Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen

Abschlussbericht zum Vorhaben RS 1180

GRS - A - 3558

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Abschlussbericht/
Final Report

Reaktorsicherheitsforschung-Vorhabens Nr.:/
Reactor Safety Research-Project No.:
RS1180

Vorhabenstitel / Project Title:

Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen

Development and Test Applications of Methods and Tools for Probabilistic Safety Analyses

Autor / Author:
M. Röwekamp, W. Faßmann, W. Frey, L. Gallner, H. Grebner, J. Hartung, M. Kloos, A. Kreuser, M. Leberecht, F. Michels, J. Peschke, E. Piljugin, W. Preischl, N. Reinke, J. Sievers, J.-C. Stiller, M. Türschmann, A. Wielenberg

Berichtszeitraum / Publication Date:
August 2010

Anmerkung:
Das diesem Bericht zugrunde liegende F&E-Vorhaben wurde im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi) unter dem Kennzeichen RS1180 durchgeführt.

GRS - A - 3558

Kurzfassung

Probabilistische Sicherheitsanalysen (PSA) sind inzwischen weltweit ein überaus wichtiges und immer intensiver genutztes Instrument für die Sicherheitsbewertung von Kernkraftwerken. Seit der Neufassung des Atomgesetzes (AtG) vom April 2002 ist die Durchführung einer PSA für alle Kernkraftwerke in Deutschland im Rahmen der in § 19a AtG geforderten (Periodischen) Sicherheitsüberprüfungen (SÜ) verpflichtend. Dies hat zu umfangreichen sicherheitstechnischen Verbesserungen in den Kernkraftwerken geführt und damit wesentlich zum hohen Sicherheitsniveau der deutschen Kernkraftwerke beigetragen.

In einer PSA werden Kenntnisse über die Auslegung und Betriebsweise der Anlage, die Betriebserfahrung der untersuchten Anlage und ähnlicher Anlagen sowie Erkenntnisse der Sicherheitsforschung, wie auch der generelle wissenschaftlich-technische Sachverstand zu einer Gesamtbewertung des Sicherheitszustandes der zu untersuchenden Anlage zusammengeführt. Dabei wird – soweit möglich – auch der Einfluss evident gewordener Kenntnisstandunsicherheiten auf die Ergebnisse dieser Bewertung ausgewiesen.

Die Methoden zur Durchführung einer PSA haben sich kontinuierlich weiterentwickelt. Dennoch verbleiben noch einige offene Punkte, bei denen methodische Weiterentwicklungen erforderlich sind. Dies resultiert u. a. daraus, dass sich aus dem Einsatz neuer Technologien, veränderten Betriebsweisen und neuen Erkenntnisse aus der Betriebserfahrung weitergehende Anforderungen an Umfang und Aussagesicherheit von PSA ergeben. Ebenso entwickelt sich auch international der Stand von Wissenschaft und Forschung weiter. Deshalb hat die GRS in Wahrnehmung der Kompetenzträgerschaft für die probabilistische Sicherheitsanalyse in Deutschland im Vorhaben RS1180 ’Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen’ vorhandene Methoden und Werkszeuge weiterentwickelt und für die Anwendung in zukünftigen PSA nutzbar gemacht und erprobt.

In den nachfolgend aufgeführten fachlichen Themenbereichen erfolgten entsprechende Arbeiten:

Das erste Ziel war eine Entwicklung von Methoden zur probabilistischen Bewertung softwarebasierter digitaler Leittechnik. Da weltweit bislang keine anerkannten Methoden dazu existieren, der Einsatz softwarebasierter Leittechnik mit unmittelbarer Sicherheitsfunktion aber in absehbarer Zeit auch in deutschen Kernkraftwerken im Rahmen

einer tiefgreifenden Modernisierung der Sicherheitsleittechnik zu erwarten ist, sollten Ansätze zur Zuverlässigkeitsbewertung digitaler Leittechnik einschließlich der Software erarbeitet werden. Ergänzend sollten die Relevanz der Mensch-Maschine-Schnittstelle softwarebasierter Leittechnik für die PSA untersucht und gegebenenfalls einen Ansatz für deren Bewertung entwickelt werden. Dabei war vorrangig die Frage zu beantworten, wie sich der Wechsel von analoger zu softwarebasierter Leittechnik und die damit verbundenen Änderungen in der Schnittstelle zum Menschen für die Zuverlässigkeit von Personenhandlungen und deren Bewertung auswirken.

Als zweites Teilziel sollten die Bewertungsmethoden zur Berücksichtigung wissensbasierter Personalhandlungen und organisatorischer Einflüsse in der PSA verbessert werten. Zum einen wurde daher eine Methode bereitgestellt, um sicherheitstechnisch erforderliche, wissensbasierte Handlungen in einer PSA zu berücksichtigen. Diese umfasst ein Verfahren zur Identifikation der zu untersuchenden Handlungen, ein Kognitionsmodell, sowie einen zweistufigen Bewertungsansatz. Des Weiteren wurde eine Methode zur Berücksichtigung organisatorischer Einflussfaktoren in der PSA entwickelt. Mit Hilfe der Forschungsergebnisse ist es möglich, die sicherheitstechnische Relevanz organisatorischer Einflussfaktoren und des Sicherheitsmanagements herauszuarbeiten, zu quantifizieren und in das PSA-Modell zu integrieren.

Ein weitere Zielsetzung betraf eine Reihe von Fragestellungen zu einer verbesserten Berücksichtigung auslösender Ereignisse und übergreifender Einwirkungen von innen und außen in der PSA:
Vorhandene Methoden zur Ermittlung von Leck- und Bruchhäufigkeiten druckführender Komponenten wurden für die PSA weiterentwickelt. Ein weites Ziel bestand in der Entwicklung eines systematischen Auswahlverfahrens zur Bestimmung kritischer Anlagenteilen bei einer seismischen probabilistischen Sicherheitsanalyse (SPSA), welches es ermöglicht, diese Auswahl kritischer Anlagenteile unter technisch-wissenschaftlichen Gesichtspunkten optimal durchzuführen. Außerdem erfolgten erste Untersuchungen hinsichtlich eines möglichen Bedarfs einer Methodenentwicklung für eine probabilistische Bewertung von Transienten aufgrund von Überspannungen oder Fremdspannungseinträgen.

Eine weitere Aufgabe bestand darin, durch eine Reihe einzelner Fragestellungen die Methoden zur Berücksichtigung von Unsicherheiten und zum Ausschluss von Fehlerquellen in der PSA zu verbessern. Dazu wurden Methoden zur Durchführung von Unsicherheits- und Sensitivitätsanalysen in probabilistischen Dynamikanalysen (dynami-

schen PSA) bereitgestellt. Des Weiteren wurde eine Methodik zur Anpassung von Beta-Verteilungen an vorgegebene Lognormal-Verteilungen unter Berücksichtigung zusätzlicher Benutzervorgaben erarbeitet. Ein weiteres Ziel der Arbeiten bestand in der Entwicklung, Erprobung und programmtechnischen Realisierung eines in sich geschlossenen Verfahrens zur Ermittlung von Verteilungen für Zuverlässigkeitskenngrößen, mit dem relevante epistemische Unsicherheiten aus unterschiedlichen Quellen in konsistenter und umfassender Weise berücksichtigt werden können. Außerdem wurde das Vorgehen bei der ingenieurmäßigen Bewertung der Übertragbarkeit beobachteter GVA-Ereignisse auf die in der PSA zu bewertenden Komponentengruppen durch die Entwicklung eines Verfahrensrahmens systematisiert, um damit die Unsicherheiten der Schätzung bei der Bewertung durch unterschiedliche Experten zu minimieren. Mit go-PSA wurde eine auf MS WINDOWS® basierende gemeinsame Benutzeroberfläche bereitgestellt, unter der die von der GRS entwickelten Hilfsprogramme für die Erstellung einer PSA der Stufe 1 sowie entsprechende Benutzerhilfen zu bestimmten Einzelfragestellungen zusammengefasst sind. Damit konnte eine Reihe von potenziellen Fehlerquellen eliminiert werden.

Die letzte Zielsetzung bestand in einer methodischen Weiterentwicklung und Überprüfung von ASTEC dahingehend, ob es zur Analyse von Unfallszenarien eingesetzt werden kann. Dazu wurde die aktuelle Version von ASTEC auf ihre Tauglichkeit für den Einsatz in einer PSA der Stufe 2 erfolgreich erprobt und dazu mit MELCOR verglichen.

Die Ergebnisse des Vorhabens dienen dazu, abgesicherte Methoden zur probabilistischen Sicherheitsanalyse entsprechend dem internationalen Stand von Wissenschaft und Technik zur Verfügung zu stellen. Die Arbeiten haben die Belastbarkeit von PSA-Ergebnissen weiter abgesichert und damit die Aussagesicherheit der PSA erhöht. Dies stärkt die Rolle der PSA als kontinuierlich zu nutzendes Instrument der Sicherheitsbewertung von Kernkraftwerken - in Ergänzung der deterministischen Vorgehensweise. Damit leistet das Vorhaben einen wesentlichen Beitrag zu den in /BMW 05/ formulierten Zielen der Reaktorsicherheitsforschung.

Eine systematische Erprobung der weiterentwickelten Methoden anhand einer Referenz-PSA steht aber noch aus.

Abstract

Probabilistic safety analyses (PSA) meanwhile represent a highly important and worldwide more and more applied tool for assessing the safety of nuclear power plants. PSA have to be obligatory performed for all nuclear power plants in Germany in the frame of (periodic) safety reviews (SR) required by § 19a of the recent Atomic Energy Act promulgated in April 2002.

A PSA comprises knowledge on the design and operation of the plant as well as the operation experience of the plant being analyzed and insights of the nuclear safety research, but also the general expertise for a comprehensive assessment of the safety status of the nuclear power plant to be analyzed. This assessment provides as far as possible the effects of evident knowledge uncertainties on the results.

The methods for performing have continuously been enhanced. However, there are still open issues with the potential for further methodological developments. This results i. e. from the use of new technologies, changes in the operational modes, and new insights from operation experience feedback leading to new demands with respect to extent and level of confidence of PSA.

Within the framework of the reactor safety research program of BMWi according to the research focus 'Probabilistic Safety Analysis' GRS has therefore enhanced, improved and tested existing methods and tools in the research and development project RS1180 'Development and Test Applications of Methods and Tools for Probabilistic Safety Analyses' for application in future PSA.

The research activities were focused on the following issues:

As a first goal, methods for considering digital, software-based instrumentation and control in probabilistic assessment have been developed. Up to the time being generally accepted methods of this type do not exist. Nevertheless, safety significant software-based I&C is expected to be installed in German nuclear power plants in the frame of a profound modernization in the near future. This is reason for developing an approach for assessing the reliability of digital I&C including the software. In addition, the relevance of the human machine interface of software-based I&C for PSA should be analyzed and an approach for the assessment should be developed. Priority should be given to investigate what the change from analog to digital I&C and the potential corre-

sponding changes in the human machine interface and their consequences for human reliability and human reliability analysis.

As a second goal, the consideration of knowledge based behaviour and organizational influence in PSA should be enhanced. On the one hand, a methodology to identify, investigate and evaluate knowledge based operator behaviour in the context of a PSA has been developed. On the other hand, a methodology for considering the influence of organisational factors on operator performance in the context of a PSA has been provided. The research and development results make it possible to identify, quantify and integrate to the PSA model the safety significance of organisational factors and of the safety management.

Another goal concerned a variety of questions on developing and improving methods with regard to initiating events and to external and internal hazards within a PSA:
Existing methods for determining leak and break probabilities of pressurized components have been improved. A further goal fulfilled was the development of a screening approach for a seismic probabilistic safety analysis (SPSA). This method should enable to detect critical parts of systems at NPP in the case of seismic events in an optimal way beneath scientific and technical points of view. Moreover, first investigations have been carried out to assess the necessity for developing methods for probabilistic assessment of transients caused by high voltage or impacts of external voltages beyond design of electrical equipment.

Another task was to enhance the methods for analyzing the effects of uncertainties on the PSA results and to exclude sources of error in the PSA. In this context, methods for performing uncertainty and sensitivity analyses in dynamic PSA as well as those for adapting beta to given lognormal distributions have been developed. Another goal of the activities was the development and testing of corresponding computer programs to be able to systematically consider relevant epistemic uncertainties from different sources. In addition, a systematic approach for an engineering assessment of the transferability of common cause events observed to the groups of components will be possible to minimize the uncertainties of the estimates within the assessment by different experts has been developed. By means of goPSA a MS WINDOWS® based common user interface with all the necessary tools for Level 1 PSA methods including users guidance has be set up and tested to eliminate several sources of error in the PSA.

The last goal was to improve and test ASTEC with regard to its applicability for accident analyses. The current version of ASTEC has therefore been assessed in view of its suitability for application in Level 2 PSA studies. ASTEC has been successfully validated and compared to MELCOR.

The results of the project provide validated methods for probabilistic safety analysis corresponding to the international state of the art in science and technology. The activities have enhanced the reliability of PSA results with the objective, to secure the confidence in PSA as supplement to the deterministic approach assessing the safety of nuclear power plants. By this, the project contributes significantly to the goals of the nuclear research as mentioned in /BMW 05/.

However, a systematic testing and validation of the enhanced methods in the frame of a reference PSA is still needed.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Zielsetzung

In Wahrnehmung der Kompetenzträgerschaft für die Probabilistische Sicherheitsanalyse (PSA) in Deutschland hat die GRS bereits vor einigen Jahren ein ‘Vier-Säulen-Konzept‘ für Forschungs- und Entwicklungsarbeiten zur PSA erarbeitet. Dieses Konzept sieht vor, die derzeit in Deutschland verfügbaren PSA-Methoden entsprechend dem internationalen Stand von Wissenschaft und Technik weiterzuentwickeln (Säule I), Defizite bei PSA-Methoden durch Neuentwicklungen abzubauen (Säule II), die Werkzeuge für eine effiziente Durchführung von PSA bis zur Stufe 2 zu verbessern (Säule III) sowie neue und weiterentwickelte Methoden und Werkzeuge anhand einer ‘Referenz-PSA‘ zu erproben (Säule IV).

Alle Arbeiten, die in diesem ‘Vier-Säulen-Konzept‘ der GRS vorgesehen sind, sollen die Belastbarkeit von PSA-Ergebnissen absichern sowie die Aussagesicherheit der PSA weiter erhöhen und auf diese Weise die Rolle der PSA als Instrument der Sicherheitsbewertung von Kernkraftwerken - in Ergänzung der deterministischen Vorgehensweise - festigen.

Probabilistische Sicherheitsanalysen für Kernkraftwerke werden in Deutschland seit rund 30 Jahren durchgeführt. Inzwischen gibt es für alle deutschen Kernkraftwerke zumindest eine PSA der Stufe 1 (Ermittlung der Kernschadenshäufigkeit). Obwohl die meisten PSA als Forschungs- und Entwicklungsvorhaben oder als - jedenfalls formal - freiwilliger Beitrag der Betreiber zur Periodischen Sicherheitsüberprüfung (PSÜ) durchgeführt wurden, haben Erkenntnisse aus diesen PSA wesentliche Beiträge zum hohen Sicherheitsniveau der deutschen Kernkraftwerke geliefert.

Seit der Neufassung des Atomgesetzes (AtG) vom April 2002 ist für alle Kernkraftwerke in Deutschland im Rahmen der in § 19a AtG geforderten (Periodischen) Sicherheitsüberprüfungen (SÜ) eine PSA durchzuführen und der zuständigen Aufsichtsbehörde vorzulegen. Umfang und Methoden der PSA sind in dem im November 2005 veröffentlichten Leitfaden Probabilistische Sicherheitsanalyse /BMU 05/ und seinen Fachanhängen (Methodenband /FAK 05/ und Datenband /FAK 05a/) festgelegt.

Die PSA ist inzwischen weltweit ein wichtiges und immer intensiver genutztes Instrument für die Sicherheitsbewertung von Kernkraftwerken. Mit der PSA werden Kenntnisse über die Auslegung und Betriebsweise der Anlage, die Betriebserfahrung der untersuchten und ähnlicher Anlagen sowie Erkenntnisse der Sicherheitsforschung, wie

auch der generelle wissenschaftlich-technische Sachverstand zu einer Gesamtbewertung des Sicherheitszustandes der zu untersuchenden Anlage zusammengeführt. Wissenslücken werden bei dieser Vorgehensweise evident und ihr Einfluss auf das Ergebnis wird - soweit wie möglich - in Form von Ergebnisunsicherheiten quantifiziert. Wie bei jeder Art der Sicherheitsbeurteilung fließen auch in die PSA subjektive Expertenschätzungen ein. Die Methodik der PSA erlaubt es jedoch, den Einfluss von Schätzungen auf das Ergebnis quantitativ zu bewerten.

International wird die PSA im Bereich der Kernenergie auf verschiedenen Gebieten eingesetzt /IAE 01/, /NEA 07/, beispielsweise:

- bei der Auslegung neuer Kernkraftwerke.
- bei Nachrüstungen oder Änderungen bestehender Kernkraftwerke,
- für die Planung von Wartungs- und Instandhaltungsarbeiten,
- bei der Anpassung von Betriebsbedingungen (z. B. erlaubte Zeiten von Unverfügbarkeiten, Testintervalle wiederkehrender Prüfungen),
- bei der Auswertung und Gewichtung betrieblicher Vorkommnisse,
- bei der periodischen Sicherheitsüberprüfung,
- zur Planung von Notfall- und Katastrophenschutzmaßnahmen,
- zur Verbesserung der Ausbildung des Kraftwerkspersonals.

Die PSA liefert belastbare Grundlagen für Entscheidungen über die Notwendigkeit und den Nutzen sicherheitstechnischer Verbesserungen.

Auch für die PSA gilt die bei der Sicherheitsbeurteilung von Kernkraftwerken generell bestehende Forderung, dass Methoden anzuwenden sind, die dem internationalen Stand von Wissenschaft und Technik entsprechen. Zur Erfüllung dieser Forderung reicht es nicht aus, die internationalen Entwicklungen in Bezug auf die Methoden für die PSA (passiv) zu verfolgen. Die Fortschreibung der Anforderungen an eine PSA und deren sachgerechte Begutachtung erfordern auch bei den durch die Aufsichtsbehörden beauftragten Gutachterorganisationen Erfahrungen mit eigenen Analysen.

Der Einsatz neuer Technologien, veränderte Betriebsweisen und neue Erkenntnisse aus der Betriebserfahrung führen zu neuen Anforderungen an die PSA-Methodik. So

sind in den letzten Jahren u. a. folgende sicherheitsrelevante Entwicklungen zu beobachten:

- Softwarebasierte Sicherheits-Leittechnik ersetzt zunehmend die konventionelle Leittechnik und wird in absehbarer Zeit auch sicherheitsrelevante Aufgaben übernehmen.
- Die Betriebserfahrung weist auf die sicherheitstechnische Bedeutung von bisher nicht untersuchten auslösenden Ereignissen (z. B. Fremdspannungseintrag in die Elektro- und Leittechnik) sowie von Einflüssen der Organisation und des Sicherheitsmanagements hin.
- Das im Rahmen einer Sicherheitsbeurteilung zu untersuchende Aufgabenspektrum des Personals hat sich erweitert (u. a. Eingriffe in Situationen, für die keine Prozeduren verfügbar sind).
- Umfang und Detaillierungsgrad der durchzuführenden Untersuchungen erweitern sich (u. a. auf anlageninterne und externe übergreifende Ereignisse, Störfälle im Nichtleistungsbetrieb, Verhalten der Anlage in Unfallsituationen).

Im Vorhaben RS1180 ‘Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen‘ sollen für die nachfolgend aufgeführten fachlichen Themenbereiche vorhandene Methoden und Werkzeuge weiter entwickelt und für die Anwendung in zukünftigen PSA nutzbar gemacht und erprobt werden.

- Methoden zur Bewertung digitaler Leittechnik,
- Berücksichtigung wissensbasierter Personalhandlungen und organisatorischer Einflüsse,
- Methodische Ansätze zur Berücksichtigung auslösender Ereignisse und Einwirkungen von innen und außen in der PSA,
- Berücksichtigung von Unsicherheiten und Ausschluss von Fehlerquellen in der PSA,
- Methodenweiterentwicklung für Unfallszenarien.

Dabei sollen insbesondere die Fragestellungen bearbeitet werden, bei denen eine erhöhte Dringlichkeit für derartige Analysen gegeben ist.

2 Wissenschaftliche und technische Aufgabenstellung

2.1 Entwicklung von Methoden zur probabilistischen Bewertung der Zuverlässigkeit softwarebasierter digitaler Leittechnik

Unter dem Begriff Leittechnik oder Automatisierungseinrichtungen bezeichnet man die Gesamtheit der Einrichtungen zum Ausführen von Leittechnik-Funktionen zum Messen, Steuern, Regeln, Überwachen, Aufzeichnen und Schützen eines Prozesses oder einer Einrichtung. Typische Einsatzgebiete der Leittechnik sind beispielsweise:

- Prozessleittechnik,.
- Kraftwerksleittechnik,
- Netzleittechnik der Energieversorgung,
- Verkehrsleittechnik,
- Leittechnik in der Avionik,
- Fertigungs- bzw. Produktionsleittechnik.

Bereits in der ersten Hälfte des vorigen Jahrhunderts wurden erste leittechnische Einrichtungen mittels Analogtechnik (z. B. Relais, elektrische Messeinrichtungen) realisiert und für einfache Steuerungsfunktionen eingesetzt. In den 60er Jahren lösten festverdrahtete (verbindungsprogrammierte) elektronische Steuerungen zunehmend die Relaistechnik ab und es wurden Prozessrechner für Prozessüberwachung eingeführt. Beginnend in den 80er Jahren wurden in den meisten Industriezweigen zunehmend digitale Automatisierungseinrichtungen, zuerst auf der Basis digitaler integrierter Schaltkreise (IC) und später auf der Basis der Prozessortechnik (u. a. µP - Mikroprozessor, µC - Mikrocontroller, CPU - Zentrale Verarbeitungseinheiten der Rechner) eingesetzt. Mit dem Einzug der rechnerbasierten Automatisierungssysteme wurden zahlreiche Funktionen der Leittechnik im industriellen Bereich auf der Basis von Software realisiert, u. a.:

- Informationsaufbereitung / Messdatenerfassung (u. a. Berechnung des Messwertes, Überwachung des Messbereichs, Kalibrierung),
- Informationsverarbeitung / Logik (u. a. Grenzwertüberwachung, Auswahl- und Steuerlogik, Statusverarbeitung der Signale, Erzeugung von Meldungen),

- Informationsaustausch (u. a. Kommunikation zwischen redundanten Einrichtungen oder Teilsystemen),
- Steuerung verfahrenstechnischer Einrichtungen (z. B. Vorrangsteuerung für Hand- bzw. Automatikbefehle),
- Überwachung und Steuerung der Hardware der Leittechnik (u. a. Betriebssystem, Geräte-Treiber, Netzwerkprotokolle).

In der Industrie wird die Leittechnik immer dann als sicherheitsbezogenes System bezeichnet /DIN 09/, wenn dieses zur Ausführung von einer oder mehrerer Sicherheitsfunktionen erforderlich ist. Die Aufgabe von Sicherheitsfunktionen ist, das Risiko von Prozessen zu minimieren, von denen Gefahren für Mensch, Umwelt und Sachwerte ausgehen. Die Anforderungen an die Leittechnik mit Sicherheitsfunktionen sind anwendungsunabhängig im DIN-IEC-61508-Industriestandard /DIN 09/ formuliert. Dieser Industriestandard beschreibt sowohl die Art der Risikobewertung als auch die Maßnahmen zur Auslegung entsprechender Sicherheitsfunktionen bezüglich ‘Fehlervermeidung und ‘Fehlerbeherrschung‘ und gilt für alle Anwendungen, in denen elektrische, elektronische oder programmierbar elektronische sicherheitsbezogene Systeme zur Ausführung von Sicherheitsfunktionen eingesetzt werden.

Zur Minimierung des Risikos schreiben sowohl DIN-IEC-61508- /DIN 09/ als auch DIN-EN-61511-Standard //DIN 05/ im Wesentlichen folgende Schritte vor:

- Risikodefinition und -bewertung nach detaillierten Versagenswahrscheinlichkeiten vom Sensor über die Steuerung bis hin zum Antrieb über die gesamte Lebensdauer der Komponenten,
- Festlegung und Umsetzung der Maßnahmen zur Minimierung des Restrisikos,
- Einsatz geeigneter Geräte,
- Wiederkehrende Prüfung der korrekten Einhaltung der Sicherheitsfunktionen.

In kerntechnischen Anlagen unterscheidet man beim Einsatz der Leittechnik zwischen Betriebs- und Sicherheitsleittechnik. Dabei ist die Sicherheitsleittechnik die Leittechnik des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung. Für die Sicherheitsleittechnik gelten hinsichtlich Nachweisführung der erforderlichen Zuverlässigkeit zusätzlich die Anforderungen und Empfehlungen des kerntechnischen Regelwerkes (u. a. KTA-Regeln, RSK-Leitlinien).

Die Einführung der softwarebasierten Leittechnik erfolgt auch in die kerntechnischen Anlagen. So wurde bisher schon z. B. die softwarebasierte digitale Sicherheitsleittechnik bei der Modernisierung ausländischer Kernkraftwerke eingesetzt. Neue Reaktoranlagen im Ausland werden generell unter Berücksichtigung des Einsatzes softwarebasierter Leittechnik für praktisch alle Automatisierungsaufgaben ausgelegt. Bei modernen Druckwasserreaktoren vom Typ EPR sind beispielsweise die softwarebasierten Leittechniksysteme sowie die vollständig rechnergestützte Kraftwerkswarte in das Auslegungskonzept integriert (siehe Abb. 2-1).

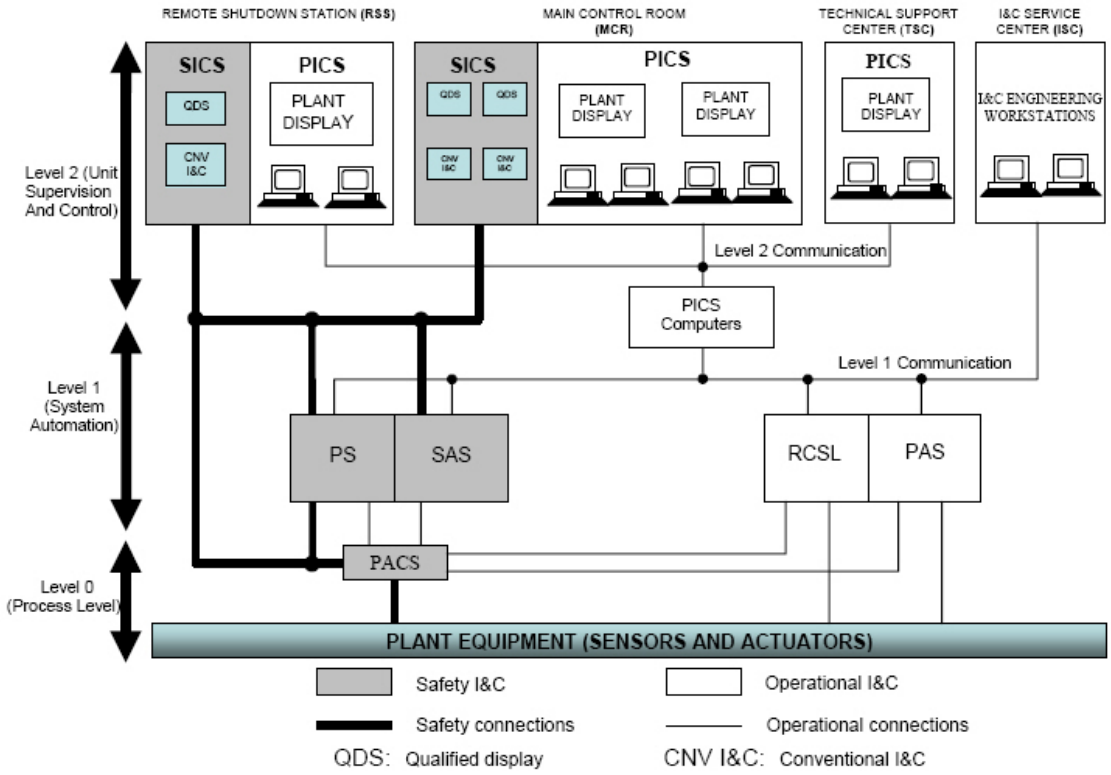


Abb. 2-1 Leittechnikkonzept einer modernen U.S. EPR-Reaktoranlage /KOR 09/

In deutschen Kernkraftwerken hingegen kommt softwarebasierte Leittechnik bisher vorwiegend in betrieblichen und Begrenzungssystemen zum Einsatz, z. B.:

- Prozessrechner zur Beurteilung des Betriebszustandes und zur Aufzeichnung der Prozessparameter,
- Regel- und Begrenzungseinrichtungen für die Durchführung des bestimmungsgemäßen Betriebes der Anlage,
- digitale Messeinrichtungen (u. a. Neutronenflussmessung),

- Steuerung der Brennelementlademaschine,
- Begrenzungssysteme,
- Turbine: Steuer- und Schutzsysteme.

Der Einsatz softwarebasierter Leittechnik mit unmittelbaren Sicherheitsfunktionen ist in absehbarer Zeit auch in deutschen Kernkraftwerken im Rahmen einer Modernisierung der Sicherheitsleittechnik zu erwarten.

Die softwarebasierte Leittechnik unterscheidet sich in Struktur und Funktionsweise wesentlich von der analogen Leittechnik auf Grund spezifischer Eigenschaften, u. a.:

- hohe Integrationsdichte der Schaltkreise der Baugruppen. Die Hersteller elektronischer Baugruppen (Hardware) setzen auf fortschreitende Miniaturisierung von Produkten und auf die Erhöhung der Integrationsdichte zur Verbesserung der Leistungsfähigkeit einzelner Baugruppen (z. B. Multitasking - eine Baugruppe kann eine Vielzahl von Funktionen gleichzeitig ausführen, Co-Prozessoren, interne Speichermanagement),
- flexibler Einsatz der Leittechnik-Baugruppen durch Verwendung einheitlicher Hardware und deren Anpassung durch die Konfiguration- und Anwendungssoftware. Damit kann eine Baugruppe für die Steuerung unterschiedlicher Antriebe (z. B. für Pumpen oder Ventile) mit flexibler Konfiguration der Vorrangsteuerung verwendet werden.
- flexible konfigurierbare Arten der Signal- bzw. Datenübertragung (z. B. LAN-lokale Datennetze (Ethernet), Feldbus - dezentrale Kommunikation (u. a. CAN-Bus, PROFIBUS)) und deren Kombinationen,
- unterschiedliche Architekturen der Signal- bzw. Datenübertragung (u. a. Point-to-Point-, Stern-, Bus- und Ring-Topologien) und deren Kombinationen.

Außerdem haben softwarebasierte leittechnische Einrichtungen in der Regel die erweiterten Möglichkeiten der Fehlerdiagnose und einer fehlertoleranten Funktionsweise (z. B. Fehlerfilterung, erneuter Start der Hardware).

Alle o. g. Merkmale können sowohl das Ausfallverhalten und als auch die Auswirkungsbreite von Fehlern (z. B. unerkannte Ausbreitung fehlerhafter Information im Netzwerk redundanter Einrichtungen) in der Hard- und Software beeinflussen. Ferner

kann die Verwendung softwarebasierter Leittechnik an der Schnittstelle zwischen Mensch und Maschine (vor allem in der Leitwarte und bei der Instandhaltung der rechnergestützten Systeme) zu sicherheitsrelevanten Änderungen in den Mensch-Maschine-Wechselwirkungen führen.

Die Bestimmung der Zuverlässigkeit der Hardware softwarebasierten Leittechnik kann konventionell auf der Grundlage der empirisch gewonnenen Ausfallhäufigkeiten (Ausfallraten) erfolgen und dann deren Ausfälle im Fehlerbaummodell des zu analysierenden Systems berücksichtigt werden. Für die Bestimmung der Ausfallarten der Hardware ist prinzipiell die Methode der Fehlerart- und Auswirkungsanalyse (FMEA) geeignet. Für die probabilistische Bewertung der Software existierten bisher keine anerkannten Methoden. Die bekannten Grundmodelle der Zuverlässigkeits- und Verfügbarkeitsmodellierung technischer Anlagen lassen sich prinzipiell in die Kategorien der kombinatorischen und der zustandsraumorientierten Modelle. Zur Kategorie der kombinatorischen Methoden zählen die Ereignisbaumanalyse, die Fehlerbaumanalyse und der Risikograph (gemäß Industrienorm ISO 13849-1, DIN/IEC 62061). Zu den zustandsraumorientierten Modellen der Zuverlässigkeitsanalyse zählen das Markov-Netz sowie die stochastischen Petri-Netze.

Die wesentlichen Modelle zur Bewertung der Software-Zuverlässigkeit stammen aus einer Phase, die vom Beginn der 70er Jahre bis in die 80er Jahre reicht. In diesem Zeitraum wurde intensiv an dieser Problematik gearbeitet. In der Folge hat sich hinsichtlich der Software-Zuverlässigkeit das Interesse der Industrie vermehrt auf die konstruktive Seite verlagert (fortschrittliche Software-Entwicklungsumgebungen, Standards und Methoden zur Qualitätssicherung der Software), während Software-Zuverlässigkeitsmodelle praktisch nicht mehr weiter entwickelt wurden.

In einem Forschungs- und Entwicklungsvorhaben des BMU (SR 2418) hat die GRS bereits einen ersten Ansatz für eine probabilistische Zuverlässigkeitsbewertung entwickelt /PIL 04/. Die dort durchgeführten Arbeiten zur Zuverlässigkeitsbewertung softwarebasierter Leittechnik haben allerdings gezeigt, dass die konventionelle Methode der Fehlerbaumanalyse der Hardware allein nicht geeignet ist, ein nachvollziehbares Ausfallverhalten eines vernetzten softwarebasierten Leittechniksystems in der PSA zu modellieren. Eine konsequente Behandlung softwarebasierter Leittechnik auch in probabilistischer Sicherheitsanalyse (PSA) erfordert deshalb weiterhin Entwicklungsarbeiten in diesem Bereich. Das Ziel des Vorhabens RS1180 besteht darin, diesen Ansatz zunächst hinsichtlich seiner Realisierbarkeit zu überprüfen und, soweit

erforderlich, dem Stand von Wissenschaft und Technik anzupassen. Dabei sollen die zu entwickelnden Methoden zur Zuverlässigkeitsbewertung der digitalen Leittechnik deren spezifische Eigenschaften einschließlich der Software berücksichtigen und belastbare quantitative Aussagen liefern. Auf den Forschungs- und Entwicklungsbedarf zu diesem Thema wird auch in /BMW 05/ hingewiesen.

Ergänzend soll die Relevanz der Mensch-Maschine-Schnittstelle für die probabilistische Bewertung der Zuverlässigkeit der softwarebasierten Leittechnik untersucht werden. Zunächst ist die Frage zu beantworten, was der Wechsel von analoger zu softwarebasierter Leittechnik und die gegebenenfalls damit verbundenen Änderungen der Schnittstelle zum Menschen (Mensch-Maschine-Schnittstelle, kurz MMS) für die Zuverlässigkeit von Personenhandlungen und deren Bewertung bedeuten. Dazu sollen die neuen Aspekte der MMS softwarebasierter Leittechnik im Hinblick auf die Durchführung der Bewertung der menschlichen Zuverlässigkeit dargestellt werden. Weiterhin soll ein methodischer Ansatz zur Bewertung der menschlichen Zuverlässigkeit in der PSA beim Einsatz softwarebasierter Leittechnik entwickelt werden.

2.2 Berücksichtigung wissensbasierter Personalhandlungen und organisatorischer Einflüsse

2.2.1 Entwicklung von Methoden zur Berücksichtigung wissensbasierter Personalhandlungen in einer probabilistischen Sicherheitsanalyse

Bei Durchführung einer PSA kann es immer wieder zu Ereignisabläufen kommen, die Eingriffe des Personals erfordern, für deren Beherrschung keine Prozeduren und kein Training vorgesehen sind. Das Personal steht in solchen Situationen vor der Aufgabe, ad hoc ein Vorgehen zu entwickeln, mit dem es die Anlage in einen sicheren Zustand bringen, die Diskrepanz zum sicheren Zustand verringern oder zumindest verhindern kann, dass sich der Ist-Zustand weiter verschlechtert. Fälle aus der Betriebserfahrung zeigen, dass das Personal wissensbasierte Handlungen dieser Art ausführt. Eine probabilistische Sicherheitsanalyse (PSA) hat deshalb auch diese Art des Handelns einzubeziehen, um den Beitrag der Personalhandlungen zum Gesamtergebnis möglichst genau zu bestimmen. Mangels geeigneter Methoden ist es bislang aber nicht möglich gewesen, in einer PSA sicherheitstechnisch erforderliche, wissensbasierte Handlungen zu berücksichtigen. Dieser Einschränkung unterliegt auch die Methode, die der Leitfa-

den für die PSA deutscher Kraftwerke vorsieht /FAK 05/, SWA 83/. Aus diesem Sachstand ergab sich der Bedarf für die Entwicklung und Erprobung einer geeigneten Analyse- und Bewertungsmethode.

Im Mittelpunkt steht die Entwicklung einer Methode, mit der das Entscheidungsverhalten des Betriebspersonals, das zu wissensbasierten Handlungen führt, modelliert und untersucht werden kann. Hierbei wird in Übereinstimmung mit den Definitionen im Fachband zu PSA-Methoden /FAK 05/ des PSA-Leitfadens von wissensbasierten Handlungen gesprochen, auch wenn sich die erforderlichen methodischen Entwicklungen auf die Modellierung und Untersuchung der diesen Handlungen vorausgehenden kognitiven Prozesse beziehen.

Das Vorhaben trägt dazu bei, derzeit vorhandene Beschränkungen bei der Durchführung einer PSA zu reduzieren und die Aussagekraft von Ergebnissen probabilistischer Sicherheitsanalysen zu erhöhen. Um dieses Ziel zu erreichen, soll entsprechend den nachstehend beschriebenen Schritten vorgegangen werden.

2.2.2 Probabilistische Bewertung organisatorischer Einflüsse sowie von Einflüssen des Sicherheitsmanagements auf die Zuverlässigkeit von Personalhandlungen

Die Bewertung des Beitrags des Menschen zur Vermeidung und Beherrschung von Störfällen ist eine wesentliche Teilaufgabe der PSA. Leistungsbeeinflussende Faktoren (‘performance shaping factors‘) haben erheblichen Einfluss auf die Wahrscheinlichkeit einer Fehlhandlung. Der Planungsaspekt eines leistungsbeeinflussenden Faktors im Arbeitssystem wird als ‘organisatorischer Einflussfaktor‘ definiert. Damit werden also diejenigen Konzepte charakterisiert, nach denen der Betreiber Arbeitsaufgaben und Arbeitssysteme im Kernkraftwerk gestaltet und die Qualität der durchgeführten Arbeiten überwacht. Um festzustellen, ob ein fehlerfördernder Zustand eines leistungsbeeinflussenden Faktors im Arbeitssystem durch Planungsdefizite hervorgerufen werden kann, müssen

- die dafür zuständigen Arbeitssysteme des Kraftwerks,
- die Maßnahmen zur Gestaltung, Implementierung, Überwachung und Modifikation von Personalhandlungen im Rahmen des Sicherheitsmanagements sowie
- die möglichen übergreifenden Auswirkungen (d. h. auf andere Arbeitssysteme)

in die Bewertung der Zuverlässigkeit einer Personalhandlung einbezogen werden. Eine genauere Betrachtung der empfohlenen Bewertungsmethoden zeigt allerdings, dass Einflüsse des Sicherheitsmanagements nicht oder in nur geringem Umfang berücksichtigt werden können. Ansätze, mit denen die übergreifenden Wirkungen (z. B. auf Handlungsfehler und Fehlerkorrektur- bzw. Fehlerkompensationsmöglichkeiten) organisatorischer Einflüsse und damit auch des Sicherheitsmanagements als einen Teilaspekt organisatorischer Einflussfaktoren untersucht werden können, fehlen gänzlich.

Die deutsche Betriebserfahrung hat gezeigt, dass ungünstig gestaltete organisatorische Einflussfaktoren zu Fehlhandlungen und darüber hinaus zum Versagen von Vorkehrungen zur Fehlerentdeckung und zur Fehlerkompensation geführt haben. In Einzelfällen führte dies zu einer Beeinträchtigung redundanter und diversitärer Systemelemente Anlage. Das Fehlen geeigneter Methoden zur Bewertung solcher Zusammenhänge schränkt die Aussagekraft von der PSA erheblich ein.

In diesem Vorhaben sollen die vorhandenen, bei der probabilistischen Sicherheitsbewertung eingesetzten Methoden so weiterentwickelt werden, dass der Einfluss organisatorischer Faktoren in einer PSA untersucht werden kann. Das Sicherheitsmanagement wird hierbei als Teilmenge der organisatorischen Einflussfaktoren betrachtet. Die in diesem Zusammenhang zu generierenden Daten sollen soweit möglich aus der der GRS vorliegenden Betriebserfahrung zu ausgewählten meldepflichtigen Ereignissen mit den in /GAS 01/ beschriebenen Methoden abgeleitet werden. Reichen die Informationen nicht aus, um entsprechend /GAS 01/ vorzugehen, so werden die Daten entsprechend den in /FAS 03/ dargestellten Vorgehensweisen geschätzt.

Das Vorhaben soll dazu beitragen, vorhandene Beschränkungen bei der Zuverlässigkeitsbewertung von Personalhandlungen zu reduzieren und die Aussagekraft von Ergebnissen probabilistischer Sicherheitsanalysen zu erhöhen.

2.3 Auslösende Ereignisse und Einwirkungen von innen und außen

2.3.1 Weiterentwicklung von Methoden zur Ermittlung von Leck- und Bruchhäufigkeiten druckführender Komponenten

Übergeordnete Zielsetzung dieses Arbeitspaketes ist es, die vorhandenen Methoden zur Ermittlung von Leck- und Bruchhäufigkeiten druckführender Komponenten gemäß dem Stand von Wissenschaft und Technik für die PSA weiterzuentwickeln. Dabei ergeben sich die folgenden Einzelzielsetzungen:

- Es ist eine Schnittstelle zwischen der Anwendung der statistischen Methodik basierend auf der Betriebserfahrung und der Methodik basierend auf Strukturzuverlässigkeitsmodellen zu entwickeln und zu erproben. Dazu sollen Rissverteilungen auf Basis von geeigneten Abfragen der Datenbank KomPass mit meldepflichtigen Ereignissen aus deutschen Kernkraftwerken sowie der OECD/NEA-Datenbank OPDE mit Ereignissen ausländischen Anlagen abgeleitet werden. Diese Verteilungen sollen beispielhaft als Eingabeparameter für Berechnungen mit Strukturzuverlässigkeitsmodellen zur Bestimmung der Leck- und Bruchwahrscheinlichkeiten von Rohrleitungen und Behältern verwendet werden.

- Es sind geeignete Strukturzuverlässigkeitsmodelle für Behälter mit hohem Energieinhalt (Innendruck ≥ 20 bar oder Temperatur ≥ 100 °C) z. B. für den Speisewasserbehälter, zu entwickeln und zu erproben.

- Im Hinblick auf die Nutzung generischer Datensätze für Leck- und Bruchhäufigkeiten sind auf Grundlage der verfügbaren Daten zur Betriebserfahrung mit druckführenden Komponenten Ansätze zur Berücksichtigung und differenzierten Bewertung der Einflüsse verschiedener Schädigungsmechanismen sowie von Prüfkonzepten und Lerneffekten zu entwickeln und zu erproben.

2.3.2 Weiterentwicklung und Erprobung eines Auswahlverfahrens zur Bestimmung von kritischen Anlagenteilen bei einer seismischen probabilistischen Sicherheitsanalyse (SPSA)

Im Fachband zu PSA-Methoden /FAK 05/ des Leitfadens probabilistische Sicherheitsanalysen für Kernkraftwerke wird zur Durchführung seismischer probabilistischer Si-

cherheitsanalysen (SPSA) ein Screening-Verfahren für die Auswahl solcher Anlagenteilen (Bauwerke, Systeme, Komponenten, englisch: structures, systems and components, SSC) vorgeschlagen, für welche intensitätsabhängige Versagenswahrscheinlichkeiten bestimmt werden müssen. Zielsetzung dieses Arbeitspaketes des Forschungs- und Entwicklungsvorhabens RS1180 ist die Entwicklung eines Verfahrens zur optimalen Auswahl kritischer Anlagenteile. Als Ergebnis des Vorhabens wird ein systematisches Auswahlverfahren standardisiert zur sachgerechten Anwendung bereitgestellt. Das Verfahren wird an einem umfassenden Beispiel erprobt und erläutert.

Grob umrissen umfasst eine SPSA folgende Arbeitsschritte:

1. Durchführung einer seismischen Gefährdungsanalyse zur Ermittlung standortspezifischer Häufigkeiten von Erdbebenwirkungen,
2. Ermittlung von erdbebenbedingten Versagenswahrscheinlichkeiten für Bauwerke, Systeme und Komponenten,
3. Berechnung erdbebenbedingter Gefährdungs- und Kernschadenszustände.

Das Vorhaben umfasst insbesondere vorbereitende methodische Untersuchungen zum zweiten Arbeitsschritt der seismischen PSA. Es ist nicht möglich, die erdbebenbedingten Versagenswahrscheinlichkeiten für alle Bauwerke, Systeme und Komponenten eines Kernkraftwerks zu bestimmen. Deshalb ist durch ein Auswahlverfahren die Anzahl der im Detail zu analysierenden Bauwerke, Systeme und Komponenten des Kernkraftwerks auf der Grundlage zu definierender Auswahlkriterien schrittweise zu reduzieren.

Durch Anwendung eines solchen Auswahlverfahrens wird sichergestellt, dass nur solche Bauwerke, Systeme und Komponenten in die nachfolgende Quantifizierung einbezogen werden (Arbeitsschritte 2 und 3), von denen erwartet werden kann, dass ihr erdbebenbedingter Ausfall nennenswert zu den Gefährdungs- und Kernschadenszuständen beiträgt.

Das Auswahlverfahren soll anhand eines konkreten umfassenden Beispiels effektiv entwickelt und überprüft werden.

2.3.3 Untersuchungen zum Bedarf einer Methodenentwicklung für eine probabilistische Bewertung von Transienten aufgrund von Überspannungen oder Fremdspannungseinträgen

Ziel dieses Arbeitspaketes ist es, im Sinne einer Vorstudie den aktuellen Stand von Wissenschaft und Technik bei der probabilistischen Bewertung von Überspannungstransienten zu erfassen und die Möglichkeiten der Entwicklung bzw. Fortentwicklungen von Methoden aufzuzeigen, mit denen die Einwirkungen von Überspannung oder Fremdspannung auf sicherheitstechnisch wichtige Anlagenteile eines Kernkraftwerkes im Rahmen einer PSA probabilistisch bewertet werden können. Diese Einwirkungen werden in den PSA für deutsche Kernkraftwerke bislang nur unzureichend berücksichtigt, da keine geeigneten Methoden zur Verfügung stehen.

In diesem Vorhaben sollen

- der Stand von Wissenschaft und Technik für eine Bewertung von Überspannungen bzw. Fremdspannungen ermittelt,
- die Wirksamkeiten der in den Kernkraftwerken vorhandenen Schutzmaßnahmen untersucht und
- die in der GRS verfügbare Betriebserfahrung zu Ereignissen mit Einwirkungen durch Überspannung bzw. Fremdspannung ausgewertet

werden.

Im Einzelnen ergeben sich daher folgenden Aufgaben:

- Feststellung des internationalen Standes von Wissenschaft und Technik zu PSA-Methoden zur Bewertung von Überspannungstransienten (Ermittlung des PSA-Status),
- Systemtechnische Analyse zur Wirksamkeit der in deutschen Kernkraftwerken vorhandenen Maßnahmen zur Vermeidung des Eintrags von Überspannung auf die Energieversorgung des Sicherheitssystems sowie auf die Sicherheitsleittechnik,
- Auswertung der in deutschen und ausländischen Kernkraftwerken aufgetretenen Ereignisse (Besondere Vorkommnisse, IRS-Meldungen).

Die Ereignisse werden sowohl hinsichtlich der aufgetretenen Phänomene als insbesondere auch im Hinblick auf ihre methodische Berücksichtigung im Rahmen der probabilistischen Bewertung ausgewertet. Sofern eine Relevanz erkennbar ist, sind die Phänomene und die sich daraus ergebenden Anforderungen bei einer Methodenentwicklung zu berücksichtigen.

- Ermittlung der Anforderungen für eine zu entwickelnde Methode zur probabilistischen Quantifizierung des Risikos aufgrund von Überspannungen bzw. Fremdspannungseinträgen

Im letztgenannten Arbeitspunkt sollen ggf. vorhandene Defizite der existierenden Methoden zur probabilistischen Bewertung von Transienten mit Überspannung bzw. Fremdspannungen dargestellt werden. Mit Hilfe der Auswertungen und Untersuchungen sollen die Relevanz sowie die Möglichkeiten einer Entwicklung bzw. Weiterentwicklung von Methoden zur probabilistischen Bewertung von Transienten mit Überspannungen bzw. Fremdspannungseinträge aufgezeigt werden.

2.4 Methodenentwicklung zur Analyse des Einflusses von Unsicherheiten auf PSA-Ergebnisse und zum Ausschluss von Fehlerquellen in der PSA

2.4.1 Bereitstellung von Methoden zur Durchführung von Unsicherheits- und Sensitivitätsanalysen in probabilistischen Dynamikanalysen (dynamische PSA)

Um die übliche Unsicherheits- und Sensitivitätsanalysen im Rahmen einer probabilistischen Dynamikanalyse mit MCDET (*M*onte *C*arlo *D*ynamic *E*vent *T*ree) durchführen zu können, muss eine getrennte Berücksichtigung aleatorischer und epistemischer Größen erfolgen. Dies erfolgt normalerweise durch eine zweistufig geschachtelte Monte Carlo-Simulation. In der äußeren Simulationsschleife werden Werte der epistemischen Größen variiert. In der inneren Simulationsschleife wird der Einfluss der aleatorischen Größen auf die Ergebnisse unter der Bedingung der jeweils gegebenen epistemischen Werte der äußeren Schleife ermittelt. Jede innere Simulation liefert ein probabilistisches Ergebnis unter der Bedingung der in der äußeren Schleife ausgespielten Werte des epistemischen Vektors. Als Ergebnis der zweistufig geschachtelten Simulation erhält man schließlich eine Stichprobe solcher bedingten probabilistischen

Ergebnisse, die dann in geeigneter Weise einer Unsicherheits- und Sensitivitätsanalyse zugeführt werden können.

Wenn im Rahmen der probabilistischen Dynamikanalyse mit MCDET der zugrundeliegende deterministische Rechencode, der zur Simulation des betreffenden Stör- bzw. Unfallablaufs verwendet wird, sehr rechenzeitintensiv ist, wird die zweistufig geschachtelte Monte Carlo-Simulation in der Regel nicht praktikabel sein. Vielmehr erfolgt bei rechenzeitintensiven Analysen eine gleichzeitige Variation aleatorischer und epistemischer Größen. Um gemäß dem Stand von Wissenschaft und Technik dennoch epistemische Unsicherheits- und Sensitivitätsaussagen im Rahmen einer probabilistischen Dynamikanalyse zu ermöglichen, müssen dazu entsprechende Methoden entwickelt werden, mit denen man mit möglichst geringem zusätzlichen Rechenaufwand verwertbare Unsicherheits- und Sensitivitätsaussagen herleiten kann.

Die Zielsetzung dieses Arbeitspaktes besteht demzufolge in der Entwicklung und Erprobung entsprechender Methoden.

2.4.2 Bereitstellung einer Methodik zur Anpassung von Beta-Verteilungen an vorgegebene Lognormal-Verteilungen unter Berücksichtigung zusätzlicher Benutzervorgaben

Zur Quantifizierung der Unsicherheit von Zuverlässigkeitskenngrößen, wie z. B. Ausfallraten bzw. Versagenswahrscheinlichkeiten pro Anforderung von Systemkomponenten oder Versagenswahrscheinlichkeiten menschlicher Handlungen, wurde in probabilistischen Sicherheitsanalysen bislang die Lognormal-Verteilung verwendet, ohne die speziellen Eigenschaften der zu schätzenden Zuverlässigkeitskenngrößen zu unterscheiden.

Lognormal-Verteilungen sind definiert auf dem rechtsseitig unendlichen offenen Intervall (0, ∞). Wenn sie Werte größer als eins mit einer nicht zu vernachlässigenden subjektiven Wahrscheinlichkeit zulassen, sind sie prinzipiell ungeeignet, die Unsicherheiten von Versagenswahrscheinlichkeiten für technische Systeme oder von Wahrscheinlichkeiten für fehlerhaft durchgeführte Personalhandlungen zu quantifizieren. Denn Werte größer als eins sind definitionsgemäß für Wahrscheinlichkeiten unzulässig. Es ist daher in gewissen Fällen erforderlich, die ‘problematischen‘ Lognormal-

Verteilungen durch besser geeignete Verteilungen zu ersetzen. Als geeignete Verteilungen bieten sich in diesem Zusammenhang die Beta-Verteilungen an.

Da in den vergangenen Jahrzehnten die Unsicherheiten von Zuverlässigkeitskenngrößen für PSAs ausschließlich in Form von Log-Normal-Verteilungen angegeben wurden, liegen diese Informationen in den jeweiligen Datenbanken folglich auch nur in Form der entsprechenden Parameter von Log-Normal-Verteilungen vor. Eine erneute Schätzung aus den riesigen Datenmengen unter Verwendung von Schätzmethoden, die zu geeigneteren Verteilungen zur Beschreibung der Kenntnisstandunsicherheiten für die interessierenden Zuverlässigkeitskenngrößen führen, würde einen sehr großen Aufwand bedeuten. Insbesondere gilt dies auch für die Zuverlässigkeitskenngrößen, die für die Analyse der menschlichen Zuverlässigkeit bereits ermittelt worden sind.

Um die vorliegenden Informationen zu den Unsicherheiten von Versagenswahrscheinlichkeiten dennoch in künftigen PSAs verwenden zu können, müssten die entsprechenden Lognormal-Verteilungen in besser geeignete Beta-Verteilungen transformiert werden.

In diesem Vorhaben sollten deshalb mathematische Methoden für eine solche Transformation entwickelt werden. Diese Methoden sollten in einem benutzerfreundlichen Tool realisiert werden, welches dem Experten eine schnelle und leichte Umwandlung der gegebenen Lognormal-Verteilungen in eine entsprechende Beta-Verteilung ermöglicht.

2.4.3 Entwicklung von Methoden zur konsistenten und umfassenden Berücksichtigung epistemischer Unsicherheiten in Verteilungen von Zuverlässigkeitskenngrößen

Wenn Unsicherheitsquellen nicht explizit im Modell zur Schätzung von Zuverlässigkeitskenngrößen berücksichtigt werden, ist es nicht möglich, den Einfluss der nicht im Schätzmodell berücksichtigten Unsicherheitsquellen auf die Schätzunsicherheiten der Zuverlässigkeitskenngrößen zu quantifizieren. Aus diesem Grund wird von der GRS eine nachträgliche Varianzerhöhung (Verbreiterung) der Verteilungen von Zuverlässigkeitskenngrößen vorgeschlagen, um deren potentiellen Einfluss zumindest in grober Näherung in die Schätzverteilungen der Zuverlässigkeitskenngrößen einfließen zu lassen.

Das Ziel dieses Arbeitspunktes besteht in der grundlegenden Untersuchung zur Bewertung der Frage, ob die nachträgliche Varianzerhöhung von Schätzverteilungen generell eine sinnvolle Methode darstellt, um den Einfluss zusätzlicher Unsicherheitsquellen auf die sich aus den Schätzmodellen ergebenden Verteilungen von Zuverlässigkeitskenngrößen zu berücksichtigen. Dazu werden der mathematische Hintergrund des bisher in der GRS verwendeten Verfahrens, welches ausschließlich nur auf Lognormal-Verteilungen angewendet werden kann, ausführlich beschrieben sowie die damit verbundenen Einschränkungen und kritischen Aspekte diskutiert. Um die Einschränkungen und Schwachstellen des bisherigen, auf Lognormal-Verteilungen basierenden Verfahrens zu vermeiden, wird aufbauend auf der im Rahmen des BMU-Vorhabens SR 2595 entwickelten Methode /SON 01a/, /SON 06/ und /STI 09/ ein neues Verfahren zur Varianzerhöhung von Verteilungen vorgeschlagen, welches allgemein auf beliebige parametrische wie nicht-parametrische Schätzverteilungen von Zuverlässigkeitskenngrößen angewendet werden kann. Dabei handelt es sich insbesondere um Zuverlässigkeitskenngrößen, die eine Wahrscheinlichkeit ausdrücken, wie z. B. Ausfallwahrscheinlichkeiten pro Anforderung für unabhängige Komponentenausfälle, Wahrscheinlichkeiten gemeinsam verursachter Ausfälle (GVA) und Wahrscheinlichkeiten menschlicher Fehlhandlungen.

2.4.4 Methodenentwicklung zur konsistenten Berücksichtigung gemeinsam verursachter Ausfallereignisse (GVA) in PSA

Mit diesem Arbeitspaket wird das Ziel verfolgt, das Vorgehen bei der ingenieurmäßigen Bewertung der Übertragbarkeit beobachteter Ereignisse aus gemeinsamer Ursache (GVA-Ereignisse) auf die in der PSA zu bewertenden Komponentengruppen durch die Entwicklung eines Verfahrensrahmens zu systematisieren. Die Bewertung der Übertragbarkeit ist für die Ermittlung von GVA-Wahrscheinlichkeiten notwendig, da auf Grund der geringen Anzahl beobachteter GVA-Ereignisse die Betriebserfahrung für ähnliche Gruppen von Komponenten zusammenzufassen und die Unterschiede im technischen Aufbau, der Betriebsweise etc. zu berücksichtigen sind. Insgesamt sollen damit die Unsicherheiten der Schätzung bei der Bewertung durch unterschiedliche Experten minimiert werden.

In probabilistischen Sicherheitsanalysen (PSA) erfordert die Ermittlung von GVA-Daten die Zusammenführung von Ergebnissen aus verschiedenen Auswerte- und Bewertungsschritten. Bei jedem Schritt sind Parameter zu ermitteln, die in die Berechnung

der GVA-Daten einfließen. Für die Verknüpfung der einzelnen Schritte und für eine qualitätsgesicherte Übergabe und Dokumentation der zur Berechnung der GVA-Wahrscheinlichkeiten verwendeten Parameter soll ein geschlossenes Programmsystem erstellt werden. Damit sollen eine möglichst rationelle Bearbeitung und qualitätsgesicherte Ergebnisse gewährleistet werden.

2.4.5 Bereitstellung einer Benutzeroberfläche mit den erforderlichen Hilfsprogrammen für PSA-Methoden der Stufe 1 zum Ausschluss von Fehlerquellen

Ziel dieses Arbeitspakets war es, die für die Erstellung einer PSA der Stufe 1 und der Schnittstelle zur Stufe 2 erforderlichen Hilfsprogramme der GRS unter einer MS WINDOWS©-basierten Benutzeroberfläche – direkt oder über eine Schnittstelle – zur Verfügung zu stellen. Dabei sollten die vorhandenen PSA-Programme berücksichtigt und – soweit erforderlich – weiterentwickelt werden.

Mit den unter einer MS WINDOWS©-basierten Benutzeroberfläche zusammengefassten Hilfsprogrammen sollte die Effizienz der Analysen gesteigert, deren Fehlerquellen verringert sowie die Nachvollziehbarkeit und Überprüfbarkeit der PSA verbessert werden. Damit wird ein benutzerfreundlicher Einsatz von Methoden ermöglicht, die von der GRS entsprechend den Anforderungen an eine nach Stand von Wissenschaft und Technik durchgeführte PSA entwickelt wurden und die mit dem in Deutschland überwiegend verwendeten PSA-Rechenprogramm RiskSpectrum® bisher nicht effizient eingesetzt werden konnten.

2.5 Untersuchung der PSA-Tauglichkeit des Integralcodes ASTEC für Unfallanalysen unter Einbeziehung neuerer Erkenntnisse zum Radionuklidverhalten

In der Vergangenheit hat die GRS Studien zu PSA der Stufe 2 mit dem US-amerikanischen Integralcode MELCOR (*M*ethods for *E*stimation of *L*eakages and *C*onsequences *o*f *R*eleases) durchgeführt und punktuell mit den Systemcodes ATHLET und COCOSYS (bzw. deren Vorgängercodes) abgesichert /SON 98/, /SON 01/, /SON 06/. Seit gut 15 Jahren entwickelt die GRS gemeinsam mit der französischen Partnerorganisation IRSN (*I*nstitut de *R*adioprotection et de *S*ûreté *N*ucléaire) den Integralcode

ASTEC (*A*ccident *S*ource *T*erm *E*valuation *C*ode), der auf Dauer MELCOR in der GRS ersetzen soll. Die Entwicklung von MELCOR bei Sandia National Laboratories (SNL) erfolgt im Auftrag der U.S. NRC seit den späten 80er Jahren. Die Zielsetzung beider Programme ist es, den Ablauf von Unfällen (Szenarien mit Kernzerstörung), in der Regel ausgehend vom Nennleistungsbetrieb einer Anlage, bis zur Freisetzung von Radionuklide in die Umgebung zu berechnen. Während ASTEC in den zurückliegenden Jahren zunächst für Anlagen mit Druckwasserreaktor (DWR) entwickelt wurde, kann MELCOR für DWR und SWR (Siedewasserreaktoren) eingesetzt werden.

In diesem Arbeitspaket soll die aktuelle Version von ASTEC auf ihre Tauglichkeit für den Einsatz in einer PSA der Stufe 2 erprobt werden. Es ist vor allem zu untersuchen, inwieweit mit ASTEC in vertretbarer Zeit die für eine solche PSA erforderlichen integralen Unfallanalysen /FAK 05/ mit den PSA-spezifischen, unterschiedlichen Randbedingungen entsprechend dem Stand von Wissenschaft und Technik durchgeführt werden können.

Die in der Vergangenheit gewonnenen Ergebnisse und Erfahrungen sollen so aufbereitet werden, dass sie als Maßstab zur Bewertung der Qualität von Unfallanalysen im Allgemeinen und diesem Fall von ASTEC im Besonderen dienen können.

Über diese Eignungsuntersuchung hinaus sollen diese Arbeiten auch einen Beitrag zur Klärung des Einflusses unterschiedlicher Modellierungen in verschiedenen Rechenprogrammen auf die PSA-Ergebnisse leisten. Zu diesem Zweck werden die Analysen mit ASTEC den Analysen mit dem Rechenprogramm MELCOR gegenübergestellt. Dabei ist insbesondere das Aerosol- und Spaltproduktverhalten in der Kernregion im Verlauf des Transports durch den Kühlkreislauf bis zum Freisetzungsort in den Sicherheitsbehälter (Containment) und im Containment selbst von Interesse. Dort beeinflussen die auftretenden Phänomene die Radionuklidfreisetzung aus dem Containment (den so genannten Quellterm) und damit ein wesentliches Endergebnis der PSA der Stufe 2.

3 Durchgeführte Arbeiten

3.1 Methoden zur probabilistischen Bewertung softwarebasierter digitaler Leittechnik

Zu Beginn des BMWi-Vorhabens RS1180 plante die GRS die Weiterentwicklung des Konzepts zur probabilistischen Bewertung softwarebasierter Leittechnik aus einem Forschungs- und Entwicklungsvorhaben des BMU /PIL 04/ fortzusetzen. Hierzu war es erforderlich, die Konzeptansätze anhand des aktualisierten Standes von Wissenschaft und Technik zu überprüfen. Dementsprechend wurden vertiefte Recherchen zu Methoden der Zuverlässigkeitsbewertung der Hard- und Software einschließlich der Mensch-Maschine-Schnittstelle durchgeführt.

Der Schwerpunkt der Literaturstudie lag in der Auswertung der Ergebnisse aus den aktuellen Forschungsprojekten der U.S. NRC zum Thema ‘Zuverlässigkeitsbewertung digitaler Leittechnik‘ (vgl. Abb. 3-1), insbesondere:

- NUREG/CR-6901: Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments/NRC 06/,
- NUREG/CR-6942: Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments/NRC 07/,
- NUREG/CR-6962: Traditional Probabilistic Risk Assessment Methods for Digital Systems/NRC 08/,
- NUREG/CR-6842: Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants /NRC 04/.

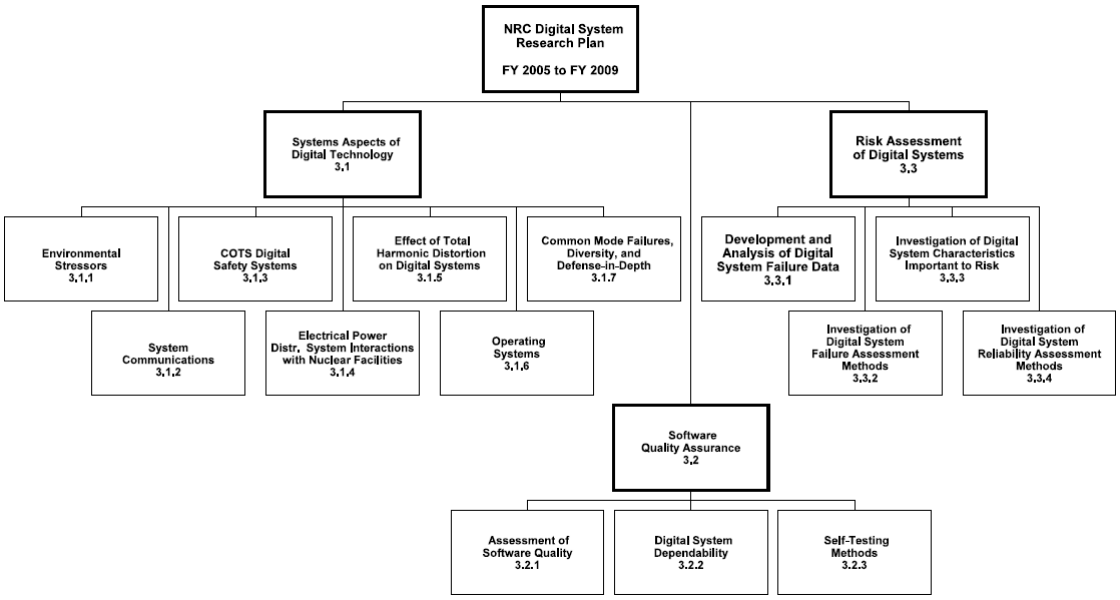


Abb. 3-1 Übersicht zum Forschungsvorhaben der U.S. NRC: 'U.S. Nuclear Regulatory Commission Strategic Plan for FY 2004 – FY 2009' (NUREG-1614 /NRC 00/)

Weitere Recherchen umfassten unter anderem:

- relevante Berichte des BMWi-Forschungsvorhabens 'VeNuS' über das 'Vorgehen zum effizienten Nachweis der Benutzbarkeit und Sicherheit rechnergestützter Leittechniksysteme' /GLO 07/, /GLO 08/,
- relevante Beiträge bei Fachkonferenzen wie PSAM9 und PSAM10 sowie Forschungsberichte des OECD Halden Reactor Project, u. a.:
  - Beiträge zum Thema 'PRA Modeling of Digital Instrumentation and Control Systems' /PSA 08/ und /PSA 10/,
  - Beiträge zu den Themen 'Quantitative Dependability Assessment', 'Fault Tolerance and Error Propagation' auf der Web-Seite des HRP-Projekts: www.ife.no/hrp,
- Informationsquellen (u. a. Veröffentlichungen, Konferenzbeiträge) zum Einsatz digitaler Leittechnik bei sicherheitsrelevanten Anwendungen im nicht-nuklearen Bereich (u. a. Flugzeug- und Automobilindustrie, Bahntechnik) betreffend:
  - Risikomanagement für sicherheitskritische Software-Systeme, Publikation Fraunhofer Institutes für Experimentelles Software Engineering (IESE),

- Publikationen zum Thema ‘Zuverlässigkeitsbewertung der Software‘ der Organisationen des U.S. Departments of Defense (RIAC - Reliability Information Analysis Center und DACS - Data & Analysis Center for Software, www.thedacs.org),
- Vorträge und Publikationen zum Thema ‘Sicherheit und Zuverlässigkeit von Fly-by-Wire Systemen im Flugzeug‘ (ILS Institut für Luftfahrtsysteme, Universität Stuttgart, www.ils.uni-stuttgart.de).

Hinzu erfolgte eine Teilnahme von Fachleuten der GRS an diversen nationalen und internationalen Veranstaltungen, wie der

- Tagung ’SAFECOMP 2007’ in Nürnberg,
- Meeting zum Thema ’Halden Reactor Project, MTO R&D, Topic: Software Systems Dependability’, 2007 in Hamburg,
- OECD-HRP-Summer School on Design and Evaluation of Human System Interfaces in Halden (Norwegen), 2008,
- Technical Meeting on Common Cause Failures in Digital Instrumentation and Control Systems of Nuclear Power Plants, Bethesda, Maryland, USA, 2007
- IAEA Technical Meeting ’Integrating Analog and Digital Instrumentation and Control Systems in Hybrid Main Control Rooms at Nuclear Power Plants’ in Toronto, Canada, November 2007,
- Technical Meeting on Digital I&C Reliability, OECD-NEA, WGRisk Digital I&C, Paris, October 21-24, 2008,
- Halden Programme Group’s Workshop on Common Cause Failures, Garching, 2009,
- Internationale Fachkonferenzen PSAM 9 im Jahr 2008 und PSAM 10 im Jahr 2010.

