MCDET

Methode zur Integralen Deterministisch-Probabilistischen Sicherheitsanalyse

GRS - 520

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

MCDET

Methode zur Integralen Deterministisch-Probabilistischen Sicherheitsanalyse

Methodische Weiterentwicklung und Anwendungen zur probabilistischen Dynamikanalyse

Joerg Peschke
Nadine Berner
Werner Faßmann
Alexander Kerner
Martina Kloos
Gerhard Mayer
Wolfgang Preischl
Josef Scheuer

September 2018

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des BMWi (Bundesministerium für Wirtschaft und Energie) unter dem Kennzeichen RS1529 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Auftragnehmer.

Der Bericht gibt die Auffassung und Meinung des Auftragnehmers wieder und muss nicht mit der Meinung des Auftraggebers übereinstimmen.

GRS - 520
ISBN 978-3-947685-05-9

Deskriptoren

Aleatorische und Epistemische Unsicherheiten, Crew-Modul, Integrale Deterministisch-Probabilistische Sicherheitsanalyse (IDPSA), MCDET, MCDET/ ATHLET-CD, Thermisch-Induziertes Heizrohr Versagen, Wissensbasiertes Handeln

Kurzfassung

Die integrale deterministisch-probabilistische Sicherheitsanalyse (IDPSA), oft auch als probabilistische Dynamikanalyse oder dynamische PSA bezeichnet, ist ein aktuelles und praktisch bedeutsames Forschungsgebiet, auf dem international Forschungseinrichtungen tätig sind. Der wesentliche Vorteil der Anwendung einer IDPSA in der Reaktorsicherheit besteht darin, die Vielfalt möglicher Verläufe sicherheitstechnisch wichtiger Prozesse unter möglichst realistischen Annahmen repräsentieren, analysieren und angemessen bewerten zu können. Insbesondere schafft es die IDPSA unter Verwendung von MCDET, den zufälligen Schwankungen der Zeitpunkte, zu denen Ereignisse eintreten, und den komplexen Wechselwirkungen von Phänomenen eines Unfallablaufs gerecht zu werden und ihre Auswirkungen auf den Prozessablauf zu quantifizieren. Durch den Einsatz fortschrittlicher dynamischer Methoden, wie sie in diesem Projekt entwickelt und erfolgreich angewendet wurden, kann die Sicherheitsbeurteilung von Risikotechnologien deutlich verbessert werden.

Mit den in diesem Projekt durchgeführten Entwicklungsarbeiten zum MCDET-Scheduler und ATHLET-CD Treiber wurde die Anwendung von MCDET insbesondere in Verbindung mit den GRS-Programmen ATHLET und ATHLET-CD erheblich vereinfacht. Gleichzeitig wird durch den neu entwickelten MCDET-Scheduler eine wesentlich effizientere Abarbeitung der vielfältigen Unfallabläufe erzielt, die im Rahmen einer MCDET-Analyse gerechnet werden. In Verbindung mit dem Werkzeug MCDET können ATHLET und ATHLET-CD nun auch zur Durchführung von integralen deterministisch-probabilistischen Sicherheitsanalysen eingesetzt werden, womit das Anwendungsspektrum dieser Programme erheblich erweitert wird.

Der neu entwickelte MCDET-Scheduler und ATHLET-CD Treiber wurde im Rahmen einer durchgeführten IDPSA zum thermisch induzierten Dampferzeuger-Heizrohrversagens in einem Hochdruck-Kernschmelzunfall erfolgreich angewendet. Dabei wurden stochastische Einflussgrößen berücksichtigt sowie deren Auswirkungen auf den Unfallablauf quantifiziert, die mit den bisherigen Methoden nicht ausreichend berücksichtigt werden können, z. B. Einfluss zufälliger Ausfallzeitunkte der DH-Ventile oder Auswirkungen von Vorschädigung des DE-Heizrohrs auf das DEHEIRO-Versagen.

Eine weitere Zielsetzung des Projekts bestand in der Entwicklung und beispielhaften Anwendung einer Methode, mit der wissensbasiertes Handeln auch in Ereignisabläufen berücksichtigen werden kann, die wegen ihrer Dynamik und Komplexität bevorzugt mit

einer dynamischen ausgelegten Methodik analysiert und bewertet werden sollten. Aus diesem Grund wurde die Methodik zum wissensbasierten Handeln so weiterentwickelt, dass sie mit dem Crew-Modul im Rahmen einer dynamischen menschlichen Zuverlässigkeitsanalyse modelliert werden kann. Die entwickelte Methode wurde an einem ausgewählten Ereignis aus der deutschen Betriebserfahrung erprobt und verifiziert.

Abstract

Internationally the integral deterministic-probabilistic safety analysis (IDPSA) is considered as an important research area. The advantage applying an IDPSA in reactor safety analysis is to appropriately represent and evaluate the large variety of possible accident sequences which may arise from stochastic influences. Above all, an IDPSA with MCDET allows to consider time dependent interactions as well as the variety of random times of events and to quantify their effect on the accident sequence. Safety assessment can be considerably improved by application of advanced dynamic methods as, for example, MCDET which can be used to perform an IDPSA.

With the development of the new MCDET-scheduler and ATHLET-CD driver the practicability of applying MCDET in combination with ATHLET and ATHLET-CD was essentially improved. Additionally, the large variety of accident sequences simulated in an MCDET analysis were processed more efficiently. In addition to mere deterministic analysis ATHLET and ATHLET-CD in combination with MCDET now can be applied to perform an integrated deterministic-probabilistic safety analysis.

The newly developed MCDET-scheduler and driver of ATHLET-CD were successfully applied within an IDPSA on a thermally induced steam generator tube rupture in a high-pressure scenario. Stochastic influences were considered and probabilistically quantified which until now could not be analyzed in the required detail due to the lack of appropriate methods. For example, the influence of random failure time of pressurizer valves or the degradation of steam generator U-tube at the beginning of the accident scenario on steam generator tube rupture.

A further objective was the development of knowledge-based behavior in the context of a dynamic analysis. Due to its complexity and inherent interactions knowledge-based behavior should be preferably modeled and quantified with advanced dynamic methods which allow a more detailed analysis. For that reason, the method of knowledge-based behavior was modeled with the Crew-Module which is a method to model and simulate a human procedure as a dynamic process. The proposed methodology of dynamic human reliability analysis was successfully applied on a selected incident from the German operational experience data-base.

Inhaltsverzeichnis

1 Einleitung und Überblick

Die in der GRS entwickelten deterministischen Rechenprogramme ATHLET und ATHLET-CD sind unentbehrliche Werkzeuge, die für Stör- und Unfallanalysen zur Sicherheitsbewertung von Kernkraftwerken eingesetzt werden. Deterministische Rechenprogramme sind dazu ausgelegt, Szenarien unter fest vorgegebenen Randbedingungen zu berechnen. Auswirkungen stochastischer Einflüsse, die eine zufällige Änderung der Randbedingungen zu bestimmten Zeitpunkten während des Unfallablaufs bewirken, können in den deterministischen Rechenprogrammen nicht berücksichtigt und probabilistisch bewertet werden.

Die Arbeiten in diesem Vorhaben dienen u. a. dazu, das Anwendungsspektrum der deterministischen Rechenprogramme um den probabilistischen Aspekt zu erweitern sowie die Qualität und Aussagekraft von Sicherheitsanalysen zu verbessern. Dazu wird ein Werkzeug bereitgestellt, das mit deterministischen Rechenprogrammen gekoppelt werden kann, um damit den Einfluss beliebiger Unsicherheiten – sowohl aufgrund des Kenntnisstands (epistemisch) als auch aufgrund zufälliger Ereignisse (aleatorisch) – in den zu analysierenden Stör- und Unfallsimulationen zu berücksichtigen. Die Ergebnisse dieser Simulationen liefern Informationen sowohl über den zeitlichen Verlauf von Prozessgrößen in Abhängigkeit der berücksichtigten Unsicherheiten als auch über die Wahrscheinlichkeit, mit der diese Verläufe eintreten. Durch geeignete statistische Auswertungen der Simulationsergebnisse können probabilistische und risikoinformierte Aussagen abgeleitet werden.

Im Rahmen des Projekts RS1111 /HOF 01/ hat die GRS mit der Entwicklung der Methode MCDET (Monte Carlo Dynamic Event Tree) begonnen, die aus einer Kombination von Monte Carlo Simulation und Dynamischer Ereignisbaumanalyse besteht. Die Methodik wurde in dem gleichnamigen Werkzeug als Prototypversion umgesetzt und erfolgreich an verschiedenen Anwendungsbeispielen /KLO 06/, /PES 14/ erprobt. Anhand der durchgeführten Anwendungsbeispiele konnte gezeigt werden, dass unter Verwendung von MCDET eine integrale deterministisch-probabilistische Sicherheitsanalyse (IDPSA) durchgeführt werden kann. Dabei lassen sich sowohl epistemische als auch beliebige aleatorische Unsicherheiten berücksichtigen, die zum Zeitpunkt ihres zufälligen Auftretens direkt in die Simulationen des deterministischen Rechenprogramms eingehen.

Eine IDPSA (oft als probabilistische Dynamikanalyse oder dynamische PSA bezeichnet) unter Verwendung von MCDET ermöglicht eine umfassende und realitätsnahe

Berücksichtigung der Wechselwirkungen zwischen den als relevant erachteten Unsicherheiten und der mit dem deterministischen Rechenprogramm simulierten Prozessdynamik. Der wesentliche Vorteil ihrer Anwendung in der Reaktorsicherheit besteht darin, die Vielfalt möglicher Abläufe sicherheitstechnisch wichtiger Prozesse unter möglichst realistischen Annahmen modellieren, analysieren und probabilistisch quantifizieren zu können. Die Unsicherheiten werden dabei gemäß ihrer spezifizierten Wahrscheinlichkeitsverteilung in der Analyse repräsentiert.

Insbesondere schafft es die IDPSA wie keine andere Analyse, den Variationen der zufälligen Zeitpunkte, zu denen Ereignisse eintreten, und den komplexen Wechselwirkungen von Phänomenen eines Unfallablaufs gerecht zu werden und ihre Auswirkungen auf den Prozessablauf zu quantifizieren. Eine solche dynamische (zeitabhängige) Analyse sprengt die Möglichkeiten einer klassischen probabilistischen Sicherheitsanalyse (PSA), die aufgrund ihres statischen Charakters und der in der praktischen Anwendung beschränkten Möglichkeit des Bezugs auf bestimmte wenige Simulationsläufe mit erheblichen Modellvereinfachungen und groben Abschätzungen arbeiten muss. Durch den Einsatz der fortschrittlichen dynamischen Methode MCDET können die aus Sicherheitsanalysen gewonnenen Aussagen sowohl qualitativ als auch quantitativ verbessert werden.

Trotz der großen Fortschritte, die bei der Methodenentwicklung in den letzten Jahren erzielt wurden, erfordert die praktische Umsetzung und allgemeine Anwendbarkeit einer IDPSA unter Verwendung des Werkzeugs MCDET aufgrund ihrer hohen Komplexität noch weitere Entwicklungsarbeiten. Zum einen müssen die mathematischen Modelle und die Einsatzmöglichkeiten aktueller Computertechnologie so weiterentwickelt werden, dass die Durchführung einer IDPSA durch einen Anwender in der Praxis schneller und einfacher durchgeführt werden kann. Zum anderen müssen die Ergebnisse in einer Form aufbereitet werden, die dem Anwender die wesentlichen Erkenntnisse zutreffend und übersichtlich vermittelt.

Ein weiterer thematischer Schwerpunkt ist die Einbeziehung der zeitabhängigen Wechselwirkungen zwischen menschlichen Handlungen und dem zu analysierenden Stör- bzw. Unfallablauf in eine probabilistische Dynamikanalyse. Zu diesem Zweck sind Methoden zu entwickeln und umzusetzen, mit denen menschliche Handlungen als dynamischer Prozess modelliert und simuliert werden können. Im Vorhaben RS1148 wurde das Analysewerkzeug MCDET um das Crew-Modul erweitert /PES 06/. Handlungsabläufe des Personals, die synchron und in Wechselwirkung mit der Prozessdynamik erfolgen,

können damit sehr detailliert analysiert und bewertet werden. Dies wurde an dem durchgeführten Anwendungsfall zur sekundärseitigen Druckentlastung infolge eines unterstellten „Station Black Out“ (SBO)-Szenarios am Beispiel eines generischen DWR-Simulationsmodells demonstriert.

Das vorliegende Projekt RS1529 umfasst sowohl methodische und programmtechnische Entwicklungsarbeiten als auch deren Umsetzung und Anwendung in konkreten Analysen. Das Projekt gliedert sich in drei Arbeitspunkte:

1. Methodische und programmtechnische Weiterentwicklungen zur Vereinfachung und Verbesserung der Anwendungsmöglichkeiten des Analysewerkzeugs MCDET

2. Analyse und Bewertung des Einflusses relevanter Unsicherheiten auf thermisch induziertes Dampferzeuger-Heizrohrversagen bei Hochdruck-Kernschmelze nach einem SBO

3. Methodenentwicklung zur Analyse und Bewertung wissensbasierter Handlungen unter Verwendung der MCDET-Methode sowie Erprobung an einem Ereignis aus der deutschen Betriebserfahrung

Die Arbeiten zur methodischen und programmtechnischen Weiterentwicklung, um die Praktikabilität von MCDET-Analysen zu verbessern und für den Anwender einfacher zu gestalten, werden in Abschnitt 2 behandelt.

Ein wesentliches Merkmal zur Verbesserung der Praktikabilität von MCDET-Analysen besteht in der Reduzierung des hohen Rechenzeitbedarfs, der sich durch die hohe Anzahl der verschiedenen Rechenläufe mit dem zugrundeliegenden deterministischen Rechenprogramm ergibt. Eine Möglichkeit zur Reduzierung der Rechenzeit besteht in einer effizienten Steuerung des Ablaufs der Simulationen im Rahmen einer MCDET-Analyse. In Abschnitt 2.1 werden die grundlegenden Arbeiten zur Entwicklung und Umsetzung des neuen Konzepts für ein standardisiertes Steuerungsprogramm von MCDET (MCDET-Scheduler) beschrieben. Durch den neu entwickelten MCDET-Scheduler wird die Durchführung von parallelen Simulationen auf Multiprozessor-Systemen innerhalb eines dynamischen Ereignisbaumes ermöglicht. Außerdem werden in diesem Abschnitt die zugehörigen Entwicklungsarbeiten zur Erstellung eines ATHLET und ATHLET-CD Treiberprogramms erläutert, mit denen MCDET speziell mit den GRS-eigenen Programmen ATHLET und ATHLET-CD verbunden werden kann. Dadurch können die gekoppelten MCDET/ATHLET bzw. MCDET/ATHLET-CD Versionen zur Durchführung von

integrierten deterministisch-probabilistischen Sicherheitsanalysen eingesetzt werden. Unter Verwendung des neu entwickelten MCDET-Schedulers und dem ATHLET-Treiberprogramm können die umfangreichen IDPSA Rechenläufe wesentlich einfacher angewendet und effizienter durchgeführt werden. Daneben wird die Umsetzung weiterer Möglichkeiten diskutiert, um den hohen Rechenaufwand von MCDET-Analysen reduzieren zu können.

Abschnitt 2.2 behandelt die Arbeiten zur Weiterentwicklung des Crew-Moduls, das zur Modellierung und Simulation von dynamischen Handlungsabläufen eingesetzt werden kann. Dazu wurde ein Konzept entwickelt und umgesetzt, das dem Anwender ermöglicht, den zu analysierenden Handlungsablauf über eine grafische Benutzeroberfläche in einer strukturierten Form zu beschreiben. Außerdem wurden Arbeiten durchgeführt, die die aufwendige Erstellung des kodierten Eingabedatensatzes für das Crew-Modul automatisiert. Diese Arbeiten tragen zu einer erheblichen Vereinfachung und Verringerung der Fehleranfälligkeit bei der Erzeugung des umfangreichen Eingabedatensatzes und für die allgemeine Anwendbarkeit des Crew-Moduls bei.

Die Arbeiten zur Auswertung und Visualisierung der umfangreichen Ergebnisse einer IDPSA, die unter Verwendung von MCDET erzeugt worden sind, werden in Abschnitt 2.3 beschrieben. Dabei werden Konzepte vorgestellt, die zur Aufbereitung, Auswertung und Darstellung der Ergebnisse für unterschiedliche sicherheitsrelevante Fragestellungen eingesetzt werden können.

Als interessanter Anwendungsfall, in dem die MCDET-Methode zur Durchführung einer IDPSA eingesetzt werden kann, wird die Problematik des thermisch induzierten Dampferzeuger-Heizrohrlecks angesehen. Ein nicht absperrbares, thermisch induziertes Dampferzeuger-Heizrohrleck bei einem schweren Unfall mit Kernschmelze kann zu sehr hohen Radionuklidfreisetzungen in die Umgebung führen.

Abschnitt 3 beschäftigt sich mit der Analyse und Bewertung des Einflusses relevanter epistemischer und aleatorischer Unsicherheiten auf thermisch induziertes Dampferzeuger-Heizrohrversagen in einer Hochdruck-Kernschmelzsituation. Dem thermisch-induzierten Heizrohrversagen unter Hochdruck-Kernschmelze wird ein SBO-Unfallszenario unterstellt. Die Analyse erfolgt über eine IDPSA unter Verwendung von MCDET/ATHLET-CD. Diese Anwendung diente zugleich der erfolgreichen Erprobung des neu entwickelten MCDET-Schedulers und der Kopplung von MCDET mit ATHLET-CD. Die Analyse zeigt, dass Auswirkungen stochastischer Einflussgrößen quantifiziert

werden können, deren Berücksichtigung mit den Methoden der klassischen PSA nicht möglich ist. Die Analyse kann somit Fragestellungen behandeln, die bisher noch nicht untersucht wurden und aus denen neue Einsichten und Kenntnisse bzgl. des Dampferzeuger-Heizrohrversagens erzielt werden können.

Die Abschnitte 3.1 und 3.2 beschäftigten sich mit dem Anwendungsfall und dem deterministischen Modell. Dazu wird erläutert welche Arbeiten am ATHLET-CD Eingabedatensatz für die Analyse vorgenommen und welche Annahmen bzgl. des SBO-Unfallszenarios zugrunde gelegt wurden.

Die in der Analyse berücksichtigten Unsicherheiten werden in Abschnitt 3.3 behandelt. Dabei wird insbesondere auf die Herleitung der Wahrscheinlichkeitsmodelle eingegangen, die zur Abschätzung der aleatorischen Unsicherheiten

- bzgl. der Ausführungszeiten menschlicher Handlungen im Rahmen des sekundärseitigen Druckentlastens,
- bzgl. des Ausfallverhaltens der Druckbegrenzungsventile in Abhängigkeit ihrer Anforderungszyklen sowie
- bzgl. des Schädigungsgrades des DE-Heizrohrs zu Beginn des Unfallablaufs

angewendet werden. Des Weiteren werden die Wahrscheinlichkeitsverteilungen derjenigen Parameter definiert, die als epistemische Unsicherheiten in die Analyse eingehen.

Die wesentlichen aleatorischen Unsicherheiten beziehen sich auf die Unsicherheit

- bzgl. der Zeit, die die Schichtmannschaft zur Durchführung verschiedener Teilaufgaben im Rahmen der Notfallmaßnahme ‚Sekundärseitiges Druckentlasten' benötigt. Die Unsicherheiten der Ausführungszeiten für die Teilaufgaben wurden über das Crew-Modul ermittelt. Dabei wurden insbesondere diejenigen Teilaufgaben analysiert, die abgeschlossen sein müssen, bevor die entsprechenden Prozesskriterien zur Druckentlastung anstehen und es somit zu Wechselwirkungen zwischen dem Handlungsablauf und Prozesszustand kommen kann,
- bzgl. des Anforderungszyklus bzw. des Zeitpunkts, wann die Ventile zur automatischen Druckbegrenzung (DH-Abblaseventil sowie Sicherheitsventil 1 und 2) zufällig ausfallen. Für das zufällige Ausfallverhalten der einzelnen Ventile wurde auf Basis von Daten aus der Betriebserfahrung ein Modell erstellt, mit dem die

Wahrscheinlichkeit ermittelt werden kann, bei der ein Ventil zu einem bestimmten Anforderungszyklus in geschlossener oder offener Stellung ausfällt,

- bzgl. der Schädigung, die das Heizrohr zu Beginn des Unfallablaufs hat. Zur Ermittlung dieser Unsicherheit wurde ein Modell entwickelt, das auf einer Markov-Kette basiert und den zeitlichen Abstand zwischen zuletzt erfolgtem Test des Heizrohrs und Eintritt des auslösenden SBO-Ereignisses berücksichtigt. Die Annahmen, die der Entwicklung des Modells zugrunde liegen, wurden aus den Informationen der KTA 3201 abgeleitet.

In Abschnitt 3.4 wird auf die Modellierung eingegangen, in welcher Form die aleatorischen und epistemischen Unsicherheiten in die Analyse eingebunden werden. In diesem Zusammenhang wird gezeigt, dass die Modellierung, wie die Unsicherheiten in die Analyse eingebunden werden, Einfluss auf die Rechenzeit der Analyse haben kann. Auf die Auswertung und Darstellung einiger Analyseergebnisse wird in Abschnitt 3.5 eingegangen. In Abschnitt 3.6 erfolgt eine ausführliche Diskussion, welchen Nutzen und Vorteil die Anwendung der Methode MCDET im Rahmen einer probabilistischen Sicherheitsanalyse erbringt.

Lange lag der Schwerpunkt bei der menschlichen Zuverlässigkeitsanalyse in der Analyse regelbasierten Handelns. Seit einigen Jahren wird auch an der Entwicklung von Methoden für die Analyse und Bewertung wissensbasierter Handlungen gearbeitet (vgl. /FAS 10/). In der erfolgreichen Durchführung wissensbasierter Handlungen, z. B. Reparaturhandlungen oder neuer situativ geplanter Ersatzhandlungen, ist noch eine erhebliche Sicherheitsreserve zu erwarten, durch die Unfälle verhindert oder deren Auswirkungen verringert werden können. Für alle diese Methoden gilt, dass ihr Anwendungsbereich bisher auf die klassische PSA beschränkt war. Viele Methoden sehen zudem nur eine globale Expertenschätzung vor, um den Beitrag wissensbasierten Handelns zu quantifizieren. Bei wissensbasiertem Handeln muss das Personal jedoch in der Situation ad hoc das erforderliche Vorgehen erkennen, entwickeln und implementieren. Das kann zahlreiche Schritte der Aufnahme und Verarbeitung von Informationen sowie der Planung und Bewertung von Handlungsoptionen erfordern, woraus sich vielfältige Handlungsabläufe ergeben können, welche die klassische PSA nicht im Detail erfasst. Dazu bedarf es eines dynamischen Ansatzes.

Auf die Methodenentwicklung zur Analyse und Bewertung wissensbasierter Handlungen sowie deren Erprobung und Einbindung in eine probabilistische Dynamikanalyse wird in Abschnitt 4 eingegangen. Die Methodik zur Modellierung wissensbasierter Handlungen wird in Abschnitt 4.1 beschrieben. In Abschnitt 4.2 wird die Methodik an einem Ereignis aus der deutschen Betriebserfahrung unter Verwendung des Crew-Moduls und MCDET angewendet. Bei der Beispielanwendung handelt es sich um ein Ereignis aus der deutschen Betriebserfahrung, in dem das Personal wissensbasiert einen Precursor eines LOCA beherrscht hat. Das Ereignis wird ausführlich beschrieben und mit dem Crew-Modul unter Berücksichtigung wissensbasierter Handlungen modelliert und simuliert. Die Simulationsergebnisse werden ausgewertet und diskutiert.

2 Methodische und programmtechnische Weiterentwicklung des Analysewerkzeugs MCDET

Trotz der großen Fortschritte, die die GRS bei der Methodenentwicklung in den letzten Jahren zur probabilistischen Dynamikanalyse erzielt hat, erfordert die praktische Umsetzung und allgemeine Anwendbarkeit einer IDPSA unter Verwendung des Werkzeugs MCDET aufgrund ihrer hohen Komplexität noch weitere Entwicklungsarbeiten. Zum einen müssen die mathematischen Modelle und Methoden für eine benutzerfreundliche Anwendung so weiterentwickelt werden, dass die Durchführung einer IDPSA durch einen Anwender in der Praxis schneller und einfacher durchgeführt werden kann. Zum anderen müssen die umfangreichen Ergebnisse einer IDPSA mit MCDET so ausgewertet und aufbereitet werden, dass sie dem Anwender die wesentlichen Erkenntnisse und Antworten zu den Fragestellungen zutreffend und übersichtlich vermitteln können. Dazu sind entsprechende Postprocessing Programme zu entwickeln, die eine möglichst benutzerfreundliche Anwendung zur Auswertung bei gleichzeitig hoher Flexibilität der darzustellenden Ergebnisse ermöglichen.

In Abschnitt 2.1 wird die Struktur des MCDET-Scheduling-Systems sowie dessen Vorteile in Bezug auf MCDET-Analysen beschrieben. Außerdem werden die Entwicklungsarbeiten zur Erstellung eines ATHLET und ATHLET-CD Treiberprogramms erläutert, mit denen MCDET speziell mit den GRS eigenen Programmen ATHLET und ATHLET-CD verbunden werden kann.

Abschnitt 2.2 behandelt die Arbeiten zur Weiterentwicklung des Crew-Moduls, das zur Modellierung und Simulation von dynamischen Handlungsabläufen eingesetzt werden kann.

Durch den neu entwickelten MCDET-Scheduler und der damit verbundenen neuen Ausgabestruktur der Ergebnisse, müssen auch die Postprocessing Programme daran angepasst werden, um mit den fortschrittlichen programmiertechnischen Methoden kompatibel zu sein. Abschnitt 2.3 beschreibt die Entwicklungsarbeiten zum Postprocessing für die umfangreichen Ergebnisse, die im Rahmen einer MCDET-Analyse erzeugt wurden.

Eine der größten Herausforderungen bei der gekoppelten Anwendung von MCDET mit deterministischen Rechenprogrammen ist der erhebliche Rechenaufwand und die dazu benötigte Rechenzeit. Aus diesem Grund sind Überlegungen und Konzeptentwicklungen zur Reduzierung der Rechenzeit ein ständig aktuelles Thema für Weiterentwicklungs-

arbeiten. Abschnitt 2.4 diskutiert Möglichkeiten, die nach aktuellem Stand zur Reduzierung der Rechenzeit eingesetzt werden können.

Insgesamt zielen die in diesem Abschnitt beschrieben Arbeiten vornehmlich darauf ab, dass die Anwendung und der Einsatz von MCDET für Anwender vereinfacht und damit die Anwendungsmöglichkeiten von MCDET vorangetrieben werden.

2.1 Entwicklung des MCDET-Scheduling-Systems

Um die Einsatzmöglichkeiten von MCDET weiter voranzutreiben und einem breiteren Anwenderkreis zugänglich zu machen, musste die ursprüngliche Prototypversion von MCDET weiterentwickelt werden, für deren Anwendung noch tiefgehendes Detailwissen über Programmstruktur und dessen Konfiguration erforderlich war und welche praktisch nur von den Entwicklern eingerichtet werden konnte. Bei diesen Weiterentwicklungsarbeiten wurde insbesondere darauf Wert gelegt, aktuelle Methoden der Softwareentwicklung einzusetzen, um MCDET für ein breites Anwendungsspektrum vorzubereiten und es schnell, flexibel und möglichst einfach anwenden zu können.

2.1.1 Problemstellung und Übersicht

Die Durchführung von MCDET-Analysen erfordert das Zusammenspiel vieler verschiedener Komponenten. Abhängig vom Computersystem, welches hierzu eingesetzt wird, kann es zu Unterschieden im Aufbau oder in der Ausführung einzelner Programmteile kommen. Außerdem müssen Gegebenheiten wie Speicherausstattung, Eigenschaften des zugrundeliegenden Betriebssystems, Eigenheiten des deterministischen Rechencodes oder auch die Verfügbarkeit von Laufzeitbibliotheken berücksichtigt werden. Diese Anforderungen sind zwar essentiell, um die Ablauffähigkeit aller Programmteile sicherzustellen, dennoch wird von einer benutzerfreundlichen Anwendung erwartet, die Komplexität dieser Ebene vor dem Benutzer zu verbergen.

In der Entwicklung von Systemen wird allgemein versucht der hohen Komplexität durch eine möglichst modulare Struktur zu begegnen und die Verflechtung der unterschiedlichen Programmteile durch klare Schnittstellen zu vermeiden. Wie in Abb. 2.1 dargestellt, wurde deshalb auch im Aufbau des MCDET-Scheduling-Systems der Ansatz verfolgt den generischen Teil der Ablaufsteuerung (Scheduler) von den spezifischen Teilen zu trennen, welche die Ansteuerung sowie den Datenaustausch mit dem Probabilistikmodul

(MCDET-Kern) und dem gekoppelten Rechencode regeln. Die einzelnen Komponenten übernehmen dabei folgende Aufgaben:

- **Probabilistikmodul (PM):** Übernimmt die regelbasierte Bewertung von Simulationszuständen und bestimmt die Zustandsänderungen beim Abzweigen neuer Simulationspfade,
- **Simulator (Sim):** Deterministischer Rechencode zur dynamischen Simulation,
- **Scheduler:** Übernimmt die Ablaufsteuerung und überwacht die Abarbeitung aller Simulationsprozesse,
- **Analysemodule (AM):** verschiedene Funktionsmodule zur graphischen Darstellung und probabilistischen Analyse der Simulationsergebnisse.

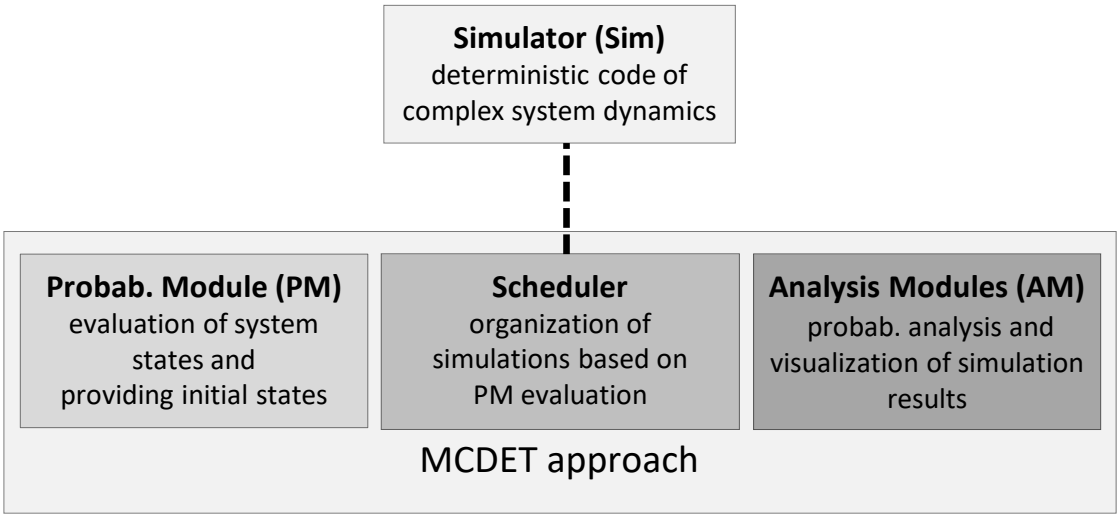


Abb. 2.1 Grundlegende Komponenten des Analysewerkzeugs MCDET

2.1.2 Anforderungen an koppelbare Rechencodes

Das Scheduling-System wurde entworfen, um sowohl mit verschiedenen Probabilistikmodulen als auch mit unterschiedlichen Simulatoren verwendet werden zu können. Allerdings haben diese Rechencodes oft eine sehr lange Entwicklungsgeschichte und bringen dadurch meist auch sehr unterschiedliche Voraussetzungen mit. In aller Regel ist der entsprechende Quellcode nicht verfügbar, wodurch die Simulatoren auch nicht in ihrem Verhalten angepasst werden können. Um dennoch abschätzen zu können ob und mit welchem Aufwand ein Rechencode mit dem Scheduling-System gekoppelt werden kann, wurden folgende grundlegenden Eigenschaften angenommen:

- **Taktsteuerung:** Der Simulator teilt die simulierte Zeit in diskrete Schritte ein und berechnet die einzelnen Zeitschritte entsprechend eines von außen vorgegebenen Takts (tick-Befehl).
- **Statusangabe:** Der Status des Simulators kann von außen abgefragt werden. Dieser gibt Auskunft darüber, ob der Simulator gerade einen Zeitschritt berechnet (busy), auf einen neuen Befehl wartet (idle) oder bereits beendet ist (zombie).
- **Datenzugriff:** Der Simulator stellt den Zustand der Simulation, d. h. sämtliche für die Kopplung notwendigen Signale und Systemgrößen bereit und erlaubt auch diese für die weiteren Berechnungen zu verändern.
- **Klonfähigkeit:** Der Simulator bietet für die Behandlung von Verzweigungspunkten eine Möglichkeit eine laufende Simulation zu duplizieren (fork). Eine Methode hierfür ist die Speicherung des aktuellen Systemzustandes als Restartpunkt und die Erstellung eines neuen Simulationsprozesses, der die Berechnung an diesem Punkt fortführt.
- **Terminierung:** Der Simulator bietet für den Fall einer zu unwahrscheinlichen Ereignissequenz die Möglichkeit eine laufende Simulation explizit zu beenden.

Da die Rechencodes in aller Regel diese Anforderungen nicht direkt erfüllen und auch zu dem vom Scheduler verwendeten Befehlssatz nicht kompatibel sind, wurde die Simulator-Ansteuerung über eine Treiber-Schnittstelle realisiert, die es erlaubt, fehlende oder inkompatible Eigenschaften in Form eines Simulator-Treibers zu implementieren (siehe auch Abschnitt 2.1.6). Grundsätzlich lässt sich damit ein sehr breites Spektrum an Simulatorcodes unterstützen. Abhängig von den Möglichkeiten des Simulatorcodes können die so bereitgestellten Befehle aber in ihrem Laufzeitverhalten eventuell sehr ineffizient sein.

2.1.3 Ablauf von MCDET-Rechenläufen

Die essentielle Herausforderung an das MCDET-Analysewerkzeug ergibt sich aus der Notwendigkeit, mit begrenzten Systemressourcen möglichst effizient eine sehr große Anzahl von Simulationspfaden zu berechnen. Für alle Pfade müssen die einzelnen Systemzustände der jeweiligen Simulationen gemäß der im MCDET-Input spezifizierten Regeln bewertet werden. Diese Bewertungen finden nach jedem Zeitschritt statt, um Unterpfade mit veränderten Bedingungen abspalten zu können und so mit einem deterministischen Rechencode stochastisches Verhalten zu simulieren.

Zur Berechnung eines DETs (siehe Abb. 2.2, (A)) müssen alle Simulationspfade einzeln und voneinander unabhängig verfolgt werden. Ausgehend von der DET-Wurzel wird dazu ein Simulationsprozess (Root Process) gestartet, welcher die deterministische Simulation schrittweise durchführt und nach jedem Zeitschritt dem Probabilistikmodul seinen Systemzustand zur Bewertung bereitstellt. Entscheidet das Probabilistikmodul, dass zum gegebenen Simulationszeitpunkt ein nicht-deterministisches Ereignis auftritt, kommt es zur Abspaltung von möglicherweise mehreren Simulationsprozessen, in denen die Auswirkungen des Ereignisses in eigenen Unterpfaden weiterverfolgt werden. Nachdem alle Abspaltungen des Ereignispunkts als Unterprozesse gestartet wurden, wird der ursprüngliche Simulationsprozess ohne Veränderungen fortgesetzt.

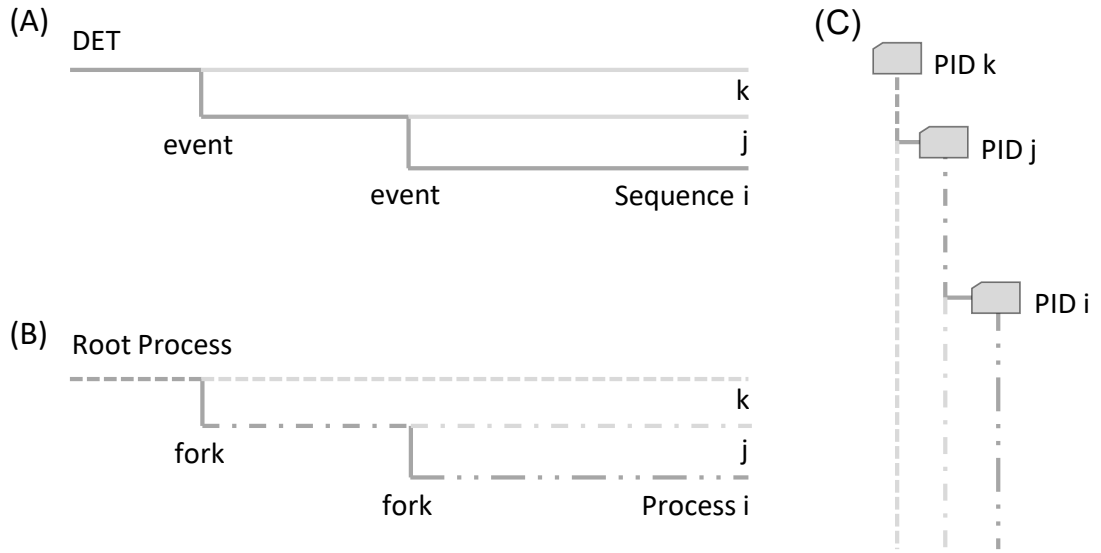


Abb. 2.2 Die Hierarchie eines berechneten DETs (A) spiegelt sich in der Struktur der Simulationsprozesse (B) und der erzeugten Daten wider

Für die Implementierung des Schedulers, welcher diesen automatisierten Ablauf steuert (siehe Abschnitt 2.1.4), mussten Lösungen gefunden werden, die eine effiziente Abarbeitung aller Simulationspfade erlauben und Mehrfachberechnungen möglichst vermeiden. Hierzu ist es entscheidend die Simulationsprozesse flexibel zu verwalten und die verfügbaren Systemressourcen kontrolliert nutzen zu können. Da auf modernen Rechnern normalerweise mehrere CPUs zur Verfügung stehen, sollten diese auch zur parallelen Abarbeitung von Simulationspfaden genutzt werden. Hier ist es wichtig, die gegenseitige Beeinflussung gleichzeitig laufender Simulationsprozesse auszuschließen und auch sicherzustellen, dass die durch deren Überwachung erzeugten Daten wohlorganisiert abgelegt werden.

Wie in Abb. 2.2 dargestellt, ergibt sich aus dem beschriebenen Ablauf eine hierarchische Struktur, welche dazu verwendet werden kann, um diese Anforderungen zu erfüllen. Die Teilabbildungen zeigen dabei die Struktur der als eigenständig ablaufenden Simulationsprozesse (B), welche jeweils in einem eigens für sie erstellten Arbeitsverzeichnis gestartet werden (C). Dieses Vorgehen bietet mehrere Vorteile. Zum einen erlaubt es eine gute Ausnutzung der zur Verfügung stehenden Rechenleistung, da die separaten Simulationsprozesse vom Betriebssystem automatisch auf die verfügbaren CPUs verteilt werden. Durch die einzelnen Prozesse und deren Arbeitsverzeichnisse werden die einzelnen Simulationen auch voneinander abgeschirmt, was die gegenseitige Beeinflussung verhindert und so die Verwendung von klassischen Rechencodes erlaubt, welche für eine multi-thread-Ausführung ungeeignet sind. Zum anderen kann anhand des entstehenden Verzeichnisbaums die Abarbeitung des DETs verfolgt und die abgelegten Daten direkt den entsprechenden Simulationsprozessen sowie den Ereignispfaden im DET zugeordnet werden.

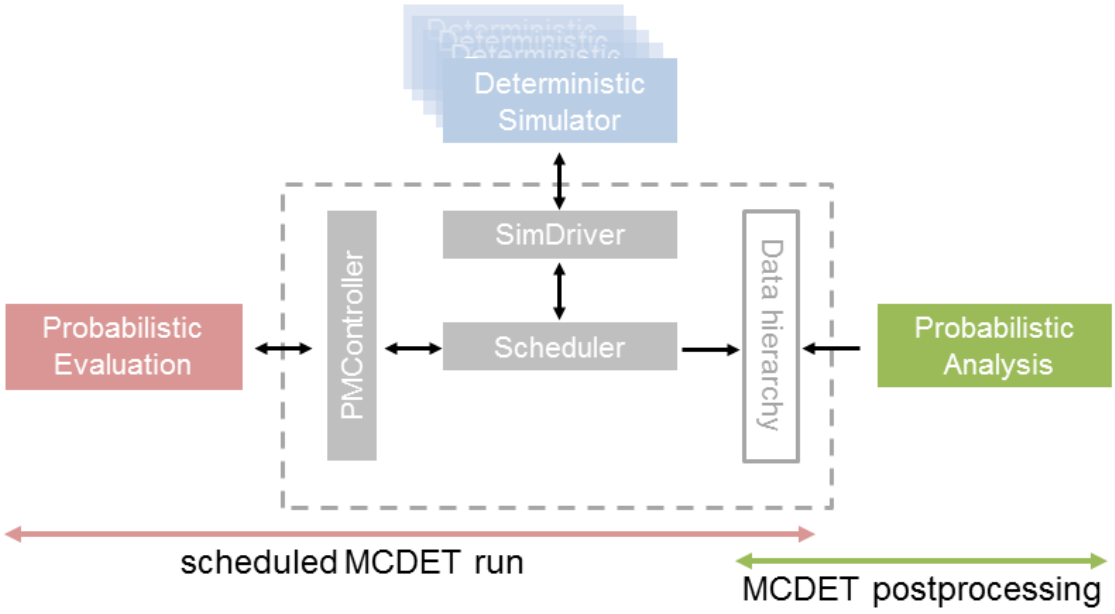


Abb. 2.3 Schematische Darstellung einer MCDET-Analyse

Durch die dynamische Abarbeitung der vom Probabilistikmodul evaluierten Systemzustände der Simulationsläufe spiegeln die Simulationsprozesse die Hierarchie der einzelnen DETs wider. In Folge dessen können auch die generierten Daten in einer intuitiven Datenhierarchie abgelegt werden. Insbesondere für komplexe MCDET-Analysen erlaubt diese Kongruenz zwischen den DETs, den Simulationsprozessen und den Ergebnisdaten eine Verfolgung des MCDET-Laufs schon zur Rechenzeit und begünstigt die Entdeckung möglicher Fehler im prozeduralen Ablauf oder im Spezifikationsschema der

Unsicherheiten. Abb. 2.3 stellt die Schritte einer MCDET-Analyse schematisch dar. Dabei ermöglicht der generische Scheduler mit Hilfe von spezifizierten Zwischenschichten für die jeweiligen Komponenten (grau umrandet) eine automatisierte, parallele Ausführung eines MCDET-Rechenlaufs (scheduled MCDET run). Durch Organisation der überwachten Simulations- und Probabilistikdaten in einem geeigneten hierarchischen Datenformat (HDF5) wird die Grundlage für eine flexible visuelle und statistische Auswertung (MCDET postprocessing) der Ergebnisse geschaffen (siehe Abschnitt 2.3).

2.1.4 Scheduling-Strategie

Der Begriff Scheduling bezeichnet das Vorgehen bei der zeitlichen Einteilung von Simulations-Rechenschritten. Hierbei muss sowohl die Reihenfolge als auch die optionale Verteilung auf mehrere Recheneinheiten festgelegt werden um eine reibungslose Berechnung zu ermöglichen. Besonders das Ziel einer performanten Parallelisierung von Simulationspfaden stellt einige Anforderungen an den Scheduling-Algorithmus:

- **Kein "Verhungern" von Simulationsprozessen:**
  Alle Simulationspfade müssen verfolgt werden, bis ein vom Probabilistikmodul vorgegebenes Abbruchkriterium erfüllt ist. Für alle Simulationsprozesse muss gewährleistet werden, dass kein Prozess unendlich lange auf den Takt (tick-Befehl) warten muss, weil dieser vom Scheduler „vergessen“ wurde.

- **Bestmögliche Nutzung verfügbarer Recheneinheiten:**
  Simulationsprozesse, die bereit sind den jeweilig nächsten Zeitschritt zu rechnen, sollten bei verfügbaren Recheneinheiten nicht unnötig auf den Takt (tick-Befehl) warten müssen.

- **Konfigurierbarer Parallelisierungsgrad:**
  Je nach Nutzung des Rechnersystems ist eine Auslastung aller verfügbaren Recheneinheiten nicht unbedingt gewünscht. Um z. B. auf Desktopsystemen eine grundlegende Reaktionszeit zu gewährleisten, ist es sinnvoll, das System nicht voll auszulasten, indem die Anzahl der gleichzeitig rechnenden Simulationen begrenzt wird.

- **Minimierung der Anzahl inaktiver Prozesse:**
  Auch der Verbrauch des Arbeitsspeichers ist eine wichtige Größe die im Auge behalten werden muss, um die Systemlast zu begrenzen und die Zuverlässigkeit bei der Berechnung von Ereignisbäumen zu erhöhen. Besonders auf Mehrbenutzersystemen ist dies relevant, da Prozesse, für die nicht mehr ausreichend Speicher zur

Verfügung steht, vom Betriebssystem automatisch beendet werden. Deshalb ist es für den Scheduling-Algorithmus sehr wichtig die Anzahl an inaktiven Simulationen durch ein kontrolliertes Erstellen von Rechenprozessen zu minimieren.

- **Priorisierung der Berechnung lokaler Teilbäume:**
  Gerade im Hinblick auf den Speicherverbrauch durch inaktive Prozesse ist es nicht unerheblich welche Simulationsprozesse parallel rechnen dürfen. Besonders Prozesse, die an Verzweigungspunkten auf die Erstellung ihrer Kindsprozesse warten müssen, können die Anzahl an inaktiven Simulationsprozessen im Speicher anwachsen lassen. Für die Zuteilung von Rechentakten erweisen sich dabei bekannte Schedulingstrategien, wie *„First Come – First Served“* oder *„Round Robin“* als wenig geeignet. Vielmehr ist eine dynamische Priorisierung sinnvoll, welche Prozesse lokaler Teilbäume bevorzugt behandelt.

Der unten dargestellte Pseudocode (Abb. 2.4) verdeutlicht die implementierte Scheduling-Strategie. Wie man erkennen kann, wird die Abarbeitung von Unterprozessen deutlich priorisiert. Zum einen werden neu erstellte immer vorne in die Liste wartender Tasks (taskList) eingefügt, wodurch diese priorisiert (*1) bearbeitet werden (evaluate_and_tick) und freie CPUs belegen dürfen. Zum anderen versucht die Abspaltung (*2) alle Kindsprozesse einer wartenden Task möglichst auf einmal zu erstellen. Durch diese Priorisierung wird sichergestellt, dass Teilbäume nach Möglichkeit erst zu Ende gerechnet werden, bevor neue beginnen. Dadurch kann vor allem die Speicherauslastung deutlich begrenzt werden, weil selbst bei einem hohen Grad an parallel abgearbeiteten Simulationen die Anzahl der im Speicher gehaltenen Simulationsprozesse minimiert wird.

```
while taskList not empty:
   idle  = get_idle_tasks( taskList )
   N_cpu = num_free_CPUs()

   # evaluate & tick only the first N idle tasks...
   foreach task in idle[:N_cpu]: #<< (*1)
      evaluate_and_tick( task )

   remove_ended_tasks( taskList )

   forkable = get_forkable_tasks( taskList )
   N_ready  = length( taskList ) - length( forkable )
   N_forks  = MAX_PROC - N_ready #<< number of allowed forks
   # spawn off child tasks (*2) ...
   foreach task in forkable:
      # try to fork as many children as possible
      foreach i in (1, ..., N_forks):
         newTask = fork( task )
         if is_OK( newTask ):
            taskList = newTask + taskList #<< insert new task at front
            N_forks  = N_forks - 1
```

Abb. 2.4 Der Scheduling-Algorithmus zur Priorisierung lokaler Teilbäume

2.1.5 Architektur des Scheduling-Systems

Aus den in Abschnitt 2.1.1 erläuterten Gründen wurde für die Implementierung des MCDET-Scheduling-Systems versucht, einen möglichst modularen Aufbau zu erzielen und die generischen Programmteile von den spezialisierten durch klare Schnittstellen zu trennen. Abb. 2.5 zeigt die Architektur und das Zusammenspiel aller wichtigen Komponenten in vereinfachter Form:

- **Scheduler:** Der Scheduler stellt den vom Benutzer gestarteten Programmteil dar. Dieser erstellt die in der Eingabe spezifizierte Root-Simulation und verwaltet alle anschließend ausgeführten Simulationsprozesse in Form von Tasks. Die dabei realisierte Ablaufsteuerung wird gemäß dem im Abschnitt 2.1.4 beschriebenen Verfahren durchgeführt.

- **PM:** Das zentrale Probabilistikmodul bildet die Schnittstelle zur als shared library (DLL) vorliegenden Bibliothek des MCDET-Kerns. Es bewertet die den einzelnen

Tasks zugeordneten Systemzustände und bestimmt die Zustandsänderungen für neu zu erstellenden Simulationsprozesse.

- **PMController:** Der PMController übernimmt die Kommunikation mit dem Probabilistikmodul (PM) und verwaltet die für die Bewertung herangezogenen Daten in Form einer geeigneten Datenstruktur (data map). Diese enthält die für die Probabilistik wichtigen Daten des Simulationspfades als auch den für die Bewertung relevanten Teil des Simulationszustands.

- **PM data link:** Dieser dynamische Link gibt dem Probabilistikmodul Zugriff auf die im PMController abgelegten Systemzustand. Dieser Link wird vor jeder durchgeführten Bewertung aktualisiert und verweist somit immer auf die Daten der aktuell zu bewertenden Task.

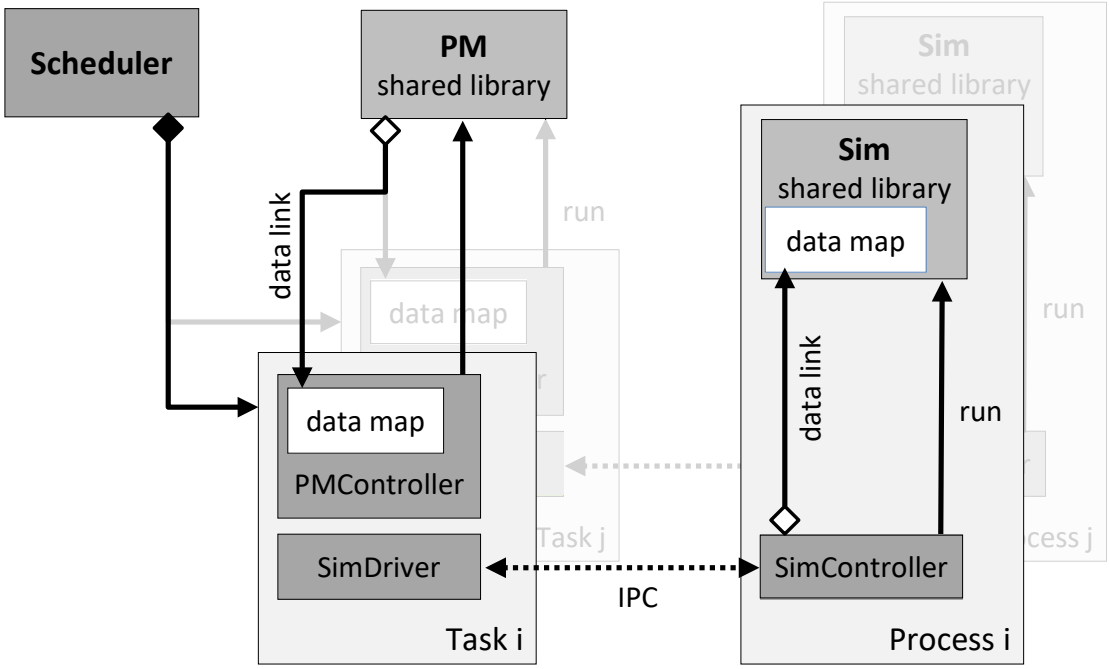


Abb. 2.5 Architektur und Zusammenspiel von Komponenten

- **Sim:** Diese Komponente repräsentiert den deterministischen Rechencode des Simulators (z. B. ATHLET/ATHLET-CD), welcher hier in Form einer shared library (DLL) eingebunden wurde (siehe Abschnitt 2.1.6).

- **SimController:** Der SimController stellt die Befehlsschnittstelle zu als shared library (DLL) vorliegende Rechencodes zur Verfügung, kontrolliert den Ablauf einer Simulation entsprechend der empfangenen Befehle und erlaubt den aktuellen Systemzustand der Simulation von außen abzufragen.

- **SimDriver:** Der Simulations-Treiber organisiert den bidirektionalen Datentransfer zwischen PMController und SimController. Die Daten und Steuerbefehle werden über einen geeigneten Kommunikationskanal (IPC) ausgetauscht.
- **Task:** Eine Task dient der Verwaltung eines Simulationspfades und setzt sich, wie Abb. 2.6 zeigt, aus einem SimDriver zur Kommunikation mit dem Simulationsprozess und einem PMController zusammen. Während des Simulationslaufs überwacht jede Task den Zustand ihrer Simulation, leitet Befehle des Schedulers über den SimDriver an die Simulation weiter und aktualisiert die vom PMController angeforderten Simulationsdaten. Darüber hinaus werden die so überwachten Daten zusammen mit den Ereignisdaten des PMControllers in einem geeigneten Datenformat für das Postprocessing abgelegt.

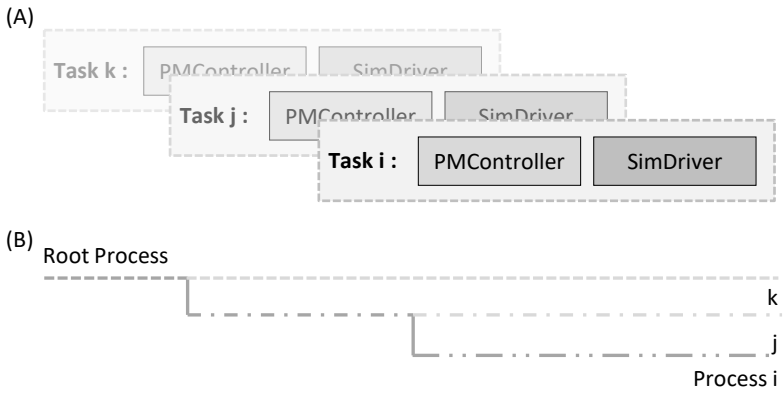


Abb. 2.6 Jeder Task (A) entspricht einem Simulationspfad (B)

2.1.6 Der Simulator-Treiber für ATHLET / ATHLET-CD

Um die im Projekt geplante MCDET-Analyse durchzuführen war es notwendig ATHLET-CD als deterministischen Rechencode nutzen zu können. Für die Kopplung mit dem Scheduling-System musste ATHLET-CD die im Abschnitt 2.1.2 beschriebenen Anforderungen erfüllen. Wie auch ATHLET ist ATHLET-CD zwar für Datenzugriffe und Eingriffe in den Simulationsablauf von außen vorbereitet, allerdings gibt es weder eine eingebaute Taktsteuerung noch können die notwendigen Steuerbefehle interpretiert werden.

Die in ATHLET-CD fehlende Funktionalität musste anhand der im Scheduling-System festgelegten Schnittstelle als eigener Simulator-Treiber implementiert werden. Dieser konnte durch die modulare Aufteilung zu ATHLET kompatibel gehalten werden und kann somit für beide Varianten des Rechencodes genutzt werden. Der Treiber stellt die

Verbindung zwischen Scheduler und Simulator her und versucht die notwendigen Befehle mit den Möglichkeiten des Simulators bestmöglich zu realisieren. Diese Erweiterungen wurden in der Komponente SimController wie folgt implementiert:

- **Taktsteuerung:** ATHLET-CD verfügte bislang über keine Taktsteuerung, d.h. er lässt die Simulation mit der größtmöglichen Geschwindigkeit ablaufen. Da MCDET nach jedem Zeitschritt eine Bewertung des Simulationszustands vornehmen muss, musste in die Hauptschleife eingegriffen und am Beginn eines Zeitschritts ein Ausprungpunkt (hook) eingefügt werden. Vor dem Start der Simulation wird vom SimController an diesem Punkt (NewTimeStep) eine Funktion registriert, welche von ATHLET-CD immer vor einem neuen Zeitschritt aufgerufen wird. Da diese Funktion die Befehlsschleife des Treibers implementiert und ihren Rücksprung bis zum Empfang eines tick-Befehls verzögert, wartet ATHLET-CD mit der weiteren Berechnung und kann so im vorgegebenen Takt betrieben werden. Abb. 2.7 stellt diese Art der Taktsteuerung schematisch dar.

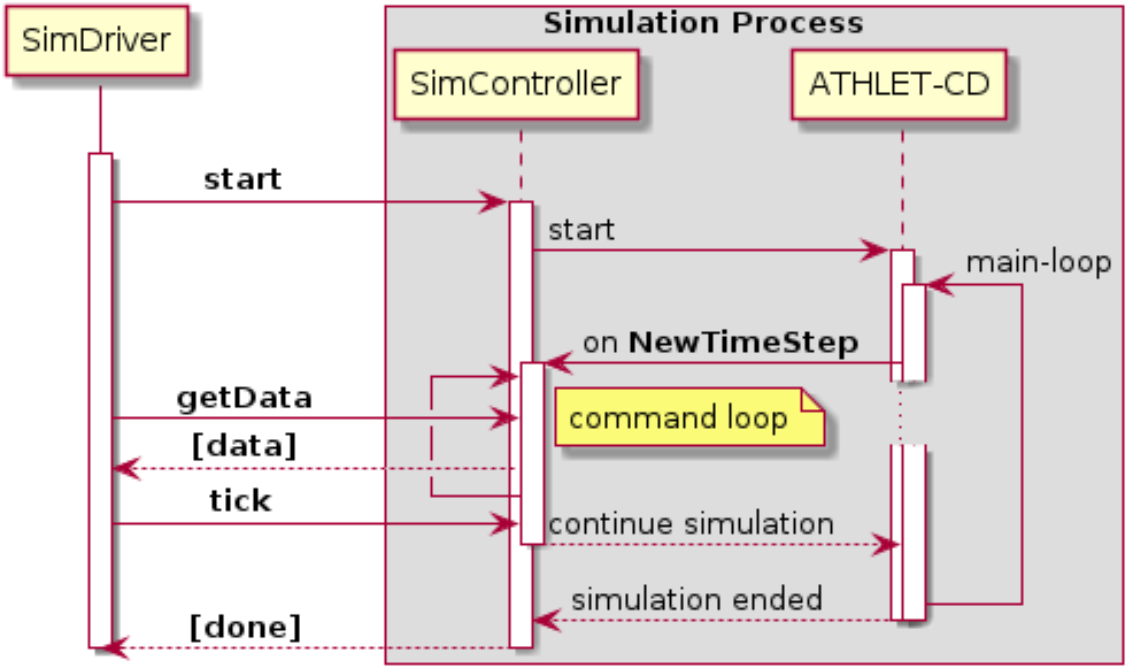


Abb. 2.7 Taktsteuerung von ATHLET-CD durch den Treiber

- **Statusangabe:** Der Status der Simulation konnte bislang in ATHLET-CD nicht abgefragt werden. Diese Funktion wurde im Treiber durch eine Statusabfrage auf den Simulationsprozess und die Synchronisation des IPC-Kanals realisiert.

- **Datenzugriff:** Als shared library (DLL) verwendet, erlaubt ATHLET-CD einen sehr detaillierten Zugriff auf den aktuellen Zustand der Simulation. Im Treiber musste

hierfür ein geeignetes Protokoll für die gezielte und effiziente Abfrage von Daten implementiert werden. Dieses Protokoll erlaubt das Auslesen und Verändern von Datenelementen. Um die Datenkonsistenz sicherzustellen, ist ein Zugriff nicht während der Berechnung eines Zeitschritts möglich.

- **Klonfähigkeit:** Da das Klonen von Prozessen unter Windows nicht unterstützt wird, nutzt der Treiber die in ATHLET-CD vorhandene Restart-Funktion, um den aktuellen Zustand zu sichern und diesen in einen neu gestarteten Simulationsprozess einzuladen. Für den so abgespaltenen Prozess wird eine neue Treiberinstanz mit eigenem Kommunikationskanal erstellt, um diesen unabhängig von der Elternsimulation kontrollieren zu können.

- **Terminierung:** ATHLET-CD bietet standardmäßig keine Möglichkeit, um eine Simulation vorzeitig zu beenden. Durch den detaillierten Zugriff auf den Zustand der Simulation kann der Treiber den Simulationsabbruch auf mehrere Arten erreichen. Allerdings ist hier zu beachten, dass im Falle eines zu unwahrscheinlich gewordenen Simulationspfades oder dem Erreichen eines Save-States kein Fehlerfall vorliegt und somit auch im Simulator ein ganz regulärer Abschluss ausgelöst werden soll. Die wirkungsvollste Methode in ATHLET-CD war hier das Setzen der Simulationsendzeit auf null.

2.2 Crew Modul – Werkzeug zur dynamischen Analyse menschlicher Handlungsabläufe

Im Vorhaben RS1148 /PES 06/ wurden erste Entwicklungsarbeiten zum sogenannten Crew-Modul begonnen. Die Grundidee für das ‚Crew-Modul' bestand darin, dass die Handlungen des Personals als eigener dynamischer Prozess simuliert werden können, der sich im zeitlichen Ablauf parallel und in Wechselwirkung zur System- und Prozessdynamik entwickelt. Durch die Verbindung des Crew-Moduls mit MCDET können die Wechselwirkungen zwischen menschlichen Handlungen, System- und Prozesszuständen sowie stochastischen Einflussgrößen im zeitlichen Ablauf berücksichtigt werden. Außerdem können Handlungen des Personals sowohl in der Warte als auch außerhalb der Warte modelliert werden.

Das Crew-Moduls kann nicht nur eigesetzt werden, um eine genauere Beurteilung und Abschätzung bzgl. der menschlichen Zuverlässigkeit zu erreichen, sondern es kann auch als Werkzeug zur Lösung bestimmter Problemstellungen dienen, z. B:

- Entwicklung von Handlungsstrategien, die zu einer Verbesserung der menschlichen Zuverlässigkeit führen.
- Identifikation von Fehlhandlungen, die die größten negativen Effekte aufweisen und Analyse von Optionen, die zur Verminderung der negativen Konsequenzen beitragen können.

Zum besseren Verständnis des Crew-Moduls und der durchgeführten Weiterentwicklungsarbeiten wird in Abschnitt 2.2.1 kurz auf die Motivation und in Abschnitt 2.2.2 auf das Konzept des Crew-Moduls eingegangen. Abschnitt 2.2.3 beschreibt die durchgeführten Weiterentwicklungen, die die Anwendungen des Crew-Moduls erheblich erleichtern.

2.2.1 Motivation zur Berücksichtigung des zeitlichen Einflusses bei der Modellierung menschlichen Handlungen

Das Ziel des Crew-Moduls ist es, Handlungsabläufe des Personals, die synchron und in Wechselwirkung sowohl mit der System- und Prozessdynamik erfolgen als auch von Zufallsereignissen beeinflusst werden können, als dynamischen Prozess modellieren und analysieren zu können. Die Entwicklung wurde insbesondere dadurch motiviert, um in der Realität auftretende Zusammenhänge und Abhängigkeiten, die Einfluss auf die Zuverlässigkeitsbewertung menschlicher Handlungen haben können, in die Analyse menschlichen Handelns einbeziehen zu können. Dazu ist es insbesondere wichtig, den Faktor Zeit und Wechselwirkungsprozesse in menschlichen Handlungsabläufen (z. B. Kommunikation zwischen beteiligten Personen) zu berücksichtigen.

Eine maßgebliche Größe, die Einfluss auf die Zuverlässigkeit für den Erfolg einer menschlichen Handlungsmaßnahme hat, sind menschliche Fehler, die bzgl. einiger Aktionen mit mehr oder weniger großen Wahrscheinlichkeiten auftreten können. Wenn ausschließlich menschliche Fehler in der Analyse betrachtet werden, ergibt sich die in Abb. 2.8 dargestellte Ablaufstruktur zur Bestimmung der Zuverlässigkeit einer Handlungsmaßnahme:

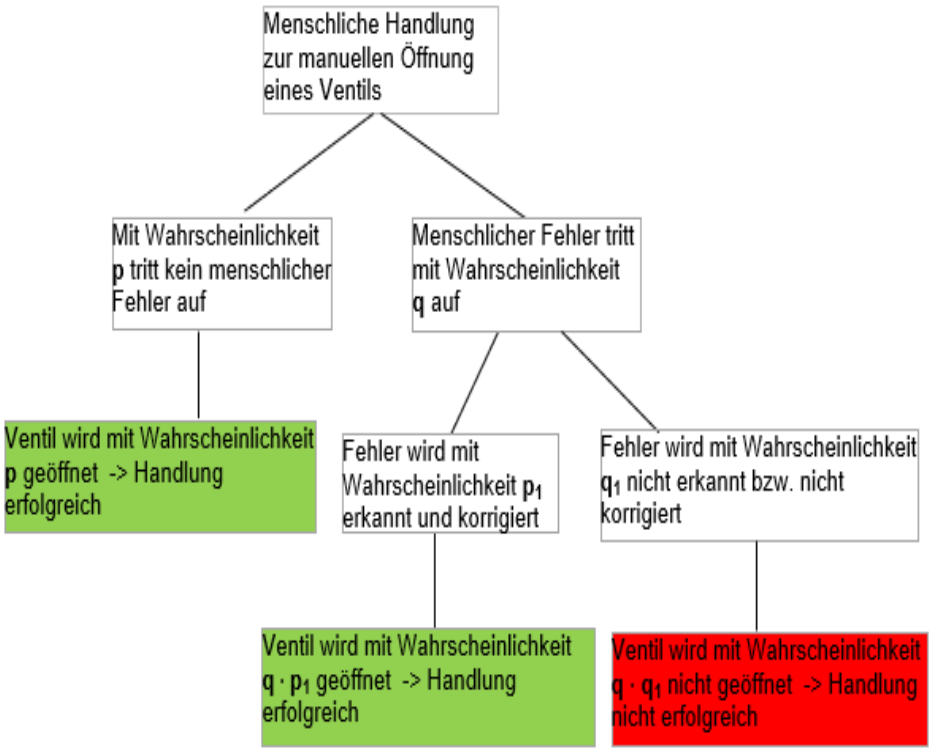


Abb. 2.8 Ablaufstruktur der Zuverlässigkeitsbestimmung einer Maßnahme bei ausschließlicher Berücksichtigung menschlicher Fehler

Abb. 2.8 skizziert, welche Ablaufmöglichkeiten sich für die Zuverlässigkeitsbestimmung einer Maßnahme ergeben können, wenn nur menschliche Fehler in der Zuverlässigkeitsanalyse berücksichtigt werden. Für den Fall, dass bzgl. der durchzuführenden Handlung (manuelle Öffnung eines Ventils) kein menschlicher Fehler erfolgt, wird das Ventil, wie beabsichtigt, manuell geöffnet und die Maßnahme gilt als erfolgreich durchgeführt. Wenn ein menschlicher Fehler auftritt, kann er behoben werden, wenn der Fehler erkannt wird. Wenn der Fehler erkannt und behoben wird, kann es – wenn auch verspätet – zur erfolgreichen Durchführung der Maßnahme kommen. Wenn der Fehler nicht erkannt wird oder nicht korrigiert werden kann, ist die Durchführung der Maßnahme nicht erfolgreich.

In dem in Abb. 2.8 dargestellten Beispiel ergibt sich die Wahrscheinlichkeit einer erfolgreichen Durchführung der Maßnahme aus der Summe der Wahrscheinlichkeiten, dass die Maßnahme ohne Fehler durchgeführt wird oder, dass ein menschlicher Fehler auftritt, dieser aber im nachfolgenden Ablauf erkannt und korrigiert wird. D. h.,

$$P(\text{Maßnahme erfolgreich}) = P(\text{kein menschlicher Fehler}) + P(\text{menschlicher Fehler}) \cdot P(\text{Fehler wird erkannt und korrigiert}) = p + q \cdot p_1 \quad (2.1)$$

Die Wahrscheinlichkeit, dass die Maßnahme nicht erfolgreich ist, ergibt sich aus dem Produkt der Wahrscheinlichkeit, dass ein menschlicher Fehler auftritt und dieser im nachfolgenden Ablauf nicht erkannt wird, d. h.,

$$\begin{aligned} &P(\text{Maßnahme nicht erfolgreich}) = \\ &P(\text{menschlicher Fehler}) \cdot P(\text{Fehler wird nichterkannt}) = q \cdot q_1 \end{aligned} \tag{2.2}$$

Die Ablaufstruktur, die sich bzgl. der Zuverlässigkeitsbestimmung ergibt, wenn neben dem menschlichen Fehler auch der Zeitfaktor berücksichtigt wird, ist in Abb. 2.9 skizziert. Dabei beschreibt t den Zeitpunkt, wann die Handlung ausgeführt wurde und t_{crit} einen kritischen Zeitpunkt, bei dessen Überschreiten die Maßnahme als nicht erfolgreich betrachtet wird. Erfolgt die Durchführung der Maßnahme vor dem Zeitpunkt t_{crit}, entwickelt sich der Prozess im weiteren Verlauf in einen unkritischen Zustand, so dass die Maßnahme als erfolgreich betrachtet werden kann.

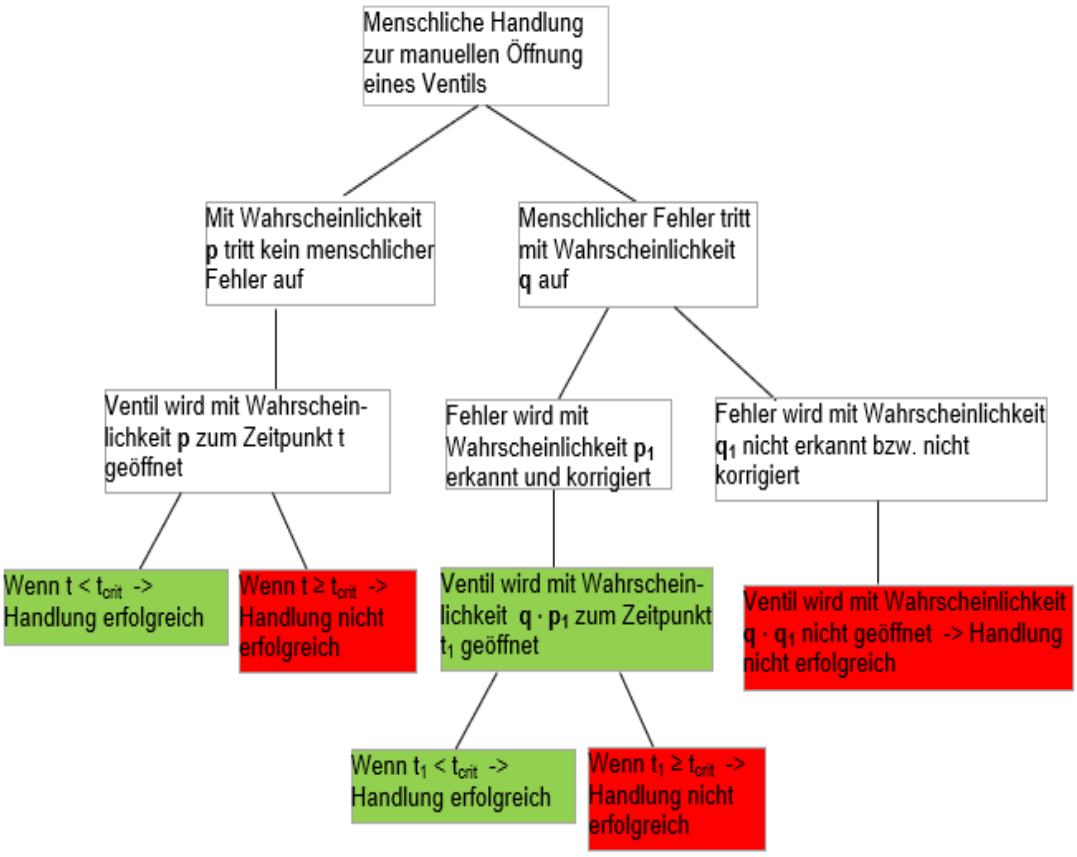


Abb. 2.9 Ablaufstruktur der Zuverlässigkeitsbestimmung einer Maßnahme unter Berücksichtigung menschlicher Fehler und des zeitlichen Einflusses

Abb. 2.9 zeigt, dass der Erfolg einer Maßnahme nicht nur davon abhängt, ob bzgl. der Maßnahme ein Fehler gemacht und nicht behoben wird, sondern auch abhängig vom Zeitpunkt ist, wann die Maßnahme durchgeführt wird. So können Situationen eintreten, bei denen die Maßnahme nicht erfolgreich ist, obwohl die Handlungen ohne Fehler durchgeführt werden. Das sind die Situationen, in denen die Öffnung des Ventils zu spät erfolgt.

Der kritische Zeitpunkt t_{crit} wird in der Regel durch den zugrungeliegenden physikalischen Prozess bestimmt. Erfolgt die Durchführung der Maßnahme vor dem Zeitpunkt t_{crit}, entwickelt sich der Prozess im weiteren Verlauf in einen unkritischen Zustand, so dass die Maßnahme als erfolgreich betrachtet werden kann. Benötigt die Ausführung der Maßnahme länger als t_{crit}, wird im weiteren Prozessablauf ein unerwünschter Zustand erreicht, so dass die Maßnahme als nicht erfolgreich bewertet wird.

Wenn in Abb. 2.9 die Zeitpunkte t und t_1 als Zufallsgrößen betrachtet werden, deren Unsicherheiten jeweils durch eine Wahrscheinlichkeitsverteilung beschrieben werden, so können unter der Voraussetzung, dass t_{crit} bekannt ist, die jeweiligen Wahrscheinlichkeiten $P(t < t_{crit})$ und $P(t_1 < t_{crit})$ bzw. $P(t \geq t_{crit})$ und $P(t_1 \geq t_{crit})$ berechnet werden. Unter Verwendung dieser Wahrscheinlichkeiten ergeben sich für eine erfolgreiche bzw. nicht erfolgreiche Durchführung der Maßnahme die aus den Gleichungen (2.3) bzw. (2.4) berechneten Wahrscheinlichkeiten:

$$P(\text{Maßnahme erfolgreich}) = p \cdot P(t < t_{crit}) + q \cdot p_1 \cdot P(t_1 < t_{crit}) \tag{2.3}$$

$$P(\text{Maßnahme nicht erfolgreich}) = q \cdot q_1 + p \cdot P(t \geq t_{crit}) + q \cdot p_1 \cdot P(t_1 \geq t_{crit}) \tag{2.4}$$

Vergleicht man die Zuverlässigkeit mit und ohne Berücksichtigung der Ausführungszeiten der Handlung (s. Gleichungen (2.3) und (2.1)), so gilt:

$$p + q \cdot p_1 \geq p \cdot P(t < t_{crit}) + q \cdot p_1 \cdot P(t_1 < t_{crit}) \tag{2.5}$$

Die Gleichheitsbeziehung in Gleichung (2.5) ist nur dann gegeben, wenn gilt:

$P(t < t_{crit}) = 1$ und $P(t_1 < t_{crit}) = 1$

Ist $P(t < t_{crit}) < 1$ oder $P(t_1 < t_{crit}) < 1$ dann gilt:

$p < p \cdot P(t < t_{crit})$ oder $q \cdot p_1 < q \cdot p_1 \cdot P(t_1 < t_{crit})$,

woraus sich die Ungleichheitsbeziehung in (2.5) ergibt.

Gleichung (2.5) zeigt somit, dass in den Fällen, in denen $P(t < t_{crit}) < 1$ oder $P(t_1 < t_{crit}) < 1$ gilt, die Zuverlässigkeit einer menschlichen Handlung systematisch überschätzt wird, wenn entsprechende Zeitabhängigkeiten in der menschlichen Zuverlässigkeitsanalyse nicht berücksichtigt werden.

Beim Vergleich der Gleichungen (2.2) und (2.4), in denen die Wahrscheinlichkeit ausgedrückt wird, dass die Handlung nicht erfolgreich durchgeführt wird, ergibt sich zwischen den Bewertungen ohne und mit Berücksichtigung der Zeitabhängigkeiten folgende Beziehung:

$$q \cdot q_1 \leq q \cdot q_1 + p \cdot P(t \geq t_{crit}) + q \cdot p_1 \cdot P(t_1 \geq t_{crit}) \qquad (2.6)$$

Die Gleichheit der Wahrscheinlichkeiten in Gleichung (2.6) ist nur dann gegeben, wenn $P(t \geq t_{crit}) = 0$ und $P(t_1 \geq t_{crit}) = 0$ ist.

In den Fällen, in denen $P(t \geq t_{crit}) > 0$ oder $P(t_1 \geq t_{crit}) > 0$ gilt, wird die Wahrscheinlichkeit, dass die Handlung nicht erfolgreich durchgeführt wird, systematisch unterschätzt, wenn entsprechende Zeitabhängigkeiten nicht berücksichtigt werden.

Mit den obigen Ausführungen wurde gezeigt, dass die Zuverlässigkeit einer menschlichen Handlung ohne Berücksichtigung des zeitlichen Einflusses als zu optimistisch bewertet werden kann. Außerdem kann nicht eingeschätzt werden, ob und in welchem Ausmaß die Zuverlässigkeit überschätzt wird. Daraus ergibt sich die Schlussfolgerung, dass sowohl menschliche Fehler als auch die Ausführungszeiten der menschlichen Handlung relevante Faktoren sind, die Einfluss auf die Zuverlässigkeit einer Handlung haben und deshalb gleichermaßen in der Zuverlässigkeitsanalyse menschlicher Handlungen zu berücksichtigen sind.

Um den zeitlichen Einfluss in der menschlichen Zuverlässigkeitsanalyse berücksichtigen zu können, besteht eine wesentliche Aufgabe darin, die Wahrscheinlichkeitsverteilungen der Zeiten zu schätzen, wann relevante Handlungen im Rahmen eines Handlungs-

ablaufs durchgeführt werden, die einen Einfluss auf den Prozessablauf haben können. In der GRS wurde mit dem Crew-Modul /PES 06/ eine Methode entwickelt, mit der zeitliche Einflüsse bei den Handlungsausführungen berücksichtigt und damit Wahrscheinlichkeitsverteilungen von Ausführungszeiten relevanter Handlungen ermittelt werden können.

Ein weiteres wichtiges Argument zur Berücksichtigung des zeitlichen Einflusses in menschlichen Zuverlässigkeitsanalysen ist, dass je nachdem ob eine Handlung schnell oder erst nach einer längeren Verzögerungszeit durchgeführt wird, sich erhebliche Unterschiede im Unfallablauf ergeben können. Um den Einfluss des Zeitpunkts einer Handlungsausführung (z. B. Öffnen eines Ventils) auf den Prozessablauf zu quantifizieren, müssen zunächst die Unsicherheiten bzgl. des Zeitpunkts quantifiziert werden, wann die entsprechende Handlung ausgeführt wird. Wenn diese Unsicherheiten als aleatorische Unsicherheiten in die Berechnung des Prozessablaufs eingehen, können Aussagen abgeleitet werden, mit welcher Wahrscheinlichkeit die Maßnahme rechtzeitig durchgeführt wird, um den beabsichtigten Erfolg zu erzielen bzw. mit welcher Wahrscheinlichkeit die Handlung so spät erfolgt, so dass die Maßnahme den beabsichtigten Zweck nicht oder nur zum Teil erfüllt. Damit lassen sich dann auch die Wahrscheinlichkeiten $P(t < t_{crit})$ bzw. $P(t \geq t_{crit})$ ermitteln, die zur Zuverlässigkeitsschätzung einer menschlichen Handlung benötigt werden.

Aufgrund dieser Überlegungen wurde in der GRS mit dem Crew-Modul eine Methode entwickelt, mit der menschliche Handlungsabläufe als zeitabhängiger (dynamischer) Ablauf modelliert und simuliert werden kann. In Verbindung des Crew-Moduls mit MCDET können Handlungsabläufe auch in Abhängigkeit von zufälligen Ereignissen und Systemzuständen modelliert und analysiert werden. Ein Anwendungsschwerpunkt des Crew-Moduls besteht darin, zum einen die Variation bzgl. des Zeitpunkts zu ermitteln, wann relevante Handlungen ausgeführt werden, die Auswirkungen auf die Prozessentwicklung haben. Zum anderen soll auch die Abhängigkeit eines Handlungsablaufs von zufällig eintretenden Situationen möglichst umfassend berücksichtigt werden können. Dabei wird dem Umstand Rechnung getragen, dass in Abhängigkeit unterschiedlicher Situationen, die durch zufällige Einflüsse eintreten, ganz andere Handlungsabläufe ausgeführt werden müssen.

Das Crew-Modul in Verbindung mit dem Werkzeug MCDET erlaubt es, zeitliche Einflüsse sowie Abhängigkeiten menschlicher Handlungsabläufe von aleatorischen Unsicherheiten umfassender berücksichtigen und analysieren zu können. Im folgenden Abschnitt 2.2.2 wird das Konzept des Crew-Moduls beschrieben.

2.2.2 Konzept des Crew-Moduls

Im Gegensatz zur Modellierung physikalischer Prozesse, die durch Gesetzmäßigkeiten und mathematische Gleichungen definiert werden, können menschliche Handlungsabläufe und Entscheidungsprozesse, die ein bestimmtes Ziel verfolgen, im Allgemeinen nicht über mathematische Gleichungen beschrieben werden. Aus diesem Grund ist man gezwungen, dass mögliche Handlungsabläufe, die sich in Abhängigkeit stochastischer Einflussgrößen oder aus den Informationen verschiedener relevanter System- und Prozesszustände ergeben können, antizipiert und explizit beschrieben werden müssen.

Bei der Konzeptentwicklung für das Crew-Modul wurden folgende Überlegungen in Anlehnung an reale Gegebenheiten zugrunde gelegt:

- Ein Handlungsablauf setzt sich aus einer Vielzahl einfacherer Einzelhandlungen (im Folgenden auch Basishandlung genannt) zusammen. Die Ausführung einer Basishandlung kann in der Regel einer bestimmten Person zugeordnet werden. Zur Ausführung einer Basishandlung wird eine gewisse Zeit benötigt. Die Erfahrung zeigt, dass der Mensch für die Ausführung der gleichen Handlung auch unter konstanten Ausführungsbedingungen normalerweise unterschiedlich viel Zeit benötigt. Ebenso wird auch die Reaktionszeit, mit der eine Person auf den Eintritt eines Ereignisses reagiert nicht konstant sein, sondern mehr oder weniger stark variieren. Diese zeitlichen Schwankungen ergeben sich aus vielfältigen Faktoren, die von der Art und dem Ausmaß der aktuellen Beanspruchung, Stress durch persönliche Probleme, Ablenkung durch andere Personen, bis hin zu individuellen Leistungsunterschieden (Tagesform) reichen.

  Demzufolge wird davon ausgegangen, dass die Ausführungszeit einer Handlung eine Zufallsgröße ist und somit einer aleatorischen Unsicherheit unterliegt, die durch eine bestimmte Wahrscheinlichkeitsverteilung beschrieben wird. Wenn es sich bei den Basishandlungen überwiegend um einfache elementare Tätigkeiten handelt, kann davon ausgegangen werden, dass sich die Verteilungen der Ausführungszeiten in der Regel relativ einfach durch Expertenurteil abschätzen lassen, ohne auf Daten aus der Betriebserfahrung oder experimentelle Daten zurückgreifen zu müssen.

- Bei der Ausführung menschlicher Maßnahmen sind oftmals mehrere Individuen beteiligt, die miteinander kommunizieren und deren Handlungen von den Handlungen der anderen Operateure, von ergonomischen und kognitiven Faktoren und von der Wahrnehmung und Interpretation des Systemzustandes abhängen können.

  Informationen über den Zustand des Handlungsablaufs (und ggf. auch über den System- und Prozesszustand) erhalten die beteiligten Personen neben den Anzeigen in der Warte unter anderem auch über die Kommunikation, die zwischen ihnen stattfindet. Kommunikationen können unterlassen oder auch falsch verstanden werden. Dies kann zu Zeitverzögerungen, Unterlassungsfehlern oder Ausführungsfehlern führen, was wiederum Einfluss auf den Handlungsablauf und schließlich auf den Unfallablauf haben kann. Demzufolge stellt die Kommunikation zwischen den Personen eines Teams und deren Fehlerpotential einen wesentlichen Einflussfaktor dar, der sich auf den Handlungsablauf und letztlich auch auf die Zuverlässigkeit menschlichen Handelns auswirken kann.

  Sind mehrere Personen am Handlungsablauf beteiligt, sollten die Eigenschaften berücksichtigt werden, dass

  - Handlungen verschiedener Personen zeitlich parallel ablaufen können und
  - Abhängigkeiten zwischen den Handlungen verschiedener Personen und vom Prozesszustand bestehen können. D. h., es gibt Handlungen, die erst dann beginnen, wenn bestimmte Bedingungen erfüllt sind. Die Bedingungen können System- oder Prozessbedingungen sein oder auch durch bestimmte Informationen von anderen Personen definiert werden. Die Abhängigkeit bestimmter Handlungen von Systembedingungen oder Informationen hat einen Einfluss auf die Zeit, wann relevante Maßnahmen durchgeführt werden, was wiederum Einfluss auf den weiteren Prozessablauf haben kann.

- Zufällige Ereignisse können unterschiedliche Handlungsabläufe zur Folge haben. Außerdem können sie den Stress des Personals beeinflussen, wobei sich der Stresszustand wiederum auf den weiteren Handlungsablauf auswirken kann. Ein typisches Zufallsereignis besteht z. B. darin, ob ein Operateur bzgl. einer durchzuführenden Handlung einen Fehler begeht oder nicht. Dies können Fehler sein, die zu einer Auslassung einer relevanten Handlung (failure of omission) führen oder fehlerhafte Ausführungen einer Handlung (failure of commission) zur Folge haben können.

- Der Zustand des physikalischen Prozesses kann einen wesentlichen Einfluss auf den Handlungsablauf und die Zuverlässigkeit der durchzuführenden Handlungen haben. So werden z. B. Notfallmaßnahmen eingeleitet, wenn bestimmte Prozesskriterien erfüllt sind. Es kann vorkommen, dass bei Erreichen bestimmter Prozesszustände Handlungen abgebrochen und andere Handlungen durchgeführt werden müssen.

Aufgrund dieser Gegebenheiten sieht das grundlegende Konzept des Crew-Moduls vor, einen komplexen Handlungsablauf, bei dem eine oder mehrere Personen beteiligt sind und interagieren können, durch eine Vielzahl von einfachen Einzelhandlungen zu beschreiben. D. h., das Konzept des Crew-Moduls zur Simulation von Handlungsabläufen als dynamischer Prozess besteht im Wesentlichen darin, eine durch menschliche Handlungen durchzuführende Maßnahme in mehr oder weniger kleine Einzelhandlungen (Basishandlungen) zu zerlegen.

2.2.2.1 Basishandlungen

Für das Crew-Modul wird eine Basishandlung als eine abgeschlossene einfache Einzelhandlung verstanden, die von einem bestimmten Operateur durchgeführt wird. Die Basishandlungen können dabei einfache Tätigkeiten sein (z. B. Bedienung eines Schaltknopfes) oder auch eine Kommunikation zwischen Personen beschreiben (z. B. Schichtleiter weist Reaktorfahrer an, Hauptkühlmittelpumpen abzustellen). Je feiner die Zerlegung eines komplexen Handlungsablaufs in Basishandlungen erfolgt, desto detaillierter kann der Handlungsablauf der zu bewertenden Maßnahme und die darin stattfindenden Wechselwirkungen modelliert und analysiert werden. Der Grad, wie fein die Maßnahme in Basishandlungen zerlegt wird, steht im Ermessen des Benutzers.

Jeder Basishandlung sind Attribute zugeordnet, die eine nähere Beschreibung der Basishandlung erlauben. Die Definition der Basishandlungen ist bisher auf folgende Attribute beschränkt:

- Identifikationsnummer der Basishandlung. Die Identifikationsnummern werden verwendet, um Handlungslisten zu erstellen die den Ablauf einer bestimmten Teilhandlung beschreiben.
- Angabe der Person, die die Basishandlung durchführt. Die Person kann durch eine vom Benutzer gewählte Kurzbezeichnung (z. B. SL für Schichtleiter, RF für Reaktorfahrer, EL1 für 1. Elektriker) angegeben werden.

- Angabe der Person oder der technischen Komponente, die durch die Basishandlung beeinflusst wird. Diese Information, welche Person von der Handlung beeinflusst wird, ist wichtig, um den Zeitpunkt zuordnen zu können, wann diese Person durch die Handlung aktiviert wird oder eine bestimmte Information erhält. Entsprechend ist es für eine technische Komponente wichtig, in welcher Form die Beeinflussung der Komponente durch die Handlung erfolgt und zu welchem Zeitpunkt dies geschieht.

- Angabe der Zeit, die die Person für die Ausführung der Basishandlung benötigt. Die Ausführungszeit einer Basishandlung wird grundsätzlich als eine zufällige Größe betrachtet. Ausführungszeiten, die nur sehr kleinen zufälligen Variationen unterworfen sind, können jedoch auch als konstante Größen spezifiziert werden. Wenn die Ausführungszeit als Zufallsgröße spezifiziert wird, werden Minimalwert t_{min} und Maximalwert t_{max} des möglichen Zeitbereichs angegeben. Soll die Ausführungszeit als konstante Größe spezifiziert werden, wird der entsprechende konstante Wert zweimal eingegeben. Dadurch erkennt das Programm, welche der Ausführungszeiten als Zufallsvariable und welche Zeiten als konstante Werte in die Analyse eingehen. Da die Anzahl der Basishandlungen für einen Handlungsablauf sehr hoch sein kann, wird aus Effizienzgründen die Spezifikation der Unsicherheiten für die Ausführungszeiten der Basishandlungen sowie deren zufällige Auswahl über das Programmsystem SUSA /KLO 18/ vorgenommen. Die über SUSA ausgespielten Zufallswerte werden im Rahmen der Simulation des Handlungsablaufs mit dem Crew-Modul den Ausführungszeiten der entsprechenden Basishandlungen automatisch zugeordnet.

- Kurzbeschreibung der Basishandlung. Dieses Attribut einer Basishandlung ist optional, da es für die eigentliche Simulation des Handlungsablaufs nicht benötigt wird. Es wird jedoch empfohlen, eine sinnvolle Kurzbeschreibung des Inhalts der jeweiligen Basishandlung zu geben. Damit wird die Beschreibung der simulierten Sequenzen des Handlungsablaufs und damit die Nachvollziehbarkeit des Handlungsmodells erheblich vereinfacht.

Die Komplexität einer Basishandlung kann unterschiedlich hoch sein. Beispielsweise ist die Basishandlung „Elektriker führt Arbeiten am Reaktorschutz aus“ komplexer zusammengesetzt als die Basishandlung „Schichtleiter liest Anzeige zum DE-Füllstand ab“. Je elementarer (weniger komplex) eine Basishandlung definiert ist, desto leichter kann auch ein Zeitrahmen für die Ausführung der Handlung abgeschätzt werden. Bei der Spezifikation von Basishandlungen sollte darauf geachtet werden, dass die Basishandlung nicht zu komplex ist und keine wichtigen Interaktionen beinhaltet, die dann in der Analyse

nicht explizit berücksichtigt werden können. Es sollte versucht werden Basishandlungen, die zu komplex erscheinen, weiter zu zerlegen.

Neben den Basishandlungen, die Aktionen von Personen beschreiben, werden im Crew-Modul zusätzlich Verzweigungselemente verwendet, mit denen z. B. angegeben wird, an welcher Stelle des Handlungsablaufs es zu Verzweigungen kommt. Über die Verzweigungselemente können Abhängigkeiten des Handlungsablaufs von aleatorischen Unsicherheiten (stochastischen Ereignissen) sowie Abhängigkeiten von Prozesszuständen modelliert werden. Die Abhängigkeit des Handlungsablaufs vom Prozesszustand tritt z. B. in der Situation auf, wenn im Rahmen einer Brandbekämpfung der Brandraum aufgrund der Verrauchung betreten werden kann oder nicht.

Verzweigungselemente können durch zwei oder auch mehrere Alternativen definiert werden, die dann jeweils unterschiedliche Handlungsabläufe zu Folge haben. Die Definition der Alternativen eines Verzweigungselements und die jeweiligen Wahrscheinlichkeiten, mit denen die entsprechenden Alternativen auftreten, werden im Probabilistik-Modul von MCDET spezifiziert.

Alle Basishandlungen, in die ein komplexer Handlungsablauf zerlegt worden ist, werden in einer separaten Datei *(‚cBasAct'*) aufgelistet, wobei für jede einzelne Basishandlung die Informationen der oben beschriebenen Attribute aufgeführt werden. Ein Ausschnitt für eine Datei der Basishandlungen ist in Tab. 2.1 dargestellt.

Tab. 2.1 Basishandlungen eines Handlungsablaufs

4001	4	4	# 1	1	20	// Verzögerungszeit mit der LF die Anzeigen der DE-FH beachtet.
4002	4	4	# 2	16	32	// Ablesen der 8 FH-DE Anzeigen
4003	4	1	# 3	4	8	// LF informiert SL über FH-DE
1001	1	1	# 4	1	5	// SL begibt sich zu den FH-DE Anzeigen
1002	1	1	# 5	16	32	// SL kontrolliert FH-DE Anzeigen
1003	1	1	# 6	30	45	// SL schlägt Prozedur im NHB auf, liest und trifft Entscheidung zu SDE
1004	1	2	# 7	4	8	// SL weist SLVE an ALW zurückzurufen
2001	2	2	# 8	1	5	// SLVE begibt sich auf den Weg zur Lautsprecheranlage
2002	2	2	# 9	20	30	// Rückruf der Anlagenwärter über Lautsprecheranlage
2003	2	5	0	0	0	// Zuordnung der Rückrufzeit zu AWE1
2004	2	6	0	0	0	// Zuordnung der Rückrufzeit zu AWE2
2005	2	7	0	0	0	// Zuordnung der Rückrufzeit zu AWM1
2006	2	8	0	0	0	// Zuordnung der Rückrufzeit zu AWM2
5001	5	5	# 10	240	350	// E1 begibt sich zur Warte
6001	6	6	# 11	120	240	// E2 begibt sich zur Warte
7001	7	7	# 12	240	350	// AWM1 begibt sich zur Warte
8001	8	8	# 13	480	600	// AWM2 begibt sich zur Warte
1005	1	1	5	5	5	// Weg des SL zum Nebenleitstand CWQ, um Stromversorgung abzulesen
1006	1	1	# 14	32	64	// Liest Spannung von Notstrom 1 bzw. 2 . 4x4 Anzeigen
1007	1	3	# 15	10	20	// SL weist SLVM an Führung der Mannschaft zu übernehmen und Prozedur weiter abzuarbeiten
1008	1	1	# 16	240	360	// Krisenorganisation durch SL
3001	3	2	# 17	120	150	// Anweisung Anlagenzustand fortlaufend kontrollieren (BF)
2007	2	2	# 18	5	10	// SLVE beginnt Kontrolle
3002	3	4	# 19	15	25	// Anw.: Anschlussleitungen überprüfen (BE)
4004	4	4	# 20	120	240	// Anschlussleitungen überprüft
3003	3	-113	1	1	1	// SLVM vergisst Anweisung ja / nein
3004	3	6	# 21	90	180	// Anw.: Stromversorgung Bleed - Schiene herstellen (BB2)
6002	6	6	# 22	150	220	// Weg: Schaltanlagengebäude
6003	6	6	# 23	300	420	// Umschaltungen im Schaltanlagengebäude
6004	6	6	# 24	320	480	// Weg: Schaltanlagengebäude - Notspeisegebäude
6005	6	-114	1	1	1	// allU aufgrund techn. Probleme kommt es bei den Umschaltungen zu Verzögerungen.
6006	6	-6	# 25	1200	1680	// Umschaltungen im NotspGeb. (BB2-Ende)
1009	1	3	2	2	2	// SL informiert, dass er zu Rücknahme des Kommandos bereit ist.
3005	3	1	# 26	60	90	// SLVM informiert SL über Stand der Dinge.
1010	1	5	# 27	120	150	// Anw: Simulationen RS
1011	1	7	# 28	120	150	// Anw: mobile Pumpe anschließen
5002	5	5	# 29	240	360	// weg: NotspGeb
5003	5	-3	# 30	1400	1800	// Simulationen im Reaktorschutz
7002	7	7	# 31	240	360	// weg: NotspGeb

Die Datenstruktur in Tab. 2.1 ist gegeben durch:

- **Spalte 1:** Nummer der Basishandlung.
- **Spalte 2:** Indexnummer der Person, die Handlung durchführt.
- **Spalte 3:** Indexnummer der Person, die von der Handlung beeinflusst wird. Negative Indexnummern < 100 geben besondere Ereignisse an, z. B. ob der Zustand einer Komponente geändert wird, wann eine bestimmte Handlung durchgeführt wird, die ggf. Einfluss auf den Prozessablauf hat oder wann eine Verzweigung des Handlungsablaufs stattfindet.

- **Spalte 4:** Durch das Zeichen ‚#' wird angedeutet, dass es sich bei der Ausführungszeit der Basishandlung um eine Zufallsgröße handelt. Die darauffolgende Zahl gibt die Nummer der unsicheren Größe an. Die Nummern werden zur richtigen Zuordnung der in SUSA simulieren Werte der Ausführungszeiten zu den entsprechenden Basishandlungen, die im Crew-Modul verarbeitet werden, benötigt.
- **Spalte 5 – 6:** Minimum und Maximum der Ausführungszeit der jeweiligen Basishandlung.
- Nach dem Zeichen ‚//' kann eine kurze Beschreibung der Basishandlung gegeben werden.

2.2.2.2 Handlungslisten

Die Basishandlungen, in die ein Handlungsablauf zerlegt worden ist, werden sequentiell zusammengefügt, um bestimmte Teilhandlungen zu beschreiben. Diese sequentielle Abfolge von Basishandlungen wird als eine Handlungsliste bezeichnet. Eine Handlungsliste (Sequenz von Basishandlungen) endet dann, wenn der weitere Handlungsablauf von bestimmten Bedingungen abhängt, die z. B. durch Prozesszustände oder zufälligen Ereignissen gegeben sind.

Eine Handlungsliste ist definiert durch eine

- eindeutige Identifikationsnummer,
- Bedingung, wann die jeweilige Handlungsliste aktiviert wird und
- Angabe der Identifikationsnummern von Basishandlungen, durch die die Handlungsliste beschrieben wird.

