

**Einsatz dynamischer
Simulationsmethoden für
die Analyse von
Notfallmaßnahmen bei
erschwerenden
Randbedingungen
infolge übergreifender
Einwirkungen**

**Methodische Erweiterung
bestehender PSA
unter Berücksichtigung
spezieller Anforderungen
aus übergreifenden
Einwirkungen**

**Einsatz dynamischer
Simulationsmethoden für
die Analyse von
Notfallmaßnahmen bei
erschwerenden
Randbedingungen
infolge übergreifender
Einwirkungen**

**Abschlussbericht zum
Arbeitspaket AP 2**

Florian Berchtold
Werner Faßmann
Jörg Peschke
Marina Röwekamp

September 2021

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit (BMU) unter dem Förderkennzeichen 4718R01500 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMU übereinstimmen.

Deskriptoren

Crew-Modul, dynamische PSA, MCDET, menschliche Handlungen, Probabilistische Sicherheitsanalyse (PSA),
übergreifende Einwirkungen, Unsicherheiten

Kurzfassung

In der GRS wurden in den letzten Jahren fortschrittliche Methoden zur dynamischen PSA entwickelt, die mittlerweile für Anwendungen zur Verfügung stehen. Methoden der dynamischen PSA können eingesetzt werden, um zeitabhängige Wechselwirkungen zwischen Prozessablauf, menschlichen Handlungen und stochastischen Einflüssen umfassender mit einem höheren Detaillierungsgrad modellieren und analysieren zu können, als dies mit den Methoden der konventionellen PSA möglich ist. Solche Wechselwirkungen sind insbesondere auch bei Ereignissen infolge übergreifender Einwirkungen zu erwarten, bei denen Notfallmaßnahmen durch das Anlagenpersonal oftmals unter erschwerten Randbedingungen durchzuführen sind.

In diesem Vorhaben werden die bei der GRS entwickelten fortschrittlichen Methoden zur dynamischen PSA (MCDET und Crew-Modul) bei einer Untersuchung der Wirksamkeit von Notfallmaßnahmen unter erschwerten Randbedingungen angewendet, wobei Abhängigkeiten und zufällige Einflussgrößen auf den Handlungsablauf berücksichtigt werden. Bei dem zu analysierenden Szenario handelt es sich um ein Überflutungsereignis, welches zeitgleich zur übergreifenden Einwirkung eines anlageninternen Brandereignisses im Reaktorgebäude-Ringraum stattfindet. Es wurde dabei unterstellt, dass der Brand in einem Kabelschacht des Reaktorgebäude-Ringraums ausbricht und während der Löscharbeiten eine Leckage in der Feuerlöschwasserleitung auftritt, wodurch die Einspeisung von Löschwasser zur Brandbekämpfung unterbrochen wird. Die erschwerende Randbedingung für den Löschvorgang besteht in der mehr oder minder großen Verzögerung der Löscharbeiten durch die Dauer und den Erfolg der Erkennung, Lokalisierung und Absperrung des Lecks.

Mittels der durchgeführten dynamischen PSA konnte demonstriert werden, wie ein komplexer Handlungsablauf unter Berücksichtigung verschiedener unsicherer Einflussgrößen und Abhängigkeiten modelliert und analysiert werden kann. Außerdem wurde durch die Untersuchungen gezeigt, dass es mit den GRS-Methoden zur dynamischen PSA möglich ist, die Auswirkung stochastischer Einflussfaktoren auf die Zeiten zu quantifizieren, zu denen relevante Handlungen für den Prozessablauf durchgeführt werden. Damit können Einflussfaktoren identifiziert werden – auch diejenigen, die mit nur sehr geringer Wahrscheinlichkeit auftreten, bei denen die Ausführungszeiten wichtiger Handlungen signifikant verzögert sind. Zeitliche Verzögerungen können dann einen sicherheitstechnisch relevanten Einfluss haben, wenn notwendige Handlungen nicht rechtzei-

tig ausgeführt werden und damit die Notfallmaßnahme nicht erfolgreich durchgeführt werden kann.

Der Kenntnisk Gewinn, der durch die probabilistischen Ergebnisse der dynamischen PSA erzielt wird, kann als Grundlage dafür verwendet werden, Maßnahmen zur Vermeidung solcher zeitlichen Verzögerungen zu entwickeln, womit sich die Sicherheit einer Anlage erhöhen lässt.

Summary

In the recent past, advanced methods for dynamic PSA have been developed by GRS: These methods are now available for applications. Dynamic PSA methods are used to model and analyse time-dependent interactions between the plant process, human actions and stochastic influences in a more detailed and comprehensive manner. This is not possible with the conventional PSA methodology. Such interactions may arise in event sequences induced by hazards, where emergency measures are carried out by plant personnel even under aggravated conditions.

In this project, the advanced methods for dynamic PSA developed by GRS have been applied to investigate the effectiveness of emergency measures under such aggravated conditions, where the influence of dependencies and uncertainties from stochastic parameters on human actions is considered in the time sequence. The scenario analysed is a fire event, during which an internal flooding from a leakage of the fire water supply in the reactor annulus is assumed. The scenario starts with a fire in a cable duct of the reactor annulus. During the firefighting activities, a break of the fire water supply pipe in the reactor annulus is postulated, interrupting the water supply needed for extinguishing the fire successfully. The aggravating condition for the extinguishing process is given through the delay of the fire fighting activities due to the time needed to stop the leakage.

The analyses performed have demonstrated how a human procedure can be modelled and analysed in detail applying dynamic PSA methods, where various uncertain influencing factors and dependencies have been taken into account. In addition, it has been shown that the probabilistic results derived from a dynamic PSA can be used to quantify the impact of stochastic influencing factors on times when relevant actions are carried out. This information can be used to identify influencing factors – even those that occur with only a very low probability – for which the execution times of such actions are significantly delayed. Time delays of necessary actions may present an impact important to safety if the actions are not carried out during the required time period with the result that the emergency measure is not successful.