Die Mitarbeit der GRS-Experten in der internationalen DICRel-Arbeitsgruppe (Arbeitsgruppe der OECD/NEA CNSI WGRisk) hat wichtige Impulse zur Weiterentwicklung des GRS-Konzeptes geliefert. In der Veranstaltung in Paris, 21. - 24.10.2008 fand neben Fachvorträgen (u. a. zur Anwendung dynamischer PSA-Methoden) eine ausführliche Diskussion des Standes probabilistischer Modellierung softwarebasierter Leittechnik bezüglich der angewandten Methoden und der zur Quantifizierung verwendeter Daten

anhand eines Fragenkataloges statt. Die Ergebnisse der Umfrage und der Diskussionen wurden in einem Bericht /NEA 09/ dokumentiert.

Die GRS wurde zudem im Oktober 2008 von der U.S. NRC ersucht, an einem Review des Berichtes der Brookhaven National Laboratory ‘Modeling a Digital Feedwater Control System (DFWCS) Using Traditional Probabilistic Risk Assessment Methods‘ /CHU 08/ teilzunehmen. Die GRS hat die darin vorgestellte Fehlerbaummodellierung der softwarebasierten Leittechnik der Speisewasserregelung in einem Siedewasserreaktor (SWR, englisch: BWR) hinsichtlich der Anwendbarkeit dieser Methode für generische Sicherheitsleittechnik in der PSA analysiert und die Ergebnisse in einer Technischen Notiz (siehe Anhang zum Fachbericht /AP1a/ PIL 10/) festgehalten.

Auf der Grundlage der vorgenannten Literaturrecherchen sowie einer Analyse der digitalen Leittechnik eines sicherheitsrelevanten Systems im Vorhaben SR 2418 /PIL 04/ wurde ein Konzept zur Modellierung softwarebasierter Sicherheitsleittechnik weiterentwickelt. Im Vorhaben wurde auf den anfangs geplanten Einsatz zustandsraumorientierten Modelle zur Zuverlässigkeitsbewertung dynamischer Wechselwirkungen der Hard- und Software (z. B. Anwendung der Markov-Methodik, Petry-Netze) verzichtet, weil bisher weltweit kein deutlicher Fortschritt hinsichtlich Verifizierung, Nachvollziehbarkeit der Quantifizierung zustandsraumorientierter Modellierung komplexer Strukturen softwarebasierter Sicherheitsleittechnik erreicht wurde. Für die Konzeptentwicklung wurden auf der Basis der o. g. Erfahrungen zunächst folgende Randbedingungen festgelegt.

Der Modellansatz im neuen Konzept sollte eine Plattform für eine Analyse einer generischen auf der TELEPERM-XS-System basierten Sicherheitsleittechnik darstellen, um die Auswirkungen potentieller Fehler der Hard- und Software in einem Kernkraftwerk probabilistisch zu analysieren. TELEPERM-XS ist ein softwarebasiertes Leittechniksystem der Firma AREVA. Zurzeit planen einige deutsche Betreiber das derzeit existierende, festverdrahtete Reaktorschutzsystem gegen das TELEPERM-XS-System auszutauschen.

- Das Konzept sollte weiterhin die Methode traditioneller Fehlerbaumanalyse der Baugruppenausfälle der Leittechnik (Hardware) nutzen und die geeigneten Schnittstellen zur Berücksichtigung potentieller Software-Fehler vorsehen.
- Um einen adäquaten Detaillierungsgrad der Fehlerbaummodellierung der Hardware zu erreichen, sollte die Struktur des Modells ausgehend vom

unerwünschten Ereignis, durch eine schrittweise Aufgliederung bis auf Basisereignisse mithilfe logischer Verknüpfungen, erfolgen. Die Aufgliederung der Fehlerbäume sollte so erfolgen, dass

- Basisereignisse keine gemeinsamen funktionellen Abhängigkeiten besitzen bzw. zu verschiedenen verfahrenstechnischen Konsequenzen (z. B. Ausfall redundanter Pumpen und Ausfall gemeinsamer Ölversorgung der Pumpen) führen können,
- die Eintrittswahrscheinlichkeit von Basisereignissen für die Hardwareausfälle möglichst aus der Betriebserfahrung ermittelbar ist,
- die relevanten Folgefehler im Modell berücksichtigt werden. Unter Folgefehler werden Ausfälle von Einheiten verstanden, die dadurch verursacht werden, dass sie übergreifenden Einwirkungen als Folge von Ausfällen anderer Einheiten ausgesetzt werden. Ein Beispiel auf dem Gebiet der Software ist eine Anwendungssoftware, die Ressourcen nicht wieder freigibt und so zum Ausfall anderer Anwendungsprogramme (z. B. andere Leittechnik-Funktionen) oder des Betriebssystems (die Software, die den Betrieb eines Rechners ermöglicht) und hiermit zum Ausfall des gesamten Systems führt.

Bei der Modellierung der Softwarefehler in einem Fehlerbaummodell ist die Wahl der Detaillierung bzgl. der Software ein zentrales Problem, zu welchem auch international noch kein etablierter Ansatz zur probabilistischen Bewertung der Softwarezuverlässigkeit zur Verfügung steht. Für die Konzeptentwicklung wurde festgelegt, zunächst die Software jedes einzelnen Rechners grob zu skizzieren, und danach auf die Ausfallart orientierte Module (Basiselemente, die Auswirkung potentieller Softwarefehler repräsentieren sollen) aufzuteilen:

- Module der Anwendungssoftware, die spezifische Leittechnik-Funktion (LEFU) ausführen; LEFU können Funktionen zum Messen, Steuern, Regeln, Überwachen, Aufzeichnen und Schützen eines Prozesses oder einer Einrichtung sein;
- Betriebssystem eines Rechners: Ein Betriebssystem ist die Software, die den Betrieb eines Rechners ermöglicht. Es verwaltet u. a. Speicher, Ein- und Ausgabegeräte, den Datenaustausch und steuert die Ausführung der Anwendungssoftware.

Diese Vorgehensweise bietet den Vorteil, dass die Ausfallarten relativ einfach, z. B. mit Hilfe der Fehlerart- und Auswirkungsanalyse, festgelegt werden können.

Bei der Konzeptentwicklung soll die Frage beantwortet werden, wie die möglichen funktionalen Abhängigkeiten der unterschiedlichen Software und die Folgefehler im Fehlerbaum korrekt modelliert werden können. So ist es denkbar, dass das Betriebssystem eines Rechners als Folge eines Fehlers der Anwendungssoftware (z. B. Modul LEFU X) versagt. Die weiteren Module (LEFU Y, Z) dieses Rechners sind funktional vom Betriebssystem abhängig und können demzufolge auch ausfallen. Der o. g. Ansatz sollte helfen, die funktionale Abhängigkeit und die Ausbreitung von Folgefehlern im Fehlerbaummodell zu analysieren.

Im Rahmen des BMU-Vorhabens SR 2418 wurde ein Bewertungsverfahren für die Komplexität der Software entwickelt, in dem die Zuverlässigkeit verschiedener Softwarekomponenten (u. a. verschiedene Module der Anwendungssoftware) eines softwarebasierten Leittechniksystems quantitativ in Beziehung (z. B. über so genannte Komplexitätsmaße) gesetzt werden sollte. Diese Vorgehensweise hat allerdings den entscheidenden Nachteil, dass zunächst die Quantifizierung der Zuverlässigkeit eines der zu vergleichenden Softwaremodule erfolgen sollte. Dafür steht ebenfalls keine anerkannte Methode zur Verfügung. Um eigene methodische Ansätze zur Ermittlung von Zuverlässigkeitskenngrößen softwarebasierten Leittechnik weiterentwickeln zu können, wurde im aktuellen Vorhaben ein Versuch unternommen die Betriebserfahrung eines softwarebasierten Leittechniksystems hinsichtlich Häufigkeit und der Quellen der im System intern erfassten Fehler auszuwerten. Dazu wurden die Protokolldateien aus acht Jahren Betrieb eines softwarebasierten Begrenzungssystems erfasst und hinsichtlich Häufigkeit des Auftretens der Fehler und weiteren Korrelationen (z. B. Zusammenhang mit einer bestimmten Baugruppe) ausgewertet.

In Rahmen des Vorhabens wurde ein weiterer Aspekt der Einführung softwarebasierter Leittechnik untersucht, was der Wechsel von analoger zu softwarebasierter Leittechnik und den damit zu erwartenden Änderungen der Schnittstelle der Mensch-Maschine-Schnittstelle (MMS) für die Zuverlässigkeit von Personenhandlungen und deren Bewertung in der PSA bedeutet. Die Literaturrecherchen zum Thema ‘Mensch-Maschine-Schnittstelle‘ konzentrierten sich zunächst auf die Identifikation der Änderungen (u. a. Gestaltung der Schnittstellen, Handlungen), welche sich bei der Einführung von softwarebasierter Leittechnik für das Personal in einem Kernkraftwerk ergeben.

Danach wurde für die Entwicklung eines methodischen Ansatzes ein generisches Referenzsystem in Anlehnung an die Leittechnik-Konzepte der Gerätesysteme TELEPERM XS (AREVA) und SPPA-T2000 (vormals TELEPERM XP, Siemens) und deren Mensch-Maschine-Schnittstelle untersucht. Für die Identifizierung der spezifischen Aspekte der Mensch-Maschine-Schnittstelle softwarebasierter Leittechnik wurde folgende Vorgehensweise gewählt:

- Identifizierung neuer Aspekte von softwarebasierter Leittechnik bei fertigkeits- und regelbasierten Handlungen,
- Identifizierung neuer Aspekte von softwarebasierter Leittechnik bei schädlichen Eingriffen.

Die Analyse erfolgte auf folgender Basis:

- Theoretische Untersuchung der Interaktionsmöglichkeiten mit dem System TELEPERM XS,
- Untersuchung eines praktischen Beispiels der Füllstandsimulation mit dem Servicegerät,
- Gestaltungsrichtlinien der U.S. NRC zur MMS /OHA 02/.

Im Technischen Fachbericht /AP1/ HAR 10/ sind die identifizierten spezifischen Aspekte der Mensch-Maschine-Schnittstelle softwarebasierter Leittechnik dargestellt.

3.2 Berücksichtigung wissensbasierter Personalhandlungen und organisatorischer Einflüsse

3.2.1 Methoden zur Berücksichtigung wissensbasierter Personalhandlungen in einer probabilistischen Sicherheitsanalyse

Gegenstände der Arbeiten waren die Entwicklung einer Methode für die Erfassung, Analyse und Bewertung wissensbasierter Handlungen, die zur Bewältigung eines Ereignisablaufs erforderlich sind, und die Erprobung dieser Methode an einem Beispiel aus der Betriebserfahrung. Im Einzelnen wurden hierzu folgende Arbeiten durchgeführt:

- Bereitstellung eines Verfahrens zur Identifikation von zu untersuchenden wissensbasierten Handlungen

  Mit dem Verfahren sollen in der PSA zu berücksichtigende wissensbasierte Handlungen des Personals und die wesentlichen Randbedingungen für die Ausführung solcher Handlungen ermittelt werden. Hierbei ist davon auszugehen, dass das Personal bei der Auswahl, Planung und Durchführung auf Erfahrungen aus Schulung und beruflicher Praxis zurückgreift und dass die Handlungen nach den Informationen, über die der Operateur in der gegebenen Situation verfügt, als erlaubt und sicherheitsgerichtet erscheinen.

- Bereitstellung eines Modells zur Beschreibung und Wertung der kognitiven Prozesse bei der Identifikation, Planung und Auswahl einer wissensbasierten Handlung

  Als kognitiv werden die psychischen Aktivitäten bezeichnet, die dem Erwerb, der Organisation und der Nutzung von Wissen dienen /NEI 76/. In Situationen, welche vom Kraftwerkspersonal Handlungen erfordern, die für diese Situationen im Betriebshandbuch, im Notfallhandbuch und aufgrund des Trainings nicht vorgesehenen sind, sind die kognitiven Prozesse bei der Informationsaufnahme und Informationsverarbeitung maßgeblich, um das Entscheidungsverhalten zu beurteilen. Die günstige bzw. ungünstige Gestaltung der diesen Prozess beeinflussenden Faktoren ist entscheidend für die Wahrscheinlichkeit, dass derartige Handlungen identifiziert und ausgeführt werden. Es war somit ein Modell bereitzustellen, das Aufbau und Arbeitsweise menschlicher Kognition in ihren wesentlichen Merkmalen darstellt und eine systematische Identifikation und Wertung der den Kognitionsprozess beeinflussenden Faktoren ermöglicht.

  Die Forschung zum Problemlösen hat zu zahlreichen Erkenntnissen über den Prozess des Problemlösens und über Faktoren geführt, die Erfolg, Misserfolg und Effizienz des Problemlösens bestimmen. Diese Erkenntnisse wurden gesammelt, gewertet und in das Kognitionsmodell eingefügt.

- Generierung quantitativer Daten zu wissensbasierten Handlungen

  Derzeit liegen keine ausreichend detaillierten und verifizierten quantitativen Daten zur Zuverlässigkeit wissensbasierter Handlungen vor. Der Mangel konnte im Rahmen des Vorhabens nur teilweise behoben werden. Die hier vorgeschlagenen Daten beruhen auf einer Expertenschätzung, die sich im Wesentlichen auf den empfohlenen Daten zu Diagnose und Entscheidungsaufgaben stützt /SWA 83/. Zur weiteren Absicherung der Ergebnisse wurden der GRS vorliegende Erkenntnisse

aus ausgewählten meldepflichtigen Ereignissen /PRE 10/ und aus der Anwendung pessimistischer Bewertungsmethoden herangezogen.

- Erprobung der Untersuchungs- und Bewertungsmethode
  Die Eignung der Untersuchungs- und Bewertungsmethode war an Hand von Fallstudien zu erproben. Erkenntnisse aus der Erprobungsphase wurden zur Weiterentwicklung und Verbesserung genutzt.

3.2.2 Probabilistische Bewertung organisatorischer Einflüsse sowie von Einflüssen des Sicherheitsmanagements auf die Zuverlässigkeit von Personalhandlungen

Anerkannte Bewertungsmethoden gehen davon aus, dass sich die Fehlerwahrscheinlichkeit einer Handlung ableiten lässt aus der Kenntnis der Fehlerwahrscheinlichkeit dieser Handlung bei optimalen Bedingungen für die Handlungsausführung und der Wirkung sogenannter leistungsbeeinflussender Faktoren (PSF, *P*erformance *S*haping *F*actor).

$$P = f\,(P_{opt}, PSF_1 \ldots PSF_N)$$

Wahrscheinlichkeitsverteilungen und Unsicherheitsbänder berücksichtigen die vorhandenen individuellen Leistungsunterschiede der handelnden Personen. Die Methoden stellen die erforderlichen Daten zur Verfügung und legen fest, wie diese zu einem Ergebnis zu verknüpfen sind.

Wesentliches Ziel des Forschungsvorhabens war es, von diesem Bewertungsansatz auszugehen und ihn so zu erweitern, dass organisatorische Einflüsse in einer PSA untersucht und bewertet werden können. Um dieses Ziel zu erreichen wurden folgende Arbeiten durchgeführt.

- Entwicklung eines Organisationsmodells
  Das Organisationsmodell soll den Bezug zwischen Organisation und Zuverlässigkeit von in einer PSA zu untersuchenden Handlungen herstellen. Es ist somit die Grundlage für die Analyse und Bewertung organisatorischer Einflüsse. Im Rahmen der Modellentwicklung waren
  - die theoretischen Grundlagen hinsichtlich Organisation und organisatorischer Abläufe aufzuarbeiten,

- Begriffe zu definieren (u. a. Organisation, organisatorischer Einflussfaktor),
- der Stand von Wissenschaft und Technik hinsichtlich vorgeschlagener Verfahren zur Berücksichtigung organisatorischer Faktoren in der PSA zu ermitteln und
- die Betriebserfahrung mit Bezug zu organisatorischen Einflüssen zu sichten, um daraus Erkenntnisse für die Modellentwicklung zu gewinnen.

- Weiterentwicklung der Methode zur Modellierung von Arbeitssystemen
  Das Arbeitssystemmodell beschreibt die wesentlichen Merkmale und Wirkungsbeziehungen, die zum Verständnis der Vorgänge bei der Durchführung einer Handlung, der Wirkung leistungsbeeinflussender Faktoren und des Auftretens von Fehlern erforderlich sind. Das von der GRS bei der Auswertung der Betriebserfahrung in Kernkraftwerken eingesetzte Modell wurde im Rahmen des Vorhabens so weiterentwickelt, dass es in das Organisationsmodell integriert werden kann.
- Zusammenführen von Arbeitssystemmodell und Organisationsmodell zu einem Gesamtansatz
- Konkrete Ausarbeitung der methodischen Vorgehensweise zur Integration organisatorischer Einflüsse in den PSA Bewertungsprozess
  Die Vorgehensweise zur Selektion der zu untersuchenden, relevanten organisatorischen Einflüsse wurde erarbeitet und durch Testen anhand von Ereignissen kontinuierlich weiterentwickelt. In diesem Zusammenhang war auch eine Vorgehensweise zur probabilistischen Bewertung zu erarbeiten.

Die in diesem Vorhaben durchgeführten Entwicklungsarbeiten schließen mit einem Fallbeispiel ab, welches die Anwendbarkeit und die Vorgehensweise der Methode demonstriert.

3.3 Auslösende Ereignisse und Einwirkungen von innen und außen

3.3.1 Methoden zur Ermittlung von Leck- und Bruchhäufigkeiten druckführender Komponenten

Zunächst wurden verfügbare Untersuchungsergebnisse bzw. Analysemodelle aus abgeschlossenen Vorhaben im Hinblick auf ihre Anwendbarkeit im Sinne der Zielsetzung überprüft. Für Rohrleitungen des Typs DN 50 des Volumenregelsystems (TA-System) von deutschen Anlagen mit Druckwasserreaktor (DWR) sind aus statistischen Untersuchungen basierend auf der Betriebserfahrung entsprechende Ergebnisse verfügbar. Weiterhin wurde die im Rahmen der Vorhaben RS1127 und RS1163 entwickelte probabilistische Analysemethodik (PROST - *Pro*babilistische *St*rukturberechnung) zur Berechnung von Leck- und Bruchwahrscheinlichkeiten /GRE 04/, /GRE 10/ bereitgestellt und im Rahmen des Anwendungsbeispiels thermomechanische Ermüdungsbelastung im TA-System eines DWR, in dem es in einer Anlage zu einem Leckvorkommnis kam, erprobt. Dieser Anwendungsfall wurde für die Entwicklung der Schnittstelle zwischen der Anwendung der statistischen Methodik basierend auf der Betriebserfahrung und der Methodik basierend auf Strukturzuverlässigkeitsmodellen ausgewählt.

Weiterhin wurde eine Auswertung der Betriebserfahrung (bis einschließlich 2006) im Hinblick auf Rissereignisse in deutschen Druckwasserreaktoranlagen auf Basis der GRS-Datenbanken KomPass für Rohrleitungsschäden durchgeführt, um daraus, unter Einbeziehung der dazu verfügbaren einschlägigen Literatur, Anfangsrissverteilungen für den Einsatz in Strukturzuverlässigkeitsprogrammen (z. B. PROST) abzuleiten. Für die gefundenen Ereignisse aus der Datenbank KomPass wurde jeweils das mittlere Risstiefen- zu Wanddickenverhältnis bestimmt sowie das mittlere Verhältnis von Risstiefe zu halber Risslänge ermittelt. Die Datenbank KomPass mit etwa 800 Ereignissen in Rohrleitungen enthält jedoch insgesamt für Druckwasserreaktoranlagen nur 8 verwertbare Ereignisse mit Riss, wobei unterschiedliche Wanddicken, Werkstoffe und Nennweiten zusammengefasst sind. Für einen exemplarischen Rohrleitungsbereich des TA-Systems wurden die mittlere Anfangsrisstiefe und deren Standardabweichung abgeschätzt.

Die Vorgehensweise zur Bestimmung von Risstiefenverteilungen basierend auf Auswertungen der Betriebserfahrung als Eingangsgröße für Strukturzuverlässigkeitsprogramme (z. B. PROST) zur Bestimmung von Leck- und Bruchwahrscheinlichkeiten

in Rohrleitungsbereichen wurde durch eine Erweiterung der statistischen Basis weiterentwickelt. Während bisher nur Ereignisse aus deutschen Kraftwerken (Datenbank KomPass) herangezogen wurden, wurde nun auch die internationale Datenbank OPDE mit derzeit etwa 3700 Einträgen aus 11 Ländern ausgewertet, wobei zunächst nur schwedische und amerikanische Einträge verwendet wurden, weil diese nach bisherigen Erkenntnissen repräsentativ sind. Eine weitere Auswertung der OPDE-Datenbank wurde für Lecks in Volumenregelsystemen vorgenommen. Außerdem wurde die KomPass-Datenbank nach Lecks und Rissen in Behältern (insbesondere Speisewasserbehälter) abgefragt. Aus den gefundenen Ereignissen wurde ein Fall eines Speisewasserbehälters, bei dem nach kurzer Betriebszeit (458 Tage) mehrere Rissbefunde infolge Spannungsrisskorrosion festgestellt wurden, ausgewählt und dazu Berechnungen mit PROST zur Leckwahrscheinlichkeit durchgeführt.

Mit den aus der Betriebserfahrung über Abfragen der Datenbanken KomPass und OPDE ermittelten Verteilungen für Anfangsrissgrößen wurden Berechnungen zum Anwendungsbeispiel thermische Ermüdung im Volumenregelsystem eines DWR mit dem Rechenprogramm PROST durchgeführt. Weiterhin wurde die Wahrscheinlichkeit für das Auftreten eines Risses an der betrachteten Stelle abgeschätzt und die Ergebnisse mit denen der statistischen Methodik basierend auf der Betriebserfahrung verglichen.

Zur Bewertung der Einflüsse verschiedener Schädigungsmechanismen sowie von Prüfkonzepten und Lerneffekten wurden Auswertungen der KomPass- und OPDE-Datenbank im Hinblick auf Leckereignisse durchgeführt.

Die erzielten Ergebnisse sind in Abschnitt 4.3.1 zusammengefasst. Weitere Details zu den durchgeführten Arbeiten und Ergebnissen in diesem Arbeitspaket sind in dem technischen Fachbericht /GRE 10/ zusammengestellt.

3.3.2 Auswahlverfahren zur Bestimmung von kritischen Anlagenteilen bei seismischen probabilistischen Sicherheitsanalysen

Ausgehend von der allgemeinen Vorgabe des Methodenbandes zum PSA-Leitfaden /FAK 05/ die Notwendigkeit der Durchführung eines Auswahlverfahrens bei seismischen probabilistischen Analysen betreffend, wurde erstmals eine Verfahrensvorschrift zur Unterstützung des Erstellers einer seismischen PSA (SPSA) erarbeitet. Dazu wurde eine Vielzahl internationaler Quellen ausgewertet. Auf der Grundlage der gewonnenen Erkenntnisse wurde ein zweistufiges, durch Begehungen gestütztes Auswahl-

verfahren zur Bereitstellung der seismischen Ausrüstungsliste (SAL) entwickelt. Zur Durchführung des Auswahlverfahrens wurde eine Datenbank einschließlich der entsprechenden Auswertungsprozeduren bereitgestellt.

Mit Unterstützung des Referenzkraftwerks konnte die Verfahrensvorschrift für das Auswahlverfahren anlagenspezifisch getestet werden.

Das Auswahlverfahren bei der Durchführung einer SPSA hat zwei Ziele:

- Ableitung einer seismischen Ausrüstungsliste und Beschreibung der Abhängigkeiten im seismischen Ausfallverhalten relevanter Bauteile, Systeme und Komponenten,
- Klassifikation aller Bauteile, Systeme und Komponenten der seismischen Ausrüstungsliste im Hinblick auf ihre sicherheitstechnische Bedeutung sowie Quantifizierung der Unsicherheiten.

Beide Ziele werden durch ein zweistufiges, durch Begehungen gestütztes Auswahlverfahren realisiert (vgl. Abb. 3-2).

Abb. 3-2 Auswahlverfahren

Das Auswahlverfahren geht von der Menge aller baulichen Anlagen, Systeme und Komponenten (BSK) im Kernkraftwerk aus.

Als seismisch relevante BSK innerhalb einer SPSA werden solche BSK bezeichnet, die bei Ausfall oder Funktionsverlust einen Beitrag zur Häufigkeit von Gefährdungs- oder Kernschadenszuständen leisten. Dabei werden sowohl BSK berücksichtigt, deren Aus-

fall direkt einen Beitrag leistet (z. B. Komponenten von Sicherheitssystemen) als auch solche, die nur indirekt aufgrund von räumlichen oder funktionellen Abhängigkeiten dazu beitragen (z. B. BSK der Klasse II, deren Funktionsverlust zum Ausfall von Sicherheitskomponenten führt). Bei der Auswahl der relevanten BSK ist immer zu berücksichtigen, dass das eigentlich Besondere seismischer Einwirkungen in deren Potential besteht, abhängige Ereignisse hervorzurufen. Die Bedeutung von Sekundäreffekten ist bei SPSA wesentlich größer als bei PSA der Stufe 1 für anlageninterne auslösende Ereignisse.

Es ist nicht möglich, für alle BSK der SAL anlagenspezifische seismische Versagenswahrscheinlichkeiten zu bestimmen, deshalb werden in einer zweiten Auswahlstufe die BSK der seismischen Ausrüstungsliste nach ihrer sicherheitstechnischen Relevanz klassifiziert:

- Sicherheitstechnische Relevanz 0:
  Versagen bei Erdbeben kann ausgeschlossen werden / wird ausgeschlossen
  oder
  Versagen bei Erdbeben liefert keinen bzw. einen vernachlässigbaren Beitrag zur Häufigkeit von Gefährdungs- oder Kernschadenszuständen.

- Sicherheitstechnische Relevanz 1:
  Versagen kann durch generische Versagenskurven beschrieben werden.

- Sicherheitstechnische Relevanz 2:
  Die Ableitung anlagenspezifischer Versagenskurven ist erforderlich.

- **Auswahlstufe 1: Bestimmung der seismischen Ausrüstungsliste**

Ziel der Auswahlstufe 1 ist es, eine umfassende Liste von BSK zusammenzustellen, deren Fehlfunktion bei seismischer Einwirkung einen Beitrag zur Häufigkeit der Gefährdungszustände liefert. Diese Liste wird SAL genannt (seismische Ausrüstungsliste). Es ist mit einer systematischen Vorgehensweise sicherzustellen, dass keine relevanten BSK übersehen werden können.

Zur Durchführung des Auswahlverfahrens wird eine Datenbank <*DB SPSA.mdb*> bereitgestellt. Kernstück dieser Datenbank ist eine Tabelle von BSK einschließlich ihrer räumlichen Zuordnung. Die Eingabe von BSK-Raum-Zuordnungen erfolgt in Abhängigkeit der im Kernkraftwerk vorliegenden Dokumentationsunterlagen. Unabhängig von diesen Unterlagen ist mit der Auswahlstufe 1 sicherzustellen, dass die Datenbank

<*DB SPSA.mdb*> alle seismisch relevanten BSK enthält und diese entsprechend gekennzeichnet sind. Als seismisch relevant werden die BSK innerhalb einer SPSA bezeichnet, die bei Ausfall oder Funktionsverlust einen Beitrag zur Häufigkeit von Gefährdungs- oder Kernschadenszuständen leisten.

Folgende BSK sind seismisch relevante BSK:

- BSK - Sicheres Abfahren:
  Es ist eine systematische Vorgehensweise abzuleiten, um sämtliche BSK zu identifizieren, die zum sicheren Abfahren und zum Erhalt der Nachwärmeabfuhr bei seismisch induzierten auslösenden Ereignissen benötigt werden.

- BSK - Auslösende Ereignisse:
  Es ist eine systematische Vorgehensweise abzuleiten, um sämtliche BSK zu identifizieren, deren Ausfall allein oder zusammen mit dem Funktionsverlust weiterer BSK zu einem auslösenden Ereignis führen kann.

- BSK - sonstige:
  Unter sonstigen relevanten BSK werden BSK verstanden, die in der PSA Stufe 1 von der detaillierten Betrachtung aus verschiedenen Gründen ausgeschlossen wurden, sowie solche BSK, von denen bei Ausfällen aufgrund seismischer Einwirkungen eine Brand- bzw. Überflutungsgefahr ausgeht. Weiterhin gehören dazu die BSK, die aufgrund der bei seismischen Einwirkungen wirkenden Abhängigkeiten, in der Lage sind, andere, oben genannte relevante BSK zu schädigen. Dazu gehören z. B. BSK der Klasse II (siehe /KTA 90/).

- **Auswahlstufe 2: Klassifikation der SAL-Ausrüstungen nach ihrer sicherheitstechnischen Bedeutung**

Die Auswahlstufe 2 beschäftigt sich ausschließlich mit den BSK der in der Auswahlstufe 1 definierten SAL. Die SAL enthält alle BSK, die bei einem seismisch bedingten Ausfall einen Beitrag zur Häufigkeit der seismisch bedingten Kernschadenszustände leisten können. Eventuelle Abhängigkeiten im seismischen Ausfallverhalten der BSK sind in der SAL vermerkt.

Es ist das Ziel der Auswahlstufe 2 alle BSK der SAL nach ihrer sicherheitstechnischen Bedeutung zu klassifizieren und die in der Auswahlstufe 1 festgestellten qualitativen Abhängigkeiten zu quantifizieren.

3.3.3 Methoden für eine probabilistische Bewertung von Transienten aufgrund von Überspannungen oder Fremdspannungseinträgen

Bei einem meldepflichtigen Ereignis am 25. Juli 2006 im schwedischen Kernkraftwerk Forsmark1 trat neben anderen Ereignissen auch eine Überspannungstransiente auf, bei der in Folge zwei von vier Strängen der Notstromversorgung ausfielen. Bislang werden solche Transienten allenfalls deterministisch und nicht probabilistisch behandelt. Diese Fakten waren Initiator für die die Durchführung einer Vorstudie für eine probabilistische Bewertung von Transienten aufgrund von Überspannung oder Fremdspannungseintrag im Rahmen des Vorhabens RS1180.

Die Konzeption dieser Untersuchung bestand darin, festzustellen, inwieweit Methoden vorhanden sind bzw. wie diese angewendet werden, um Überspannungen und Fremdspannungseinträge zu bewerten. Falls keine adäquaten Methoden vorhanden sind, sollte der Entwicklungsbedarf und auch die Durchführbarkeit einer probabilistischen Bewertung näher konkretisiert werden. Dementsprechend sollte ein Lastenheft erstellt werden, in dem die Schritte für eine methodische Weiterentwicklung und eine beispielhafte Durchführung dargestellt sind.

Es wurden daher zunächst die vielfältigen Ursachen für das Auftreten von Überspannungen bzw. Fremdspannungseinträge aufgrund physikalisch-technischer Grundlagen ermittelt und mögliche Folgeausfälle, soweit bekannt, erörtert. Grundsätzlich ist hierfür die Kenntnis der Schutzeinrichtungen oder -maßnahmen für die verschiedenen Ursachen und deren Funktionsweise erforderlich. Die wichtigsten Schutzeinrichtungen und Schutzmaßnahmen werden demzufolge vorgestellt und ihre Funktionsweise erläutert.

Die Betriebserfahrungen mit Überspannung und Fremdspannungseinträgen wurden sowohl für Kernkraftwerke in Deutschland als im Ausland, soweit zugänglich, ausgewertet. Einen breiten Raum nahmen dabei der o. g. Störfall im schwedischen Kernkraftwerk Forsmark und eine Überspannungstransiente im finnischen Kernkraftwerk Olkiluoto ein. Die Überspannungstransiente in Forsmark wurde begleitet von weiteren Störungen (wie z. B. dem Ausfall der Gasturbine), die ihre direkte Ursache nicht in der Überspannungstransiente selbst hatten. Daher ist die Bedeutung der Überspannungstransiente in Bezug auf das Gesamtgeschehen und dessen Relevanz zu relativieren.

Überspannungen entstehen am häufigsten entweder aufgrund von Störungen in Regelungsvorgängen oder aufgrund von Blitzschlag. Auch Schaltvorgänge von Leistungs-

schaltern können Überspannung verursachen. Die Energieinhalte von Blitzeinschlägen sind im Vergleich zu Störungen in der Leistungserzeugung der Energiequelle ‘Hauptgenerator‘ erheblich geringer aber häufiger, wie eine Auswertung einer GRS-eigenen Datenbank zeigte, die auch nicht meldepflichtige Ereignisse mit Überspannungen durch Blitzeinschlag enthält. Überspannungen des Hauptgenerators verbreiten sich zudem praktisch nur auf galvanischem Weg. Die Ströme von Blitzeinschlägen oder auch die Schaltüberspannungen von Schaltern können aufgrund der hochfrequenten Anteile zur Einkopplung von Fremdspannungen in leittechnische Kabel und Geräte führen. Solche Fehler können zu Ausfällen, u. U. auch mit Zerstörungen, zu unerwünschten Fehlauslösungen oder Regelungsvorgängen führen.

In einem weiteren Schritt wurde ermittelt, wie Überspannungstransienten bzw. Fremdspannungseinträge national wie international behandelt werden. Es stellte sich heraus, dass diese Art von Transienten weitgehend nur deterministisch, also im Wesentlichen systemanalytisch behandelt wird. Forderungen oder gar Vorschriften zur probabilistischen Behandlung von Überspannungstransienten wurden weder national noch international gefunden. Im Rahmen des internationalen Workshops DiDelSys in Stockholm im Jahre 2007, der nahezu zeitgleich mit dem Beginn der vorliegenden Arbeiten stattfand, wurde u. a. festgestellt, dass die Einwirkungen aus dem Netz noch weiter untersucht werden müssen, weil die verschiedenen Ursachen und Rückwirkungen auf die elektrischen Anlagen in Kraftwerken noch nicht ausreichend analysiert sind.

Aufbauend auf den oben erworbenen Kenntnisstand wurde ein methodisches Vorgehen entwickelt, wie, ausgehend von bestimmten Überspannungen oder Fremdspannungseinträgen, vom örtlichen Eintrag und der Spannungsverschleppungen bzw. Ausbreitungen, in der Folge das Schadensbild bzw. der Schadenszustand bei diesem Ereignis zu ermitteln ist. Dieses Schadensbild wird hinsichtlich der Einleitung überspannungsbedingter bzw. fremdspannungsbedingter (anlageninternen) auslösender Ereignissen untersucht. Dieser Arbeitsschritt wird auch als Identifizierung des auslösenden Ereignisses bezeichnet.

Die nächsten Schritte bestehen zum einen in einer Anpassungen vorhandener Fehlerbäume aus der PSA für Betriebsphasen des Leistungs- oder Nichtleistungsbetriebs für das identifizierte auslösende Ereignis bei Überspannung oder Fremdspannungseintrag, zum anderen in der Bewertung der Basisereignisse, die überspannungsbedingte bzw. fremdspannungsbedingte Ausfälle repräsentieren. Die grafische Modellierung der Fehlerbäume kann mit dem bereits bei PSA der Stufe 1 für Zustände des Leistungsbe-

triebs eingesetzten analytischen Programm RiskSpectrum® umgesetzt werden. Die rechnerische Bewertung kann ebenfalls mittels dieses Programms erfolgen. Es ist aber auch möglich, das GRS-eigene Simulationsprogramm CRAVEX zu verwenden, welches schon für Brandanalysen eingesetzt wurde, weil der prinzipielle Mechanismus, wie eine Propagation von Bränden in einer PSA zu behandeln ist, und wie die Propagation von Überspannungen bzw. Fremdspannungen zu behandeln ist, sehr ähnlich ist. Welches Programm bei einer konkreten Modellierung tatsächlich Anwendung findet, hängt von der Komplexität und von der möglichen Anzahl der einzelnen Ereignisse ab. Anhand einiger Beispiele wurden die Methodik für die Modellierung mit einem der beiden Programme erläutert und Ausfallwahrscheinlichkeiten, allerdings mit fiktiven Zuverlässigkeitskenngrößen, berechnet.

Bei den durchgeführten Arbeiten zeigte sich, dass Überspannungstransienten bzw. Fremdspannungseinträge derzeit nicht systematisch probabilistisch bewertet werden können. Es fehlen im Wesentlichen folgende wesentlichen Informationen:

- Die möglichen Ausfallmechanismen und Folgeausfälle sind nicht genügend erforscht.
- Gerade hinsichtlich der elektromagnetischen Kopplung mit der Folge von Fremdspannungseinträgen in leittechnischen Anlagen liegen kaum probabilistische Zahlen für die Zuverlässigkeitskenngrößen vor.

Entsprechend der Aufgabenstellung wurde demzufolge mit Hilfe eines Arbeitsablaufdiagramms ein Lastenheft für künftige Arbeiten aufgrund der Ergebnisse der durchgeführten Untersuchungen erstellt.

3.4 Methodenentwicklung zur Analyse des Einflusses von Unsicherheiten auf PSA-Ergebnisse und zum Ausschluss von Fehlerquellen in der PSA

3.4.1 Methoden zur Durchführung von Unsicherheits- und Sensitivitätsanalysen in probabilistischen Dynamikanalysen (dynamische PSA)

Im Rahmen der Arbeiten zu diesem Arbeitspaket wurden zwei approximative Methoden entwickelt und erprobt, mit denen man mit möglichst geringem zusätzlichen Rechenaufwand zu verwertbaren Unsicherheits- und Sensitivitätsaussagen im Rahmen einer

probabilistischen Dynamikanalyse mit der MCDET-Methode gelangen kann. Da die entwickelten alternativen Methoden jeweils ihre Vor- und Nachteile bei der Durchführung einer approximativen Unsicherheits- und Sensitivitätsanalyse haben, wird eine effiziente Vorgehensweise vorgeschlagen, welche abhängig von der gegebenen Situation der Modellierung eine der beiden alternativen Methoden auswählt und anwendet, um den zusätzlichen Aufwand für die approximative Unsicherheits- und Sensitivitätsanalyse möglichst gering zu halten.

Als Anwendungsbeispiel zur Erprobung der entwickelten Methoden zur approximativen Unsicherheits- und Sensitivitätsanalyse wurde ein vereinfachtes Modell zur Wasserstoffverbrennung im Containment nach einem Kühlmittelverluststörfall verwendet. Es wurden sowohl die aleatorischen als auch die epistemischen Größen des Modells spezifiziert, und es wurde die Dynamik des Prozesses der Wasserstoffentwicklung und -verbrennung beschrieben.

Das Anwendungsbeispiel bietet neben der Eigenschaft, dass es eine interessante Problematik zur Reaktorsicherheitsforschung behandelt, den zusätzlichen Vorteil, dass mit diesem vereinfachten Modell eine zweistufig geschachtelte Simulationsschleife im Rahmen einer probabilistischen Dynamikanalyse unter Verwendung der MCDET-Methode durchgeführt werden kann. Dies ist im Rahmen der durchgeführten Arbeiten insofern von Bedeutung, um die Qualität der entwickelten Methoden abschätzen zu können. Dazu wurden die approximativen Unsicherheits- und Sensitivitätsaussagen, die sich mit den entwickelten approximativen Methoden bzgl. des Anwendungsbeispiels ergeben haben, mit denjenigen Unsicherheits- und Sensitivitätsaussagen verglichen und diskutiert, die man auf der Basis der Ergebnisse einer zweistufig geschachtelten Simulationsschleife erhalten hat.

Für das Anwendungsbeispiel wurde zum einen eine MCDET-Analyse unter Verwendung einer zweistufig geschachtelter Monte Carlo-Simulation durchgeführt. Für die sich daraus ergebenden Ergebnisse wurde eine Unsicherheits- und Sensitivitätsanalyse durchgeführt. Ferner wurde eine weitere MCDET-Analyse durchgeführt, in der die aleatorischen und epistemischen Größen des Modells gleichzeitig variiert wurden. Unter Verwendung der entwickelten alternativen Methoden wurde für diese Ergebnisse ebenfalls eine approximative Unsicherheits- und Sensitivitätsanalyse durchgeführt.

Die durchgeführten Arbeiten sind im Detail in einem technischen Fachbericht /PES 10/ dokumentiert.

3.4.2 Methoden zur Anpassung von Beta-Verteilungen an vorgegebene Lognormal-Verteilungen unter Berücksichtigung zusätzlicher Benutzervorgaben

Es wurde ein Verfahren entwickelt, das den Anwender dabei unterstützt, auf der Grundlage einer vorgegebenen Lognormal-Verteilung eine geeignete Beta-Verteilung zu ermitteln. Dieses Verfahren wurde im FORTRAN-Programm ‘BetaFit.f90‘ implementiert. Zusätzlich wurden zwei Versionen einer Benutzeroberfläche erstellt. Unabhängig von der Version werden dabei über ein Eingabefenster die Daten für das FORTRAN-Programm angefordert, die Eingaben überprüft, danach automatisch das FORTRAN-Programm aufgerufen und schließlich die Rechenergebnisse dokumentiert und grafisch dargestellt.

Eine Version der Benutzeroberfläche wurde als VBA-Programm (*V*isual *B*asic for *A*pplications) mit der Bezeichnung ‘BetaFit.xlsm‘ unter MS EXCEL 2007® (als Bestandteil von Microsoft Office®) entwickelt. Die andere Version ist ein Visual Basic 2008®-Programm (‘BetaFit.exe‘) unter der Microsoft .NET Umgebung. Es wurde zusätzlich entwickelt, weil Microsoft VBA langfristig durch eine .NET-basierte Technologie ersetzen wird.

Beim Aufruf von ‘BetaFit.xlsm‘ (VBA-Programm) oder ‘BetaFit.exe‘ (Visual Basic 2008®-Programm) wird das Dialogfenster ‘BetaFit‘ (vgl. Abb. 3-3) angezeigt, in welchem der Anwender spezifizieren soll,

- welche Größen der vorliegenden Lognormal-Verteilung eingegeben werden (‘Spezifikation der Lognormal-Verteilung durch:‘) und
- welche Anpassung für die Beta-Verteilung durchgeführt werden soll (‘Anpassung einer Beta-Verteilung an:‘).

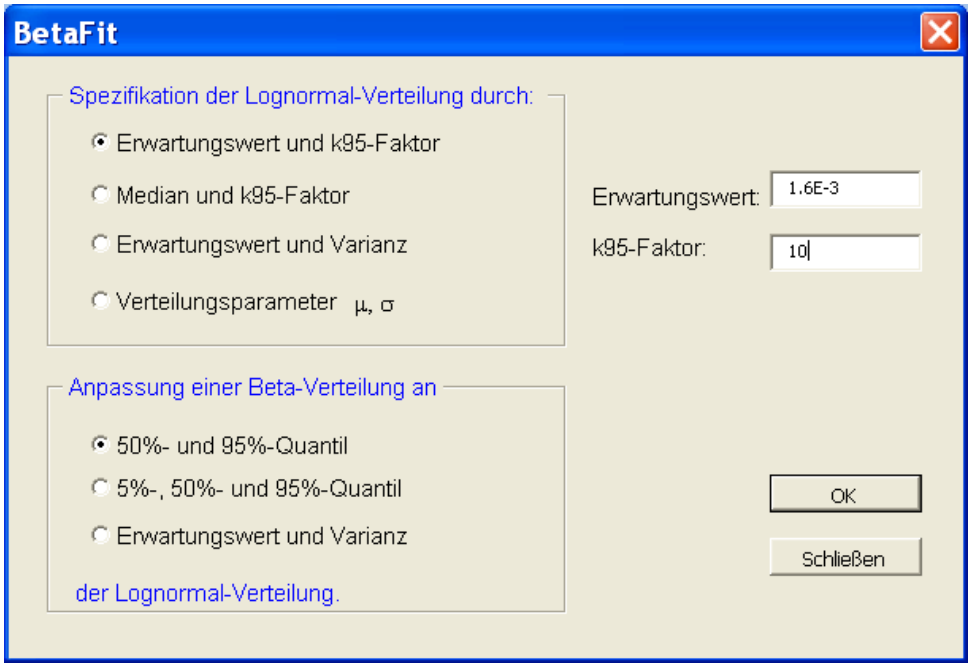


Abb. 3-3 Dialogfenster ‘BetaFit‘

Wenn die Eingaben im Dialogfenster ‘BetaFit‘ mit OK bestätigt wurden, wird automatisch das dazugehörige FORTRAN-Programm aufgerufen, das aus den Angaben zur Lognormal-Verteilung zunächst weitere Kenngrößen der Lognormal-Verteilung berechnet.

Die Anpassung einer Beta-Verteilung erfolgt unter Berücksichtigung einer der folgenden Bedingungen:

1. 50 %- und 95 %-Quantil,
2. 5 %-, 50 %- und 95 %-Quantil oder
3. Erwartungswert und Varianz

von Lognormal- und Beta-Verteilung sollen übereinstimmen.

Sind bei der vorgegebenen Lognormal-Verteilung Werte größer als 1 mit einer subjektiven Wahrscheinlichkeit von mindestens 1,0 E-04 möglich, so wird eine Beta-Verteilung an die Quantile bzw. an Erwartungswert und Varianz der gestutzten Lognormal-Verteilung angepasst. Zusätzlich wird die ungestutzte Lognormal-Verteilung berücksichtigt, wenn eine Anpassung an die Quantile erfolgen soll und das 95 %-Quantil der ungestutzten Lognormal-Verteilung nicht größer als 0,95 ist.

Die Stutzung einer Lognormal-Verteilung wird durchgeführt, um sowohl für die Quantile als auch für Erwartungswert und Varianz automatisch Werte vorgeben zu können, die für eine Versagenswahrscheinlichkeit zulässig sind und die deshalb für die Ermittlung einer entsprechenden Beta-Verteilung geeignet sind. Die Berechnung zur Ermittlung einer Beta-Verteilung würde zu keinem Ergebnis führen, wenn mindestens ein Quantil der vorgegebenen ungestutzten Lognormal-Verteilung größer als eins ist.

Die Anpassung einer Beta-Verteilung an die (5 % -,) 50 % - und 95 % - Quantile der vorgegebenen Lognormal-Verteilung erfolgt durch ein adaptives zufälliges Suchverfahren nach Tarasenko (vgl. /TAR 77/, /TAR 80/ und /RAP 88/). Die dafür erforderlichen Startwerte für die Verteilungsparameter der Beta-Verteilung werden aufgrund der Beziehung zwischen Beta- und Binomial-Verteilung sowie aufgrund einer Approximation der Binomial-Verteilung durch die Standard-Normal-Verteilung berechnet.

Die Ermittlung der Parameter α und β der Beta-Verteilung, deren Erwartungswert $E(P)$ und Varianz $Var(P)$ mit den entsprechenden Größen der (ungestutzten bzw. gestutzten) Lognormal-Verteilung übereinstimmen, erfolgt analytisch.

Es gilt:

$$\beta = \frac{E(P)(1-E(P))^2}{Var(P)} - (1-E(P))$$

$$\alpha = \beta \cdot \frac{E(P)}{1-E(P)}$$

Die Ergebnisse zur Anpassung einer Beta-Verteilung an eine vorgegebene Lognormal-Verteilung werden zusammen mit den Eingabedaten in der Datei ‘BetaFit.out‘ dokumentiert. Zusätzlich wird die angepasste Beta-Verteilung zusammen mit der vorgegebenen Lognormal-Verteilung grafisch dargestellt. Dabei werden sowohl die Verteilungsfunktion als auch die Dichtefunktion der beiden Verteilungen verglichen. Liefert die vorgegebene Lognormal-Verteilung mit einer subjektiven Wahrscheinlichkeit von mindestens 1,0 E-04 Werte $p > 1$, wird zusätzlich die gestutzte Lognormal-Verteilung zusammen mit der angepassten Beta-Verteilung grafisch dargestellt.

3.4.3 Konsistente und umfassende Berücksichtigung epistemischer Unsicherheiten in Verteilungen von Zuverlässigkeitskenngrößen

Bei der Ermittlung von Zuverlässigkeitskenngrößen für unabhängige Ausfälle werden bisher fast ausschließlich nur statistische Unsicherheiten berücksichtigt, welche sich durch den relativ geringen Umfang an Daten ergeben, die den Schätzungen zugrunde liegen. Neben den statistischen Unsicherheiten existieren allerdings noch weitere Unsicherheitsquellen, die einen Einfluss auf die Unsicherheiten der Zuverlässigkeitskenngrößen haben können.

Zur Ermittlung der Wahrscheinlichkeiten gemeinsam verursachter Ausfälle (GVA-Wahrscheinlichkeiten) wird in der GRS das Kopplungsmodell verwendet, das eine Modifikation des ‘Binomial Failure Rate‘-Modells ist. Das in der GRS entwickelte Kopplungsmodell zeichnet sich durch die Eigenschaft aus, dass sich verschiedene Unsicherheitsquellen, die sich in der Betriebserfahrung gezeigt haben, explizit im Modell berücksichtigt werden. Der Einfluss der berücksichtigten Unsicherheitsquellen pflanzt sich über das Modell auf die Modellergebnisse fort und ist somit vollständig zu quantifizieren. Wie bei den unabhängigen Ausfällen der Komponenten erhält man anstatt lediglich eines Punktwertes eine subjektive Wahrscheinlichkeitsverteilung als Ergebnis, die den Kenntnisstand bezüglich der zu schätzenden GVA-Wahrscheinlichkeit in Abhängigkeit der berücksichtigten Unsicherheitsquellen quantitativ ausdrückt.

Generell ist sowohl bei den unabhängigen Ausfällen als auch bei den Ausfällen aufgrund einer gemeinsamen Ursache (GVA) davon auszugehen, dass neben den im Schätzmodell berücksichtigten Unsicherheiten noch zusätzliche, teils unbekannte Unsicherheitsquellen existieren, die einen Einfluss auf die Unsicherheiten bzgl. der zu schätzenden Zuverlässigkeitskenngrößen haben können. Dies wurde bereits in dem Vorhaben /STI 09/ untersucht und technisch begründet. Da diese zusätzlichen Unsicherheitsquellen nicht explizit im Schätzmodell berücksichtigt werden, kann ihr Einfluss auf die Ergebnisunsicherheiten der Zuverlässigkeitskenngrößen nicht quantifiziert werden.

Da des Weiteren anzunehmen ist, dass der Einfluss der zusätzlich existierenden Unsicherheitsquellen nicht vollständig durch die bereits im Schätzmodell berücksichtigten Unsicherheitsquellen abgedeckt wird, wird eine nachträgliche Varianzerhöhung (Verbreiterung) der Schätzverteilungen von Zuverlässigkeitskenngrößen vorgeschlagen. Durch die nachträgliche Varianzerhöhung der Verteilungen wird die Möglichkeit ge-

schaffen, den zusätzlichen und nicht explizit im Schätzmodell berücksichtigten Unsicherheitsquellen Rechnung zu tragen und deren potentiellen Einfluss, zumindest in grober Näherung, in den Schätzverteilungen der Zuverlässigkeitskenngrößen zu berücksichtigen.

In diesem Arbeitspaket wird die bisher von der GRS bei der Ermittlung von Verteilungen für Zuverlässigkeitskenngrößen angewendete Methode zur Verteilungsverbreiterung (Varianzerhöhung von Verteilungen) mathematisch beschrieben. Diese analytische Vorgehensweise ist allerdings auf Lognormal-Verteilungen beschränkt und kann nicht auf andere Verteilungen, die sich aus den Schätzmodellen in parametrischer oder nicht-parametrischer Form ergeben, übertragen werden. Um die Einschränkungen und Schwachstellen des bisherigen auf Lognormalverteilungen basierenden Verfahrens zu vermeiden, wird aufbauend auf der im Rahmen des BMU-Vorhabens SR2595 entwickelten Methode /STI 09/ ein neues, allgemein anwendbares Verfahren zur Varianzerhöhung von Verteilungen vorgeschlagen. Da die in /STI 09/ entwickelte Methode nur für Verteilungswerte < 0,5 angewendet werden konnte, wurde eine Weiterentwicklung durchgeführt, wodurch die Methode uneingeschränkt für alle Verteilungswerte im Intervall (0,1) angewendet werden kann. Das numerische Verfahren zur nachträglichen Varianzerhöhung (Verbreiterung) von Schätzverteilungen mit der vorgeschlagenen Methodik wurde mathematisch beschrieben und an einem Beispiel demonstriert.

Um die Auswirkung der neu entwickelten Methodik zur nachträglichen Varianzerhöhung von Verteilungen für Zuverlässigkeitskenngrößen im Vergleich zum bisherigen Verfahren zu untersuchen, wurden an einigen ausgewählten Fallbeispielen Vergleichsrechnungen durchgeführt. Für die Fallbeispiele wurden Schätzungen für GVA-Wahrscheinlichkeiten gewählt, die mit dem Kopplungsmodell ermittelt wurden und die als nicht-parametrische Verteilungen vorliegen.

Es wird die grundsätzliche Frage diskutiert, ob die nachträgliche Varianzerhöhung von Verteilungen für Zuverlässigkeitskenngrößen generell eine hinreichend zufriedenstellende Methode darstellt, den Einfluss zusätzlicher Unsicherheitsquellen auf die sich aus den Schätzmodellen ergebenden Verteilungen von Zuverlässigkeitskenngrößen zu quantifizieren. Die Diskussion stützt sich dabei auf die Verteilungen der GVA-Wahrscheinlichkeiten, die unter Verwendung der ausgewählten Fallbeispiele über das Kopplungsmodell ermittelt wurden. Das in der GRS entwickelte Kopplungsmodell zur Schätzung von Verteilungen für GVA Wahrscheinlichkeiten eignet sich deshalb für eine

solche Untersuchung, da verschiedene Unsicherheitsquellen im Kopplungsmodell explizit berücksichtigt und deren Einfluss auf die Ergebnisunsicherheiten quantifiziert werden können.

Die zu diesem Arbeitspunkt durchgeführten Arbeiten wurden im Detail in einem technischen Bericht //AP4.3 /PES 10a/ dokumentiert.

3.4.4 Methoden zur konsistenten Berücksichtigung gemeinsam verursachter Ausfallereignisse (GVA) in PSA

Die in diesem Arbeitspaket durchgeführten Arbeiten gliedern sich in zwei Teile: Arbeiten zur Weiterentwicklung des Verfahrensrahmens, mit denen die Bewertung der Übertragbarkeit beobachteter GVA-Ereignisse auf die in der PSA modellierten Komponentengruppen erfolgt, sowie Arbeiten zur Entwicklung eines geschlossenen Programmsystems zur Berechnung von GVA-Wahrscheinlichkeiten.

Die Bewertung der Übertragbarkeit beobachteter GVA erfolgt über die Bewertung von Randbedingungen, die Unterschiede zwischen der Komponentengruppe, in der ein GVA-Ereignis beobachtet wurde, und der in der PSA modellierten Komponentengruppe (Zielkomponentengruppe) beschreiben. Für die Zielkomponentengruppe wird bewertet, mit welcher Rate unter der für sie gültigen Randbedingung das beobachtete Phänomen zu erwarten ist und welche Komponentenschädigungen auftreten würden. Um den Verfahrensrahmen zur ingenieurmäßigen Bewertung der Übertragbarkeit von GVA-Ereignissen zu systematisieren und weiterzuentwickeln, wurden zunächst die bisher bei der Bewertung von GVA-Ereignissen in deutschen Kernkraftwerken definierten Randbedingungen untersucht. Dazu wurden alle Randbedingungen gesichtet und die Formulierung inhaltlich identischer Randbedingung vereinheitlicht.

Alle verschiedenen Randbedingungen wurden daraufhin untersucht, welche Aspekte der Unterschiede zwischen der Komponentengruppe, in der ein Ereignis aufgetreten ist, und der Komponentengruppe der Zielanlage, für die eine GVA-Wahrscheinlichkeit im PSA-Fehlerbaum ermittelt werden soll, durch die Randbedingung beschrieben werden.

Es wurden sechs unterschiedliche Kategorien von Randbedingungen identifiziert. Je nach Kategorie ist ein unterschiedliches Vorgehen bei der Durchführung der Expertenbewertungen oder eine unterschiedliche mathematisch-statistische Behandlung erfor-

derlich. Die vorhandenen Randbedingungen wurden den Kategorien zugeordnet, wobei bei den meisten Randbedingungen eine Mehrfachzuordnung erfolgen musste, da die meisten Randbedingungen mehrere Bewertungsaspekte beinhalten.

Global für alle definierten Randbedingungen sowie differenziert nach den einzelnen Kategorien bzw. Unterkategorien wurde untersucht und bewertet, welche quantitativen Expertenbewertungen bisher vorgenommen wurden. Hierbei wurde versucht, wo möglich eine unterliegende Systematik der Bewertungen zu identifizieren.

Aufbauend auf den gewonnenen Erkenntnissen wurde ein allgemeines Konzept für Randbedingungen entwickelt. Dies umfasst die Definition von Randbedingungen, die Aufteilung von Populationen, eine qualitative und quantitative Skala für die Bewertung der Übertragbarkeit von Ereignissen sowie die Verwendung von Randbedingungen bei der Ermittlung für Zuverlässigkeitskenngrößen für die PSA.

Für die verschiedenen Kategorien wurden spezifische Vorgehensweisen und zu stellende Anforderungen diskutiert sowie Verbesserungsmöglichkeiten bei der bisherigen Vorgehensweise identifiziert. Darauf aufbauend wurden einzelne Randbedingungen betreffende konkrete Weiterentwicklungsvorschläge erarbeitet.

Weiterhin wurde die Extrapolation von GVA-Ereignissen auf stark abweichende Redundanzgrade, insbesondere von kleinen auf sehr große Redundanzgrade, im Bezug auf die Möglichkeit diskutiert, das bisherige Verfahren mit Hilfe einer weiterentwickelten mathematischen Modellierung zu verbessern.

Um ein geschlossenes Programmsystem zur Berechnung von GVA-Wahrscheinlichkeiten zu erstellen, wurde das Java-basierte Programm POOL entwickelt. Mit POOL können die in die Berechnungen einfließenden Informationen zusammengestellt und die notwendigen Rechenparameter ermittelt werden. Das Programmsystem wurde so gestaltet, dass die für die Rechnungen zusammengestellten Informationen dokumentiert, das Programm PEAK zur mathematischen Berechnung der GVA-Wahrscheinlichkeiten /GRS 03/ aufgerufen und die notwendigen Informationen übergeben werden können. Da Programm PEAK wurde erweitert durch eine Ausgabefunktion, bei der die Ergebnisse in einem Format ausgegeben werden, welches direkt in das Fehlerbaumprogram RiskSpectrum® eingelesen werden kann.

Bei den für die Berechnung von GVA-Wahrscheinlichkeiten für eine Komponentengruppe unter Verwendung des GRS-Kopplungsmodells notwendigen Informationen handelt es sich um Informationen über die Komponentengruppe selbst sowie um Informationen über die beobachteten GVA-Ereignisse. Zusätzlich wird zur Berechnung noch die Beobachtungszeit der Population von Komponentengruppen, die zur gleichen Komponentenart gehören, benötigt.

Die Informationen aus der systematischen Auswertung der GVA-Ereignisse sind in der Datenbank GVA, die Teil des Datenbanksystems ‘Generische Wissensbasis‘ WISBAS ist, abgelegt. Für die Berechnung von GVA-Wahrscheinlichkeiten sind dabei die von den Experten geschätzten Schädigungsvektoren und Übertragbarkeitsfaktoren, die Größe der betroffenen Komponentengruppe und die Randbedingungen, für die die Expertenbewertungen abgegeben worden sind, relevant. Des Weiteren sind die bewertete Komponenten- und Ausfallart von Belang. Für diese Informationen wurde eine Transfermöglichkeit nach POOL geschaffen.

Für die Erfassung der anlagenspezifischen Parameter der Komponentengruppe, für die GVA-Wahrscheinlichkeiten berechnet werden sollen, wurde eine Eingabemaske in Pool entwickelt. Bei den anlagenspezifischen Parametern handelt es sich um die Komponentenart, die betrachtete Ausfallart, die Größe der Komponentengruppe und die Fehlerentdeckungszeit.

Zur Berechnung der Beobachtungszeit wurde bisher für die meisten Komponentenarten die Anzahl der Komponentengruppen in einer generischen Druckwasser- bzw. Siedewasserreaktoranlage abgeschätzt und aus einer starren Liste mit festen Auswertezeiträumen per Hand ausgewählt. Aus dieser Abschätzung und der bekannten Betriebsdauer deutscher Kernkraftwerke wurde dann die Beobachtungszeit berechnet. Für einige ausgewählte Komponentenarten (z. B. Notstromdiesel) wurden bereits exakte Zählungen durchgeführt. Die Ermittlung der Beobachtungszeiten wurde weiterentwickelt und ein Algorithmus zur genauen Berechnung der Beobachtungszeiten in POOL integriert.

Für die Zusammenstellung der zu einer Population gehörenden GVA-Ereignisbewertungen unter Berücksichtigung der Randbedingungen und die Verknüpfung dieser Parameter mit den zugehörigen anlagenspezifischen Parametern wurde in Pool eine menügeführte Auswahlmöglichkeit geschaffen.

Bisher erfolgte die Dokumentation der erstellten Datensätze per Hand über zusätzlich eingefügte Kommentarfelder. Auch dieser Vorgang wurde mithilfe einer Report-Funktion in POOL automatisiert.

3.4.5 Benutzeroberfläche mit den erforderlichen Hilfsprogrammen für PSA-Methoden der Stufe 1

Um die Ziele des Teilvorhabens ‘Bereitstellung einer Benutzeroberfläche mit den erforderlichen Hilfsprogrammen für PSA-Methoden der Stufe 1 zum Ausschluss von Fehlerquellen‘ mit den zur Verfügung stehenden Mitteln zu erreichen, musste zunächst eine Analyse des Datenflusses in einer PSA der Stufe 1 durchgeführt werden. Hierzu konnte auf Anforderungen des Fachbandes zu PSA-Methoden /FAK 05/ des Leitfadens Probabilistische Sicherheitsanalyse aufgebaut werden. Ein wesentliches Ziel bestand dabei darin, die Randbedingungen und Schnittstellen für die GRS-Hilfsprogramme für eine PSA der Stufe 1 herauszuarbeiten. Die Ergebnisse dieser Analyse sind in einem technischen Fachbericht für dieses Arbeitspaket /WIE 10/ dargestellt.

Als wesentliches Ergebnis dieser Analyse kann festgehalten werden, dass eine Integration sämtlicher im Umfeld einer PSA verwendeter Programme unter einer gemeinsamen Oberfläche mit den für das Teilvorhaben vorgesehenen Mitteln nicht durchführbar war. Bei einigen Programmen, wie zum Beispiel Textverarbeitungen (MS WORD®), wäre eine Integration überdies auch nicht sinnvoll gewesen. Daher musste im Rahmen des Vorhabens RS1180 eine Beschränkung auf vordringliche Arbeiten vorgenommen werden. Dabei wurde der Schwerpunkt auf die notwendigen Arbeiten zu einer Integration der von der GRS erstellten Hilfsprogramme für eine PSA der Stufe 1 in eine gemeinsame Oberfläche gelegt. Als Name für diese Oberfläche wurde goPSA gewählt.

Vor diesem Hintergrund wurde ein Konzept für die gemeinsame Oberfläche goPSA entwickelt. Diese sollte in einer ersten Version die folgenden Programme umfassen:

- **STREUSL**

  Das Programm STREUSL /ZIP 81/ wird von der GRS zur Durchführung von Unsicherheits- und Importanzanalysen an Hand der mit RiskSpectrum® bestimmten Minimalschnitte verwendet.

- **RSAscii**

  Das Programm RSAscii wird von der GRS zur Konvertierung des Datenformats ‘RSA‘, das in RiskSpectrum® zum Datenexport verwendet werden kann, in ein zum Beispiel von STREUSL lesbares Datenformat genutzt.

- **EXCELRS**

  Das Programm EXCELRS wird von der GRS genutzt, um Daten aus einem von STREUSL und MS EXCEL® lesbaren Format in das von RiskSpectrum® lesbare RSA-Format zu konvertieren. Auf diese Weise wird insbesondere der Import der Daten zu Zuverlässigkeitskenngrößen ermöglicht.

- **CRAVEX**

  Das Programm CRAVEX /GRS 03a/ lag in einer Prototypversion vor. Es wird von der GRS genutzt, um probabilistische Analysen zu übergreifenden Einwirkungen, wie beispielsweise Brand oder Flugzeugabsturz, durchzuführen, bei denen eine Ausbreitung von sogenannten Raumausfällen durch z. B. Brandausbreitung oder Trümmerwirkung relevant ist.

Für das Programm CRAVEX wurde ein erheblicher Weiterentwicklungsbedarf identifiziert, mit dem die Prototyp-Version von CRAVEX an die Anforderungen einer MS WINDOWS®-basierten Oberfläche angepasst werden musste. Eine Integration des GRS-Programms SUSA /KLO 08/ war zwar vorgesehen, konnte wegen der dazu erforderlichen Anpassung von SUSA an neue IT-Umgebungen noch nicht erfolgen. Verschiedene Module von SUSA wurden während der Laufzeit dieses Vorhabens weiter entwickelt bzw. sollen noch realisiert werden. Daher stand vor Ablauf des Vorhabens keine SUSA-Version zur Verfügung, die in goPSA integriert werden konnte.

Zusätzlich zur Integration der Programme unter der gemeinsamen Oberfläche goPSA mussten auch Benutzeranleitungen für die GRS-Hilfsprogramme erstellt und unter goPSA bereitgestellt werden. Für einige der geforderten Funktionalitäten einer gemeinsamen Oberfläche mussten keine eigenen Programme entwickelt werden. Stattdessen

wurden entsprechende Benutzerhilfen bzw. Vorlagen unter goPSA integriert. Dies betrifft die folgenden Punkte:

- Verfahren zur Berechnung von GVA-Modulen
  Bei der Modellierung von GVA-Komponentengruppen, die aus mehr als sechs Komponenten bestehen, in den Fehlerbäumen einer PSA werden von der GRS bei einer detaillierten Modellierung so genannte GVA-Module gebildet. Die dafür vorliegende MS EXCEL®-Anwendung musste aktualisiert und das entsprechende Verfahren neu beschrieben werden.

- Benutzerhilfe zur Bewertung von Handmaßnahmen
  Die GRS nutzt für die Bewertung von Handmaßnahmen im Rahmen einer PSA in der Regel das in /FAK 05/ empfohlene THERP-Verfahren. Es wurde eine Benutzerhilfe entwickelt, in der dargestellt wird, wie eine Bewertung nach THERP mit RiskSpectrum® modelliert und ausgewertet werden kann.

- Benutzerhilfe zur Definition einer Schnittstelle zwischen Stufe 1 und Stufe 2
  Für den Übergang aus der Stufe 1 einer PSA zur Stufe 2 der PSA wird eine Schnittstelle benötigt. Diese hat eine besondere Bedeutung, wenn wegen eines zweistufigen Verfahrens über diese Schnittstelle Daten zwischen unterschiedlichen Programmen übergeben werden müssen. Für die Definition der Schnittstelle wurde ein Vorschlag für ein systematisches Benennungsschema für die Endzustände der Stufe 1 gemacht und in einer Benutzeranleitung beschrieben.

- Benutzerhilfe zur Dokumentation einer PSA der Stufe 1
  Der PSA-Methodenband /FAK 05/ enthält eine Reihe von Vorgaben zu Ergebnissen, die bei der Auswertung eines PSA-Modells erzeugt und dokumentiert werden sollten. Es wurde daher eine Vorlage erstellt, die als Orientierung hinsichtlich Darstellung und Vollständigkeit PSA-Ergebnissen (wie Kernschadenshäufigkeiten und Übergangswahrscheinlichkeiten) dienen kann.

Für die oben genannten Programme und Benutzerhilfen wurden die notwendigen Entwicklungs- und Programmierarbeiten durchgeführt. Die in goPSA die erforderlichen Benutzeroberflächen für den Aufruf der Programme und Benutzerhilfen wurden erstellt. Ein weiterer Schwerpunkt der Arbeiten lag dabei in der notwendigen Weiterentwicklung von CRAVEX und der für CRAVEX erstellen grafischen Benutzeroberfläche. Eine detailliertere Darstellung der durchgeführten Arbeiten kann dem technischen Fachbericht /WIE 10/ entnommen werden.

3.5 Untersuchungen der PSA-Tauglichkeit des Integralcodes ASTEC© für Unfallanalysen unter Einbeziehung neuerer Erkenntnisse zum Radionuklidverhalten

Dieses Kapitel behandelt die deterministische Analyse ausgewählter Unfälle (Störfälle mit Kernschmelzen), wie sie im Rahmen einer PSA der Stufe 2 für den Leistungsbetrieb bei der GRS den Empfehlungen im PSA Leitfaden /FAK 05/ folgend durchgeführt werden, d. h. startend mit den Vorgängen ab Störfallinitiierung (z. B. Leck) über den Beginn des Kernschmelzens bis hin zu der Freisetzung von Radionukliden in die Umgebung. Die Phänomene bei Unfällen mit Kernzerstörung werden seit langem intensiv untersucht. Die dabei gewonnenen Kenntnisse fließen in Rechenprogramme zur deterministischen Simulation des Unfallablaufs und damit zur Sicherheitsbewertung ein, die auch in den hier durchgeführten Analysen verwendet worden sind. Die nachfolgend vorgestellten Rechnungen zielen zunächst nur auf eine prinzipielle Bewertung von ASTEC V1.33 hinsichtlich des Einsatzes als Werkzeug im Rahmen einer PSA der Stufe 2 gemäß den o. g. Randbedingungen ab. Die dabei untersuchten Unfallszenarien stellen somit nur einen Ausschnitt aus dem breiten Spektrum möglicher Analysen dar. Demzufolge lassen sich aus den Ergebnissen keine Aussagen hinsichtlich der Sicherheit der untersuchten Anlage ableiten.