Eine Handlungsliste wird dann aktiviert und ausgeführt, wenn die ihr zugeordnete Bedingung erfüllt ist. Dazu muss die einer Handlungsliste zugeordnete Bedingung eindeutig sein. Die Spezifikation einer Bedingung kann durch beliebige Parameter erfolgen. Durch die Zuordnung einer speziellen Bedingung zu jeder Handlungssequenz ist es möglich, Handlungsabläufe z. B. in Abhängigkeit

- von den dynamischen Entwicklungen des Prozess- und Systemzustands,
- vom Zustand des bisher erfolgten Handlungsablaufs,
- von kognitiven und ergonomischen Faktoren und

– von stochastischen Einflussfaktoren

zu berücksichtigen. Die Flexibilität des Konzepts erlaubt es dem Benutzer, die Handlungsabläufe in Wechselwirkung mit Prozesszuständen und stochastischen Einflussgrößen in einem beliebigen Detaillierungsgrad darzustellen.

Alle Handlungslisten, die zur Beschreibung eines Handlungsablaufs definiert werden, werden in einer separaten Datei (*‚cActLst'*) in einer bestimmten Struktur abgelegt, die in Tab. 2.2 beispielhaft dargestellt wird.

Tab. 2.2 Handlungslisten und zugehörige Bedingungen eines Handlungsablaufs

```
1    26 4001 4002 4003 1001 1002 1003 1004 2001 2002 2003 2004 2005 2006 5001 6001 7001 8001 1005 1006 1007 1008 3001 2007 30
1.1  5  3004 6002 6003 6004 6005  2   3 =  1.0   13 <= 1.0
1.1  5  3004 6002 6003 6004 6005  1   3 =  1.3
2    1  6006  2   3 =  1.1   14 <= 1.0
4    13 1009 3005 1010 1011 5002 5003 7002 7003 1012 8002 8003 8004 8005  4   3 >= 2.0   3 <= 3.0   5 <= -9509 9 <= -9511
25   6  1013 8006 8007 1014 8008 8009  3   3 >= 4.0   3 <= 9.0   18 <= 1.0
25   6  1013 8006 8007 1014 8008 8009  3   3 >= 1.6   3 <= 1.65  18 <= 1.0
26   1  1015  2   3 =  25.0  5 < -9516
27   12 1016 4005 1017 8010 1018 7004 1019 4006 1020 4007 1021 7005  2   3 =  25.0  5 >= -9516
27   12 1016 4005 1017 8010 1018 7004 1019 4006 1020 4007 1021 7005  1   3 =  26.0
-99  0   1   3 =  27.0
28   8  1022 8006 1018 7006 8011 1019 4006 4008  3   3 >= 4.0   3 <= 9.0   18 =  2.0
28   8  1022 8006 1018 7006 8011 1019 4006 4008  3   3 >= 1.6   3 <= 1.65  18 =  2.0
29   1  1015  3   2 =  1.0   3 =  28.0  5 < -9516
21   4  1020 4007 1021 7005  3   2 =  1.0   3 =  29.0  5 >= -9516
-99  0   2   2 =  1.0   3 =  21.0
5    13 1009 3005 1011 1010 7002 7003 5002 5003 1012 8012 8003 8004 8005  4   3 >= 2.0   3 <= 3.0   5 <= -9511 11 <= -9509
6    13 3006 1009 3005 1011 5002 5003 7002 7003 1012 8012 8003 8004 8005  4   3 >= 2.0   3 <= 3.0   9 <= -9505 5 <= -9511
7    13 3006 3007 1009 3005 5002 5003 7002 7003 1012 8012 8003 8004 8005  4   3 >= 2.0   3 <= 3.0   9 <= -9511 11 <= -9505
8    13 3007 1009 3005 1010 7002 7003 5002 5003 1012 8012 8003 8004 8005  4   3 >= 2.0   3 <= 3.0   11 <= -9505 5 <= -9509
9    13 3007 3006 7002 7003 5002 5003 1009 3005 1012 8012 8003 8004 8005  4   3 >= 2.0   3 <= 3.0   11 <= -9509 9 <= -9505
3    2  6007 6006  2   3 =  1.1   14 =  2.0
1.2  1  3008  2   3 =  1.0   13 =  2.0
1.3  1  3009  2   3 =  1.2   27 <= 1.0
1.4  3  1009 3005 1023  4   3 =  1.2   27 =  2.0   5 <= -9509 9 <= -9511
```

Die Datenstruktur in Tab. 2.2 liegt kodierter Form vor und ist gegeben durch:

– **Spalte 1:** Nummer der Handlungsliste. Die Nummern der Handlungslisten können auch als Gleitkommazahlen z. B. 1.1, 1.124 etc. definiert werden, um eine bessere Strukturierung der Handlungslisten zu ermöglichen.

- **Spalte 2:** Gibt die Anzahl der Basishandlungen der jeweiligen Handlungsliste an. Danach folgen die Indexnummern der entsprechenden Anzahl der Basishandlungen.
- Nach den Indexnummern der Basishandlungen folgt die Anzahl der Bedingungen und die jeweiligen Anweisungen der Bedingungen in kodierter Form.

Mit den in Abschnitt 2.2.3 beschriebenen Weiterentwicklungen des Crew-Moduls werden die kodierten Eingabedatensätze für das Crew-Modul aus den Informationen der grafischen Oberfläche automatisch erstellt.

2.2.2.3 Definition von Zustandsänderungen während des Handlungsablaufs

Handlungen, die eine Zustandsänderung von Systemkomponenten zur Folge haben (z. B. Abstellen der Hauptkühlmittelumpe), werden durch eine bestimmte Kodierung in Form einer negativen Zahl gekennzeichnet. Die Kodierung erfolgt in dem Attribut einer Basishandlung, auf wen oder was die Basishandlung einen Einfluss hat. Was die Kodierung bewirken soll, d.h. welche Komponente in welchen Zustand geändert wird, muss für das Crew-Modul in einer gesonderten Anweisung in der Datei *‚cState‘* definiert werden. Ein Beispiel solcher kodierten Anweisungen wird in Tab. 2.3 dargestellt.

Tab. 2.3 Kodierte Anweisungen für handlungsbedingte Zustandsänderungen

```
2  1  4 =  -113  13  = 0  13  = 1
2  1  4 =  -114  14  = 0  14  = 1
2  1  4 =  -6    15  = 0  15  = -9510
2  1  4 =  -3    16  = 0  16  = -9509
2  1  4 =  -4    17  = 0  17  = -9511
2  1  4 =  -118  18  = 0  18  = 1
2  1  4 =  -8    19  = 0  19  = -9512
2  1  4 =  -9    20  = 0  20  = -9512
1  1  4 =  -10   5   =  -9516
2  1  4 =  -11   21  = 0  21  = -9508
2  1  4 =  -12   22  = 0  22  = -9512
2  1  4 =  -15   23  = 0  23  = -9511
```

Die Datenstruktur in Tab. 2.3 ist gemäß einer IF … THEN Anweisung angeordnet. Die erste Zeile der Tab. 2.3 ist z. B. wie folgt zu lesen:

Die 1. und 2. Spalte geben jeweils die Anzahl der Bedingungen und Ausführungen der Anweisung an.

Der darauffolgende kodierte Teil ‚4 = -113 13 = 0 13 = 1‘ wird als folgende Anweisung im Crew-Modul verarbeitet: IF Parameter 4 = -113 und Parameter 13 = 0 THEN Parameter 13 = 1 s. Die Nummern der Parameter beziehen sich auf die Parameter, die in der Key-Liste des Crew-Moduls enthalten sind. In der Key-Liste, die durch die Weiterentwicklungen des Crew-Moduls automatisch erstellt wird, sind alle für das Handlungsmodell relevanten Parameter enthalten.

2.2.3 Weiterentwicklung des Crew-Moduls

In der ursprünglichen Version des Crew-Moduls musste der Eingabedatensatz in kodierter Form manuell erstellt werden, was sich als sehr aufwändig und fehleranfällig erwiesen hat. Eine Vorstellung davon erhält man, wenn man sich den kleinen Ausschnitt aus einem Datensatz anschaut, der in den Tab. 2.1 – Tab. 2.3 auszugsweise dargestellt ist. Zudem musste der Nutzer mit den Details der Kodierung vertraut sein, die zur Erstellung des Eingabedatensatzes verwendet werden.

Anwendungen haben außerdem gezeigt, dass nicht nur bei der Erstellung des Eingabedatensatzes für das Crew-Modul ein erheblicher Aufwand durch die Vielzahl der Einzelinformationen besteht. Als weitere Schwierigkeit hat sich auch die Darstellung erwiesen, wie der Handlungsablauf mit seinen vielen Basisereignissen und Verzweigungen, die sich aus stochastischen Ereignissen (aleatorischen Unsicherheiten) und Abhängigkeiten vom Prozesszustand ergeben können, in möglichst übersichtlicher und strukturierter Form beschrieben werden kann.

Dadurch, dass unterschiedliche Handlungssequenzen, die sich in Abhängigkeit von stochastischen Ereignissen und Prozesszuständen ergeben, explizit durch ihre Basishandlungen beschrieben werden müssen, kann der Aufwand für die Beschreibung des Handlungsmodells recht umfangreich, unübersichtlich und damit auch fehleranfällig werden. Aus diesem Grund wurde das Crew-Modul in diesem Projekt so weiterentwickelt, dass die Beschreibung bzw. Modellierung eines Handlungsablaufs über eine grafische Oberfläche durchgeführt werden kann. Durch die Verwendung einer grafischen Oberfläche wird die Beschreibung eines Handlungsablaufs wesentlich vereinfacht und erfolgt in einer übersichtlicheren und strukturierteren Form. Ein erheblicher Vorteil zeigt sich auch darin, dass die über die Oberfläche erstellten Modelle von Handlungsabläufen relativ einfach modifiziert und erweitert werden können.

In Abschnitt 2.2.3.1 wird die grafische Oberfläche zur Modellierung von Handlungsabläufen beschrieben. Die Struktur, wie der Ablauf von menschlichen Handlungen unter Berücksichtigung von stochastischen Ereignissen und Prozesszuständen über die grafische Oberfläche spezifiziert werden kann, wird in Abschnitt 2.2.3.2 vorgestellt.

Mit der grafischen Oberfläche kann zwar die Modellierung eines Handlungsablaufs erheblich vereinfacht und wesentlich übersichtlicher durchgeführt werden. Dennoch bleibt ein erheblicher Aufwand, die Vielzahl der Einzelinformationen zur Erstellung des Eingabedatensatzes für das Crew-Modul in seiner kodierten Form einzugeben. Dies schränkt die Praktikabilität und Benutzerfreundlichkeit des Crew-Moduls erheblich ein. Um diese Einschränkung zu beheben, wurde ein Programm entwickelt, mit dem die Informationen, die in die grafische Benutzeroberfläche zur Modellierung des Handlungsablaufs eingegeben wurden, gelesen und so verarbeitet werden, dass daraus der Eingabedatensatz für das Crew-Modul automatisch erstellt werden kann. Dies stellt einen erheblichen Fortschritt in der Benutzerfreundlichkeit bei der Anwendung des Crew-Moduls dar.

2.2.3.1 Grafische Oberfläche zur Modellierung eines Handlungsablaufs

Die Beschreibung menschlicher Handlungsabläufe kann sehr schnell komplex und unübersichtlich werden, wenn zeitabhängige Wechselwirkungen mit Prozess und Systemzuständen sowie stochastische Einflussgrößen berücksichtigt werden. Diese Komplexität ergibt sich dadurch, dass in Abhängigkeit unterschiedlicher Ausprägungen von Zufallsereignissen oder unterschiedlicher Bedingungen von Systemzuständen oftmals unterschiedliche Handlungsabläufe durchgeführt werden müssen.

Wenn beispielsweise im Rahmen der Notfallmaßnahme ‚Sekundärseitiges Druckentlasten' (SDE) die Kriterien zur Dampferzeuger-Druckentlastung (DE-DrE) durch den Prozess zu einem bestimmten Zeitpunkt t_{crit} anstehen, kann das Personal die DE-DrE erst durchführen, wenn die Arbeiten am Reaktorschutz durchgeführt worden sind. D. h., wenn zum Zeitpunkt t_{crit} die Arbeiten am Reaktorschutz abgeschlossen sind, kann die Druckentlastung der DE durchgeführt werden. Wenn nicht, muss mit den Handlungen zur Druckentlastung der DE so lange gewartet werden, bis die Information kommt, dass die Arbeiten am Reaktorschutz erledigt sind.

Das in dem Vorhaben entwickelte Konzept besteht darin, die Beschreibung bzw. Modellierung von Handlungsabläufen über ein grafisches Mind-Mapping Tool durchzuführen. Ein Mind-Map besteht aus einer Baumstruktur, in deren Zweige beliebige Informationen

eingetragen werden können. Diese Art der Darstellung wurde als geeignet erachtet, Zusammenhänge und Abfolgen von Handlungen zu erstellen und zu visualisieren. Das Konzept wurde umgesetzt, indem für das Crew-Modul das plattformunabhängige Mind-Mapping Tool ‚FreeMind' verwendet wird, das als freie Software (Open Source) zur Verfügung steht. Mit dem Mind-Mapping Tool ‚FreeMind' können Informationen in Form eines Diagramms strukturiert dargestellt werden.

Die Vorteile einer Beschreibung menschlicher Handlungsabläufe über ein grafisches Mind-Mapping Werkzeug, besteht einerseits in der Möglichkeit, die Handlungsabläufe übersichtlicher darzustellen, wobei die Verzweigungen von Handlungsabläufen in Abhängigkeit stochastischer Ereignisse sowie System- und Prozesszuständen über die grafische Darstellung sofort sichtbar sind. Andererseits können Modifikationen im Handlungsablauf relativ unkompliziert vorgenommen werden. Wenn z. B. der Wunsch besteht, einzelne Handlungen differenzierter zu modellieren, oder wenn verschiedene Handlungsstrategien in das Handlungsmodell eingebaut und analysiert werden sollen.

An dem nachfolgenden Beispiel soll veranschaulicht werden, wie die Beschreibung- bzw. Modellierung eines Handlungsablaufs über die grafische Oberfläche sukzessive entwickelt werden kann. Die Struktur, in der die Informationen einzugeben sind, um gelesen und zur automatischen Erstellung des Eingabedatensatzes verwendet werden zu können, wird im nachfolgenden Abschnitt 2.2.3.2 erläutert.

Beispiel: Modellierung eines Handlungsablaufs über die grafische Benutzeroberfläche

Das Beispiel soll veranschaulichen, in welcher Art Handlungsabläufe über die grafische Oberfläche des Mind-Mapping Tools ‚FreeMind' spezifiziert und modifiziert werden können. Zur Veranschaulichung sollen der Einfachheit halber nur die ersten einleitenden Handlungsschritte beschrieben werden, die bzgl. der Notfallmaßnahme SDE durchgeführt werden. Für die ersten Handlungsschritte, die hier beschrieben werden sollen, sind zunächst zwei Personen beteiligt, der Schichtleiter (SL) und der Leitstandfahrer (LF).

Nach dem Aufruf von ‚FreeMind' erscheint zunächst eine Arbeitsfläche, in die die Handlungsabläufe einzugeben sind. Zu Beginn enthält die Arbeitsfläche nur einen leeren Knoten mit der Bezeichnung ‚Neue Mindmap' (s. Abb. 2.10).

In diesen Anfangsknoten sind bestimmte Informationen bzgl. des Handlungsablaufs einzugeben:

- der Titel mit einer Kurzbezeichnung der Maßnahme,
- die Anzahl der an dem Handlungsablauf beteiligten Personen und
- die Kurzbezeichnung der beteiligten Personen. (Die hier angegebenen Kurzbezeichnungen der Personen werden bei der Definition der einzelnen Basishandlungen verwendet.)

Durch Anklicken des Knotens erscheint ein Editor für den Knoten, in den die entsprechenden Informationen eingegeben werden können. Nach der Eingabe enthält der Eingangsknoten die in Abb. 2.10 dargestellten Informationen.

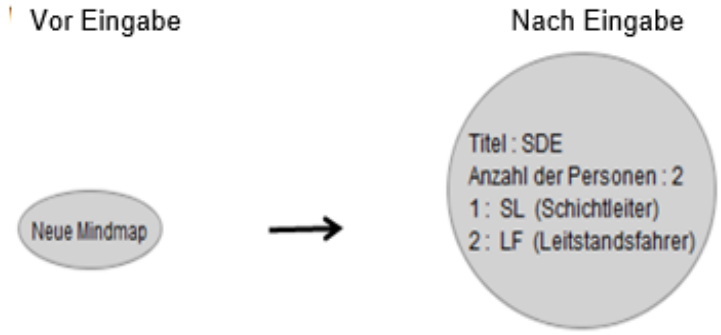


Abb. 2.10 Eingangsknoten zur Definition der an der Handlung beteiligten Person

Nach dem Ausfall der Dampferzeugerbespeisung ist nach einer gewissen Zeit das Kriterium zur Aktivierung der einleitenden Arbeiten für die Notfallmaßnahme SDE gegeben. Das Kriterium ist durch den Prozessablauf bestimmt und steht an, wenn die Füllhöhestände aller vier Dampferzeuger < 4 m sind. Die Dampferzeuger-Füllhöhestände (DE-FH) sind in der Warte über die entsprechenden Anzeigen abzulesen.

Der LF, der für das Ablesen der Anzeigen zuständig ist, kann zufällig die entsprechenden Anzeigen im Blick haben und sofort erkennen, dass alle vier DE einen Füllhöhestand < 4 m aufweisen. Er könnte aber auch zufällig abgelenkt und mit anderen Sachen beschäftigt sein, so dass er seine Aufmerksamkeit erst nach einer gewissen Verzögerungszeit wieder auf die Anzeigen der Füllhöhestände richtet. Um diese Zufälligkeiten (aleatorische Unsicherheiten) zu berücksichtigen, wird die Verzögerungszeit, mit der der LF die Anzeigen registriert, als Zufallsvariable betrachtet. Dabei soll der Einfachheit halber angenommen werden, dass die zufällige Verzögerungszeit zwischen 3 s und 20 s liegen

kann. (In die Abschätzung der Zeitintervalle sollten, soweit vorhanden, Informationen aus der Betriebserfahrung eingehen, um möglichst realistische Verhältnisse in dem Modell abbilden zu können.) Diese Situation des LF soll nun als erste Basishandlung des Handlungsablaufs spezifiziert werden.

Wie bereits in Abschnitt 2.2.2 beschrieben wurde, besteht das Konzept des Crew-Moduls darin den Handlungsablauf in Form von so genannten Handlungslisten zu beschreiben, in denen jeweils eine zugehörige Abfolge von Basishandlungen aufgelistet sind. Um eine erste Handlungsliste zu erzeugen, wird ausgehend vom Eingangsknoten ein Unterknoten über den entsprechenden Aufruf in der Oberfläche erzeugt (s. Abb. 2.11).

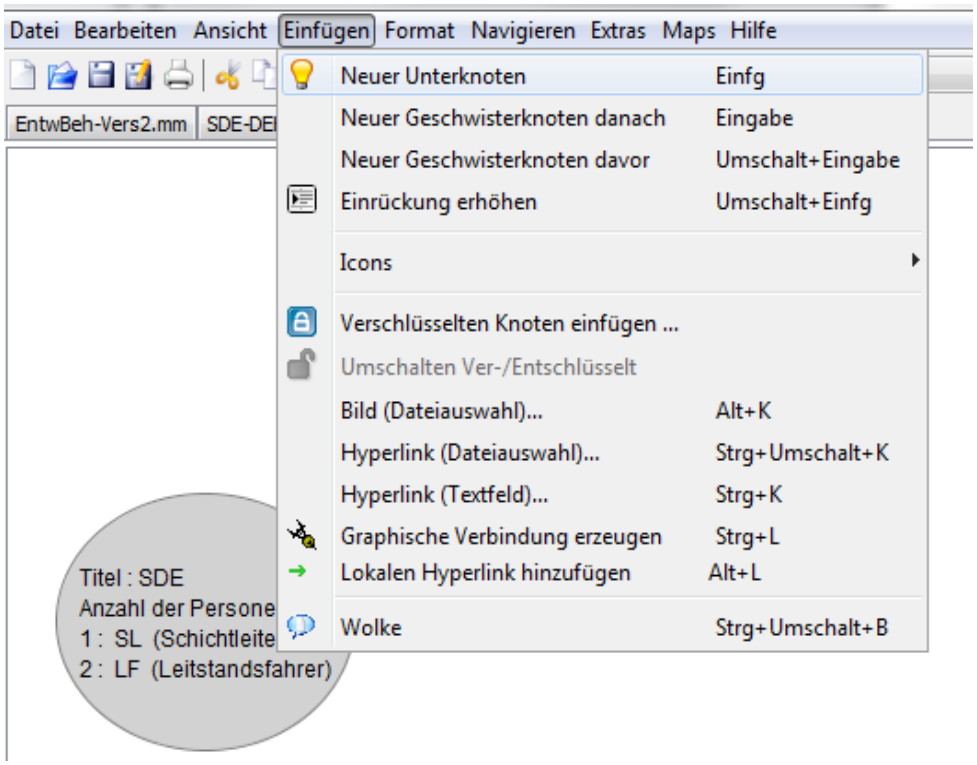


Abb. 2.11 Erzeugung einer neuen Handlungsliste

Jeder neu erzeugte Unterknoten repräsentiert eine Handlungsliste (HL), die eine bestimmte Teilsequenz eines Handlungsablaufs beschreibt. Zur Kennzeichnung einer HL muss in der ersten Zeile des Unterknotens die Identifikationsnummer der HL spezifiziert werden. Außerdem muss für jede neu erzeugte Handlungsliste eine eindeutige Bedingung definiert werden, durch die die Aktivierung der Handlungsliste verursacht wird. Auf die Struktur der Eingabe wird im nachfolgenden Abschnitt 2.2.3.2 eingegangen.

Für den neu erzeugten Unterknoten kann nun die oben beschriebene erste Basishandlung für den LF eingegeben werden, in der er die DE-FH Anzeigen mit einer zufälligen Verzögerungszeit registriert. Dies dient zugleich als ein Beispiel, dass eine Basishandlung nicht unbedingt eine konkrete Aktion beschreiben muss, sondern auch nur aus einer bestimmten Verzögerungszeit bestehen kann, bis die betreffende Person etwas erkennt bzw. Informationen erhält, die ihn dann zu einer gewissen Aktion veranlasst.

Nach einer zufälligen Verzögerungszeit steht der LF vor den Pulten des Hauptleitstandes mit den Informations- und Bedieneinrichtungen für die Sekundärseite. Es sind insgesamt acht Füllstandsanzeigen (zwei pro DE) abzulesen. Für das Ablesen der acht Füllstandsanzeigen wird eine Zufallszeit zwischen 16 und 32 s abgeschätzt. Dabei wird angenommen, dass für das Ablesen einer Anzeige eine Ausführungszeit zwischen 2 und 4 s benötigt werden. Diese Aktion soll als zweite Basishandlung in der HL 1 spezifiziert werden.

Nach der entsprechenden Eingabe der beiden Basishandlungen des LF hat der bisher modellierte Handlungsablauf die in Abb. 2.12 dargestellte Form.

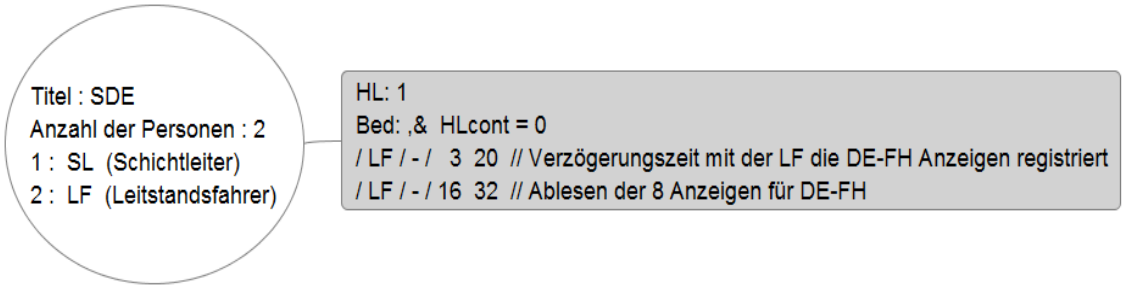


Abb. 2.12 Eingabe der Basishandlungen zum Ablesen der DE-FH Anzeigen

Die nächste vom LF durchzuführende Handlung besteht darin, dass der LF den SL darüber informiert, dass Füllhöhestände der DE unter 4 m gesunken sind. Dies ist eine Handlung, die eine Kommunikation zwischen LF und SL beschreibt, und über die der SL eine neue Information enthält. Die Handlung hat somit einen Effekt auf den SL. Es wird davon ausgegangen, dass sich der SL in der Nähe des LF in der Warte befindet, ohne dass es zu großen Verzögerungen in der Kommunikationshandlung kommt. Für diese Handlung bzw. Kommunikation wird somit eine relativ kurze Zeit zwischen 4 und 8 s abgeschätzt. Nach Eingabe dieser dritten Basishandlung Handlung enthält die HL 1 die in Abb. 2.13 dargestellte Information.

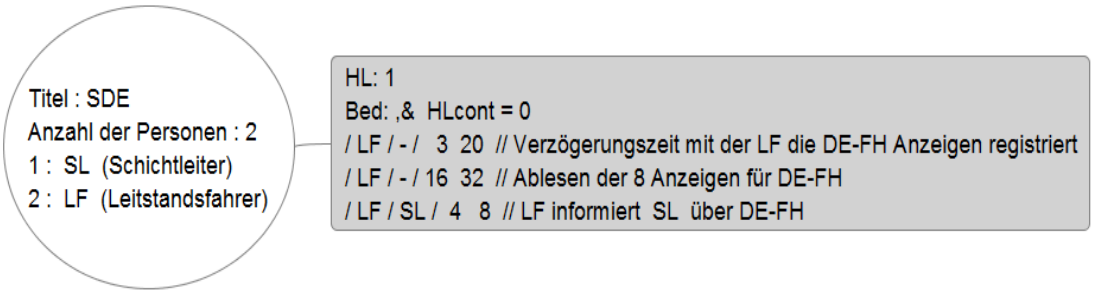


Abb. 2.13 Eingabe der Basishandlung, dass SL über DE-FH informiert wird

Nachdem der SL über den Zustand der DE-FH vom LF informiert wurde, begibt er sich zum Pult des Hauptleitstandes, um selbst die Anzeigen der DE-FH zu kontrollieren und bestätigen zu können. Dazu muss sich der SL, der sich irgendwo in der Warte aufhält, zum Pult begeben. Der SL kann sich in unmittelbarer Nähe zum Hauptleitstand befinden, bei der die benötigte Zeit für den Weg zu den Anzeigen relativ klein sein wird. Der SL kann aber auch etwas weiter entfernt sein. In dem Fall wird er etwas mehr Zeit benötigen, um den Weg zum Hauptleitstand zurückzulegen. In Abhängigkeit davon, wo sich der SL in der Warte zufällig aufhält, wird er für den Weg mehr oder weniger Zeit benötigen. Aus diesem Grund wird die Zeit für den Weg als Zufallsvariable betrachtet, die zwischen 5 s und 15 s liegt. Die Zeit, die der SL für das Ablesen der acht Füllstandsanzeigen benötigt entspricht dem Zeitrahmen, der für den LF abgeschätzt wurde.

Für die beschriebene Aktion des SL werden zwei getrennte Basishandlungen erzeugt, die zur HL 1 hinzugefügt werden (s. Abb. 2.14). Diese zwei Basishandlungen beschreiben einmal den Weg des SL zum Hauptleitstand und zum anderen das Ablesen der DE-FH Anzeigen. Beide Handlungen haben keinen Effekt auf andere Personen oder Komponenten.

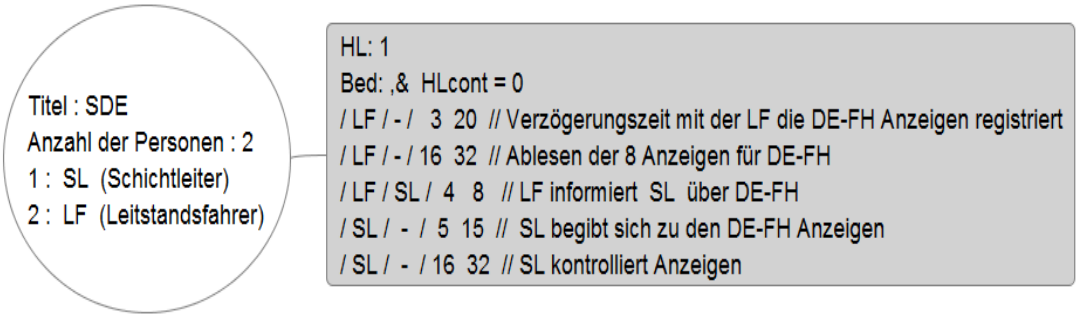


Abb. 2.14 Eingabe der ersten beiden Basishandlungen des SL

Analog kann der Handlungsablauf durch die Definition von Basishandlungen weiter beschrieben werden.

Eine Handlungsliste endet bzw. wird unterbrochen, wenn der weitere Handlungsablauf von bestimmten Bedingungen abhängt. Diese Bedingungen können durch Prozessgrößen oder stochastische Einflussgrößen bestimmt sein. Im Nachfolgenden soll diese Abhängigkeit anhand der oben verwendeten Basishandlungen kurz veranschaulicht werden. Gleichzeitig soll damit demonstriert werden, wie einfach eine Modifikation des Handlungsablaufs unter Verwendung der grafischen Oberfläche durchgeführt werden kann. Aufgesetzt wird bei der Basishandlung, in der der LF den SL darüber informiert, dass die Füllhohestände der DE < 4 m sind. Nun könnten sich zufällig folgende Situationen ergeben:

i) Der SL ist nicht abgelenkt und kann sich sofort auf die Information des LF konzentrieren. In diesem Fall erfasst der SL die Information richtig und reagiert sofort, indem er sich zu den Anzeigen begibt, um sie zu kontrollieren. Das ist genau der Ablauf, der in Abb. 2.14 dargestellt ist. Allerding soll diese Situation jetzt nur als eine von mehreren Möglichkeiten betrachtet werden, die zufällig eintreten kann. Es wird angenommen, dass der SL in ca. 60 % seiner Zeit in der Warte nicht abgelenkt ist. Für solche Art von Abschätzungen sollten Erfahrungswerte aus der Anlage herangezogen werden.

ii) Eine andere Möglichkeit besteht darin, dass der SL die Information vom LF zwar wahrnimmt, aber momentan mit einer anderen Aufgabe beschäftigt ist. D. h., der SL wird nicht sofort reagieren, sondern erst, wenn er seine Aufgabe beendet bzw. unterbrochen hat. Dies resultiert dann in einer gewissen Verzögerungszeit, die von der jeweiligen Handlung abhängt, mit der der SL beschäftigt ist. Der SL ist des Öfteren mit kleineren oder routinemäßigen Aufgaben beansprucht, die er relativ schnell in einem Zeitrahmen von 15 – 30 s unterbrechen kann. Es wird abgeschätzt, dass der SL sich in ca. 38 % seiner Arbeitszeit mit solchen kleineren Aufgaben beschäftigt. Diese Situation unterscheidet sich von der in i) nur durch eine zusätzliche Verzögerungszeit, nach der der SL auf die Information vom LF reagiert.

iii) Es wird angenommen, dass der SL in ca. 2 % seiner Arbeitszeit mit wichtigen und komplexeren Aufgaben beschäftigt ist und für den LF nicht ansprechbar ist. Dazu wir angenommen, dass sich der LF nach einer gewissen Wartezeit von 35 – 45 s entschließt, den SL-Stellvertreter zu informieren, der dann die entsprechende Kontrolle der Füllstandanzeigen durchführt. In diesem Fall tritt mit dem SL-Stellvertreter (SL-V) ein neuer Akteur in den Handlungsablauf ein, der zusätzlich im Eingangsknoten definiert werden muss.

Um die zufälligen Situationen im Handlungsablauf zu modellieren, muss der bisherige in Abb. 2.14 beschriebene Ablauf modifiziert werden. Nach der Basishandlung, in der der LF die DE-FH Anzeigen abgelesen hat und den SL informieren möchte, muss eine sog. Verzweigungsvariable definiert werden. Verzweigungsvariablen werden verwendet, um die Abhängigkeit des Handlungsablaufs von zufälligen Ereignissen (aleatorischen Unsicherheiten) modellieren zu können. Eine Verzweigungsvariable wird mir einem vorangestellten ‚b_' gekennzeichnet. Dem ‚b_' folgt eine vom Benutzer frei wählbare Bezeichnung, durch die die Verzweigungsvariable identifiziert wird, z. B. ‚b_SLverf' für die Verfügbarkeit des SL.

Um die aleatorische Unsicherheit der in i) – iii) beschriebenen Situationen im Handlungsablauf modellieren zu können, muss die Unsicherheit durch die Verzweigungsvariable ‚b_SLverf' beschrieben werden. In der Simulation des Handlungsablaufs durch das Crew-Modul erhalten die Verzweigungsvariablen ihre Werte durch Kommunikation mit MCDET, in dem die Wahrscheinlichkeiten der Verzweigungen spezifiziert werden müssen. Für jede Sequenz werden dem Crew-Modul automatisch die entsprechenden Werte der Verzweigungsvariablen über MCDET geliefert. Durch MCDET werden die Verzweigungen des Handlungsmodells strukturiert abgearbeitet, dass alle möglichen Kombinationen von Verzweigungen dem Crew-Modul übergeben und in der Analyse berücksichtigt werden. Durch die Kopplung des Crew-Moduls mit MCDET können somit die Einflüsse aleatorischer Unsicherheiten auf den Handlungsablauf berücksichtigt werden.

Die Modellierung der beschriebenen zufälligen Situationen, in denen der SL mehr oder weniger schnell verfügbar ist, wird in Abb. 2.15 dargestellt.

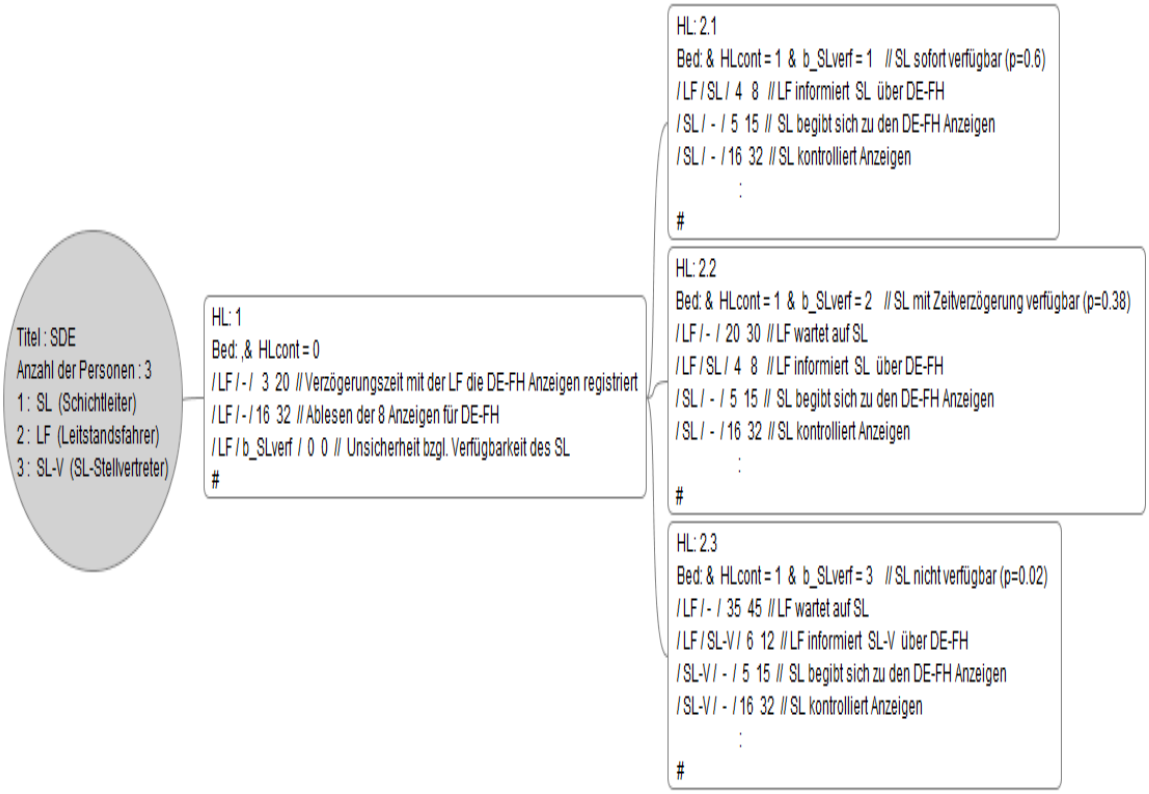


Abb. 2.15 Einbindung aleatorischer Unsicherheiten bzgl. der Verfügbarkeit des SL

Wie Abb. 2.15 zeigt, werden zur Modellierung der zufälligen Situationen i) – iii) drei neue Handlungslisten erstellt, die von HL 1 abzweigen.

Die erste neu hinzugefügte Handlungsliste, die von HL 1 abzweigt, erhält die Identifikationsnummer 2.1. In HL 2.1 wird die unter i) beschriebene Situation modelliert, dass der SL auf die Information vom LF sofort reagiert. Diese Situation wird durch ‚b_SLverf=1' gekennzeichnet, die in der Bedingung der HL 2.1 aufgeführt werden muss. Die Handlungen, die ausgeführt werden, wenn der SL sofort reagiert, wurden bereits in der ersten Version der HL 1 (s. Abb. 2.14) beschrieben. Diese Handlungen befinden sich nun nicht mehr in der HL 1, sondern werden in der HL 2.1 aufgeführt.

Durch die Bedingung in HL 2.1 wird angegeben, dass die HL 2.1 aktiviert wird, wenn ‚HLcont = 1 und b_SLverf = 1' ist. HLcont gibt ID-Nummer derjenigen HL an, auf die die aktuelle HL aufsetzt. Nach der Bedingung werden die Basishandlungen angegeben, die den Ablauf der HL 2.1 beschreiben.

Die anderen beiden Situationen werden über HL 2.2 und HL 2.3 modelliert, die entsprechend HL 2.1 zu interpretieren sind.

In analoger Weise zu dem oben beschriebenen Vorgehen kann der gesamte Handlungsablauf mit der grafischen Oberfläche strukturiert und übersichtlich modelliert werden. Auf Besonderheiten in der Eingabe und Modellierungsmöglichkeiten wird in Abschnitt 2.2.3.2 eingegangen.

Durch die grafische Oberfläche konnte die Modifikation des Handlungsablaufs um die aleatorische Unsicherheit bzgl. der Verfügbarkeit des SL mit minimalem Aufwand umgesetzt werden. Obwohl die Anzahl der Handlungslisten und Basishandlungen mit zunehmender Berücksichtigung von Abhängigkeiten und stochastischen Einflüssen schnell anwächst und entsprechend viele Basishandlungen definiert werden müssen, was sehr aufwändig erscheint, ist die Erstellung eines Modells zu einem Handlungsablauf durch die Möglichkeiten der grafischen Oberfläche relativ einfach und übersichtlich durchzuführen. Auch die Modifikation von Handlungsabläufen, z. B. durch Einfügen von aleatorischen Unsicherheiten über Verzweigungsvariable, kann relativ unkompliziert durchgeführt werden.

2.2.3.2 Konzept der Eingabestruktur in die Oberfläche

Die Modellierung einer Handlungsmaßnahme im Crew-Modul erfolgt durch die explizite Beschreibung der zu analysierenden Handlungsabläufe, die unter bestimmten System- und Prozessbedingungen durchgeführt werden. Wie oben bereits erwähnt, werden Teilhandlungen, die unter bestimmten Bedingungen durchgeführt werden, durch Handlungslisten beschrieben. Handlungslisten setzen sich aus einer Sequenz von Basishandlungen zusammen, die von bestimmten Personen ausgeführt werden und die einen Effekt auf Komponenten (z. B. Pumpe wird ausgeschaltet) oder andere Personen (z. B. LF informiert den SL über Füllhöhestände der DE) haben können. Ein weiteres wichtiges Attribut einer Basishandlung ist die Zeit, die benötigt wird, um die Basishandlung auszuführen. Die Struktur, wie Handlungslisten zur Beschreibung einer menschlichen Handlung in die graphische Oberfläche eingegeben werden, wurde bereits in Abschnitt 2.2.3.1 veranschaulicht.

In diesem Abschnitt wird beschrieben, wie die Informationen innerhalb der Handlungslisten einzugeben sind. Um die Informationen der Oberfläche zur automatischen Erzeugung der Eingabedateien für das Crew-Modul lesen und verarbeiten zu können, müssen

die in die grafische Oberfläche einzugebenden Informationen einer festen vorgegebenen Struktur folgen.

Die Beschreibung der Datenstruktur, mit der die Informationen in die Oberfläche einzugeben sind, erfolgt anhand des in Abschnitt 2.2.3.1 verwendeten Beispiels. Als typischer Fall sollen die Handlungslisten in Abb. 2.15 dienen, in denen verschiedene Teilhandlungen beschrieben wurden, die sich in Abhängigkeit einer aleatorischen Unsicherheit ergeben können. Die aleatorische Unsicherheit besteht hier in der Verfügbarkeit des SL, der eine Situation beurteilen muss und Entscheidungen zur Durchführung von Maßnahmen zu treffen hat. Die Handlungsliste 1 (HL 1) in Abb. 2.15 enthält folgende Informationen:

```
HL: 1
Bed:  & HLcont = 0
/ LF  / - /   3  20      // Verzögerungszeit mit der LF die Anzeigen der DE-FH registriert
/ LF  / - / 16  32       // Ablesen der 8  FH-DE Anzeigen
/ LF  / b_SLverf /  0  0  // Unsicherheit bzgl. Verfügbarkeit des SL
#
```

- Die erste Zeile einer Handlungsliste beginnt mit dem Keyword **‚HL:‘** und es folgt eine eindeutige Identifikationsnummer der Handlungsliste. Die Identifikationsnummer ist eine positive Zahl. Um die Benennung der Handlungslisten besser strukturieren zu können, können auch Identifikationsnummern der Art 2.1, 2.2, 2.12 etc. verwendet werden.

- Die zweite Zeile einer Handlungsliste wird mit dem Keyword **‚Bed:‘** eingeleitet. In dieser Zeile wird die Systembedingung angegeben, die erfüllt sein muss, damit die jeweilige Handlungsliste aktiviert wird. Die einzelnen Bedingungen werden durch das Zeichen **‚&‘** voneinander getrennt.

- Eine Variable, die in jeder Bedingung einer Handlungsliste vorkommen muss, ist die Variable **‚HLcont‘**. Diese Variable erhält die Nummer derjenigen Handlungsliste, auf die die aktuelle Handlungsliste aufsetzt. Da die HL 1 die erste Handlungsliste im Ablauf darstellt und auf keine vorherige HL aufsetzt, ist in diesem Fall die Bedingung gegeben durch ‚HLcont = 0‘. Da keine weitere Bedingung gegeben ist, wird durch ‚HLcont = 0‘ die HL 1 sofort aktiviert. Mit dieser Handlungsliste beginnt der Handlungsablauf.

- Die nachfolgenden Zeilen dienen zur Eingabe der einzelnen Basishandlungen, die in der jeweiligen Handlungsliste durchgeführt werden. Die Informationen der Basishandlungen bestehen aus den jeweiligen Attributen, wer die Basishandlung ausführt, welche Komponente bzw. welche Person wird durch die Basishandlung beeinflusst, Ausführungszeit der Basishandlung und kurze Beschreibung der Basishandlung. Jede Basishandlung wird mit einem **‚/‘** eingeleitet und die einzelnen Informationen zu den Attributen werden ebenfalls durch das Zeichen **‚/‘** voneinander getrennt. Die Kurzbeschreibung der Basishandlung wird mit dem Zeichen **‚//‘** eingeleitet.

- Jede Basishandlung wird in einer separaten Zeile beschrieben. Die Informationen der Zeile 3 in HL 1 beschreiben die Basishandlung, in der der LF die Füllhöhestände der DE erst nach einer zufälligen Verzögerungszeit zwischen 3 und 20 s registriert.

- Falls die Basishandlung nur diejenige Person beeinflusst, die die Handlung auch ausführt, wird für das Attribut, welche Komponente bzw. welche Person wird durch die Basishandlung beeinflusst wird, entweder ‚**-**‘ oder das gleiche Kürzel der ausführenden Person angegeben. Da von der Basishandlung in Zeile 3 nur der LF betroffen ist, der die Handlung ausführt, wird als Information, wer durch die Basishandlung beeinflusst wird, das Zeichen ‚**-**‘ eingegeben. Alternativ hätte in diesem Fall statt ‚-‘ auch ‚LF‘ eingegeben werden können.

- Das Attribut, in dem die Ausführungszeit der Basishandlung eingegeben wird, besteht aus zwei Zahlen (z. B. 3 20). Wenn die Ausführungszeit der Basishandlung als Zufallsvariable betrachtet werden soll, drückt die erste der beiden Zahlen das Minimum und die zweite das Maximum der möglichen Ausführungszeit aus. Die Zufallszeiten werden aus einer Gleichverteilung ausgespielt. Sollten detailliertere Informationen zu den Ausführungszeiten vorliegen, können auch andere Wahrscheinlichkeitsverteilungen zugrunde gelegt werden.

- Wenn die Ausführungszeit der Basishandlung nicht als Zufallsgröße, sondern als fester Wert berücksichtigt werden soll, wird zweimal die gleiche Zahl eingegeben. Wenn z. B. die Verzögerungszeit als feste Größe von 10 s in die Modellierung eingehen soll, ist ‚**10 10**‘ als Ausführungszeit anzugeben.

- Die Beschreibung einer Basishandlung wird durch das Zeichen ‚//‘ eingeleitet. Obwohl die Beschreibung einer Basishandlung optional ist, sollte sie grundsätzlich angegeben werden, um das Modell des Handlungsablaufs besser nachvollziehen und überprüfen zu können.

- Eine Ausnahme stellt die Zeile / LF / b_SLverf / 0 0 // Unsicherheit bzgl. Verfügbarkeit des SL der HL 1 dar. Hier wird ein Sonderfall einer Basishandlung dargestellt, durch den eine Verzweigung aufgrund einer aleatorischen Unsicherheit erzeugt wird. Zur Erzeugung von Verzweigungen aufgrund aleatorischer Unsicherheiten werden im zweiten Attribut Variablen mit einem vorangestellten ‚**b_**' verwendet. D. h., immer dann, wenn im zweiten Attribut einer Basishandlung eine Variable mit vorangestelltem ‚**b_**' auftritt bedeutet dies zwangsläufig, dass von dieser HL mehrere alternative Handlungslisten in Abhängigkeit der Ausprägung der zufälligen Größe abzweigen. Des Weiteren bedeutet dies, dass dies die letzte Anweisung (bzw. Basishandlung) der jeweiligen Handlungsliste ist und dass für das Attribut der Ausführungszeit zweimal die 0 einzugeben ist. Durch das erste Attribut wird in diesem Fall die Person oder im weiteren Sinne der Zeitpunkt beschrieben, wann die Unsicherheit auftritt.
- Das Ende einer Handlungsliste muss mit dem Zeichen ‚**#**' gekennzeichnet werden.

Alle Handlungslisten und alle Basishandlungen in einer Handlungsliste sind in dieser Struktur analog zu beschreiben.

Einen kleinen beispielhaften Ausschnitt, wie die Eingabedateien für das Crew-Modul aussehen, zeigen die Tab. 2.1, 2.2 und 2.3 in Abschnitt 2.2.2. Daraus sollte ersichtlich sein, dass eine manuelle Erstellung der Eingabedateien für das Crew-Modul aus den Informationen der Oberfläche sehr aufwändig und fehleranfällig ist. Aus diesem Grund wurde ein Programm entwickelt, mit dem die Informationen aus der Oberfläche gelesen und so verarbeitet werden, so dass die notwendigen Eingabedateien automatisch erstellt werden können. Die entsprechende Routine wurde als Python-Programm implementiert. Das Programm wurde für das Anwendungsbeispiel in Abschnitt 4.3 sowie für die Notfallmaßnahme SDE, deren aleatorische Unsicherheit in die in Abschnitt 3 beschriebene MCDET/ATHLET-CD Analyse eingeht, erfolgreich eingesetzt.

Es hat sich gezeigt, dass mit der Entwicklung der Oberfläche zur Beschreibung und dynamischen Modellierung von Handlungsabläufen sowie mit der Entwicklung des Programms zur automatischen Erstellung der Eingabedateien für das Crew-Modul, der Arbeitsaufwand für die Modellierung und Analyse menschlicher Handlungen erheblich reduziert und vereinfacht werden kann. Gleichzeitig verringert sich mit den entwickelten Werkzeugen die Fehleranfälligkeit bei der Erstellung der Eingabedatensätze und das Model des Handlungsablaufs ist im Einzelnen besser nachvollziehbar und überprüfbar. Insgesamt ist durch die Entwicklungsarbeiten in diesem Projekt die Anwendbarkeit des

Crew-Moduls zur dynamischen Modellierung und Simulation von Handlungsabläufen wesentlich vereinfacht worden.

2.3 Entwicklung zum Postprocessing – Zusammenfassung, Auswertung und Darstellung von Ergebnissen einer MCDET Analyse

In der bisherigen Version von MCDET wurden die Ergebnisse einer MCDET-Analyse gemäß ihrer sequentiellen Abarbeitung in getrennte Textfiles geschrieben. Die gesamte probabilistische Information wurde in einem sogenannten ‚Sequence'-File zusammengefasst. Für die Zeitreihen der Prozessgrößen wurde für jede gerechnete Sequenz ein separates Output-File erzeugt. Um die Ergebnisdaten einer MCDET-Analyse auszuwerten, mussten diese Daten gelesen und entsprechend verarbeitet werden. Dies erfolgte bisher über speziell erstellte Fortran-Programmroutinen. Diese Programmroutinen mussten in Abhängigkeit von der gewünschten Auswertung und Fragestellung jeweils manuell modifiziert und kompiliert werden.

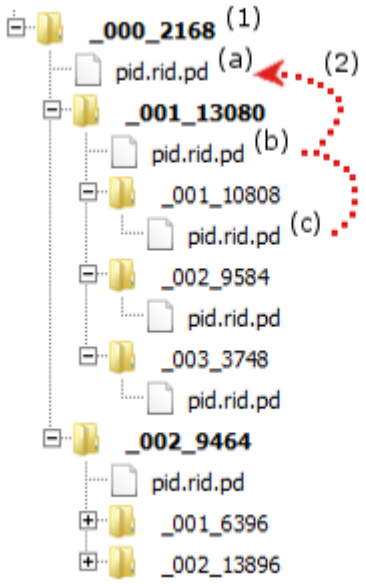
Durch den neu entwickelten MCDET-Scheduler hat sich die Ablaufstruktur einer MCDET-Analyse komplett geändert. Während bisher die einzelnen Sequenzen eines dynamischen Ereignisbaumes (DET) sequenziell nach dem ‚First In Last Out'-Prinzip berechnet wurden, werden die Sequenzen mit dem neu entwickelten MCDET-Scheduler weitestgehend parallel abgearbeitet. Mit der geänderten Abarbeitung der Sequenzen eines DETs ändert sich auch die Ausgabestruktur der Ergebnisse. Diese geänderte Ausgabestruktur hat zur Folge, dass die bisher erstellten Programmroutinen zum Postprocessing nicht mehr verwendet werden können und neu erstellt werden müssen.

Zur Auswertung und Visualisierung der umfangreichen Ergebnisse einer IDPSA unter Verwendung von MCDET sind Konzepte zur benutzerfreundlichen Anwendung von Postprocessing Programmen erstellt und implementiert worden. Bei der Neuentwicklung der Auswertung wird insbesondere darauf geachtet, die Auswerteroutinen plattformunabhängig und benutzerfreundlich zu gestalten, um MCDET einem breiteren Anwenderkreis zugänglich zu machen.

In Abschnitt 2.3.1 wird beschrieben wie die Ergebnisse einer MCDET-Analyse zusammengefasst und im HDF5-Format strukturiert werden. Die darauffolgenden Abschnitte 2.3.2 und 2.3.3 befassen sich mit dem Vorgehen zur Erstellung der Auswerteroutinen bzw. der aussagekräftigen Visualisierung der Ergebnisse.

2.3.1 Zusammenfassung und Strukturierung der Ergebnisse

Wie in Abschnitt 2.1.3 beschrieben, wird die von der DET-Struktur vorgegebene Hierarchie verwendet, um die große Anzahl von Simulationsläufen, die bei einem MCDET-Rechenlauf entstehen können organisiert abzulegen. Die daraus resultierende Verzeichnisstruktur (siehe Abb. 2.16) enthält dann alle von den Simulationsprozessen erzeugten Ausgabedateien, welche dazu verwendet werden können, um den Verlauf der Simulationen im Detail zu analysieren. Hierbei ist zu beachten, dass die durch die Abspaltung der Kindsprozesse entstehende Hierarchie vor allem auch genutzt wird, um redundante Daten zu vermeiden. Die von den Simulationen abgelegten Zeitreihen (im Fall von ATHLET-CD sind dies pd-Dateien) beginnen immer erst zum dem Zeitpunkt, an dem die neue Sequenz von ihrem Elternprozess abgespalten wurden. Für die Analyse der gesamten Entwicklung eines Simulationspfades wird es dadurch notwendig, auch die Daten der jeweiligen Elternprozesse zu berücksichtigen und die Zeitreihendaten entsprechend zusammenzusetzen.



- Alle Arbeitsverzeichnisse werden nach dem Schema `_<Index>_<ProzessId>` benannt.

(1) Das Arbeitsverzeichnis des Root-Simulationsprozesses ist durch den Index `000` erkennbar, da es nicht durch Abspaltung erstellt wurde.

(2) Der Weg von den Blattverzeichnissen hin zur Wurzel erlaubt durch umgekehrtes Zusammensetzen den Zugriff auf die gesamte Zeitreihenentwicklung aller Simulationspfade.

Abb. 2.16 Die Struktur der Arbeitsverzeichnisse eines MCDET-Rechenlaufs

Basierend auf der oben beschriebenen Hierarchie der Arbeitsverzeichnisse wurde ein Postprocessor-Programm (SequenceWalker) vorbereitet, welches das nachträgliche Zusammensetzen der Zeitreihen aller Simulationspfade automatisiert und somit die klassische Auswertung der Simulatordaten erlaubt. Neben den Zeitreihen der Simulationspfade werden für eine MCDET-Analyse allerdings noch zusätzliche probabilistische Daten benötigt, wie z. B. Ereignis- und Pfadwahrscheinlichkeiten, die bei der Zusammenstellung der Zeitreihen über den SequenceWalker zunächst nicht enthalten sind.

Darüber hinaus werden von ATHLET-CD aus Speicherplatzgründen bei weitem nicht alle Zeitschritte gespeichert, welche aber in der MCDET-Analyse gebraucht werden, da hier die Ereignisanalyse zeitschrittgenau erfolgt. D. h., im ATHLET-Eingabesatz kann angegeben werden, nach wie vielen Zeitschritten ein Zeiteintrag (Zeile in PD-Datei) gespeichert werden soll. Diese Einstellung kann bei großen Simulationen nur sehr grob (100, meist eher 1000) gewählt werden, um die PD-Datei nicht übermäßig anwachsen zu lassen. Für MCDET werden jedoch alle Zeitschritte benötigt, weil nach jedem Schritt prinzipiell ein Zufallsereignis eintreten kann.

2.3.1.1 Die HDF5-Ausgabe

Um in den Analyseschritten des Postprocessings alle wichtigen Daten – Zeitreihen aller Simulationspfade und die zu den jeweiligen Zeitreihen gehörigen probabilistischen Daten – vorliegen zu haben und trotzdem den Speicherplatzbedarf der Simulationen in Grenzen zu halten, wurde die Ausgabe aller relevanten Daten im HDF5-Format implementiert. Wie in Abschnitt 2.1.3 beschrieben, synchronisiert das Scheduling-System den getakteten Ablauf aller Simulationen, steuert den Zeitpunkt der Zustandsbewertungen, fordert die dafür benötigten Simulationsdaten von den Simulationsprozessen an und überträgt diese an das Probabilistik-Modul (MCDET-Kern). Durch diese zentrale Funktion eignet sich das Scheduling-System sehr gut, um auch die Ausgabe aller für das Postprocessing benötigten Daten zu übernehmen.

Das HDF5-Format bietet viele Möglichkeiten Daten frei strukturiert in einer Datei abzulegen und ist gleichzeitig für die Speicherung sehr großer Datenaufkommen optimiert. Fortlaufende Daten, wie Zeitreihen, werden dabei als Tabellen abgespeichert, die durch eine hierarchische Gruppenstruktur, sehr ähnlich zu Verzeichnisstrukturen, flexibel organisiert und mit Metadaten ausgezeichnet werden können. Aufgrund dieser Eigenschaften eignet sich HDF5 hervorragend, um alle überwachten Größen eines MCDET-Rechenlaufs aufzunehmen und später den Postprocessing-Werkzeugen mit schnellem Zugriff bereitzustellen.

Die für die HDF5-Ausgabe gewählte Struktur wurde auf die Bedürfnisse des Postprocessings angepasst und konnte dadurch deren Entwicklung erheblich vereinfachen. Abb. 2.17 gibt einen Überblick darüber, wie die Daten in der HDF5-Ausgabedatei organisiert werden. Wie man links in der Baumdarstellung erkennen kann, wird auch hier die DET-Hierarchie als grundlegende Struktur verwendet. Die Gruppen werden dabei nach dem gleichen Namensschema benannt, welches auch schon für die Arbeitsverzeichnisse der Simulationsprozesse verwendet wird. Dadurch können alle Daten leicht ihrem Ursprung zugeordnet werden. Die je Simulationspfad gespeicherten Daten werden in drei Arten unterteilt, und in separaten Tabellen abgelegt.

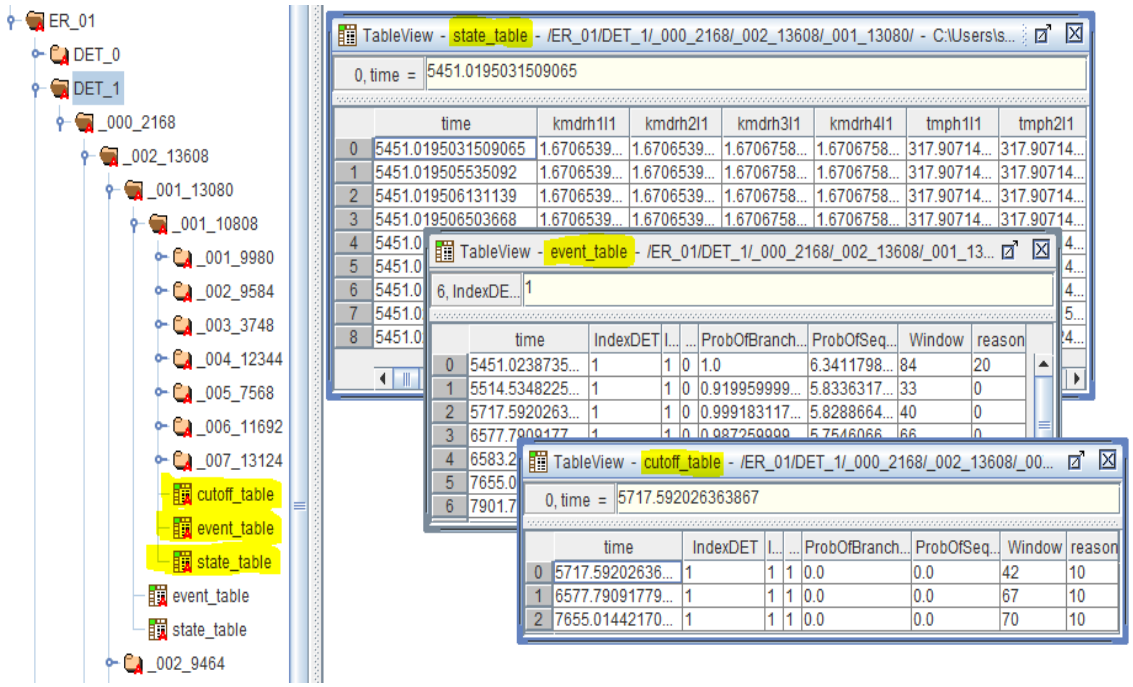


Abb. 2.17 Die Datenstruktur in der HDF5-Ausgabedatei

- **state_table:** Die Zustandstabelle speichert einen ausgewählten Teil des Simulationszustandes zeitschrittgenau und umfasst sämtliche Simulationsgrößen, welche für die Bewertung durch das Probabilistik-Modul oder in der späteren Analyse des Postprocessings herangezogen werden. Durch die Auswahl einiger hundert Simulationsvariablen und tausenden von Zeitschritten kann diese Tabelle schnell eine beachtliche Größe annehmen.

- **event_table:** Die Ereignistabelle speichert alle wichtigen Daten zu stochastischen Ereignissen und Abbruchkriterien, welche im Verlauf eines Simulationspfades auftreten und die zu einer Abspaltung von Unterpfaden oder zum vorzeitigen Beenden der Simulation führen. Diese Daten enthalten sowohl die Pfadwahrscheinlichkeiten

als auch die Auslöser der Ereignisse. Dadurch kann die Entwicklung der Sequenzen sehr gut nachvollzogen werden.

- **cutoff_table:** Diese Tabelle entspricht der event_table, enthält aber im Unterschied dazu nur Ereignisse, die aufgrund zu geringer Wahrscheinlichkeit nicht weiter berechnet wurden. Dadurch gehen diese Wahrscheinlichkeitsbeiträge nicht verloren und können in der Auswertung berücksichtigt werden. Diese Tabelle wird nur erstellt, falls im Simulationspfad entsprechende Ereignisse auftreten.

- HDF5 speichert die Daten sehr effizient und kann zusätzlich durch Datenkompression sehr viel Speicherplatz einsparen. Trotzdem ist es durch die große Anzahl an Simulationspfaden auch hier wichtig die Daten nicht redundant zu speichern. Da auch die HDF5-Ausgabe ihre Gruppenhierarchie gemäß der DET-Struktur organisiert, kann für alle Simulationspfade die vollständige Entwicklung der Zeitreihen und der aufgetretenen Ereignisse nach Bedarf einfach zusammengesetzt werden. Wie bei der Rekonstruktion der Simulatordaten, die über die Hierarchie der Arbeitsverzeichnisse verteilt abgelegt sind (siehe auch Abb. 2.16), kann mit den HDF5-Tabellen nach dem gleichen Schema verfahren werden. Für die nachfolgenden Schritte der Ergebnisauswertung wurde ein Postprocessor-Programm (HDF5Walker) erstellt, welches auf Basis der HDF5-Dateien arbeitet und der Analyse viele Möglichkeiten für den schnellen Datenzugriff bietet.

- Die Speicherung der Ergebnisse der MCDET/ATHLET-CD Analysen im HDF5-Format wurde auch dahingehend optimiert, um die abgelegten Daten möglichst effizient für das Postprocessing nutzen zu können. Z. B. wurde die Ausgabe der probabilistischen Daten so eingerichtet, dass für jeden Verzweigungspunkt die Identifikationsnummer des für die Verzweigung verantwortlichen Transition-Windows angegeben wird. Durch ein Transition-Windows werden in MCDET die Verzweigungen und zugehörige Wahrscheinlichkeiten von Zufallsgrößen definiert.

- Diese Zuordnung hat sich in der Testphase der MCDET-Analysen als sehr hilfreich erwiesen, da man durch die Kennzeichnung des Transition-Windows sofort feststellen kann, welches Ereignis zur jeweiligen Verzweigung geführt hat und welche Prozessgrößen durch die Verzweigung betroffen sind.

2.3.2 Erstellung von Auswerteroutinen über iPython-Notebooks

Durch den neu entwickelten MCDET-Scheduler hat sich die Ablauf- und Ausgabestruktur einer MCDET-Analyse komplett geändert. Durch die neue Ausgabestruktur der MCDET-

Analyseergebnisse im HDF5-Format können die FORTRAN-Programme, die bisher für das Postprocessing verwendet wurden, für die neu entwickelte Version von MCDET nicht weiter eingesetzt werden. Aus diesem Grund wurde begonnen, Funktionen für das Postprocessing auf der Basis von Python Programmen neu zu erstellen. Dabei wurde von Beginn an darauf geachtet, gleichartige Funktionen in typische methodische Klassen zusammenzufassen, um so die notwendigen Analyseschritte des MCDET-Postprocessings modular zu organisieren.

Um kontinuierlich und flexibel an der Weiterentwicklung und Strukturierung der Funktionenklassen zu arbeiten werden die zu entwickelnden Funktionen zunächst in Form eines iPython-Notebooks erstellt. Ein iPython-Notebook ist eine interaktive Entwicklungsumgebung, mit der die verschiedenen Funktionen für das Postprocessing sukzessive erstellt und interaktiv aufgerufen und getestet werden können. Diese Entwicklungsumgebung dient als nützliche Vorstufe zu einer graphischen Benutzeroberfläche, da bei dieser Form der Implementierung ein einheitlicher Aufbau der Funktionenaufrufe und der Darstellungsoptionen einfach getestet und bei Bedarf ohne viel Aufwand nachgebessert werden kann. Ein weiterer Vorteil des iPython-Notebooks ist, dass Auswertebeispiele für den Benutzer so vorbereitet werden können, um später als methodische Einheiten in eine neue, flexible graphische Benutzeroberfläche übernommen werden zu können.

Ein iPython Notebook ist ein Python-basiertes Dokument, das in einem beliebigen Internet-Browser geöffnet und ausgeführt werden kann. Somit ist die Plattformunabhängigkeit für diese neue Version des Postprocessings von Anfang an gewährleistet. Das Notebook erlaubt es ein Anwendungsskript in unabhängige Skript-Zellen zu unterteilen, die nacheinander und auch mehrfach ausgeführt werden können. Dabei wird pro Zelle das Ergebnis des jeweils letzten abgearbeiteten Rechenschrittes ausgegeben oder darin generierte Abbildungen dargestellt. Des Weiteren kann zwischen den Zellen Text eingebunden werden, um beispielsweise die Rechenschritte direkt im Notebook zu dokumentieren. Diese Eigenschaften erleichtern insbesondere die unabhängige Erstellung und umfassende Erprobung neuer Funktionen für das Postprocessing.

Da man sich bei der Entwicklung auf die einzelnen Funktionen beschränken kann, können auch Optionen, die mit dieser Funktion verbunden sein können, erstellt und getestet werden, wie z. B. Plotten einer oder mehrerer Funktionen in einer Grafik. Im Hinblick auf die später zu erstellende graphische Oberfläche kann bereits hier darauf geachtet werden, wie die Argumente (bzw. der Input) zum Aktivieren der einzelnen Optionen in der graphischen Oberfläche aussehen könnte. Die einzelnen erstellten Funktionen können

später flexibel miteinander verbunden werden, um im Rahmen einer Auswertung verschiedene Funktionen auszuführen, z. B. Berechnung einer bedingten Verteilung einer Prozessgröße und graphische Darstellung der bedingten Verteilung.

Eine Übersicht über die neu erstellten Funktionen für das Postprocessing auf der Basis der neu entwickelten Ausgabestruktur ist in Abb. 2.18 dargestellt.

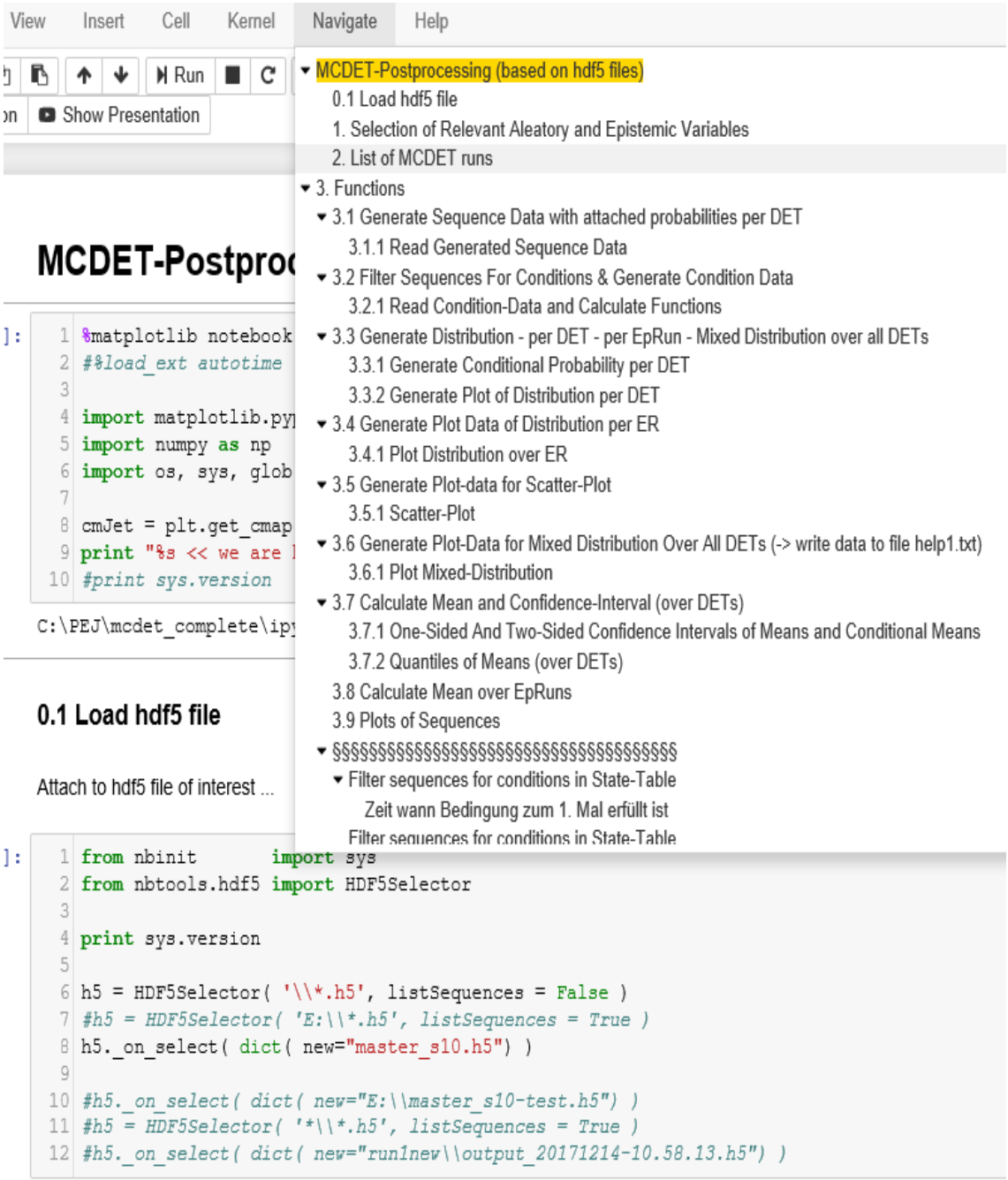


Abb. 2.18 Funktionen für das Postprocessing in einem iPython Notebook

Zur Veranschaulichung zeigt Abb. 2.18 zwei Zellen des erstellten iPython Notebooks mit Python-Code. Jede der einzelnen Zellen führt eine bestimmte Funktion aus. Die Zelle unter Punkt 0.1 „Load hdf5 file“ liest den HDF5-File ein, der die auszuwertenden Ergebnisse der durchgeführten MCDET/ATHLET-CD Analyse enthält.

Im Folgenden werden einige Funktionen beschrieben, die für das Postprocessing erstellt und für die Auswertung der Ergebnisse der in Abschnitt 3 beschriebenen MCDET/ATHLET-CD Analyse bereits erfolgreich eingesetzt wurden.

Eine Funktion, die in Abb. 2.18 unter Punkt 3.1 aufgeführt ist (‚Generate Sequence Data with Attached Probabilities‘), betrifft die automatische Zusammenstellung aller erzeugten Sequenzen aus den jeweiligen Teilsequenzen der HDF5-Ausgabestruktur und die Zuordnung der zugehörigen Eintrittswahrscheinlichkeit der jeweiligen Sequenzen. Für jeden erzeugten dynamischen Ereignisbaum (DET) werden die Informationen ermittelt, wieviel Sequenzen in den jeweiligen DETs gerechnet worden sind und es wird die kumulierte Wahrscheinlichkeit der gerechneten Sequenzen in einem DET angegeben. Ist die kumulierte Wahrscheinlichkeit der Sequenzen eines DET < 1, so weist dies darauf hin, dass es Sequenzen in dem DET gibt, deren Berechnung aufgrund zu geringer Wahrscheinlichkeiten unterlassen wurde. Dieser Schwellenwert der Wahrscheinlichkeit, ab dem eine Sequenz nicht mehr gerechnet wird, kann vom Benutzer definiert werden.

Mit der Funktion „Filter Sequences for Conditions and Generate Condition Data“ unter Punkt 3.2 (s. Abb. 2.18) werden alle in der Analyse erzeugten Sequenzen daraufhin untersucht, ob bestimmte, vom Benutzer definierte Bedingungen erfüllt sind. Wenn die definierte Bedingung erfüllt ist, können für diese Sequenzen bestimmte interessierende Informationen berechnet werden. Mit dieser Funktion können z. B. alle diejenigen Sequenzen gefiltert werden, bei denen das DE-Heizrohr ein Schädigungsgrad zwischen 30 % und 40 % aufweist und ein DEHEIRO-Versagen auftritt. Für die gefilterten Sequenzen können dann bestimmte Informationen über Prozessgrößen ermittelt werden, z. B.

- Zeitpunkt, wann DEHEIRO versagt,
- Duck und Temperatur im Heizrohr, die zum Zeitpunkt des DEHEIRO-Versagens vorliegen,
- Maximaler Druck und maximale Temperatur, die in den jeweiligen Sequenzen erreicht werden,

- Zeitdauer, wie lange z. B. ein Heizrohr-Druck > 14 MPa in den jeweiligen Sequenzen vorliegt.

Da zu jeder Sequenz die zugehörige Eintrittswahrscheinlichkeit vorliegt, können die mit der Filter-Funktion ermittelten Werte probabilistisch ausgewertet werden.

Die Funktion unter Punkt 3.3 (s. Abb. 2.18) berechnet aus den Daten der gefilterten Sequenzen die entsprechenden Verteilungsfunktionen. Über diese Funktion kann z. B. die Verteilung der Zeitpunkte berechnet werden, wann das DEHEIRO bei einem Schädigungsgrad von 30 – 40 % versagt. Entsprechend könnten zusätzlich die Verteilungen des Heizrohrdrucks oder der Heizrohrtemperatur berechnet werden, die zum Zeitpunkt des DEHEIRO-Versagens und bei einem Schädigungsgrad von 30 – 40 % vorliegen.

Analog zur Berechnung von Verteilungsfunktionen können mit der Funktion unter Punkt 3.3.1 auch entsprechende bedingte Verteilungen berechnet werden, z. B. die bedingte Verteilung der Zeitpunkte des DEHEIRO-Versagens unter der Bedingung, dass das Heizrohr versagt und das Heizrohr einen Schädigungsgrad von 30 – 40 % aufweist.

Die Verteilungen bzw. bedingten Verteilungen können pro erzeugten dynamischen Ereignisbaum, pro epistemischem Lauf der mehrere DETs mit variierenden aleatorischen Unsicherheiten enthalten kann (s. Abschnitt 3.5.1) sowie als Mischverteilung über alle erzeugten DETs berechnet werden.

Die Funktionen unter Punkt 3.4 – 3.6 beziehen sich auf die Zusammenstellung von Daten zur Erzeugung von graphischen Darstellungen.

Die Funktion unter Punkt 3.7 in Abb. 2.18 berechnet die Mittelwerte von Wahrscheinlichkeiten und Prozessgrößen pro DET und über alle DETs. Zu den berechneten Mittelwerten können die zugehörigen ein- oder zweiseitigen 90 %, 95 % und 99 % Konfidenzintervalle ermittelt werden.

Die Vielzahl der hierbei aufgeführten Funktionen können mit Hilfe des iPython Notebooks rasch in eine generische Form umgewandelt werden. Letztendlich handelt es sich dabei stets um beliebig komplexe Bedingungsabfragen an alle Sequenzen eines oder mehrerer DETs. Die Zeitreihen der zutreffenden Sequenzen können dann weiter untersucht werden. Die Umformulierung aller Funktionen passend zu diesem generischen Schema stellt den zentralen Arbeitspunkt einer flexiblen graphischen Benutzeroberfläche dar, da

alle zukünftig zu implementierenden Funktionen sich an diesem Schema orientieren werden.

2.3.3 Visualisierung der Ergebnisse

In dem erstellten iPython-Notebook wurden Funktionen zur Erstellung verschiedener graphischer Darstellungen erarbeitet. Mit diesen Funktionen wurden im Rahmen der durchgeführten Anwendungen in den Abschnitten 3 und 4 z. B. folgende grafische Darstellungen erzeugt:

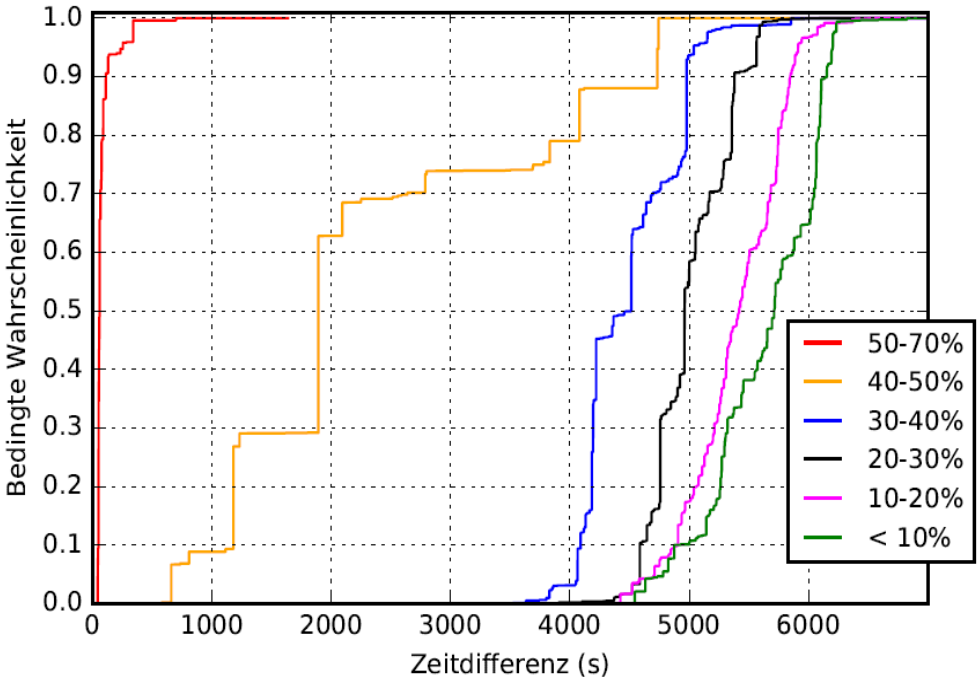


Abb. 2.19 kumulierte Verteilungsfunktionen (z. B. kumulierte Verteilungsfunktion der Zeitdifferenz zwischen Durchführung der SDE und DEHEIRO-Versagen und Versagen der HKML in Abhängigkeit des Schweregrades der DE-Heizrohr Schädigung)

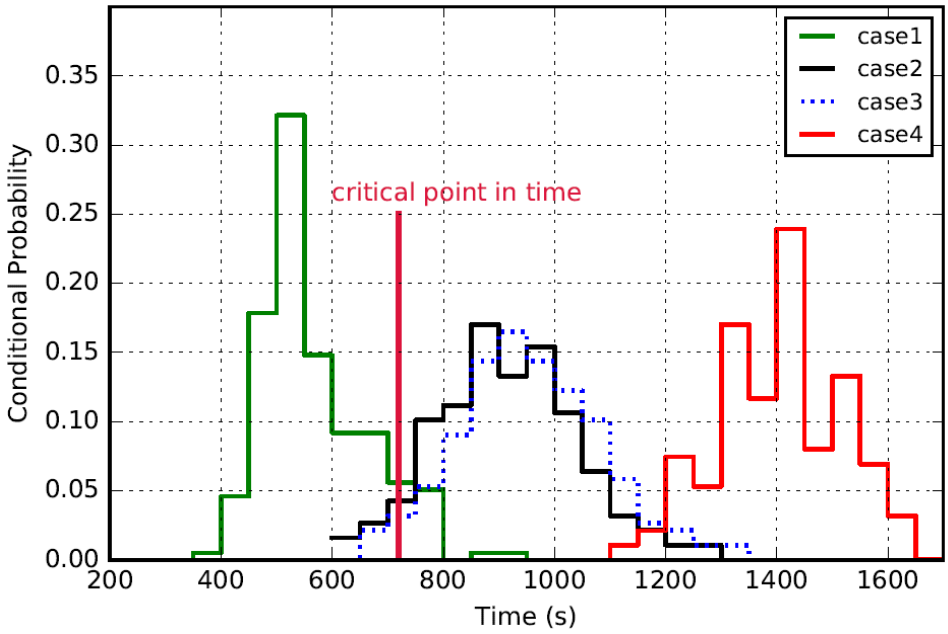


Abb. 2.20 Wahrscheinlichkeitsverteilungen, Histogramme (z. B. bedingte Wahrscheinlichkeitsverteilungen wann Ereignisse unter bestimmten Bedingungen eintreten)

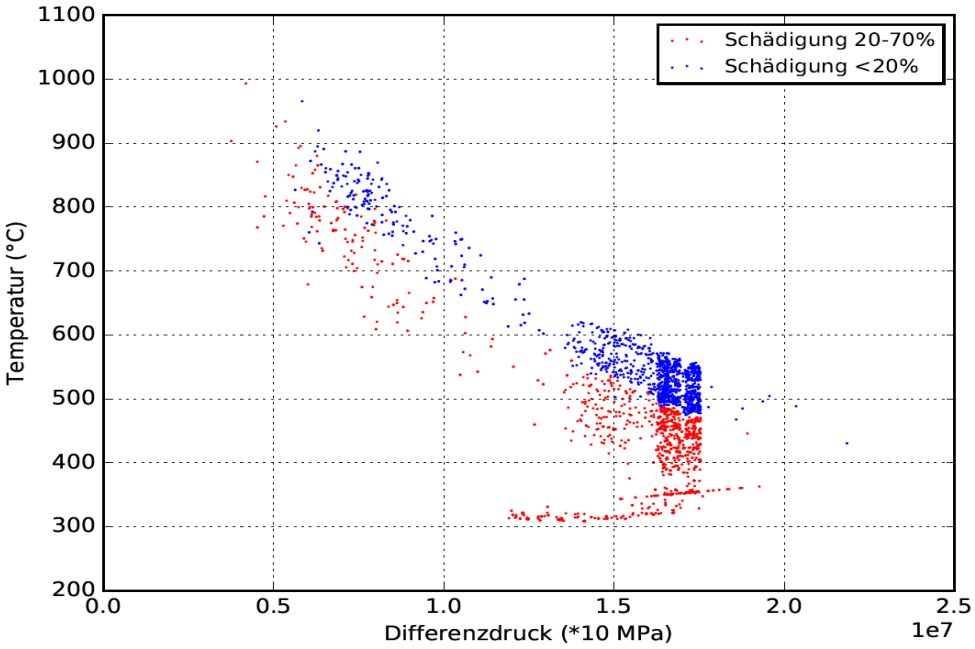


Abb. 2.21 Scatterplots (z. B. Scatterplot von Differenzdruck und Temperatur des DE-Heizrohrs in Abhängigkeit des Schädigungsgrads des DE-Heizrohrs)

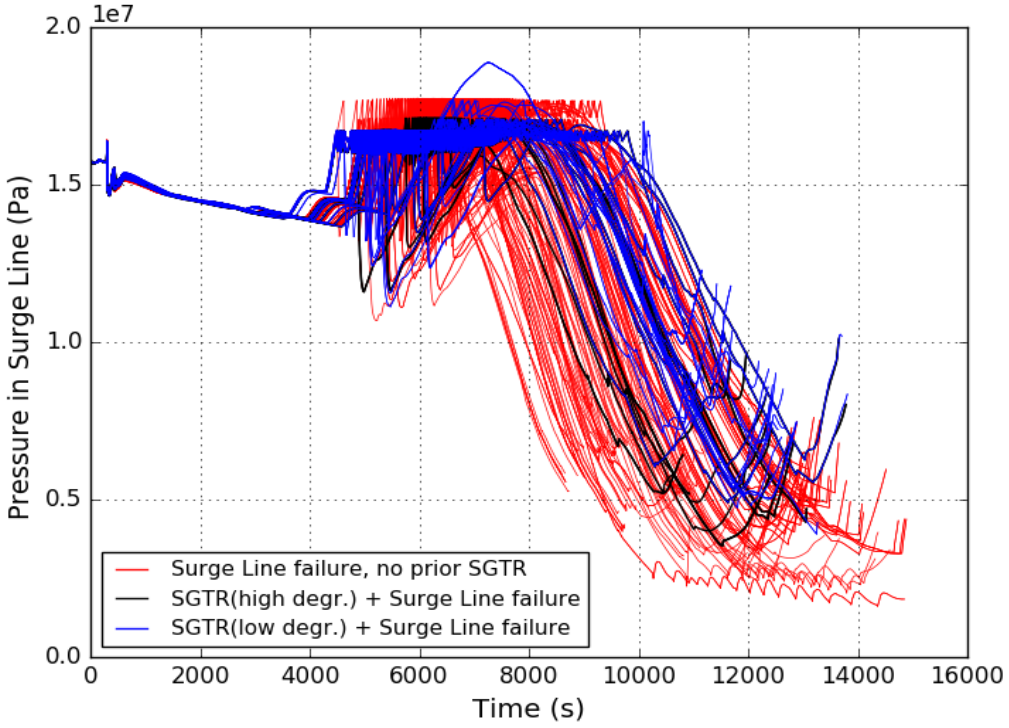


Abb. 2.22 Prozessgrößen-Verläufe bzgl. bestimmter Bedingungen (z. B. Druck in VAL für Seq. mit VAL-Versagen aber kein DEHEIRO-Versagen – rote Kurven; Druck in VAL für Seq. mit VAL-Versagen nach DEHEIRO-Versagen bei Schädigungsgrad < 20 % – blaue Kurven)

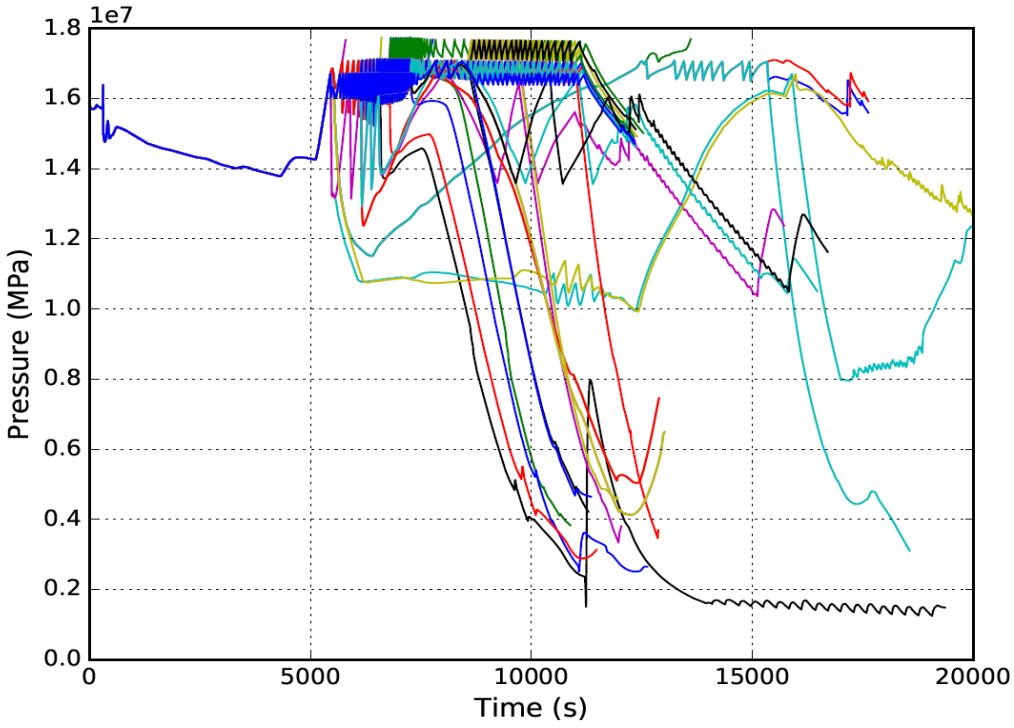


Abb. 2.23 Prozessgrößen-Verläufe innerhalb bestimmter dynamischer Ereignisbäume (z. B. Kühlmitteldruck der erzeugten Sequenzen in DET 1)

Um die Einbettung dieser erarbeiteten Visualisierungsfunktionen in eine graphische Benutzeroberfläche zu gewährleisten, wurde bei der Erstellung der Funktionen auf die Verwendung einheitlicher optionaler Argumente geachtet. Somit können die Funktionen relativ einfach über die Eingaben von Optionen (z. B. Legenden, Achsenbeschriftung, Titel etc.) einer späteren Benutzeroberfläche angesteuert werden.

2.4 Reduktion der Rechenzeit

Während mit der bisherigen MCDET-Prototypversion die einzelnen Sequenzen eines dynamischen Ereignisbaumes (DET) sequenziell nach dem ‚First In Last Out'-Prinzip berechnet wurden, werden die Sequenzen mit dem neu entwickelten MCDET-Scheduler weitestgehend parallel abgearbeitet. Mit der Neuentwicklung des Schedulers wurde auch das Probabilistik-Modul angepasst und verbessert. Mit diesen Entwicklungen werden identische Ereignisabläufe auch dann nur einmal gerechnet, wenn sie zu unterschiedlichen Ereignisbäumen gehört. Mit dieser Einsparung der Rechenläufe kann ein nicht unerheblicher Beitrag zur Verringerung der Rechenzeit verbunden sein.

Wenn z. B. in einem Unfallablauf der erste Verzweigungspunkt nach t_1 durch eine zufällige Größe erzeugt wird, dann wäre mit der bisherigen Version von MCDET für jeden erzeugten DET der Unfallablauf von t_0 bis t_1 gerechnet worden, obwohl diese Teilsequenz für jeden erzeugten DET gleich ist. Diese Situation wird in Abb. 2.24 skizziert.

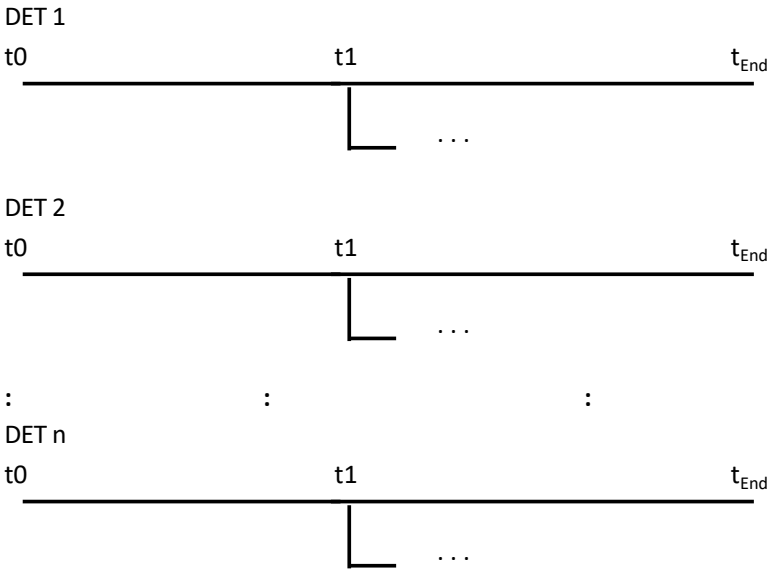


Abb. 2.24 Ablaufstruktur nach der bisherigen MCDET-Version

Abb. 2.25 zeigt die neue Ablaufstruktur von MCDET, in der die Teilsequenz von t_0 bis t_1 nur einmal gerechnet wird und die einzelnen unterschiedlichen DETs erst zum Verzweigungspunkt t_1 generiert werden. D. h., anstatt jeden Baum separat zu konstruieren wird jetzt ein einziger dynamischer Mega-Ereignisbaum erstellt, der sämtliche Ereignisbäume einer Stichprobe umfasst.

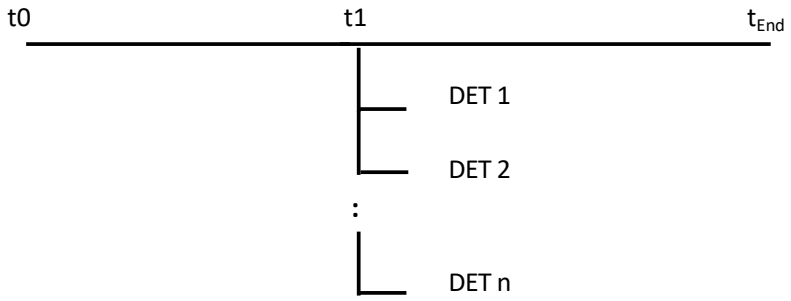


Abb. 2.25 Neue Ablaufstruktur von MCDET

Durch die Erzeugung eines Mega-Ereignisbaumes anstatt separater dynamischer Ereignisbäume wird ein weiterer Beitrag zu einem effizienten Ablauf der Simulationsläufe geleistet und erhebliche Rechenzeit eingespart, da die identischen Sequenzen in den einzelnen Ereignisbäumen nur einmal gerechnet werden. So kann mit der neuen Ablaufstruktur eine Reduktion der Rechenzeit von $(n-1)\cdot T_{CPU}$ (wobei T_{CPU} die CPU-Zeit zur Berechnung der Teilsequenz von t_0 bis t_1 beträgt) bei insgesamt n erzeugten DETs erreicht werden. Wie groß die Verringerung der Rechenzeit durch die neue Ablaufstruktur in einer Anwendung tatsächlich ist, hängt von der Anzahl der erzeugten DETs und der benötigten Rechenzeit T_{CPU} für die Teilsequenz von t_0 bis t_1 ab.

Durch die Berücksichtigung von Abbruchkriterien, die in der MCDET-Eingabedatei spezifiziert werden können, wird weitere Rechenzeit eingespart, da ein Simulationslauf vorzeitig abgebrochen wird, sobald der berechnete Systemzustand mit einem angegebenen Abbruchkriterium übereinstimmt. Die Abbruchkriterien sind dabei in Abhängigkeit der Zielsetzung für jede Anwendung separat zu definieren. Eine Einschränkung in der Anzahl der Abbruchkriterien gibt es in MCDET nicht.

In der durchgeführten MCDET/ATHLET-CD Analyse (s. Abschnitt 3) wurden beispielsweise fünf Abbruchkriterien definiert. Die Berechnung einer Sequenz wird beendet, sobald eins der folgenden Ereignisse eingetreten ist:

1. Rechenzeit > 19990 s
2. Versagen der Hauptkühlmittelleitung
3. Versagen der Volumenausgleichsleitung
4. DH-Abblaseventil und Sicherheitsventil 1 und Sicherheitsventil 2 öffnen nicht
5. DH-Absperrventil ist zu und Sicherheitsventil 1 und Sicherheitsventil 2 öffnen nicht

Die Ereignisse zu 4 und 5 wurden als Abbruchkriterien definiert, da im Rahmen der Testläufe festgestellt wurde, dass bei einem gemeinsamen geschlossenen Versagen der Druckbegrenzungsventile die Prozessbedingungen dazu führen, dass ATHLET-CD sehr lange mit extrem kleinen Zeitschritten weiter rechnet und schließlich den Rechenlauf abbricht. Obwohl in diesem Fall zwar sehr lange gerechnet wird, bringen die Rechnungen keine Zusatzinformation über das Verhalten der Sequenz. Um diesen Rechenaufwand zu vermeiden, wurden die entsprechenden absorbierenden Zustände 4 und 5 definiert. Um den Beitrag der Rechenzeitreduktion zu bestimmen muss festgestellt werden, wie viele Sequenzen solche Zustände aufweisen und wie lange es vom Eintreten des Zustands in einer Sequenz bis zum Abbruch durch ATHLET-CD dauert.

Die ursprüngliche Absicht bestand darin, dass zur Vermeidung von überflüssigen Simulationen eine Methode entwickelt werden sollte, die eine Online-Klassifizierung von Ereignisabläufen erlauben, bei denen ein Schadenszustand erwartet wird oder nicht. Ereignisabläufe ohne Schadenszustand sollten so bald wie möglich, vorzeitig abgebrochen werden. Damit wird zum einen der Rechenaufwand reduziert, wodurch eine MCDET-Analyse auch für langlaufende Rechenprogramm-Anwendungen praktikabler wird. Außerdem würde sich die Analyse mehr auf die relevanten Abläufe mit Schadenspotenzial konzentrieren können. Im Rahmen des Vorhabens RS1198 wurden bereits zwei Methoden zur Online-Klassifizierung identifiziert. Dies sind zum einen die Hidden-Markov-Methode und zum anderen ein probabilistisches Cluster-Verfahren.

Die Clusteranalyse ist ein Instrument der multivariaten Statistik, das zum Erkennen von Strukturen in einer Menge von Objekten angewendet wird. Nimmt man an, dass eine Menge von Objekten so strukturiert ist, dass sie in mehrere unterscheidbare Klassen (Cluster) zerfällt, so lassen sich diese Klassen mit Hilfe der Clusteranalyse bestimmen.

Das Ziel der Clusteranalyse zur Reduktion der Rechenzeit in einer MCDET-Analyse wäre, die Menge von Sequenzen, die in einer MCDET-Analyse berechnet werden, während ihrer Laufzeit in die beiden Cluster K_1 (Sequenz mit Schadenszustand) und K_2 (Sequenz ohne Schadenszustand) klassifizieren zu können. Die Entwicklung der Sequenzen wird durch die zufällig ausgespielten Werte der einbezogen aleatorischen und epistemische Größen bestimmt. Angenommen es wäre bekannt, welche Wertekombinationen der aleatorischen und epistemischen Größen eine Sequenz in einen Schadenzustand führen und welche nicht, so könnte eine laufende Sequenz in die Klassen K_1 oder K_2 klassifiziert werden, wenn alle Werte der aleatorischen und epistemischen Größen feststehen, die den Ablauf der Sequenz beeinflussen. Nun ist grundsätzlich die Situation gegeben, dass nur eine Stichprobe von Wertekombinationen vorliegt, anhand derer man die Klassifizierung durchführen kann. Dabei wird in der Clusteranalyse davon ausgegangen, dass Objekte bzw. in diesem Fall Sequenzen der gleichen Klasse zugeordnet werden, deren Wertekombinationen der aleatorischen und epistemischen Größen ähnlich sind. Demgegenüber wird angenommen, dass die Wertekombinationen der verschiedenen Klassen möglichst unterschiedlich sind.

Um die Wertekombinationen zu ermitteln, die eine frühzeitige Klassifikation der Sequenzen während ihrer Berechnung ermöglichen, ist eine sogenannte Lernstichprobe notwendig. Die Lernstichprobe beinhaltet eine Stichprobe von Sequenzen, bei denen sowohl die Wertekombinationen der aleatorischen und epistemischen Werte als auch der Zustand bekannt ist, welcher Klasse die jeweilige Sequenz zuzuordnen ist. Die Wahrscheinlichkeit einer fehlerhaften Zuordnung wird dabei umso kleiner, je größer die Lernstichprobe ist, anhand derer man die Klassifikation durchführt.