In that way the probabilistic results of a dynamic PSA of emergency operating procedures can be used as a basis for developing measures to avoid such time delays and therefore can contribute to improve plant safety.

Inhaltsverzeichnis

	Kurzfassung	I
	Summary	III
	Inhaltsverzeichnis	V
1	Einführung	1
2	Zielsetzung und Arbeitsschritte	5
3	Überblick über den Stand von Wissenschaft und Technik	7
3.1	Überblick über die GRS-Methoden zur Durchführung einer dynamischen PSA	9
3.2	Modellierung von Personalhandlungen als dynamischer Ablauf.....	13
3.2.1	Motivation	13
3.2.2	Konzept des Crew-Moduls und Entwicklungsstand.....	16
3.2.3	Überblick der bisherigen Arbeiten zur dynamischen Analyse von Personalhandlungen.....	19
4	Festlegung eines zu analysierenden Szenarios	23
5	Beschreibung des Handlungsablaufs zur Beherrschung des Szenarios als Grundlage für eine dynamische Modellierung	29
5.1	Modellierung des Handlungsablaufs	30
5.1.1	Brandentstehung, -alarmierung und Vorbereitung des Löschvorgangs	31
5.1.2	Bruch der Feuerlöschleitung und Erkennung des Lecks in der Warte	33
5.1.3	Erkennung des Lecks im Reaktorgebäude-Ringraum durch die Feuerwehr	35
5.1.4	Absperrung der Streckenschieber und Gebäudeeintrittsschieber.....	35
5.1.5	Fortsetzung und erfolgreiche Beendigung der Löscharbeiten	36
5.2	Untersuchung des Handlungsablaufs auf menschliche Fehlermöglichkeiten.....	36
5.3	Quantifizierung der Zeitbedarfe der Handlungen	38

6	Modellierung des beschriebenen Handlungsablaufs zur dynamischen Analyse mit dem Crew-Modul.....	39
6.1	Beschreibung der berücksichtigten Unsicherheiten, Abhängigkeiten und Annahmen	39
6.1.1	Unsicherheit bzgl. der Wassereintrittsrates.....	39
6.1.2	Unsicherheit der Zeit, wann Überflutungsmeldung für den betroffenen Quadranten an der Reaktorschutztafel angezeigt wird.....	41
6.1.3	Unsicherheit bzgl. des akustischen Alarms zur Signalisierung eines Druckabfalls in der Feuerlöschwasserleitung	44
6.1.4	Unsicherheit bzgl. des Stressniveaus des Schichtleiter-Stellvertreters durch einen zusätzlichen Alarm	45
6.1.5	Unsicherheit bzgl. der Zeitdauern bis Anzeigen des Überflutungsalarms in Abhängigkeit des Stressniveaus bewertet werden	46
6.1.6	Verfügbarkeit des Werkzeugs vor Ort	49
6.1.7	Schließzuverlässigkeit des Streckenschiebers.....	49
6.2	Beschreibung des modellierten Handlungsablaufs für das Crew-Modul	49
6.3	Probabilistische Auswertung und Diskussion der Simulationsergebnisse.....	58
7	Zusammenfassung und Ausblick.....	79
	Literaturverzeichnis.....	85
	Abbildungsverzeichnis.....	89
	Tabellenverzeichnis.....	91
	Abkürzungsverzeichnis.....	93
A	Anhang: Beschreibung des Handlungsablaufs für eine dynamische PSA.....	95

1 Einführung

Nach den Reaktorunfällen von Fukushima Dai-ichi im Jahr 2011 haben internationale Diskussionen ebenso wie die Stresstests von Kernkraftwerken gezeigt, dass der Bedarf besteht, das Notfallschutzkonzept deutscher Kernkraftwerke dahingehend weiterzuentwickeln, dass die Wirksamkeit von Notfallmaßnahmen auch bei erschwerenden Randbedingungen durch einzelne, aber auch kombinierte übergreifende Einwirkungen von innen und außen gewährleistet bleibt.

Gegenstand einschlägiger Anpassungen und Weiterentwicklungen sind insbesondere die Methoden der probabilistischen Sicherheitsanalyse (PSA). Zur Durchführung von PSA wurden bisher fast ausschließlich die Methoden der konventionellen PSA verwendet, die im Wesentlichen durch die Anwendung der Fehler- und Ereignisbaumanalyse gekennzeichnet sind. Diese Methoden haben einen mehr oder weniger statischen Charakter, bei dem zeitabhängige Wechselwirkungen auf den zugrundeliegenden physikalischen Prozess – wenn überhaupt – nur sehr grob und vereinfacht berücksichtigt werden können.

In Ergänzung zur konventionellen PSA der Stufen 1 und 2 sind in den letzten Jahren vermehrt fortschrittliche Methoden der dynamischen PSA entwickelt worden, die mittlerweile für Anwendungen zur Verfügung stehen. Mit den dynamischen PSA-Methoden können zeitabhängige Wechselwirkungen zwischen Prozessablauf, menschlichen Handlungen und zufälligen Einflussgrößen wesentlich detaillierter und umfassender als mit den konventionellen PSA-Methoden modelliert und analysiert werden. Solche Wechselwirkungen sind insbesondere auch bei übergreifenden Ereignissen zu erwarten, bei denen Notfallmaßnahmen durch das Anlagenpersonal durchzuführen sind. Es ist daher sinnvoll und notwendig, dynamische Methoden auch für die Anwendung auf übergreifende Einwirkungen weiterzuentwickeln und zur Verfügung zu stellen, wenn die Beherrschung übergreifender Einwirkungen durch Notfallmaßnahmen genauer analysiert und bewertet werden soll, als es mit den konventionellen Methoden möglich ist.