- **Stand der Entwicklung von ASTEC und MELCOR:**

Anliegen dieses Arbeitspunktes ist es, mit einer möglichst aktuellen Version der Programme ASTEC und MELCOR die spezifizierten Unfallanalysen durchzuführen. Die Entscheidung bezüglich der verwendeten ASTEC Version V.1.33 rev3 war deshalb besonders schwierig, da während der Laufzeit des Projekts mehrere signifikant überarbeitete Versionen freigegeben worden sind. Gegen Ende 2007 war zunächst eine aktualisierte Version von ASTEC V1.32 verfügbar. Im Zeitraum des Vorhabens wurden weitere Verbesserungen in ASTEC implementiert. Die letzte bereitgestellte Version der Serie V1 war die im Vorhaben verwendete Version V1.33 rev3. Als wesentlicher Nachteil für dieses Vorhaben erwies sich letztlich die verspätete Freigabe (erst in der zweiten Jahreshälfte des Jahres 2009) der neuen Entwicklungsstufe ASTEC V2 von Seiten des Hauptentwicklers IRSN, die ursprünglich bereits für Ende 2008 geplant war und im Vorhaben eingesetzt werden sollt. Diese neue Version zeichnet sich insbesondere durch ein neues Modul zur Berechnung der Kernzerstörungsphase im Reaktordruckbehälter (RDB) aus. Das Modul DIVA in ASTEV V1.33 wurde mit dem Übergang auf

die Version ASTEC V2.0 durch das wesentlich detailliertere französische Programm ICARE2 ersetzt. Mit Blick auf die Restlaufzeit des Vorhabens und die notwendigen Schritte und ggf. Probleme beim Übergang auf eine signifikant erweiterte Programmversion wurde entschieden, weiterhin mit der bis dato verfügbaren aktuellsten Version ASTEC V1.33 rev3 zu arbeiten. Bei der Auswahl der verwendeten MELCOR-Version war die Sachlage ähnlich, die Auswirkungen blieben jedoch sehr gering. Die ursprünglich für 2007 angekündigte Version MELCOR 2.0, die sich durch eine vollständige Umstellung der Programmiersprache auf den FORTRAN 95-Standard bei gleichen physikalischen Modellen auszeichnet, wurde durch die U.S. NRC (*U*nited *S*tates *N*uclear *R*egulatory *C*ommission) ebenfalls erst verspätet freigegeben. Somit wurde auf das letzte Update von MELCOR 1.8.6, die Version YU, zurückgegriffen. Dies ist insofern kein Nachteil, da sich diese Version modellmäßig nicht vom Stand der Version 2.0 unterscheidet.

Beide Programmversionen wurden mit Freigabe durch den Entwickler (IRSN für ASTEC bzw. SNL für MELCOR) auf den Rechnersystemen der GRS (PC mit MS WINDOWS® bzw. LINUX OS) installiert. Im Anschluss daran wurden für ASTEC Testrechnungen mit bereits verfügbaren Eingabedatensätzen durchgeführt. Dies ist insofern notwendig, da unterschiedliche Rechnersysteme und Betriebssysteme den Rechnungsablauf manchmal beeinflussen können. Ein direkter Vergleich der Rechnungsergebnissen von Beispieldatensätzen mit entsprechend Daten von IRSN stellt die korrekte Ablauffähigkeit sicher.

In beiden Programmen werden die unterschiedlichen Anlagenteile und wesentliche, damit verbundene physikalische Prozesse bei Unfallabläufen in Modulen (ASTEC) oder so genannten ‘Packages‘ (MELCOR) behandelt. Diese können vom Nutzer einzeln ausgewählt und aktiviert werden. Unterschiedlich sind die mathematische Behandlung dieser Teile der Programme sowie die einzelne Tiefe der Modelle und deren Validierungsstand. In ASTEC werden die jeweils ausgewählten Module automatisch entsprechend dem Ablauf der physikalischen Prozesse aktiviert und tauschen zum Ende eines Makrozeitschritts entsprechend der vom Benutzer vorgegebenen Makrozeitschrittweite die Daten aus. Jedes Modul läuft dabei mit seinem eigenen Mikrozeitschritt entsprechend den ihm eigenen Konvergenzanforderungen. In MELCOR werden alle aktivierten Packages in einem einheitlichen System behandelt und mit dem gleichen Zeitschritt berechnet. Eine ‘stand alone‘-Nutzung einzelner Module ist bei ASTEC eine beabsichtigte Programmoption, die z. B. bei IRSN in der PSA der Stufe 2 für einen französischen DWR verbreitet zum Einsatz kommt und auch bei der Validierung einzelner eng

definierter Experimente gewisse Vorteile hat. Dagegen ist dies bei MELCOR eher die Ausnahme und auch nur bedingt möglich.

Wie erwähnt und gemäß der Empfehlungen aus /FAK 05/ wurden beim Einsatz von MELCOR in der GRS in PSA der Stufe 2 für DWR vom Typ KONVOI und SWR der Baulinie 69 auch immer komplette Unfallszenarien analysiert /SON 01/, /SON 06/. Analog sollte der Einsatz von ASTEC erprobt werden. ASTEC ist derzeit nur für den Einsatz in Druckwasserreaktoren ausgelegt. Die Anwendung auf SWR, speziell solche deutscher Baulinien, ist noch nicht möglich. Entsprechende Arbeiten insbesondere zur Modellierung der Kernzerstörung eines SWR Kerns sind im Gange, werden u. a. im europäischen Exzellenznetzwerk SARNET2 koordiniert und im Wesentlichen von IRSN und GRS durchgeführt teilweise unter Einbeziehung weitere nationaler wie internationaler Partner.

Einen Überblick über die in beiden Programmen eingesetzten Module und Packages für bestimmte Phänomene oder Anlagenbereiche enthält Tab. 3-1.

Tab. 3-1 Vergleich wesentlicher Module bzw. Packages aus ASTEC bzw. MELCOR

Modelle/Phänomene	ASTEC V1.33	MELCOR 1.8.6
Thermohydraulik	**CESAR**: zweiphasige Thermohydraulik des Kühlmittels in Reaktorkühlkreislauf und Reaktordruckbehälter und Wärmeübertragung an Strukturen	**CVH/CVT, FL, HS:** einheitliches Modell (6-Gleichungs-Modell) für Thermohydraulik unabhängig vom Anwendungsgebiet auf Reaktor oder Gebäude; Unterteilung in Definition der Volumina (CV), Strömungsverbindungen (FL) und Wärmestrukturen (HS)
	CPA / THY: Thermohydraulik im Sicherheitseinschluss (lumped parameter-Ansatz) und Wärmeübertragung an Strukturen	
Kernschmelzen	**DIVA:** 2D-Modul zur Beschreibung des Kernschmelzens bis zum RDB-Versagen	**COR:** 2D-Simulation des Kernschmelzens bis zum RDB-Versagen; einfaches Schmelzepoolmodell im Kernbereich und im unteren Plenum
Spaltprodukt-Freisetzung und -Transport	**ELSA**: Spaltproduktfreisetzung aus den Brennstäben	**RN:** Spaltproduktfreisetzung aus den Brennstäben (CORSOR-Modelle) und der Kernschmelze in der Reaktorgrube (VANESA), Transport der Spaltprodukte mit dem Kühlmittel und Aerosolverhalten in Gebäuden
	SOPHAEROS: Transport, Ablagerung sowie Wiederfreisetzung von Spaltprodukten in Dampfform oder als Aerosol im Reaktorkühlkreislauf	
Spaltproduktverhalten	**CPA/AFP:** Aerosol- und Spaltproduktverhalten im Sicher-	

Modelle/Phänomene	ASTEC V1.33	MELCOR 1.8.6
	heitseinschluss	
	ISODOP: Zerfall von Spaltprodukten und Aktinid-Isotopen	kein Modell in MELCOR
Jodverhalten	**IODE:** Jod- und Ruthenium-verhalten im Sicherheitsbehälter (Sumpf- und Gasphase)	**RN:** einfaches Modell (MAEROS) für Jodverhalten im Sumpf, bisher nicht für Anlagenrechnung angewendet
RDB-Versagen / DCH	**RUPUICUV, CORIUM**: Direkte Aufheizung der Atmosphäre des Sicherheitsbehälters (DCH) durch fein fragmentierte Schmelze nach RDB-Versagen unter hohem Druck	**FDI:** parametrisches Modell zur Berechnung der Freisetzung der Schmelze aus dem RDB und ggf. der direkten Aufheizung der Atmosphäre des Sicherheitsbehälters (DCH) durch fein fragmentierte Schmelze nach RDB-Versagen unter erhöhtem Druck
Schmelze-Beton-Wechselwirkung	**MEDICIS**: Schmelze-Beton-Wechselwirkung	**CAV:** Schmelze-Beton-Wechselwirkung basierend auf CORCON
H2-Verbrennungen	**PROCO, COMB:** Berechnung der H2-Verbrennung im Sicherheitsbehälter	**BUR:** Berechnung der H2-Verbrennung im Sicherheitsbehälter (HECTOR)
Steuerung von Sicherheitseinrichtungen	**SYSINT**: Management technischer Sicherheitseinrichtungen	**CF:** ‘control function‘ zur Steuerung und Regelung von Komponenten und Vorgängen

Bei der GRS wurden seit 1995 die Grundzüge des MELCOR-Datensatzes für DWR am Beispiel von GKN-2 geschaffen. Es wurden erste Rechnungen mit MELCOR 1.8.2 zum Verhalten des Reaktorkreislaufes durchgeführt und der erstellte Datensatz durch einen Codevergleich mit dem Detailcode ATHLET der GRS abgesichert. Im Vorhaben SR 2227 wurde seit 1995 MELCOR 1.8.3 mit einem einheitlichen, erweiterten Datensatz für GKN-2 für alle Unfallanalysen angewendet /ERV 98/. Vorher wurden die Modellierung des Sicherheitsbehälters (SB) der Referenzanlage vom Typ DWR 1300 KONVOI komplettiert und der Datensatz durch Vergleiche mit den Detailcodes RALOC mod4 bezüglich der Thermohydraulik im SB und WECHSL 3.2 bezüglich der Berechnung der Beton-Schmelze-Wechselwirkung (BSWW) weiter abgesichert /SON 98/. Schließlich wurden mit der Version MELCOR 1.8.4 im Rahmen eine Vorhabens zur ‘Bewertung von Maßnahmen des anlageninternen Notfallschutzes zur Schadensbegrenzung für LWR‘ umfangreiche Untersuchungen für eine Vielzahl von Leckstörfällen und Transienten durchgeführt /SON 01/ und der erstellte Datensatz erneut durch einen Codevergleich mit dem Detailcode ATHLET-CD der GRS abgesichert /SON 01a/.

Für ASTEC wurden erste Analysen beginnend mit der Version ASTEC V0 seit 1998 durchgeführt. Dabei wurde die Phase des Ausdampfens des Kerns nur vereinfacht simuliert. Das in ASTEC V0 verwendete Modul VULCAIN beginnt mit der Simulation, wenn der Wasserspiegel im RDB die obere Kerngitterplatte erreicht hat. Das Verdampfen des Wassers im Kern wird mit einer vereinfachten Modellierung berechnet. In der späten Phase wird die Bildung und Entwicklung eines Schmelzesees, das Abstürzen der Kernschmelze in die Kalotte des RDB-Bodens und - mit gröberer Modellierung - das Verhalten der Kernschmelze in der Kalotte sowie das RDB-Versagen simuliert. Die Ergebnisse zweier Leckstörfälle wurden mit MELCOR-Rechnungen verglichen. Für den Bruch der Druckhalterverbindungsleitung war eine MELCOR 1.8.3-Analyse verfügbar und für das 200 cm² Leck im heißen Strang eine MELCOR 1.8.4-Analyse /SCH 03/.

Mit Übergang auf die Version V1 beschreiben die neu entwickelten die Module CESAR und DIVA die Phänomene und transienten Prozessparameter im Kühlkreislauf und im Kern sowohl vor als auch während der Kernzerstörungsphase. CESAR simuliert die Thermohydraulik im gesamten Primärkreis bis zum Beginn der Kernzerstörung. Ab diesem Zeitpunkt wird das Modul DIVA aktiviert und übernimmt die Beschreibung der Thermohydraulik und Zerstörungen im Kernbereich bis zur oberen Gitterplatte, das untere Plenum und einen Teil des Fallraums (‘downcomer‘), während CESAR das obere Plenum, den Deckelbereich, den oberen Teil des Fallraums den Kühlkreislauf (sowohl primär- als auch sekundärseitig) erfasst.

Eine erste Analyse im Rahmen des RS1147 mit der neuen ASTEC-Version zeigte, dass die Stabilität des Codes signifikant erhöht worden ist /ALL 07/ Eine Rechnung mit allen Modulen war möglich. Einige Parameter für die Simulation eines Leckstörfalls wurden mit MELCOR verglichen und zeigten, dass in den wesentlichen thermohydraulischen Ergebnissen wie Primärkreisdruck, Druck im Sicherheitsbehälter qualitativ und quantitativ ähnliche Resultate erzielt werden konnten. Große Unterschiede wurden beobachtet bei der Wasserstoffproduktion während der Kernzerstörung (‘in-vessel Phase‘). Nur 50 % der H_2-Masse, die MELCOR ausrechnete, konnten erzielt werden. Außerdem traten Unterschiede in der Freisetzungsrate der Spaltprodukte bedingt durch Unterschiede in der Berechnung des Kernzerstörungsablaufs auf. Die in den Sicherheitsbehälter gelangten Aerosol und Jodmassen waren im untersuchten Fall zu gering, möglicherweise wegen zu hoher Ablagerungen im oberen Plenum des RDB. Weitere Verbesserungen wurden mit dem Fortgang der Entwicklung erwartet.

3.5.1 Definition der Unfallszenarien für einen deutschen DWR 1300 KONVOI

Die Arbeiten im Rahmen dieses Arbeitspunktes beinhalten einerseits zunächst die Diskussion und Auswahl charakteristischer Unfallszenarien für einen Druckwasserreaktor des Typs KONVOI und andererseits die Erarbeitung einer abgestimmten Vorgehensweise für den Vergleich der ASTEC Rechnungen mit solchen von MELCOR. Als Ergebnis der Diskussionen wurden zwei Szenarien ausgewählt, die sich in ihrem prinzipiellen Störfallablauf unterscheiden und dabei möglichst alle Module (ASTEC) oder Packages (MELCOR) der beiden Programme ansprechen und insbesondere mit Blick auf die Analyse der Aerosol,- Radionuklid- und Wasserstofffreisetzung beim kernschmelzen von Bedeutung sind. Die Auswahl ist Konform mit Empfehlungen des PSA-Fachbands für die Durchführung von Unfallanalysen in PSA der Stufe 2 /FAK 05/. Dies geschah unter Einbeziehung der Erfahrungen aus früheren Projekten z. B. zu Unfallanalysen mit MELCOR und zur Bewertung des Unfallrisikos bei DWR deutscher Bauart. Für die Auswahl der zu bearbeitenden Fälle innerhalb dieses Vorhabens waren unterschiedliche Gesichtspunkte ausschlaggebend. Dies betraf insbesondere:

- verschiedenartige auslösende Ereignisse – *Leck bzw. Transiente*,
- die Verfügbarkeit von System- und Sicherheitseinrichtungen – *mit bzw. ohne Notkühlsysteme und Abfahren der Dampferzeuger*,
- den Zeitpunkt des Beginns und des Ablaufs der Kernzerstörungsphase – *früher bzw. später(er) Beginn der Kernzerstörung*,
- den Ort der Kühlmittel-, Wasserstoff,- und Spaltproduktfreisetzung in den Sicherheitsbehälter – *Leck im kalten Strang oder DH-Abblasetank*, sowie
- den Zustand innerhalb des SB während der Kühlmittel-, Wasserstoff,- und Spaltproduktfreisetzung sowie als Folge der Kernzerstörungsphase – *unterschiedliche konvektive Randbedingungen und mittlere Dampfgehalte*.

Die ausgewählten Unfallabläufe ergeben sich wie folgt:

- Kleines Leck (50 cm²) im kalten Strang der Hauptkühlmittelleitung des Druckhalterstrangs sowie
- Transiente infolge Totalausfalls der Speisewasserversorgung.

Die Fallauswahl orientiert sich an deren Eintrittshäufigkeit und der Risikorelevanz basierend auf Ergebnissen der PSA der Stufe 1.

Bei den ausgewählten Szenarien mussten Annahmen über die Systemverfügbarkeiten dem Analyseziel angepasst werden. So werden einerseits z. B. schadensverhindernde Maßnahmen, die Wärmeabfuhr über die Sekundärseite und aktive Einspeisesysteme (Notkühlsysteme) teilweise als unwirksam oder ausgefallen angenommen, um einerseits den Bereich von Unfallabläufen zu erreichen, der hier analysiert werden soll und andererseits unterschiedliche Anforderungen an die erforderlichen Module und Packages der Programme zu bekommen. Des Weiteren werden die passiven autokatalytischen Rekombinatoren im Sicherheitsbehälter modelliert, ggf. trotzdem mögliche Verbrennungsvorgänge aber unterdrückt. Beim Leckstörfall wird ein vollständiger Ausfall der Hochdruck- und Niederdrucksicherheitseinspeisung unterstellt, so dass hier nur die Druckspeicher als passives Einspeisesystem zur Verfügung stehen.

3.5.2 Beschreibung der eingesetzten Datensätze

Die Aussagesicherheit der zu erzielenden Ergebnisse hängt maßgeblich von zwei Faktoren ab. Einerseits sind dies die im jeweiligen Programmsystem aktivierten Modelle zur realistischen Abbildung der entsprechenden Phänomene. Dazu sind die notwendigen Eingabeparameter zur Berechnung spezifischer Phänomene entsprechend den Anforderungen im Eingabedatensatz zu spezifizieren. Abhängig von der Umsetzung im jeweiligen Programmsystem sind teils unterschiedliche Parameter zu definieren. Andererseits bestimmen im Allgemeinen der Grad der Detaillierung der Anlage und ihre programmtechnische Umsetzung in ein geeignetes Nodalisierungsschema die Qualität der Ergebnisse. Schließlich sind die Erfahrung des Codeanwenders bei der Erstellung des Datensatzes sowie der Auswertung der Rechnungsergebnisse von nicht zu unterschätzender Bedeutung. Aus zurückliegenden Vorhaben der GRS stand für beide Programme ein Basisdatensatz für einen DWR vom Typ KONVOI zur Verfügung. Die prinzipielle Nodalisierung von Reaktorkreislauf und Sicherheitsbehälter ist in beiden Datensätzen weitgehend ähnlich, was unter Gesichtspunkten der Vergleichbarkeit der Rechnungen im Vorhaben wichtig ist.

Die Nodalisierung wird im Nachfolgenden kurz erläutert und stellt quasi den Basisdatensatz dar, der für das jeweils betrachtete Störfallszenario gewisse Modifikationen erfährt, wie z. B. unterschiedliche Verfügbarkeiten von Not- und Nachkühlsystemen, Leckposition, usw..

Der Reaktorkreislauf besteht in beiden Programmen aus zwei Modellloops, einer separaten Abbildung des Druckhalters und seines Abblasetanks sowie maßgeblicher betrieblicher Systeme (Pumpen, Ventile, Behälter). Abb. 3-4 bzw. Abb. 3-5 zeigen das jeweilige Schema der Nodalisierung des Reaktorkühlsystems für MELCOR bzw. ASTEC, das für diese Analysen verwendet wurde. Die zwei Loops (Kreisläufe) stellen einerseits den einzelnen Kreislauf dar, der den Druckhalter und ein eventuelles Leck beinhaltet, während der zweite Kreislauf die anderen drei identisch aufgebauten Kühlkreisläufe zusammenfasst, was im Allgemeinen nicht nur eine Vereinfachung des Datensatzes zur Folge hat sondern insbesondere auch den Rechenaufwand und somit die Rechenzeit vermindert. Dieses Vorgehen ist gängige Praxis und wurde auch hier angewendet. Die Anzahl verwendeter Zonen unterscheidet sich etwas zwischen beiden Programmen z. B. im Bereich des Reaktorkerns und der Dampferzeuger, was unter anderem durch die Art der Modellierung der Thermodynamik in den beiden Programmen bedingt ist. Die unabhängig von der Nodalisierung des Reaktorkreislaufs vorzunehmende Unterteilung des Reaktorkerns in radiale Zonen und axiale Bereiche ist in beiden Programmen ähnlich gewählt. In MELCOR sind es wie bisher fünf radiale Bereiche und zehn axiale Schichten für den aktiven Kernbereich; in ASTEC sechs radiale Ringe bei gleicher Anzahl axialer Schichten von zehn.

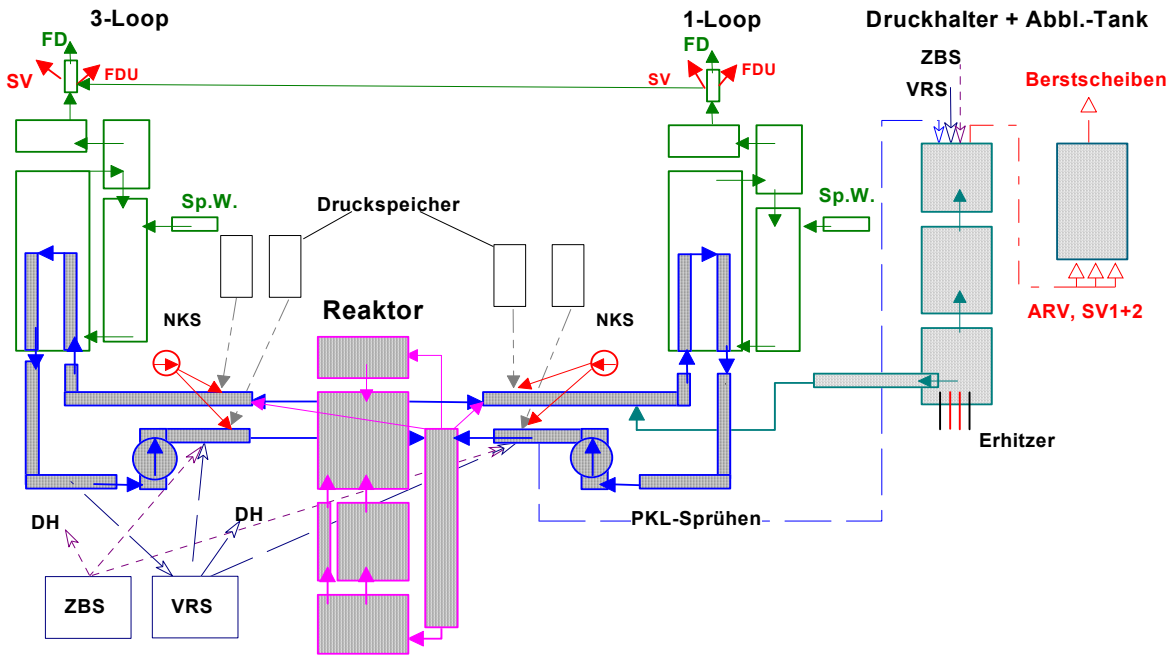


Abb. 3-4 MELCOR – detailliertes Schema des DWR-Reaktorkühlkreislaufs

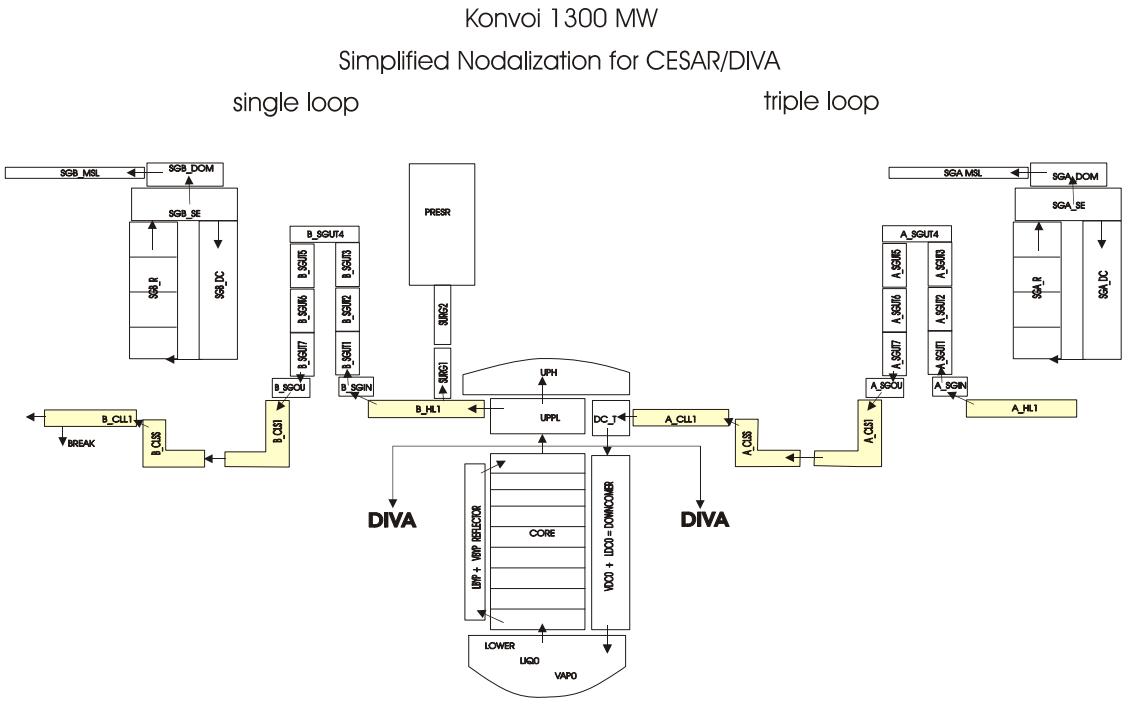


Abb. 3-5 ASTEC V1– CESAR Nodalisierung für den Primärkreis

Auch für die Nodalisierung des Sicherheitsbehälters wurde eine weitgehende Übereinstimmung beider Modelle angestrebt. In beiden Programmen können die Raumbereiche inner- und außerhalb des SB durch eine frei wählbare Anzahl von Kontrollvolumen abgebildet werden, die durch zu definierende Strömungsverbindungen gekoppelt sind. Diese sind an die realen Gegebenheiten weitestgehend angepasst. Ein Unterschied zwischen dem CPA-Modul aus ASTEC und demjenigen aus MELCOR besteht darin, dass in CPA wasser- und gasführende Strömungen getrennt simuliert werden müssen. In MELCOR wird dies in einem einzigen Strömungspfad simuliert. Bei der Modellierung des Sicherheitsbehälters wurden charakteristische Raumbereiche einzeln abgebildet und kleinere zusammengefasst dargestellt. Prinzipiell erfolgte eine Unterteilung des Sicherheitsbehälters in zwei Hälften.

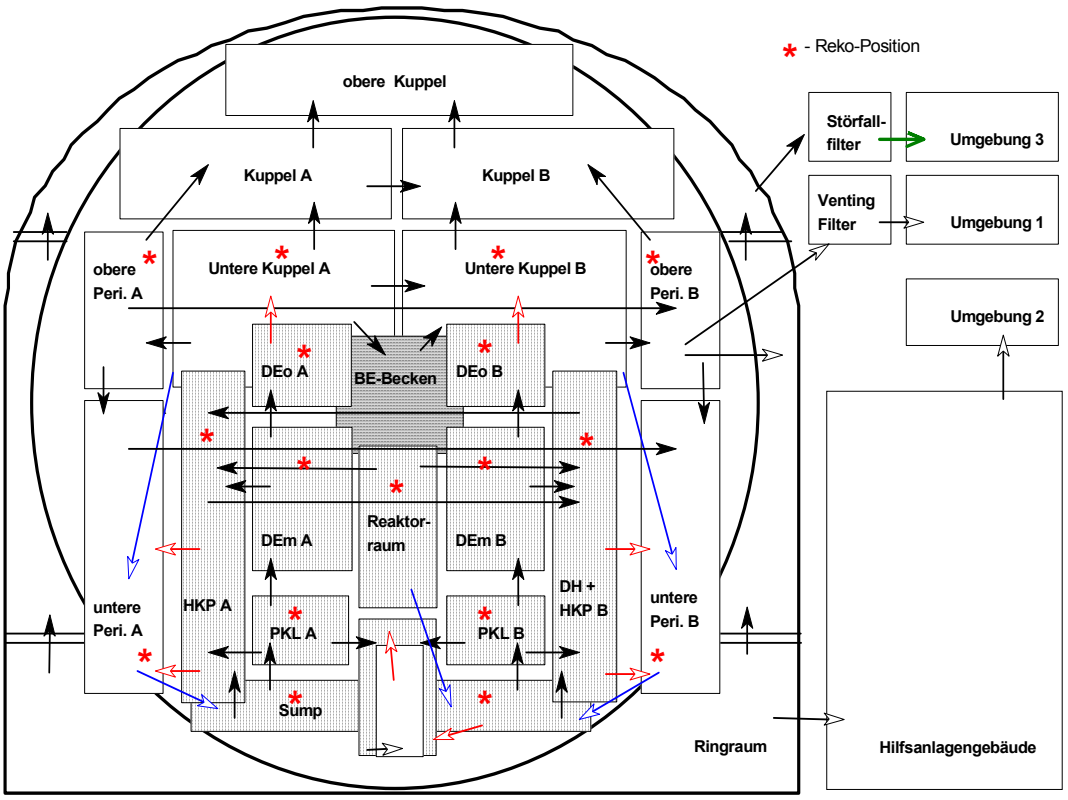


Abb. 3-6 MELCOR – Nodalisierung des Sicherheitsbehälters

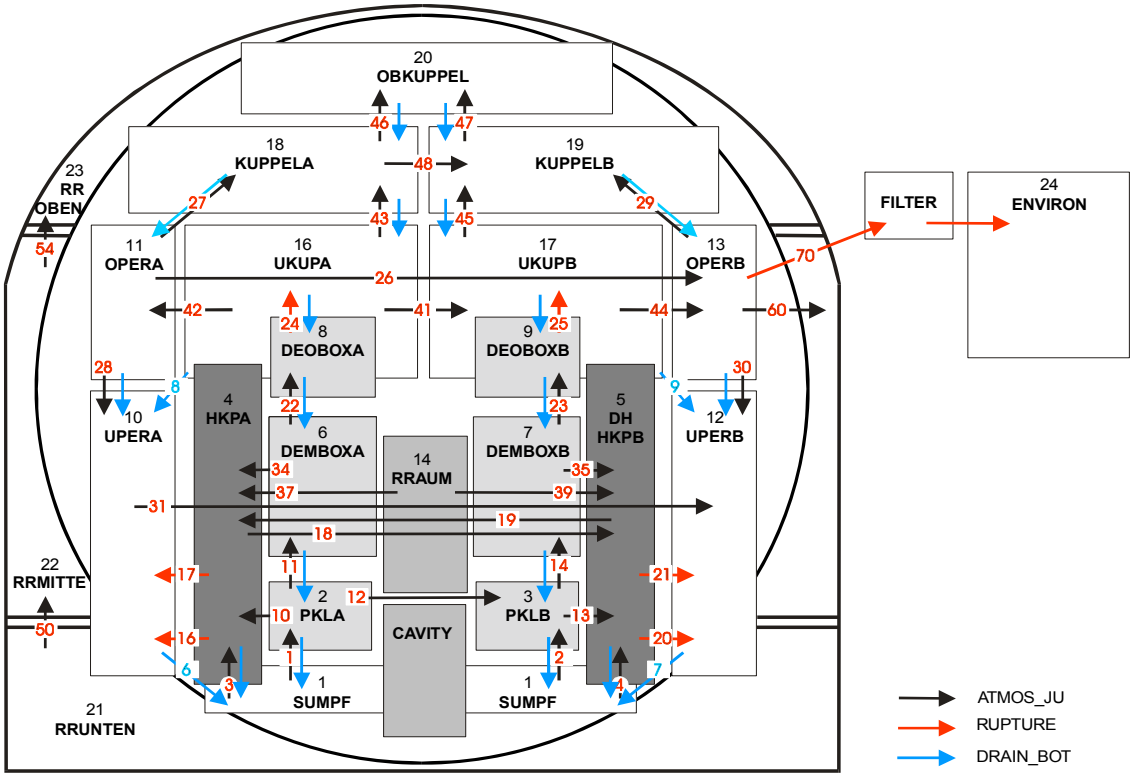


Abb. 3-7 ASTEC – Nodalisierung des Sicherheitsbehälters

Im Rahmen des Vorhabens wurden weiterhin verschiedene Erweiterungen insbesondere im ASTEC Datensatz realisiert, um einen ähnlichen Systemzustand wie in der MELCOR-Modellierung sicherzustellen. In MELCOR erfolgten die für den Übergang von MELCOR 1.8.4 (Basisdatensatz) auf MELCOR 1.8.6 erforderlichen Änderungen und es wurde ein neues Ausgangsinventar radioaktiver Stoffe im Kern in Abstimmung mit ASTEC in den Datensatz eingefügt. Die Änderungen für ASTEC sind nachfolgend kurz zusammengefasst:

- **Nachzerfallsleistung**

Nach dem Einfallen der Steuerstäbe und mit dem Abfallen der Neutronenleistung stellt ASTEC das eigenständige Modul ISODOP zur Verfügung, das die Nachzerfallsleistung aus dem Spaltprodukt-Spektrum der eingegebenen Nuklide unter Berücksichtigung der Nachzerfallsketten berechnet. Die notwendige Ausgangszusammensetzung des Kerninventars an Aktiniden und Spaltprodukten wird vorab von COCOSYS berechnet. Erste Testrechnungen auf Basis dieses Isotopeninventars erzeugten dann aber eine Nachzerfallsleistung, die deutlich von der entsprechend für MELCOR aufbereiteten neuen Eingabe des Ausgangsinventars abwich. Umfangreiche Analysen auch in Verbindung mit IRSN als Entwickler dieses Moduls führten dann dazu, dass die Eingabe des Isotopeninventars modifiziert werden musste. Die Ursache der Unstimmigkeiten lag darin, dass einige der aufgeführten Elemente nicht in der Database (MDB) von ASTEC vorhanden waren. Außerdem muss bei Eingabe der Nuklide eine bestimmte Reihenfolge der Elemente erfolgen (Tochternuklide nach den Mutternukliden). Nachfolgende Testrechnungen führten integral zu einer identischen Nachzerfallsleistung. Abweichungen der Radionuklidmassen ergeben sich ggf. zu späteren Zeitpunkten auf Grund der Zerfallsketten, die langfristig die Isotopenzusammensetzung verändern und nur in ASTEC berücksichtigt werden. Angenommen wurde eine typische Kernbeladung mit einem mittleren Abbrand von 40 GWd/tU.

- **100 K/h-Abfahren**

Das 100 K/h-Abfahren wird ausgelöst durch das Signal ‘Primärkreisdruck < 13,1 MPa‘. Für ASTEC muss dazu mittels sogenannter Analyse-Strukturen, ähnlich einer einfachen Programmiersprache, eine sogenannte EVENT-Steuerung für das Abfahren programmiert. Der aktuelle Druck wird mit einem in einer Tabelle vorgegebenen Druck verglichen. Die Ventilöffnung wird so gesteuert, dass die Abweichung kleiner als

0,1 MPa ist. Das Abfahren wird dabei über eine Abblasestation am Sammler, die den Ventilquerschnitt aller Dampferzeuger repräsentiert, durchgeführt.

- **Bespeisen der Dampferzeuger**

Ähnlich dem 100 K/h-Abfahren wurde eine EVENT-Steuerung für die Füllstandsregelung der Dampferzeuger erstellt. Im Rahmen eines mehrtägigen Arbeitsaufenthaltes beim französischen Hauptentwickler IRSN wurde der Datensatz eingehend analysiert und notwendige Modifikationen vorgenommen. Die Dampferzeuger werden mit den Notspeisepumpen bespeist. Hierbei soll der Füllstand nach dem 100 K/h Abfahren auf einen Wert von 11,6 m angehoben und gehalten werden. Nach dem Ausfall der Bespeisung sinkt der Füllstand dann wieder kontinuierlich ab.

- **Primärseitige Druckentlastung**

Die an die Regel- und Sicherheitsventile des Druckhalters anschließende Leitung sowie der Abblasetank selbst sollten ursprünglich als Objekte des Primärkreislaufs in CESAR modelliert werden um auch die in der Rohrleitung auftretenden Phänomene für die Aerosol- und Spaltproduktablagerung mittels des dafür zuständigen Moduls SOPHAEROS zu simulieren. Dies konnte aber auch nach Rücksprache mit dem für das CESAR Modul verantwortlichen IRSN nicht realisiert werden, so dass alternativ diese Objekte vom Containmentmodul CPA modelliert wurden. Die Simulation war dann aber nur ohne die Berücksichtigung von hygroskopischen Aerosolen im CPA Modul möglich. Die Öffnung sämtlicher Druckhalterventile wird in der Event-Steuerung eingeleitet nachdem die Durchschnittstemperatur im Kern 400 °C überschreitet oder das RDB-Füllstandskriterium MIN3 unterschritten wird. Modelliert wurde ferner das Versagen der Berstscheiben des Abblasetanks.

- **Lüftungssysteme in den Anlagenräumen**

Vereinfacht modelliert wurde das betriebliche Lüftungssystem der Anlagenräume des SB. Im Modell wird die Zuluft über einen so genannten FAN in den Systemeingaben aus der Umgebung (ENVIRON) in die unteren Anlagenräume (HKPA, DHHKPB, PKLA; PKLB, CAVITY und RRAUM) eingeleitet. Die Abluft wird über einen entsprechenden FAN aus den oberen Anlagenräumen und ebenso aus der Reaktorgrube abgegeben.

Das Anstehen der Notkühlkriterien wird über eine Eventsteuerung (STRU EVENT) abgefragt. Mit anstehenden Notkühlkriterien werden die SB-Lüftungssysteme ausgeschaltet. Sie werden außerdem alternativ abgeschaltet 60 s nachdem der Druckhalterfüllstand unter die 2,28 m Marke gesunken ist.

Der Ringraum besteht vereinfachend aus drei Volumina (vgl. Abb. 3-6). Lüftungseintritt für das betriebliche Lüftungssystem ist in RRUNTEN und Lüftungsaustritt von RRMITTE in die Umgebung. 300 s nach dem Anstehen der Notkühlkriterien wird die betriebliche Lüftung komplett abgeschaltet und eine gefilterte Ringraumabsaugung über den EVENT zugeschaltet. Der Lüftungsaustritt erfolgt von RRMITTE über einen Filter mit vorgegebener Rückhaltung für Aerosole und Iod von 99.9 %.

3.5.3 Durchgeführte Rechnungen mit ASTEC 1.33 und MELCOR 1.8.6

Die Rechnung wurde mit den ASTEC-Modulen CESAR, DIVA, CPA, CORIUM, RUPUICUV, SOPHAEROS, IODE, ISODOP und MEDICIS durchgeführt. Somit sind alle Module zur Berechnung der wesentlichen Phänomene während des Unfalls aktiviert.

In MELCOR werden wie in den früheren Rechnungen auch alle Packages bis auf das Iode-Modul verwendet. Zur Simulation der Spaltproduktfreisetzung aus Kern und RDB können verschiedene Modelle aktiviert werden. Von den Entwicklern wurde früher das Modell ‘CORSOR-M basierend auf dem Verhältnis Oberfläche / Volumen‘ vorgeschlagen. Neu ist das ‘überarbeitete CORSOR-Booth Modell für hoch abgebrannten Brennstoff‘. Bei dieser Arbeit wird das neue Modell (rev. C-Booth) eingesetzt.

Basierend auf den beiden Störfallszenarien „kleines Leck“ und „Ausfall Speisewasser“ wurden verschiedene Rechnungen durchgeführt. Zusätzliche Rechnungen wurden mit ASTEC durchgeführt um den Wassereinbruch vom Containmentsumpf in die Reaktorgrube nach Durchschmelzen des Innenschilds in der späten Phase des Unfalls nach RDB-Versagen näherungsweise zu simulieren und vergleichbare Daten wie MELCOR zu erzeugen. Weitere Wiederholungsrechnungen wurden mit ASTEC notwendig, da bis dato mit Eintreten des RDB-Versagens standardmäßig die Module zur Thermohydraulik im Primärkreis (CESAR) sowie zur Kernzerstörung (DIVA) abgeschaltet wurden. Bei den abschließend durchgeführten Rechnungen liefen beide Module auch nach RDB-Versagen weiter, was für die Fortführung der Kernzerstörungsphase und die Verlagerung von Kernmaterial in die Reaktorgrube wesentlich ist. Die bei Rechnungen mit Integralprogrammen naturgemäß große Anzahl an Ergebnisparametern für die In-Vessel-

und Ex-Vessel-Phase sowie für das Containment, mit thermohydraulischen Daten, Daten zum Spaltprodukt- und Aerosoltransport sowie zur Kernzerstörung und Kernschmelze-Beton-Wechselwirkung erfordern einen erhöhten Aufwand bei der Auswertung und zur Erstellung konsistenter Datenfiles beider Programme.

4 Ergebnisse

4.1 Methoden zur probabilistischen Bewertung softwarebasierter digitaler Leittechnik

Die Ergebnisse umfangreicher Untersuchungen der GRS zum Stand von Wissenschaft und Technik auf dem Gebiet der Zuverlässigkeitsbewertung softwarebasierter Leittechnik haben gezeigt, dass derzeit intensiv und branchenübergreifend nach einer anerkannten Methode hinsichtlich einer quantitativer Bewertung softwarebasierter Leittechnik geforscht wird.

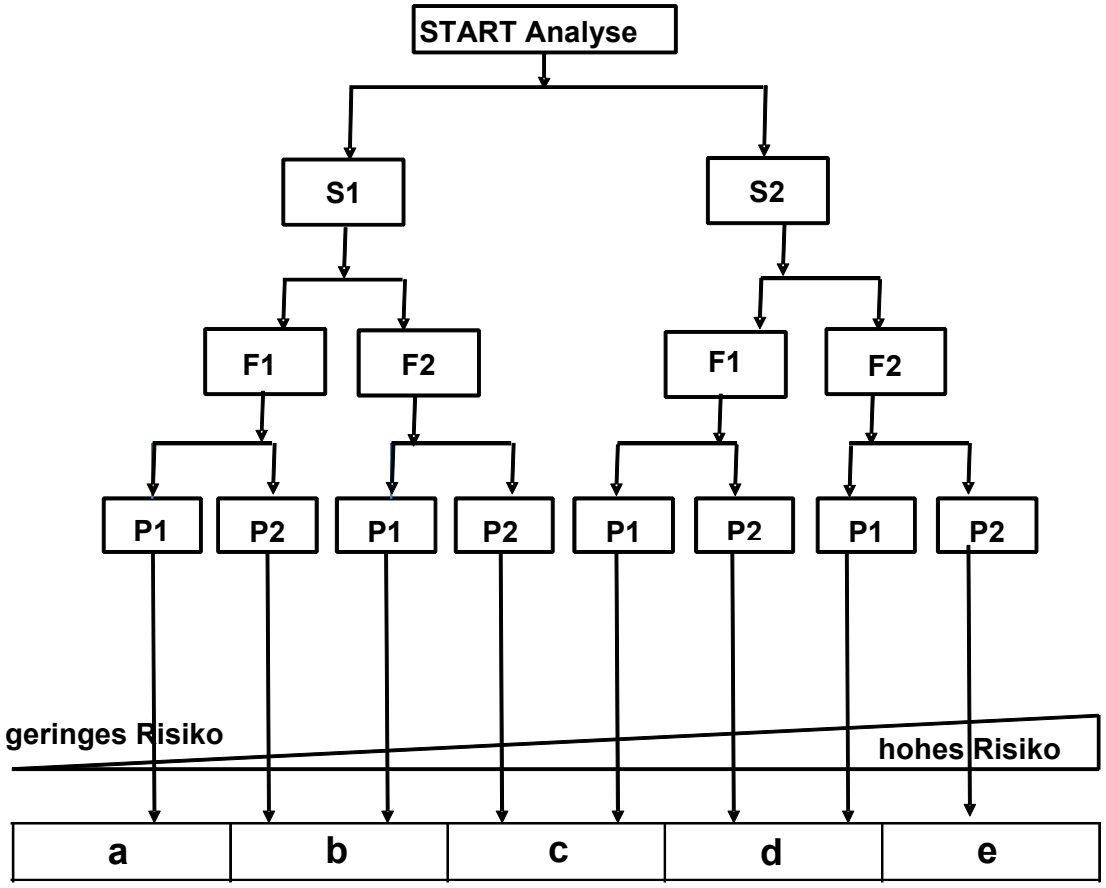
Im nicht-nuklearen Bereich wird bereits die Anwendung eines probabilistischen Bewertungsansatzes von sicherheitsbezogenen Funktionen (u. a. im Maschinen- und Anlagenbau) durch die Sicherheitsnormen (DIN-EN-Normen, Typ A: Gestaltungsgrundsätze und Risikobeurteilung für Maschinen und Anlagen) im Rahmen der Gefahrenanalyse gefordert. Dieser Ansatz wurde in den DIN-IEC-Normen, ausgehend von der IEC-61508, auch in den untergeordneten Normen wie IEC 61511 (Anlagenbau) und IEC (EN) 62061 (Maschinenbau) umgesetzt. Die Norm ISO 13849 bietet dazu einen relativ einfachen Ansatz der Risikograph-Methode (s. Abb. 4-1) unter Anwendung probabilistischer Kriterien (Wahrscheinlichkeit gefahrbringender Ausfälle pro Stunde) zur Bestimmung des Sicherheits-Integritätslevels (SIL):

- Sicherheits-Integritätslevel 1 - 4:
  Dabei handelt es sich um vier diskrete Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität der Sicherheitsfunktionen, wobei der SIL 4 die höchste Stufe der Sicherheitsintegrität und der SIL1 die niedrigste darstellen.

- Sicherheitsintegrität:
  Die Sicherheitsintegrität ist die Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt.

Die Bestimmung der Wahrscheinlichkeit eines risikorelevanten Ausfalls der Hardware (Baugruppe) kann nach dem Berechnungsmodell aus der Normen DIN-IEC-62061 oder ISO 13849 unter Verwendung der Herstellerdaten (z. B. MTTF – Mittlere Zeit bis zum Ausfall), von Daten aus der Betriebserfahrung (z. B. empirische Ausfallraten) und von Schätzungen (z. B. β-Faktor, als Anteil von Ausfällen, die eine gemeinsame Ursache

haben) erfolgen. Für die Software werden in den DIN-IEC-Sicherheitsnormen gegenwärtig lediglich deterministische Methoden wie z. B. Software-FMEA und qualitative Bewertungskriterien genannt.



S = Schwere der Verletzung
S1 - leichte, reversible Verletzungen
S2 - schwere, irreversible Verletzungen, einschließlich Tod
F = Häufigkeit/Aufenthaltsdauer der Gefährdungsaussetzung
F1 - seltene oder kurze Gefährdungsexposition
F2 - häufige oder dauernde Gefährdungsexposition
P = Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens
P1- möglich unter bestimmten Bedingungen
P2 – kaum möglich

Performance Level PL nach EN ISO 13849-1	**Wahrscheinlichkeit PFH gefahrbringender Ausfälle pro Stunde (t/h)**	**Sicherheitsintegritäts-level SIL nach DIN-EN/IEC 62061**
a	10^{-5} ≤ PFH < 10^{-4}	SIL -
b	3×10^{-6} ≤ PFH < 10^{-5}	SIL 1
c	10^{-6} ≤ PFH < 3×10^{-6}	SIL 2
d	10^{-7} ≤ PFH < 10^{-6}	SIL 3
e	10^{-8} ≤ PFH < 10^{-7}	SIL 4

a, b, c, d, e = Ziele des sicherheitsgerichteten Performance Level
Übersicht über Performance Level und Ausfallwahrscheinlichkeiten

Abb. 4-1 Anwendung der Risikograph-Methoden nach ISO 13849

Die Bewertung sicherheitsrelevanter Software bleibt auch ein zentrales Thema der jährlich stattfindenden SAFECOMP-Tagungen. Auf diesen Fachveranstaltungen (www.safecomp.org) werden moderne Verfahren zum Thema Risikobewertung und Risikomanagement in verschiedenen Industriezweigen unter den Aspekten Sicherheit, Sicherung und Zuverlässigkeit vorgestellt und diskutiert. Auf der ‘SAFECOMP 2009‘ wurde deutlich, dass in naher Zukunft noch keine etablierte Methode zur quantitativen Zuverlässigkeitsbewertung von softwarebasierten Einrichtungen zu erwarten ist. Die Verlässlichkeit von Maßnahmen der Verifizierung und Validierung von Software (V&V-Prozess: phasenspezifische Qualitätssicherung der Software) ist ebenfalls nicht quantifizierbar, weil hierzu keine nachvollziehbaren Methoden existieren. So sind z. B. die formalen Methoden (u. a. Syntax-, Logikprüfmethoden), welche die Korrektheit von Software nachweisen sollen, für praktische Anwendungen derzeit wenig geeignet. Deshalb hat sich in vielen Industriezweigen bei sicherheitsrelevanten Anwendungen, wo eine sehr hohe Zuverlässigkeit erreicht werden muss, wie in der Steuerung von Flugzeugen und der Eisenbahnsignaltechnik, neben Maßnahmen zum Erzielen einer hohen Qualität der Einsatz diversitärer (dissimilarer) Einrichtungen mit unterschiedlicher Hard- und Software etabliert.

Dennoch befinden sich einige Methoden bereits in der Erprobungsphase, die grundsätzlich in der Lage zu sein scheinen, einzelne Aspekte softwarebasierter Leittechnik hinsichtlich ihres Ausfallverhaltens zu bewerten /AP1a/ PIL 10/. Dazu zählen:

- Statische Methoden wie
  - die Ereignisbaumanalyse,
  - die traditionelle Fehlerbaumanalyse (vgl. z. B. /PIL 04/,/ALD 07/).
- Dynamische Methoden u. a.
  - Markov-Modelle,
  - Dynamic Flowgraph Methodology (DFM), Cell-To-Cell-Mapping Technique (CCMT) /ALD 07/),
  - Bayesian Analysis Methoden,
  - Petri-Netz-Modelle,
  - die simulative Analyse der Auswirkungen von Hard- und Softwarefehler (z. B. Fault Injection Methodology),

- Software-Metriken,
- Black-box methodologies (Schneidewind Model).

Eine Untersuchung zum Stand von Wissenschaft und Technik auf dem Gebiet der Methoden der Zuverlässigkeitsbewertung digitaler Leittechnik und deren Anerkennungskriterien für Bewertungen in den Kernkraftwerken wurde in der Ohio Universität im Auftrag der U.S. NRC /ALD 06/ durchgeführt. Tab. 4-1 enthält die Kriterien, die auf der Basis regulatorischer Anforderungen entwickelt wurden.

Tab. 4-1 Anforderungen an die Modellierung

Nr.	Requirement
1	The model must be able to predict encountered and future failures well
2	The model must account for the relevant features of the system under consideration
3	The model must make valid and plausible assumptions
4	The model must quantitatively be able to represent dependencies between failure events accurately
5	The model must be designed so it is not hard for an analyst to learn the concepts and it is not be hard to implement
6	The data used in the quantification process must be credible to a significant portion of the technical community
7	The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones
8	The model must be able to differentiate between faults that cause function failures and intermittent failures
9	The model must have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results
10	The methodology must be able to model the interaction of the digital I&C system portions of accident scenarios with non-digital I&C system portions of the scenarios
11	The model should not require highly time-dependent or continuous plant state information

Die Erfüllung der in der Tab. 4-1 gestellten Anforderungen wurde für die einzelnen Methoden entsprechend den Kriterien (X – erfüllt Anforderung, 0 – nicht erfüllt, ? – weitere Untersuchungen notwendig) bewertet und in Tab. 4-2 zusammengestellt.

Tab. 4-2 Erfüllung der Anforderungen durch die Methoden

Method	Requirements										
	1	2	3	4	5	6	7	8	9	10	11
Continuous Event Trees	X	X	X	X	0	?	?	X	?	?	0
Dynamic Event Trees	X	X	X	?	X	?	?	?	X	X	0
Markov Models	X	X	X	X	0	?	X	X	?	?	0
Monte Carlo Simulation	X	X	X	X	?	?	?	?	?	?	0
Petri Nets	X	X	X	X	0	?	?	?	?	?	0
Dynamic Flowgraph Methodology (DFM)	X	X	X	?	X	?	?	?	X	X	X
Dynamic Fault Trees	X	?	?	?	X	?	X	?	X	?	X
Event-Sequence Diagram (ESD)	X	X	X	X	0	?	?	?	X	X	0
GO-FLOW, system modeling technology which could be used for the quantitative calculation of reliability analysis	X	?	X	?	0	?	?	?	X	X	X
Bayesian Methodologies	X	?	?	?	0	0	?	?	?	?	X
Test Based Approaches	?	?	X	0	X	?	X	X	?	0	X
Software Metric Based Approaches	0	?	0	0	?	?	X	X	0	0	X
Schneidewind Model, non-homogeneous Poisson process (NHPP) software reliability model	X	?	?	?	?	?	?	?	0	0	X

Aus Tabelle 4-2 ergibt sich, dass z. Zt. kein Modell alle Anforderungen erfüllt. Außerdem fällt auf, dass zu vielen Modellen nach Ansicht der Ohio University die Kenntnisse fehlen, um abschätzen zu können, welche die Anforderungen erfüllen.

Auch die internationale Arbeitsgruppe DICRel der OECD/Nuclear Energy Agency (NEA)/CSNI//WGRISK, an deren Arbeit Fachleute der GRS beteiligt waren, hat auf der Basis einer Umfrage in den Mitgliedsländern der OECD/NEA die Bewertungsmethoden ausgewertet und Empfehlungen für die Bewertung digitaler Leittechnik in der PSA erarbeitet /NEA 09/. Die bisherigen Erfahrungen der teilnehmenden Fachinstitutionen auf dem Gebiet probabilistischer Analyse softwarebasierter Leittechnik hinsichtlich einer

Modellierung relevanter Abhängigkeiten softwarebasierter Leittechnik sind in der Tab. 4-3 zusammengefasst.

Tab. 4-3 Erfahrungen internationaler Teilnehmer der DICRel Arbeitsgruppe, hinsichtlich Modellierung relevanter Abhängigkeiten SBLT

		Dependencies of the Digital Instrumentation and Control (DIC) modeled by several participants					
Organisation	**Country**	***Communication functions of the DIC***	**Support functions of the DIC**	**Sharing of hard-ware of the DIC**	**Fault-tolerance features of the DIC**	**Dynamic interactions of the DIC**	**CCF of the DIC**
VTT Technical Research Centre of Finland	Finland	X	XX	X			XX
IRSN, EDF, AREVA	France	X	X	X	X		X
GRS	Germany	X	XX	XX			X (of Hard-ware only)
JNES Japan Nuclear Energy Safety Organisation	Japan						XX
KAERI Korea Atomic Energy Research Institute	Republic of Korea	X			X		XX
HRP Halden Reactor Project	Norway						XX
INER, Institute of Nuclear Energy Research	Taiwan	XX	X	X	X		XX
BNL Brookhaven National Laboratory	USA	X	X	X	X		X
EPRI Electric Power Research Institute	USA		X	X			X
OSU The Ohio State University	USA	X	X	X	X	XX	X

Anmerkung: X – im Modell berücksichtigt, XX – wesentlicher Risiko-Beitrag

Auffallend ist hier, dass dynamische Interaktionen bisher nirgendwo berücksichtigt worden sind und das auch keine Einschätzung über die Höhe des Risikobeitrages besteht. Der CCF (Common Cause Failure) wird allgemein als hohes Risiko angesehen.

Des Weiteren haben die Experten besonders wichtige Aspekte für die zukünftige Methodenentwicklung identifiziert (vgl. Tab. 4-4).

Tab. 4-4 Übersicht wichtiger Aspekte für die zukünftige Methodenentwicklung /NEA 09/

		Most important topics of probabilistic modeling of the digital Instrumentation and Control (DIC)					
Organisation	**Country**	**Identification of failure modes**	**Dependencies of the DIC**	**Coverage by Fault-tolerance features**	**Failure Data (Hardware)**	**Software Failures**	**Human Reliability related DIC**
CNSC Canadian Nuclear Safety Commission	Canada			X			
IRSN, EDF, AREVA	France						X
GRS	Germany		X		X	X	
JNES Japan Nuclear Energy Safety Organisation	Japan					X	
KAERI Korea Atomic Energy Research Institute	Republic of Korea			X		X	X
INER, Institute of Nuclear Energy Research	Taiwan	X				X	
BNL Brookhaven National Laboratory	USA	X			X	X	
OSU The Ohio State University	USA		X				X

Aus der Mitwirkung der GRS-Experten an der Arbeit der DICRel-Arbeitsgruppe haben sich folgende, zusammengefasste Erkenntnisse ergeben:

- Die Ausfälle softwarebasierter Leittechnik werden zurzeit weltweit in der PSA der Kernkraftwerke entweder partiell (u. a. Analyse von Teilaspekten, kein Softwarefehlermodell) oder auf der Basis von Expertenschätzungen berücksichtigt,
- Die Anwendung dynamischer PSA-Methoden (u. a. Markov-Modell, Bayesian Belief Network (BBN), Dynamic Flowgraph Methodology,) für eine probabilistische Bewertung softwarebasierte Leittechnik wird seitens der Mehrheit der Fachleuten als nicht zielführend angesehen. Einige Ausnahmen stellen spezielle Fragestellungen hinsichtlich der Bewertung der Zuverlässigkeit von Personalhandlungen

in Zusammenhang mit der Mensch-Maschine-Schnittstelle softwarebasierter Leittechnik (u. a. Bedienung der Einrichtungen, Instandhaltung) dar.

Weitere Impulse bekam die Konzeptentwicklung der GRS aus dem Review einer beispielhaften Anwendung traditioneller probabilistischer Methoden für die Analyse eines softwarebasierten Leittechniksystems der Speisewasserregelung einer Siedewasserreaktoranlage. Die in /CHU 08/ vorgestellte Methode präsentiert sehr hohen Detaillierungsgrad der Modellierung der Hardware (u. a. CPU, Speicher, interne Bus-Verbindungen). Zur Modellierung der Betriebs- und Fehlerzustände dieser Komponenten wurde die Markov-Methode angewendet. Die Auswirkungen der Fehlerzustände der Komponenten auf die Verfügbarkeit der modellierten Regeleinrichtung wurden mit Hilfe eines automatisierten Werkzeugs bestimmt, das im Wesentlichen auf der Originalsoftware der leittechnischen Einrichtung basiert ist.

Aus der Sicht der GRS (siehe auch /AP1a/ PIL 10/) sind folgende Erkenntnisse relevant für die Anwendung traditioneller probabilistischer Methoden für die Analyse softwarebasierter Leittechnik:

- Bei einem hohen Detaillierungsgrad der Modellierung der Hardware sind automatisierte Werkzeuge zur Bestimmung der Auswirkungen von Ausfällen erforderlich. Die analytische Fehlerart- und Auswirkungsanalyse wird in diesem Fall extrem umfangreich und schwer durchführbar, da die Reihenfolge von Ausfällen das Ergebnis wesentlich beeinflussen kann.
- Der Rechenaufwand für die Simulation aller Fehlerkombinationen ist schon für das in /CHU 08/ analysierte relativ kleine System zweifach redundante Struktur der Signalverarbeitung) sehr hoch.
- Für die entwickelte Methodik besteht noch ein erheblicher Weiterentwicklungsbedarf hinsichtlich:
  - Verifikation und Validierung des verwendeten Werkzeugs zur Simulation des Systemverhaltes,
  - Modellierung von gemeinsam verursachten Ausfällen (GVA),
  - Bestimmung der Zuverlässigkeitskenngrößen der Hardware, insbesondere unter Verwendung von Betriebserfahrungen aus der Nuklearindustrie und vergleichbarer Anwendungen

- Unsicherheiten der Modellierung.

Unter Berücksichtigung der o.g. Erfahrungen wurde das Konzept zur Modellierung eines softwarebasierten Leittechniksystems in der PSA aus dem BMU-Vorhaben SR 2418 /PIL 04/ zum Teil modifiziert und den neuen Erfordernissen angepasst, wobei die Methode der Fehlerbaumanalyse weiterhin zu Grunde gelegt wurde. Die Details des modifizierten Konzepts sind im technischen Fachbericht /AP1a/ PIL 10/ erläutert.

In der nachfolgenden Tab. 4-5 sind wesentliche Merkmale des modifizierten Modellansatzes im Vergleich zum Modell aus dem Vorhaben SR 2418 dargestellt.

Tab. 4-5 Gegenüberstellung der Modellentwicklung zur Bewertung softwarebasierter Leittechnik

	Konzept aus dem Vorhaben SR 2418 /PIL 04/	**Konzept des aktuellen Modellansatzes /PIL10/**
Probabilistische Analysemethode	traditionelle Fehlerbaummodellierung	traditionelle Fehlerbaummodellierung
Gegenstand der Analyse	Sicherheitsleittechnik einer Referenzanlage: zweisträngiges Notstandssystem einer Siedewasserreaktoranlage	Sicherheitsleittechnik einer generischen Reaktoranlage: Leittechnik-Funktion eines generischen Reaktorschutzsystems
Leittechniksystem	TELEPERM XS, 1. Generation	TELEPERM XS, 1. und 2. Generation
Struktur der Leittechnik-Funktionen	2-fache Redundanz: 3 Teilsysteme mit interner 2-von-3-Logik für Steuerung der verfahrenstechnischer Komponenten jedes Stranges	4-fache Redundanz: 2-von-4-Logik für Steuerung der verfahrenstechnischer Komponenten jedes Stranges
Struktur der Signalverarbeitung in jeder Redundanz bzw. Teilsysteme jeder Redundanz	1. Feldebene: analoge Messwerterfassung) 2. Signalverarbeitung: softwarebasierter Erfassungs- und Verarbeitungsrechner 3. Ansteuerung: analoge Wertungslogik und analoge Antriebssteuerung (GEAMATIC)	1. Feldebene: analoge Messwerterfassung) 2. Signalverarbeitung: softwarebasierter Erfassungs- und Verarbeitungsrechner 3. Ansteuerung: softwarebasierter Voter-Rechner und digitale Antriebssteuerung 4. Schaltanlage

	Konzept aus dem Vorhaben SR 2418 /PIL 04/	Konzept des aktuellen Modellansatzes /PIL10/
	4. Schaltanlage	
Detaillierungstiefe (Hardware)	TXS-Baugruppen, GEAMATIC-Baugruppen (analoge Voter und Antriebssteuerung)	TXS-Baugruppen, digitale programmierbare Antriebssteuerung (u.a. AV42)
Bestimmung der Ausfallart der Hardware	Ergebnisse der Fehlerart- und Auswirkungsanalyse (FMEA), TXS-Betriebserfahrung	Ergebnisse der Fehlerart- und Auswirkungsanalyse (FMEA), generische Betriebserfahrung, Expertenschätzungen
Berücksichtigung der Software	Software ist im Fehlerbaummodell nicht berücksichtigt. Es wurde zunächst ein Ansatz zur Bewertung der Komplexität der Anwendungssoftware entwickelt.	Im Fehlerbaummodell sind Basisereignisse implementiert, die Auswirkung der GVA unterschiedlicher Software (Betriebssystem, Anwendungssoftware) repräsentieren sollen. Die Quantifizierung dieser Basisereignisse sollte zum späteren Zeitpunkt durch Schätzungen auf der Basis der Betriebserfahrungen erfolgen.

Seit einigen Jahren wird national und international intensiv über die Möglichkeit von gemeinsam verursachten Ausfällen im redundanten Reaktorschutzsystem, welche mit softwarebasierter Technik (Rechner-Technik) ausgestattet werden soll, diskutiert. Deshalb gibt es Entscheidungen einiger Aufsichtsbehörden, strukturelle und gerätetechnische Maßnahmen in einer diversitären (dissimilaren) Leittechnik (mit unterschiedlicher Soft- und Hardware) für die Sicherheitsfunktionen zu fordern. International ist bereits zu erkennen, dass konkrete Maßnahmen zur Beherrschung der GVA in der softwarebasierten Leittechnik ganz unterschiedlich sein können /WOO 10/. So gibt es zwei- bzw. dreifach dissimilare Leittechnik-Strukturen für den Reaktorschutz wie heterogene Leittechnik-Strukturen mit dem Einsatz so genannter Back-up-Leittechnik-Funktionen.

In dem im Vorhaben RS1180 entwickelten neuen Konzept /AP1a/ PIL 10/ ist vorgesehen, die aktuellen Entwicklungen hinsichtlich des Einsatzes diversitärer (dissimilarer) Leittechnik zur Beherrschung der gemeinsam verursachten Ausfällen in der softwarebasierten Sicherheitsleittechnik durch die Modellanpassungen bzw. Variantenuntersuchungen mittels Fehlerbaumtechnik zu berücksichtigen. Dazu soll zukünftig eine Bewertung des Diversitätsgrades der Hard- und Software erfolgen.

Zur Entwicklung von Ansätzen zur Quantifizierung softwarebasierter Leittechnik wurden versuchsweise die Protokolldateien eines softwarebasierten Begrenzungssystems ausgewertet, um die Erkenntnisse über Umfang und Relevanz der aufgetretenen Meldungen in der Ablaufumgebung eines modernen softwarebasierten Leittechniksystems zu gewinnen. Die Idee bei der Auswertung war, dass die Meldungen u. U. als ‘Precursor‘ für sich anbahnende Fehler im System bewertet werden können. E sollte versucht werden, aus diesen ‘Precusorn‘ Ausfallwahrscheinlichkeiten abzuleiten. Die in der Analyse der Daten aufgetretenen, verschiedenen Fragen wurden in einem allgemeinen Fragenkatalog zusammengefasst. Beispielhaft sind folgende Fragen zu nennen:

- Wie wird der Zeitstempel für die Protokolldateien generiert?
- Wann treten abrupte Dateiabbrüche auf?

Durch einen Quervergleich der Häufigkeit eines bestimmten Meldungstypen mit den zugehörigen Zeitstempeln, konnten als „auffällig“ erkannte Tage mit einer besonders hohen Anzahl von Einträgen lokalisiert werden. Dadurch wurden weitere Fragen aufgeworfen, wie z. B.:

- Wie kann dieses Verhalten erklärt werden?
- Was ist an diesen Tagen vorgefallen?

Es wurden auch die Meldungen bezogen auf einzelne CPUs untersucht /PIL 10/. Aufgrund der uns zur Verfügung stehenden Informationen war es nicht möglich, die aufgetretenen Fragestellungen nachvollziehbar zu klären. Für eine vertiefte Analyse mit Beschaffung der notwendigen Informationen wäre ein erheblicher Aufwand notwendig geworden. Aufgrund der vorliegenden Datenlage sind wir zu der Auffassung gekommen, dass der Versuch aus den Meldungen des Begrenzungssystems Zuverlässigkeitskenngrößen zu generieren nicht zielführend ist.

In diesem Arbeitspaket des Vorhabens RS1180 wurden zudem Aspekte der Mensch-Maschine-Schnittstelle zur softwarebasierten Leittechnik untersucht. Die durchgeführten Literaturrecherchen deuten darauf hin, dass die Unterschiede in der Mensch-Maschine-Schnittstelle zwischen analoger und softwarebasierter Leittechnik für das Kraftwerkspersonal zu einer Veränderung der Tätigkeiten führen. Zudem wurden einige mögliche Einflussfaktoren auf die Zuverlässigkeit der Personalhandlungen durch den Einsatz softwarebasierter Leittechnik identifiziert, die nachfolgend aufgeführt sind:

- Vorteilhafte Auswirkungen:
  - Verbesserte Überwachung von Personenhandlungen,
  - Verminderung kognitiver Beanspruchung.
- Nachteilige Auswirkungen:
  - Verlust des Überblicks über den Gesamtanlagenzustand,
  - Nachteile beim Zugriff auf Bedienelemente und Anzeigen,
  - Verlust des Überblicks über Handlungen der Bedienmannschaft,
  - Beeinträchtigung der Kommunikation in der Mannschaft,
  - erhöhte kognitive Beanspruchung durch das Interfacemanagement,
  - Verlust von Informationsqualität (räumliche Orientierung entfällt),
  - Schwierigkeit bei der Bildung mentaler Modelle.

Außerdem wurde festgestellt, dass sich der Schwerpunkt tendenziell zu höheren kognitiven Anforderungen verlagert und solche Effekte an Bedeutung gewinnen, die bisher nur eine untergeordnete Rolle spielten (z. B. der ‘Keyhole-Effekt‘: Einschränkung des Blickfeldes bei der Überwachung des Anlagenzustandes). Dies ist allerdings stark abhängig von Design der Mensch-Maschine-Schnittstelle und von der Art und Weise, wie das Bedienkonzept gestaltet wird.

Die internationalen Erfahrungen auf diesem Gebiet unterstreichen, dass durch die Einführung softwarebasierter Leittechnik eine Verschiebung der Rollen und Tätigkeiten des Personals in einem Kernkraftwerk erwarten lässt. Durch die höhere Verfügbarkeit von Informationen sinkt die Notwendigkeit der Kommunikation in der Warte, und es stellt eine Zusatzaufgabe dar, alle Personen auf der Warte auf dem gleichen Informationsstand hinsichtlich des Anlagenzustandes und des Standes der Handlungen der einzelnen Personen zu halten, was früher durch den ständigen Wechseln von Nachfragen, Anweisungen und Beobachtung automatisch erfolgte.