Im Rahmen der sequentiellen Berechnung der Sequenzen bei der Erzeugung der dynamischen Ereignisbäume, wie dies in der Prototypversion von MCDET durchgeführt wurde, würde sich die Lernstichprobe für jede berechnete Sequenz sukzessive erhöhen. Dies war eine geeignete Voraussetzung, die Qualität und Zuverlässigkeit eines gewählten Klassifikationsverfahrens zu untersuchen und zu erproben.

Durch die Entwicklung des neuen MCDET-Schedulers und der damit verbundenen parallelen Berechnungen alternativer Sequenzen für die jeweiligen Verzweigungspunkte eines dynamischen Ereignisbaumes, wurde die Ablaufstruktur zur Erzeugung der dynamischen Ereignisbäume komplett umgestellt. Damit sind jedoch auch die günstigen Voraussetzungen zur kontrollierten Erstellung einer Lernstichprobe entfallen. Wenn auch eine Lernstichprobe durch die beendeten Sequenzen erstellt werden kann, ist eine kontrollierte Klassifikation der laufenden Prozesse nur sehr schwer zu steuern. Aus diesem Grund musste die ursprüngliche geplante Idee einer Online-Klassifizierung zur frühzeitigen Einschätzung der Sequenzen aufgegeben werden. Zu Beginn des Projekts wurden diese Zusammenhänge noch nicht gesehen.

Im Laufe der Projektarbeiten und insbesondere im Rahmen der vorbereitenden Arbeiten der MCDET/ATHLET-CD Analysen wurden jedoch andere Möglichkeiten zur Reduzierung des Rechenzeitbedarfs erkannt und umgesetzt. Diese Möglichkeiten beziehen sich auf die Modellierung zur Einbindung aleatorischer Unsicherheiten in die MCDET Analyse. Diese Modellierung erfolgt in der Eingabedatei von MCDET und steuert den Ablauf bei der Erzeugung eines dynamischen Ereignisbaumes. In Abschnitt 3.4.3 wird am Beispiel der DE-Heizrohr Schädigung veranschaulicht, wie durch die Modellierung der Einbindung einer aleatorischen Größe eine Verringerung des Rechenaufwands erzielt werden kann.

3 IDPSA eines thermisch induzierten Dampferzeuger-Heizrohrversagens in einem Hochdruck-Kernschmelzunfall

Bisherige Analysen zum Dampferzeuger-Heizrohrleck (DEHEIRO-Leck) betrafen überwiegend Ereignisabläufe, bei denen das Heizrohrleck ein auslösendes Ereignis ist. Diese Analysen (z. B. in /SON 01/) zeigen, dass die Radionuklidfreisetzung bei derartigen Abläufen sehr hoch sein kann (z. B. mehr als 50 % des Kerninventars an Jod oder Cäsium). Arbeiten zu Hochdruck-Kernschmelzfällen haben sich darauf konzentriert, ob und wie eine Druckabsenkung möglich ist bzw. erfolgt, bevor der RDB unter Hochdruck versagt – sei es durch eine aktive Notfallmaßnahme, oder durch Versagen von thermisch hochbelasteten Primärkreiskomponenten. Der Risikobeitrag dieser Phänomene wurde als dominant eingeschätzt.

Neuere Erkenntnisse relativieren jedoch diese Einschätzung und führen zu dem Schluss, das Phänomen des DEHEIRO-Versagens genauer untersuchen zu müssen. Eine mittels der klassischen Ereignisbaumanalyse durchgeführten PSA der Stufe 2 für eine ausländische Anlage hat gezeigt, dass sich unter Berücksichtigung möglicher Vorschäden an Dampferzeuger-Heizrohren und Einbezug einer ungleichmäßigen Temperaturverteilung im Dampferzeuger unter Naturkonvektionsbedingungen ein hoher Risikobeitrag durch induzierte DEHEIRO-Lecks ergeben kann /LIA 09/. Wenn grundsätzlich mehr oder weniger starke Vorschädigungen nicht auszuschließen sind und lokal hohe Temperaturen im Dampferzeuger aufgrund zufälliger Einflüsse (aleatorische Unsicherheiten) auftreten können, ist der potentielle Risikobeitrag durch ein induziertes DEHEIRO-Versagen nicht ohne weiteres zu vernachlässigen.

Die Vorgehensweise der klassischen PSA ist angesichts der zahlreichen, eng miteinander verbundenen und zeitlich wechselwirkenden Phänomene nicht befriedigend, da sie viele relevante Aspekte nicht berücksichtigen kann. So führt z. B. eine stärkere Hüllrohr-Oxidation zu einer erhöhten Temperatur der aus dem RDB austretenden Gase. Dies wiederum erhöht die Temperaturbelastung sowohl der heißen Leitung, der Volumenausgleichsleitung und der Druckhalter-Ventile, als auch der Dampferzeuger-Heizrohre. Ferner ist für die Belastung der Dampferzeuger-Heizrohre der Druck auf der Sekundärseite von Bedeutung, der wiederum vom Verhalten der Frischdampf-Ventile abhängt. Für die Bewertung des Risikopotenzials ist es entscheidend, mit welcher Wahrscheinlichkeit die Dampferzeuger-Heizrohre wie lange vor den anderen Komponenten des Primärkreises versagen. Dies zu ermitteln ist mit einer klassischen Ereignisbaumanalyse und nur einer begrenzten Anzahl von Simulationen des Unfallablaufes jedoch kaum zuverlässig

möglich. Aus diesem Grund wird das thermisch induzierte DEHEIRO-Versagen als wichtiger Anwendungsfall für eine IDPSA unter Verwendung des Analysewerkzeugs MCDET betrachtet.

Grundlage für die MCDET-Analyse zum thermisch induzierten DEHEIRO-Versagen ist die Modellierung eines vollständigen Ausfalls der Wechselstromversorgung. Eine Beschreibung des zugrunde gelegten Station Black Out (SBO) Unfallszenarios und der getroffenen Annahmen, unter denen die Analyse durchgeführt wird, erfolgt in Abschnitt 3.1. Zur Simulation des Unfallablaufs wurde das in der GRS entwickelte deterministische Rechenprogramm ATHLET-CD eingesetzt. Die Arbeiten, die zur Erstellung des deterministischen Modells für eine gekoppelte MCDET/ATHLET-CD Analyse durchgeführt wurden, werden in Abschnitt 3.2 beschrieben.

In der durchzuführenden Analyse werden zahlreiche Unsicherheiten berücksichtigt, die den Unfallablauf entscheidend beeinflussen können. Diese betreffen sowohl epistemische Unsicherheiten, wie z. B. Schmelztemperatur für UO_2, Wärmekapazitäten für UO_2 und Zr oder Unsicherheiten bzgl. des Zirkonium-Oxidationsmodells, als auch aleatorische Unsicherheiten. Die in der Analyse berücksichtigten epistemischen Unsicherheiten werden in Abschnitt 3.3.1 beschrieben.

Während die Einbeziehung von epistemischen Unsicherheiten in eine deterministische Unfallablaufanalyse mittlerweile als Stand von Wissenschaft und Technik gilt und im Rahmen von ‚Best Estimate Plus Uncertainty' (BEPU) Analysen grundsätzlich durchzuführen sind, bleibt die Einbeziehung von aleatorischen Unsicherheiten in eine Unfallanalyse bisher weitestgehend unberücksichtigt. In der in diesem Projekt erstmals durchgeführten gekoppelten MCDET/ATHLET-CD Analyse wird gezeigt, dass neben epistemischen Unsicherheiten auch beliebige aleatorische Unsicherheiten in deterministischen Rechenprogrammen in Verbindung mit MCDET berücksichtigt werden können.

Im Rahmen der klassischen PSA können aleatorische Unsicherheiten aufgrund der methodischen Voraussetzungen nur sehr eingeschränkt und sehr vereinfacht modelliert werden, z. B. System bei Anforderung verfügbar ja/nein oder menschliche Handlung erfolgreich ausgeführt ja/nein. Aleatorische Unsicherheiten, die sich auf zeitliche Einflüsse oder Abhängigkeiten beziehen, konnten in probabilistischen Sicherheitsanalysen mangels geeigneter Methoden bisher nicht analysiert werden. Demzufolge mangelt es auch an Methoden und Modellen, um eine Schätzung aleatorischer Unsicherheiten zu ermöglichen, die über die in einer klassischen PSA verwendeten hinausgehen. In der in diesem

Projekt durchgeführten gekoppelten MCDET/ATHLET-CD Analyse wurden aleatorische Unsicherheiten berücksichtigt, die sich

- auf die Zeiten beziehen, wann bestimmte Handlungen im Rahmen der ‚Sekundärseitigen Druckentlastung' durchgeführt werden,
- auf das Ausfallverhalten der Druckbegrenzungsventile in Abhängigkeit ihrer Anforderungszyklen und
- auf den Grad der Schädigung, die das modellierte Heizrohr zu Beginn des Unfallablaufs hat.

Zur Schätzung der jeweiligen aleatorischen Unsicherheiten wurden Modelle hergeleitet, die den Abschnitten 3.3.2.1 – 3.3.2.3 im Einzelnen beschrieben werden.

Abschnitt 3.4 beschreibt, wie die aleatorischen Unsicherheiten in die MCDET-Analyse eingehen und berücksichtigt werden können. In diesem Zusammenhang wird gezeigt, wie die Einbindung der aleatorischen Unsicherheiten die Struktur eines dynamischen Ereignisbaumes bestimmt und wie dadurch eine Reduktion der Rechenzeit erzielt werden kann.

In Abschnitt 3.5 werden erste Ergebnisse der durchgeführten IDPSA bzgl. des thermisch induzierten DEHEIRO-Versagens unter Verwendung von MCDET/ATHLET-CD vorgestellt.

In Abschnitt 3.6 erfolgt eine ausführliche Diskussion, welchen Nutzen und Vorteil die Anwendung der Methode MCDET im Rahmen einer probabilistischen Sicherheitsanalyse erbringt.

3.1 Unfallszenario

In diesem Abschnitt erfolgt eine Beschreibung des Unfallszenarios, das der durchgeführten Analyse zugrunde liegt sowie eine Diskussion der Annahmen, die zur Durchführung der MCDET/ATHLET-CD Analyse vorausgesetzt wurden.

3.1.1 Beschreibung des SBO-Unfallszenarios

Für die Analyse wird ein Unfallablauf angenommen, der in eine Hochdrucksituation führt, in der thermisch induziertes DEHEIRO-Versagen durch den Einfluss einer hohen Druckdifferenz zwischen Primär- und Sekundärseite und durch hohe Temperaturen in den Dampferzeuger-Rohren auftreten kann. Zum Erreichen der Hochdrucksituation wird der gekoppelten MCDET/ATHLET-CD Analyse ein totaler Ausfall der Spannungsversorgung (SBO – total Station Black Out) zugrunde gelegt.

Als einleitendes Ereignis wird ein Totalausfall der batterieunabhängigen Eigenbedarfsversorgung angenommen. Dabei wird unterstellt, dass keine Versorgung aus dem Hauptnetz, durch den Turbogenerator und aus dem Fremdnetz erfolgt. Ferner wird von einem kompletten Ausfall des D1- und des D2-Notstromnetzes (d. h. der Notstrom- und Notspeisediesel) ausgegangen. Eine Wiederherstellung der Stromversorgung innerhalb der Analysezeit von 20000 s wird nicht unterstellt.

Durch den Ausfall der Eigenbedarfsversorgung werden große Verbraucher nicht mehr mit Strom versorgt. Damit laufen die Hauptkühlmittelpumpen (HKMP) aus und infolgedessen wird durch das Kriterium „2v4 HKMP < 94%“ die Reaktorschnellabschaltung eingeleitet, welche eine Turbinenschnellabschaltung nach sich zieht. Aufgrund der Unverfügbarkeit der Hauptwärmesenke erfolgt eine Verblockung der Frischdampfumleitstation (FDU). Begünstigt durch die auslaufenden HKMP stellt sich primärseitig ein Naturumlauf ein, so dass die Reaktorwärme immer noch an das Speisewasser der Dampferzeuger abgegeben werden kann.

Durch den Ausfall der Hauptwärmesenke kann der durch den sich einstellenden Naturumlauf immer noch produzierte Frischdampf sekundärseitig nicht abgeführt werden. Damit steigt der Druck in den Dampferzeugern an. Beim Anstieg des Frischdampfdruckes auf p_{FD} = 8,6 MPa öffnen die Absperrventile vor den Abblaseregelventilen. Diese öffnen ebenfalls und die Dampferzeuger werden mit dT_{FD} = 100 K/h auf p_{FD} = 7,5 MPa „teilabgefahren“ und zunächst bei diesem Druck gehalten. Die Dampferzeuger geben ohne eine Bespeisung ihr begrenztes Inventar in die Atmosphäre ab, mit der Folge, dass die Füllhöhestände aller vier DE unter 4 m sinken („4v4 DEF < 4 m“).

Die Kriterien „Eigenbedarfsversorgung nicht verfügbar“ und „4v4 DEF < 4 m“ sind gemäß Notfallhandbuch ODER-verknüpft und sehen ein sekundärseitiges Druckentlasten und Bespeisung vor. Dies beinhaltet das Aufladen des Speisewasserbehälters mit dem

Dampf aus den Dampferzeugern und das anschließende Druckentlasten der DE. Ist der Speisewasserbehälter aufgeladen, die DE druckentlastet und die Speisewasserleitungen durchgeschaltet, werden die Dampferzeuger passiv aus dem Speisewasserbehälter bespeist, solange das Druckdifferential ausreichend ist. Ferner besteht die Möglichkeit der Einspeisung über eine mobile Pumpe. Solche Maßnahmen können einen signifikanten Zeitgewinn für Reparaturmaßnahmen im Unfall ermöglichen, um die Kernkühlung mit den Notkühlsystemen wiederherzustellen.

In Abhängigkeit von dem Erfolg bzw. der Wirksamkeit des sekundärseitigen Druckentlastens und der sekundärseitigen Bespeisung kann es früher oder später zu einer Aufheizung des Primärkreises und zu einem Ansteigen des Drucks im Primärkreis kommen. Ab einem Druck von $p_{PKL} = 16{,}4$ MPa öffnet das Abblaseregelventil und Kühlmittel wird in den Abblasebehälter eingeleitet. Erreicht der Abblasebehälter einen Druck von $p_{AbbBeh} = 1{,}4$ MPa, gibt mindestens eine der vier Berstscheiben nach und Kühlmittel dringt in den Sicherheitsbehälter ein. Danach erfolgt ein Ansteigen der Druckdifferenz zwischen Sicherheitsbehälter und Reaktorgebäude. Wird eine Druckdifferenz von $\Delta p_{SHB\text{-}RG} = 3{,}0 \cdot 10^3\ \mathrm{Pa}\ (=30\ \mathrm{mbar})$ erreicht oder liegt eine Kühlmittelaustrittstemperatur von mindestens $T_{RDBaus} = 350$ °C vor, ist das Schutzziel „Primärseitiger Wärmetransport“ verletzt und laut Notfall-handbuch ist eine primärseitige Druckentlastung und eine Bespeisung des RDB vorgesehen.

Die Bespeisung des RDB ist in diesem Fall nur durch die acht Druckspeicher möglich. Nachdem das zu diesem Zeitpunkt verfügbare Inventar der Druckspeicher eingespeist wurde, setzen sich die Kernschadensmechanismen fort, so dass anschließend die Kernfreilegung und das Abschmelzen des Kerns bei geringem Druck im Primärkreislauf erfolgt. Der Druck im Sicherheitsbehälter wird dadurch weiter steigen und beim Erreichen eines Druckes von $p_{SHB} = 0{,}53$ MPa wird das SHB-Venting vorbereitet und bei $p_{SHB} = 0{,}6$ MPa (Überdrücke) gemäß Notfallhandbuch eingeleitet. Ab diesem Zeitpunkt wäre eine Radionuklidfreisetzung in die Umgebung des Kraftwerkes gegeben /SON 01/, /GRS 15/ und /GRS 17/.

3.1.2 Annahmen der Analyse

Zielsetzung dieser Analyse ist neben der Anwendung und Erprobung des neu Entwickelten MCDET-Schedulers sowie des ATHLET-CD Treiber zur Kopplung von MCDET mit ATHLET-CD auch die Gewinnung von neuen Erkenntnissen bzgl. der Bedingungen,

wann ein thermisch-induziertes DEHEIRO-Leck im Falle einer Hochdrucksituation auftritt.

Für die Untersuchungen zum induzierten Dampferzeuger-Heizrohrleck sind somit nur solche Abläufe von Interesse, die mindestens so lange einen hohen primärseitigen Druck aufweisen, bis Kernschmelzen einsetzt. Daraus folgt, dass für die Analyse diejenigen Ereignisse ausgeschlossen wurden, bei denen eine primärseitige Hochdrucksituation verhindert wird. Dabei geht es insbesondere um die Auswirkungen stochastischer Einflüsse (aleatorische Unsicherheiten), durch die eine primärseitige Hochdrucksituation ausgeschlossen wird.

Im Folgenden werden verschiedene Unsicherheitsquellen diskutiert, die sich auf das Ausfallverhalten von Komponenten, auf menschliche Handlungen bzgl. durchzuführender Notfallmaßnahmen und auf physikalische Phänomene beziehen. Im Rahmen der Diskussion werden Begründungen geliefert, warum einzelne Unsicherheiten nicht in die Analyse einbezogen werden und welche Annahmen diesbezüglich für die Analyse getroffen wurden.

Annahme zur Notfallmaßnahme ‚Primärseitige Druckentlastung'

Zielsetzung der durchzuführenden Analyse ist die Untersuchung eines DEHEIRO-Versagens in Hochdruck-Kernschmelzsituationen. Eine Hochdruck-Kernschmelzsituation wird als Voraussetzung dafür betrachtet, dass es zu einem DEHEIRO-Versagen kommen kann.

Um das Entstehen einer Hochdrucksituation im Primärkreis in Unfallsituationen zu vermeiden, ist die durch menschliche Eingriffe durchzuführende Notfallmaßnahme ‚Primärseitiges Druckentlasten' (PDE) vorgesehen. Da bei erfolgreicher Durchführung einer PDE eine Hochdruck-Kernschmelzsituation vermieden wird und damit ein DEHEIRO-Versagen ausgeschlossen ist, wirkt die Durchführung eine PDE dem eigentlichen Ziel der Untersuchung entgegen.

Für die Analyse wird somit von der Annahme ausgegangen, dass die Notfallmaßnahme PDE unterlassen wird. Durch diese Annahme soll gewährleistet werden, dass durch die in der Analyse berücksichtigten stochastischen Einflüsse überwiegend Unfallabläufe erzeugt werden, die in eine Hochdruck-Kernschmelzsituation führen und ein DEHEIRO-Versagen zur Folge haben können.

Die Durchführung einer primärseitigen Druckentlastung und Bespeisung kurz vor dem Kriechversagen eines Heizrohrs könnte ggf. ein Untersuchungsgegenstand zur Bestimmung von Karenzzeiten sein. Diese Untersuchung kann jedoch erst dann erfolgen, wenn die Zeitverteilung des Heizrohrversagens aus der in diesem Projekt durchzuführenden Analyse vorliegt. Dies wäre ein möglicher Untersuchungsgegenstand für ein Nachfolgeprojekt.

Annahme zur Notfallmaßnahme ‚Sekundärseitige Druckentlastung'

Die sekundärseitige Druckentlastung (SDE) erzeugt eine Druckdifferenz im Dampferzeuger und kann sich dadurch auf die Integrität der Dampferzeuger-Heizrohre auswirken. Um diesen Einfluss untersuchen zu können, wird die Notfallmaßnahme ‚Sekundärseitiges Druckentlasten' in der Analyse berücksichtigt. Dazu wurde ein dynamisches Modell für den Handlungsablauf zum sekundärseitigen Druckentlasten erstellt (s. Abschnitt 3.3.2.1).

Wie in Abschnitt 3.1.1 erwähnt wurde, sieht die Notfallmaßnahme SDE vor, nach der Druckentlastung der DE eine passive Bespeisung durch das Inventar des druckaufgeladenen Speisewasserbehälters und des Leitungsinventars oder eine Bespeisung durch eine mobile Pumpe durchzuführen. Eine Bespeisung der DE bewirkt eine Verzögerung im Ablauf der Kernschmelzphänomene.

Aus diesem Grund wird postuliert, dass im Rahmen der Notfallmaßnahme SDE eine Bespeisung (sowohl durch die mobile Pumpe als auch die passive Bespeisung durch das Leitungs- und Speisewasserbehälterinventar) entfällt, um möglichst schnell eine Kernschmelzsituation und damit die Randbedingung für den eigentlichen Untersuchungsgegenstand zu erhalten.

Hochsetzen des Absicherungsdrucks für die Dampferzeuger

Durch das Hochsetzen des Absicherungsdrucks für die Dampferzeuger würden die Heizrohre tendenziell entlastet werden. Damit würde sich jedoch die Wahrscheinlichkeit für das Versagen des Primärkreislaufes an anderer weniger kritischer Stelle (insbesondere in der heißen Leitung) erhöhen.

Da ein Hochsetzen des Absicherungsdrucks zum Isolieren des DE wenig Sinn macht und im Fall, dass eine SDE durchgeführt wird, technisch ggf. auch nicht möglich ist, wird diese Maßnahme für die Analyse nicht berücksichtigt.

Batterien

Zur Durchführung der in einem SBO-Unfallablauf vorgesehenen Notfallmaßnahmen, sind entsprechende Batteriekapazitäten erforderlich. Da die Analyse jedoch nur bis zu den ersten fünf Stunden nach dem einleitenden Ereignis gerechnet werden und nach Expertenangaben eine Batteriekapazität von mindestens 10 Stunden gewährleistet sein soll, wird in dieser Analyse auf eine probabilistische Modellierung von Batteriekapazitäten verzichtet. Es wird somit angenommen, dass die notwendigen Batteriekapazitäten zur Verfügung stehen.

FD-Abblase und FD-Sicherheitsventil

Beim Anstieg des Frischdampfdruckes in den Dampferzeugern werden die Frischdampfventile (FD-Abblaseventil und FD-Sicherheitsventil) zur Druckentlastung der Dampferzeuger auf der Sekundärseite angefordert. Gemäß /GRS 01/ reicht bereits eins von den acht zur Verfügung stehenden Ventilen aus, um den Druck aller vier Dampferzeuger auf den auslegungsgemäßen Wert zu senken. Außerdem wird davon ausgegangen, dass der wenig wahrscheinliche geschlossene Ausfall aller acht Ventile keine Erhöhung des Differenzdruckes zwischen Primär- und Sekundärseite zur Folge hätte, der als wichtige Einflussgröße für den Ausfall eines Heizrohrlecks angenommen wird. Aufgrund dieser Überlegungen wird in der Analyse auf die Berücksichtigung der Unsicherheit bzgl. des Ausfallverhaltens der FD-Ventile verzichtet.

Druckhalterventile zur automatischen Druckbegrenzung

Durch einen gemeinsam verursachten Ausfall (GVA) der Druckhalter (DH)-Ventile (Abblaseventil, Sicherheitsventil 1 und 2) für die Ausfallart ‚schließt nicht' würde eine Hochdrucksituation im Primärkreis verhindert. Aus diesem Grund wird angenommen, dass der 3v3-GVA der DH-Ventile für die Ausfallart ‚schließt nicht' nicht eintritt. Der 2v3-GVA der Ausfallart ‚schließt nicht' wird in der Analyse jedoch berücksichtigt, um diesbezügliche Einflüsse ggf. bewerten zu können.

Heizrohrschädigung

Für die zugrunde gelegten Annahmen zur Modellierung der Vorschädigungen von DE-Heizrohren, wurde auf Stellungnahmen des KTA 3201 Bezug genommen. Auf die daraus abgeleiteten Annahmen wird ausführlich in Abschnitt 3.3.2.3 eingegangen.

3.2 Deterministisches Modell

Zur Modellierung des SBO-Szenarios wurde der in der GRS entwickelte Code ATHLET-CD verwendet. In der Analyse werden eine Vielzahl von Unfallabläufen unter verschiedenen sich zufällig ergebenden Randbedingungen durchgeführt. Deshalb wurde ein vorhandener schnelllaufender Eingabedatensatz eines Vorkonvoi DWR ausgewählt, der an die Aufgabenstellung angepasst wurde. Da das DEHEIRO-Leck erst nach dem Schmelzen des Kerns induziert wird, musste zunächst der ATHLET-Eingabedatensatz, der nur für Rechnungen bis zum Kernschmelzen vorgesehen ist, auf die Programmversion ATHLET-CD umgestellt werden. Hierzu wurde im Wesentlichen das Kernmodell des ATHLET-Datensatzes entfernt und durch entsprechende ATHLET-CD-Modelle im Datensatz ersetzt.

Erste Rechnungen (bzw. Vergleichsrechnungen mit einem Konvoi-Datensatz) haben gezeigt, dass mit der ursprünglichen Modellierung die Temperaturen in den Dampferzeugern auch nach Kernschmelzen nicht über 360 °C ansteigen. Das heißt, dass ein thermisch induziertes Versagen von Dampferzeugerheizrohren in diesem Fall nicht berechnet wurden. Der Grund hierfür war, ist dass die Pumpenbögen mit Wasser gefüllt sind und die heißen Gase aus dem RDB nicht in den Loops und den Dampferzeugern zirkulieren können. Daher wird angenommen, dass hohe Temperaturen in den Dampferzeugerheizrohren nur bei einer auftretenden Zirkulationsströmung innerhalb der Dampferzeuger auftreten können. Dabei strömen heiße Gase durch den Dampferzeuger und gelangen von der Dampferzeuger-Austrittsseite durch andere U-Rohre wieder zurück auf die Eintrittsseite.

Dieses Verhalten kann bei einer 1-dimensionalen Modellierung, wie sie ursprünglich in ATHLET vorlag, nicht auftreten. Deshalb wurden die heißen Stränge und der Dampferzeugereintritt der Länge nach aufgeteilt, damit es für die Strömung einen Vor- und einen Rücklauf gibt. Nach der Modifikation der Modellierung haben die durchgeführten Testrechnungen die erwarteten hohen Temperaturen im Dampferzeuger-U-Rohr und in der

Surge-Line gezeigt. Z. B. steigen die Temperaturen für den Vorlauf des Dampferzeuger-U-Rohres auf über 1000 °C an. Die modifizierte Modellierung des heißen Stranges und der Dampferzeuger-U-Rohre zeigt die folgende Abb. 3.1.

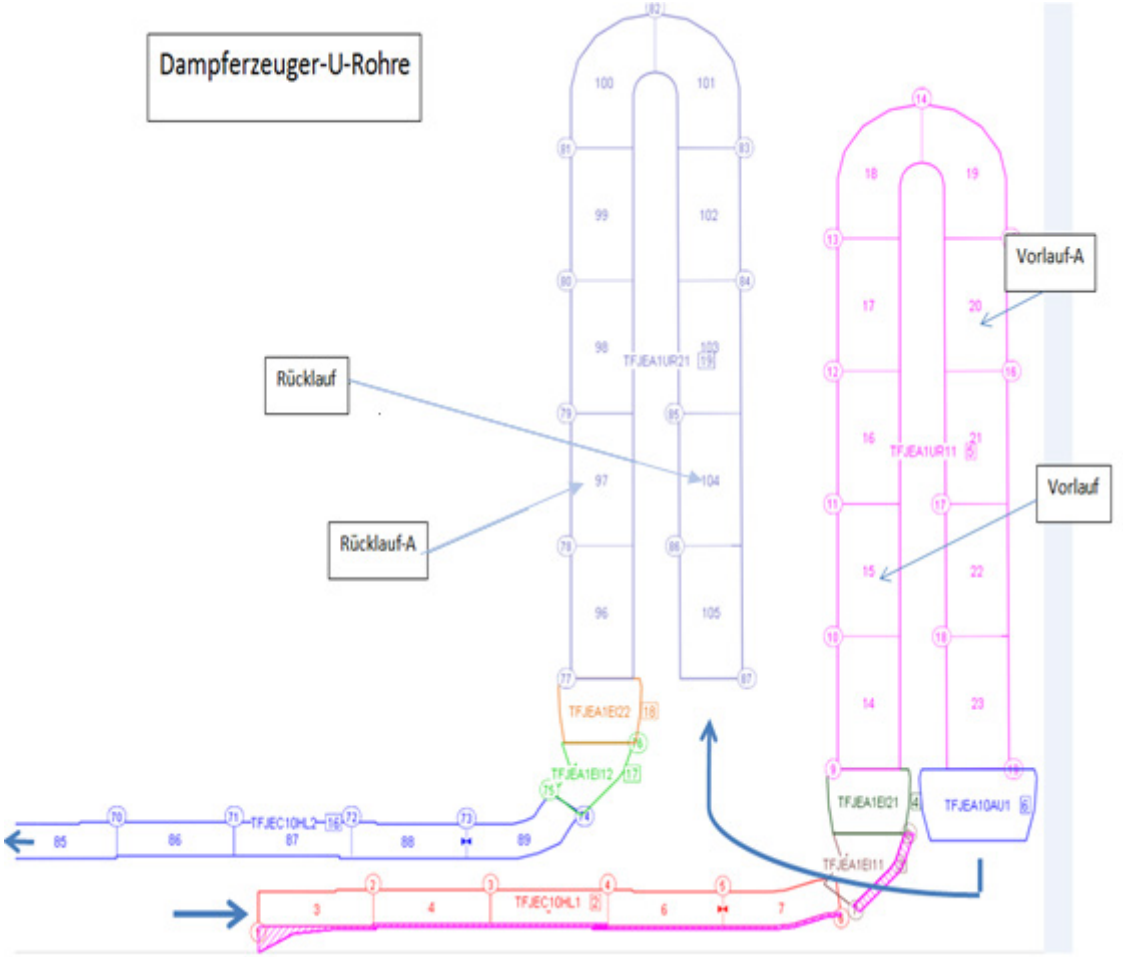


Abb. 3.1 Modellierung des Dampferzeuger-U-Rohrs

Um das Versagen der Rohrleitung durch Druck- und Temperaturbelastung im ATHLET-CD-Modell darstellen zu können, wurde das Kriechmodell nach Larson-Miller in den Datensatz integriert. Dabei wurden die für das Kriechen maßgebenden Größen: Wandschwächung sowie Druck und Temperatur im Primärkreis mit GCSM-Signalen verknüpft, über die das Versagen der jeweiligen Leitung im Anlagenmodell abgebildet wird. Damit können die Ausfallzeitpunkte der heißen Leitung, des Dampferzeuger U-Rohrs und der Volumenausgleichsleitung zum Druckhalter, wie sie nach dem Larson-Miller-Modell ermittelt werden, bei einer angenommenen Vorschädigung des Dampferzeuger U-Rohrs angezeigt werden. Das Larsson-Miller Modells ist ausführlicher in Abschnitt 3.2.1 beschrieben.

Für eine Kopplung des ATHLET-CD-Modells mit dem neuen MCDET-Scheduler musste für ATHLET-CD eine aktuellere Programmversion verwendet werden. Da auf einen Datensatz eines SBO-Szenarios aufgesetzt wurde, der für eine ältere Programmversion erstellt wurde, musste für die aktuelle Programmversion die Anordnung sowie die Struktur von GCSM-Signalen im Datensatz geändert werden.

3.2.1 Larsson-Miller Modell

Im Folgenden wird der Larsson-Miller-Parameter Ansatz kurz zusammengefasst.

Für die Kriechbruchzeit t_B [h] einer metallischen Komponente wird folgende Gleichung (3.1) verwendet:

$$t_B = 10^{\left[\frac{P_{LM}}{T} - C\right]} \tag{3.1}$$

mit P_{LM}: Larson-Miller-Parameter (LMP), T: Temperatur[K], C: Materialkonstante.

Für die Spannungsabhängigkeit des LMP wird angesetzt:

$P_{LM} = a_1 + a_2 * log(\sigma)$ (Anpassung durch Gerade) oder

$P_{LM} = a_1 + \sqrt{a_2 + a_3 * log(\sigma)}$ (Anpassung durch Parabel).

Die Parabelform ermöglicht unter Umständen eine Anpassung mit geringerem Fehler, nachteilig ist jedoch eine mögliche Beschränkung der verwendbaren Spannung, da der Wurzelausdruck negativ werden kann.

$$\sigma = \frac{\left(r_a^2 + r_i^2\right)\Delta p}{(r_a + r_i)(r_a - r_i)}$$

mit r_a: Außenradius; r_i: Innenradius; Δp: Differenzdruck

Bei Verwendung der aufgelisteten LMP müssen folgende Einheiten verwendet werden: Spannung [MPa], Zeit [h] und Temperatur [K].

Für die in diesem Projekt durchgeführte Analyse wurden folgende werkstoffspezifischen Koeffizienten für DE-Heizrohr, HKL und VAL eingesetzt:

- DE-Heizrohr (Werkstoff: Alloy800mod; Anpassung: Gerade)
  Koeffizienten: a_1 = 5.443E+04 a_2 = -1.702E+04 C = 19
- HKL (Werkstoff: 20MnMoNi55; Anpassung Parabel):
  Koeffizienten: a_1 = 1.6819E+04 a_2 = 2.5736E+08 a_3 = -9.023E+07 C = 25
- VAL (Werkstoff: X10CrNiNb189; Anpassung Parabel):
  Koeffizienten: a_1 = 1.4995E+04 a_2 = 4.3602E+08 a_3 = -1.584E+08 C = 22

Die entsprechenden Werte wurden aus Versagensflächen, die im Rahmen von zahlreichen Finite-Elemente-Berechnungen für Rohrleitungskomponenten von DWR-Anlagen der Baureihe Konvoi mit werkstoffspezifischen, experimentell bestimmten Spannungs-Dehnungs-Kurven und entsprechenden Kriechkurven berechnet wurden, abgeleitet.

Eine Schädigung des Dampferzeuger-Heizrohrs wird über eine Schwächung der Wandstärke in [%] bezogen auf die ursprüngliche Wandstärke modelliert. Hierbei wird eine Reduktion (Schwächung) der Außenwand angenommen, wodurch der äußere Durchmesser reduziert wird.

Die in der Analyse verwendeten Nominalwerte des inneren und äußeren Radius eines nicht geschädigten Heizrohrs betragen:

r_i = 0.0098 cm und r_a = 0.011 cm

Eine Schädigung von beispielsweise D = 20 % würde demzufolge eine Verringerung des äußeren Radius auf r_a‘ = 0.01076 bedeuten. Der Wert des verringerten äußeren Radius wird durch Gleichung (3.2)

$$r_a' = ri + (1-D) * (r_a - r_i) \qquad (3.2)$$

berechnet.

3.3 Probabilistische Modellierung

Eine Zielsetzung der Analyse in diesem Arbeitspunkt ist die Gewinnung von neuen Erkenntnissen bzgl. des thermisch-induzierten DEHEIRO-Versagens. Dabei geht es insbesondere um die Einbeziehung und Quantifizierung der Auswirkungen stochastischer Einflussgrößen (aleatorische Unsicherheiten), die mit den Methoden der klassischen PSA nicht ausreichend berücksichtigt werden können, z. B. Einfluss zufälliger Ausfallzeitunkte von Komponenten oder Auswirkungen von Komponentenschädigungen mit unterschiedlichen Schweregraden. Dazu wurden potentielle Einflussgrößen diskutiert, die bei einem vollständigen Ausfall der Wechselstromversorgung den Zeitpunkt und die Wahrscheinlichkeit eines induzierten Dampferzeugerheizrohrversagens wesentlich beeinflussen können. In der Analyse wird von einer Hochdrucksituation ausgegangen, da nur in diesen Fällen ein thermisch-induziertes Dampferzeuger-Heizrohrleck erwartet werden kann.

In der durchgeführten MCDET/ATHLET-CD Analyse zum DEHEIRO-Versagen wurden sowohl epistemische als auch aleatorische Unsicherheiten berücksichtigt. Die epistemischen Unsicherheiten, die in Abschnitt 3.3.1 aufgeführt sind, beziehen sich zum einen auf verschiedene Parameter des deterministischen Rechenmodells ATHLET-CD sowie auf Kenntnisstandunsicherheiten, die in den entwickelten Wahrscheinlichkeitsmodellen bzgl. des Ausfallverhaltens der DH-Ventile und der Vorschädigung des DE-Heizrohrs berücksichtigt wurden. Zur Quantifizierung der aleatorischen Unsicherheiten der als relevant eingeschätzten Einflussgrößen wurden separate Wahrscheinlichkeitsmodelle hergeleitet, die ausführlich in Abschnitt 3.3.2 erläutert werden.

3.3.1 Epistemische Unsicherheiten

Die epistemischen Unsicherheiten bzgl. des in der IDPSA verwendeten deterministischen Rechenprogramms ATHLET-CD beziehen sich auf die in Tab. 3.1 angegebenen Parametern. Die Auswahl dieser Parameter und die Bestimmung ihrer Unsicherheiten beruhen u. a. auf Erfahrungswerten aus Validierungsrechnungen und durchgeführten Unsicherheitsanalysen, wie diese bspw. in den Vorhaben SR2567 /GRS-A-3436/, RS1173 /GRS-A-3514/, RS1184 /GRS-A-3644/, 3611R01318 /GRS-A-3752/ und 3614R01306 /GRS-462/ durchgeführt wurden. Die Tabelle stellt diese Parameter einschließlich der Informationen bzw. Quellenangaben zur Definition ihrer Unsicherheit zusammen:

Tab. 3.1 Liste der berücksichtigten epistemischen Unsicherheiten

Par-Nr.	Parameter	Beschreibung	Referenzwert und Definition der Parameterunsicherheiten	Quelle / Referenz
1	t_{RESA}	Verzögerungszeit bis RESA	Referenzwert: 0.6 s; Gleichverteilung: 0.4 s – 1.2 s	GRS-A-3752
2	QTOT	Korrekturfaktor für Nachzerfallswärme	Referenzwert: 1 s; Gleichverteilung: 0.9 s – 1.1 s	Ingenieur-mäßige Abschätzung
3	OWP	Oberer Wert für FD-Druck	Referenzwert: 8,83E+06; Polygonverteilung Wert / rel. Wert 8.63E+06 0.0 8.73E+061.0 8.93E+061.0 9.03E+060.0	GRS-A-3752
4	FAS	Sollwertveränderung FD-Maximaldruck	Referenzwert: 0 Gleichverteilung: zwischen -0.15E+06 und 0.15E+06	GRS-A-3752
5	FCONTR	Kontraktionsziffer für Dampfausströmung bei FSA- und DH-Ventilen	Referenzwert: 1 s Polygonverteilung Wert / rel. Wert 6.00E-01 0.0 7.00E-011.0 9.00E-011.0 1.00E+000.0	GRS-A-3644 GRS-A-3752 GRS-462
6	FD_AVV	Darcy-Weisbach Reibungsfaktor FSA-Ventile	Referenzwert: 0,2 Polygonverteilung Wert / rel. Wert 0.0050.0 0.011.0 0.041.0 0.060.0	GRS-A-3752 GRS-462
7-9	A2VVF A3AVVF1 A3AVVF2	Korrekturfaktor für Öffnungsquerschnitt der FD-SiV (A2_VVF), DH-SiV (A3_AVV1) und DH_ABRV (A3_AVV2)	Referenzwert: 1.0 s Gleichverteilung: 0.9 s – 1.1 s	GRS-A-3752
10	WLFMUO2	Korrekturfaktor Wärmeleitfähigkeit des Brennstoffs	Referenzwert: 1.0 s Gleichverteilung: 0.88 s – 1.12 s	GRS-A-3752
11	WLFMZR	Korrekturfaktor Wärmeleitfähigkeit des Hüllrohrmaterials (Zircaloy)	Referenzwert: 1.0 s Gleichverteilung: 0.9 s – 1.1 s	Ingenieur-mäßige Abschätzung GRS-A-3514
12	WLFMZRO2	Korrekturfaktor Wärmeleitfähigkeit des oxidierten Hüllrohrmaterials (ZrO_2)	Referenzwert: 1.0 s Gleichverteilung: 0.9 s – 1.1 s	Ingenieur-mäßige Abschätzung GRS-A-3514
13, 14	CPLUO2, CPLZR	Korrekturfaktor Wärmekapazität des Brennstoffs und des Hüllrohrmaterials	Referenzwert: 1.0 s Gleichverteilung: 0.88 s – 1.12 s	GRS-A-3644, Ingenieur-mäßige Abschätzung GRS-A-3514

Par-Nr.	Parameter	Beschreibung	Referenzwert und Definition der Parameterunsicherheiten	Quelle / Referenz
15	MTLP1	Versagenskriterium der unteren Kerngittertrageplatte in Abhängigkeit von der gesamten verlagerten Masse	Referenzwert: 65000 kg Gleichverteilung: 55000 kg – 75000 kg	Ingenieurmäßige Abschätzung
16	MTLP2	Versagenskriterium der unteren Kerngittertrageplatte in Abhängigkeit der verlagerten keramischen Masse	Referenzwert: 10000 kg Gleichverteilung: 8000 kg – 12000 kg	Ingenieurmäßige Abschätzung
17	M-IDAM	Modellauswahl für das Versagen des unteren Plenums	Referenzwert: Model 1 1: ASTOR approximation 2: Larson-Miller approach 5: ASTEC rupture model Diskrete Verteilung mit gleichen Wahrscheinlichkeiten für die Modelle	Ingenieurmäßige Abschätzung
18	WSLMAX	Schmelzeverlagerungsgeschwindigkeit (metallische Schmelze)	Referenzwert: 0.075 Gleichverteilung: 0.001 – 0.1	Ingenieurmäßige Abschätzung GRS-A-3514
19	WSLUO	Schmelzeverlagerungsgeschwindigkeit (keramische Schmelze)	Referenzwert: 0.014 Gleichverteilung: 0.001 – 0.1	Ingenieurmäßige Abschätzung GRS-A-3514
20	IOXMOD (ZrOxModell)	Modellauswahl für Zr-Oxidationsmodell	Referenzwert: 16 16: Cathcart-Urbanic / Heidricks-Modell 15: Cathcart-Prater / Courtright-Modell 19: Leistikow-Prater / Courtright-Modell Diskrete Verteilung mit gleichen Wahrscheinlichkeiten für die Modelle	Ingenieurmäßige Abschätzung GRS-A-3514
21	TCOMPM	Schmelztemperatur Urandioxid	Referenzwert: 2600 K Gleichverteilung: 2400 K – 2800 K	Ingenieurmäßige Abschätzung GRS-A-3514
22	TAM	Schmelztemperatur von metallischem Zirkaloy	Referenzwert: 2000 K Gleichverteilung: 1900 K – 2100 K	Ingenieurmäßige Abschätzung

In die in den Abschnitten 3.3.2.2 und 3.3.2.3 hergeleiteten Wahrscheinlichkeitsmodellen gehen sowohl aleatorische als auch epistemische Unsicherheiten ein. Die epistemischen Unsicherheiten zum Wahrscheinlichkeitsmodell bzgl. des Ausfallverhaltens der Druckbegrenzungsventile sind in Abschnitt 3.3.2.2 erläutert.

Die epistemischen Unsicherheiten bzgl. des Modells zur Schätzung der Verteilung des Schädigungsgrades, den das Heizrohr zu Beginn des Unfallablaufs aufweist (siehe Abschnitt 3.3.2.3, beziehen sich auf die Übergangswahrscheinlichkeiten, die in die Matrix der Gleichung (3.6) eingehen. Die epistemischen Unsicherheiten der Übergangswahrscheinlichkeiten sind in Tab. 3.9 in Abschnitt 3.3.2.3 angegeben.

3.3.2 Aleatorische Unsicherheiten

In den Abschnitten 3.3.2.1 – 3.3.2.3 werden die hergeleiteten Wahrscheinlichkeitsmodelle beschrieben, die zur Quantifizierung der in der Analyse zu berücksichtigten aleatorischen Unsicherheiten eingesetzt werden.

Dabei soll insbesondere gezeigt werden, dass die Entwicklung probabilistischer Modelle nützlich sein kann, um aleatorische Unsicherheiten quantifizieren zu können die ansonsten – wenn überhaupt – nur sehr schwer abzuschätzen sind. Zum anderen soll deutlich werden, dass aleatorische Unsicherheiten wesentlich umfassender und in einem höheren Detaillierungsgrad in eine IDPSA eingebunden werden können, als dies in einer klassischen PSA möglich ist.

3.3.2.1 Modell zur Schätzung von Zeitverteilungen relevanter Handlungen bzgl. der Notfallprozedur ‚Sekundärseitiges Druckentlasten

Die vorgesehenen Notfallmaßnahmen in einem SBO-Unfallablauf sind das „Primärseitige Druckentlasten (PDE) und Bespeisen“ sowie das „Sekundärseitige Druckentlasten (SDE) und Bespeisen“. Die für die Analyse getroffenen Annahmen zu PDE und SDE wurden bereits in Abschnitt 3.1.2 erläutert.

Die sekundärseitige Druckentlastung erzeugt eine Druckdifferenz im Dampferzeuger und kann sich dadurch auf die Integrität der Dampferzeuger-Heizrohre auswirken. Um diesen Einfluss in der Analyse untersuchen zu können, wurde ein dynamisches Modell für den Handlungsablauf zum sekundärseitigen Druckentlasten erstellt. Dieses dynamische Handlungsmodell wird mit dem Crew-Modul von MCDET simuliert, um Wahrscheinlichkeitsverteilungen der Ausführungszeiten relevanter Handlungen berechnen zu können. Da die Notfallmaßnahme SDE sehr umfangreich ist, wird der grobe Ablauf in Abb. 3.2 dargestellt. In der Tab. 3.2 werden die wesentlichen Tätigkeitsblöcke grob beschrieben, die in Abb. 3.2 in den Rechtecken durch Abkürzungen gekennzeichnet sind.

Die Rauten beschreiben die Abhängigkeiten des Handlungsablaufs von System- und Prozesszuständen.

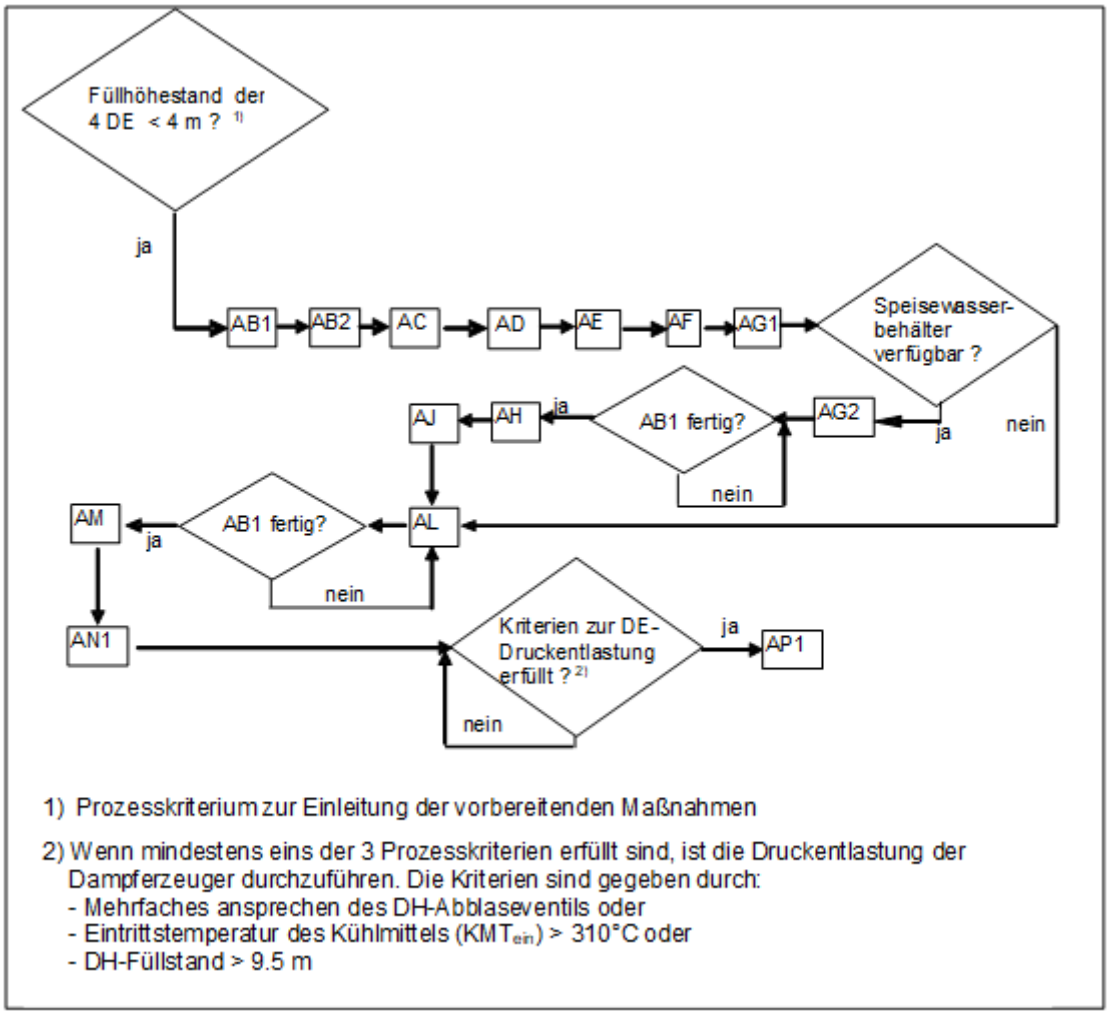


Abb. 3.2 Flussdiagramm zur Notfallmaßnahme SDE

Tab. 3.2 Beschreibung der Tätigkeitsblöcke der Notfallmaßnahme SDE

Bez.	Beschreibung
AB1	Simulationen im Reaktorschutzsystem (wird im Notspeisegebäude durchgeführt).
AB2	Herstellung der Stromversorgung der Bleed-Schiene, um im Anforderungsfall die Steuerung von Armaturen (FD-ARV, Notspeiseabsperrventile) zu ermöglichen.
AC	Installation der mobilen Pumpe (wird im Notspeisegebäude durchgeführt).
AD	Besetzung des Maschinenhauses, um Verfügbarkeit des Speisewasser (Spw)-Behälters zu überprüfen. Dient zur eventuellen Nutzung des Spw-Behälterinventars zur DE-Bespeisung.
AE	Anschlussleitungen an den Primärkreis und DE auf Leckagen überprüfen.
AF	Fortlaufende Kontrolle des Anlagenzustands.
AG1	Schließen der Anwärmventile der Speisewasser-Pumpen. Dient zur Nutzung des Leitungsinventars zur Einspeisung in den DE.

Bez.	Beschreibung
AG2	Isolieren des Speisewasserbehälters.
AH	Druckaufladung des Speisewasserbehälters.
AJ	Blockieren der Stützdampf-Schnellschlussventile am Spw-Behälter um den hohen Druck im Spw-Behälter auch während der nachfolgenden Druckentlastung zu erhalten.
AL	Spw-Leitungen durchschalten, um die DE-Bespeisung mit dem Leitungs- und Spw-Behälterinventar zu ermöglichen.
AM	Durchschalten der Notspeisestränge, um die Bespeisung mit der mobilen Pumpe zu ermöglichen.
AN1	Starten der mobilen Pumpe, um DE-Bespeisung ohne Verzögerung zu ermöglichen.
AP1	Druckentlasten der DE über Frischdampf-Abblaseregelventil (FD-ARV). Wenn FD-ARV nicht öffnet erfolgt als redundante Maßnahme die DE-Druckentlastung über das FD-Sicherheitsventil (FD-SiV).

Da in der Analyse ein totaler Spannungsausfall unterstellt wird, bezieht sich der Handlungsablauf auf die Situation, dass die Stromversorgung in der Anlage nicht verfügbar ist. Um in der Analyse möglichst schnell in eine Hochdruck-Kernschmelzsituation zu kommen, wird postuliert, dass eine Bespeisung (sowohl durch die mobile Pumpe als auch die passive Bespeisung durch das Leitungs- und Speisewasserbehälterinventar) der Dampferzeuger entfällt.

Wie aus Abb. 3.2 und Tab. 3.2 deutlich wird, beziehen sich die meisten Tätigkeitsblöcke der Notfallmaßnahme darauf, eine Bespeisung der DE durch die mobile Pumpe sowie die Nutzung des Inventars der Spw-Leitungen und des Spw-Behälters zu ermöglichen. Da in der Analyse eine Bespeisung der DE entfällt, müssen für die Analyse nur die aleatorischen Unsicherheiten derjenigen Tätigkeitsblöcke ermittelt werden, die entweder Einfluss auf den physikalischen Prozess haben (Tätigkeitsblock AP1) oder Einfluss darauf haben, wann die Druckentlastung der DE durchgeführt werden kann, wenn die Prozesskriterien vorliegen. Dies betrifft die Tätigkeitsblöcke AB1 und AB2.

Der skizzierte Ablauf der Handlungsblöcke in Abb. 3.2 ist vereinfacht dargestellt, weil zum einen der Eindruck vermittelt wird, als würden die Tätigkeiten sequentiell ablaufen und zum anderen die Tätigkeitsblöcke selber komplex sind und zeitliche Wechselwirkungen sowie Unsicherheiten enthalten. Z. B. können einige der Tätigkeiten zeitlich parallel ablaufen, während bestimmte Tätigkeiten erst dann beginnen können, wenn andere Arbeiten abgeschlossen sind.

Die für die Analyse relevanten Tätigkeitblöcke AB1, AB2 und AP1 wurden deshalb unter Verwendung des Crew Moduls genauer modelliert und simuliert. Aus den Ergebnissen

der Simulationen wurden schließlich die Wahrscheinlichkeitsverteilungen bzgl. der Ausführungszeiten der jeweiligen Handlungen ermittelt, die als aleatorische Unsicherheiten in die MCDET/ATHLET-CD eingebunden werden.

AB1 – Simulationsarbeiten am Reaktorschutz

Die Auslegung der Anlage sieht vor, die Dampferzeuger durch automatische Aktionen des Reaktorschutzsystems abzusperren, sobald deren Drücke bei Störungen und Störfällen so stark abnehmen, dass bestimmte Kriterien erfüllt sind. Diese automatischen Aktionen würden die erforderliche Druckentlastung der Dampferzeuger verhindern. Deshalb muss ein Schichtmitarbeiter für elektrotechnische Aufgaben im Notspeisegebäude möglichst frühzeitig und zügig Eingriffe in den entsprechenden leittechnischen Einrichtungen des Reaktorschutzsystems ausführen, um die Auslösung dieser automatischen Aktionen zu verhindern. Ein Misserfolg würde das Scheitern der gesamten Notfallmaßnahme nach sich ziehen. Da es sich bei der Notfallmaßnahme SDE um ein regelbasiertes Vorgehen handelt, wird für die Analyse angenommen, dass die Simulationsarbeiten am Reaktorschutzsystem ohne Fehler durchgeführt werden. Die Unsicherheit besteht allerdings noch darin, wann der jeweilige Schichtarbeiter mit den Simulationsarbeiten am Reaktorschutz fertig ist. Dieser Zeitpunkt unterliegt zufälligen Variation und ist eine aleatorische Größe, die Einfluss darauf haben kann, wann die Arbeiten zur DE-Druckentlastung (AP1) beginnen können.

Die zwischen den Tätigkeitsblöcken AB1 und AP1 bestehende zeitliche Wechselwirkung ist in Abb. 3.3 skizziert.

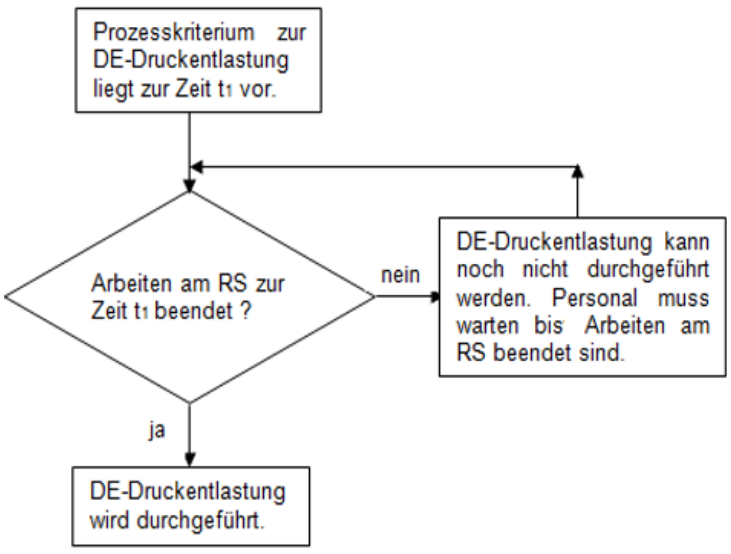


Abb. 3.3 Zeitliche Wechselwirkung zwischen Tätigkeitblöcken AB1 und AP1

Abb. 3.3 zeigt, dass die Fertigstellung der Simulationsarbeiten am Reaktorschutz eine notwendige Bedingung zur Durchführung der Druckentlastung der DE ist. D. h., wenn die Prozesskriterien zur DE-Druckentlastung zu einem Zeitpunkt t_1 vorliegen, die Simulationsarbeiten am Reaktorschutz zu diesem Zeitpunkt jedoch noch nicht beendet sind, dann kann die Druckentlastung der DE noch nicht durchgeführt werden. In diesem Fall muss das Personal so lange warten, bis die Arbeiten am Reaktorschutzsystem beendet sind. Erst dann können die DE druckentlastet werden.

Um die zeitliche Abhängigkeit zwischen dem Vorliegen von Prozesskriterien und der Beendigung der Tätigkeiten in AB1 in der Analyse möglichst realistisch berücksichtigen zu können, muss die Zeit berechnet werden, wie lange das Personal für die Beendigung der Simulationsarbeiten am Reaktorschutz benötigt. Da diese Zeit von verschiedenen zufälligen Einflussfaktoren abhängt (z. B. zufällig variierende Ausführungszeiten von einzelnen Handlungen aus denen sich der komplexe Ablauf zusammensetzt oder Verzögerungen, die sich durch zufällige Systembedingungen oder Prozesszuständen ergeben), ist diese Zeit ebenfalls einer mehr oder weniger großen Variationen unterworfen. Die zeitliche Variation, wann die Simulationsarbeiten am RS beendet sind, ist eine aleatorische Unsicherheit, die durch eine Wahrscheinlichkeitsverteilung beschrieben wird. Zur Schätzung dieser Wahrscheinlichkeitsverteilung wird das Crew-Modul in Verbindung mit MCDET eingesetzt.

AB2 – Stromversorgung der Bleed-Schiene herstellen

Die Herstellung der unterbrechungslosen Spannungsversorgung der SDE/PDE-Schiene dient dazu, um im Anforderungsfall die Ansteuerung des FD-ARV bzw. FD-SiV zum Druckentlasten der DE zu ermöglichen. Die Durchführung der Druckentlastung der Dampferzeuger über das Auffahren des FD-Abblaseventils (Tätigkeitsblock AP1) hängt somit vom Erfolg der Stromversorgung der Bleed-Schiene ab.

Als stochastische Einflussgrößen sollen sowohl menschliche Fehler als auch die Möglichkeit berücksichtigt werden, dass es aufgrund technischer Probleme zu Verzögerungen bei der Umschaltung kommen kann. Bzgl. der menschlichen Fehler handelt es sich um die Situation, dass der Schichtleiter Stellvertreter (SLVM) vergisst, dem Elektriker die Anweisung zur Herstellung der Bleed-Schiene zu geben. Als Recovery-Maßnahme wird berücksichtigt, dass der SLVM die Auslassung innerhalb einer gewissen Verzögerungszeit selbst erkennt, oder die Auslassung durch den SL bei der Rücknahme des Kommandos (nachdem er die Aufgabe der Organisation des Krisenstabs beendet hat) mit

einer gewissen Wahrscheinlichkeit bemerkt wird. Wenn die Auslassung der Anweisung nicht bemerkt wird, hat dies zur Folge, dass die Stromversorgung der Bleed-Schiene nicht hergestellt wird und damit die FD-Ventile zur DE-Druckentlastung nicht angesteuert werden können. Im Handlungsablauf haben die stochastischen Einflüsse die in Abb. 3.4 dargestellten Verzweigungen zur Folge.

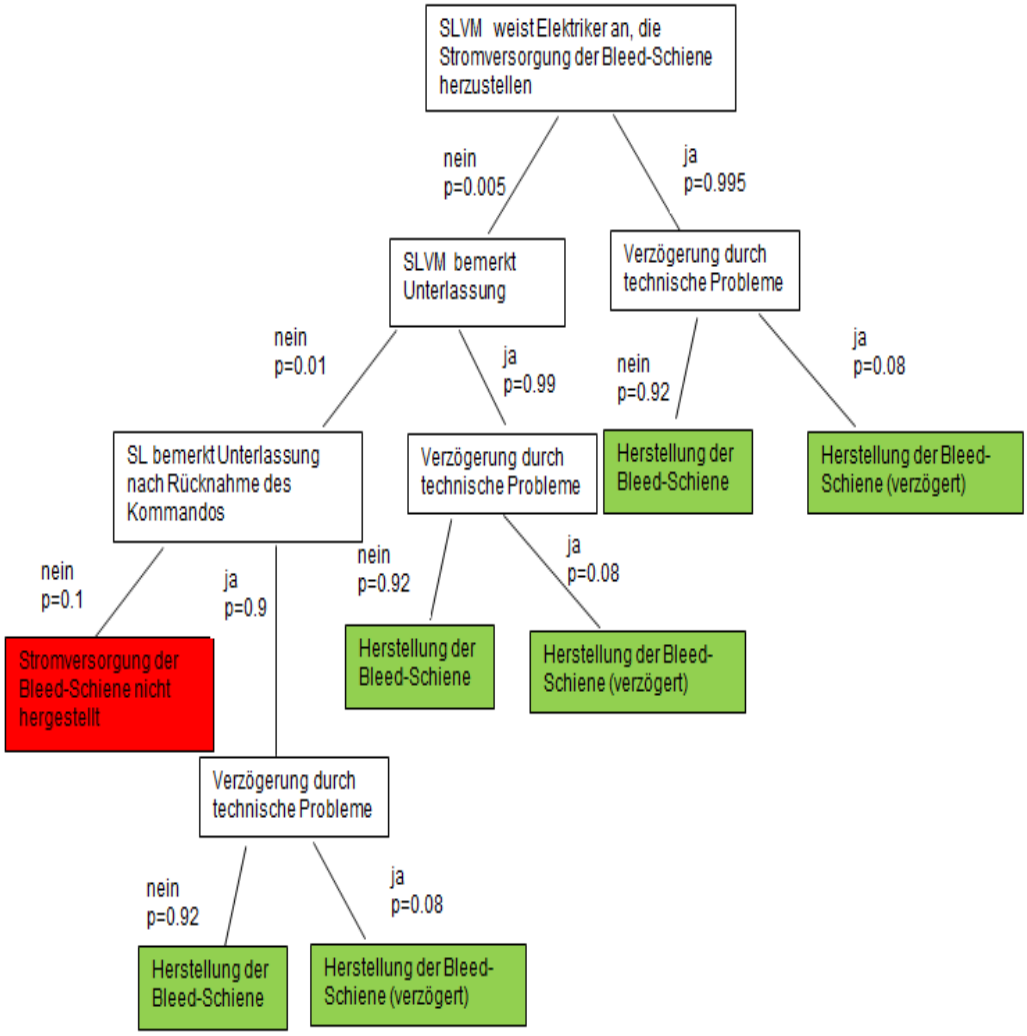


Abb. 3.4 Unsicherheiten im Handlungsablauf bzgl. der Erstellung der Stromversorgung der Bleed-Schiene

Um den Einfluss der SDE und der damit verbundenen Erhöhung der Druckdifferenz zu bewerten, wird für die DEHEIRO-Analyse angenommen, dass die Stromversorgung der Bleed-Schiene hergestellt werden kann. Der in Abb. 3.4 gekennzeichnete rote Zweig, in der die Stromversorgung der Bleed-Schiene nicht hergestellt wird und demzufolge die FD-Ventile zur DE-Druckentlastung nicht geöffnet werden, wird in der MCDET/ATHLET-CD Analyse nicht berücksichtigt.

AP1 – Druckentlastung der Dampferzeuger

Es wird angenommen, dass das Personal die Druckentlastung der Dampferzeuger ohne Fehler durchführt, wenn die entsprechenden Kriterien durch den Prozess gegeben sind. Diese Annahme erscheint gerechtfertigt, da die Druckentlastung der DE das wesentliche Ziel der eingeleiteten Notfallmaßnahme ist und die an der Notfallmaßnahme beteiligten Personen sich auf die Erreichung dieses Ziel konzentrieren. Damit wird auch die geringe Wahrscheinlichkeit in Abb. 3.4 begründet, dass die Unterlassung des SLVM zur Stromversorgung der Bleed-Schiene nicht erkannt wird.

Aufgrund der redundanten Auslegung der DE und der FD-Ventile sowie der Tatsache, dass für die DE-Druckentlastung nur eines der FD-Ventile öffnen muss, wird angenommen, dass nicht alle acht FD-Ventile aufgrund technischen Versagens ausfallen und somit eine Druckentlastung der DE zu dem Zeitpunkt stattfindet, wenn die entsprechenden Handlungen vom Personal durchgeführt worden.

Für den Handlungsablauf zum sekundärseitigen Druckentlasten wurde ein dynamisches Modell unter Verwendung der grafischen Oberfläche des Mind-Mapping Tools ‚FreeMind' erstellt. Aus dem erstellten Handlungsmodell in der grafischen Oberfläche wurde automatisch der Eingabedatensatz für das Crew-Modul erstellt. Der modellierte Handlungsablauf wurde unter Verwendung des Crew-Moduls simuliert und aus den Simulationsergebnissen eine Verteilungsfunktion der Ausführungszeiten für die jeweiligen Maßnahmen berechnet. Im Einzelnen sind das die Verteilungen der Zeit

- wann die Simulationsarbeiten am Reaktorschutz beendet sind (AB1),
- wann die Stromversorgung der Bleed-Schiene hergestellt ist (AB2) und
- wann die Ventile zur Druckentlastung der Dampferzeuger nach dem Anstehen der Prozesskriterien geöffnet werden (AP1).

Die Bezugszeit t=0 ist dabei die Zeit, wann die Einleitung der Maßnahme durch das Vorliegen der Prozesskriterien initiiert wird.

In Abb. 3.5 und Abb. 3.6 sind die Verteilungen für die Ausführungszeiten der jeweiligen Maßnahmen AB1, AB2 und AP1 grafisch dargestellt.

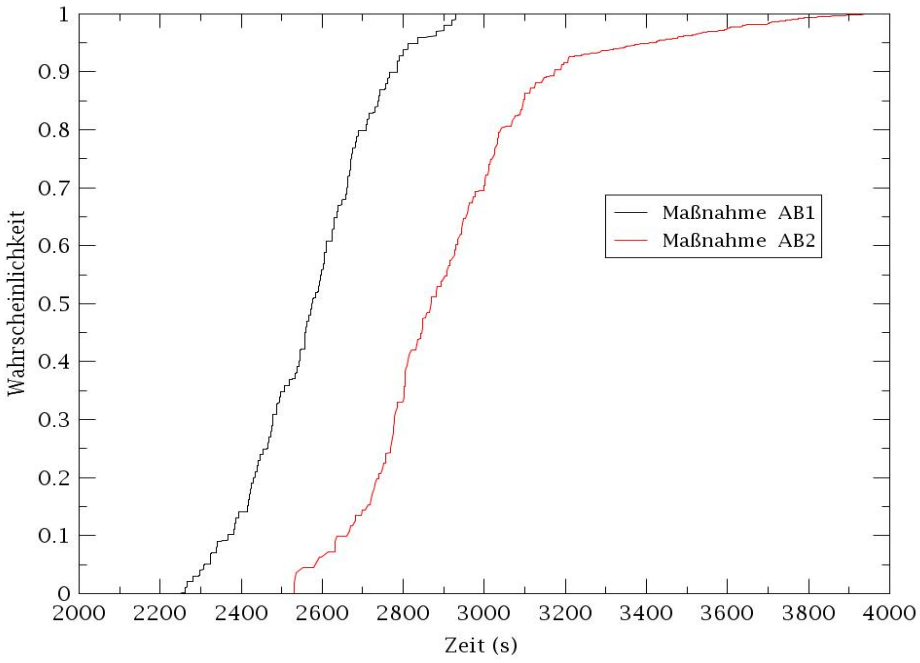


Abb. 3.5 Verteilung der Ausführungszeiten zu den Maßnahmen AB1 und AB2

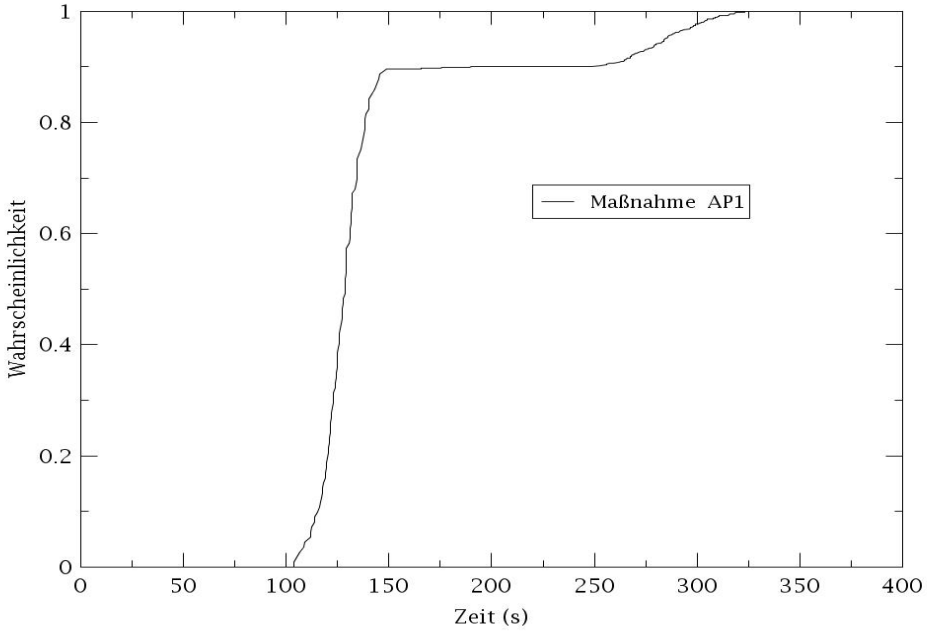


Abb. 3.6 Verteilung der Ausführungszeiten zur Maßnahme AP1

Aus Abb. 3.5 und Abb. 3.6 erkennt man, dass die Ausführungszeiten der Maßnahme AP1 deutlich geringer sind als die der Maßnahmen AB1 und AB2. Der Grund liegt darin, dass die Handlungen zur Ausführung des Tätigkeitsblockes AP1 erst beginnen können,

wenn durch den Prozess bestimmte Kriterien erfüllt sind und die Maßnahmen AB1 und AB2 erfolgreich durchgeführt wurden. Um die Ausführungszeiten der Maßnahme AP1 zu ermitteln, wurden die Handlungen zu AP1 unter der Annahme simuliert, dass die Prozesskriterien vorliegen. Dies wird dann als der Startzeitpunkt t=0 betrachtet, zu dem die Handlungen bzgl. des Tätigkeitsblockes AP1 beginnen.

Im Folgenden soll noch kurz auf die Berücksichtigung der Abhängigkeit zwischen den Ausführungszeiten verschiedener Handlungsmaßnahmen eingegangen werden. Die Abb. 3.5 und Abb. 3.6 zeigen die Verteilungen der Ausführungszeiten, die sich unabhängig für die Maßnahmen AB1, AB2 und AP1 ergeben. D. h., die Verteilungen wurden hier so dargestellt, als ob die Ausführungszeiten der einzelnen Maßnahmen voneinander unabhängig sind. Diese Unabhängigkeitsannahme in der Ausführung verschiedener Tätigkeitsblöcke ist in der Realität oftmals nicht haltbar. Der Grund besteht darin, dass die Ausführung einer Maßnahme oftmals stark mit der Ausführung einer anderen Maßnahme korreliert ist. Beispielsweise, wenn der Beginn einer Handlungsmaßnahme von der Durchführung einer anderen Maßnahme abhängt. Diese Abhängigkeitsstruktur würde nicht berücksichtigt, wenn man unabhängige Stichproben aus den jeweiligen Verteilungen der Abb. 3.5 und Abb. 3.6 ziehen würde.

Das Crew-Modul wurde im Rahmen des Vorhabens so weiterentwickelt, dass die Abhängigkeitsstruktur zwischen verschiedenen Handlungen bzw. Tätigkeitsblöcken berücksichtigt werden kann. Dazu wird aus den Simulationsergebnissen des Crew-Moduls eine empirische multivariate Verteilung erzeugt, indem für eine Maßnahme die Verteilungsfunktion der Ausführungszeiten berechnet wird, wobei jedem Zeitpunkt der Verteilung die Zeiten der anderen Handlungen aus der jeweils berechneten Sequenz zugeordnet werden. Dies ist möglich, da durch das Crew-Modul für jede Sequenz in einem erzeugten DET die Ausführungszeiten aller als relevant gekennzeichneten Handlungen berechnet werden und mit der zugehörigen Pfadwahrscheinlichkeit gespeichert werden. Die Methodik zur Erzeugung der multivariaten Stichprobe der Ausführungszeiten von Handlungen wurde in einer entsprechenden Programmroutine implementiert.

Zur Veranschaulichung wird angenommen, dass beispielsweise die Zeiten von k Handlungen ermittelt werden. Ein Stichprobenwert liefert somit ein k-Tupel von Ausführungszeiten. Die Werte eines k-Tupels beziehen sich auf die Ausführungszeiten der k Handlungen, die jeweils für einen Simulationslauf (Sequenz) des Crew-Moduls ermittelt wurden. Dadurch wird die Abhängigkeit zwischen den jeweiligen Handlungen

berücksichtigt. Eine Stichprobe vom Umfang n unter Berücksichtigung der Abhängigkeitsstruktur zwischen den Handlungen liefert damit eine Matrix

$$\mathbf{S} = \begin{pmatrix} t_{1,1} & \cdots & t_{1,k} \\ & \vdots & \\ t_{n,1} & \cdots & t_{n,k} \end{pmatrix}$$

wobei die i-te Zeile den i-ten zufälligen Stichprobenwert kennzeichnet (i=1,…,n), in dem die jeweiligen Zeiten für die k Maßnahmen enthalten sind. Eine Zufallsstichprobe der Zeiten, die aus den unabhängig berechneten Verteilungen der k Handlungen gezogen wird, würde zu einer Verzerrung der Ausführungszeitpunkte der Handlungen in der Stichprobe führen. Die ausgespielten Stichprobenwerte der multivariaten Verteilung werden als aleatorische Unsicherheiten für die Ausführungszeitpunkte der entsprechenden Handlungen in MCDET spezifiziert und können somit in die Analyse unter Berücksichtigung der Abhängigkeitsstruktur zwischen den Handlungen eingebunden werden.

Die Abhängigkeit der Ausführungszeiten der Tätigkeitsblöcke AB1 und AB2 ist in Abb. 3.7 dargestellt. Abb. 3.7 zeigt die Zeit, die für die Ausführung der Tätigkeit AB1 benötigt wurde, sowie den zeitlichen Abstand zwischen der Ausführungszeit von AB1 und AB2. Daraus ist ersichtlich, dass mit zunehmender Ausführungszeit von AB1 die Zeitdifferenz zur Ausführung von AB2 geringer wird. D. h., je länger es dauert AB1 auszuführen, desto kürzer ist der zeitliche Abstand, mit dem die Tätigkeit AB2 ausgeführt wird. Bei Ausführungszeiten von AB1 > 2600 s treten häufiger Fälle auf, in denen AB2 vor AB1 ausgeführt wurde.

Dieses Beispiel dient lediglich zur Veranschaulichung, dass Ausführungszeiten von Tätigkeiten Abhängigkeiten aufweisen können. In diesem Fall sollten die Verteilungen der Ausführungszeiten nicht unabhängig voneinander betrachtet werden, da dies zu verzerrten Zeiten führt, wann die Tätigkeiten ausgeführt werden. Das Crew-Modul wurde weiterentwickelt, um Abhängigkeiten bei der Bestimmung der aleatorischen Unsicherheiten der Ausführungszeiten von Tätigkeiten zu berücksichtigen.

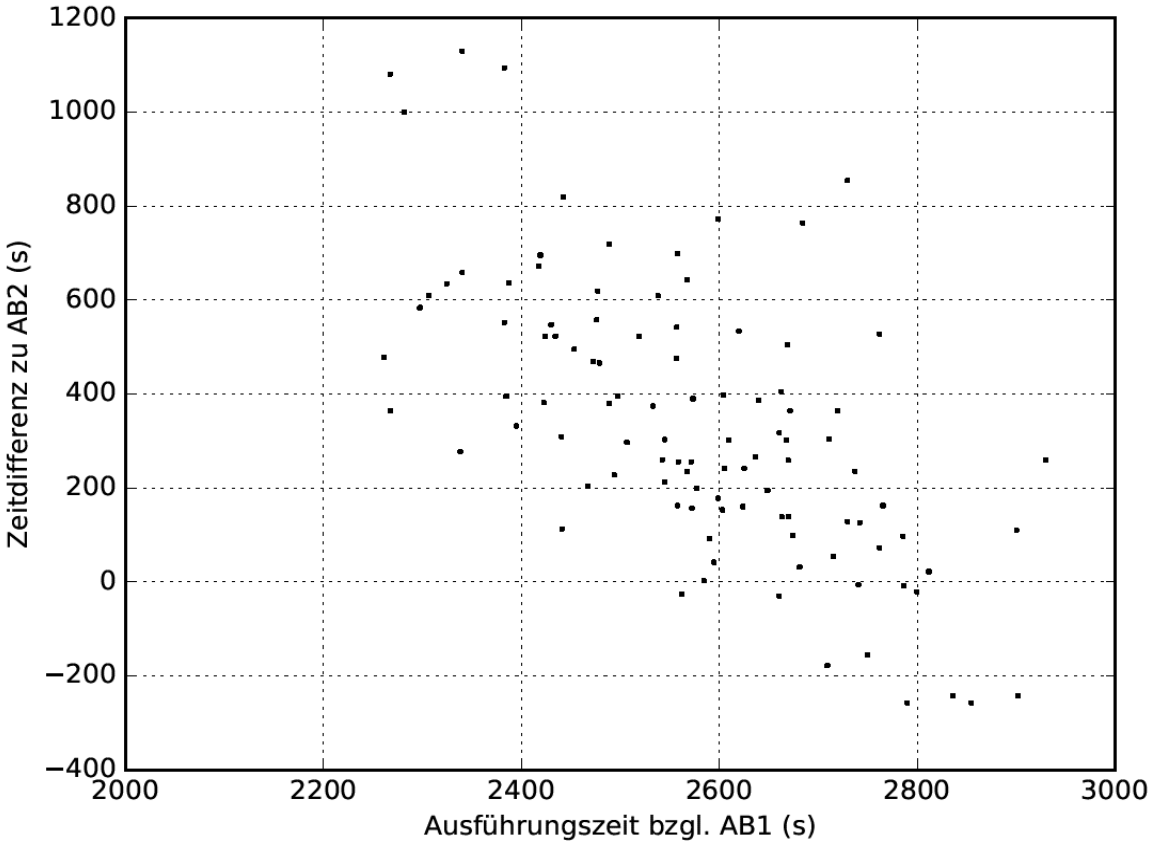


Abb. 3.7 Zusammenhang zwischen Ausführungszeit der Tätigkeit AB1 und der Zeitdifferenz zwischen der Ausführungszeit von AB1 und AB2

3.3.2.2 Herleitung eines Wahrscheinlichkeitsmodells zur Schätzung des Ausfallverhaltens der Druckbegrenzungsventile

Während des zeitlichen Ablaufs eines SBO-Unfallszenarios werden für die automatische Druckbegrenzung das Druckhalter-Abblaseventil (DH-AV) und die beiden Druckhalter-Sicherheitsventile (DH-SiV) wiederholt zum Öffnen und Schließen zyklisch angefordert. Der Zeitpunkt bzw. der Anforderungszyklus, bei dem die jeweiligen Ventile ausfallen können, sowie der Ausfallmodus (‚öffnet nicht' bzw. ‚schließt nicht') sind Zufallsgrößen, die Einfluss auf den Unfallablauf haben.

Zur Schätzung der aleatorischen Unsicherheiten des Ausfallverhaltens der Druckbegrenzungsventile wird ein Wahrscheinlichkeitsmodell für das geschlossene bzw. offene Versagen der jeweiligen Ventile in Abhängigkeit ihrer Anforderungszyklen erstellt. Eine Zufallsstichprobe aus dem entwickelten Wahrscheinlichkeitsmodell liefert schließlich eine Schätzung der aleatorischen Unsicherheit des Anforderungszyklus bzw. des Zeitpunktes, wann die jeweiligen Ventile im Unfallablauf versagen.

Das entwickelte Wahrscheinlichkeitsmodell liefert ein Beispiel dafür, in welcher Art Modelle zur Schätzung aleatorischer Unsicherheiten entwickelt und wie diese umfassend und detailliert in eine IDPSA eingebunden werden können.

Schätzung Versagenswahrscheinlichkeit pro Anforderung für DH-AV und DH-SiV

Da die Anforderungen der Druckbegrenzungsventile in einem auslegungsüberschreitenden Unfallablauf unter Hochdruckbedingungen stattfinden, kann vermutet werden, dass die Versagenswahrscheinlichkeit der jeweiligen Ventile durch die hohen Belastungen mit wachsender Anzahl der Anforderungen zunimmt. Da diesbezüglich jedoch keine Daten aus der Betriebserfahrung vorliegen und auch keine Expertenabschätzungen abgegeben wurden, wird in dieser Analyse eine konstante Versagenswahrscheinlichkeit für die jeweiligen Anforderungszyklen angenommen.

Zur Schätzung der Versagenswahrscheinlichkeit pro Anforderung des DH-AV und der DH-SiV werden Daten aus der Betriebserfahrung verwendet, die sich jeweils auf den Ausfallmodus ‚öffnet nicht' und ‚schließt nicht' beziehen. Zusätzlich liegen GVA-Daten vor, die zur Schätzung von GVA-Wahrscheinlichkeiten für die jeweiligen Ventile bzgl. der Ausfallarten ‚öffnet nicht' und ‚schließt nicht' verwendet werden.

Die in Tab. 3.3 aufgeführten Daten der Einzelfehler für unabhängige Ausfälle sind der Datenbasis /ZED 10/ entnommen. Die Anzahl der Betätigungen für die Sicherheitsventile wird aus einer Gesamtbeobachtungszeit von 428,6 Jahren ermittelt, wobei die Ventile jährlich getestet werden. Für das DH-Abblaseventil liegt eine Gesamtbeobachtungszeit von 161,6 Jahren zugrunde. Anforderungen infolge von aufgetretenen Ereignissen wären aus meldepflichtigen Ereignissen abzuleiten. Solche liegen allerdings nicht vor.

Tab. 3.3 Ausfallereignisse für Einzelfehler des DH-AV und der DH-SiV

DH-AV Ausfallmodus	Anzahl der Ereignisse	Anzahl der Betätigungen
Öffnet nicht	0	161
Schließt nicht	0	161
DH-SiV Ausfallmodus	**Anzahl der Ereignisse**	**Anzahl der Betätigungen**
Öffnet nicht	2	428
Schließt nicht	1	428

Die Schätzung der Versagenswahrscheinlichkeit pro Anforderung aus den in Tab. 3.3 angegebenen Daten für einen Einzelfehler erfolgt über eine Bayes'sche Schätzung mit nichtinformativer a-priori Verteilung /PES 95/. Dabei ergeben sich für die Versagenswahrscheinlichkeit pro Anforderung die in Tab. 3.4 aufgeführten Verteilungen, die die Kenntnisstandunsicherheiten (epistemische Unsicherheiten) bzgl. der jeweiligen geschätzten Zuverlässigkeitskenngrößen ausdrücken:

Tab. 3.4 Geschätzte Verteilungen für die Versagenswahrscheinlichkeit pro Anforderung der DH-Ventile

DH-AV Ausfallmodus	Verteilung für die Versagenswahrscheinlichkeit pro Anforderung	Erwartungswert (Referenzwert)
Öffnet nicht	$F_{DH\text{-}AV;ön}$ = Beta (0.5 , 161.5)	3.09E-03
Schließt nicht	$F_{DH\text{-}AV;sn}$ = Beta (0.5 , 161.5)	3.09E-03
DH-SiV Ausfallmodus		
Öffnet nicht	$F_{SiV;ön}$ = Beta (2.5 , 426.5)	5.83E-03
Schließt nicht	$F_{SiV;sn}$ = Beta (1.5 , 427.5)	3.50E-03

Die Verteilungen in Tab. 3.4 drücken die epistemische Unsicherheit bzgl. der Versagenswahrscheinlichkeit pro Anforderung der jeweiligen Ventile aus. Die epistemischen Unsicherheiten der Ventile werden dabei durch eine Betaverteilung Beta (α , β) mit den entsprechenden Parametern α und β beschrieben.

Da nach Expertenmeinung das DH-AV und die DH-SiV die gleiche Funktion erfüllen, werden die drei Ventile als eine Komponentengruppe betrachtet, die durch ein GVA-Phänomen betroffen sein kann. Die berechneten GVA-Daten beziehen sich somit auf eine Komponentengruppe von drei Komponenten. Die GVA-Daten betreffen nur die Hauptventile. Die jeweilige Ansteuerung ist dabei nicht berücksichtigt, da die Vorsteuerventile Unterschiede aufweisen. Die GVA-Wahrscheinlichkeiten für die Ausfallarten ‚öffnet nicht' und ‚schließt nicht' sind der Datenbasis aus [FAK 14] entnommen und sind in Tab. 3.5 dargestellt.

Tab. 3.5 GVA-Wahrscheinlichkeiten der Ausfallarten ‚öffnet nicht' und ‚schließt nicht' für DH-Ventile

Öffnet nicht

AFK	5%-Quantil	50%-Quantil	95%-Quantil	ErwWert	StdDev
2	2.06E-06	1.35E-04	1.90E-03	4.42E-04	8.87E-04
3	2.92E-08	1.25E-05	5.67E-04	1.23E-04	4.31E-04

Schließt nicht

AFK	5%-Quantil	50%-Quantil	95%-Quantil	ErwWert	StdDev
2	1.57E-08	1.32E-06	3.06E-05	6.87E-06	1.92E-05
3	1.97E-10	9.56E-08	6.07E-06	1.38E-06	6.10E-06

Die GVA-Daten in Tab. 3.5 liefern die GVA-Wahrscheinlichkeit für einen 2v3- bzw. einen 3v3-Ausfall. Für einen 2v3-GVA (d. h. zwei Ausfälle von drei Komponenten) gibt es drei Möglichkeiten, dass zwei von drei Komponenten ausfallen. D. h., wenn man die Wahrscheinlichkeit für einen bestimmten Komponentenausfall aufgrund eines 2v3-GVA bestimmen möchte (z. B. Ausfall von SiV1 und SiV2), müssen die Werte der 2v3-GVA in Tab. 3.5 durch die Anzahl der möglichen Ausfallkombinationen dividiert werden. Die entsprechenden Werte für die Quantile einer bestimmten Ausfallkombination eines 2v3-GVA für die Ausfallart ‚öffnet nicht' lauten demnach 6.87E-7, 4.5E-5 und 6.30E-4.

An die Quantile für eine bestimmte 2v3-GVA Ausfallkombination wurde eine Betaverteilung angepasst. Dabei wurde ein numerischer Suchalgorithmus angewendet, um eine optimale Anpassung an die Quantile zu erhalten. Um die Qualität der Anpassung für die höheren Quantile zu verbessern, wurden die Quantile mit 1, 2 und 10 gewichtet. Für die Anpassung wurde das Programm SUSA /KLO 18/ verwendet, in dem ein entsprechender Suchalgorithmus implementiert ist. Analog wurde mit den Werten eines 2v3-GVA für die Ausfallart ‚schließt nicht' verfahren.

Da es für einen 3v3-Ausfall nur eine Kombinationsmöglichkeit gibt, können für einen gemeinsam verursachten Ausfall aller drei Druckhalterventile die Quantile aus der Tab. 3.5 verwendet werden, an die wiederum eine Betaverteilung angepasst wird. In Tab. 3.6 sind die angepassten Betaverteilungen bzgl. der GVA-Wahrscheinlichkeiten eines 2v3 bzw. 3v3-GVA für die Ausfallarten ‚öffnet nicht' und ‚schließt nicht' angegeben.

Tab. 3.6 Approximierte Betaverteilungen an die Quantile der GVA-Wahrscheinlichkeiten eines bestimmten 2v3- bzw. 3v3-Ausfalls

Ausfallmodus	Ausfallkombination	Angepasste Betaverteilung
öffnet nicht	2v3 - Ausfall	$GVA_{2v3}(ön) \sim Beta(0.43 , 3094)$
	3v3 - Ausfall	$GVA_{3v3}(ön) \sim Beta(0.31 , 4838)$
schließt nicht	2v3 - Ausfall	$GVA_{2v3}(sn) \sim Beta(0.39 , 277967)$
	3v3 - Ausfall	$GVA_{3v3}(sn) \sim Beta(0.24 ,450846)$

Die geschätzten Beta-Verteilungen in Tab. 3.3 und Tab. 3.6 werden verwendet, um die epistemischen Unsicherheiten bzgl. der Versagenswahrscheinlichkeit pro Anforderung für die unabhängigen Ausfälle der Ventile sowie die der GVA-Wahrscheinlichkeiten eines bestimmten 2v3 bzw. 3v3 Ausfalls der DH-Ventile in der Analyse zu berücksichtigen.

Herleitung eines Wahrscheinlichkeitsmodells für das Versagen eines Ventils in Abhängigkeit des Anforderungszyklus

Nach der Aufbereitung der Daten und den daraus abgeleiteten Verteilungen für die Versagenswahrscheinlichkeiten pro Anforderung bzgl. der Ausfallarten ‚öffnet nicht' und ‚schließt nicht', wird in diesem Abschnitt ein Wahrscheinlichkeitsmodell für die Ausfallwahrscheinlichkeit eines Ventils in Abhängigkeit des Anforderungszyklus hergeleitet. Im Folgenden sei:

$p_{ön}$ - die Wahrscheinlichkeit, dass Ventil bei Anforderung nicht öffnet und

p_{sn} - die Wahrscheinlichkeit, dass Ventil bei Anforderung nicht schließt.

Erster Anforderungszyklus:

Der Ausfall eines Ventils in seinem ersten Anforderungszyklus setzt sich aus zwei Ereignissen zusammen:

1. Ventil lässt sich bei Anforderung nicht öffnen.
2. Ventil kann geöffnet werden, lässt sich aber bei nachfolgender Anforderung nicht schließen.

Die Wahrscheinlichkeit, dass das Ventil im ersten Anforderungszyklus nicht öffnet ist gegeben durch:

$$P(\text{ön im Zyklus 1}) = p_{ön} \tag{3.3}$$

Das Ereignis, dass das Ventil bei seinem ersten Anforderungszyklus nicht schließt, kann nur unter der Bedingung eintreten, dass es zuvor geöffnet werden konnte. Die Wahrscheinlichkeit wird durch Gleichung (3.4) berechnet:

$$\begin{aligned} &P(\text{sn im Zyklus 1}) \\ &= P(\text{sn im Zyklus 1} \mid \text{öffnet im Zyklus 1}) \cdot P(\text{öffnet im Zyklus 1}) \\ &= p_{sn} \cdot (1-p_{ön}) \end{aligned} \tag{3.4}$$

Die Wahrscheinlichkeit, dass das Ventil im ersten Zyklus ausfällt, ergibt sich aus der Summe der in Gleichung (3.3) und (3.4) berechneten Wahrscheinlichkeiten, d. h.:

$$\begin{aligned} &P(\text{Ausfall im Zyklus 1}) = P(\text{ön im Zyklus 1}) + P(\text{sn im Zyklus 1}) \\ &= p_{ön} + p_{sn} * (1-p_{ön}) \end{aligned} \tag{3.5}$$

Zweiter Anforderungszyklus:

Das Ventil kann im zweiten Anforderungszyklus nur dann ausfallen, wenn es den ersten Anforderungszyklus überlebt hat d. h., dass es im ersten Zyklus weder beim Öffnen noch beim Schließen ausgefallen ist. Unter Verwendung von Gleichung (3.5) kann die Wahrscheinlichkeit, dass das Ventil im Zyklus 1 nicht ausfällt, berechnet werden durch:

$$\begin{aligned} &P(\text{überlebt Zyklus 1}) = 1 - P(\text{Ausfall im Zyklus 1}) \\ &= 1 - (p_{ön} + p_{sn} \cdot (1-p_{ön})) \\ &= (1 - p_{ön}) \cdot (1 - p_{sn}) \end{aligned} \tag{3.6}$$

Die Wahrscheinlichkeit, dass das Ventil im 2. Zyklus nicht öffnet unter der Bedingung, dass es den 1. Zyklus überlebt hat, wird berechnet durch Gleichung (3.7):

$$\begin{aligned} &P\ (\text{ön im Zyklus 2}) \\ &= P\ (\text{ön im Zyklus 2} \mid \text{überlebt Zyklus 1}) \cdot P\ (\text{überlebt Zyklus 1}) \\ &= p_{ön} \cdot (1- p_{ön}) \cdot (1- p_{sn}) \end{aligned} \tag{3.7}$$

Da angenommen wurde, dass $p_{ön}$ bzw. p_{sn} konstant ist für alle Anforderungszyklen, gilt $P\ (\text{ön im Zyklus 2} \mid \text{überlebt Zyklus 1}) = p_{ön}$.

Das Ereignis, dass das Ventil im 2. Zyklus nicht schließt, setzt die Bedingung voraus, dass das Ventil den Zyklus 1 überlebt hat und im Zyklus 2 geöffnet werden konnte. Die Wahrscheinlichkeit, dass das Ventil den ersten Zyklus überlebt und im Zyklus 2 öffnet, wird berechnet durch:

$$\begin{aligned} &P\ (\text{überlebt Zyklus 1 und öffnet im Zyklus 2}) \\ &= P\ (\text{öffnet im Zyklus 2} \mid \text{überlebt Zyklus 1}) \cdot P\ (\text{überlebt Zyklus 1}) \\ &= (1- p_{ön}) \cdot (1- p_{ön}) \cdot (1- p_{sn}) \end{aligned} \tag{3.8}$$

Die Wahrscheinlichkeit, dass das Ventil im Zyklus 2 nicht schließt, wird unter Verwendung von Gleichung (3.8) berechnet durch:

$$\begin{aligned} &P\ (\text{sn im Zyklus 2}) \\ &= P\ (\text{sn im Zyklus 2} \mid \text{überlebt Zyklus 1 und} \\ &\quad \text{öffnet im Zyklus 2}) \cdot P(\text{überlebt Zyklus 1 und öffnet im Zyklus 2}) \\ &= p_{sn} \cdot (1-p_{ön}) \cdot (1- p_{ön}) \cdot (1- p_{sn}) \end{aligned} \tag{3.9}$$

Die Wahrscheinlichkeit des Ausfalls im zweiten Anforderungszyklus ergibt sich aus der Summe der Wahrscheinlichkeiten aus den Gleichungen (3.7) und (3.9), d. h.:

$$\begin{aligned} &P\ (\text{Ausfall im Zyklus 2}) = \\ &P\ (\text{ön im Zyklus 2}) + P(\text{sn im Zyklus 2}) = \\ &p_{ön} \cdot (1- p_{ön}) \cdot (1- p_{sn}) + p_{sn} \cdot (1-p_{ön}) \cdot (1- p_{ön}) \cdot (1- p_{sn}) = \\ &[p_{ön} + p_{sn} \cdot (1-p_{ön})] \cdot [(1- p_{ön}) \cdot (1- p_{sn})] \end{aligned} \tag{3.10}$$

n-ter Anforderungszyklus:

Aus der analogen Fortführung der Berechnungen ergibt sich folgende allgemeine Formel zur Berechnung der Ausfallwahrscheinlichkeit eines Ventils bei seiner n-ten Anforderung:

$$P\ (\text{Ausfall im Zyklus } n) = [p_{ön} + p_{sn} \cdot (1-p_{ön})] \cdot [(1- p_{ön}) \cdot (1- p_{sn})]^{n-1} \qquad (3.11)$$

Die Wahrscheinlichkeitsverteilung für einen Ausfall eines Ventils bei seiner n-ten Anforderung folgt nach Gleichung (3.11) einer Geometrischen-Verteilung mit dem Parameter $p_{ön} + p_{sn} \cdot (1-p_{ön})$.

Für gegebene Werte von $p_{ön}$ und p_{sn} kann nun unter Verwendung der Gleichung (3.11) die Wahrscheinlichkeitsverteilung des Ausfalls in Abhängigkeit des Anforderungszyklus ermittelt werden. Setzt man z. B. die in Tab. 3.3 aufgeführten Referenzwerte für die jeweiligen DH-Ventile für $p_{ön}$ und p_{sn} ein, so erhält man für die jeweiligen Ventile die in Abb. 3.8 dargestellten Versagenswahrscheinlichkeiten in Abhängigkeit des Anforderungszyklus.

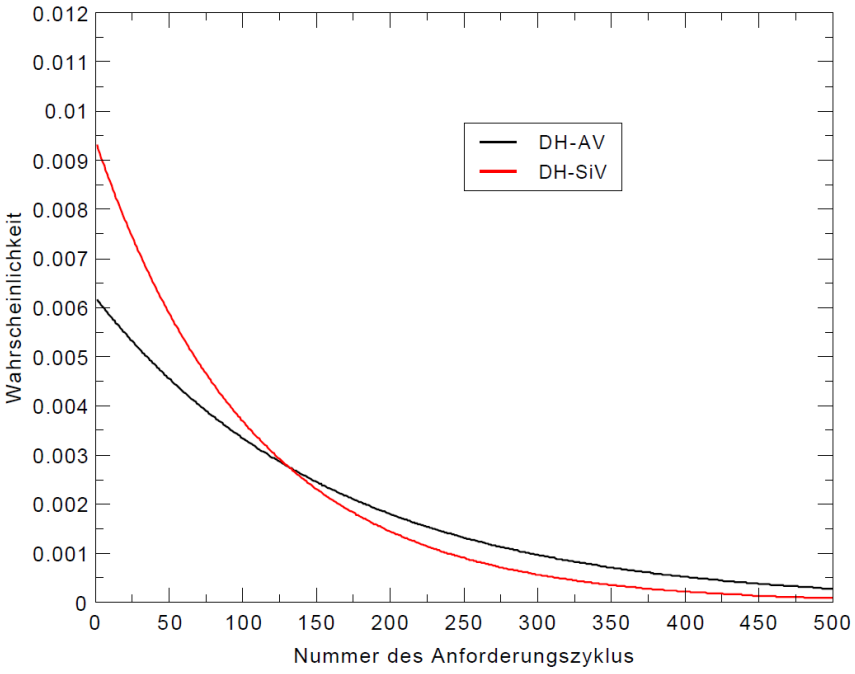


Abb. 3.8 Versagenswahrscheinlichkeit der DH-Ventile in Abhängigkeit vom Anforderungszyklus

Aus den in Abb. 3.8 dargestellten Wahrscheinlichkeitsverteilungen ist abzulesen, mit welcher Wahrscheinlichkeit das jeweilige Ventil beim Anforderungszyklus n ausfällt. Die zu Abb. 3.8 ermittelten Verteilungsfunktionen für das DH-AV und die DH-SiV sind in Abb. 3.9 dargestellt.