Übergreifende Einwirkungen sind Einwirkungen von innen oder außen, die das Potenzial für redundanzübergreifende Ausfälle haben. Einwirkungen von innen resultieren aus Ereignissen auf dem Anlagengelände, innerhalb oder außerhalb von Gebäuden, wie z. B. Brände oder anlageninterne Überflutungen. Einwirkungen von außen treten außerhalb des Anlagengeländes auf, d. h. außerhalb des Zuständigkeitsbereiches des Anlagenbetreibers.

Einwirkungen von außen können durch Umgebungsbedingungen, Naturereignisse oder sonstige zivilisatorisch bedingte Ereignisse, wie z. B. Flugzeugabsturz, hervorgerufen werden.

Die erschwerenden Bedingungen, die bei übergreifenden Einwirkungen auftreten können, entstehen insbesondere dann, wenn mehrere übergreifende Einwirkungen in Kombinationen auftreten oder zu kaskadierenden Ereignisketten führen, deren Beherrschung das Personal vor besondere Herausforderungen stellt. Als Beispiel sei der Reaktorunfall von Fukushima genannt, der durch eine Kombination übergreifender Einwirkungen (Erdbeben und Tsunami) zu Ereignisketten mit Wasserstoffexplosionen sowie anlageninternen Bränden und Überflutungen geführt haben.

Solche übergreifenden Ereignisse sind durch vielfältige Abhängigkeiten und Wechselwirkungen im zeitlichen Ablauf sowie diverse stochastische Einflussfaktoren (als aleatorische Unsicherheiten bezeichnet) und Kenntnisstandunsicherheiten (als epistemischen Unsicherheiten bezeichnet) gekennzeichnet. Die Berücksichtigung solcher zeitabhängigen Wechselwirkungen und Abhängigkeiten in einer PSA erfordert fortschrittliche Methoden, mit denen sowohl der zeitliche Aspekt als auch die gegenseitigen Abhängigkeiten in einem Ereignisablauf genauer modelliert und analysiert werden können. Solche fortschrittlichen Methoden sind beispielsweise die in der GRS entwickelten Methoden zur dynamischen PSA:

- **MCDET** (*Monte Carlo Dynamic Event Tree*), welche in Verbindung mit einem deterministischen Rechencode einen physikalischen Prozess in Abhängigkeit verschiedener unsicherer Einflussgrößen und Wechselwirkungen simulieren kann. Dabei können beliebige stochastische (aleatorische) Einflussgrößen sowie epistemische Unsicherheiten in Abhängigkeit vom Prozesszustand in der Analyse berücksichtigt werden.
- **Crew-Modul** zur dynamischen Modellierung und Simulation menschlicher Handlungsabläufe. In Verbindung mit MCDET können die Handlungsabläufe in Abhängigkeit von stochastischen Einflüssen und Prozess- bzw. Systemzuständen modelliert und analysiert werden.

Das Crew-Modul in Verbindung mit MCDET soll in diesem Forschungs- und Entwicklungsvorhaben beispielhaft an einem Handlungsablauf angewendet werden, der unter erschwerten Randbedingungen für ein ausgewähltes Beispiel übergreifender Einwirkungen durchgeführt wird.

Zielsetzung und Arbeitsschritte der Arbeiten sind in Kapitel 2 erläutert. Ein kurzer Überblick über Stand von Wissenschaft und Technik der dynamischen PSA wird in Kapitel 3 gegeben. In Kapitel 4 erfolgt eine Beschreibung des ausgewählten Szenarios, welches durch eine Ereigniskombination von zwei übergreifenden Einwirkungen definiert ist. Eine Beschreibung des Handlungsablaufs sowie die Modellierung des Handlungsablaufs für das Crew-Modul finden sich in Kapitel 5. In Kapitel 6 sind einige Auswertungsbeispiele der Simulationsergebnisse dargestellt.

2 Zielsetzung und Arbeitsschritte

Aus den Diskussionen auf internationaler Ebene und den in Folge der Reaktorunfälle von Fukushima Dai-ichi im Jahr 2011 durchgeführten Stresstests für Kernkraftwerke, insbesondere auf europäischer Ebene, hat sich die Notwendigkeit für methodische Anpassungen und Weiterentwicklungen zur umfassenden Berücksichtigung übergreifender Einwirkungen (von innen wie außen) einschließlich Einwirkungskombinationen ergeben. Deshalb sollen die in Deutschland verfügbaren Methoden der PSA an den aktuellen Stand von Wissenschaft und Technik angepasst werden. Dabei besteht eine wesentliche Aufgabe in einem Einsatz dynamischer Simulationsmethoden für die Analyse von Notfallmaßnahmen bei erschwerenden Randbedingungen infolge übergreifender Einwirkungen.

Ziel der im Arbeitspaket AP 2 des BMU-Vorhabens 4718R01500 durchgeführten Arbeiten ist es, mittels der Methode MCDET für dynamische Probabilistische Sicherheitsanalysen (DPSA) die Wirksamkeit von Notfallmaßnahmen zu untersuchen, die das Personal unter erschwerenden Randbedingungen bei übergreifenden Einwirkungen von innen und bei ggf. zerstörter oder zumindest zeitweise unverfügbarer Infrastruktur durchzuführen hat. Die GRS-Methode zur DPSA soll in dieser Arbeit an einem beispielhaften Anwendungsfall demonstriert sowie deren zusätzlicher Nutzen gegenüber der klassischen PSA-Methodik diskutiert werden.