Eine allgemeine Aussage, dass die Einführung softwarebasierter Leittechnik und der damit verbundenen MMS die Zuverlässigkeit von Personalhandlungen erhöht oder senkt, kann nicht getroffen werden, da dies (wie bei der konventionellen. Leittechnik auch) von der jeweiligen technischen Umsetzung abhängt. Unter Umständen können

schon kleinste Details (z. B. Wahl der Farbgebung, Begriffswahl, Art des implementierten Bedienelementes) massive Auswirkungen auf die Verständlichkeit und die Bedienbarkeit des Systems haben.

Die bisherigen Grundlagen für die ergonomische Gestaltung der konventionellen Schnittstelle zum Menschen sind weitgehend übertragbar, einige müssen an die verwendeten neuen Medien angepasst werden /AP1/ HAR 10/. Grundlegende Änderung bei der Einführung softwarebasierter Leittechnik mit bildschirmbasierten Arbeitsplätzen ist die Reduktion der Bedienelemente und Anzeigen der Warte auf einen oder mehrere Bildschirmschirme, was zum einen eine Einschränkung der Sicht auf die Anlage bedeutet. Zum anderen bedeutet dies das Hinzufügen einer neuen Aufgabe, der Navigation zwischen den Inhalten. Die Nutzung von zwei außerordentlich gut ausgeprägten Fähigkeiten des Menschen, der Orientierung in und am Raum sowie des Erkennens von Mustern und darin enthaltenen Abweichungen, kann beim Übergang von der konventionellen Warte zu Bildschirm-basierten Arbeitsplätzen weitestgehend verloren gehen.

Auf Basis der recherchierten Informationen ist zu erwarten, dass statt einfachen Fehlhandlungen (z. B. Auslassungsfehler, Verwechslungsfehler), Fehler bei Problemlösungsvorgängen (z. B. Interpretationsfehler, Diagnosefehler, Planungsfehler, Fehler bei wissensbasierten Handlungen) an Bedeutung gewinnen.

Anhand eines Referenzsystems, welches weitestgehend auf dem Leittechniksystem TELEPERM XS basiert, wurde untersucht, welche neuen Aspekte (Tätigkeiten, Fehlermöglichkeiten, Fehlerentdeckungsmöglichkeiten, Korrekturmöglichkeiten) konkret bei der Bewertung der menschlichen Zuverlässigkeit zu erwarten sind /AP1/ HAR 10/. Für das Referenzsystem (vgl. Abb. 4-2) wurde angenommen, dass den Operateuren über eine begrenzte Anzahl von Bildschirmen nur Teilansichten der zu bedienenden Systeme präsentiert werden und die Möglichkeiten von Software im Hinblick auf Datenaggregation und -darstellung und sowie Automation genutzt werden.

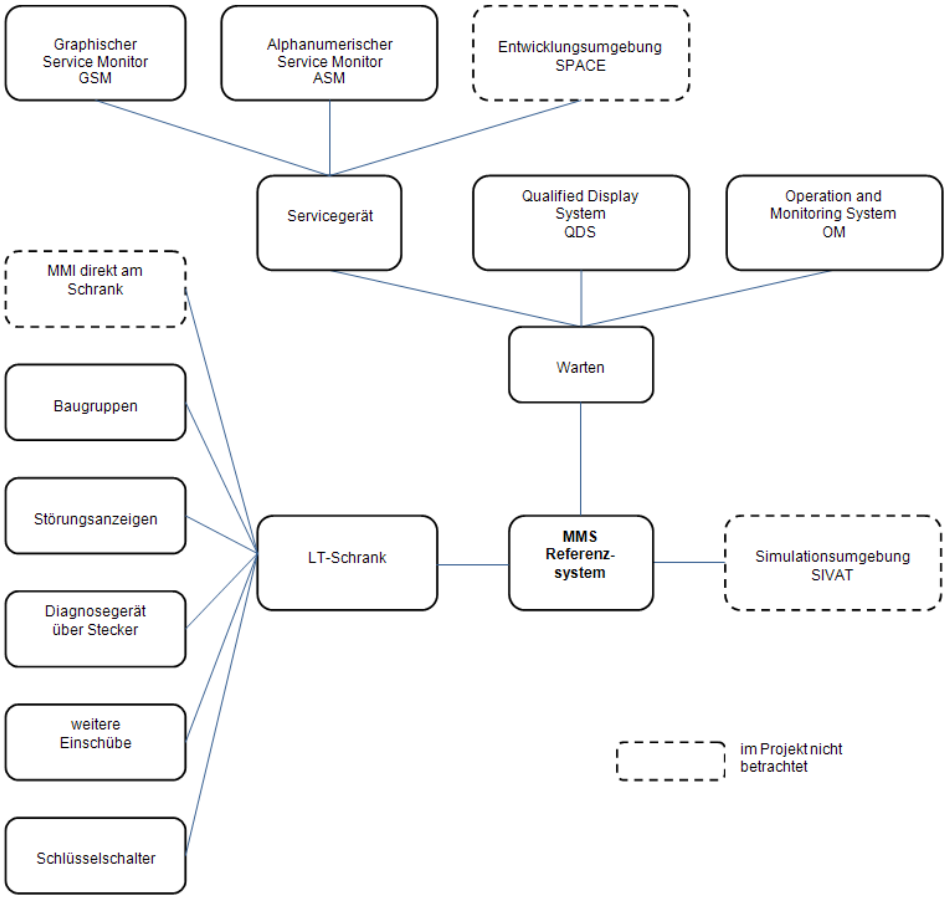


Abb. 4-2 Übersicht der Mensch-Maschine-Schnittstellen des Referenzsystems

Das generische technische Grundkonzept der Personalhandlungen wurde wie folgt festgelegt:

- Die automatische Steuerung der Verfahrenstechnik erfolgt durch die softwarebasierte Betriebs- und Sicherheitsleittechnik.
- Die Reaktorfahrer können über die bildschirmbasierten Arbeitsplätze (OM) die Anlage überwachen und mit Eingabegeräten oder über die Bildschirmdarstellungen (Touch-screens QDS) Änderungen am Komponentenzustand vornehmen.
- Über das Servicegerät kann je nach Konfiguration eine Vielzahl von Tätigkeiten (u. a. Fehlerdiagnose, Simulierungen, Softwareänderungen) erfolgen.
- Die Leittechnikschränke stellen die Mensch-Maschine-Schnittstelle bei durchzuführenden Installations-, Prüf-, Wartungs- und Reparaturarbeiten dar.

Die Untersuchungen im Rahmen dieses Vorhabens /AP1/ HAR 10/ haben gezeigt, dass die grundlegenden Vorgehensweisen zur Bewertung der menschlichen Zuverläs-

sigkeit auch beim Einsatz von softwarebasierter Leittechnik und dessen Schnittstelle weiter eingesetzt werden können.

4.2 Berücksichtigung wissensbasierter Personalhandlungen und organisatorische Einflüsse

4.2.1 Methoden zur Berücksichtigung wissensbasierter Personalhandlungen in einer probabilistischen Sicherheitsanalyse

Ziel der Arbeiten war die Entwicklung eines methodischen Gesamtansatzes zur probabilistischen Bewertung wissensbasierter, sicherheitstechnisch notwendiger Eingriffe, die in der Warte oder vor Ort auszuführen sind. Wie in Abschnitt 3.2.1 dargestellt, wurde hierzu schrittweise, wie nachfolgend dargestellt, vorgegangen.

- Ein Verfahren zur Identifikation und Beschreibung von zu untersuchenden wissensbasierten Handlungen war bereitzustellen.
- Ein Modell zur Beschreibung und Wertung der kognitiven Prozesse (Erkennung, Auswahl und Planung einer wissensbasierten Handlung) war zu entwickeln.
- Für die zu erwartenden qualitativen Bewertungsergebnissen waren Wahrscheinlichkeiten für das Misslingen wissensbasierter Handlungen vorzuschlagen, und die Bewertungsmethode war an Hand von Fallbeispielen zu erproben.

Der nun vorliegende methodische Gesamtansatz wird in Abb. 4-3 dargestellt. Er setzt sich zusammen aus dem Identifikationsverfahren, dem Kognitionsmodell und dem Quantifizierungsmodell. Alle drei Elemente werden im Folgenden ausführlicher erläutert.

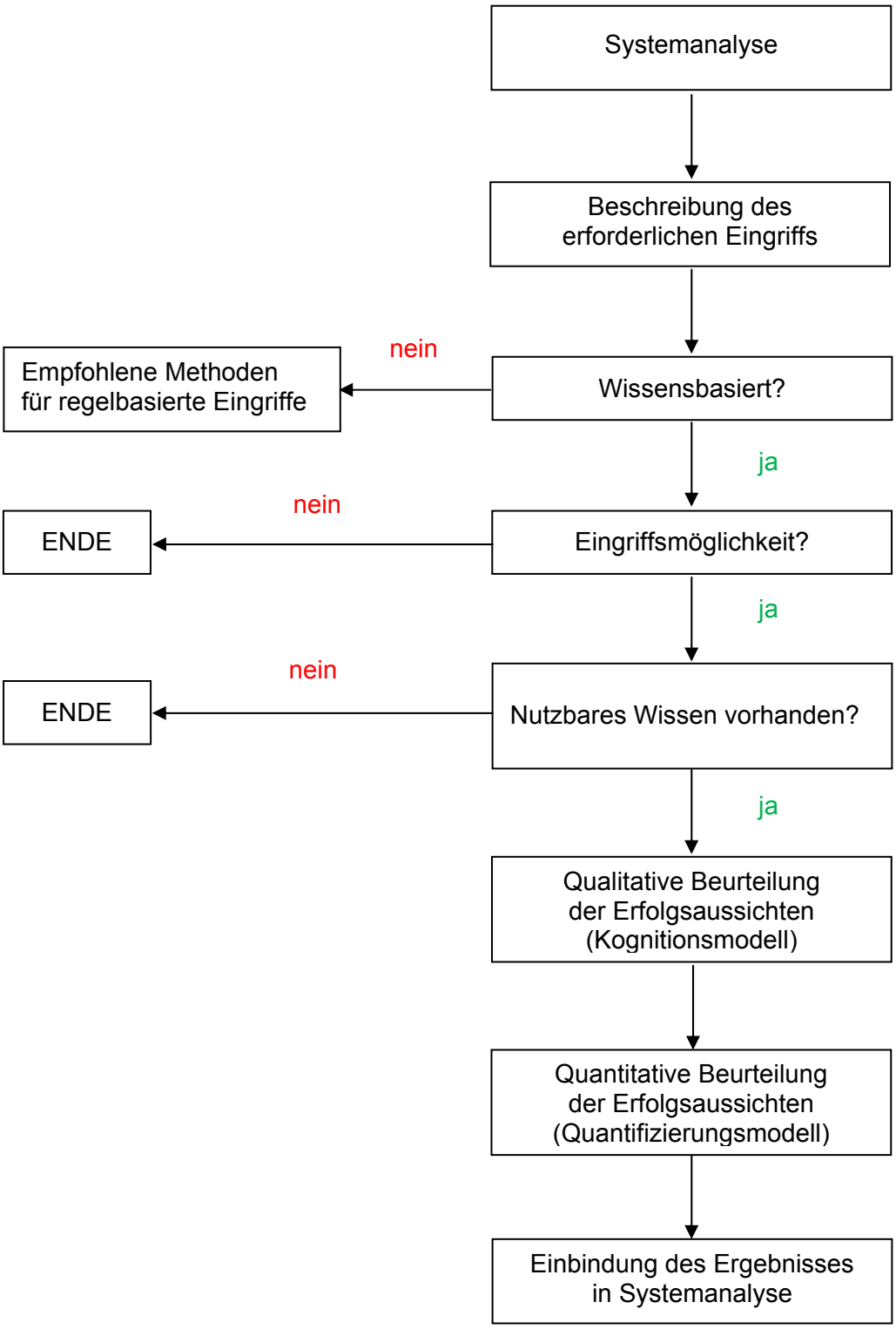


Abb. 4-3 Methodischer Ansatz

- **Identifikationsverfahren**

Das Identifikationsverfahren soll diejenigen wissensbasierten Operateureingriffe bestimmen, die der qualitativen und quantitativen Beurteilung zuzuführen sind.

Die Untersuchungen gehen von vorgegebenen, im Rahmen der System- und Ereignisablaufanalysen ermittelten Anlagensituationen aus, für die festzustellen ist, ob Operateureingriffe erforderlich sind. Dieser Schritt erfordert eine Zusammenarbeit der Arbeitsgebiete ‘System-/Ereignisablaufanalyse‘ und ‘Zuverlässigkeitsbewertung von Personalhandlungen‘. Vor einer weiteren Bearbeitung müssen erforderliche Eingriffe im Detail beschrieben werden. Hierzu ist ein Handlungsmodell zu entwickeln, welches den zu erwartenden Ablauf des Handlungsgeschehens und alle wesentlichen Randbedingungen repräsentiert (vgl. dazu auch /MEI 85/, /SWA 83/, /GRS 02/).

Beim Aufbau des Handlungsmodells sind Informationen aus der Begehung der Handlungsorte und den Gesprächen mit sachkundigem Personal des Betreibers mit einzubeziehen.

Im nächsten Schritt ist zu prüfen, ob die in Betracht zu ziehenden Operateureingriffe als wissensbasiert zu klassifizieren sind.

Die verfügbaren und im Fachband zu PSA-Methoden /FAK 05/ des PSA-Leitfadens empfohlenen Methoden zur probabilistischen Bewertung der Zuverlässigkeit von Personalhandlungen klassifizieren Personalhandlungen entsprechend den bei Erkennung, Planung und Handlungskontrolle zu erwartenden kognitiven Beanspruchungen:

- *Fertigkeitsbasiertes Verhalten (skill-based behaviour)*
  Darunter wird ein häufig geübtes Verhalten verstanden, welches nach Wahrnehmung der Eingangsinformation aufgrund der vorhandenen Erfahrung bzw. Übung quasi ‘automatische‘ Verhaltensweisen auslöst.

- *Regelbasiertes Verhalten (rule-based behaviour)*
  Darunter wird ein Verhalten verstanden, bei dem nach Erkennen der Eingangsinformation aufgrund bereits vorhandener Regeln die entsprechenden vorgeplanten Aktionen abgearbeitet werden. Regeln können schriftlich niedergelegt (u. a. im Betriebshandbuch (BHB) und Notfallhandbuch (NHB)) oder im Gedächtnis gespeichert (verinnerlicht, nachweislich häufig geübt bzw. angewandt) sein.

- *Wissensbasiertes Verhalten (knowledge-based behaviour)*
  Darunter wird ein Verhalten in ungewohnten oder neuartigen Situationen verstanden, die eine Problemlösung durch den Operateur erfordern. Nach Identifizierung der vorliegenden Merkmale einer Störfallsituation hat der Operateur erforderliche Maßnahmen zu planen und auszuführen. Hierbei stützt er sich vor allem auf sein Fachwissen. Ein ‘Problem‘ liegt dann vor, wenn der Handelnde einen Ist-Zustand in einen Soll-Zustand zu überführen hat, zunächst aber nicht weiß, wie er dieses Ziel erreichen kann. Die erfolgreiche Suche nach einem geeigneten Vorgehen und dessen Anwendung wird als ‘Problemlösung‘ bezeichnet.

Fertigkeits- und regelbasiertes Verhalten kann mit den vorhandenen Methoden bewertet werden. Handlungen der Operateure, die diesen beiden Kategorien zuzuordnen sind, sind in der Praxis u. a. durch folgende Merkmale gekennzeichnet:

- Die Handlungen sind in der den Operateuren im Anforderungsfall zur Verfügung stehenden Dokumentation (vor allem Betriebs- und Notfallhandbuch) beschrieben.
- Dem Operateur wird ein im Wesentlichen lückenloser Weg aufgezeigt, wie er ausgehend von den in der konkreten Anlagensituation beobachtbaren Informationen zu den dafür vorgesehene Gegenmaßnahmen gelangen kann. Als Hilfsmittel werden hier u. a. bereitgestellt:
  - Störfallentscheidungsbaum,
  - Schutzzieltabelle mit Verweisen auf vorgeplante Maßnahmen im BHB oder im NHB zur Wiederherstellung gefährdeter oder verletzter Schutzziele,
  - Maßnahmenleitschemata, um bei einer Reihe von möglichen Gegenmaßnahmen bei Gefährdung oder Verletzung eines bestimmten Schutzzieles die Auswahl des erforderlichen Vorgehens zu treffen,
  - Kriterien, die vorgeben, wann welche Maßnahmen vorzubereiten bzw. durchzuführen sind.

Wirksamkeit und Ausführbarkeit dieser Maßnahmen und der damit verbundenen Handlungen werden im Rahmen einer detaillierten Vorplanung geprüft.

Das Vorgehen wird im Rahmen von anlageninternen und externen Schulungsmaßnahmen ausreichend häufig geübt.

Davon abzugrenzen sind Handlungen, bei denen die sogenannte ‘wissensbasierte Verhaltensebene‘ dominant ist. Solche Handlungen und dadurch eingeleitete Maßnahmen sind beispielsweise durch folgende Merkmale gekennzeichnet:

- Es gibt für die unterstellte Situation keine vorgeplante und eingeübte Vorgehensweise.
- Hilfsmittel, die den Operateur lückenlos zu noch verfügbaren Gegenmaßnahmen leiten, stehen nicht zur Verfügung.
- Der Einsatz der Maßnahmen wird für solche Situationen geübt, die deutlich von der in der PSA postulierten Ereignissituation abweichen.

Als wissensbasiert einzuschätzende Operateureingriffe sind einer weiteren Selektion zu unterziehen. Zu bewerten sind nur solche Eingriffe, für die in ausreichendem Umfang Eingriffsmöglichkeiten und Eingriffsbefugnisse vorhanden sind und für die das Betriebspersonal im Grundsatz das erforderliche Wissen hat, um diese Eingriffe zu erkennen, zu planen und auszuführen.

Zur Beurteilung der Eingriffsmöglichkeiten ist zu klären, ob vorrangige automatische Einrichtungen in der gegebenen Situation die in Betracht zu ziehenden Schalthandlungen verhindern. Falls solche Automatiken wirksam sind, ist in der Folge zu prüfen, ob diese abgeschaltet bzw. die von ihnen generierten Signale zurückgesetzt werden können. Weiterhin ist zu überprüfen, ob die Eingriffsorte zugänglich und die Arbeitsbedingungen zumutbar sind. Zu klären ist auch, ob der Eingriff nicht gegen einschlägige Regeln und Vorschriften verstößt. Maßnahmen, die bei Berücksichtigung solcher Randbedingungen als ausführbar eingeschätzt werden, sind weiter zu untersuchen.

Theoretisch ist in einer Situation mit geringer Vorplantiefe eine große Zahl wissensbasierter Handlungen des Betriebspersonals denkbar. Der größte Teil davon ist aber in einer gegebenen Situation nicht wahrscheinlich. Die Modellentwicklung beschränkt sich auf wissensbasierte Handlungen des Betriebspersonals, die aus dessen Sicht sinnvoll und adäquat sind.

Wissensbasierte Handlungen, welche aus der Sicht des Betriebspersonals als sinnvoll erscheinen können, sind dadurch gekennzeichnet, dass die Handlungen und ihr Einsatzbereich dem Betriebspersonal durch Ausbildung und durch in anderen Situationen erworbene berufliche Praxis bekannt sind und dass sie sich auf Grundlage der zur Verfügung stehenden Information als situationsverbessernd darstellen.

Als Quelle wissensbasierten Handelns wird nur das professionelle Wissen des Betriebspersonals berücksichtigt. Professionelles Wissen geht auf Prozeduren, Training und berufliche Praxis zurück. Teil des Fachwissens ist auch die Kenntnis der Quellen, in denen erforderliche Informationen zu finden sind. Sonstige Wissensquellen können zwar Hinweise auf wissensbasierte Eingriffe geben, diese Quellen ordnen sich jedoch den individuellen außerberuflichen Erfahrungen und Beschäftigungen des Betriebspersonals zu, die sich einer systematischen und umfassenden Analyse entziehen und daher vereinfachend ausgeklammert werden.

Zur Erfassung des im Grundsatz vorhandenen Wissens sind schriftliche Unterlagen (u. a. Betriebshandbuch, Notfallhandbuch, Schichtbuch, Übungs- und Ausbildungspläne, Systembeschreibungen, Prüfhandbuch) und Erkenntnisse aus Beobachtungen und Befragungen während einer Anlagenbegehung bzw. Übungen auf der Anlage und/oder am Simulator. Für Beobachtungen und Interviews soll Personal des Betreibers mit folgenden Zuständigkeiten zur Verfügung stehen:

- Planung wissensbasierter Eingriffe (z. B. Festlegung erforderlicher Freischaltungen),
- Entscheidung für wissensbasierte Eingriffe,
- Ausführung wissensbasierter Eingriffe.

Liegt ausreichend gefestigtes Wissen vor, so werden die Eingriffe mit dem im Folgenden vorgestellten Kognitionsmodell weiter untersucht.

- **Kognitionsmodell**

Als kognitiv werden psychische Aktivitäten bezeichnet, die der Aneignung, der Organisation und der Nutzung von Wissen dienen /NEI 76/. In Situationen, die vom Kraftwerkspersonal wissensbasierte Eingriffe erfordern, sind die kognitiven Prozesse bei der Informationsaufnahme und Informationsverarbeitung maßgeblich, um einschätzen zu können, inwieweit das Personal mögliche, wissensbasierte Eingriffe erkennt. Die günstige bzw. ungünstige Gestaltung der diesen Prozess beeinflussenden Faktoren ist entscheidend für die Wahrscheinlichkeit, dass derartige Eingriffsmöglichkeiten identifiziert und ausgeführt werden. Es muss somit ein Modell bereitgestellt werden, das Aufbau und Arbeitsweise menschlicher Kognition in ihren wesentlichen Merkmalen darstellt und eine systematische Identifikation und Wertung der den Kognitionsprozess beeinflussenden Faktoren ermöglicht.

Das Modell soll den Anwender durch alle für die Zuverlässigkeitseinschätzung relevanten Aspekte führen und ihm erlauben, günstige und ungünstige Einflüsse im Detail herauszuarbeiten, um auf der Grundlage dieser Detailkenntnis eine qualitative und quantitative Gesamteinschätzung zur Frage vornehmen zu können, welche Eingriffe das Personal voraussichtlich für sinnvoll und situationsadäquat halten wird.

Das hier entwickelte Kognitionsmodell ging zunächst von dem in /SWA 83/ vorgestellten Ansatzes des ‘Kognitionsrades‘ aus und erweitert diesen um die Merkmale ‘Wissen‘, ‘Tendenzen zur Steuerung der kognitiven Beanspruchung‘ und ‘Problemlösungsstrategien‘. Dieses in Abb. 4-4 dargestellte Modell strukturiert die kognitiven Aktivitäten in zunächst sechs Teilbereiche:

- Wahrnehmen (Aufmerksamkeitslenkung; bemerken, dass sich etwas verändert hat),
- Unterscheiden (Abgrenzen eines Signals oder einer Gruppe von Signalen von anderen Signalen),
- Interpretieren (einem Signal oder einer Gruppe von Signalen eine Bedeutung zuordnen, z. B. Pumpe ausgefallen),

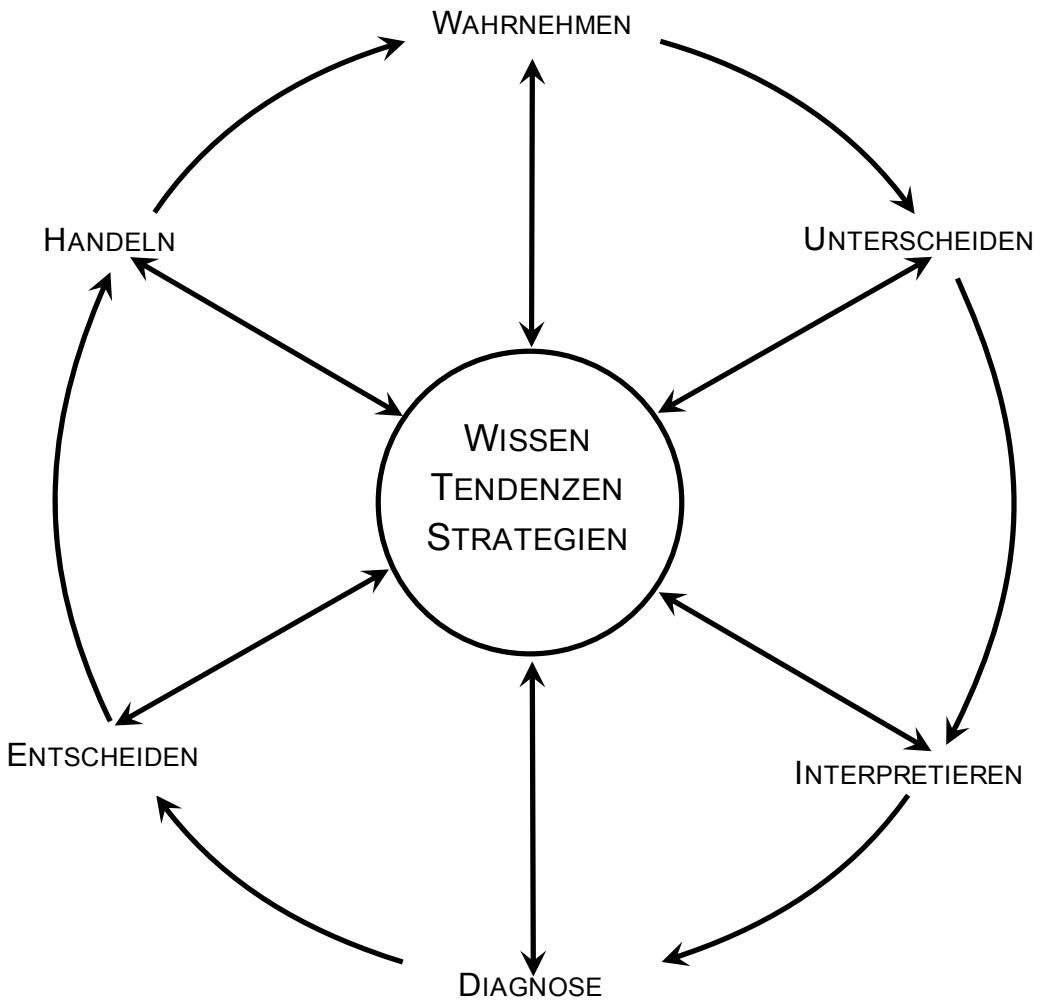


Abb. 4-4 Kognitionsmodell

- Diagnose (Ursachen bzw. Erklärungszuordnung; z. B. Pumpe ist ausgefallen, weil …, sonst keine Probleme),
- Entscheiden (zwischen mehreren möglichen Ursachen oder mehreren möglichen Handlungen),
- Handeln.

Die äußeren, gebogenen Pfeile deuten an, in welcher Reihenfolge die einzelnen kognitiven Teilbereiche durchlaufen werden, wenn man vereinfachend von Rückkopplungen absieht. Die Teilbereiche interagieren miteinander über das vorhandene Wissen, die Tendenzen zur Regulation der kognitiven Beanspruchung und die erlernten Problemlö-

sungsstrategien. Über diese Interaktionen können sowohl Abkürzungen (z. B. Wahrnehmung führt über ein hochtrainiertes Verhaltensmuster direkt zu einer Handlung) als auch interne Schleifen (z. B. Suche nach weiteren Informationen zur Generierung einer Diagnose) dargestellt werden.

Die Tendenzen zur Regulation der kognitiven Beanspruchung sind ein wichtiger Bestandteil des Kognitionsmodells ohne den der Kognitionsprozess nicht erklärt werden kann. Sie stellen wesentliche Verbindungen zwischen den Randbedingungen einer Situation und dem Denkprozess her. Sie regulieren die kognitive Beanspruchung, die unter ungünstigen Randbedingungen soweit ansteigen kann, dass es zu einer Desorganisation des Denkprozesses kommt.

Tab. 4-6 gibt einen Überblick über die in das Kognitionsmodell integrierten Tendenzen, ihre Zuordnung zu den einzelnen kognitiven Aktivitäten und die Folgen, die sich für diese Aktivitäten ergeben. Eine wesentliche Folge ist die Möglichkeit, dass der Informationsverarbeitungsprozess fehlerhaft ablaufen kann und damit das angestrebte Ergebnis, d. h. Erkennung, Planung und Ausführung eines wissensbasierten Eingriffs, nicht zustande kommt. Tab. 4-6 stellt die Begriffe und die Bezüge in vereinfachter Form dar. Eine wissenschaftliche Diskussion unter Verwendung der einschlägigen Fachbegriffe findet sich in /FAS 03/.

Das Kognitionsmodell muss auch aufzeigen welche Lösungsstrategien Experten unter welchen Randbedingen nutzen, um einen Ausgangszustand in einen Zielzustand zu überführen, und wie sie dabei ihr professionellen Wissen anwenden, um das Problem und seine Lösungsmöglichkeiten zu erkennen.

Tab. 4-6 Tendenzen bei zunehmender kognitiver Beanspruchung

Kognitive Aktivität	Tendenz	Folgen
Wahrnehmen, Unterscheiden, Interpretieren von Information	Filtern	– Bevorzugt bearbeitet wird einfach zu erwerbende oder die Erwartungen bestätigende Information. – Blockiert, zurückgestellt wird negative, als unzuverlässig empfohlene, schwer zu erwerbende, den Erwartungen widersprechende Information
	Sampling	Auswahl von Repräsentanten aus einer Gruppe zusammengehörender Informationen.
	Zeitwahrnehmung	Die Fähigkeit, die Dauer zeitabhängiger Vorgänge einzuschätzen oder zu vergleichen wird eingeschränkt.
Diagnose, Maßnahmenplanung	Regression	– Bevorzugung automatischer, reflexartiger Verhaltensweisen – Beschränkung der Mustersuche. Bevorzugt werden vertraute, vor kurzem angewendete Muster. Die Ähnlichkeit von Mustern wird auf der Grundlage von nur wenigen Informationen beurteilt. Bevorzugt werden Muster, die den Weg zum Ziel verkürzen. An einmal ausgewählten Mustern wird festgehalten. – Fixierung auf aktuelles, begrenztes Problem.
	Modellbildung	– Bekannte Muster werden verallgemeinert und auf aktuelles Problem übertragen. – Aktuelle Probleme werden verallgemeinert oder vereinfacht und danach einem passenden Muster zugeordnet.
	Prognose	– Die Fähigkeit Wahrscheinlichkeiten einzuschätzen oder zu vergleichen wird eingeschränkt. – Nicht lineares Verhalten wird linear extrapoliert. – Prognostizierte Information wird überbewertet.
	Kosten-/Nutzen-Bewertung	– Sichere oder unmittelbar eintretende Opfer werden vermieden, auch wenn die Verluste gering sind. – Entscheidungen, die hohe Verluste mit sich bringen, werden verzögert oder delegiert.
Handlungskontrolle	Reduktion der Beanspruchung	– Nachlassende Aufmerksamkeit beim Ausführen von Aufgaben – Bevorzugung von einfachen Aufgaben

Das im Vorhaben entwickelte Modell des Problemlösungsprozesses wird in /FAS 10a/ ausführlich beschrieben und hier zusammenfassend dargestellt.

- Das Personal versucht eine Problemlösung, indem es Prozeduren, Teile von Prozeduren und (oder) sonstige Handlungen, deren Kenntnis zum Fachwissen gehört, entweder einzeln oder in Kombination anwendet, um die Anlage in einen sicheren Zustand zu bringen, die Diskrepanz zu sicheren Zustand zu vermindern oder zumindest eine weitere Verschlechterung des Ist-Zustandes zu verhindern und dadurch Zeit zu gewinnen. Eine Lösung besteht also aus der technisch zulässigen, zielführenden Anwendung einzelner oder einer Kombination mehrerer bekannter Vorgehensweisen in einer Situation, für die mindestens eine dieser Vorgehensweisen weder vorgesehen noch eingeübt ist.

- Das Personal prognostiziert anhand der verfügbaren Informationen, ob es eine Lösung realisieren kann. Zu nutzen sind zum Beispiel Informationen über die verfügbare Zeit für die Ausführung erforderlicher Handlungen, die Zugänglichkeit der Handlungsorte sowie die Verfügbarkeit von Personen mit eventuell benötigten Spezialqualifikationen und spezieller Mittel. Relevant sind auch Informationen, die erforderlich sind, um eine Maßnahme aus dem dafür vorgeplanten Kontext in die konkrete Situation zu übertragen (z. B. Informationen zur Auslegungsreserve von Komponenten).

- Die Problemlösung erfolgt systematisch. Das Modell vernachlässigt die Möglichkeiten, durch blindes Raten und andere unsystematische Vorgehensweisen herauszufinden, welche wissensbasierten Eingriffe der betrachtete Ereignisablauf erfordert. Systematisches Problemlösen zeichnet sich dadurch aus, dass die Problemlöser den gegebenen Anlagenzustand, das genaue Ziel und die Möglichkeiten analysieren, das Ziel in der gegebenen Situation zu erreichen. Eventuell bilden sie Teilziele und definieren dadurch Teilprobleme, die sie auf die gleiche Weise systematisch lösen. Effektives Problemlösen erfordert es, dass die benötigten Informationen auf den Benutzungsoberflächen und in den Unterlagen (Prozeduren, System- und Komponentenbeschreibungen, Schaltpläne, usw.) verfügbar, klar, zuverlässig und leicht zugänglich sind. Informationen in Unterlagen sind deshalb wichtig, weil das Personal laut Modell die Problemlösung versucht, indem es Prozeduren, Teile von Prozeduren und (oder) sonstige Handlungen, deren Kenntnis zum Fachwissen gehört, entweder einzeln oder in Kombination anwendet.

Um ein praktikables auch durch Anwender, die keine vertieften kognitionswissenschaftlichen Kenntnisse besitzen, nutzbares Model bereitstellen, war es erforderlich, das in Abb. 4-4 dargestellte Kognitionsmodell weiter zu konkretisieren und in einen Bewertungsansatz einzubetten. In Abb. 4-5 ist dargestellt, wie die qualitative Beurteilung der Erfolgsaussichten wissensbasierter Eingriffe erfolgen soll. Vorausgesetzt wird hierbei, dass als Ergebnis der Systemanalyse und der Analgenbegehungen bzw. Beobachtungen von Übungen eine umfassende Beschreibung der zu untersuchenden Eingriffe vorliegt (vgl. auch Abb. 4-3). Die zu generierenden Inhalte eines zu bewertenden wissensbasierten Eingriffs müssen bekannt sein. Diese Inhalte werden dann im Detail mit Hilfe des Kognitionsmodells untersucht.

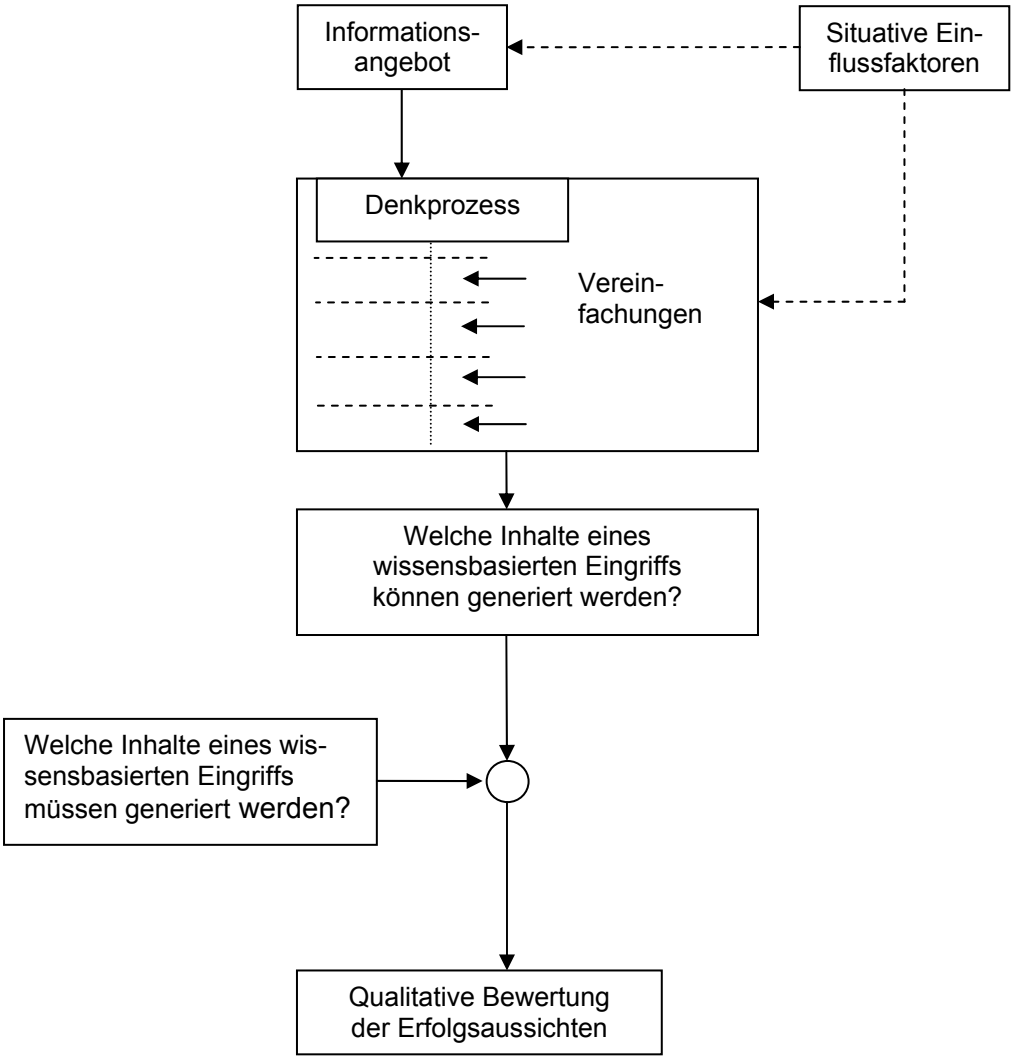


Abb. 4-5 Anwendung des Kognitionsmodells zur Beurteilung der Erfolgsaussichten

Ausgehend vom objektiv vorliegenden Informationsangebot und der Auswirkungen situativer Einflussfaktoren, die sowohl die Qualität des Informationsangebotes, als auch die Zuverlässigkeit der Informationsverarbeitung durch Auslösen kognitiver Tendenzen verändern, können sich die Aussichten, das Inhalte wissensbasierter Eingriffe generiert werden, sehr unterschiedlich darstellen.

So kann der Eingriff aus anderen Handlungssituationen gut bekannt sein und es gibt auch eine geeignete Problemlösungsstrategie. Für den Eingriff erforderliche Informationen könnten jedoch aufgrund zu unterstellender kognitiver Tendenzen ggf. nicht wahr genommen oder falsch interpretiert werden. Der konkrete Zusammenhang zwischen kognitiven Aktivitäten und den bei steigender Beanspruchung wirksamen kognitiven Tendenzen ist in Abb. 4-6 dargestellt.

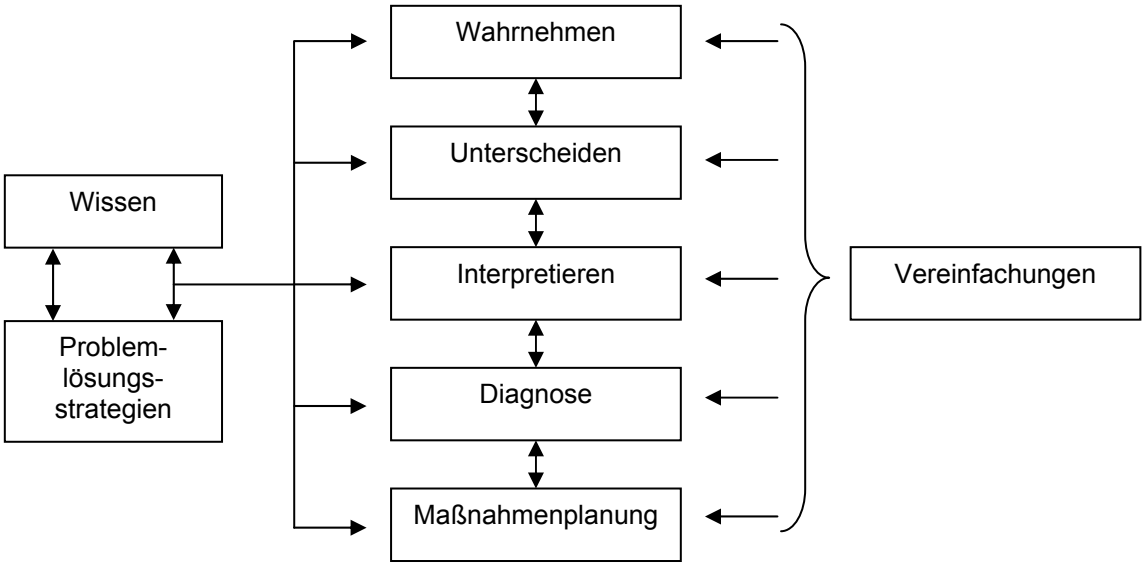


Abb. 4-6 Modellierung des Denkprozesses zur Beurteilung der Erfolgsaussichten wissensbasierter Eingriffe

Die Erfolgsaussichten einer wissensbasierten Handlung werden als gering eingeschätzt, wenn eine der folgenden Bedingungen zutrifft.

- Das Fachwissen ist nicht ausreichend.
- Erforderliche Informationen sind nicht verfügbar (Ursache: Technische Ausfälle, gravierende ergonomische Defizite, kognitive Tendenzen, die eine Verzerrung der Informationswahrnehmung erwarten lassen).

- Der Problemlösungsprozess stellt sich als insgesamt schwierig bzw. kaum durchführbar dar (z. B. mangels geeigneter Hinweise auf benötigtes Wissen oder extrem hohem Stress).

Die zu treffenden Einschätzungen sind durch Erkenntnisse abzusichern, die sich aus Beobachtungen und Befragung der handelnden Personen in der Anlage ergeben. Hierbei sollte auch der zu erwartenden Zeitbedarf für eine Problemlösung abgeschätzt werden.

Aufgrund der Erfolgsaussichten der einzelnen Inhalte eines wissensbasierten Eingriffs hat der Anwender eine qualitative Gesamteinschätzung vorzunehmen.

Tab. 4-7 zeigt, wie die zusammenfassende Wertung vorzunehmen ist. Kommentare im Anschluss an die Tabelle erläutern einige zusätzliche Aspekte.

Tab. 4-7 Stufen der zusammenfassenden qualitativen Wertung der Analyseergebnisse

Ergebnis der Analyse	Erfolgsaussichten
Mindestens eine der drei folgenden Aussagen trifft zu: – Fachwissen nicht ausreichend – Erforderliche Informationen nicht verfügbar – Problemlösungsprozess schwierig bzw. kaum durchführbar	keine
Erforderliche Informationen teilweise nicht verfügbar und kein extrem hoher Stress und Anlagenbegehung zeigt, dass Informationsdefizite behoben werden.	mäßig
Alle drei Aussagen treffen zu: – Fachwissen ausreichend – Erforderliche Informationen verfügbar – Problemlösungsprozess durchführbar	gut

Laborexperimentelle Studien zeigten, dass eine partielle Verfügbarkeit erforderlichen Wissens in der Problemsituation mit einer etwa fünfzig-prozentigen Wahrscheinlichkeit einhergeht, das anstehende Problem zu lösen /HUS 84/. Diese Ergebnisse sind die Grundlage für die Einführung einer mittleren Stufe. Die zu treffende Wertung ist verknüpft mit einer Einschätzung des Stressniveaus.

Effektives Problemlösen kann auch in lebensbedrohlichen Situationen stattfinden /REA 97/. Bis zum Vorliegen genauerer Erkenntnisse hierzu geht die Bewertung aber davon aus, dass Menschen Probleme erfolgreich lösen, wenn Stress und Beanspruchung zumindest keine extremen Ausprägungen annimmt. Aufbauend auf die qualitative Einschätzung wird folgender in Tab. 4-8 dargestellter Quantifizierungsansatz vorgeschlagen (angegeben wird der Erwartungswert der Fehlerwahrscheinlichkeit, Unsicherheitsfaktor k = 10).

Tab. 4-8 Quantitative Einschätzung der Erfolgsaussichten

Qualitative Einschätzung der Erfolgsaussichten	**Fehlerwahrscheinlichkeit**
keine	P = 1
mäßig und seit Ereignisbeginn sind mindestens 20 Minuten verstrichen	P = 0,5
gut	je nach Zeit ab Ereigniseintritt (min.) mit Verlauf entsprechend /SWA 83/, S. 12-13 zwischen den hier angegebenen Stützpunkten T ≤ 20 min P = 1 T = 30 min P = 0,1 T = 60 min P = 0,01 T ≥ 1 d P = 0,003

Die Schätzung der Fehlerwahrscheinlichkeit bei insgesamt guten Randbedingungen ist Ergebnis einer wesentlichen Erweiterung des Modells, mit dem Swain die Wahrscheinlichkeit abschätzt, ein Ereignis richtig und rechtzeitig zu diagnostizieren (vgl. /SWA 83/, Kapitel 12). Ereignis kann eine Störung, ein Störfall oder ein Notfall sein. Die Erweiterung beruht auf den nachfolgenden Überlegungen:

- Diagnostizieren bedeutet nach Swain, die wahrscheinlichste Ursache eines Ereignisses zu bestimmen, aus der man erkennen kann, welche Systeme oder Komponenten eine Zustandsänderung erfahren müssen, um die Situation zu beherrschen oder zumindest ihre nachteiligen Folgen zu mildern (siehe /SWA 83/, S. 12-6, 12-8, 12-10). Die Bestimmung der Ursachen und des zielführenden Vorgehens hängen somit auf das Engste zusammen. Allerdings berücksichtigt Swain nur solche Handlungen zur Änderung von System- und Komponentenzuständen, die Prozeduren und Training für den Zweck vorsehen, das anstehend Ereignis zu bewältigen (vgl. /SWA 83/ S. 12-8).

- Bei fehlerfreier Ausführung führt ein Problemlösungsprozess wie das Diagnostizieren zur Erkenntnis zulässiger Eingriffe. Swains Diagnosemodell war daher um die Leistung bzw. die Fehlermöglichkeit zu erweitern, dass es dem Personal gelingt bzw. nicht gelingt, zulässige Einsatzmöglichkeiten technischer Einrichtungen zu erkennen, die Prozeduren und Training nicht vorsehen, um den betrachteten Ereignisablauf zu beenden oder dazu beizutragen.

- Die Schätzung orientiert sich an der oberen Kurve des Modells zur pessimistischen Bewertung von Diagnoseaufgaben.
  Die oberste Kurve ist unter anderem zu nutzen, wenn die Bewältigung des Ereignisablaufs zwar durch eine Prozedur geregelt ist, aber nicht trainiert wird (siehe /SWA 83/, S. 12-23). Fehlendes Training der Handlung für den betrachteten Ereignisablauf ist eines der beiden Merkmale, die sicherheitstechnisch erforderliches wissensbasiertes Handeln auszeichnen. Das zweite Merkmal besteht darin, dass die Handlung keiner Prozedur angehört, die das Personal beim betrachteten Ereignisablauf auszuführen hat. Die Bewertung geht von der begründeten Annahme aus, dass die folgenden Aufgaben gleiche Anforderungen stellen:

  - Erinnerung an eine vorhandene, für den betrachteten Ereignisablauf aber nicht geübte Prozedur stellt,

  - Erkennung der Notwendigkeit, Zulässigkeit und Ausführbarkeit wissensbasierter Handlungen, die zu gut bekannten und trainierten Prozeduren oder Routineaufgaben für andere Situationen gehören.

  Problemlösen erfordert mehr Zeit als das Erinnern vorgegebener und eintrainierter Handlungen. Es fehlen Untersuchungen vor allem zum Zeitbedarf des Personals bei Ereignisabläufen mit sicherheitstechnisch erforderlichen, wissensbasierten Handlungen. Die Methodenentwicklung hat daher auf ein Bewertungsmodell zurückgegriffen, das der Zeit, die das Personal zur Diagnose nutzen kann, hohe Bedeutung zuweist.

- Die Methode wurde an fünf Fallbeispielen aus der Betriebserfahrung zu meldepflichtigen Ereignissen in deutschen Kernkraftwerken erprobt (vgl. /FAS 10a/). In diesen Ereignissen führte das Personal wissensbasierte Handlungen aus, die teilweise scheiterten (zwei Fälle), aber auch teilweise erfolgreich waren (drei Fälle). Die Ereignisberichte enthalten nur einen Teil der Informationen, die erforderlich sind, um die Methode vollständig anzuwenden. Sie

reichten jedoch aus, um die wesentlichen Gründe für Erfolg oder Misserfolg nachzuvollziehen und somit die Anwendbarkeit der Methode zumindest teilweise zu überprüfen. Grundsätzlich können alle für die Anwendung der Methode erforderlichen Informationen im Rahmen einer PSA erhoben werden.

4.2.2 Probabilistische Bewertung organisatorischer Einflüsse sowie von Einflüssen des Sicherheitsmanagements auf die Zuverlässigkeit von Personalhandlungen

Im Rahmen des Vorhabens wurde eine Methode entwickelt, die den Einfluss organisatorischer Faktoren auf die Zuverlässigkeit PSA-relevanter Personalhandlungen untersuchen und bewerten kann. Das Sicherheitsmanagement wird hierbei als Teilmenge der organisatorischen Einflussfaktoren betrachtet. Wie in Abschnitt 3.2.2 dargestellt, wurde hierzu schrittweise vorgegangen.

- Ausgehend von den Erkenntnissen aus der Grundlagenforschung war ein Organisationsmodell zu entwickeln, das den Zusammenhang zwischen Organisation und sicherheitsrelevanter Personalhandlung herstellt.
- Die Verbindung zwischen Organisationsmodell und den bisher verwendeten anerkannten Bewertungsmethoden wurde mittels eines an die spezifische Fragestellung angepasstes Arbeitssystemmodell geschlossen.
- Ein probabilistischer Bewertungsansatz war bereitzustellen, und die Vorgehensweise der gesamten Methode sollte an einem Fallbeispiel demonstriert werden.

Die folgende Darstellung der Ergebnisse orientiert sich an diesem Forschungskonzept.

- **Organisationsmodell**

Der Begriff Organisation steht für den Prozess und das auf bestimmte oder unbestimmte Dauer angelegte Ergebnis einer planmäßigen Auswahl, Zusammenführung und Nutzung von Produktionsfaktoren, um angestrebte Ziele unternehmerischer Tätigkeiten unter den gegebenen oder angenommenen Bedingungen zu verwirklichen, die das Umfeld der betrachteten unternehmerischen Tätigkeit bestimmen.

Prozess und Ergebnis des Organisierens bestehen beim Faktor Arbeit darin, für das Verhalten der Beschäftigten Prinzipien und Regeln aufzustellen, einzuführen und auf-

recht zu erhalten, mit denen menschliche Leistung in den Dienst des Unternehmens und seiner Ziele gestellt werden soll.

Abb. 4-7 stellt die wesentlichen Schritte und Ergebnisse des Organisationsprozesses dar. Im Folgenden wird ausführlicher auf die Ergebnisse des Organisierens eingegangen, die Ausgangspunkte für das Organisationsmodell sind. Das nachfolgend beschriebene Vorgehen entspricht den Erkenntnissen und Forderungen der Organisationswissenschaft (z. B. /SCH 03a/, S. 30ff, /SCH 04/, Spalte 45ff, /WIE 98/, S. 41ff).

Die Aufbauorganisation geht aus der Bestimmung und Zusammenfassung der Aufgaben hervor, mit denen eine Unternehmung die Verwirklichung ihrer Ziele anstrebt. Man spricht auch von der Analyse und Synthese von Aufgaben.

In der organisationswissenschaftlichen Aufgabenanalyse zerlegt man die Gesamtaufgabe(n) der Unternehmung sukzessive in immer spezifischere Teile oder Einzelaufgaben, die nach verschiedenen Kriterien identifiziert und gegeneinander abgegrenzt werden können.

Die Aufgabensynthese fasst die Einzelaufgaben, die sich aus der Aufgabenanalyse ergeben haben, nach verschiedenen Gesichtspunkten zusammen.

- Einzelaufgaben werden einzelnen Stellen zugeordnet und damit auf verschiedenen Stellen verteilt bzw. auf verschiedenen Stellen gebündelt, für die jeweils ein Inhaber vorgesehen ist.
- Die Stelle bildet die kleinste Einheit innerhalb der Organisation. Sie zeichnet sich durch Inhalt und Umfang der zugewiesenen Aufgaben aus, für deren Ausführung der Stelleninhaber zuständig, befugt und verantwortlich ist. Art und Anzahl der Aufgaben einer Stelle haben sich nach den Leistungsvoraussetzungen eines durchschnittlichen Stelleninhabers zu richten.

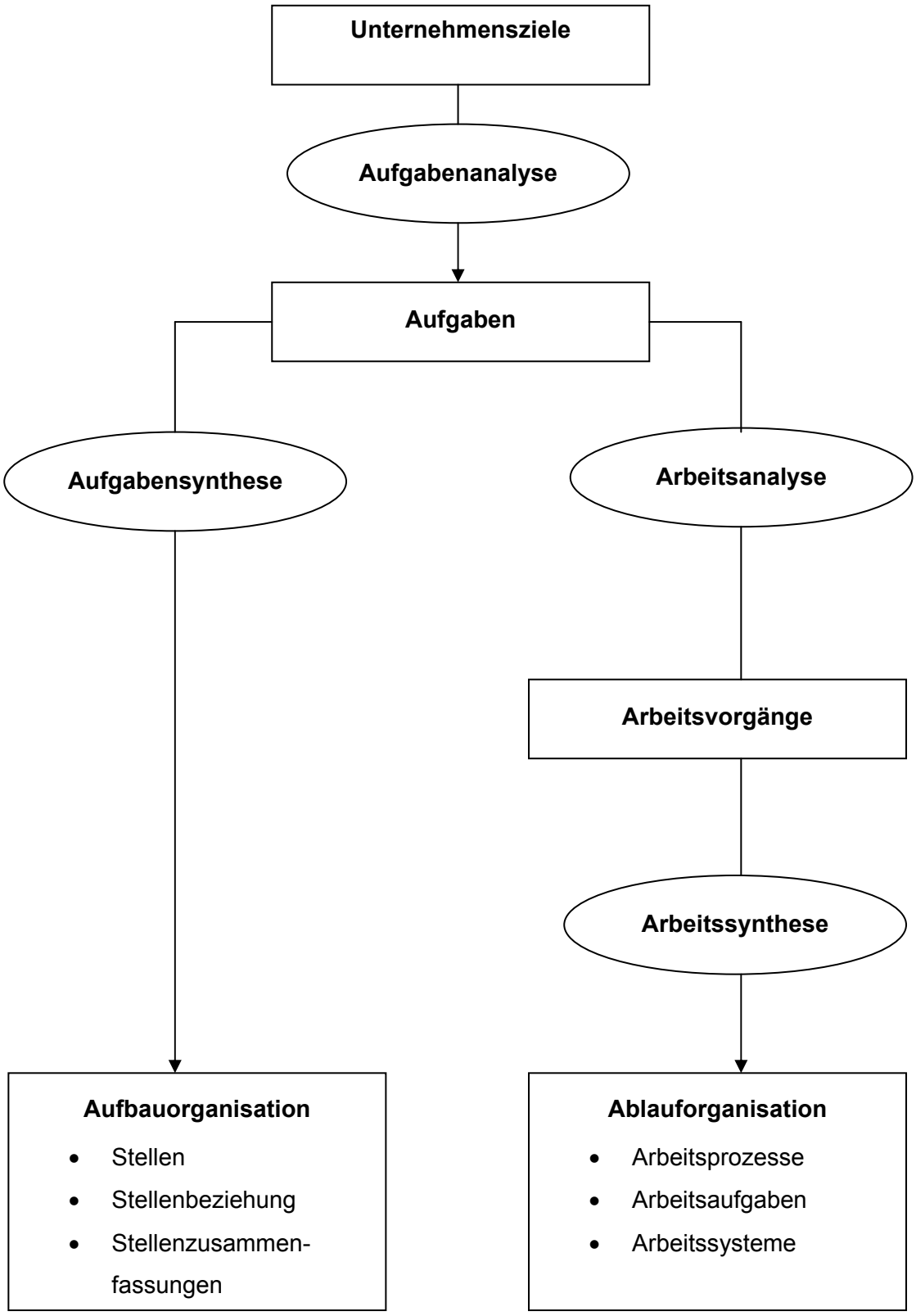


Abb. 4-7 Prozess und Ergebnis des Organisierens

- Bezieht man sich auf eine spezifische Aufgabe aus dem Aufgabenbündel einer Stelle, spricht man von der zugehörigen Stelle bzw. dem zuständigen Stelleninhaber auch als ‘Aufgabenträger‘. Für automatisierte Aufgaben oder Aufgabenteile kann der Aufgabenträger auch ein technisches System sein.

- Bei der Zusammenführung von Aufgaben nach dem Leitungszusammenhang bildet man mit den einzelnen Stellen größere Organisationseinheiten, indem man mehrere Stellen nach bestimmten Gesichtspunkten zusammenfasst und einem Leiter unterordnet. Leitungsstellen heißen auch ‘Instanzen‘. Diese Zusammenfassung lässt sich für immer umfangreichere Organisationseinheiten bis zur Führungsspitze der Unternehmung wiederholen. Leitungsstellen können Stäbe mit Beratungsaufgaben zugeordnet sein.

Die arbeitsteilige Aufgabenerfüllung erfordert es, Beziehungen zwischen Organisationseinheiten vorzusehen, um die Ausführung der Einzelaufgaben abstimmen und bewältigen zu können.

Zusammenfassend ist festzuhalten, dass die Aufbauorganisation die statischen Strukturen der Aufgabenverteilung innerhalb eines Unternehmens beschreibt. Die Verwirklichung von Unternehmenszielen hängt auch vom Zuschnitt der Aufgabenbündel, Befugnisse, Stellen und Stellenbeziehungen ab, die aus den aufbauorganisatorischen Synthesen hervorgehen, da diese organisatorischen Gegebenheiten in Bezug auf die Aufgabenerfüllung und die Beanspruchung von Stelleninhabern mehr oder weniger zweckmäßig ausgelegt sein können. Bewertungskonzept und Bewertungsmethode gehen auf diese Aspekte ein.

Die Ablauforganisation regelt, wie die Erfüllung absehbarer Aufgaben in der Unternehmung zeitlich und räumlich als Arbeitsprozess zu gestalten ist. Dabei handelt es sich um Arbeitsprozesse im Inneren der Organisation und an ihren Schnittstellen mit der Außenwelt. Im Folgenden wird der Arbeitsprozess kurz auch nur ‘Prozess‘ genannt.

Die Ablauforganisation geht wie die Aufbauorganisation von den Einzelaufgaben aus, die aus der organisationswissenschaftlichen Aufgabenanalyse resultieren. Sie unterwirft diese Aufgaben der ‘Arbeitsanalyse‘ und der ‘Arbeitssynthese‘, an deren Ende die dauerhaft festgelegten Arbeitsläufe im Unternehmen stehen. Diese Prozesse beschreiben, welche Stellen welche Aufgaben oder Teilaufgaben unter Einsatz bestimmter Mittel an festgelegten Ort und zu vorgesehenen Zeiten auszuführen haben, um Leistungen zu erbringen, die das Unternehmen zur Erfüllung seiner Ziele benötigt.

Ein Arbeitssystem besteht aus der Organisationseinheit und den Mitteln, die der Betreiber eines Kernkraftwerks für die Erfüllung einer bestimmten Aufgabe vorsieht. Zu den Mitteln gehören auch die Betriebsanweisungen und Prozeduren, die das Verhalten auf der Anlage und das Vorgehen zur Erfüllung der Aufgabe festlegen.

Vergleicht man dieses Ergebnis der Ablaufanalyse mit den Bestandteilen und der Funktion eines Arbeitssystems, so erkennt man, dass Arbeitssysteme Ergebnisse der ablauforganisatorischen Planung darstellen. Aufbauorganisatorische Regeln kommen dabei insofern zum Tragen, als Prozesse auch verschiedene Stellen aus unterschiedlichen Organisationseinheiten einbinden, die durch Kooperations- und Kommunikationsbeziehungen verknüpft sind. Ein Arbeitsprozess lässt sich somit auch durch die Art und die Leistungen der verschiedenen Arbeitssysteme darstellen, die an diesem Prozess beteiligt sind. Damit ist der Zusammenhang zwischen Arbeitssystem- und Organisationsmodell hergestellt, welcher eine wesentliche Grundlage für die Entwicklung der Bewertungsmethode bildet.

Aufbau- und Ablauforganisation bilden zwei Aspekte eines umfassenden Gestaltungsprozesses der Unternehmensorganisation mit unterschiedlichen Betrachtungsweisen und Detaillierungsgraden. Während die Aufbauorganisation Strukturen der Aufgabenteilung schafft, regelt die Ablauforganisation Prozesse der arbeitsteiligen Aufgabenerfüllung im Dienst der Unternehmensziele. Beide Aspekte lassen sich zwar gedanklich trennen, sie müssen aber stets beide berücksichtigt werden, um eine erfolgreiche Zusammenarbeit im Unternehmen zu unterstützen. Dabei kann entweder die Aufbau- oder, wie in einem prozessorientierten Ansatz, die Ablauforganisation im Vordergrund stehen.

Die Methodenentwicklung greift den Grundgedanken auf, dass

- Art, Zahl, Dauer, zeitliche Dichte und Abfolge von Arbeitsvorgängen unter Einschluss von Wege- und Beschaffungszeiten sowie
- die ergonomische Qualität der Anordnung und Ausstattung von Arbeitsplätzen und ihrer Umgebungen

mit der menschlichen Leistungsfähigkeit in Einklang zu stehen haben, um die Erfüllung von Arbeitsaufgaben wirksam zu unterstützen (vgl. /KOS 62/).

Arbeitsleistung und zuverlässige Aufgabenerfüllung hängen wesentlich auch von den Anreizen, die ein Unternehmen für die Aufgabenerfüllung vorsieht, ab. Anreize sind Ereignisse bzw. Aussichten auf solche Ereignisse, die für den Handelnden einen positiven oder negativen Wert haben und die dazu motivieren, in der gegebenen Handlungssituation erforderliche, positiv bewerte Handlungen auszuführen und negativ bewertete zu unterlassen. Regelungen zu Art und Einsatz der Anreize bilden zusammen das Anreizsystem, das die Organisation der Unternehmung vorsieht.

- **Zusammenhang zwischen Organisation und Zuverlässigkeit**

Auf der Grundlage der Ausführungen zu Prozess und Ergebnis des Organisierens lässt sich ein Organisationsmodell erstellen, mit dem der Bezug zwischen Organisation und Zuverlässigkeit von in einer PSA zu untersuchenden Handlungen hergestellt werden kann. Das Modell beruht auf folgenden Grundsätzen:

- Organisation lässt sich als Kollektiv von Stellen und Organisationseinheiten darstellen, das entsprechend den Regeln der Aufbau- und Ablauforganisation vorgegebene Aufgaben ausführt, um die Unternehmensziele zu erreichen. Das Unternehmen setzt zudem Anreize für regelkonformes Handeln im Dienst der Zielerreichung.
- Im Fokus der PSA steht das Ziel ‘Sicherheit‘.
- Das Handeln der Aufgabenträger findet in Arbeitssystemen statt.
- Die Zuverlässigkeit des Handelns hängt von leistungsbestimmenden Faktoren ab. Dazu gehören die Faktoren der ergonomischen Gestaltung des Arbeitssystems und die Qualifikation des Handelnden. Unter den gegebenen leistungsbestimmenden Faktoren kann der Handelnde je nach Qualifikation unter- oder überfordert sein und damit mehr oder weniger optimal beansprucht werden. Leistung und Zuverlässigkeit sind am höchsten, wenn die Beanspruchung in einem mittleren, optimalen Bereich liegt.
- Der Betreiber legt mit der Organisation auch die leistungsbestimmenden Faktoren und folglich auch die Beanspruchung fest, unter der das Personal handeln wird, wenn es seine Aufgaben so erfüllt, wie sie festgelegt sind.
- Die ergonomische Auslegung der Rahmenbedingungen zuverlässigen Handelns in der Warte oder vor Ort ist eine organisatorische Aufgabe, die Mitarbeiter der Anlage zu erfüllen haben. Sie sind zum Beispiel für die Planung einer Instandhaltungs-

aufgabe zuständig. Sie legen u. a. durch den Detaillierungsgrad der Unterlagen, Vorgabe von Zeitbudgets für die Aufgabenerfüllung, Schulungsbedarf an Fremdpersonal, Zahl der Personen für die Aufgabe usw. wesentliche leistungsbestimmende Faktoren fest, die sich nachhaltig auf die Zuverlässigkeit der Aufgabenerfüllung auswirken können.

- Die Erfüllung dieser organisierenden Aufgabe findet selbst in einem Arbeitssystem mit bestimmten leistungsbestimmenden Faktoren statt. An der ergonomischen Auslegung der leistungsbestimmenden Faktoren einer sicherheitstechnisch wichtigen Handlung können mehrere Organisatoren mitwirken, deren Handeln von den Bedingungen in den Arbeitssystemen abhängen, in denen sie ihre organisatorischen Aufgaben erfüllen.
- Auch für die Arbeitssysteme der Organisatoren gilt, dass sie einmal festgelegt worden sind. Der Betreiber hat zum Beispiel entschieden, wie viele Mitarbeiter für die Vorbereitung von Instandhaltungsaufgaben zum Eigenpersonal gehören, welche Arbeitsmittel sie haben usw.

Das Grundkonzept für die probabilistische Bewertung organisatorischer Einflüsse ergibt sich aus der Überlegung, dass sich Personenhandlungen in organisatorisch vorgelagerten Arbeitssystemen (siehe auch Abb. 4-9, Arbeitssystem 4 bis 8) durch die Qualität ihrer Arbeitsergebnisse auf organisatorisch nachgeordnete Arbeitssysteme (vgl. Abb. 4-9, Arbeitssystem 1 bis 3) auswirken und dies einen relevanten Beitrag zum Ergebnis einer probabilistischen Sicherheitsanalyse liefern könnte.

- **Arbeitssystemmodell**

Im Arbeitssystem wirken auf den Ausführenden Faktoren ein, die seine Leistung bei der Erledigung seiner Aufgaben beeinflussen können (z. B. verfügbare Zeit, Gestaltung der Mensch-Maschine-Schnittstelle, Zustand und Eignung von Arbeitsmitteln). Der Planungsaspekt eines solchen leistungsbeeinflussenden Faktors (kurz PSF für ‘performance shaping factor‘) des Arbeitssystems wird als ‘organisatorischer Einflussfaktor‘ definiert.

Das in diesem Vorhaben verwendete Modell eines Arbeitssystems (Abb. 4-8) ist aus arbeitswissenschaftlichen Grundlagen abgeleitet und wurde bereits in anderen Vorhaben verwendet /HAR 09/.

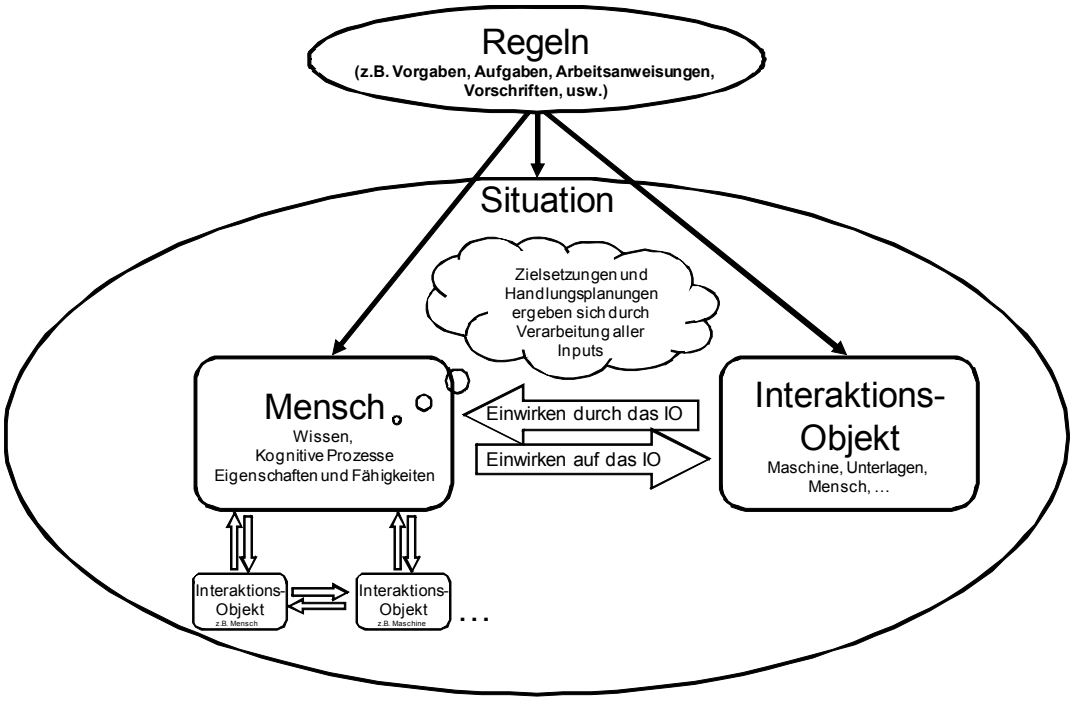


Abb. 4-8 Modell des Arbeitssystems

Ein Arbeitssystem wird immer aus einem Menschen und einem Interaktionsobjekt gebildet. Das Interaktionsobjekt kann dabei ein Mensch, eine Maschine, ein Werkzeug oder jedes andere Objekt sein, mit dem oder an dem Handlungen ausgeführt werden. Der Mensch leitet aus den anwendbaren Regelungen, der Situation und dem Zustand des Interaktionsobjektes auf Basis seines Wissens Aufgaben ab, die er mit oder an dem Interaktionsobjekt über die Schnittstelle zwischen Mensch und Interaktionsobjekt ausführen soll. Diese Schnittstelle kann z. B. ein Bedienelement, eine Anzeige oder, im Falle eines Menschen, sprachliche Kommunikation sein. Das gesamte Arbeitssystem ist in die jeweilige Situation eingebettet, welche Einflüsse auf die einzelnen Elemente des Systems haben kann. Der Mensch und das Interaktionsobjekt können ihrerseits wieder mit anderen Interaktionsobjekten interagieren. Das Modell des Arbeitssystems beschreibt somit die wesentlichen Merkmale und Wirkungszusammenhänge die zum Verständnis der Vorgänge bei der Ausführung einer Handlung, der Wirkung leistungsbeeinflussender Faktoren und des Auftretens von Fehlern erforderlich sind. In /HOY 74/ wird ein Arbeitssystem durch die Aufgabe, die handelnde Person, die Arbeitsmittel, den Arbeitsort und die leistungsbeeinflussenden Faktoren definiert. Abb. 4-8 stellt einen demgegenüber weiterentwickelten, insbesondere im Bereich der Aufgabenstellungen differenzierteren Modellansatz dar, den die GRS bereits bei der Auswertung von Betriebserfahrungen erfolgreich einsetzt /GRS 02/.

