.

3.2 Verteilungsannahmen zur Beschreibung der Unsicherheiten von Wahrscheinlichkeiten menschlicher Fehlhandlungen

Die HEP-Schätzwerte werden in THERP bzw. ASEP als Medianwerte einer Log-Normalverteilung betrachtet, die die Kenntnisunsicherheit bzgl. der Fehlerwahrscheinlichkeit ausdrückt. Die ungestutzte Log-Normalverteilung stellt keine geeignete Vereilung dar, um die Kenntnisunsicherheiten bzgl. der Wahrscheinlichkeiten zu beschreiben, da sie abhängig von ihren Parametern auch Wahrscheinlichkeiten größer als 1 ermöglicht.

Dies kann an folgendem kleinen Beispiel leicht veranschaulicht werden: Sei beispielsweise für eine Fehlerwahrscheinlichkeit einer menschlichen Handlung ein HEP-Schätzwert von 0.09 mit einem Fehlerfaktor von 8 angegeben, dann würden sich bei Verwendung der Log-Normalverteilung folgende Quantile ergeben:

5 %-Quantil: 9,44 E-03

50 %-Quantil: 0,075

95 %-Quantil: 0,596

99 %-Quantil: 1,407

Aus den oben angegebenen Quantilen der Log-Normalverteilung, die die Unsicherheit bei einem gegebenen HEP-Schätzwert von 0,09 mit einem Fehlerfaktor von 8 beschreibt, ist zu erkennen, dass das 99 %-Quantil der Verteilung einen Wert von 1,407 aufweist. Da die Log-Normalverteilung die Unsicherheiten bzgl. der HEP-Schätzung ausdrückt, wird z. B. im Rahmen einer Unsicherheitsanalyse mit einer Wahrscheinlichkeit von ca. 2 % ein HEP-Wert ausgespielt, der größer als 1 ist.

Um diese Schwachstelle bei Verwendung der Log-Normalverteilung zu vermeiden, kann eine Stutzung der Log-Normalverteilung im Wert 1 durchgeführt. Die Stutzung der Log-Normalverteilung in 1 - d.h. Ausschluss aller Verteilungswerte, die größer als 1 sind – hat zur Folge, dass sich wesentliche Kennwerte (z. B. Erwartungswert, Median oder Standardabweichung) ändern und nicht mehr den Werten der Ausgangsverteilung entsprechen.

Aus den oben genannten Gründen muss die Log-Normalverteilung insgesamt als ungeeignet dafür betrachtet werden, die Unsicherheiten bzgl. der Wahrscheinlichkeiten menschlicher Fehler auszudrücken. Eine besser geeignete Verteilung zu diesem Zweck wäre z. B. die Standard-Beta-Verteilung, weil sie genau über den Bereich zwischen 0 und 1 definiert ist.

3.3 Modellunsicherheiten aufgrund der Vollständigkeit (completeness) des verwendeten Modells

Analog zur üblichen Ereignisbaumanalyse gibt ein HRA-Baum eine Wirkungslinie wieder, die weitgehend unabhängig von der Zeitachse ist. Die Wirkungslinie ist das Ergebnis einer Analyse der Auswirkungen von Erfolg und Misserfolg durchzuführender Handlungsschritte einer Handmaßnahme. Der Bezug auf eine Wirkungslinie schließt nicht aus, dass zur Herleitung von Zuverlässigkeitskenngrößen menschlicher Handlungen ein Zeitbudget für die Erledigung der durchzuführenden Handlung benötigt wird. Das Zeitbudget ist die zur Verfügung stehende Zeit für die Diagnose des Problems und die durchzuführenden Handlungen. Eine Abschätzung dieses Zeitfensters, das als eine wichtige Größe zur Ermittlung der Diagnosewahrscheinlichkeit verwendet wird, erfolgt nur sehr grob aufgrund weniger als abdeckend beurteilten Simulationsrechnungen.

Das ermittelte Zeitfenster wird zur Bestimmung der Wahrscheinlichkeit verwendet, mit der die Diagnose, die zur Entscheidung einer Initiierung der Handlungsmaßnahme führt, im gegebenen Zeitrahmen durchgeführt wird. Der gegebene Zeitrahmen, in der die Diagnose durchgeführt werden muss, setzt sich aus der Differenz des gesamten Zeitbudgets und einer mittleren Zeitdauer zusammen, die zur Durchführung der Handlungsschritte benötigt wird. Eine fehlerhafte Diagnose bedeutet in diesem Zusammenhang, dass die Zeit zum Erstellen der Diagnose den gegebenen Zeitrahmen (d.h. gesamtes Zeitbudget – Zeitdauer zur Durchführung der Handlungen) überschreitet.

Wechselbeziehungen zwischen Personalhandlungen und Prozessgeschehen werden grob abgeschätzt durch das aus Simulationsrechnungen ermittelte Zeitfenster für Diagnose und Handmaßnahmen sowie durch die Abschätzungen der mittleren Ausführungszeiten der Handmaßnahmen und der leistungsbeeinflussenden Faktoren (sog. Performance Shaping Factors). Die Angaben zu leistungsbeeinflussenden Faktoren und Zeitbudgets werden zur Quantifizierung der Wahrscheinlichkeit verwendet, mit der eine Personalhandlung (Handmaßnahme) nicht erfolgreich durchgeführt wird. Die Ermittlung der Fehlerwahrscheinlichkeit basiert dabei auf der Logik des HRA-Baums und den jeweiligen Wahrscheinlichkeiten (inklusive der Diagnosewahrscheinlichkeit), mit der die mehr oder weniger grob zusammengefassten Handlungsschritte der Personalhandlung unterlassen oder fehlerhaft durchgeführt werden. Die Fehlerwahrscheinlichkeit findet schließlich im jeweiligen Ereignisbaum als Verzweigungswahrscheinlichkeit oder als Wahrscheinlichkeit des entsprechenden Basisereignisses in einem Fehlerbaum Verwendung, analog zur Wahrscheinlichkeit für das Versagen eines angeforderten Systems.

Ein Nachteil der konventionellen Zuverlässigkeitsanalyse menschlicher Handlungen im Rahmen einer PSA ist, dass sie weitgehend abgekoppelt von der Analyse des physikalisch-technischen Prozesses durchgeführt wird. In der Realität finden die im Rahmen einer PSA berücksichtigten menschliche Handlungen jedoch im Wechselspiel mit dem Systemverhalten, dem physikalischem Prozess und den zufälligen Einflussfaktoren statt. D.h., menschliche Handlungen, Systemkomponenten, Prozessgrößen und stochastische Ereignisse müssen als sich gegenseitig beeinflussende Teile eines Gesamtsystems (Mensch-Maschine-System) betrachtet werden, das sich im zeitlichen Ablauf entwickelt.

Um die Wechselwirkungen menschlicher Handlungen mit der System- und Prozessdynamik und den zufälligen Einflussfaktoren realistischer modellieren zu können, müssen folgende Tatsachen berücksichtigt werden:

- Die Handlung eines Operateurs benötigt eine gewisse Zeit, um durchgeführt zu werden. Die Ausführungszeiten menschlicher Handlungen sind dabei als Zufallsgrößen zu betrachten, da die Zeitdauern zur Durchführung derselben Handlung mehr oder weniger stark variieren können. Die zufällig variierenden Ausführungszeiten von Handlungen haben einen Einfluss auf den weiteren Prozessablauf.

- Menschliche Handlungen werden durch ein Team von Individuen durchgeführt, die miteinander kommunizieren und deren Handlungen von den Handlungen der anderen Operateure abhängen.

- Es gibt Handlungen, die parallel durchgeführt werden können, und Handlungen, die erst beginnen können, wenn eine bestimmte Bedingung erfüllt ist. Diese Bedingungen können durch einen bestimmten Zustand von Prozessgrößen gegeben sein (z. B. Temperatur > 310° C etc.) oder aber durch die erfolgreiche/nicht erfolgreiche Beendigung einer Aufgabe.

- Der Prozessverlauf kann die nachfolgenden Handlungen der Operateure und die Zuverlässigkeit der durchzuführenden Handlungen beeinflussen (wenn z. B. während der Durchführung einer Tätigkeit ein bestimmter kritischer Anlagenzustand erreicht wird, der die Unterbrechung der aktuellen Tätigkeit zur Folge hat und die Durchführung einer anderen Tätigkeit verlangt). Des Weiteren können kritische Prozesszustände den Stresslevel der Operateure erhöhen, was eine Erhöhung der Fehlerwahrscheinlichkeiten bei der Durchführung verschiedener Handlungen zur Folge haben kann. Handlungsbeeinflussende Faktoren, wie z. B. der Stresslevel der Operateure, sind dynamische Größen, die von der Prozess- und Systemdynamik abhängen und die umgekehrt über die Zuverlässigkeit der menschlichen Handlungen Einfluss auf die Prozess- und Systemdynamik haben.

- Zwischen menschlichen Handlungen, Systemkomponenten, Prozessgrößen und stochastischen Ereignissen finden zahlreiche Wechselwirkungen im zeitlichen Ablauf statt. Beispielsweise haben Handlungen, die eine Änderung des Zustands einer Systemkomponente bewirken, aber auch Unterlassungen von Handlungen einen unmittelbaren Einfluss auf den weiteren Prozessablauf, der umgekehrt aber auch einen Einfluss auf den weiteren Handlungsablauf hat. Zu berücksichtigen

sind zusätzliche zufällige Einflussfaktoren, die sowohl den Ablauf der menschlichen Handlungen als auch die Prozess- und Systemdynamik betreffen können.

Mit der konventionellen Methodik der Zuverlässigkeitsanalyse menschlicher Handlungen ist man gezwungen, eine Reihe von Vereinfachungen und grober Abschätzungen durchzuführen, wobei die oben erwähnten Aspekte der zeitlich ablaufenden Wechselwirkungen – wenn überhaupt – nur sehr grob und unvollständig berücksichtigt werden können. Es stellt sich deshalb die Frage, wie genau man die Zuverlässigkeit menschlicher Handlungen im Rahmen eines komplexen dynamischen Systems mit den konventionellen Methoden überhaupt modellieren kann und wie sich die Einschränkungen der Modellierungsmöglichkeiten auf die PSA-Ergebnisse auswirken. Eine diesbezügliche Quantifizierung konnte bisher noch nicht durchgeführt werden, weil die notwendigen Methoden nicht zur Verfügung standen.