Die Notwendigkeit für den Einsatz dynamischer PSA-Methoden ergibt sich durch die vielfältigen zeitabhängigen Wechselwirkungen und Unsicherheiten, die einen menschlichen Handlungsablauf beeinflussen können. Dies gilt insbesondere dann, wenn sich für das Personal erschwerte Randbedingungen, u. a. bei einem Auftreten einer Ereigniskombination übergreifender Einwirkungen oder von kaskadierenden Ereignisketten ergeben.

Eine wesentliche Aufgabe besteht dabei darin, die in der GRS entwickelten fortschrittlichen Methoden zur dynamischen PSA bei einer Untersuchung der Wirksamkeit von Notfallmaßnahmen unter erschwerten Randbedingungen infolge übergreifender Einwirkungen anzuwenden. Diese Methoden erlauben es, für menschliche Handlungsabläufe kontextbezogene Abhängigkeiten sowie den Einfluss zufälliger Größen (d. h. aleatorischer Unsicherheiten) auf den Handlungsablauf im zeitlichen Ablauf des Ereignisses simulieren und bewerten zu können.

Die Informationen, die aus solchen Untersuchungen gewonnen werden, können zur sicherheitstechnischen Bewertung eines Kernkraftwerkes herangezogen werden.

Zur Erreichung der vorgenannten Zielsetzung wurden die nachfolgend aufgeführten Arbeitsschritte durchgeführt:

- Kurzer Überblick über den einschlägigen Stand von Wissenschaft und Technik;
- Festlegung eines Szenarios für übergreifende Einwirkungen und Ermittlung der Randbedingungen, welche die Bewältigung des Szenarios erschweren;
- Spezifikation der zu berücksichtigenden Unsicherheiten und Abhängigkeiten bzgl. des zu analysierenden Handlungsablaufs.
- Modellierung des Handlungsablaufs als dynamischer Prozess unter Berücksichtigung der spezifizierten Unsicherheiten.
- Kopplung des Crew-Moduls mit MCDET zur Simulation der Handlungsabläufe unter Berücksichtigung der spezifizierten stochastischen Einflussgrößen und Abhängigkeiten.
- Auswertung der Simulationsergebnisse und Beurteilung der Wirksamkeit der betrachteten Notfallmaßnahme für das zugrunde gelegte Szenario mit seinen zeitlich veränderlichen Randbedingungen für eine exemplarisch ausgewählte Referenzanlage in Deutschland und Quantifizierung der Sicherheit dieser Beurteilung.

Nachfolgend sind die Arbeiten und Ergebnisse zu diesen Einzelzielsetzungen kapitelweise dokumentiert. Ein Schlusskapitel fasst die gewonnenen Erkenntnisse und die erreichten Erkenntnisfortschritte zusammen.

3 Überblick über den Stand von Wissenschaft und Technik

Methoden für die dynamische probabilistische Sicherheitsanalyse finden weltweit zunehmendes Interesse. Das zeigen einschlägige Entwicklungsarbeiten, Publikationen und Fachkonferenzen (wie u. a. ESREL, PSAM und ANS PSA) ebenso wie internationale Workshops (z. B. Workshop zur IDPSA – Integrated Deterministic Probabilistic Safety Assessment an der Royal Institute of Technology (KTH) in Stockholm, Schweden, 2012) /ADO 12/). Das Interesse an fortschrittlichen Methoden zur dynamischen PSA (DPSA) besteht im Wesentlichen darin, die zeitabhängigen Wechselwirkungen, die zwischen Prozessablauf, menschlichen Handlungen und zufälligen Einflussgrößen stattfinden, realitätsnäher modellieren und analysieren können.

Seitens der Working Group on Risk Assessment (WGRISK) des OECD Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) wurde im Herbst 2019 eine Aktivität mit dem Titel „Dynamic PSA – Preparing for the Future“ /NEA 19/ initiiert. Ziel dabei ist es, die künftige Rolle der dynamischen PSA für probabilistische Sicherheits- und Risikoanalysen, sowie die zu deren Durchführung entwickelten Methoden und Werkzeuge einzuschätzen und zu bewerten. Weiterhin sollen Probleme identifiziert werden, die bei der Durchführung einer dynamischen PSA auftreten, und Möglichkeiten erarbeitet werden, wie man solchen Herausforderungen begegnen kann.

Bei der Vielzahl von Veröffentlichungen zum Thema dynamische PSA fällt auf, dass die angewendeten Methoden erhebliche Unterschiede aufweisen. Viele Anwendungen erfolgen über sogenannte Zustandsmodelle wie z. B. Markov-Modelle oder Petri-Netze. Obwohl solche Modelle eine gewisse Berücksichtigung des Zeitfaktors erlauben, ist ihr Anwendungsspektrum aufgrund des bei zunehmender Anzahl von Systemkomponenten exponentiell anwachsenden Zustandsraumes auf kleinere Systeme begrenzt. Außerdem kann das zeitabhängige Verhalten von Prozessgrößen kaum bzw. nur grob modelliert werden.

Wesentlich leistungsfähiger sind diejenigen Werkzeuge, die auf der dynamischen Ereignisbaum-Methode (Englisch: Dynamic Event Tree, DET) basieren und die mit einem deterministischen Rechencode gekoppelt werden können. Neben den in der GRS entwickelten Werkzeugen, die die dynamische Ereignisbaummethode anwenden, sind aus der Literatur u. a. die Werkzeuge ADS-IDAC /CHA 07/, ADAPT /OSB 18/, RAVEN /RAB 14/ und SCAIS /IZQ 08/ zu nennen. Diese sind neben MCDET ebenfalls sehr mächtige Werkzeuge, die zur Analyse von komplexen Prozessen verwendet werden können.