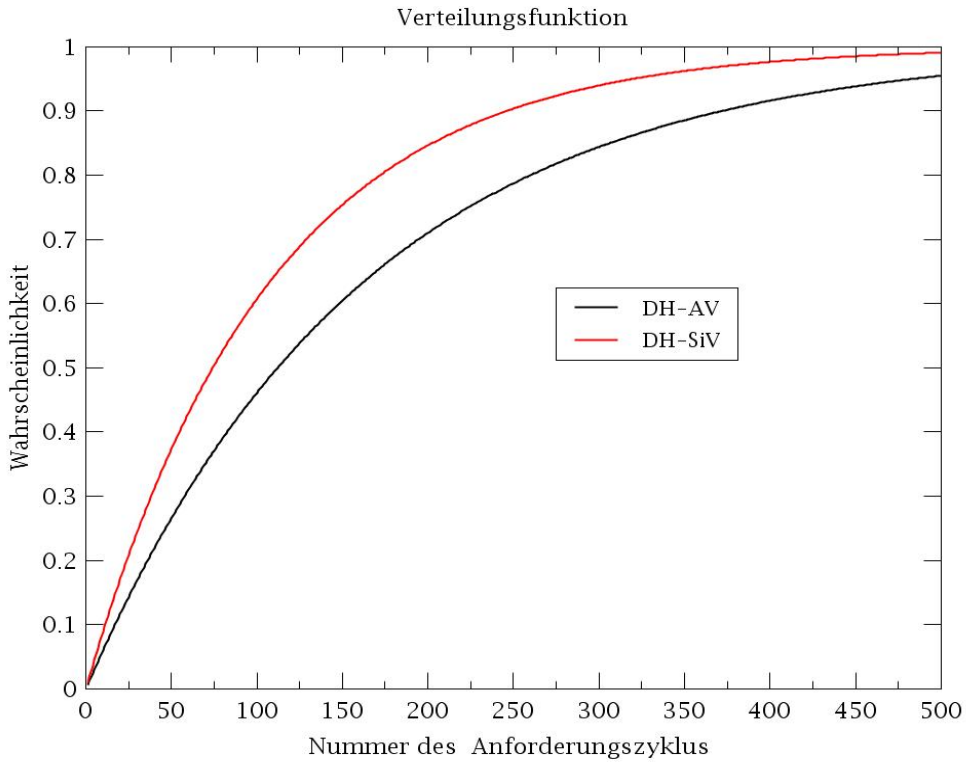


Abb. 3.9 Kumulierte Verteilungsfunktion der Versagenswahrscheinlichkeit über die Anforderungszyklen

Für die Analyse wird das Versagen der DH-Ventile in drei Versagensklassen eingeteilt. Damit sollen die Situationen berücksichtigt werden, in denen die jeweiligen Ventile zu einem frühen Anforderungszyklus (Zyklus ≤ 20), zu einem mittleren Anforderungszyklus (Zyklus 21 – 60) und zu einem späten Anforderungszyklus (Zyklus > 60) geschlossen bzw. offen versagen. Aus den in Abb. 3.9 dargestellten Verteilungsfunktionen können die entsprechenden Wahrscheinlichkeiten ermittelt werden, dass die jeweiligen Ventile innerhalb der ersten 20 Anforderungszyklen, zwischen dem 21. und 60. Anforderungszyklus und zu einem Anforderungszyklus > 60 ausfallen. Für die gegebenen Referenzwerte der jeweiligen Ventile (s. Tab. 3.3) ergeben sich die in Tab. 3.7 aufgeführten Wahrscheinlichkeiten.

Tab. 3.7 Wahrscheinlichkeiten (bzgl. Referenzwerte von $p_{ön}$ und p_{sn}), dass Ventile zu einem frühen, mittleren bzw. späten Anforderungszyklus versagen

Anforderungszyklus	Ausfallwahrscheinlichkeit DH-AV
1 - 20	0.116
21 - 60	0.194
> 60	0.69
Anforderungszyklus	**Ausfallwahrscheinlichkeit DH-SiV1**
1 - 20	0.171
21 - 60	0.259
> 60	0.57
Anforderungszyklus	**Ausfallwahrscheinlichkeit DH-SiV2**
1 - 20	0.171
21 - 60	0.259
> 60	0.57

Die Auswirkung der epistemischen Unsicherheiten von $p_{ön}$ und p_{sn} auf die Verteilungsfunktionen bzgl. des DH-AV und der DH-SiV sind in Abb. 3.10 dargestellt. Die epistemischen Unsicherheiten von $p_{ön}$ und p_{sn} werden durch die jeweiligen Beta-Verteilungen in Tab. 3.3 beschrieben.

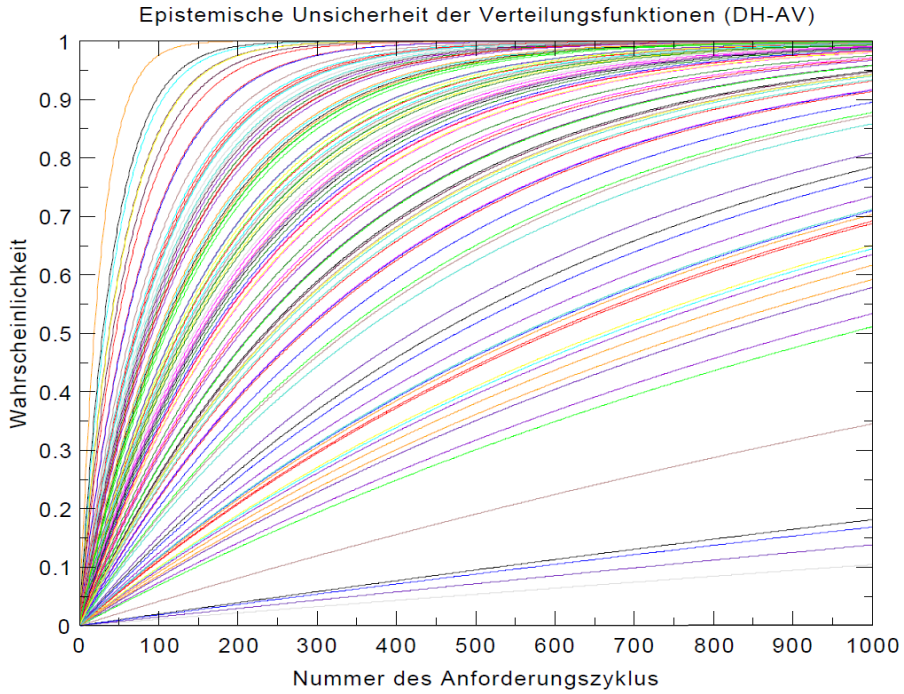


Abb. 3.10 Auswirkung der epistemischen Unsicherheiten von $p_{ön}$ und p_{sn} auf die Verteilungsfunktionen bzgl. des DH-AV

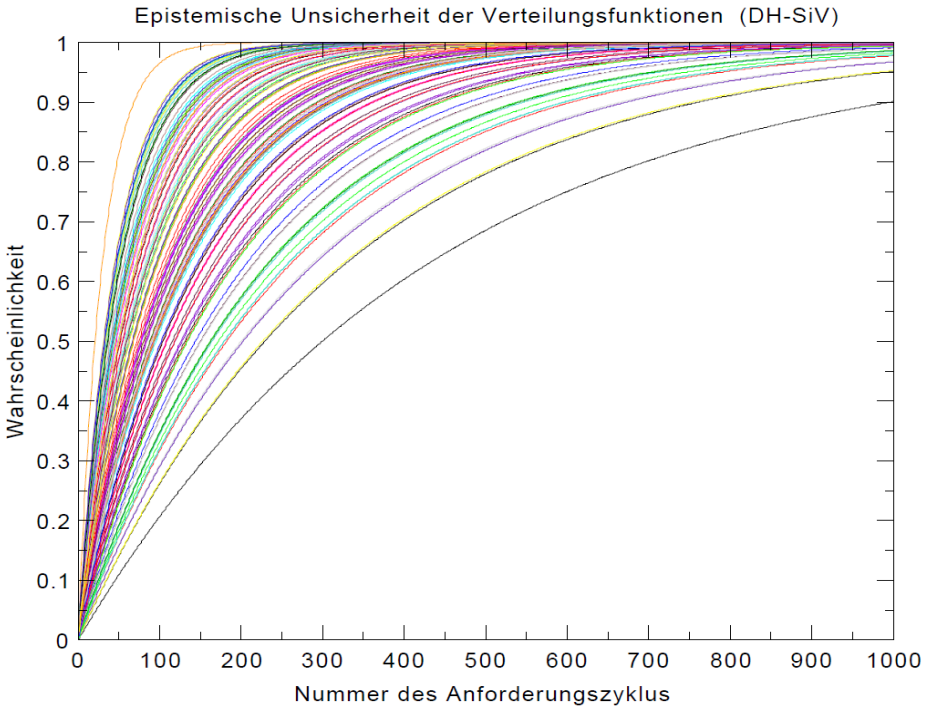


Abb. 3.11 Einfluss der epistemischen Unsicherheiten von $p_{ön}$ und p_{sn} auf die Verteilungsfunktionen bzgl. DH-SiV

Abb. 3.11 zeigt, dass sich die epistemische Unsicherheit von $p_{ön}$ und p_{sn} für das DH-AV stärker auf die kumulierte Verteilungsfunktion auswirkt als für die DH-SiV. Dies wird daraus deutlich, dass die Unsicherheit der Verteilungsfunktion für das DH-AV größer ist als die Unsicherheit der Verteilungsfunktion für die DH-SiV. Die Unsicherheit bzgl. der der Verteilungsunktion wirkt sich des Weiteren auf die Wahrscheinlichkeiten aus, mit denen die jeweiligen Ventile zu einem frühen, mittleren bzw. späten Anforderungszyklus versagen. Die epistemische Unsicherheit der Wahrscheinlichkeit, dass das DH-AV bzw. DH-SiV z. B. frühzeitig zu einem Anforderungszyklus ≤ 20 ausfällt, ist in Tab. 3.8 durch die 5-, 50- und 95%-Quantile der jeweiligen Verteilungen angegeben.

Tab. 3.8 Epistemische Unsicherheit der Versagenswahrscheinlichkeit innerhalb der ersten 20 Anforderungszyklen

Quantil	DH-AV	DH-SiV
5%	5.0 E-3	6.1 E-2
50%	7.7 E-2	1.46 E-1
95%	2.8 E-1	2.47 E-1

Tab. 3.8 zeigt, wie sich die epistemische Unsicherheit von $p_{ön}$ und p_{sn} auf die kumulierten Verteilungsfunktionen (s. Abb. 3.10) und damit auf die Wahrscheinlichkeit auswirkt, innerhalb der ersten 20 Anforderungszyklen auszufallen. Die entsprechenden Wahrscheinlichkeiten bzgl. der Referenzwerte sind 0,116 für das DH-AV und 0.171 für die DH-SiV (s. Tab. 3.7).

Zur Berechnung der Verteilungen für die jeweiligen DH-Ventile und der daraus abgeleiteten Wahrscheinlichkeiten für ein Versagen zu einem frühen, mittleren und späten Anforderungszyklus wurden entsprechende Programmroutinen erstellt. Mit den erstellten Programmroutinen können die aleatorischen Unsicherheiten (Versagenszeitpunkte der Ventile) in Abhängigkeit der epistemischen Unsicherheiten von $p_{ön}$ und p_{sn} ermittelt und in die Analyse einbezogen werden.

3.3.2.3 Herleitung eines Modells zur Schätzung der aleatorischen Unsicherheit der Heizrohrschädigung zu Beginn des Unfallablaufs

Während ihres betrieblichen Einsatzes unterliegen die DE-Heizrohre Belastungen, die zu Wandschwächungen und im Extremfall bis zu einem DE-Heizrohrleck führen könnten. Regelmäßige Inspektionen sollen Wandschwächungen aufspüren, und ggf. wird durch Gegenmaßnahmen (Schließen verdächtiger Rohre) das Auftreten eines Lecks verhindert. Diese Inspektionen werden nicht bei jeder Prüfung für alle Rohre durchgeführt. Die Prüfungen haben eine Messtoleranz, und nicht bei jedem Befund wird das betroffene Rohr geschlossen. Also können auch unmittelbar nach einer Inspektion gewisse tolerierte Schädigungen an DE-Heizrohren fortbestehen, deren Zustand sich nach der Inspektion infolge der Belastungen im Laufe eines Zyklus verschlechtern. Selbst wenn durch die durchgeführten Gegenmaßnahmen ein DE-Heizrohrleck im bestimmungsgemäßen Betrieb praktisch ausgeschlossen ist, kann sich bei einem auslegungsüberschreitenden Unfallablauf im geschwächten Heizrohr möglicherweise ein induziertes Leck entwickeln.

Für die Modellierung bzgl. der Vorschädigungen von DE-Heizrohren wird auf Stellungnahmen des KTA Bezug genommen. Gemäß KTA 3201 zur Messhäufigkeit beträgt das Prüfintervall der Dampferzeuger fünf Jahre, wobei je Dampferzeuger-Prüfung 20 % aller Rohre über ihre gesamte Länge geprüft werden. Damit könnten maximal 25 Jahre zwischen den Prüfungen eines Heizrohres vergehen. Es wird davon ausgegangen, dass sich eine gewisse Anzahl von Rohren bei der Prüfung kurz unterhalb der Verschlusskriterien befinden können und nicht verschlossen werden. Während der Betriebszeit bis zur

nächsten Prüfung – die voraussichtlich mehrere Jahre beträgt – kann sich die Wandstärke durch die Belastungen der DE-Heizrohre weiter verringern. Es kann also möglich sein, dass zum Zeitpunkt des Störfalleintrittes eines oder mehrere Rohre so geschädigt sind, dass sie bei den extremen Belastungen eines auslegungsüberschreitenden Unfalls die Versagensgrenze überschreiten.

In der Analyse wird die Schädigung durch eine Verringerung der Wanddicke des DE-Heizrohrs modelliert. In den nachfolgenden Ausführungen wird eine Schädigung deshalb auch als Wandschwächung bezeichnet.

Annahmen zur Modellierung der Vorschädigung

- Unter Verwendung der Informationen aus KTA 3201 wird für die Analyse von folgenden Annahmen ausgegangen:

  (i) Die Heizrohre sind unterschiedlichen Druck- und Temperaturbelastungen im Dampferzeuger ausgesetzt. Für die Analyse wird angenommen, dass das modellierte Heizrohr in einem Bereich mit hoher Belastung liegt.

  (ii) Gemäß KTA wird davon ausgegangen, dass während der Heizrohrprüfung Wandschwächungen ≥ 20 % auf jeden Fall erkannt werden. D. h. aber auch, dass Heizrohre unmittelbar nach der Prüfung eine Schädigung kleineren Ausmaßes aufweisen können. Für die Analyse wird deshalb angenommen, dass das modellierte Heizrohr unmittelbar nach Prüfung eine Schädigung geringeren Ausmaßes (< 10 %) aufweist, die während der Prüfung nicht entdeckt wurde.

  (iii) Ein Heizrohr, das nach der Prüfung geringe Schädigungen aufweist, wird durch die Belastungen während der Betriebszeit weiter geschwächt und entwickelt mit zunehmender Zeit höhere Schädigungsgrade.

  (iv) Die Widerstandskraft des Heizrohrs gegenüber Druck- und Temperaturbelastungen nimmt mit zunehmendem Schädigungsgrad ab.

Aus den Annahmen (i) – (iv) wird davon ausgegangen, dass in dem Bündel der Heizrohre mindestens ein U-Rohr existiert, das mit einer gewissen Vorschädigung beim Eintritt des Unfallablaufs belastet ist. Für die Analyse wird somit ein potentiell schwaches Heizrohr zugrunde gelegt, das nach zuletzt durchgeführtem Test eine Wandschwächung < 10 % aufweist und im Dampferzeuger einer hohen Belastung ausgesetzt ist.

Da gemäß Annahme (iii) die Schädigung des unterstellten Heizrohrs sich in Abhängigkeit der zeitlichen Belastung weiter erhöht und der Zeitpunkt, wann das auslösende Ereignis des Unfallszenarios eintritt, eine Zufallsvariable darstellt, ist zu schließen, dass auch das Ausmaß der Vorschädigung des Heizrohres zu Beginn des zu analysierenden Unfallszenarios eine Zufallsgröße darstellt, die einer aleatorischen Unsicherheit unterliegt. Zur Schätzung der aleatorischen Unsicherheit bzgl. des Ausmaßes der Heizrohr-Schädigung zu Beginn des Unfallablaufs wurde das nachfolgend beschriebene Wahrscheinlichkeitsmodell entwickelt.

Herleitung eines Modells zur Schätzung der aleatorischen Unsicherheit der Heizrohrschädigung zu Beginn des Unfallszenarios

Die Ausgangssituation zur Modellierung der Wandschwächung kann unter Verwendung der in Abb. 3.12 dargestellten Skizze beschrieben werden.

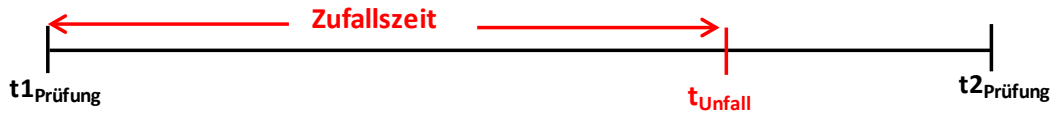


Abb. 3.12 Abhängigkeit der Wandschwächung zu Beginn des Unfallszenarios von dem Zeitpunkt der letzten Prüfung des DE-Heizrohrs

Es wird davon ausgegangen, dass das modellierte Heizrohr zum Zeitpunkt $t_{Prüfung}$ untersucht wird und dass es unmittelbar nach der Prüfung eine Wandschwächung < 10 % aufweist (s. Annahme ii), die nicht entdeckt wurde. Der Zeitpunkt t_{Unfall}, bei dem das auslösende Ereignis für das Unfallszenario auftritt und der Unfallablauf beginnt, ist eine zufällige Größe, deren Wert im Intervall $[t1_{Prüfung}, t2_{Prüfung}]$ zwischen zwei nachfolgenden Prüfungen des U-Rohrs liegt (s. Abb. 3.12). Demzufolge ist auch das Zeitintervall $T = t_{Unfall} - t1_{Prüfung}$ eine Zufallsgröße, in dem die anfängliche Wandschwächung des DE-Heizrohrs weiter zunehmen kann. Je länger das Zeitintervall T ist, umso mehr kann sich die Schädigung vom Zeitpunkt $t1_{Prüfung}$ bis zum Beginn des Unfallablaufs t_{Unfall} vergrößern.

In welchem Ausmaß das DE-Heizrohr zu Beginn des Unfallablaufs geschädigt ist, wird von verschiedenen zufälligen Größen beeinflusst und unterliegt damit selbst einer aleatorischen Unsicherheit. Die zufälligen Einflussgrößen, die zur aleatorischen Unsicherheit bzgl. des Ausmaßes der Heizohrschädigung zu Beginn des Unfallszenarios beitragen, sind:

- Zeitdauer von zuletzt erfolgter Prüfung des Heizrohrs bis zum zufälligen Zeitpunkt des auslösenden Ereignisses, bei dem der Unfallablauf beginnt. Je länger diese Zeitdauer ist, desto mehr kann das Heizrohr durch die andauernden Belastungen geschwächt werden (vgl. Abb. 3.12).
- Zufällige Einflüsse, die die zeitliche Entwicklung der Heizrohrschwächung beeinflussen können, z. B. Ausmaß der Schädigung, die bei zuletzt erfolgter Prüfung übersehen wurde, variierende Belastungen während des Betriebs.

Für die Herleitung des Modells zur Schätzung der aleatorischen Unsicherheit für das Ausmaß der Wandschwächung zu Beginn des Unfallablaufs wird die Schädigung des Heizrohrs in fünf Schädigungsklassen (SK) eingeteilt, deren Intervallgrenzen in Tab. 3.9 aufgeführt sind:

Tab. 3.9 Einteilung der Schädigung des Heizrohrs in fünf Schädigungsklassen

Schädigungsklasse (SK)	Schädigung (in %)
1	< 10
2	10 – 20
3	20 – 30
4	30 – 50
5	50 – 70

Da Testrechnungen gezeigt haben, dass eine Wandschwächung von mehr als 70 % zu einem sofortigen Versagen des DE-Heizrohrs führt, wird für die Analyse eine maximale Wandschwächung von 70 % angenommen, die das zugrunde gelegte schwache Heizrohr zu Beginn des Unfallablaufs aufweisen kann. Als Schädigung des DE-Heizrohrs wird hier das Ausmaß bezeichnet, in dem die Wand des Heizrohrs geschwächt ist. Eine Schädigung von 15 % bedeutet z. B., dass die Wanddicke des U-Rohrs um 15 % geringer ist als die im nicht geschädigten Zustand. Die Schwächung des Heizrohrs wird im Modell durch die entsprechende Verringerung des äußeren Wandradius modelliert.

Im Folgenden wird ein Modell hergeleitet, das die zeitliche Entwicklung der Schädigung des DE-Heizrohrs von zuletzt erfolgter Prüfung bis zum zufälligen Eintreten des Unfallszenarios berücksichtigt. Dazu wird angenommen, dass sich die Schädigungs-

entwicklung des vorausgesetzten „potentiell schwachen“ Heizrohrs von einer Schädigungsklasse in die nächst höhere unter auslegungsgemäßen Druck- und Temperaturbelastungen innerhalb einer Betriebszeit von einem Jahre mit einer gewissen Wahrscheinlichkeit vollzieht. Um die Annahme (iv) zu berücksichtigen, dass die Widerstandskraft des Heizrohrs gegenüber Druck- und Temperaturbelastungen mit zunehmender Schädigung abnimmt, soll die Übergangswahrscheinlichkeit von einer Schädigungsklasse in die nächst höhere vom aktuellen Zustand der Schädigung zu den jeweiligen Berechnungszeitpunkten abhängen.

Die Zustandswahrscheinlichkeit, dass sich das Heizrohr nach n, n = 0, …, 25, Jahren in der Schädigungsklasse j, j = 1, …, 5 befindet, wird durch $p_j\,(n)$ ausgedrückt und im Zustandsvektor $\mathbf{\Pi}\,(n) = [p_1\,(n), p_2\,(n), p_3\,(n), p_4\,(n), p_5\,(n)]$ zusammengefasst.

Gemäß den oben erwähnten Annahmen wird davon ausgegangen, dass das zugrunde gelegte schwache DE-Heizrohr eine nach dem letzten Test unentdeckte Schädigung mit einem zufälligen Wert < 10% aufweist. D. h., das zu analysierende Heizrohr befindet sich unmittelbar nach der letzten Prüfung (n = 0) mit Wahrscheinlichkeit $p_1(0) = 1$ in der Schädigungsklasse 1 (SK 1), in der das Heizrohr eine Schädigung von < 10 % aufweist und mit Wahrscheinlichkeit 0 in den SK 2, ⋯ , SK 5, d. h. $p_2(0) = \cdots = p_5(0) = 0$. Der Vektor der Zustandswahrscheinlichkeiten zum Zeitpunkt der letzten Prüfung (n=0) beträgt somit $\mathbf{\Pi}\,(0) = [1, 0, 0, 0, 0]$ und beschreibt den Anfangszustand der Heizrohrschädigung unmittelbar nach der zuletzt erfolgten Prüfung.

Als Zeiteinheit wird 1 Betriebsjahr angenommen, in dem sich die Schädigung des DE-Heizrohrs mit einer gewissen Wahrscheinlichkeit von einer Schädigungsklasse (SK) in die nächst höhere entwickeln kann. D. h., durch die Druck- und Temperaturbelastungen, denen das DE-Heizrohr während eines Betriebsjahres ausgesetzt ist, kann die Schwächung weiter fortschreiten, so dass sich das Heizrohr nach Ablauf eines Betriebsjahres mit einer gewissen Wahrscheinlichkeit in der nächst höheren SK befinden kann. Dabei wird angenommen, dass sich das Heizrohr innerhalb eines Betriebsjahres nur in die nächst höhere SK und nicht darüber hinaus entwickeln kann.

Die Entwicklung der Schädigung innerhalb eines Betriebsjahres wird durch Wahrscheinlichkeiten ausgedrückt, mit der das Heizrohr von einer SK in die nächst höhere SK übergeht. Die Übergangswahrscheinlichkeiten von der SK i (i = 1, …, 5) in die SK j (j = i, i+1) können in folgender Matrix dargestellt werden:

$$\mathbf{P} = \begin{pmatrix} p_{1,1} & p_{1,2} & 0 & 0 & 0 \\ 0 & p_{2,2} & p_{2,3} & 0 & 0 \\ 0 & 0 & p_{3,3} & p_{3,4} & 0 \\ 0 & 0 & 0 & p_{4,4} & p_{4,5} \\ 0 & 0 & 0 & 0 & p_{5,5} \end{pmatrix} \tag{3.12}$$

$p_{i,j}$ (i = 1, ...,5 ; j = i, i+1) bezeichnen die Wahrscheinlichkeiten, dass nach Ablauf eines Betriebsjahres die Schädigung des Heizrohrs von der SK i in die SK j übergegangen ist. Wenn sich z. B. das Heizrohr in der SK 1 befindet, wird es nach Ablauf eines Betriebsjahres mit Wahrscheinlichkeit $p_{1,2}$ einen Schädigungsgrad aufweisen, der in der SK 2 liegt und mit Wahrscheinlichkeit $p_{1,1}$ einen Schädigungsgrad, der in SK 1 liegt. Weist das Heizrohr eine Wandschwächung der SK 2 auf, wird sich die Wandschwächung innerhalb eines Betriebsjahres mit der Wahrscheinlichkeit $p_{2,3}$ zu einem Wert entwickeln, der in der SK 3 liegt und mit Wahrscheinlichkeit $p_{2,2}$ zu einem Wert, der weiterhin in der SK 2 liegt. Analog sind die Übergangswahrscheinlichkeiten für die restlichen Schädigungsklassen zu interpretieren.

Durch die Matrix **P** der Übergangswahrscheinlichkeiten in Gleichung (3.12) ist es möglich, in der Modellierung die Annahme zu berücksichtigen, dass sich die Widerstandskraft des Heizrohrs mit zunehmendem Schädigungsgrad vermindert. Eine Verringerung der Widerstandskraft bedeutet, dass sich die Wandschwächung umso schneller in die nächsthöhere Schädigungsklasse entwickelt, je höher der aktuelle Schädigungsgrad des Heizrohrs ist. Eine verminderte Widerstandskraft wird durch eine höhere Übergangswahrscheinlichkeit in die nächst höhere Schädigungsklasse ausgedrückt. D. h., die Wahrscheinlichkeit, dass das Heizrohr nach Ablauf eines Betriebsjahres einen Wert aufweist, der sich in der nächsthöheren SK befindet, nimmt mit steigender SK zu.

Für die Schätzung der Übergangswahrscheinlichkeiten von einer SK in die nächst höhere SK innerhalb eines Betriebsjahres liegen keine Daten aus der Betriebserfahrung vor. Da die durchzuführende Analyse das Ziel verfolgt, den Einfluss der aleatorischen Unsicherheit der Heizrohrschädigung zu Beginn des Unfallablaufs auf das DE-Heizrohrversagen zu untersuchen, soll aufgrund der begrenzten Mittel auf aufwändige strukturmechanische Analysen verzichtet werden, mit denen man die Übergangswahrscheinlichkeiten fundierter bestimmen könnte. Für die angestrebten Ziele des Projektes soll hier eine gröbere Abschätzung der Übergangswahrscheinlichkeiten ausreichen. Der Abschätzung werden folgende Annahmen zugrunde gelegt:

Wenn sich das zugrunde gelegte Heizrohr nach der Prüfung in der SK 1 befindet, kann es zufällig eine Wandschwächung zwischen 1 % und 9 % aufweisen, die beim Test nicht entdeckt worden sind. Es wird angenommen, dass sich eine geringe Schädigung, deren Wert in SK 1 liegt, innerhalb eines Betriebsjahres aufgrund der noch relativ hohen Widerstandskraft des Heizrohrs nur wenig verändert und deshalb mit hoher Wahrscheinlichkeit p_{11} in SK 1 verbleibt. Als epistemische Unsicherheit der Wahrscheinlichkeit p_{11} wird eine Gleichverteilung zwischen 0.95 und 0.999 angenommen, d. h. $p_{11} \sim U(0.99,0.999)$. Aufgrund der Bedingung $p_{11} + p_{12} = 1$ ergibt sich, dass die Übergangwahrscheinlichkeit p_{12} gemäß U (0.001, 0.01) verteilt ist. Die Verteilung drückt die epistemische Unsicherheit bzgl. der Wahrscheinlichkeit p_{12} aus, mit der sich die Schädigung des Heizrohrs innerhalb eines Betriebsjahres von einem Wert in SK 1 zu einem Wert entwickelt, der in SK 2 liegt.

Bei zunehmender Schädigung wurde eine verminderte Widerstandskraft angenommen. Dies wirkt sich in dem Modell durch eine höhere Übergangswahrscheinlichkeit aus. D. h., es wird davon ausgegangen, dass $p_{45} > p_{34} > p_{23} > p_{12}$. Um diese Beziehung zu berücksichtigen, werden die in Tab. 3.10 aufgeführten Verteilungen für die Übergangswahrscheinlichkeiten p_{12}, p_{23}, p_{34} und p_{45} angenommen.

Tab. 3.10 Epistemische Unsicherheit der Übergangswahrscheinlichkeiten in die nächst höhere Schädigungsklasse innerhalb eines Betriebsjahres

Übergangs-wahrscheinlichkeit	Epistemische Unsicherheit	Referenzwert
p_{12}	U(0.001 , 0.01)	0.005
P_{23}	U(0.01 , 0.07)	0.04
P_{34}	U(0.07 , 0.15)	0.11
p_{45}	U(0.15 , 0.3)	0.225

An dieser Stelle wird nochmals ausdrücklich darauf hingewiesen, dass die in Tab. 3.10 ausgewiesenen epistemischen Verteilungen und Referenzwerte nicht durch Daten aus der Betriebserfahrung oder strukturmechanische Analysen gestützt werden, sondern für die Anwendungsrechnung gewählte Abschätzungen sind, die den oben getroffenen Annahmen entsprechen. Durch strukturmechanische Analysen könnten die Werte der

Übergangswahrscheinlichkeiten auf eine fundiertere Basis gestellt werden. Für die Ziele des Projektes, sollten die groben Abschätzungen zunächst ausreichen.

Die Zustandswahrscheinlichkeit, dass sich die Wandschwächung des Heizrohrs n Jahre nach dem zuletzt erfolgten Test in der Schädigungsklasse i, i= 1, …, 5 befindet, kann unter Verwendung der in Gleichung (3.12) dargestellten Matrix **P** der Übergangswahrscheinlichkeiten und dem Anfangsvektor **Π** (0) der Zustandswahrscheinlichkeiten über eine Markov-Kette gemäß Gleichung (3.13) ermittelt werden durch:

$$\mathbf{\Pi}(n) = \mathbf{\Pi}(0) \cdot \mathbf{P}^n \tag{3.13}$$

Für die in Tab. 3.10 angegebenen Referenzwerte ist die Matrix **P** der Übergangswahrscheinlichkeiten gegeben durch:

$$\mathbf{P} = \begin{pmatrix} 0.995 & 0.005 & 0 & 0 & 0 \\ 0 & 0.96 & 0.04 & 0 & 0 \\ 0 & 0 & 0.89 & 0.11 & 0 \\ 0 & 0 & 0 & 0.775 & 0.225 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.14}$$

Bei gegebenem Anfangsvektor **Π** (0) = [$p_1(0)$, $p_2(0)$, $p_3(0)$, $p_4(0)$, $p_5(0)$] = [1, 0, 0, 0, 0] und der Übergangmatrix **P** in Gleichung (3.14) für die gegebenen Referenzwerte, ergibt sich für den Fall, dass sich das einleitende Ereignis z. B. n=10 Jahre nach dem zuletzt erfolgten Test des Rohrs ereignet, die Zustandsverteilung

Π (10) = [0.951, 4.09E-2, 5.97E-3, 1.36E-3, 6.6E-4]

D. h., wenn der Unfall 10 Jahre nach dem zuletzt erfolgten Test des Heizrohrs eintritt, dann wird das DE-Heizrohr mit der Wahrscheinlichkeit von ca. 0.951 einen Schädigungswert aufweisen, der in der SK 1 liegt, mit Wahrscheinlichkeit von 4.09E-2 einen Wert, der in der SK 2 liegt, usw.

Die Zeit, wann das einleitende Ereignis nach dem zuletzt erfolgten Test auftritt, wird als gleichverteilte Zufallsvariable betrachtet, die zwischen 1 und 25 Jahren liegen kann. Wird für die Zeit eine Stichprobe aus der Gleichverteilung U (1,25) ausgespielt und setzt die Werte der Stichprobe für n in Gleichung (3.13) ein, erhält man eine entsprechende Stichprobe von Zustandsverteilungen.

Neben der aleatorischen Unsicherheit der Zeit, wann das einleitende Ereignis nach der letzten Prüfung des Heizrohrs auftritt, werden in der Analyse auch die in Tab. 3.10 spezifizierten epistemischen Unsicherheiten der Übergangswahrscheinlichkeiten p_{ij} der Matrix **P** berücksichtigt. Die Berücksichtigung der epistemischen und aleatorischen Unsicherheiten des Modells erfolgt über eine 2-fach geschachtelte Simulationsschleife. In der äußeren Simulationsschleife werden pro Simulationslauf aus den jeweiligen epistemischen Verteilungen der Übergangswahrscheinlichkeiten p_{12}, p_{23}, p_{34} und p_{45} Zufallswerte ausgespielt, die für die entsprechenden Werte p_{ij} (i=1, ..., 5, j=i, i+1) der Übergangsmatrix **P** eingesetzt werden. Für diese Matrix **P** wird in der zweiten Simulationsschleife die Zeitdauer n zwischen Eintritt des Unfalls und dem zuletzt erfolgten Test des Heizrohrs zufällig ausgespielt. Mit den Werten der Anfangsverteilung **Π** (0) = [1, 0, 0, 0, 0], der Übergangsmatrix **P** und der Zufallszeit n wird die Zustandsverteilung **Π** (n) mittels Gleichung (3.13) berechnet. Unter Verwendung dieser 2-fach geschachtelten Monte-Carlo Simulation erhält man eine Stichprobe von Zustandsverteilungen der Wahrscheinlichkeiten, mit denen sich das Heizrohr zu Beginn des Unfallablaufs in den jeweiligen Schädigungsklassen i, i=1, …, 5 befindet.

Für die Durchführung der zweifach geschachtelten Monte-Carlo Simulation wurde ein Programm erstellt, mit dem die Stichprobe der Zustandsverteilungen unter Berücksichtigung der epistemischen und aleatorischen Unsicherheiten erzeugt wurde. Die Unsicherheit bzgl. des Schädigungsgrades des DE-Heizrohrs zu Beginn des Unfallablaufs, die durch die Stichprobe der Zustandsverteilungen ausgedrückt wird, geht schließlich in durchzuführende IDPSA ein, die unter Verwendung von MCDET und ATHLET-CD durchgeführt wird.

3.4 Modellierung der Einbindung aleatorischer Unsicherheiten in die MCDET/ATHLET-CD Analyse

In diesem Abschnitt wird beschrieben, wie die aleatorischen Unsicherheiten, die unter Verwendung der in den Abschnitten 3.3.2.2 und 3.3.2.3 hergeleiteten Modelle ermittelt wurden, in die MCDET/ATHLET-CD Analyse eingebunden werden.

Abschnitt 3.4.1 beschreibt die Einbindung der aleatorischen Unsicherheit bzgl. des Versagenszeitpunktes und der Ausfallart der DH-Ventile. In Abschnitt 3.4.2 wird die Einbindung der aleatorischen Unsicherheit bzgl. des Schweregrades der Heizrohrschädigung in die MCDET-Analyse beschrieben.

3.4.1 Einbindung der aleatorischen Unsicherheit des Versagenszeitpunktes und Ausfallart der DH-Ventile

Bei der automatischen Druckbegrenzung in einem Unfallablauf wird zuerst das DH-AV zyklisch angefordert. Bei Ausfall des DH-AV oder im Fall, dass der Druck trotz DH-AV weiter steigt, wird das DH-SiV1 angefordert. Fällt das DH-SiV1 aus oder ist die Druckentlastung nicht ausreichend, wird als letzte Möglichkeit zur automatischen Druckbegrenzung das DH-SiV2 angefordert. Bei welchem der vielen Anforderungszyklen das jeweilige Ventil ausfällt, ist eine zufällige Größe und stellt eine aleatorische Unsicherheit dar. Fällt ein Ventil aus, dann ist auch die Ausfallart, ob das Ventil geschlossen oder offen ausfällt, als eine aleatorische Unsicherheit zu betrachten.

Um den Einfluss des Ausfallzeitpunktes der Druckhalterventile auf den Unfallablauf genauer untersuchen zu können, sollen in der MCDET-Analyse in jedem erzeugten dynamischen Ereignisbaum folgende drei Klassen gemeinsam berücksichtigt werden, wann die jeweiligen Ventile ausfallen:

- Ausfall innerhalb der ersten 20 Anforderungszyklen (frühzeitiger Ausfall)
- Ausfall innerhalb der Anforderungszyklen 21 – 60 (mittelfristiger Ausfall)
- Ausfall zu einem Anforderungszyklus > 60 (später Ausfall)

Während in einer einfachen Monte-Carlo Simulation nur ein Zufallswert eines Anforderungszyklus ausgespielt wird, bei dem das jeweilige Ventil ausfällt, gehen im Rahmen der Simulation eines dynamischen Ereignisbaumes drei Zufallswerte ein, wobei jeweils ein Zufallswert eines Anforderungszyklus aus der Klasse der frühzeitigen, einer aus der Klasse der mittleren und ein Zufallswert aus der Klasse der späten Ausfälle ausgespielt wird.

Aus der in Abschnitt 3.3.2.2 hergeleiteten Geometrischen-Verteilung können die entsprechenden Wahrscheinlichkeiten ermittelt werden, dass ein DH-Ventil zu einem frühen, mittleren oder späten Anforderungszyklus versagt. Für die nachfolgenden Ausführungen bezeichnet

- $p_{k,\leq 20}$ – die Wahrscheinlichkeit, dass Ventil k innerhalb der ersten 20 Anforderungszyklen ausfällt,
- $p_{k,21\text{-}60}$ – die Wahrscheinlichkeit, dass Ventil k zu einem Anforderungszyklen 21 – 60 ausfällt,

- $p_{k,>60}$ – die Wahrscheinlichkeit, dass Ventil zu einem Zyklus > 60 ausfällt,
- $p_{2v3,ön}$ – die GVA-Wahrscheinlichkeit für einen bestimmten 2v3-Ausfall der Ausfallart ‚öffnet nicht',
- $p_{2v3,sn}$ – die GVA-Wahrscheinlichkeit für einen bestimmten 2v3-Ausfall der Ausfallart ‚schließt nicht', und
- $p_{3v3,ön}$ – die GVA-Wahrscheinlichkeit für einen 3v3-Ausfall Ausfallart ‚öffnet nicht'.

Aus der hergeleiteten Geometrischen-Verteilung wird für jede der drei Klassen eine bedingte Verteilung erzeugt, aus denen zufällige Versagenszyklen $n_{k;\leq 20}$, $n_{k;21\text{-}60}$, $n_{k;>60}$ für die entsprechenden Ventile k = AV, SiV1, SiV2 und für jeden dynamischen Ereignisbaum ausgespielt werden. Dabei bezeichnet:

- $n_{k;\leq 20}$ – zufälliger Zyklus zwischen 1 und 20, bei dem Ventil k versagt.
- $n_{k;21\text{-}60}$ – zufälliger Zyklus zwischen 21 und 60, bei dem Ventil k versagt.
- $n_{k;>60}$ – zufälliger Zyklus > 60, bei dem Ventil k versagt.

Die Wahrscheinlichkeiten in welchem Ausfallmodus (‚öffnet nicht' oder ‚schließt nicht') ein Ventil bei seinem zufälligen Versagenszyklus ausfällt, werden aus den Versagenswahrscheinlichkeiten $p_{ön}(n)$ und $p_{sn}(n)$ zum jeweiligen Versagenszyklus n ermittelt, die sich unter Verwendung von Gleichung (3.11) berechnen lassen.

Wenn ein Ventil im Anforderungszyklus n ausfällt, dann erfolgt der Ausfall mit den Wahrscheinlichkeiten

$$\pi_{k,ön} = \frac{p_{ön}}{p_{ön} + (1\text{-}p_{ön}) \cdot p_{sn}} \qquad (3.15)$$

im Ausfallmodus ‚öffnet nicht'

und

$$\pi_{k,sn} = \frac{(1\text{-}p_{ön}) \cdot p_{sn}}{p_{ön} + (1\text{-}p_{ön}) \cdot p_{sn}} \qquad (3.16)$$

im Ausfallmodus ‚schließt nicht'

wobei für $p_{ön}$ und p_{sn} die jeweiligen Werte $p_{ön}(n)$ und $p_{sn}(n)$ zum Versagenszyklus n verwendet werden.

Bei einer einfachen Monte-Carlo Simulation würde aus den hergeleiteten Wahrscheinlichkeitsverteilungen der Ventile für jeden dynamischen Ereignisbaum jeweils ein zufälliger Versagenszyklus ausgespielt. Der Nachteil wäre, dass Versagenszyklen mit geringen Wahrscheinlichkeiten (z. B. frühe Versagenszyklen) in der Zufallsstichprobe entweder gar nicht, oder nur sehr selten vorkommen würden. Eine Quantifizierung des Einflusses der aleatorischen Unsicherheit wäre damit ungenauer, weil man z. B. den Einfluss früher Versagenszyklen nicht erfassen würde. Dieser Nachteil der reinen Monte-Carlo Simulation kann durch die Verwendung der dynamische Ereignisbaum Methode vermieden werden.

Die Verzweigungsstruktur, die sich bei der Erzeugung eines dynamischen Ereignisbaumes bzgl. der DH-Ventile ergibt, ist in den Abb. 3.13 – Abb. 3.15 skizziert. In der Analyse werden sowohl die unabhängigen Ausfälle der jeweiligen DH-Ventile als auch die Ausfallkombinationen aufgrund gemeinsam verursachter Ausfälle (GVA) berücksichtigt. Abb. 3.13 beschreibt die Verzweigungsstruktur im dynamischen Ereignisbaum (DET) bzgl. DH-AV, Abb. 3.14 bzgl. SiV1 und Abb. 3.15 die Verzweigungsstruktur im DET bzgl. SiV2.

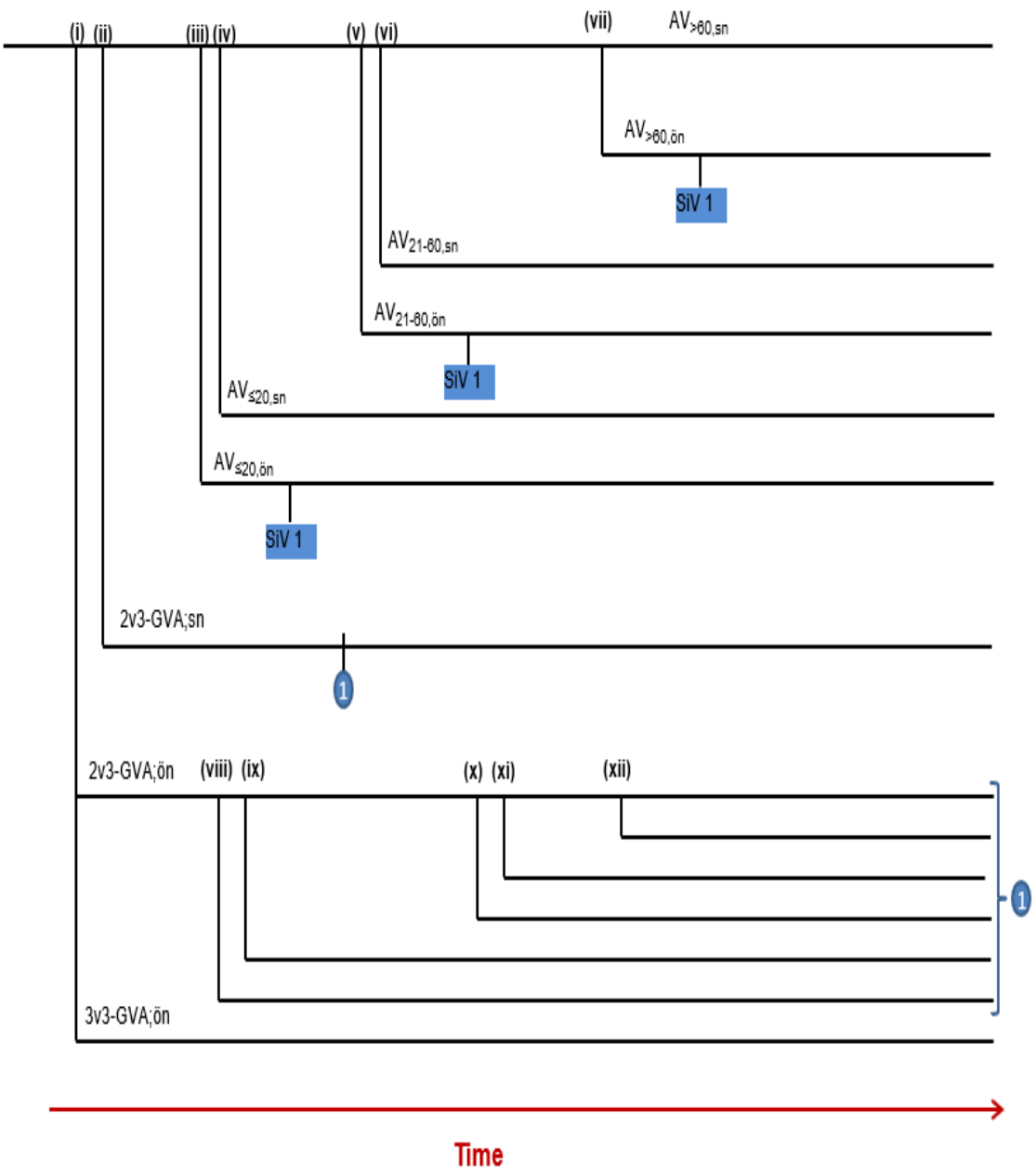


Abb. 3.13 Verzweigungsstruktur im dynamischen Ereignisbaum bzgl. DH-AV

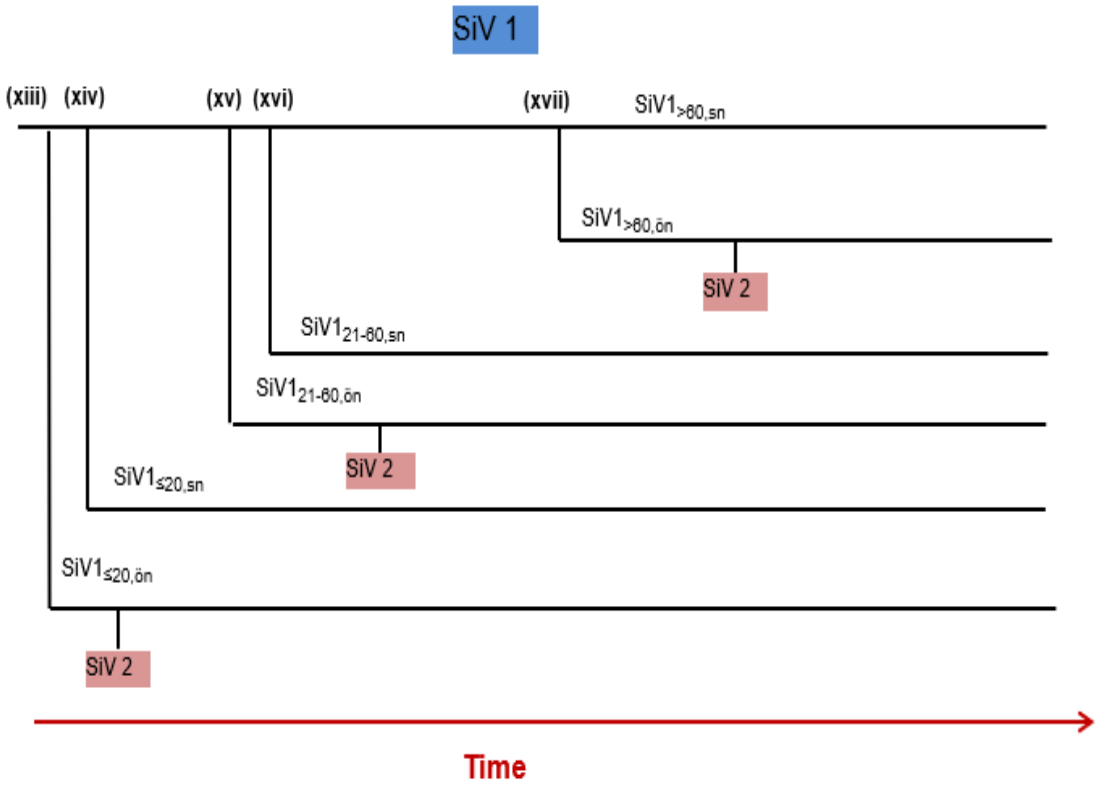


Abb. 3.14 Verzweigungsstruktur im DET bzgl. SiV1

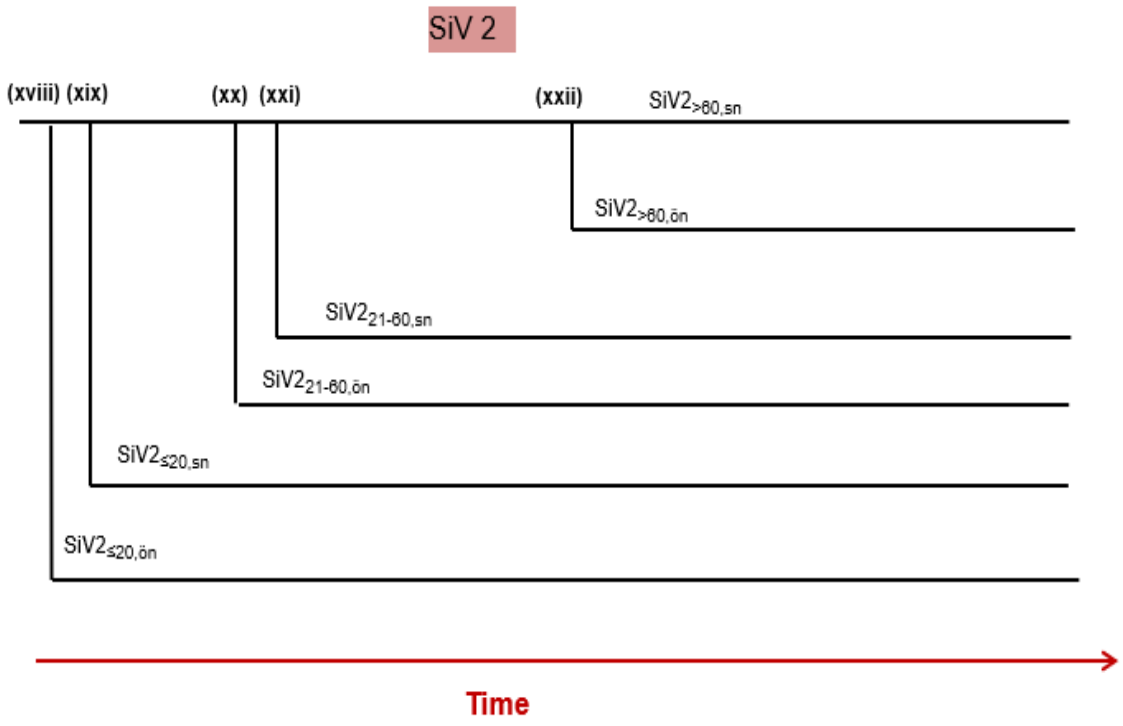


Abb. 3.15 Verzweigungsstruktur im DET bzgl. SiV2

In den Abb. 3.13 – Abb. 3.15 sind die verschiedenen Verzweigungspunkte und die sich daraus ergebenden Sequenzen (Pfade) für die DH-Ventile durch die Kennzeichnungen **(i)**–**(xxii)** angegeben. Im Folgenden werden die Verzweigungspunkte und Sequenzen beschrieben, die in Abb. 3.13 dargestellt sind. Die Verzweigungspunkte und Sequenzen der Tab. 3.13 und Tab. 3.14 sind analog zu interpretieren.

Verzweigungspunkt (i):

Im Rahmen der automatischen Druckbegrenzung wird während des Unfallablaufs zunächst das DH-AV zyklisch angefordert. Wenn das DH-AV zum ersten Mal zum Öffnen angefordert wird, kann sich zu diesem Zeitpunkt ein GVA bzgl. der DH-Ventile bemerkbar machen. Zu diesem Zeitpunkt besteht die aleatorische Unsicherheit darin, ob ein 2v3-GVA, ein 3v3-GVA oder kein GVA vorliegt.

Die Sequenz, die mit *3v3-GVA,ön* bezeichnet ist, beschreibt das Zufallsereignis, dass ein 3v3-GVA bzgl. der Ausfallart ‚öffnet nicht' vorliegt. D. h., DH-AV, DH-SiV1 und DH-SiV2 verbleiben im geschlossenen Zustand. Da von der Annahme ausgegangen wird, dass kein 3v3-GVA im Ausfallmodus ‚schließt nicht' berücksichtigt wird, ist die Wahrscheinlichkeit durch die bedingte Wahrscheinlichkeit $p_{3v3,ön} / (1-p_{3v3,sn})$ gegeben. Da aber $1-p_{3v3,sn} \approx 1$ ist, ist die bedingte Wahrscheinlichkeit nahezu mit $p_{3v3,ön}$ gleichzusetzen. Die epistemische Unsicherheit $p_{3v3,ön}$ wird durch die entsprechende Verteilung in Tab. 3.6 beschrieben.

In dem Pfad mit der Bezeichnung 2*v3-GVA,ön* besteht das Ereignis darin, dass ein 2v3-GVA bzgl. der Ausfallart ‚öffnet nicht' vorliegt. Bei einem 2v3-GVA gibt es drei mögliche Kombinationen, dass zwei von den drei Ventilen durch GVA eine gemeinsame Ursache ausgefallen sind. Von diesen drei möglichen Ausfallkombinationen wird pro DET zufällig eine Kombination ausgewählt. Wenn 2 von 3 Ventilen durch einen GVA ausgefallen sind, kann noch das verbleibende funktionierende Ventil zur Druckbegrenzung angefordert werden. Das mögliche Ausfallverhalten des nicht vom GVA betroffenen Ventils wird durch die Verzweigungen (**viii**) – (**xii**) beschrieben, die analog zu den Verzweigungen **(iii)** – **(vii)** des DH-AV interpretiert werden können. Die Wahrscheinlichkeit für den 2v3-GVA sei mit $p_{2v3,ön}$ bezeichnet, deren Verteilung der epistemischen Unsicherheit in Tab. 3.6 angegeben ist.

Verzweigungspunkt (ii):

Wenn bei der ersten Anforderung des DH-AV zum Öffnen kein GVA vorliegt (die Wahrscheinlichkeit dafür ist gegeben durch $p = 1- p_{2v3,ön} - p_{3v3,ön}$), wird das DH-AV geöffnet und der Unfallablauf bis zum Zeitpunkt weiter berechnet, an dem das DH-AV zum ersten Mal zum Schließen angefordert wird. Zu diesem Zeitpunkt wird der Verzweigungspunkt **(ii)** mit der Verzweigung für einen 2v3-GVA der Ausfallart ‚schließt nicht' erzeugt, die mit der Wahrscheinlichkeit $p_{2v3,sn}$ eintritt Diese Verzweigung ist in Abb. 3.13 durch den Pfad mit der Bezeichnung *2v3-GVA;sn* dargestellt. Da die Analyse unter der Bedingung einer Hochdruck-Situation durchgeführt werden soll, wird der 3v3-GVA für die Ausfallart ‚schließt nicht' in der Analyse nicht berücksichtigt, da davon ausgegangen wird, dass es bei diesem Ereignis nicht zum Hochdruck-Fall kommt.

Sollte es bei einem 2v3-GVA der Ausfallart ‚schließt nicht' zu einer Anforderung zum Öffnen des verbleibenden Ventils kommen, werden zusätzlich die durch **(viii)** – **(xii)** gekennzeichneten Verzweigungen erzeugt. Andernfalls werden diese Verzweigungen bei der Erzeugung des DET nicht generiert.

Verzweigungspunkt (iii):

Unter der Bedingung, dass bei der ersten Anforderung des DH-AV kein GVA vorliegt, erfolgt der nächste Verzweigungspunkt **(iii)** zum Zeitpunkt, wenn die Anzahl der Anforderungen des DH-AV den Wert $n_{AV;\leq 20}$ erreicht und das DH-AV zum Öffnen angefordert wird. Bei diesem Verzweigungspunkt wird die aleatorische Unsicherheit berücksichtigt, ob das DH-AV bei der Anforderung mit der Wahrscheinlichkeit $p_{AV,\leq 20} \cdot \pi_{AV,ön}$ geschlossen versagt (Pfad $AV_{\leq 20;ön}$) oder mit der Wahrscheinlichkeit $1 - p_{AV,\leq 20} \cdot \pi_{AV,ön}$ erfolgreich geöffnet werden kann. Da die GVA-Wahrscheinlichkeiten sehr klein sind, gilt für die Wahrscheinlichkeit, dass kein GVA vorliegt, $1 - p_{2v3,ön} - p_{3v3,ön} - p_{2v3,sn} \sim 1$. Deshalb wird oben auf die Angabe der bedingten Wahrscheinlichkeit verzichtet. Der Zufallswert $n_{AV;\leq 20}$ wurde unter Verwendung der oben hergeleiteten Geometrischen-Verteilung ausgespielt.

Wenn das DH-AV bei der Anforderung $n_{AV;\leq 20}$ nicht öffnet, baut sich der Druck weiter auf, so dass im weiteren Unfallablauf das Sicherheitsventil 1 (SiV1) zyklisch angefordert wird. Bei der zyklischen Anforderung des SiV1 ergibt sich die Verzweigungsstruktur, die durch die Verzweigungspunkte **(xiii)** – **(xvii)** in Abb. 3.14 dargestellt sind. Die Beschreibung der Verzweigungspunkte ist analog zu den Verzweigungspunkten **(iii)** – **(vii)**, die für das DH-AV erzeugt werden. Wenn die Anzahl der Anforderungen des SiV1 den Wert $n_{SiV1;\leq 20}$

erreicht und SiV1 zum Öffnen angefordert wird, wird der Verzweigungspunkt **(xiii)** in Abb. 3.14 erzeugt. Die Verzweigung führt mit Wahrscheinlichkeit $p_{SiV1,\leq 20} \cdot \pi_{SiV1,\ddot{o}n}$ zum Pfad $SiV1_{\leq 20;\ddot{o}n}$ und beschreibt das Ereignis, dass SiV1 frühzeitig bei der Anforderung $n_{SiV1;\leq 20}$ geschlossen ausfällt.

Wenn sowohl das DH-AV bei der Verzweigung **(iii)** als auch das SiV1 bei **(xiii)** frühzeitig geschlossen ausgefallen sind, ist davon auszugehen, dass im weiteren Unfallablauf das SiV2 zyklisch angefordert wird. Bei der zyklischen Anforderung des SiV2 werden die Verzweigungen generiert, die durch die Verzweigungspunkte **(xviii)** – **(xxii)** für das SiV2 in Abb. 3.15 dargestellt sind und analog zu den Verzweigungspunkten für SIV1 zu interpretieren sind.

Wenn das DH-AV bei der Verzeigung **(iii)** nicht geschlossen ausfällt und bestimmungsgemäß öffnet, wird der Druck abgebaut, so dass das DH-AV im weiteren Ablauf zum Schließen angefordert wird.

Verzweigungspunkt (iv):

Wenn das DH-AV im Anforderungszyklus $n_{AV;\leq 20}$ zum Schließen angefordert wird, wird der Verzweigungspunkt **(iv)** mit der Verzweigung zum Pfad $AV_{\leq 20;sn}$ erzeugt. Im Pfad $AV_{\leq 20;sn}$ wird das Ereignis gerechnet, dass das DH-AV im Anforderungszyklus $n_{AV;\leq 20}$ offen versagt. Wenn durch das offene DH-AV der Druck im weiteren Unfallablauf nicht weiter ansteigt, werden SiV1 und SiV2 nicht angefordert. In dem besonderen Fall, dass trotz des offenen Versagens des DH-AV der Druck weiter ansteigt, wird im weiteren Ablauf das SiV1 angefordert. Ob SiV1 zum Öffnen angefordert wird oder nicht, hängt in diesem Pfad somit davon ab, ob der Druck bei offenem DH-AV weiter ansteigt oder nicht. Diese Situation ist in Abb. 3.13 durch SiV1 gekennzeichnet. Die Verzweigungen zu SiV1 in Abb. 3.13 sind analog zu den Verzweigungen **(iii)** – **(vii)** des DH-AV zu interpretieren.

Das Ereignis, dass das DH-AV im Anforderungszyklus $n_{AV;\leq 20}$ offen versagt, kann nur unter der Bedingung eintreten, dass das DH-AV zuvor geöffnet werden konnte. Für die Verzweigungswahrscheinlichkeit für den Pfad $AV_{\leq 20;sn}$ wird die bedingte Wahrscheinlichkeit berechnet durch:

$$\frac{p_{AV,\leq 20} \cdot \pi_{AV,sn}}{1 - p_{AV,\leq 20} \cdot \pi_{AV,\ddot{o}n}} \tag{3.17}$$

Die Erfolgswahrscheinlichkeit des Verzweigungspunktes **(iv)** beschreibt die Situation, dass das DH-AV nicht frühzeitig ausfällt (weder offen noch geschlossen) und ist gegeben durch $1 - p_{AV,\leq 20}$.

Verzweigungspunkt (v):

Wenn das DH-AV die ersten 20 Anforderungszyklen überlebt, kann es im weiteren Verlauf zu einem zufälligen Zyklus $n_{AV;21\text{-}60}$ innerhalb der Anforderungszyklen 21 – 60 geschlossen oder offen ausfallen. Zum Zeitpunkt, an dem das DH-AV im weiteren Prozessablauf den zufällig ausgespielten Anforderungszyklus $n_{AV;21\text{-}60}$ erreicht und zum Öffnen angefordert wird, erzeugt MCDET den Verzweigungspunkt **(v)**. Hier wird die aleatorische Unsicherheit berücksichtigt, dass das DH-AV beim Öffnen versagen oder nicht versagen kann.

Der Pfad $AV_{21\text{-}60;ön}$ in Abb. 3.13 beschreibt die Situation, dass das DH-AV im Anforderungszyklus $n_{AV;21\text{-}60}$ geschlossen ausfällt. Dieses Ereignis kann nur eintreten, wenn das DH-AV nicht zu einem frühen Anforderungszyklus ausgefallen ist. Die bedingte Wahrscheinlichkeit ist somit gegeben durch:

$$\frac{p_{AV,21\text{-}60} \cdot \pi_{AV,ön}}{1 - p_{AV,\leq 20}} \tag{3.18}$$

Wenn das DH-AV bei der Anforderung $n_{AV;21\text{-}60}$ nicht öffnet, baut sich der Druck weiter auf, so dass im weiteren Unfallablauf das Sicherheitsventil 1 (SiV1) zyklisch angefordert wird. Bei der zyklischen Anforderung des SiV1 ergibt sich die Verzweigungsstruktur, die durch die Verzweigungspunkte **(xiii)** – **(xvii)** in Abb. 3.14 dargestellt sind. Die weitere Erklärung ist analog zur Verzweigung **(iii)** in den Pfad $AV_{\leq 20;ön}$.

Die bedingte Wahrscheinlichkeit, dass das DH-AV im Anforderungszyklus $n_{AV;21\text{-}60}$ nicht geschlossen ausfällt ist gegeben durch:

$$\frac{1 - p_{AV,\leq 20} - p_{AV,21\text{-}60} \cdot \pi_{AV,ön}}{1 - p_{AV,\leq 20}} \tag{3.19}$$

Verzweigungspunkt (vi):

Wenn das DH-AV im Anforderungszyklus $n_{AV;21\text{-}60}$ auslegungsgemäß öffnet, wird Druck abgebaut, so dass das DH-AV wird im weiteren Ablauf zum Schließen angefordert wird. Wenn das DH-AV im Anforderungszyklus $n_{AV;\leq 20}$ zum Schließen angefordert wird, wird der Verzweigungspunkt **(vi)** mit der Verzweigung zum Pfad $AV_{21\text{-}60;sn}$ erzeugt.

Im Pfad $AV_{21\text{-}60;sn}$ wird das Ereignis gerechnet, dass das DH-AV im Anforderungszyklus $n_{AV;21\text{-}60}$ offen versagt. Wenn das offene DH-AV bewirkt, dass der Druck im weiteren Unfallablauf nicht weiter ansteigt, werden SiV1 und SiV2 nicht angefordert. Im extremen Fall, dass das offene Versagen des DH-AV einen weiteren Druckanstieg nicht verhindert, wird im weiteren Ablauf das SiV1 angefordert. Ob SiV1 zum Öffnen angefordert wird oder nicht, hängt in diesem Pfad davon ab, ob der Druck bei offenem DH-AV weiter ansteigt oder nicht. Diese Situation ist in Abb. 3.13 durch SiV1 gekennzeichnet. Die Verzweigungen zu SiV1 in Abb. 3.13 sind analog zu den Verzweigungen **(iii)** – **(vii)** des DH-AV zu interpretieren.

Das Ereignis, dass das DH-AV im Anforderungszyklus $n_{AV;21\text{-}60}$ offen versagt kann nur unter der Bedingung eintreten, dass das DH-AV zuvor geöffnet werden konnte. Die bedingte Wahrscheinlichkeit für das Ereignis wird berechnet durch:

$$\frac{p_{AV,21\text{-}60} \cdot \pi_{AV,sn}}{1 - p_{AV,\leq 20} - p_{AV,21\text{-}60} \cdot \pi_{AV,\ddot{o}n}} \tag{3.20}$$

Die Erfolgswahrscheinlichkeit des Verzweigungspunktes **(vi)** beschreibt die Situation, dass das DH-AV während der ersten 60 Anforderungszyklen weder offen noch geschlossen ausfällt und ist gegeben durch $1 - p_{AV,\leq 20} - p_{AV,21\text{-}60} = p_{AV,>60}$.

Verzweigungspunkt (vii):

Unter der Bedingung, dass das DH-AV die ersten 60 Anforderungszyklen überlebt hat, wird es mit Wahrscheinlichkeit 1 zu irgendeinem zufälligen Anforderungszyklus > 60 ausfallen. Dieser Anforderungszyklus $n_{AV;>60}$ wird aus der bedingten Wahrscheinlichkeitsverteilung des DH-AV für Anforderungszyklen > 60 zufällig ausgespielt.

Wenn die Anzahl der Anforderungen des DH-AV den zufällig ausgespielten Wert $n_{AV,>60}$ bis zum Ende der Rechenzeit nicht erreicht, fällt das DH-AV in dieser Sequenz bis zum

Ende der Rechenzeit nicht aus. Wenn die Anzahl der Anforderungen den Wert $n_{AV,>60}$ innerhalb der Rechenzeit erreicht und das DH-AV zum Öffnen angefordert wird, erzeugt MCDET den Verzweigungspunkt (**vii**). Hier wird die aleatorische Unsicherheit berücksichtigt, dass das DH-AV beim Öffnen versagen oder nicht versagen kann.

Der Pfad $AV_{>60;ön}$ der vom Verzweigungspunkt (**vii**) abzweigt, beschreibt die Situation, dass das DH-AV zum Anforderungszyklus $n_{AV,>60}$ zum Öffnen angefordert wird und geschlossen ausfällt. Die Wahrscheinlichkeit, dass das DH-AV zu einem Anforderungszyklus > 60 geschlossen ausfällt, erfolgt unter der Bedingung, dass das DH-AV die ersten 60 Anforderungszyklen überlebt hat. Die bedingte Wahrscheinlichkeit der Sequenz ist somit gegeben durch:

$$\frac{p_{AV;>60} \cdot \pi_{AV;ön}}{p_{AV;>60}} = \pi_{AV;ön} \tag{3.21}$$

Hat das DH-AV im Verzweigungspunkt (**vii**) geöffnet, wird es kurze Zeit später zum Schließen angefordert, bei der das DH-AV offen versagt. Die Wahrscheinlichkeit dieser Sequenz beträgt $1 - \pi_{AV;ön} = \pi_{AV;sn}$.

Damit sind alle Möglichkeiten, dass das DH-Ventil frühzeitig, mittelfristig oder zu einem späten Anforderungszeitpunkt ausfällt, berücksichtig. Diese Art der Einbindung der aleatorischen Unsicherheit des DH-AV geht davon aus, dass das DH-AV mit Wahrscheinlichkeit 1 zu irgendeinem Anforderungszyklus ausfällt.

Die Verzweigungen bzgl. des SiV1 und SiV2 sind in den Abb. 3.14 und Abb. 3.15 dargestellt und sind analog zu denen des DH-AV von zu interpretieren. Die Abb. 3.13 – Abb. 3.15 geben einen Eindruck, dass die Modellierung, wie die aleatorischen Unsicherheiten bzgl. der DH-Ventile in die MCDET-Analyse eingebunden werden, ein relativ komplexes Verzweigungsmuster ergeben können. Außerdem ist zu betonen, dass jede Sequenz, die in den Abb. 3.13 – Abb. 3.15 skizziert sind, in der MCDET-Analyse gerechnet werden. Jede Sequenz wird dabei mit den entsprechenden Wahrscheinlichkeiten der in der Sequenz aufgetretenen Ereignisse bewertet. Zur Berücksichtigung der zeitlichen Variation bzgl. der frühzeitigen, mittelfristigen und späten Ausfälle der DH-Ventile wird eine Stichprobe von dynamischen Ereignisbäumen erzeugt.

Bzgl. des Ausfallverhaltens der DH-Ventile gehen sowohl epistemische als auch aleatorische Unsicherheiten ein. Für die Erzeugung der benötigten Stichprobenwerte bzgl. der DH-Ventile zur Erzeugung der dynamischen Ereignisbäume wurde ein Programm entwickelt, dessen Vorgehen zur Erzeugung der Stichprobe in den nachfolgenden Schritten erläutert wird.

Schritt 1: Aus den epistemischen Verteilungen der jeweiligen DH-Ventile (vgl. Tab. 3.3 und Tab. 3.6) wird für jeden Ausfallmodus ‚öffnet nicht' und ‚schließt nicht' eine Stichprobe von Zufallswerten vom Umfang n = 50 gezogen. Damit erhalten wir 50 Stichprobenvektoren mit den epistemischen Größen $\mathbf{S_{ep}}$ = ($p_{AV,ön}$ $p_{AV,sn}$, $p_{SV1,ön}$, $p_{SV1,sn}$, $p_{SV2,ön,}$ $p_{SV2,sn,}$ $p_{2v3,ön,}$ $p_{2v3,sn,}$ $p3_{v3,ön}$).

Schritt 2: Unter Verwendung von Gleichung (3.11) wird für jeden Stichprobenvektor $\mathbf{S_{ep}}$ die Wahrscheinlichkeitsverteilungen für das DH-AV, DH-SiV1 und DH-SiV2 erzeugt, dass das jeweilige Ventil zum Anforderungszyklus n , n=1, 2, … ausfällt. Unter Verwendung der erzeugten Wahrscheinlichkeitsverteilungen bzw. der daraus abgeleiteten kumulierten Verteilungsfunktionen können die Wahrscheinlichkeiten $p_{\leq 20,}$ $p_{21\text{-}60,}$ $p_{>60}$ der spezifizierten Versagensklassen bzgl. der jeweiligen DH-Ventile ermittelt werden. Des Weiteren werden für jeden Stichprobenvektor $\mathbf{S_{ep}}$ die bedingten Wahrscheinlichkeitsverteilungen $F_{k;\leq 20|p\leq 20}$, $F_{k;21\text{-}60|p21\text{-}60,}$ $F_{k;>60||\ p>60}$, k = DH-AV, DH-SiV1, DH-SiV2, für die Klassen von Versagenszyklen der jeweiligen DH-Ventile erzeugt.

Schritt 3: Aus jeder der bedingten Wahrscheinlichkeitsverteilungen werden pro epistemischen Vektor zwei Zufallsvektoren der aleatorischen Größen ausgespielt. Die Zufallsvektoren der aleatorischen Größen beinhalten zufällig ausgespielte Werte $n_{k;\leq 20}$, $n_{k;21\text{-}60,}$ $n_{k;>60}$, k = DH-AV, DH-SiV1, DH-SiV2, bei welchem Anforderungszyklus die jeweiligen DH-Ventile in den einzelnen Versagensklassen ausfallen. Für die aus den bedingten Verteilungen zufällig ausgespielten Versagenszyklen werden die entsprechenden Wahrscheinlichkeiten ermittelt, mit der die jeweiligen Ventile im Ausfallmodus ‚öffnet nicht' bzw. ‚schließt nicht' ausfallen.

Schritt 4: Die ausgespielten Werte der aleatorischen und epistemischen Größen werden pro DET in MCDET eingelesen und zur Entwicklung des jeweilig DET sowie zur Berechnung der Sequenzwahrscheinlichkeiten verwendet.

3.4.2 Einbindung der Unsicherheit bzgl. des Schweregrades der Heizrohrschädigung

Um den Einfluss des Schweregrades der Schädigung, den das DE-Heizrohr zu Beginn des Unfallablaufs aufweist, auf das DEHEIRO-Versagen genauer analysieren zu können, sollen in der Analyse sowohl geringe Schädigungen (< 20 %) als auch schwerere Schädigungen (20 – 70 %), in einem DET gemeinsam berücksichtigt werden.

Bei gegebener Zustandsverteilung **Π** = [p_1, p_2, p_3, p_4, p_5] ergibt sich die Wahrscheinlichkeit, dass das Ausmaß der Wandschwächung < 20 % ist, aus der Summe $p_1 + p_2$. Um einen zufälligen Wert < 20% auszuspielen, werden die bedingten Wahrscheinlichkeiten $\frac{p_1}{p_1 + p_2}$ für SK 1 und $\frac{p_2}{p_1 + p_2}$ für SK 2 berechnet.

Der Schädigungswert d_1 einer schwachen Schädigung wird dann aus einer Histogramm-Verteilung zufällig ausgespielt. D. h., der Wert d_1 wird

mit Wahrscheinlichkeit $\frac{p_1}{p_1 + p_2}$ aus U (0, 0.1) der SK 1 und

mit Wahrscheinlichkeit $\frac{p_2}{p_1 + p_2}$ aus U (0.1, 0.2) der SK 2

zufällig ausgespielt.

Analog wird der Zufallswert d_2 einer schweren Schädigung aus der Histogramm-Verteilung ermittelt, wobei d_2

mit Wahrscheinlichkeit $\frac{p_3}{p_3 + p_4 + p_5}$ aus U (0.2, 0.3),

mit Wahrscheinlichkeit $\frac{p_4}{p_3 + p_4 + p_5}$ aus U (0.3, 0.5) und

mit Wahrscheinlichkeit $\frac{p_5}{p_3 + p_4 + p_5}$ aus U (0.5, 0.7)

zufällig ausgespielt wird.

Unter Verwendung der ausgespielten Werte d_1 und d_2 leichter bzw. starker Schädigungen werden die entsprechenden Wanddicken ermittelt und in die GCSM-Signale des Larsson-Miller Modells eingelesen, das im ATHLET-CD Modell implementiert wurde. Außerdem wurden in ATHLET-CD GCSM-Signale eingerichtet, dass während eines Unfallablaufs der Ausfall des Heizrohrs sowohl aufgrund leichter als auch aufgrund starker Schädigung ermittelt werden kann.

Für jede Sequenz, die im Ereignisbaum auftritt und mit ATHLET-CD gerechnet wird, ermittelt das Larsson-Miller Modell, ob und wann das Heizrohr bzgl. der leichten Schädigung d_1 und der starken Schädigung d_2 ausfällt. Erfolgt der Ausfall des Heizrohrs aufgrund der schweren Schädigung d_2 zum Zeitpunkt t_1, so wird eine Verzweigung mit der Wahrscheinlichkeit $p_{20\text{-}70}$ generiert. Dabei ist $p_{20\text{-}70} = p_3 + p_4 + p_5$ aus der Zustandsverteilung $\mathbf{\Pi} = [p_1, p_2, p_3, p_4, p_5]$. Diese Verzweigung ist in Abb. 3.16 skizziert.

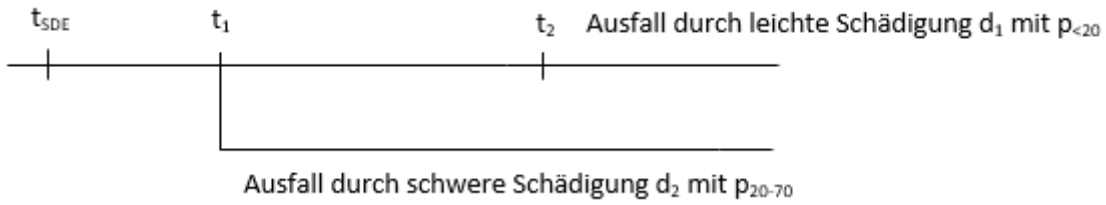


Abb. 3.16 Verzweigung bzgl. DEHEIRO-Versagen aufgrund geringer und starker Schädigung

Aufgrund der Beziehung $p_{<20} + p_{20\text{-}70} = 1$ erhält der bei t_1 oben weiterführende Pfad die Wahrscheinlichkeit $p_{<20}$.In diesem Pfad wird das Heizrohrverhalten bei geringem Schädigungswert d_1 gerechnet und der Zeitpunkt t_2 ermittelt, wann das Heizrohr bei geringer Schädigung d_1 ausfällt. Nach Auftreten eines DEHEIRO-Versagens zum Zeitpunkt t_1 bzw. t_2 werden die Rechnungen der Sequenzen so lange fortgeführt, bis es zum Ausfall der HKL oder der VAL kommt. Kommt es nicht zum Ausfall von HKL bzw. VAL, werden die Rechnungen bis zum Rechenzeitende fortgesetzt.

Die Variabilität der leichten bzw. schweren Schädigungsgrade werden über die Stichprobe der erzeugten DETs mittels Monte-Carlo Simulation aus den oben genannten Histogramm-Verteilungen berücksichtigt. Wie bereits in Abschnitt 3.3.2.3 erwähnt, wurde zur Erzeugung der Stichprobe der Zustandsverteilungen und der zufälligen Schädigungswerte aus den jeweiligen Histogramm-Verteilungen ein entsprechend dafür entwickeltes Programm eingesetzt.

3.4.3 Reduzierung der Rechenzeit durch die Modellierung der Einbindung aleatorischer Unsicherheiten in MCDET

Durch eine geschickte Modellierung, wie die aleatorischen Unsicherheiten in MCDET eingebunden werden, kann eine erhebliche Reduzierung des Rechenaufwandes erreicht werden. Die soll am Beispiel der Einbindung der schweren und leichten Heizrohr-Schädigungen erläutert werden.

Eine Möglichkeit, die aleatorischen Unsicherheiten bzgl. der Schädigungen in MCDET zu modellieren besteht darin, dass zu Beginn des Unfallablaufs bereits eine Verzweigung wie in Abb. 3.17 generiert wird.

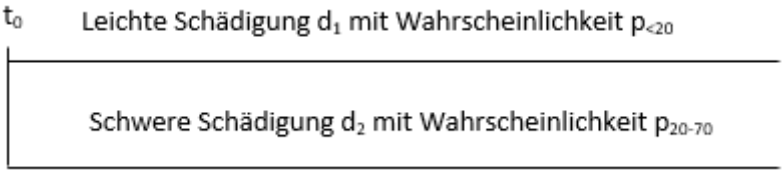


Abb. 3.17 Verzweigung zu Beginn des Unfallablaufs

Bei der Modellierung in Abb. 3.17 wird zu Beginn des Unfallablaufs t_0 ein Verzweigungspunkt mit zwei Alternativen generiert. In der oberen Sequenz wird dem DE-Heizrohr über MCDET eine leichte Schädigung d_1 mit der Wahrscheinlichkeit $p_{<20}$ zugeordnet, in der unteren Sequenz eine schwere Schädigung d_2 mit der Wahrscheinlichkeit p_{20-70}. Die Schädigungsgrade d_1 und d_2 werden aus den entsprechenden Histogramm-Verteilungen ausgespielt, die sich aus den jeweiligen Zustandsverteilungen $\mathbf{\Pi} = [p_1, p_2, p_3, p_4, p_5]$ ergeben.

Mit dieser Modellierung würden für jeden erzeugten DET beide Sequenzen vom Anfang des Unfallablaufs bis zum Zeitpunkt gerechnet werden, bis ein Abbruchkriterium der Analyse erfüllt ist (Erreichen des Rechenzeitendes von 20000 s oder Ausfall der HKL oder Ausfall der VAL). Angenommen jede Sequenz würde bis zum Ende der Rechenzeit gerechnet, dann würden bei dieser Modellierung beide Sequenzen von 0 bis 20000 s gerechnet.

Eine erste Verringerung der Rechenzeit kann damit erreicht werden, wenn angenommen wird, dass das geschädigte Heizrohr erst dann ausfällt, wenn durch die sekundärseitige Druckentlastung eine Erhöhung der Druckdifferenz zwischen Primär- und Sekundärseite erfolgt. Unter dieser Annahme kann die Verzweigung, die in Abb. 3.17 zu Beginn des Unfallablaufs erfolgt, zum Zeitpunkt t_{SDE} gesetzt werden, zu dem die Prozesskriterien für das sekundärseitige Druckentlasten anstehen. Diese Verzweigung ist in Abb. 3.18 dargestellt.

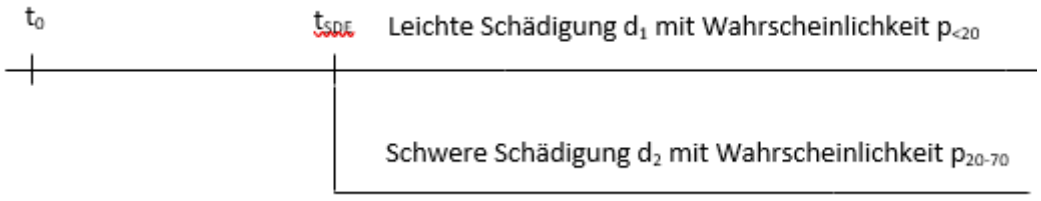


Abb. 3.18 Verzweigung zum Zeitpunkt t_{SDE}

Bei dieser Modellierung wird die obere Sequenz vom Zeitpunkt t_0 bis t_{SDE} gerechnet. Zum Zeitpunkt t_{SDE} wird durch MCDET die Verzweigung generiert. Die obere Sequenz rechnet von t_{SDE} weiter bis zum Ende der Rechenzeit. Ebenso wird die untere Sequenz von t_{SDE} bis zum Rechenzeitende gerechnet. D. h., durch die Verschiebung des Zeitpunktes, wann der Verzweigungspunkt gesetzt wird, erspart man sich in der unteren Sequenz die Rechnung von t_0 bis t_{SDE}. Angenommen t_{SDE} würde bei 5000 s anstehen, würde man sich mit dieser Modellierung für jeden DET eine Rechnung über 5000 s ersparen. Bei einer Stichprobe von 100 DETs würde man sich bei dieser Modellierung Rechnungen über 500000 s der Problemzeit ersparen.

Eine etwas komplizierte Modellierung, die schließlich in der Analyse umgesetzt wurde, besteht darin, dass der Zeitpunkt der Verzweigung noch weiter nach hinten verschoben wird. Dazu musste ATHLET-CD so eingerichtet werden, dass während eines Unfallablaufs der Ausfall des Heizrohrs sowohl aufgrund der leichten Schädigung als auch aufgrund der starken Schädigung über entsprechende GCSM-Signale ermittelt wird. In diesem Fall, der in Abb. 3.16 skizziert ist, wird zum Zeitpunkt t_{SDE} in ATHLET-CD sowohl der Wert d_1 der leichten als auch der Wert d_2 der schweren Schädigung durch MCDET eingelesen. Damit wird kann in dem gleichen Rechenlauf sowohl der Ausfall des DE-Heizrohrs aufgrund einer leichten als auch aufgrund der starken Schädigung ermittelt werden. Die Verzweigung zum Zeitpunkt t_1, bedeutet hier im Gegensatz zu den Abb. 3.17 und Abb. 3.18 nicht, dass ab t_1 zwei unterschiedliche Sequenzen gerechnet werden. In diesem Fall werden die Ausfallzeitpunkte t_1 und t_2 im Rahmen der gleichen Sequenz berechnet. Die Verzweigung in Abb. 3.16 dient ausschließlich dazu, dass dem Ausfall aufgrund schwerer bzw. leichter Schädigung die entsprechenden Wahrscheinlichkeiten korrekt zugeordnet werden. Dadurch, dass nur eine Sequenz gerechnet werden muss, um die Ausfallzeiten t_1 und t_2 zu ermitteln, erspart man sich die Berechnung einer zweiten Sequenz. Bei einer Stichprobe von 100 DETs resultiert dies in einer Verringerung der Rechnungen von 100 Sequenzen.

Diese Art der Modellierung konnte hier nur deshalb durchgeführt werden, da angenommen wurde, dass der Ausfall des DE-Heizrohrs keinen Einfluss auf den nachfolgenden Ausfall der HKL bzw. VAL hat. Andernfalls hätte man bei t_1 eine Verzweigung erzeugt, ab der nachfolgend zwei getrennte Sequenzen gerechnet werden, um den Einfluss des DEHEIRO-Versagens auf den Ausfall der HKL bzw. VAL zu berücksichtigen.

Die aufgeführten Beispiele sollten veranschaulichen, dass durch eine geschickte Modellierung von MCDET, wie die aleatorischen Unsicherheiten in die Analyse eingebunden werden, eine erhebliche Reduzierung des Rechenaufwandes erzielt werden kann.

3.5 Ergebnisse der MCDET/ATHLET-CD Analyse zum DE-Heizrohrversagen

In Abschnitt 3.5.1 wird auf die Durchführung der MCDET/ATHLET-CD Analyse eingegangen. Abschnitt 3.5.2 beschreibt die Ergebnisse der Analyse anhand einiger ausgewählter Beispiele.

3.5.1 Durchführung der Analyse

Für die Durchführung der Analyse wurde MCDET mit ATHLET-CD gekoppelt, um die Variabilität des Systemverhaltens unter Berücksichtigung der definierten Unsicherheiten zu ermitteln. Der Ablauf der Berechnungen sowie die Kommunikation zwischen MCDET und ATHLET-CD wurden unter Verwendung des neu entwickelten MCDET-Schedulers gesteuert. Der neue MCDET-Scheduler erlaubt dabei die parallele Abarbeitung von alternativen Sequenzen sowie die optimale Verteilung der Rechnungen auf verfügbare Rechenknoten. Damit können die zur Verfügung stehenden Kapazitäten optimal ausgenutzt werden.

Um eine nachträgliche Trennung zwischen epistemischen und aleatorischen Unsicherheiten und damit eine approximative Unsicherheitsanalyse durchführen zu können, wurden zur Erzeugung der Stichprobe pro epistemischem Vektor zwei Zufallsvektoren der aleatorischen Größen über Monte Caro Simulation ausgespielt. Der Erzeugung von zwei DETs liegen somit die gleichen Werte der epistemischen Größen, jedoch unterschiedliche Werte der aleatorischen Größen zugrunde.

Insgesamt wurde eine Stichprobe von 100 DETs erzeugt. D.h., für jeden der 50 Vektoren der epistemischen Größen liegen zwei unterschiedliche Vektoren bzgl. der aleatorischen Größen vor. Die Anzahl der gerechneten Pfade (Sequenzen) in den verschiedenen DETs variiert zwischen 25 und 85. Allein daraus ist der Einfluss erkennbar, den die Unsicherheiten auf das Systemverhalten haben, das durch die erzeugten Sequenzen der jeweiligen DETs beschrieben wird.

Gleichung (3.22) beschreibt die Beziehung zwischen den erzeugten DETs in Abhängigkeit der aleatorischen und epistemischen Variablen:

$$DET_{ij} = DET(\ \mathbf{A}^{*};\ \mathbf{E_i};\ \mathbf{A_j} \mid \mathbf{E_i}\ ),\ \ i=1,\ldots 50\ ,\ j=1,2 \qquad (3.22)$$

dabei beschreiben

A* – aleatorische Größen die im Rahmen der dynamischen Ereignisbaummethode behandelt werden.

$\mathbf{E_i}$ – Vektor i der Werte, die aus den Verteilungen der epistemischen Größen zufällig ausgespielt wurden, i=1, …, 50.

$\mathbf{A_j} \mid \mathbf{E_i}$ – Vektor j, j=1,2 der Werte, die aus den Wahrscheinlichkeitsverteilungen der aleatorischen Größen unter der Bedingung des epistemischen Vektors ep_i zufällig ausgespielt wurden.

Die Struktur der Daten der epistemischen und aleatorischen Größen, die der Erzeugung der 100 DETs zugrunde liegen, ist in Abb. 3.19 skizziert.

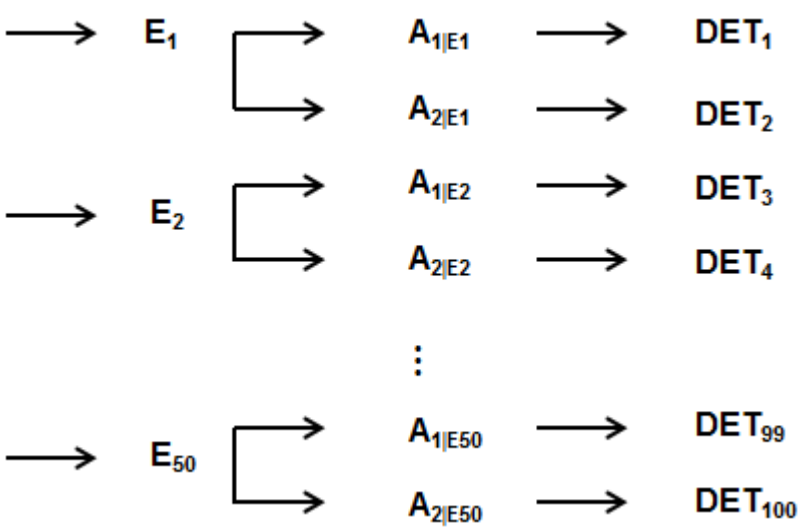


Abb. 3.19 Eingabestruktur der aleatorischen und epistemischen Daten zur Erzeugung der Stichprobe der DETs

Es ist zu beachten, dass alle aleatorischen Vektoren untereinander verschieden sind, d. h. $A_{1|E1} \neq A_{1|E2} \neq \cdots \neq A_{1|E50} \neq A_{2|E1} \neq A_{2|E2} \neq \cdots \neq A_{2|E50}$.

Bei der Berechnung der Sequenzen wurden folgende Abbruchkriterien verwendet:

- Als Rechenzeitende wurden 20000 s (~ 5.6 Stunden) der Problemzeit festgelegt.
- Die Berechnung einer Sequenz wird beendet, wenn entweder die Hauptkühlmittelleitung (HKL) oder die Volumenausgleichsleitung (VAL) versagt.

Wenn das DE-Heizrohr vor der HKL oder VAL versagt wird die Berechnung zunächst weitergeführt. Versagt die HKL und VAL nicht, wird die Berechnung bis zum Rechenzeitende (20000 s) fortgesetzt. Versagt HKL oder VAL nach dem DE-Heizrohr, wird die Berechnung der Sequenz zum jeweiligen Ausfallzeitpunkt beendet.

Versagt die HKL oder VAL vor dem DE-Heizrohr, wird die Berechnung der Sequenz beendet, da der hohe Druck im Primärkreis infolge des Bruches abgesenkt wird.

3.5.2 Darstellung ausgewählter Ergebnisse

Das Ergebnis der gekoppelten MCDET/ATHLET-CD Analyse hat ein Datenvolumen von mehreren Terabyte erzeugt, das statistisch ausgewertet werden kann. Dazu wurde ein fortschrittliches Konzept zur Speicherung der Daten im HDF5-Format umgesetzt, das in

wissenschaftlichen Anwendungen für die Speicherung derartiger Datenmengen verwendet wird. Damit werden eine effiziente Speicherung und ein effizienter Zugriff des umfangreichen Datenmaterials ermöglicht. Zur Darstellung und Auswertung der Ergebnisse, die unter Verwendung der MCDET/ATHLET-CD Analyse zum DE-Heizrohrversagen (DEHEIRO-Versagen) erzeugt wurden, sind entsprechende Postprocessing Programme entwickelt worden. Da die vorliegende Datenmenge die statistische Auswertung vieler unterschiedlicher Fragestellungen erlaubt, soll im Folgenden anhand einiger Beispiele demonstriert werden, welche probabilistischen Aussagen aus einer IDPSA unter Verwendung von MCDET erzeugt werden können.

In der erzeugten Stichprobe von 100 DETs wurden insgesamt 4216 Unfallsequenzen unter unterschiedlichen Bedingungen gerechnet. Für jede einzelne gerechnete Sequenz liegt neben dem zeitlichen Verlauf der ATHLET-Prozessgrößen die zusätzliche Information vor, welche Zufallsereignisse und epistemischen Werte dem Verlauf zugrunde liegen und mit welcher Wahrscheinlichkeit die jeweilige Sequenz eintritt.

Eine Annahme der Analyse bestand darin, dass das DE-Heizrohr zu Beginn des Unfallablaufs eine Schädigung aufweist, die zwischen 1 % und 70 % liegt. Dazu wurde in Abschnitt 3.3.2.3 ein Wahrscheinlichkeitsmodell hergeleitet, mit dem die Wahrscheinlichkeit berechnet werden kann, dass zu Beginn des Unfallszenarios eine schwache (< 20 %) bzw. eine starke Schädigung (20 – 70 %) vorliegt. In das Modell zur Schätzung der Heizrohrschädigung gehen sowohl aleatorische als auch epistemische Unsicherheiten ein. Daraus ergibt sich, dass für jeden der erzeugten 100 DETs eine unterschiedliche Wahrscheinlichkeit bzgl. einer schwachen bzw. starken Schädigung vorliegt. Die Wahrscheinlichkeitsverteilung für das Ausmaß der Schädigung zu Beginn des Unfallablaufs ist in Tab. 3.11 angegeben.

Tab. 3.11 Wahrscheinlichkeitsverteilung für das Ausmaß der Schädigung zu Beginn des Unfallablaufs

Ausmaß der Schädigung (%)	Wahrschein-lichkeit	Schädigungs-grad	Wahrschein-lichkeit
< 10	0.456	< 20 %	0.98
10 - 20	0.524		
20 - 30	5.2E-03	20 % – 70 %	0.02
30 - 40	3.9E-03		
40 - 50	2.4E-03		
50 - 70	8.E-03		

Die Werte in Tab. 3.11 zeigen, dass die Wahrscheinlichkeit, dass eine starke Schädigung (20 – 70%) zu Beginn des Unfallablaufs vorliegt, mit ca. 0.02 erheblich geringer ist als die einer schwachen Schädigung (< 20 %), die mit der Wahrscheinlichkeit von ca. 0.98 vorkommt. Die in Tab. 3.11 angegebenen Werte sind die mittleren Wahrscheinlichkeiten der Schädigungen, die sich unter Berücksichtigung der epistemischen und aleatorischen Unsicherheiten, die in das Wahrscheinlichkeitsmodell eingegangen sind, ergeben haben.

Im Weiteren interessiert die Frage, mit welcher Wahrscheinlichkeit ein DEHEIRO-Versagen in Rahmen der gerechneten Unfallabläufe aufgetreten ist. Dazu sind in Tab. 3.12 die mittleren Wahrscheinlichkeiten und zugehörigen 95 % bzw. 99 %-Konfidenzintervalle angegeben, mit denen es unter den extremen Bedingungen des zugrunde gelegten Unfallszenarios zu einem DEHEIRO-Versagen kommt. Zusätzlich werden die mittleren Wahrscheinlichkeiten angegeben, mit der es zu einer starken bzw. schwachen Schädigung und nachfolgendem DEHEIRO-Versagen kommt. Die mittleren Wahrscheinlichkeiten ergeben sich aus dem Mittelwert der jeweiligen Wahrscheinlichkeiten der 100 erzeugten DETs.

Tab. 3.12 Mittlere Wahrscheinlichkeit für DEHEIRO-Versagen

DEHEIRO-Versagen		
Mittlere Wahrscheinlichkeit	StdAbw	95% - KI 99% - KI
9.79E-01	3.42E-02	(9.72E-01 , 9.86E-01) (9.70E-01 , 9.88E-01)
Starke Schädigung (20-70%) und DEHEIRO-Versagen		
Mittlere Wahrscheinlichkeit	StdAbw	95% - KI 99% - KI
1.82E-02	2.332E-02	(1.36E-02 , 2.28E-02) (1.21E-01 , 2.43E-02)
Schwache Schädigung (<20%) und DEHEIRO-Versagen		
Mittlere Wahrscheinlichkeit	StdAbw	95% - KI 99% - KI
9.61E-01	4.24E-02	(9.53E-01 , 9.69E-01) (9.49E-01 , 9.72E-01)
Kein DEHEIRO-Versagen		
Mittlere Wahrscheinlichkeit	StdAbw	95% - KI 99% - KI
2.09E-02	3.42E-02	(1.41E-02 , 2.77E-02) (1.19E-02 , 2.98E-02)

Unter den extremen Bedingungen (Hochdruck-Unfallszenario sowie Schädigung des DE-Heizrohrs zu Beginn des Unfallablaufs), die für die Analyse angenommen wurden, tritt ein DEHEIRO-Versagen mit einer sehr hohen Wahrscheinlichkeit von ca. 98 % (s. Tab. 3.12) auf. Die mittlere Wahrscheinlichkeit, dass unter den angenommenen Bedingungen kein DEHEIRO-Versagen auftritt, beträgt lediglich 2.1 %.

Die Wahrscheinlichkeit, dass das DE-Heizrohr stark geschädigt ist und versagt, ist mit 1.82E-2 deshalb so gering, da die Wahrscheinlichkeit, dass das DE-Heizrohr zu Beginn des Unfallablaufs eine starke Schädigung aufweist, lediglich 1.83E-02 beträgt. Bemerkenswert ist allerdings, dass die Wahrscheinlichkeit einer schwachen Schädigung und nachfolgendem DEHEIRO-Versagen mit ca. 0.96 sehr hoch ist. D. h., auch bei lediglich schwachen Schädigungen, die das Heizrohr zu Beginn des Unfallablaufs aufweist, kommt es aufgrund der hohen Belastungen mit hoher Wahrscheinlichkeit zu einem DEHEIRO-Versagen.