Im Rahmen eines vom BMWi unterstützten Forschungsvorhabens (RS 1148) wurde in der GRS ein Modul (Crew-Modul) /PES 06/ entwickelt, das die Handlungen des Personals als einen eigenen dynamischen Prozess simuliert, der sich parallel zur System- und Prozessdynamik entwickelt und in Verbindung mit der MCDET-Methodik /HOF 01/ die Wechselwirkungen zwischen Komponentenverhalten, physikalischen Prozess, menschlichen Handlungen und stochastischen Einflüssen zeitnah berücksichtigt. Mit den entwickelten Methoden zur Durchführung probabilistischer Dynamikanalysen können Handlungsabläufe des Personals realitätsnah analysiert werden.

Ein Vergleich von Ergebnissen aus Zuverlässigkeitsanalysen von Personalhandlungen, die sowohl mit den klassischen Methoden als auch mit einer probabilistischen Dynamikanalyse durchgeführt werden, könnten eine Einschätzung darüber liefern, welche Unsicherheiten sich aufgrund der unterschiedlichen Modellierungen ergeben und welche Möglichkeiten die jeweiligen Methoden liefern, zusätzliche Detailaussagen aus den Analysen abzuleiten.

Die nachfolgende Diskussion der Maßnahme zur Durchführung einer intermittierenden RDB-Bespeisung mit dem TH-System bei Transienten oder Lecks außerhalb des SHB's vor Folgebruch einer FD-Leitung (siehe /LIN 06/) soll veranschaulichen, welche Wechselwirkungen im Rahmen einer dynamischen Analyse zusätzlich modelliert werden können. In /LIN 06/ heißt es:

"… Nach Eintritt einer Transiente oder eines Lecks außerhalb des Sicherheitsbehälters kann es zur Auslösung des Durchdringungsabschlusses (DDA) kommen (mögliche Anregekriterien „Durchsatz Frischdampfleitung > 120 %“, „Kondensatordruck > 0,8 bar“, „Füllstand RDB < 12 Meter“ oder „Füllstand RDB > 14,92 Meter). Aufgrund der Abtrennung der Hauptwärmesenke hat das Personal die Anlage entsprechend BHB B2.2 „Abfahren der Gesamtanlage ohne Hauptwärmesenke“ abzufahren.

Sind in einer FD-Leitung zwei in Reihe liegende DDA-Armaturen fälschlicherweise offen geblieben, so könnte es zu einem Folgebruch dieser Leitung kommen, wenn der RDB-Füllstand auf 10,5 Meter absinkt und das Reaktorschutzsystem die automatische Druckentlastung und das Niederdruckkernfluten einleitet. Ein solcher Ablauf wird zunächst durch die Systemfunktion „Hochdruckeinspeisung mit TM/TJ“ verhindert. Bei einem Füllstandsabfall auf 12 Meter wird zunächst das TM-System automatisch in Betrieb genommen. Das TJ-System wird erst gestartet, wenn der Füllstand unter 11,75 Meter abfällt. Damit steht dem Personal ausreichend Zeit zur Verfügung um den Füllstand entsprechend folgender Anweisungen des BHB's B 2.2 oberhalb von 10,5 m zu halten:

Absenken des Reaktordrucks von Hand auf 11 bar

Dies kann durch das Zuschalten des TJ-Systems im Mindestmengenbetrieb erfolgen, das dann gemeinsam mit dem TM-System in den RDB einspeist. Steht TJ nicht zur Verfügung, ist die Druckabsenkung zunächst mittels der diversitären Druckbegrenzungsventile vorzunehmen. Nach dem Öffnen der diversitären Druckbegrenzungsventile müssen der RDB-Druck- und Temperaturgradient beobachtet werden. Sind diese Werte zu niedrig, so ist zusätzlich ein S/E-Ventil zu öffnen.

Reaktorfüllstand durch intermittierendes Bespeisen mit TH zwischen 12 Meter und 15 Meter halten

Während der Durchführung dieser Handmaßnahme ist darauf zu achten, dass der RDB-Druck auch langfristig unter 11 bar bleibt (Öffnen der diversitären Druckbegrenzungsventile und ggf. eines S/E-Ventils erforderlich). Schließt nach Eintritt des auslösenden Ereignisses ein S/E-Ventil, das zur Begrenzung des Reaktordrucks geöffnet wurde, nicht wieder, so fällt der Reaktordruck über das offene Ventil soweit ab, dass auch direkt auf das intermittierende Bespeisen mit TH übergegangen werden kann.

Entsprechend /TÜV 98/, Abschnitt 6.4, stehen nach Eintritt des auslösenden Ereignisses und verfügbarer Systemfunktion „TM/TJ-Einspeisung“ für die Durchführung der beschriebenen Maßnahmen mindestens 60 Minuten Zeit zur Verfügung. Der mittlere Zeitbedarf aller dem intermittierenden Bespeisen vorausgehenden Handlungen (Nach RESA-Kontrollen, Einstieg in BHB B2.2, RS und TJ Zuschaltung, ggf. Öffnen von Druckentlastungsventilen, TH-Zuschaltung) wurde im Rahmen der hier vorliegenden Untersuchung durch eine Zeitbedarfsanalyse konservativ zu ca. 23 Minuten abgeschätzt. …..″

Aus den Aussagen wird deutlich, dass erhebliche Wechselwirkungen und zeitliche Einflüsse den Ablauf bestimmen. Beispielsweise muss bei der Maßnahme ″Absenken des Reaktordrucks auf 11 bar″ die Druckabsenkung mittels der diversitären Druckbegrenzungsventile durchgeführt werden, wenn das TJ-System nicht zur Verfügung steht. Nach dem Öffnen sind RDB-Druck- und Temperaturgradient zu beobachten. Sind diese Werte zu niedrig, so muss ein weiteres S/E-Ventil geöffnet werden. Aus dieser Beschreibung wird unmittelbar die Wechselbeziehung zwischen Prozess, Systemverhalten, menschlichen Handlungen und zufälligen Einflussfaktoren klar. Durch eine Handlung erfolgt die Zustandsänderung von Systemkomponenten (Öffnen von Druckbegrenzungsventilen). Zufällige Einflussfaktoren bestimmen, ob sich die Komponenten verändern lassen. Dies hat wiederum Auswirkung auf Prozessgrößen (z. B. Änderung des Temperaturgradienten). In Abhängigkeit vom Prozesszustand (Gradienten zu niedrig) ist eine weitere Personalhandlung vorgeschrieben (Öffnen eines zusätzlichen S/E-Ventils), die nicht erforderlich wäre, wenn die Gradienten den Sollwert annehmen. Sind die sich einstellenden Gradienten zu groß, müssen S/E-Ventile wieder geschlossen werden.

Sowohl die Durchführung einer Handlung (z. B. Öffnen von Druckbegrenzungsventilen) als auch das Monitoring des Prozessablaufs und die daraus abzuleitende Entscheidung (z. B. ob ein zusätzliches S/E-Ventil zu öffnen bzw. wieder zu schließen ist), erfordern eine mehr oder weniger lange Zeitspanne, die von zufälligen Einflussfaktoren abhängt.

Dazu folgende Beispiele:

1. Bei der Bestimmung der benötigten Zeitdauer zur Durchführung einer Maßnahme ist zu berücksichtigen, dass z. B. die Handlung ″Öffnen von Druckbegrenzungsventilen″ aus mehreren Einzelaktionen zusammengesetzt ist, die durch stochastische

Einflüsse bestimmt werden. Der Schichtleiter muss die Situation diagnostizieren und eine Entscheidung treffen, was mehr oder weniger Zeit in Anspruch nimmt. Nach der Anweisung durch den Schichtleiter kann der zuständige Operateur das Öffnen durchführen. Es kann aber auch passieren, dass der Operateur auf die Anweisung nicht reagiert. Nach einer gewissen zufälligen Verzögerungszeit kann der Schichtleiter die unterlassene Handlung bemerken und die Anweisung zum Öffnen der S/E-Ventile erneut geben, worauf die Handlung dann durchgeführt wird. Die unterschiedlichen Abläufe, die sich mit bestimmten Wahrscheinlichkeiten einstellen, haben nicht nur einen Effekt darauf, ob die Druckbegrenzungsventile geöffnet werden oder nicht, sondern auch, wann die Ventile geöffnet werden.

2. Nach dem Öffnen der diversitären Druckbegrenzungsventile müssen der RDB-Druck- und Temperaturgradient beobachtet werden. Sind diese Werte zu niedrig, so ist zusätzlich ein S/E-Ventil zu öffnen. Ist eine ausreichende Druckabsenkung erfolgt, müssen Ventile wieder geschlossen werden. Aus dieser Beschreibung wird deutlich, dass die Durchführung einer Handlung (z. B. Öffnen oder Schließen der Druckbegrenzungsventile) vom Zustand physikalischer Prozessgrößen (z. B. Druckabsenkung, Temperaturgradient) abhängen kann und die Ausführung einer Handlung (z. B. Öffnen eines S/E-Ventils) unmittelbaren Einfluss auf Prozessgrößen und dem weiteren Ablauf des Prozesses haben. Des Weiteren ist zu berücksichtigen, dass es durch zufällige Einflussfaktoren vorkommen kann, dass sich Ventile nur mit einem verringerten Querschnitt oder gar nicht öffnen lassen und damit eventuell eine langsamere bzw. nicht ausreichende Druckabsenkung stattfindet. Entsprechend kann es vorkommen, dass sich Ventile nicht mehr oder nicht vollständig schließen lassen, was einen weiteren Druckabfall zur Folge hätte. Es bestehen somit vielfältige gegenseitige Abhängigkeiten zwischen physikalischem Prozess, Systemverhalten, menschlichen Handlungen sowie stochastischen Einflüssen, die eine Vielzahl unterschiedlicher Abläufe zur Folge haben, von denen einige möglicherweise in kritische Zustände laufen können.