In der GRS wurde 2001 mit der Entwicklung der Methode MCDET begonnen, die auf einer Kombination von Monte-Carlo-Simulation und dynamischer Ereignisbaum-Methode basiert. Eine kurze Beschreibung von MCDET findet sich nachfolgend in Abschnitt 3.1. Durch die Kopplung von MCDET mit einem deterministischen Rechenprogramm werden die Unsicherheiten, die unter definierten Prozessbedingungen entstehen, unmittelbar zum Zeitpunkt ihres Auftretens in das deterministische Programm eingelesen und für den weiteren Simulationsablauf berücksichtigt. Durch diese Eigenschaft von MCDET wird die Durchführung einer sogenannten integralen deterministisch-probabilistischen Sicherheitsanalyse (IDPSA) ermöglicht. Die Methoden, die für eine IDPSA eingesetzt werden können, nutzen in großem Umfang die in einer deterministischen Sicherheitsanalyse angewendeten Simulationscodes und wenden probabilistische Verfahren an, um die Einflüsse epistemischer wie insbesondere aleatorischer Unsicherheiten auf das simulierte Systemverhalten umfassender und detaillierter zu berücksichtigen, als dies mit anderen Methoden möglich ist.

Ein vergleichbares Werkzeug zu MCDET, das in den USA von der Ohio State University (OSU) in Zusammenarbeit mit Sandia National Laboratories (SNL) mit Unterstützung der U.S. NRC entwickelt wurde, ist ADAPT (*Analysis of Dynamic Accident Progression Trees*) /OSB 18/, mit welchem ebenfalls eine IDPSA durchgeführt werden kann. Der methodische Unterschied zwischen ADAPT und MCDET besteht im Wesentlichen darin, dass bei ADAPT eine Diskretisierung stetiger Einflussgrößen vorgenommen wird, während MCDET den Einfluss stetiger Zufallsgrößen über eine Monte-Carlo-Simulation und Erzeugung einer Stichprobe von dynamischen Ereignisbäumen ermittelt. Die von der GRS entwickelte und angewendete Methodik hat den Vorteil, dass zur Auswertung der Daten, die aus einer MCDET-Analyse gewonnen werden, das gesamte statistische Instrumentarium zur Datenanalyse verwendet werden kann. Bei einer künstlichen Diskretisierung der stetigen Einflussgrößen oder einem sogenannten „Importance Sampling“-Verfahren ist dies nicht ohne weiteres möglich.

Im Vorhaben RS1148 des BMWi wurde begonnen, das Analysewerkzeug MCDET um das Crew-Modul /PES 06/ zu erweitern. Das Ziel dieser Entwicklung bestand darin, menschliche Handlungen als dynamische Abläufe unter Berücksichtigung von Unsicherheiten und Abhängigkeiten von Prozess- und Systemzuständen modellieren und simulieren zu können. Das Crew-Modul wurde bereits für einige Anwendungen, in denen menschliche Handlungsabläufe im Rahmen einer dynamischen PSA analysiert wurden, erfolgreich eingesetzt, so z. B. zur Modellierung von Brandbekämpfungsmaßnahmen in einem Brandszenario /PES 14/.

3.1 Überblick über die GRS-Methoden zur Durchführung einer dynamischen PSA

Ausgehend von einem auslösenden Ereignis, entwickeln sich die in einer probabilistischen Sicherheitsanalyse (PSA) zu untersuchenden Unfallabläufe durch die Wechselwirkung zwischen Prozess- und Systemdynamik, menschlichen Handlungen und stochastischen Einflussgrößen im zeitlichen Ablauf. Stochastische Einflüsse (aleatorische Unsicherheiten) verursachen Veränderungen in den Systembedingungen, die jeweils unterschiedliche Auswirkungen auf den weiteren Prozessablauf haben. Umgekehrt können jedoch auch Prozesszustände einen Einfluss auf das stochastische Verhalten verschiedener Größen haben. So kann beispielsweise ein Temperaturanstieg über eine kritische Grenze hinaus ein erhöhtes Ausfallverhalten bestimmter Komponenten verursachen. In diesem Fall müsste die Ausfallrate einer Komponente in Abhängigkeit der aktuell vorherrschenden Temperatur modelliert werden. Diese gegenseitigen Abhängigkeiten zwischen Prozesszustand und stochastischen Einflussgrößen werden als Dynamik-Stochastik-Wechselwirkungen bezeichnet.

Um die Einflüsse und Wechselwirkungen möglichst realitätsnah im zeitlichen Ablauf modellieren und analysieren zu können, hat die GRS im Forschungs- und Entwicklungsvorhaben RS111 des BMWi /HOF 01/ damit begonnen, die Methode MCDET und das gleichnamige Werkzeug zur Durchführung probabilistischer Dynamikanalysen (dynamische PSA, kurz DPSA) zu entwickeln. Die Methode MCDET basiert im Wesentlichen auf einer Kombination von Monte-Carlo-Simulation und der Methode der dynamischen Ereignisbaumanalyse.

In der herkömmlichen Ereignisbaumanalyse, die in der konventionellen PSA der Stufen 1 und Stufe 2 durchgeführt werden, geben die Analysten die zu betrachtenden Ereignisse und ihre Reihenfolge ohne Angabe von Zeitpunkten und zeitlichen Abständen vor. D. h., die Ereignisse werden ausschließlich entlang einer sogenannten Wirkungslinie ohne Zeitachse beschrieben. Für die Analyse ergeben sich daraus mehr oder weniger einschneidende Einschränkungen, die die Gefahr in sich bergen, dass wichtige Abläufe, die sich aus den zeitlichen Details und der Reihenfolge von Ereignissen ergeben, nicht erkannt werden.