Aufgrund der in der Analyse berücksichtigten epistemischen Unsicherheiten der Parameter des ATHLET-CD-Modells (s. Abschnitt 3.3.1) sowie der epistemischen Unsicherheiten bzgl. der Zuverlässigkeitskenngrößen in den hergeleiteten Wahrscheinlichkeitsmodellen (s. Abschnitt 3.3.2.2 und 3.3.2.3) erhält man für jeden epistemischen Vektor eine bestimmte Wahrscheinlichkeit für das Heizrohrversagen. Die Verteilung der Heizrohr-Versagenswahrscheinlichkeit bzgl. der 50 epistemischen Vektoren ist in Abb. 3.20 dargestellt.

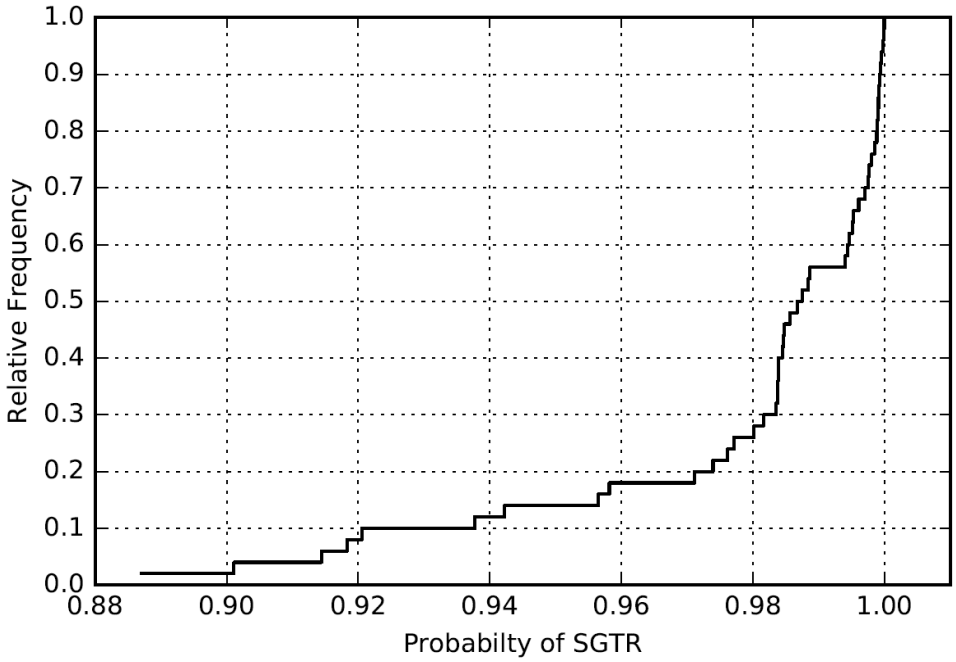


Abb. 3.20 Epistemische Unsicherheit des DE-Heizrohrversagens

Abb. 3.20 zeigt, dass die Versagenswahrscheinlichkeit des Heizrohrs für die epistemischen Rechnungen zwischen 0.88 und 1.0 variiert. Diese durchweg hohen Versagenswahrscheinlichkeiten lassen sich durch die extremen Bedingungen erklären, die der Analyse zugrunde liegen. Das sind zum einen das angenommene und über längere Zeit anhaltende Hochdruck-Unfallszenario und zum anderen, dass jedem gerechneten Szenario ein mehr oder weniger geschädigtes Heizrohr zugrunde liegt. Die relative Häufigkeit der y-Achse bezieht sich auf die 50 epistemischen Rechnungen. Die Verteilung in Abb. 3.20 beschreibt somit die Variation der Wahrscheinlichkeit für das DEHEIRO-Versagen bzgl. der 50 epistemischen Vektorwerte, die den Rechnungen zugrunde liegen. Mit der Verteilung in Abb. 3.20 wird somit die Aussagesicherheit zur Wahrscheinlichkeit des DEHEIRO-Versagens aufgrund der in der Analyse berücksichtigten epistemischen Unsicherheiten beschrieben. Aus der Verteilung kann z. B. abgelesen werden, dass mit einer Aussagesicherheit von ca. 10 % die Wahrscheinlichkeit eines DEHEIRO-

Versagens zwischen 0.88 und 0.92 liegt. Mit einer Aussagesicherheit von ca. 72 % liegt die Wahrscheinlichkeit eines DEHEIRO-Versagens über 0.98.

Um zu untersuchen, ob sich die Wahrscheinlichkeit eines thermisch-induzierten DE-Heizrohrlecks in einem Hochdruck-Unfallszenario zwischen schwacher und starker Schädigung unterscheiden, werden in Abb. 3.21 die bedingten Wahrscheinlichkeiten eines DE-Heizrohrlecks unter der Bedingung einer schwachen Schädigung (< 20 %) bzw. unter der einer starken Schädigung (> 20 %) dargestellt.

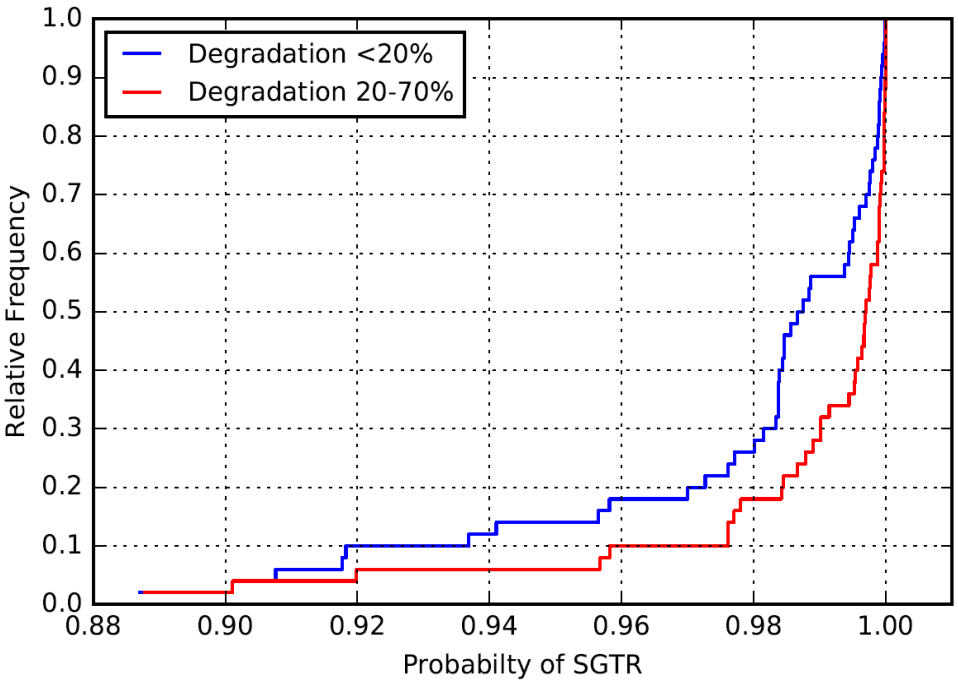


Abb. 3.21 Epistemische Unsicherheit der Wahrscheinlichkeit des Heizrohrversagens unter der Bedingung einer starken bzw. schwachen Schädigung

Wie Abb. 3.21 zeigt, ist die Verteilung der Versagenswahrscheinlichkeit unter der Bedingung starker Schädigungen zu geringfügig größeren Werten hin verschoben (rote Kurve). Auffallend ist jedoch, dass sich nicht nur bei den starken Schädigungen, sondern auch bei schwachen Schädigungen ähnlich hohe Wahrscheinlichkeiten für das Heizrohrversagen ergeben. Die Verteilung in Abb. 3.20 ergibt sich aus dem gewichteten Mittel der bedingten Verteilungen in Abb. 3.21. Da die Wahrscheinlichkeit einer schwachen Schädigung sehr viel höher ist als die einer starken Schädigung (s. Tab. 3.11), trägt die bedingte Verteilung der schwachen Schädigung im Wesentlichen zur Gesamtverteilung bei. Dies ist die Erklärung, dass sich die Verteilung in Abb. 3.20 und die bedingte Verteilung bzgl. der schwachen Schädigungen in Abb. 3.21 kaum unterscheiden.

Da sich bzgl. der starken und schwachen Schädigungen gleichermaßen hohe DEHEIRO-Versagenswahrscheinlichkeiten zeigen, soll im Folgenden für beide Gruppen untersucht werden, wann es zu einem DEHEIRO-Versagen kommt. Abb. 3.22 zeigt die bedingten Wahrscheinlichkeitsverteilungen, wann es zum Versagen des DE-Heizrohrs unter der Bedingung schwacher bzw. starker Schädigungen kommt.

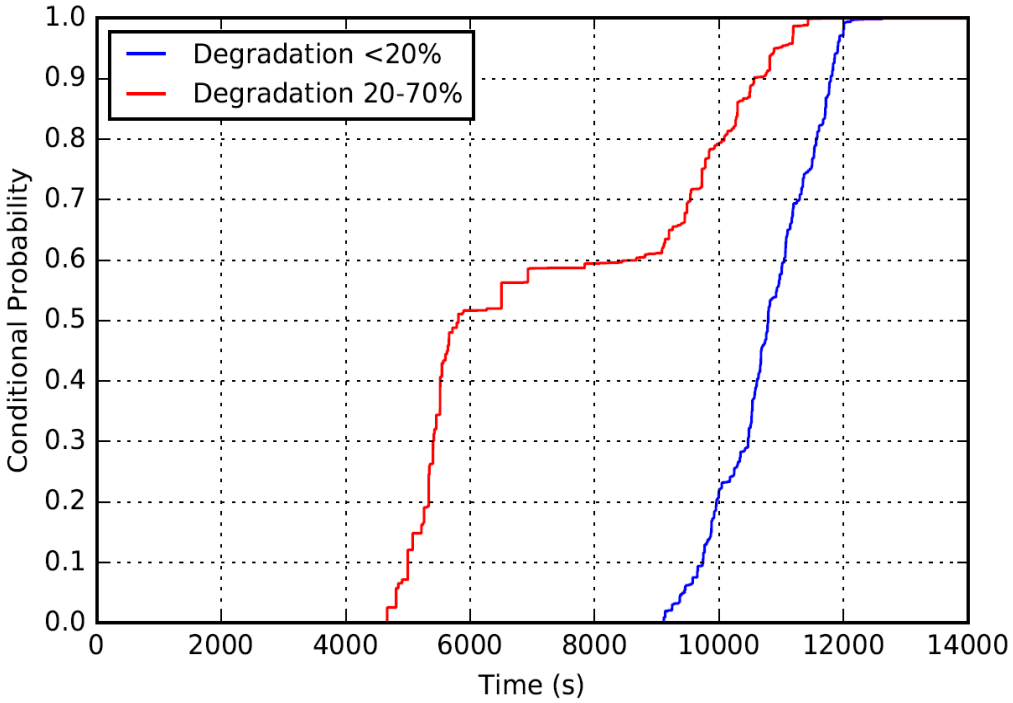


Abb. 3.22 Bedingte Verteilung des Versagenszeitpunktes bzgl. starker und schwacher Schädigungen des DE-Heizrohrs

Jede der in Abb. 3.22 dargestellten bedingten Verteilungen resultiert aus der Mischung (Mittelung) der einzelnen Verteilungen, die sich für die jeweiligen 100 DETs ergeben haben. Die Verteilungen beschreiben den gemeinsamen Einfluss der epistemischen und aleatorischen Unsicherheiten. Abb. 3.22 zeigt, dass Heizrohre mit starken Schädigungen früher versagen als diejenigen, die eine Schädigung < 20 % aufweisen. Während Heizrohre mit schwacher Schädigung mit 99%iger Wahrscheinlichkeit erst später als 2.5 h nach dem einleitenden Ereignis versagen, beträgt die Wahrscheinlichkeit ca. 60 %, dass die Heizrohre mit starker Schädigung zwischen 1.2 und 2 h nach Eintritt des einleitenden Ereignisses versagen. Späte Versagenszeiten, die z. B. zwischen 3 h und 4.5 h nach dem einleitenden Ereignis auftreten, kommen bei schwachen Schädigungen mit einer Wahrscheinlichkeit von ca. 48 %, bei starken Schädigungen jedoch nur mit einer Wahrscheinlichkeit von ca. 9 % vor. Entsprechend kann man aus den bedingten

Verteilungen in Abb. 3.22 die in Tab. 3.13 aufgeführten Wahrscheinlichkeiten dafür berechnen, dass das Heizrohr in bestimmten Zeitintervallen versagt.

Tab. 3.13 Wahrscheinlichkeit für DEHEIRO-Versagen in bestimmten Zeitintervallen

Versagenszeit (nach einleitendem Ereignis)	Wahrscheinlichkeit Schädigung	
	< 20%	20-70%
4600 s – 7200 s (1.2 h – 2 h)	0	0.587
7200 s – 9000 s (2 h – 2.5 h)	2.9E-05	2.6E-02
9000 s – 10800 s (2.5 h – 3 h)	0.522	0.305
10800 s – 12600 s (3 h – 3.5 h)	0.477	8.15E-2
12600 s – 16200 s (3.5 h – 4.5 h)	6.0E-04	4.3E-04

Alle bisher erwähnten DEHEIRO-Versagenswahrscheinlichkeiten beziehen sich auf Situationen, in denen das DE-Heizrohr vor der Hauptkühlmittelleitung und vor der Volumenausgleichsleitung ausgefallen ist. Demzufolge ist die Wahrscheinlichkeit sehr hoch, dass ein DEHEIRO-Leck vor dem Versagen der HKL oder VAL auftritt. Da bei einem Ausfall des DE-Heizrohrs das Containment umgangen wird, ist damit auch eine hohe Wahrscheinlichkeit gegeben, dass radioaktive Stoffe vom Primärkreis in die Umgebung freigesetzt werden. Wenn die HKL oder VAL nach dem Versagen des Heizrohrs zusätzlich versagt, erfolgt auch eine Freisetzung in den Sicherheitsbehälter. Unter diesem Aspekt ist die Frage von Interesse, ob nach dem DEHEIRO-Versagen zusätzlich die HKL oder VAL versagt und wenn ja, wieviel Zeit bis dahin vergeht.

In Tab. 3.14 sind die mittleren Wahrscheinlichkeiten und zugehörigen 95 % bzw. 99 %-Konfidenzintervalle angegeben, mit denen ein Bruch der HKL oder VAL auftritt, bevor oder nachdem es zu einem DHEIRO-Versagen kommt. Die mittleren Wahrscheinlichkeiten werden aus dem Mittelwert der jeweiligen Wahrscheinlichkeiten der 100 erzeugten DETs ermittelt.

Tab. 3.14 Wahrscheinlichkeiten und Konfidenzintervalle für ein Versagen der HKL bzw. VAL vor bzw. nach DEHEIRO-Versagen

Versagen HKL vor DEHEIRO-Versagen		
Mittlere Wahrscheinlichkeit	**StdAbw**	**95% - KI** **99% - KI**
1.06E-02	2.08E-02	(6.51E-03 , 1.48E-02) (5.17E-03 , 1.61E-02)
Versagen VAL vor DEHEIRO-Versagen		
Mittlere Wahrscheinlichkeit	**StdAbw**	**95% - KI** **99% - KI**
3.38E-03	2.12E-02	(0 , 7.59E-03) (0 , 8.96E-03)
Versagen HKL nach DEHEIRO-Versagen		
Mittlere Wahrscheinlichkeit	**StdAbw**	**95% - KI** **99% - KI**
7.05E-01	3.54E-01	(6.35E-01 , 7.75E-01) (6.12E-01 , 7.98E-01)
Versagen VAL nach DEHEIRO-Versagen		
Mittlere Wahrscheinlichkeit	**StdAbw**	**95% - KI** **99% - KI**
4.35E-04	2.73E-03	(0. , 9.77E-04) (0. , 1.15E-03)
Kein HKL oder VAL Versagen nach DEHEIRO-Versagen		
Mittlere Wahrscheinlichkeit	**StdAbw**	**95% - KI** **99% - KI**
1.18E-02	2.04E-02	(7.78E-03 , 1.59E-02) (6.47E-03 , 1.72E-02)
Kein HKL oder VAL Versagen		
Mittlere Wahrscheinlichkeit	**StdAbw**	**95% - KI** **99% - KI**
2.8E-01	3.57E-01	(2.09E-01 , 3.51E-01) (1.87E-01 , 3.74E-01)

Die Wahrscheinlichkeiten in Tab. 3.14 sind nicht als bedingte Wahrscheinlichkeiten, sondern als die Wahrscheinlichkeiten des gemeinsamen Auftretens der jeweiligen Ereignisse zu interpretieren. So ist z. B. die Wahrscheinlichkeit von 0.705 für ein Versagen der HKL nach DEHEIRO-Versagen die Wahrscheinlichkeit des Ereignisses, dass ein DEHEIRO-Versagen auftritt und im weiteren Unfallablauf ein Bruch der HKL erfolgt. Die Ergebnisse in Tab. 3.14 zeigen, dass mit einer relativ hohen bedingten Wahrscheinlichkeit von ca. 71 % ein Bruch der HKL auftritt, nachdem es zu einem DEHEIRO-Versagen gekommen ist. Dagegen kommt es nach einem DEHEIRO-Versagen nur sehr selten zu einem zusätzlichen Bruch der VAL. Die mittlere Wahrscheinlichkeit dafür beträgt ca. 4.E-04. D. h., wenn es nach einem DEHEIRO-Versagen zu einem zusätzlichen

Bruch einer der beiden Leitungen kommt, dann wird dies mit 99.9%iger Wahrscheinlichkeit ein Bruch der HKL sein. Die mittleren Wahrscheinlichkeiten, dass ein Bruch der HKL bzw. VAL auftritt, bevor es zum DEHEIRO-Versagen kommt, sind mit 1.06E-02 bzw. 3.38E-03 eher gering. Von der gleichen Größenordnung ist die mittlere Wahrscheinlichkeit (1.18E-02), dass es nach dem DEHEIRO-Versagen zu keinem zusätzlichen Bruch der HKL oder VAL kommt. Die mittlere Wahrscheinlichkeit, dass es unabhängig vom Ausfall des DE-Heizrohrs weder zu einem Bruch der HKL noch einem Ausfall der VAL kommt beträgt ca. 0.28.

In Tab. 3.14 wurde die Wahrscheinlichkeit von 0.705 angegeben, dass ein Bruch der HKL nach einem DEHEIRO-Versagen auftritt. Dieses Ereignis tritt in Verbindung mit einer starken Schädigung des Heizrohrs mit einer Wahrscheinlichkeit von 6.4E-3 und in Verbindung mit einer schwachen Schädigung des Heizrohrs mit einer Wahrscheinlichkeit von 0.699 auf. Diese großen Unterschiede in den Wahrscheinlichkeiten ergeben sich dadurch, dass das Heizrohr zu Beginn des Unfallablaufs mit einer wesentlich geringeren Wahrscheinlichkeit eine starke als eine schwache Schädigung aufweist (s. Tab. 3.11).

Da in Tab. 3.12 die Wahrscheinlichkeit gegeben ist, mit der ein DEHEIRO-Versagen eintritt, können auch verschiedene bedingte Wahrscheinlichkeiten ermittelt werden. Zum Beispiel die bedingte Wahrscheinlichkeit, dass kein Bruch der HKL oder VAL unter der Bedingung eintritt, dass das DE-Heizrohrs vorher versagt hat. Die bedingte Wahrscheinlichkeit kann durch folgende Rechnung ermittelt werden:

P (Kein Ausfall der HKL oder VAL | DEHEIRO versagt) =

$$\frac{\mathrm{P(Kein\ Ausfall\ der\ HKL\ oder\ VAL\ \ nach\ DEHEIRO-Versagen\ )}}{\mathrm{P\ (DEHEIRO\ versagt)}}$$

= 1.18E-02 / 0.979 = 1.205E-02

Die bedingte Wahrscheinlichkeit weicht kaum von dem Wert der unbedingten Wahrscheinlichkeit in Tab. 3.14 ab, da die Wahrscheinlichkeit der Bedingung, dass das DE-Heizrohr versagt, mit 0.979 sehr groß ist.

Wie zuvor bereits diskutiert, kann durch einen Bruch der HKL oder VAL, der nach dem Versagen des Heizrohrs auftritt, die Freisetzung radioaktiver Stoffe in die Umgebung reduziert werden. Das Ausmaß der Reduktion wird dabei von der Zeitspanne zwischen

DEHEIRO-Versagen und dem nachfolgenden Bruch der jeweiligen Leitung abhängen. Je kürzer die Zeitspanne, desto geringer die Freisetzung über das Dampferzeugerheizrohrleck. Die Ergebnisse aus der MCDET/ATHLET-CD Analyse erlauben es, die Zeitspanne zwischen DEHEIRO-Versagen und nachfolgendem Bruch der jeweiligen Leitungen probabilistisch auszuwerten. Da der nachfolgende Bruch der VAL aufgrund seiner geringen Wahrscheinlichkeit (s. Tab. 3.14) eher geringe Bedeutung hat, wird in Abb. 3.23 die bedingte Verteilung der Zeitspanne zwischen DEHEIRO-Versagen und Bruch der HKL unter der Bedingung einer schwachen und starken Schädigung dargestellt.

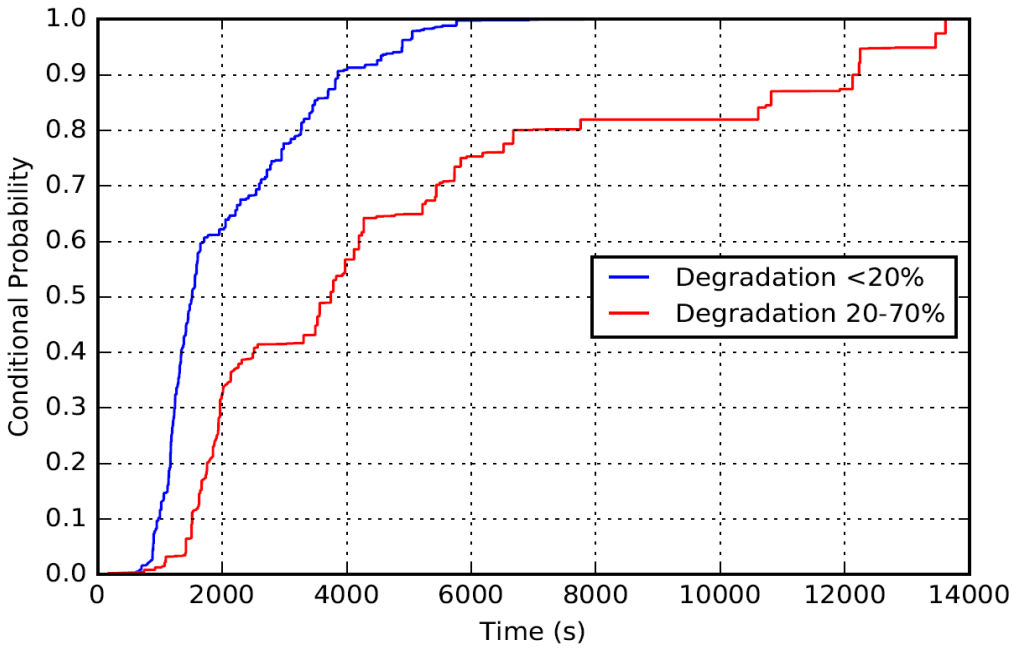


Abb. 3.23 Bedingte Verteilung der Zeit zwischen DEHEIRO-Versagen und Bruch der HKL in Abhängigkeit des Schädigungsgrades

Die bedingten Verteilungen in Abb. 3.23 zeigen, dass die Zeitspannen zwischen Ausfall des DE-Heizrohrs mit schwacher Schädigung und HKL-Bruch deutlich kürzer sind als die Zeitspannen bzgl. des DE-Heizrohrs mit starken Schädigungen. Dies war zu erwarten, da das schwach geschädigte Heizrohr deutlich später ausfällt als das Heizrohr mit starken Schädigungen (s. Abb. 3.22).

Bei einem gegebenen Ausfall des schwach geschädigten Heizrohrs erfolgt der Bruch der HKL mit einer Wahrscheinlichkeit von ca. 54 % innerhalb 15 und 30 min nach dem Versagen des Heizrohrs, mit einer Wahrscheinlichkeit von ca. 25 % zwischen 30 und 60 min und mit einer Wahrscheinlichkeit von ca. 12 % zwischen 60 und 90 min. Kürzere

Zeitspannen als 15 min treten mit einer Wahrscheinlichkeit von 7 % und längere Zeitspannen von 90 – 130 min mit einer Wahrscheinlichkeit von ca. 2 % auf.

Bei gegebenem Ausfall des stark geschädigten Heizrohrs erfolgt der Bruch der HKL mit einer Wahrscheinlichkeit von ca. 20 % innerhalb 15 und 30 min nach dem Versagen des Heizrohrs, mit einer Wahrscheinlichkeit von ca. 28.3 % zwischen 30 und 60 min und mit einer Wahrscheinlichkeit von ca. 18 % zwischen 60 und 90 min. Kürzere Zeitspannen als 15 min treten kaum auf (0.8 %). Längere Zeitspannen von 90 – 240 min kommen hier allerdings mit einer erheblich höheren Wahrscheinlichkeit von ca. 33 % vor.

Obwohl ein Bruch der VAL nur mit einer geringen Wahrscheinlichkeit von 3.81E-03 auftritt, darf dies nicht darüber hinwegtäuschen, dass in der Analyse nicht wenige Sequenzen gerechnet wurden, bei denen ein Bruch der VAL aufgetreten ist. Dies wird aus Abb. 3.24 und Abb. 3.25 deutlich, in denen der Druck- und Temperaturverlauf in der Volumenausgleichsleitung für alle diejenigen Sequenzen dargestellt wird, bei denen es zu einem Bruch der VAL gekommen ist. Die geringe Wahrscheinlichkeit für einen Bruch der VAL ergibt sich daraus, dass jede der in Abb. 3.24 und Abb. 3.25 dargestellten Sequenzen eine sehr kleine Eintrittswahrscheinlichkeit aufweist. D. h., die Summe der Eintrittswahrscheinlichkeiten aller dargestellten Sequenzen, bei denen ein Bruch der VAL aufgetreten ist, summieren sich auf die Wahrscheinlichkeit 3.81E-3.

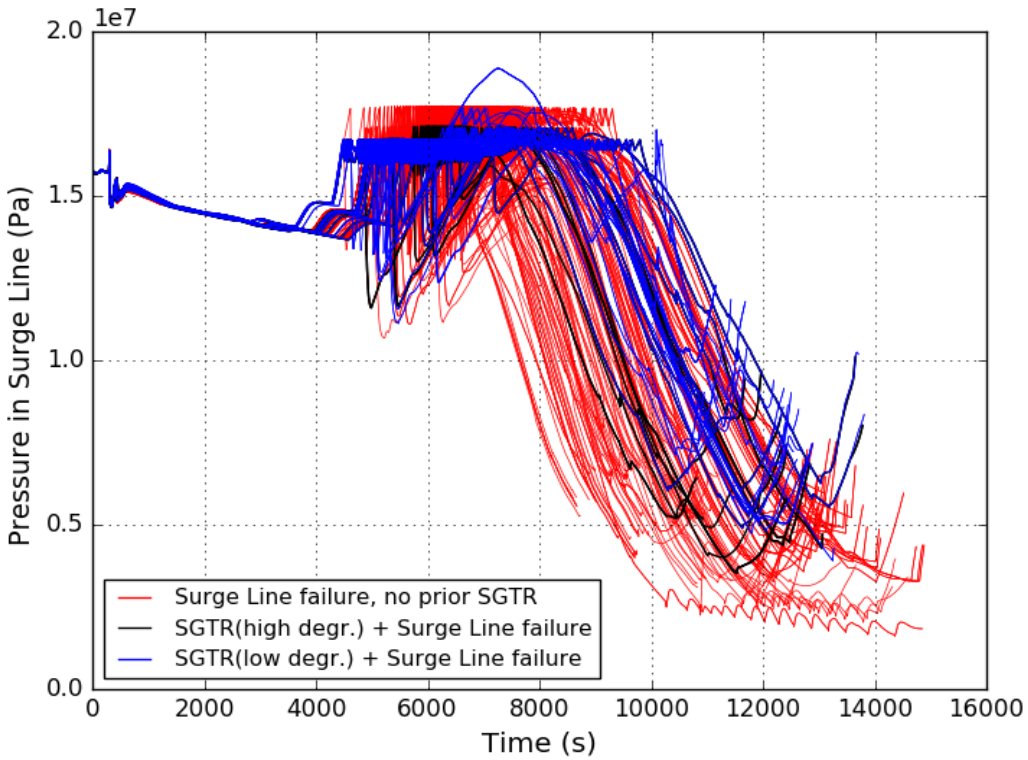


Abb. 3.24 Druckverlauf in der VAL für alle Sequenzen, bei denen ein Bruch der VAL aufgetreten ist

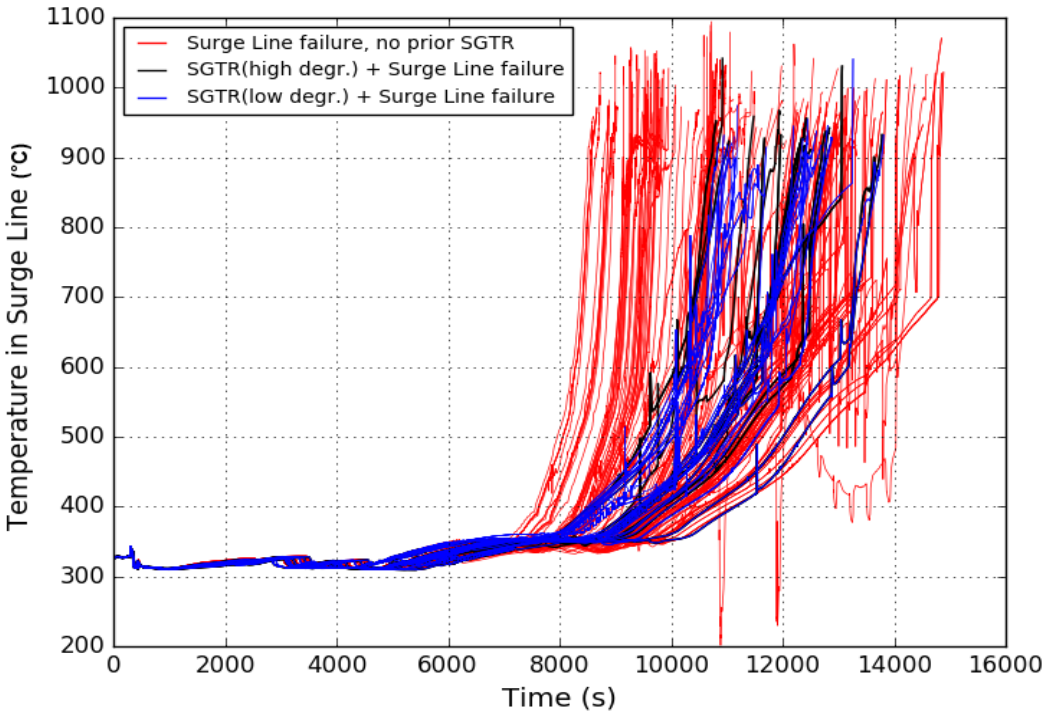


Abb. 3.25 Temperaturverlauf in der VAL für alle Sequenzen, bei denen ein Bruch der VAL aufgetreten ist

Die Druck- und Temperaturverläufe in Abb. 3.24 und Abb. 3.25 wurden gesondert für die Sequenzen gekennzeichnet, bei denen die VAL vor dem DEHEIRO versagt hat (rot) oder es nach dem DEHEIRO-Versagen zu einem Buch der VAL gekommen ist. Im letzteren Fall wurden die Sequenzen noch zusätzlich in solche klassifiziert, bei denen das DEHEIRO-Versagen mit schwacher (blau) bzw. starker (schwarz) Schädigung aufgetreten ist.

Aus Abb. 3.24 und Abb. 3.25 ist ersichtlich, dass ein Bruch der VAL aus einem starken Temperaturanstieg auf mehr als 900 °C bei gleichzeitigem Druckabfall auf weniger als 10 MPa folgt. Nur in wenigen Sequenzen, bei denen der Bruch der VAL nach einem DEHEIRO-Versagen auftritt und eine schwache Schädigung des Heizrohrs vorliegt, liegt der Druck zum Zeitpunkt des Bruchs der VAL zwischen 10 und 12 MPa. Der Druckabfall wird dadurch verursacht, dass während der automatischen Druckbegrenzung eines oder mehrerer Druckbegrenzungsventile (DH-AV, SiV1, SiV2) zufällig in Offenstellung ausfallen. Die Ausfälle in Offenstellung führen zu einem schnellen Kühlmittelverlust und Kernfreilegung, womit ein massiver Temperaturanstieg in der HKL und VAL verbunden ist.

Entsprechend der oben dargestellten Sequenzen könnte man auch die Druck- und Temperaturverläufe im Heizrohr für alle die Sequenzen darstellen, bei denen es zu einem DEHEIRO-Versagen gekommen ist. Da ein DEHEIRO-Versagen jedoch bei den meisten Sequenzen vorkommt, wären die Darstellungen der Druck- und Temperaturverläufe zu unübersichtlich. Stattdessen können aus den vorliegenden Ergebnissen der MCDET/ATHLET-CD Analyse für die Druck- und Temperaturverteilungen ermittelt werden, die zum Zeitpunkt des DEHEIRO-Versagens im Heizrohr vorliegen.

In Abb. 3.26 werden die bedingten Verteilungen der Heizrohrtemperatur dargestellt, die zum Zeitpunkt des DEHEIRO-Versagens vorliegen. Die bedingten Verteilungen beziehen sich auf Heizrohre mit Schädigungen < 20 % (in blau) und Schädigungen von 20 – 70 % (in rot). In Abb. 3.27 werden die Drücke bei den jeweils vorliegenden Temperaturen in Form eines Scatter-Plots dargestellt.

Die Variationen der Temperatur- und Druckwerte ergeben sich aus dem gemeinsamen Einfluss der in der Analyse berücksichtigten aleatorischen und epistemischen Unsicherheiten.

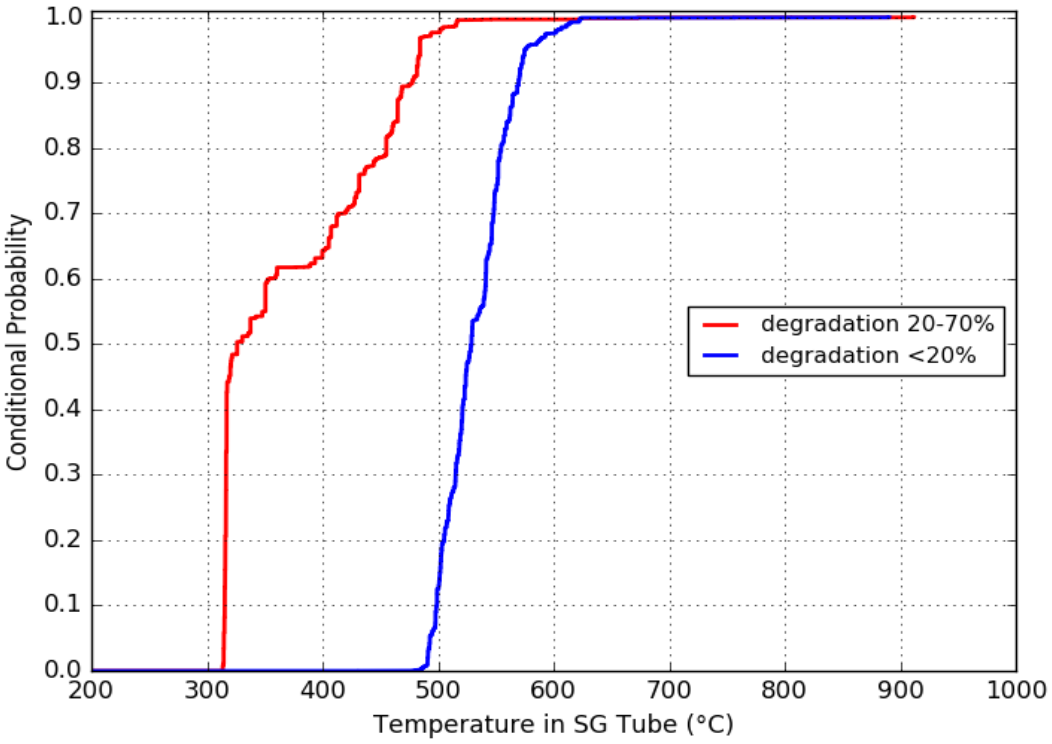


Abb. 3.26 Heizrohr-Temperatur zum Zeitpunkt des DEHEIRO-Versagens

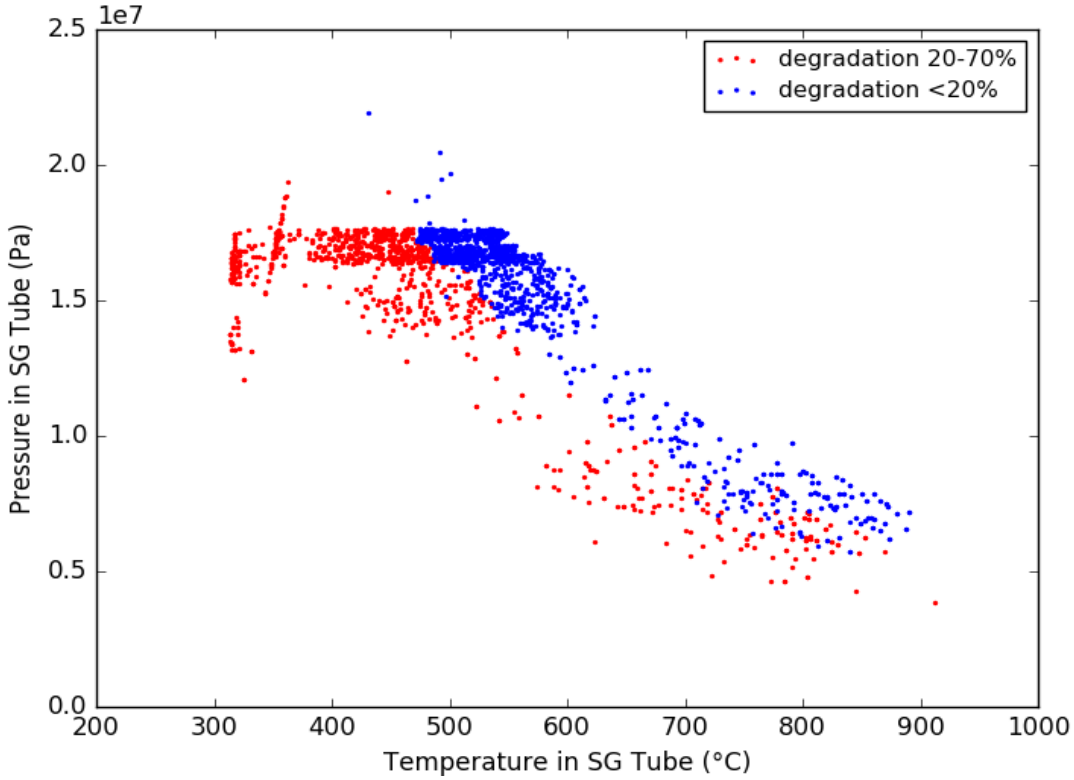


Abb. 3.27 Druck und Temperatur im Heizrohr zum Zeitpunkt des DEHEIRO-Versagens

Abb. 3.26 zeigt, dass die Temperaturbelastung des schwach geschädigten Heizrohrs zum Zeitpunkt des DEHEIRO-Versagens mit einer bedingten Wahrscheinlichkeit von 95 % zwischen 480 °C und 600 °C liegt. Der vorherrschende Druck in diesem Temperaturbereich liegt zwischen 12 und 20 MPa wie aus Abb. 3.27 für die Schädigungen < 20 % ersichtlich ist. Die Temperatur, die beim Ausfall des stark geschädigten Heizrohrs vorliegt, variiert mit einer bedingten Wahrscheinlichkeit von 95 % zwischen 315 °C und 500 °C. Der Druck in diesem Temperaturbereich liegt ungefähr zwischen 12 MPa und 19 MPa. Auffällig ist die hohe bedingte Wahrscheinlichkeit von ca. 0.5, dass das stark geschädigte Heizrohr bei einer Temperaturbelastung zwischen 310 °C und 320 °C versagt. Demgegenüber variieren die Drücke in diesem engen Temperaturbereich relativ stark zwischen 13 MPa und 17.5 MPa. Diese Temperatur- und Druckbelastungen treten insbesondere in der frühen Phase des Unfallablaufs zwischen 4900 und 5900 s auf (s. Abb. 3.22). Während dieser Phase sind die Dampferzeuger nahezu trocken, der Druck steigt im Primärkreis stetig an und der Füllhöhestand erreicht den Grenzwert bei dem erstmals das DH-Abblaseventil zur automatischen Druckbegrenzung angefordert wird. Die große Variation des Drucks im engen Temperaturbereich zwischen 310 °C und 320 °C wird durch das Ausfallverhalten des DH-Abblaseventils verursacht, dass

während seiner ersten Anforderungszyklen frühzeitig offen oder geschlossen ausfallen oder auslegungsgemäß funktionieren kann.

Abb. 3.28 zeigt die Beziehung zwischen dem Schädigungsgrad des Heizrohrs (ausgedrückt durch eine entsprechende Verringerung der Wanddicke des Heizrohrs) und der Temperaturbelastung die zum Zeitpunkt des DEHEIRO-Versagens vorliegt. Hier zeigt sich, dass ein Heizrohr mit einer Wanddicke < 0.62 mm (entspricht in etwa einer Heizrohr-Schädigung von mehr als 48 %) bereits bei Temperaturen zwischen 310 °C und 350 °C ausfallen können. Dies sind Temperaturen, die bereits in einer sehr frühen Phase des Unfallablaufs vorliegen. Das deutet darauf hin, dass ein Heizrohr, dessen Schädigung zu Beginn des Unfallablaufs > 48 % beträgt, bereits zu einem relativ frühen Zeitpunkt während des Unfallablaufs ausfällt. Dies wird in Abb. 3.29 gezeigt, in der die Ausfallzeitpunkte des DE-Heizrohrs bei Schädigungsgraden > 48 % bzw. Wanddicken < 0.62 mm dargestellt werden.

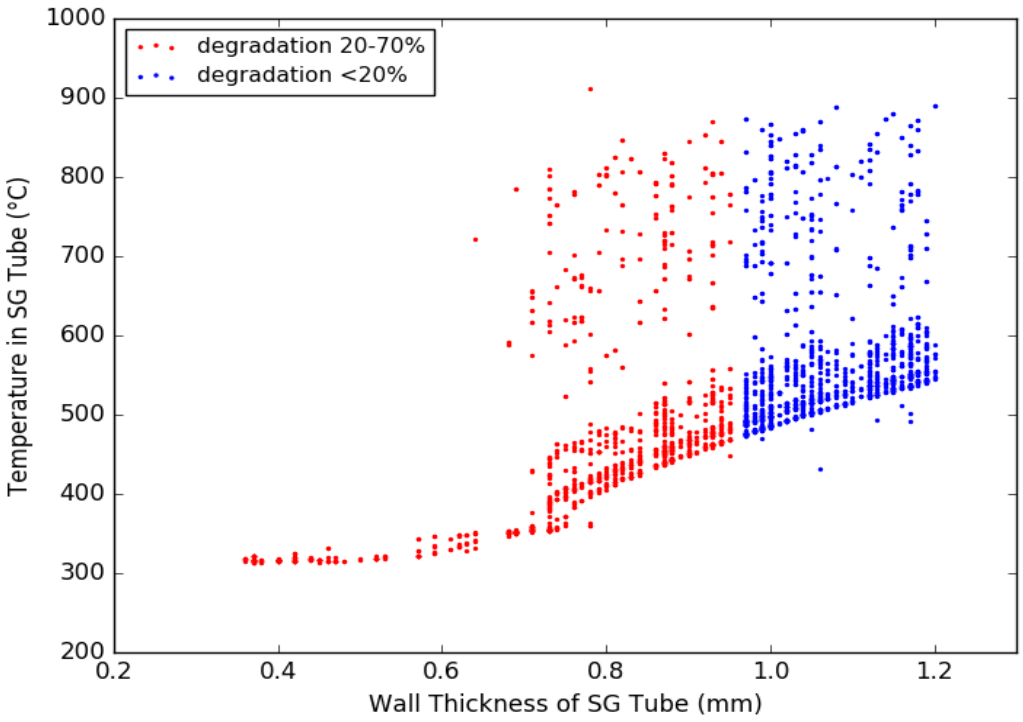


Abb. 3.28 Beziehung zwischen Wanddicke und Temperatur des Heizrohrs zum Zeitpunkt des DEHEIRO-Versagens

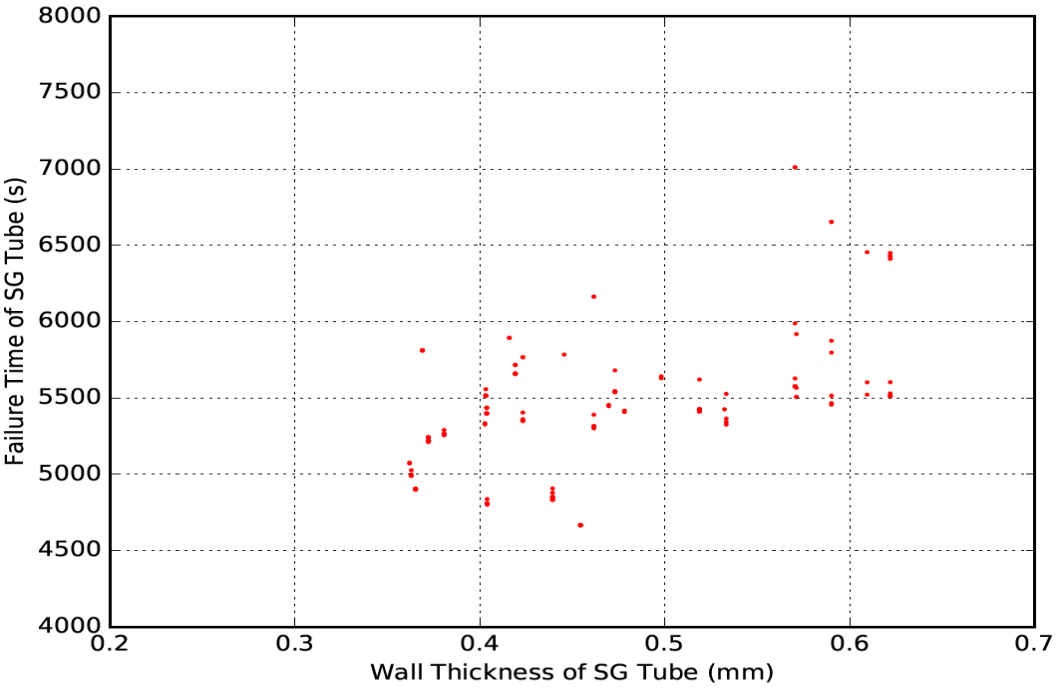


Abb. 3.29 Beziehung zwischen Schädigungen > 48 % und Ausfallzeitpunkt des DE-Heizrohrs

Wie Abb. 3.29 zeigt, liegen bei Schädigungsgraden > 48 % die Ausfallzeitpunkte des Heizrohrs größtenteils zwischen 4500 s und 6000 s nach Beginn des Unfallablaufs. eintritt. Nur in wenigen Fällen liegen die Ausfallzeitpunkte zwischen 6000 s und 7000 s. Diese treten bei Wanddicken von ca. 0.57 – 0.62 mm auf. In diesem Zusammenhang ist zu betonen, dass die Wahrscheinlichkeit einer Schädigung von mehr als 48 % mit einer mittleren Wahrscheinlichkeit von 9.4E-3 relativ gering ist.

Diese beispielhaft ausgewählten Ergebnisse sollen verdeutlichen in welchem Umfang und Detaillierungsgrad die Auswertungen der Ergebnisse einer MCDET-Analyse erfolgen können. Für die Auswertung der Ergebnisse einer IDPSA unter Verwendung von MCDET kann prinzipiell das gesamte Methodenspektrum der statistischen Analyse eingesetzt werden. In den oben aufgeführten Beispielen beschränkte sich die Auswertung lediglich auf die Berechnung und grafische Darstellung von bedingten Verteilungsfunktionen und den daraus abgeleiteten probabilistischen Aussagen.

Für nachfolgende Weiterentwicklungen ist geplant, das Auswertespektrum von MCDET um multivariate statistische Methoden (z. B. Clusteranalyse, Diskriminanzanalyse) zu erweitern.

3.6 Diskussion des Nutzens und Vorteils einer IDPSA unter Verwendung der Methode MCDET

Um den Nutzen und Vorteil einer IDPSA unter der Verwendung der Methode MCDET zu zeigen, muss insbesondere die Mehrinformation dargestellt werden, die durch diese Methodik erzielt werden kann und durch die ein Kenntnisgewinn über das Systemverhalten unter dem Einfluss verschiedener Unsicherheitsquellen abgeleitet werden kann.

Um den Vorteil einer IDPSA unter Verwendung von MCDET darzustellen soll in Abschnitt 3.6.1 anhand von Beispielen bzw. Aussagen aus der klassischen PSA gezeigt werden, in welch größerem Umfang und Detaillierungsgrad Ergebnisse aus MCDET-Analysen ausgewertet werden können. In diesem Zusammenhang soll auch der Mehrwert an Informationen dargestellt und diskutiert werden, der durch eine IDPSA mit MCDET erzielt werden kann. Dabei soll insbesondere der Kenntnisgewinn herausgestellt werden, den man über das Systemverhalten unter dem Einfluss von Unsicherheiten erhält.

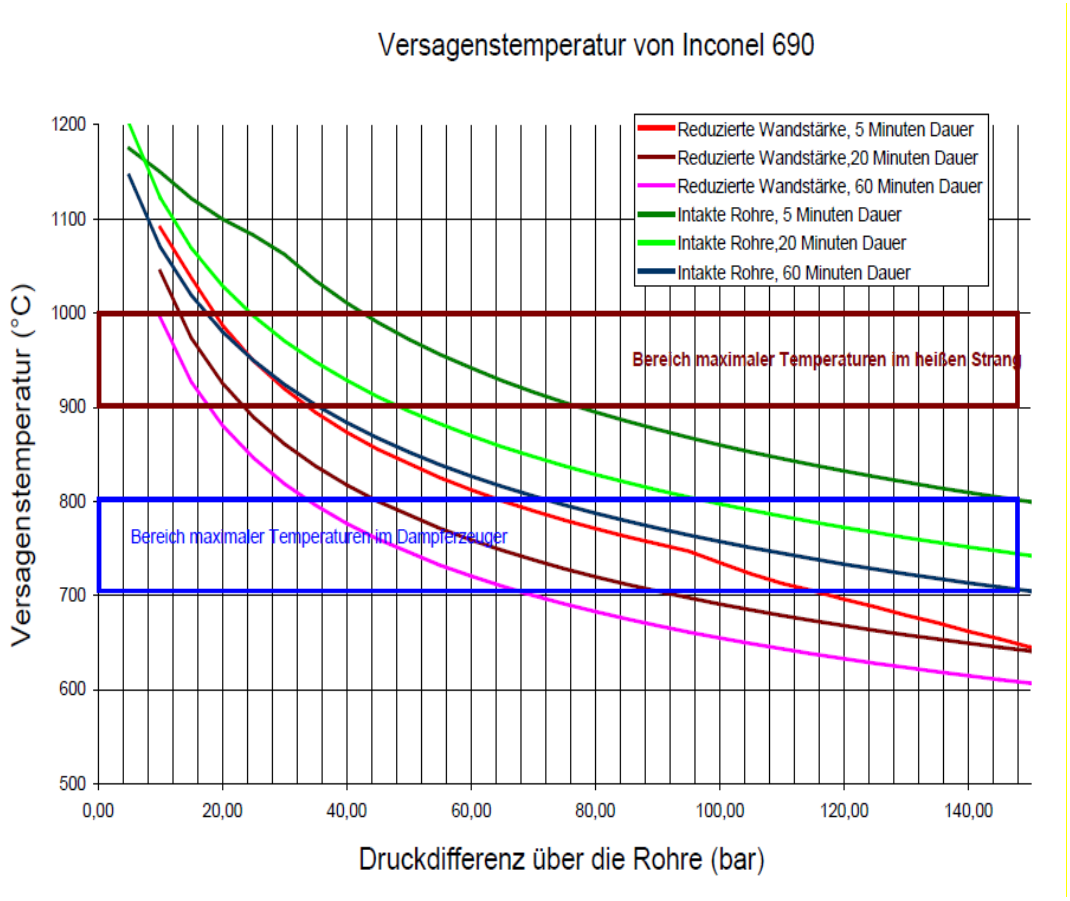
Um den Nutzen einer IDPSA mit MCDET darzustellen soll in Abschnitt 3.6.2 demonstriert werden, wie die Ergebnisse der Auswertungen der MCDET/ATHLET-CD Analyse verwendet werden können, um den Ereignisbaum einer klassischen PSA um bestimmte interessante Fragestellungen erweitern zu können. Dabei wird auf Arbeiten Bezug genommen, die im Rahmen des BMUB Vorhabens 3615R01345 durchgeführt wurden. In diesem Zusammenhang soll diskutiert und am Beispiel eines konkreten Ereignisbaumes veranschaulicht werden, in welcher Form die Ergebnisse der IDPSA zu einer verbesserten probabilistischen Schätzung komplexer Phänomene, die in einen Ereignisbaum einer PSA der Stufe 2 eingehen, beitragen können.

3.6.1 Vorteile einer IDPSA unter Verwendung von MCDET

Zu Beginn dieses Abschnitts werden beispielhaft Aussagen und Informationen zugrunde gelegt, wie sie im Rahmen einer herkömmlichen PSA zum Thema DE-Heizrohrversagen vorliegen und bisher verwendet wurden. Auf der Basis dieser Aussagen und Informationen soll anhand von zwei Beispielen gezeigt werden, welche zusätzlichen probabilistischen Aussagen aus der in diesem Projekt durchgeführten MCDET/ATHLET-CD Analyse zum DE-Heizrohrversagen abgeleitet werden können. Damit soll der Mehrwert an Informationen veranschaulicht werden, der prinzipiell durch eine IDPSA unter Verwendung von MCDET erzielt wird.

Beispiel 1:

Im Datenband des PSA-Leitfadens /FAK 05/ wird am Beispiel des EPR für den Werkstoff INCONEL 690 eine Abschätzung für das induzierte Versagen der Dampferzeuger-heizrohre vorgestellt. Die nachfolgende Abbildung und die kursiv geschriebene Text-stelle sind dem Datenband des PSA-Leitfadens entnommen.



„*Abb. 7.1: Versagenstemperatur von DE-Heizrohren in Abhängigkeit des Differenzdruckes für verschiedene Zeitbereiche mit und ohne Vorschädigung***“** (entnommen aus /FAK 05/)

Die Beschreibung im Datenband lautet wie folgt (Zitat):

„Die Abb. 7.1 zeigt die Versagenstemperatur in Abhängigkeit des Differenzdruckes für verschiedene Zeitbereiche mit und ohne Vorschädigung. Bei Rohrtemperaturen zwischen 973 K und 1173 K ergibt sich bei je nach Leckgröße sich einstellender Druckdifferenz von 5 bis 7 MPa daraus eine hohe Versagenswahrscheinlichkeit für vorgeschädigte Rohre (mechanische Vorschädigung aus DE-Einsatzzeit) und eine deutlich kleinere Versagenswahrscheinlichkeit für intakte Rohre. Dies wird für vorgeschädigte Rohre subjektiv als eine Versagenswahrscheinlichkeit von 50 % interpretiert. Umgekehrt

liegt im Falle intakter Rohre nur ein marginales Überlappen der entsprechenden Kurven mit dem Versagenstemperaturbereich vor. Dies wird als eine um den Faktor 10 geringere (0,05) Versagenswahrscheinlichkeit für die 50 % Fraktile interpretiert. Es ist basierend darauf praktisch unmöglich, detailliertere Angaben zu einer möglichen Wahrscheinlichkeitsverteilung zu machen. Im Rahmen einer Unsicherheitsanalyse sollte eine breite Verteilung angenommen werden: Faktor 5 geringer (0,01) für die 5 % Fraktile, Faktor 10 höher (0,5) für die 95 % Fraktile. Für die Verteilung selbst kann eine einfache Dreiecksverteilung angenommen werden."

In diesem Text aus dem Datenband des PSA-Leitfadens wird mangels zur Verfügung stehender Daten und Informationen eine probabilistische Aussage aus den Kurven der oben gezeigten Abbildung abgeleitet. Wie man aus den Kurven der obigen Abbildung zu den probabilistischen Abschätzungen gelangt, ist nur schwer nachzuvollziehen und ist qualitativ als eine grobe Expertenabschätzung zu bewerten.

Zum Vergleich soll im Folgenden demonstriert werden, welche Art probabilistischer Aussagen und Informationen über Auswertungen der Ergebnisse der durchgeführten MCDET/ATHLET-CD bzgl. Druckdifferenz und Temperaturen zum Zeitpunkt des Heizrohrversagens abgeleitet werden können. Dabei ist zu betonen, dass es in diesem Beispiel insbesondere um die Darstellung der Unterschiede bzgl. Qualität und des Informationsgehaltes der probabilistischen Aussagen geht, die man aus einer IDPSA unter Verwendung von MCDET erhält, und weniger um einen direkten Vergleich der Ergebnisse. Der direkte Vergleich der Ergebnisse ist hier deshalb nicht möglich, da sich die Versagenstemperaturen in „*Abb. 7.1*" auf den Werkstoff INCONEL 690 eines EPR beziehen. Die Parameter des Larsson-Miller Modells, die in der MCDET/ATHLET-CD Analyse zur Bestimmung des DEHEIRO-Versagens verwendet wurde, beziehen sich auf den Werkstoff Alloy800mod für das DE-Heizrohr eines Druckwasserreaktors.

Zu Beginn der Auswertung werden in Abb. 3.30 die Werte der Druckdifferenz und der Temperatur des DE-Heizrohrs zum Zeitpunkt des DEHEIRO-Versagens dargestellt. Dabei wurden die Daten getrennt für schwache (< 20 %) und starke (20 – 70 %) Schädigungen ermittelt.

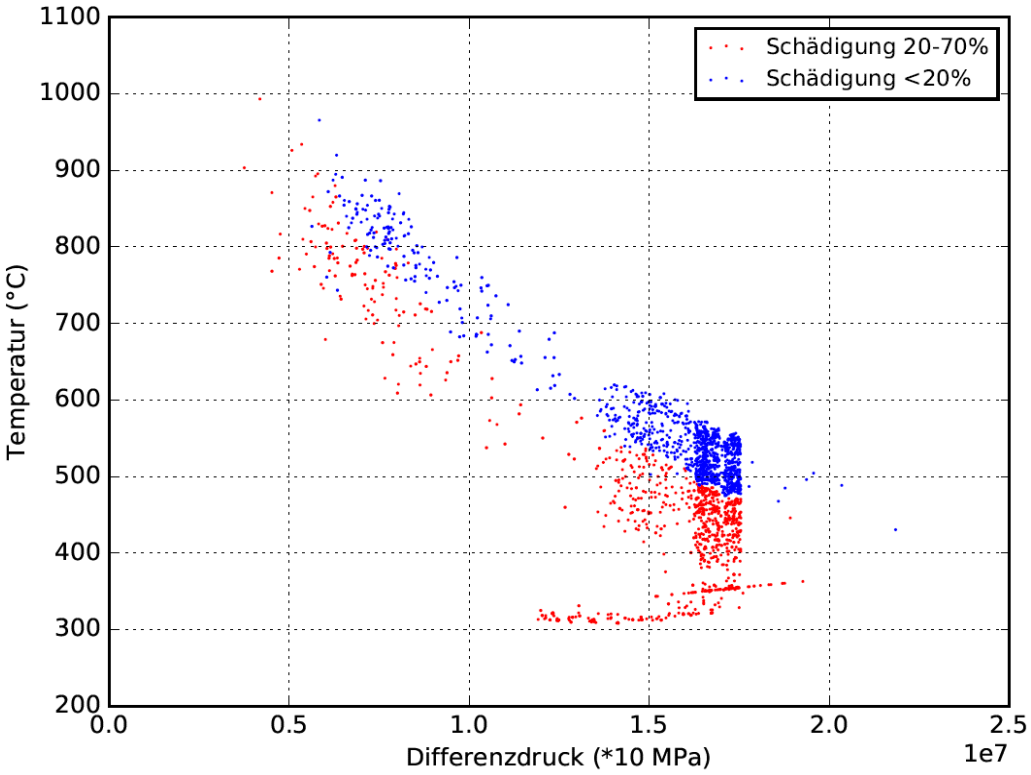


Abb. 3.30 Druckdifferenz und Temperatur des DE-Heizrohrs zum Zeitpunkt des DEHEIRO-Versagens bzgl. starker und schwacher Heizrohrschädigungen

In Abb. 3.30 wurden die Werte der Druckdifferenz und Temperatur bzgl. schwacher und starker Schädigungen des DE-Heizrohrs dargestellt. Während die Variation des Differenzdruckes bei starken und schwachen Schädigungen ungefähr den gleichen Wertebereich abdeckt (zwischen ca. 50 und 200 bar) lässt sich zwischen den beiden Schädigungsklassen eine gewisse Clusterbildung in den Temperaturen erkennen, die bei den verschiedenen Differenzdrücken vorliegen.

Bei den starken Schädigungen variieren die Temperaturen bei Druckdifferenzen von 120 – 170 bar ungefähr zwischen 310 °C und 580 °C. Bei den schwachen Schädigungen liegen die Temperaturen bei entsprechenden Druckdifferenzen zwischen ca. 570 °C und 690 °C. Bei Druckdifferenzen zwischen 50 und 100 bar variieren die Temperaturen bei starken Schädigungen zwischen ca. 600 °C und 930 °C und bei schwachen Schädigungen zwischen ca. 680 °C und 970 °C. D. h., mit niedrigeren Differenzdrücken sind relativ hohe Temperaturen zum Zeitpunkt des DEHEIRO-Versagens verbunden.

Eine weitere Auffälligkeit, die genauer untersucht wird, bezieht sich auf die starken Heizrohr-Schädigungen, die zum Zeitpunkt ihres Versagens sehr geringe Temperaturen von 300 – 320 °C aufweisen. Die starken Schädigungen wurden bisher relativ grob in

Schädigungen von 20 – 70 % klassifiziert. Nun könnte man annehmen, dass ggf. eine feinere Klassifizierung der starken Schädigungen, zeigen könnte, dass die niedrigen Heizrohrtemperaturen zum Ausfallzeitpunkt diejenigen Fälle betreffen, bei denen eine sehr hohe Schädigung von beispielsweise > 50 % vorliegt. Um diese Hypothese zunächst deskriptiv zu beurteilen, wird eine feinere Klassifizierung der Schädigungen vorgenommen und zwar in die Schädigungsklassen < 10 %, 10 – 20 %, 20 – 30 %, 30 – 40 %, 40 – 50 % und 50 – 70 %.

Über die Auswertung der Ergebnisse, die aus der MCDET/ATHLET-CD Analyse vorliegen, werden alle diejenigen Sequenzen herausgefiltert, bei denen ein DEHEIRO-Versagen für die jeweiligen Schädigungsklassen aufgetreten ist. Für jede dieser gefilterten Sequenzen wird dann der Differenzdruck und die Temperatur bestimmt, die zum Versagenszeitpunkt des DE-Heizrohrs vorliegt. Diese Werte werden für die jeweiligen Schädigungsklassen ermittelt und in Abb. 3.31 dargestellt.

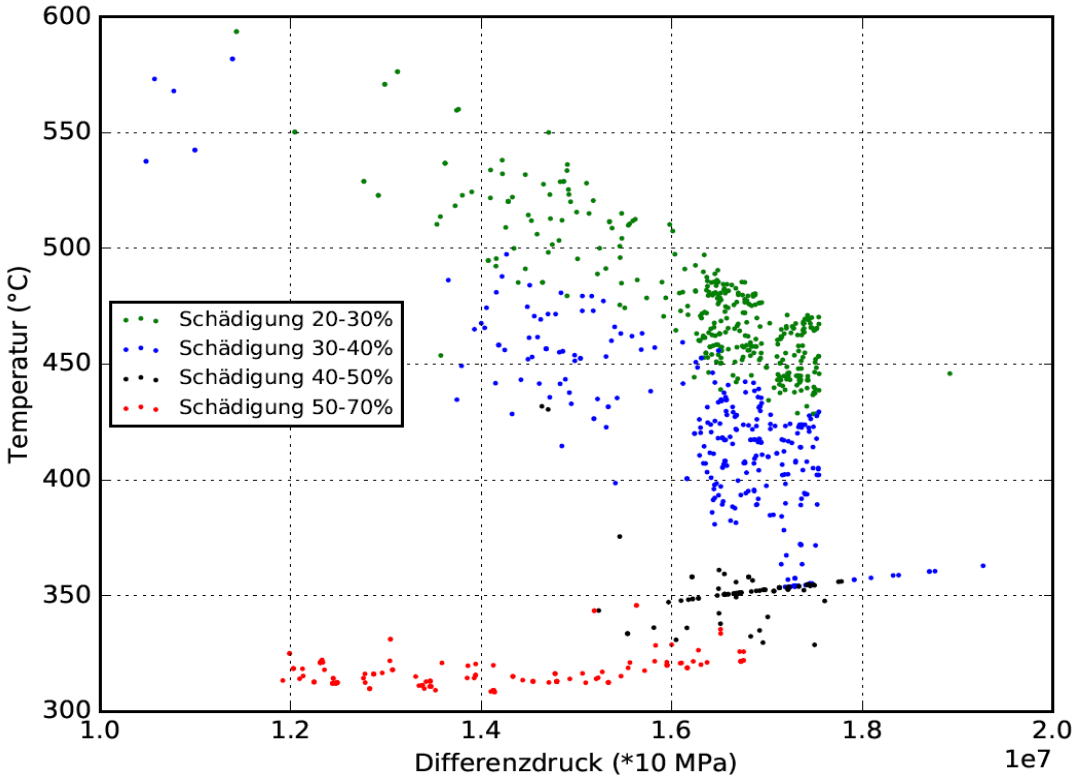


Abb. 3.31 Druckdifferenz und Temperatur des DE-Heizrohrs zum Zeitpunkt des DEHEIRO-Versagens in Abhängigkeit der Heizrohrschädigung

Wie angenommen ist aus Abb. 3.31 ersichtlich, dass sehr geringe Versagenstemperaturen von 300 – 320 °C ausschließlich bei sehr hohen Schädigungsgraden von 50 – 70% auftreten, was einer Wanddicke von 0.36 – 0.6 mm entspricht. Hier zeigt sich, dass ein Heizrohr mit derartig hohen Schädigungen bereits in einer sehr frühen Phase

des Unfallablaufs ausfällt, die durch eine hohe Druckdifferenz von 12 – 16 MPa gekennzeichnet sind. Diese hohe Druckdifferenz ergibt sich durch die sekundärseitige Druckentlastung, die im Rahmen der Notfallprozedur ausgeführt wird.

Dass die unterschiedlichen Schädigungsgrade einen erheblichen Einfluss auf die Versagenstemperaturen bei Differentialdrücken zwischen 12 und 17.5 MPa haben, erkennt man aus der Clusterbildung bzgl. der Schädigungsklassen. Dies erkennt man sehr deutlich im Differenzdruckbereich von 14 – 17.5 MPa. In diesem Bereich treten Versagenstemperaturen von ca. 350 °C bei Schädigungen von 40 – 50 % auf, Versagenstemperaturen zwischen 350 °C und 500 °C bei Schädigungen von 30 – 40 % und Versagenstemperaturen zwischen 430 °C und 550 °C bei Schädigungen von 20 – 30 %. Bei Schädigungen < 20 % liegen die Versagenstemperaturen in diesem Differenzdruckbereich zwischen ungefähr 480 °C und 620 °C wie aus Abb. 3.30 ersichtlich ist.

Bislang wurde lediglich eine deskriptive Auswertung vorgenommen. Nun soll beispielhaft gezeigt werden, welche probabilistischen Aussagen man durch entsprechende Auswertungen der MCDET-Ergebnisse erhalten kann. Jeder Datenpunkt, der in Abb. 3.30 bzw. Abb. 3.31 aufgeführt ist, gehört zu einer gerechneten Sequenz, die zu einem DEHEIRO-Versagen geführt hat. Zu jeder dieser gerechneten Sequenzen ist eine Wahrscheinlichkeit zugeordnet, mit der diese Sequenz eintritt. Mit diesen Eintrittswahrscheinlichkeiten der Sequenzen lassen sich schließlich probabilistische Aussagen bzgl. verschiedenster Fragestellungen berechnen.

Oben wurde ausgeführt, dass Heizrohre mit Schädigungen von 50 – 70 % in einer sehr frühen Phase des Unfallablaufs ausfallen können, die durch eine hohe Druckdifferenz und niedrige Temperaturen gekennzeichnet sind, die etwa den Temperaturen im Normalbetrieb entsprechen. Diese hohe Druckdifferenz ergibt sich durch die sekundärseitige Druckentlastung (SDE), die im Rahmen der Notfallprozedur ausgeführt wird. In diesem Zusammenhang könnten z. B. folgende Fragen interessieren:

- Zu welchem Zeitpunkt erfolgt die SDE?
- Wie groß ist die Zeitspanne zwischen SDE und DEHEIRO-Versagen?
- Wie hoch ist die maximale Druckdifferenz, die sich innerhalb von 5 min nach SDE bildet?
- Wie lange stehen Druckdifferenzen > 10 MPa bis zum DEHEIRO-Versagen an?

Aufgrund der in der Analyse berücksichtigten epistemischen Unsicherheiten bzgl. der Parameter des ATHLET-CD Modells und der aleatorischen Unsicherheiten bzgl. der menschlichen Handlungen im Rahmen der Notfallmaßnahme SDE sind die Zeitpunkte, wann SDE ausgeführt wird, ebenfalls mit einer Unsicherheit behaftet. Demzufolge interessiert es, in welchem Zeitrahmen die SDE nach dem einleitenden Ereignis durchgeführt wird. Obwohl der phänomenologische Ablauf keinen Zusammenhang aus Schädigungsgrad und Zeitpunkt der SDE-Durchführung liefert, werden in Abb. 3.32 dennoch die bedingten Verteilungen der Zeiten dargestellt, wann die sekundärseitige Druckentlastung der Dampferzeuger ausgeführt wurde. Die nachfolgenden Verteilungen wurden jeweils unter der Bedingung ermittelt, dass ein DEHEIRO-Versagen bei starken bzw. schwachen Schädigungen aufgetreten ist sowie unter der Bedingung, dass das DE-Heizrohr nicht ausgefallen ist. Der Grund liegt zum einen darin, mögliche Scheinkorrelationen auszuschließen und zum anderen zu erläutern, wie die aus den bedingten Verteilungen abgeleiteten Wahrscheinlichkeiten zu interpretieren sind.

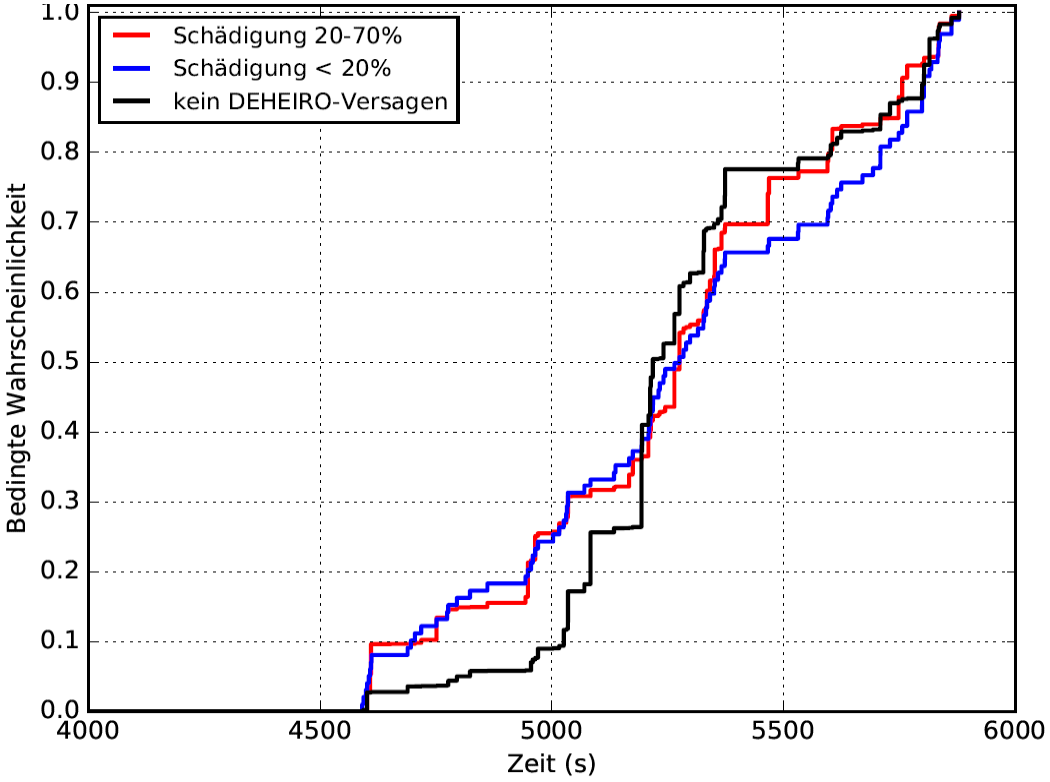


Abb. 3.32 Bedingte Verteilung der Zeit, wann SDE ausgeführt wird

Abb. 3.32 zeigt, dass unter allen drei Bedingungen die sekundärseitige Druckentlastung der Dampferzeuger zwischen ca. 4600 s und 5900 s nach dem auslösenden Ereignis durchgeführt wird. Da sich die dargestellten Verteilungen nicht wesentlich voneinander

unterscheiden, weist dies darauf hin, dass der Zeitpunkt, wann SDE durchgeführt wird, weder durch den Schädigungsgrad des Heizrohrs noch dadurch beeinflusst wird, ob das DE-Heizrohr nachfolgend versagt oder nicht.

Der Nutzen solcher Verteilungen, die man aus den Ergebnissen von MCDET-Analysen berechnen kann ist, dass man aus solchen Verteilungen verschiedene probabilistische Aussagen bzgl. der interessierenden Größe (hier: Zeitpunkt wann SDE durchgeführt wird) ableiten kann. So kann man z. B. aus den Verteilungen in Abb. 3.32 ablesen, dass im Fall eines DEHEIRO-Versagens (sowohl aufgrund starker als auch schwacher Schädigung) die Wahrscheinlichkeit ca. 25 % beträgt, dass SDE zwischen 4600 und 5000 s, mit einer Wahrscheinlichkeit von ca. 51 % zwischen 5000 und 5500 s und mit 24%iger Wahrscheinlichkeit zwischen 5500 und 5900 s nach dem einleitenden Ereignis durchgeführt wird. In den Fällen, in denen es nicht zum DEHEIRO-Versagen gekommen ist, ist die Wahrscheinlichkeit, dass SDE innerhalb 4600 – 5000 s durchgeführt wird, mit 0.09 etwas geringer als in den Fällen mit DEHEIRO-Versagen. Die bedingten Verteilungen eignen sich durch ihre Normierung sehr gut dazu, den Einfluss von aleatorischen Unsicherheiten (hier z. B. Schädigungsgrad und DEHEIRO-Versagen) auf die Verteilung interessierender Prozessgrößen zu veranschaulichen.

Bei der Interpretation der bedingten Verteilungen ist darauf zu achten, dass die Wahrscheinlichkeiten der Verteilungen durch die Wahrscheinlichkeiten, mit denen die Bedingungen auftreten, normiert sind. Z. B. sind in Abb. 3.32 die drei Bedingungen, unter denen die Zeitverteilung der SDE ermittelt wurden, durch folgende Ereignisse festgelegt:

i) DEHEIRO hat eine Schädigung von 20 – 70 % und versagt.

ii) DEHEIRO hat eine Schädigung < 20 % und versagt.

iii) DEHEIRO versagt nicht.

Die Wahrscheinlichkeiten der Ereignisse (z. B. dass eine Schädigung von 20 – 70 % auftritt und DEHEIRO versagt) wurden ebenfalls über Auswertungen der MCDET-Ergebnisse ermittelt und sind in den Tab. 3.11 und Tab. 3.12 in 3.5.2 angegeben. Um nun z. B. die Wahrscheinlichkeit des gemeinsamen Eintritts der Ereignisse zu bestimmen, dass SDE zwischen 4600 und 5000 s durchgeführt wird (t_{SDE} < 5000) und ein DEHEIRO-Versagen bei einer Schädigung von 20 – 70 % auftritt ($DE_{fail20\text{-}70\%}$), ist folgende Berechnung unter Verwendung der Definition der bedingten Wahrscheinlichkeit $P(A \mid B) \cdot P(B) = P(A \cdot B)$ durchzuführen:

$P\ (t_{SDE} < 5000\ s\ und\ DE_{fail20\text{-}70\%}) \cdot P\ (DE_{fail20\text{-}70\%}) =$

$P\ (t_{SDE} < 5000\ s \mid DE_{fail20\text{-}70\%}) \cdot P\ (DE_{fail20\text{-}70\%}) =$

$0.25 \cdot 1.82E\text{-}02 = 4.55E\text{-}03$

Die Wahrscheinlichkeit $P\ (t_{SDE} < 5000\ s \mid DE_{fail20\text{-}70\%})$ ist aus der entsprechenden bedingten Verteilung in Abb. 3.32 abzuleiten. Die Wahrscheinlichkeit $P\ (DE_{fail20\text{-}70\%})$ ist Tab. 3.12 zu entnehmen. Dieses Beispiel zeigt, dass über die Anwendung der Wahrscheinlichkeitsrechnung aus Ergebnissen der bisherigen Auswertung die Wahrscheinlichkeitsaussagen für das gemeinsame Auftreten mehrerer Ereignisse berechnet werden kann.

Anhand der Verteilungen in Abb. 3.32 ist bekannt, in welchem Zeitrahmen die SDE im zugrunde gelegten Unfallszenario durchgeführt wird. Im Folgenden soll untersucht werden, wie lange es nach der Durchführung der SDE dauert, bis das DE-Heizrohr versagt. Die Beantwortung dieser Frage erfolgt unter den Bedingungen

i) dass eine Schädigung von 20 – 70 % vorliegt und das DE-Heizrohr versagt

ii) dass eine Schädigung von < 20 % vorliegt und das DE-Heizrohr versagt

Mit den berechneten bedingten Verteilungen in Abb. 3.33 soll ein erster Eindruck vermittelt werden, ob in den Zeitspannen zwischen SDE und DEHEIRO-Versagen Unterschiede in Abhängigkeit starker und schwacher Schädigungsgrade erkennbar sind. Oder anders ausgedrückt, ob das Ausmaß der Schädigung des DE-Heizrohrs einen erkennbaren Einfluss auf die Zeitspanne zwischen der Ausführung der SDE und DEHEIRO-Versagen hat. Die Zeitspanne wird im Nachfolgenden durch die Zeitdifferenz $t_{Ausfall} - t_{SDE}$ beschrieben. t_{SDE} bezeichnet den Zeitpunkt, wann SDE durchgeführt wird und $t_{Ausfall}$ den Zeitpunkt des DEHEIRO-Versagens.

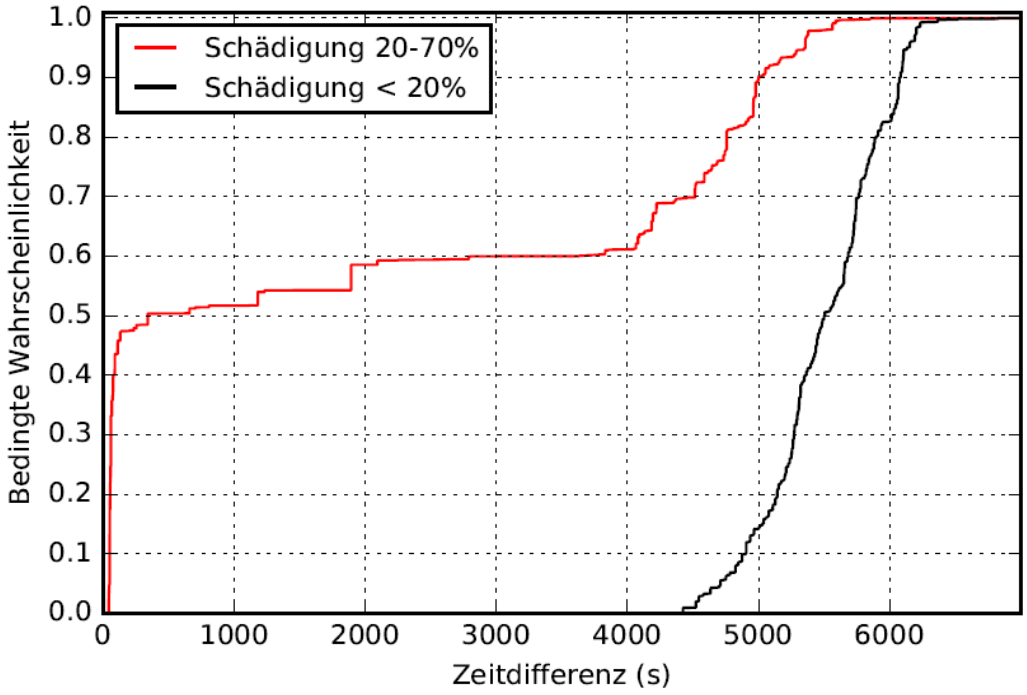


Abb. 3.33 Verteilung der Zeitdifferenz $t_{Ausfall}$ - t_{SDE} unter der Bedingung starker und schwacher Schädigungen

Abb. 3.33 zeigt einen signifikanten Unterschied zwischen den bedingten Verteilungen der Zeitdifferenzen $t_{Ausfall}$ - t_{SDE} in Abhängigkeit des Schweregrades der Heizrohrschädigung. Die Verteilungen zeigen erwartungsgemäß, dass ein stark geschädigtes DE-Heizrohr wesentlich früher nach Durchführung der SDE ausfällt als ein schwach geschädigtes Heizrohr. Die bedingten Verteilungen erlauben es, konkrete Wahrscheinlichkeitsaussagen abzuleiten.

Der Verlauf der bedingten Verteilung der Zeitdifferenz $t_{Ausfall}$ - t_{SDE} bei starken Schädigungen von 20 – 70 % ist durch eine sehr hohe Variation gekennzeichnet und lässt sich grob in vier Bereiche einteilen. Der erste Bereich ist durch relativ hohe Wahrscheinlichkeit von ca. 46 % gekennzeichnet, dass ein DE-Heizrohr mit schwerer Schädigung innerhalb von 2 min nach Durchführung der SDE versagt. Der zweite Bereich erstreckt sich von 2 – ca. 68 min (4100 s). Die Wahrscheinlichkeit beträgt ca. 16 %, dass ein schwer geschädigtes DE-Heizrohr in diesem Zeitbereich nach Durchführung der SDE versagt. Mit einer Wahrscheinlichkeit von ca. 38 % fällt ein schwer geschädigtes Heizrohr erst nach 68 – 97 min (~ 5800 s) nach Durchführung der SDE aus. Mit einer geringen Wahrscheinlichkeit von ca. 3.E-03 erst später als 97 min nach Durchführung der SDE aus.

Die Verteilung der Zeitdifferenzen bei schwachen Schädigungen (<20 %) ist wesentlich enger. Die frühesten Zeitpunkte wann ein DE-Heizrohr mit schwacher Schädigung nach Durchführung der SDE ausfällt liegt bei ca. 68 min. Mit 95%iger Wahrscheinlichkeit erfolgt das DEHEIRO-Versagen bei Vorliegen einer schwachen Schädigung zwischen 75 und 103 min nach Durchführung der SDE.

Um die Abhängigkeit der Zeitdifferenz vom Schädigungsgrad des DE-Heizrohrs detaillierter zu beschreiben, können die Schädigungsgrade in feinere Klassen unterteilt werden. Die bedingten Verteilungen der feineren Schädigungsklassifizierung kann z. B. dazu dienen, einen Schwellenwert des Schädigungsgrades zu erkennen, bei dem ein besonders großer Einfluss auf die Zeitdifferenz zwischen DEHEIRO-Versagen und Zeitpunkt der SDE auftritt. Zur Veranschaulichung wurden die Schädigungen in folgende sechs Klassen eingeteilt: 50 – 70 %, 40 – 50 %, 30 – 40 %, 20 – 30 %, 10 – 20 % und < 10 %. Für jede dieser sechs Schädigungsklassen wurde die bedingte Verteilung bzgl. der Zeitdifferenzen $t_{Ausfall}$ - t_{SDE} berechnet, um wieviel später das DEHEIRO-Versagen nach Durchführung der SDE auftritt. Die bedingten Verteilungen der Zeitdifferenzen sind in Abb. 3.34 dargestellt.

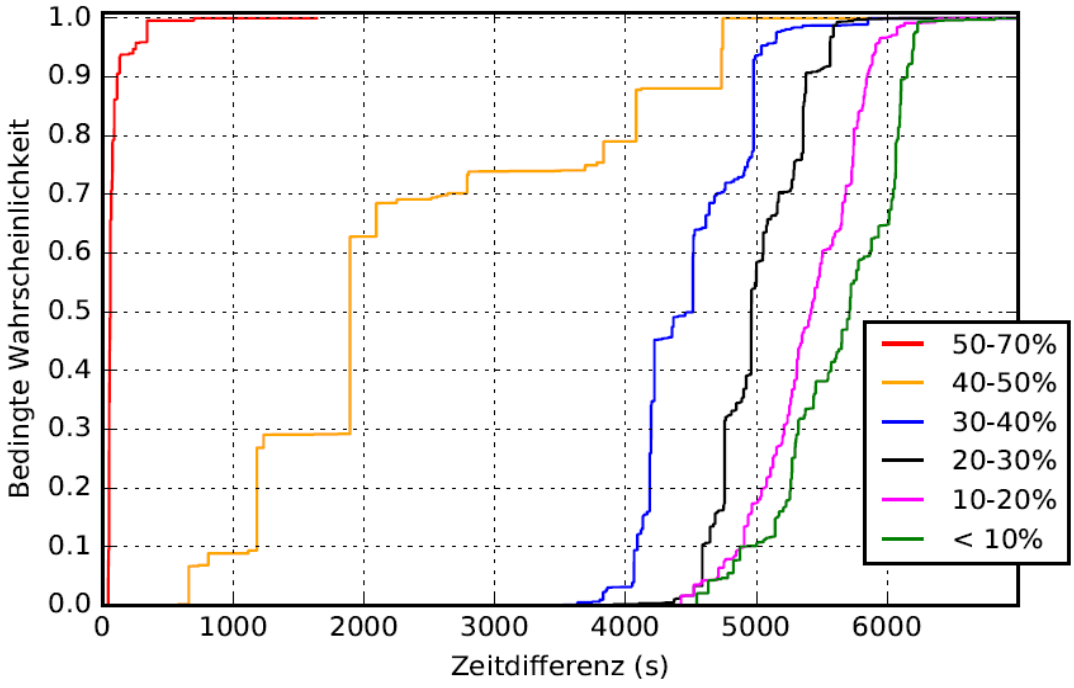


Abb. 3.34 Verteilung der Zeitdifferenz $t_{Ausfall}$ - t_{SDE} in Abhängigkeit des Schweregrades der DE-Heizrohr Schädigung

Aus den bedingten Verteilungen in Abb. 3.34 ist leicht zu erkennen, bei welchen Schädigungsgraden sich die größten Einflüsse auf die Zeitdifferenzen $t_{Ausfall}$ - t_{SDE} ergeben.

Während die Verteilungen der Zeitdifferenzen bzgl. der Schädigungsklassen < 40 % relativ nahe beieinanderliegen, weisen die bedingten Verteilungen der Zeitdifferenzen bzgl. der Schädigungsklassen 40 – 50 % und 50 – 70 % erhebliche Unterschiede auf. In Tab. 3.15 sind die Mittelwerte sowie 5 %-, 50 %- und 95 %-Quantile als Kennwerte der bedingten Verteilungen angegeben.

Tab. 3.15 Kennwerte bedingte Verteilungen der Zeitdifferenz $t_{Ausfall}$ - t_{SDE} (s)

Schädigung :	< 10%	10 - 20%	20 - 30%	30 - 40%	40 - 50%	50 - 70%
Mittelwert :	5636	5397	5013	4496	2331	79
5% - Quantil	4778	4707	4586	4065	658	41
50% - Quantil	5710	5417	4958	4513	1857	59
95% - Quantil	6199	5910	5562	5036	4733	238

Aus Tab. 3.15 ist abzulesen, dass die mittlere Zeitdauer zwischen dem Zeitpunkt, wann SDE durchgeführt wird, und DEHEIRO-Versagen mit zunehmendem Schädigungsgrad abnimmt. Während sich die mittleren Zeitdauern bei den Schädigungsklassen < 40 % um ca. 300 – 500 s voneinander unterscheiden, verringert sich die mittlere Zeitdifferenz bei Schädigungen von 40 – 50 % und 50 – 70 % signifikant um jeweils mehr als 2000 s. Um statistisch zu überprüfen, ob sich die bedingten Verteilungen voneinander unterscheiden, könnte an dieser Stelle z. B. der Kolmogorov-Smirnov Test auf die jeweiligen zu überprüfenden bedingten Verteilungen angewendet werden. Dies sei nur als Bemerkung beigefügt um zu veranschaulichen, dass die Ergebnisse einer MCDET-Analyse unter Verwendung des gesamten statistischen Methodenspektrums und deshalb für verschiedenste Fragestellungen ausgewertet werden können.

Anhand Abb. 3.34 bzw. Tab. 3.14 konnte gezeigt werden, dass die Zeit, wann das DE-Heizrohr nach Durchführung der SDE versagt, vom Schädigungsgrad des DE-Heizrohrs abhängt. Da das Versagen des DE-Heizrohrs im Wesentlichen durch die Druckdifferenz zwischen Primär und Sekundärkreis sowie durch die vorherrschende Temperatur im DE-Heizrohr bestimmt wird, soll im Folgenden untersucht werden, wie groß der Differenzdruck und die Temperatur zum Zeitpunkt des DEHEIRO-Versagens in Abhängigkeit der einzelnen Schädigungsklassen ist. Hierzu zeigt Abb. 3.35 die bedingten Verteilungen des Differenzdruckes zum Zeitpunkt des DEHEIRO-Versagens.

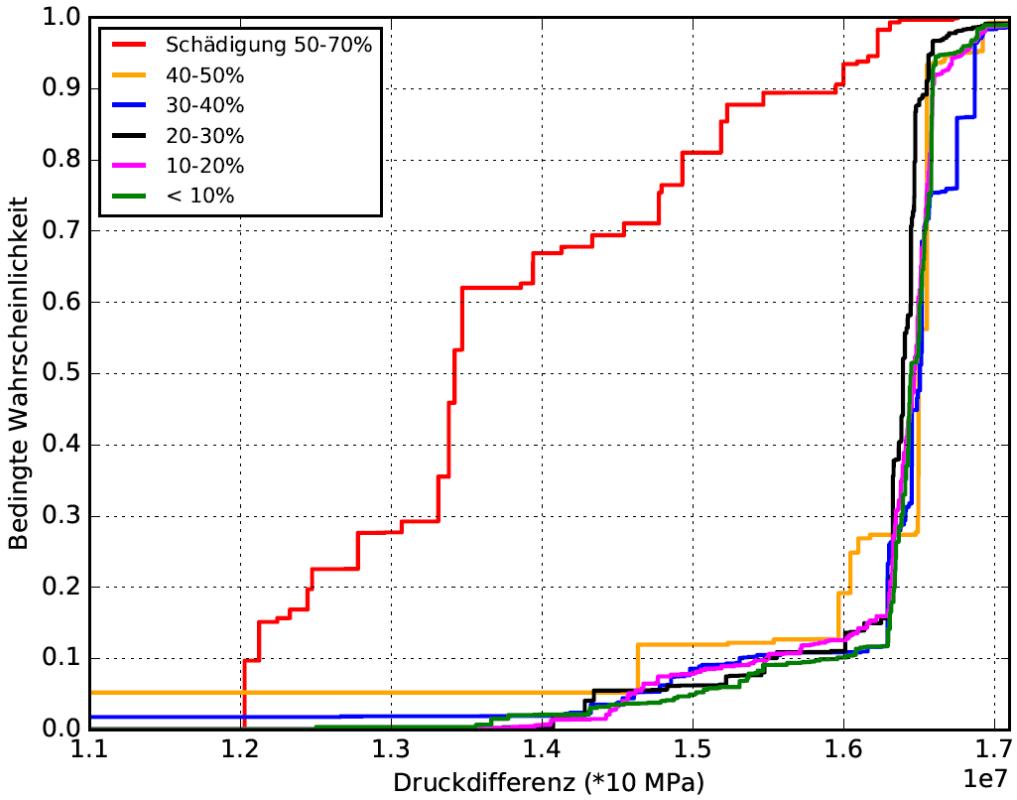


Abb. 3.35 Bedingte Verteilung der Druckdifferenz zum Zeitpunkt des DEHEIRO-Versagens in Abhängigkeit der DE-Heizrohr Schädigung

Bis auf die Schädigungsklasse 50 – 70 % weisen in Abb. 3.35 alle Schädigungsklassen eine ähnliche Verteilung auf. Diese sind dadurch gekennzeichnet, dass mit Wahrscheinlichkeiten von knapp 90 % das DEHEIRO-Versagen bei Druckdifferenzen > 16 MPa erfolgt. Für die Schädigungsklasse 40 – 50 % beträgt die Wahrscheinlichkeit ca. 80 %. Demgegenüber erfolgt in der Schädigungsklasse 50 – 70 % das DEHEIRO-Versagen mit einer Wahrscheinlichkeit von 0.8 zwischen 12 und 15 MPa Druckdifferenz. Druckdifferenzen > 16 MPa liegen hier nur mit einer Wahrscheinlichkeit von ca. 7 % vor.

Interessant erscheint noch die Tatsache, dass in der Schädigungsklasse 50 – 70 %, beim DEHEIRO-Versagen keine geringeren Druckdifferenzen als 12 MPa vorliegen. In allen anderen Schädigungsklassen konnten Sequenzen beobachtet werden, bei denen zum Zeitpunkt des DEHEIRO-Versagens Druckdifferenzen < 8 MPa vorliegen. Die Wahrscheinlichkeiten, dass Druckdifferenzen < 8 MPa vorliegen, sind mit < 0.01 allerdings sehr gering, wie aus Abb. 3.36 zu erkennen ist. Diese geringen Druckdifferenzen sind jedoch mit hohen Temperaturen im DE-Heizrohr verbunden, wie anhand Abb. 3.30 bereits gezeigt wurde. Zum Zeitpunkt des DEHEIRO-Versagens liegen Differenzdrücke < 10 MPa ausschließlich zusammen mit Temperaturen > 600 °C vor. Für die geringeren

Schädigungsklassen 10 – 20 % und < 10 % sind die Temperaturen bei Differenzdrücken < 10 MPa noch höher und liegen bei > 680 °C.

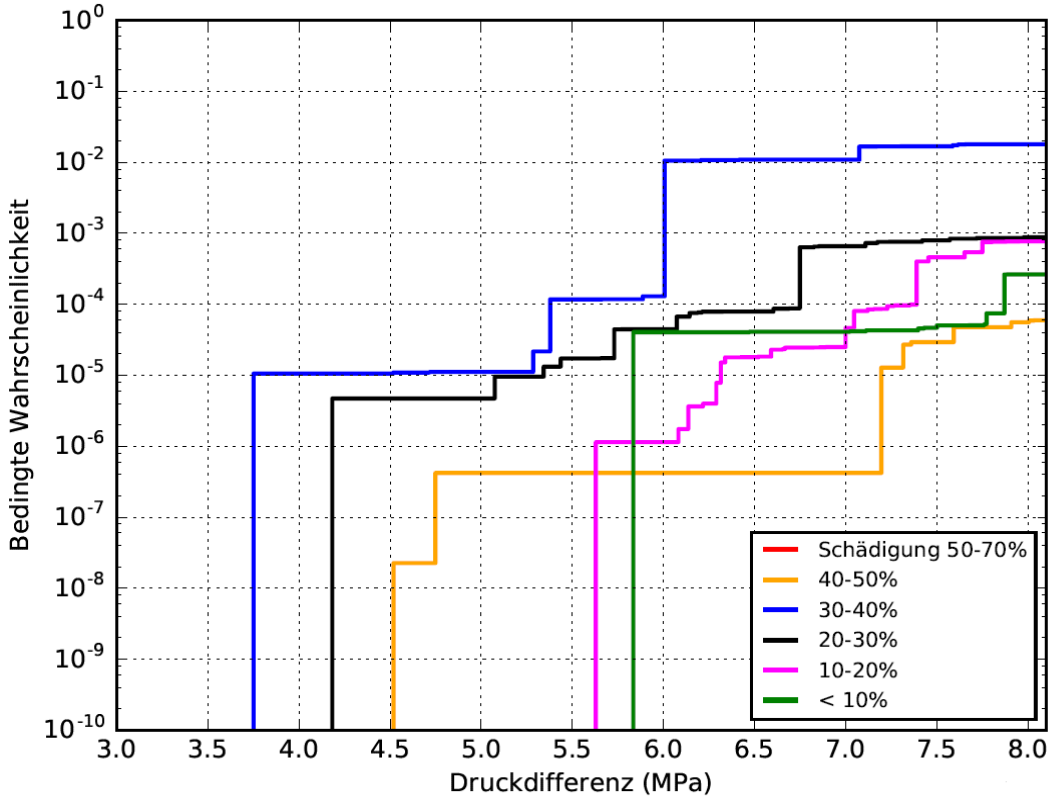


Abb. 3.36 Bedingte Verteilung der Druckdifferenzen < 8 MPa zum Zeitpunkt des DEHEIRO-Versagens in Abhängigkeit der DE-Heizrohr Schädigung

In den herkömmlichen PSA wurde als Ausfallkriterium immer nur ein bestimmter Wert betrachtet, bei dessen Erreichen eine Komponente ausfällt, z. B. Versagenstemperatur oder Versagensdruck. Realistischerweise ist allerdings davon auszugehen, dass für die Belastungen des DE-Heizrohrs nicht nur der Differenzdruck oder die Temperatur maßgeblich ist, die das DE-Heizrohr zum Zeitpunkt des Ausfalls hat, sondern auch die Zeitdauer, wie lange z. B. hohe Temperaturen oder Drücke anstehen und die Komponente belasten. Um die Möglichkeiten zu demonstrieren, in welchem Umfang die Ergebnisse einer MCDET-Analyse ausgewertet werden können, sollen für das Beispiel 1 abschließend die bedingten Verteilungen der Zeitdauern berechnet werden, wie lange Differenzdrücke von beispielsweise > 14 MPa von der Durchführung der SDE bis zum DEHEIRO-Versagen anstehen. Die Verteilungen werden wieder unter der Bedingung der einzelnen Schädigungsklassen berechnet. Abb. 3.37 zeigt die bedingten Verteilungen der Zeitdauern, wie lange Druckdifferenzen > 14 MPa zwischen der Durchführung der SDE und dem DEHEIRO-Versagen in den jeweiligen Schädigungsklassen anstehen.