Eine wesentliche Schwachstelle der konventionellen Vorgehensweise besteht darin, dass

- menschliche Handlungen und physikalischer Prozess mehr oder weniger abgekoppelt voneinander modelliert werden und deshalb
- die unter (1) und (2i) ausgeführten Wechselwirkungen nur unter vereinfachten Annahmen und groben Abschätzungen durchgeführt werden können.

Eine solche grobe Abschätzung sind beispielsweise die im Zitat aufgeführten Zeitangaben. So stehen nach Eintritt des auslösenden Ereignisses und verfügbarer Systemfunktion ″TM/TJ-Einspeisung″ für die Durchführung der beschriebenen Maßnahmen mindestens 60 Minuten Zeit zur Verfügung. Dies ist offensichtlich keine konservative Aussage, da von der Verfügbarkeit der Systemfunktion ″TM/TJ-Einspeisung″ für die Durchführung der beschriebenen Maßnahmen ausgegangen wird. Das Zeitfenster von 60 Minuten würde sich vermutlich ändern, wenn die TM/TJ-Einspeisung nicht verfügbar oder erst nach einer (zufälligen) Verzögerungszeit erfolgt oder die TM/TJ – Pumpen aufgrund zufälliger Einflussfaktoren lediglich eine kleinere Einspeisemenge fördern können.

Des Weiteren stellt sich die Frage, welche Variationen sich für das zur Verfügung stehende Zeitfenster ergeben, wenn die Modell- und Parameterunsicherheiten im deterministischen Rechencode berücksichtigt werden, der zur Ermittlung des Zeitfensters von 60 Minuten verwendet wurde. Sowohl zufällige Einflüsse im Verhalten technischer Komponenten als auch die Berücksichtigung von Kenntnisstandunsicherheiten im deterministischen Rechencodes können einen nicht unerheblichen Einfluss auf das Zeitfenster haben, das der Schichtmannschaft zur Durchführung ihrer Maßnahme zur Verfügung steht.

Entsprechendes gilt für den mittleren Zeitbedarf aller dem intermittierenden Bespeisen vorausgehenden Handlungen, für die durch eine Zeitbedarfsanalyse konservativ ca. 23 Minuten abgeschätzt wurden. Auch hier wäre es interessant zu untersuchen, welche Zeitverteilung man erhalten würde, wenn man die in (1) erwähnten Aspekte bzgl. möglicher zufälliger Abläufe berücksichtigen würde.

Im Rahmen einer probabilistischen Dynamikanalyse können Abläufe in komplexen Systemen, die aus den Wechselwirkungen zwischen physikalischem Prozess, Systemverhalten, Personalhandlungen und stochastischen Einflussfaktoren resultieren, realitätsnah modelliert und angemessen bewertet werden. Als Beispiel sei die Analyse der Notfallmaßnahme ″Sekundärseitiges Druckentlasten und Bespeisen″ nach Ausfall der Dampferzeugerbespeisung in /PES 06/ genannt.

Mit den Methoden der probabilistischen Dynamikanalyse stehen Werkzeuge zur Verfügung, die eine Validierung der konventionellen Methodik zur Analyse von Personalhandlungen erlauben. Dabei können die Ergebnisse der konventionellen Methodik mit denen verglichen, die man über eine probabilistische Dynamikanalyse erhält. Mit die-

sem Vergleich wäre eine Quantifizierung der Unsicherheit möglich, die eine vereinfachte (und damit unvollständige) Modellierung auf das PSA-Ergebnis hat.

Diese Untersuchungen können an ausgewählten Beispielen ggf. n Nachfolgeprojekten zu diesem Vorhaben durchgeführt werden.

4 Unsicherheit in den Thermohydraulik-Modellergebnissen

Im Rahmen von thermohydraulischen Untersuchungen erfolgt die Bestimmung von Mindestanforderungen

- an die Funktionen der Sicherheits-, ATWS- und Notstandssysteme zur Vermeidung von Systemschadenszuständen,
- an die präventiven Notfallmaßnahmen zur Vermeidung von Kernschadenszuständen sowie
- an die mitigativen Notfallmaßnahmen zur Vermeidung von Anlagenschadenszuständen.

Mindestanforderungen betreffen die Zahl der erforderlichen Sicherheits-, ATWS- und Notstandssysteme, deren Anforderungszeitpunkte und Einsatzzeiten sowie die für Personalhandlungen verfügbaren Zeitfenster.

Die thermohydraulischen Untersuchungen beginnen mit der Bestimmung der Anfangs- und Randbedingungen, die für die zu analysierenden Störfälle in der betreffenden Anlage zugrunde zu legen sind. Dabei werden alle Anlagenzustände in Betracht gezogen, bei denen Systeme des bestimmungsgemäßen Betriebs zur Wärmeabfuhr ausfallen oder nur unzureichend wirksam sind.

Zur Festlegung der Mindestanforderungen an Notfallfunktionen werden diejenigen Bedingungen bestimmt, die vorliegen, wenn auslösende Ereignisse aufgrund des Versagens angeforderter Sicherheitssysteme und des Misslingens von schutzzielorientierten Maßnahmen des Betriebshandbuches nicht beherrscht werden können. Anschließend wird anhand von Modellrechnungen untersucht, welche Mindestanforderungen an die Sicherheits- und Notfallfunktionen gestellt werden müssen, und bis zu welchem Zeitpunkt die Maßnahmen wirksam werden müssen.

Zur Durchführung der Modellrechnungen stehen verschiedene Thermohydraulik- und Integralcodes zur Verfügung, wie z. B. ATHLET, ASTEC oder MELCOR. Wie genau die Ergebnisse der einzelnen Rechenmodelle die Realität widerspiegeln ist unsicher.

4.1 Relevante Unsicherheitsquellen im Thermohydraulik-Modell

Eine Quantifizierung der Unsicherheit von Ergebnissen komplexer Thermohydraulik-Modelle erhält man über eine Unsicherheitsanalyse, wie sie bei der GRS praktiziert wird (vgl. Abschnitt 5.1). Dabei werden Modell- und Parameterunsicherheiten auf der Ebene der Teil-Modelle des komplexen Modells (z. B. Teil-Modelle zur Verdampfung, Kondensation, kritischen Ausströmung oder zum Wärmeübergang) quantifiziert. Bei den Teil-Modellen besteht oft die Möglichkeit, deren Ergebnis-Unsicherheit anhand der Validierungsunterlagen der Modellentwickler zu beurteilen. Der gemeinsame Einfluss der quantifizierten Unsicherheiten in den Teil-Modellen zeigt sich schließlich in der Ergebnis-Unsicherheit des komplexen Modells.

Zur Quantifizierung der Ergebnis-Unsicherheit auf der Ebene der Teil-Modelle gibt es verschiedene Möglichkeiten:

Wenn Messergebnisse und entsprechende Modellnachrechnungen vorliegen, werden Korrekturterme (additiver Term, Korrekturfaktor) angewendet, um das Modellergebnis angemessen zu modifizieren. Da die Messergebnisse i. A. streuen (unter anderem wegen Messfehlern) und in den Teil-Modellen nicht festgelegt ist, welcher Wert aus dem Streubereich für einen Korrekturterm zutreffend ist, ist dieser als unsichere Größe zu berücksichtigen.

Liegen mehrere alternative Teil-Modelle vor, die den wahren Zusammenhang möglicherweise hinreichend genau beschreiben, so sollten alle diejenigen Modelle berücksichtigt werden, mit denen ein Spektrum an hinreichend repräsentativen Ergebniswerten erzielt werden kann. Die Unsicherheit darüber, welches Modell den Zusammenhang am besten abbildet, sollte entsprechend berücksichtigt werden. So kann jedem Modell eine subjektive Wahrscheinlichkeit zugeordnet werden, die den Grad an Vertrauen darüber ausdrückt, wie gut das Modell den wahren Zusammenhang beschreibt. Zusätzlich muss in Betracht gezogen werden, dass jede Modellalternative eigene unsichere Parameter haben kann. Kann der Unterschied zwischen einem Modellergebnis und dem wahren Zusammenhang durch eine Korrektur ausgedrückt werden und die Unsicherheit bzgl. der Korrektur quantifiziert werden, dann genügt es, nur eine Modellalternative zu betrachten.

Zu den relevanten Modellunsicherheiten im Thermohydraulik-Modell zählen die Finite Volumen und Finite Elemente Modelle. Sie geben eine Diskretisierung des Untersu-

chungsgegenstands wie z. B. des Reaktorkühlkreislaufs oder der Sicherheitsbehälterstruktur zum Zwecke der rechentechnischen Handhabung. Die Orts- und Zeitdiskretisierung zur Lösung der zugrunde liegenden partiellen Differentialgleichungen kann einen deutlichen Einfluss auf das Modellergebnis haben.

Zu den relevanten Parameter- bzw. Datenunsicherheiten gehören die Anfangs- und Randbedingungen, die für die zu analysierenden Störfälle in der betreffenden Anlage zugrunde zu legen sind. Je nach Fragestellung der Modellanwendung können die Anfangs- und Randbedingungen entweder fest und ungenau bekannt sein (epistemische Unsicherheit) oder inhärent unsicher aufgrund stochastischer Variabilität (aleatorische Unsicherheit). Der Reaktorzustand nach Störfalleintritt ist im Allgemeinen eine epistemische Unsicherheit. Der Reaktorzustand vor Störfalleintritt ist im Rahmen einer PSA eine aleatorische Unsicherheit.

Aleatorische Unsicherheiten werden in PSA-Aussagen berücksichtigt. Ihretwegen ist die Sicherheitsanalyse probabilistisch. Epistemische Unsicherheiten hingegen bestimmen, wie genau die PSA-Aussagen getroffen werden können.

Zur Analyse der Einzelbeiträge von sowohl epistemischen als auch aleatorischen Unsicherheiten zur Gesamtunsicherheit des Thermohydraulik-Ergebnisses müssen beide Typen von Unsicherheitsquellen gesondert (z. B. in einer zweistufig geschachtelten Monte-Carlo-Simulationsschleife) berücksichtigt werden. Mit einer Sensitivitätsanalyse erhält man unter anderem Aussagen darüber, wo der Kenntnisstand primär zu verbessern ist, um die Unsicherheit im Thermohydraulik-Ergebnis und schließlich auch im PSA-Ergebnis zu reduzieren.