Im Gegensatz dazu entwickelt sich ein dynamischer Ereignisbaum (DET) mit der Methode MCDET automatisch durch die zeitlichen Einflüsse und Wechselwirkungen des dynamischen Prozesses mit den berücksichtigten unsicheren Einflussfaktoren. Diese organisieren die Simulation der Ablaufmöglichkeiten eines Unfallszenarios entsprechend der Struktur eines Ereignisbaums, allerdings mit dem wesentlichen Unterschied, dass die Zeitpunkte, wann die Verzweigungen von Ereignissen und in welcher Reihenfolge die Ereignisse stattfinden, explizit in

einem DET angegeben werden und zwischen verschiedenen DET variieren. Alle Verzweigungen in einem DET – auch die mit geringer Wahrscheinlichkeit – können systematisch berücksichtigt und berechnet werden.

Die dynamische Ereignisbaum-Methode hat folgende Vorteile:

- Um Ereigniskombinationen, die nur mit einer geringen Wahrscheinlichkeit auftreten, probabilistisch adäquat bewerten zu können, würde unter Verwendung einer Monte-Carlo-Simulation eine sehr hohe Anzahl von Rechenläufen benötigt, damit die Stichprobe von Rechenläufen solche Ereigniskombinationen enthält. Mit der dynamischen Ereignisbaum-Methode kann der Rechenaufwand erheblich reduziert werden, da diskrete Ereignisse mit ihren Wahrscheinlichkeiten explizit angegeben werden können und daraus alle möglichen Ereigniskombinationen gerechnet und probabilistisch bewertet werden.
- Die im Allgemeinen aufwändigen Dynamikrechnungen brauchen nicht von Anfang an gerechnet werden, sondern setzen an den entsprechenden Verzweigungspunkten auf, um die Rechnungen fortzusetzen. Damit können wiederholte Berechnungen identischer Unfallsituationen, die in unterschiedlichen Abläufen vorkommen, vermieden werden, wodurch eine erhebliche Rechenzeiterparnis erreicht werden kann.
- Dynamische Ereignisbäume enthalten gegenüber den klassischen Ereignisbäumen zusätzliche Informationen darüber, wann und in welcher Reihenfolge Ereignisse auftreten, die den weiteren Prozessablauf beeinflussen.

Durch die Kopplung von MCDET mit einem deterministischen Rechenprogramm werden für alle Verzweigungen und Ereigniskombinationen, die in einem DET erzeugt werden, die jeweiligen Prozessabläufe ermittelt. Damit lassen sich die jeweiligen Einflüsse der aleatorischen Unsicherheiten auf den Prozessablauf explizit ermitteln. Des Weiteren wird für jede Ereignissequenz, die in einem DET erzeugt wird, die entsprechende Eintrittswahrscheinlichkeit durch Multiplikation der in einer Sequenz vorkommenden Ereigniswahrscheinlichkeiten berechnet.

Mit der Methode MCDET werden die stochastischen Einflussgrößen, die durch eine diskrete Wahrscheinlichkeitsverteilung definiert sind, in einem DET systematisch berücksichtigt. Dabei werden alle möglichen Kombinationen von diskreten Verzweigungen in der Analyse gerechnet und probabilistisch bewertet.

Sofern allerdings stochastische Einflussfaktoren berücksichtigt werden, für die eine stetige Wahrscheinlichkeitsverteilung vorliegt, bietet die DET-Methode allein keine befriedigende Lösung an, da in diesem Fall die Anzahl der Verzweigungen und die damit verbundenen, zu

rechnenden Prozessabläufe exponentiell ansteigen würden. Der damit verbundene Rechenaufwand wäre nicht mehr praktikabel. Dieses Problem wurde durch die Methode MCDET gelöst, indem eine Stichprobe von dynamischen Ereignisbäumen (DETs) erzeugt wird, wobei die Variation der stetigen Größen über die Stichprobe der DETs erfasst wird. D. h., die stetigen aleatorischen Unsicherheiten werden näherungsweise über Monte-Carlo Simulationen erfasst und über die Stichprobe der DETs in der MCDET-Analyse berücksichtigt.

Das Ergebnis einer MCDET-Analyse ist somit eine Stichprobe von dynamischen Ereignisbäumen, aus der zu jedem Zeitpunkt Wahrscheinlichkeitsangaben zu Schadenszuständen sowie zu vielen anderen Fragestellungen bzgl. des Unfallablaufs abgeleitet werden können. Zusätzlich können aus einer MCDET-Analyse auch quantitative Angaben zum Einfluss des Stichprobenfehlers aus der Monte-Carlo-Simulation ermittelt werden.

Erste Anwendungen von MCDET haben gezeigt, dass die zeitabhängigen Wechselwirkungen zwischen einem durch ein deterministisches Rechenprogramm simulierten dynamischen Prozess und stochastischen Einflussfaktoren sehr detailliert und umfassend modelliert und analysiert werden können /KLO 06/. Bei diesen Anwendungen wurde jedoch deutlich, dass für die dynamische Analyse menschlicher Handlungsabläufe eine Methode fehlte, mit der menschliche Handlungen als dynamische Abläufe modelliert und simuliert werden konnten.

Im Forschungs- und Entwicklungsvorhaben RS1148 wurde mit der Entwicklung einer Methode zur dynamischen Modellierung und Simulation menschlicher Handlungsabläufe begonnen /PES 06/. Das dazu entwickelte Werkzeug wird als Crew-Modul bezeichnet, welches in Verbindung mit MCDET menschliche Handlungsabläufe unter Berücksichtigung stochastischer Einflüsse und in Abhängigkeit von System- und Prozesszuständen simulieren kann.

Die Zielsetzung des in der GRS entwickelten Crew-Moduls besteht darin, menschliche Handlungen als dynamischen Ablauf so modellieren zu können, dass

- die Zusammenarbeit und Kommunikation des beteiligten Personals,
- zufällige Schwankungen der Reaktions- und Handlungszeiten bei der Ausführung einzelner Handlungen sowie
- die Einbindung stochastischer Einflussgrößen, die sich auf die Ausführung der Handlungen auswirken können sowie Abhängigkeiten des Handlungsablaufs von Prozess- und Systemzuständen

in der Analyse berücksichtigt werden können.