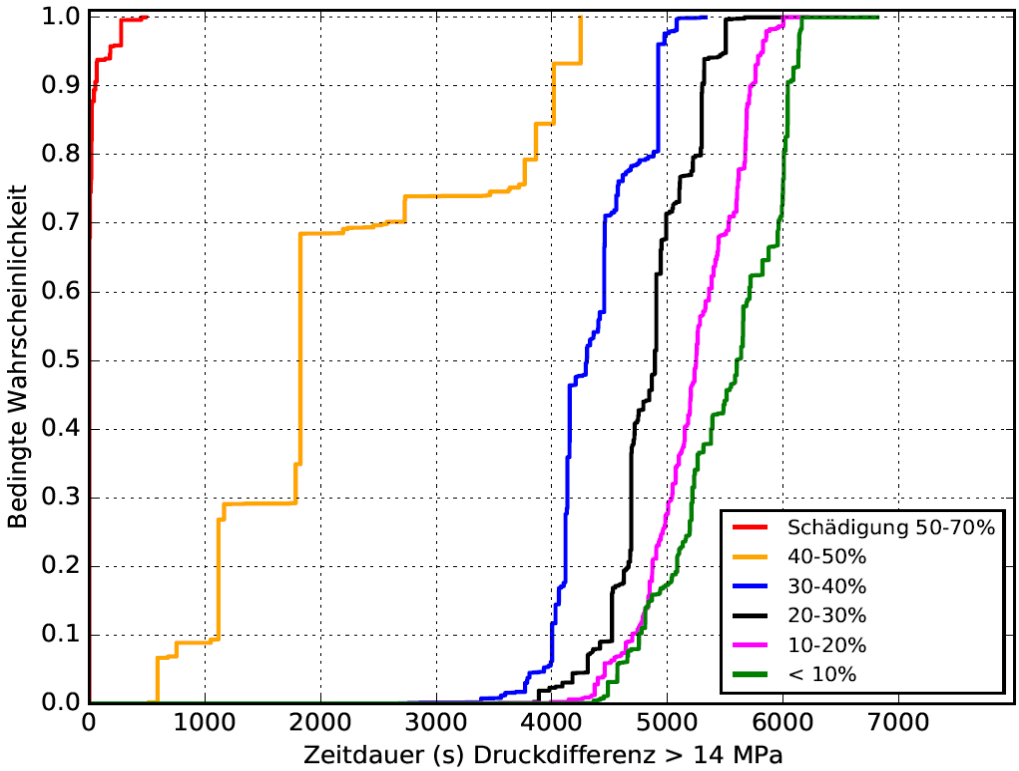


Abb. 3.37 Bedingte Verteilung der Zeitdauern, wie lange Druckdifferenzen > 14 MPa zwischen der Durchführung der SDE und DEHEIRO-Versagen anstehen

Abb. 3.37 zeigt eine Abhängigkeit der Zeitdauern vom Schweregrad der Schädigungen. Je größer die Schädigung desto kürzer sind die Zeitdauern von Druckdifferenzen > 14 MPa. Besonders deutlich wird dies in der Klasse der Schädigungen von 50 – 70 %. In dieser Schädigungsklasse ist die Situation gegeben, dass mit einer Wahrscheinlichkeit von ca. 0.68 zwischen SDE und DEHEIRO-Versagen keine Differenzdrücke > 14 MPa erreicht wurden und somit die Zeitdauer 0 beträgt. D. h., bei diesen schweren Schädigungen reichen schon kleinere Differenzdrücke aus, um das DE-Heizrohr versagen zu lassen. Bzgl. der Schädigungen von 40 – 50 % zeigt sich ein signifikanter Unterschied zu längeren Zeitdauern hin, der sich bzgl. der Schädigungen < 40 % nochmals fortsetzt. Unterschiede zeigen sich bzgl. der Schädigungsklassen < 40 % auch weiterhin, die Unterschiede in den Zeitdauern sind jedoch nicht mehr so ausgeprägt. In Tab. 3.16 sind die 5 %-, 50 %- und 95 %-Quantile der bedingten Verteilungen angegeben.

Tab. 3.16 5 %-, 50 %- und 95 %-Quantile der bedingten Verteilungen der Zeitdauern anstehender Druckdifferenzen > 14 MPa in den einzelnen Schädigungsklassen

Schädigung :	< 10%	10 - 20%	20 - 30%	30 - 40%	40 - 50%	50 - 70%
5% - Quantil	4565	4455	4308	3931	570	0
50% - Quantil	5598	5248	4889	4300	1821	0
95% - Quantil	6131	5823	5504	4919	4119	179

Neben den bisher gezeigten Auswertungen könnten auch die Zeitdauern bzgl. des Auftretens mehrerer Größen analysiert werden, z. B. Zeitdauern, wie lange Druckdifferenzen > 12 MPa und Temperaturen des DE-Heizrohrs zwischen 500 und 600 °C anstehen.

Die bisher dargestellten Auswertungen zeigen aber bereits umfassend verschiedene Analysemöglichkeiten, die eine IDPSA unter Verwendung der MCDET-Methode bietet. Die Auswertungen der Ergebnisse einer MCDET-Analyse ermöglichen, dass wesentlich fundiertere und detailliertere probabilistische Aussagen bzgl. relevanter Prozessgrößen und Zusammenhänge abgeleitet werden können als dies bisher möglich war. Dies wird bereits dadurch sichtbar, wenn die in diesem Bericht präsentierten probabilistischen Aussagen aus der MCDET/ATHLET-CD Analyse mit der probabilistischen Aussage aus dem Datenband des PSA-Leitfadens verglichen werden. Die umfangreichen und detaillierten probabilistischen Ergebnisse, die man aus einer MCDET-Analyse erzeugt, können dazu beitragen, zusätzliche Erkenntnisse bzgl. des Prozessverhaltens abzuleiten und das System- und Prozessverhalten unter Berücksichtigung von Unsicherheiten besser einzuschätzen. Aufgrund dieser Kenntnisse könnten Maßnahmen und Strategien entwickelt werden, die zu einer Verbesserung des Sicherheitsniveaus der Anlage führen.

Beispiel 2:

Die Fragestellungen zum induzierten Dampferzeuger-Heizrohrleck in einer klassischen PSA beziehen sich auf folgende Aspekte:

- Wahrscheinlichkeit für Heizrohr-Vorschädigungen
- Verhalten von Sicherheitsventilen
- Versagen von heißer Leitung

Heizrohr-Vorschädigungen:

In der klassischen PSA wird aufgrund bisher durchgeführter Analysen davon ausgegangen, dass ein Versagen eines DE-Heizrohrs nur in einem Hochdruck-Unfallszenario und nur dann auftreten kann, wenn ein DE-Heizrohr zu Beginn des Unfallablaufs eine Vorschädigung aufweist. Die Wahrscheinlichkeit einer Vorschädigung und deren Auswirkung auf das DEHEIRO-Versagen wurde in bisherigen PSA nicht berücksichtigt.

In diesem Projekt wurde erstmals versucht, ein Wahrscheinlichkeitsmodell zur Schätzung der aleatorischen Unsicherheit einer Vorschädigung eines DE-Heizrohrs zu Beginn des Unfallablaufs herzuleiten (s. Abschnitt 3.3.2.3). Die Modellierung der Vorschädigungen von DE-Heizrohren basiert dabei insbesondere auf Informationen und Stellungnahmen des KTA. Das entwickelte Modell liefert eine Wahrscheinlichkeitsverteilung des Ausmaßes der Schädigung, mit den das DE-Heizrohr zu Beginn des Unfallablaufs belastet ist. Diese Wahrscheinlichkeitsverteilung kann als aleatorische Unsicherheit des Ausmaßes der Heizrohrschädigung betrachtet werden. In Abschnitt 3.4.2 wurde gezeigt, wie diese aleatorische Unsicherheit in die MCDET/ATHLET-CD Analyse eigebunden wurde. Bei der Darstellung ausgewählter Ergebnisse in Abschnitt 3.5.2 wurde demonstriert, welche probabilistischen Aussagen bzgl. des Einflusses der Vorschädigungen auf das DEHEIRO-Versagen aus der MCDET-Analyse ermittelt werden konnten.

Um einen Unterschied zur klassischen PSA zu verdeutlichen stelle man sich die Frage, wie man die aleatorische Unsicherheit der Heizrohrschädigung zu Beginn des Unfallablaufs im Rahmen einer klassischen PSA eingebunden hätte. Man würde einige wenige deterministische Rechnungen mit bestimmten ausgewählten Heizrohrschädigungen durchführen und diese wenigen Informationen verwenden, um daraus die Wahrscheinlichkeit eines DEHEIRO-Versagens zu bestimmen. Eine weitere Frage stellt sich, wie die Variation anderer aleatorischer Größen in den wenigen Rechnungen berücksichtigt werden.

Ein gravierender Unterschied einer MCDET-Analyse zur klassischen PSA-Methodik besteht somit darin, dass aleatorische Unsicherheiten über die MCDET-Methodik repräsentativ und wesentlich umfassender in Sicherheitsanalysen berücksichtigt werden können als mit der klassischen PSA-Methodik. Durch die wesentlich umfangreicheren Rechnungen ergibt sich eine fundierte Datengrundlage, mit der detailliertere und genauere probabilistische Ergebnisse erzielt werden können als über die Vorgehensweise der klassischen PSA. Aus diesen probabilistischen Ergebnissen können zusätzliche

Kenntnisse bzgl. des Anlagenverhaltens in Abhängigkeit der berücksichtigten Unsicherheiten gewonnen werden.

Dabei ist jedoch zu betonen, dass grundsätzliche Modellannahmen und Modell-vereinfachungen in den Datensätzen verbleiben und die Frage nach einer möglichst guten Validierung des Modells notwendig ist.

DH-Ventile:

In einer klassischen PSA bezieht sich der Ausfall der Druckbegrenzungsventile im Rahmen des Unfallablaufs lediglich auf den ersten Anforderungszyklus des jeweiligen Ventils. Dabei kann es jeweils im Ausfallmodus ‚öffnet nicht ' oder ‚schließt nicht' ausfallen oder es arbeitet auslegungsgemäß weiter. Bezieht man die Ausfallwahrscheinlichkeit eines Ventils lediglich auf seinen 1. Anforderungszyklus, ergibt sich folgende Situation:

Angenommen, die Wahrscheinlichkeit beträgt $p_{ön}$, dass das Ventil pro Anforderungszyklus geschlossen versagt. In der klassischen PSA wäre dann die Wahrscheinlichkeit, dass das Ventil geschlossen versagt $p_{ön}$. Mit der Wahrscheinlichkeit $(1-p_{ön})$ fällt das Ventil nicht aus und funktioniert auslegungsgemäß. Diese Wahrscheinlichkeiten gehen als Zuverlässigkeitswerte in die PSA ein.

Da die DH-Ventile in einem Hochdruck-Unfallablauf zyklischen Anforderung unterliegen, wird das Ventil, wenn es nicht beim 1. Anforderungszyklus ausgefallen ist, im weiteren Ablauf zu einem bestimmten Zeitpunkt zum zweiten Mal angefordert. Auch hier könnte das Ventil mit der Wahrscheinlichkeit $p_{ön}$ ausfallen. D. h. das Ventil kann beim ersten oder zweiten Anforderungszyklus ausfallen. Die Wahrscheinlichkeit, dass das Ventil bei ersten oder zweiten Anforderungszyklus geschlossen ausfällt, ist gegeben durch:

$p_{ön} + (1- p_{ön}) \cdot p_{ön.}$.
Ist $p_{ön}$ sehr klein (z. B. < 0.01), dann ist $(1 - p_{ön}) \sim 1$ und es gilt:
$p_{ön} + (1- p_{ön}) \cdot p_{ön} \approx 2 \cdot p_{ön.}$

Entsprechend gilt für die Wahrscheinlichkeit, dass das Ventil auch nach dem zweiten Anforderungszyklus nicht ausgefallen ist und auslegungsgemäß funktioniert:

$$1 - [\, p_{ön} + (1- p_{ön}) \cdot p_{ön} \,] = (1- p_{ön})^2$$

Eine genauere und realitätsnähere probabilistische Modellierung der Zuverlässigkeit eines zyklisch angeforderten Ventils, resultiert in einer höheren Ausfallwahrscheinlichkeit und geringeren Zuverlässigkeit des Ventils, als wenn nur die Ausfallwahrscheinlichkeit des Ventils bei seinem ersten Anforderungszyklus berücksichtigt wird. Demzufolge stellt sich die Frage, ob die Zuverlässigkeit der DH-Ventile in der klassischen PSA nicht überschätzt und die Ausfallwahrscheinlichkeiten unterschätzt werden.

An diesem Beispiel wird deutlich, dass eine zu grobe bzw. vereinfachte Modellierung zu einer zu optimistischen Einschätzung der Zuverlässigkeit von Komponenten führen kann. Aus diesem Grund sollte in einer PSA grundsätzlich nicht nur auf eine möglichst genaue Abbildung der Systemtechnik Wert gelegt werden, sondern auch auf eine möglichst genaue und realitätsnahe probabilistische Modellierung zur Schätzung der aleatorischen Unsicherheit zufälliger Einflussgrößen.

In Abschnitt 3.3.2.2 wurde ein Wahrscheinlichkeitsmodell zur Schätzung des Ausfallverhaltens der Druckbegrenzungsventile hergeleitet. Mit diesem Modell werden die Ausfallwahrscheinlichkeiten der Ventile in Abhängigkeit ihrer Anforderungszyklen ermittelt. Aus diesem Wahrscheinlichkeitsmodell können die aleatorischen Unsicherheiten ermittelt werden, bei welchen Anforderungszyklus das jeweilige Ventil geschlossenen oder offenen ausfällt. Die Einbindung dieser aleatorischen Unsicherheiten in die MCDET-Analyse wird ausführlich in Abschnitt 3.4.1 beschrieben.

Hier zeigt sich der grundlegende Vorteil der MCDET-Methodik darin, dass aleatorische Unsicherheiten, die durch genauere probabilistische Modelle ermittelt wurden, umfassend in eine MCDET-Analyse eingebunden werden können. In einer klassischen PSA würden diese aleatorischen Unsicherheiten, z. B. bzgl. der Wahrscheinlichkeitsverteilungen bzgl. des Versagenszyklus der jeweiligen DH-Ventile, nur rudimentär berücksichtigt werden können. Durch die umfassende Einbindung aleatorischer Unsicherheiten unter Verwendung der MCDET-Methode können auch die Einflüsse der Zufallsgrößen auf den Prozessablauf genauer analysiert und quantifiziert werden. Diese Analysemöglichkeiten bietet die Methodik der klassischen PSA nicht.

Versagen Heißer Leitung:

Zur Bewertung der Konsequenzen eines thermisch-induzierten Ausfalls des DE-Heizrohrs ist die Integrität der HKL bzw. der VAL von besonderer Bedeutung. Da bei einem Ausfall des DE-Heizrohrs das Containment umgangen wird, können radioaktive Stoffe vom Primärkreis in die Umgebung freigesetzt werden. Wenn die HKL oder VAL nach dem Versagen des Heizrohrs zusätzlich ausfällt, erfolgt eine Druckentlastung des Primärkreises und ein weiterer Freisetzungspfad in das Containment. Unter diesem Aspekt ist die Frage von Interesse, ob nach dem DEHEIRO-Versagen zusätzlich die HKL oder VAL ausfällt und wenn ja, wieviel Zeit bis dahin vergeht.

Um diese Fragen beantworten zu können, müssen in der klassischen PSA die entsprechenden Informationen aus deterministischen Rechnungen verwendet werden. Die dazu durchgeführten deterministischen Rechnungen beschränken sich dabei auf einige wenige Rechnungen unter festen Randbedingungen. Zufällige Variationen bzgl. relevanter aleatorischer Größen (z. B: zufälliger Schädigungsgrad des DE-Heizrohrs zu Beginn des Unfallablaufs oder zufälliger Versagenszyklus der jeweiligen DH-Ventile), werden in diesen wenigen Rechnungen nicht berücksichtigt. Die Informationen aus den deterministischen Rechnungen werden mehr oder weniger grob unter Verwendung der Wahrscheinlichkeiten der gewählten Randbedingungen probabilistisch bewertet. Die Einflüsse, wann und in welcher Reihenfolge bestimmte Ereignisse zufallsbedingt eintreten und den Unfallablauf beeinflussen, werden hier nicht berücksichtigt.

Unter Verwendung der MCDET-Methode können solche zufällig variierenden Einflüsse berücksichtigt und probabilistisch bewertet werden, ohne dass der Experte in die Rechnungen eingreifen muss, um die entsprechenden Ereignisse, die zu zufälligen Zeitpunkten eintreten, im Eingabedatensatz zu spezifizieren. In MCDET wird dies automatisch gesteuert, was eine erhebliche Vereinfachung für den Anwender bedeutet. Zugleich wird durch den Automatismus der subjektive Einfluss verringert, den der Experte durch seine Wahl der zugrunde gelegten Ereignisse in der Analyse bewirkt.

Durch die Auswertung der MCDET-Ergebnisse wurden in Abschnitt 3.5.2 verschiedene probabilistische Ergebnisse im Zusammenhang der HKL und VAL beschrieben:

- Wahrscheinlichkeit eines HKL-Ausfalls vor bzw. nach DEHEIRO-Versagen (siehe Tab. 3.14)
- Wahrscheinlichkeit eines VAL-Ausfalls vor bzw. nach DEHEIRO-Versagen (siehe Tab. 3.14)
- Bedingte Wahrscheinlichkeitsverteilung der Zeitdifferenz zwischen DEHEIRO-Versagen und Bruch der HKL für Schädigungen < 20 % und Schädigungen von 20 – 70 % (s. Abb. 3.23). Aus diesen bedingten Wahrscheinlichkeitsverteilungen können verschiedene Wahrscheinlichkeitsaussagen bzgl. der Zeit abgeleitet werden, wann die HKL nach einem DEHEIRO-Versagen ausfällt.

Ein erheblicher Nutzen besteht u. a. darin, dass die probabilistischen Ergebnisse einer MCDET-Analyse für eine klassische PSA verwendet werden können. Wie dies umgesetzt werden kann, wird im nachfolgenden Abschnitt 3.6.2 anhand eines Beispiels beschrieben.

3.6.2 Nutzen der Ergebnisse einer MCDET-Analyse zur Erweiterung und Verbesserung von Ereignisbäumen im Rahmen der klassischen PSA

Im Vorhaben 3615R01345 wurde untersucht, ob und wie ein klassischer Ereignisbaum durch die Ergebnisse der im Vorhaben RS1529 durchgeführten MCDET/ATHLET-CD Analyse zum thermisch induzierten DE-Heizrohrversagen ergänzt werden kann. Zur Erweiterung der Struktur des Ereignisbaumes wurden probabilistische Aussagen zu folgenden Fragen ergänzend benötigt.

DH-Ventile:

i) Wahrscheinlichkeit, dass mindestens ein DH-Ventil offen ausfällt

ii) Zeitpunkt des Versagens von mind. ein DH-Ventil in offenem Zustand

iii) Wahrscheinlichkeit, dass alle drei DH-Ventile geschlossen versagen

iv) Zeitpunkt, wann alle drei DH-Ventile geschlossen versagt haben

v) Wahrscheinlichkeit, dass mindestens eins der drei DH-Ventile normale Funktion aufweist.

Notfallmaßnahme SDE:

vi) Zeitpunkt wann die Druckentlastung der DE durchgeführt wird.

Heiße Leitung (HKL) und Volumenausgleichsleitung (VAL):

vii) Zeitpunkt, wann Leck an HKL bzw. VAL auftritt.

viii) Zeitdifferenz zwischen DEHEIRO-Versagen und Ausfall der HKL bzw. VAL

ix) Wahrscheinlichkeit für Leck an HKL unter der Bedingung, dass alle drei DH-Ventile geschlossen ausgefallen sind.

x) Wahrscheinlichkeit für Leck an HKL oder VAL unter der Bedingung, dass alle drei DH-Ventile geschlossen ausgefallen sind.

Vorschädigung des DE-Heizrohrs:

xi) Wahrscheinlichkeit, dass Ausmaß der Vorschädigung zu Beginn des Unfallablaufs < 20 %, 20 – 40% und 40 – 70% beträgt.

DEHEIRO-Versagen:

xii) Zeitpunkt, wann DEHEIRO-Versagen nach dem einleitenden Ereignis in Abhängigkeit des Schädigungsgrades auftritt.

xiii) Wahrscheinlichkeit für DEHEIRO-Versagen in Abhängigkeit des Zeitpunktes, wann SDE erfolgt.

Zum besseren Verständnis soll zunächst erläutert werden, wie probabilistische Aussagen bzgl. der Fragen i) – xiii) aus den Ergebnissen der MCDET/ATHLET-CD Analyse ermittelt werden. Wie bereits in Abschnitt 3.5.2 erwähnt, wurden in der Analyse 100 dynamische Ereignisbäume (DETs) mit insgesamt 4216 Unfallsequenzen unter unterschiedlichen Bedingungen gerechnet. Zur Veranschaulichung sind in Abb. 3.38 z. B. die Sequenzen des ersten dynamischen Ereignisbaums (DET 1) für die Prozessgröße ‚Kühlmitteldruck in der heißen Leitung' dargestellt.

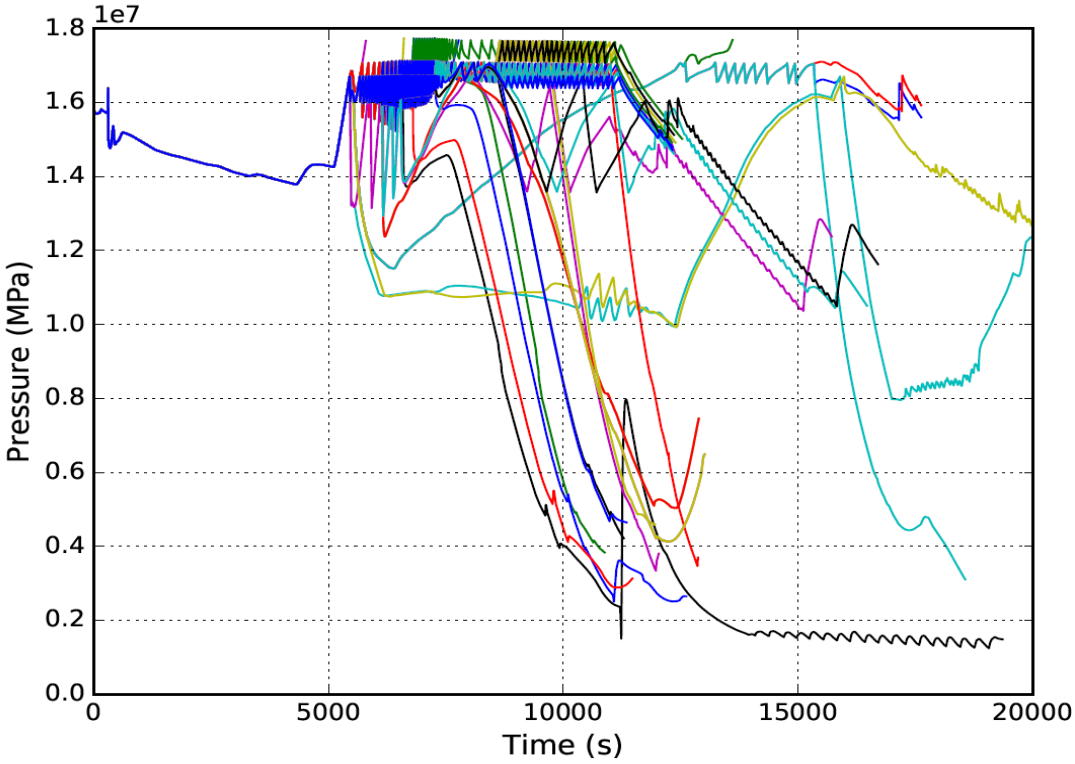


Abb. 3.38 Zeitlicher Verlauf des Kühlmitteldrucks in der heißen Leitung für die Sequenzen von DET1

DET 1 enthält 36 Sequenzen, die sich durch verschiedene zufällige Ereignisse unterscheiden. Schon allein aus den Verläufen in Abb. 3.38 erkennt man, welchen erheblichen Einfluss die in der Analyse berücksichtigten aleatorischen Unsicherheiten auf die Prozessabläufe innerhalb eines dynamischen Ereignisbaumes haben. Da sich jeder dynamische Ereignisbaum von den anderen unterscheidet, verstärkt sich die Variation der Abläufe, wenn man die Sequenzen über mehrere DETs darstellt. Dies wird in Abb. 3.39 veranschaulicht in dem die zeitlichen Verläufe des Kühlmitteldrucks in der heißen Leitung von drei DETs dargestellt ist.

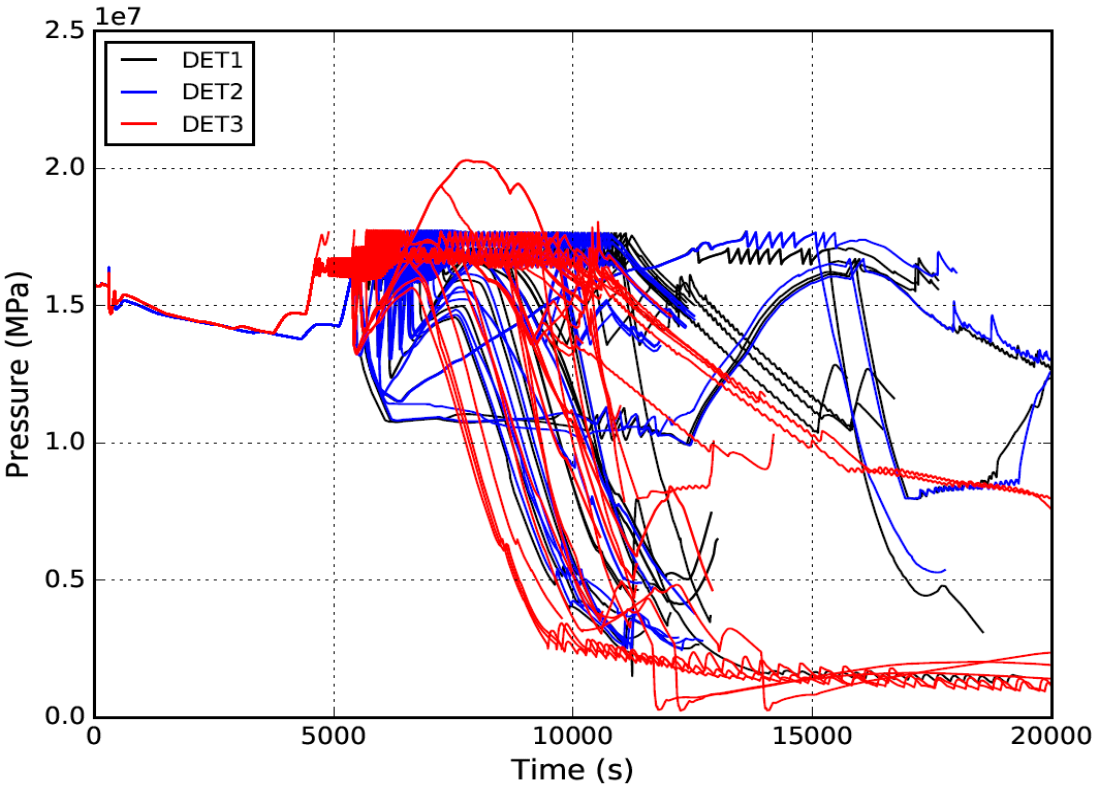


Abb. 3.39 Zeitlicher Verlauf des Kühlmitteldrucks in der heißen Leitung für die Sequenzen von DET1, DET2 und DET3

Für jede einzelne gerechnete Sequenz liegt neben dem zeitlichen Verlauf der Prozessgröße die zusätzliche Information vor, welche Zufallsereignisse und epistemischen Werte dem Verlauf zugrunde liegen und mit welcher Wahrscheinlichkeit die jeweilige Sequenz eintritt. Entsprechend der in den Abb. 3.38 und Abb. 3.39 dargestellten Prozessgröße können auch die Verläufe beliebiger anderer Größen, die in ATHLET über gcsm-Signale berechnet und für die MCDET-Analyse definiert wurden, gelesen und entsprechend ihrer zugeordneten Wahrscheinlichkeiten probabilistisch ausgewertet werden. Um die zeitlichen Verläufe der Prozessgrößen über alle Sequenzen lesen und probabilistisch auswerten zu können, wurden verschiedene Routinen entwickelt, die im Rahmen des Postprocessing angewendet werden, um z. B. Wahrscheinlichkeiten und Verteilungen von Ereignissen berechnen zu können. Zur Berechnung der gesuchten Wahrscheinlichkeiten und Verteilungen wurden alle 4216 Unfallsequenzen gelesen und diejenigen Sequenzen ermittelt, bei denen das interessierende Ereignis aufgetreten ist. Da jeder dieser Sequenzen eine Eintrittswahrscheinlichkeit zugeordnet ist, konnten daraus die entsprechenden probabilistischen Berechnungen durchgeführt werden.

Im Folgenden werden die Ergebnisse zu den oben genannten Fragen i) – xiii) dargestellt:

DH-Ventile:

In MCDET wurde der Versagenszyklus für die jeweiligen DH-Ventile zufällig aus einer Geometrischen-Verteilung ausgespielt. Die Geometrische-Verteilung ist das Ergebnis eines in diesem Vorhaben entwickelten Wahrscheinlichkeitsmodells für das Ausfallverhalten der DH-Ventile in Abhängigkeit der Anforderungszyklen. Die Herleitung des Wahrscheinlichkeitsmodells ist in Abschnitt 3.3.2.2 beschrieben.

Aus den Ergebnissen der MCDET/ATHLET-CD Analyse können nun für jede Sequenz die Zeitpunkte ermittelt werden, wann die DH-Ventile (AV, SiV1, SiV2) innerhalb der Rechenzeit offen bzw. geschlossen versagt haben und mit welcher Wahrscheinlichkeit dies geschieht. Die Auswertung der 4216 gerechnet Sequenzen haben zu folgenden Ergebnissen geführt.

i) P (mindestens ein DH-Ventil in Offenstellung ausgefallen) = 0.1605

In diesem Zusammenhang wären auch detaillierte Aussagen möglich, z. B.

P (nur DH-AV in Offenstellung ausgefallen) = 0.160499
P (nur SiV1 in Offenstellung ausgefallen) = 4.4E-07
P (DH-AV und SiV1 in Offenstellung ausgefallen) = 4.78E-07

Der offene Ausfall von DH-AV und SiV1 ergibt sich durch zwei unterschiedliche Ereignisse:

1. DH-AV und SiV1 fallen aufgrund eines 2v3-GVA aus bei denen das DH-AV und SiV1 betroffen ist p= 4.243E-07.
2. DH-AV fällt als Einzelfehler offen aus und es liegt ein 2v3-GVA bzgl. SiV1 und SiV2 vor. Dieses Ereignis tritt mit der Wahrscheinlichkeit p = 5.404E-08 auf.

Aus diesen Detailergebnissen ist ein wesentlicher Vorteil der MCDET Methodik gegenüber der reinen Monte-Carlo Simulation zu erkennen. Wären die 4216 Sequenzen aufgrund reiner Monte-Carlo Simulation ermittelt worden, würden sich allenfalls Wahrscheinlichkeiten von ca. 2.3E-4 ergeben. Dies wäre die Wahrscheinlichkeit, wenn ein Ereignis nur in einer Sequenz vorkommt.

Mit MCDET können dagegen auch sehr kleine Wahrscheinlichkeiten (z. B. < 1.E-06 oder < 1.E-07) ermittelt werden, obwohl nur 4216 Sequenzen gerechnet worden sind. Dies liegt an dem Umstand, dass MCDET eine so genannte varianzreduzierende Methode mit der Eigenschaft ist, dass sie gegenüber der reinen Monte-Carlo Simulation bei gleichem Stichprobenumfang genauere Schätzungen liefert.

ii) Zeitpunkt des Versagens von mindestens einem DH-Ventil in offenem Zustand:

Die Ausfallzeitpunkte der jeweiligen DH-Ventile sind Zufallsgrößen. Daraus folgt, dass die Ausfallzeitpunkte mehr oder weniger stark variieren und einer Verteilung folgen. Aus diesem Grund wird zur Beantwortung der obigen Fragestellung die bedingte Verteilungsfunktion des Versagenszeitpunktes ermittelt. Die Bedingung des Versagens von mindestens einem DH-Ventil in Offenstellung ist genau dann gegeben, wenn eines der DH-Ventile zum ersten Mal offen versagt. Die bedingte Verteilung der Versagenszeit von mindesten einem DH-Ventil in Offenstellung ist in Abb. 3.40 grafisch dargestellt.

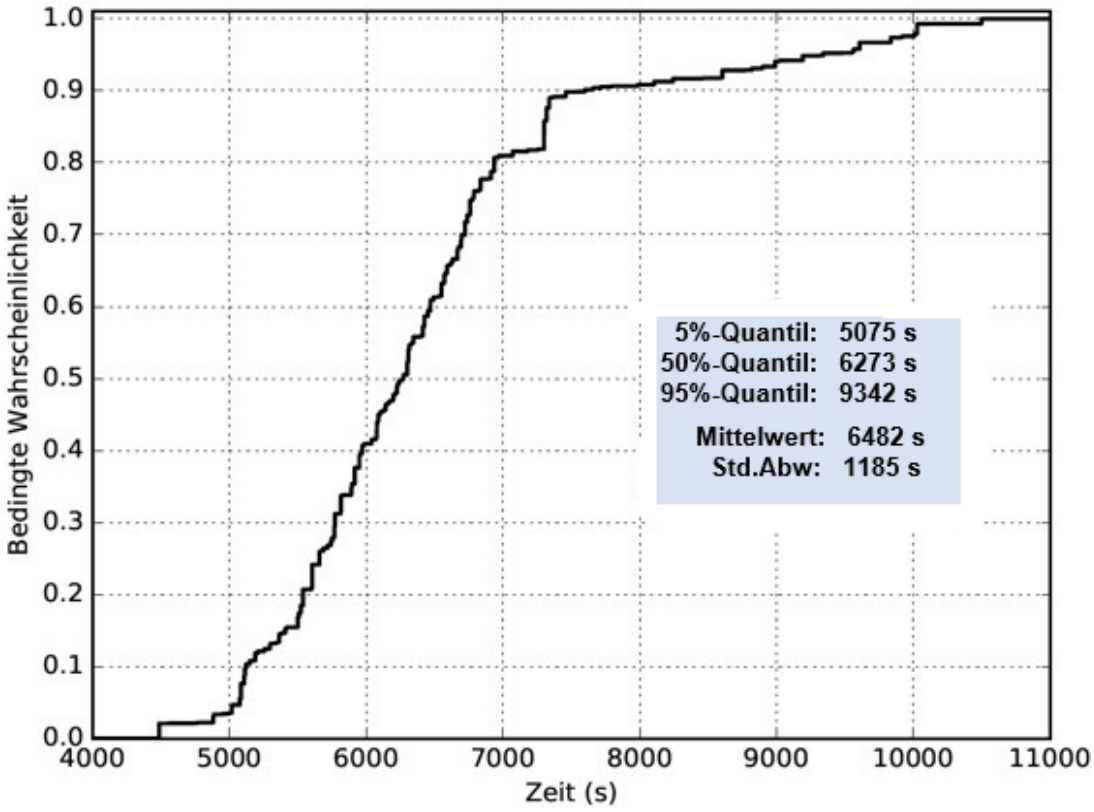


Abb. 3.40 Bedingte Verteilung des Versagenszeitpunktes von mindestens einem DH-Ventil in Offenstellung

Aus Abb. 3.40 können z. B. folgende Wahrscheinlichkeitsaussagen bzgl. des Versagenszeitpunktes abgeleitet werden, die dann ggf. zur Ergänzung des Ereignisbaums verwendet werden können. Unter der Bedingung des offenen Ausfalls von mindestens einem DH-Ventil nach dem einleitenden Ereignis beträgt die Wahrscheinlichkeit, dass der Ausfall

zwischen	75 und 90 min erfolgt	0.147
zwischen	90 und 120 min	0.67
zwischen	120 und 150 min	0.124
zwischen	150 und 180 min	5.85E-02
und später als	180 min	5.E-04

iii) Wahrscheinlichkeit, dass alle drei DH-Ventile geschlossen versagen:

Die Wahrscheinlichkeit, dass alle drei DH-Ventile geschlossen versagen setzt sich aus den folgenden Ereignissen zusammen:

- Alle drei Ventile fallen unabhängig voneinander geschlossen aus.
- Geschlossener Ausfall von zwei Ventilen durch 2v3-GVA und funktionierende Komponente fällt zusätzlich geschlossen durch unabhängigen Ausfall aus.
- Geschlossener Ausfall aller drei Ventile durch 3v3-GVA.

Die Wahrscheinlichkeit, dass alle drei DH-Ventile geschlossen versagen ergibt sich zu:
P (alle drei DH-Ventile geschlossen ausgefallen) = 1.996E-03

Für

- E_1 = DH-Ventile aufgrund unabhängiger Ausfälle geschlossen ausgefallen
- E_2 = DH-Ventile aufgrund eines 2v3-GVA und zusätzlichen unabhängigen Ausfall geschlossen ausgefallen
- E_3 = DH-Ventile aufgrund eines 3v3-GVA geschlossen ausgefallen
- Es wurden dabei folgende Wahrscheinlichkeiten ermittelt:

$P(E_1)$ = 1.906E-03
$P(E_2)$ = 2.896E-05
$P(E_3)$ = 5.078E-05

Der unerwartet hohe Beitrag der unabhängigen Ausfälle lässt sich folgendermaßen erklären:

Die Referenzwerte für ‚DH-AV öffnet nicht' und ‚SiV1 bzw. SiV2 öffnet nicht' wurden in Tab. 3.3 (s. Abschnitt 3.3.2.2) mit 3.09E-03 und 5.83E-03 ermittelt. Im Rahmen der klassischen PSA würde die Wahrscheinlichkeit, dass alle drei DH-Ventile auf Anforderung nicht öffnen, durch das Produkt der jeweiligen Referenzwerte berechnet, d. h.
$p = 3.09E\text{-}03 \cdot 5.83E\text{-}03 \cdot 5.83E\text{-}03 = 1.05E\text{-}7$.

Die Analyseergebnisse zeigen, dass wenn alle drei DH-Ventile im Rahmen des Unfallablaufs unabhängig voneinander geschlossen ausfallen, die Ausfälle der Ventile relativ früh, d. h. innerhalb ihrer ersten 20 Anforderungszyklen erfolgen. Über das Wahrscheinlichkeitsmodell, das in Abschnitt 3.3.2.2 unter Berücksichtigung der zyklischen Anforderungen hergeleitet wurde, ergeben sich die Wahrscheinlichkeiten, dass DH-AV bzw. die SiV bei den gegebenen Referenzwerten jeweils innerhalb der ersten 20 Anforderungszyklen ausfallen zu 0.116 bzw. 0.171. Die Wahrscheinlichkeit, dass alle drei DH-Ventile jeweils innerhalb ihrer ersten 20 Anforderungszyklen ausfallen, beträgt p = 3.42E-03. Die hier berechneten Werte beziehen sich auf die Referenzwerte der Wahrscheinlichkeiten (siehe Tab. 3.7) für einen frühen Ausfall, d. h. geschlossen oder offen. Der Unterschied zu dem oben ausgewiesenen Wert von 1.906E-3 ergibt sich dadurch, dass sich der oben ausgewiesene Wert nur auf den geschlossenen Ausfall bezieht und unter Berücksichtigung der epistemischen Unsicherheiten ermittelt wurde.

In diesem Beispiel wird deutlich, dass realistischere Modellierungen des Ausfallverhaltens von Komponenten zu probabilistischen Ergebnissen führen können, die man nach der Vorgehensweise der klassischen PSA bisher nicht erwarten würde.

iv) Zeitpunkt, wann alle drei DH-Ventile geschlossen versagt haben:

Wie bereits unter ii) bemerkt, sind die Ausfallzeitpunkte der jeweiligen DH-Ventile Zufallsgrößen, die mehr oder weniger stark variieren. Der Zeitpunkt des geschlossenen Versagens aller drei DH-Ventile folgt deshalb einer Wahrscheinlichkeitsverteilung. Aus diesem Grund wird zur Beantwortung der obigen Fragestellung die bedingte Verteilungsfunktion des Zeitpunktes ermittelt, wann alle DH-Ventile geschlossen ausgefallen sind. Die Bedingung des geschlossenen Versagens der DH-Ventil ist genau dann gegeben, wenn das letzte der DH-Ventile geschlossen versagt hat. Die bedingte Verteilung ist in Abb. 3.41 grafisch dargestellt.

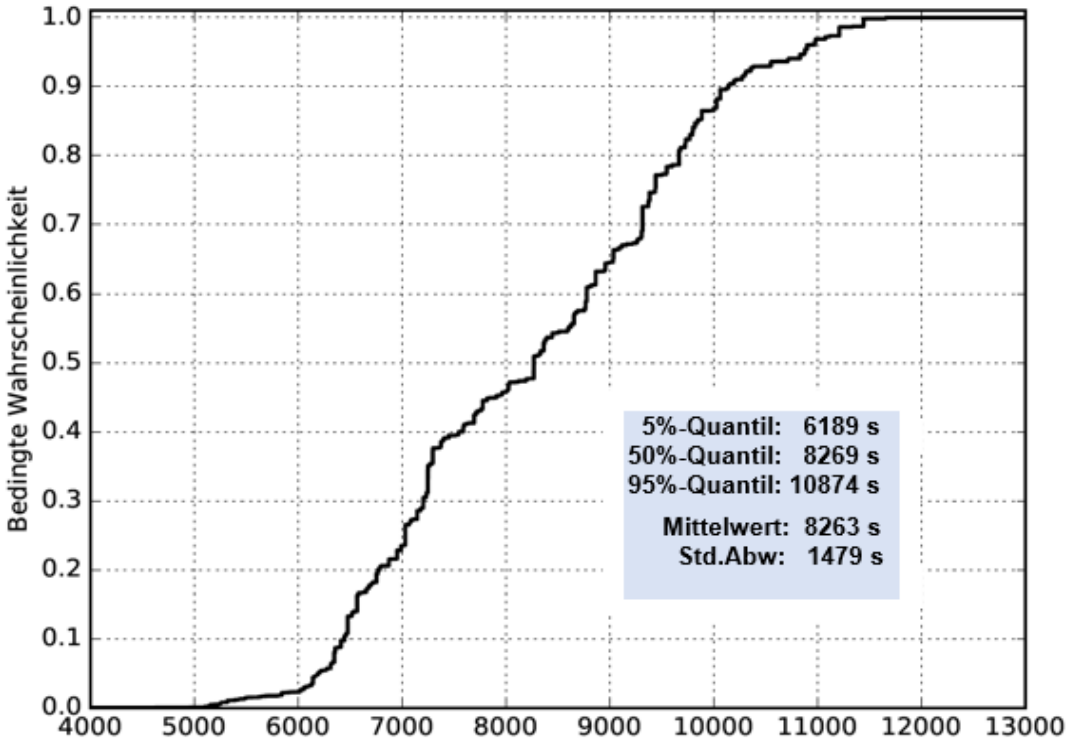


Abb. 3.41 Bedingte Verteilung der Zeit für das geschlossene Versagen aller drei DH-Ventile

Aus der Abb. 3.41 können verschiedene Wahrscheinlichkeitsaussagen abgeleitet werden, wie z. B.: Unter der Bedingung, dass alle drei DH-Ventile geschlossen versagen, beträgt die Wahrscheinlichkeit, dass dies

zwischen 75 und 90 min erfolgt	0.012
zwischen 90 und 120 min	0.278
zwischen 120 und 150 min	0.355
zwischen 150 und 180 min	0.295
zwischen 180 und 240 min	6.E-02

Die frühen Versagenszeiten < 90 min werden zum größten Teil durch die 3v3-GVA verursacht.

v) Wahrscheinlichkeit, dass mindestens eines der drei DH-Ventile auslegungsgemäß funktioniert:

Diese Wahrscheinlichkeit setzt sich zusammen aus den Ereignissen, dass entweder DH-AV oder SiV1 oder SiV2 bis zum Rechenzeitende auslegungsgemäß arbeitet und ist gegeben durch:

P (mindestens 1 DH-Ventil funktioniert bis zum Rechenzeitende) = 0.998

Notfallmaßnahme SDE:

vi) Zeitpunkt wann die Druckentlastung der DE durchgeführt wird:

Die Ausführungszeiten der notwendigen Handlungen variieren durch zufällige Einflüsse mehr oder weniger stark. Deshalb variiert auch der Zeitpunkt, wann die DE sekundärseitig druckentlastet werden. Die Verteilung des Zeitpunktes, wann SDE erfolgt, ist in Abb. 3.42 dargestellt.

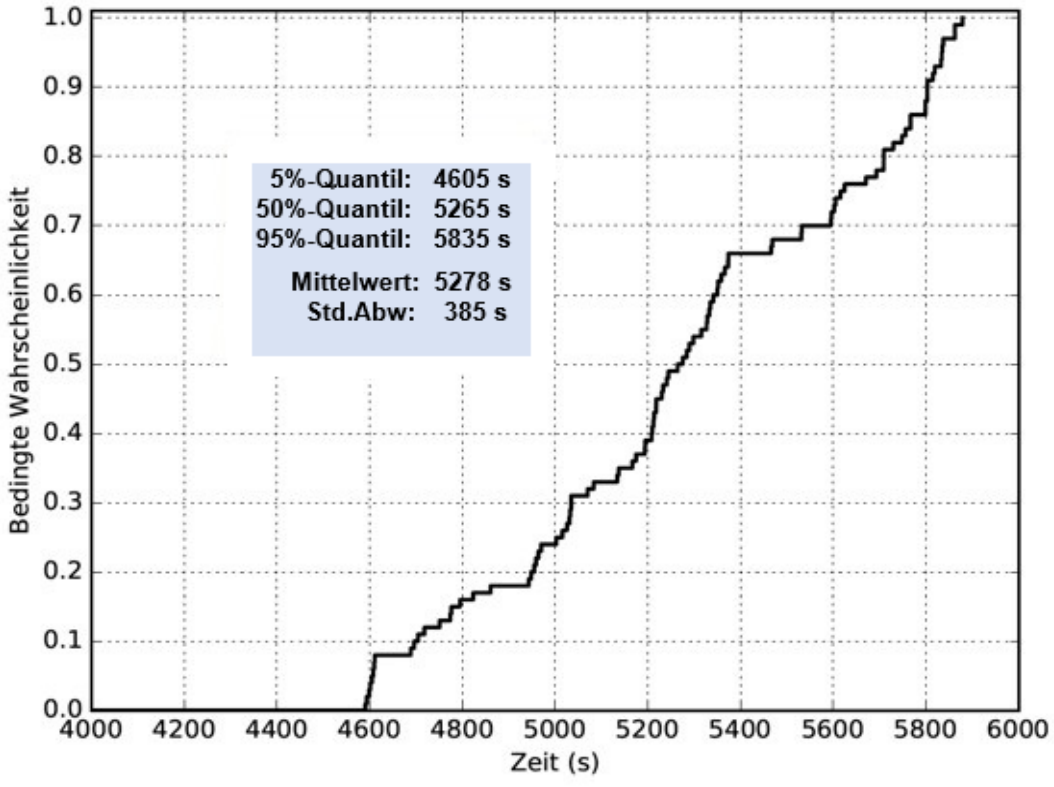


Abb. 3.42 Verteilung des Zeitpunktes, wann SDE durchgeführt wird

In Abb. 3.42 wurden die Verteilung der Ausführungszeit von SDE für beide Schädigungsgruppen für die Fälle dargestellt, in denen kein DEHEIRO-Versagen aufgetreten ist. Die Verteilung in Abb. 3.42 ist die Mischverteilung der drei in Abb. 3.32 dargestellten Verteilungen.

Heiße Leitung (HKL) und Volumenausgleichsleitung (VAL):

vii) Zeitpunkt, wann Leck an HKL bzw. VAL unabhängig vom DEHEIRO-Versagen auftritt:

Aufgrund der in der Analyse berücksichtigten epistemischen und aleatorischen Einflüsse, ist die Frage ob und wann ein Leck in der HKL bzw. VAL auftritt, ebenso durch Unsicherheiten gekennzeichnet. In Abb. 3.43 sind die bedingten Verteilungen der Zeiten dargestellt, wann ein Leck in der HKL bzw. in der VAL auftritt.

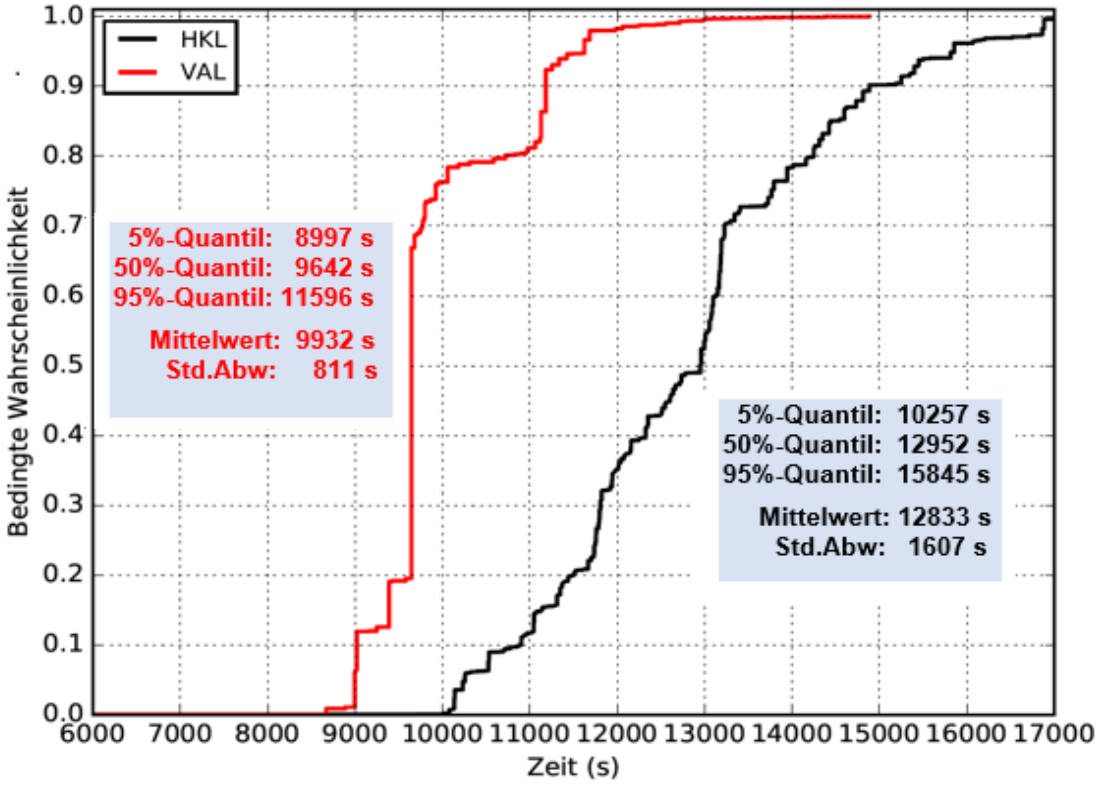


Abb. 3.43 Bedingte Verteilung der Zeit, wann Leck an HKL bzw. VAL eintritt

viii) Zeitdifferenz zwischen DEHEIRO-Versagen und Versagen der HKL:

In Abb. 3.44 sind die bedingten Verteilungen der Zeitspanne zwischen DEHEIRO-Versagen und Bruch der HKL bzw. VAL dargestellt. Die Verteilungen wurden unter der Bedingung berechnet, dass DEHEIRO Versagen und Bruch der HKL bzw. VAL eingetreten ist.

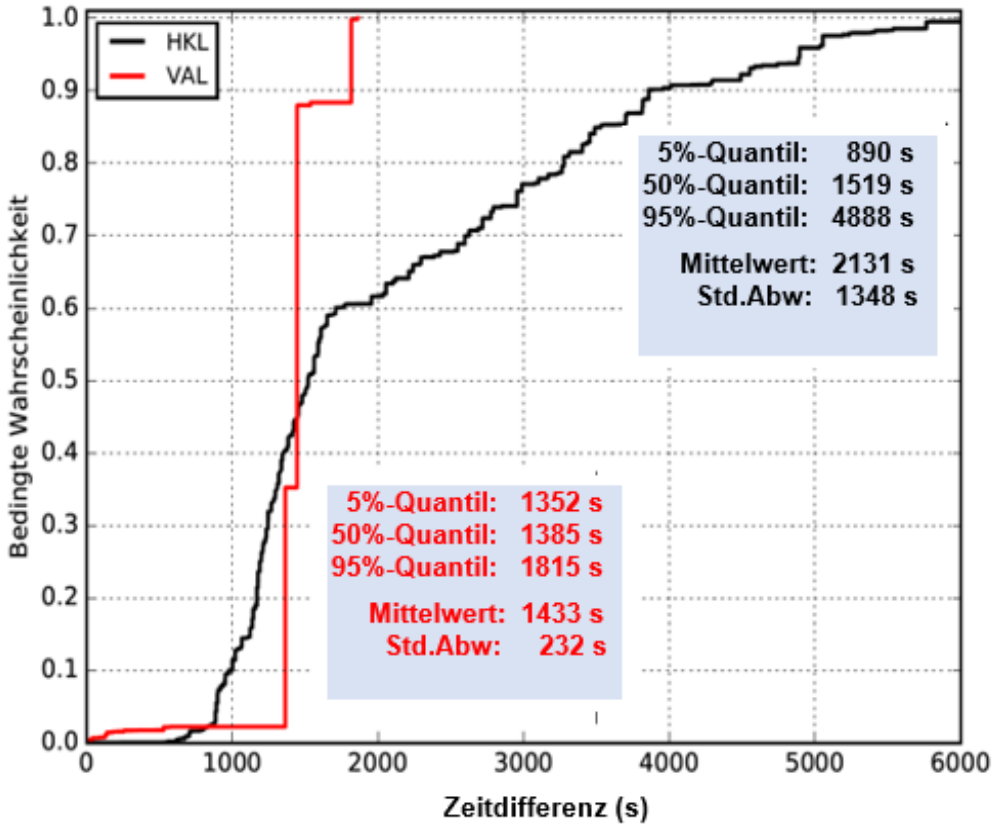


Abb. 3.44 Bedingte Verteilungen der Zeitspanne zwischen DEHEIRO-Versagen und Bruck der HKL bzw. VAL

In Abb. 3.23 (s. Abschnitt 3.5.2) ist die bedingte Verteilung der Zeitspanne zwischen DEHEIRO-Versagen und Bruch in der HKL in Abhängigkeit des Schädigungsgrads des DE-Heizrohrs angegeben. Die bedingten Verteilungen in Abb. 3.44 zeigen die Zeitdifferenz unabhängig vom Schädigungsgrad.

ix) Wahrscheinlichkeit für Leck an HKL unter der Bedingung, dass alle drei DH-Ventile geschlossen ausgefallen sind:

Die Wahrscheinlichkeit, dass alle drei Ventile geschlossen ausfallen und ein Bruch der HKL auftritt, ergibt sich durch die Auswertung der Analyseergebnisse zu:

P (DH-Ventile geschl. ausgefallen und Bruch HKL) = 7.237E-05

Die Wahrscheinlichkeit, dass ein Bruch der HKL eintritt unter der Bedingung, dass alle drei DH-Ventile geschlossen ausgefallen sind, ergibt sich unter Verwendung der Definition der bedingten Wahrscheinlichkeit zu:

P (Bruch HKL | DH-Ventile geschlossen ausgefallen) = 3.626E-02.

Die Wahrscheinlichkeit, dass alle drei DH-Ventile geschlossen ausfallen, ist unter Punkt iii) angegeben.

x) Wahrscheinlichkeit für Leck an HKL oder VAL unter der Bedingung, dass alle drei DH-Ventile geschlossen ausgefallen sind.

Die Wahrscheinlichkeit, dass alle drei DH-Ventile geschlossen ausfallen und ein Bruch der HKL oder VAL auftritt ist:

P (DH-Ventile geschl. ausgefallen und Bruch HKL oder VAL) = 7.241E-05

Die Wahrscheinlichkeit, dass ein Bruch der HKL oder VAL eintritt unter der Bedingung, dass alle drei DH-Ventile geschlossen ausgefallen sind, ergibt sich unter Verwendung der Definition der bedingten Wahrscheinlichkeit zu:

P (Bruch HKL oder VAL | DH-Ventile geschlossen ausgefallen) = 3.628E-02

Aufgrund der geringen Wahrscheinlichkeit von 3.75E-08, dass ein Bruch der VAL zusammen mit einem geschlossenen Ausfall aller DH-Ventile auftritt, unterscheidet sich die bedingte Wahrscheinlichkeit nur geringfügig von der in Punkt ix).

Vorschädigung des DE-Heizrohrs:

xi) Wahrscheinlichkeit, dass Ausmaß der Vorschädigung zu Beginn des Unfallablaufs < 20 %, 20 – 40 % und 40 – 70 % beträgt.

In Tab. 3.11 sind die mittleren Wahrscheinlichkeiten für die einzelnen Schädigungsklassen angegeben. Eine Annahme der Analyse bestand darin, dass das DE-Heizrohr zu Beginn des Unfallablaufs eine mehr oder weniger große Schädigung aufweist. Aus den mittleren Wahrscheinlichkeiten in Tab. 3.11 ergibt sich:

P (< 20 %) = 0.98
P (20 – 40 %) = 9.1E-03
P (40 – 70 %) = 1.04E-02

DEHEIRO-Versagen:

xii) Zeitpunkt, wann DEHEIRO-Versagen nach dem einleitenden Ereignis in Abhängigkeit des Schädigungsgrades auftritt.

In Abb. 3.22 (s. Abschnitt 3.5.2) sind die bedingten Verteilungen des Versagenszeitpunktes des DE-Heizrohrs in Abhängigkeit starker und schwacher Schädigungen grafisch dargestellt. Aus diesen bedingten Verteilungen können Wahrscheinlichkeiten abgeleitet, werden, dass das DE-Heizrohr bei gegebener Schädigung innerhalb eines bestimmten Zeitintervalls ausfällt. Als Beispiel dienen die Wahrscheinlichkeiten, die in Tab. 3.13 (siehe Abschnitt 3.5.2) angegeben sind.

xiii) Zeitspanne zwischen SDE und DEHEIRO-Versagen in Abhängigkeit des Zeitpunktes, wann SDE erfolgt

In Abb. 3.45 sind die bedingten Verteilungen der Zeiten dargestellt, wann DEHEIRO nach Durchführung der SDE versagt. Die Verteilungen wurden in Abhängigkeit unterschiedlicher Zeitintervalle berechnet, wann SDE durchgeführt wird.

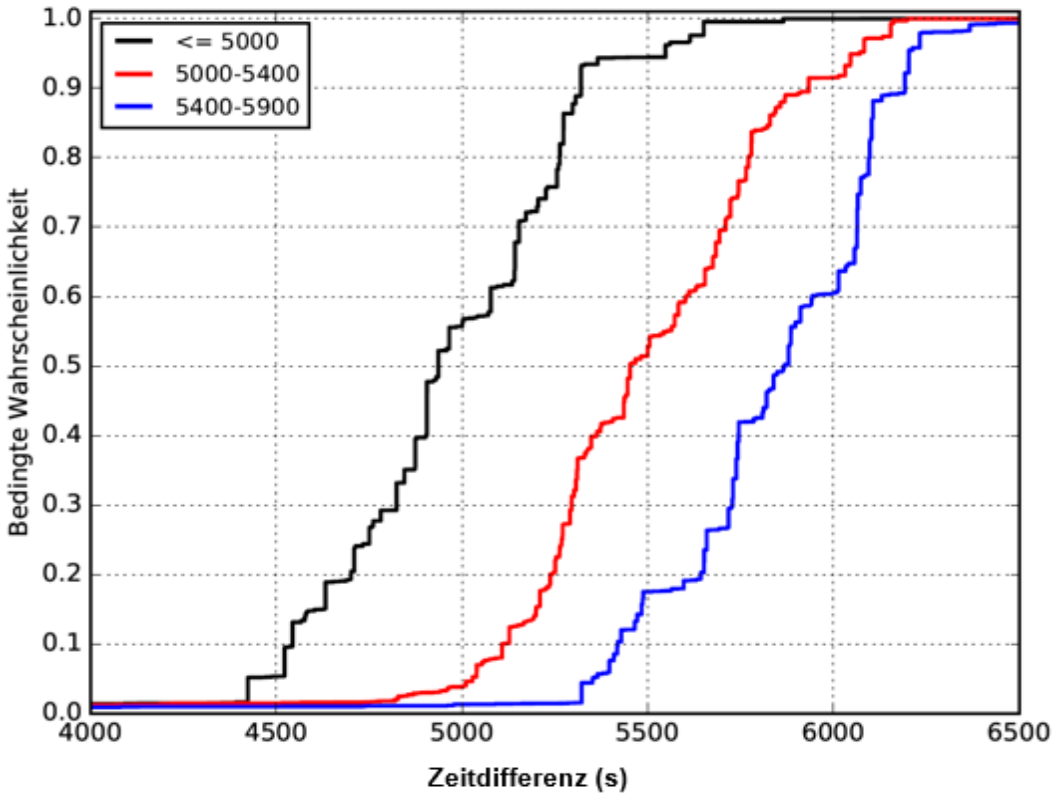


Abb. 3.45 Zeitdifferenz zwischen SDE und DEHEIRO-Versagen in Abhängigkeit der Zeit, wann SDE durchgeführt wurde

Aus Abb. 3.45 ist zu erkennen, dass die Zeitdifferenzen zwischen SDE und DEHEIRO-Versagen größer werden, je später SDE durchgeführt wird.

Wenn SDE zwischen 4600 und 5000 s durchgeführt beträgt die mittlere Zeitdifferenz zwischen Durchführung der SDE und DEHEIRO-Versagen 4918 s. Erfolgt die Durchführung der SDE zwischen 5000 – 5400 s bzw. 5400 – 5900 s, steigt der Mittelwert der Zeitdifferenz auf 5446 s bzw. 5800 s an.

Fazit: Die Vielfalt und der Detaillierungsgrad der probabilistischen Aussagen, die aus der in diesem Projekt durchgeführten MCDET/ATHLT-CD Analyse berechnet werden konnten, zeigen den Vorteil und Nutzen einer IDPS unter Verwendung von MCDET. Viele dieser probabilistischen Aussagen können dabei für eine Erweiterung eines Ereignisbaums der klassischen PSA verwendet werden.

Stochastische Einflussgrößen lassen sich wesentlich umfassender und detaillierter in der Analyse berücksichtigen und liefern Kenntnisse über deren Einfluss auf den Unfallablauf. Diese stochastischen Einflüsse können quantifiziert und hinsichtlich ihrer Signifikanz bewertet werden.

4 Methodenentwicklung zur dynamischen Analyse und Bewertung wissensbasierter Handlungen sowie Erprobung an einem Ereignis aus der deutschen Betriebserfahrung

Neben der Ausführung regelbasierter Aufgaben kann die Überwachung und Führung eines Kernkraftwerks sowie anderer komplexer Technologien, bei deren Nutzung der Schutz von Mensch und Umwelt zu gewährleisten ist, wissensbasierte Handlungen des Personals erfordern. Die Betriebserfahrung zeigt, dass in der Praxis mit solchen Handlungen zu rechnen ist, wenn unvorhergesehene Situationen auftreten, für deren Beherrschung keine geplanten und eintrainierten (regelbasierte) Vorgehensweisen existieren. In solchen unvorhergesehenen Situationen, in denen Probleme auftreten und zu beheben sind, kann in der erfolgreichen Durchführung wissensbasierter Handlungen allerdings noch eine erhebliche Sicherheitsreserve bestehen, durch die Unfälle verhindert oder deren Auswirkungen verringert werden können. Deshalb sollte eine aussagekräftige probabilistische Sicherheitsanalyse wissensbasierte Handlungen innerhalb und außerhalb der Warte mit ihren Beiträgen zum Gesamtergebnis angemessen berücksichtigen, wozu geeignete Methoden entwickelt werden müssen.

Die GRS hat Methoden entwickelt, um kognitive Faktoren und wissensbasiertes Handeln im Rahmen einer klassischen PSA analysieren und bewerten zu können /FAS 03/, /FAS 10/. Die Methoden berücksichtigen wichtige Rahmenbedingungen des Handelns, wie z. B. Stress und die Qualität der Informationen auf Benutzungsoberflächen in der Warte. Die Methode für die kognitiven Faktoren konzentriert sich auf deren Beitrag zu Handlungsfehlern, während die Methode für das wissensbasierte Handeln den Erfolg des Problemlösens zum Gegenstand hat. Die vielfältigen, einschlägigen Entwicklungsarbeiten haben bisher noch zu keiner international anerkannten Methode geführt. Diese Feststellung trifft auf die Analyse- und Bewertungsmethoden sowohl für die klassische PSA als auch für die dynamische probabilistische Sicherheitsanalyse gleichermaßen zu.

Für die bisherigen Entwicklungen gilt, dass ihr Anwendungsbereich auf die klassische PSA beschränkt war und dynamische Aspekte in der Modellierung nicht berücksichtigt werden konnten. Bei wissensbasiertem Handeln muss das Personal das bestehende Problem ad hoc erkennen und das Vorgehen sowie dessen praktische Umsetzung entwickeln, mit dem das Problem gelöst werden kann. Das kann zahlreiche Schritte der Aufnahme und Verarbeitung von Informationen sowie der Planung und Bewertung von Handlungsoptionen erfordern, woraus sich vielfältige Handlungsabläufe mit unterschiedlichem Zeitbedarf ergeben können. Um die wechselwirkenden Aspekte wissensbasierten

Handelns in Abhängigkeit von Prozesszuständen und zufälligen Einflüssen berücksichtigen und modellieren zu können, bedarf eines dynamischen Ansatzes. Die Methodik der klassischen PSA kann die zeitlichen Abhängigkeiten und Wechselwirkungen wissensbasierten Handelns im Detail erfassen.

Ziel der nachfolgend beschriebenen Arbeiten ist es, eine Methode für die Analyse und Bewertung wissensbasierten Handelns in einer dynamischen probabilistischen Sicherheitsanalyse zu entwickeln und beispielhaft anzuwenden. Diese Methode baut auf Erkenntnissen von Entwicklungsarbeiten auf, die in einem früheren Projekt zu einer Analyse- und Bewertungsmethode für wissensbasiertes Handeln geführt haben, deren Anwendungsbereich jedoch auf eine klassische (nicht-dynamische) probabilistische Sicherheitsanalyse abzielt (/FAS 10/). Mit der Weiterentwicklung in diesem Projekt ist es möglich, wissensbasiertes Handeln auch in Ereignisabläufen zu berücksichtigen, die wegen ihrer Dynamik und Komplexität bevorzugt mit einer dynamisch ausgelegten Methodik analysiert und bewertet werden sollten.

Die Ausführungen in Abschnitt 4.1 präsentieren einen Überblick über die Entwicklungsschritte einschließlich ihrer fachlichen Grundlagen. Abschnitt 4.2 beschreibt die Methode zur dynamischen Modellierung wissensbasierten Handelns. Das Kapitel schließt mit einer Diskussion des erreichten Standes und möglicher weiterführender Arbeiten.

Die Entwicklungen zur dynamischen Modellierung wissensbasierter Handlungen werden an einem ausgewählten Ereignis aus der deutschen Betriebserfahrung erprobt und verifiziert. Für das Anwendungsbeispiel wurde ein meldepflichtiges Ereignis ausgewählt, das in einer inzwischen stillgelegten und sich im Rückbau befindlichen Anlage auftrat. Abschnitt 4.3 behandelt die Anwendung und Erprobung der entwickelten Methodik zum wissensbasierten Handeln an einem ausgewählten Precursor-LOCA Ereignis aus der deutschen Betriebserfahrung.

4.1 Überblick der Entwicklungsschritte und ihre fachlichen Grundlagen

Dieser Überblick führt zum einen die erforderlichen, grundlegenden Fachbegriffe ein und fasst zum anderen die Erkenntnisse zusammen, auf denen die Entwicklungsarbeiten der Methodik basieren.

4.1.1 Grundlegende Begriffsbestimmungen

Methoden für die Analyse und Bewertung menschlicher Zuverlässigkeit sehen oft eine Einteilung der Personalhandlungen in die Ebenen des fertigkeits-, regel- und wissensbasierten Handelns nach Rasmussen vor (z. B. /RAS 83/, S. 258 ff.). Diese Ebenen sind begrifflich wie folgt bestimmt:

- „Fertigkeitsbasiert“ dient als Sammelbegriff für die sensomotorischen Leistungen, d. h. die unbewusste Steuerung und Kontrolle automatisierter Reizverarbeitungs- und Bewegungsabläufe, die zur Erreichung eines Handlungsziels eingeleitet werden (siehe /RAS 83/, S. 258 ff.). Diese Leistungen werden ohne Beteiligung des Bewusstseins vollzogen.

- „Regelbasiert“ heißen Handlungen, die auf erlernten, bewährten und in der Situation erinnerten Regeln beruhen (siehe /RAS 83/, S. 259). Die Person erinnert sich z. B. beim Vorliegen bestimmter Merkmale in der Situation mehr oder minder automatisch, wie sie sich zu verhalten hat. Übung und Routine können dazu führen, dass regelbasiertes Handeln so stark automatisiert ist, dass es mit einer nur geringen Beteiligung des Bewusstseins vollzogen wird.

- „Wissensbasiert“ ist ein Handeln in Situationen, für die der Handelnde zunächst nicht weiß, wie er im Einzelnen vorgehen könnte, um sein Ziel zu erreichen. Solche Situationen erfordern es, sowohl Ziel als auch Situation genauer zu analysieren und ein ausreichend präzises Ziel des Handelns zu formulieren, um auf dieser Grundlage einen Plan für das weitere Vorgehen zu entwickeln (siehe /RAS 83/, S. 259). Diese gedanklichen Analysen und Synthesen erfordern bewusstes Nachdenken, sind also „bewusstseinspflichtig“.

Mit diesen Ebenen werden die Schwerpunkte der psychischen Beanspruchung bei der Erfüllung von Aufgaben erfasst. Im Zentrum steht dabei die Beanspruchung des Bewusstseins mit seinen eher engen Grenzen. Sie führen dazu, dass sowohl das bewusste Erinnern eines regelbasierten Vorgehens als auch bewusste wissensbasierte Überlegungen Schritt für Schritt vollzogen werden und entsprechend zeitaufwendig, aber auch fehleranfällig sind. Man denke z. B. an die Fehlermöglichkeiten bei umfangreicheren Schlussfolgerungen mit u. U. vielfältigen logischen Verknüpfungen, über die man schnell die Übersicht verlieren kann, auch wenn man Notizen und vergleichbare Hilfen nutzt.

Der Bezug auf das Bewusstsein hat eine wichtige methodologische Konsequenz: Insofern das Handeln bewusstseinsfähig oder sogar bewusstseinspflichtig ist, kann der Handelnde darüber Auskunft geben. Man kann ihn z.B. auffordern, auszusprechen, was ihm durch den Kopf geht (sog. „lautes Denken“) und (oder) geeignete Fragen zu seinen Überlegungen stellen. Diese Fähigkeit bewusster Reflexion und sprachlicher Kommunikation sollte bei der Untersuchung des regel- und wissensbasierten Handelns so weit als möglich genutzt werden, um Informationen über die Überlegungen zu gewinnen, auf denen das Handeln beruht.

Die Begriffsbestimmungen sind um folgende Punkte zu ergänzen, die für die anstehende Methodenentwicklung bedeutsam sind:

- Ein „Problem“ liegt vor, wenn eine Person oder eine Gruppe von Personen vor der Anforderung steht, einen Istzustand in einen Sollzustand zu überführen, ohne zunächst zu wissen, wie sie dieses Ziel erreichen könnte. Deshalb muss ein Vorgehen erarbeitet werden, mit dem der Übergang vom Ist- zum Sollzustand ermöglicht wird. Ein solches Vorgehen heißt in der Fachliteratur „Problemlösen“ (engl: „problem solving“).
- „Wissensbasiertes Handeln“ und „Problemlösen“ sind als gleichbedeutende Begriffe zu verstehen, wenn man beim Problemlösen neben der Lösungsfindung auch die Umsetzung einer gefundenen Lösung versteht.

Es hängt vom von Kenntnisstand und der Erfahrung der Person ab, ob eine Aufgabenstellung für sie überhaupt ein Problem darstellt oder nicht. Ein Experte kann im Vergleich zu einem Neuling mit der Aufgabenstellung und dem Vorgehen zur Bewältigung der Aufgabe so vertraut sein, dass er regelbasiert handeln kann. Der Neuling kann dagegen vor der Frage stehen, was zu tun sei, um die Aufgabe zu bewältigen. Sein Handeln ist somit im Wesentlichen wissensbasiert.

Auch kann eine Person für eine Situation A Kenntnisse besitzen, die ein regelbasiertes Handeln unterstützen, wohingegen eine Situation B ihr ein wissensbasiertes Handeln abverlangt. In der Situation B besteht eine Möglichkeit darin, sich auf Handlungsweisen zu besinnen, mit denen man aus anderen Situationen so vertraut ist, dass sie für diese anderen Situationen als regelbasierte anzusehen sind, und darüber nachzudenken, ob sie nicht zur Lösung des Problems mit der Situation B herangezogen werden können. Besteht diese Möglichkeit, dann ist das Problem lösbar. Als Problemlösung gilt deshalb auch die Erkenntnis, dass ein aus anderen Situationen vertrautes Vorgehen objektiv

zielführend ist, um das Problem zu lösen. Die Person erkennt somit korrekter Weise, dass der Anwendungsbereich eines regelbasierten Handelns auf die Problemsituation erweitert werden kann.

Als letzter Punkt ist festzuhalten, dass ein Problem der Person als solches bewusst werden muss, damit sie es als Problem erkennt und darauf reagiert. Es besteht also die Fehlermöglichkeit, sich einer tatsächlich bestehenden Problemsituation gar nicht bewusst zu werden und fälschlicherweise gar nicht zu handeln.

4.1.2 Aktualisierung der Erkenntnisse aus relevanten Vorgängerprojekten

Die durchzuführende Methodenentwicklung baut soweit wie möglich auf Erkenntnissen aus Vorgängerprojekten auf. Die nachfolgenden Ausführungen beschränken sich deshalb auf eine Zusammenfassung des damals erreichten Standes und geben einen Überblick über Erkenntnisse, die darüber hinaus in die Methodenentwicklung eingegangen sind.

Der Erkenntnisstand zu den Ebenen des Handelns darf als Stand von W&T angesehen werden. Das zeigt v. a. das Lehrbuch zu Arbeitspsychologie von Hacker und Sachse (/HAC 14/). Dort werden Faktoren erläutert, von denen Erfolg und Misserfolg des wissensbasierten Handelns bzw. Problemlösens abhängen. Der Erkenntnisstand aus den einschlägigen Vorgängerprojekten (/FAS 10/, S. 39ff, /FAS 14/, S. 65ff) kann demzufolge beibehalten werden. Zum gleichen Schluss führt die Auswertung einer umfangreichen, praxisgerechten, strukturierten Zusammenstellung der kognitiven Faktoren zuverlässigen Handelns (/WHA 16/, bes. Anhang B). Sie ist Ergebnis einer Auswertung v. a. der englischsprachigen Fachliteratur (/WHA 16/, Gliederungspunkt 1.1 und S. 79 ff).

Eine Bewertung menschlicher Zuverlässigkeit erfordert Informationen über die Handlungen, die das Personal üblicherweise ausführt, um eine zur Bewertung anstehende Aufgabe zu erfüllen. Das grundsätzliche, methodische Vorgehen ist seit langem in der Analyse und Bewertung menschlicher Zuverlässigkeit etabliert. Es wurde in einem Vorgängerprojekt auf das wissensbasierte Handeln übertragen (/FAS 10/, S. 45 ff.) und ist auch hinreichend allgemein, um in einer dynamischen probabilistischen Sicherheitsanalyse Anwendung finden zu können (Kapitel 4.3: Beschreibung des Analyseteils der Methode).

Neuere Entwicklungen zur Methodik der Analyse und Bewertung wissensbasierten Handelns haben keinen Anlass gegeben, Änderungen an der Analysemethode aus dem Vorgängerprojekt vorzunehmen. Diese Schlussfolgerung ist Ergebnis der folgenden Recherchen und Analysen:

Die Recherche einschlägiger Entwicklungen beschränkt sich auf Ansätze, die auf eine Zerlegung des Handlungsablaufs in einzelne Schritte abzielen und deren öffentlich zugängliche Dokumentation so detailliert ist, dass sie Verständnis und Beurteilung des betrachteten Ansatzes erlaubt. Die Konzentration auf Ansätze, die eine Handlungszerlegung vorsehen, fußt auf der Begriffsbestimmung der Verhaltensebenen (s. o.). Dieser Begriffsbestimmung zufolge gehören zum Handeln unterschiedliche Teilprozesse (im Folgenden vereinfachend als „Schritte“ bezeichnet). Beim wissensbasierten Handeln sind dies z. B. die Schritte i) Erkennung, dass ein Problem vorliegt und ii) Überlegung, wie von der gegebenen Situation aus ein Ziel erreicht werden könnte.

Eine Zerlegung des Handlungsablaufs unterstützt eine genaue Beschreibung des Handlungsablaufs. Sie ermöglicht ferner die Berücksichtigung von Fehlermöglichkeiten in den einzelnen Schritten (z. B. Fehldiagnose der Situation) und der denkbaren Fehlerursachen. Z. B., wenn ein objektiv falscher Messwert, der für richtig gehalten wird, die Diagnose der Situation verfälscht und zur Auswahl eines ungeeigneten Vorgehens führt. Man erreicht Analysen solcher Tiefe nicht, wenn eine Methode bzw. ihre veröffentlichte Dokumentation keine entsprechenden detaillierteren Vorgaben enthalten. Diese Kritik wurde bereits an den Analyse- und Bewertungsmethoden für wissensbasiertes Handeln formuliert, die im einschlägigen Vorgängerprojekt näher betrachtet worden sind (/FAS 10/, S. 12 ff.).

Zwischenzeitlich sind v.a. in den USA und in Südkorea publizierte Methoden entstanden, die Schritte im kognitiven Bereich (Wahrnehmen, Verstehen, Entscheiden u. Ä.) unterscheiden und dadurch eine entsprechende Zerlegung des Handlungsablaufs unterstützen (/KAE 16/, /LIU 12a/, /LIU 12b/, /PAR 09/, /WHA 16/). Diese Ansätze enthalten jedoch keine genaueren Hinweise darauf, wie diese Schritte in den Prozess des wissensbasierten Handelns (bzw. Problemlösens) eingehen und wie sie in diesem Prozess zusammenspielen. Es fehlt mit anderen Worten ein erfahrungswissenschaftlich fundiertes Modell, wie der Problemlöseprozess verläuft und wie er mit den Rahmenbedingungen des Handelns (wie z. B. der Verfügbarkeit korrekter Informationen über den Zustand der Anlage) in Wechselwirkung tritt.

Der prinzipiell unveränderte Erkenntnisstand zu Verhaltensebenen und damit wissensbasiertem Handeln hat es erlaubt, das umfassende Modell des Problemlösens aus dem Vorgängerprojekt als Grundlage zu übernehmen und zu erweitern (/FAS 10/, S. 32 ff.). Das übernommene Modell stellt eine Synthese wesentlicher erfahrungswissenschaftlicher Beiträge zum Ablauf und zu Erfolgs- bzw. Misserfolgsfaktoren des Problemlösens dar. Der Erweiterung des Modells geht auf die Notwendigkeit zurück, es im Rahmen einer dynamischen probabilistischen Sicherheitsanalyse einsetzen zu können. Die nachfolgenden Ausführungen zeigen, dass der Bewertungsansatz aus dem Vorgängerprojekt mit dem Vorgehen in einer dynamischen probabilistischen Sicherheitsanalyse nur eingeschränkt verwendet werden kann. Diese Beschränkung wird in diesem Vorhaben durch die Weiterentwicklungsarbeiten zur Modellierung des Problemlöseprozesses überwunden.

Die Bewertungsmethode aus dem Vorgängerprojekt beruht auf einem Bewertungsansatz, den Swain für die Diagnose von Situationen und die dazu gehörige Auswahl der erforderlichen Prozedur(en) entwickelt hat. Der Swain'sche Ansatz unterliegt der Einschränkung, dass diese Diagnosen bzw. Prozeduren dem Personal soweit vertraut sind, dass es im Prinzip regelbasiert handeln kann (/FAS 10/, S. 54 ff.). Die Argumentation läuft darauf hinaus, dass regelbasierte Diagnosen einschließlich der richtigen Auswahl der erforderlichen Prozedur(en) unter den nach Swain ungünstigsten Rahmenbedingungen (/SWA 83/, Tab. 12-5) die gleichen Anforderungen an das Personal stellen wie ein wissensbasiertes Handeln unter günstigen Rahmenbedingungen. Zu diesen Rahmenbedingungen vergleiche man die Dokumentation der Bewertungsmethode in Abschnitt 4.2.3 dieses Berichts bzw. die einschlägigen Ausführungen zum Vorgängerprojekt. Da die korrekte Diagnose bei Swain die Auswahl der erforderlichen Prozeduren einschließt, dient der Begriff der Diagnose im Folgenden dazu, sowohl die Diagnose der Situation als auch die Wahl der Prozeduren zu bezeichnen, die für die Bewältigung der Situation geplant und dem Personal im Prinzip bekannt sind.

Der Ansatz von Swain erfordert zur Quantifizierung der Zuverlässigkeit, mit der das Personal das Problem rechtzeitig und korrekt diagnostiziert, die Bestimmung der Zeitspanne, die dem Personal für die Diagnoseaufgabe ab Eintritt der zu diagnostizierenden Situation maximal zur Verfügung steht (/SWA 83/, Kapitel 12). Diese Zeitspanne T_D ergibt sich nach Swain als Differenz aus dem Zeitintervall T_{MAX}, in dem das Personal die erforderliche(n) Prozedur(en) mit Erfolg auszuführen hat, um die Situation zu bewältigen, und dem Zeitaufwand T_A, den die Ausführung der ausgewählten Prozedur(en) im Mittel

erfordert: $T_D = T_{MAX} – T_A$. Das Zeitintervall T_{MAX} läuft vom Eintritt der zu bewältigenden Situation bis zu dem Zeitpunkt, ab dem die erforderliche(n) Prozedur(en) unwirksam bleiben, auch wenn das Personal sie korrekt (aber zu langsam) ausführt.

In die Quantifizierung der Diagnosezuverlässigkeit gehen somit die beiden Bedingungen ein, dass sowohl die Ausführungszeit T_A der erforderlichen Prozedur(en) also auch die Länge des Zeitintervalls T_{MAX} bekannt sein müssen, zu dessen Ende die Prozedur(en) wirksam werden müssen. Die Anwendbarkeit dieses Ansatzes beruht auf den Bedingungen, dass zum einen T_{MAX} nicht von Eingriffen des Menschen in den technischen Prozess abhängen darf, wodurch sich T_{MAX} ändern kann. Andererseits muss auf der Basis vorliegender Informationen, z.B. aus der Anlagenbegehung und über die Ausführungszeiten für die einzelnen menschlichen Handlungen, der Gesamtzeitbedarf T_A der erforderlichen Prozedur zu Beginn der Simulation abzuschätzen sein. Hier ist zusätzlich zu berücksichtigen, dass die Ausführungszeit T_A zufälligen Variationen unterliegt, die mehr oder weniger groß sein können.

Liegen Informationen zu T_{Max} bzw. T_A nicht vor, kann der Ansatz nach Swain nicht angewendet werden. In diesem Fall bietet der Einsatz des Crew-Moduls (s. Abschnitt 2.2) die Möglichkeit, die Diagnosezuverlässigkeit im Rahmen einer probabilistischen Dynamikanalyse unter Verwendung von MCDET zu ermitteln. In diesem Fall werden für die einzelnen Schritte des Problemlöseprozesses stochastisch verteilte Ausführungszeiten und Schätzwerte für die Wahrscheinlichkeit ihrer erfolgreichen Durchführung bereitgestellt (Details können der Methodenbeschreibung in Abschnitt 4.2 entnommen werden). Im Rahmen der Simulation werden die Schritte dann sukzessive mit ihren Beiträgen zu Zeitdauer und Zuverlässigkeit des Problemlösens und den sich ergebenden Folgen für den weiteren Ereignisablauf berücksichtigt. Das gilt auch für wiederholte Durchläufe (Iterationen) von Schritten, wenn der Problemlöseprozess dies erfordert.

Beim wissensbasierten Handeln bzw. Problemlösen wird zwischen den beiden übergeordneten Phasen der Findung und der Umsetzung eines geeigneten Vorgehens unterschieden. Die Zuverlässigkeit für die Findung des Vorgehens („Lösungsfindung“) kann mit dem Ansatz nach Swain durchgeführt werden, wenn die oben erwähnten Bedingungen erfüllt sind. Zu dieser Diagnose gehört auch die Entscheidung für die Ausführung der erforderlichen Prozedur(en). Im Fall, dass die Bedingungen nicht erfüllt sind besteht die Hauptaufgabe für die Methodenentwicklung darin, Zeit und Zuverlässigkeit für das Problemlösen zu ermitteln.

In Anlehnung an einschlägige Studien aus der Grundlagenforschung unterscheidet die Methode bei der Phase der Lösungsfindung zwei Hauptschritte. Erstens zu erkennen, dass ein aus anderen Situationen bekanntes, regelbasiertes Vorgehen im Prinzip anwendbar ist. D. h. der Handelnde findet heraus, wie er prinzipiell vorgehen könnte, um das Problem zu lösen. Zweitens ist zu prüfen, ob das prinzipiell als geeignet erkannte Vorgehen auch tatsächlich anwendbar ist. Dieser zweite Schritt entspricht der Diagnose, ob in der gegebenen Situation die notwendigen Voraussetzungen vorliegen, damit das gefundene Vorgehen ausgeführt werden kann und darf („Anwendbarkeitsprüfung"). Für den ersten Schritt wurden Zeitbedarf und Zuverlässigkeit mangels anderer Daten durch eine erste, ausbau- und revisionsfähige Expertenschätzung festgelegt. Für den zweiten Schritt der „Anwendbarkeitsprüfung" liegen nutzbare Daten aus empirischen Studien mit US-amerikanischen Operateuren vor (/WES 87/). Diese Daten zeigen, wie die Zuverlässigkeit, mit der die Operateure richtig erkennen, dass sie ein bestimmtes, regelbasiertes Vorgehen zur Bewältigung einer vorgegebenen, aus Übungen vertrauten Situation anzuwenden haben, von der Zeit abhängt, die nach Eintritt der Situation verstreicht.

Diese Daten unterscheiden sich von denjenigen, die Swain für die Bewertung der Zuverlässigkeit einer Diagnose bereitstellt. Es entfallen die Bedingungen, dass man das maximale Zeitfenster für die Beherrschung der Situation (T_{MAX}) und den Zeitaufwand für die Bearbeitung der Prozedur (T_A) kennen muss, um die Zuverlässigkeit der Diagnose quantifizieren zu können. Darüber hinaus präsentiert die Publikation Zeit- und Zuverlässigkeitsdaten für zwölf Kategorien von Aufgaben und Situationen, in denen die Aufgabe auszuführen ist (/WES 87/, S. 23). Der Anwender hat zu prüfen, in welche Kategorie sein Anwendungsfall fällt. Die Publikation unterstützt auch die Quantifizierung der zugehörigen Unsicherheitsbänder.

Als eine wichtige Erkenntnis- und Datenquelle wurden die Untersuchungen am „Halden Reactor Project" (HRP) zum Handeln der Operateure betrachtet. Eine genaue Recherche vor Ort hat aber gezeigt, dass die Erschließung und Nutzung des archivierten Datenmaterials sowie die Beteiligung an empirischen Untersuchungen einen Aufwand erfordert, der den finanziellen und den zeitlichen Rahmen des Projekts gesprengt hätte (/PET 14/). Bei Vorhandensein entsprechender Ressourcen könnte eine solche Recherche aber prinzipiell unternommen werden.

4.2 Methode zur Berücksichtigung wissensbasierten Handelns im Rahmen einer dynamischen Analyse

Die Methodenbeschreibung in diesem Abschnitt umfasst drei Teile: das zugrundeliegende Modell des wissensbasierten Handelns, den Analyseteil der Methode und die Vorgehensweisen bei der quantitativen Bewertung, welche die Methode bereitstellt. „Wissensbasiertes Handeln“ und „Problemlösen“ dienen nachfolgend als gleichbedeutende Begriffe. Das Gleiche gilt für „Vorgehen“, „Vorgehensweise“ und „Prozedur“.

4.2.1 Modell des Problemlösens

Das Modell dient dazu, den Ablauf des Problemlösens, Art und Zusammenspiel der zugehörigen Schritte sowie die Faktoren zu beschreiben, von denen die Zuverlässigkeit dieser Schritte abhängt.

Prozess des Problemlösens: Das vorliegende Modell beschreibt das Problemlösen als einen Prozess, der mit den Stufen einer Vorphase, dem Problemlöseversuch und der Ausführung einer gefundenen Lösung verbunden ist.

Die Vorphase umfasst die Zeitspanne, in der die handelnde(n) Person(en) erkennen, dass sie vor einem Problem stehen. In dieser Phase können in rascher Folge Ideen zu Möglichkeiten der Problembewältigung entstehen und wieder verworfen werden. Beim gegenwärtigen Entwicklungsstand der vorliegenden Methode wird für die Vorphase zum einen die Zeitspanne ermittelt, die verstreicht, bis die handelnde(n) Person(en) verstehen, dass sie ein Problem zu lösen haben und mit Hilfe ihres Wissens systematisch ein zielführendes Vorgehen finden müssen. Zum anderen kann in dieser Vorphase Stress in einer Art und Höhe entstehen, die das nachfolgende Handeln und seine Zuverlässigkeit beeinträchtigen (/FAS 14/, S. 108 ff.). Wichtige Ursachen erhöhten oder hohen Stresses sind Zeitdruck, Aufgabenvielfalt, eingeschränkte Vorhersagbarkeit des Anlagenverhaltens, ungenaue Informationen über den Anlagenzustand, erwartete Konsequenzen fehlerhaften Handelns und bereits eingetretene Fehler.

Der anschließende Problemlöseversuch besteht aus den mehr oder minder systematischen Anläufen, mit dem Wissen und den in der Situation vorhandenen Mitteln und Ressourcen ein Vorgehen zur Erreichung des Ziels zu finden. Zufall und blindes Raten (trial and error) gelten im vorliegenden Modell nicht als Problemlöseversuch, weil ihnen das Merkmal einer zumindest ansatzweisen Systematik der Lösungsfindung fehlt.

Ressourcen und Mittel sind z. B. die Informationen in der Warte, Betriebs-, Prüf- und Notfallhandbuch, weitere Arbeitsmittel etc.

Die Ausführungsphase setzt im vorliegenden Modell ein, nachdem die Entscheidung gefallen ist, ein gefundenes Vorgehen tatsächlich auszuführen. Diese Phase entfällt, wenn die handelnde(n) Person(en) kein Vorgehen finden oder sich gegen die Ausführung eines gefundenen Vorgehens entscheiden.

Die Phasen bauen aufeinander auf. Das Modell lässt prinzipiell aber auch Rücksprünge von späteren auf frühere Phasen zu, wenn z. B. ein Abbruch der Ausführung und eine Wiederaufnahme des Problemlöseversuchs erforderlich werden sollte.

Problemlösung: Als Problemlösungen zählen nur Vorgehensweisen,

- die zum regelbasierten Fachwissen aus Schulung und Berufspraxis gehören,
- deren Anwendung in der gegebenen Problemsituation zulässig und zielführend ist,
- deren Nutzbarkeit vom Personal in der Problemsituation jedoch selbst erkannt werden muss, weil diese spezielle Anwendungsmöglichkeit weder durch Schulung noch durch Berufspraxis vermittelt worden ist.

Eine Problemlösung ist also eine regelbasierte Vorgehensweise, die sich eignet, eine neue Problemsituation zu bewältigen ohne dass diese Nutzungsmöglichkeit Teil der regelbasierten Kenntnisse und Erfahrungen der Person(en) ist, die vor der Problemsituation stehen. „Problemlösung“ bezeichnet somit das Ergebnis einer erfolgreichen Lösungsfindung im Prozess des Problemlösens. Die vorliegende Methode versteht „Problemlösen“ und „Problemlösung“ nicht als bedeutungsgleiche Begriffe. Entscheidet sich das Personal für ein ungeeignetes Vorgehen, sollte dieses nicht als „Problemlösung“ bezeichnet werden.

Als Lösungen zählen also nur Vorgehensweisen (Prozeduren), die zum regelbasierten Fachwissen aus Ausbildung und Berufspraxis gehören. Außer Acht bleiben Lösungsmöglichkeiten, die sich aus Wissen ergeben könnten, das sich die Operateure z. B. über Freizeitbeschäftigungen angeeignet haben und folglich nicht der beruflichen Sphäre angehört. Diese Beschränkung hat den praktischen Grund, dass diese außerberuflichen Quellen wissensbasierter Vorgehensweisen kaum zu überblicken sind und für fachspezifische Fragestellungen kaum von Bedeutung sein dürften.

Prozess der Lösungsfindung (Problemlöseversuch): Dem vorliegenden Modell zufolge gehören zum Prozess der Lösungsfindung folgenden Schritte und Aktivitäten:

Hauptschritte sind erstens die im Idealfall korrekte Erkenntnis, dass ein Vorgehen, das die handelnden Personen aus Schulung und Berufspraxis für die Bearbeitung bestimmter Aufgaben kennt und regelbasiert abarbeiten kann, auch zur Bewältigung der anstehenden Problemsituation nutzbar ist. Zweitens hat das Personal zu prüfen (zu „diagnostizieren"), dass die Voraussetzungen erfüllt sind, damit die prinzipiell nutzbare Vorgehensweise in der Problemsituation ausgeführt werden darf. Beide Schritte können sich mehr oder minder überschneiden, je nachdem, wie weit die Kriterien für die Einleitung des Vorgehens schon im Zuge der Suche nach prinzipiell möglichen Vorgehensweisen kontrolliert worden sind. Hat man erst einmal erkannt, dass ein Vorgehen, das aus anderen Situationen vertraut und folglich regelbasiert ausführbar ist, stellt auch die Bearbeitung des Diagnoseschrittes nur noch Anforderungen, die regelbasiert bewältigt werden können.

Grundlage der Findung prinzipiell nutzbarer Prozeduren ist eine Suchstrategie mit den kognitiven Aktivitäten der Ziel- und der Situationsanalyse. Letztere umfasst ihrerseits die Material- und die Konfliktanalyse.

Zielanalyse: Die Zielanalyse dient der Klärung der Fragen: „Was will ich erreichen und was soll vermieden werden?" Mit ihr erfolgt eine Präzisierung des zu erreichenden Zielzustandes. Dieser lässt sich durch eine mehr oder minder konkrete und vollständige Liste an Kriterien für den zu erreichenden Zustand beschreiben. Die genaue Formulierung des Ziels entwickelt sich üblicherweise durch einen sukzessiven Konkretisierungsvorgang unter Berücksichtigung der Inputs aus Konflikt- und Materialanalyse.

Konfliktanalyse: Die Konfliktanalyse erfolgt zur Klärung der Fragen: „Was muss ich ändern und wo bestehen Hindernisse, die überwunden werden müssen?". Dieser Teil der Situationsanalyse dient, unter Berücksichtigung des Inputs aus Ziel- und Materialanalyse, der Bestimmung der Diskrepanzen zwischen Ist- und Zielzustand sowie der Erfassung der Hindernisse, die der direkten Zielerreichung im Wege stehen. Je konkreter die Diskrepanzen und die Charakteristika der Hindernisse erfasst werden, desto konkretere Anforderungen können an die zu findende Vorgehensweise zur Erreichung des Zielzustandes gestellt werden. Je konkreter wiederum die Anforderungen sind, desto stärker wird der Raum aller potentiell möglichen Vorgehensweisen auf konkret passende

eingegrenzt und damit die Lösungssuche unterstützt. Im Idealfall aktiviert eine Anforderungsliste direkt eine zugehörige Vorgehensweise.

Materialanalyse: Die Materialanalyse dient der Klärung der Fragen: „Was kann zur Durchführung der Änderung verwendet werden, was kann ich brauchen?“ Als Teil der Situationsanalyse erfolgt die Materialanalyse zur Bestimmung materialgegebener Änderungsmöglichkeiten und zum Überprüfen relevanten Materials bzw. verfügbarer Mittel (z. B. Werkzeug) hinsichtlich der Verwendbarkeit zur Erfüllung der Anforderungen. Für die Lösungsfindung ist sie von zweifacher Bedeutung: Zum einen kann mit ihr das vorliegende Material hinsichtlich der Eignung zur Umsetzung eines gefundenen prinzipiellen Lösungsweges untersucht werden. Zum anderen kann das vorliegende Material dahingehend untersucht werden, ob es Anregungen zur Vorgehensfindung bietet.

Im Regelfall werden Fragen dieser Art iterativ in wechselnder Abfolge beantwortet, was im Idealfall dazu führt, die Problemstellung und die Anforderungen an die zielführenden Mittel und Wege immer mehr zu präzisieren. Dieser zweite Punkt ist besonders wichtig, denn dieser Präzisierungsprozess treibt die Klärung des Vorgehens voran, das von der gegebenen Situation zum Ziel führen soll, wobei evtl. Hindernisse erkannt und Wege zu deren Umgehung konkretisiert werden. In der Materialanalyse bestimmt die handelnde Person oder Gruppe z. B. die Ressourcen (z. B. Zeit) und Dinge (z. B. etwas, das als Stromquelle dienen kann: man denke an die Autobatterien, die in Fukushima zur Versorgung bestimmter leittechnischer Einrichtungen zum Einsatz gekommen sind), die zur Umsetzung der möglichen Vorgehensweise(n) notwendig sind. In diesem Anforderungsprofil werden die gesuchten, zielführenden Eigenschaften zunächst mehr oder minder abstrakt, dann aber (im Idealfall) zunehmend konkret vorweggenommen. Die handelnde Person oder Gruppe formuliert und präzisiert also das Lösungsprinzip und sucht dementsprechend in der Situation mögliche Vorgehensweisen und vorhandene Dinge, die sich eignen, um als konkrete Problemlösung zu fungieren.

Wegen ihrer zielführenden Funktion spricht man in der Fachliteratur auch vom „Funktionalwert“ der betreffenden Vorgehensweise oder Materialien, also von den Merkmalen, die sie besitzen und die dem Lösungsprinzip entsprechend zielführend sind. Lösungsprinzip und „Funktionalwert“ sind also Such- und Erinnerungshilfen für nutzbare regelbasierte Kenntnisse und Erfahrungen. Sie helfen dem Gedächtnis mehr oder minder effektiv und schnell „auf die Sprünge“.