Relevante epistemische Unsicherheitsquellen der thermohydraulischen Analysen sind in **Tab. 4-1** aufgelistet. Die Tabelle enthält Unsicherheitsbeiträge aus Modellformulierungen (wie etwa für Wärmeübergänge oder Verdampfung) und Modellparametern (z. B. Dittus-Boelter Korrelation für die einphasige Konvektion in Wasser).

Tab. 4-1 Relevante epistemische Unsicherheitsquellen in den thermohydraulischen Analysen

Nr.	Unsicherheit
	Wärmeübergang (alle Flächen betroffen, an denen Wärmeübertragung stattfindet)
1	Korrekturfaktor f. einphasige Konvektion in Wasser (Dittus-Boelter-Korrelation)
2	Korrekturfaktor f. einphasige Naturkonvektion in Wasser (McAdams-Korrelation)
3	Modell f. einphasige Zwangskonvektion in Dampf (Dittus-Boelter II oder McEligot)
4	Korrekturfaktor auf Modell 'Einphasige Zwangskonvektion in Dampf'
5	Korrekturfaktor Blasensieden (modifizierte Chen-Korrelation)
6	Modell für kritische Heizflächenbelastung (Minimalwert aus 3 Korrelationen oder Biasi-Korrelation)
7	Korrekturfaktor auf Modell für kritische Heizflächenbelastung
8	Korrekturfaktor für minimale Filmsiedetemperatur (Groeneveld-Stewart-Korrelation)
9	Modell f. Dampftropfenkühlung (modifizierte Dougall-Rohsenow oder Condie-Bengson-Korrelation)
10	Korrekturfaktor auf Modell f. Dampftropfenkühlung
11	Korrekturfaktor für Pool Filmsieden bei Naturkonvektion (Bromley-Korrelation)
12	Wärmeverluste an die Umgebung
13	Korrekturfaktor für Direktkondensation
	Drift
14	Korrekturfaktor für relative Geschwindigkeit in vertikalen Rohrleitungen
15	Korrekturfaktor für relative Geschwindigkeit im vertikalen Annulus
16	Korrekturfaktor für relative Geschwindigkeit im vertikalen Bündel
17	Korrekturfaktor für relative Geschwindigkeit in horizontalen Rohrleitungen
	Verdampfung, Wärme- und Massenübergang
18	Zahl der Blasen pro Einheitsvolumen (m^{-3})
19	Zahl der Tropfen pro Einheitsvolumen (m^{-3})
	Reaktorleistung
20	Korrekturfaktor für Reaktorleistung
21	Korrekturfaktor für Nachzerfallswärme
22	Korrekturfaktor für Reaktivitätstabelle als Funktion der Kühlmitteldichte
	Reaktivität
23	Korrekturfaktor für Reaktivitätstabelle als Funktion der Brennstofftemperatur
24	Korrekturfaktor für Externreaktivität (Steuerstabwirksamkeit)
	Numerik
25	maximaler lokaler relativer Fehler EPS, der noch zugelassen wird

Weitere Unsicherheitsquellen sind

- anlagen- und störfallspezifische Parameter wie z. B.
  - die Signallaufzeit für RESA,
  - der RDB-Füllstand für RESA,
  - der RDB-Füllstand für das Abfahren der Kühlmittelumwälzpumpen,
  - die Einschießzeit der Steuerstäbe,
  - die Wasserenthalpie,

…und

- vereinfachende Darstellungen wie z. B. die Zusammenfassung von Brennelementbündel in Kern-Kanäle oder die Orts- und Zeitdiskretisierung zur Lösung der zugrunde liegenden partiellen Differentialgleichungen.

4.2 Thermohydraulische Analysen im Rahmen der PSA für die Anlage KKP1 (SWR 69)

Die thermohydraulischen Berechnungen zur Bestimmung der Mindestanforderungen an Sicherheitsfunktionen und Notfallmaßnahmen wurden mit dem von der GRS entwickelten Störfallsimulator KKP 1 durchgeführt. Der Simulator verwendet die von der GRS entwickelten Codes

- ATHLET (Thermohydraulik-Code) und
- CONDRU (Containment-Code für Druck- und Kondensationskammer).

4.2.1 Modellierung und Anfangs- und Randbedingungen

Der Störfallsimulator hat zwei Varianten mit unterschiedlichem Detaillierungsgrad bzgl. der Nachbildung des thermohydraulischen Systems. Die detaillierte Nachbildung umfasst die Nachbildung mit Thermofluidobjekten folgender Komponenten bzw. Teilsysteme und Systeme:

- Reaktordruckbehälter,
- Frischdampfsystem 4-strängig bis zur Turbine,

- Speisewassersystem, Einspeiseleitungen 4-strängig,
- Speisewasserpumpen, 3-strängig,
- Hochdruckvorwärmstrecke, 2-strängig,
- Kondensatsystem, 1-strängig.

In der vereinfachten Variante wird das Frischdampfsystem 1-strängig abgebildet. Außerdem wird für das Kondensat- und Speisewassersystem ein vereinfachtes Gleichungssystem für die Masse-, Energie- und Impulsbilanzen mit der Annahme quasistationärer, einphasiger Wasserströmung zugrunde gelegt. In einer Unsicherheitsanalyse müssten die Unsicherheiten, die aus diesen Vereinfachungen resultieren, berücksichtigt werden.

Die Anfangs- und Randbedingungen der thermohydraulischen Rechnungen im Rahmen der PSA für die Anlage KKP1 sind in **Tab. 4-2** aufgeführt. Für die Nachzerfallsleistung wurden best-estimate Werte zugrunde gelegt. Dabei wurde von der aktuellen Kernbeladung mit 100 % Leistung ohne Sonderfahrweisen ausgegangen. Die berechnete Nachzerfallskurve wurde im Analysesimulator integriert.

Tab. 4-2 Anfangs- und Randbedingungen der thermohydraulischen Analysen

Parameter	Parameterwert
Kernleistung	2566 MW
Füllstand	14,32 m
Druck	69,3 bar
Kondensationskammer-Füllstand	16,54 m
Kondensationskammer-Temperatur	35 °C
Nebenkühlwassertemperatur	24 °C

Folgende Systeme bzw. Systemfunktionen werden in den Rechnungen berücksichtigt:

- Schnellabschaltsystem,
- Automatische Druckentlastung durch die Sicherheits- und Entlastungsventile (S/E-Ventile),
- Automatische Druckentlastung durch die S/E-Ventile und die diversitären Druckbegrenzungsventile,
- Durchdringungsabschluss der Frischdampfleitungen,

- Nachwärmeabfuhrsystem TH,
- Hochdruckeinspeisesystem TJ,
- Hochdrucknachspeisesystem TM,
- Hauptspeisewasserversorgung RL,
- USUS-System TF.

Die Mindestanforderungen an die Systemfunktionen müssen sicherstellen, dass die Nachzerfallsleistung (dauerhaft) geringer ist als die abgeführte Leistung und sowohl die Kerntemperatur von 1200°C als auch die Auslegungswerte in **Tab. 4-3** (bzw. der RDB-Prüfdruck) nicht überschritten werden.

Die thermohydraulischen Berechnungen wurden deshalb mindestens bis zum Erreichen eines der folgenden Kriterien fortgeführt:

- Nachzerfallsleistung ist geringer als die abgeführte Leistung (beherrschter Fall),
- einer der in **Tab. 4-3** genannten Auslegungswerte bzw. der RDB-Prüfdruck von 113,5 bar (entspricht dem 1,3-fachen Auslegungsdruck) wird überschritten,
- die Kerntemperatur überschreitet 1200 °C.

Tab. 4-3 In den thermohydraulischen Analysen berücksichtigte Auslegungswerte und Abbruchkriterien

Parameter	**Auslegungswert (Abbruchkriterium)**
Druck im RDB	87,3 bar (113,5 bar)
Druck in Kondensationskammer	3,5 bar
Druck in Druckkammer	3,8 bar
Druckdifferenz zwischen Druck- und Kondensationskammer	1,25 bar
Temperatur in Kondensationskammer	75 °C
Temperatur an Kondensationskammerdecke	140 °C
Temperatur in Druckkammer	140 °C
Betätigung des S/E-Ventils RA 11 S221	Max. 3000 mal
Betätigung aller übrigen S/E-Ventile	500 mal
Druckbereich für reine Wasserausströmung aus S/E-Ventilen	< 19 bar

Bei Überschreitung der Kerntemperatur von ca. 1200 °C wird aufgrund chemischer Wechselwirkungen und der Bildung eutektischer Verbindungen von einem weiteren sehr raschen Temperaturanstieg ausgegangen, der zum Schmelzen der Steuerstäbe führt. Das Schmelzen des ersten Steuerstabes wird als Beginn des Kernschadenszustandes definiert.

4.2.2 Mindestanforderungen

Die im Rahmen der PSA für die Anlage KKP1 ermittelten Mindestanforderungen zur Beherrschung der analysierten auslösenden Ereignisse sind in /LIN 06/ in Abschnitt 4.2.3 tabellarisch aufgeführt. Sie sind Ergebnis der in der GRS durchgeführten thermohydraulischen Analysen. Bei der Festlegung der Mindestanforderungen darf keiner der Auslegungswerte aus **Tab. 4-3** oder die Kerntemperatur von 1200 °C überschritten werden. Außerdem muss die Abfuhr der Nachzerfallsleistung auf Dauer sichergestellt sein.