Die Literaturrecherche (vgl. /FAS 10/) zu bereits bestehenden Methoden zur Integration von organisatorischen Faktoren zeigte, dass die dargestellten Methoden aufgrund ihrer Gestaltung nicht geeignet sind, um in transparenter Weise eine Beziehung zwischen in der Organisation entstehenden Einflussfaktoren und Zuverlässigkeit von Personenhandlung bzw. Zuverlässigkeit von Komponenten herzustellen. Diese sind somit auch nicht zielführend für die Bewertung organisatorischer Einflussfaktoren, deren Quantifizierung in der PSA und der Ableitung von entsprechenden Abhilfemaßnahmen, da hierbei die Herstellung des konkreten Bezugs zwischen Organisation und sicherheitsrelevanter Tätigkeit von grundlegender Bedeutung ist.

Das in diesem Vorhaben entwickelte Grundkonzept für die probabilistische Bewertung organisatorischer Einflüsse basiert auf der Überlegung, dass sich Personenhandlungen in organisatorisch vorgelagerten Arbeitssystemen durch die Qualität ihrer Arbeitsergebnisse auf organisatorisch nachgeordnete Arbeitssysteme konkret auswirken und dies einen relevanten Beitrag zum Ergebnis einer probabilistischen Sicherheitsanalyse liefern könnte. Fehlerhafte oder fehlende Planung kann alle Bestandteile eines Arbeitssystems betreffen. So können für eine durchzuführende Aufgabe durch ein organisatorisch vorgelagertes Arbeitssystem z. B. ungeeignete Arbeitsmittel beschafft oder bereitgestellt werden. Dies wirkt sich direkt auf die Leistung im organisatorisch nachgeordneten Arbeitssystem aus. Ein Beitrag wird insbesondere bei Arbeitssystemen erwartet, deren Arbeitsergebnisse auf mehrere, organisatorisch nachgeordnete Arbeitssysteme wirken können. Dies ist beispielsweise der Fall, wenn eine fehlerhaft erstellte Prozedur in mehreren Redundanzen angewendet wird.

Ziel des entwickelten Verfahrens ist es deshalb, die relevanten Beziehungen zwischen den am Ereignisablauf beteiligten Arbeitssystemen und den organisatorisch vorgelagerten Arbeitssystemen zu identifizieren, zu modellieren, hinsichtlich relevanter Fehlermechanismen zu analysieren und an das PSA-Modell anzukoppeln.

Hierfür wird ein Modell der Organisation der zu modellierenden Tätigkeiten erstellt. Dabei wird folgende grundlegende Vorgehensweise verfolgt:

- Aufgliederung der Tätigkeiten in eine zeitliche Abfolge von Handlungen, die jeweils durch ein Arbeitssystem repräsentiert werden,
- Identifizieren möglicher, sicherheitsrelevanter Fehlhandlungen in den Arbeitssystemen,

- Identifizieren der leistungsbeeinflussenden Faktoren für die möglichen sicherheitsrelevanten Fehler. Dabei ist gegebenenfalls auch zu überlegen, in welcher Form Anreize berücksichtigt werden sollen.
- Identifizieren der Arbeitssysteme, die entsprechend vorgegebener organisatorischer Regeln leistungsbeeinflussende Faktoren festlegen oder dazu beitragen,
- Iteratives Fortsetzen dieses Prozesses für die neu identifizierten Arbeitssysteme.

Dies führt zu einem sich immer weiter verzweigenden Modell der Organisation der Arbeitsabläufe im Kraftwerk (vgl. Abb. 4-9).

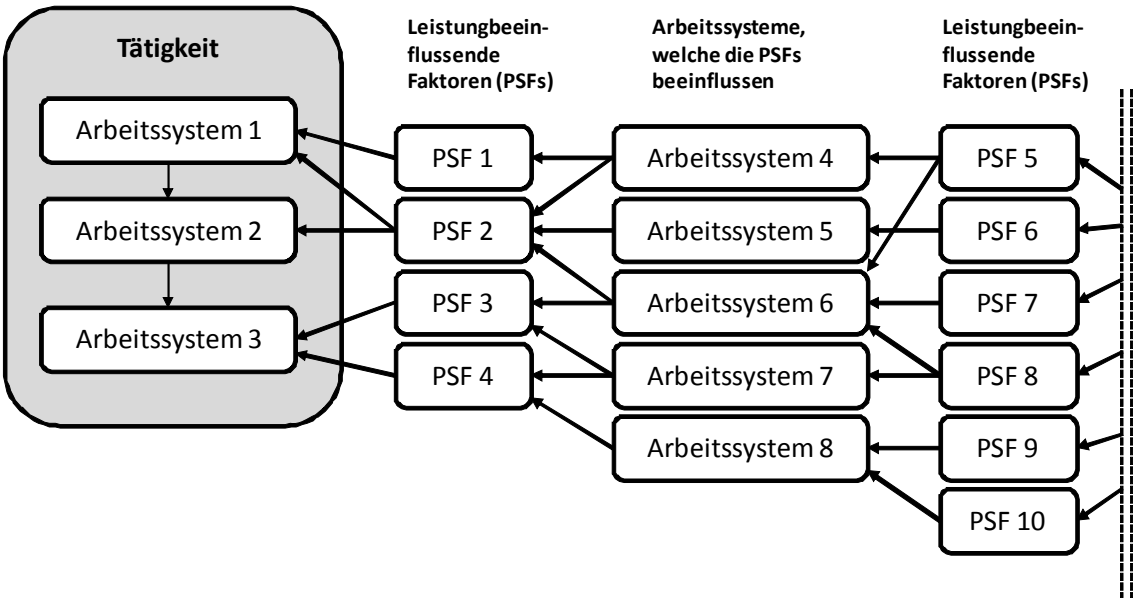


Abb. 4-9 Prinzip der Modellierung der organisatorischen Beziehungen

In Abb. 4-9 ist die Analyse nur einer organisatorisch vorgelagerten Ebene von Arbeitssystemen dargestellt. Der Prozess ist iterativ auch für die weiteren vorgelagerten Ebenen fortzuführen. Die Darstellung verdeutlicht, dass durch die iterative Einbeziehung immer weiterer Arbeitssysteme ein stark anwachsender Analyseaufwand zu erwarten ist. Deshalb wurden Maßnahmen entwickelt durch Aussortieren von irrelevanten Pfaden den Analyseaufwand zu begrenzen.

Als erste grundlegende Maßnahme diesbezüglich werden, wie bereits beschrieben, nur solche Pfade betrachtet, die zu einem für die Systemzuverlässigkeit relevanten Fehler bei der Ausführung der Tätigkeit führen können. Ein weiteres Selektionskriterium für die zu betrachtenden Pfade ist die Relevanz des jeweiligen leistungsbeeinflussenden

Faktors für den identifizierten sicherheitsrelevanten Fehler. Weiterhin können selbstmeldende Fehler und Fehler, für die ausreichende Fehlerauffangbarrieren existieren, vernachlässigt werden. Zeigen sich zudem während der Analyse Fehler mit einem hohen Beitrag zur Gesamtfehlerwahrscheinlichkeit können andere Fehler demgegenüber gegebenenfalls vernachlässigt werden. Des Weiteren können Fehlerpfade vernachlässigt werden, für die unabhängige Mehrfachfehler vorausgesetzt werden müssen, um wirksam zu werden. Die Vernachlässigung einzelner Pfade soll stets aufgrund probabilistischer Betrachtungen begründet werden.

Nach dem Abschluss der iterativen Betrachtung der Arbeitssysteme ist im nächsten Schritt zu überprüfen, ob die gefundenen Fehlermechanismen in weiteren Arbeitssystemen wirksam sind. Damit lässt sich insbesondere der Aspekt der Breitenwirkung organisatorischer Faktoren berücksichtigen, Hierfür wird untersucht, ob Elemente der Arbeitssysteme gleich sind (z. B. gleiche Person, gleiche bzw. ähnliche Prozedur, gleiches oder ähnliches technisches System). Oft ist dies z. B. der Fall bei den verschiedenen Redundanzen technischer Systeme. Zudem ist zu untersuchen, welche Bedeutung die Fehlerentdeckungsmöglichkeiten in einem Arbeitssystem für die Entdeckung des gleichen Fehlermechanismus in anderen Arbeitssystemen hat.

Durch die Komponentendaten, Betrachtungen zu gemeinsam verursachten Ausfällen (GVA) sowie die Abhängigkeitsanalysen bei der Analyse der menschlichen Zuverlässigkeit werden unter Umständen bereits dieselben Zusammenhänge berücksichtigt wie bei der Modellierung der organisatorischen Einflüsse. Es ist deshalb im Rahmen des entwickelten Verfahrens ein Abgleich zwischen den verschiedenen Quellen für die PSA-Eingangsdaten durchzuführen, um eine Doppelbewertung zu vermeiden. Die probabilistische Modellierung der organisatorischen Einflüsse erfolgt im Prinzip durch das Einbringen neuer Basisereignisse in den Fehlerbaum.

- **Probabilistische Bewertung**

Grundlage der probabilistischen Bewertung ist die in Abb. 4-9 dargestellte Modellierung organisatorischer Beziehungen. Die Fehlerwahrscheinlichkeit einer darin durch ein Arbeitssystem beschriebenen Handlung ergibt sich aus einer Basiswahrscheinlichkeit (Zuverlässigkeitsgrenze für den betrachteten Handlungstyp unter optimalen Bedingungen P_N) und der Wirkung der im Arbeitssystem vorhandenen leistungsbeeinflussenden Faktoren (PSF).

$$P = f(P_N, PSF_1 \ldots PSF_i)$$

Organisatorische Vorgänge sind in diesem Modell als Einflussfaktoren aufzufassen, die die Zuverlässigkeit einer Handlung mitbestimmen (z. B. Regeln zur Aufgabenstellung eines Handlungsausführenden). Ausgehend von diesen Überlegungen kann die probabilistische Bewertung in die nachfolgend aufgeführten sechs Schritte gegliedert werden:

1. Basisanalyse
   Die in der PSA modellierten Handlungen werden zunächst mit den empfohlenen Methoden /FAK 05/ ausgehend vom aktuellen Zustand der leistungsbeeinflussenden Faktoren (PSF) bewertet.

2. Einschätzung der Variabilität leistungsbeeinflussender Faktoren
   Kann sich die Qualität eines PSF ändern (z. B. Arbeitsunterlagen sind neu zu erstellen oder müssen gelegentlich modifiziert werden) so ist die Häufigkeit dieser Änderung zu schätzen. Kann diese nicht ermittelt werden, so ist pessimistisch davon auszugehen, dass eine Änderung im Beobachtungszeitraum mit der Wahrscheinlichkeit P=1 eintritt.

3. Bewertung von Arbeitssystemen innerhalb der Organisation
   Über das Organisationsmodell sind die für die Qualität eines PSF zuständigen, vorgelagerten Arbeitssysteme zu bestimmen. Fehlhandlungen der zuständigen Aufgabenträger sind zu identifizieren und zu quantifizieren.

4. Die Zuverlässigkeit von Vorkehrungen (Barrieren) zur Fehlererkennung und Behebung ist zu ermitteln.

5. Abhängigkeiten zwischen zueinander redundanten Handlungen (d. h. mehr als ein Handlungsfehler muss auftreten, damit das postulierte unerwünschte Ereignis eintritt) und ihre ungünstigen Wirkungen auf die Gesamtfehlerwahrscheinlichkeit sind einzuschätzen.

6. Fehler von Arbeitssystemen innerhalb der Organisation sind in der PSA durch Basisereignisse darzustellen und in die Ergebnisse der Basisanalyse (vgl. Schritt 1) zu integrieren.

Eine Überprüfung, ob die Datenquelle ‘Betriebserfahrung zu meldepflichtigen Ereignissen in deutschen Kernkraftwerken‘ für die Quantifizierungsschritte 3, 4 und 5 herangezogen werden kann, führte zu keinem tragfähigen Ergebnis. Fehlhandlungen von

Aufgabenträgern in der Organisation stehen in der Regel nicht im Fokus der Ereignisberichte, so dass die Zahl der bewertbaren Stichproben zu gering ist, um daraus Daten für das Forschungsvorhaben zu gewinnen (vgl. auch /PRE 10/). Hier wird daher ein Quantifizierungsansatz vorgeschlagen, der sich auf Bewertungselemente der anerkannten Bewertungsmethoden ASEP /SWA 87/ und THERP /SWA 83/ stützt und besser abgesichert ist als der in /FAS 03/ dargestellte Weg zur Schätzung von Zuverlässigkeitsdaten. Ziel des gewählten Ansatzes ist es,

- den Analyseaufwand durch Vereinfachungen zu reduzieren,
- den durch Vereinfachungen bedingten Verlust an Genauigkeit durch pessimistische Basisdaten zu kompensieren,
- obere Abschätzungen für den Beitrag organisatorischer Einflüsse zu erhalten sowie
- sicherheitsrelevante Zusammenhänge mit probabilistischen Methoden herauszuarbeiten.

In den Bewertungsschritten 3,4 und 5 sind quantitative Einschätzungen vorzunehmen. Im Folgenden werden die Kernpunkte des dafür erforderlichen Quantifizierungsansatzes vorgestellt.

- Bewertungsschritt 3, Arbeitssysteme innerhalb der Organisation
  Als Basiswahrscheinlichkeit für einen Handlungsfehler eines Aufgabenträgers im Organisationsmodell ist ein Wert von $P_{50} = 3 \cdot 10^{-2}$ / K = 5 anzusetzen. Dieser Wert wird in /SWA 87/, (Screening Ansatz, Abschnitt 5) als pessimistische Abschätzung für Wahrscheinlichkeit, dass ein Handlungsfehler (Auslassungs- oder Ausführungsfehler) auftritt, vorgeschlagen. Er ist abhängig von der Qualität der Randbedingungen, unter denen die Tätigkeit auszuführen ist (inklusive organisatorischer Regeln), entsprechend drei einzuschätzender Stufen zu modifizieren:
  - bewertungsrelevante PSF teilweise ungünstig gestaltet, Modifikationsfaktor x2
  - bewertungsrelevante PSF überwiegend ungünstig, Faktor x10
  - mindestens ein bewertungsrelevanter PSF sehr fehlerfördernd gestaltet, Übergang zu Fehlerwahrscheinlichkeit P = 1

Die hier vorgeschlagenen Modifikationsfaktoren orientieren sich an in /SWA 83, SWA 87/ genannten Daten zum Einfluss ungünstiger Randbedingungen auf die Zuverlässigkeit von Personalhandlungen. Die für den Quantifizierungsansatz getroffenen Einschätzungen passen auch gut zu den in /IRS 07/ vorgeschlagenen Zuverlässigkeitskenngrößen, die auf Erkenntnissen aus Simulatorversuchen in Frankreich beruhen.

Bewertungsschritt 4, Barrieren:
Jede Fehlerbarriere ist mit Aufgabenträgern innerhalb der Organisation verknüpft, die Fehler erkennen und korrigieren sollen. Damit ist Bewertungsschritt 3 zur Bewertung einer Barriere immer anwendbar. Zur Reduktion des Analyseaufwandes, kann alternativ auch das in Tab. 4-9 dargestellte Bewertungskonzept eingesetzt werden, das in /SWA 87/ vorgeschlagen wird. Vorausgesetzt wird, dass eine Barriere prinzipiell in der Lage ist den unterstellten Fehler aufzufangen. In Tab. 4-9 sind beispielhaft Fehlerwahrscheinlichkeiten für Barrieren im Rahmen dieses vereinfachten Bewertungskonzeptes dargestellt.

Tab. 4-9 Fehlerwahrscheinlichkeiten für Barrieren

Barriere	**Fehlerwahrscheinlichkeit/ Unsicherheitsfaktor**
Funktionsprüfung nach Instandhaltungsvorgang	$P_{50} = 1 \cdot 10^{-2}$ / K = 3
Schichtübergabe (mit Checkliste, keine besondere Aufmerksamkeitslenkung auf Fehler)	P_{50} = 0,1 / K = 5
Überprüfung durch Ausführenden (mit Unterlage, zeitlich, räumliche Distanz vorausgesetzt)	P_{50} = 0,1 / K = 5
Überprüfung durch 2. Person (mit Unterlage)	P_{50} = 0,1 / K = 5
Erkennung über Alarm	vgl. /SWA 83/, Tab. 20-23

- Bewertungsschritt 5, Abhängigkeiten:
  Abhängigkeiten sind einzuschätzen, wenn die Gesamtfehlerwahrscheinlichkeit zueinander redundanter Handlungen zu ermitteln ist. Abhängigkeiten können vorliegen, wenn Elemente der zugehörigen Arbeitssysteme gleich oder ähnlich sind (z. B. Aufgabenstellung, Person oder PSFs, auch organisatorische PSFs). Zur

Einschätzung und Quantifizierung von Abhängigkeiten kann das in /SWA 83/, Kapitel 10 vorgeschlagene Modell verwendet werden.

In /FAS 10/ wurde der gesamte Modellierungs- und Bewertungsansatz auf ein Beispiel aus der Betriebserfahrung angewendet. Dort wurden durch ungünstige organisatorische Einflüsse und dadurch verursachte Fehlhandlungen Komponenten des Sicherheitssystems geschädigt. Die Komponenten sind auch in einer der GRS vorliegenden PSA-Studie modelliert, sodass das Fallbeispiel sowohl einen Bezug zur Betriebserfahrung als auch einen Bezug zur PSA hat. Das Beispiel zeigt, dass die im Forschungsvorhaben entwickelte Methode die relevanten Zusammenhänge modelliert und die probabilistische Relevanz abschätzt. Der dem Fallbeispiel zugrundeliegende Fehler ‘Falsche Vorgabe von Schraubenanzugsmomenten‘ kann potentiell auch zur Schädigung von Komponenten führen, die andere sicherheitsrelevante Aufgaben erfüllen. Solche Zusammenhänge werden in dieser PSA noch nicht systematisch untersucht.

4.3 Auslösende Ereignisse und Einwirkungen von innen und außen

4.3.1 Methoden zur Ermittlung von Leck- und Bruchhäufigkeiten druckführender Komponenten

4.3.1.1 Ergebnisse zur Schnittstellenentwicklung und -erprobung

Bei der Erprobung der probabilistischen Analysemethodik zur Bestimmung von Leck- und Bruchwahrscheinlichkeiten ergab sich, dass die bisher mit großen Kenntnisunsicherheiten getroffenen Annahmen zur Rissverteilung wesentlichen Einfluss auf die Berechnungsergebnisse haben.

Mit Hilfe geeigneter Abfragen lassen sich aus den in der GRS verfügbaren Datenbanken KomPass und OPDE Ereignisse mit Oberflächenrissen ausgeben. Die Abfrage der KomPass-Datenbank ergab in deutschen Anlagen mit Druckwasserreaktoren 34 Fälle, von denen sich ohne weitergehende Nachforschungen acht verwenden ließen, um Werte für die Verhältnisse Risstiefe zu Wanddicke (a/t) und Risstiefe zu halber Risslänge (a/c) zu bestimmen. Aus den acht Fällen ergaben sich ein mittlerer a/t-Wert von 0,42 mit einer Standardabweichung von 0,15 und ein mittlerer a/c-Wert von 0,43 mit einer Standardabweichung von 0,31.

Im nächsten Schritt wurde zur Erweiterung der statistischen Basis die OPDE-Datenbank herangezogen. Die Abfrage bei der OPDE beschränkte sich zunächst auf die amerikanischen und schwedischen Einträge, weil diese nach bisherigen Erkenntnissen repräsentativ sind. Dabei wurden über 700 Ereignisse ausgewiesen. Von diesen konnten 94 zur Ermittlung von a/t-Werten und 57 zur Ableitung von a/c-Resultaten verwendet werden. An die gewonnenen Ergebnisse können Verteilungsfunktionen angepasst werden, wie beispielhaft in Abb. 4-10 für die a/t-Daten aus den verwendbaren KomPass- und OPDE-Einträgen dargestellt. Daraus ergibt sich z. B. für den Rohrleitungsbereich DN 50 beispielsweise für das des Volumenregelsystem (t = 6,3 mm) als Maximalwert der Risstiefenverteilung (Dichtefunktion) ein Wert von etwa 1,4 mm.

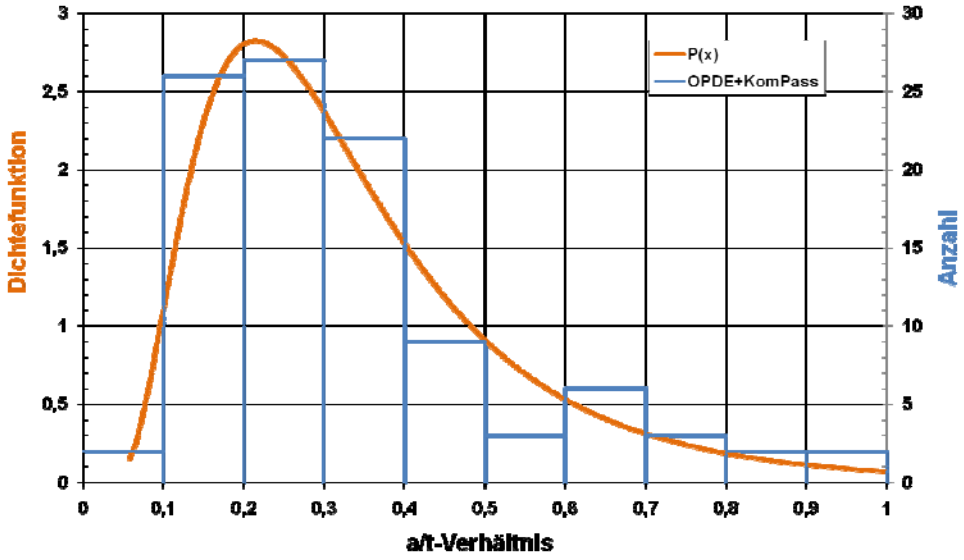


Abb. 4-10 Anpassung einer Lognormalverteilung an die a/t-Werte aus KomPass und OPDE

Mit den ermittelten Verteilungen für a/t und a/c wurden Berechnungen mit dem Strukturzuverlässigkeitsprogramm der GRS PROST zum Anwendungsbeispiel thermomechanische Ermüdungsbelastung im TA-System eines DWR durchgeführt. Dabei wird basierend auf Ansätzen aus der Literatur eine abgeschätzte Wahrscheinlichkeit für das Auftreten eines Risses an der betrachteten Stelle berücksichtigt. Abb. 4-11 zeigt die zeitliche Entwicklung der berechneten Bruchhäufigkeit.

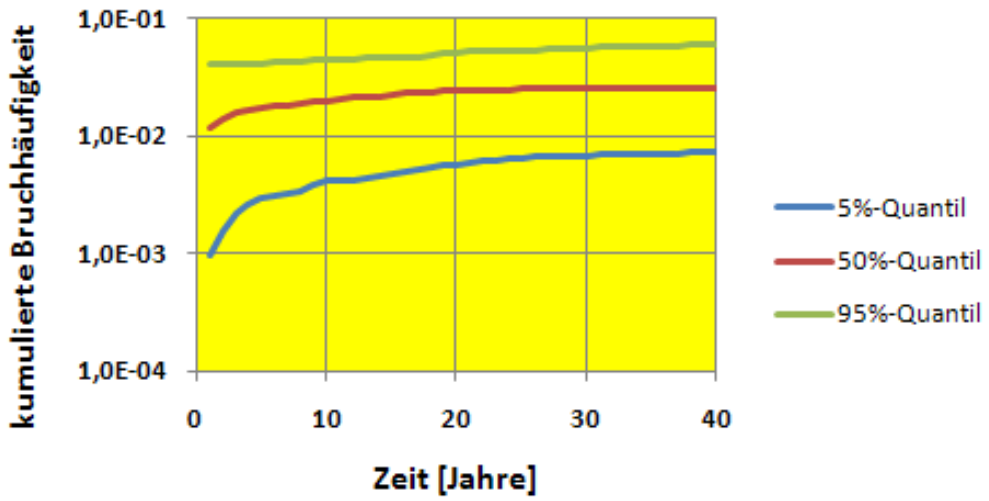


Abb. 4-11 Bruchhäufigkeit in Abhängigkeit von der Betriebszeit, PROST-Berechnung zu Anwendungsfall thermomechanische Ermüdungsbelastung im TA-System eines DWR

Die mit PROST ermittelten Leck- bzw. Bruchwahrscheinlichkeiten für das Anwendungsbeispiel liegen jeweils über den Ergebnissen aus der statistischen Auswertung. Dies deutet daraufhin, dass die untersuchte Stelle bei der realistischen Nachbildung der Belastung in PROST höher beansprucht wird als im Mittel bei den mit der statistischen Methode betrachteten Fällen. Weitere PROST-Berechnungen für andere Positionen der Rohrleitung mit anderen Lastannahmen würden dann auch Hinweise zur Aussagegenauigkeit der angesetzten Risswahrscheinlichkeit ermöglichen.

Aus der Betriebserfahrung abgeleitete Rissverteilungen, die Eingabeparameter für die Strukturzuverlässigkeitsmodelle zur Bestimmung von Leck- und Bruchwahrscheinlichkeiten in druckführenden Komponenten sind, bilden die Schnittstelle zu der statistischen Methodik.

4.3.1.2 Ergebnisse zur Entwicklung von Strukturzuverlässigkeitsmodellen für Behälter

Im Rahmen des Vorhabens RS1163 wurde PROST bezüglich Berücksichtigung des Schädigungsmechanismus Spannungsrisskorrosion für austenitische und ferritische Stähle erweitert. Dabei wurden vier Modelle implementiert, wobei im Rahmen der hier durchgeführten Analysen zum Speisewasserbehälter zwei Modelle eingesetzt wurden. Im Modell 1 kann eine konstante Risswachstumsgeschwindigkeit berücksichtigt wer-

den, wobei der Wert normal verteilt sein kann. Im Modell 2 können Geschwindigkeiten abhängig von der Rissbeanspruchung in Form des Spannungsintensitätsfaktors K_I berücksichtigt werden mit dem funktionellen Zusammenhang:

$$\frac{da}{dt} = A \cdot K_I^{\ m}$$

Dabei ist K_I in MPa · $m^{1/2}$ einzusetzen und da/dt ergibt sich in mm/s.

Bei den Berechnungen der GRS mit PROST für einen Speisewasserbehälter mit Rissbefunden infolge Spannungsrisskorrosion wurden die Korrosionsmodelle bezüglich der Risswachstumsgeschwindigkeit den Befunden angepasst. Es ergab sich bei Annahme einer konstanten Rissgeschwindigkeit (Modell 1 und 1*) von etwa $3{,}1 \cdot 10^{-7}$ mm/s nach etwa drei Jahren eine nahezu hundertprozentige Leckwahrscheinlichkeit (Abb. 4-12). Die Unterschiede zwischen Modell 1 und 1* sind Annahmen bezüglich der Initiierungsrisstiefe (normalverteilt mit Mittelwert 1 mm oder konstant 1 mm), die hier jedoch nicht relevant sind. Dagegen ist die Berechnung mit dem angepassten Modell 2 nicht zufriedenstellend, weil bei kleinen Risstiefen und damit kleinen K-Werten zu kleine Rissgeschwindigkeiten auftreten, die nicht die Befunde reproduzieren können. Eine verbesserte Anpassung des Korrosionsmodells müsste auf Basis von entsprechenden Laboruntersuchungen mit dem Werkstoff unter Mediumeinfluss durchgeführt werden.

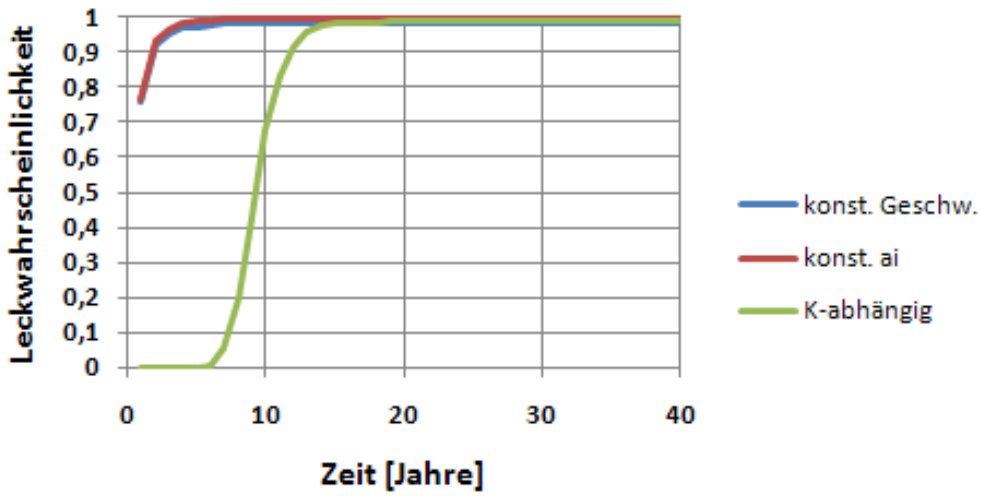


Abb. 4-12 Berechnete Leckwahrscheinlichkeiten für das Beispiel Speisewasserbehälter

4.3.1.3 Ergebnisse zur Entwicklung von Ansätzen zur Berücksichtigung verschiedener Einflüsse

Die Auswertung der deutschen Betriebserfahrung zur Entwicklung von Ansätzen zur Berücksichtigung verschiedener Einflüsse ergab folgende Resultate:

Die schon in vorangegangenen Untersuchungen festgestellte Nennweitenabhängigkeit von Leckereignissen an sicherheitstechnisch bedeutsamen Rohrleitungen in deutschen Anlagen mit Druck- und Siedewasserreaktor wurde bestätigt, d. h. von Leckereignissen waren vor allem Rohrleitungen mit kleineren Durchmessern betroffen. Abb. 4-13 zeigt dieses Ergebnis für Rohrleitungen der Nuklearen Wärmeerzeugung (J-System) und der Hilfssysteme (K-System) deutscher Druck- und Siedewasserreaktoren.

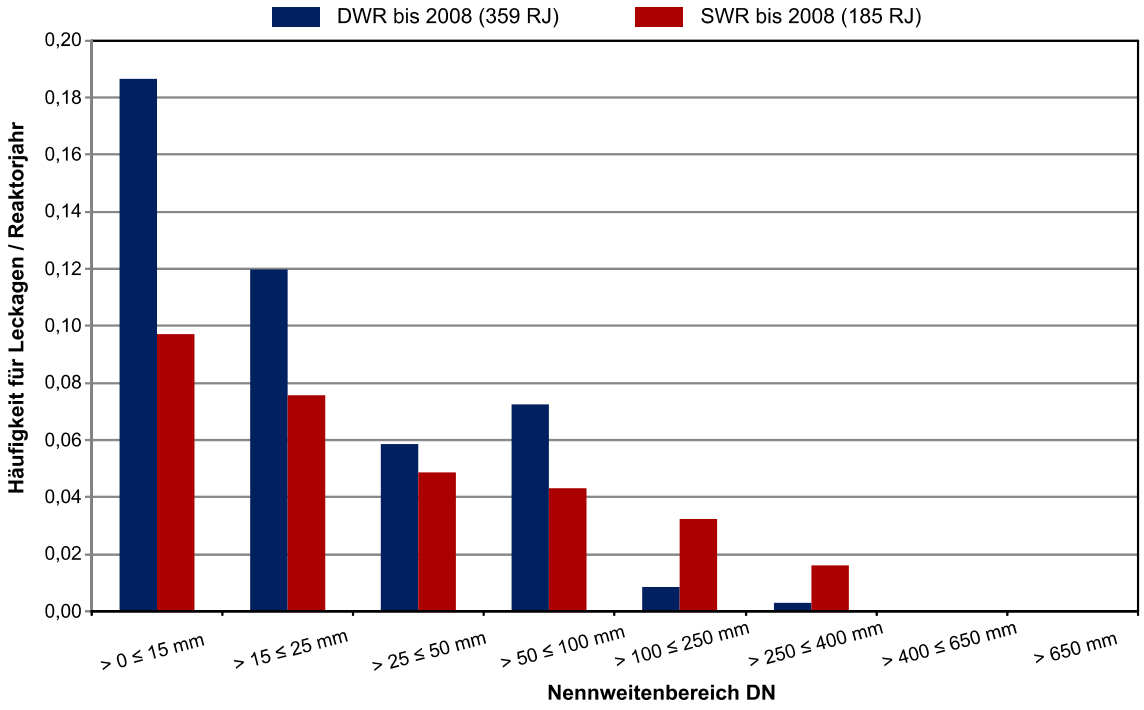


Abb. 4-13 Nennweitenabhängige Häufigkeit von Leckagen an Rohrleitungen der J- und K-Systeme deutscher Anlagen mit Druck- und Siedewasserreaktoren

Die Häufigkeit von Rohrleitungsleckagen an Schweißnahtbereichen sicherheitstechnisch bedeutsamer Rohrleitungen in deutschen Anlagen mit Druck- und Siedewasserreaktoren hat im Betrachtungszeitraum abgenommen. Dagegen haben Rohrleitungsleckagen, die im Grundwerkstoffbereich aufgetreten sind, insbesondere in Anlagen mit

Druckwasserreaktor an Bedeutung gewonnen. Dies wird am Beispiel der Druckwasserreaktoranlagen in Abb. 4-14 gezeigt.

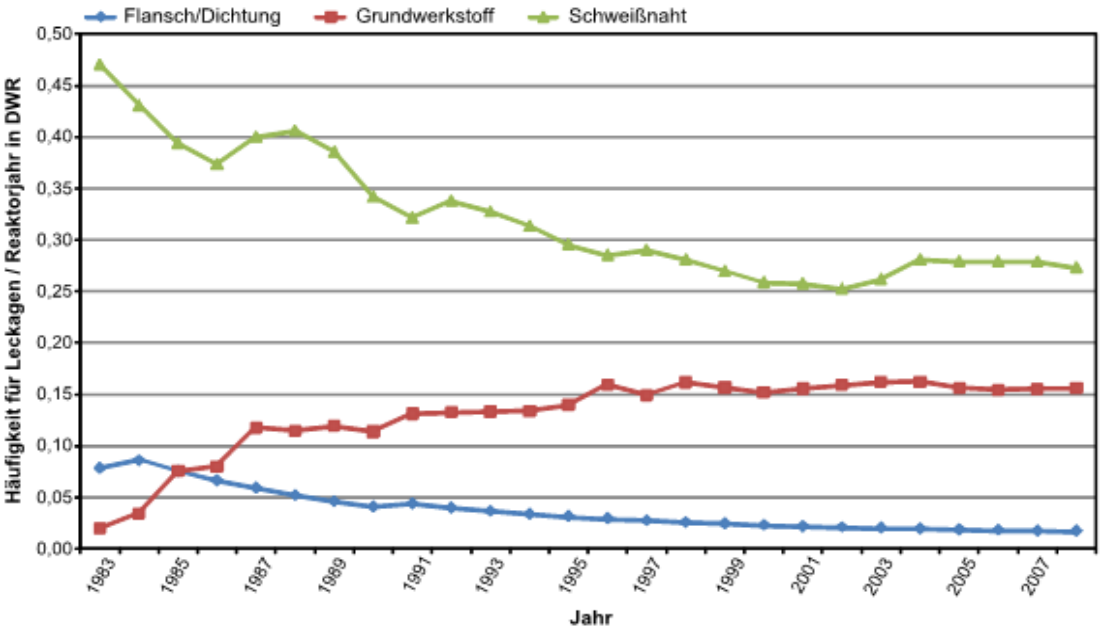


Abb. 4-14 Zeitliche Entwicklung der Häufigkeit von Leckagen an Rohrleitungen der J- und K-Systeme deutscher Druckwasserreaktoranlagen nach Schadensort

Die Leckereignisse wurden durch verschiedene Schädigungsmechanismen ausgelöst, von denen keiner über den gesamten Betrachtungszeitraum dominiert. Abb. 4-15 zeigt die Ereignisse mit Leckage an Rohrleitungen der J- und K-Systeme deutscher DWR differenziert nach Schädigungsmechanismen.

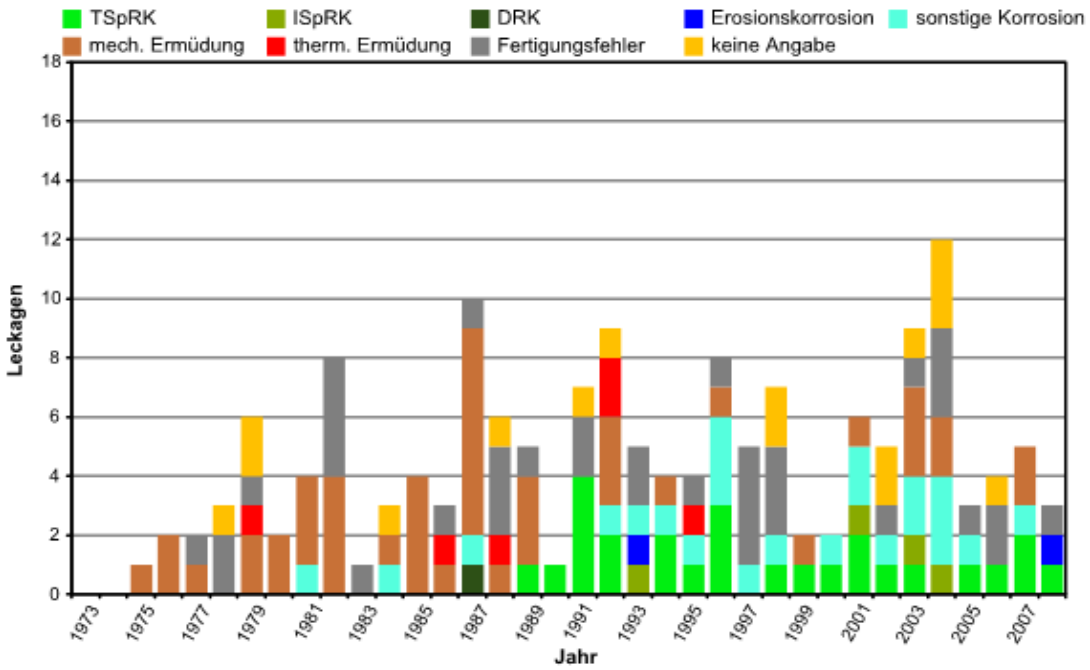


Abb. 4-15 Leckagen an Rohrleitungen der J- und K-Systeme deutscher Druck wasserreaktoranlagen differenziert nach Schädigungsmechanismus

Ein signifikanter, mechanismus-spezifischer Trend bei der Anzahl der Leckereignisse war nur für den Mechanismus ‘mechanische Ermüdung‘ zu erkennen.

4.3.2 Auswahlverfahren zur Bestimmung von kritischen Anlagenteilen bei seismischen probabilistischen Sicherheitsanalysen

Eine seismische PSA (SPSA) umfasst drei Hauptarbeitsschritte:

- Durchführung einer seismischen Gefährdungsanalyse zur Ermittlung standortspezifischer Häufigkeiten von Erdbebenwirkungen,
- Ermittlung von erdbebenbedingten Versagenswahrscheinlichkeiten für Bauteile, Systeme und Komponenten (BSK),
- Berechnung erdbebenbedingter Gefährdungs- und Kernschadenszustände.

Es wird ein Verfahren zur Auswahl von BSK abgeleitet und erprobt, für die bei der Durchführung einer SPSA tatsächlich erdbebenbedingte Versagenswahrscheinlichkeiten, sogenannte Fragilities, ermittelt werden müssen. In PSA der Stufe 1 werden für viele Komponenten Nichtverfügbarkeiten benötigt, die meistens statistisch ermittelt werden können. Dies ist bei der Bewertung von Nichtverfügbarkeiten aufgrund seismischer Einwirkungen nicht möglich. Die Fragilities sind zusätzlich von der Erdbebenin-

tensität abhängig, d. h. eine BSK fällt bei einem Erdbeben mit einer Wahrscheinlichkeit aus, die abhängig von der Stärke des Erdbebens ist.

Die anlagen- und BSK-spezifische Ermittlung von Fragilities ist sehr aufwändig, insofern wird ein Verfahren benötigt, welches unter allen BSK eines Kernkraftwerks diejenigen herausfindet, für die zum einen überhaupt Fragilities ermittelt werden müssen, und das zum anderen festlegt, in welcher Tiefe die Untersuchungen durchgeführt werden müssen. Dabei stellt sich die Frage, ob generische Fragilities das Ausfallverhalten der BSK ausreichend beschreiben oder ob Untersuchungen erforderlich sind, die die Spezifik der BSK in der entsprechenden Anlage einbeziehen.

Das entwickelte Auswahlverfahren trifft eine Vorauswahl für den zweiten Hauptarbeitsschritt. Es ist nicht möglich (und auch nicht notwendig) für alle BSK eines Kernkraftwerks seismische Versagenswahrscheinlichkeiten zu ermitteln. Dabei werden zwei Auswahlstufen unterschieden:

- Erste Auswahlstufe:

Ziel der ersten Auswahlstufe ist es, eine umfassende Liste von BSK zusammenzustellen, deren Fehlfunktion bei seismischer Einwirkung einen Beitrag zur Häufigkeit der Gefährdungszustände liefert. Diese Liste wird seismische Ausrüstungsliste (SAL) genannt. Es wird mittels einer systematischen Vorgehensweise sichergestellt, dass keine relevanten BSK übersehen werden können.

Grob zusammengefasst wird folgendermaßen vorgegangen:

- Aufbau einer vorläufigen SAL,
- Bestimmung der seismisch relevanten Räume,
- Begehung aller seismisch relevanten Räume,
- Aufbau der endgültigen SAL.

Die vorläufige SAL besteht im Wesentlichen aus den Komponenten, die im entsprechenden PSA-Modell der Stufe 1 als Basisereignisse enthalten sind. Weiter werden solche BSK hinzugenommen, deren Ausfall allein oder zusammen mit dem Funktionsverlust weiterer BSK zu einem auslösenden Ereignis führen kann.

Zu jeder BSK der vorläufigen SAL ist der zugehörige Standort (Raum entsprechend Anlagenkennzeichnung (AKZ)) zu bestimmen. Ein Raum, der eine BSK aus der SAL enthält, wird seismisch relevant genannt. Alle seismisch relevanten Räume werden begangen. Für die Begehungen werden raumbezogene Begehungsformblätter mit einer Vielzahl von Informationen zur Verfügung gestellt, damit kein Bewertungsaspekt übersehen werden kann. Bei den Begehungen geht es vor allem um die Ergänzung der vorläufigen SAL um weitere, seismisch relevante BSK. Das werden vor allem solche BSK sein, die aufgrund von Abhängigkeiten verschiedener Art bei einem eigenen Ausfall (z. B. Verlust der Standsicherheit) Einfluss auf das Ausfallverhalten von BSK haben, die schon in der vorläufigen SAL enthalten sind.

Nach Abschluss der Begehungen enthält die SAL sämtliche BSK mit dem Potential, bei einem Erdbeben zur Häufigkeit von Gefährdungszuständen beitragen zu können.

- Zweite Auswahlstufe:

Die zweite Auswahlstufe beschäftigt sich ausschließlich mit den BSK der in der ersten Auswahlstufe definierten SAL. Eventuelle Abhängigkeiten im seismischen Ausfallverhalten der BSK sind in der SAL vermerkt. Ziel der zweiten Auswahlstufe ist es, alle BSK der SAL nach sicherheitstechnischen Bedeutung zu klassifizieren und die festgestellten qualitativen Abhängigkeiten zu quantifizieren.

Dabei wird folgendermaßen klassifiziert:

- Ein Versagen bei Erdbeben liefert keinen Beitrag zur Häufigkeit von Gefährdungszuständen (BSK der Klasse 0).
- Die Versagenswahrscheinlichkeit bei Erdbeben kann durch generische Versagenskurven beschrieben werden (BSK der Klasse 1).
- Die Ableitung anlagenspezifischer Versagenskurven ist zur Bestimmung der Versagenswahrscheinlichkeit bei Erdbeben erforderlich (BSK der Klasse 2).

In der Auswahlstufe 2 wird bei der Klassifikation der BSK nach sicherheitstechnischer Bedeutung ebenfalls zweistufig vorgegangen. Zunächst wird versucht, möglichst viele BSK auf der Grundlage der erarbeiteten Daten und Informationen unter Einbeziehung von Expertenwissen zu klassifizieren. Dazu können die BSK nach Ähnlichkeitsmerkmalen gruppiert werden. Ist eine Klassifikation aufgrund der vorliegenden Informationen nicht möglich, werden diese BSK (kritische BSK) zur Entscheidungsfindung im Rah-

men einer weiteren Begehung zurückgestellt. Entsprechend wird bei der Bewertung der Abhängigkeiten vorgegangen. Sollte eine Quantifizierung auf der Grundlage der in der Datenbank vorhandenen Informationen nicht möglich sein, sind Vor-Ort-Begutachtungen durchzuführen.

Zur unterstützenden Durchführung einer SPSA wurde eine MS ACCESS©-Datenbank <*DB SPSA*> entwickelt. Diese Datenbank dient dazu, im Verlauf der Erarbeitung einer SPSA die erforderlichen Daten aufzunehmen, aufzubereiten und in den verschiedenen Phasen der Projektbearbeitung geeignet zur Verfügung zu stellen. Diese Datenbank konnte im Rahmen des Vorhabens RS1180 nur in ihren Grundzügen beschrieben und entwickelt werden. Eine Spezifizierung aller benötigten Daten, die Nutzung der Daten und die Einbindung der Datenbank in den Gesamtprozess der SPSA-Erstellung und Anwendung bleibt einem weiteren Projekt vorbehalten.

Zur Beschreibung der Daten- und Informationsflüsse bei probabilistischen Analysen ist die Unterscheidung zwischen Primär- und Sekundärdaten hilfreich. Unter Primärdaten versteht man alle Daten und Informationen, die sich ohne zusätzlich vertiefte Analysen aus der Aufgabenstellung ergeben. Sekundärdaten entstehen als Ergebnis eines informationsverarbeitenden Prozesses.

Bei der Durchführung des Auswahlverfahrens betrifft die Haupttabelle der Datenbank die Bauteile, Systeme und Komponenten. Das datenbankorientierte Auswahlverfahren besteht nun darin, diese Tabelle mit Primärdaten zu füllen, um auf dieser Grundlage alle benötigten Sekundärdaten abzuleiten und diese dann ebenfalls in der Tabelle abzulegen. Zu den Sekundärdaten gehören dann natürlich auch die Ergebnisse des Verfahrens wie die Zugehörigkeit einer BSK zur SAL und die Klassifizierung nach sicherheitstechnischer Bedeutung.

Die Datenbank ist so gestaltet, dass sie allgemein für SPSA-Projekte anwendbar ist. Erfahrungen aus anderen PSA-Projekten haben allerdings gezeigt, dass nur in Ausnahmefällen die Datenstrukturen in den einzelnen Kernkraftwerken gleich sind, insbesondere gibt es große Abweichungen bei den jeweils verwendeten Nomenklaturen. Die Struktur und Anwendung der Datenbank ist so allgemein wie möglich beschrieben. Zur Erprobung wurden Daten des Referenzkraftwerks herangezogen. Diese Datenbank wird <*DB SPSA GKN2*> genannt, um herauszustellen, dass die praktische Anwendung der allgemeinen Datenbankstruktur <*DB SPSA*> immer auch eine Anpassung an die konkreten (Daten-)verhältnisse in einem zu untersuchenden Kernkraftwerk bedeutet.

Für die Datenbank wurde eine Oberfläche gestaltet, über die eine Vielzahl von Eingaben, Standardabfragen und -auswertungen angewählt werden können. Es muss in diesem Zusammenhang angemerkt werden, dass die Nutzungsmöglichkeiten der Datenbank und die Kopplung der Informationen in einer konkreten SPSA-Anwendung so vielfältig sein können, dass ein direkter Zugriff auf die Tabellen der Datenbank für den Ersteller einer SPSA erforderlich bleibt. Dennoch ist die Oberfläche der Datenbank - insbesondere für den Gutachter und sonstige Nutzer der PSA-Ergebnisse - geeignet, sich einen flexiblen Überblick zu verschaffen und alle Ergebnisse anhand der Primärdaten nachvollziehen zu können.

Mit Hilfe der Datenbank wird im Verlauf der Erstellung einer SPSA die Durchführung folgender Aufgaben unterstützt:

- Zusammenstellung der vorläufigen SAL,
- Bereitstellung der BSK-Raum-Zuordnung, Zuordnung weiterer zur BSK-Klassifikation (Auswahlstufe 2) benötigter Eigenschaften,
- Qualitative Beschreibung von Abhängigkeiten zwischen BSK,
- Ermittlung seismisch relevanter Räume,
- Bereitstellung von Begehungsformularen für seismisch relevante Räume,
- Ergänzung der vorläufigen SAL durch weitere BSK,
- Zusammenfassung und tabellarische Darstellungen zu den Ergebnissen des Auswahlverfahrens,
- Bereitstellung von Informationen zur Begutachtung, Nachvollziehbarkeit der Analysen.

Als Referenzanlage stand das Kernkraftwerk GKN-2 zur Verfügung. Ein Vorhaben dieses Umfangs bleibt ohne die Möglichkeit des Zugriffs auf anlagenspezifische Daten pure Theorie. Nur mit echten Daten und Informationen können eine Datenbank und die Durchführung von Teilen einer SPSA realitätsnah erprobt werden.

Es wurde gezeigt, wie die SAL für das Referenzkraftwerk schrittweise in und mit Hilfe der Datenbankstruktur <*DB SPSA*> zur konkreten SPSA-Datenbank <*DB SPSA GKN2*> für das Referenzkraftwerk aufgebaut wird. Der Vorhabensumfang reichte nicht

aus, um den gesamten Umfang der benötigten Daten zu bewältigen. Im Wesentlichen beschränkte man sich auf zwei relevante Gebäude.

4.3.3 Methoden für eine probabilistische Bewertung von Transienten aufgrund von Überspannungen oder Fremdspannungseinträgen

Die durchgeführten Untersuchungen zum Bedarf einer Methodenentwicklung für eine probabilistische Bewertung von Transienten aufgrund von Überspannungen oder Fremdspannungseinträgen haben, wie bereits aus dem Titel zu interpretieren ist, den Charakter einer Vorstudie. Mit dieser Studie wurde geprüft, welche Defizite für die Durchführung einer PSA mit Überspannungen oder Fremdspannungseinträgen als auslösende Ereignisse vorhanden sind, wo der Bedarf für Methodenentwicklungen liegt und wie in einem weiterführenden Projekt die Methoden verbessert werden sollen. Erst nach Durchführung und Erprobung dieser Methoden anhand eines Beispiels lässt sich abschätzen, ob sich daraus nennenswerte Beiträge die Häufigkeit von Gefährdungs- bzw. Kernschadenszuständen ergeben können.

Als Ergebnis ist Folgendes festzuhalten:

Die qualitative Auswertung der Betriebserfahrung zeigt, dass sich aus dem Auftreten von Überspannungen im Netz oder elektrischen Stromerzeugungsanlagen in Deutschland in der Vergangenheit keine wesentlichen Beiträge für die Häufigkeit von Gefährdungszuständen ergeben haben. Soweit in deutschen Anlagen Störungen aufgetreten sind, wurden Umschaltungen auf das Reservenetz oder Notstromfälle ausgelöst. Soweit Notstromfälle aufgetreten sind, sind diese bei der numerischen Ermittlung der Eintrittshäufigkeiten von Notstromfällen berücksichtigt worden. Gleichzeitige Folgeausfälle des Sicherheitssystems bei diesen Notstromfällen wurden nicht beobachtet. Andererseits ist das Auftreten von Überspannung oder Fremdspannungseinträgen kein seltenes Ereignis.

Darüber hinaus zeigt das Ereignis im Kernkraftwerk Forsmark, dass eine Überspannung, die aus dem Netz oder dem Hauptgenerator kommt, das Potential hat, in allen Redundanzen des Notstromsystems weitere Störungen in Folge zu verursachen. Dies war in Forsmark der Ausfall von zwei der vier Dieselaggregate mit der Tendenz eines Totalausfalls aller Dieselaggregate. Allerdings ist dabei zu berücksichtigen, dass die Kette von Ereignissen, die zu dem Störfall geführt hat, sich nicht allein aus der aufge-

tretenen Überspannung, sondern auch durch Überlagerung des Versagens weiterer Systeme bzw. Komponenten ergeben hatte.

Daneben sind durch Überspannungseinträge in das Erdungssystem Spannungsverlagerungen möglich, die Fehlsignale der Leittechnik verursachen können. Solche Überspannungen und ihre Folgen wurden bisher im Rahmen von Prüfungs- und Reparaturarbeiten mit Hochspannungsgeneratoren beobachtet. Direkte Blitzeinschläge in die Gebäude einer Anlage könnten ähnliche Wirkungen haben. Daher sind ergänzende Untersuchungen durchzuführen, inwieweit, abhängig vom Erdungssystem, Spannungsverschiebungen und daraus resultierende Fehlauslösungen der empfindlichen Leittechnik möglich sind.

Die durchgeführte Analyse hat gezeigt, dass einerseits durch die nicht zu vernachlässigende Häufigkeit des Auftretens von Überspannungen und Fremdspannungseinträgen und andererseits dem vorhanden Potential, anlageninterne auslösende Ereignisse ggf. mit Beeinträchtigung des Sicherheitssystems zu verursachen, sich durchaus die Notwendigkeit ergibt, solche Ereignisse systematisch zu untersuchen. Solche Untersuchungen würden zum einen zu einer Abrundung der Ereignispalette beitragen, die im PSA-Leitfaden zu untersuchen empfohlen ist, und zum anderen auch aufzeigen, inwieweit die eingesetzten aktiven und passiven Sicherheitseinrichtungen zur Ausgewogenheit des Sicherheitszustandes der Anlage beitragen. Dadurch können auch Schwachstellen aufgezeigt und ein Beitrag zur Erhöhung der Sicherheit der Anlagen durch deren Beseitigung geleistet werden.

Im Verlaufe der Untersuchungen konnten Defizite hinsichtlich der Ereignisablaufanalyse und der probabilistischen Bewertung von überspannungsbedingten Ausfällen von elektrischen Einrichtungen bzw. von fremdspannungsbedingten Einkopplungen in leittechnische Systeme festgestellt werden, die zeigen, dass es im Wesentlichen zwei wichtige Aufgaben gibt, die zukünftig bei der Durchführung einer PSA in diesem Zusammenhang vorrangig sind:

Zum einen ist die Analyse des Ablaufs eines Ereignisses, ausgehend von der Ursache bis hin zu möglichen Schadenszuständen, notwendig. Diese Aufgabe wird mit Hilfe deterministischer Systemanalysen vollzogen. Soweit sich daraus mehrere Schadensendzustände ergeben, werden die Pfade zu diesen Schadensendzuständen in den Ereignisbäumen in Abhängigkeit von der Funktion bzw. dem Funktionsausfall der betrachteten Systeme abgebildet. Es sind systematisch mögliche Quellen einer Über-

spannung zu identifizieren sowie die Reaktion der Systeme auf das Eintreten einer Überspannung und die Auswirkungen zu analysieren, wenn die vorhandenen Schutzmaßnahmen nicht greifen. Primär sollten dabei solche Überspannungstransienten detailliert untersucht werden, die das Potential haben, redundanzübergreifende Schäden zu verursachen, weil diese grundsätzlich die Eigenschaft haben, nicht zu vernachlässigende Beiträge zur Häufigkeit von Kernschadenszuständen zu liefern.

Aufgrund des jetzigen Kenntnistandes sind dies Störungen, die aus dem Netz oder dem Hauptgenerator kommen. Es handelt sich aber auch um Störungen, die Potentialverschiebungen in der Erdungsanlage verursachen können und damit ggf. Fehlsignale auslösen. Ein gewisses Potential haben möglicherweise auch Fehlhandlungen des Personals bei Wartungs- und Instandsetzungsarbeiten. Ob es darüber hinaus noch weitere Störquellen und Effekte gibt, konnte im Rahmen dieser Vorstudie nicht beantwortet werden.

Eine weitere, methodisch zu lösende Aufgabe ist die Beeinflussung der Leittechnik durch Überspannungs- bzw. Fremdspannungseinträge. Es ist ggf. mittels Experimente zu analysieren, wie vor allem hochfrequente Überspannungen, die aus dem Netz durch Blitzschlag oder durch Schaltvorgänge innerhalb der Anlage herrühren, Leittechnikkabel beeinflussen können. Dabei sind auch die Fragen zu beantworten, wie groß die dabei auftretenden eingekoppelten Spannungen werden können und was passiert, wenn die Schutzeinrichtungen versagen?

Während die ersten beiden Aufgaben im Wesentlichen dem Bereich der Systemanalysen zuzuordnen sind, um das Schadensbild festzustellen, wird die dritte Hauptaufgabe im Bereich der Probabilistik durchzuführen sein. Bei dieser Aufgabe müssen die Ausfallwahrscheinlichkeiten aktiver und passiver Überspannungsschutzeinrichtungen ermittelt werden. Dabei sollte eine methodische Vorgehensweise gefunden werden, wie die Wahrscheinlichkeiten von induzierten Fremdspannungseinträgen auf leittechnischen Einrichtungen ermittelt bzw. abgeschätzt werden können. Sinnvoll wäre es, geeignete Kriterien zu finden, mit denen der Ersteller der PSA entweder eine Störeinkopplung ausschließen bzw. diese als wenig wahrscheinlich, als wahrscheinlich oder als sehr wahrscheinlich einstufen kann. Soweit diesbezüglich eine Auswertung der Betriebserfahrung möglich ist, sollten sich die numerischen Zahlen darauf stützen. Falls eine Abschätzung der Zuverlässigkeitskenngrößen für diese Barrieren nicht möglich ist, ist zu überlegen, ob nicht ersatzweise die numerische Bewertung durch Exper-

ten geschätzt werden kann, wobei dem Experten aber geeignete Informationen zur Verfügung gestellt werden müssten.

In diesem Zusammenhang muss hinsichtlich des Auftretens von Folgeausfällen geklärt werden, wie groß die ‘Reichweite‘ von Störstrahlungen oder von eingekoppelten Überspannungen ist. Die Ausbreitung von Störstrahlungen wird durch Abschirmungen, wie Wände, geerdete Metallteile, Kabelpritschen, andere Leiter, mehr oder weniger gedämpft. Die leitungsgebundenen Fremdspannungen werden vor allem durch Ohmsche Widerstände und Induktivitäten abgebaut.

Unter der Voraussetzung, dass die oben genannten Hauptaufgaben gelöst sind, können die relevanten Ereignisbäume und Fehlerbäume modelliert und mit Hilfe der vorhandenen Werkzeuge RiskSpectrum® bzw. CRAVEX die notwendigen Berechnungen durchgeführt werden. Mit CRAVEX bzw. dessen Programmteil RAVE können das Schadensbild auf simulative Art und Weise ermittelt und mittels einer FMEA durch den Experten das zu untersuchende auslösende Ereignis ermittelt werden. Die von CRAVEX benötigte Raumdatenbank liegt vor, sofern für die untersuchte Anlage bereits eine Brand-PSA vorhanden ist. Für die Bildung der Komponentengruppen ist auf Kabel- und Funktionspläne zurückzugreifen.

Soweit auf bestehende PSAs zurückgegriffen wird, sind diese so zu ergänzen, dass die Schutzeinrichtungen zur Vermeidung der Auswirkungen von Überspannungen ergänzend modelliert werden. Inwieweit die PSA ausschließlich mit CRAVEX durchgeführt wird, hängt auch davon ab, ob die Software so angepasst werden kann, dass damit Unsicherheitsanalysen durchgeführt werden können. Im BMU-Vorhaben R0801316 (‘PSA-Methoden für Brand bei Nichtleistungsbetrieb‘) wurden zwei Ansätze für eine Unsicherheitsanalyse mit CRAVEX entwickelt. CRAVEX wird dabei in Verbindung mit der Software SUSA für Unsicherheits- und Sensitivitätsanalysen /KLO 08/ eingesetzt. Zur Reduktion des Rechenaufwands sind allerdings noch weitere programmtechnische Anpassungen in CRAVEX erforderlich.

Gemäß Auftragsbeschreibung ist eine Art Lastenheft für ein künftiges detaillierteres Projekt erstellt worden, welches durch das nachfolgende Ablaufschema (vgl. dazu Abb. 4-8 bis Abb. 4-19) dargestellt, welches in anschaulicher Form aufzeigt, wie in einer PSA die Aufgabenblöcke für die Modellierung eines auslösenden Ereignisses mit Überspannung durchzuführen sind. Die Aufgabenblöcke sind farblich unterschiedlich gestaltet, so dass erkennbar ist, wo mehr oder weniger Entwicklungsbedarf in der Zu-

kunft besteht. Die Farbe ‘rot‘ bedeutet dabei ‘großer Bedarf, ggf. hoher Aufwand‘. Die Farbe ‘violett‘ bedeutet ‘Bedarf je nach Analysenfortschritt, ggf. hoher Aufwand, während ‘gelb‘ ‘wenig Bedarf an methodischer Weiterentwicklung, mittlerer Aufwand‘ bedeutet. Die Farbe ‘grün‘ steht für ‘geringer Bedarf hinsichtlich einer Methodenentwicklung, niedriger Aufwand‘. Der personelle Aufwand bei der konkreten Durchführung einer PSA ist von den Ergebnissen der künftigen Methodenentwicklung abhängig und kann derzeit noch nicht quantifiziert werden.

Zur Durchführung einer PSA, insbesondere für die Erstellung von Ereignisbäumen und Fehlerbäumen, sind System- bzw. Störfallablaufanalysen notwendig.

Die möglichen Schadensbilder, die sich aufgrund einer Überspannungstransiente oder eines Fremdspannungseintrags ergeben können, sind von vielen Ursachen abhängig. Die Ausbreitungsmechanismen sind jedoch derzeit nur teilweise erforscht. Für die probabilistische Bewertung liegen bislang nur in geringem Umfang Zuverlässigkeitsdaten vor, insbesondere sind keine Daten für das Auftreten von induzierten Spannungseinträgen vorhanden. Es liegen kaum Daten für das Versagen der Schirmung, des Potentialausgleichs und für Erdungsfehler vor. Insbesondere ist fraglich, wie Näherungen zwischen elektrischen Energieversorgungskabeln und leittechnischen Kabeln bzw. Geräten probabilistisch zu bewerten sind, wenn im Energieversorgungskabel eine Überspannung bzw. als Folge Überstrom auftritt.

Dagegen kann festgestellt werden, dass mit den vorhanden PSA-Werkzeugen, ggf. mit gewissen Modifikationen, die Berechnungen zur Ermittlung von Gefährdungs- bzw. Kernschadenshäufigkeit durchführbar sind, wenn die Fehler- und Ereignisbäume aufgrund der durchgeführten Schadensbild- bzw. Systemanalysen und auch die erforderlichen Zuverlässigkeitskenngrößen vorliegen. Allerdings zeigt die bisherige Betriebserfahrung, dass für deutsche Anlagen zwar Handlungsbedarf für eine Weiterentwicklung von PSA-Methoden zur Bewertung von Überspannungstransienten besteht, dieser aber nicht von hoher Dringlichkeit ist.

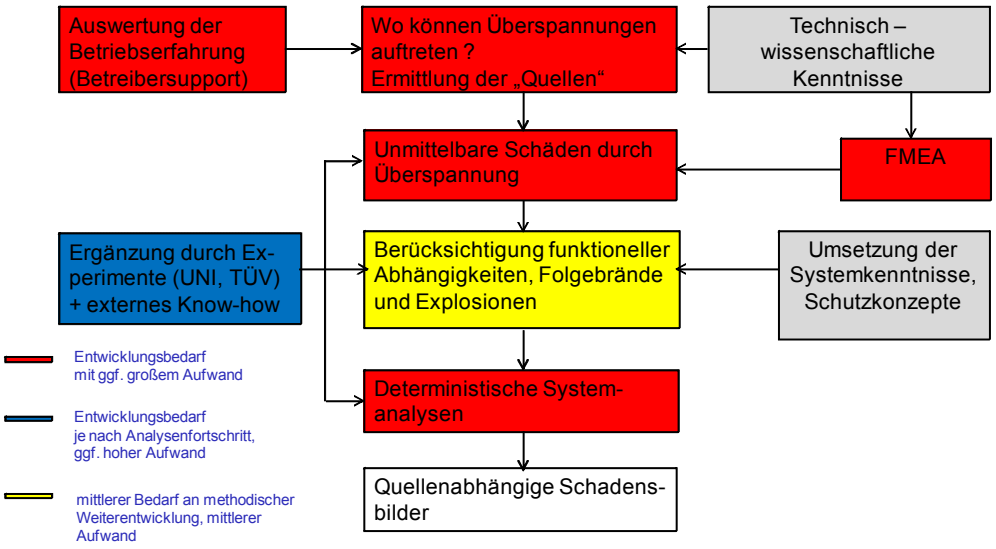


Abb. 4-16 Aufgaben bei der Identifizierung von Schadensbildern

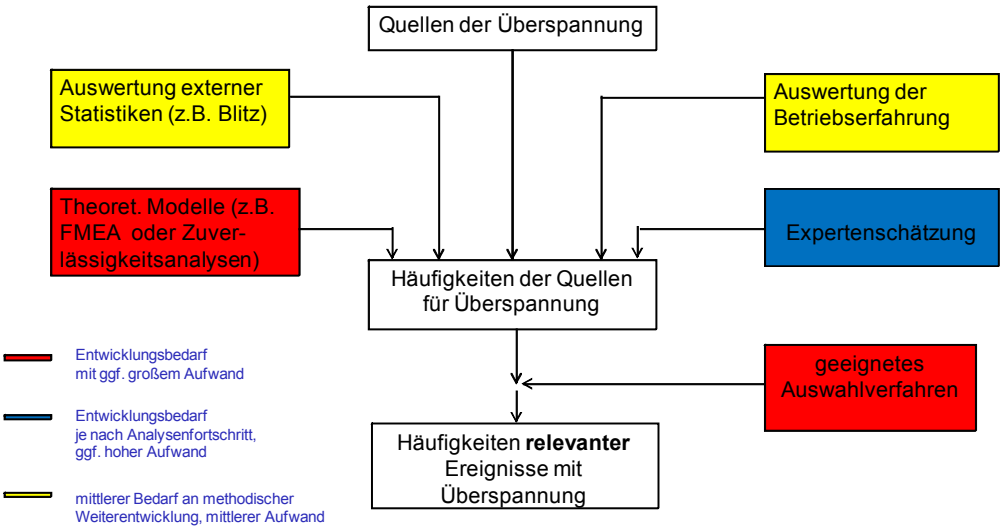


Abb. 4-17 Aufgaben zur Ermittlung der Eintrittshäufigkeiten von Überspannungen

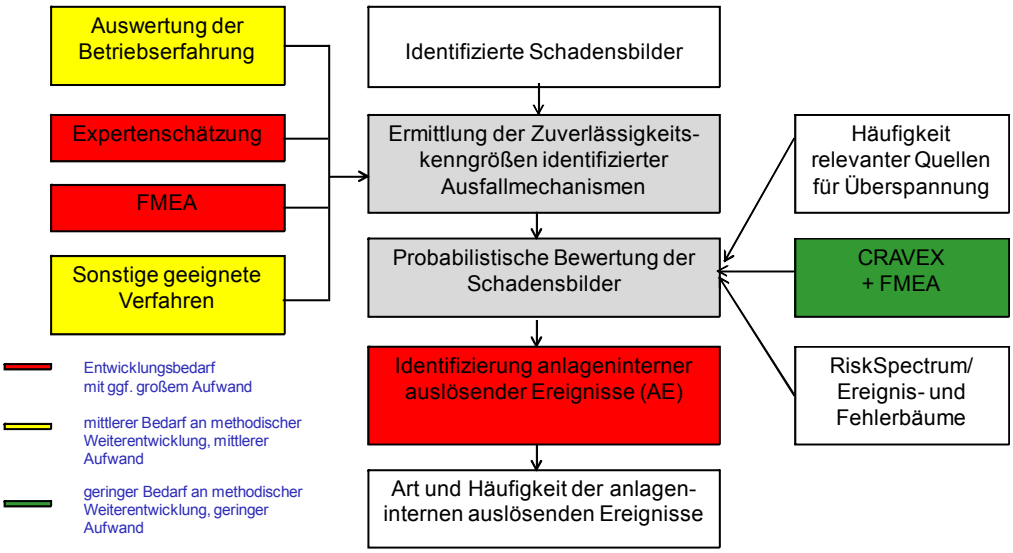


Abb. 4-18 Aufgaben zur Ermittlung der Eintrittshäufigkeit der Transienten (auslösende Ereignisse)

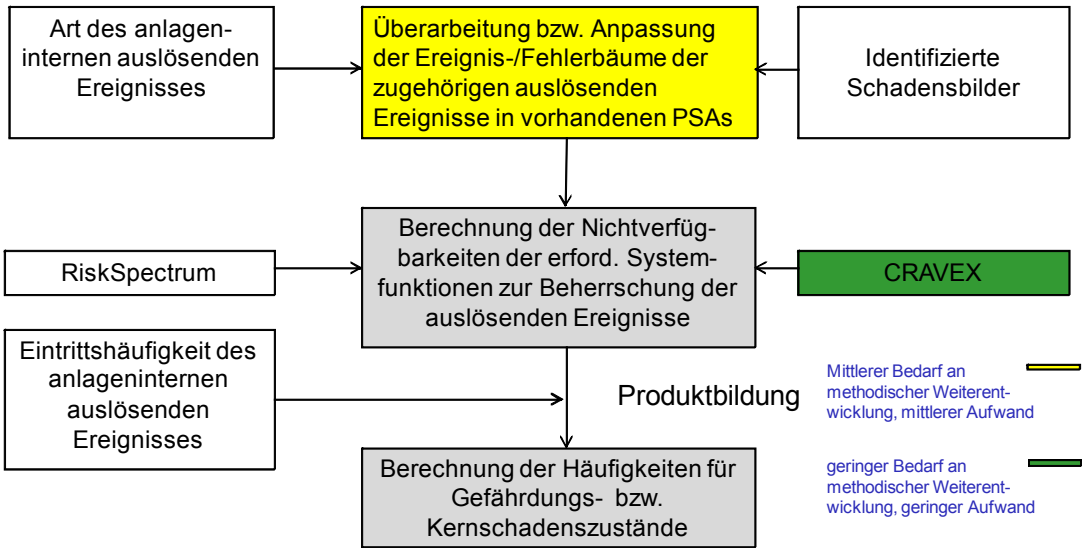


Abb. 4-19 Aufgaben zur Berechnung der Gefährdungs- bzw. Kernschadenshäufigkeiten

4.4 Methoden zur Analyse des Einflusses von Unsicherheiten auf PSA-Ergebnisse und zum Ausschluss von Fehlerquellen in der PSA

4.4.1 Methoden zur Durchführung von Unsicherheits- und Sensitivitätsanalysen in probabilistischen Dynamikanalysen (dynamische PSA)

Wenn in einer probabilistischen Dynamikanalyse mittels MCDET-Analyse aus Gründen der Rechenzeitersparnis die aleatorischen und epistemischen Größen gemeinsam variiert werden, dann kann der spezielle Einfluss der epistemischen Größen auf die Unsicherheit der probabilistischen Aussagen nicht über die übliche Unsicherheits- und Sensitivitätsanalyse quantifiziert werden. Dazu wäre eine getrennte Analyse von aleatorischen und epistemischen Größen erforderlich, die über eine zweistufig geschachtelte Monte Carlo-Simulation durchgeführt werden kann. Eine MCDET-Analyse unter Verwendung einer zweistufigen Monte Carlo-Simulation beansprucht in der Regel jedoch einen zu hohen Aufwand an Rechenzeit und ist daher nicht praktikabel.