Auf dem Weg zur endgültigen Problemlösung können unterschiedliche Lösungsprinzipien erarbeitet, geprüft und auch verworfen werden. Der Problemlöseversuch kann also zeitaufwendig und recht verschlungen sein. Es können auch Fehler auftreten und Korrekturen solcher Fehler vorgenommen werden. Aus verbleibenden Fehlern kann sich ein ungeeignetes Vorgehen ergeben und umgesetzt werden. Suchen und Finden der Problemlösung können zudem zu langsam verlaufen, um mit der Entwicklung der Situation Schritt zu halten. Es ist auch denkbar, dass die handelnde(n) Person(en) aufgeben oder sich fruchtlos um eine Problemlösung bemühen.

Da diese Prozesse mehr oder minder bewusst verlaufen, ist es möglich, Informationen über den Prozess durch Befragung der handelnden Person(en) bzw. ihren spontanen verbalen Äußerungen zu gewinnen. Dieser Punkt ist für den Analyseteil der Methode wichtig.

Das vorliegende Modell definiert das erfolgreiche Ende der Phase der Ziel-, Material- und Konfliktanalyse durch den Zeitpunkt, zu dem die handelnde(n) Personen(en) eine Vorgehensweise gefunden haben, die ihnen aus anderen Situationen so vertraut ist, dass sie bei der Ausführung regelbasiert vorgehen können, und die sie als geeignet für die Problemlösung halten. An diese Findungs-Phase schließt sich die Phase der Diagnose an.

Phase der Diagnose: In der Diagnose-Phase prüfen die handelnden Personen, ob die Kriterien für die Ausführung des Vorgehens in der Problemsituation erfüllt sind, entscheiden sich für die Ausführung und führen erforderliche Planungen durch (z. B. Verteilung der anstehenden Aufgaben auf die einzelnen Personen). Im vorliegenden Modell wird davon ausgegangen, dass nur im Fehlerfall eine Entscheidung gegen die Ausführung einer zulässigen bzw. für die Umsetzung einer ungeeigneten Vorgehensweise fällt.

Das Modell sieht eine Rückkopplung zwischen der Diagnose und der Phase vor, in der Ziel-, Konflikt- und Materialanalyse die Lösungssuche und Lösungsfindung vorantreiben. Auf diese Weise kann eine Wiederaufnahme dieser Analysen im Modell berücksichtigt werden, wenn die Diagnose dazu geführt hat, ein gefundenes Vorgehen zu verwerfen.

Abb. 4.1 skizziert das beschriebene Modell des Problemlösens.

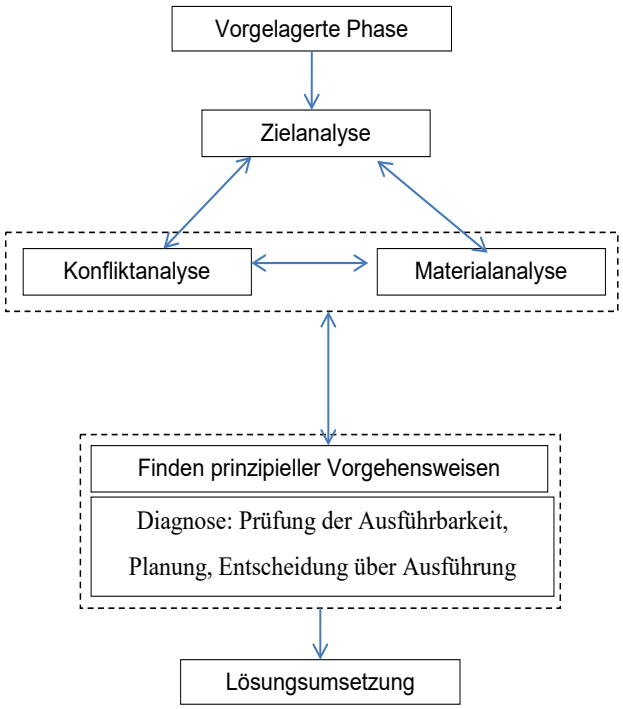


Abb. 4.1 Modell des Problemlösens

4.2.2 Beurteilung der Qualität des Problemlösens

Die qualitative Einschätzung der Erfolgsaussichten des Problemlösens dient als Grundlage für die quantitative Bewertung. Zur Vorbereitung der qualitativen Einschätzung untersucht der Methodenanwender die Aspekte „Stress“, „Systematik des Problemlösens“ und „Güte der Informationen für das Problemlösen“.

Die Systematik des Problemlösens ist zu werten, wobei folgende Merkmale ein systematisches bzw. unsystematisches Vorgehen auszeichnen:

– Die Problemlöser verfolgen ein klares Ziel, das sie während des Problemlöseprozesses nicht aus den Augen verlieren. Das Ziel der Problemlöser entspricht demjenigen, das nach den Ergebnissen der System- und Ereignisablaufanalysen erreicht werden muss. Während der Problemlösung überwacht das Personal den Anlagenzustand und prüft, ob eine Änderung des Ziels erforderlich ist (Stichwort „Zielanalyse“). Werden mehrere Ziele verfolgt, sind Prioritäten entsprechend der objektiv gegebenen Dringlichkeit und Wichtigkeit der einzelnen Ziele zu setzen. Ziele werden in Teilziele zerlegt, wenn die Problemlöser kein Vorgehen finden, das die gegebene Situation direkt in den Zielzustand überführt. Die Teilziele erfassen lückenlos die Etappen, die

zur Erreichung des Ziels durchlaufen werden müssen. Teilziele führen zur Zerlegung des Gesamtproblems in Teilprobleme, die alle systematisch bearbeitet werden. Teilziele können ihrerseits in weitere Teilziele zerlegt werden usw. Die Merkmale der Systematik des Problemlösens sind auf alle Teilprobleme anzuwenden, die das Personal im Zuge der Problemlösung aufstellt.

- Ein unsystematisches Vorgehen besteht dagegen darin, keine, zu allgemeine oder ungenaue Ziele zu setzen, Ziele ohne sachlich triftigen Grund zu wechseln, an Zielen festzuhalten, die geändert werden müssten, oder Ziele zu verfolgen, die eng formuliert sind und dadurch allenfalls zu Teillösungen des Problems führen. Bei mehreren Zielen unterbleiben klare Prioritätensetzungen oder eventuell definierte Prioritäten orientieren sich nicht an der objektiv gegebenen Dringlichkeit und Wichtigkeit der Ziele. Das hat die Folge, dass Ziele zu hoch oder zu niedrig bewertet werden.

- Das Personal sucht und findet die genauen Ursachen dafür, dass das Ziel vom gegebenen Istzustand aus zunächst unerreichbar scheint (Stichwort „Konfliktanalyse“). Bei der Suche werden alternative mögliche Ursachen gesucht und auf Stichhaltigkeit geprüft. Zum Beispiel: Geht die ausbleibende Förderleistung auf einen Defekt der Pumpe zurück oder auf einen vorrangigen Befehl der Automatik, die den Start auslegungsgemäß verhindert? Die Suche nach den Ursachen ist in der verfügbaren Zeit und mit den vorhandenen Informationen möglichst detailliert durchzuführen d.h., Ursachenketten werden soweit möglich bis an ihren Ausgangspunkt zurückverfolgt. Bei Ursachenbündeln werden Wechselwirkungen einbezogen.

- Qualität und Erfolg des Problemlösens stehen infrage, wenn mögliche Ursachen, Ursachenbereiche oder Alternativen zu gefundenen Ursachen und/oder Wechselwirkungen zwischen Ursachen ungeprüft verworfen werden („Es kann doch gar nicht sein, dass …“), wenn die Suche vorzeitig und nicht bei der Erstursache endet, wenn scheinbar offensichtliche Ursachen nicht näher überprüft werden und/oder wenn ein planvolles Vorgehen zur Eingrenzung und Bestimmung der Ursachen fehlt.

- Im Zuge des Problemlösungsprozesses werden zutreffende Lösungsprinzipien formuliert und dem Stand der Ursachenerkenntnis entsprechend verfeinert (bzw. revidiert). Lösungsprinzipien nehmen in genereller Form das tatsächliche Vorgehen zur Lösung des Problems vorweg. Sie bringen zum Ausdruck, was die Lösung ausmacht. Dies unterstützt die Suche nach den konkreten und richtigen Vorgehensweisen und Mitteln. Man weiß, wonach man zu suchen hat und was eine Lösung auszeichnet bzw. welche Merkmale diese Vorgehensweise und Mittel befähigen, als Lösung zu

fungieren (siehe „Funktionalwert“). Dagegen beeinträchtigen oder verhindern vage, unzutreffende oder fehlende Lösungsprinzipien die Suche nach adäquaten Lösungen.

- Problemlösen umfasst in der gegebenen Situation die Suche nach Möglichkeiten, einen anvisierten Lösungsweg in die Tat umzusetzen (Stichwort „Materialanalyse“). Die Methode definiert als Lösung sicherheitstechnisch zulässige Vorgehensweisen bei Routineaufgaben oder Teile daraus, die einzeln oder in Kombination die Erreichung des angestrebten Sicherheitszieles (oder eines Teilziels auf dem Weg zu diesem Ziel) ermöglichen. Systematische Lösungssuche zeichnet sich dadurch aus, die vorhandenen Unterlagen wie Betriebs- und Notfallhandbuch nach nutzbaren Vorgehensweisen zu durchsuchen und Fachkräfte nach solchen Vorgehensweisen zu befragen. Die an der Problemlösung beteiligten Personen achten darauf, dass jedes einzelne Teilziel den Kriterien und Bedingungen der Anwendung des Vorgehens entspricht, mit dem das nächste Teilziel erreicht werden soll.

- Die Problemlöser prüfen die gefundene(n) Vorgehensweise(n) zur Zielerreichung auf ihre sicherheitstechnische Zulässigkeit, Ausführbarkeit, Wirksamkeit und Nebeneffekte in der gegebenen Situation (Stichwörter „mentale Simulation“ und „Auswahl der Vorgehensweise“). Die Ausführbarkeit ist zum Beispiel zu beurteilen, indem man die verfügbare Zeit für die Ausführung, die Einsatzbereitschaft erforderlicher Fachkräfte, die Erreichbarkeit der Ausführungsorte und die Arbeitsbedingungen an diesen Orten in Betracht zieht und wertet. Die Ausführung kann Freischaltungen voraussetzen, die das Personal in die Betrachtung einbeziehen muss. Werden Anwendungsbedingungen gelockert oder Nebeneffekte in Kauf genommen, erfolgt dies nach sorgfältiger Prüfung des Für und Wider. Erfüllen gefundene Vorgehensweisen die Anforderungen an Anwendbarkeit, Ausführbarkeit, Wirkung und Nebeneffekte nicht, verzichten die Problemlöser auf die Umsetzung. Entscheiden sie sich für die Umsetzung, sind mögliche Hindernisse und Fehler bei der Ausführung zu antizipieren, wobei geeignete Vorkehrungen festzulegen sind.

- In einem unsystematischen Problemlösungsprozess bleibt die Nutzung der Quellen für Vorgehensweisen in inakzeptabler Weise selektiv. In einem solchen Fall setzt das Personal eine gefundene Vorgehensweise um, ohne genau zu prüfen, ob sie die Anforderungen an Zulässigkeit, Ausführbarkeit und Wirksamkeit wirklich erfüllen.

In einem Problemlösungsprozess benötigt das Personal Informationen bzw. Kenntnisse über

- den Zustand der Anlage, Systeme und Komponenten,
- den Aufbau der Systeme und Komponenten,
- ihre system- und verfahrenstechnischen Zusammenhänge,
- Prozeduren und andere Beschreibungen von Vorgehensweisen, mit denen sich System- und Komponentenzustände ändern lassen, und
- Lage, Aufbau und Aufteilung von Gebäuden, Gebäudebereichen, Räumen etc.

Der Methodenanwender hat die Güte der Informationen zu beurteilen. Zu betrachten sind Informationen auf den Benutzungsoberflächen und solche in Unterlagen. Dabei steht „Benutzungsoberfläche“ für alle Teile der Anlage innerhalb und außerhalb der Warte, an denen das Personal Kontrollen und/oder Eingriffe vorzunehmen hat. Zu den Kontrollen gehört nicht nur das Ablesen von Informationseinrichtungen, sondern auch Sichtprüfungen zum Beispiel auf Leckagen an Komponenten vor Ort. Gesichtspunkte zur Einschätzung der Güte der Informationen sind

- für Informationen auf Benutzungsoberflächen: Eindeutigkeit, Zuverlässigkeit, Genauigkeit, Übersichtlichkeit und Zugänglichkeit,
- für Unterlagen: inhaltliche Korrektheit, Vollständigkeit und Klarheit, Übersichtlichkeit sowie Orientierungshilfen, mit denen der Nutzer zuverlässig erforderliche Informationen findet,
- für erinnertes Wissen (Fachkunde): Präsenz dieses Wissens aufgrund Trainings und Anwendung in der Praxis.

Vollständigkeit, Genauigkeit und ergonomisches Design der Informationen sind zu werten. Der Anwender der Methode untersucht, inwieweit es dem Personal gelingt, das Problem trotz unvollständiger, unpräziser und/oder ergonomisch suboptimal gestalteter Informationen zu lösen. Zu berücksichtigen sind Zeitverluste durch die Suche nach benötigten Informationen, Rückgriff auf zusätzliche Informationsquellen wie zum Beispiel erfahrene Kollegen, die aus ihrer Freizeit auf die Anlage geholt werden, und/oder Abschätzungen zur Ausprägung von Prozessgrößen, für die keine genaue Information auf der Benutzungsoberfläche vorliegt, etc. Liegen solche Bedingungen vor, hat der

Anwender zu beurteilen, ob der Problemlösungsprozess trotz solcher Hindernisse und Fehlerquellen systematisch weiterläuft.

Um solche Einschätzungen durchführen zu können ist es vorteilhaft, wenn die notwendigen Informationen im Rahmen einer Anlagenbegehung und (oder) Simulatorübungen eingeholt werden können. Dabei ist der Ereignisablauf, der den wissensbasierten Eingriff erfordert, vorzugeben. Das zuständige Anlagenpersonal erläutert daraufhin, wie es den Ereignisablauf bewältigen würde. Ein wesentlicher Teil der Anlagenbegehung besteht darin, Informationen zu sammeln,

- inwieweit das Personal das erforderliche regelbasierte Wissen über den jeweils betrachteten Eingriff aus anderen Aufgaben hat,
- ob der Eingriff überhaupt durchführbar ist,
- wie systematisch das Personal bei der Ziel-, Konflikt und Materialanalyse sowie bei der Diagnose vorgeht und
- unter welchen weiteren leistungsbestimmenden Faktoren das Personal handeln muss.

Sollte sich herausstellen, dass der wissensbasierte Eingriff nicht Teil des Fachwissens und (oder) nicht durchführbar ist, endet die weitere Untersuchung dieses Eingriffs. In die probabilistische Sicherheitsanalyse geht in diesem Fall das Ergebnis ein, dass der Eingriff mit Wahrscheinlichkeit 1 unterbleibt. Zeigt sich, dass das Personal ein sicherheitstechnisch zulässiges Vorgehen findet, das den Eingriff einschließt, ohne dass dieses Vorgehen aus anderen Aufgaben vertraut und regelbasiert ausführbar ist, liegt ein Fall vor, der den Anwendungsbereich der vorliegenden Methode überschreitet. Der Eingriff ist mit dieser Methode nicht bewertbar. Der Methodenanwender sollte auf nutzbare andere Methoden zurückgreifen oder, wenn keine Alternative besteht, konservativ vom Unterbleiben des Eingriffs ausgehen, das beobachtete Vorgehen aber dokumentieren und als Beleg anführen, dass seine Bewertung des Eingriffs konservativ ist.

Bei der Modellierung und Analyse des Handlungsablaufs erstellt der Methodenanwender auf der Basis seiner Informationen aus der Anlagenbegehung ein Modell („Handlungsmodell“), das den erwarteten Ablauf des wissensbasierten Handelns bei der Bearbeitung der betrachteten Aufgabe durch das Personal repräsentiert. Die Schritte der beobachteten und erfragten Problemlöseversuche sollten in diesem Handlungsmodell möglichst detailliert beschrieben werden. Im Idealfall sollte das Modell die Fragen nach Akteur, Art,

Anlass, Zweck, Objekt, Mittel, Resultat, Zeit, Ort und Rahmenbedingungen der einzelnen Handlungen von der Vorphase bis zum Ende der Ausführungsphase beinhalten. Das Handlungsmodell ist mit dem beteiligten Personal und weiteren, kompetenten Vertretern der Anlage zu diskutieren. Im Rahmen der Diskussion sind alle Punkte zu bereinigen, die nach stichhaltigen Überlegungen der Korrektur bedürfen.

Erfolg und Misserfolg des Problemlöseversuchs hängen von Rahmenbedingungen ab, die in der probabilistischen Sicherheitsanalyse auch „leistungsbestimmende Faktoren“ o. ä. heißen. Das vorliegende Modell berücksichtigt Abhängigkeiten von folgenden Faktoren:

- Negative Effekte aus der Vorphase, wie z. B. Stress durch Zeitdruck.
- Fachwissen des Personals. Z. B., das Personal verfügt nur bedingt über das erforderliche Fachwissen.
- Qualität der Informationseinrichtungen und Dokumentationen. Sie stellen die Informationen bereit, die für den Problemlöseprozess erforderlich sind. Einschränkungen können z. B. wegen eines Ausfalls entsprechender Anzeigeeinrichtungen oder Unklarheiten in der Dokumentation bestehen. Zu den Informationseinrichtungen zählen auch Bedieneinrichtungen, deren Stellung anzeigt, welcher Eingriff über diese Bedieneinrichtung ausgeführt worden ist.
- Systematisches Vorgehen beim Problemlöseversuch. Das Personal geht beim systematisch oder eher unsystematisch bis (im Extremfall) chaotisch vor. Dieser Punkt zählt im vorliegenden Modell als leistungsbestimmender Faktor, weil er die Problemlöseversuche strukturiert, was sich auf Leistung und Erfolg beim Problemlösen auswirkt.

Der Methodenanwender verknüpft die gewonnenen Erkenntnisse über das Fachwissen, die Systematik des Problemlösens und die Rahmenbedingungen für das Problemlösen zu einer Gesamtbeurteilung der Erfolgsaussichten des Problemlösungsprozesses. Tab. 4.1 zeigt, wie die zusammenfassende Wertung vorzunehmen ist. In ihren ersten drei Stufen basiert sie auf den in /FAS 10/ dargestellten Überlegungen.

Tab. 4.1 Stufen der zusammenfasssenden qualitativen Wertung der Analyseergebnisse

Ergebnis der Analyse	**Erfolgsaussichten**
Mindestens eine der drei folgenden Aussagen trifft zu: • Fachwissen unzureichend • Erforderliche Informationen (auf Benutzungsoberflächen und in Unterlagen) nicht oder nicht in der erforderlichen Qualität verfügbar • Problemlösungsprozess (wg. Stress, Übervereinfachungen des Denkens und/oder mangelnder Systematik) nicht oder kaum in geordneter Form durchführbar	keine
Alle vier Aussagen treffen zu: • Fachwissen ausreichend • Erforderliche Informationen (auf Benutzungsoberflächen und in Unterlagen) teilweise nicht verfügbar • Anlagenbegehung zeigt, dass trotz der Informationsdefizite Nutzung des erforderlichen Wissens prinzipiell möglich, aber auch fehleranfälliger ist • Problemlösungsprozess systematisch durchführbar	mäßig
Alle drei Aussagen treffen zu, allerdings sind negative Einflüsse der vorgelagerten Phase zu berücksichtigen: • Fachwissen ausreichend • Erforderliche Informationen (auf Benutzungsoberflächen und in Unterlagen) verfügbar • Problemlösungsprozess systematisch ohne schwerwiegende Fehlermöglichkeiten durchführbar	gut
Alle drei Aussagen treffen zu, negative Einflüsse der vorgelagerten Phase sind nicht zu berücksichtigen: • Fachwissen ausreichend • Erforderliche Informationen (auf Benutzungsoberflächen und in Unterlagen) verfügbar • Problemlösungsprozess systematisch ohne schwerwiegende Fehlermöglichkeiten durchführbar	sehr gut

Im Rahmen dieses Vorhabens wurde eine zusätzliche Stufe neu eingeführt, da das erweiterte Prozessmodell zum wissensbasierten Handeln (vgl. Abb. 4.1) neben der Modellierung der Phase des Problemlösens nun auch die vorgelagerte Phase umfasst. Hierdurch wird die Möglichkeit berücksichtigt, dass Einflüsse von Stress und damit

zusammenhängend die Bewältigung negativer Emotionen das Problemlösen verzögern (oder sogar ganz verhindern) können. Ein Beispiel hierfür ist der Eintritt eines auslösenden Ereignisses, bei dem es vor Beginn des Problemlöseversuchs zu einer RESA Auslösung kommt. Sind keine negativen Einflüsse aus der Vorphase zu berücksichtigen und die Aussagen aus Stufe 3 treffen zu, so ist die Gesamtsituation als sehr gut einzuschätzen.

4.2.3 Quantitative Bewertung wissensbasierten Handelns

Die vorliegende Methode unterstützt zwei Ansätze für die quantitative Bewertung des Problemlöseversuchs. Sie unterscheiden sich durch die Art und Weise, wie sie Zeit und Zuverlässigkeit des Problemlösens und seiner Schritte berücksichtigen:

- Das eine Verfahren zur Quantifizierung beruht auf einem Bewertungsansatz, den Swain für die Diagnose von Situationen und die dazu gehörige Auswahl der erforderlichen Prozedur(en) entwickelt hat. Dieser Ansatz kann jedoch nur angewendet werden, wenn sowohl der Zeitaufwand für die Ausführung der Prozedur T_A als auch die Länge des Zeitfensters T_{MAX}, in dem die Prozedur ausgeführt sein muss, im Vorfeld der Analyse bekannt sind. Zufällige Schwankungen dieser Zeiten werden berücksichtigt.

- Liegen Informationen zu T_{Max} bzw. T_A nicht vor, kann der Ansatz nach Swain nicht angewendet werden. In diesem Fall bietet der Einsatz des Crew-Moduls (s. Abschnitt 2.2) die Möglichkeit, die Zuverlässigkeit des Problemlösens im Rahmen einer probabilistischen Dynamikanalyse unter Verwendung von MCDET zu ermitteln. In diesem Fall werden für die einzelnen Schritte des Problemlöseprozesses stochastisch verteilte Ausführungszeiten und Schätzwerte für die Wahrscheinlichkeit ihrer erfolgreichen Durchführung bereitgestellt. Im Rahmen der Simulation werden die Schritte dann sukzessive mit ihren Beiträgen zu Zeitdauer und Zuverlässigkeit des Problemlösens und den sich ergebenden Folgen für den weiteren Ereignisablauf berücksichtigt.

- Beide Methoden sind bereits einsatzfähig. Untersuchungen sind erforderlich, um eventuelle Unterschiede der beiden Methoden erklären zu können. Ideen dazu findet man in der Diskussion der Methodenentwicklung und Methodenanwendung im Rahmen des vorliegenden Projekts. Es folgt eine Beschreibung beider Modellansätze.

Modellansatz 1 zur Bewertung des Problemlöseversuchs mit Hilfe von Swains Daten für die Zuverlässigkeitsbewertung der Diagnose:

Eine ausführliche Begründung für die Nutzbarkeit der Swain'schen Daten ist im Vorgängerbericht (/FAS 10/, S. 54 ff.) gegeben. Die Bewertung fußt auf der qualitativen Beurteilung der Erfolgsaussichten des Problemlöseversuchs (s. Tab. 4.1). Abb. 4.2 präsentiert die Zeit-Zuverlässigkeitskurve aus Swain, die als Grundlage der Modellentwicklung gedient hat. Bei mäßigen, guten und sehr guten Aussichten muss der Anwender die Länge der Zeitspanne einbeziehen, die dem Personal für die Problemlösung zur Verfügung steht. D. h. die quantitative Bestimmung der Zuverlässigkeit des Problemlösens ist in diesen Fällen außerdem abhängig vom zur Verfügung stehenden Zeitfenster, in dem das Problem gelöst werden muss. Die Zeitspanne des zur Verfügung stehenden Zeitfensters beginnt mit dem Eintritt des Anlagenzustandes, der ein wissensbasiertes Handeln erfordert.

Aus Tab. 4.2 können die Schätzwerte für die Misserfolgswahrscheinlichkeit des Problemlöseversuchs in Abhängigkeit von den Erfolgsaussichten und dem zur Verfügung stehenden Zeitfensters ermittelt werden.

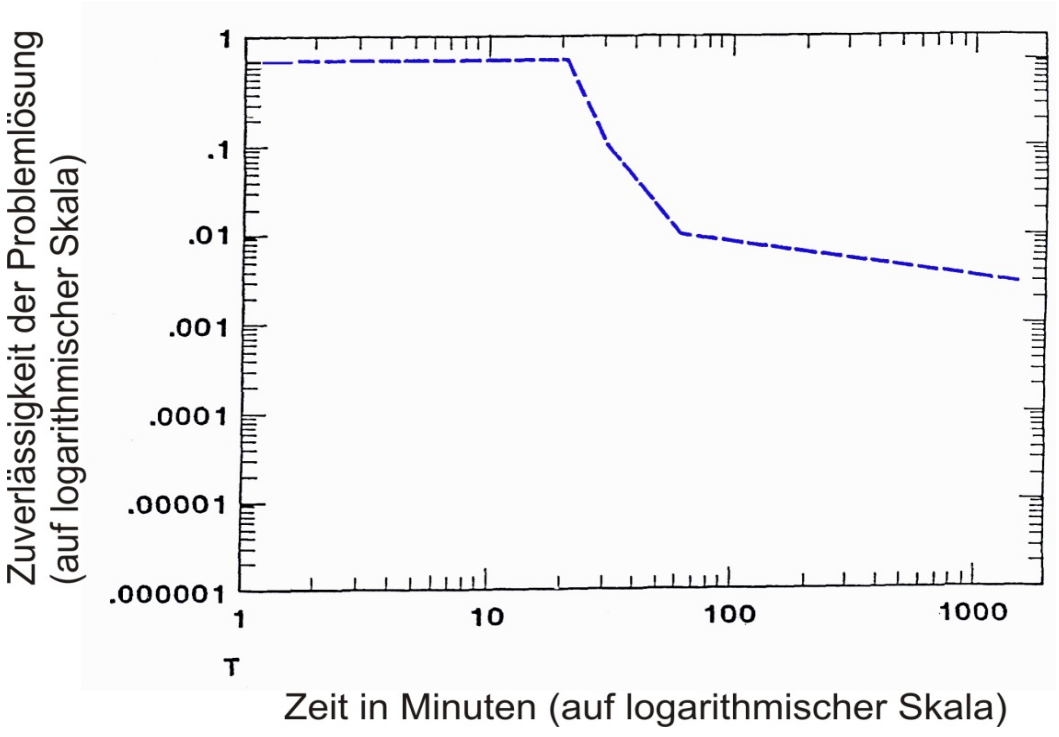


Abb. 4.2 Fehlerwahrscheinlichkeit des Problemlösens unter guten Erfolgsaussichten in Abhängigkeit von dem zur Verfügung stehenden Zeitfenster

Tab. 4.2 Funktion zur Interpolation der Fehlerwahrscheinlichkeit des Problemlösens (nach Swain) in Abhängigkeit der Erfolgsaussichten

Erfolgsaussichten → Folge für die Problemlösung	**Schätzwert für die Wahrscheinlichkeit P, dass die Problemlösung ausbleibt, in Abhängigkeit von der zur Verfügung stehenden Zeit T (in min)**
Sehr gut → Die Problemlösung ist sehr wahrscheinlich.	Horizontale Verschiebung der Kurve in Abb. 4.2 nach links, so dass: Falls T ≤ 2: P = 1 Falls 2 < T ≤ 12: P = 1 – 0.09 * (T – 2) Falls 12 < T ≤ 42: P = 0.1 – 0.003 * (T – 12) Falls 42 < T ≤ 1000: P = 0.01 – 6.263 E-06 * (T – 42)
Gut → Die Problemlösung ist wahrscheinlich.	Entsprechend der Kurve in Abb. 4.2: Falls T ≤ 20: P = 1 Falls 20 < T ≤ 30: P = 1 – 0.09 * (T - 20) Falls 30 < T ≤ 60: P = 0.1 – 0.003 * (T - 30) Falls 60 < T ≤ 1000: P = 0.01 – 6.263 E-06 * (T – 60)
Mäßig → Die Problemlösung ist mäßig wahrscheinlich.	P = 1.0, falls 0 – 20 min für den Problemlöseversuch zur Verfügung stehen. P = 0.5, falls 20 min oder mehr für den Problemlöseversuch zur Verfügung stehen.
Keine → Die Problemlösung wird sicher nicht gefunden.	P = 1.0 unabhängig von der Zeit, die für den Problemlöseversuch zur Verfügung steht.

Die Kurve in Abb. 4.2 stellt einen sehr konservativen Bewertungsansatz dar (/SWA 83/, S. 12-13). Er wird Erkenntnissen aus der Betriebserfahrung zum wissensbasierten Handeln nicht gerecht. Daher wurde eine „Justierung“ der Kurve für den Fall vorgenommen, dass die Erfolgsaussichten des Problemlöseversuchs als sehr gut eingeschätzt werden. Als Beispiel kann das Ereignis genannt werden, das im vorliegenden Projekt als Anwendungsfall dient (s. Abschnitt 4.3). Zur Orientierung für die Zeitschwelle von zwei min dienten Erkenntnisse aus dem Ereignis und die Beurteilung auf Seiten der Methodenentwickler, dass diese Zeitschwelle auch bei zügiger Ziel-, Konflikt- und Materialanalyse mit den Informationen auf der Warte eines Kernkraftwerkes eher nicht unterboten werden wird.

Bei mäßigen Erfolgsaussichten sieht die Tabelle eine Sprungfunktion vor. Geht man von der Abb. 4.2 aus, erkennt man, dass eine Gerade durch die beiden Punkte (T = 20 min, P = 1,00) und (T = 1000 min, P = 0,50) im Koordinatensystem mit logarithmischen Achsen ein flaches Gefälle aufweist. Eine eventuelle Weiterentwicklung der Methode soll auch die Recherche einschließen, ob man die Zuverlässigkeit der Problemlösung unter mäßigen Erfolgsaussichten hinreichend genau mit einer solchen Geraden und den zugehörigen Unsicherheitsbändern erfassen kann.

Die Funktionen in Tab. 4.2 wurden anhand von Referenzwerten der Fehlerwahrscheinlichkeiten des Problemlösens ermittelt. Bei Berücksichtigung von Unsicherheiten müssten die Funktionen entsprechend modifiziert werden. Um diese Modifikation der Funktionen zu automatisieren müssten entsprechende Algorithmen entwickelt und implementiert werden. Diese Weiterentwicklung muss ggf. in einem Nachfolgeprojekt erfolgen. Aus diesem Grund wurde in der Analyse des Anwendungsfalles auf die Berücksichtigung der epistemischen Unsicherheiten bzgl. der Wahrscheinlichkeitsschätzungen verzichtet.

Dem Problemlöseversuch geht im Regelfall eine Phase voraus („Vorphase“, siehe Abb. 4.1), in der sich das Personal noch nicht systematisch mit der Problemsituation auseinandersetzt. Diese Vorphase ist durch das Zeitintervall abgedeckt, in dem sicher keine Lösung gefunden wird.

Das charakteristische Merkmal der hier beschriebenen Methodik besteht in der Abhängigkeit der Zuverlässigkeit des Problemlösens vom Zeitfenster, das dem Personal zur Lösung des Problems (d. h. Lösungsfindung und Ausführung) zur Verfügung steht. In mehr oder minder vielen Fällen ist jedoch die Situation gegeben, dass die für eine Problemlösung zur Verfügung stehende Zeit im Vorfeld der Analyse nicht bekannt ist und – wenn überhaupt – nur mit eheblichen Aufwand zu ermitteln ist. In diesem Fall kann die Quantifizierung der Zuverlässigkeit des Problemlösens mit dem Modellansatz 1 nicht bzw. nur unter erheblichem Aufwand durchgeführt werden kann. Dagegen kann die in diesem Vorhaben entwickelte Methodik zur Quantifizierung der Zuverlässigkeit der Problemlösung (Modellansatz 2) ohne diese Einschränkung angewendet werden. Beide Modellansätze werden für den Anwendungsfall eingesetzt und diskutiert.

Modellansatz 2 zur Bewertung des Problemlöseversuchs basierend auf der Bewertung der einzelnen Hauptschritte:

Das Modell des Problemlösens sieht zwei Hauptschritte des Problemlöseversuchs vor.

- Zum ersten Schritt gehören die Ziel-, Konflikt- und Materialanalysen, aus denen im Idealfall eine immer präzisere Bestimmung der Anforderung hervorgeht, aus denen sich ein Vorgehen zur Überwindung der Problemsituation herauskristallisiert. Das Ergebnis dieser Analysen ist die Erkenntnis, dass die Problemsituation einer Aufgabe gleicht, für deren Bearbeitung eine regelbasiert ausführbare Prozedur eingesetzt werden kann, die aus Schulung und (oder) beruflicher Praxis bekannt ist.

- Im zweiten Schritt wird diagnostiziert, ob die gefundene Vorgehensweise tatsächlich zielführend und ausführbar ist. Dieser Schritt endet im Idealfall mit der Entscheidung für die Ausführung der Prozedur.

Für beide Schritte sind Schätzwerte für Zeitbedarf und Zuverlässigkeit einschließlich ihrer Unsicherheiten festzulegen.

Zur Bestimmung des Zeitbedarfs für den ersten Schritt sieht die vorliegende Methode zwei Möglichkeiten vor:

i) Der Methodenanwender schätzt auf der Basis seiner Informationen aus der Anlagenbegehung den Zeitaufwand ab. Um mögliche zufällige Variationen bzgl. des Zeitaufwands zu berücksichtigen, sollte ein Minimal- und Maximalwert für den Zeitaufwand abgeschätzt werden, die der erste Schritt realistischer Weise in Anspruch nehmen könnte. Um die Unsicherheit zu berücksichtigen, wird im einfachsten Fall eine Gleichverteilung des Zeitaufwands zwischen diesen beiden Grenzwerten angenommen.

ii) Fehlen derartige Informationen, wird folgender generische Ansatz vorgeschlagen: Der Anwender rekonstruiert mit den verfügbaren Informationen die einzelnen Überlegungen, die zu Ziel-, Konflikt- und Materialanalyse bis zur Identifikation des Vorgehens gehören. Ein Überlegungsschritt wird mit der „Unit Task“ der Arbeitsweise des menschlichen kognitiven Systems lt. Newell (/NEW 94/, S. 122) gleichgesetzt. Die Grundlage dieser Gleichsetzung sind Erkenntnisse aus der experimentellen Grundlagenforschung zum Problemlösen (/NEW 94/, S. 144 ff.). Richtwert für die Durchführung einer „Unit Task“ sind 10 s. Diese 10 s werden vereinfachend als feste untere Grenze für die Dauer der „Unit Task“ behandelt. Laut Saifert (/SAI 93/, S. 399) ist mit der zuverlässigen Erfüllung informatorischer (aus der Verarbeitung von Information bestehenden) Arbeit zu rechnen, wenn die ausführende Person für die Durchführung ein Zeitbudget zur Verfügung hat, das etwa das 1.5-fache bis 1.7-fache der reinen Ausführungszeit beträgt. Steht die Liste der einzelnen Überlegungen fest, kann man aus dem Zeitbedarf der Einzelüberlegungen (inklusive der zufälligen Schwankungen) den Gesamtzeitbedarf abschätzen. Der Einfachheit halber wird pro einzelner Überlegung eine Gleichverteilung der Zeitspanne zwischen 10 und 17 s angenommen.

Neben den Durchführzeiten der Vorphase ist auch die Zuverlässigkeit der Ziel-, Konflikt- und Materialanalyse quantitativ zu bewerten. In Abhängigkeit der qualitativen

Einschätzung der Erfolgsaussicht der Problemlösung sind in Tab. 4.3 Schätzwerte für die Wahrscheinlichkeit angegeben, dass am Ende der Ziel-, Konflikt- und Materialanalysen die korrekte Problemlösung steht. Deren Anwendbarkeit ist anschließend im Diagnoseschritt zu verifizieren.

Tab. 4.3 Quantitative Bewertung der Zuverlässigkeit erfolgreicher Ziel-, Konflikt- und Materialanalyse (Vorphase)

Erfolgsaussichten → Folge für die Problemlösung	**Schätzwert für die Wahrscheinlichkeit P, die Problemlösung zu finden**
Sehr gut → Die Problemlösung ist sehr wahrscheinlich.	5 % – 0.70 ≤ P < 0.80 * 10 % – 0.80 ≤ P < 0.90 85 % – 0.90 ≤ P ≤ 1.00 * Mit einer Wkt. von in 5 % liegt die Zuverlässigkeit P, eine Lösung des Problems zu finden, im Intervall zwischen 0.70 ≤ P < 0.80. Die Werte zwischen 0.70 und 0.80 werden als gleichverteilt angenommen. Alle restlichen Angaben sind analog zu lesen.
Gut → Die Problemlösung ist wahrscheinlich.	10 % – 0.60 ≤ P < 0.80 60 % – 0.80 ≤ P < 0.90 30 % – 0.90 ≤ P ≤ 1.00
Mäßig → Die Problemlösung ist mäßig wahrscheinlich.	15 % – 0. ≤ P < 0.40 75 % – 0.40 ≤ P < 0.70 10 % – 0.70 ≤ P ≤ 1.00
Keine → Die Problemlösung wird sicher nicht gefunden.	P = 0.00

Grundlage dieser Wahrscheinlichkeitsangaben bildet eine erste Abschätzung von der Entwicklerseite. Sie war erforderlich, weil die Recherchen empirischer Datenbestände im vorliegenden Projekt zu keinen nutzbaren Daten geführt haben. Eine eventuelle Weiterentwicklung der Methode könnte den Schritt einschließen, diese erste Abschätzung auf eine breitere Grundlage zu stellen.

Die aufgeführten Verteilungen sind mit dem Ziel gewählt worden, Problemlöseversuche unter mäßigen Erfolgsaussuchten deutlich von denjenigen unter guten bzw. sehr guten Voraussetzungen Erfolgsfaktoren zu unterscheiden. Unter mäßigen Voraussetzungen einer erfolgreichen Lösungsfindung sollte die gesamte Spannbreite der Erfolgswahrscheinlichkeit zwischen 0.00 und 1.00 erfasst werden, wobei der Schwerpunkt in den Bereich der mittleren Erfolgswahrscheinlichkeiten mit einem „Bias“ zu Werten oberhalb der Marke von 0.50 gelegt wurde. Die Begründung liegt darin, dass es dem Personal

trotz der informatorischen Handicaps gelingen kann, mit seinem Wissen und seinem systematischen Vorgehen die Problemlösung zu finden (vgl. Tab. 4.1).

Unter guten und sehr guten Voraussetzungen ist zu erwarten, dass die handelnden Personen die erforderliche Problemlösung mit einer hohen Wahrscheinlichkeit finden, deren Ausprägung deutlich über dem Wert von 0.50 liegt. Der Unterschied zwischen „guten“ und „sehr guten“ Erfolgsaussichten spiegelt sich v. a. im Schwerpunkt der Verteilungen, mit denen eine hohe Erfolgswahrscheinlichkeit erwartet wird.

Es ist zu betonen, dass die ersten Abschätzungen in Tab. 4.3 durch Werte ersetzt werden können, die je nach Anwendungsfall besser zu begründen sind.

Der zweite Schritt der Methodik umfasst die Diagnose in der zu prüfen ist, ob ein gefundenes Verfahren in der gegebenen Situation angewendet werden kann und soll. Die gefundene Vorgehensweise gehört, den Voraussetzungen des Modells zufolge, den regelbasierten Kenntnissen an. Daher stützt sich die Bewertung der Diagnose in der vorliegenden Methode auf entsprechende, öffentlich zugängliche Daten. Diese stammen aus Untersuchungen in den Sandia National Laboratories. Dabei hatten Teams von Operateuren Szenarien, die ihnen aus Training und/oder Praxis vertraut waren, zu diagnostizieren, die zugehörige(n) Prozeduren zu identifizieren und auszuführen. Ein Untersuchungsteam hat das Vorgehen beobachtet, die Szenarien in zwölf Kategorien eingeteilt und aus den Beobachtungen pro Kategorie eine Verteilung abgeleitet. Diese Verteilung zeigt, wie die Wahrscheinlichkeit der korrekten Diagnose mit der Zeit anwächst. Die Ergebnisse dieser Untersuchungen sind ausführlich in /WES 87/ dokumentiert.

Für das im Abschnitt 4.3 beschriebene Anwendungsbeispiel wurde die Zeit-Zuverlässigkeitsverteilung der Kategorie 11 verwendet. Die Beschreibung der Handlungen in Kategorie 11 lautet gemäß /WES 87/:

Group 11: „Local operation of manually controlled components normally operated from the control-room when control room operation fails “.

Die dazugehörige Verteilung ist Tab. 4.4 angegeben.

Tab. 4.4 Zeitabhängige Verteilung der Fehlerwahrscheinlichkeit für die Diagnose von Handlungen (Auszug entnommen aus /WES 87/)

Table 2.1.9-9

Group 11, Parameter Estimates from Fit of Lognormal Function
(N = 15, Mean = .85, Standard Deviation = .50)

Time (min.)	Standard Deviation of Point	Probability of Failure	Upper 95% Confidence Limit	Lower 95% Confidence Limit
1	.039	.96	.99	.78
2	.072	.87	.96	.66
3	.088	.77	.90	.56
4	.096	.69	.85	.48
5	.10	.62	.79	.41
6	.10	.56	.74	.36
7	.10	.51	.70	.31
8	.11	.46	.66	.27
9	.11	.42	.63	.24
10	.10	.39	.60	.21
11	.10	.35	.57	.18
12	.10	.33	.55	.16
13	.10	.30	.53	.14
14	.10	.28	.51	.13
15	.098	.26	.49	.11
16	.096	.24	.47	.10
17	.094	.23	.46	.092
18	.092	.21	.44	.083
19	.090	.20	.43	.075
20	.088	.19	.42	.068
21	.086	.18	.41	.062
22	.084	.16	.40	.056
23	.082	.16	.39	.051
24	.080	.15	.38	.047
25	.079	.14	.37	.043
26	.077	.13	.36	.039
27	.075	.12	.35	.036
28	.073	.12	.35	.033
29*	.071	.11	.34	.030
30	.069	.11	.33	.028
31	.068	.10	.33	.026
32	.066	.097	.32	.024
33	.064	.092	.31	.022
34	.063	.088	.31	.020
35	.061	.084	.30	.019
36	.060	.081	.30	.018
37	.058	.077	.29	.016
38	.057	.074	.29	.015
39	.056	.071	.29	.014
40	.054	.068	.28	.013
41	.053	.065	.28	.012

*Extrapolated beyond time = 28.9 min.

Mit dem Ereigniseintritt und der Anforderung des Problemlösens setzt der Prozess des Problemlösens nicht unbedingt sofort oder nur geringfügig verzögert ein. Es ist zu beachten, dass aus unterschiedlichen Gründen mehr oder minder viel Zeit verstreichen kann, bis der Handelnde sich systematisch mit dem Problem auseinandersetzt, um zu einer Lösung zu kommen. Die Methode sieht daher eine Vorstufe oder Vorphase vor, die Zeit kostet und deshalb in die Chronologie des Handlungsablaufs einzugehen hat. Die Vorphase umfasst die Zeitspanne, in der die handelnde(n) Person(en) erkennen müssen, dass sie vor einem Problem stehen und mit Hilfe ihres Wissens ein zielführendes Vorgehen finden müssen, mit dem das Problem zu lösen ist.

4.3 Anwendung des Modells zum wissensbasierten Handeln an einem Ereignis aus der deutschen Betriebserfahrung

Dem Fallbeispiel liegt ein meldepflichtiges Ereignis zugrunde, das in einer inzwischen stillgelegten und sich im Rückbau befindlichen Anlage auftrat. Zum Zeitpunkt des Ereigniseintritts befand sich die Anlage im störungsfreien Volllastbetrieb.

Nach Ermittlung und Aufbereitung der Informationen zum Referenzereignis kann der Ablauf des Ereignisses wie in Abschnitt 4.3.1 beschrieben werden. Auf die Analyse und Bewertung des Problemlöseprozesses des Ereignisses wird in Abschnitt 4.3.2 eingegangen. In den Abschnitten 4.3.3 und 4.3.4 werden die beiden, oben beschriebenen Modellansätze zum wissensbasierten Handeln auf das Referenzereignis angewendet. In Abschnitt 4.3.5 werden die Ergebnisse der beiden Modellansätze verglichen und diskutiert.

4.3.1 Beschreibung des Fallbeispiels

Im Rahmen einer routinemäßig durchzuführenden Maßnahme sollte der Druckhalterabblasetank gespült werden, da sich bei Betrieb der Anlage dort Spalt- und Radiolysegase sammeln. Die Spülung wird mit Stickstoff durchgeführt und ist in gewissen Zeitabständen, die vom Ergebnis der regelmäßigen Gasanalysen abhängen, erforderlich. Die Entgasung erfolgt über das Anlagenentwässerungssystem TE1. Hierzu ist eine Verbindung zwischen Druckhalterabblasetank, der Stickstoffversorgung TN, dem Anlagenentwässerungssystem TE1 und dem Abgassystem TG durchzuschalten. Die Spülung selbst wird durch schrittweises Öffnen der Armatur TE1 A32 über das Bedienfeld am Wartenpult eingeleitet, wobei parallel der Druck im Abblasetank einzustellen und zu kontrollieren ist.

Bei diesem Vorgang öffnete der Operateur versehentlich die Armatur TE1 A10, deren Bedienelemente am Pult direkt über der eigentlich zu fahrenden Armatur TE1 A32 angeordnet sind und die damals nicht gegen ein versehentliches Betätigen gesichert war. Die beiden Bedienfelder sind identisch aufgebaut (Form, Farben, Funktion). Die Beschriftungen unterscheiden sich nur geringfügig. Durch das Öffnen der Armatur TE1 A10 wurde eine direkte Verbindung zwischen dem Primärkreis und dem Entwässerungsbehälter TE1 B01 hergestellt, da die Handarmatur TE1 A21 sich in der Stellung „offen" befand (vgl. Abb. 4.3). Der Handarmatur war damals im Betriebshandbuch keine definierte Grundstellung zugeordnet.

Die Armatur TE1 A10 erreichte schon nach wenigen Sekunden die Endlage „voll offen". Heißes Primärkühlmittel strömte unter hohem Druck zum Entwässerungsbehälter (Leckquerschnitt ca. 13 cm^2). Über die Kontrolle der Zustandsmeldungen bemerkte der Operateur seinen Fehler bereits kurz nach der Fehlbedienung. Sein Schließversuch war allerdings erfolglos. In Schließrichtung besaß die Armatur TE1 A10 einen Drehmomentschutz, der ein Schließen bei zu hohem Drehmoment vorrangig unterbinden kann. Der Schutz spricht noch deutlich vor Erreichen der maximalen Stellkraft des Motors an. Das in den Entwässerungsbehälter einströmende Kühlmittel führte in diesem zu einem schnellen Druckanstieg auf etwa 17 bar. Dieser Wert wurde im Nachhinein aus einer Gleichgewichtsbetrachtung „zuströmende Menge und über das Sicherheitsventil TE1 A05 und die noch offene Gebäudeabschlussarmatur TE1 A53 abströmende Menge (vgl. Abb. 4.3) ermittelt. Der Behälter blieb zunächst intakt, obwohl sein höchstzulässiger Betriebsdruck 6 bar beträgt.

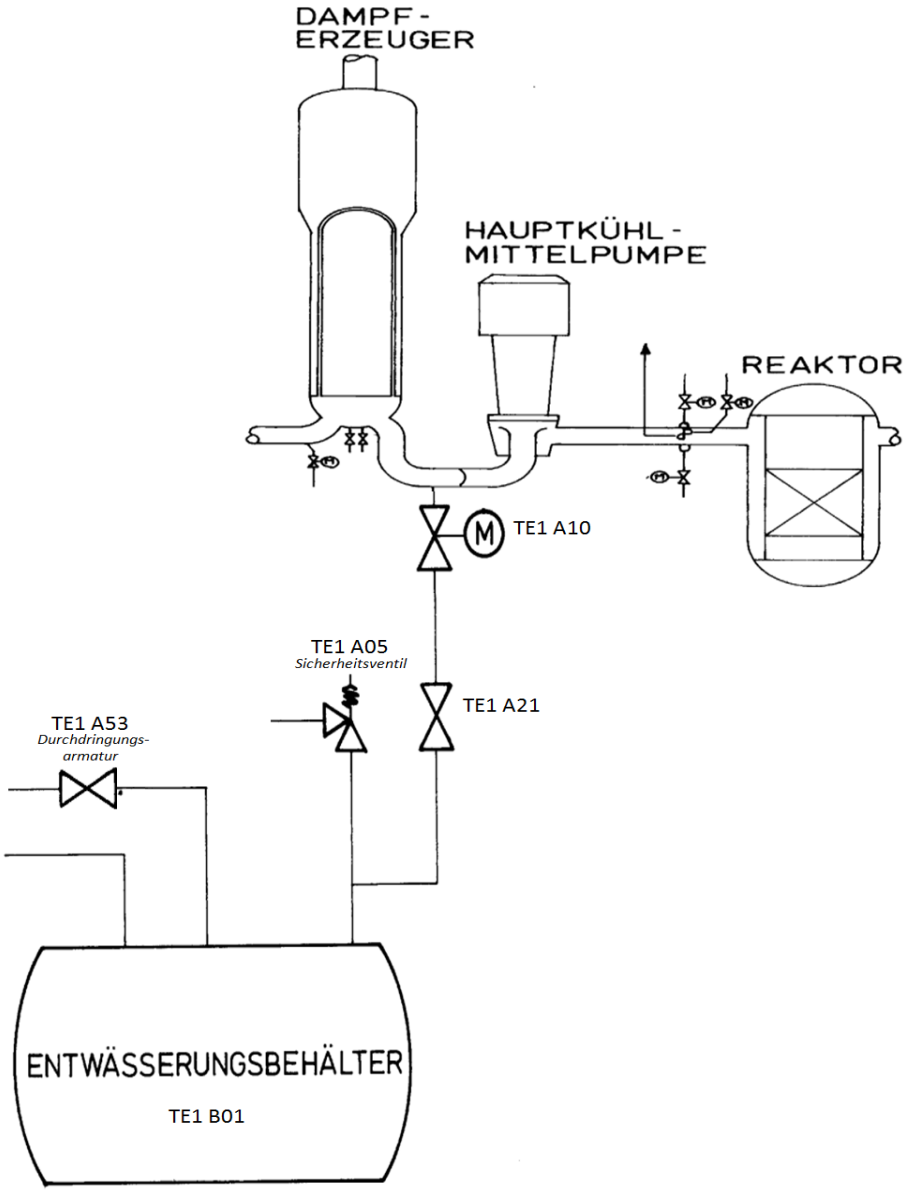


Abb. 4.3 Übersicht zu den relevanten Komponenten des Fallbeispiels

Der Kühlmittelverlust führte zu einem starken Druckeinbruch im Primärkreis. Über den Grenzwert „Siedeabstand zu gering“ löste das Reaktorschutzsystem bereits ca. 35 s nach Auftreten der Fehlhandlung die Reaktorschnellabschaltung aus. Das weitere Absinken des Druckhalterniveaus konnte auch über die automatisch zugeschaltete Hochdruckförderpumpe nicht verhindert werden.

Etwa 2.5 min nach Störungseintritt wurde der Grenzwert „Druckhalterniveau zu tief“ erreicht. Das Reaktorschutzsystem startete nun die Hochdrucksicherheitseinspeisung in den Primärkreis und schloss alle Gebäudeabschlussarmaturen, darunter auch die Armatur TE1 A53.

Durch das Schließen von TE1 A53 entfiel ein wesentlicher Entlastungsquerschnitt des Behälters TE1 B01, der unmittelbar danach geborsten ist. Dies verursachte Folgeschäden an im gleichen Raum angeordneten Systemen, wobei das Primärkühlmittel nun direkt in diesen Raum (Primärkreisleck innerhalb des Sicherheitsbehälters) strömte. Die fälschlich offenstehende Armatur TE1 A10 konnte etwa 13 min nach Störungseintritt vor Ort am Leittechnikschrank durch direktes Ansteuern mittels Adapter geschlossen werden. Die manuelle Maßnahme war notwendig, da der Drehmoment-Motorschutz das Schließen von der Warte aus verhinderte. Diese auf eine erfolgreiche ad hoc Problemlösung beruhende Maßnahme beendete den Kühlmittelverlust aus dem Primärkreis.

4.3.2 Analyse und qualitative Bewertung des Problemlöseprozesses

Die nachfolgende Analyse und Bewertung orientiert sich an dem in Abschnitt 4.1 beschriebenen Modell zum wissensbasierten Handeln und den dort verwendeten Begriffen.

Der Reaktorfahrer öffnete im Zuge eines routinemäßigen Spülvorganges des Druckhalters fälschlicherweise das Entwässerungsventil TE1 A10, was durch die räumliche Nähe der Bedienelemente und der ähnlichen Beschriftung auf dem Steuerungspult begünstigt wurde. Das fehlerhafte Öffnen des Ventils TE1 A10 beschreibt den Beginn (t = 0) einer unerwünschten Situation, die nur durch wissensbasiertes Handeln des Personals behoben werden konnte.

Der Reaktorfahrer bemerkte die falsche Schalthandlung innerhalb einer Reaktionszeit von 1 – 5 s. Hierzu trug die hochgeübte Handlungsroutine „Befehlsgabe und Nachkontrolle der Komponentenreaktion“ bei. Er führte daraufhin unmittelbar einen Korrekturversuch durch (Gegenbefehl). Solche Gegenreaktionen sind Teil des Handlungsspielraums des Operateurs und werden auch in anderen Anlagensituationen durchgeführt. Die Korrektur misslang, da der Drehmoment-Motorschutz unmittelbar das Schließen des Ventils verhinderte. Die Ursache des drehmomentabhängigen Blockierens des Stellantriebs ist darin zu suchen, dass durch die hohe Strömungsgeschwindigkeit des Kühlmittels am Ventilteller grenzwertüberschreitende Querkräfte zur Ventilspindel vorlagen.

Der Eingriff des Drehmomentschutzes wird dem Reaktorfahrer direkt am Bedienfeld der Armatur angezeigt. Die Interpretation des Meldebildes (Verhalten der Zustandsmeldelampe und der Störmeldelampe) ist Bestandteil des hochgeübten Fachwissens des Operateurs. Auch sind für den Operateur die Ursache und die Folgen der Fehlstellung leicht erkennbar (Fachwissen zum Systemaufbau und der Aufgabe der Armatur TE1 A10, das

Absinken des Primärkreisdrucks und des Druckhalterfüllstandes weisen auf einen einsetzenden Kühlmittelverlust aus dem Primärkreis hin, der Zusammenhang zwischen zu hohen Strömungskräften und Ansprechen des Drehmomentschutzes ist Bestandteil des Fachwissens). Ziel musste es sein, diese Armatur wieder zu schließen. Die Randbedingungen für eine erfolgreiche **Ziel- und Konfliktanalyse** sind für dieses Fallbeispiel als günstig einzuschätzen.

Das Schließen der Armatur kann entweder vor Ort mit Handrad oder mittels Elektronikadapter und Stellbefehl unter Umgehung des Schutzes am Schaltschrank erfolgen. Beide Vorgehensweisen sind Bestandteil des Fachwissens und werden im Zusammenhang mit anderen Aufgaben häufig durchgeführt. Die Voraussetzungen für das **Finden von prinzipiell möglichen Vorgehensweisen** sind als günstig einzuschätzen.

Die **Materialanalyse und die mentale Simulation** der Vorgehensweisen lassen allerdings erwarten, dass eine Entscheidung für ein Schließen der Armatur vor Ort wenig wahrscheinlich ist. Die Variante „Stellbefehl am Schaltschrank“ ist schneller durchführbar, der erforderliche Adapter ist griffbereit, es bestehen unter den gegebenen Randbedingungen keine Probleme, den Eingriffsort zu erreichen, und die volle Schließkraftreserve des Elektromotors steht zur Verfügung. Der Zugang zur Armatur selbst ist eingeschränkt und mit möglichen Gefahren für die handelnde Person verbunden. Auch ist es ungewiss, ob der erforderliche Kraftaufwand für ein Schließen mit dem Handrad nicht zu hoch ist.

Die erforderlichen Handlungen zur **Umsetzung der Problemlösung** „Stellbefehl am Schaltschrank“ sind Bestandteil der Fachkunde eines Anlagenelektrikers und werden bei vielen routinemäßig anfallenden Aufgaben durchgeführt.

Die Randbedingungen für einen erfolgreichen Problemlöseversuch sind als mindestens „gut“ einzuschätzen. Folgende Wissenselemente werden zu einer Problemlösung verbunden:

- Wissen um die systemtechnischen Zusammenhänge und der Folgen für die Anlagensicherheit.
- Wissen um den physikalischen Zusammenhang „je höher die Strömungsgeschwindigkeit in der Armatur desto höher die erforderliche Antriebskraft“. Hierdurch wurde die wahrscheinlichste Ursache für das Ansprechen der Schutzeinrichtung identifiziert.

- Wissen um den Aufbau der elektronischen Schutzeinrichtungen der Armatur.
- Wissen um die Auslegungsreserven von Antriebsmotor und Armatur, die deutlich über den Ansprechwerten der Schutzeinrichtung liegen. Hierdurch wurde die Möglichkeit gefunden, die Armatur ggf. noch unter Umgehung des Schutzes zu schließen.
- Wissen um die erforderlichen technischen Eingriffe am Steuerschrank (welcher Schrank, welche Baugruppe, welche Hilfsmittel, welche Stellbefehle sind wo zu simulieren). Vergleichbare Eingriffe in die Steuerung einer Armatur werden ausreichend häufig (u. a. bei Prüfungen) durchgeführt.

Entsprechend der in Abb. 2.1 dargestellten Vorgehensweise zur qualitativen Analyse und Bewertung wissensbasierter Eingriffe verbleibt noch die Aufgabe, den Einfluss der vorgelagerten Phase zu untersuchen und zu bewerten. Im konkret aufgetretenen Ereignis hat der Operateur seinen Fehler und die Fehlerfolgen schnell bemerkt und die einfachste (allerdings wirkungslose) Gegenmaßnahme „Schließen durch Gegenbefehl am Leitstand“ sofort eingeleitet. Wesentliche Teile des Problemlöseprozesses waren bereits erfolgreich bewältigt, noch bevor es zu Reaktionen des Reaktorschutzsystems (u. a. Schnellabschaltung, automatischer Start von Sicherheitssystemen) kam. Die Anlage befand sich im störungsfreien Leistungsbetrieb. Negative Einflüsse der vorgelagerten Phase sind nicht zu berücksichtigen. Die Randbedingungen für eine erfolgreiche Lösung des Problems können insgesamt als „sehr gut“ eingeschätzt werden (vgl. Stufe 4 in Tab. 4.1).

4.3.3 Modellansatz 1 zur Analyse des Referenzereignisses

Zielsetzung des Modellansatzes 1 ist es, den Ablauf des Referenzereignisses in Anlehnung an die klassische Vorgehensweise zu modellieren. Der Unterschied zur klassischen Vorgehensweise ist, dass aleatorische Unsicherheiten in das Modell eingehen, die über Simulationen des erstellten Ereignisbaumes berücksichtigt werden.

Abschnitt 4.3.3.1 liefert eine Beschreibung des Modells. In Abschnitt 4.3.3.2 werden die Analyseergebnisse des Modells dargestellt und Abschnitt 4.3.3.3 liefert eine Beschreibung des Ablaufs der Simulation unter Verwendung des Crew-Moduls und MCDET.

4.3.3.1 Beschreibung des Modells

Wie in Abschnitt 4.3.1 dargestellt, war es die Aufgabe des Operateurs, die Spülung des Druckhalterabblasebehälters durch schrittweises Öffnen der Armatur TE1 A32 einzuleiten. Parallel zum Öffnungsvorgang war der Druck im Abblasebehälter einzustellen und zu kontrollieren. Die Einstellung des Drucks ist ein wichtiges aufmerksamkeitslenkendes Ziel zu Beginn des Spülvorgangs. Es kann angenommen werden, dass der Operateur zunächst auf die Druckanzeige fixiert ist und die Stellungskontrolle der Armatur verzögert durchführt. Dauert die Phase der Ablenkung zu lange (z. B. durch Warten auf eine Reaktion des Druckanzeigers), so treten, in einem solchen Fall dann überraschend, die ersten gravierenden Prozessreaktionen ein (Schnellabschaltung nach etwa 35 s, Start der Notkühlsysteme durch das Reaktorschutzsystem nach etwa 2.5 min). Die Problemerkennung und Lösung haben noch nicht begonnen. Bei einem solchen Ablauf ist mit stressbedingten negativen Einflüssen in der vorgelagerten Phase zu rechnen, die die Problemlösung verzögern können, auch wenn die anderen Randbedingungen für eine Problemlösung sich nicht ändern. Die Erfolgsaussichten des Problemlöseversuchs sind der Stufe 3 der Tab. 4.1 (Erfolgsaussichten gut) zuzuordnen. Das Vorgehen des Operateurs in der vorgelagerten Phase ist ein relevantes Merkmal, das in der folgenden Aufbereitung des Fallbeispiels in der Modellierung berücksichtigt werden muss.

Aufgrund zufällig eintretender Ausfälle und zeitabhängiger Einflüsse sind unterschiedliche Ereignisabläufe und Endzustände mit unterschiedlicher Sicherheitsrelevanz möglich. In Abb. 4.2 wird die Struktur des Modells (nach Modellansatz 1) zur Analyse des Referenzereignisses skizziert.

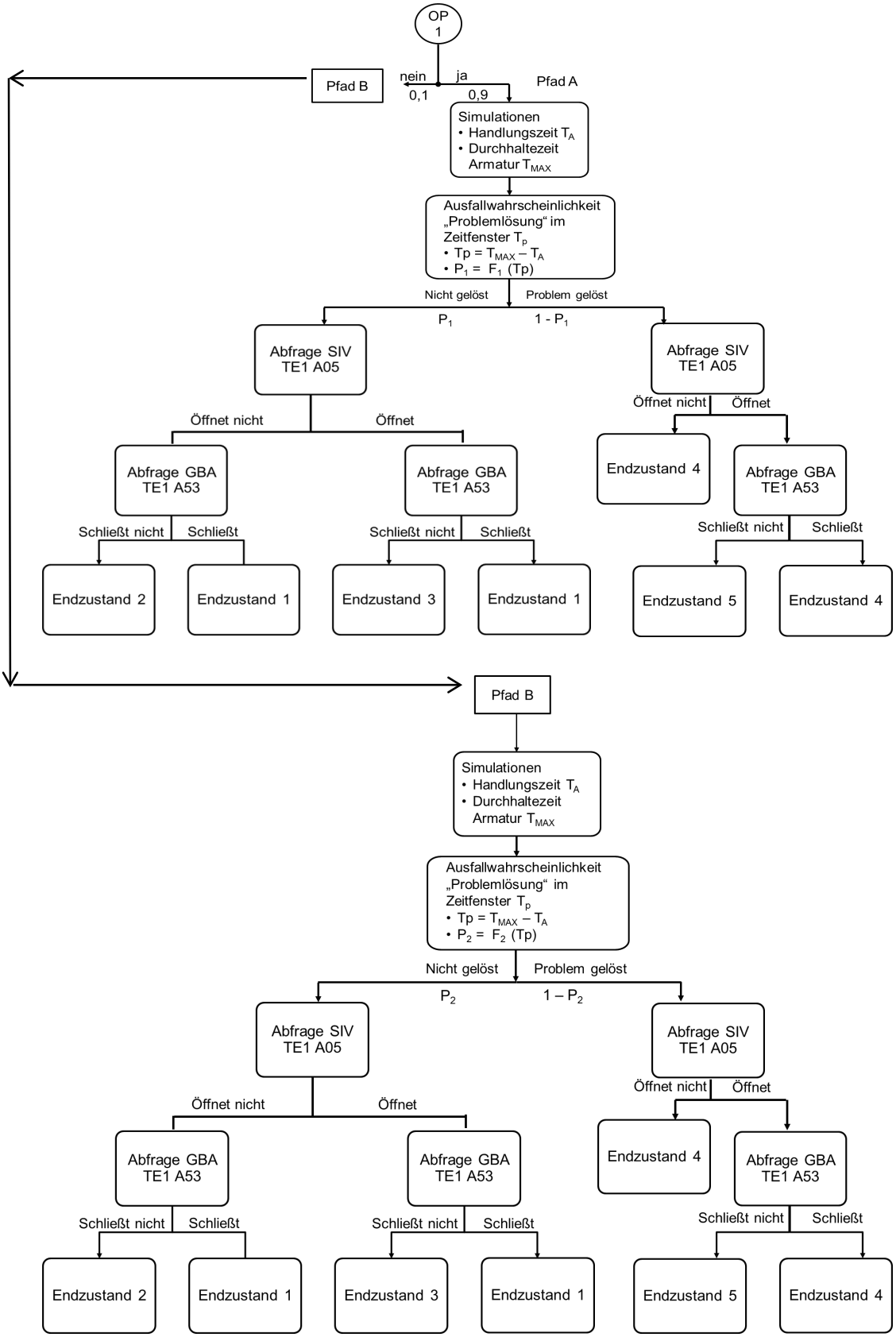


Abb. 4.4 Modell 1 zum Ereignisablauf des zu analysierenden Referenzereignisses

Das Modell in Abb. 4.4 berücksichtigt folgende acht Größen, die einen wesentlichen Einfluss auf den Ereignisablauf haben können:

- Die aleatorische Unsicherheit bzgl. OP1 besteht darin, ob der Operateur die Stellungsrückmeldung des bedienten Ventils sofort registriert und den Fehler erkennt, oder ob er die Stellungsrückmeldung des Ventils nicht sofort kontrolliert und damit den Fehler nicht vor Auslösung der Reaktorschnellabschaltung bemerkt. Die Wahrscheinlichkeit, dass er den Fehler nicht sofort bemerkt, wurde in Anlehnung der im PSA Methodenband empfohlenen Methode ASEP auf p = 0.1 geschätzt.

- T_{MAX} beschreibt die Zeit, in der das Ventils TE1 A10 nach dem fehlerhaften Öffnen noch geschlossen werden kann. Bei Überschreiten der Zeit T_{MAX} wird angenommen, dass es zum vollständigen Schließversagen des Ventils TE1 A10 kommt. Es wird davon ausgegangen, dass bei andauernder Beanspruchung durch die Strömungskräfte und aufgrund der zunehmenden temperaturbedingten mechanischen Verformung der Schließwiderstand soweit zunimmt, dass das Ventil auch durch die Schließkraftreserve des Antriebsmotors nicht mehr geschlossen werden kann. Die Zeit ist abhängig von zufällig vorliegenden konstruktiven Merkmalen und ist damit selbst eine Zufallsgröße. Da keine durch Versuche ermittelten Daten vorliegen, musste die Verteilung dieser Zufallsgröße und deren Parameter durch Expertenurteil abgeschätzt werden. In die Schätzung ist das im Ereignis beobachtete tatsächliche Verhalten des Ventils eingeflossen. Aufgrund mangelnder Informationen wird angenommen, dass diese Zeit gleichverteilt ist mit einem Minimum von 13 min und einem Maximum von 26 min d. h., $T_{MAX} \sim U\ (13, 26)$.

- T_A ist die Zeit, die benötigt wird, um nach erfolgreicher Lösung des Problems die Korrekturmaßnahme durchzuführen. Da diese Zeit durch verschiedene zufällige Einflüsse mehr oder weniger stark variieren kann, geht diese Ausführungszeit ebenfalls als eine Zufallsgröße in das Modell ein. So kann die zeitliche Variation z. B. aufgrund der Verfügbarkeit des die Maßnahme ausführenden Elektrikers und dessen Arbeitsverhaltens beeinflusst werden. Mangels experimenteller Daten wird die Verteilung dieser Zeit ebenfalls durch Expertenurteil abgeschätzt. In die Schätzung sind die im Ereignis tatsächlich benötigte Zeit und Erfahrungen aus der Begehung der Handlungsorte in dieser Anlage eingeflossen. Für die Simulation wird angenommen, dass T_A gleichverteilt ist mit einem Minimalwert von 5 min und einem Maximalwert von 15 min d. h., $T_A \sim U\ (5, 15)$

- T_P ist die für die Erarbeitung der Problemlösung maximal zur Verfügung stehende Zeit. Sie ergibt sich aus der Differenz von T_{MAX} und T_A. Durch die Informationen, die aus der Beschreibung des Ereignisses vorliegen, konnten die beobachteten Zeiten als Referenzwerte für die Größen T_{MAX} und T_A verwendet werden. Damit ist die Situation gegeben, dass die maximal zur Verfügung stehende Zeit, in der die Problemlösung erarbeitet werden kann, berechnet werden kann. Mit der Kenntnis der für die Problemlösung maximal zur Verfügung stehenden Zeit ist die Voraussetzung dafür gegeben, dass die Fehlerwahrscheinlichkeit der Problemlösung über die in Tab. 4.2 angegebene Funktion ermittelt werden kann. Diese Funktion berechnet die Fehlerwahrscheinlichkeit bzw. die Erfolgsaussicht der Problemlösung in Abhängigkeit der verfügbaren Zeit. Zu berücksichtigen ist dabei, dass die Erfolgsaussicht für eine rechtzeitige Problemlösung von der „Vorphase“, d. h. von der frühzeitigen Entdeckung des Bedienfehlers (OP1) abhängt und damit zwei Pfade abzubilden sind, für die unterschiedliche Wahrscheinlichkeiten für den Misserfolg bzw. Erfolg der Problemlösung ermittelt werden.

- Wenn T_P nicht im Vorfeld der Analyse ermittelt werden kann, ist die entsprechende Funktion in Tab. 4.2 zur Berechnung der Fehlerwahrscheinlichkeit nicht anwendbar.

- P_1 und P_2 stehen für die Wahrscheinlichkeit, dass die Problemlösung in der maximal dafür zur Verfügung stehenden Zeit nicht erfolgreich ist. Sie werden in Abhängigkeit von der Zufallsgröße OP1 und der Zeit T_P unter Verwendung des Quantifizierungsansatzes 1 ermittelt, der in Abschnitt 4.2.3 beschrieben wurde. Pfad A und Pfad B des Modells unterscheiden sich lediglich durch die unterschiedlichen Erfolgswahrscheinlichkeiten der Problemlösung.

- Die aleatorischen Unsicherheiten bzgl. der Gebäudeabschlussarmatur (GBA) TE1 A53 und des Sicherheitsventils (SiV) TE1 A05 bestehen darin, dass sie bei Anforderung ihre Funktionen erfüllen oder nicht erfüllen. Die Wahrscheinlichkeiten, dass TE1 A53 auf Anforderung nicht schließt wird mit p_{GBA}=1.E-3 und TE1 A05 auf Anforderung nicht öffnet mit p_{SiV}=1.1E-3 abgeschätzt. Diese Schätzwerte wurden der deutschen Datenbasis für Zuverlässigkeitskenngrößen für Kernkraftwerkskomponenten entnommen.

Es ist anzumerken, dass aufgrund des Beispielcharakters des Modells und aus Gründen einer übersichtlicheren Darstellung die Simulation des Ereignisablaufs lediglich unter Berücksichtigung der aleatorischen Unsicherheiten durchgeführt wurde. Für die epistemischen Unsicherheiten, die in dem Modell bzgl. der Zuverlässigkeitskenngrößen

(Ausfallwahrscheinlichkeiten) der technischen Komponenten sowie bzgl. der Wahrscheinlichkeiten für OP1 sowie für P_1 und P_2 einer erfolgreichen Problemlösung in Abhängigkeit der zur Verfügung stehenden Zeit vorliegen, wurden die entsprechenden Referenzwerte eingesetzt.

Aus dem in Abb. 4.4 skizzierten Modellablauf ist ersichtlich, dass sich aufgrund der aleatorischen Unsicherheiten und zeitlichen Abhängigkeiten fünf verschiedene Endzustände für den Ereignisablauf ergeben können. Diese Endzustände können wie folgt beschrieben werden:

- **Endzustand 1:** „Kühlmittelverluststörfall mit Kühlmittelverlust in den Sicherheitsbehälter und Überdruckversagen des Entwässerungsbehälters“. Dieser Zustand tritt ein, wenn das Ventil TE1 A10 nicht geschlossen werden kann und die Gebäudeabschlussarmatur (GBA) auslegungsgemäß schließt. Das Primärkühlmittel strömt in diesem Fall weiter zum Entwässerungsbehälter. Das Schließen der GBA Armatur führt zu einem weiteren Druckanstieg im Behälter mit Überdruckversagen als Folge des weiteren Druckanstiegs. Das Überdruckversagen kann auch dann nicht verhindert werden, wenn das Sicherheitsventil TE1 A05 auslegungsgemäß öffnet.

- **Endzustand 2:** „Kühlmittelverluststörfall mit Kühlmittelverlust in den Sicherheitsbehälter, Überdruckversagen des Entwässerungsbehälters und Dampfleckage aus dem Sicherheitsbehälter“. Dieser Zustand tritt ein, wenn das Ventil TE1 A10 nicht geschlossen werden kann, das Sicherheitsventil TE1 A05 nicht öffnet (mit der unmittelbaren Folge „Überdruckversagen des Behälters“) und die GBA Armatur nicht schließt. In diesem Fall tritt ein Teil des Primärkühlmittels in Form von Dampf über die durch die GBA Armatur nicht abgesperrte Leitung aus dem Sicherheitsbehälter aus.

- **Endzustand 3:** „Kühlmittelverluststörfall mit Kühlmittelverlust aus dem Sicherheitsbehälter heraus“. Diese Situation ergibt sich, wenn das Ventil TE1 A10 nicht geschlossen werden kann, das Sicherheitsventil TE1 A05 auslegungsgemäß öffnet und die GBA Armatur TE1 A53 nicht schließt. In diesem Ablauf bleibt der Entwässerungsbehälter intakt und Primärkühlmittel strömt über das offene Ventil TE1 A10, den Behälter und die offene GBA Armatur aus dem Sicherheitsbehälter heraus.

- **Endzustand 4:** „Kein andauernder Kühlmittelverlust und Überdruckversagen des Entwässerungsbehälters“. Dieser Zustand ist im zugrunde gelegten Ereignis aus der Betriebserfahrung konkret eingetreten. Dort konnte das Ventil TE1 A10 nach einer

gewissen Zeit geschlossen werden. Der Behälter versagt, wenn entweder das Sicherheitsventil TE1 A05 nicht öffnet oder die GBA Armatur TE1 A53 auslegungsgemäß schließt. Im konkret beobachteten Ereignis wurde das Sicherheitsventil geöffnet und die GBA Armatur konnte auslegungsgemäß geschlossen werden.

- **Endzustand 5:** „Kein andauernder Kühlmittelverlust und kein Überdruckversagen des Entwässerungsbehälters“. Dieser Zustand wird erreicht, wenn das Ventil TE1 A10 rechtzeitig geschlossen wird, das Sicherheitsventil auslegungsgemäß öffnet und die GBA Armatur fälschlicherweise nicht schließt.

4.3.3.2 Analyseergebnisse zu Modell 1

Der im vorherigen Abschnitt 4.3.3.1 beschriebene Ereignisablauf kann über einen klassischen Ereignisbaum modelliert werden. Für die Analyse des Ereignisablaufs muss der erstellte Ereignisbaum jedoch mehrmals gerechnet werden, um die Unsicherheiten bzgl. der Zeiten T_{MAX} und T_A und damit auch die Unsicherheiten bzgl. des verfügbaren Zeitfensters berücksichtigen zu können. Die Unsicherheiten des verfügbaren Zeitfensters wirken sich wiederum auf die Zuverlässigkeit des Problemlösens aus. In den durchgeführten Simulationen wurde die Abhängigkeit der Zuverlässigkeit des Problemlösens von den ausgespielten Zeiten für T_{MAX} und T_A berücksichtigt, wobei die funktionale Beziehung in Abb. 4.2 bzw. Tab. 4.2 verwendet wurde.

Das Crew Modul in Verbindung mit MCDET ist so flexibel, dass mit diesem Werkzeug neben dynamischen Ereignisbäumen auch ein klassischer Ereignisbaum modelliert werden kann. Für die Analyse des Modells 1 wurde das Crew-Modul in Verbindung mit MCDET angewendet, da zur Berücksichtigung der Unsicherheiten die Abläufe des Ereignisbaums im Rahmen einer Simulation mehrmals gerechnet werden müssen. Da MCDET eine so genannte varianzreduzierende Methode darstellt, erwiest sich MCDET gegenüber einer reinen Monte-Carlo Simulation als vorteilhaft in dem Sinne, dass MCDET bei gleichem Stichprobenumfang genauere Ergebnisse liefert.

Mit MCDET wurden 100 Ereignisbäume erzeugt, wobei jeder Ereignisbaum die Abläufe enthält, die in Abb. 4.4 dargestellt sind. Für jeden der 100 erzeugten Ereignisbäume wurden jeweils Werte aus den Verteilungen der der Zeiten für T_{Max} und T_A zufällig ausgespielt. Aus den ausgespielten Zufallswerten wurde das verfügbare Zeitfenster $T_P = T_{MAX} – T_A$ und aus diesem die Zuverlässigkeit des Problemlösens über die entsprechenden funktionalen Beziehungen (s. Tab. 4.3 und Tab. 4.4) berechnet und für den entsprechen Ereignisablauf eingesetzt.

Im Rahmen der 100 erzeugten Ereignisbäume wurden insgesamt ca. 1200 Abläufe simuliert. Diese Anzahl ergibt sich aus der Tatsache, dass für jeden einzelnen Ereignisbaum mehrere Ablaufsequenzen gerechnet werden, die sich aus den Verzweigungen des Modells ergeben. Für jeden Ablauf wurden die dazugehörige Wahrscheinlichkeit sowie der Endzustand der Sequenz ermittelt. Die Ereignisbäume unterscheiden sich durch die zufällig ausgespielten Zeiten T_A und T_{MAX} der jeweiligen Bäume. Aus den Ergebnissen der 100 gerechneten Ereignisbäume wurden schließlich die Wahrscheinlichkeiten ermittelt, mit denen die jeweiligen Endzustände eintreten.

Die in Tab. 4.5 angegebenen Wahrscheinlichkeiten sind als Mittelwerte der Wahrscheinlichkeiten zu interpretieren. Da sich aufgrund der Abhängigkeiten zwischen den ausgespielten Zeiten und der Zuverlässigkeit des Problemlösens für jeden DET andere Wahrscheinlichkeiten der Endzustände ergeben, wurden die Wahrscheinlichkeiten der Endzustände über alle erzeugten Bäume gemittelt. Durch die Ergebniswerte der 100 berechneten Ereignisbäume können der Mittelwert sowie die Standardabweichung der Wahrscheinlichkeiten der einzelnen Zustände berechnet werden. Unter Verwendung des Mittelwertes und der Standardabweichung wurden das 95 %-Konfidenzintervall für die mittleren Wahrscheinlichkeiten der jeweiligen Zustände über eine Students-t-Verteilung berechnet. Die Mittelwerte der Wahrscheinlichkeiten, Standardabweichungen und ihre zugehörigen 95 %-Konfidenzintervalle sind für die fünf Endzustände in Tab. 4.5 angegeben.

Tab. 4.5 Mittelwert, Standardabweichung und 95 %-Konfidenzintervall der Wahrscheinlichkeit für die Endzustände des Ereignisablaufs von Modell 1

Zustand 1: KMV Störfall mit Kühlmittelverlust in den SB ; Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95% - KI**
0.49	0.31	(0.43 , 0.55)
Zustand 2: KMV Störfall mit Kühlmittelverlust in den SB sowie Dampfleckage aus dem SB; Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95%-KI**
5.39E-07	3.38E-07	(4.7E-07 , 6.1E-07)
Zustand 3: KMV Störfall mit Kühlmittelverlust aus dem SB; Kein Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95%-KI**
4.89E-04	3.07E-04	(4.3E-04 , 5.5E-04)
Zustand 4: KMV wurde gestoppt; Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95%-KI**
0.509	0.307	(0.45 , 0.57)
Zustand 5: KMV wurde gestoppt; Kein Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95%-KI**
5.09E-04	3.07E-04	(4.5E-04 , 5.7E-04)

Der beobachtete Endzustand, der sich im beobachteten Ereignis aus der Betriebserfahrung ergeben hat, war der Endzustand 4. In dem beobachteten Fall konnte der LOCA aufgrund wissensbasierten Handelns unterbunden werden, wobei der Tank jedoch geborsten ist. Für diesen Endzustand wurde in der Analyse eine mittlere Wahrscheinlichkeit von ca. 0.51 ermittelt. Nahezu gleich hoch ist allerdings auch die Wahrscheinlichkeit, dass die Fehlbedienung einen Kühlmittelverluststörfall in den Sicherheitsbehälter (Endzustand 1) zur Folge hat. Für den Endzustand 1 wurde eine mittlere Wahrscheinlichkeit von 0.49 ermittelt. Aufgrund der Analyse ist der Eintritt einer dieser beiden Endzustände 1 bzw. 4 mit einer Wahrscheinlichkeit von mehr als 99% zu erwarten. Die Standardabweichungen von Zustand 1 und Zustand 4 sind annähernd gleich, was auf die gleiche

Unsicherheit der Zustandswahrscheinlichkeiten bzgl. der 100 Ereignisbäume schließen lässt.

Sicherheitstechnisch besonders bedeutsam ist Endzustand 3, da hier das für eine primärseitige Langzeitnotnachkühlung benötigte Kühlmittel aus dem Sicherheitsbehälter verloren geht. Hierfür wurde eine eher geringe Eintrittswahrscheinlichkeit von 4.9E-04 ermittelt. Etwa gleich gering ist die Wahrscheinlichkeit, dass der Ereignisablauf ohne ernstere Folgen (d. h. kein andauernder Kühlmittelverlust und keine Zerstörung des Entwässerungsbehälters, Endzustand 5) beendet werden kann. Ein Szenario bei dem es zu einer andauernden Dampfleckage aus dem Sicherheitsbehälter kommt, hat mit einem Wert von 5.4E-07 die geringste Eintrittswahrscheinlichkeit.

Neben den in Tab. 4.5 dargestellten Ergebnissen, wurden weitere Auswertungen der Simulationsergebnisse für das Modell 1 durchgeführt. Diese Auswertungen haben ergeben, dass mit einer Wahrscheinlichkeit von 12 % der Problemlöseprozess aufgrund zeitlicher Einflüsse nicht erfolgreich durchgeführt werden konnte. In 4 % der Simulationsläufe wurde eine Handlungszeit $T_A > T_{MAX}$ ausgespielt. D. h. die benötigte Zeit t der durchgeführten Maßnahme übersteigt die maximale Zeit, in der das Ventil noch manuell geschlossen werden kann. In 8 % der Simulationen beträgt die Zeit, die zur Problemlösung zur Verfügung steht, weniger als 2 min. Gemäß der Funktion in Abb. 4.2 bzw. Tab. 4.2 beträgt die Wahrscheinlichkeit 1, dass das Problem in der Kürze der zur Verfügung stehenden Zeit von < 2 min nicht gelöst werden kann. Die Wahrscheinlichkeit, dass der Problemlöseprozess aufgrund zeitlicher Einflüsse erfolgreich bzw. nicht erfolgreich durchgeführt werden kann, darf nicht verwechselt werden mit den in Tab. 4.5 angegebenen Wahrscheinlichkeiten ob der LOCA erfolgreich gestoppt werden konnte. Für das erfolgreiche Beenden des LOCA Ereignisses gehen sowohl die erfolgreiche Durchführung der wissensbasierten Handlung als auch die Zuverlässigkeit des Sicherheitsventils TE1 A05 und der Gebäudeabschlussarmatur TE1 A53 ein.

Um den Zugewinn an Sicherheit durch das Problemlösen einschätzen zu können, wäre ein Vergleich mit Ergebnissen notwendig, bei denen die wissensbasierte Handlung nicht durchgeführt, sondern die Anlage abgefahren wird. Hierbei würde die Zeiten eine wesentliche Rolle spielen, wie lange das Abfahren der Anlage dauert und wie lange man für das erfolgreiche beenden des LOCA durch die wissensbasierte Handlung benötigt. Diese Zeiten sind maßgeblich, um den jeweiligen Betrag des Kühlmittelverlustes im Rahmen von deterministischen Rechnungen ermitteln zu können.

4.3.3.3 Ablaufbeschreibung der Simulation mit dem Crew-Modul und MCDET

Der Ablauf der Simulation kann durch folgende Schritte beschrieben werden:

- **Schritt 1:** Der Nutzer legt zu Beginn die Zahl der zu erzeugenden Ereignisbäume (EB) fest.
- **Schritt 2:** Für jeden EB wird im zweiten Schritt T_{MAX} und T_A zufällig aus den dafür festgelegten Verteilungen gezogen. Daraus wir T_P berechnet und über die entsprechende Funktion in Tab. 4.2 die Wahrscheinlichkeit bestimmt, dass die Problemlösung nicht erfolgreich ist.
- **Schritt 3:** Das Crew-Modul erkennt, an welchem Verzweigungspunkt sich der Ablauf befindet, z. B. ob das Fehlöffnen des Ventils vor oder nach RESA erkannt wird.
- **Schritt 4:** Wenn ein Verzweigungspunkt erreicht wird, kommuniziert das Crew-Modul an MCDET, um welchen Verzweigungspunkt es sich handelt.
- **Schritt 5:** MCDET kontrolliert, welche Alternativen des Verzweigungspunkts noch nicht abgearbeitet sind und legt eine noch nicht abgearbeitete Alternative des für den weiteren Ablauf fest.
- **Schritt 6:** Das Crew-Modul erhält von MCDET die Information über die ausgewählte Alternative und die dazugehörige Eintrittswahrscheinlichkeit. (In diesem Anwendungsbeispiel wurden die epistemischen Unsicherheiten zu den Wahrscheinlichkeiten der Verzweigungsalternativen nicht berücksichtigt.)
- **Schritt 7:** Die Schritte 2 – 6 werden wiederholt durchlaufen, bis alle Pfade des betreffenden Ereignisbaumes abgearbeitet sind.
- **Schritt 8:** Danach wird der nächste Ereignisbaum erzeugt.

Der Vorteil der Simulation über das MCDET-Verfahren besteht gegenüber der reinen Monte-Carlo Simulation in der Vermeidung der Problematik, dass z. B. bei Verzweigungsalternativen mit sehr kleiner Eintrittswahrscheinlichkeit die Stichprobe entsprechend groß gewählt werden muss, damit solche Ereignisse in der Analyse enthalten sind und ausgewertet werden können.

4.3.4 Modell 2: Dynamisches Modell zur Analyse des Precursor-LOCA Ereignisses unter Berücksichtigung der entwickelten Methode zum wissensbasierten Handeln

Der in Abb. 4.4 dargestellte Ereignisablauf wurde im Modell 1 unter Verwendung von MCDET simuliert und analysiert. Die Analyse unterschied sich von der klassischen Ereignisbaumanalyse dadurch, dass für die Zeiten T_{MAX} (Maximale Zeit in der das Ventil noch geschlossen werden kann) und T_A (Ausführungszeit des Personals) die entsprechenden Unsicherheiten berücksichtigt wurden. Aus diesen beiden Zeitangaben konnte im Rahmen der Simulation jeweils das Zeitfenster ermittelt werden, das zur Problemlösung in dem jeweiligen Simulationslauf zur Verfügung stand. Mit dem ermittelten Wert des zur Verfügung stehenden Zeitfensters wurde über die Funktion in Tab. 4.2 die Wahrscheinlichkeit ermittelt, dass das Problem erfolgreich gelöst bzw. nicht gelöst werden kann.

Obwohl in diesem konkreten Anwendungsfall Informationen zur Verfügung standen, die eine Abschätzung von T_{MAX} und T_A ermöglichten und damit das zur Verfügung stehende Zeitfenster zur Problemlösung ermittelt werden konnte, ist in mehr oder minder vielen Fällen die Situation gegeben, dass die für eine Problemlösung zur Verfügung stehende Zeit im Vorfeld der Analyse nicht bekannt ist oder – wenn überhaupt - nur mit eheblichen Aufwand ermittelt werden könnte. Die Ermittlung des zur Verfügung stehenden Zeitfensters ist im Vorfeld insbesondere dann schwierig, wenn der Prozess durch vielfältige stochastische Einflüsse und Wechselwirkungen gekennzeichnet ist. Diese Einflusskette ist in Abb. 4.5 veranschaulicht.

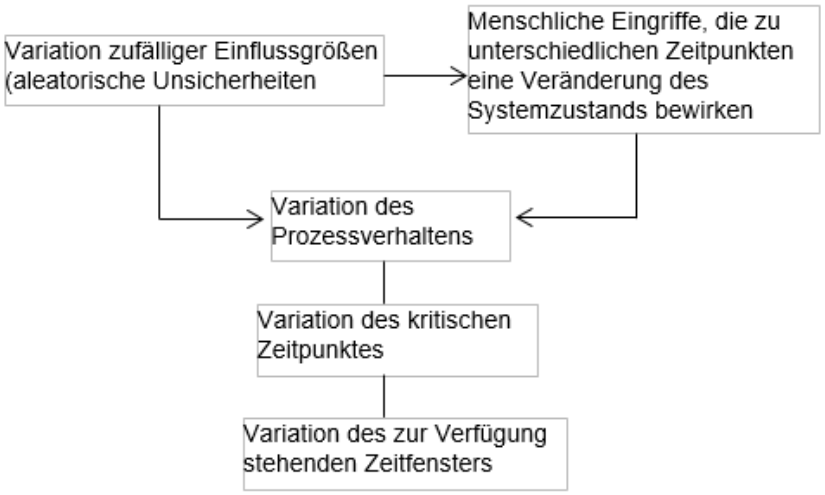


Abb. 4.5 Einflüsse auf das Zeitfenster, das zur Problemlösung zur Verfügung steht

Durch die Variation der zufälligen Einflüsse, variiert auch der jeweilige Prozessablauf. Durch die Variation des Prozessablaufs kann ein kritischer Zeitpunkt früher oder später erreicht werden. Da mit dem Erreichen des kritischen Zustands das zur Verfügung stehende Zeitfenster für die Problemlösung und deren Ausführung festgelegt wird, folgt, dass zur Ermittlung des Zeitfensters der entsprechende Prozessablauf bekannt sein muss. Es ist davon auszugehen, dass diese Situation bei auftretenden Problemen in einer Anlage, bei denen wissensbasiertes Handeln erforderlich ist, nicht immer gegeben ist, insbesondere wenn der zugrundeliegende Prozess komplexen Wechselwirkungen unterworfen ist. Wenn der Prozess nicht durch komplexe Wechselwirkungen charakterisiert ist, könnte eine grobe Abschätzung der Unsicherheiten des kritischen Zeitpunktes T_{MAX} (wie z. B. in Abschnitt 4.3.3) erfolgen.

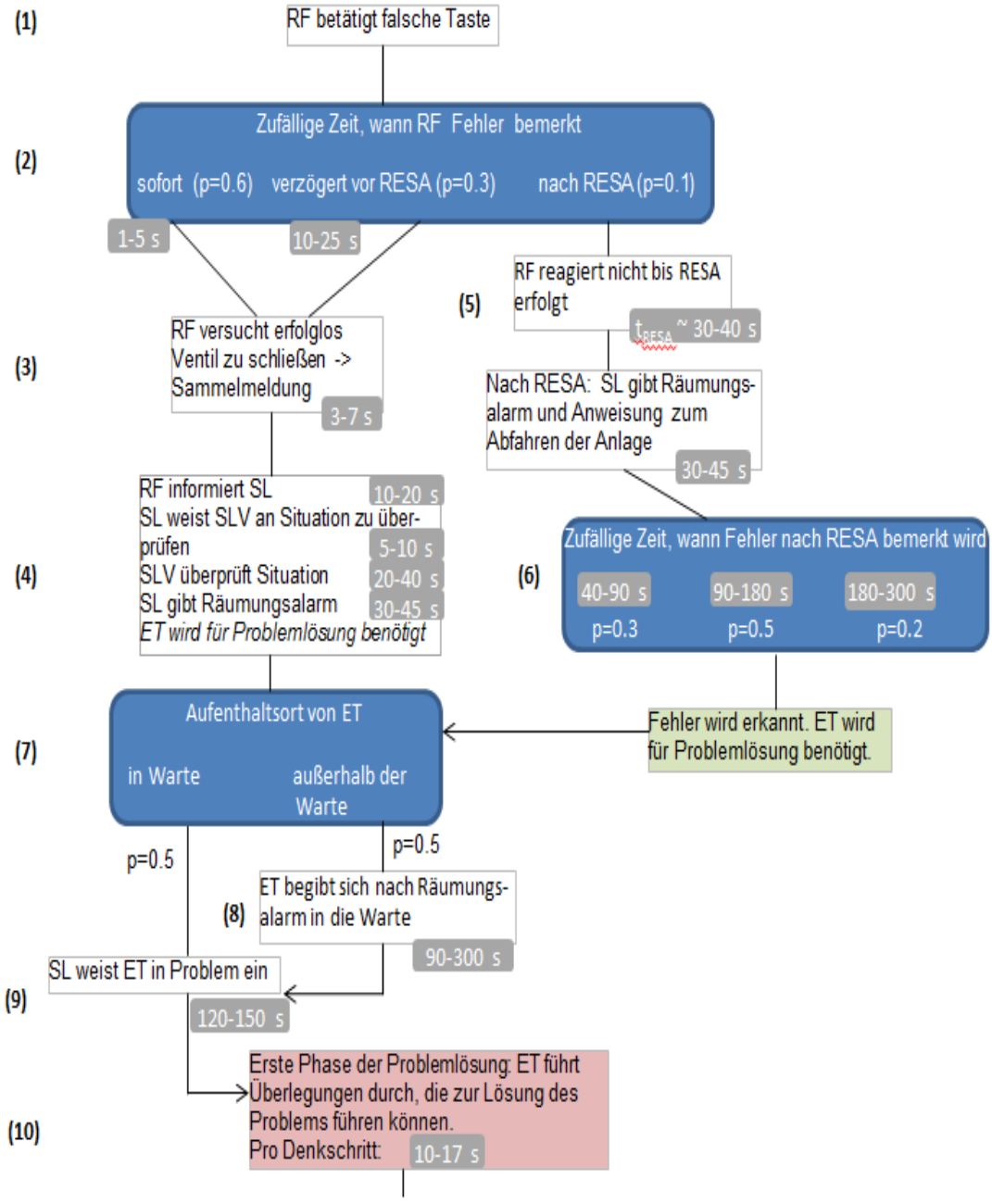
Die Kenntnis des zur Problemlösung zur Verfügung stehenden kritischen Zeitfensters ist notwendige Voraussetzung zur Anwendung des Modellansatzes 1. Um diese notwendige Voraussetzung des Bewertungsansatzes 1 zu vermeiden, wurde im Rahmen des Projekts eine Methodik entwickelt, bei der die Bestimmung des zur Verfügung stehenden Zeitfensters keine Bedingung für die Analyse darstellt. Diese Methodik basiert auf einer dynamischen Analyse des Handlungsablaufs unter Verwendung des Crew-Moduls (s. Abschnitt 2.2) in Verbindung mit MCDET. Unter Verwendung des Crew-Moduls wird die aleatorische Unsicherheit der Ausführungszeit T_A, die im Modell 1 durch eine Verteilung grob abgeschätzt wurde, durch eine Zerlegung der Handlungsmaßnahme und des Problemlösungsprozesses in einfachere Handlungsschritte ermittelt (vgl. Abb. 4.6). Der Vorteil des dynamischen Ansatzes ist, dass zeitliche Wechselwirkungen von Handlungen in Abhängigkeit von Systemzuständen und zufälligen Einflussgrößen explizit modelliert und in der Analyse berücksichtigt werden können.

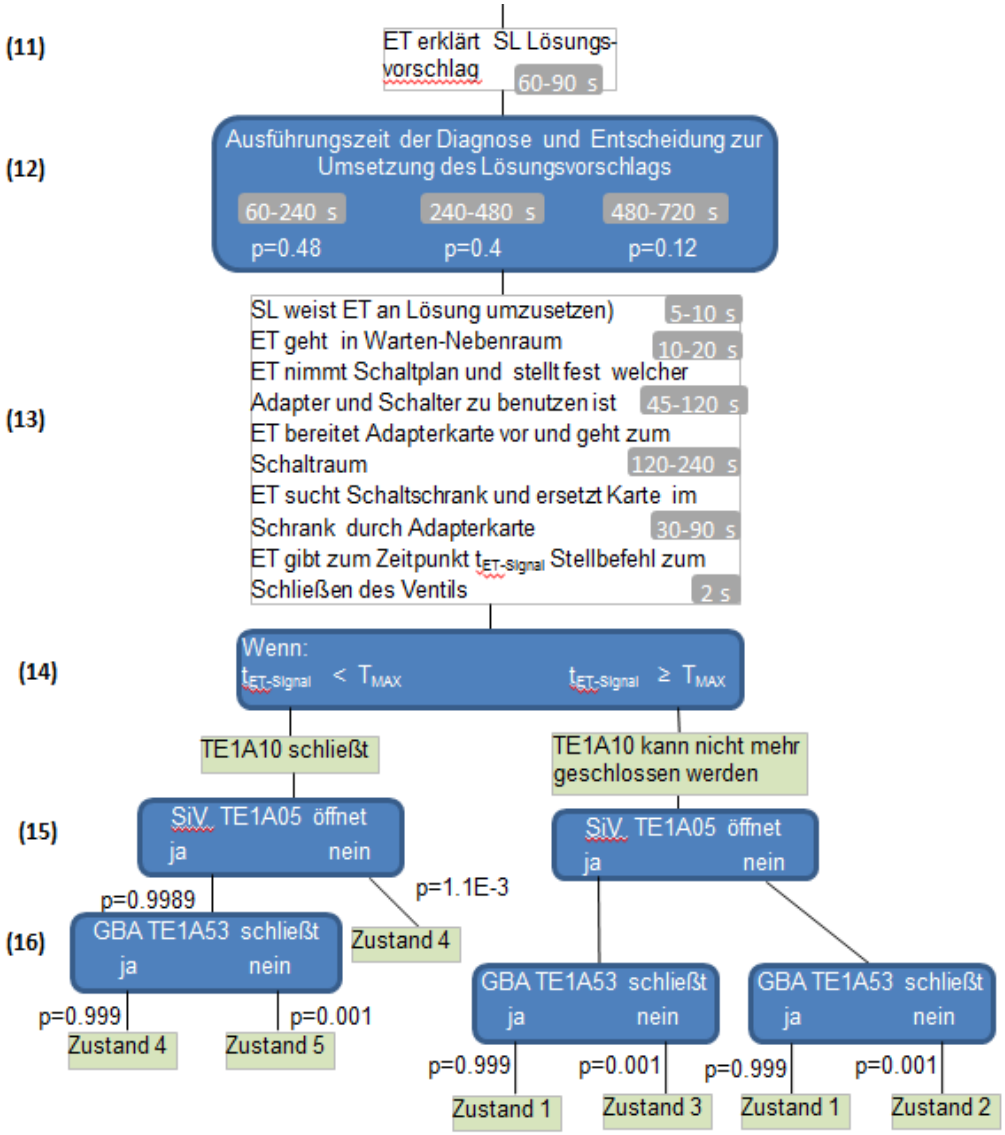
Der dynamische Ansatz wird im Modell 2 für das Fallbeispiel des LOCA-Precursor Ereignisses angewendet. Im Abschnitt 4.3.4.1 erfolgt zunächst eine Beschreibung des Handlungsablaufs, wie er im Crew-Modul modelliert wird. In Abschnitt 4.3.4.2 werden die Ergebnisse der dynamischen Analyse für das Fallbeispiel präsentiert. Der Ablauf der Simulation unter Verwendung des Crew-Moduls und MCDET erfolgt in Abschnitt 4.3.4.3.