Die thermohydraulischen Berechnungen haben z. B. gezeigt, dass für die Systemfunktion ‚Druckbegrenzung' das Öffnen mindestens eines der acht Eigenmedium betätigten S/E-Ventile oder mindestens zwei der sechs diversitären Druckbegrenzungsventile (Motorventile) erforderlich ist. Dabei ist zum Öffnen eines S/E-Ventils die Funktion ″Öffnen″ mindestens eines der jeweils zwei bzw. drei vorhandenen Magnet- oder Motor-Vorsteuerventile erforderlich. Ein S/E-Ventil fällt demnach aus, wenn das Hauptventil nicht öffnet oder die zugehörigen Vorsteuerventile nicht öffnen. Die Vorsteuerventile bzw. die diversitären Druckbegrenzungsventile werden durch die ″Automatische Druckbegrenzung″ (ADB) abhängig vom vorliegenden Druck gestaffelt in verschiedenen Ansteuerungsgruppen angesteuert.

Für den Notstromfall ergaben sich aus den Rechnungen unterschiedliche Anforderungen an die diversitären Druckbegrenzungsventile (d.h. bei Versagen aller S/E-Ventile), je nachdem ob die Hochdruckeinspeisung mit dem Einspeisesystem TJ funktioniert oder nicht. Bei Einspeisung mit TJ ist das Öffnen nur eines der sechs diversitären Druckbegrenzungsventile erforderlich, um den RDB-Druck unterhalb des Prüfdruckes zu halten. Dagegen übersteigt der RDB-Druck bei Versagen aller S/E-Ventile und Öffnen nur eines diversitären Druckbegrenzungsventils den Prüfdruck von 113,5 bar, wenn als Hochdruckeinspeisung nur das Nachspeisesystem TM zur Verfügung steht, d.h. wenn TJ ausfällt. In der PSA für die Anlage KKP-1 wird zur Vereinfachung generell

von einer Mindestanforderung von 2 von 6 diversitären Druckbegrenzungsventilen ausgegangen.

In einer vom Anlagenbetreiber von KKP 1 erstellten PSA der Stufe 1 für den Leistungsbetrieb wird bezüglich der diversitären Druckbegrenzungsventile das Öffnen von mindestens 4 von 6 Ventilen gefordert (/KKP 98/, Tab. 3.2.1-1).

Werden die Unsicherheitsquellen in den thermohydraulischen Berechnungen berücksichtigt, so lässt sich die Unsicherheit bzgl. des Ergebnisses, ob Auslegungswerte aus **Tab. 4-3** oder die Kerntemperatur von 1200 °C überschritten werden, und bzgl. der Zeit, wann Grenzwerte überschritten werden, quantifizieren. Wenn Unsicherheit bzgl. des Ergebnisses, ob Grenzwerte verletzt werden, vorhanden ist, dann besteht auch Unsicherheit bei der Festlegung von Mindestanforderungen. Die Unsicherheit bzgl. der Zeit, wann Grenzwerte überschritten werden, beeinflusst wiederum die nachfolgenden Bewertungsmodelle für Handmaßnahmen. Je mehr Zeit für eine Handmaßnahme zur Verfügung steht, desto höher ist i. A. die Wahrscheinlichkeit, dass sie erfolgreich durchgeführt wird.

Werden Auslegungswerte aus **Tab. 4-3** oder die Kerntemperatur von 1200 °C überschritten, so können i. A. auch Handmaßnahmen einen Kernschaden nicht mehr verhindern. Wenn Handmaßnahmen wirksam sein sollen, so müssen sie vor Überschreiten der Grenzwerte abgeschlossen sein. Die Ergebnisse der thermohydraulischen Analysen bzgl. der Zeitpunkte, wann Grenzwerte verletzt werden, liefern also Informationen zu verfügbaren Zeitfenstern für Handmaßnahmen.

Bei den von der GRS durchgeführten thermohydraulischen Analysen wurden Grenzwerte in einigen Fällen überschritten (vgl. /STE 04/). Im Folgenden sind zwei Fälle skizziert, bei denen die Auslegungstemperatur von 75 C für die Kondensationskammer (KoKa) überschritten wird.

- Notstrom-Fall: Die Druckbegrenzung erfolgt mit einem S/E-Ventil, die Druckentlastung mit einem S/E-Ventil (ADE1); die Steuerstabspülwasser-Pumpe läuft bei Eintritt des Notstromfalls aus und läuft nicht wieder an; die Niederdruck (ND)-Einspeisung erfolgt mit dem USUS-System TF21; der zugehörige Kühler ist nicht verfügbar; KoKa-Kühlen erfolgt mit dem USUS-System TF11 im Mindestmengenbetrieb; Handmaßnahmen zum Zurücksetzen des anstehenden FLUT-Signals für TF11 werden nicht durchgeführt; ca. 2 h 10 min nach Störfallauslösung übersteigt

die KoKa-Temperatur den Auslegungswert von 75 °C, weil die KoKa-Kühlung mit TF11 nur auf Mindestmenge läuft und damit die KoKa nicht gekühlt werden kann.

- Ausfall der Stromversorgung und Notstromversorgung (Station Blackout): Die vier Notstromdiesel für die Notstromversorgung der Pumpen vom Hochdrucknachspeisesystem TM, vom Kernflutsystem TK und vom Nachwärmeabfuhrsystem TH und die zwei Diesel zur Stromversorgung der USUS-Pumpen stehen nicht zur Verfügung; S/E-Ventile sind nicht verfügbar; die Hochdruck-Einspeisung erfolgt mit dem Hochdruckeinspeisesystem TJ; die Druckentlastung erfolgt mit 3 (diversitären) Notdruckventilen. Überschreiten der KoKa-Auslegungstemperatur nach ca. 4 h; nach 7 h 13 min wird mit einer KoKa-Temperatur von 100°C die Auslegungstemperatur des TJ-Systems (Saugleitung, Pumpe, Druckleitung) überschritten; ca. 13 h 43 min nach Störfallauslösung (Rechenende) erreicht KoKa-Temperatur einen Wert von 136 C und der RDB-Druck einen Wert von 31,7 bar. Die thermohydraulische Berechnung lieferte das Ergebnis, dass es mit 3 Notdruckventilen nicht möglich ist, den RDB-Druck schnell auf den Einspeisedruck der mobilen Pumpen (Pumpendifferenzdruck = 2 bar) abzusenken, die bei einer Notfallmaßnahme eingesetzt werden könnten.

Bei Ausfall der KoKa-Kühlung wird langfristig vom Ausfall der Hochdruck- bzw. Niederdruckeinspeisesysteme (durch Überschreiten der Auslegungstemperaturen) und damit vom Versagen der RDB-Bespeisung ausgegangen. Im Zusammenhang mit der KoKa-Temperatur interessieren deshalb die subjektive Wahrscheinlichkeit für das Überschreiten der Auslegungstemperaturen der Hochdruck- bzw. Niederdruckeinspeisesysteme und die subjektive Wahrscheinlichkeitsverteilung für die entsprechende Ausfallzeit der Systeme.

Mit dem Versagen der RDB-Bespeisung beginnt der RDB auszudampfen. Einige Zeit später beginnt die Kernaufheizung. Die Zeitdauer bis zum Ausfall der Hochdruck- bzw. Niederdruckeinspeisesysteme (durch Überschreiten der Auslegungstemperaturen) wirkt sich auf das Zeitbudget aus, das für die Durchführung von Handmaßnahmen zur Wiederherstellung der KoKa-Kühlung (z. B. Zurücksetzen des anstehenden FLUT-Signals für TF11) und damit zur Sicherstellung der RDB-Bespeisung zur Verfügung steht. Wenn ein großes Zeitbudget für die Diagnose des Problems und die Durchführung der Handmaßnahme zu Verfügung steht, ist es sehr unwahrscheinlich, dass die Handmaßnahme nicht rechzeitig durchgeführt wird. Umgekehrt wird bei einem geringen Zeitbudget eine große Versagenswahrscheinlichkeit für die Handmaßnahme erwartet.

Bei Berücksichtigung der Unsicherheitsquellen in den thermohydraulischen Rechnungen erhält man eine subjektive Wahrscheinlichkeitsverteilung für das verfügbare Zeitbudget und damit eine subjektive Wahrscheinlichkeitsverteilung für die erwartete Versagenswahrscheinlichkeit. Darüber hinaus erhält man nach THERP /SWA 83/ in Abhängigkeit von der Länge des verfügbaren Zeitfenster (unterschiedliche) bedingte subjektive Verteilungen, die die Kenntnisunsicherheit bzgl. der Versagenswahrscheinlichkeit für die Handmaßnahme ausdrücken. Aus der subjektiven Wahrscheinlichkeitsverteilung für das verfügbare Zeitbudget und den bedingten subjektiven Verteilungen für die Versagenswahrscheinlichkeit erhält man schließlich die unbedingte subjektive Verteilung für die Versagenswahrscheinlichkeit.

Die Unsicherheit im Thermohydraulik-Ergebnis wirkt sich also auf andere PSA-Modelle (wie beispielsweise die Modelle zur Bewertung von Personalhandlungen) und schließlich auf die PSA-Ergebnisse und ihre Unsicherheiten aus.

4.3 Illustration der Fortpflanzung von Thermohydraulik-Ergebnisunsicherheiten

An zwei Fortpflanzungsketten wird beispielhaft gezeigt, wie Thermohydraulik-Ergebnisunsicherheiten zur Unsicherheit der PSA Ergebnisse beitragen können.

Die erste Fortpflanzungskette beginnt mit der Unsicherheit bzgl. der aus einer thermohydraulischen Berechnung abgeleiteten Zahl von erforderlichen Sicherheitssystemen zur Beherrschung eines Störfalls:

Unsicherheit bzgl. der Zahl n der zur Störfallbeherrschung erforderlichen Sicherheitssysteme.

↓

Unsicherheit in der Spezifikation des Basisereignisses „Ausfall von n Sicherheitssystemen“ im Ereignisbaummodell.

↓

Unsicherheit in der „Struktur“ der zugrunde liegenden Fehlerbaum-Modelle:
Unterschiedliche Basisereignisse im Ereignisbaum bedeuten zum einen unterschiedliche TOP-Ereignisse und damit unterschiedliche Fehlerbäume. Zum anderen ist mit jedem Fehlerbaum eine Unsicherheit aufgrund des konzeptionellen Modells verbunden. Die Annahmen im Fehlerbaum können ungenau, unvollständig oder sogar ungeeignet sein.