Es wurden zwei alternative Methoden entwickelt und erprobt, mit denen approximative Unsicherheits- und Sensitivitätsaussagen hergeleitet werden können und die auf MCDET Rechenläufen basieren, bei denen im Rahmen einer einstufigen Monte Carlo-Simulation aleatorische und epistemische Variable gemeinsam variiert werden und daher weit weniger Rechenläufe benötigen, als die Analyse auf der Basis einer zweistufig geschachtelten Monte Carlo-Simulation.

Die Grundidee der ersten Methode besteht in der Anpassung multipler Regressionsfunktionen an interessierende Ergebnisgrößen aus der MCDET-Analyse. Unter Verwendung der angepassten Regressionsfunktionen erfolgt eine nachträgliche getrennte Betrachtung der aleatorischen und epistemischen Größen über eine zweistufige Simulationsschleife. Für die über die multiplen Regressionsfunktionen ermittelten approximativen Ergebnisse kann man dann eine Unsicherheits- und Sensitivitätsanalyse in gewohnter Weise durchführen.

Bei sehr komplexen Analysenkann jedoch die Erzeugung von multiplen Regressionsfunktionen, abgesehen von der Qualität ihrer Anpassung, problematisch bzw. unmöglich sein. Für solche Fälle wurde deshalb eine alternative Methode zur Durchführung einer approximativen Unsicherheits- und Sensitivitätsanalyse entwickelt. Der Vorteil

dieser Methode ist, dass sie ohne jede Einschränkung anwendbar und unabhängig von der Anzahl der beteiligten Variablen ist. Der Nachteil besteht allerdings darin, dass die MCDET-Analyse zweimal mit jeweils unterschiedlichen Parametersätzen durchgeführt werden muss. In der zweiten MCDET-Analyse werden die Werte der aleatorischen Größen neu ausgespielt, während die Werte der epistemischen Größen die gleichen bleiben wie bei der ersten durchgeführten MCDET-Analyse.

Die Ergebnisse aus der approximativen Unsicherheits- und Sensitivitätsanalyse, die sich über die Methode des multiplen Regressionsverfahrens ergeben haben, stimmen relativ gut mit denen überein, die sich aus der Unsicherheits- und Sensitivitätsanalyse bzgl. der MCDET-Analyse mit zweistufig geschachtelter Monte Carlo-Simulation ergeben haben. Insbesondere stimmen die Aussagen der approximativen Sensitivitätsanalyse fast genau mit den Sensitivitätsaussagen aus der MCDET-Analyse mit voller zweistufiger Monte Carlo-Simulation überein. Diese relativ guten Übereinstimmungen konnten trotz der teilweise nur mäßigen Anpassungen der multiplen Regressionsfunktionen erzielt werden. Allerdings neigte diese Methode zu einer leichten Verschiebung der Verteilung der untersuchten probabilistischen Ergebnisgrößen zu kleineren Werten hin.

Die Ergebnisse der approximativen Unsicherheits- und Sensitivitätsanalyse, die über die alternative Methode bei doppelter Ausführung der MCDET-Analyse mit verändertem Parametersatz ermittelt wurden, konnten schon bei relativ niedrigen Stichprobenumfängen (z. B. mit 2 x 100 dynamischen Ereignisbäumen) als weitgehend akzeptabel betrachtet werden. Tendenziell neigten die approximativen Werte zu einer leichten Überschätzung der Verteilung der untersuchten probabilistischen Ergebnisgröße, also zur sicheren Seite hin. Die zugehörige qualitativ-approximative Sensitivitätsanalyse hat zu der gleichen Parameterrangfolge geführt, wie die Sensitivitätsanalyse, die auf der Basis der MCDET-Analyse mit voller zweistufiger Monte Carlo Simulation durchgeführt worden ist.

Insgesamt betrachtet, konnten bzgl. des vorliegenden Anwendungsbeispiels mit beiden entwickelten Methoden zur approximativen Unsicherheits- und Sensitivitätsanalyse brauchbare bis gute Ergebnisse erzielt werden.

4.4.2 Methoden zur Anpassung von Beta-Verteilungen an vorgegebene Lognormal-Verteilungen unter Berücksichtigung zusätzlicher Benutzervorgaben

Die Ergebnisse des in diesem Vorhaben entwickelten Verfahrens werden dementsprechend anhand eines Beispiels veranschaulicht. Dabei wird eine Beta-Verteilung an eine Lognormal-Verteilung angepasst, für welche Erwartungswert und k95-Faktor gegeben sind. Der Erwartungswert beträgt 1.6 E-03; der k95-Faktor beträgt 10. Die Beta-Verteilung wird an das 50 %- und 95 %-Quantil der vorgegebenen Verteilung angepasst.

Die für das Beispiel erforderlichen Eingaben in das Dialogfenster der Benutzeroberfläche ‘BetaFit‘ sind in Abb. 3-3 veranschaulicht. Sobald die Eingaben bestätigt werden, wird automatisch das dazugehörige FORTRAN-Programm zur Ermittlung der Beta-Verteilung aufgerufen. Es dokumentiert Eingabedaten und Ergebnisse in der Datei ‘BetaFit.out‘.

Der Inhalt dieser Datei bzgl. des obigen Beispiels sieht wie folgt aus:

```
******************************Lognormal-Verteilung ******************************

 Eingabe:
 ---------------------------------------------------
 Erwartungswert:  1.6000E-03
 k95-Faktor    :  1.0000E+01

 Weitere Charakteristika der Lognormal-Verteilung:
 ---------------------------------------------------------------
 Par. my     : -7.4174E+00
 Par. sigma  :  1.3997E+00
 Varianz     :  1.5601E-05
  5 %-Quantil:  6.0071E-05
 50 %-Quantil:  6.0071E-04
 95 %-Quantil:  6.0071E-03

 ******************************Beta-Verteilung**********************************

 Beta-Verteilung wird angepasst an
 Quantile der ungestutzten Lognormal-Verteilung.
 ---------------------------------------------------------------
 50 %-Quantil :  6.0071E-04
 95 %-Quantil :  6.0071E-03

 Parameter Suche: Iterationsverfahren nach Tarasenko ("Random Search" Algorithmus):
 ---------------------------------------------------------------------------------------
 Startwerte für Parameter der Betaverteilung:
 ---------------------------------------------------
 Par. a       :  8.3201E-01
 Par. b       :  5.5287E+02
 1. Quantil:   6.0071E-04, Wahrscheinlichkeit:   3.6735E-01, Fehler:   1.326544E-01
 2. Quantil:   6.0071E-03, Wahrscheinlichkeit:   9.7518E-01, Fehler:  -2.517664E-02

 Standardisierter mittlerer quadratischer Fehler:   9.547525E-02

 Endwerte für Parameter der Betaverteilung:
 ---------------------------------------------------
 Par. a       :  4.3863E-01
 Par. b       :  2.9316E+02
 1. Quantil:   6.0071E-04, Wahrscheinlichkeit:   5.0000E-01, Fehler:   5.960464E-07
 2. Quantil:   6.0071E-03, Wahrscheinlichkeit:   9.5000E-01, Fehler:  -1.251698E-06

 Standardisierter mittlerer quadratischer Fehler:   9.803107E-07

 Erwartungswert:  1.4940E-03
 Varianz      :  5.0636E-06


Benötigte Rechenzeit für Parametersuche=277.76 s
```

Zusätzlich zur Dokumentation der Ergebnisse in der Datei ‘BetaFit.out‘ erfolgt eine grafische Darstellung der Ergebnisse. Die folgenden beiden Abbildungen veranschaulichen die Verteilungs- und Dichtefunktionen von vorgegebener Lognormal- und angepasster Betaverteilung bzgl. des obigen Beispiels.

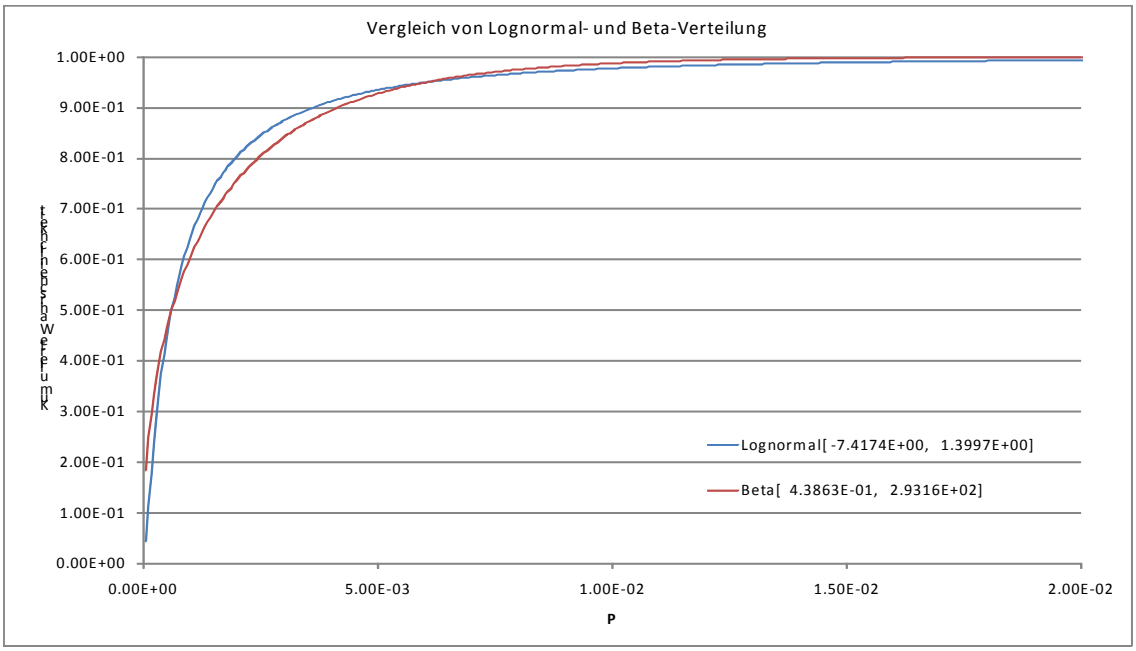


Abb. 4-20 Vergleich der Verteilungsfunktionen von vorgegebener Lognormal- und angepasster Betaverteilung

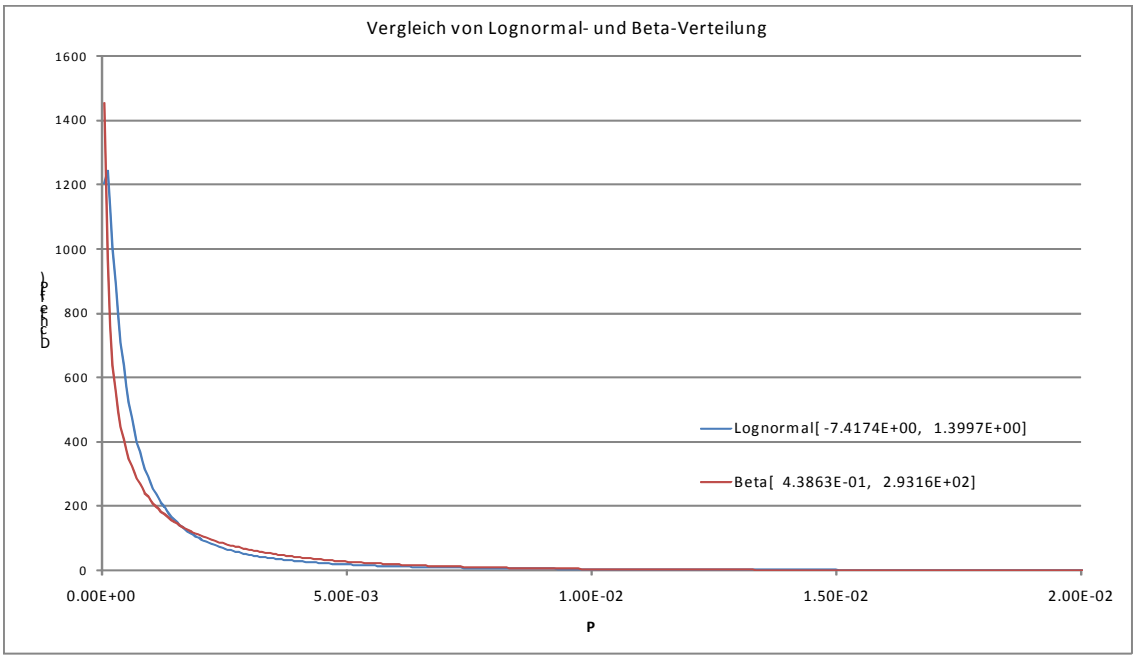


Abb. 4-21 Vergleich der Dichtefunktionen von vorgegebener Lognormal- und angepasster Betaverteilung

Mit ‘BetaFit‘ steht eine flexibel anwendbare Methode zur Verfügung, mit der Beta-Verteilungen an vorgegebene Lognormal-Verteilungen unter Berücksichtigung verschiedener Verteilungsinformationen angepasst werden können.

4.4.3 Konsistente und umfassende Berücksichtigung epistemischer Unsicherheiten in Verteilungen von Zuverlässigkeitskenngrößen

Um nicht explizit im Schätzmodell berücksichtigten Unsicherheitsquellen Rechnung zu tragen und deren potentiellen Einfluss zumindest in grober Abschätzung in die Verteilungen von Zuverlässigkeitskenngrößen einfließen zu lassen, wird eine nachträgliche Varianzerhöhung (Verbreiterung) der aus den Schätzmodellen resultierenden Verteilungen von Zuverlässigkeitskenngrößen vorgenommen.

Bisher wurde eine einfache analytische Methode der Verbreiterung von Verteilungen durchgeführt. Diese analytische Vorgehensweise ist allerdings auf Lognormal-Verteilungen beschränkt und kann nicht auf andere Verteilungen, die sich aus den Schätzmodellen in parametrischer oder nicht-parametrischer Form ergeben, übertragen werden. Zur Vermeidung von Einschränkungen und kritischen Aspekten des bisherigen, auf Lognormal-Verteilungen basierenden Verfahrens wird ein neues, allgemein anwendbares Verfahren zur nachträglichen Varianzerhöhung von Verteilungen für Zuverlässigkeitskenngrößen vorgeschlagen.

Das auf //SON 01a/ /SON 06/ /STI 09/ aufbauende und in diesem Vorhaben weiterentwickelte Verfahren, mit dem die Varianz jeder beliebigen parametrischen und nicht-parametrischen Schätzverteilung vergrößert werden kann, ist insbesondere für Verteilungen von Zuverlässigkeitskenngrößen geeignet, die eine Wahrscheinlichkeit beschreiben (z. B. Ausfallwahrscheinlichkeit pro Anforderung, GVA-Wahrscheinlichkeit, menschliche Fehlerwahrscheinlichkeiten). Diese allgemein anwendbare Methodik kann jedoch nicht mehr wie bei dem bisherigen, auf Lognormal-Verteilung basierenden Verfahren analytisch durchgeführt werden, sondern erfolgt numerisch über eine Monte Carlo-Simulation. Ein weiterer Unterschied zur bisherigen Vorgehensweise der Verbreiterung ist, dass mit dem entwickelten neuen Verfahren der Mittelwert der ursprünglichen Schätzverteilung beibehalten wird. Mit dem bisherigen, auf der Lognormal-Verteilung basierenden Verfahren wurde der Median beibehalten. Mit dem vorgeschlagenen neuen Verfahren kann außerdem ausgeschlossen werden, dass sich durch die nachträgliche Varianzerhöhung der Schätzverteilungen Wahrscheinlichkeiten ergeben, deren Werte > 1 sind. Mit dem bisherigen Verfahren zur Verbreiterung der Schätzverteilungen konnte dies nicht gewährleistet werden.

Zur Erprobung wurde die entwickelte Methodik zur nachträglichen Varianzerhöhung von Verteilungen für Zuverlässigkeitskenngrößen in dem GRS-Rechenprogramm zur

Schätzung von GVA-Wahrscheinlichkeiten (PEAK) über eine Subroutine implementiert. Die Ergebnisse der durchgeführten Vergleichsrechnungen deuten darauf hin, dass das neu vorgeschlagene Verfahren zur nachträglichen Varianzerhöhung von Verteilungen für Zuverlässigkeitskenngrößen den Einfluss zusätzlicher Unsicherheitsquellen, die nicht explizit im Schätzmodell berücksichtigt werden, besser bzw. vollständiger abschätzt als das bisherige, auf der Lognormal-Verteilung basierende Verbreiterungsverfahren. Außerdem können durch die Anwendung des neu vorgeschlagenen Verfahrens verschiedene Einschränkungen und kritische Aspekte des bisherigen, auf der Lognormal-Verteilung basierenden Verfahrens vermieden werden.

Aus der Untersuchung zur Frage, ob die nachträgliche Varianzerhöhung von Schätzverteilungen generell eine hinreichend zufriedenstellende Methode darstellt, den Einfluss zusätzlicher Unsicherheitsquellen auf die Schätzverteilungen von Zuverlässigkeitskenngrößen zu berücksichtigen, konnten verschiedene Schlussfolgerungen gezogen werden.

Grundsätzlich ist der Einfluss potentieller, nicht explizit im Schätzmodell berücksichtigter Unsicherheitsquellen auf die Unsicherheiten der Schätzverteilungen nicht zu quantifizieren. Deshalb kann auch mit dem neu vorgeschlagenen Verfahren zur nachträglichen Varianzerhöhung von Schätzverteilungen für Zuverlässigkeitskenngrößen nicht garantiert werden, dass es den tatsächlichen Einfluss zusätzlicher Unsicherheitsquellen auf die Unsicherheiten der Schätzverteilungen hinreichend genau abschätzt. D. h., es ist keine Aussage darüber möglich, wie gut der tatsächliche Einfluss der zusätzlichen Unsicherheitsquellen durch die nachträgliche Verbreiterung von Schätzverteilungen beschrieben wird.

Trotz dieser methodischen Schwächen ist die Durchführung einer nachträglichen Varianzerhöhung von Verteilungen für Zuverlässigkeitskenngrößen jedoch immer noch dem Vorgehen vorzuziehen, das den potentiellen Einfluss zusätzlicher epistemischer Unsicherheitsquellen auf die Ergebnisunsicherheiten ignoriert und generell unberücksichtigt lässt. Die Aussage kann folgendermaßen begründet werden:

1. Wenn die verbreiterte Verteilung den tatsächlichen Einfluss der zusätzlichen Unsicherheitsquellen überschätzt, so kann sie als konservativ in dem Sinne aufgefasst werden, dass sie zu hohe Unsicherheiten insbesondere auch in Richtung größerer Werte der Zuverlässigkeitskenngröße ausweist.

2. Wenn der tatsächliche Einfluss unterschätzt wird, so liefert die verbreiterte Verteilung durch die Varianzerhöhung immer noch eine bessere Abschätzung des Einflusses der zusätzlichen Unsicherheitsquellen als die ursprüngliche Schätzverteilung, bei der der Einfluss der zusätzlichen Unsicherheitsquellen gar nicht berücksichtigt wird.

Angesichts dieser Verhältnisse ist eine Varianzerhöhung (Verbreiterung) der Schätzverteilung grundsätzlich vorzuschlagen, wenn davon ausgegangen wird, dass zusätzliche Unsicherheitsquellen existieren, die nicht explizit im Schätzmodell berücksichtigt werden und die einen Einfluss auf die Unsicherheit der Schätzverteilungen der jeweiligen Zuverlässigkeitskenngrößen haben.

Allerdings ist es auch mit dem neu vorgeschlagenen Verfahren zur nachträglichen Varianzerhöhung von Verteilungen für Zuverlässigkeitskenngrößen nicht möglich, den Einfluss der Unsicherheitsquellen, die nicht explizit im Schätzmodell berücksichtigt werden, methodisch korrekt zu quantifizieren. Deshalb sollte die nachträgliche Varianzerhöhung von Schätzverteilungen lediglich als eine Hilfslösung betrachtet werden, um den Einfluss potentiell relevanter epistemischer Unsicherheitsquellen zumindest in grober Näherung berücksichtigen zu können.

Um den Einfluss zusätzlicher Unsicherheitsquellen methodisch korrekt quantifizieren zu können, ist es unerlässlich, dass möglichst viele relevante Unsicherheitsquellen, die potentiell einen Einfluss auf die Unsicherheiten der Schätzverteilungen von Zuverlässigkeitskenngrößen haben können, identifiziert und explizit in das Schätzmodell eingehen. Nur so kann der Einfluss von Unsicherheitsquellen auf die Unsicherheiten der Verteilungen für Zuverlässigkeitskenngrößen methodisch richtig ermittelt und quantifiziert werden. Dazu sind allerdings eine genaue Erfassung und Auswertung der Betriebserfahrung sowie eine durchgängige Weiterentwicklung der jeweiligen Schätzmodelle notwendig.

4.4.4 Methoden zur konsistenten Berücksichtigung gemeinsam verursachter Ausfallereignisse (GVA) in PSA

Wie bereits in Kapitel 3.4.4 dargestellt, gliedert sich dieser Arbeitspunkt auf in die Weiterentwicklung des Verfahrensrahmens zur Bewertung der Übertragbarkeit beobachteter GVA-Ereignisse sowie die Entwicklung eines geschlossenen Programmsystems zur Berechnung von GVA-Wahrscheinlichkeiten.

Um die Verfahrensweise zur Bewertung der Übertragbarkeit beobachteter GVA-Ereignisse auf in der PSA modellierte Komponentengruppen weiterzuentwickeln, wurden zunächst die derzeit vorhandenen Bewertungsrandbedingungen untersucht.

Nach der Vereinheitlichung der Formulierung inhaltlich identischer Randbedingungen zur Bewertung meldepflichtiger Ereignisse in deutschen Kernkraftwerken sind 209 verschiedene Randbedingungen vorhanden. Die meisten Randbedingungen werden nur für ein einziges Ereignis verwendet. In den allermeisten Fällen bestehen die Randbedingungen aus der Verknüpfung von mehreren Einzelaspekten. Bis zu vier Einzelbedingungen kommen vor.

Bei der Untersuchung der verschiedenen Randbedingungen daraufhin, welche Aspekte der Unterschiede zwischen der Komponentengruppe, in der ein Ereignis aufgetreten ist, und der Komponentengruppe der Zielanlage, für die eine GVA-Wahrscheinlichkeit im PSA-Fehlerbaum ermittelt werden soll, durch die Randbedingung beschrieben werden, wurden sechs Hauptkategorien von Bewertungsaspekten identifiziert. Diese erfordern teilweise eine unterschiedliche Vorgehensweise bezüglich der Expertenbewertungen bzw. bezüglich der mathematisch-statistischen Behandlung. Die sechs Kategorien von Aspekten beschreiben

- kleine und große Redundanzgrade,
- verschiedene Anforderungsdauern,
- unterschiedliche Anlagenbetriebsphasen,
- Ereignisablauf- spezifische Randbedingungen,
- technische Unterschiede, Unterschiede im Betrieb, in der Überwachung und Instandhaltung der Systeme und Komponenten, sowie
- Randbedingungen zur Darstellung von Ausfallarten.

Hierbei sind die Randbedingungen zur Darstellung von Ausfallarten keine Randbedingungen im engeren Sinn, sondern wurden dazu benutzt, auszudrücken, dass bei den meldepflichtigen Ereignissen die Komponenten in speziellen Ausfallarten ausgefallen sind, die nicht den üblicherweise in der PSA verwendeten Ausfallarten entsprechen.

Die Untersuchung der Randbedingungen ergab, dass die in der Datenbasis definierten Randbedingungen bisher keiner allgemeinen Systematik genügen. Bei der Durchfüh-

rung der Ereignisbewertungen sahen die Experten vielfach die Notwendigkeit, Randbedingungen neu zu definieren, um möglichst realistische Bewertungen zu ermöglichen. Die mit der daraus resultierenden großen Anzahl von Randbedingungen verknüpften Probleme wurden noch nicht gesehen. Randbedingungen wurden also bei der Bewertung einzelner Ereignisse definiert, ohne dass ein generelles Konzept darüber vorlag, wann die Einführung neuer Randbedingungen zulässig und erforderlich ist. Dies führte dazu, dass vielfach Randbedingungen

- sich auf sehr spezifische Gegebenheiten der aufgetretenen GVA-Ereignisse bzw. der betroffenen Einrichtungen beziehen (z. B. technische Details wie die Verwendung von Tantalkondensatoren auf elektronischen Baugruppen oder Teflonbeschichtungen von Messumformern) und
- sehr spezifische Gegebenheiten in Anlagen, für die GVA-Daten zu ermitteln waren, berücksichtigen (z. B. „Mit Wirkleistungsmessung über Strom- und Spannungsmessung bei allen Armaturenfahrten sowie Auswertung bzgl. Wirkleistungsaufnahme, Drehmoment und Reibbeiwert (z. B. durch Vergleich mit regelmäßigen Prüfstandsmessungen) und Trendauswertung)“.

Im Ergebnis führte dies dazu, dass

- die meisten Randbedingungen nur in einer einzigen Ereignisbewertung verwendet wurden,
- die meisten Randbedingungen die Kombination von mehreren (bis zu vier) Einzelbedingungen sind,
- es vielfach sehr ähnliche, aber nicht vollständig identische Randbedingung gibt.

Wenn in einer PSA unterschiedliche Randbedingungen für verschiedene Komponentengruppen aus derselben Population verwendet werden sollen, ist es zur statistisch korrekten Schätzung von Zuverlässigkeitskenngrößen erforderlich, die zu jeder definierten Randbedingung entsprechenden Beobachtungszeiten bzw. Anzahl der Anforderungen zu ermitteln. Bei dem vorliegenden System ist dies nicht praktikabel. Deshalb wurde bisher die Gesamtbeobachtungszeit aller Komponentengruppen verwendet.

Eine umfassende systematische Bewertung, ob nicht bestimmte aufgetretene Phänomene in manchen modellierten Komponentengruppen häufiger zu erwarten sind oder gravierendere Schadensbilder verursacht hätten (z. B. weil Überwachungseinrichtun-

gen fehlen), wurde nicht vorgenommen. Hierbei wäre prinzipiell auch zu berücksichtigen, dass diese Phänomene unter den gegebenen Randbedingungen eventuell gar nicht zu einem GVA geführt haben, während sie unter anderen Randbedingungen einen GVA auslösen würden.

Die beiden vorgenannten Gründe könnten prinzipiell zu einer systematischen Unterschätzung von GVA-Wahrscheinlichkeiten für solche Komponentengruppen führen. Deshalb muss aus den gewonnenen Erkenntnissen der Schluss gezogen werden, dass das vorhandene System der Randbedingungen erheblich zu überarbeiten ist. Dabei sollte die Anzahl verschiedener Randbedingungen deutlich reduziert werden, so dass für alle Randbedingungen bzw. alle möglichen Kombinationen die Bezugsgrößen (Betriebszeiten oder -anzahlen) ermittelbar sind. Dazu sollte auf überdetaillierte Randbedingungen verzichtet werden, Populationen aufgeteilt werden, wenn dies technisch sinnvoll und bei der vorliegenden Menge Betriebserfahrung möglich ist und die verbleibenden Randbedingungen vereinheitlicht werden.

Es sollte dabei von einem System, das sich eng an die beobachteten Ereignisse anlehnt, zu einem System übergegangen werden, das sich an den wesentlichen Unterschieden innerhalb von Populationen orientiert. Für in diesen Populationen aufgetretene Ereignisse sind dann jeweils alle Randbedingungen zu bewerten, wodurch automatisch die Vollständigkeit der Bewertungen sichergestellt wird und die oben erwähnte mögliche systematische Unterschätzung beim heutigen System von Randbedingungen vermieden wird. Weiterhin wird durch eine wesentlich geringere Zahl verschiedener Randbedingungen die Erfassung der Beobachtungszeiten (bzw. Anzahlen von Anforderungen) wesentlich vereinfacht bzw. erst möglich gemacht.

Im Hinblick darauf wurden grundsätzliche Anforderungen für ein verbessertes System von Randbedingungen entwickelt. Wesentliche Anforderungen betreffen, neben den oben bereits genannten Aspekten, Regeln für die Einführung und Charakterisierung von Randbedingungen, die Aufteilung von Populationen sowie die Durchführung von Expertenbewertungen. Es wird vorgeschlagen, eine stärker formalisierte Vorgehensweise (z. B. in Form von Flussdiagrammen) zu entwickeln.

Für die quantitative Bewertung wurde eine Skala von Werten für die Übertragbarkeitsfaktoren entwickelt, welche sich bezüglich ihrer Abstufung an die bisher meist gewählten Bewertungen anlehnt, jedoch auch Übertragbarkeitsfaktoren größer 1 umfasst.

Durch den einzelnen Stufen zugeordnete Kriterien könnte eine bessere Nachvollziehbarkeit der Bewertungen erreicht werden.

Weiterhin wurden Anforderungen zur Verwendung von Randbedingungen bei der Ermittlung für Zuverlässigkeitskenngrößen für die PSA entwickelt. Diese umfassen die Forderung, einen einheitlicher Detaillierungsgrad zu verwenden. D. h. wenn bezüglich eines Aspektes mithilfe von Randbedingungen differenziert werden soll, ist dies konsistent für alle Komponentengruppen zu tun. Weiterhin wird gefordert, bezüglich modellierter Anlagenbetriebsphasen sowie Ereignisabläufe eine eindeutige Aufteilung zu definieren und jeweils die für die Anlagenbetriebsphase bzw. den Ereignisablauf zutreffenden Randbedingungen zum Bestimmen der verwendeten Zuverlässigkeitskenngrößen zu benutzen.

Eine Betrachtung der Übertragung von Ereignissen auf Komponentengruppen deutlich abweichender Größe ergab, dass auch in Zukunft prinzipiell die bisherige Vorgehensweise beibehalten werden muss, bei der durch Experten beurteilt wird, ob die sich aus der mathematischen Modellierung mit dem Kopplungsmodell ergebende Extrapolation sachgerecht ist, und gegebenenfalls notwendige Änderungen durch Expertenschätzungen bestimmt werden.

Das Programmsystems POOL zur Erstellung von Datensätzen zur Berechnung von GVA-Wahrscheinlichkeiten ist fertiggestellt. POOL liest aus der Datenbank GVA die darin vorhandenen Expertenbewertungen aus und bietet in einem übersichtlichen Bearbeitungsmenü die Möglichkeit, Datensätze mit Hilfe von Auswahlkriterien individuell zusammenzustellen und an die Randbedingungen der Komponentengruppen, für die GVA-Wahrscheinlichkeiten bestimmt werden sollen, anzupassen. Aus dem Programm POOL kann dann direkt das Programm PEAK zur Berechnung der GVA-Wahrscheinlichkeiten aufgerufen werden.

Die GVA-Wahrscheinlichkeiten selbst werden wie bisher mit PEAK berechnet. Die Ergebnisausgabe von PEAK wurde dahingehend modifiziert, dass die Ergebnisse in einer im Fehlerbaumprogramm RiskSpectrum® importierbaren rsa-Datei ausgegeben werden.

Für verschiedene, voneinander unabhängige Auswertungen (z. B. anlagenspezifische oder generische Datensätze) können in POOL einzelne Projekte erzeugt werden, deren Daten unabhängig voneinander behandelt werden.

Die Bildung der zu einem Projekt gehörigen Datensätze erfolgt über eine mehrstufige Auswahl. Zunächst ist mit Hilfe eines Baumdiagramms die Population zu wählen, zu der die Komponenten der Zielanlage, für die AGVA-Wahrscheinlichkeiten berechnet werden sollen, gehören. Dies geschieht gegebenenfalls über mehrere Auswahlschritte (z. B. Armaturen → Absperrventile (motorbetätigt) → Wasser führende Systeme). Als letzter Schritt im Baumdiagramm findet stets die Auswahl der Ausfallart statt (z. B. ‘schließt nicht‘).

Die nächste Stufe stellt die Auswahl der Quellen und die Berechnung der Beobachtungszeit dar. Prinzipiell sind in der Datenbank GVA drei unterschiedliche Quellen vorhanden, wobei für keine Komponentenart alle Quellen Auswertungen enthalten. Die Quelle BEV (Besondere Vorkommnisse) /KRE 97/ enthält Informationen über GVA-Ereignisse, die im Rahmen der Auswertung von meldepflichtigen Ereignissen erfasst und bewertet wurden. Die Quelle IRS /KRE 97/ enthält GVA-Ereignisse aus der Auswertung des Incident Reporting Systems (IRS) der IAEA. Die Quelle BIB /KRE 97/ enthält GVA-Ereignisse aus der ausgewerteten Betriebserfahrung einer deutschen DWR-Anlage. Die Auswertungen der beiden letzteren Quellen fanden beide im Rahmen der deutschen Risikostudie Phase B statt. Die für die Berechnung zu verwendenden Quellen sind vom Benutzer aus einer Liste auszuwählen. PEAK berechnet für jede Quelle eigene Ausfallwahrscheinlichkeiten, die bei der Ausgabe des Gesamtergebnisses logarithmisch gemittelt werden. Die jeweilige Beobachtungszeit ergibt sich aus der gewählten Quellen und den vorher gewählten Komponenten und Ausfallarten.

Um in Zukunft auch Betrachtungen mit flexiblen Auswertezeiträume, z. B. im Rahmen von Trendanalysen, ohne größeren zusätzlichen Aufwand handhaben zu können, wurde in POOL ein tabellenbasierter Algorithmus implementiert, mit dem bereits bei der Erstellung der Datensätze die zu einem benutzerdefinierten Zeitraum passenden Beobachtungszeiten berechnet werden können. Von den restlichen PSA-relevanten Parametern werden ebenfalls automatisch nur diejenige weiterverarbeitet, bei denen das Ereignisdatum des zugehörigen GVA-Ereignisses in den spezifizierten Zeitraum fällt.

Dies wurde für die Quelle BEV realisiert. Für diese Quelle besteht die Möglichkeit, über zwei Eingabefelder den auszuwertenden Zeitraum zusätzlich anzupassen oder zu beschränken. GVA-Ereignisse, deren Ereignisdaten nicht in den so definierten Zeitraum fallen, werden nicht weiter bei der Zusammenstellung der Datensätze berücksichtigt. Die Beobachtungszeit wird dann mit Hilfe zweier Tabellen berechnet. Die sogenannte Quellenliste enthält Informationen über die Zeiträume, innerhalb derer von der GRS

Auswertungen für die jeweiligen Komponentenarten und Ausfallarten durchgeführt wurden. Die Komponentengruppenliste enthält kraftwerksspezifische Informationen über die In- und Außerbetriebnahme einzelner Komponentengruppen, sowie die Anzahl der vorhandenen Komponentengruppen innerhalb einer Anlage. An Hand dieser Informationen kann für jede Auswertung in jeder Anlage, die berücksichtigt werden soll, der Beitrag jeder einzelnen Komponentengruppe zur Gesamtbeobachtungszeit errechnet werden. Durch entsprechende Summationen ergeben sich dann der Beitrag eines Kraftwerks zur Gesamtbeobachtungszeit der Population und die gesamte Beobachtungszeit selbst. Da für ausländische Anlagen keine detaillierten Informationen über den Aufbau der sicherheitsrelevanten Systeme hinsichtlich der Anzahl oder der Betriebsdaten von PSA-relevanten Komponentengruppen vorliegen, kann für die Quelle IRS nicht auf diesen Algorithmus zurückgegriffen werden. Die Quelle BIB soll mittelfristig in die Quelle BEV integriert werden. Bis auf wenige Ausnahmen ist dies bereits geschehen, daher steht diese Funktionalität für die Quelle BIB ebenfalls nicht zur Verfügung. Diese beiden Quellen können nur komplett oder gar nicht berücksichtigt werden. Ihre Beobachtungszeiten sind feste Größen, die nicht verändert werden können.

Das der Berechnung der Beobachtungszeit zu Grunde liegende Datenmaterial wurde im Rahmen der Implementierung der neuen Rechenmethode geprüft und teilweise verbessert. Für zahlreiche Komponentenarten, für die vorher lediglich Abschätzungen für generische Druckwasser- oder Siedewasserreaktoranlagen existierten, wurden im Rahmen der Erstellung der Komponentengruppenliste detaillierte Zählungen vorgenommen.

In der dritten Stufe der Bildung der Datensätze werden die zu verwendenden Randbedingungen ausgewählt. Für jedes GVA-Ereignis werden alle Randbedingungen, für die Bewertungen in der Datenbank GVA vorhanden sind, aufgelistet. Der Benutzer muss für jedes Ereignis die zu verwendenden Randbedingungen auswählen. GVA-Ereignisse mit identischen Randbedingungen werden zu einer Auswahl zusammengefasst. Es obliegt dem ingenieurstechnischen Sachverstand des Benutzers, keine sich widersprechenden Randbedingungen auszuwählen (z. B. bei Pumpen ‘Trockener Aufstellort‘ und ‘Tauchpumpen‘).

Die vierte und letzte Stufe besteht aus der Auswahl der Experten, deren Einschätzungen bezüglich der Schädigungsvektoren und des Übertragbarkeitsfaktors bei den zur ausgewählten Population gehörigen GVA-Ereignissen berücksichtigt werden sollen.

Während des gesamten Auswahlprozesses geben zwei aufeinander aufbauende Tabellen dem Benutzer eine Übersicht, welche GVA-Ereignisse bei der ausgewählten Population innerhalb des definierten Zeitraums beobachtet wurden und welche Experten die jeweilige Ereignisse wie bewertet haben.

Zusätzlich existiert in dem POOL-Programm auch eine Übersicht der bisher vorhandenen Populationen.

Zur Eingabe der Anlagendatensätze, also der GVA-relevanten Parameter der Komponentengruppen, für die GVA-Wahrscheinlichkeiten berechnet werden sollen, besitzt das POOL-Programm eine Eingabemaske. Dort wählt der Benutzer an Hand zweier aufeinander aufbauender Tabellen aus, zu welcher der vorher definierten Population der Anlagendatensatz gehört und gibt dann die weiteren notwendigen Parameter (Fehlerentdeckungszeit, Komponentengruppengröße, optional einen Kommentar) ein.

Das Programm PEAK, mit dem die GVA-Wahrscheinlichkeiten berechnet werden, kann direkt aus dem POOL-Programm heraus gestartet werden.

Auch der Export der in POOL erstellten Datensätze ist weitestgehend automatisiert, es muss lediglich die MS ACCESS®-Datei angegeben werden, in der die berechneten Ausfallwahrscheinlichkeiten gespeichert und die Ausgangsparameter dokumentiert werden sollen.

Eine weitere Möglichkeit zur Dokumentation der zusammengestellten Datensätze bietet die Report-Funktion des POOL-Programms. Sie bietet dem Benutzer die Möglichkeit, die erstellten Populationsdatensätze sowie gegebenenfalls die zugehörigen Anlagendatensätze in verschiedenen Formaten (z. B. PDF, MS WORD®) und verschiedenen Formatierungen abzuspeichern. Wird der maximale Detailierungsgrad gewählt, werden alle für die Berechnung und die Interpretation der GVA-Wahrscheinlichkeiten relevanten Daten protokolliert (Komponentenart, Ausfallart, zugehörige Randbedingungen, vorhandene Quellen, Beschränkungen im auszuwertenden Zeitraum, Beobachtungszeit, Fehlerentdeckungszeit, Größe der Zielkomponentengruppe, relevante GVA-Ereignisnummern, dazu gehörig: Ereignisdatum, betroffene Anlage, Größe der betroffenen Komponentengruppe, Kurzbeschreibung der betroffenen Komponentengruppe, bewertende Experten und die von ihnen geschätzten Schädigungsvektoren und Übertragbarkeitsfaktoren).

Um zu überprüfen ob die mit dem POOL-Programm generierten Datensätze in PEAK auch mit Datensätzen, die nach der bisherigen Vorgehensweise manuell erstellt wurden, übereinstimmende Ergebnisse liefern, wurden für jede Komponentenart, jede Ausfallart, jede verwendete Kombination an Randbedingungen und jede aufgeführte Fehlerentdeckungszeit der in Anhang A von /FAK 05a/ dokumentierten Datensätzen ein Anlagendatensatz im POOL-Programm mit einer zufällig gewählten Anzahl an Zielkomponenten erstellt, nach PEAK exportiert und die GVA-Wahrscheinlichkeiten für die möglichen Ausfallkombinationen errechnet. Diese Zahlen wurden mit den in /FAK 05a/ aufgeführten GVA-Wahrscheinlichkeiten verglichen.

Die Ergebnisse aus dem Datenband waren durch die Programme POOL und PEAK reproduzierbar. Einzelne Abweichungen konnten auf Änderungen am Datenmaterial oder bekannte Begrenzungen des PEAK-Programms zurückgeführt werden.

4.4.5 Benutzeroberfläche mit den erforderlichen Hilfsprogrammen für PSA-Methoden der Stufe 1

Basierend auf dem in Abschnitt 3.4.5 dargestellten Überlegungen ist eine erste Version von goPSA erstellt worden, aus der die relevanten GRS-Hilfsprogramme mit Hilfe von Eingabemasken aufgerufen werden können und unter der die entsprechenden Benutzerhilfen verfügbar sind, ausreichend. goPSA wurde in der Sprache Visual Basic .NET implementiert.

Der Startbildschirm von goPSA ist in Abb. 4-22 dargestellt. Es bieten sich die folgenden Möglichkeiten:

- **GVA:**
  GVA ruft ein Auswahlfenster für die GRS-Hilfen zur Modellierung von GVA-Modulen auf.

- **RiskSpectrum®:**
  RiskSpectrum® startet das Programm RiskSpectrum® von Scandpower AB[1], sofern dieses auf dem Rechner installiert ist. Dies ist nicht im Installationsumfang von goPSA enthalten.)

- **CRAVEX:**
  CRAVEX startet die Bedienoberfläche des GRS-Rechenprogramms CRAVEX, sofern dieses auf dem Rechner installiert ist. (Dies ist nicht im Installationsumfang von goPSA enthalten.)

- **STREUSL:**
  STREUSL öffnet ein Auswahlfenster für den Aufruf des GRS-Programms STREUSL.

- **SUSA:**
  SUSA startet das GRS-Programm SUSA, sofern dieses auf dem Rechner installiert ist. (Diese Funktionalität ist derzeit noch nicht implementiert.)

- **HRA-Bewertung:**
  HRA-Bewertung startet eine Benutzerhilfe, die erläutert wie man HRA-Ereignisbäume der Methode THERP mit RiskSpectrum® modelliert.

- **Dokumentation:**
  Dies öffnet ein Auswahlfenster, aus dem heraus die Benutzerhilfen der GRS zur Auswertung einer PSA der Stufe 1 entsprechend dem PSA-Methodenband /FAK 05/ aufgerufen werden können.

- **RSAscii:**
  RSAscii öffnet die grafische Bedienung für das Programm RSAscii von der GRS, das RSA-Dateien in ein von GRS-Programmen (STREUSL, CRAVEX) lesbares Format umschreibt).

- **EXCELRS:**
  EXCELRS öffnet die grafische Bedienung für das Programm RSAscii von der GRS, Dateien werden im Format für STREUSL und CRAVEX in das RSA-Format von RiskSpectrum® konvertiert.

- **CmpFt:**
  CmpFt öffnet die grafische Bedienung für das Programm RSAscii von der GRS, welches an Hand von RSD-Dateien einen Vergleich von Fehlerbäumen in RiskSpectrum-Projekten vornimmt**.**

---

[1] RiskSpectrum® ist eine eingetragene Marke der Fa. Scandpower AB, die seit 2009 ein Teil von Lloyd‘s Register Group ist. Die Verwendung von Markennamen in diesem Bericht impliziert keine Beeinträchtigung der jeweiligen Eigentums- und Urheberrechte.

- **Schnittstelle:**
  Dies öffnet ein Auswahlfenster für die GRS-Hilfen zur Schnittstelle zwischen Stufe 1 und Stufe 2 der PSA.

In den folgenden Abschnitten werden einige ausgewählte Ergebnisse zu den unter goPSA verfügbaren Programmen und Benutzerhilfen vorgestellt. Eine detailliertere Beschreibung von goPSA und den darin verfügbaren Programmen kann dem technischen Fachbericht /WIE 10/ entnommen werden.

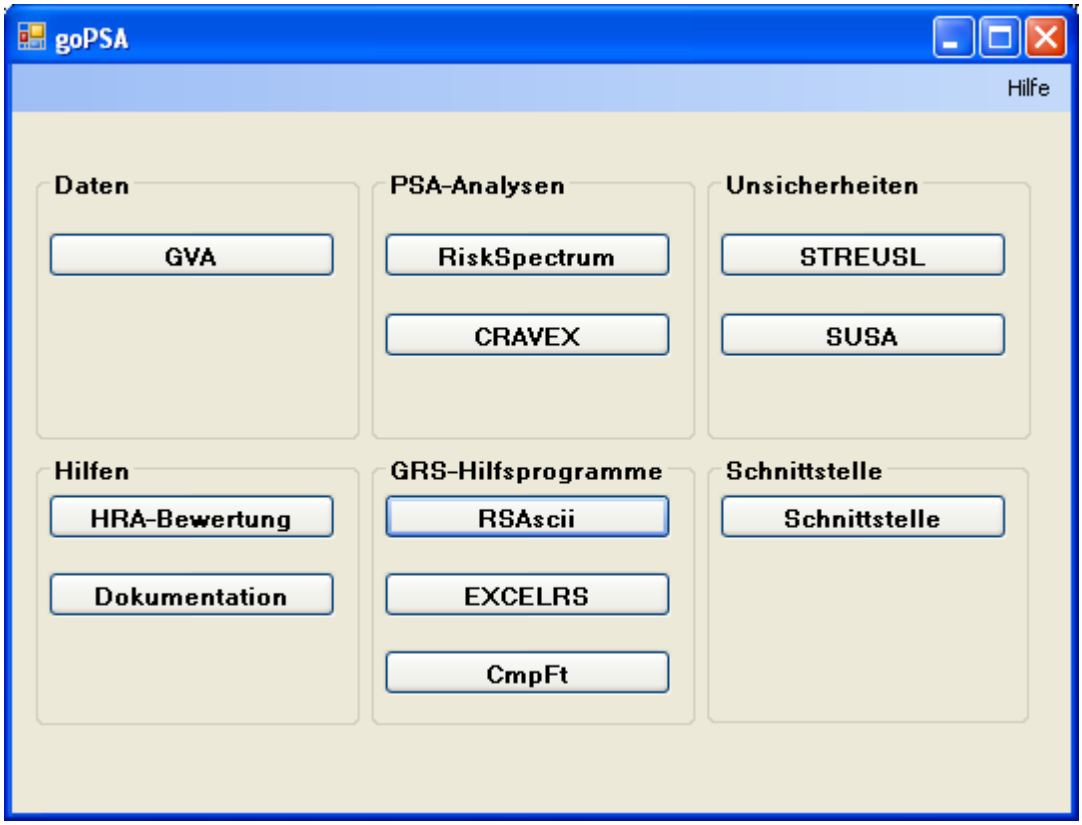


Abb. 4-22 Startbildschirm von goPSA

4.4.5.1 STREUSL

Das Programm STREUSL ist von der GRS erstellt worden, um Unsicherheits- und Importanzanalysen nach dem Stand von Wissenschaft und Technik mit Hilfe der mit RiskSpectrum® ermittelten Minimalschnitte durchführen zu können. Unter goPSA wird erstmals eine ausführliche Benutzeranleitung für STREUSL bereitgestellt, die in /WIE 10/ dokumentiert ist. Außerdem wurden zusätzliche Startmasken für STREUSL entwickelt. Die Startmaske für das Teilprogramm STREUSL2, mit dem eigentlichen

Unsicherheits- und Importanzanalysen auf Basis der Minimalschnittdaten, die mit RiskSpectrum® ermittelt worden sind, durchgeführt werden, ist in Abb. 4-23 dargestellt. Zusätzlich zu den notwenigen Parametern, um die Analysen mit STREUSL durchführen zu können, kann über das Fenster ‘Minimalschnitt-Dateien‘ eine Liste dieser Dateien angegeben werden. Für alle angegebenen Dateien werden dann von goPSA Rechenfälle für STREUSL erzeugt und automatisch nacheinander abgearbeitet.

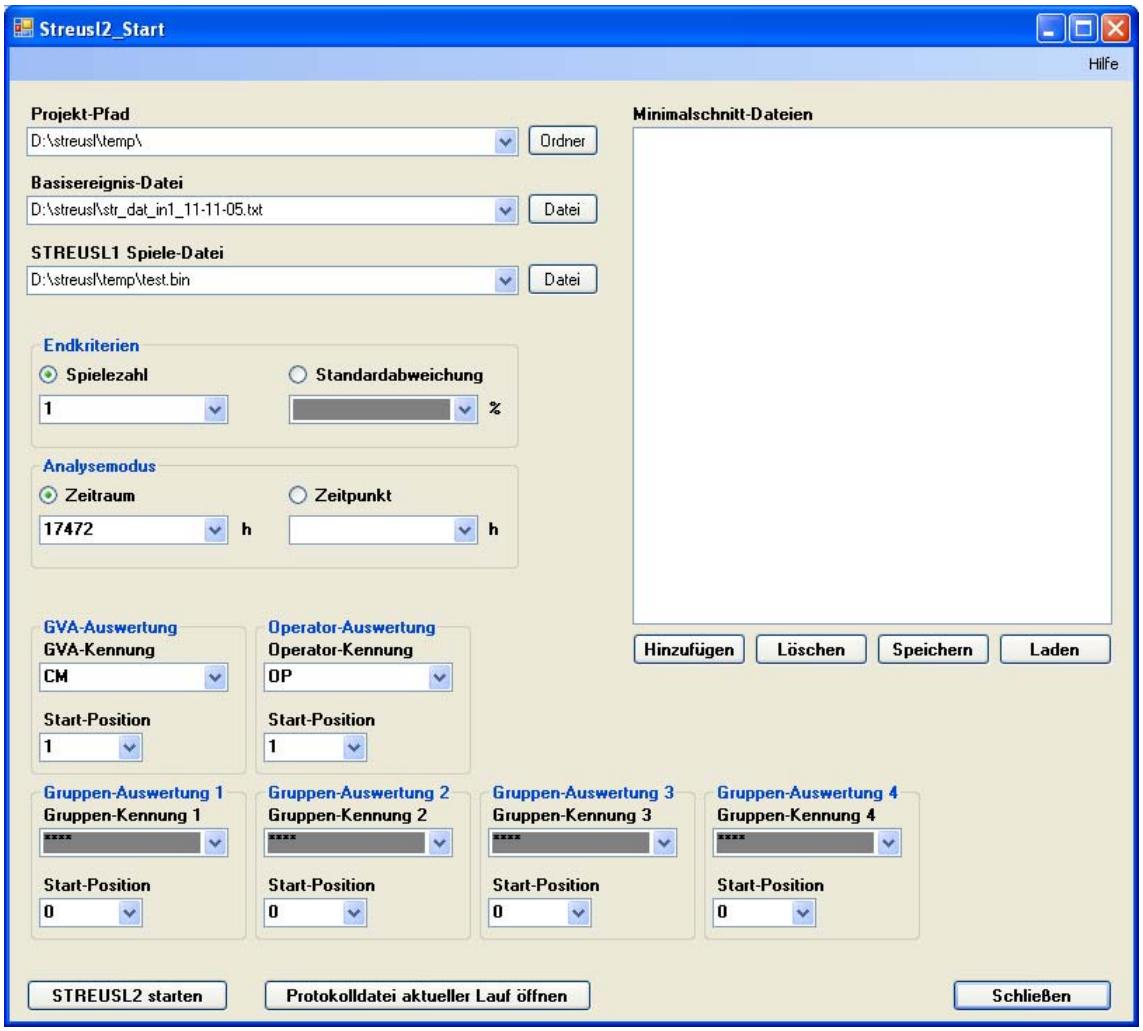


Abb. 4-23 Startmaske STREUSL2

4.4.5.2 CRAVEX

Für die Einbindung von CRAVEX in goPSA waren umfangreiche Vorarbeiten notwendig, da zu Beginn des Vorhabens RS1180 lediglich eine Prototyp-Version des Programms CRAVEX /GRS 03a/ zur Verfügung stand.

Vor diesem Hintergrund wurden unter anderem die folgenden Arbeiten durchgeführt.

- Es wurde eine integrierte Version von CRAVEX erstellt, mit welcher das Importieren eines RiskSpectrum®-Modells, das Einlesen des definierten Szenarios für eine übergreifende Einwirkung und die Auswertung und Berechnung des Gesamtmodells mit nur einem Programmaufruf erfolgt und keine manuellen Eingriffe mehr notwendig sind. Diese Arbeiten erforderten insbesondere die Integration des Programms RSAscii als Modul in CRAVEX.
- Für die Durchführung eines Screenings für ein Szenario einer übergreifenden Einwirkung wurde das eigenständige Programm RAVE aus dem entsprechenden Modul von CRAVEX entwickelt.
- Die Anzahl der Stellen für Komponentennamen, die von CRAVEX und RAVE ausgewertet werden, kann in vom Anwender als Eingabeparameter vorgegeben werden.
- Die vorhandene grafische Benutzeroberfläche für CRAVEX wurde umfangreich verbessert. Dazu wurden die Eingabemöglichkeiten für die Definition von Einwirkungen (so genannte Schadensbilder) verbessert und in ihrer Anwendung vereinfacht.

Zudem wurde eine Benutzerhilfe für CRAVEX erstellt, die aus der CRAVEX-Benutzeroberfläche heraus aufgerufen werden kann.

Mit der verbesserten CRAVEX-Benutzeroberfläche können die Daten zur Ermittlung der Schadensbilder bei übergreifenden Einwirkungen eingegeben werden. Dazu könne zum einen Raumausfallwahrscheinlichkeiten in einem bestimmten Raum bzw. Übergangswahrscheinlichkeiten für Folgewirkungen einer übergreifenden Einwirkung (z. B. Brandausbreitung) zwischen verschiedenen Räumen eingegeben werden. Dazu stehen die Kategorien ‘Erschütterungen‘ und ‘Brand‘ sowie ‘Barrierenintegrität‘ (für das Versagen von Brandschutzbarrieren) zur Verfügung (Abb. 4-24). Zusätzlich erlaubt es die CRAVEX-Oberfläche auf einfache Weise eine Teilmenge der Komponenten, die einem Raum zugeordnet sind, zu Komponentengruppen zusammenzufassen (Abb. 4-25) und diesen Komponentengruppen Versagenswahrscheinlichkeiten sowie Wahrscheinlichkeiten für Folgewirkungen sowohl zwischen Komponentengruppen als auch zwischen der Kategorie ‘Erschütterungen‘ und Komponentengruppen (Abb. 4-26) zu definieren. Das so definierte Schadensbild kann dann durch Aufruf von CRAVEX aus der Oberfläche heraus Abb. 4-27) gemeinsam mit dem Fehlerbaum-Modell der Anlage

ausgewertet werden. Damit erhält man eine probabilistische Bewertung von Versagenswahrscheinlichkeiten bzw. Schadenshäufigkeiten durch das Zusammenwirkungen übergreifender Einwirkungen, davon verursachter Folgeausfälle sowie möglicher Zufallsausfälle.

Zusätzlich kann über die CRAVEX-Oberfläche das Modul RAVE aufgerufen werden. Damit lässt sich das definierte Schadensbild unabhängig vom Fehlerbaum-Modell der Anlage auswerten. Auf diese Weise kann für unterschiedliche Szenarien die Ausbreitung von Folgewirkungen übergreifender Einwirkungen bestimmt werden. So können zum Beispiel bei einem Brandereignis in einem bestimmten Raum die dafür probabilistisch relevanten Ausbreitungspfade ermittelt und die Ausfallwahrscheinlichkeiten für die von einer Brandausbreitung betroffenen Räume bestimmt werden. An Hand der betroffenen Komponenten kann dann ein Screening-Verfahren durchgeführt werden.

Eine detailliertere Beschreibung der zu CRAVEX erzielten Ergebnisse findet sich im technischen Fachbericht /WIE 10/.

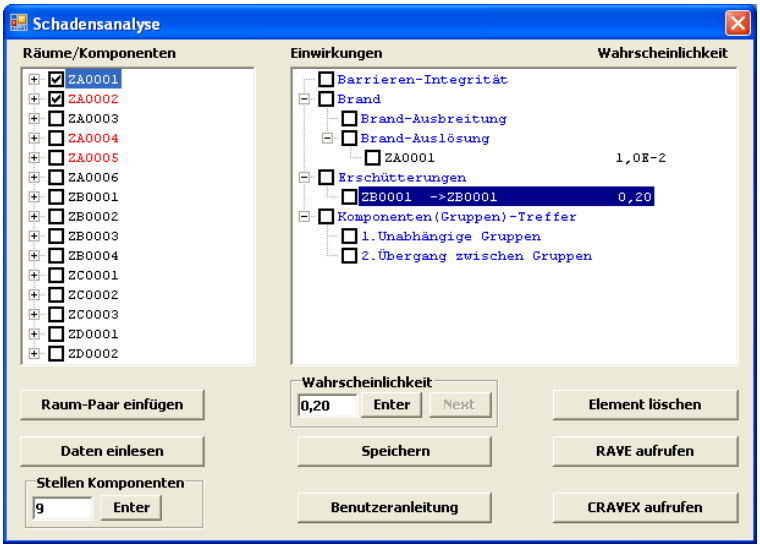


Abb. 4-24 Definition eines Raumpaars über CRAVEX-Oberfläche

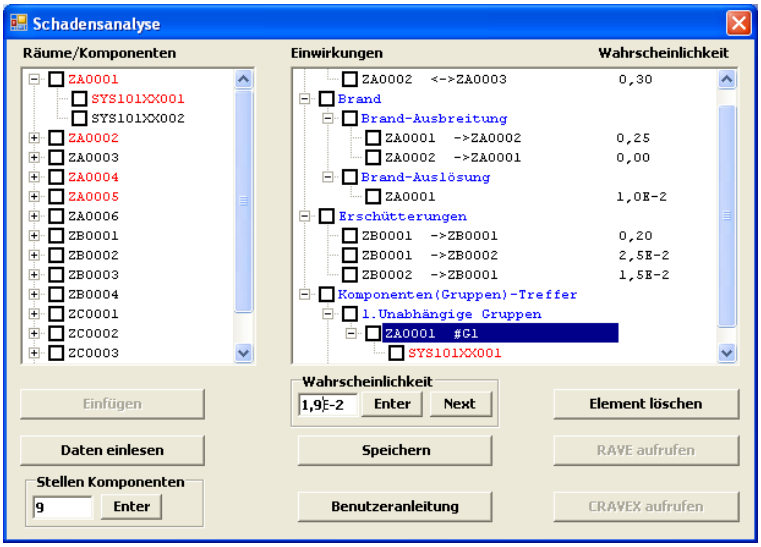


Abb. 4-25 Komponentengruppe in der CRAVEX-Oberfläche

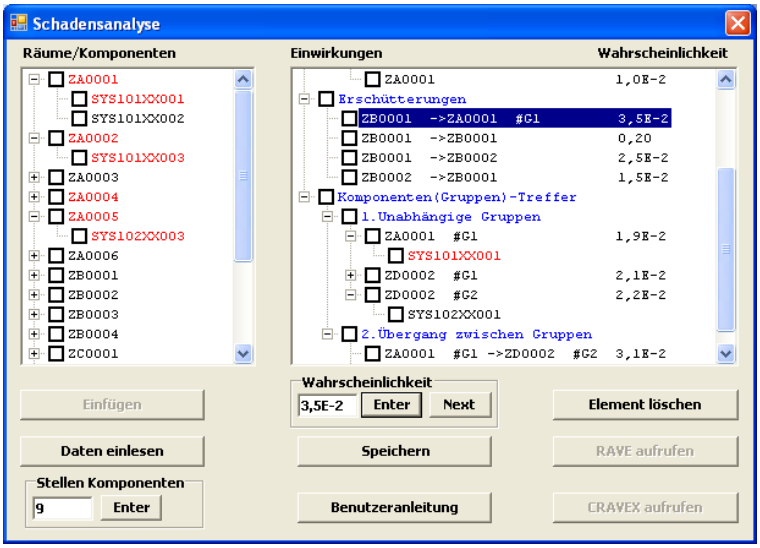


Abb. 4-26 Übergangswahrscheinlichkeiten für Komponentengruppen in der CRAVEX-Oberfläche

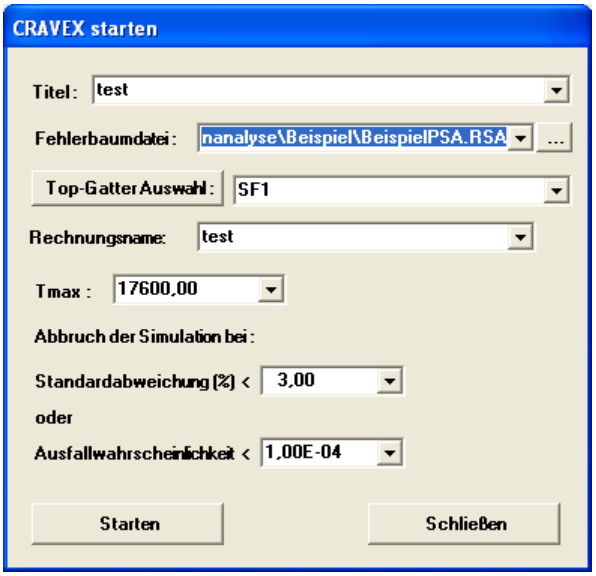


Abb. 4-27 Startmaske für CRAVEX

4.4.5.3 Weitere GRS-Hilfsprogramme

Unter goPSA sind Startmasken für die drei GRS-Hilfsprogramme RSAsii, EXCELRS und CmpFt realisiert worden. In Abb. 4-28 ist ein Beispiel für das Programm RSAsii gezeigt. Über diese Maske kann die Konsolenanwendung RSAsciiN.exe gestartet werden. Mit dem Pull-Down-Menü ‚Hilfe' lässt sich die im Rahmen dieses Teilvorhabens erstellte Benutzerhilfe aufrufen. Vergleichbare Startbildschirme und Benutzerhilfen sind auch für die Programme EXCELRS und CmpFt erstellt worden. Eine ausführlichere Beschreibung befindet sich in /WIE 10/.

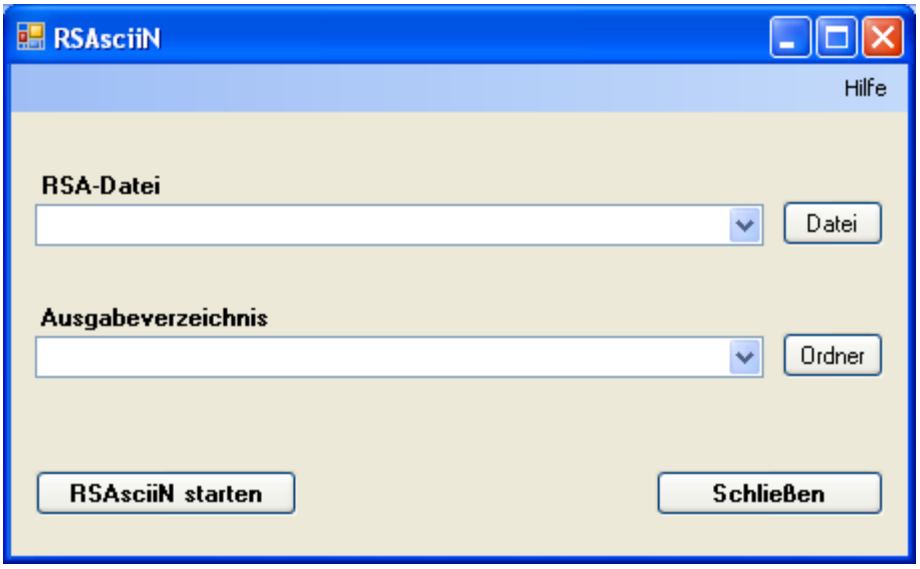


Abb. 4-28 Startmaske RSAscii

4.4.5.4 Benutzerhilfen und Vorlagen unter goPSA

Aus goPSA heraus könne Benutzerhilfen und Vorlagen zu den Themen HRA (*H*uman *R*eliability *A*nalysis)-Bewertungen nach THERP, Definition einer Schnittstelle zwischen Stufe 1 und Stufe 2, Dokumentation einer PSA der Stufe 1 sowie Berechnungen zu GVA-Modulen aufgerufen werden. Auf die wesentlichen Ergebnisse, die zum letzten Punkt erzielt wurden, wird in diesem Bericht kurz eingegangen. Für eine detailliertere Darstellung wird auf den technischen Fachbericht /WIE 10/ verwiesen.

Von der GRS wird eine explizite Modellierung von GVA-Ereignissen in Fehlerbäumen durchgeführt. Sofern eine GVA-Komponentengruppe aus mehr als ca. sechs Komponenten besteht, ist es jedoch praktisch nicht mehr sinnvoll möglich, die Ausfallkombinationen (z. B. der Ausfall der ersten fünf von insgesamt sieben GVA-Komponenten) jeweils einzeln zu modellieren. Daher werden die Ausfälle nach geeigneten Kriterien zu GVA-Modulen zusammengefasst. Dabei muss häufig berücksichtigt werden, dass die einzelnen GVA-Komponenten auf verschiedene Redundanzen verteilt sind und GVA-Ereignisse in einem Teilsystem unterschiedliche Auswirkungen auf die Verfügbarkeit eines Teilsystems haben können, je nachdem wie viele GVA-Komponenten des jeweiligen Teilsystems betroffen sind. Diese Verhältnisse werden über die so genannten Ausfalllogiken abgebildet.