4.3.4.1 Beschreibung des dynamischen Modells des Handlungsablaufs

Im Folgenden wird der Handlungsablauf mit dem darin stattfindenden Problemlöseprozess für das Anwendungsbeispiel beschrieben, wie es im Crew-Modul in Verbindung mit MCDET modelliert und simuliert wird. Dabei werden verschiedene Abhängigkeiten des

Handlungsablaufs von zufälligen und zeitlichen Einflüssen berücksichtigt. Der im Crew-Modul modellierte Handlungsablauf ist im Diagramm in Abb. 4.6 skizziert, wobei die einzelnen Punkte des Handlungsablaufs im nachfolgenden genauer erläutert werden.





Zustand 1 -> KMV-Störfall mit Kühlmittelverlust in den SB ; Entwässerungsbehälter (EB) versagt
Zustand 2 -> KMV-Störfall mit Kühlmittelverlust in den SB ; EB versagt ; Dampfleckage aus dem SB
Zustand 3 -> KMV-Störfall mit Kühlmittelverlust aus dem SB ; EB versagt nicht
Zustand 4 -> KMV gestoppt ; EB versagt
Zustand 5 -> KMV gestoppt ; EB versagt nicht

Abb. 4.6 Dynamisches Modell des Handlungsablaufs

Die Zustände in Abb. 4.6 sind mit den Endzuständen in Abb. 4.4 identisch.

Im Modell des Handlungsablaufs sind vier Personen beteiligt

- Schichtleiter (SL)
- SL-Vertreter (SLV)
- Reaktorfahrer (RF)
- E- und Leittechniker (ET)

(1): Der Handlungsablauf beginnt damit, dass der RF eine falsche Taste betätigt und damit das Ventil TE1 A10 fälschlicherweise geöffnet wird.

(2): Der Zeitpunkt, wann RF seinen Fehler realisiert, wird als Zufallsgröße betrachtet. Dabei wird davon ausgegangen, dass er mit Wahrscheinlichkeit 0.6 den Fehler sofort (innerhalb 1 – 5 s), mit Wahrscheinlichkeit 0.3 zeitverzögert aber noch vor RESA (innerhalb 10 – 25 s) und mit Wahrscheinlichkeit 0.1 erst nach RESA realisiert.

(3): Realisiert der RF seinen Fehler vor der RESA-Auslösung (entweder sofort oder etwas zeitverzögert), versucht er, den Knopf zum Schließen des Ventils zu betätigen. Aufgrund des hohen Drucks bleibt das Schließen des Ventils erfolglos und es erscheint die Sammelmeldung „Stellglied gestört oder Schalterfall HA 1-10“. In diesem Moment ist dem RF bewusst, dass der Korrekturversuch misslungen ist.

(4): Er informiert den SL, der den SLV anweist, die Situation zu überprüfen. Durch den Druckabfall im Primärkreis wird nach einer gewissen Zeit RESA ausgelöst. Daraufhin gibt der SL Räumungsalarm und weist das Abfahren der Anlage an. Parallel dazu begibt sich der SLV zum Pult des RF und überprüft die Situation. Es wird davon ausgegangen, dass zu diesem Zeitpunkt klar ist, dass der ET am besten zur Problemlösung beitragen kann.

(5): Falls der RF seinen Fehler nicht vor der RESA erkennt, wird vom Personal zunächst kein Zusammenhang zwischen der RESA-Auslösung und dem fehlerhaft geöffneten Ventil hergestellt. Das Personal reagiert, wenn RESA ausgelöst wird, wissen jedoch noch nicht den Grund der Auslösung. SL gibt Räumungsalarm und Anweisung zum Abfahren der Anlage.

(6): Es wird angenommen, dass aufgrund der durch RESA ausgelösten Signale und Anzeigen das Personal früher oder später erkennen wird, dass die RESA mit dem fehlerhaft geöffneten Ventil zusammenhängt. Die Zeit, wann das Personal diesen Zusammenhang erkennt, wird als aleatorische Unsicherheit betrachtet, die durch eine Histogramm-Verteilung beschrieben wird. Dazu wird angenommen, dass das Personal den Zusammenhang mit einer Wahrscheinlichkeit von p = 0.3 innerhalb 45 – 90 s, mit p = 0.5 innerhalb 90 – 180 s und mit p = 0.2 innerhalb 180 – 300 s herstellt. Die Zeiten innerhalb der Intervalle werden als gleichverteilt betrachtet.

(7): Es wird angenommen, dass die Mitglieder der Schichtmannschaft die Problemsituation so einschätzen, dass sie den ET als Wissensträger identifizieren und ihn für die Problemlösung benötigen, da er aufgrund seiner Kenntnisse und täglichen Aufgaben mit dem Eingriff am besten vertraut ist. In dieser Situation besteht die aleatorische Unsicherheit darin, dass sich der ET entweder bereits in der Warte befindet und vom SL sofort in die Problemsituation eingewiesen werden kann oder sich zufällig außerhalb der Warte befindet. Im letzteren Fall begibt sich der ET in die Warte, da vom SL Räumungsalarm gegeben wurde. Um die Warte zu erreichen benötigt er je nach Aufenthaltsort mehr oder weniger Zeit. Die Wahrscheinlichkeit, dass sich ET außerhalb der Warte befindet, wird beispielhaft mit p = 0.5 angenommen. Um diesbezüglich eine genauere Abschätzung zu erhalten, müssten spezifische Informationen aus der Anlage herangezogen werden (z. B. Arbeitspläne oder protokollierte Arbeiten des ET in der Anlage).

(8): Für die Zeitdauer, die der ET benötigt, um von seinem Aufenthaltsort in die Warte zu gelangen, wird eine gleichverteilte Zufallszeit zwischen 90 und 300 s angenommen. Diese Werte könnten durch anlagenspezifische Informationen präzisiert werden, wie oft der ET während seiner Arbeitszeit außerhalb der Warte und an welchen Orten er beschäftigt ist.

(9): Nach Ankunft in der Warte wird der ET vom SL in die Problemsituation eingewiesen, wofür eine gleichverteilte Zufallszeit zwischen 120 und 150 s angenommen wird. Dabei wird davon ausgegangen, dass SL eine sorgfältige Beschreibung des Problems gibt, damit der ET möglichst gut in die Lage zu versetzt wird, über Lösungsmöglichkeiten nachzudenken.

(10): Nach der Einweisung in die Problemsituation beginnt der 1. Schritt der Lösungsfindung, in der zu erkennen ist, welches regelbasierte Vorgehen prinzipiell zur Lösung des Problems anwendbar ist. Es wird angenommen, dass in der Kommunikation nichts vom

Lösungsprozess antizipiert wird, so dass der ET das Problem von Grund auf durchdenken muss. Es wird unterstellt, dass ET die Situation sorgfältig überdenkt, um dem Ernst der Lage gerecht zu werden. Dabei werden folgende Denkschritte des ET angenommen:

- Klärung des Ist-Zustandes: ET rekapituliert für sich die Problemsituation. *„Es liegt ein Precursor vor …“*
- Zielsetzung: *„Das Ventil TE1 A10 muss geschlossen werden.“*
- Hindernis für die Zielerreichung: *„Von der Warte aus geht es nicht …“*
- Grund für das Bestehen des Hindernisses: *„…vorrangige Automatik blockiert das Schließen.“*
- Generisches Lösungsprinzip: *„Wir müssten eingreifen können, um die Automatik zu umgehen.“*
- Option eines konkreten Lösungsansatzes, der dem generischen Lösungsprinzip entspricht, aber nicht umsetzbar ist*: „Manuell ginge es vom Raum aus. Diesen Eingriff könnte die Automatik nicht blockieren. Aber aufgrund der widrigen Gegebenheiten kann den Raum jetzt keiner betreten. Diese Möglichkeit geht also nicht.“* Option muss verworfen werden.
- Präzisierung des generischen Lösungsprinzips mit Fokus auf ein Eingreifen in die Leittechnik*: „Wir müssten den Stellbefehl über die Leittechnik geben können, wir brauchen also einen Bypass zur Automatik.“*
- Konkrete Überlegung: *„Wo könnten wir wie eingreifen? Wie machen wird das in anderen Fällen.“*
- Option des Lösungsansatzes: *„Signalweg ginge über den Schaltschrank. Da können wir den Adapter setzen, bekommen den Bypass zur Automatik und können den Schließbefehl absetzen.“*

Die einzelnen Denkschritte sind im Modell des Crew Moduls einzeln berücksichtigt, wobei für jeden einzelnen Denkschritt, den der ET vollzieht, eine gleichverteilte Zufallszeit zwischen 10 und 17 s angenommen wird (vgl. Abschnitt 4.2.3).

(11): ET kommuniziert dem SL den Lösungsvorschlag und die zugehörigen Überlegungen. Für die Beschreibung der anstehenden Aufgabe mit ihren wesentlichen Schritten wird eine gleichverteilte Zufallszeit zwischen 60 und 90 s angenommen.

(12): Nachdem der ET dem SL die Lösung kommuniziert hat, setzt sofort die Diagnose ein, ob die Situation so geartet ist, wie sie sich dem ET darstellt, und ob eine Entscheidung für das Vorgehen zulässig ist. Es wird angenommen, dass die Kommunikationen fehlerfrei verlaufen, weil die Beteiligten SL und ET ihnen die volle Aufmerksamkeit zuwenden und sich so klar wie möglich ausdrücken. Des Weiteren gibt es im Denkprozess des vorliegenden Anwendungsfalls keine Ansatzpunkte für kognitive Fehler oder sonstige Fehler (z. B. das Ablesen eines Instruments, wenn ein Denkschritt dies erfordert). Da der gefundene Lösungsweg überschaubar ist und keine komplexeren Wechselwirkungsprozesse zu berücksichtigen sind, wird angenommen, dass die Diagnose des Lösungsweges nicht weniger als 1 Minute, aber auch nicht länger als 10 min in Anspruch nehmen wird. Unter dieser Bedingung wird auf Basis der Daten in /WES 87/ die in Tab. 4.6 dargestellte Histogramm-Verteilung für die Ausführungszeit der Diagnose des gefundenen potentiellen Lösungsweges angenommen:

Tab. 4.6 Histogramm-Verteilung der Diagnosezeit für den gefundenen Lösungsweg

Zeit t_{Diag} für Diagnose u. Entscheidung zur Umsetzung (Min)	**Wahrscheinlichkeit**	**5 %-Quantil**	**95 %-Quantil**
t_{Diag} ~ U (1 , 4) min	0.48	0.23	0.64
t_{Diag} ~ U (4 , 8) min	0.40	0.17	0.57
t_{Diag} ~ U (8 , 10) min	0.12	0.07	0.40

t_{Diag} ~ U (1 , 4) Minuten bedeutet, dass die Diagnosezeit t_{Diag} zufällig aus einer Gleichverteilung zwischen 1 und 4 min ausgewählt wird. Dies erfolgt mit einer Wahrscheinlichkeit von 0.48. Analog sind die anderen Zeiten zu interpretieren.

(13): Ist die Diagnose durchgeführt und die Entscheidung zur Umsetzung getroffen, weist der SL den ET an, den Lösungsvorschlag umzusetzen. Da SL und ET im Rahmen der Diagnose eng miteinander kommunizieren, ist davon auszugehen, dass die Anweisung des SL relativ kurz ausfällt (t ~ 4 – 10 s). Der ET begibt sich zum Wartennebenraum (t~10-20 s) und besorgt sich den entsprechenden Schaltplan, mit dem er bestimmt, welche Brücke auf der Adapterkarte zu ziehen ist, um das Signal vom Tremorendschalter zu trennen und welcher Schalter zur Signalgebung zu kippen ist (t ~ 45 – 120 s). Daraufhin bereitet ET die entsprechende Adapterkarte vor und geht zum Schaltraum (t ~ 120 – 240 s). Dort sucht er den zutreffenden Schaltschrank auf und wechselt die betreffende Karte mit der Adapterkarte aus (t ~ 25 – 50 s). Anschließend gibt er über

diese Adapterkarte das Signal zum Schließen des Ventils TE1 A10. Der Zeitpunkt, in dem ET das Signal gibt, sei mit $t_{ET\text{-}Signal}$ bezeichnet.

(14): Wie in Abschnitt 4.3.3.1 ausgeführt wurde, definiert T_{MAX} die maximale Zeit, in der das Ventil TE1 A10 nach dem fehlerhaften Öffnen aufgrund des hohen Drucks und der thermischen Belastungen noch geschlossen werden kann. T_{MAX} wurde für den Anwendungsfall als gleichverteilte Zufallszeit zwischen 13 und 26 min angenommen, d. h. T_{MAX} ~ U (13,26) Minuten. Der Motor ist in der Lage das Ventil zu schließen, wenn das Signal vor dem Zeitpunkt T_{MAX} gegeben wird, d. h. $t_{ET\text{-}Signal} < T_{MAX.}$ Erfolgt der Stellbefehl nach T_{MAX}, d.h. $t_{ET\text{-}Signal} \geq T_{MAX}$, kann das Ventil nicht mehr geschlossen werden. Dabei wird angenommen, dass bei längerer Beanspruchung durch die Strömungskräfte und aufgrund der zunehmenden temperaturbedingten mechanischen Verformung der Schließwiderstand soweit zunimmt, dass das Ventil auch durch die Schließkraftreserve des Antriebsmotors nicht mehr geschlossen werden kann. D. h., wenn der Stellbefehl nach T_{MAX} erfolgt, ist es nicht mehr möglich, den Kühlmittelverlust durch die wissensbasierte Handlung zu stoppen.

(15) und **(16):** Wie im Modell 1 (vgl. Abschnitt 4.3.3.1) beschrieben, bestehen die aleatorischen Unsicherheiten bzgl. der Gebäudeabschlussarmatur (GBA) TE1A53 und des Sicherheitsventils (SiV) TE1A05 darin, dass sie bei Anforderung ihre Funktionen erfüllen oder nicht erfüllen. Die Wahrscheinlichkeit, dass TE1A53 auf Anforderung nicht schließt wird mit p_{GBA}=1.E-03 und dass Sicherheitsventil TE1A05 auf Anforderung nicht öffnet mit p_{SiV}=1.1E-03 abgeschätzt. Diese Schätzwerte wurden der deutschen Datenbasis für Zuverlässigkeitskenngrößen für Kernkraftwerkskomponenten entnommen. In Abhängigkeit der Verfügbarkeiten von TE1A53 und TE1A05 ergeben sich die Endzustände des Ereignisablaufs, wie sie in Abschnitt 4.3.3.1 bzgl. Modell 1 beschrieben wurden.

Der Handlungsablauf wurde wie oben beschrieben im Crew-Modul modelliert. Die Ausführungszeiten der Basishandlungen wurden über SUSA ausgespielt und im Rahmen der Simulation automatisch in das Crew-Modul eingelesen sowie den entsprechenden Basishandlungen zugeordnet. Die Wahrscheinlichkeiten der aleatorischen Unsicherheiten bzgl. der Verfügbarkeit der Komponenten, Aufenthaltsort des ET, Zeiten für Erkennung des Fehlers in Abhängigkeit der RESA Auslösung sowie für die Diagnose und Entscheidungsfindung des Lösungsvorschlags werden innerhalb von MCDET festgelegt. Die Simulation des modellierten Handlungsablaufs erfolgt mit dem Crew-Modul in Verbindung mit MCDET.

4.3.4.2 Analyseergebnisse zu Modell 2

Zur Simulation des in Abb. 4.6 skizzierten Handlungsablaufs wurde das Crew-Modul in Verbindung mit MCDET eingesetzt. Dabei wurden 100 dynamische Ereignisbäume erzeugt. Die Anzahl der gerechneten Sequenzen in den jeweiligen dynamischen Ereignisbäumen variiert zwischen 115 und 120 Sequenzen. Damit wurden in der Analyse insgesamt ca. 11800 unterschiedliche Sequenzen gerechnet. Die hohe Anzahl an Sequenzen innerhalb eines dynamischen Ereignisbaumes ergibt sich durch die Verzweigungen bzgl. der aleatorischen Unsicherheiten, die im Modell des Handlungsablaufs berücksichtigt wurden.

Für jeden erzeugten dynamischen Ereignisbaum wurde die Wahrscheinlichkeit der jeweiligen fünf Zustände ermittelt. Aus den sich ergebenden 100 Wahrscheinlichkeiten der erzeugten dynamischen Ereignisbäume wurden der Mittelwert und die Standardabweichung der Wahrscheinlichkeiten der fünf Endzustände berechnet. Unter Verwendung des Mittelwertes und der Standardabweichung wurde das 95 %-Konfidenzintervall für den Mittelwert der Wahrscheinlichkeit der jeweiligen Zustände über eine Students-t-Verteilung berechnet. Diese Ergebnisse sind in Tab. 4.7 aufgeführt.

Tab. 4.7 Mittelwert, Standardabweichung und 95 %-Konfidenzintervall der Wahrscheinlichkeit für die Endzustände des Ereignisablaufs von Modell 2

Zustand 1: KMV Störfall mit Kühlmittelverlust in den SB ; Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95% - KI**
5.95E-01	3.29E-01	(5.30E-01 , 6.61E-01)
Zustand 2: KMV Störfall mit Kühlmittelverlust in den SB sowie Dampfleckage aus dem SB; Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95%-KI**
6.6E-07	3.6E-07	(5.8E-07 , 7.3E-07)
Zustand 3: KMV Störfall mit Kühlmittelverlust aus dem SB; Kein Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95%-KI**
5.9E-04	3.3E-04	(5.3E-04 , 6.6E-04)
Zustand 4: KMV wurde gestoppt; Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95%-KI**
4.04E-01	3.29E-01	(3.49E-01 , 4.58E-01)
Zustand 5: KMV wurde gestoppt; Kein Versagen des Entwässerungsbehälters		
Mean	**StdDev**	**95%-KI**
4.0E-04	3.3E-04	(3.4E-04 , 4.7E-04)

Aus Tab. 4.7 ist ersichtlich, dass im Modell 2 der Kühlmittelverlust, der durch die Fehlhandlung ausgelöst wurde, mit einer Wahrscheinlichkeit von ca. 0.4 aufgrund der wissensbasierten Maßnahme gestoppt werden konnte. Mit einer Wahrscheinlichkeit von ca. 0.6 konnte das Problem nicht erfolgreich durch wissensbasiertes Handeln gelöst werden.

Obwohl im Modell 2 eine größere Anzahl aleatorischer Unsicherheiten berücksichtigt wurde als im Modell 1, weisen die Standardabweichungen der berechneten Mittelwerte der Zustandswahrscheinlichkeiten kaum Unterschiede auf. Dies kann damit zusammen-

hängen, dass die relevanten Unsicherheitsquellen, die die Wahrscheinlichkeiten der Zustände maßgeblich bestimmen, zwischen beiden Modellen annähernd gleich sind. Ein weiterer Grund könnte darin bestehen, dass ein Wahrscheinlichkeitswert durch das Intervall [0,1] beschränkt ist und sich allein aus diesem Grund keine gravierenden Abweichungen in den Standardabweichungen ergeben können. Um den tatsächlichen Grund zu ermitteln, müssten weiterführende Untersuchungen erfolgen, die im Rahmen dieses Projekts allerdings nicht mehr durchgeführt werden können. Wegen der annähernd gleichen Standardabweichungen lassen sich die mittleren Zustandswahrscheinlichkeiten beider Modelle unmittelbar vergleichen.

Da die Handlungen im Modell 2 durch einen dynamischen Handlungsablauf detaillierter modelliert und simuliert wurden, können im Gegensatz zu der relativ groben Analyse im Modell 1 weiterführende Auswertungen durchgeführt werden, aus denen zusätzliche Informationen abgeleitet werden können.

Die Ausführungszeiten der Handlungen haben einen erheblichen Einfluss darauf, ob die Lösung eines bestehenden Problems rechtzeitig gefunden und umgesetzt werden kann und damit das wissensbasierte Handeln erfolgreich ist. Aus diesem Grund werden im Folgenden die Verteilungen der Zeitpunkte unter den Bedingungen einer erfolgreichen bzw. nicht erfolgreichen Handlungsausführung ermittelt. Die Verteilungen beziehen sich auf den Zeitpunkt, wann der Stellbefehl zum Schließen des Ventils nach erfolgtem Problemlösungsprozess gegeben wurde. Die bedingten Verteilungen der Zeiten sind in Abb. 4.7 dargestellt.

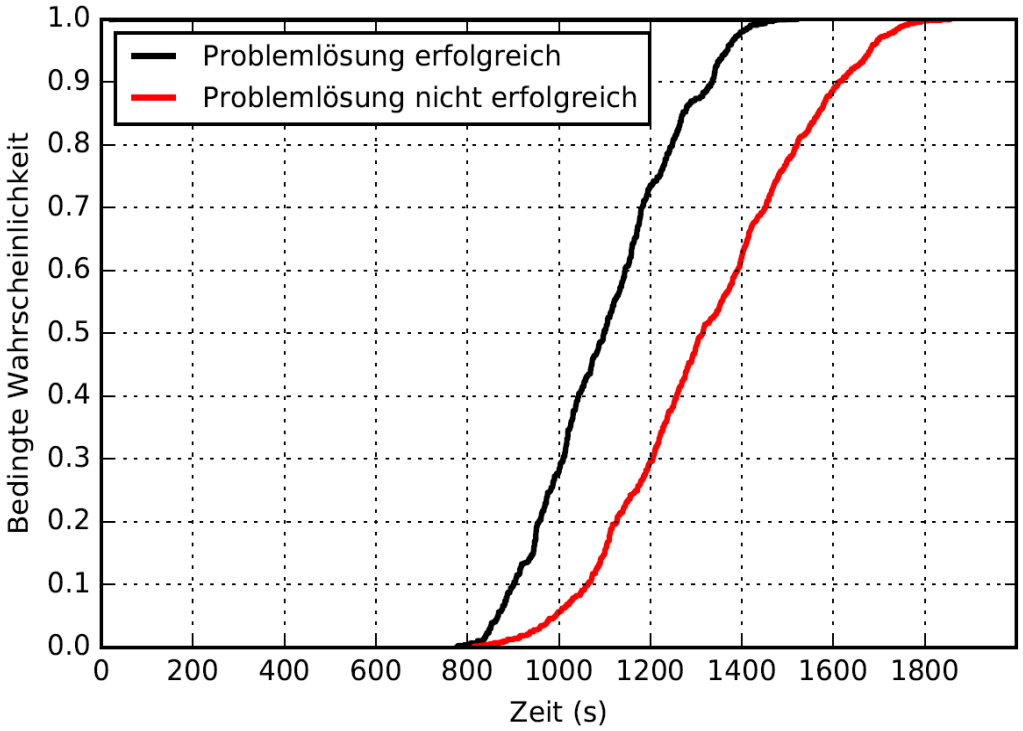


Abb. 4.7 Verteilung der Zeit, wann Stellbefehl zum Schließen des Ventils TE1 A10 unter der Bedingung eines erfolgreichen bzw. nicht erfolgreichen Versuchs der Beherrschung des Ereignisses gegeben wurde

Im Gegensatz zum Modell 1, bei der die Wahrscheinlichkeit einer erfolgreichen bzw. nicht erfolgreichen Problemlösung durch eine funktionale Beziehung in Abhängigkeit der zur Verfügung stehenden Zeit berechnet wurde (s. Abb. 4.2), wird im vorliegenden Modell 2 die nicht erfolgreiche Handlungsausführung allein durch die Zeit bestimmt, wann der Stellbefehl zum Schließen des Ventils TE1 A10 gegeben wird. Überschreitet diese Zeit den Zeitpunkt T_{MAX}, bis zu der das Ventil noch manuell geschlossen werden kann, so ist die wissensbasierte Maßnahme als nicht erfolgreich zu bewerten, auch wenn davon ausgegangen wird, dass das Problem erkannt und ein Konzept zur Lösung des Problems vorliegt. Der Grund liegt darin, dass zur erfolgreichen Problemlösung neben der Erkennung des zugrundeliegenden Problems und der Entwicklung eines Lösungskonzeptes auch die praktische Umsetzung des Lösungskonzepts gehört. Erst wenn das geeignete Lösungskonzept rechtzeitig durchgeführt werden kann, ist der Problemlöseprozess bzw. die wissensbasierte Handlung als erfolgreich zu bewerten.

Wie zu erwarten, zeigt Abb. 4.7, dass die Zeiten, wann der Stellbefehl zum Schließen des Ventils TE1 A10 gegeben wird, unter der Bedingung einer erfolgreichen Problemlösung kürzer sind als die Zeiten, die bei nicht erfolgreicher Problemlösung vorliegen. In

Tab. 4.8 sind die 5%-, 50%- und 95%-Quantile der bedingten Verteilungen der Zeiten angegeben, wie lange es dauert, bis der Stellbefehl zum Schließen des Ventils gegeben wird.

Tab. 4.8 Quantile der bedingten Zeitverteilungen, wann Stellbefehl gegeben wird

Problemlösung erfolgreich		
5%-Quantil	50%-Quantil	95%-Quantil
867 s	1099 s	1367 s
Problemlösung nicht erfolgreich		
5%-Quantil	50%-Quantil	95%-Quantil
992 s	1314 s	1680 s

Aus den Werten in Tab. 4.7 ist ersichtlich, dass bei erfolgreicher Problemlösung mit 90%iger Wahrscheinlichkeit die Problemerkennung, Lösungsfindung und Umsetzung des Lösungsweges zwischen ca. 14.5 und 23 min nach Fehlöffnen des Ventils TE1 A10 erfolgt. Bei nicht erfolgreicher Durchführung der wissensbasierten Maßnahme liegt der Zeitpunkt, wann der Stellbefehl zum Schließen des Ventils TE1 A10 gegeben wird, mit 90%iger Wahrscheinlichkeit zwischen 16.5 und 28 min nach Fehlöffnen des Ventils.

Die zunächst widersprüchlich erscheinende Situation, dass z. B. eine Ausführungszeit von 22 min zu einer erfolgreichen und 17 min zu einer nicht erfolgreichen Handlungsausführung führt liegt daran, dass die Ausführungszeit, wann der Stellbefehl zum Schließen des Ventils gegeben wird, mit dem Zeitpunkt T_{MAX} verglichen wird. Da T_{MAX} als Zufallsvariable definiert wurde, können kürzere Ausführungszeiten des Stellbefehls zufallsbedingt zu spät sein, wodurch die Handlungsausführung als nicht erfolgreich bewertet werden muss. Umgekehrt können längere Ausführungszeiten durchaus zum Erfolg der wissensbasierten Handlung führen und zwar dann, wenn T_{MAX} in dieser Simulation zufallsbedingt entsprechend groß ist. T_{MAX} wurde in der Analyse zufällig aus einer Gleichverteilung zwischen 780 und 1560 s ausgespielt.

Um zu demonstrieren, welche Auswertungsmöglichkeiten durch die Anwendung des Crew-Moduls mit MCDET gegeben sind, soll im Folgenden die Frage untersucht werden, um wieviel früher als zum erforderlichen Zeitpunkt T_{MAX} das Personal den Kühlmittelverlust stoppen konnte bzw. um wieviel Zeit das Personal die Maximalzeit überschritten hat.

Aus der Beantwortung dieser Frage kann z. B. eine probabilistische Abschätzung der Zeitmarge abgeleitet werden, wieviel Zeit dem Personal bei Ausführung des Stellbefehls noch zur Verfügung gestanden hätte, wenn sie das Problem bis dahin noch nicht gelöst hätten. Oder, um wieviel schneller das Personal hätte das Problem lösen müssen, um erfolgreich zu sein. Die bedingten Verteilungen der Zeitdifferenzen zu T_{MAX} sind in Abb. 4.8 dargestellt.

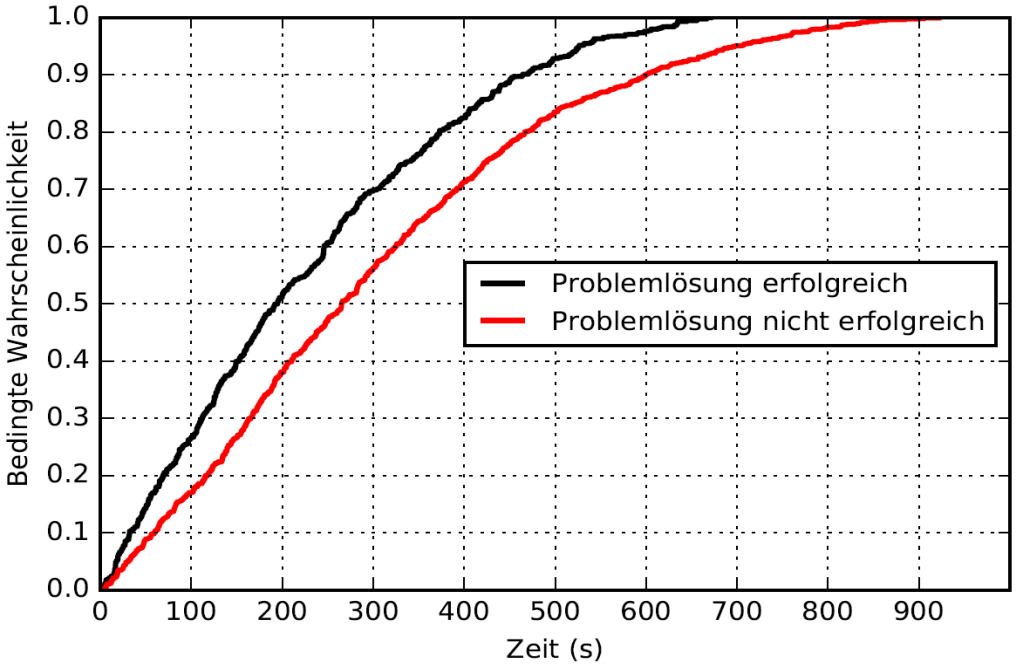


Abb. 4.8 Bedingte Verteilungen der Zeitmargen, die für erfolgreiche Problemlöseversuche zusätzlich zur Verfügung gestanden hätten bzw. zur Verfügung hätten stehen müssen

Unter der Bedingung, dass der Problemlösungsprozess erfolgreich durchgeführt wurde, konnte das Ventil mit einer Wahrscheinlichkeit ca. 32 % relativ knapp in weniger als 2 min vor Erreichen des kritischen Zeitpunkts T_{MAX} wieder geschlossen werden. Mit einer bedingten Wahrscheinlichkeit von ca. 47 % gelang dies innerhalb von 3 min. D. h., in diesen 32 % bzw. 47 % der Fälle hätten kleinere zeitliche Verzögerungen von 2 bzw. 3 min zu einem Misserfolg der wissensbasierten Handlung geführt. Damit wäre die Erfolgswahrscheinlichkeit von 0.404 auf ca. 0.27 bzw. 0.21 gesunken. D. h., die Erfolgswahrscheinlichkeit von ca. 40 % hätte aufgrund kleinerer zeitlicher Verzögerungen auch deutlich geringer ausfallen können. Aus der Verteilung kann ebenfalls abgeleitet werden, dass das Personal mit einer bedingten Wahrscheinlichkeit von ca. 30 % um 3 – 6 min und mit einer bedingten Wahrscheinlichkeit von ca. 22 % um 6 – 11 min früher als nötig mit dem bestehenden Problem fertig geworden ist.

Bei nicht erfolgreicher Durchführung der Problemlösung interessiert, um wieviel schneller das Personal das Problem hätte lösen müssen, um den Kühlmittelverlust zu stoppen. Unter der Bedingung, dass die Problemlösung nicht erfolgreich durchgeführt werden konnte, wird mit einer Wahrscheinlichkeit von 0.21 bzw. 0.34 der kritische Zeitpunkt T_{MAX} für eine erfolgreiche Problemlösung um weniger als 2 bzw. weniger als 3 min überschritten. Wäre der Problemlösungsprozess um 2 – 3 min schneller erfolgt, hätte dies eine Verminderung der Misserfolgswahrscheinlichkeit von 0.59 auf 0.47 bzw. 0.39 zur Folge. Mit einer bedingten Wahrscheinlichkeit von ca. 32 % hat das Personal zwischen 3 – 6 min und mit einer bedingten Wahrscheinlichkeit von ca. 35 % zwischen 6 und 15 min die Zeit überschritten, um den Kühlmittelverlust erfolgreich zu beenden.

Der Vergleich der beiden Modelle 1 und 2 sollte demonstrieren, dass durch die dynamische Modellierung des Handlungsablaufs unter Verwendung des Crew-Moduls in Verbindung mit MCDET eine detaillierte Analyse von Handlungsabläufen in Abhängigkeit von aleatorischen Unsicherheiten und Prozesszuständen durchgeführt werden kann, aus der umfassendere und detailliertere probabilistische Aussagen bzgl. der modellierten Handlung abgeleitet werden können.

4.3.4.3 Ablauf der Simulation

Der Ablauf der Simulation bzgl. Modell 2 unter Verwendung des Crew-Moduls und MCDET erfolgt analog zur Beschreibung des Ablaufs von Modell 1 (s. Abschnitt 4.3.3.3) mit der Erweiterung, dass die Zufallszeiten für die Basishandlungen über die erzeugte Stichprobe der dynamischen Ereignisbäume berücksichtigt und simuliert werden. Die Zufallszeiten der Basishandlungen wurden dabei mit Hilfe von SUSA generiert. Für jeden neu erzeugten dynamischen Ereignisbaum wird dann jeweils ein neuer Vektor von Zufallswerten für die Ausführungszeiten der Basishandlungen in das Crew-Modul automatisch eingelesen, wobei den jeweiligen Basishandlungen die entsprechen zufälligen Ausführungszeiten zugeordnet werden.

4.3.5 Vergleich und Diskussion der Ergebnisse bzgl. der Modelle 1 und 2

In Abschnitt 4.3.5.1 werden nochmals die wesentlichen Unterschiede der Modellierungsansätze von Modell 1 und Modell 2 erläutert. In Abschnitt 4.3.5.2 werden Analyseergebnisse beider Modelle diskutiert und qualitativ bewertet.

4.3.5.1 Unterschiede zwischen Modell 1 und Modell 2

Die beiden Modelle weisen Gemeinsamkeiten, aber auch Unterschiede auf. Aus den Unterschieden kann ein Kriterium für die Auswahl eines der beiden Modelle abgeleitet werden. Beide Modelle sehen vor, den Handlungsablauf in einzelne Schritte zu zerlegen. Die Zerlegung kann abhängig von der verfügbaren Information über den Handlungsablauf und von weiteren Entscheidungen des Anwenders unterschiedlich weit vorangetrieben und damit mehr oder minder detailliert sein. Der Anwender könnte z. B. das Erkenntnisziel einer möglichst genauen Klärung des Handlungsablaufs verfolgen und diesen in entsprechend kleine und viele Schritte analysieren. Anwender könnten aber auch durch die Ressourcen, die sie für die Analyse zur Verfügung haben, veranlasst sein, den Handlungsablauf nur in größere Schritte zu zerlegen. Die für den Anwendungsfall erstellten Modelle 1 und 2 geben gewissermaßen ein Beispiel für einen kleinen (Modell 1) und einen größeren Detaillierungsgrad (Modell 2) für die Schritte vor, in die der Handlungsablauf zerlegt werden kann.

In Bezug auf die „Ausführung einer gefundenen Lösung“ kann der Anwender den Detaillierungsgrad im Modell 1 maximal bis auf das Niveau vorantreiben, das durch die Bewertungsmethoden THERP bzw. ASEP in Bezug auf Kontrollen, Schalthandlungen, Kommunikationsvorgänge usw. gegeben ist. Die Wahl von THERP und ASEP ist dadurch begründet, dass diese Methoden zur Anwendung in den probabilistischen Sicherheitsanalysen deutscher Kernkraftwerke empfohlen sind. Der Anwender hat aber auch die Möglichkeit, die gesamte Ausführung als eine Einheit zu behandeln und als Ganzes in Bezug auf Ausführungszeit und Zuverlässigkeit zu bewerten.

Für beide Modelle sind mindestens die Schritte „Handeln in der Vorphase“, „Problemlöseversuch“ und „Ausführung einer gefundenen Lösung“ zu unterscheiden. Modell 2 sieht zudem die Aufgliederung des „Problemlöseversuchs“ in zwei Schritte vor, in denen die Problemlöser im Idealfall (1) das prinzipielle Vorgehen für die Lösung finden und (2) die Anwendbarkeit des Lösungsprinzips in der konkreten Situation prüfen (vgl. Abb. 4.1: „Finden der prinzipiellen Vorgehensweise“ und Diagnose zur Prüfung der Ausführbarkeit, Planung der Ausführung und Entscheidung für die Ausführung). In beiden Modellen werden im Problemlöseversuch weitere Aktivitäten unterschieden (insbes. die Analysen von Ziel, Situation, Konflikt und Material). Diese werden aber nicht als unterschiedliche Schritte modelliert, sondern gehen mit weiteren Informationen in eine Beurteilung der Qualität der Lösungsfindung ein.

Die beiden Modelle 1 und 2 unterscheiden sich in Bezug auf die Informationen, die dem Anwender vorliegen müssen, um die Modelle anwenden zu können:

- Für Modell 2 muss die Zerlegung des Handlungsablaufs in mehr oder weniger detaillierte Einzelhandlungen (Basishandlungen) vorliegen. Für jede Basishandlung müssen die stochastischen Verteilungen für die Ausführungszeit Handlung definiert werden. Abhängigkeiten des Handlungsablaufs von zufälligen Ereignissen können berücksichtigt werden. Dazu sind die Verzweigungswahrscheinlichkeiten der aleatorischen Größen zu definieren. Die Verarbeitung und Verknüpfung dieser Informationen erfolgt automatisch und liefert als Ergebnis eine Stichprobe von dynamischen Ereignisbäumen, deren Informationen statistisch ausgewertet werden können. Im Modell 2 erfolgt die Simulation des Handlungsablaufs gemäß dem realen Ablauf streng kausal. D. h., die zu einem Zeitpunkt vorliegenden Ergebnisse folgen ausschließlich aus den Resultaten des bisherigen Rechenlaufes und können auf die bisher erfolgten Handlungsschritte und den stochastischen Effekten der Ausführungszeit und der aleatorischen Größen zurückgeführt werden. Die notwendigen Informationen beschränken sich für den dynamischen Ansatz im Modell 2 im Wesentlichen auf eine möglichst realitätsnahe Beschreibung des Handlungsablaufs.

- Im Modell 1 sind in Verbindung mit dem Bewertungsansatz für den Problemlöseversuch entsprechend Abb. 4.2 und Tab. 4.2 Informationen erforderlich, die eigentlich erst am Ende des zu simulierenden Ereignisablaufs zur Verfügung stehen können. Das Problem ist, dass diese Informationen für den Swain‘schen Bewertungsansatz in Modell 1 jedoch vor Beginn der Analyse vorliegen müssen, damit diese durchgeführt werden kann. Der Anwender muss diese Informationen also aus Überlegungen gewinnen, die den Simulationen vorausgehen. Bei diesen Informationen handelt es sich im Wesentlichen um die Ausprägung der Zeitschwelle T_{MAX}, zu der das wissensbasierte Handeln soweit abgeschlossen sein muss, um wirksam zu sein und den Ereignisablauf beenden kann. Erst aus dieser Information kann nach dem beschriebenen Verfahren unter Nutzung der Ausführungszeit T_A die Länge des Zeitfensters bestimmt werden, das für den Problemlöseversuch zur Verfügung steht und aus dem die Zuverlässigkeit des Lösungsversuchs über eine funktionale Beziehung ermittelt wird.

  Modell 1 erfordert also eine Antizipation wichtiger Ergebnisse des Ereignisablaufs vor dem Beginn der Analyse. Diese Vorwegnahme ist umso schwieriger oder zumindest aufwendiger, je komplexer und dynamischer der betrachtete wissensbasierte Handlungsablauf ist. Die Übersicht über den Ablauf wird umso schwerer sein, je

zahlreicher die Wechselwirkungen zwischen technischen Prozessen und dem Handeln des Menschen sind und (oder) je stärker sich diese Wechselwirkungen auf den Zeitablauf des Ereignisses auswirken können. Z. B. könnte es erforderlich sein, in Abhängigkeit von Teilerfolgen mehrere Zeitschwellen $T_{MAX}(1)$ bis $T_{MAX}(n)$ abzuschätzen.

Mit der eingeschränkten Übersicht über die möglichen Entwicklungen erhöht sich auch die Chance, in die Modellierung Fehler einzubringen, die das Bewertungsergebnis u. U. gravierend verfälschen können.

Auf Grund dieser Überlegungen kann der Anwender folgendes Kriterium bzgl. der Wahl zwischen Modell 1 und Modell 2 zugrunde legen:

- Die Vorgehensweise nach Modell 2 sollte angewendet werden, wenn die Analyse streng kausal ohne Vorgriff auf Informationen erfolgen soll, die erst nach Abschluss der anstehenden Analyse vorliegen, oder wenn diese Vorinformationen wegen der Komplexität des Ereignisablaufs nicht oder nur mit erheblichem Aufwand bereitgestellt werden können.
- In allen anderen Fällen besteht Wahlfreiheit zwischen dem Swain‘schen Bewertungsansatz von Modell 1 und dem dynamischen, kausalen Ansatz von Modell 2.

Prinzipiell kann der Anwender weitere Gesichtspunkte für die Modellwahl formulieren, sofern diese Auswahlgesichtspunkte mit dem vorgestellten Kriterium kompatibel sind. Ein solcher Gesichtspunkt könnte z. B. darin bestehen, dass die Bewertung ausschließlich mit dem Ansatz nach Swain erfolgen soll, um die Ergebnisse mit anderen Analyseergebnissen vergleichen zu können, die ebenfalls den Swain’schen Bewertungsansatz verwendet haben.

4.3.5.2 Diskussion und qualitative Bewertung der Modellergebnisse

In Abschnitt 4.3.3 und 4.3.4 wurde der Anwendungsfall einer wissensbasierten Handlung anhand von zwei unterschiedlichen Modellen analysiert. Das zu lösende Problem bestand darin, dass ein fehlerhaft geöffnetes Ventil, das zu einem Kühlmittelverlust aus dem Primärkreis führte, von der Warte aus nicht mehr geschlossen werden konnte. Das Ziel der wissensbasierten Handlung bestand in der möglichst schnellen Beendigung des Kühlmittelverlusts. Als erfolgreich wurde die wissensbasierte Handlung bewertet, wenn das fehlerhaft geöffnete Ventil vor dem kritischen Zeitpunkt T_{MAX} geschlossen werden

konnte, da angenommen wurde, dass es bei Überschreitung von T_{MAX} aufgrund der hohen Druck- und Temperaturbelastungen zu einem vollständigen Schließversagen des Ventils kommt. Die Annahme wurde dadurch begründet, dass bei andauernder Beanspruchung durch die Strömungskräfte und aufgrund der zunehmenden temperaturbedingten mechanischen Verformung der Schließwiderstand soweit zunimmt, dass das Ventil auch durch die Schließkraftreserve des Antriebsmotors nicht mehr geschlossen werden kann.

Im vorliegenden Abschnitt sollen die Ergebnisse der beiden Modelle miteinander verglichen und diskutiert werden. Aus den Werten in den Tab. 4.5 (Modell 1) und Tab. 4.6 (Modell 2) wird deutlich, dass die Zustandswahrscheinlichkeiten, die sich unter Verwendung der beiden Modelle ergeben haben, die gleichen Größenordnungen aufweisen. Beispielsweise wurde in beiden Modellen die geringste Wahrscheinlichkeit für das Ereignis ermittelt, dass es trotz der wissensbasierten Maßnahme zu einem Kühlmittelverluststörfall mit einer Dampfleckage in den SB sowie zum Versagen des Entwässerungsbehälters kommt (Zustand 2). Die Wahrscheinlichkeiten, die für diesen Zustand unter Verwendung von Modell 1 bzw. Modell 2 berechnet wurden, betragen 5.39E-07 bzw. 7.91E-07.

Der besseren Übersicht halber sind die Wahrscheinlichkeiten der Systemzustände, die sich unter Berücksichtigung der beiden Handlungsmodelle ergeben haben nochmals in Tab. 4.9 gegenübergestellt.

Tab. 4.9 Wahrscheinlichkeiten der Systemzustände bzgl. der Handlungsmodelle

Zustand	Modell 1	Modell 2
1	4.9E-01	5.9E-01
2	5.4E-07	6.6E-07
3	4.9E-04	5.9E-04
4	5.1E-01	4.0E-01
5	5.1E-04	4.0E-04

Durch die Zustände 4 und 5 ist ein erfolgreicher Problemlösungsprozess inklusive Umsetzung der gefundenen Lösung definiert. Der Problemlösungsprozess ist nicht erfolgreich, d. h. der Kühlmittelverlust kann durch die Maßnahme nicht gestoppt werden, wenn die Zustände 1, 2 oder 3 eintreten. Die Bedeutung der Zustände ist genauer in den Tab. 4.5 und Tab. 4.6 beschrieben. Obwohl die beiden Modelle recht unterschiedliche Methoden in der Quantifizierung der Zustandswahrscheinlichkeiten aufweisen, stimmen

die Ergebnisse größenordnungsmäßig relativ gut überein. Die wissensbasierte Handlung weist im Modell 1 eine Erfolgswahrscheinlichkeit von ca. 0.51 auf während die über Modell 2 berechnete Erfolgswahrscheinlichkeit ca. 0.4 beträgt. D. h., die Wahrscheinlichkeiten bzgl. Modell 2 weisen tendenziell eher auf einen zu erwartenden Misserfolg hin, während die Wahrscheinlichkeiten für Erfolg und Misserfolg im Modell 1 eher ausgeglichen sind.

Die Unterschiede der Erfolgs- und Misserfolgswahrscheinlichkeit zwischen den Modellen sind u. a. dadurch erklärbar, dass der Zeitbedarf für die Fehlererkennung nach RESA im Modell 2 im Gegensatz zu Modell 1 berücksichtigt worden ist. Hätte man den Zeitbedarf inklusive der Unsicherheit entsprechend in Modell 1 berücksichtigt, würde sich die zur Diagnose zur Verfügung stehende Zeit verkürzen und dadurch die Misserfolgswahrscheinlichkeit erhöhen. Die Vernachlässigung des Zeitbedarfs in Modell 1 geht darauf zurück, dass Modell 1 dem Stand der klassischen PSA entsprechend entwickelt worden ist. Im Vordergrund stand dabei die Gegenüberstellung der Vorgehensweisen, die jeweils bzgl. der klassischen PSA und der dynamischen Analyse praktiziert werden. Hätte man die Zeiten entsprechend in Modell 1 berücksichtigt, wäre zu erwarten, dass die Ergebnisse noch näher beieinanderliegen.

Die Qualität eines probabilistischen Modells ist oftmals nur sehr schwer zu beurteilen. Dies ist insbesondere dann der Fall, wenn Ereignisse, über die probabilistische Aussagen getroffen werden, in der Realität entweder noch gar nicht oder nur sehr selten beobachtet wurden, so dass die Ergebnisse des Modells nicht verifiziert werden können. In solchen Fällen kann die Qualität der probabilistischen Ergebnisse nur indirekt eingeschätzt werden. Dazu muss versucht werden, die Inhalte der Modelle nachzuvollziehen und es muss überprüft werden, ob die getroffenen Annahmen und Abschätzungen der Modelle plausibel und möglichst realistisch sind. Eine weitere Möglichkeit zur Einschätzung der Qualität eines probabilistischen Modells ist die Untersuchung, welche probabilistischen Aussagen aus dem Modell abgeleitet werden können und als wie plausibel diese Aussagen eingeschätzt werden. Dies soll im Folgenden für die Modelle 1 und 2 bzgl. des Anwendungsbeispiels demonstriert werden.

Im Modell 1 (s. Abschnitt 4.3.3.1) wurde angenommen, dass das Fehlöffnen des Ventils mit einer Wahrscheinlichkeit von 0.9 vor RESA und mit einer Wahrscheinlichkeit von 0.1 nach RESA Auslösung erkannt wird. Im Fall, dass die Fehlhandlung nach RESA erkannt wird, wurde die Funktion in Abb. 4.2 (s. Abschnitt 4.2.3) zur Ermittlung der Wahrscheinlichkeit verwendet, dass die Findung einer Problemlösung in der zur Verfügung

stehenden Zeit nicht erfolgreich ist. Die Funktion besagt, dass bei einer zur Verfügung stehenden Zeit von < 20 min die Misserfolgswahrscheinlichkeit 1 ist, bzw. die Wahrscheinlichkeit 0 beträgt, dass eine Lösung in der zur Verfügung stehenden Zeit gefunden wird. Aus den Simulationsrechnungen, die für das Modell 1 durchgeführt worden sind, lassen sich demnach folgende Ergebnisse ableiten:

- Unter der Bedingung, dass die Fehlhandlung vor RESA erkannt wird ($p_{vorRESA} = 0.9$) und damit der Problemlösungsprozess eingeleitet wird, beträgt die mittlere bedingte Wahrscheinlichkeit $p_{Erfolg \mid vorRESA} = 0.566$ dass der Kühlmittelverlust (KMV) erfolgreich gestoppt werden kann.
- Unter der Bedingung, dass der Fehler nach RESA erkannt wird ($p_{nachRESA} = 0.1$), beträgt die mittlere bedingte Wahrscheinlichkeit $p_{Erfolg \mid nachRESA} = 0$, dass der Kühlmittelverlust gestoppt wird.

Nach dem Gesetz der totalen Wahrscheinlichkeit ergibt sich die Wahrscheinlichkeit, dass der KMV durch die wissensbasierte Handlung des Personals erfolgreich gestoppt werden kann zu:

$$\begin{aligned} p_{Erfolg} &= p_{Erfolg \mid vorRESA} \cdot p_{vorRESA} + p_{Erfolg \mid nachRESA} \cdot p_{nachRESA} \\ &= 0.566 \cdot 0.9 + 0 \cdot 0.1 = 0.509 \end{aligned} \tag{4.1}$$

was der in Tab. 4.5 aufgeführten Erfolgswahrscheinlichkeit bzgl. Modell 1 entspricht.

Fragwürdig erscheint nun bei diesem Ergebnis von Modell 1, ob bei einer Fehlererkennung nach RESA eine erfolgreiche Problemlösung tatsächlich ausgeschlossen werden kann, was durch das Ergebnis $p_{Erfolg \mid nachRESA} = 0$ ausgedrückt wird.

Entsprechende Berechnungen werden auch für das Modell 2 durchgeführt. Für Modell 2 wurde analog zu Modell 1 für die Fehlererkennung vor bzw. nach RESA eine Wahrscheinlichkeit von 0.9 bzw. 0.1 angenommen. Wie aus der Beschreibung des Handlungsablaufs aus Abb. 4.6 (s. Abschnitt 4.3.4.1) ersichtlich ist, wurde bei der Fehlererkennung vor RESA noch unterschieden, ob der Fehler sofort (p=0.6) oder mit einer kleinen Zeitverzögerung (p = 0.3) erkannt wird. Außerdem wurde im Modell 2 auch eine Verteilung zur Beschreibung der Unsicherheit definiert, nach welcher Zeit der Fehler nach der RESA Auslösung bemerkt wird. Dazu wurde angenommen, dass der Fehler mit Wahrscheinlichkeit p = 0.3 zwischen 40 und 90 s, mit p = 0.5 zwischen 90 und 180 s

und mit p = 0.2 zwischen 180 und 300 s erkannt wird. D. h., im Gegensatz zu Modell 1 gehen in das Modell 2 konkrete Zeiten ein, wann der Fehler nach RESA erkannt wird und damit der Problemlösungsprozess beginnt.

Die Auswertung der Simulationsrechnungen für Modell 2 unter Verwendung des Crew-Moduls und MCDET haben folgende Ergebnisse geliefert:

- Unter der Bedingung, dass Fehlerkennung vor RESA erfolgt ($p_{vorRESA} = 0.9$) gilt:

  $p_{Erfolg \mid vorRESA} = 0.4023$

- Unter der Bedingung, dass Fehlerkennung nach RESA erfolgt ($p_{nachRESA} = 0.1$) gilt:

  $p_{Erfolg \mid nachRESA} = 0.419$

Nach dem Gesetz der totalen Wahrscheinlichkeit ergibt sich:

$$p_{Erfolg} = p_{Erfolg \mid vorRESA} \cdot p_{vorRESA} + p_{Erfolg \mid nachRESA} \cdot p_{nachRESA}$$
$$= 0.4023 \cdot 0.9 + 0.419 \cdot 0.1 = 0.404 \qquad (4.2)$$

Diese Erfolgswahrscheinlichkeit entspricht dem Ergebnis in Tab. 4.6 bzgl. Modell 2.

Der wesentliche Unterschied der Ergebnisse zwischen beiden Modellen, der zu einer Qualitätsbewertung der Modellergebnisse herangezogen werden kann, zeigt sich in der bedingten Wahrscheinlichkeit von $p_{Erfolg \mid nachRESA}$, d. h. der Erfolgswahrscheinlichkeit unter der Bedingung, dass der Fehler erst nach der RESA Auslösung erkannt wird. Bzgl. der beiden Modelle ergibt sich:

unter Modell 1: $p_{Erfolg \mid nachRESA} = 0$

unter Modell 2: $p_{Erfolg \mid nachRESA} = 0.419$

Der Grund, dass sich unter Modell 1 eine bedingte Wahrscheinlichkeit von 0 ergibt, liegt an der funktionalen Beziehung, mit der die Erfolgswahrscheinlichkeit der Problemlösung in Abhängigkeit des zur Verfügung stehenden Zeitfensters ermittelt wird. Die Funktion besagt, dass bei einer zur Verfügung stehenden Zeit von < 20 min die Erfolgswahrscheinlichkeit der Problemlösung 0 beträgt. Durch die in Modell 1 angenommenen Verteilungen von $T_A \sim U(5,15)$ und $T_{MAX} \sim U(13, 26)$ haben sich im Rahmen der Simulationen keine Zeiten ergeben, bei denen das für die Problemfindung zur Verfügung

stehendes Zeitfenster ≥ 20 min war. Aus diesem Grund wurde anhand der angewendeten Funktion in allen Simulationen eine Erfolgswahrscheinlichkeit von 0 ermittelt.

Wie in Abschnitt 4.3.4 beschrieben, verfolgt Modell 2 einen grundsätzlich anderen Ansatz, bei dem die konkreten Ausführungszeiten der Handlungen zur Ermittlung der Erfolgswahrscheinlichkeiten herangezogen werden. Mit diesem Ansatz ergaben sich auch in den Situationen, in denen der Fehler erst nach der RESA Auslösung erkannt wurde, eine positive Wahrscheinlichkeit einer erfolgreichen Problemfindung sowie deren zeitgerechte Umsetzung.

Bzgl. der Qualitätsbewertung der Modellergebnisse kann man sich nun die Frage stellen, welche Erfolgswahrscheinlichkeit plausibler erscheint. Eine Wahrscheinlichkeit von 0 besagt, dass eine erfolgreiche Problemfindung unmöglich ist, wenn die Fehlererkennung nach RESA erfolgt. Diese Aussage erscheint jedoch nicht gerechtfertigt, da in ca. 47 % der Simulationen das zur Verfügung stehende Zeitfenster zwischen 10 und 19 min beträgt. In diesem zur Verfügung stehenden Zeitrahmen kann man sich bei dem gegebenen Problem durchaus vorstellen, dass sowohl die Fehlererkennung nach RESA als auch die darauf stattfindende Problemfindung erfolgreich durchgeführt werden kann. Aus diesem Grund erscheinen die Modellergebnisse von Modell 2 realitätsnäher und plausibler zu sein als die von Modell 1. Als Konsequenz könnte daraus abgeleitet werden, dass der dynamische Modellierungsansatz von Modell 2 dem Swain'schen Bewertungsansatz von Modell 1 vorzuziehen ist. Ob diese Aussage zutrifft und allgemein gültig ist, muss jedoch anhand mehrerer unterschiedlicher Anwendungen bestätigt werden. Die hier für das Anwendungsbeispiel durchgeführte Untersuchung kann lediglich als ein erster Hinweis dienen.

Wie oben erwähnt, wurde für die Fehlererkennung nach RESA in Modell 2 eine Zeitverteilung in Form einer Histogramm-Verteilung zugrunde gelegt (s. Abb. 4.6). Hier könnte man z. B. weiter untersuchen, innerhalb welcher Erkennungszeiten eine erfolgreiche Problemlösung möglich war. Unter der Bedingung einer Fehlererkennung nach RESA und einer Fehlererkennungszeit von 40 – 90 s ergibt sich:

$$p_{Erfolg \mid nachRESA \,\&\, 40\text{-}90} = 0.467$$

$$p_{Erfolg \mid nachRESA \,\&\, 90\text{-}180} = 0.424$$

$$p_{Erfolg \mid nachRESA \,\&\, 180\text{-}300} = 0.33$$

Unter der Bedingung, dass die Fehlhandlung erst nach RESA erkannt wird, zeigen die Zeitklassen der Erkennungszeiten, die für die Histogramm-Verteilung angenommen wurden, lediglich einen leichten Einfluss auf die bedingten Erfolgswahrscheinlichkeiten. Wenn der Fehler erst nach RESA erkannt wird und die Zeit, die zur Erkennung des Fehlers benötigt wird zwischen 40 und 90 s liegt, beträgt die Erfolgswahrscheinlichkeit 0.467. Liegt die Zeit zur Fehlererkennung zwischen 1.5 und 3 min ist die Erfolgswahrscheinlichkeit mit 0.424 immer noch relativ hoch. Erst bei einer Erkennungszeit zwischen 3 und 5 min wird eine etwas deutlichere Verringerung der Erfolgswahrscheinlichkeit auf 0.33 erkennbar. Die Zeiten, wann der Fehler nach RESA erkannt wird, wurden für den Anwendungsfall in Modell 2 relativ kurz gewählt, da davon ausgegangen wird, dass der Fehler und seine Auswirkung nicht sehr komplex ist und aufgrund der Prozessindikatoren relativ schnell erkannt werden müsste.

Da für die Beurteilung des Handlungserfolges die Zeit relevant ist, wann die wissensbasierte Handlung abgeschlossen ist, werden in Abb. 4.9, die bedingten Zeitverteilungen der Beendigung der Handlung in Abhängigkeit der Fehlererkennungszeiten nach RESA angegeben.

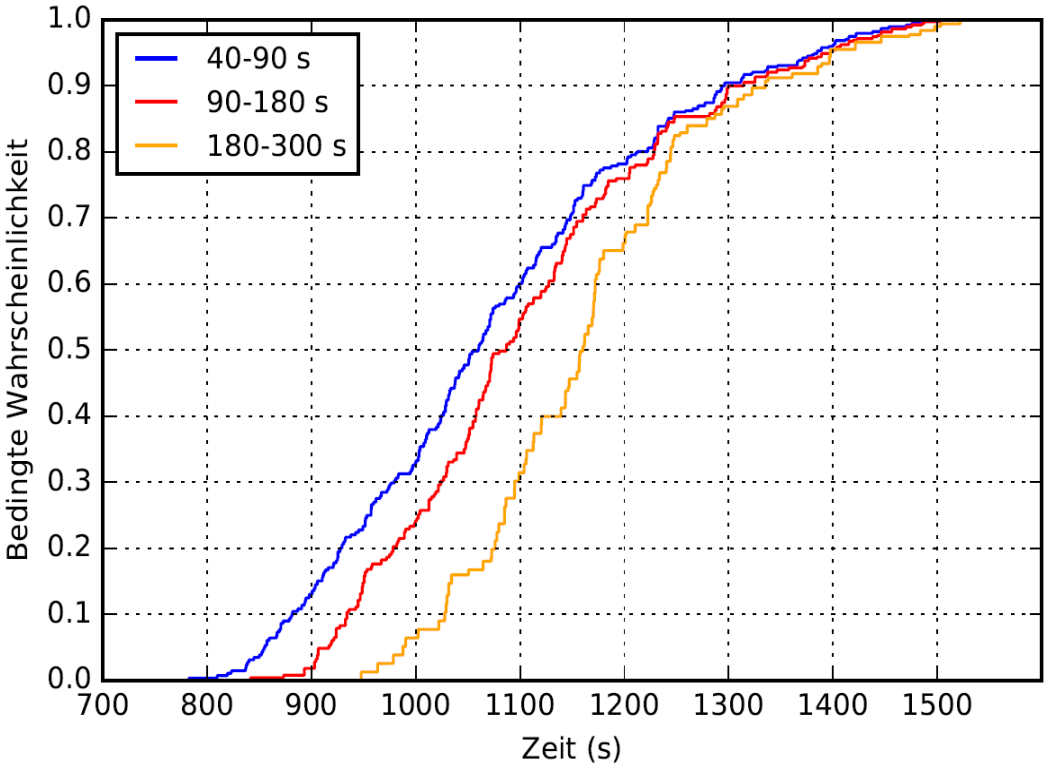


Abb. 4.9 Bedingte Verteilungen der Zeiten, wann wissensbasierte Handlung abgeschlossen wurde, in Abhängigkeit der Fehlererkennungszeit nach RESA

Abb. 4.9 zeigt, dass sich die bedingten Verteilungen im Bereich der oberen 20 % kaum unterscheiden. Bei den unteren 50 % der Verteilungswerte liegen die Zeitdifferenzen bzgl. der Beendigung der Handlung zwischen den Zeitklassen ‚40-90 s' und ‚90-180 s' der Fehlererkennung zwischen 30 s und 60 s. In der Klasse ‚180-300 s' erfolgt die Beendigung der Handlung in den unteren 50 % der Fälle nochmals um ca. 1.5 min später. Insgesamt wirken sich die Fehlererkennungszeiten nicht so stark auf die Zeiten aus, wann die wissensbasierte Handlung beendet wird. Daraus erklärt sich auch der relativ geringe Einfluss der Fehlerkennungszeit auf die Erfolgswahrscheinlichkeit der Handlung.

Fazit: Die Diskussion der Analyseergebnisse der angewendeten Modelle hat ergeben, dass Modell 2 unter Verwendung des Konzepts des Crew-Moduls allgemein zur dynamischen Modellierung und Simulation von Handlungsabläufen (sowohl regel- als auch wissensbasiert) angewendet werden kann. Der dynamische Modellierungsansatz von Modell 2 ist im Detail nachzuvollziehen, leicht zu modifizieren und entspricht der realen Situation, wie der Erfolg einer Handlung bestimmt wird. Beim Swain'schen Bewertungsansatz wird die Erfolgswahrscheinlichkeit anhand einer funktionalen Beziehung in Abhängigkeit des zur Problemfindung zur Verfügung stehenden Zeitfensters bestimmt. Mit welcher Begründung diese funktionale Beziehung hergeleitet wurde bzw. welche Informationen dieser funktionalen Beziehung zugrunde liegen, bleibt dem Anwender verborgen.

Der Swain'sche Bewertungsansatz im Modell 1 ist nur unter der Bedingung anwendbar, dass das Zeitfenster, das für die Problemfindung zur Verfügung steht, im Vorfeld der Analyse bekannt ist. Dazu muss im Vorfeld der kritische Zeitpunkt bekannt sein, zu dem eine Maßnahme abgeschlossen sein muss, um erfolgreich zu sein. Diese Bedingung ist jedoch in manchen Fällen nur schwer einzuschätzen, da der kritische Zeitpunkt eines Prozesses aufgrund unterschiedlicher Einflüsse und Wechselwirkungen erst nach Ablauf des Prozesses bestimmt werden kann. Dies gilt insbesondere dann, wenn aleatorische und epistemische Unsicherheiten berücksichtigt werden, wodurch der kritischen Zeitpunkt mehr oder weniger stark variieren kann.

Die Vorteile des dynamischen Ansatzes unter Verwendung des Crew-Moduls in Verbindung mit MCDET, der in Modell 2 angewendet wurde, zeigen sich in folgenden Aspekten:

- Handlungsabläufe (sowohl regel- als auch wissensbasiert) können allgemein und ohne Bedingungen modelliert werden.

- Der dynamische Modellierungsansatz von Modell 2 folgt dem kausalen Ablauf einer Handlung, wie sie in der Realität erfolgt. Der Modellierungsansatz von Modell 1, dem der Swain‘sche Bewertungsansatz zugrunde liegt, entspricht in einigen aber wichtigen Teilen eher einer Black Box.

- Die Modellierung kann beliebig detailliert erfolgen und ist bis ins Detail nachzuvollziehen. D. h., an jeder Stelle des Modells ist erkennbar, welche Informationen, Unsicherheiten und Abschätzungen in das Modell eingegangen sind. Dies ist eine wichtige Voraussetzung dafür, dass das Modell leicht nachzuvollziehen ist und eine Identifikation derjenigen Stellen des Modells erlaubt, die ggf. unter Verwendung genauerer Informationen verbessert werden können.

- Die Modellierung eines Handlungsablaufs über die in diesem Vorhaben entwickelte Oberfläche zum Crew-Modul ist so flexibel, dass eine Modifikation des Modells relativ einfach und schnell durchgeführt werden kann.

- Die Auswertungen der Analyseergebnisse von Modell 2 haben gezeigt, dass sehr detaillierte probabilistische Aussagen bzgl. des modellierten Handlungsablaufs ermittelt werden können. Diese Detailergebnisse können ggf. Hinweise auf die Qualität des Modells geben.

- So haben sich beispielswiese zwischen Modell 1 und Modell 2 signifikante Unterschiede bzgl. der bedingten Erfolgswahrscheinlichkeit gezeigt, wenn die Fehlöffnung des Ventils erst nach der RESA Auslösung erkannt wird. Bzgl. Modell 1 hat sich eine bedingte Wahrscheinlichkeit von 0 ergeben. Im Gegensatz dazu wurde unter Verwendung von Modell 2 eine bedingte Wahrscheinlichkeit von 0.419 ermittelt. Im Kontext des Handlungsablaufs ist das Ergebnis der bedingten Wahrscheinlichkeit von Modell 2 als plausibler einzuschätzen als das von Modell 1.

- Der dynamische Ansatz ermöglicht es, aleatorische Unsicherheiten (stochastische Ereignisse) und Abhängigkeiten des Handlungsablaufs von Prozesszuständen umfassend und detailliert zu modellieren und deren Einflüsse auf den Handlungsablauf probabilistisch zu quantifizieren.

5 Zusammenfassung und Schlussfolgerung

Die integrale deterministisch-probabilistische Sicherheitsanalyse (IDPSA), oft auch als probabilistische Dynamikanalyse oder dynamische PSA bezeichnet, ist ein aktuelles und praktisch bedeutsames Forschungsgebiet, auf dem international Forschungseinrichtungen tätig sind, welche zum Teil auch durch nationale Behörden für die Aufsicht über kerntechnische Anlagen unterstützt werden (z. B. USNRC). Methoden zur Durchführung probabilistischer Dynamikanalysen können nicht nur in der Kerntechnik, sondern auch in anderen Risikotechnologiebereichen angewendet werden, um Sicherheitsbeurteilungen durchzuführen. Methodenentwicklungen zur Durchführung von IDPSA besitzen somit einen umfangreichen Anwendungsbereich, der weit über die Kerntechnik hinausgehen kann.

Der wesentliche Vorteil der Anwendung einer IDPSA in der Reaktorsicherheit besteht darin, die Vielfalt möglicher Verläufe sicherheitstechnisch wichtiger Prozesse unter realistischen Annahmen repräsentieren, analysieren und angemessen bewerten zu können. Insbesondere schafft es die IDPSA wie keine andere Analyse, den zufälligen Schwankungen der Zeitpunkte, zu denen Ereignisse eintreten, und den komplexen Wechselwirkungen von Phänomenen eines Unfallablaufs gerecht zu werden und ihre Auswirkungen auf den Prozessablauf zu quantifizieren. Eine solche zeitabhängige Analyse sprengt die Möglichkeiten einer klassischen probabilistischen Sicherheitsanalyse (PSA), die aufgrund ihres statischen Charakters und der nur beschränkten Möglichkeit des Bezugs auf entsprechende Simulationsläufe mit Modellvereinfachungen und groben Abschätzungen arbeiten muss. Durch den Einsatz fortschrittlicher dynamischer Methoden, wie sie in diesem Projekt entwickelt und erfolgreich angewendet wurden, kann die Sicherheitsbeurteilung von Risikotechnologien deutlich verbessert werden.

In dem vorliegenden Projekt wurden sowohl methodische und programmtechnische Entwicklungsarbeiten sowie deren Umsetzung und Anwendung in konkreten Analysen durchgeführt. Das Projekt umfasst drei Themenbereiche:

1. Methodische und programmtechnische Weiterentwicklungen zur Vereinfachung und Verbesserung der Anwendungsmöglichkeiten des Analysewerkzeugs MCDET

2. Analyse und Bewertung des Einflusses relevanter Unsicherheiten auf thermisch induziertes Dampferzeuger-Heizrohrversagen bei einem Hochdruck-Kernschmelz-Unfallablauf

3. Methodenentwicklung zur Analyse und Bewertung wissensbasierter Handlungen unter Verwendung der MCDET-Methode sowie Erprobung an einem Ereignis aus der deutschen Betriebserfahrung

Die Arbeiten wurden im wesentlich so strukturiert, dass die methodischen und programmtechnischen Entwicklungen im Rahmen der durchzuführenden Analyse zum thermisch induzierten Dampferzeuger-Heizrohrversagen und der Analyse wissensbasierter Handlungen an einem Ereignis aus der deutschen Betriebserfahrung, angewendet und erprobt werden konnten.

Mit den in diesem Projekt durchgeführten Entwicklungsarbeiten zum MCDET-Scheduler und ATHLET-CD Treiber wurde die Anwendung von MCDET insbesondere in Verbindung mit den GRS-Programmen ATHLET und ATHLET-CD erheblich vereinfacht. Gleichzeitig wird durch den neu entwickelten MCDET-Scheduler eine wesentlich effizientere Abarbeitung der vielfältigen Unfallabläufe erzielt, die im Rahmen einer MCDET-Analyse gerechnet werden. In Verbindung mit dem Werkzeug MCDET können ATHLET und ATHLET-CD nun auch zur Durchführung von integralen deterministisch-probabilistischen Sicherheitsanalysen eingesetzt werden, womit das Anwendungsspektrum dieser Programme erheblich erweitert wird.

Bzgl. der Weiterentwicklung des Crew-Moduls, das zur Modellierung und Simulation von dynamischen Handlungsabläufen eingesetzt werden kann, wurde ein Konzept entwickelt und umgesetzt, welches dem Anwender ermöglicht, den zu analysierenden Handlungsablauf über eine grafische Benutzeroberfläche in einer strukturierten Form zu beschreiben. Außerdem wurden Arbeiten durchgeführt, um die aufwendige Erstellung des Eingabedatensatzes für das Crew-Modul zu automatisieren. Diese Arbeiten tragen zu einer erheblichen Vereinfachung und Verringerung der Fehleranfälligkeit bei der Modellerstellung und der Erzeugung des umfangreichen Eingabedatensatzes bei. Die Entwicklungen zum Crew-Modul wurden in den Arbeitspunkten 2 und 3 erfolgreich eingesetzt. Dabei hat sich gezeigt, dass durch die Entwicklungsarbeiten die Anwendung des Crew-Moduls durch den Benutzer erheblich vereinfacht werden konnte.

Zur Auswertung und Visualisierung der umfangreichen Ergebnisse einer IDPSA, die unter Verwendung von MCDET erzeugt werden, wurden entsprechende Routinen entwickelt, mit denen die Auswertungen der Anwendungsbeispiele in den Arbeitspunkten 2 und 3 durchgeführt worden sind. Aufgrund des neuen MCDET-Schedulers mussten die Auswerteroutinen neu erstellt werden. Die Routinen liegen in Form eines iPython-

Notebooks vor, was als Vorstufe zu einer grafischen Benutzeroberfläche betrachtet werden kann. Die bisher entwickelten Auswerteroutinen stellen einen Basissatz dar, der sukzessive um zusätzliche statistische Auswerteoptionen erweitert werden kann.

Neben der Erprobung des neu entwickelten MCDET-Schedulers und des ATHLET-CD Treibers (siehe Abschnitte 2.1 und 2.2) bestand eine weitere Zielsetzung darin, anhand der durchgeführten IDPSA detailliertere probabilistische Aussagen und ggf. neue Erkenntnissen bzgl. des thermisch-induzierten DEHEIRO-Versagens zu erhalten. Dabei geht es insbesondere um die Einbeziehung und Quantifizierung der Auswirkungen stochastischer Einflussgrößen (aleatorische Unsicherheiten), die mit den Methoden der klassischen PSA nicht ausreichend berücksichtigt werden können. Der Analyse liegen deshalb Fragestellungen zugrunde, die bisher mangels geeigneter Methodik noch nicht untersucht werden konnten, z. B. Einfluss zufälliger Ausfallzeitunkte der DH-Ventile oder Auswirkungen von Vorschädigung des DE-Heizrohrs auf das DEHEIRO-Versagen.

Zur Schätzung der aleatorischen Unsicherheiten bzgl. des Ausfallverhaltens der DH-Ventile und der Vorschädigung des DE-Heizrohrs wurden separate Wahrscheinlichkeitsmodelle hergeleitet, in die ihrerseits aleatorische und epistemische Unsicherheiten eingehen. Aus den entwickelten Wahrscheinlichkeitsmodellen können z. B. die mittleren Wahrscheinlichkeiten dafür bestimmt werden, dass

- DH-AV, DH-SiV1 und DH-SiV2 jeweils frühzeitig, mittelfristig oder spät Ausfallen oder
- dass die Vorschädigung des DE-Heizrohrs zu Beginn des Unfallablaufs < 10 %, 10 – 20 %, …, 50 – 70 % beträgt.

Hierbei sollte insbesondere gezeigt werden, dass die Entwicklung probabilistischer Modelle nützlich sein kann, um aleatorische Unsicherheiten quantifizieren zu können die ansonsten - wenn überhaupt - nur sehr schwer abzuschätzen sind.

Die in dem Anwendungsbeispiel berücksichtigten aleatorischen Unsicherheiten zum Ausfallverhalten der DH-Ventile und Vorschädigung des DE-Heizrohrs geben ein Beispiel, in welchem Umfang und Detaillierungsgrad aleatorische Unsicherheiten in einer MCDET-Analyse berücksichtigt werden können. Um den Einfluss des Ausfallzeitpunktes der Druckhalterventile auf den Unfallablauf genauer untersuchen zu können, wurden in der MCDET-Analyse in jedem erzeugten dynamischen Ereignisbaum frühzeitige (Ausfall innerhalb der ersten 20 Anforderungszyklen), mittelfristige (Ausfall innerhalb der

Anforderungszyklen 21 – 60) und späte Ausfälle (Ausfall zu einem Anforderungszyklus > 60) gemeinsam berücksichtigt. Neben den unabhängigen Ausfällen wurden zusätzlich auch gemeinsam verursachte Ausfälle, d. h. 2v3-GVA und 3v3-GVA, in die Analyse einbezogen. Da das Ausfallverhalten möglichst realistisch modelliert werden sollte, wurden bzgl. eines 2v3-GVA diejenigen DH-Ventile zufällig ausgespielt, die vom GVA betroffen sind. Die restliche nicht vom GVA betroffene Komponente kann dann zusätzlich zu einem zufälligen späteren Zeitpunkt unabhängig ausfallen.

In der erzeugten Stichprobe von 100 DETs wurden insgesamt 4216 Unfallsequenzen unter unterschiedlichen Bedingungen gerechnet, die sich durch die aleatorischen und epistemischen Unsicherheiten ergeben. Für jede einzelne gerechnete Sequenz liegt neben dem zeitlichen Verlauf der ATHLET-Prozessgrößen die zusätzliche Information vor, welche Zufallsereignisse und epistemischen Werte dem Verlauf zugrunde liegen und mit welcher Wahrscheinlichkeit die jeweilige Sequenz eintritt. Die Ergebnisse der MCDET/ATHLET-CD Analyse wurden bzgl. unterschiedlicher Fragestellungen ausgewertet, wodurch sich eine Vielzahl probabilistischer Aussagen ergeben haben. z. B.:

Wahrscheinlichkeit des DEHEIRO-Versagens.

- Wahrscheinlichkeitsverteilung des Zeitpunktes, wann DEHEIRO unter der Bedingung schwacher (< 20 %) und starker (20 – 70 %) Vorschädigung versagt.
- Aus dieser Verteilung können bedingte Wahrscheinlichkeiten berechnet werden, dass ein stark bzw. schwach geschädigtes DE-Heizrohr in bestimmten Zeitintervallen (z. B. zwischen 2 und 2.5 h nach dem einleitenden Ereignis) versagt.
- Wahrscheinlichkeit, dass ein Bruch der HKL (VAL) vor bzw. nach DEHEIRO-Versagen auftritt, oder Wahrscheinlichkeit, dass weder ein Bruch der HKL noch ein Bruch der VAL nach DEHEIRO-Versagen auftritt.
- Wahrscheinlichkeitsverteilung der Zeit, wann HKL bzw. VAL versagt.
- Wahrscheinlichkeitsverteilung der Zeitdauer zwischen DEHEIRO-Versagen und Bruch der HKL bzgl. schwacher (< 20 %) und starker (20 – 70 %) Vorschädigungen.
- Wahrscheinlichkeitsverteilung der Heizrohr-Temperatur zum Zeitpunkt des DEHEIRO-Versagens bzgl. schwacher (< 20 %) und starker (20 – 70 %) Vorschädigungen.
- Wahrscheinlichkeitsverteilung des Zeitpunkts, wann SDE erfolgt.

- Wahrscheinlichkeitsverteilung der Zeitspanne zwischen SDE und DEHEIRO-Versagen in Abhängigkeit des Schweregrades der DE-Heizrohr Schädigung.
- Wahrscheinlichkeitsverteilung der Druckdifferenz zum Zeitpunkt des DEHEIRO-Versagens in Abhängigkeit des Ausmaßes der DE-Heizrohr Schädigung zu Beginn des Unfallablaufs.
- Wahrscheinlichkeitsverteilung der Zeitdauer, wie lange Druckdifferenzen > 10 MPa von SDE bis zum DEHEIRO-Versagen anstehen. Die Verteilungen werden unter der Bedingung verschiedener Schädigungsgrade ermittelt, um die Abhängigkeit der Zeitdauern vom Ausmaß der Schädigung quantifizieren zu können.
- Wahrscheinlichkeitsverteilung des Versagenszeitpunktes von mindestens einem DH-Ventil in Offenstellung
- Wahrscheinlichkeit, dass alle drei DH-Ventile geschlossen versagen.
- Wahrscheinlichkeitsverteilung des Zeitpunktes, wann alle drei DH-Ventile geschlossen versagen.

Ein Ziel der Auswertung war es, eine Vorstellung über die Möglichkeiten zu geben, welche Vielfalt an probabilistischen Aussagen aus den Ergebnissen einer MCDET-Analyse berechnet werden können. Die obige Auflistung der probabilistischen Ergebnisse gibt dabei nur einen relativ kleinen beispielhaften Ausschnitt der Möglichkeiten an. Diese Möglichkeiten würden sich noch deutlich steigern, wenn die Auswerteroutinen des Postprocessing von MCDET sich auf den gesamten Satz der Prozessgrößen von ATHLET-CD beziehen könnte. Hierzu sind noch Programmentwicklungen nötig, die im Rahmen eines Nachfolgevorhabens umgesetzt werden sollen.

Die Vielfalt und der Detaillierungsgrad der probabilistischen Aussagen, die aus der in diesem Projekt durchgeführten MCDET/ATHLET-CD Analyse berechnet werden konnten, beschreibt einen wesentlichen Vorteil einer IDPSA unter Verwendung von MCDET. Berücksichtigt man, dass viele dieser probabilistischen Aussagen für eine Erweiterung eines Ereignisbaums der klassischen PSA verwendet können, liefert dies gleichzeitig ein Beispiel, welchen Nutzen solche Analysen mit fortschrittlichen Methoden haben können.

Stochastische Einflussgrößen lassen sich wesentlich umfassender und detaillierter in der Analyse berücksichtigen und liefern Kenntnisse über deren Einfluss auf den

Unfallablauf. Diese stochastischen Einflüsse können quantifiziert und hinsichtlich ihrer Signifikanz bewertet werden. Aus diesen Analysen unter Verwendung fortschrittlicher Methoden lassen sich eine Vielzahl probabilistischer Aussagen ableiten, die man mit anderen Methoden in diesem Detaillierungsgrad nicht – oder mit äußerst viel Aufwand, der eine praktische Anwendung ausschließt – erhalten würde.

Obwohl die MCDET-Methode im Vergleich zu einer reinen Monte-Carlo Simulation wesentlich effizienter ist, wird im Rahmen der Weiterentwicklungsarbeiten der Methode immer darauf geachtet, den Rechenaufwand reduzieren zu können, um MCDET für die praktische Anwendung noch effizienter zu machen. In diesem Zusammenhang wurde gezeigt, dass durch eine geschickte Einbindung der aleatorischen Unsicherheiten (z. B. zeitlich variierende Ausfälle der jeweiligen DH-Ventile, zufällige Vorschädigung des DE-Heizrohrs zu Beginn des Unfallablaufs) in die MCDET-Analyse eine erhebliche Reduzierung des Rechenaufwandes erzielt werden kann. D. h., der Anwender kann durch eine geschickte Modellierung, wie die aleatorischen Unsicherheiten in MCDET eingebunden werden, eine erhebliche Einsparung des Rechenzeitbedarfs erzielen. Wie gezeigt wurde, erfordert dies jedoch eine sorgfältige Berücksichtigung der jeweiligen Wahrscheinlichkeiten für die im dynamischen Ereignisbaum generierten Verzweigungen, die nicht immer trivial ist.

Eine weitere Zielsetzung des Projekts bestand in der Entwicklung und beispielhaften Anwendung einer Methode, mit der wissensbasiertes Handeln auch in Ereignisabläufen berücksichtigen werden können, die wegen ihrer Dynamik und Komplexität bevorzugt mit einer dynamischen ausgelegten Methodik analysiert und bewertet werden sollten. Die dazu entwickelte Methode wurde an einem ausgewählten Ereignis aus der deutschen Betriebserfahrung erprobt und verifiziert. Für das Anwendungsbeispiel wurde ein meldepflichtiges Ereignis ausgewählt, das in einer inzwischen stillgelegten und sich im Rückbau befindlichen Anlage auftrat. Bei dem ausgewählten Ereignis handelt es sich um einen Precursor-LOCA aus der deutschen Betriebserfahrung. Das zu lösende Problem bestand darin, dass ein fehlerhaft geöffnetes Ventil, dass zu einem Kühlmittelverlust aus dem Primärkreis führte, von der Warte aus nicht mehr geschlossen werden konnte. Das Ziel der wissensbasierten Handlung bestand in der möglichst schnellen Beendigung des Kühlmittelverlusts.

Die Analyse wurde mit zwei unterschiedlichen Modellansätzen durchgeführt. Der erste Modellansatz modelliert den wissensbasierten Ablauf des Referenzereignisses in Anlehnung an die klassische Vorgehensweise unter Verwendung des Swain’schen

Bewertungsansatzes für die Lösungsfindung eines Problems. Der Unterschied zur klassischen Vorgehensweise ist, dass aleatorische Unsicherheiten für die Handlungsausführung und des maximalen Zeitpunktes in das Modell eingehen, bis wann die wissensbasierten Handlungen abgeschlossen sein müssen. Die aleatorischen Unsicherheiten werden über Simulationen des erstellten Ereignisbaumes berücksichtigt. Eine Beschränkung des Swain‘schen Bewertungsansatzes besteht darin, dass vor Beginn der Analyse Informationen vorliegen müssen, die man prinzipiell erst nach der Analyse kennen kann. Der Anwender muss diese Informationen also aus Überlegungen ableiten, in dem er die möglichen Ergebnisse von Prozessgrößen, die vom Handlungsablauf abhängen, in Vorfeld abschätzt. Diese Vorwegnahme ist umso schwieriger oder zumindest aufwendiger, je komplexer und dynamischer der betrachtete wissensbasierte Handlungsablauf ist.

Um die Beschränkung zu vermeiden, wurde die Analyse mit einem zweiten Modellansatz durchgeführt, der auf dem dynamischen Konzept des Crew-Moduls basiert. Der Vorteil der dynamischen Modellierung über das Crew-Modul ist, dass zeitliche Wechselwirkungen von Handlungen in Abhängigkeit von zufälligen Einflussgrößen und Systemzuständen explizit modelliert und in der Analyse berücksichtigt werden können.

Für den Modellansatz 1 wurden ca. 1200 unterschiedliche Abläufe simuliert. Aus diesen Abläufen wurden die Wahrscheinlichkeiten sowie die 95 %-Konfidenzintervalle bzgl. der Wahrscheinlichkeiten für die sich ergebenden Endzustände berechnet. In der Analyse unter Berücksichtigung des Modellansatzes 2 wurden ca. 11800 unterschiedliche Abläufe gerechnet. Die hohe Anzahl an unterschiedlichen Abläufen ergibt sich durch die größere Anzahl an aleatorischen Größen und Abhängigkeiten, die im Modell 2 berücksichtigt worden sind. Analog zu Modell 1 wurden aus den Abläufen die Wahrscheinlichkeiten sowie die 95 %-Konfidenzintervalle bzgl. der Endzustände berechnet.

Im Vordergrund der Analysen mit den beiden unterschiedlichen Modellansätzen stand die Gegenüberstellung der Vorgehensweisen, die jeweils bzgl. der klassischen PSA und der dynamischen Analyse praktiziert werden. Die wissensbasierte Handlung weist im Modell 1 eine Erfolgswahrscheinlichkeit von ca. 0.51 auf während die über Modell 2 berechnete Erfolgswahrscheinlichkeit ca. 0.4 beträgt. Die Unterschiede der Erfolgs- bzw. Misserfolgswahrscheinlichkeiten zwischen den Modellen sind dadurch erklärbar, dass im Modell 2 im Gegensatz zu Modell 1 verschiedene zusätzliche Unsicherheiten (z. B. Zeitbedarf für die Fehlererkennung nach RESA) berücksichtigt worden ist. Hätte man den Zeitbedarf inklusive der Unsicherheit entsprechend in Modell 1 berücksichtigt, würde

sich die zur Diagnose zur Verfügung stehende Zeit verkürzen und dadurch die Misserfolgswahrscheinlichkeit erhöhen, wodurch sich die Ergebnisse weiter angenähert hätten.

Die Diskussion der Analyseergebnisse der angewendeten Modelle hat ergeben, dass Modell 2 unter Verwendung des Konzepts des Crew-Moduls allgemein zur dynamischen Modellierung und Simulation von Handlungsabläufen (sowohl regel- als auch wissensbasiert) angewendet werden kann. Der dynamische Modellierungsansatz von Modell 2 ist im Detail nachzuvollziehen, leicht zu modifizieren und entspricht der realen Situation, wie der Erfolg einer Handlung bestimmt wird. Beim Swain'schen Bewertungsansatz wird die Erfolgswahrscheinlichkeit der Problemfindung anhand einer funktionalen Beziehung in Abhängigkeit des zur Problemfindung zur Verfügung stehenden Zeitfensters bestimmt. Mit welcher Begründung diese funktionale Beziehung hergeleitet wurde bzw. welche Informationen dieser funktionalen Beziehung zugrunde liegen, bleibt dem Anwender verborgen.

Die dynamische Modellierung kann beliebig detailliert erfolgen und ist bis ins Detail nachzuvollziehen. D. h., an jeder Stelle des Modells ist erkennbar, welche Informationen, Unsicherheiten und Abschätzungen in das Modell eingegangen sind. Dies ist eine wichtige Voraussetzung dafür, dass das Modell leicht nachzuvollziehen ist und eine Identifikation derjenigen Stellen des Modells erlaubt, die ggf. unter Verwendung genauerer Informationen verbessert werden können. Die Modellierung eines Handlungsablaufs über die in diesem Vorhaben entwickelte Oberfläche zum Crew-Modul ist so flexibel, dass eine Modifikation des Modells relativ einfach und schnell durchgeführt werden kann.

Die Auswertungen der Analyseergebnisse von Modell 2 haben gezeigt, dass sehr detaillierte probabilistische Aussagen bzgl. des modellierten Handlungsablaufs ermittelt werden können. Diese Detailergebnisse können ggf. Hinweise auf die Qualität des Modells geben. So haben sich beispielswiese zwischen Modell 1 und Modell 2 signifikante Unterschiede bzgl. der bedingten Erfolgswahrscheinlichkeit gezeigt, wenn die Fehlöffnung des Ventils erst nach der RESA Auslösung erkannt wird. Bzgl. Modell 1 hat sich eine bedingte Wahrscheinlichkeit von 0 ergeben. Eine Wahrscheinlichkeit von 0 besagt, dass eine erfolgreiche Problemfindung unmöglich ist, wenn die Fehlererkennung nach RESA erfolgt. Im Kontext des Handlungsablaufs erscheint dies nicht sehr plausibel zu sein. Im Gegensatz dazu wurde unter Verwendung von Modell 2 eine bedingte Wahrscheinlichkeit von 0.419 ermittelt.

Der dynamische Ansatz unter Verwendung des Crew-Moduls in Verbindung mit MCDET ermöglicht es, aleatorische Unsicherheiten (stochastische Ereignisse) und Abhängigkeiten des Handlungsablaufs von Prozesszuständen umfassend und detailliert zu modellieren und deren Einflüsse auf den Handlungsablauf probabilistisch zu quantifizieren.

Um das Anwendungsspektrum von MCDET zu erweitern sind als nächstes folgende Weiterentwicklungsarbeiten durchzuführen:

- Zugriff von MCDET auf den gesamten Satz der ATHLET-CD Prozessgrößen
- Entwicklung von Treibern, um den neu entwickelte MCDET-Scheduler auch mit deterministischen Rechenprogrammen verbinden zu können, in deren Quellcode man nicht eingreifen kann.
- Erweiterung der Auswerteoptionen für das Postprocessing und der grafischen Darstellung

Bzgl. der Analyse der wissensbasierten Handlungen wäre als weiterführende Untersuchung interessant, welchen Zugewinn an Sicherheit durch das wissensbasierte Handeln erreicht wird. Durch die dynamische Analyse der wissensbasierten Handlung für das Anwendungsbeispiel konnte die Wahrscheinlichkeit des Handlungserfolges sowie die Zeitverteilung ermittelt werden, wann der Kühlmittelverlust durch die Handlung gestoppt werden konnte. Anhand dieser Zeiten könnte man berechnen, wie groß der Kühlmittelverlust aus dem Primärkreis ist. Dieser Kühlmittelverlust wäre dem gegenüberzustellen, der ohne die wissensbasierte Handlung eingetreten wäre.

Weitere Themen für Entwicklungsarbeiten bzgl. wissensbasierter Handlungen sind insbesondere:

1. Verbesserung der Expertenschätzung der Tab. 4.3 durch Datenerhebung bei Operateuren und anderem relevanten Personal.
2. Aufbereitung der Daten aus /WES 87/ für die einzelnen Aufgabenkategorien. Das hätte den Vorteil, dass die Experten die Eigenarten der Aufgabenkategorie explizit berücksichtigen können, wobei Wissen und Erfahrung der Problemlöser in die Daten eingehen können.
3. Vertiefte Prüfung der Kategorisierung der Aufgaben /WES 87/ (Vollständigkeit, weitere Unterteilungen – erfassen die Kategorien „alle“ wissensbasierten Handlungen, die in der Betriebserfahrung beobachtet worden sind?)

4. Anwendung der Methode auf weitere wissensbasierte Handlungen insbesondere für Handlungsabläufe bei übergreifenden Einwirkungen, die i. A. stark von den Einschätzungen und Überlegungen der Schichtleiter abhängt.

Literatur

/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.

/FAS 03/ Faßmann, W., W. Preischl: 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.

/FAS 10/ 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.

/FAS 14/ Faßmann, W.: Methode für die Analyse und Bewertung der Wechselwirkung zwischen Stress und der Zuverlässigkeit wissensbasierten Handels in der probabilistischen Sicherheitsanalyse, GRS-332, Juni 2014.

/GRS 01/ Verstegen, C., von Linden, J., Löffler, H., Müller-Ecker, D.: Bewertung des Unfallrisikos fortschrittlicher Druckwasserreaktoren in Deutschland – Methoden und Ergebnisse einer umfassenden Probabilistischen Sicherheitsanalyse (PSA), GRS-175, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Oktober 2001.

/GRS 15/ Steinrötter, T., Hage, M., Kowalik, M., Sonnenkalb, M.: Untersuchungen zum anlageninternen Notfallschutz deutscher Kernkraftwerke und Darstellung der Wirksamkeit von Optimierungsmaßnahmen, Abschlussbericht, GRS-A-3839, November 2017.

/GRS 17/ Band, S., Bläsius, C., Scheurer, M., Steinrötter, T.: Thermohydraulisches Verhalten und Komponentenverhalten eines DWR bei ausgewähltem Kernschmelzszenarium infolge Station Blackout (SBO), Abschlussbericht, GRS-473, September 2017.

/HAC 14/ Hacker, W., Sachse, P. (2014). Allgemeine Arbeitspsychologie: Psychische Regulation von Tätigkeiten (3. vollständig überarb. Aufl.). Göttingen: Hogrefe.

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

/KAE 16/ Korean Atomic Energy Research Institute: Application of the HUREX framework for collecting human error probabilities from the operation experience of domestic nuclear power plants – preliminary report, /KAE/TR-6474/2016.

/KLO 06/ Kloos M. and J. Peschke: MCDET – A Probabilistic Dynamics Method Combining Monte Carlo Simulation with the Discrete Dynamic Event Tree Approach, Nuclear Science and Engineering, 153, pp. 137 – 156 (2006).

/KLO 18/ Kloos M: Software for Uncertainty and Sensitivity Analyses – User's Guide and Tutorial (SUSA Version 4.1), GRS-P-5, Rev. 4, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Garching, 2018.

/LIA 09/ Liao, Y., S. Guentay: Potential steam generator tube rupture in the presence of severe accident thermal challenge and tube flaws due to foreign object wear, Nuclear Engineering and Design, 239, S. 1128 – 1135, 2009.

/LIU 12a/ Liu P, Li ZZ, Wang Z.: Task complexity measure for emergency operating procedures based on resource requirements in human information processing. In: 11th International Probabilistic Safety Assessment and Management Conference and the annual European Safety and Reliability Conference, Helsinki, Finland, 2012.

/LIU 12b/ Liu P. and Zhizhong Li.: “Task complexity: a review and conceptualization framework." International Journal of Industrial Ergonomics 42.6, 553 – 568, 2012.

/NEW 94/ Newell, A.: Unified Theory of Cognition, Cambridge (Mass.): Harvard University Press, 1994.

/PAR 09/ Park, J.: Complexity of Proceduralized Tasks (pp. 13 – 21), Springer London, 2009.

/PES 95/ Peschke J.: Methoden zur Gewinnung von Verteilungen für Zuverlässigkeitskenngrößen aus Vorinformationen und anlagenspezifischer Betriebserfahrung, GRS-A-2220, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Garching, Januar 1995.

/PES 06/ Peschke J., Kloos M., Fassmann W., Sonnenkalb M.: Methodenentwicklung für die Berücksichtigung menschlicher Eingriffe im Rahmen einer dynamischen PSA der Stufen 1 und 2, GRS, GRS-A-3340, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Garching, Juni 2006.

/PES 14/ Peschke J., Forell B., Hartung J., Preischl W.: Methodenentwicklung zur Analyse von Personalhandlungen im Rahmen probabilistischer Dynamikanalysen am Beispiel von Brandereignisabläufen mit Brandbekämpfung, GRS-331, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), ISBN 978-3-944161-11-2, Garching, Juni 2014.

/PET 14/ Petermeier, B.: Reisebericht über den Besuch des OECD Halden Reactor Projects Halden, Østfold Norwegen, 31. August – 05. September 2014, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Oktober 2014.

/RAS 83/ Rasmussen, J.: Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models, IEEE Transactions on Systems, Man, and Cybernetics, SMC-13, S. 257 – 266, 1983.

/SAI 93/ Studie von Saifert (1978), zitiert in Schmidtke, H.: Lehrbuch der Ergonomie, München: Hanser, S. 399, 1993.

/SON 01/ Sonnenkalb, M.: Unfallanalysen für DWR vom Typ KONVOI (GKN-2) mit dem Integralcode MELCOR 1.8.4, GRS-A-2954, Dezember 2001.

/SWA 83/ Swain, A. D., H. E. Guttmann: Handbook on Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, NUREG/CR-1278, August 1983.

/WES 87/ Weston, L. et al.: Recovery Actions in FRA for the Risk Methods integration and Evaluation Program (RMiEP), NUREG/CR-4834/1 and 2, Washington (DC): U. S. Nuclear Regulatory Commission, 1987.

/WHA 16/ Whaley, A. et al.: Cognitive Basis for Human Reliability Analysis, Washington (DC): U. S. Nuclear Regulatory Commission, 2016.

/ZED 10/ Zentrale Zuverlässigkeits- und Ereignisdatenbank: Zuverlässigkeitskenngrößen für Kernkraftwerkskomponenten, German; ISSN 1439-7498; ord.no. TW805-11, Juni 2010.

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AM	Analysemodul
DE-DrE	Dampferzeuger-Druckentlastung
DE-FH	Dampferzeuger-Füllhöhe
DEHEIRO	Dampferzeuger-Heizrohr
DET	Dynamischer Ereignisbaum
DH	Druckhalter
DH-AV	Druckhalter-Abblaseventil
DH-SiV	Druckhalter-Sicherheitsventil
DLL	shared library
EB	Ereignisbaum
EL1	1. Elektriker
EPR	European Pressurized Water Reactor
ET	E- und Leittechniker
FD	Frischdampfdruck
GBA	Gebäudeabschlussarmatur
GVA	Gemeinsam verursachter Ausfall
HDF	Hierarchisches Datenformat
HKL	Hauptkühlmittelleitung
HL	Handlungsliste
HRP	Halden Reactor Project
IDPSA	Integrale deterministisch-probabilistische Sicherheitsanalyse
IPC	Kommunikationskanal
KMV	Kühlmittelverlust
KTA	Kerntechnischer Ausschuss
LF	Leitstandfahrer
MCDET	Monte Carlo Dynamic Event Tree
PDE	Primärseitiges Druckentlasten
PM	Probabilistikmodul
PSA	Probabilistische Sicherheitsanalyse
ReakF	Reaktorfahrer (auch RF)
RESA	Reaktorschnellabschaltung
SBO	Station Black Out
SDE	Sekundärseitiges Druckentlasten
SHB	Sicherheitsbehälter (auch SB)
Sim	Simulator
SK	Schädigungsklasse
SL-SV	Schichtleiter-Stellvertreter (auch SLVM oder SLV)
VAL	Volumenausgleichsleitung

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
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

ISBN 978-3-947685-05-9