↓

Unsicherheit in den Eingangsdaten für die Fehlerbaum-Modelle.

↓

Unsicherheit in den Wahrscheinlichkeiten für die Basisereignisse im Ereignisbaum:
Unterschiedliche Fehlerbäume liefern unterschiedliche TOP-Ereignis-Wahrscheinlichkeiten.

↓

Zusätzliche Unsicherheit im Ergebnis der PSA.

Am Anfang der zweiten Fortpflanzungskette ist die Unsicherheit bzgl. des aus einer thermohydraulischen Berechnung abgeleiteten Zeitfensters, das für eine Handmaßnahme zur Verfügung steht:

Unsicherheit bzgl. des vom Thermohydraulik-Ergebnis abgeleiteten Zeitbudgets zur Durchführung der Handmaßnahme.

↓

Zusätzliche Unsicherheit bzgl. der vom ermittelten Zeitbudget abhängigen Versagenswahrscheinlichkeit für die Handmaßnahme.
Die Versagenswahrscheinlichkeit wird durch ein geeignetes Modell wie z. B. THERP ermittelt. Die Unsicherheit bzgl. der Versagenswahrscheinlichkeit ist „zusätzlich“, weil selbst bei einem festen und bekannten Zeitbudget die Versagenswahrscheinlichkeit mit einer Unsicherheit behaftet ist.

↓

Zusätzliche Unsicherheit bzgl. der Top-Ereignis-Wahrscheinlichkeit für diejenigen Fehlerbäume, bei denen das Basisereignis ‚Versagen der Handmaßnahme’ berücksichtigt wird.

↓

Zusätzliche Unsicherheit im Ergebnis der PSA.

Im Gegensatz zur Unsicherheit bzgl. der erforderlichen Zahl von Sicherheitssystemen (in der ersten Fortpflanzungskette) wirkt sich die Unsicherheit bzgl. des Zeitbudgets für Personalhandlungen (in der zweiten Fortpflanzungskette) nicht auf die Struktur der anderen PSA-Modelle aus. Unsicherheiten im Zeitbudget können in der Analyse berücksichtigt werden, ohne zusätzliche HRA-Modelle für Personalhandlungen erstellen zu müssen.

Im Rahmen des Projekts SR 2418 wurde anhand eines Demonstrationsbeispiels zum ersten Mal veranschaulicht, wie Thermohydraulik-Modellunsicherheiten berücksichtigt

werden können und wie sich die Unsicherheiten auf das verfügbare Zeitfenster für Handmaßnahmen auswirken können (/KRZ 03/). Dabei wurden zwei Handmaßnahmen im Rahmen des Störfalls ″Ausfall der Hauptspeisewasserversorgung und der Hauptwärmesenke″ in einem Siedewasserreaktor der Baulinie 72 betrachtet. Für die Störfallanalyse wurde der Rechencode ATHLET angewendet.

5 Quantifizierung von Unsicherheiten

Eine Quantifizierung der Unsicherheit von Ergebnissen komplexer Modelle, wie z. B. eines Thermohydraulik-Modells, erhält man über eine Unsicherheitsanalyse. Dabei werden Modell- und Parameterunsicherheiten auf der Ebene der Teil-Modelle des komplexen Modells bestimmt. Diese Unsicherheitsanalyse wird in Abschnitt 5.1 vorgestellt.

Bei der Anwendung von Modellen stellt sich zunächst die Frage, ob es nur ein Modell gibt, das den abzubildenden Zusammenhang beschreibt, oder ob alternative Modelle zur Verfügung stehen, die den wahren Zusammenhang möglicherweise hinreichend genau abbilden. Abschnitt 5.2 beschreibt die Quantifizierung der Unsicherheit bei Vorliegen von zwei oder mehr Modellalternativen. Wurde eine Modellalternative als best geeignete ausgewählt, so ist nicht auszuschließen, dass das entsprechende Modellergebnis mit einer Unsicherheit behaftet ist. Die Quantifizierung der Unsicherheit im Modellergebnis durch Anwendung von Korrekturtermen auf das Ergebnis ist Thema von Abschnitt 5.3.

5.1 Ergebnisunsicherheit von komplexen Rechenmodellen

Die Unsicherheitsanalyse von Ergebnissen komplexer Rechenmodelle umfasst die im Folgenden aufgelisteten Schritte (vgl. auch /HOF 99/):

1. Identifikation der relevanten Unsicherheitsquellen der Rechenmodell-Anwendung, die aus ungenauem Kenntnisstand resultieren (epistemische Eingangsunsicherheiten).

2. Festlegung des Unsicherheitsbereichs für jede epistemische Eingangsunsicherheit. Unter Unsicherheitsbereich versteht man dabei den Gesamtwertebereich, der für die jeweilige epistemische Unsicherheit in Frage kommen kann.

3. Quantifizierung des Kenntnisstandes mittels einer ″subjektiven Wahrscheinlichkeitsverteilung″. Man verwendet in diesem Zusammenhang den Begriff ″subjektive Wahrscheinlichkeit″, weil Wahrscheinlichkeit nicht im herkömmlichen frequentistischen Sinn sondern als Ausdruck des Kenntnisstands interpretiert wird.

4. Identifikation und Quantifizierung von Kenntnisstand-Abhängigkeiten.

5. Fortpflanzung der epistemischen Eingangsunsicherheiten durch das Rechenmodell bis zur Ergebnisunsicherheit mit Methoden der Monte Carlo Simulation. Ergebnis ist eine Stichprobe aus der unbekannten subjektiven Wahrscheinlichkeitsverteilung des Rechenergebnisses.

6. Quantifizierung der epistemischen Ergebnisunsicherheit auf der Grundlage der Stichprobe von Rechenergebnissen (z. B. in Form verteilungsfreier statistischer Toleranzgrenzen).

Modell- und Parameterunsicherheiten werden auf der Ebene der Teil-Modelle des komplexen Modells bestimmt. Bei den Teil-Modellen besteht oft die Möglichkeit, deren Ergebnis-Unsicherheit anhand von Validierungsunterlagen zu beurteilen. Der gemeinsame Einfluss der quantifizierten Unsicherheiten in den Teil-Modellen zeigt sich schließlich in der Ergebnis-Unsicherheit des komplexen Modells.

5.2 Subjektive Wahrscheinlichkeiten für alternative Modelle

Das Vorliegen von Modellalternativen kann verschiedene Ursachen haben, wie z. B. Unterschiede im Komplexitätsgrad, in den Anfangs- und Randbedingungen, in den experimentellen Daten oder in den Rechenergebnissen anderer Modelle, die der Modelanpassung zugrunde liegen. Existieren alternative Modelle, so kann ein Modell z. B. aufgrund der Relevanz und des Umfangs seines Validierungsprozesses oder aufgrund seiner Verfügbarkeit und Anwendbarkeit bevorzugt werden. Wird ein Modell als best mögliches für den Anwendungsbereich ausgewählt, so kann sein Ergebnis immer noch mit signifikanten Unsicherheiten behaftet sein.

Stehen alternative Modelle zur Verfügung, die den wahren Zusammenhang möglicherweise hinreichend genau beschreiben, so sollten alle Modelle berücksichtigt werden, mit denen ein Spektrum an Ergebniswerten erzielt werden kann, das als hinreichend repräsentativ gilt. Die Unsicherheit darüber, welches der Modelle den Zusammenhang am besten abbildet, muss entsprechend quantifiziert werden. Dabei sollte jedem Modell eine subjektive Wahrscheinlichkeit zugeordnet werden, die den Kenntnisstand bzw. den Grad an Vertrauen darüber ausdrückt, wie gut das Modell den wahren Zusammenhang beschreibt.

Ist p_i die subjektive Wahrscheinlichkeit dafür, dass Modell *i, i = 1,…, n,* aus einer hinreichend repräsentativen Menge von *n* Modellen den wahren Zusammenhang am "besten" beschreibt, dann gilt $\Sigma p_i = 1$. Hier liegt die Bedingung zugrunde, dass wenn Modell *i* den wahren Zusammenhang am "besten" beschreibt, dies nicht für die anderen Modelle in der Menge zutrifft.

Zur Berücksichtigung der Modellalternativen im Rahmen einer Unsicherheitsanalyse werden die Modellalternativen zunächst indiziert. Die lndexzuordnung kann dabei beliebig erfolgen. Der Modellindex repräsentiert in diesem Zusammenhang einen unsicheren Parameter. Die Unsicherheit wird durch eine Diskrete Verteilung über alle Indexwerte ausgedrückt. Die Auswahl eines lndexwertes gemäß der Diskreten Verteilung hat zur Folge, dass die entsprechende Modellalternative entsprechend ihrer subjektiven Wahrscheinlichkeit zur Anwendung kommt.

Um die Unsicherheit im Ergebnis einer Modellalternative auszudrücken, können subjektive Wahrscheinlichkeitsverteilungen für additive und/oder multiplikative Korrekturterme verwendet werden (vgl. Abschnitt 5.3).

5.3 Korrekturterme für das Modellergebnis

Häufig werden zur Quantifizierung der Unsicherheit von Modellergebnissen subjektive Wahrscheinlichkeitsverteilungen für additive und/oder multiplikative Korrekturterme (Modellparameter) verwendet (vgl. Abschnitt 5.4). Die subjektiven Wahrscheinlichkeitsverteilungen sollen den Kenntnisstand über die Korrektur ausdrücken, welche erforderlich ist, um einen zutreffenden Ergebniswert zu erhalten.

Liegen Messergebnisse aus Experimenten und dazugehörige Ergebnisse aus Modellnachrechnungen vor, so erhält man die subjektiven Wahrscheinlichkeitsverteilungen der Korrekturterme durch Anpassung der Modellergebnisse an die Messreihen. Die Quantifizierung der Unsicherheit von Korrekturtermen gestaltet sich dann schwierig, wenn sich die Randbedingungen für die Berechnungen wesentlich von den Bedingungen der Experimente unterscheiden.

Die Korrektur des Modellergebnisses lässt sich wie folgt ausdrücken:

$$y = a \cdot y_M + b \,,$$

wobei y die verwendete Korrektur des Ergebniswertes y_M aus dem (bevorzugten) Modells M ist, und a und b die unsicheren Korrekturterme darstellen.