Im Rahmen des Vorhabens RS1180 wurde nun ein allgemeines Verfahren entwickelt, mit welchem Ausfalllogiken mit einer beliebigen Zahl von Teilsystemen durch rekursive Rückführung auf Ausdrücke in zweiwertiger Boolescher Logik ausgewertet werden können. Zur Unterstützung der dafür notwendigen kombinatorischen Berechnungen wurde eine vorhandene MS EXCEL®-Anwendung aktualisiert. In der Anwendung KOMB8 kann zunächst eine Definition der Ausfalllogik in zwei Teilsystemen vorgenommen werden. Zudem wird spezifiziert, wie viele Komponenten einer GVA-Komponentengruppe zu einem der beiden Teilsysteme gehören (Abb. 4-29). Dann werden automatisch die verschiedenen Ausfallkombinationen und deren Anteil an der Gesamt-GVA-Wahrscheinlichkeit berechnet (Abb. 4-30). Mit diesen Informationen können dann mit einem ebenfalls in /WIE 10/ beschriebenen Verfahren die Zuverlässigkeitskenngrößen für die gewünschten GVA-Module geschätzt werden.

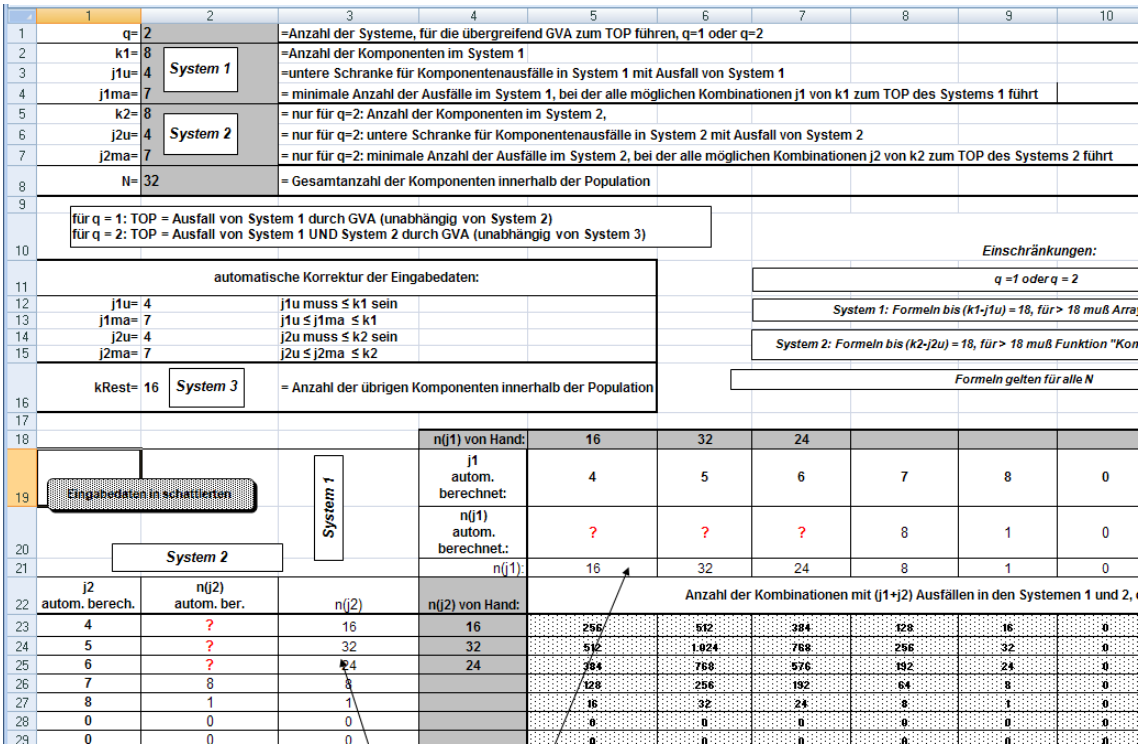
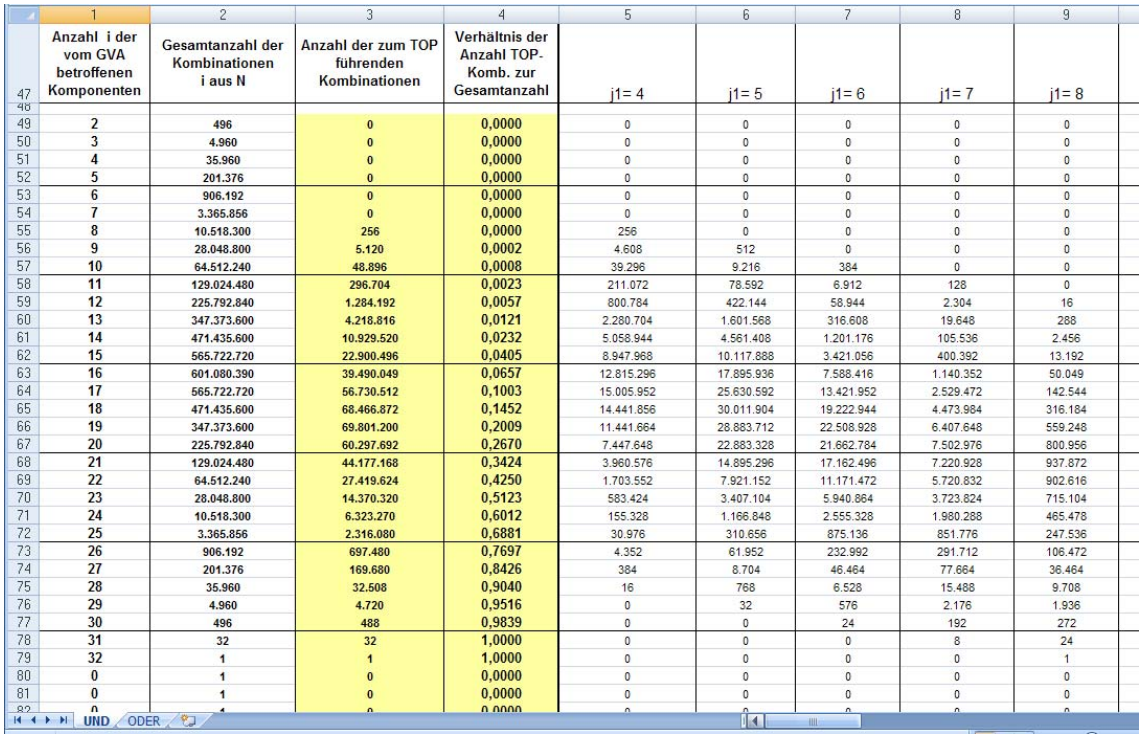


Abb. 4-29 Eingabedaten für MS EXCEL®-Anwendung KOMB8



	1	2	3	4	5	6	7	8	9
47	Anzahl i der vom GVA betroffenen Komponenten	Gesamtanzahl der Kombinationen i aus N	Anzahl der zum TOP führenden Kombinationen	Verhältnis der Anzahl TOP-Komb. zur Gesamtanzahl	j1= 4	j1= 5	j1= 6	j1= 7	j1= 8
49	2	496	0	0,0000	0	0	0	0	0
50	3	4.960	0	0,0000	0	0	0	0	0
51	4	35.960	0	0,0000	0	0	0	0	0
52	5	201.376	0	0,0000	0	0	0	0	0
53	6	906.192	0	0,0000	0	0	0	0	0
54	7	3.365.856	0	0,0000	0	0	0	0	0
55	8	10.518.300	256	0,0000	256	0	0	0	0
56	9	28.048.800	5.120	0,0002	4.608	512	0	0	0
57	10	64.512.240	48.896	0,0008	39.296	9.216	384	0	0
58	11	129.024.480	296.704	0,0023	211.072	78.592	6.912	128	0
59	12	225.792.840	1.284.192	0,0057	800.784	422.144	58.944	2.304	16
60	13	347.373.600	4.218.816	0,0121	2.280.704	1.601.568	316.608	19.648	288
61	14	471.435.600	10.929.520	0,0232	5.058.944	4.561.408	1.201.176	105.536	2.456
62	15	565.722.720	22.900.496	0,0405	8.947.968	10.117.888	3.421.056	400.392	13.192
63	16	601.080.390	39.490.049	0,0657	12.815.296	17.895.936	7.588.416	1.140.352	50.049
64	17	565.722.720	56.730.512	0,1003	15.005.952	25.630.592	13.421.952	2.529.472	142.544
65	18	471.435.600	68.466.872	0,1452	14.441.856	30.011.904	19.222.944	4.473.984	316.184
66	19	347.373.600	69.801.200	0,2009	11.441.664	28.883.712	22.508.928	6.407.648	559.248
67	20	225.792.840	60.297.692	0,2670	7.447.648	22.883.328	21.662.784	7.502.976	800.956
68	21	129.024.480	44.177.168	0,3424	3.960.576	14.895.296	17.162.496	7.220.928	937.872
69	22	64.512.240	27.419.624	0,4250	1.703.552	7.921.152	11.171.472	5.720.832	902.616
70	23	28.048.800	14.370.320	0,5123	583.424	3.407.104	5.940.864	3.723.824	715.104
71	24	10.518.300	6.323.270	0,6012	155.328	1.166.848	2.555.328	1.980.288	465.478
72	25	3.365.856	2.316.080	0,6881	30.976	310.656	875.136	851.776	247.536
73	26	906.192	697.480	0,7697	4.352	61.952	232.992	291.712	106.472
74	27	201.376	169.680	0,8426	384	8.704	46.464	77.664	36.464
75	28	35.960	32.508	0,9040	16	768	6.528	15.488	9.708
76	29	4.960	4.720	0,9516	0	32	576	2.176	1.936
77	30	496	488	0,9839	0	0	24	192	272
78	31	32	32	1,0000	0	0	0	8	24
79	32	1	1	1,0000	0	0	0	0	1
80	0	1	0	0,0000	0	0	0	0	0
81	0	1	0	0,0000	0	0	0	0	0
82	0	1	0	0,0000	0	0	0	0	0

UND ODER

Abb. 4-30 Ausfallkombinationen in KOMB8

4.5 Untersuchungen der PSA-Tauglichkeit des Integralcodes ASTEC© für Unfallanalysen unter Einbeziehung neuerer Erkenntnisse zum Radionuklidverhalten

Als erstes wichtiges Ergebnis der Analysen ist fest zu halten, dass mit beiden Codes die Rechnungen ordnungsgemäß durchgeführt werden konnten. Dies ist insofern erwähnenswert, als sowohl ASTEC als auch MELCOR teils mit Stabilitätsproblemen während der Rechnung zu kämpfen hatten. Die Numerik in beiden Programmsystemen zur Lösung großer Gleichungssysteme ist zwar hinsichtlich der mathematischen Stabilität optimiert und durch entsprechende Kriterien z. B. für die Auswahl des Zeitschritts abgesichert. Dennoch muss bei solch komplexen, miteinander wechselwirkenden mathematischen Modellen unter Einfluss großer Material- und Stoffwertdatenbanken immer mit Programmabbrüchen gerechnet werden. Dies gilt für alle Programmsysteme auf diesem Gebiet.

Die Rechnungen mit ASTEC V1.33 rev3 und MELCOR 1.8.6 YU wurden bis zu einer Problemzeit von 150000 s (~ 42 h) durchgeführt. Die Rechenzeiten bewegen sich abhängig vom unterstellten Störfallszenario zwischen 1 und 14 Tagen. Diese Werte stel-

len erfahrungsgemäß auch typische im Rahmen einer PSA Analyse der Stufe 2 auftretende obere und unter Grenzen der zu erwartenden Rechenzeiten dar. Gleichwohl könnten sich durch in manchen Bereichen sinnvoll erscheinende, aufwendigere Nodalisierungen auch noch längere Rechenzeiten ergeben, bei leichten qualitativen Verbesserungen der Rechenergebnisse. Deshalb bietet sich eine solche Vorgehensweise an, um Detailanalysen für ausgewählte Phänomene in begrenzten Bereichen des Reaktors (z. B. im Containment) durchzuführen.

Nachfolgend wird der Vergleich beispielhaft anhand des Unfalls ‘Totalausfall der Dampferzeugerbespeisung‘ diskutiert. Dazu wird neben dem Ausfall der Hauptspeisewasserpumpen zum Zeitpunkt t = 0 s gleichzeitig der Ausfall der An- und Abfahrpumpen unterstellt. Die Notbespeisung ist verfügbar, nach 8000 s Einspeisedauer wird auch hier ein Ausfall unterstellt. Im Verlaufe des Störfalls wird als anlageninterne Notfallmaßnahme das primärseitige Druckentlasten und Bespeisen durchgeführt bis die Flutbecken entleert sind.

Vor der Berechnung des eigentlichen Unfallszenarios wird eine sogenannte stationäre Rechnung vorgeschaltet. Dadurch wird sichergestellt, dass thermohydraulisch stabile Zustände in der modellierten Anlage herrschen und die Parameter der Realanlage eingehalten werden. Für ASTEC ist diese Startrechnung, die ursprünglich nur über einen Zeitraum von 500 s erfolgte, auf 30000 s ausgedehnt worden. Die Erfahrung zeigt speziell für ASTEC, dass eine lange stationäre Rechnung mit eingeschwungenem glattem Verlauf wichtiger thermohydraulischer Parameter wie Primärkreisdruck, Druckhalterfüllstand usw. eine im Allgemeinen stabilere transiente Rechnung ermöglicht. Mit Hilfe diverser Regelungen für die stationäre Phase wird über die Druckhalterheizung analog zum realen Reaktorbetrieb der Primärkreisdruck auf 15,7 MPa geregelt. Der Füllstand des Druckhalters wird vereinfachend über eine Pumpe auf den Anfangssollwert von 7,85 m angehoben und gehalten. Weiterhin wird der Dampferzeugerfüllstand geregelt und der abgeführte Dampfmassenstrom dem Speisewassermassenstrom angepasst.

Die entsprechenden Anlagenparameter vor Einleiten der Transiente sind Tab. 4-7 zu entnehmen. Es wurde generell eine gute Übereinstimmung der Parameter in ASTEC und MELCOR für wesentliche Parameter der Anlage erreicht. Gleichwohl ist festzuhalten, dass auch hier schon Unterschiede zu den verfügbaren Anlagendaten deutlich werden. Sie betreffen insbesondere die Sekundärseite der Dampferzeuger (Wasserinventar) sowohl für MELCOR als auch für ASTEC. Die Abweichungen in der Wasser-

und Dampfmasse im Vergleich zu den verfügbaren Anlagendaten ließen sich nicht klären. Diese sind teilweise auf unterschiedliche Nodalisierungen zurückzuführen, die sich jedoch auf Grund teilweise unterschiedlicher Modellierungen bei ASTEC und MELCOR nie vollständig vermeiden lassen. Ältere Vergleichsrechnungen von MELCOR mit dem Detailcode ATHLET-CD zeigten, dass mit diesen Werten anlagentypische Abläufe gut wiedergegeben werden /SON 01a/, so dass keine Änderungen vorgenommen wurden.

Tab. 4-10 Vergleich charakteristischer Anlagenparameter für MELCOR und ASTEC

	KONVOI Anlage		MELCOR	ASTEC
RDB und Kühlkreislauf				
Reaktordurchsatz bei Volllast	kg/s	19761,00	19713,00	19310,8
In DE übertragene Leistung	MW	3867,00	3781,00	3779,84
Wasservolumen (mit DH)	m^3	400,00	422,00	404,50
Druckverlust RDB und R-Kühlsystem	MPa	0,64	0,60	0,71
Druck am RDB-Eintritt	MPa	16,10	16,21	16,08
Druck am RDB-Austritt	MPa	15,80	15,89	15,74
Druckverlust RDB	MPa	0,33	0,32	0,48
KMT am RDB-Austritt	K	598,75	600,00	602,68
KMT am RDB-Eintritt	K	564,85	567,00	563,27
Aufheizspanne		33,90	33,00	39,41
Primärseite				
Durchsatz	kg/s	4940,25	4929,90	4827,7
mittlerer Druck	MPa	15,70	15,68	15,78
Eintrittstemperatur	K	564,65	566,40	564,01
Austrittstemperatur	K	598,75	600,00	597,72
Druckverlust	MPa	0,21	0,28	0,25
Sekundärseite				
Durchsatz	kg/s	524,00	511,32	511,04
FD-Druck	MPa	65,00	63,00	63,75
FD-Temperatur	K	554,15	552,00	552,74
Speisewassereintrittstemperatur	K	491,15	490,00	493,00
Gesamtvolumen	m^3	179,00	175,00	206,57

	KONVOI Anlage		MELCOR	ASTEC
Normal-Füllstand	m	12,20	12,20	10,75
Wasservolumen	m^3	63,40	98,33	84,29
Dampfvolumen	m^3	115,40	76,14	114,56

Ein erster Vergleich der transienten Phase lässt sich zunächst auf eine Gegenüberstellung von Zeitpunkten charakteristischer Ereignisse beschränken. Dazu sind im oberen Abschnitt der Tab. 4-8 Zeitpunkte für wichtige Ereignisse gelistet. Anlagenparameter für einen derartigen auslegungsüberschreitenden Störfallablauf liegen nicht vor. Ergebnisse eines ähnlichen, mit ATHLET-CD berechneten Ablaufs (Station Black-Out) könnten zum Vergleich für die Phase bis zur Einleitung der Druckentlastung des RKL aus /SON 01a/ herangezogen werden.

Tab. 4-11 Ereignisablauf und charakteristische Größen des Szenarios TLOFW

Ereignis	MELCOR	ASTEC
	Zeitpunkt	
Speisewasserausfall	0,0	0,0
RESA	30	12,7
Ausschalten der HKMP (DE-Level < 4 m)	1060	2274
Öffnen aller Druckhalterventile	6911	9219
Beginn HD-Einspeisung	7130	9474
Beginn heißseitige Akkueinspeisung	7620	9827
Beginn ND-Einspeisung	7970	10804
Ende HD- und ND-Einspeisung	13370	11224
Ende Akkueinspeisung (4x30m^3)	13830	11319
DIVA-Start (nur ASTEC)	-	17484
Erste Spaltproduktfreisetzung	19970	17999
Kernabsturz in untere Plenum	24984	22758
RDB-Versagen	33350	37792
Wassereinbruch in Reaktorgrube	56000	40000
Rechnung Ende	150000	150000
Physikalische Größe (integral)	**Menge [kg]**	
In-vessel Wasserstofffreisetzung	711	824
Verlagerte Corium-Masse in Reaktorgrube bei RDB-Versagen	174910	133592
Bis Rechnungsende verlagerte Corium-Masse aus	193430	277182

Ereignis	MELCOR	ASTEC
	Zeitpunkt	
RDB		
Ex-Vessel Wasserstofffreisetzung durch MCCI	2600	2310
Rekombinierter Wasserstoff im Sicherheitsbehälter	1800	2024

- Frühe Störfallphase

Das Szenarium lässt sich wie folgt charakterisieren. Mit dem Eintritt des Ereignisses ‘Totalausfall der Speisewasserversorgung‘ verdampft das Wasser auf der Sekundärseite der Dampferzeuger (DE) recht schnell und der Füllstand sinkt rapide ab, da vereinfachend unterstellt wurde, dass die Reaktorabschaltung erst bei einem DE-Füllstand < 9 m erfolgt. Dies erfolgte in ASTEC deutlich früher, als in MELCOR, u. a. auch wegen des niedrigeren Anfangsfüllstandes. Während der heftigen Verdampfung steigt zugleich sekundärseitig der Druck, wodurch bei Erreichen von ~ 8,5 MPa das Teilabfahren mit 100 K/h auf 7,5 MPa eingeleitet wird. Die Füllstände in den DE fallen wegen fehlender Zufuhr von Speisewasser ständig weiter. Bei einem DE-Füllstand < 4 m werden die Hauptkühlmittelpumpen (HKMP) als unterstellte Handmaßnahme abgeschaltet, wodurch der Energieeintrag der laufenden Hauptkühlmittelpumpen entfällt und das verbliebende Inventar der DE für einen etwas längeren Zeitraum zur Wärmeabfuhr genutzt werden kann. Die Abb. 4-31 zeigt den Füllstand für die Sekundärseite der Dampferzeuger für ASTEC und MELCOR. Bei qualitativ vergleichbarem Verlauf des Ausdampfens bei MELCOR und ASTEC errechnet ASTEC ein um ca. 2000 s verspätetes Ausdampfen der Dampferzeuger verglichen mit MELCOR. Dieses verspätete Ausdampfen ist auf die (unrealistische) Verlagerung von angesammeltem Wasser aus dem oberen Bereich der Dampferzeuger zurückzuführen. Der Grund für diese Ansammlung von Wasser in diesem Bereich des DE in ASTEC muss bei späteren Analysen gesucht werden. Das Ausdampfen der DE in MELCOR verläuft etwas schneller, verglichen mit früheren Analysen (siehe /SON 01a/), ist aber vor allem bedingt durch die vereinfachte Simulation der Reaktorabschaltung zu einem etwas späteren Zeitpunkt.

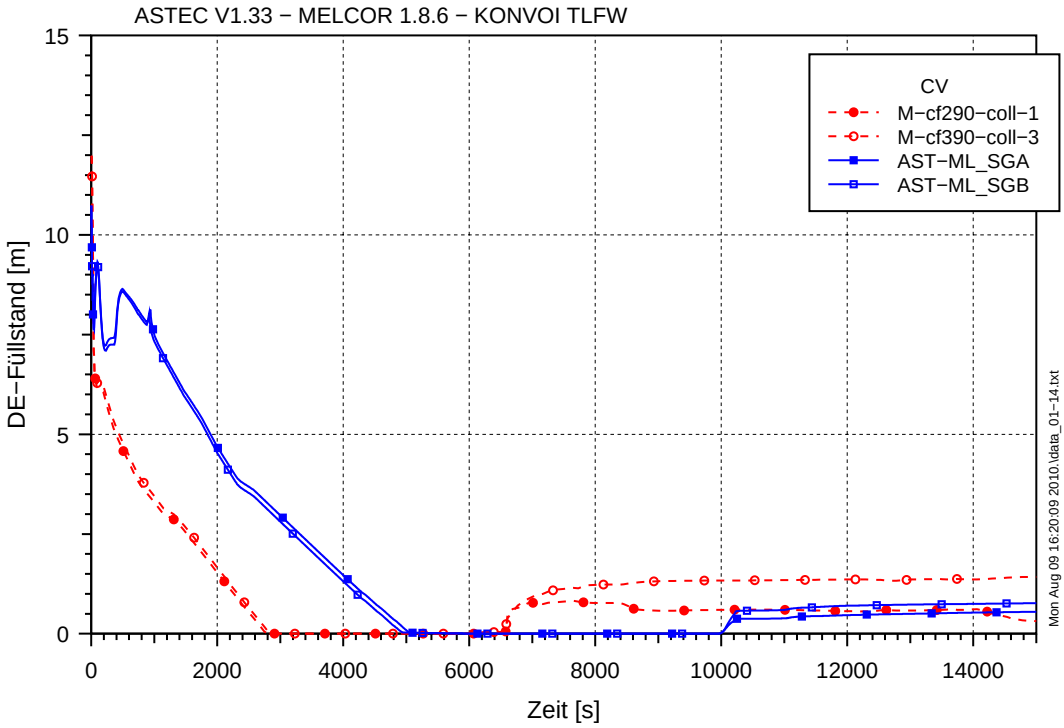


Abb. 4-31 Dampferzeuger-Füllstände für Ein- und Dreifachloop für ASTEC und MELCOR beim Störfall Totalausfall Speisewasser.

Der Einfluss der Sekundärseite auf die Primärseite infolge der veränderten Wärmeabgabe vom Primär- zum Sekundärkreislauf spiegelt sich direkt auch im Druckverlauf der Primärseite wider. Die entsprechenden Druckverläufe sind in Abb. 4-32 für beide Rechnungen dargestellt.

Generell ist aus den Daten in Tab. 4-10 ersichtlich, dass ASTEC zu Beginn der Rechnung eine deutlich langsamere Transiente rechnet, so wird das Abschalten der Hauptkühlmittelpumpen (HKMP) auf Grund eines unterschiedlichen Füllstandabfalls in den Dampferzeugern um ca. 1200 s verspätet gerechnet.

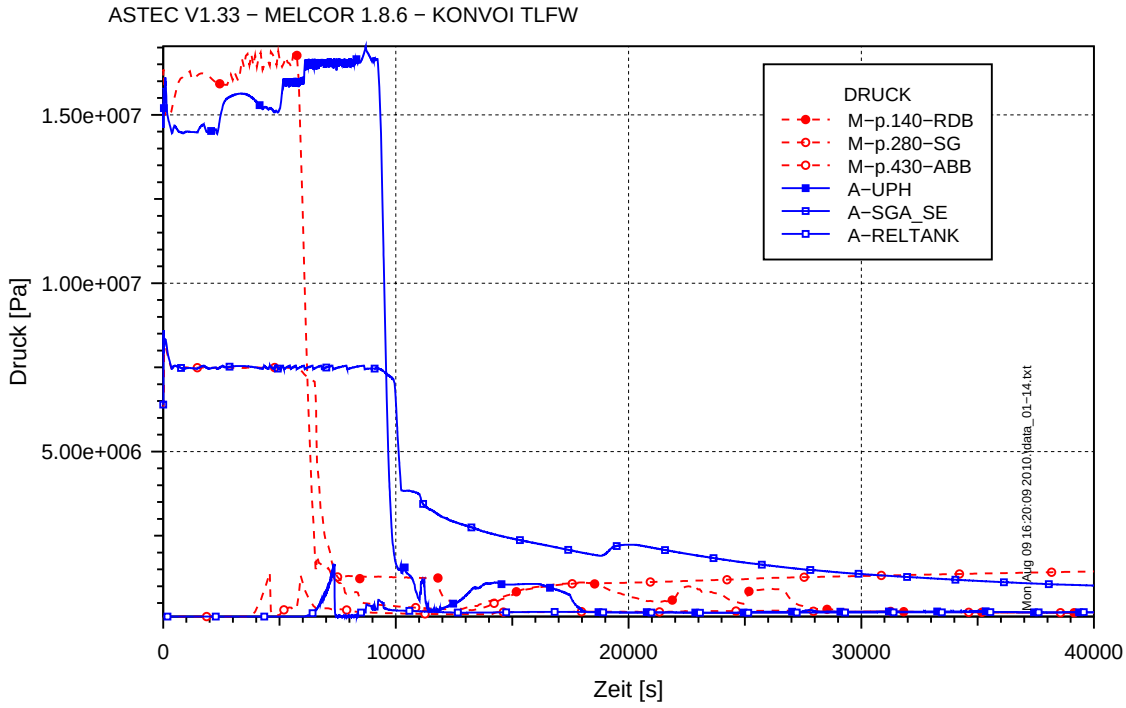


Abb. 4-32 Druck im Primär- und Sekundärkreislauf für ASTEC und MELCOR

Da während der Ausdampfphase nicht mehr genügend Energie an die DE abgeführt werden kann, steigt auch im Primärkreis der Druck an. Ab 16,4 MPa kann der Druckanstieg zunächst durch zyklisches DH-Sprühen begrenzt werden. Erst nach Anstieg des DH-Füllstands auf h_{DH} > 11 m erfolgt das ‘AUS‘-Signal für alle betrieblichen Einspeisesysteme in den Primärkreis (Primärkreisabschluss). Vorher war der DH-Füllstand stets > 2,28 m und es war noch zu keiner Freisetzung in den SB gekommen. Der dann einsetzende Druckanstieg führt schließlich zum Ansprechen des DH-Abblaseventils, das durch zyklisches Öffnen den RKL-Druck auf 16,7 MPa begrenzt. Auch das Öffnen der Druckhalter-Abblase- und Sicherheitsventile als Konsequenz des primärseitigen Druckaufbaus infolge Volumenexpansion des primärseitigen Kühlmittels wird bei ASTEC demzufolge später errechnet.

Nach Erreichen des Kriteriums ‘RDB-Füllstand < MIN3‘ (~ Mitte HKML) wird als primärseitige anlageninterne Notfallmaßnahme die primärseitige Druckentlastung durch Öffnen aller Druckhalterventile eingeleitet. Die entsprechenden Massenströme sind in Abb. 4-33 aufgetragen und bestätigen die Erkenntnis, dass durch das verzögerte Ausdampfen der DE letztendlich auch die primärseitige Maßnahme der Druckentlastung verzögert eingeleitet wird. Durch die rasche Druckentlastung kann der Druck dann bis auf den Ansprechdruck der Hochdruck-Sicherheitseinspeisung bei 11,0 MPa abge-

senkt werden, so dass nachfolgend Wasser aus den Flutbehältern in den heißen Strang des Dreifachloops eingespeist wird. Mit weiter fallendem Druck speisen ab 2,5 MPa dann auch die passiven Druckspeicher (DS) ein. Dabei speisen nur die heißseitigen DS ein, da die kaltseitigen 500 s nach Störfalleintritt abgesperrt wurden.

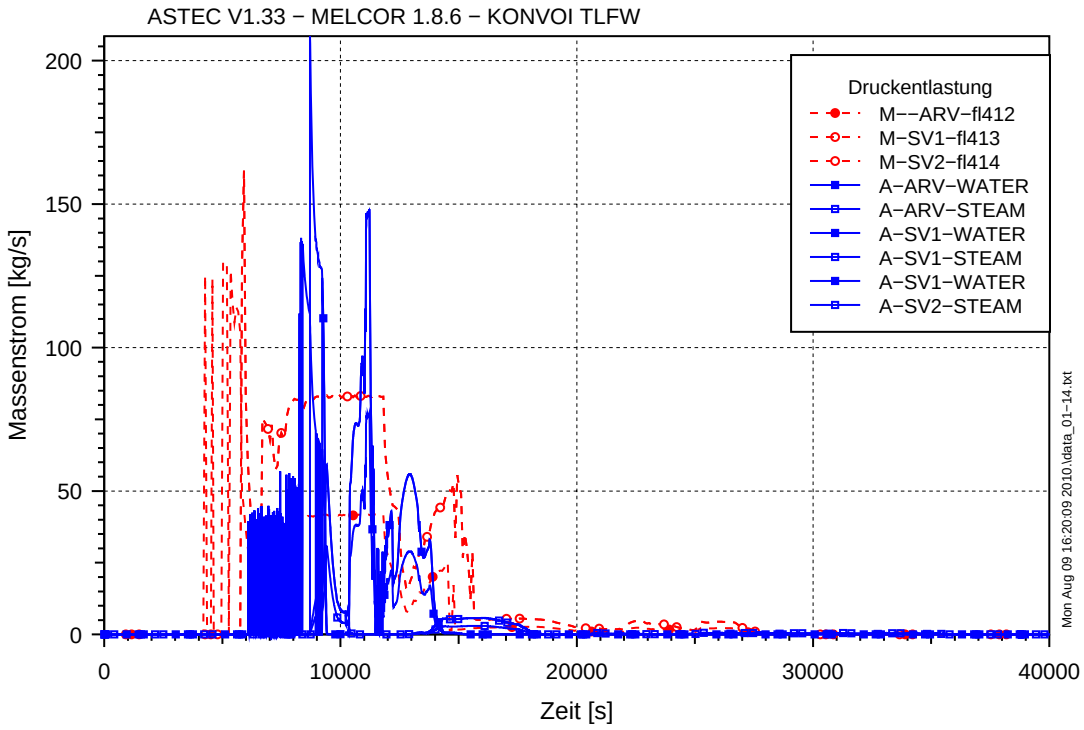


Abb. 4-33 Massenstrom über die Abblase- und Sicherheitsventile des Druckhalters für ASTEC und MELCOR beim Störfall Totalausfall Speisewasser.

- Kernzerstörungsphase

Im weiteren Verlauf wird bei Unterschreiten von 1,0 MPa zusätzlich vom Niederdruckeinspeisesystem Kühlmittel sowohl in den heißen als auch in den kalten Strang des Dreifach-Loops eingespeist. Nach Leerpumpen der Flutbecken wird die Umschaltung auf Sumpfansaugung als versagend unterstellt, was zum Ausfall aller aktiven Einspeisesysteme führt. Mit zunehmendem Ausdampfen des Kerns heizt dieser sich dann weiter auf und es kommt nachfolgend zur Kernzerstörung. Dadurch kann im nachfolgenden Zeitraum die Kernaufheizung beginnen, was letztendlich zum RDB-Versagen führt; ASTEC errechnet das RDB-Versagen ca. 4442 s nach MELCOR.

Auf Grund der unterschiedlichen Abläufe der Kernaufheizung und -verlagerung, die einerseits direkt auf die unterschiedliche Modellierung der Phänomene in dieser Phase

zurückgeführt werden können, andererseits aber auch indirekt durch die Ereigniskette im Verlaufe des Störfalls selbst beeinflusst werden (z. B. Einspeisedauer der Sicherheitseinspeisesysteme), sind auch die mit der Kernzerstörung einhergehenden Prozesse wie Wasserstofffreisetzung und Aerosol- und Spaltproduktfreisetzung teils unterschiedlich. Ein quantitativer Vergleich ist dadurch nur schwer möglich.

Dabei ist zusätzlich zu berücksichtigen, dass das ASTEC Modul zur Beschreibung der Kernzerstörung (DIVA) einigen Einschränkungen bezüglich spezifischer Zuständen einer Zweiphasenströmung wie Wassereintrag und Gegenströmung (CCFL) im Kern unterliegt. Es gibt keine Bewegungsgleichung für die flüssige Phase (Wasser). Bei Überhitzung des Wassers wird dieses sofort verdampft. Dies kann insbesondere in der späten Phase der Kernzerstörung zu Abweichungen führen, wenn zu diesem Zeitpunkt massive Wassereinspeisungen in den Kern auftreten.

Die in die Reaktorgrube verlagerte Corium-Masse bei RDB-Versagen macht bei ASTEC ca. 77 % der mit MELCOR berechneten Masse aus (d. h. 134 t). Die ca. 175 t Kernmaterial, die bei MELCOR bei RDB-Versagen verlagert werden, entsprechen weitestgehend einer kompletten Kernzerstörung. Bis zum Rechnungsende werden bei MELCOR weitere knapp 20 t verlagert. Dies ist insofern erstaunlich, weil ASTEC eine wesentlich längere Kernzerstörungsphase – gerechnet vom Zeitpunkt der ersten Freisetzung von Spaltprodukten infolge Hüllrohrversagens bis zum RDB-Versagen – errechnet (19793 s bei ASTEC und 13380 s bei MELOR). Somit könnte theoretisch auch mehr Material ins untere Plenum verlagert werden. Von Einfluss ist bei ASTEC dabei jedoch neben der Modellierung der maximalen Temperaturen, bei der die Zerstörung der Brennstäbe stattfindet, die Modellierung der unteren Kerntrageplatte, die bis zu ihrem Versagen die Schmelze im unteren Kernbereich zurückhält (vgl. Abb. 4-34). Diese Trageplatte wurde in Anlehnung an die MELCOR Nodalisierung eingefügt, ein partielles Versagen der Platte kann derzeit aber noch nicht gerechnet werden. Dies hat natürlich einen Einfluss auf den Zeitpunkt des RDB-Versagens. Durch die verzögerte Verlagerung von Kernmaterial ins untere Plenum wird auch die Aufheizung der RDB-Bodenkalotte entsprechend verzögert eingeleitet. Konsequenterweise führt dies dann bei ASTEC zu einem um 4442 s verzögerten RDB-Versagen.

Der Einfluss der Kernaufheizung und -zerstörung wird auch deutlich bei der Wasserstofffreisetzung infolge Oxidation des Zirkaloy-Hüllrohrmaterials sowie der Eisenstrukturen im Kernbereich. Ist bei beiden Rechnungen noch der Zeitpunkt des Beginns der Oxidation in guter Übereinstimmung errechnet, weichen im nachfolgenden Zeitraum

die Ergebnisse stark voneinander ab. Dies bezieht sich weniger auf die insgesamt freigesetzte Masse an Wasserstoff sondern vielmehr auf die Entstehung von Wasserstoff als Folge der Eskalation der Hüllrohr-Oxidation bzw. derjenigen des Stahls der den Kern umgebenden Strukturen. ASTEC errechnet in diesem Fall eine wesentlich höhere Freisetzung von Wasserstoff aus der Stahloxidation in einem späten Stadium der Kernzerstörung. Dies erscheint nach derzeitigen Erfahrungen zwar nicht unmöglich aber auch nicht realistisch.

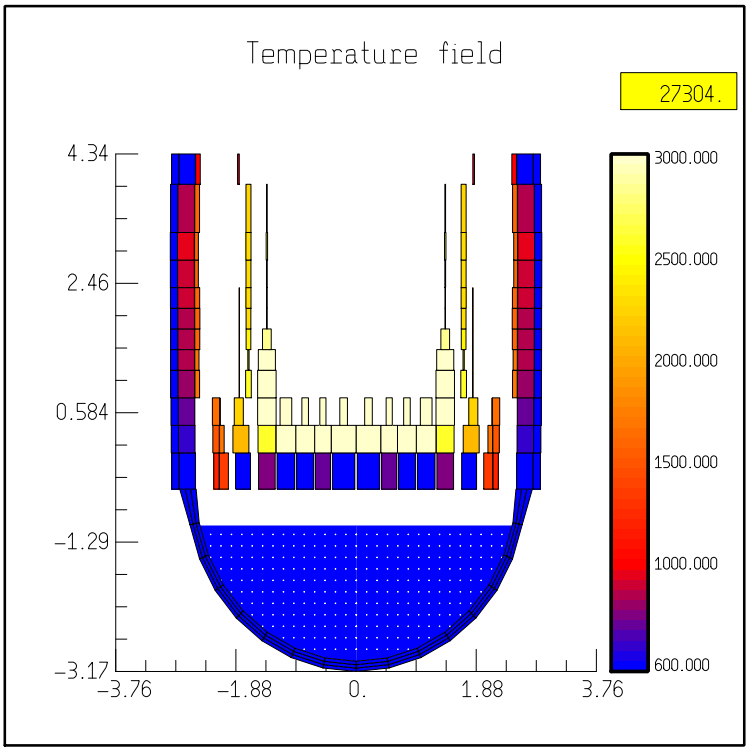


Abb. 4-34 ASTEC Visualisierung des Temperaturfeldes für RDB- und Kernstrukturen. Dargestellt sind die entsprechend der Temperaturskala farbcodierten Strukturen sowie der Wasserfüllstand im unteren Plenum

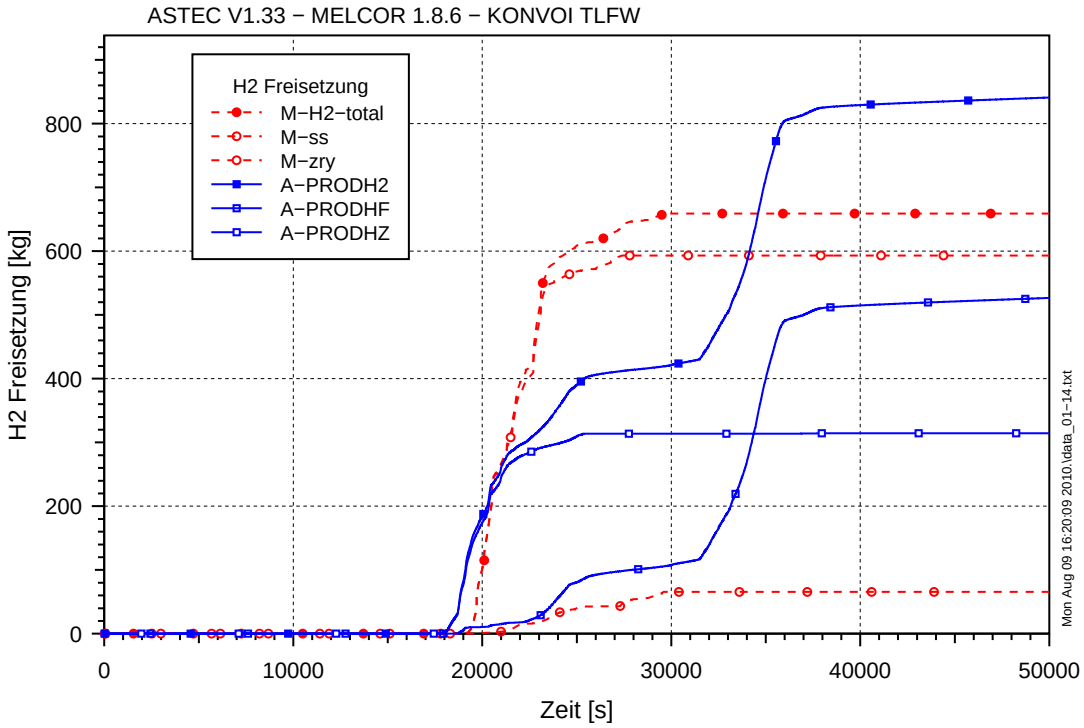


Abb. 4-35 Wasserstofffreisetzung im Kern (gesamt, aus Zr-Oxidation sowie aus Eisen-Oxidation) für ASTEC und MELCOR beim Störfall ‘Ausfall Speisewasser‘

Für die Ex-Vessel Phase nach RDB-Versagen errechnet ASTEC eine weitere verzögerte Verlagerung von Kernmaterialien aus dem RDB in die Reaktorgrube, so dass insgesamt bis zum Rechnungsende knapp 277 t verlagert werden. Bei MELCOR werden direkt bei RDB Versagen 175 t in die Reaktorgrube verlagert, im nachfolgenden Zeitraum nur noch knapp 20 t, da der Kern bereits nahezu komplett zerstört war.

Bezüglich der Verhältnisse im Containment lässt sich folgendes festhalten. Qualitativ ist eine gute Übereinstimmung festzuhalten, ersichtlich am Druckverlauf im Containment. Die Zustände im Sicherheitsbehälter werden außer von der Schmelze-Beton Wechselwirkung auch von der Energie geprägt, die mit der Strömung sowohl über die DH-Ventile als auch über die Bruchfläche im RDB in die Reaktorgrube gelangt.

In Abb. 4-36 sind die Druckverläufe in einigen ausgewählten Räumen des SB für MELCOR und ASTEC dargestellt. Charakteristisch für die Zustände in der Anfangsphase im SB ist der rasche Druckaufbau auf ca. 0,30 MPa nach dem Bruch der Berstscheibe des DH-Abblasebehälters. Er fällt zunächst wieder infolge des Wärmeaustauschs mit den kalten Strukturen und der damit verbundene Kondensationsprozesse

insgesamt ab. Im weiteren Verlauf wird der Druck im Wesentlichen durch den Dampfaustrag aus dem Primärkreis in den Sicherheitsbehälter geprägt. Der Druck in der Reaktorgrube (in MELCOR) bleibt relativ niedrig, da unterstellt wurde, dass sie bis zum Versagen des RDB-Bodens von den übrigen Räumen im SB abgetrennt ist. Mit dem Versagen des RDB-Bodens wird eine große Verbindung zu den unteren Anlagenräumen des SB entlang der HKML freigelegt. Der Druck in den SB-Räumen nimmt wieder kontinuierlich zu. Ursache hierfür ist die Freisetzung von Gasen beim Aufschmelzen des Betons. Bei ASTEC hat die Reaktorgrube von vornherein eine offene Verbindung zu den angrenzenden Räumen, so dass hier ein Druckausgleich stattfindet. Diese Abweichungen von ASTEC und MELCOR wurden erst nach Rechnungsabschluss festgestellt, sind aber für den Unfallablauf nebensächlich, so dass auf eine Wiederholungsrechnung verzichtet wurde.

Der Austritt des heißen Schmelzmaterials aus dem RDB bewirkt einen rapiden Temperaturanstieg in der Reaktorgrube. Durch die Erosion des Betons der Reaktorgrube dringt die Schmelze axial und radial in das Fundament ein und kann in Kontakt mit Wasser in der Lüftungsspinne oder im Ringspalt um den biologischen Schild kommen. Wie in der PSA der Stufe 2 für GKN-2 /SON 01/ wurde pessimistisch unterstellt, dass dann ein plötzlicher und anhaltender Wassereinbruch in die Reaktorgrube erfolgt. Das Wasser bedeckt die Schmelze und bewirkt einen Temperatureinbruch in der Reaktorgrube sowie eine anhaltende Verdampfung. Im Gegensatz zu MELCOR, bei dem der Wassereinbruch intermittierend plötzlich und dauerhaft auf die Schmelze erfolgt, wurde dieser Vorgang bei ASTEC vereinfachend modelliert und nur konstanter Wassermassenstrom unterstellt. Dadurch ergeben sich Unterschiede im nachfolgenden Druckverlauf. Bei ca. 120000 s ist bei ASTEC ein deutlicher schnellerer Druckanstieg ersichtlich, der aus der Änderung der Wärmeübertragung zwischen Schmelzeoberfläche und überdeckendem Wasserpool resultiert und auf eine nicht realistische Berechnung der Wärmeübertragungsoberfläche zurück zu führen ist.

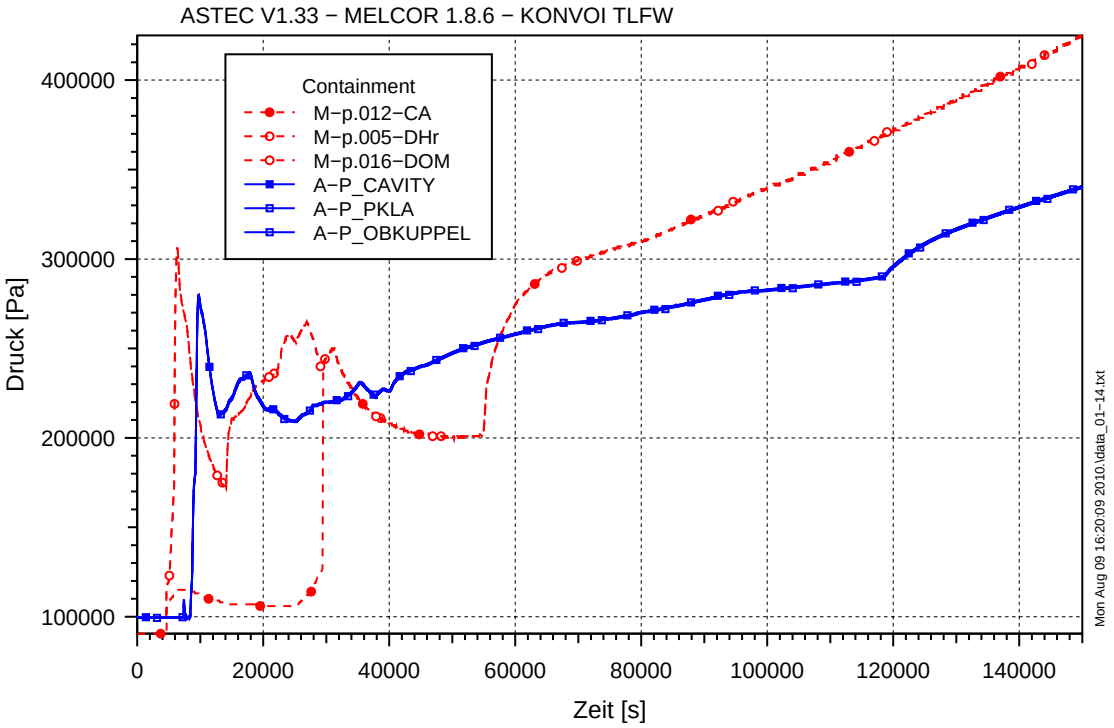


Abb. 4-36 Druck in ausgewählten Containmenträumen: Reaktorgrube, Druckhalterraum und Dom für ASTEC und MELCOR beim Störfall Totalausfall Speisewasser.

- Spaltproduktverhalten

Für den hier diskutierten Störfall ist auch ein Vergleich des Spaltproduktverhaltens durchgeführt worden. Der Vergleich ist hier auf die Darstellung integraler Werte bei Rechnungsende begrenzt. Aufgrund der Unterschiede in der Kernzerstörungsphase sind zeitliche Darstellungen mit der verwendeten Version ASTEC V1.33 noch wenig aussagekräftig. Deutliche Verbesserungen werden mit der jetzt verfügbaren Version ASTEC V2.0 erwartet.

Einen Überblick über die verschiedenen Spaltproduktgruppen und ein Vergleich mit MELCOR über die Freisetzung ist in Tab. 4-12 gegeben. Die Spalte ‚Freisetzung gesamt' gibt an, welcher relative Anteil des jeweiligen Elements bzw. der durch dieses Element repräsentierten Spaltproduktklasse aus dem Brennstoff freigesetzt worden ist. Der Bezugspunkt ist dabei jeweils das Ausgangsinventar entsprechend Tab. 4-13.

Tab. 4-12 Vergleich der Spaltproduktverteilung zwischen MELCOR und ASTEC

	MELCOR	ASTEC	MELCOR	ASTEC	MELCOR	ASTEC	MELCOR	ASTEC	MELCOR	ASTEC
	Gesamt aus Kern		Verbleibend im Kern		Im RKL		Im Containment		Außerhalb Containmen	
Xe	9,91E-01	9,99E-01	2,29E-05	1,03E-03	9,45E-04	3,32E-03	9,87E-01	9,96E-01	2,93E-03	3,99E-03
CsOH	9,85E-01	9,99E-01	3,34E-05	1,01E-03	1,18E-01	1,35E-01	8,67E-01	8,64E-01	1,14E-04	2,26E-05
Ba	4,20E-02	6,21E-03	9,43E-01	9,90E-01	4,29E-04	5,86E-03	4,15E-02	3,56E-04	3,37E-06	0,00E+00
Te	9,08E-01	9,75E-01	8,05E-02	2,52E-02	5,39E-02	2,78E-01	8,54E-01	6,97E-01	1,01E-04	1,70E-05
Ru	4,75E-02	1,47E-04	9,37E-01	9,58E-01	6,69E-03	1,02E-04	4,08E-02	4,52E-05	5,40E-06	0,00E+00
Mo als Element	5,39E-02	1,22E-01	9,46E-01	8,61E-01	2,27E-04	3,01E-02	1,35E-03	9,22E-02	1,73E-07	2,46E-06
Mo als Cs2MoO4					1,78E-03		5,06E-02		3,26E-06	
Ce	3,47E-03	3,71E-05	9,81E-01	9,59E-01	3,86E-06	1,16E-05	3,46E-03	2,56E-05	1,26E-07	0,00E+00
La	3,62E-03	3,75E-05	9,81E-01	9,59E-01	3,19E-04	1,19E-05	3,30E-03	2,56E-05	4,19E-07	0,00E+00
U	5,10E-04	3,71E-05	9,76E-01	9,59E-01	6,96E-05	1,06E-05	4,40E-04	2,65E-05	5,74E-08	2,68E-08
Cd (Sb)	6,32E-01	9,82E-01	3,57E-01	1,76E-02	7,21E-02	1,31E-01	5,60E-01	8,52E-01	7,35E-05	0,00E+00
Sn	6,07E-01	3,84E-05	3,81E-01	9,59E-01	7,19E-02	2,79E-05	5,35E-01	1,05E-05	7,06E-05	0,00E+00
CsI (I)	9,66E-01	9,99E-01	2,34E-02	1,04E-03	4,06E-02	1,04E-03	9,25E-01	8,58E-01	1,03E-04	1,45E-05
Die Freisetzungsanteile wurden auf das Anfangsinventar der radioaktiven Spaltprodukte normiert										

Tab. 4-13 Ausgangsinventar radioaktiver Spaltprodukte für die LOFW-Analyse mit MELCOR /SON 01/

Klasse	Bezeichnung		Gesamtmasse [kg]	Masse im BE-Gasspalt [kg]
1	XE	Edelgase	7,308 E+02	1,133 E+02
2	CS	Alkalimetalle	3,976 E+02	1,053 E+02
3	BA	Alkalische Erden	2,985 E+02	1,660 E-04
4	I2	Halogene	3,132 E+01	2,770 E-01
5	TE	Tellur	6,652 E+01	3,310 E-03
6	RU	Platinoide	5,232 E+02	-
7	MO	Trans-Metalle	5,163 E+02	-
8	CE	Tetravalente Gruppe	1,974 E+03	-
9	LA	Trivalente Gruppe	9,986 E+02	-
10	U	Uran	9,979E+04	-
11	CD	Leichtflüchtige Hauptgruppe	1,525 E+01	1,100 E-04
12	SN	Schwerflüchtige Hauptgruppe	1,723 E+01	-
16	CsI	CsI	0,000 E+00	-

Die MELCOR Gruppe Cd wurde in ASTEC mit dem Element Antimon (Sb) aus derselben Gruppe berechnet. In MELCOR gibt es keine Gruppe für Iod (I), sondern es wird angenommen, dass sämtliches Iod zu CsI bei der Freisetzung im Kern weiterreagiert. Daher erfolgt der Vergleich von CsI mit I in ASTEC.

Vergleicht man die einzelnen relativen Freisetzungen, so gibt es für leicht flüchtige Elemente (Xe-, Cs-, Te- sowie die I- bzw. CsI-Gruppe) eine gute Übereinstimmung zwischen ASTEC und MELCOR. Die Freisetzung aus dem Kern liegen zwischen 93,9 % für die Cs-Gruppe (MELCOR) und 99,9 % für die Edelgase (ASTEC). Die schwerer flüchtigen Elemente weisen, wenn auch tendenziell zufriedenstellend, teilweise stärkere Unterschiede bei den Freisetzungsanteilen aus dem Kern auf. Allerdings liegen diese generell bei sehr kleinen Werten weit unterhalb 1 % des Ausgangsinventars. Für die Elemente Ru und Ce liegen die Ergebnisse um zwei Größenordnungen auseinander. Für die Klasse Sn ergibt sich sogar ein Unterschied von vier Größenordnungen. Für die Elemente Ba, La, U und Cd liegen die Unterschiede bei einer Größenordnung.

Die Freisetzung des mittelflüchtigen Mo erscheint sehr hoch. Ähnliche Tendenzen wurden für ASTEC aber auch schon im Rahmen der Nachrechnung des Experimentes FPT1 aus der PHEBUS-Versuchsreihe festgestellt.

Hier sind weitere Analysen angezeigt, um die Unterschiede genauer zu untersuchen. In MELCOR könnten prinzipiell auch andere Modelle für die Freisetzung aus dem Kern getestet werden. Unterschiede werden z. B. durch ein unterschiedliches Abschmelzen des Kerns bei unterschiedlichen Spitzentemperaturen hervorgerufen. Gleichwohl sind auch unterschiedliche Modelle und Ansätze für die Freisetzung der einzelnen Elemente in den Codes verankert.

Mit Blick auf den Quellterm an die Umgebung sind radiologisch Cs und Sr wegen langer Halbwertszeiten von besondere Bedeutung, während z. B. die Jodisotope für radiologische Belastungen in den ersten Tagen nach einem schweren Störfall besonders zu beachten sind. Ein Vergleich bezüglich der Jodmodellierung ist nicht möglich, da in MELCOR keine detaillierte Jodmodellierung erfolgte. Für ASTEC wurde das Jodmodul IODE aktiviert um die den Jodquellterm beeinflussenden Wechselwirkungen der verschiedenen Jodspezies mit den Strukturen des Containments (Stahl oder Beton, trocken oder nass, gestrichen oder ungestrichen) und insbesondere in Wasservorlagen (Sumpf) zu modellieren. Mangels validierter Modelle in MELCOR konnte kein Vergleich vorgenommen werden. Bei ASTEC konnte die prinzipielle Anwendung gezeigt werden, auf eine gezielte Auswertung wurde verzichtet, da der Aufwand zur Bewertung weit über das in diesem Arbeitspunkt mögliche hinausging. Die Modelle insbesondere der Jodchemie in Wasservorlagen, die unter anderem auch von pH-Wert und Strahlendo-

sis maßgeblich beeinflusst werden, sind derart komplex, dass eine Bewertung nur im Rahmen von Detailanalysen vorgenommen werden kann.

Für die Analyse des untersuchten Leckstörfalls sei auf die detaillierte Darstellung im technischen Fachbericht /REI 10/ zum Vergleich von ASTEC und MELCOR verwiesen.

5 Zusammenfassung und Ausblick

5.1 Methoden zur probabilistischen Bewertung softwarebasierter digitaler Leittechnik

Die aus den Arbeiten zum Stand von W&T gewonnenen Erkenntnisse bestätigen den Eindruck, dass die methodischen Entwicklungen für eine probabilistische Bewertung softwarebasierter Leittechnik derzeit noch nicht so weit fortgeschritten sind, dass in unmittelbarer Zukunft mit einer Etablierung geeigneter Analyseverfahren gerechnet werden kann. Dennoch ergibt sich aus der Sicht der GRS auch weiterhin eine Notwendigkeit, die aktuellen Entwicklungen auf diesem Gebiet kontinuierlich zu verfolgen und weiterhin eigene methodischen Ansätze für eine probabilistische Bewertung softwarebasierter Leittechnik einschließlich von Ansätzen zur Quantifizierung der durch Softwarefehler verursachten Ausfälle zu untersuchen.

Gegenwärtig wird bei nationalen wie auch internationalen Gutachterorganisationen der Einsatz diversitärer (dissimilarer) Sicherheitsleittechnik im nuklearen wie auch im nichtnuklearen Bereich unter Verwendung diversitärer (dissimilarer) Hard- und Software als wegweisende Lösung beim Einsatz softwarebasierter Leittechnik-Systeme betrachtet. Grundprinzip einer solchen, nachfolgend als dissimilar bezeichnete Auslegung ist es, möglichst unähnliche (dissimilare) redundante Einrichtungen vorzusehen, so dass ein gleichzeitiges Versagen mehrerer, zueinander dissimilarer Einrichtungen aus gemeinsamer Ursache verhindert wird.

Die Einführung von Diversität (Dissimilarität) bei der Auslegung digitaler Sicherheitsleittechnik muss adäquat sowohl in der deterministischen als auch in der probabilistischen Sicherheitsbewertung berücksichtigt werden. Wichtige Fragestellungen sind dabei, welche Faktoren bzw. Merkmale für die Bewertung der Diversität (Dissimilarität) der Hard- und Software relevant sind und welchen Beitrag diese Faktoren hinsichtlich der Beherrschung der GVA leisten. Hierzu sind Bewertungsmethoden zu entwickeln.

Zur Bewertung der Mensch-Maschine-Schnittstelle wird in /AP1/ HAR 10/ ein Konzept vorgestellt, welches zur Vervollständigung der Bewertung der technischen Zuverlässigkeit im Rahmen einer PSA auch die menschliche Zuverlässigkeit beim Einsatz softwarebasierter Leittechnik berücksichtigt. Allerdings müssen für viele der neuen Tätigkeiten an und mit softwarebasierter Leittechnik neue Zuverlässigkeitskenngrößen

ermittelt werden. Zudem ergaben sich Hinweise darauf, dass bei modernen Mensch-Maschine-Schnittstellen die Methoden zur Bewertung des Problemlösens verstärkt an Bedeutung gewinnen. Bei diesen Methoden besteht allerdings noch weiterer Forschungs- und Entwicklungsbedarf. Dies bezieht sich nicht nur auf Tätigkeiten an und mit softwarebasierter Leittechnik, sondern auch auf alle Handlungen im Kraftwerk, deren Schwerpunkt im Bereich des Problemlösens liegt.

Für zukünftige Forschungs- und Entwicklungsarbeiten sind deshalb folgende Schwerpunkte zu setzen:

- Untersuchungen zur Quantifizierung von Tätigkeiten an und mit softwarebasierter Leittechnik und
- Untersuchungen zur Bewertung wissensbasierter Handlungen an der Mensch-Maschine-Schnittstelle softwarebasierter Leittechnik.

5.2 Berücksichtigung wissensbasierter Personalhandlungen und organisatorischer Einflüsse

5.2.1 Methoden zur Berücksichtigung wissensbasierter Personalhandlungen in einer probabilistischen Sicherheitsanalyse

Die Ziele des Arbeitspaketes sind erreicht worden. Es liegt nun eine Methode vor, um sicherheitstechnisch erforderliche, wissensbasierte Handlungen in einer PSA zu berücksichtigen. Diese umfasst

- ein Verfahren zur Identifikation von zu untersuchenden wissensbasierten Handlungen,
- ein Kognitionsmodell, welches den Anwender durch alle für die Zuverlässigkeitseinschätzung relevanten Aspekte führt und ihm erlaubt, günstige und ungünstige Einflüsse im Detail herauszuarbeiten,
- einen zweistufigen Bewertungsansatz, der ausgehend von der Detailkenntnis günstiger und ungünstiger Einflüsse die mit der Aufgabe verbundene kognitive Beanspruchung zunächst einer von drei Beanspruchungsstufen zuordnet. Die mit diesen Beanspruchungsstufen verbundenen Fehlerwahrscheinlichkeiten beruhen auf Expertenschätzungen. Die Schätzungen orientieren sich an anerkannten

Datenquellen, die Fehlerwahrscheinlichkeiten für Aufgaben vorschlagen, die kognitiv vergleichbaren Beanspruchungen hervorrufen.

Eine erste Erprobung dieser Methode an Fallbeispielen aus der Betriebserfahrung war erfolgreich. Die Dokumentation zu den Fallbeispielen enthält jedoch nicht den für eine vollständige Überprüfung der Methode erforderlichen Umfang an Informationen. Ein nächster logischer Schritt sollte somit die Anwendung der Methode an praktischen Beispielen im Rahmen einer PSA sein. Die dabei gewonnenen Erkenntnisse können dann in eine weitergehende Validierung oder gegebenenfalls in eine weitere Optimierung hinsichtlich der Vorgehensweise und der Gebrauchstauglichkeit einfließen.

Zukünftige Arbeiten zur Weiterentwicklung der Methode sollten sich folgenden Aspekten widmen:

- Das Modell des Problemlösungsprozesses berücksichtigt den Beitrag, welchen Beanspruchung und Stress zur Zuverlässigkeit einer Problemlösung leisten, nur summarisch. Die Wirkung der Beanspruchung und des Stresses lässt sich mit den derzeit empfohlenen Methoden nur für die Ausführung gut bekannter und eingeübter Handlungen bewerten. Dieser Bewertungsansatz beruht auf einem Modell, das mit den aktuellen fachwissenschaftlichen Erkenntnissen nicht mehr in Einklang steht. Dieser Sachstand erfordert methodische Entwicklungen, um den Beitrag der Faktoren Stress und Beanspruchung zur Zuverlässigkeit wissensbasierter und sonstiger Handlungen genauer zu erfassen, als es bisher möglich ist.
- Das Modell des Problemlösungsprozesses behandelt das Personal wie einen einzigen Problemlöser. Es vernachlässigt somit Faktoren der Arbeitsteilung, der Kooperation, der Kommunikation und der Führung. Diese Faktoren können sich erheblich auf die Zuverlässigkeit einer Problemlösung während eines Ereignisablaufs auswirken, an dessen Bewältigung zahlreiche Personen und Teams mitwirken. Im Vorhaben RS1180 wurden diese Aspekte zurückgestellt, um zunächst den Prozess des Problemlösens selbst zu klären und in späteren Schritten den Beitrag der Arbeitsteilung, der Kommunikation und der Führung auf der Basis eines praktikablen Modells problemlösender Aktivitäten zu klären.
- Die Bewertungsmethodik trennt die beiden Phasen der Diagnose bzw. problemlösender Aktivitäten von der Handlungsausführung. Eine Problemlösung kann aber auch systematisches Probieren mit Eingriffen umfassen. Die

Bewertungsmethode berücksichtigt keine Fehlermöglichkeiten durch probeweises Handeln, welches dazu dient, die Art und die Lösung des Problems besser zu erkennen. Erweiterungen der Methodik sollen erfolgen, wenn eine breitere Erprobung der Bewertungsmethode zeigt, dass systematisches Probieren im Zuge der Lösungsfindung eine wichtige Rolle spielt.

- Die Bewertungsmethode stützt sich auf Daten, die teils aus /SWA 83/ entnommen, teils aus Laborexperimenten übertragen worden sind. Die Datenbasis sollte verbessert werden. Eine Möglichkeit dazu bieten z. B. die Versuchseinrichtungen der OECD in Halden. Es sollten daher Szenarien und Versuchspläne entwickelt werden, um Problemlösungsprozesse durch ein Team von Operateuren systematisch zu untersuchen und für die Schätzung der Zuverlässigkeit erforderlicher, wissensbasierter Handlungen zu nutzen.

5.2.2 Probabilistische Bewertung organisatorischer Einflüsse sowie von Einflüssen des Sicherheitsmanagements auf die Zuverlässigkeit von Personalhandlungen

Im Arbeitspaket ‘Probabilistische Bewertung organisatorischer Einflüsse‘ des Vorhabens RS1180 wurde eine Methode zur Berücksichtigung organisatorischer Einflussfaktoren in der PSA entwickelt /FAS 10/. Mit Hilfe der Forschungsergebnisse ist es möglich, die sicherheitstechnische Relevanz organisatorischer Einflussfaktoren und des Sicherheitsmanagements herauszuarbeiten, zu quantifizieren und in das PSA-Modell zu integrieren.

Die Methode führt arbeitswissenschaftliche Erkenntnisse zur Bewertung der Zuverlässigkeit von Personalhandlungen mit Erkenntnissen aus der Organisationswissenschaft zusammen und stellt so den Bezug zwischen Organisation und Sicherheit her.

Die benötigten Zuverlässigkeitsdaten stützen sich auf Expertenschätzungen. Die Schätzungen orientieren sich an anerkannten Datenquellen, die pessimistische Werte für Handlungsfehler und die Wirkung von leistungsbeeinflussenden Faktoren vorschlagen.

Die Methode konnte zwar an Ereignissen aus der Betriebserfahrung getestet werden. Allerdings liefern diese nicht die Güte an Daten, die für eine realitätsnahe Überprüfung des Verfahrens notwendig ist.

Ein nächster logischer Schritt sollte somit die Anwendung der Methodik an praktischen Beispielen im Rahmen einer PSA sein. Die dabei gewonnenen Erkenntnisse können dann in eine weitergehende Validierung oder gegebenenfalls in eine weitere Optimierung hinsichtlich der Vorgehensweise und der Gebrauchstauglichkeit einfließen.

5.3 Auslösende Ereignisse und Einwirkungen von innen und außen

5.3.1 Methoden zur Ermittlung von Leck- und Bruchhäufigkeiten druckführender Komponenten

Im Rahmen des Vorhabens RS1180 wurden im Arbeitspaket 3.1 die Entwicklung und Erprobung

- einer Schnittstelle zwischen der Anwendung von statistischen Methoden basierend auf der Betriebserfahrung und von Strukturzuverlässigkeitsmodellen,
- geeigneter Strukturzuverlässigkeitsmodelle für Behälter mit hohem Energieinhalt (Druckhalter, Speisewasserbehälter) und
- von Ansätzen zur Berücksichtigung der Einflüsse von verschiedenen Schädigungsmechanismen, Prüfkonzepten und Lerneffekten

durchgeführt.

- **Arbeiten zur Schnittstellenentwicklung und -erprobung**

Zunächst wurden verfügbare Untersuchungsergebnisse bzw. Analysemodelle aus abgeschlossenen Vorhaben im Hinblick auf ihre Anwendbarkeit im Sinne der Zielsetzung überprüft. Für Rohrleitungen des Typs DN 50 des Volumenregelsystems von deutschen DWR-Anlagen sind aus statistischen Untersuchungen basierend auf der Betriebserfahrung entsprechende Ergebnisse verfügbar. Weiterhin wurden probabilistische Analysemethoden zur Berechnung von Leck- und Bruchwahrscheinlichkeiten in den Vorhaben RS1127 und RS1163 bereitgestellt und im Rahmen eines Anwendungsbeispiels thermomechanische Ermüdungsbelastung im Volumenregelsystem eines DWR, in dem es in einer Anlage zu einem Leckvorkommnis kam, erprobt. Dabei ergab sich, dass die bisher mit großen Kenntnisunsicherheiten getroffenen Annahmen zur Rissverteilung wesentlichen Einfluss auf die Berechnung der Leck- und Bruchwahrscheinlichkeiten haben. Daher wurde eine Auswertung der Betriebserfahrung im

Hinblick auf Rissereignisse in deutschen DWR- und SWR-Anlagen auf Basis der GRS-Datenbank KomPass für Rohrleitungsschäden vorgenommen. Darüber hinaus wurde die einschlägige Literatur ausgewertet. Ziel dieser Arbeit war die Ermittlung einer Anfangsrissverteilung für den Einsatz im GRS-Strukturzuverlässigkeitsprogramm PROST.

Für die gefundenen Ereignisse aus der Datenbank KomPass wurde jeweils das mittlere Verhältnis von Risstiefe zu Wanddicke (a/t) und Risstiefe zu halber Risslänge (a/c) ermittelt. Die Datenbank KomPass mit etwa 800 Ereignissen in Rohrleitungen enthält jedoch insgesamt nur 18 unmittelbar verwertbare Ereignisse mit Riss, wobei unterschiedliche Wanddicken, Werkstoffe und Nennweiten zusammengefasst sind.

Die Auswertung der Ereignisse aus der Betriebserfahrung in KomPass ergab einen mittleren a/t-Wert von 0,42 (mit einer Standardabweichung von 0,17) und ein mittleres a/c-Verhältnis von 0,35 (mit 0,26 als Standardabweichung).

Zur Erweiterung der Datenbasis für die Methodik zur Bestimmung von Risstiefenverteilungen basierend auf Auswertungen der Betriebserfahrung wurden auch Abfragen der OPDE Datenbank, die etwa 3700 Ereignisse aus 11 Ländern enthält, durchgeführt. Hierbei konnten 94 unmittelbar verwertbare Ereignisse zur a/t-Festlegung ermittelt werden.