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.

Beide Werkzeuge, MCDET wie das Crew-Modul, sind bereits erfolgreich erprobt und eingesetzt worden, u. a. im Vorhaben RS1198 für das Beispiel einer Brandbekämpfungsmaßnahme in einem Brandszenario /PES 14/. In dieser Analyse wurde MCDET zusammen mit dem deterministischen dreidimensionalen CFD Computational Fluid Dynamics-Code für Brandsimulationen FDS (*Fire Dynamics Simulator*) eingesetzt. Das Crew-Modul wurde dabei zur Modellierung der Brandbekämpfungsmaßnahme verwendet, um die aleatorische Unsicherheit bzgl. der Zeit zu bestimmen, wann relevante Aktionen (z. B. Zeitpunkt des Beginns der Brandbekämpfung oder Zeitpunkt, zu welchem ein Brandläufer oder die Löschgruppe den Brandraum erreichen) in Bezug auf die Brandbekämpfung durchgeführt werden. Die aleatorischen Unsicherheiten, wann bestimmte Handlungen durch das Personal ausgeführt werden, wurden mittels MCDET in den Simulationen des Brandszenarios berücksichtigt. Anhand der Ergebnisse aus der MCDET-Analyse konnte dann u. a. untersucht werden, welchen Einfluss der Zeitpunkt von Handlungsausführungen auf den Prozessablauf des Brandes hat.

Das Modell der Brandbekämpfungsmaßnahme wurde den Arbeiten im Arbeitspaket AP 3 des BMU-Vorhabens 4715R01575 zugrunde gelegt, um den Faktor Stress als dynamische Größe im Handlungsmodell der Brandbekämpfungsmaßnahme zu modellieren. Mit dem erweiterten Modell ist es möglich, zum einen den Faktor Stress als dynamische Größe im Handlungsablauf zu berücksichtigen und zum anderen die Auswirkung des Faktors Stress auf den Erfolg der Brandbekämpfungsmaßnahme zu quantifizieren. Durch die Erweiterung des Modells um den Faktor Stress konnte demonstriert werden, wie flexibel die Modellierung einer Handlungsmaßnahme unter Verwendung des Crew-Moduls gestaltet werden kann.

Im Vorhaben RS1529 /PES 18/ wurde ein methodischer Ansatz entwickelt, mit dem wissensbasierte Handlungen als dynamischer Ablauf unter Verwendung des Crew-Moduls modelliert werden können. Außerdem wurde das Crew-Modul in diesem Vorhaben weiterentwickelt, um die Modellierung und Erstellung des Eingabedatensatzes für das Crew-Modul einfacher und benutzerfreundlicher zu gestalten. Die Entwicklungen zur dynamischen Modellierung wissensbasierter Handlungen wurden an einem Precursor-Ereignis eines Kühlmittelverluststörfalls

(Loss of Coolant Accident, LOCA) aus der Betriebserfahrung in Deutschland erfolgreich erprobt. Für das Anwendungsbeispiel wurde ein meldepflichtiges Ereignis ausgewählt, welches in einem inzwischen im Rückbau befindlichen deutschen Reaktor aufgetreten war.

Mit MCDET und dem Crew-Modul stehen damit methodische Ansätze zur Verfügung, die in diesem Vorhaben für Ereignisszenarien unter erschwerenden Randbedingungen durch übergreifende Einwirkungen von außen anzuwenden und ggf. anzupassen bzw. zu erweitern sind.

3.2 Modellierung von Personalhandlungen als dynamischer Ablauf

3.2.1 Motivation

Menschliche Handlungsabläufe sind oftmals durch sehr komplexe dynamische Abläufe gekennzeichnet, die durch verschiedene aleatorische Unsicherheiten und Abhängigkeiten von System- und Prozesszuständen beeinflusst werden können. Dies gilt nicht nur dann, wenn wissensbasiertes Handeln erforderlich ist und die Handlungen maßgeblich von den Bedingungen in der Anlage und Prozessinformationen abhängen, sondern auch dann, wenn die Handlungen einer Notfallmaßnahme regelbasiert sind.

Weltweit wird intensiv an der Entwicklung von Methoden für die Analyse und Bewertung wissensbasierter Handlungen gearbeitet /FAS 10/. Die GRS hat dazu ebenfalls einschlägige Methoden vorgelegt /FAS 03/, /FAS 10/. Für alle diese Methoden gilt, dass ihr Anwendungsbereich bisher auf die klassische (nicht-dynamische) PSA beschränkt ist. Viele methodische Ansätze sehen zudem nur eine globale Expertenschätzung vor, um den Beitrag wissensbasierten Handelns zu quantifizieren. Die dynamische PSA beginnt gerade erst, kognitive Faktoren, wie z. B. das Gedächtnis, einzubeziehen, die für wissensbasiertes Handeln zwar notwendig, aber nicht konstitutiv sind (z. B. /LIU 12/, /MOH 12/).