Es gibt verschiedene Verfahren, um auf der Basis von Messergebnissen und den dazugehörigen Modellnachrechnungen die subjektiven Wahrscheinlichkeitsverteilungen zur Quantifizierung der Unsicherheit von Korrekturtermen festzulegen. Beispielsweise kann ein Bayes'sches Verfahren (/SIU 85/) angewendet werden, wenn sich die Messergebnisse direkt auf die unsicheren Korrekturterme beziehen (vgl. auch Abschnitt 5.4). Beziehen sich die Messergebnisse auf Funktionen der Korrekturterme, kann der numerische Aufwand des Bayes'sches Verfahrens sehr groß sein. Hier kann z. B. das numerische Iterationsverfahren ″CIRCE″ (/CRE 96/) angewendet werden, um die subjektiven Wahrscheinlichkeitsverteilungen der unsicheren Korrekturterme herzuleiten.

Liegen keine Messreihen vor, so kann eine Quantifizierung der Unsicherheit des Modellergebnisses nur über Expertenurteil gewonnen werden. Dabei kann beispielsweise über Korrekturfaktoren (Modellparameter) ausgedrückt werden, wie gut das Modell den wahren Zusammenhang abbildet (vgl. auch Abschnitt 5.4).

5.4 Subjektive Wahrscheinlichkeitsverteilungen für unsichere Modellparameter

Jedes Modell kann eigene unsichere Parameter haben. Korrekturterme für das Modellergebnis zählen z. B. zu diesen unsicheren Modellparametern. Für jeden potentiell wichtigen unsicheren Parameter eines Modells kann der Kenntnisstand durch eine subjektive Wahrscheinlichkeitsverteilung quantifiziert werden.

Dabei ist zwischen zwei Fällen zu unterscheiden. Während in dem einen Fall Informationen aus Beobachtungen genutzt werden können, stehen im anderen Fall keine Beobachtungen zur Quantifizierung der Unsicherheit zur Verfügung.

5.4.1 Subjektive Wahrscheinlichkeitsverteilungen auf der Grundlage von Beobachtungen

Liegen Beobachtungen zu einem unsicheren Parameter X vor, so kann die Bayes'sche Methode zur Quantifizierung der Unsicherheit angewendet werden.

Diese Methode setzt voraus, dass es zwischen Beobachtung und unsicherem Parameter eine Beziehung gibt. Diese Beziehung kann z. B. derart aussehen, dass die Wahrscheinlichkeit (Wahrscheinlichkeitsdichte) der Beobachtung *o* als Funktion eines unsicheren Parameters *P* der subjektiven Verteilung von X betrachtet werden kann.

Die Bayes'sche Methode liefert eine subjektive a posteriori Wahrscheinlichkeitsdichte *f(p|o)* für den unsicheren Verteilungsparameter *P*. Die a posteriori Verteilung von *P* drückt den Kenntnisstand über *P* auf der Grundlage der Beobachtung *o* aus. Man erhält *f(p|o)* aus der so genannten a priori Verteilung $f_o(p)$ des unsicheren Verteilungsparameters *P* und aus der Wahrscheinlichkeit *L(o|p)* für die Beobachtung *o,* wenn *P=p* der wahre Parameterwert ist. Die a priori Verteilung $f_o(p)$ drückt den Kenntnisstand über *P* aus, bevor die Beobachtung vorliegt. Liegt keine a priori Information über den unsicheren Parameter *P* vor, wird i.A. eine sogenannte nicht informative a priori Verteilung für *P* verwendet (vgl. /BOX73/).

Für die subjektive a posteriori Wahrscheinlichkeitsdichte *f(p|o)* von *P* gilt:

$$f(p \mid o) \propto L(o \mid p) \cdot f_0(p)$$

L(o|p) bezeichnet die Wahrscheinlichkeitsdichte für die Beobachtung *o* als Funktion von *P* und $f_o(p)$ ist die Wahrscheinlichkeitsdichte der a priori Verteilung von *P*.

Für die a posteriori Wahrscheinlichkeitsdichte *f(x|o)* des unsicheren Modellparameters *X* gilt schließlich nach dem Gesetz der totalen Wahrscheinlichkeit:

$$f(x \mid o) = \int f(x \mid p) \cdot f(p \mid o) dp$$

f(x|o) ist die a posteriori Wahrscheinlichkeitsdichte des unsicheren Parameters *X*, wenn die Beobachtung *o* vorliegt. *f(x|p)* ist die subjektive Wahrscheinlichkeitsdichte von X, wenn *P=p* der wahre Parameterwert ist. *f(p|o) ist* subjektive a posteriori Wahrscheinlichkeitsdichte *f(p|o)* von *P* auf der Grundlage der Beobachtung *o.*

5.4.2 Subjektive Wahrscheinlichkeitsverteilungen auf der Grundlage von Expertenurteil

Wenn keine Beobachtungen bzgl. eines unsicheren Parameters vorliegen, ist Expertenurteil eine wichtige Informationsquelle. In dieser Situation ist ein strukturiertes Vorgehen bei der Expertenbefragung empfehlenswert (vgl. z. B. /AYY 01/). Da ein solches strukturiertes Vorgehen sehr aufwendig ist, sollte es nur auf diejenigen unsicheren Größen beschränkt werden, die (möglicherweise) am meisten zur Unsicherheit des Modellergebnisses beitragen.

In allen anderen Fällen sollte die Quantifizierung des Kenntnisstands auf Plausibilitätsbetrachtungen basieren. Solche Betrachtungen können z. B. einen Unsicherheitsbereich liefern, der alle Werte eines Parameters beinhaltet, die möglicherweise zutreffend sind. Ist jeder Wert in gleichem Maße zutreffend, ist die Gleichverteilung als subjektive Wahrscheinlichkeitsverteilung geeignet. Zusätzliche Informationen können es rechtfertigen, statt der Gleichverteilung eine Dreiecksverteilung oder eine (gestutzte) Normalverteilung zu quantifizieren.

6 Zusammenfassung und Schlussfolgerung

Die bislang praktizierte Unsicherheitsanalyse im Rahmen einer PSA beschränkt sich in der Regel auf die Quantifizierung der Unsicherheiten in den Zuverlässigkeitskenngrößen, die als Eingabedaten für die Fehlerbaum- und Ereignisbaumanalysen verwendet werden. Weitere Unsicherheitsquellen, wie z. B. Parameter- und Modellunsicherheiten aus den Störfallsimulationen mit Thermohydraulik-Modellen, werden im Allgemeinen nicht berücksichtigt, obwohl nicht auszuschließen ist, dass auch sie die PSA-Ergebnisse und ihre Unsicherheiten erheblich beeinflussen können.

Die bisherige, einschlägige Literatur besteht überwiegend aus allgemeinen und mehr theoretischen Beschreibungen von Modellunsicherheiten. Im Rahmen dieses Projekts wurde ein erster Schritt in Richtung einer systematischen Betrachtung von Modellunsicherheiten im Rahmen einer PSA begonnen. Dazu wurden verschiedene Unsicherheitsquellen, die im Rahmen einer PSA auftreten können und bisher nicht berücksichtigt wurden, identifiziert und beschrieben. Wo möglich, wurden erste Ideen zur methodischen Berücksichtigung der Modellunsicherheiten diskutiert.

Am Beispiel der von der GRS im Rahmen des BMU Vorhabens SR 2414 für den Leistungsbetrieb eines Siedewasserreaktors erstellten PSA SWR 69 wurde anhand von Beispielen gezeigt, welche Unsicherheitsquellen existieren, die einen potentiell wichtigen Einfluss auf die PSA-Ergebnisse haben können. Wo möglich, wurden für die zu berücksichtigenden Modellunsicherheiten geeignete Methoden zur Quantifizierung vorgeschlagen. Es ist zu betonen, dass die in diesem Bericht erfolgten Ausführungen dazu dienen sollen, mögliche Quellen von Unsicherheiten in einer PSA zu beschreiben sowie Vorschläge und Ansatzpunkte zu liefern, wie diese Unsicherheiten zukünftig berücksichtigt bzw. quantifiziert werden können. Sie stellen keine Kritik an bisher durchgeführten PSA dar, insbesondere deshalb nicht, da einige der in diesem Bericht vorgeschlagenen Methoden, mit denen eine Berücksichtigung bzw. Quantifizierung von Modellunsicherheiten möglich geworden ist, erst seit jüngster Zeit zur Verfügung stehen.

Die Berücksichtigung der Kenntnisstandunsicherheiten bzgl. der in einen Fehler- bzw. Ereignisbaum eingehenden Zuverlässigkeitskenngrößen ist mittlerweile Stand von Wissenschaft und Technik. Aber nicht nur diese Kenntnisstandunsicherheiten tragen

zur Unsicherheit der PSA-Ergebnisse bei. Unsicherheiten in PSA-Ergebnissen können sich zusätzlich durch die Unsicherheit bzgl. der Ergebnisse der verwendeten Modelle ergeben. Gerade bei den vereinfachten statischen Modellen der Fehler- und Ereignisbaumanalyse stellt sich die Frage, wie genau sie die wahren Zusammenhänge nur beschreiben können und wie ihre probabilistischen Bewertungen einzuordnen sind. Diese Art der Modellunsicherheiten, die sich auf die Vollständigkeit des Modells (‚Completeness Uncertainty') beziehen, konnten bisher aufgrund mangelnder Methoden nicht quantifiziert werden.

Die in diesem Bericht diskutierten Beispiele haben verdeutlicht, dass sich die im Rahmen einer PSA zu untersuchenden Abläufe durch komplexe Wechselwirkungen zwischen dem System- und Prozessverhalten, den Personalhandlungen und stochastischen Einflussfaktoren ergeben. Es wurde gezeigt, dass für eine möglichst realistische Modellierung die menschlichen Handlungsabläufe als dynamische Prozesse betrachtet werden müssen, die sich in Wechselwirkung mit dem System- und Prozessverhalten im zeitlichen Verlauf entwickeln. Mit den konventionellen Methoden der PSA ist eine solche Modellierung nicht möglich. Seit jüngster Zeit stehen Methoden der probabilistischen Dynamikanalyse zur Verfügung, mit denen die in einer PSA zu untersuchenden Abläufe realitätsnah modelliert werden können. Mit dem Einsatz dieser fortschrittlichen Methoden könnten prinzipiell Analysen durchgeführt werden mit dem Ziel, die Unsicherheit der Ergebnisse aufgrund der unvollständigen bzw. vereinfachten Modellierungen zu quantifizieren.