Für das betrachtete Anwendungsbeispiel wurde eine Auswertung mit dem statistischen Verfahren mit aktuellen Daten aus KomPass und OPDE durchgeführt sowie Berechnungen mit dem GRS-Strukturzuverlässigkeitsprogramm PROST mit den neu bestimmten Anfangsrissverteilungen vorgenommen. Weiterhin wurde ein Ansatz für die Wahrscheinlichkeit, dass ein Riss an der untersuchten Stelle auftritt, aus der Literatur abgeleitet. Die mit PROST ermittelten Leck- bzw. Bruchwahrscheinlichkeiten multipliziert mit der Risswahrscheinlichkeit liegen jeweils über den Ergebnissen mit der statistischen Methode. Dies deutet daraufhin, dass die untersuchte Stelle bei der realistischen Nachbildung der Belastung in PROST höher beansprucht wird als es dem Mittel der bei der statistischen Methode betrachteten Fälle entspricht. Weitere PROST-Berechnungen für andere Positionen mit anderen Annahmen bezüglich der Belastung der Volumenausgleichsleitung würden dann auch Hinweise bezüglich der Aussagegenauigkeit der angesetzten Risswahrscheinlichkeit ermöglichen.

- **Arbeiten zur Entwicklung von Strukturzuverlässigkeitsmodellen für Behälter**

Eine Abfrage der KomPass-Datenbank nach Ereignissen mit Rissen, Lecks oder Brüchen bei Behältern ergab für den betrachteten Zeitraum bis einschließlich 2006 102 Ereignisse, wovon acht Fälle Speisewasserbehälter betreffen.

Zur Anwendung für Berechnungen mit PROST wurde einer dieser Speisewasserbehälterfälle, bei dem nach kurzer Betriebszeit (458 Tagen) mehrere Rissbefunde mit Risstiefen bis zu 82 % der Wandstärke aufgrund des Schädigungsmechanismus Spannungsrisskorrosion festgestellt wurden, ausgewählt. Zur Festlegung der Risswachstumsgeschwindigkeit wurden hier zwei der in PROST verfügbaren Korrosionsmodelle bezüglich des Schadensbefunds angepasst. Nimmt man eine konstante Rissgeschwindigkeit von $da/dt = 3{,}1 \cdot 10^{-7}$ mm/s an, so ergeben die Berechnungen eine nahezu hundertprozentige Leckwahrscheinlichkeit nach etwa drei Jahren. Dagegen ist die Berechnung mit einem Modell, bei dem sich die Risswachstumsgeschwindigkeit abhängig von der Rissgröße bzw. der Rissbeanspruchung ändert, nicht zufriedenstellend, weil bei kleinen Risstiefen zu kleine Rissgeschwindigkeiten auftreten, die nicht die Befunde reproduzieren können. Eine verbesserte Anpassung dieses Korrosionsmodells müsste auf Basis von entsprechenden Laboruntersuchungen mit dem Werkstoff unter Mediumeinfluss durchgeführt werden.

- **Arbeiten zur Entwicklung von Ansätzen zur Berücksichtigung verschiedener Einflüsse**

Die Ergebnisse aus der deutschen Betriebserfahrung können wie folgt zusammengefasst werden:

- Die Anzahl der Leckereignisse an sicherheitstechnisch bedeutsame Rohrleitungen in deutschen Anlagen mit Druck- und Siedewasserreaktoren ist insgesamt gering.
- Die schon in vorangegangenen Untersuchungen festgestellte Nennweitenabhängigkeit von Leckereignissen an sicherheitstechnisch bedeutsamen Rohrleitungen in deutschen Anlagen mit Druck- und Siedewasserreaktoren wurde bestätigt, d. h. von Leckereignissen waren vor allem Rohrleitungen mit kleineren Durchmessern betroffen.
- Die Leckereignisse wurden durch verschiedene Schädigungsmechanismen ausgelöst, von denen keiner über den gesamten Betrachtungszeitraum dominiert.

Ein signifikanter mechanismus-spezifischer Trend bei der Anzahl der Leckereignisse war nur für den Mechanismus ‘mechanische Ermüdung‘ zu erkennen.

- Die Häufigkeit von Rohrleitungsleckagen an Schweißnahtbereichen sicherheitstechnisch bedeutsamer Rohrleitungen in deutschen Anlagen mit Druck- und Siedewasserreaktoren hat im Betrachtungszeitraum abgenommen. Dagegen haben Rohrleitungsleckagen, die im Grundwerkstoffbereich aufgetreten sind, insbesondere in Anlagen mit Druckwasserreaktoren an Bedeutung gewonnen. Dies gibt Anlass, die Kriterien für die Zählung ‘leckrelevanter Stellen‘ innerhalb von Rohrleitungssystemen zu hinterfragen. Hierzu besteht weiterer Untersuchungsbedarf.

- Bei der mit geringerem Detaillierungsgrad vorgenommenen Auswertung von Leckereignissen an sicherheitstechnisch bedeutsamen Rohrleitungen in US-amerikanischen Anlagen waren bei zwei Schädigungsmechanismen Trends erkennbar, die auf einen Lerneffekt schließen lassen. Ein Vergleich mit den Daten von deutschen Anlagen zeigt hier teilweise ähnliche Trends, jedoch führen Unterschiede, die konstruktiver, system- oder werkstofftechnischer sowie betrieblicher Art sein können, auch zu deutlich anderen Entwicklungen.

- **Schlussfolgerungen**

Mit den heute zur Verfügung stehenden Strukturzuverlässigkeitsprogrammen können prinzipiell für bestimmte Schadensmechanismen quantitativ Leck- und Bruchwahrscheinlichkeiten berechnet werden. Durch ihren Einsatz zur Bestimmung der ortsabhängigen Leckwahrscheinlichkeit können Teilbereiche einer Anlage im Hinblick auf ihre Versagensrelevanz unterschieden werden. Es können Trends bezüglich der Veränderung von Einflussparametern quantitativ bestimmt werden. Einschränkungen bezüglich der Einsatzfähigkeit im Rahmen von probabilistischen Sicherheitsanalysen werden insbesondere bezüglich der Aussagegenauigkeit absoluter Leck- bzw. Bruchwahrscheinlichkeiten gesehen, da die Ergebnisse teilweise stark von den Unsicherheiten für relevante Eingabeparameter wie Rissgeometrie, erwartete Belastungen sowie bestimmter Parameter zur Charakterisierung der Schadensmechanismen abhängen.

Insgesamt können die probabilistischen Strukturzuverlässigkeitsmodelle ein wertvolles Instrument zur Ergänzung der bisher im Rahmen von PSA eingesetzten Methodik zur

Abschätzung von Leck- und Bruchhäufigkeiten basierend auf der Betriebserfahrung sein.

5.3.2 Auswahlverfahren zur Bestimmung von kritischen Anlagenteilen bei seismischen probabilistischen Sicherheitsanalysen

Im Rahmen des Forschungs- und Entwicklungsvorhabens wurde ein Verfahren zur Bestimmung kritischer Bauteile, Systeme und Komponenten (BSK) mit Hilfe einer Datenbankstruktur entwickelt. Kritische Bauteile, Systeme und Komponenten sind solche Ausrüstungen, deren seismisch bedingter Ausfall zur Häufigkeit von Gefährdungs- bzw. Kernschadenszuständen beitragen kann und für welche sogenannte Fragilities generischer oder anlagenspezifischer Art benötigt werden.

In einem weiteren Vorhaben (vgl. /TUE 10a/) wird aktuell ein Modell zur Beschreibung seismischer Abhängigkeiten entwickelt. Diese seismischen Abhängigkeiten sind insbesondere für das abhängige Ausfallverhalten kritischer BSK von Bedeutung. Es wurde gezeigt, dass sich die Abhängigkeiten durch die Menge der abhängigen Bauteile, Systeme und Komponenten und durch eine seismische Kopplungsfunktion beschreiben lassen. Diese Informationen sind ebenfalls in einer Datenbank hinterlegbar.

Die im Vorhaben RS1180 in Grundzügen erstellte Datenbank ist so weiterzuentwickeln, dass auf der einen Seite alle benötigten Informationen zur Durchführung von SPSA bereitgestellt (Eingabe von Daten) werden können und zum anderen diese Informationen wiederum zur Durchführung der Arbeitsschritte einer SPSA (z. B. zur Auswahl kritischer Komponenten, Bereitstellung von Daten zur Quantifizierung von Ereignisabläufen) aktiv durch Auswerteroutinen (Ausgabe und Nutzung der Daten und Informationen) genutzt werden können.

Für eine Weiterentwicklung des Datenbank-Ansatzes bei der Durchführung des Auswahlverfahrens wird als unbedingt notwendig vorausgesetzt, dass ein Referenzkernkraftwerk mit Zugang zu allen benötigten anlagenspezifischen Daten zur Verfügung steht. Insbesondere sollte das PSA-Modell der Stufe 1 bei Leistungsbetrieb genutzt werden können. Als Ergebnis würde eine umfassende Datenbasis zur Durchführung einer anlagenspezifischen SPSA zum Referenzkraftwerk vorliegen.

Die Datenbank <*DB SPSA*> konnte im Vorhaben nur in ihren Grundzügen beschrieben und entwickelt werden. Eine Spezifizierung aller benötigten Daten, die Nutzung der Da-

ten und die Einbindung der Datenbank in den Gesamtprozess der Erstellung und Anwendung einer SPSA ist erforderlich, wenn eine standardisierte Nutzung erfolgen soll. Dazu sind die bisherigen Forschungs- und Entwicklungsarbeiten mit den nachfolgend aufgeführten Arbeitsschwerpunkten fortzusetzen.

- **Spezifikation einer SPSA-Datenbasis**

Die Datenbasis für eine SPSA umfasst neben der Menge aller Bauteile, Systeme und Komponenten (BSK) des zu untersuchenden Kernkraftwerks und ihren Eigenschaften auch umfangreiche generische Informationen, welche bei konkreten Analysen standardisiert zur Entscheidungsfindung zur Verfügung stehen.

- Anlagenspezifische Daten und Informationen:
  Es ist eine Vorschrift für eine systematisierte Erstellung einer SPSA-Datenbasis zu erarbeiten. Diese Vorschrift schließt den Umfang der zu erfassenden Informationen, deren Nomenklatur und Klassifikation, die Beschreibung von Abhängigkeiten und alle sonstigen Aspekte der SPSA-Bearbeitung ein. Insbesondere werden die verschiedenen Arbeitsschritte (Ausgangsmenge von BSK, vorläufige SAL, endgültige SAL, Risikoklassifikation der BSK der endgültigen SAL) deutlich gemacht.

- Generische Informationen und Daten:
  Diese Daten umfassen z. B. generische Versagenswahrscheinlichkeiten und Regelmengen zur Entscheidung, ob für ausgewählte BSK anlagenspezifische Versagenswahrscheinlichkeiten abgeleitet werden müssen. Zum eigentlichen Prozess der Klassifikation von BSK aufgrund von seismisch relevanten Eigenschaften (Auswahlschritt 2) konnte im Vorhaben verwiesen werden. Für die Bewertung der seismischen Widerstandsfähigkeit von BSK gibt es keine adäquaten Regelmengen (caveats), die zum Vergleich mit der Auslegung konkreter BSK in deutschen Kernkraftwerken herangezogen werden können. Die Datenbank <*DB SPSA*> ist zur Aufnahme von Klassen von BSK und den zugehörigen Eigenschaften der Regelmengen strukturell vorbereitet. Eine Belegung mit Inhalten kann allerdings erst erfolgen, wenn die Regelmengen definiert sind.

Die Datenbasis der SPSA ist in ihrer Struktur detailliert zu beschreiben.

- **Einsatz der SPSA-Datenbasis bei Erstellung, Auswertung, Nutzung und Begutachtung einer SPSA**

Es ist eine umfassende Anwendungsbeschreibung der SPSA-Datenbank zu erstellen. Dabei werden insbesondere folgende Anwendungen beschrieben:

- Nomenklaturen, Regeln und Fallen bei der Erstellung einer Datenbank für eine SPSA; Datenkontrollabfragen, Konsistenz der Daten, Datenfehlersuche;
- Durchführung des Auswahlverfahrens zur Erstellung einer seismischen Ausrüstungsliste (SAL) unter Nutzung der BSK-Eigenschaften als Entscheidungskriterium;
- Organisation und Unterstützung von Begehungen im Rahmen von SPSA-Entscheidungsprozessen durch Datenbankfunktionen;
- Klassifikation von BSK der seismischen Ausrüstungsliste hinsichtlich ihrer sicherheitstechnischer Bedeutung mit Hilfe der in der SPSA-Datenbank abgelegten Informationen;
- Zuordnung generischer seismischer Versagenswahrscheinlichkeiten zu BSK entsprechend den Ergebnissen des Auswahlverfahrens, automatische Datenübergabe an Codes zur Berechnung der seismischen Gefährdungshäufigkeit;
- Festlegung, Beschreibung und Quantifizierung seismischer Abhängigkeiten in Bezug auf Ausfälle von BSK der seismischen Ausrüstungsliste;
- Pflege der Datenbank und die Möglichkeit, Änderungen im Betriebsgeschehen in der SPSA entsprechend umzusetzen;
- Nachvollziehbarkeit der SPSA durch Nutzung der Datenbank.

Alle Anwendungen werden durch Datenbank-Prozeduren unterstützt.

- **Datenbank generischer Versagenswahrscheinlichkeiten**

Eine BSK versagt in Abhängigkeit von der Stärke eines Erdbebens. Zur Quantifizierung werden seismische Versagenswahrscheinlichkeiten genutzt. Unter einer seismischen Versagenswahrscheinlichkeit einer BSK wird die Wahrscheinlichkeit des Ausfalls bzw. Funktionsverlustes einer BSK als Funktion der Stärke des Erdbebens verstanden. Die entsprechende Funktion wird seismische Versagenskurve der BSK genannt.

Es ist auf der Grundlage bekannter SPSA und sonstiger internationaler Studien eine Datenbank generischer Versagenswahrscheinlichkeiten aufzubauen. Diese Datenbank ist in die Datenbank <*DB SPSA*> zu integrieren.

5.3.3 Methoden für eine probabilistische Bewertung von Transienten aufgrund von Überspannungen oder Fremdspannungseinträgen

Für eine Weiterentwicklung der Methoden zur probabilistische Bewertung von Transienten aufgrund von Überspannungen oder Fremdspannungseinträgen werden aus Gründen einer Kostenoptimierung sukzessiv drei aufeinander folgende Arbeitsschritte in zunächst separaten Teilprojekten empfohlen. Dabei soll das erste Teilprojekt als Schwerpunkt den systemanalytischen Teil umfassen, im zweiten Teilprojekt sollen für die identifizierten, durch Überspannung und Fremdspannungseinträge initiierten Transienten die Zuverlässigkeitskenngrößen ermittelt werden. Das dritte Teilprojekt besteht in der konkreten beispielhaften Durchführung einer (Teil-)PSA für verschiedene Schadenszustände.

Im Teilprojekt 1 ist die Anlage hinsichtlich der Möglichkeiten des Auftretens von Überspannung bzw. Fremdspannungseinträge zu untersuchen. Dazu gehören:

- Netzstörungen,
- Regelungsfehler in der Eigenbedarfsanlage einschließlich des Hauptgenerators,
- Blitzeinwirkungen, die über das Hauptnetz in die Anlage eintreten,
- Blitzeinschläge in Freiluftschaltanlagen am Kraftwerksstandort,
- Blitzeinschläge in die Gebäude mit Untersuchungen zu Potentialverschiebungen innerhalb des Erdungssystems sowie
- Ausbreitung von Störwellen bzw. induktiver Einkopplungen durch das Öffnen von Schaltern.

Für diese Einwirkungen sind zunächst deterministische Schadensanalysen durchzuführen. Ziel des Teilprojekts 1 ist es somit, ein möglichst abdeckendes Spektrum von Schadensbildern bzw. Schadenszuständen zu erhalten. Dabei ist unseres Erachtens auch eine Unterstützung von dritter Seite (u. a. seitens Universitäten, TÜV, ISTec, Her-

stellern und Planern von Überspannungsschutzeinrichtungen) notwendig, um für diese Aufgabe das nötige Know-how zu erwerben.

Aus den Schadens- bzw. Systemanalysen können die Ausfallmodi der verschiedenen Ereignisse identifiziert werden. Für diese sind im Teilprojekt 2 die Zuverlässigkeitsdaten zu ermitteln. Hier sind insbesondere durchführbare Methoden für die Bewertung von Zuverlässigkeitskenngrößen zu finden, zum einen für seltene Ereignisse die Eintrittshäufigkeiten, zum anderen für Ereignisse, die auf den Ausfall passiver Schutzeinrichtungen beruhen (Schirmung, Entkopplung unter Berücksichtigung von Näherungen etc.), die Ausfallwahrscheinlichkeiten bzw. Ausfallraten.

Dem letzten und dritten Teilprojekt 3 ist dann die Durchführung einer PSA für ausgewählte Überspannungstransienten anhand einer realen Referenzanlage vorbehalten. Hierzu bedarf es der Unterstützung durch einen Betreiber. In diesem Schritt können dann Zuverlässigkeitsanalysen unter Zuhilfenahme der entsprechenden Analysewerkzeuge (genannt in Abschnitt 4.3.3) durchgeführt werden. Dabei ist eine methodische Vorgehensweise zu erstellen, wie bzw. unter welchen Umständen der Untersuchungsaufwand reduziert werden kann, ohne dass relevante Beiträge zur Gefährdungs- bzw. Kernschadenshäufigkeit vernachlässigt werden.

5.4 Methoden zur Analyse des Einflusses von Unsicherheiten auf PSA-Ergebnisse

5.4.1 Methoden zur Durchführung von Unsicherheits- und Sensitivitätsanalysen in probabilistischen Dynamikanalysen (dynamische PSA)

Es wurden zwei alternative Methoden entwickelt, mit denen man aus Ergebnissen einer probabilistischen Dynamikanalyse mittels MCDET-Analyse approximative Unsicherheits- und Sensitivitätsaussagen ableiten kann.

Obwohl beide Methoden an einem vereinfachten dynamischen Modell zur Wasserstoffverbrennung im Containment nach einem Kühlmittelverluststörfall erfolgreich erprobt worden sind, können bisher noch keine allgemeinen Aussagen bzgl. Anwendbarkeit und Qualität der Methoden gemacht werden.

Um diesbezügliche Erfahrungen aufzubauen, müssen diese Methoden im Rahmen probabilistischer Dynamikanalysen, die mit der MCDET-Methode durchgeführt werden, angewendet werden. Zur Abschätzung der Qualität der Methoden sind MCDET-Analysen erforderlich, die mit einer zweistufig geschachtelten Monte-Carlo-Simulation durchgeführt werden können. Diese Situation ist insbesondere dann gegeben, wenn der Rechenzeitbedarf für das zugrundeliegende Dynamikmodell nicht zu hoch ist. Grundvoraussetzung dieses Erfahrungsaufbaus ist allerdings die vermehrte Anwendung von probabilistischen Dynamikanalysen mit der MCDET-Methode. Falls die entsprechenden Bedingungen gegeben sind, werden die in diesem Vorhaben entwickelten approximativen Methoden zur Unsicherheits- und Sensitivitätsanalyse im Rahmen der im Folgevorhaben durchzuführenden MCDET-Analysen angewendet und weiter erprobt.

5.4.2 Methoden zur Anpassung von Beta-Verteilungen an vorgegebene Lognormal-Verteilungen unter Berücksichtigung zusätzlicher Benutzervorgaben

Im Rahmen dieses Vorhabens wurde ein Verfahren entwickelt, welches den Anwender dabei unterstützt, auf der Grundlage einer vorgegebenen Lognormal-Verteilung eine geeignete Beta-Verteilung zu ermitteln. Hierbei hat der Anwender die Möglichkeit, verschiedene Anpassungskriterien für die Beta-Verteilung festzulegen.

Die Anpassung einer Beta-Verteilung kann entweder an Erwartungswert und Varianz oder an die (5 % -,) 50 % - und 95 % - Quantile einer vorgegebenen Lognormal-Verteilung erfolgen. Liefert die Lognormal-Verteilung mit einer subjektiven Wahrscheinlichkeit von mindestens 1,0 E-04 Werte p größer als eins, so wird für die Anpassung die im Punkt p = 1 gestutzte Lognormal-Verteilung berücksichtigt.

Die Ermittlung der Beta-Verteilung, deren Erwartungswert und Varianz mit den entsprechenden Größen der (ungestutzten bzw. gestutzten) Lognormal-Verteilung übereinstimmen, erfolgt analytisch. Für die Ermittlung einer Beta-Verteilung, deren (5 % -,) 50 % - und 95 % - Quantile an die entsprechenden Quantile der (ungestutzten bzw. gestutzten) Lognormal-Verteilung approximiert sind, wird ein adaptives zufälliges Suchverfahren eingesetzt.

Der Algorithmus zu diesem Verfahren wurde in FORTRAN implementiert. Außerdem wurden zwei Versionen einer Benutzeroberfläche (‘BetaFit‘) entwickelt. Dabei liegt eine Version als VBA-Programm (*V*isual *B*asic for *A*pplications) unter MS EXCEL 2007® vor, die andere als Visual Basic 2008®-Programm unter der .NET Umgebung. Letztere wurde zusätzlich entwickelt, da Microsoft langfristig VBA durch eine .NET-basierte Technologie ersetzen wird und damit Kompatibilitätsprobleme auftreten könnten. Die Benutzeroberfläche ‘BetaFit‘ unterstützt den Anwender bei der Dateneingabe und Fehlervermeidung. Sie ruft automatisch das FORTRAN-Programm auf und liefert schließlich eine ausführliche Dokumentation und grafische Darstellung der Ergebnisse. Beide Versionen von ‘BetaFit‘ (einschließlich FORTRAN-Programm) wurden erfolgreich anhand von Anwendungsbeispielen erprobt.

Eine ausführliche Beschreibung der durchgeführten Arbeiten zu diesem Vorhaben ist in /KLO 10/ zu finden.

‘BetaFit‘ kann je nach Bedarf der Anwender um weitere Optionen hinsichtlich der Anpassungskriterien für eine Beta-Verteilung erweitert werden.

Zur Zeit läuft ‘BetaFit‘ als eigenständiges Programm, es kann aber als zusätzlicher Bestandteil in die im Rahmen dieses Vorhabens entwickelte grafische Benutzeroberfläche integriert werden (vgl. dazu Kapitel zu AP 4.5).

5.4.3 Konsistente und umfassende Berücksichtigung epistemischer Unsicherheiten in Verteilungen von Zuverlässigkeitskenngrößen

Die entwickelte Methodik zur nachträglichen Varianzerhöhung von Verteilungen für Zuverlässigkeitskenngrößen wurde über eine Subroutine in das GRS-Rechenprogramm PEAK zur Schätzung von GVA-Wahrscheinlichkeiten implementiert. Diese Subroutine kann zum einen relativ leicht in andere Programme eingebaut werden, mit denen Verteilungen für Zuverlässigkeitskenngrößen (z. B. Betaverteilungen für Ausfallwahrscheinlichkeiten pro Anforderung) erzeugt werden. Sie kann aber auch ohne großen Aufwand als eine eigenständige Programmversion entwickelt werden, mit denen beliebige parametrische und nichtparametrische Verteilungen verbreitert werden können, die unter Verwendung anderer Programme erzeugt wurden.

Grundsätzlich ist der Einfluss potentieller, nicht explizit im Schätzmodell berücksichtigter Unsicherheitsquellen auf die Unsicherheiten der Schätzverteilungen nicht zu quanti-

fizieren. Deshalb kann auch mit dem neu vorgeschlagenen Verfahren zur nachträglichen Varianzerhöhung von Schätzverteilungen für Zuverlässigkeitskenngrößen nicht garantiert werden, dass es den tatsächlichen Einfluss zusätzlicher Unsicherheitsquellen auf die Unsicherheiten der Schätzverteilungen hinreichend genau abschätzt.

Trotz dieser methodischen Schwächen ist die Durchführung einer nachträglichen Varianzerhöhung von Verteilungen für Zuverlässigkeitskenngrößen jedoch immer noch dem Vorgehen vorzuziehen, das den potentiellen Einfluss zusätzlicher epistemischer Unsicherheitsquellen auf die Ergebnisunsicherheiten ignoriert und generell unberücksichtigt lässt.

Um den Einfluss zusätzlicher Unsicherheitsquellen methodisch korrekt quantifizieren zu können, ist es unerlässlich, dass in der Betriebserfahrung auftretenden relevanten Unsicherheitsquellen, die potentiell einen Einfluss auf die Unsicherheiten der Schätzverteilungen von Zuverlässigkeitskenngrößen haben können, identifiziert werden und explizit in das Schätzmodell eingehen. Dazu sind allerdings eine genaue Erfassung und Auswertung der Betriebserfahrung sowie eine durchgängige Weiterentwicklung der jeweiligen Schätzmodelle notwendig.

Die Verwendung der neu entwickelten Methodik zur Verbreiterung von Verteilungen für Zuverlässigkeitskenngrößen hat zur Konsequenz, dass die Unsicherheiten der Zuverlässigkeitskenngrößen nicht mehr durch eine Lognormal-Verteilung, sondern durch eine nichtparametrische Verteilung ausgedrückt werden. Daraus ergibt sich für die PSA folgende Problematik: Das in der GRS verwendete Fehlerbaumprogramm RiskSpectrum® ist zwar in der Lage verschiedene parametrische Verteilungen für die Unsicherheiten von Zuverlässigkeitskenngrößen zu berücksichtigen. Nichtparametrische Verteilungen, die u. U. durch sehr viele Stützstellen (> 1000) definiert sind, können nicht ohne weiteres mit dem Programm RiskSpectrum® verarbeitet werden. Eine sehr pragmatische Lösung wäre, an die nichtparametrische eine parametrische Verteilung anzupassen und im Weiteren diese angepasste parametrische Verteilung in der Fehler- und Ereignisbaumanalyse zu verwenden.

Die Frage ob die Verwendung der nichtparametrischen Ergebnisverteilung gegenüber einer approximierten parametrischen Verteilung relevante Unterschiede in den Ergebnissen der Unsicherheitsanalyse des zugrundeliegenden Fehlerbaummodells zur Folge hat, wurde bisher noch nicht untersucht. Da die Untersuchung dieser Frage durch die Anwendung des neuen Verfahrens zur Verteilungsverbreiterung besondere Bedeutung

erlangt, sind die seitens der GRS für ein Folgevorhaben vorgeschlagenen Arbeiten zur konsistenten Berücksichtigung epistemischer Unsicherheiten die logisch konsequente Fortführung der Arbeiten, die auf den Ergebnissen des vorliegenden Vorhabens RS1180 basieren.

5.4.4 Methoden zur konsistenten Berücksichtigung gemeinsam verursachter Ausfallereignisse (GVA) in PSA

Die umfassende Bestandsaufnahme des zurzeit vorhandenen Systems von Randbedingungen zeigte, dass bei dem jetzigen System bezüglich mehrerer Aspekte ein Weiterentwicklungsbedarf besteht.

Dafür bestehen zwei wesentliche Gründe:

Um eine mathematisch korrekte Schätzung von GVA-Wahrscheinlichkeiten zu erhalten, ist es prinzipiell erforderlich, die Bezugszeiten bzw. Zahlen von Anforderungen für alle Komponentengruppen zu ermitteln, bei der die jeweiligen Randbedingungen zutreffen. Bei dem bisherigen System ist dies praktisch undurchführbar, da eine Vielzahl verschiedener Randbedingungen existiert, welche sich vielfach auf sehr spezielle Details in technischen Eigenschaften oder Betrieb der Komponenten beziehen.

Weiterhin liegt den definierten Randbedingungen jeweils eine Analyse zugrunde, ob beobachtete GVA-Ereignisse sich für die in der PSA modellierten Komponentengruppen nur eingeschränkt oder gar nicht übertragen lassen. Eine systematische Betrachtung, ob beobachtete GVA-Phänomene in bestimmten in der PSA modellierten Komponentengruppen häufiger zu erwarten sind oder stärkere Komponentenschädigungen erwarten lassen, fand nicht statt. Demzufolge wurden in keinem Fall Übertragbarkeitsfaktoren größer 1 vergeben. Diese Vorgehensweise könnte potentiell zu einer systematischen Unterschätzung von GVA-Wahrscheinlichkeiten für solche Komponentengruppen führen.

Weiterhin sind Randbedingungen definiert, deren Vorliegen nur sehr schwierig nachweisbar erscheint.

Deshalb ist es erforderlich, die Vorgehensweise zur Bewertung der Übertragbarkeit beobachteter GVA-Ereignisse und das System von definierten Randbedingungen grundlegend zu überarbeiten mit dem Ziel, ein wesentlich vereinfachtes System zu er-

halten, bei dem die oben genannten Probleme vermieden werden. Hierzu sollte zunächst eine allgemeine Vorgehensweise entwickelt, detailliert beschrieben und erprobt werden. Es ist nachvollziehbar festzulegen,

- unter welchen Bedingungen Randbedingungen definiert werden,
- wann Populationen aufgeteilt werden,
- wie die Übertragbarkeit von Ereignissen bzw. abweichende Komponentenschädigungen bewertet werden und
- welche Randbedingungen für die Ermittlung von GVA-Wahrscheinlichkeiten für PSA-Rechnungen jeweils zu verwenden sind.

Hierzu wurden im Rahmen dieses Vorhabens Anforderungen entwickelt, die unter anderem eine quantitative Bewertungsskala für Übertragbarkeitsfaktoren umfassen. Aufbauend auf diesen Anforderungen sind die konkreten Abläufe festzulegen und geeignet darzustellen, z. B. in Form eines Ablaufdiagramms. Diese sind praktisch zu erproben und in der Fachöffentlichkeit zu diskutieren. Der abschließende Schritt besteht in einer umfassenden Überarbeitung des Systems der Randbedingungen mit Überprüfung und gegebenenfalls Anpassung der Expertenbewertungen für alle Ereignisse und Randbedingungen.

Mit dem POOL-Programm wurde eine Möglichkeit geschaffen, die zur Berechnung einer GVA-Wahrscheinlichkeit notwendigen Parameter und Anlagendatensätze automatisch und qualitätsgesichert von einem einzigen Programm zusammenstellen zu lassen. Die Programmkombination POOL und PEAK berechnet GVA-Wahrscheinlichkeiten, die im Ergebnis mit denen des bisherig benutzten Verfahrens zur Auswertung und Berechnung übereinstimmen. Dabei verringert POOL einerseits den Arbeitsaufwand des Benutzers und schließt andererseits durch den Entfall von manuell auszuführenden Arbeiten bei der Erstellung von GVA-Datensätzen eine potentielle Fehlerquelle aus.

Die Dokumentation der zusammengestellten Parameter und Anlagendatensätzen erfolgt einerseits in Tabellen in der Datenbank selbst und andererseits durch vom Benutzer erstellbare Reports. Die Übergabe der erstellten Datensätze an das PEAK Programm erfolgt automatisch. PEAK wurde dahingehen verbessert, dass die Ausgabe direkt nach RiskSpectrum® exportiert werden kann.

Der neue Algorithmus zur Berechnung der Beobachtungszeiten erlaubt eine einfache Anpassung der auszuwertenden Betriebserfahrung auf frei wählbare Zeiträume und eröffnet so die Möglichkeit, sehr einfach Trendanalysen über verschiedene Zeiträume durchzuführen. Im Rahmen seiner Implementierung wurde außerdem das der Berechnung der Beobachtungszeit zu Grunde liegende Datenmaterial in POOL überprüft und teilweise bezüglich des Detailierungsgrads erheblich verbessert. Für viele Komponentenarten, für die vorher lediglich grobe Abschätzungen vorlagen, wurden jetzt exaktere Zählungen durchgeführt. Dennoch konnte dies im Rahmen des Projekts nicht für alle Komponentenarten durchgeführt werden. Die noch verbleibenden Abschätzungen sollten zukünftig nach Möglichkeit ebenfalls durch Zählungen ersetzt werden.

Weiterer Entwicklungsbedarf besteht bei dem Algorithmus im Hinblick auf die Berücksichtigung von Randbedingungen bei der Berechnung der Beobachtungszeit. Als Beobachtungszeit wird bei GVA-Ereignissen, bei denen diese Randbedingung bei der Bewertung der Übertragbarkeit eine Rolle spielte, vereinfacht die normale Beobachtungszeit für alle Komponentengruppen angesetzt. Wie oben beschrieben müsste die jeweils die Beobachtungszeiten bestimmt und verwendet werden, für die die jeweilige Randbedingung zutrifft. Es gilt also in Zukunft den Algorithmus anzupassen, so dass bei Benutzung einer Randbedingung bei der Bewertung eines GVA-Ereignisses auch die Beobachtungszeit, die zur Berechnung der Ausfallwahrscheinlichkeit durch dieses GVA-Phänomen verwendet wird, entsprechend eingeschränkt wird.

Prinzipiell sind die Tabellen zur Berechnung der Beobachtungszeit, insbesondere die Komponentengruppenliste, bereits so aufgebaut, dass die für die Berechnung der randbedingungsspezifischen Beobachtungszeiten notwendigen Modifikationen ohne großen Aufwand möglich sind. Umfangreicher stellt sich die zusätzlich erforderliche Datenerhebung selbst dar, da hierfür alle PSA-relevanten Komponentengruppen aller Anlagen hinsichtlich der Anwendbarkeit aller für sie potentiell zutreffenden Randbedingungen ingenieurstechnisch bewertet werden müssten. Bevor dies geschehen kann, müsste das System von Randbedingungen wie oben beschrieben weiterentwickelt werden.

Bisher sind im POOL-Programm Auswertungen der deutschen Betriebserfahrung bis 2002 eingepflegt. Sobald auch für die jüngere Betriebserfahrung Auswertungen von beobachteten GVA-Phänomenen existieren, sollen auch diese in das POOL-Programm importiert werden.

Bei zukünftig von der GRS durchgeführten PSAs soll das POOL-Programm zusammen mit PEAK bei der Ermittlung der GVA-Ausfallwahrscheinlichkeiten zum Einsatz kommen.

5.4.5 Benutzeroberfläche mit den erforderlichen Hilfsprogrammen für PSA-Methoden der Stufe 1

Ziel war es, die Hilfsprogramme der GRS, die zur Erstellung eines PSA-Modells für die Stufe 1 einschließlich der Schnittstelle zur Stufe 2 erforderlich sind, unter einer gemeinsamen MS WINDOWS®-basierten Oberfläche zusammenzufassen. Dazu wurde ein Konzept für die gemeinsame Oberfläche goPSA entworfen und der Entwicklungsbedarf für die GRS-Hilfsprogramme ermittelt.

Basierend auf diesem Konzept wurden die notwendigen Entwicklungsarbeiten an den GRS-Hilfsprogrammen, insbesondere die Weiterentwicklung der Prototyp-Version von CRAVEX, vorangetrieben und eine erste Version von goPSA erstellt. Für die unter goPSA eingebundenen GRS-Hilfsprogramme wurden Benutzeranleitungen erarbeitet und unter goPSA verfügbar gemacht. Für die Arbeitsschritte, bei denen die Erstellung eines eigenen Hilfsprogramms nicht zielführend gewesen wäre, wurden Benutzerhilfen und ggf. MS Office®-Vorlagen erstellt.

Die erste Version von goPSA umfasst somit die folgenden Funktionalitäten:

- GRS-Hilfsprogramm STREUSL zur Durchführung von Unsicherheits- und Importanzanalysen auf der Grundlage von Minimalschnitten,
- GRS-Hilfsprogramm CRAVEX für die probabilistische Analyse von übergreifenden Einwirkungen (als eigenständiges Programm),
- GRS-Hilfsprogramm EXCELRS für die Konvertierung eines mit STREUSL lesbaren Formats (als MS EXCEL®-Datei) in das von RiskSpectrum® lesbare RSA-Format,
- GRS-Hilfsprogramm RSAscii für die Konvertierung des RSA-Formats von RiskSpectrum® in ein von STREUSL lesbares Format,
- Benutzerhilfe und MS EXCEL®-Vorlage für die Berechnung von GVA-Modulen bei großen GVA-Komponentengruppen,

- Benutzerhilfe für die Bewertung von Handmaßnahmen nach THERP mittels einer Modellierung in RiskSpectrum®,

- Benutzerhilfe und Vorlagen für die Dokumentation einer PSA der Stufe 1 entsprechend den Vorgaben des PSA-Methodenbands,

- Benutzerhilfe und MS EXCEL®-Vorlage für die Definition einer Schnittstelle zwischen den Stufe 1 und Stufe 2 einer PSA.

Die Installationsprojekte für die Programme CRAVEX und goPSA sind auf der dem technischen Fachbericht /WIE 10/ beigefügten CD enthalten.

Der bisher erreichte Stand von goPSA und der darunter integrierten Programme und Benutzerhilfen stellt jedoch eine erste Version dar. Für weitere Entwicklungs- und Verbesserungsarbeiten kommen insbesondere die folgenden Punkte in Frage.

- Die Oberfläche goPSA sollte um Funktionalitäten zur PSA der Stufe 2, insbesondere bei Verwendung eines zweistufigen Verfahrens, erweitert werden.

- Für einen verbesserten Datenaustausch zwischen den einzelnen Schritten der PSA sollte ein einheitliches, auch von kommerziellen Programmen wie RiskSpectrum® direkt lesbares Datenaustauschformat verwendet werden. Durch die Entwicklung und Veröffentlichung des OpenPSA Model Exchange Format (OPSAMEF) /EPS 08/ gegen Ende der Laufzeit des Vorhabens RS1180 steht ein solches Format für Weiterentwicklungen von goPSA zur Verfügung.

- Für eine Einbindung des GRS-Hilfsprogramms SUSA sollte eine Version von SUSA erstellt werden, die ebenfalls in der .NET-Umgebung programmiert wurde.

- Zur Verringerung des Arbeitsaufwands bei der Berechnung von GVA-Modulen und zum weiteren Ausschluss von Fehlerquellen sollte das in diesem Vorhaben entwickelte Verfahren in einem eigenen Programm mit grafischer Benutzeroberflächen implementiert werden.

Darüber hinaus ist es erforderlich, die unter goPSA zusammengefassten GRS-Hilfsprogramme an die sich weiter entwickelnden Anforderung des Standes von Wissenschaft und Technik in der PSA anzupassen. Dies betrifft zum Beispiel das GRS-Hilfsprogramm CRAVEX, für das derzeit noch keine ausreichend effizienten Möglichkeit zur Unsicherheits-, Sensitivitäts- und Importanzanalyse vorliegen. Schließlich sollten die unter goPSA ansprechbaren Benutzerhilfen nach Erprobung in der Praxis an

Hand der dabei gewonnen Erkenntnisse verbessert bzw. aktualisiert werden. Auch können sich aus Anwendung und Forschung neue Themenfelder für eine Erstellung von Benutzerhilfen bzw. Vorlagen unter goPSA ergeben.

5.5 Untersuchung der PSA-Tauglichkeit des Integralcodes ASTEC für Unfallanalysen unter Einbeziehung neuerer Erkenntnisse zum Radionuklidverhalten

Die durchgeführten Rechnungen zu zwei charakteristischen Unfallszenarien für einen DWR vom Typ KONVOI zeigen die prinzipielle Anwendbarkeit von ASTEC für PSA Analysen der Stufe 2. Dabei ist für ASTEC wie auch für MELCOR festzuhalten, dass der Anspruch eines schnell laufenden Integralcodes hinsichtlich der Rechenzeit mehr und mehr einem gesteigerten Anspruch an die Qualität der Ergebnisse, bedingt durch aufwändigere Anlagennodalisierungen weichen muss. So waren zu Beginn der ASTEC Entwicklungen Rechenzeiten von zwölf Stunden für ein komplettes Störfallszenario anvisiert worden um die Rechnungen sozusagen ‘über Nacht‘ durchzuführen.

Mit fortschreitender Entwicklung mussten diese Vorgaben an die geänderte Anforderungen angepasst werden. Dies hat zwei Gründe: Zum einen ist eine deutliche Tendenz ersichtlich, einfache Modelle, die teilweise parametrischen Ansätzen folgen, durch mechanistische Modellierungen zu ersetzten und somit die Qualität der Rechnungsergebnisse zu erhöhen. Zum anderen sind die teils recht groben Nodalisierungen, z. B. des Containments im Zuge neuerer Erkenntnisse zum Strömungsverhalten und des Einflusses auf Schichtungsphänomene (z. B. Wasserstoff), zunehmend verfeinert worden. Dabei sei an dieser Stelle nochmals betont, dass der Vergleich zweier Integralcodes erstmalig bei der GRS in diesem Umfang durchgeführt worden ist. Frühere Untersuchungen und Vergleiche von MELCOR mit ATHLET-CD oder COCOSYS beschränkten sich nur auf Teilaspekte eines Unfalls, im Gegensatz zu dem hier vorgestellten Arbeiten, die den kompletten Unfallablauf beinhalten, ausgehend vom einleitenden Ereignis (z. B. Leck) bis zur Freisetzung in die Umgebung.

Die hier vorgestellten Rechnungen wurden dabei nicht, wie für PSA der Stufe 2 erforderlich, bis zum Abschluss der Freisetzung von Spaltprodukten in die Umgebung durchgeführt. Im Verlaufe der Arbeiten wurde klar, dass die Unterschiede in den durchgeführten Rechnungen schon frühzeitig, teils schon vor Beginn der Kernzerstörung und Spaltproduktfreisetzung, auftraten. Viele nachfolgende Ereignisse sind dann

direkt ein Ergebnis zeitlich früher liegender Ereignisse. Die Ereignisse, die zur Freisetzung von Spaltprodukten an die Umgebung führen und den Quellterm bestimmen, liegen naturgemäß am Ende der Rechnung. Hier erwies sich als nachteilig, dass wegen der verzögerten Freigabe nicht die deutlich modifizierte Version ASTEC V2.0 eingesetzt werden konnte. Damit ergibt sich für einen Vergleich das Problem, dass Unterschiede sowohl ein Ergebnis unterschiedlicher Modellierung sein können als auch das Ergebnis unterschiedlicher Anfangs- und Randbedingungen. Dies gilt z. B. für die Ex-Vessel Phase nach Versagen des RDB und den Beginn der Kernschmelze-Beton-Wechselwirkung (MCCI).

Ein Vergleich charakteristischer Daten wie z. B. axialer und radialer Betonerosion, wird schon allein dadurch nahezu unmöglich, dass sowohl verlagerte Schmelzemasse als auch Schmelzezusammensetzung als Ergebnis der Kernzerstörungsprozesse im RDB von beiden Programmen recht unterschiedlich berechnet werden. Davon beeinflusst werden natürlich auch die Freisetzung von Spaltprodukten aus der Schmelze, die Freisetzung von Wasserstoff, die thermohydraulischen Gegebenheiten in der Reaktorgrube und demzufolge über die Strömungsverbindungen auch in angrenzenden Containmenträumen. Aussagen hinsichtlich der Qualität der MCCI-Modellierung von ASTEC und MELCOR und eine Erklärung möglicher Unterschiede sind damit praktisch nicht mehr sinnvoll bzw. auch gar nicht möglich. Da die Unterschiede aber schon sehr frühzeitig zu Beginn der Rechnungen auftraten und ausgehend von der Thermohydraulik im Primärkreis somit auch das Aerosol- und Spaltproduktverhalten beeinflussen, ist ein bewertender Vergleich auch hier nur eingeschränkt möglich.

Des Weiteren sind in MELCOR noch keine für Anlagenrechnungen geeigneten Modelle zur Jod-Chemie verfügbar, die insbesondere die Wechselwirkung von Jod- und Jodverbindungen mit anderen Substanzen im Containmentsumpf berücksichtigen. Die mit Blick auf den Quellterm zu berücksichtigende Jodchemie konnte mangels validierter Modelle in MELCOR nicht verglichen werden. Bei ASTEC konnte die prinzipielle Anwendung gezeigt werden, auf eine gezielte Auswertung wurde verzichtet, da der Aufwand zur Bewertung weit über den in diesem Vorhaben möglichen Rahmen hinausging. Eine Analyse dieser Einzeleffekte ist nur im Rahmen einer gezielten Anwendung der Modelle im eingeschränkten Umfang möglich, im Rahmen kompletter Unfallszenarien aber nicht sinnvoll.

Für die Anwendung von ASTEC im Rahmen von PSA der Stufe 2 für komplette Unfallanalysen aber teilweise auch für die Anwendung von Integralcodes ganz allgemein bedeutet dies:

- Mit Blick auf die Qualität der Ergebnisse kann global eine gute Übereinstimmung mit MELCOR konstatiert werden. Im Einzelnen sind die Ergebnisse jedoch einerseits abhängig von der durch den Anwender zu definierenden Nodalisierung sowie naturgemäß von der Güte der in den jeweiligen Codes implementierten Modelle. Ein Vergleich der Ergebnisse legt den Schluss nahe, dass insbesondere die Rückwirkung der Nodalisierung auf die Ergebnisse einen entscheidenden Faktor darstellen kann. Dies gilt insbesondere dann wenn diese frühzeitig im Unfallablauf wirksam werden und demzufolge die nachfolgenden Ereignisse beeinflussen. Im späteren Unfallablauf auftretende Abweichungen lassen sich demzufolge nicht eindeutig einer Ursache zuordnen. Hier wären gezielte Einzelanalysen notwendig, um z. B. die Phase der Beton-Kernschmelze-Wechselwirkung nach RDB-Versagen zu analysieren und die Modelle zu bewerten.

- Eine vergleichende Bewertung von ASTEC und MELCOR wäre weiterhin angeraten, sollte aber ein anderes Konzept verfolgen. Im Gegensatz zu der hier verfolgten Vorgehensweise eines Vergleichs kompletter Rechnungen verschiedener Szenarien, sollte zukünftig ein Vergleich jeweils nur bestimmte Teilsequenzen beinhalten. Als Ergebnis der hier vorliegenden Untersuchungen ist festzustellen, dass die frühe Phase, die im Wesentlichen durch thermohydraulische Phänomene gekennzeichnet ist, auf Grund ihres großen Einflusses auf zeitlich später erfolgende Ereignisse einer genauen Analyse bedarf. Demzufolge sollte ein Vergleich von diesem Punkt ausgehen. Gegebenenfalls sind Ergebnisse von Detailcodes (ATHLET-CD) heranzuziehen. In eingeschränktem Umfang sollten hier Parameter- bzw. Sensitivitätsuntersuchungen vorgenommen werden, um maßgebliche Einflüsse herauszufiltern. Dies wäre insbesondere für die Erstellung von Nutzer-Richtlinien von Vorteil und für die GRS als Co-Entwickler von ASTEC auch angeraten. Für das von GRS hauptverantwortlich betreute ASTEC-Modul CPA zur die Berechnung der Thermohydraulik und des Spalt- und Aerosolverhaltens im Containment wird dies schon seit einiger Zeit verfolgt, da sich auch aus Erfahrungen mit COCOSYS gezeigt hat, dass ein wesentlicher Einflussfaktor der Anwender selbst darstellt. Zwar gibt es schon Richtlinien von Seiten des Hauptentwicklers IRSN für einzelne Module, für die weitere Entwicklung von ASTEC und die Anwendung von ASTEC auf PSA der Stufe 2 auf deutsche Anlagen sind aber eigene Erkenntnisse auch aus dem Vergleich mit anderen

Integralcodes wie MELCOR sinnvoll und notwendig. Mit Blick auf ein komplettes Szenario könnten einzelne Phasen separat untersucht werden. Für einen Vergleich mit MELCOR würde dies bedeuten, dass z. B. nur die MCCI-Phase von beiden Programmen gerechnet wird, wobei der Startpunkt dann der Zeitpunkt des RDB-Versagens bilden würde und identische Randbedingungen spezifiziert würden. Erst dann würden sich etwaige Unterschiede beider Programmsysteme bewerten lassen.

- Mit Blick auf die Rechenzeiten, die teils bei mehreren Wochen liegen, erscheint die Anwendung von ASTEC im Rahmen von Parameter- oder gar Unsicherheitsanalysen für komplette Unfallszenarien nicht mehr sinnvoll. Dies wäre aber insofern angeraten, als dass bisher für ein Unfallszenario immer nur eine Rechnung durchgeführt worden ist. Allerdings können und werden Ergebnisunsicherheiten in der PSA im Ereignisbaum berücksichtigt und dieser kann einfach für Unsicherheitsbetrachtungen genutzt werden. Trotzdem wäre für die Anwendung von ASTEC bei PSA der Stufe 2 die Einschätzung der Genauigkeit bzw. der Sensitivität der Ergebnisse wesentlich. Ein einzelner Wert z. B. für die Wasserstofferzeugung oder für den Quellterm lässt damit keine Aussage zu, wie sich auch nur geringfügige Änderungen in den Randbedingungen auswirken können. Dabei ist nicht allein einer Variation physikalischer Parameter wie z. B. Stoffwerten Rechnung zu tragen, sondern auch solcher Parameter, die vom Anwender frei wählbar sind. Dazu zählt insbesondere die Nodalisierung von Kühlkreislauf, Kern und Containment.

Schließlich ist festzuhalten, dass mit dieser Untersuchung nur ein Teilbereich abgedeckt worden ist. Zukünftig sollten die Analysen auf den Nicht-Leistungsbetrieb sowie auf Anlagen mit SWR erweitert werden. Derzeit ist ASTEC für beide Teilbereiche noch nicht qualifiziert, für MELCOR liegen Ergebnisse bereits vor.

Für Zustände des Nichtleistungsbetriebs existieren nach Aussage des Hauptentwicklers IRSN zwar alle Modelle, eine Validierung steht aber noch aus. Im Hinblick auf die Anwendbarkeit von ASTEC auf Siedewasserreaktoren ist derzeit nur das Modul CPA für den Einsatz im Containment getestet. Auch hier steht eine eingehende Validierung aber noch aus.

Für den Kühlkreislauf des SWR fehlen noch wesentliche Modellerweiterungen. Dies betrifft insbesondere die Darstellung des Kerns, die sich maßgeblich von der eines

DWR unterscheidet, so dass schon die Strömungssimulation nur eingeschränkt durchführbar ist. Für die Phase der Kernzerstörung sind die notwendigen Modellentwicklungen von GRS und IRSN spezifiziert worden. Die Entwicklung wird aber maßgeblich von IRSN als Hauptentwickler getragen, wobei hier die Erfahrungen von GRS unablässig sind, da in Frankreich keine Erfahrungen mit SWR-Anlagen vorliegen. Hier muss mit Verfügbarkeit eines entsprechenden Moduls die GRS entsprechende Arbeiten durchführen. Derzeit werden in enger Zusammenarbeit mit der Entwicklung von ATHLET-CD Erfahrungen ausgetauscht und Teilmodelle dahingehend analysiert, inwieweit sie für den Einsatz in ASTEC verfügbar gemacht werden können.

Die gewonnen Erkenntnisse fließen in die weitere ASTEC-Entwicklung ebenfalls mit ein. Diese betreffen insbesondere Einspeisung von Wasser in einen teilzerstörten Kern sowie die Verbesserung der Simulation der Beton-Schmelze-Wechselwirkung. Während bei ersterem die derzeitige Modellierung in ASTEC einigen Einschränkungen bezüglich spezifischer Zuständen einer Zweiphasenströmung wie Wassereintrag und Gegenströmung (CCFL) im Kern unterliegt ist bei letzterer insbesondere die Berücksichtigung dreidimensionaler Effekte sowie die Abbildung der Wärmeübergangsmechanismen zur umgebenden Reaktorgrube sowie zu Atmosphäre oder Wasserüberdeckung zu verbessern.

6 Referenzen

Die folgenden Berichte /AP1-5/ wurden als Technische Berichte innerhalb des Projektes RS1180 erstellt und sind Teilberichte für die entsprechenden Arbeitspakete zu diesem Abschlussbericht:

/AP1/ HAR 10/ Hartung, J., Piljugin, E.
Entwicklung eines methodischen Ansatzes zur Bewertung menschlicher Zuverlässigkeit beim Einsatz softwarebasierter Leittechnik, Technischer Fachbericht, GRS-A-3548, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Mai 2010

/AP1a/ PIL 10/ Piljugin, E., Herb, J.
Entwicklung eines aktualisierten Ansatzes zur Berücksichtigung softwarebasierter Sicherheitsleittechnik in der PSA, Technischer Fachbericht, GRS-A-3550, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, August 2010

/AP2.1 /FAS 10a/ Faßmann, W., Preischl, W.
Quantitative Bewertung wissensbasierter Handlungen in einer probabilistischen Sicherheitsanalyse, Technischer Fachbericht, GRS-A-3561, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, August 2010

/AP2.2 /FAS 10/ Faßmann, W., Hartung, J., Preischl, W.
Probabilistische Bewertung organisatorischer Einflüsse sowie von Einflüssen des Sicherheitsmanagements auf die Zuverlässigkeit von Personalhandlungen, Technischer Fachbericht, GRS-A-3560, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, August 2010

/AP3.1 /GRE 10a/ Grebner, H., et al.
Weiterentwicklung von Methoden zur Ermittlung von Leck- und Bruchhäufigkeiten druckführender Komponenten, Technischer Fachbericht, GRS-A-3555, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, Juli 2010

/AP3.2 /TUE 10/ Türschmann, M., et al.
Verfahren zur Klassifizierung von Bauwerken, Systemen und Komponenten in Hinblick auf ihre sicherheitstechnische Bedeutung bei seismischen Einwirkungen, Technischer Fachbericht, GRS-A-3472, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln/Berlin, Juni 2010

/AP3.3 /FRE 09/ Frey, W.
Untersuchungen zum Bedarf einer Methodenentwicklung für eine probabilistische Bewertung von Transienten aufgrund von Überspannungen oder Fremdspannungseinträgen, Technischer Fachbericht, GRS-A-3488, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Oktober 2009

/AP4.1 /PES 10/ Peschke, J.
Methodik zur Berücksichtigung epistemischer Unsicherheitsquellen bei der Schätzung von Zuverlässigkeitskenngrößen, Technischer Fachbericht, GRS-A-3540, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, April 2010

/AP4.2 /KLO 10/ Kloos, M.
Bereitstellung einer Methodik zur Anpassung von Beta-Verteilungen an vorgegebene Lognormal-Verteilungen unter Berücksichtigung zusätzlicher Benutzervorgaben, Technischer Fachbericht, GRS-A-3518, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, März 2010

/AP4.3 /PES 10a/ Peschke, J., Krzykacz-Hausmann, B.
Methodenentwicklung zur Durchführung von Unsicherheits- und Sensitivitätsanalysen im Rahmen einer probabilistischen Dynamikanalyse, Technischer Fachbericht, GRS-A-3556, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, August 2010

/AP4.4 /GAL 10/ Gallner, L, Kreuser, A., Leberecht, M., Stiller, J.-C. Methodenentwicklung zur konsistenten Berücksichtigung gemeinsam verursachter Ausfallereignisse (GVA) in PSA, Technischer Fachbericht, GRS-A-3552, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, August 2010

/AP4.5 /WIE 10/ Wielenberg, A., et al. Entwicklung der gemeinsamen Oberfläche goPSA mit den Hilfsprogrammen für PSA-Methoden der Stufe 1, Technischer Fachbericht, GRS-A-3553, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, August 2010

/AP5.1/REI 10/ Reinke, N., Erdmann, W., Nowack, H., Sonnenkalb, M. Vergleichende Unfallanalysen für einen DWR vom Typ KONVOI mit den Integralcodes ASTEC 1.33 und MELCOR 1.8.6, Technischer Fachbericht, GRS-A-3559, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, August 2010

7 Literaturverzeichnis

/ALD 06/ Aldemir, T., et.al.
Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, U.S. Nuclear Regulatory Commission, NUREG/CR-6901, February 2006

/ALD 07/ Aldemir, T., et.al.
Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments, U.S. Nuclear Regulatory Commission, NUREG/CR-6942, October 2007

/ALL 07/ Allelein, H.-J., et al.
Intensivierte Validierung der Rechenprogramme COCOSYS und ASTEC, GRS-A-3330 (Hauptband), Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, November 2007

/BMU 05/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU)
Leitfaden zur Durchführung der ‘Sicherheitsüberprüfung gemäß §19a des Atomgesetzes – Leitfaden probabilistische Sicherheitsanalyse –' für Kernkraftwerke in der Bundesrepublik Deutschland, Bundesanzeiger Nr. 207a vom 03.11.2005

/BMW 05/ Bundesministerium für Wirtschaft und Technologie (BMWi)
Weiterentwicklung und Verifikation von Rechenprogrammen für die Reaktorsicherheit – ein Bericht zum Stand der Entwicklung und zur wissenschaftlichen Weiterführung von Arbeiten der staatlich geförderten Reaktorsicherheitsforschung, BMWi, 30. November 2005

/CHU 08/ Chu, T.L., et.al.
Traditional Probabilistic Risk Assessment Methods for Digital Systems
U.S. Nuclear Regulatory Commission, NUREG/CR-6962, Oktober 2008

/DIN 05/ DIN Deutsches Institut für Normung e. V.
DIN EN 61511: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie, DE Verlag, DIN EN 61511(VDE 0810), Mai 2005

/DIN 09/ DIN Deutsches Institut für Normung e. V.
DIN EN IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme.
Teil 2: Anforderungen, VDE Verlag, E DIN EN 61508-2 (VDE 0803-2), Juni 2009

/EPS 08/ Epstein, S, Rauzy, A. (Hrsg.)
Open-PSA Model Exchange Format, - Draft 2.0d, unveröffentlicht, Mai 2008

/ERV 98/ Erven, U., et al.
Untersuchung von Maßnahmen des anlageninternen Notfallschutzes zur Schadensbegrenzung für LWR,
Abschlussbericht zum Vorhaben SR-2227, GRS-A-2598, Köln, April 1998

/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

/FAK 05a/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke:
Daten zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäumen, Stand: August 2005, BfS-SCHR-38/05,
Wirtschaftsverlag NW / Verlag für neue Wissenschaft GmbH,
Salzgitter; Oktober 2005

/FAS 03/ Faßmann, W., Preischl, W.
Bewertung von Personalhandlungen unter Unfallbedingungen − Methode zur Untersuchung und Bewertung schädlicher Eingriffe des Operateurs, Technischer Fachbericht, GRS-A-3157, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Garching, Oktober 2003

/FIS 09/ Fischer, H. D.
Stand der Einführung digitaler Leittechniksysteme: Ein Beitrag zur Behandlung von gemeinsam verursachten Ausfällen in digitalen Schutzsystemen. ATW, Heft 1/2009, 2009

/FRE 97/ Frese, E.
Organisation, Gabler Wirtschaftslexikon, Gabler Verlag,1997

/GAS 01/ Gaßmann, D., et al.
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 (GRS) mbH, Garching, Februar 2001

/GLO 07/ Glöe, G., et.al.
Integrales Nachweisverfahren, im Vorhaben 'Vorgehen zum effizienten Nachweis der Benutzbarkeit und Sicherheit rechnergestützter Leittechniksysteme', Reaktorsicherheitsforschung - Vorhaben-Nr.: 1501282,
Technischer Fachbericht zum WP 4.3, TÜV NORD SysTec GmbH,
21. Mai 2007

/GLO 08/ Glöe, G., et.al.
Sicherheitsnachweise basierend auf dem Programm-Code, im Vorhaben 'Vorgehen zum effizienten Nachweis der Benutzbarkeit und Sicherheit rechnergestützter Leittechniksysteme', Reaktorsicherheitsforschung - Vorhaben-Nr.: 1501282, Technischer Fachbericht zum WP 4.4, TÜV NORD SysTec GmbH, 29. Februar 2008

/GRE 04/ Grebner, H., Schimpfke, T., Peschke, J., Sievers J.,
Weiterentwicklung der strukturmechanischen Analysemethodik zur Bestimmung der Strukturzuverlässigkeit passiver Komponenten, GRS-A-3236, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, November 2004

/GRE 10/ Grebner, H., Wang, Y., Schimpfke, T., Sievers, J.
Weiterentwicklung der strukturmechanischen Analysemethodik zur Bestimmung der Strukturzuverlässigkeit passiver Komponenten, Phase II, Abschlussbericht, GRS-A-3544, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, 2010

/GRS 02/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH,
Bewertung von Personalhandlungen im Rahmen der Kernkraftwerks-aufsicht, Analysemethoden der GRS, Vortrag Arbeitskreisaufsicht des Länderausschusses Atomenergie, Bonn, 18. September 2002

/GRS 03/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH;
PEAK – Programm zur Ermittlung von Ausfallwahrscheinlichkeiten mit dem Kopplungsmodell; 2003

/GRS 03a/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Dringlichkeitsprojekt Äußere Einwirkungen, Entwicklung von Modellen zur Simulation der Auswirkungen verschiedener gezielter Einwirkungen von außen auf kerntechnische Einrichtungen, Ermittlung von Schadensbereichen (Arbeitsgebiet 7), Technischer Fachbericht, GRS-V-RS1146-AG07/2003, Köln, August 2003

/HAR 09/ Hartung, J.
Verbesserung der Bewertungsbasis für Aspekte des Sicherheitsmanagements und der Schnittstellen zur Sicherheitstechnik sowie für Personalhandlungen, GRS-A-3500, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Oktober 2009

/HOY 74/ Hoyos, C.
Arbeitspsychologie, Kohlhammer Verlag, Stuttgart, 1974

/HUS 84/ Hussy, W.
Denkpsychologie, Band I, Kohlhammer Verlag, Stuttgart, 1984

/IAE 01/ International Atomic Energy Agency (IAEA)
Applications of probabilistic safety assessment (PSA) for nuclear power plants, IAEA-TECDOC-1200, Wien, Februar 2001

/IRS 07/ Institut de Radioprotection et de Sûreté Nucléaire (IRSN)
Principles of PANAME HRA Method, IRSN Report IST3c/BACR, Paris, Mai 2007

/KLO 08/ Kloos, M.
SUSA – Software for uncertainty and sensitivity analyses, Version 3.6, User's Guide and Tutorial, GRS-P-5, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, 2008

/KOR 09/ Korsah, K., et.al.
Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update, U.S. Nuclear Regulatory Commission, NUREG/CR-6992, Washington, DC, Oktober 2009

/KOS 62/ Kosiol, E.
Organisation der Unternehmung, Gabler Verlag, Wiesbaden, 1962

/KRE 97/ Kreuser, A., Peschke, J., Türschmann, M.
Erfassung und Bewertung von gemeinsam verursachten Ausfällen, GRS-A-2445, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, März 1997

/KTA 90/ Kerntechnischer Ausschuss (KTA)
Sicherheitstechnische Regel des KTA: KTA 2201, Auslegung von Kernkraftwerken gegen seismische Einwirkungen, Juni 1990
Teil 1: Grundsätze, Fassung 06/90
Teil 2: Baugrund, Fassung 06/90
Teil 3: Auslegung der baulichen Anlagen (Entwurf), Fassung 06/90
Teil 4: Anforderung an Verfahren zum Nachweis der Erdbebensicherheit für maschinen- und elektrotechnische Anlagenteile, Fassung 06/90
Teil 5: Seismische Instrumentierung, Fassung 06/96
Teil 6: Maßnahmen nach Erdbeben, Fassung 06/92

/KTA 05/ Kerntechnischer Ausschuss (KTA)
Sicherheitstechnische Regel des KTA: KTA 3503, Typprüfung von elektrischen Baugruppen der Sicherheitsleittechnik, Fassung 11/05, November 2005

/MEI 85/ Meister, D.
Behavioral Analysis and Reasurement Methods, Wiley & Sons,
New York, 1985

/NEA 07/ OECD Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI)
The Use and Development of Probabilistic Safety Assessment,
NEA/CSNI/R(2007)12, Paris, November 2007

/NEA 09/ OECD Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI)
Recommendations on Assessing Digital System Reliability in Probabilistic Risk Assessments of Nuclear Power Plants, NEA/CSNI/R(2009)18, Paris, Dezember 2009

/NEI 76/ Neisser, U.
Cognition and Reality, Freeman, San Francisco, CA, 1976

/NOR 55/ Nordsieck, F.
Rationalisierung der Betriebsorganisation, 7. Auflage, Poeschel Verlag, Stuttgart, 1955

/NRC 00/ U.S. Nuclear Regulatory Commission (NRC)
Strategic Plan: Fiscal Year 2000 – Fiscal Year 2005 (NUREG-1614,
Volume 2, Part 1), NUREG/1614, Washington, DC, September 2000

/NRC 04/ U.S. Nuclear Regulatory Commission (NRC)
Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants, NUREG/CR-6842, Washington, DC, März 2004

/NRC 06/ U.S. Nuclear Regulatory Commission (NRC)
Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901, Washington, DC, Februar 2006

/NRC 07/ U.S. Nuclear Regulatory Commission (NRC)
Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments, NUREG/CR-6942, Washington, DC, Oktober 2007

/NRC 08/ U.S. Nuclear Regulatory Commission (NRC)
Traditional Probabilistic Risk Assessment Methods for Digital Systems, NUREG/CR-6962, Washington, DC, Mai 2008

/OHA 02/ O'Hara, J., Brown, W. S., Lewis P. M., Persensky, J. J.:
Human-System Interface Design Review Guidelines, U.S. Nuclear Regulatory Commission, NUREG-0700 Rev. 2, Washington, DC, 2002

/PIL 04/ Piljugin, E., Märtz, J. Heinsohn H., Frey, W.
Anpassung und Erprobung von Methoden zur probabilistischen Bewertung digitaler Leittechnik, GRS-A-3258, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching/Köln, Dezember 2004

/PRE 01/ Preischl, W., Becker, J., Behr, A.
Menschliche Zuverlässigkeit in der probabilistischen Sicherheitsanalyse (PSA) - Teil 1: Untersuchungen zu PSA-relevanten Personalhandlungen, GRS-A-2873, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Garching, Dezember 2000

/PRE 10/ Preischl, W.
Verifikation von Zuverlässigkeitsdaten für Personenhandlungen und Datenverbreiterung im Rahmen der PSA, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, GRS-A-3515, Garching, Januar 2010

/PSA 08/ 8th International Probabilistic Safety Assessment And Management Conference (PSAM9)
Conference Proceedings of PSAM9 Conference, Hong Kong, China, Mai 2008, CD-ROM

/PSA 10/ 10th International Probabilistic Safety Assessment And Management Conference (PSAM10)
Conference Proceedings of PSAM10 Conference, Seattle, WA, USA, Juni 2010, CD-ROM

/RAP 88/ Rappl, G.
On linear convergence of a class of random search algorithms, Journal of applied mathematics and mechanics (ZAMM), Band 69, Issue 1; 1988

/REA 97/ Reason, J.
Managing the Risks of Organizational Accidents, Ashgate, 1997

/REI 10/ Reinke, N., Erdmann, W., Nowack, H., Sonnenkalb, M.
Vergleichende Unfallanalysen für DWR vom Typ KONVOI mit den Integralcodes ASTEC und MELCOR, Technischer Fachbericht, GRS-A-3559, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, August 2010

/SCH 03/ Schwinges, B., et al.
Weiterentwicklung und Fortsetzung der Validierung des Containment-Codesystems COCOSYS und des deutsch-französischen Integralcodes ASTEC, GRS-A-2962, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, September 2003

/SCH 03a/ Schmidt, G.
Einführung in die Organisation, Gabler, Wiesbaden, 2003

/SCH 04/ Schreyögg, G., von Wender, A.
Organisation, Handwörterbuch Unternehmensführung und Organisation, 4. Auflage, Poeschel Verlag, Stuttgart, 2004

/SON 98/ Sonnenkalb, M.
Unfallanalysen für DWR vom Typ KONVOI mit dem Integralcode MELCOR 1.8.3, GRS-A-2579, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, Juni 1998

/SON 01/ Sonnenkalb, M.
Unfallanalysen für DWR vom Typ KONVOI (GKN-2) mit dem Integralcode MELCOR 1.8.4, GRS-A-2954, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, Dezember 2001

/SON 01a/ Sonnenkalb, M.
Vergleich: ATHLET-CD mod 1.1G und MELCOR 1.8.4; GKN-2 - Unfallablauf: Station Black-Out, GRS - V - SR 2306 - 3/2001, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, August 2001

/SON 06/ Sonnenkalb, M., 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 3 – Integrale deterministische Unfallanalysen mit MELCOR für die PSA der Stufe 2 aus dem Leistungsbetrieb, GRS-A-3294, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, April 2006

/STI 09/ Stiller, J.-C., Peschke, J.
Konsistente Berücksichtigung der Unsicherheit bezüglich der Rate von GVA-Ereignissen bei der Anwendung des Kopplungsmodells, GRS-A-3466, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, 2009

/SWA 83/ Swain, A. D., Guttmann, H. E.
Handbook on Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, NUREG/CR-1278, August 1983

/SWA 87/ Swain, A. D.
Accident Sequence Evaluation Program-Human Reliability Analysis Procedure; U.S. Nuclear Regulatory Commission (NRC), NUREG/CR–4772, Washington, DC, 1987

/TAR 77/ Tarasenko, G. S.
Convergence of adaptive algorithms of random search, Cybernetics and system analysis; 1977

/TAR 80/ Tarasenko, G. S.
Über die Konvergenzgeschwindigkeit der adaptiven zufälligen Suche (in Russisch), Problemy slucajnogo poiska, 1980

/THU 09/ Thuma, G., Türschmann, M.
Berücksichtigung von seismisch induzierten Ausfällen im PSA-Anlagenmodell, TÜV-Symposium ‘PSA in der Kerntechnik‘, München November 2009

/TUE 10a/ Türschmann, M., et al.
Modellierung und Quantifizierung erdbebenbedingter Ereignisabläufe., GRS-A-3549, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln/Berlin, August 2010

/WOO 10/ Wood, R. T., et al.
Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, U.S. Nuclear Regulatory Commission, NUREG/CR-7007, Washington, DC, Februar 2010

/ZIP 81/ Zipf, G.
STREUSL - Ein Rechenprogramm zur Ermittlung der Streuung von Zuverlässigkeitskenngrößen aufgrund der Streuungen der Eingabedaten, GRS-A-588, Gesellschaft für Reaktorsicherheit (GRS) mbH, Garching, 1981

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Forschungszentrum
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de