Anhand eines Demonstrationsbeispiels an einem Fehlerbaummodell wurde gezeigt, dass zeitliche Einflussgrößen sich erheblich auf das Ergebnis auswirken können. Da zeitliche Einflussfaktoren aufgrund einer vereinfachten Modellierung nicht explizit im Fehler- bzw. Ereignisbaum berücksichtigt werden können, kann auch ihr Einfluss auf die PSA-Ergebnisse mit den konventionellen Methoden nicht quantifiziert werden. Ein Vergleich mit Analysen, die den Zeitfaktor explizit berücksichtigen, könnte Aufschluss darüber geben, wie das Ergebnis der konventionellen Analyse einzuordnen und (mit einem Korrekturterm) zu korrigieren ist, um ein realistischeres Ergebnis zu erhalten.

Ein weiterer wichtiger Untersuchungsgegenstand des Berichts sind die Unsicherheiten im Rahmen von thermohydraulischen Berechnungen zur Bestimmung von Mindestanforderungen. Die Mindestanforderungen betreffen die Zahl der erforderlichen Sicherheits-, ATWS- und Notstandssysteme, deren Anforderungszeitpunkte und Einsatzzeiten sowie die für Personalhandlungen verfügbaren Zeitfenster. Die ermittel-

ten Mindestanforderungen können mit einer erheblichen Unsicherheit behaftet sein, weil bei der Verwendung von deterministischen Rechencodes viele Eingabeparameter aufgrund ungenauer Kenntnis als unsicher zu betrachten sind. Des Weiteren müssen die Unsicherheiten bzgl. der im Rechencode verwendeten Sub-Modelle, die ein gewisses Phänomen nur mehr oder weniger genau beschreiben, berücksichtigt werden.

Bisher wurden im Rahmen einer PSA die unsicheren Eingabeparameter sowie die Modellunsicherheiten im deterministischen Rechencode, der für die thermohydraulischen Berechnungen zur Bestimmung der Mindestanforderungen eingesetzt wurde (z. B. ATHLET), nicht berücksichtigt. Deshalb wurde im Bericht eine Methodik zu ihrer Berücksichtigung beschrieben. Die Methodik erlaubt die Nutzung paralleler Rechenknoten, so dass eine zu hohe und unpraktikable Rechenzeit vermieden werden kann. Des Weiteren wurde dargestellt, dass die Berücksichtigung von Unsicherheiten in deterministischen Rechencodes zu relevanten Ergebnisunsicherheiten führen kann, die sich in der weiteren PSA-Analysekette als Modellunsicherheiten fortpflanzen können.

Als eine wichtige Schlussfolgerung der Untersuchungen in diesem Bericht ist festzuhalten, dass die Berücksichtigung der Unsicherheiten im verwendeten deterministischen Rechencode ein wesentlicher Schritt ist zur Weiterentwicklung der Unsicherheitsanalyse im Rahmen einer PSA. Eine weitere Schlussfolgerung ist die Empfehlung für einen verstärkten Einsatz von fortschrittlichen Methoden der probabilistischen Dynamikanalyse für wichtige Teilbereiche einer PSA, bei denen die konventionellen Methoden offensichtlich an ihre Grenzen stoßen. Mit dem Einsatz dieser fortschrittlichen Methoden könnten auch Aussagen darüber gewonnen werden, welchen Einfluss die vereinfachten Modellierungen und grobe Abschätzungen der konventionellen Analyse auf PSA-Ergebnisse haben.

7 Literatur

/AYY 01/ Ayyub, B. M.
Elicitation of Expert Opinions for Uncertainty and Risks, CRC Press, 2001

/BOX 73/ Box, G.E.P. und G.C. Tiao
Bayesian Inference in Statistical analysis. Addison-Wesly, Reading, Massachusetts, 1973

/COJ 96/ Cojazzi, G.
The DYLAM approach for the dynamic reliability analysis of systems, Reliability Engineering and System Safety 52 (1996) 279-296, 1996

/CRE 96/ de Crecy, A.
Determination of the Uncertainties of the Constitutive Relationships in the Cathare 2 Code, IAEA Course, Trnava, Oct. 1996

/FAK 05/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke
Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005, BfS-SCHR-37/05, Wirtschaftsverlag NW / Verlag für neue Wissenschaft GmbH, Salzgitter ISSN 0937-4469,
ISBN 3-86509-414-7, Oktober 2005

/GAL 93/ Gallegos, D.P. und E.J. Bonano
Consideration of uncertainty in the performance assessment of radioactive waste disposal from international regulatory perspective, Reliability Engineering and System Safety, 42:111, 1993

/GAS 01/ Gaßman, D., E. Hofer, K. Kotthoff, und W. Preischl
Menschliche Zuverlässigkeit in der probabilistischen Sicherheitsanalyse (PSA), Teil 2: Methoden zur Verifikation von Swain- Daten und zur Datenverbreiterung, GRS-A-2951, Gesellschaft für Anlagen- und Reaktorsicherheit, Garching, Febr. 2001

/HOF 94/ Hofer, E.
Berücksichtigung von Modellunsicherheiten in Unsicherheits- und Sensitivitätsanalysen von Rechenmodellergebnissen, GRS-A-2203, Gesellschaft für Anlagen- und Reaktorsicherheit, Garching, Juli 1994

/HOF 99/ Hofer, E. und M. Kloos
Verwendung realistischer Anfangs- und Randbedingungen sowie Codes in Verbindung mit Unsicherheitsanalysen bei der Sicherheitsbeurteilung von Kernkraftwerken, GRS-A-2693, Gesellschaft für Anlagen- und Reaktorsicherheit, Garching, Juli 1999

/HOF 01/ Hofer, E., M. Kloos, B. Krzykacz-Hausmann, J. Peschke und M. Sonnenkalb
Methodenentwicklung zur simulativen Behandlung der Stochastik in probabilistischen Sicherheitsanalysen der Stufe 2, GRS-A-2997, Gesellschaft für Anlagen- und Reaktorsicherheit, Garching (2001)

/JUL 06/ Julius, J. A. und J.F. Grobbelaar
New Advances in Human Reliability Using the EPRI HRA Calculator , NPIC & HMIT, Albuquerque, NM, November 12-16, 2006

/KKP 98/ EnBW Kraftwerke GmbH Kernkraftwerk Philippsburg
Probabilistische Sicherheitanalyse KKP 1, Juli 1998

/KRZ 03/ Krzykacz-Hausmann, B. und E. Hofer
Quantifizierung von Modellunsicherheiten der PSA, GRS-A-3198, Gesellschaft für Anlagen- und Reaktorsicherheit, Garching, Dezember 2003

/LAB 00/ Labeau P.E., C. Smidts, S. Swaminathan
Dynamic reliability: towards an integrated platform for probabilistic risk assessment, Reliability Engineering and System Safety 68 (2000) 219-254, 2000

/LIN 06/ von Linden, J., et al.
Erprobung und Bewertung der Methoden einer PSA für SWR Anlagen der Baulinie 69 nach Stand von Wissenschaft und Technik (PSA SWR 69), Fachband 1 - Ereignisablauf- und Fehlerbaumanalysen für Ereignisse aus dem Leistungsbetrieb bis zum Kernschmelzen (ohne Brand), GRS-A-3292, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, April 2006

/NUR 75/ Rasmussen, N.C.
Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH 1400, NUREG-75/014, October 1975

/PAR 82/ Parry, G.W.
On One Type of Modelling Uncertainty in Probabilistic Risk Assessment, Nuclear Safety, 24: 634, 1982

/PES 06/ Peschke,J., M. Kloos, W. Faßmann und M. Sonnenkalb
Methodenentwicklung für die Berücksichtigung menschlicher Eingriffe im Rahmen einer dynamischen PSA der Stufen 1 und 2, GRS-A-3220, Gesellschaft für Anlagen- und Reaktorsicherheit, Garching, August 2006

/SIU 85/ Siu, N. und G. Apostolakis
On the Quantification of Modeling Uncertainty. Paper M2 115, Intl. Conf. On Structural Mechanics in Reactor Technology (SMIRT), Brussels, Belgium, August 1985

/SIU 94/ Siu, N.
Risk assessment for dynamic systems: An overview, Reliability Engineering and System Safety 43 (1994) 43-73, 1994

/STE 04/ Steinhoff, F.
Störfallanalysen für die Anlage KKP1,Mindestanforderungen beim Notstromfall, Ausfall Hauptwärmesenke, Ausfall Hauptspeisewasser, Ausfall Hauptwärmesenke und Hauptspeisewasser, Technische Notiz, PSA-KKP1 STF-TN 01/04, 03.02.2004

/SWA 83/ Swain, A.D. und H.E. Guttmann
Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, U.S. Regulatory Commission, August 1983

/SWA 87/ Swain, A.D.
Accident Sequence Evaluation Program - Human Reliability Analysis Procedure, NUREG/CR-4772, February 1987

8 Abbildungsverzeichnis

9 Tabellenverzeichnis

VERTEILER

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit

AG RS I 3			2x

Bundesamt für Strahlenschutz

SK 2			2x
SK 3, Herr Dr. Rehs			3x
	CD ROM		5x

GRS

Geschäftsführer	(hah, stj)	je	1x
Bereichsleiter	(erv, lim, prg, rot, tes, zir)	je	1x
Abteilungsleiter	(poi, stc, ver, mem)	je	1x
Projektleitung	(row)		2x
Projektcontrolling	(hab, vet)	je	1x
Bibliothek	(hog)		1x
TECDO	(rop)		1x
Autoren	(kls, pej)	je	3x

Gesamtauflage: **31 Exemplare**

5 CD ROM