Die Bewältigung von Ereignisabläufen hängt entscheidend von den Wechselwirkungen zwischen System- und Prozesszuständen, Personalhandlungen und den stochastischen Eigenschaften der Zuverlässigkeit relevanter technischer Einrichtungen und menschlicher Handlungen ab:

- Technische Ausfälle durch Einwirkungen von innen sowie von außen treten mit einer bestimmten Wahrscheinlichkeit auf. Ihre Beherrschung erfordert innerhalb eines mehr oder minder engen Zeitfensters automatische Aktionen und (oder) Handlungen des Personals. Ausfälle und Beeinträchtigungen können auch die Systeme und die Infrastruktur betreffen,

die zur Bewältigung eines Ereignisablaufs und die Durchführung der Personalhandlungen verfügbar sein muss. Das Ausfallverhalten technischer Einrichtungen unterliegt mehr oder minder großen zufälligen Schwankungen, die für das Handeln des Personals relevant sein können: Frühe Ausfallzeitpunkte lassen für Reparaturen oder Ersatzmaßnahmen mehr Zeit als späte, auch können der Ausfallzeitpunkt, die Art des Ausfalls und die Ausfallfolgen korrelieren. Man denke zum Beispiel an ein Leck, das in einem druckführenden System zufällig auftritt, nachdem letzteres unterschiedlich lange in Betrieb war und wenn Durchsatz, Temperatur und Druck des Mediums im System von der Betriebsdauer abhängen. Daraus können sich sehr unterschiedliche Herausforderungen an das Personal ergeben, das mit der Abdichtung des Lecks beauftragt wird.

Die Zuverlässigkeit menschlichen Handelns unterliegt stochastischen Effekten: Mit einer bestimmten Wahrscheinlichkeit können erforderliche Handlungen unterbleiben oder so erfolgen, dass ihre Ausführung in unzulässiger Weise von sicherheitstechnischen Anforderungen und Sollvorgaben abweicht. Es sind auch Handlungen, wie z. B. die Wartung und Instandhaltung, vor Ereigniseintritt zu berücksichtigen, die sich auf die Verfügbarkeit benötigter Einrichtungen und Infrastrukturen auswirken können. Mit einer bestimmten Wahrscheinlichkeit können auch Fehler in Form schädlicher Eingriffe auftreten, die das Personal aufgrund von Denk- und Urteilsfehlern für zulässig oder notwendig hält, um den Ereignisablauf zu beenden oder so zu beeinflussen, dass schädliche Auswirkungen auf die Anlage, Menschen, und/oder Umwelt abgemildert werden. Das Personal kann aber auch ad hoc mit einer bestimmten Wahrscheinlichkeit wissensbasiert Vorgehensweisen finden, die das Ende oder eine Abmilderung des Ereignisablaufs bewirken. „Wissensbasiert“ bedeutet, dass diese Anwendungsmöglichkeit der betreffenden Vorgehensweise weder im Training noch in den Prozeduren vorgesehen ist, die das Personal absolviert beziehungsweise zur Verfügung hat und die ein regelbasiertes Vorgehen ermöglichen. Fehler können mit einer bestimmten Wahrscheinlichkeit erkannt und behoben werden.

- Die Zuverlässigkeit der regel- und wissensbasierten Handlungen einschließlich solcher der Erkennung und Behebung von Fehlern hängt von Faktoren ab, die sich auf die Leistung des Menschen auswirken. Dazu zählen Stressauslöser (Stressoren). Zu denken sind an Zeitdruck, Unübersichtlichkeit und Unvorhersehbarkeit des Ereignisablaufs, Gefahren für Leib und Leben, der Verantwortungsdruck, der mit der Aufgabe einhergeht, einen sicheren Zustand wiederherzustellen, sowie an Ängste, an dieser Aufgabe zu scheitern.
- Leistungsrelevant sind auch organisatorische Faktoren, insbesondere die Verfügbarkeit des erforderlichen Personals und der benötigten materiellen Ressourcen: Zu bestimmten Tages- und Wochenzeiten kann alles erforderliche Personal auf der Anlage anwesend

sein, zu anderen Zeiten müssen Rufbereitschaften und (oder) Mitglieder externer Organisationen auf die Anlage geholt werden, um genügend viele, qualifizierte Personen für die anstehenden Aufgaben zur Verfügung zu haben. Vergleichbares gilt für materielle Ressourcen wie etwa Ersatzteile oder Geräte, die auf der Anlage vorrätig sein können oder erst herbeigeschafft werden müssen. Es liegt auf der Hand, dass sich die Verfügbarkeit personeller und materieller Ressourcen unmittelbar auf den Zeitablauf des Handelns und der Ereignisbewältigung auswirkt. Eine dritte Gruppe leistungsbestimmender Faktoren umfasst die verfügbaren Arbeitsmittel und gegebenen Arbeitsbedingungen, die eine korrekte Durchführung anstehender Handlungen unterstützen, beeinträchtigen oder sogar verhindern können. Arbeitsmittel sind die Informations- und Bedieneinrichtungen innerhalb und außerhalb der Warte, die Dokumente mit handlungsrelevanten Informationen, wie z. B. Betriebs- und Notfallhandbuch, sowie alle Geräte und Werkzeuge, die das Personal im Handlungsablauf nutzt. Arbeitsbedingungen sind insbesondere die Sichtverhältnisse, Geräuschpegel, Temperaturen und Beaufschlagungen des Arbeitsortes bzw. des Arbeitsweges mit radioaktiven oder sonstigen Substanzen. Es gibt im Regelwerk und der sonstigen Fachliteratur einen umfangreichen Erkenntnisstand, wie diese Faktoren für den Menschen bestmöglich gestaltet sein sollten und welche Einbußen die Handlungszuverlässigkeit bei Abweichungen von optimalen Ausprägungen dieser Faktoren erleidet. Die Wirkung auf den Handlungs- und Ereignisablauf hängt wesentlich auch davon ab, inwieweit die Arbeitsmittel unter den vorliegenden Rahmenbedingungen nutzbar sind und ihre Funktion erfüllen können bzw. Arbeitsmittel und Arbeitsorte zugänglich sind. Man denke beispielsweise an die Unverfügbarkeit der Warte, Ausfälle von Mess- und Bedieneinrichtungen oder eingeschränkte bzw. blockierte Zugänge zu Räumen, in denen notwendige Arbeiten auszuführen sind. Letzte, leistungsbestimmende Faktoren sind Fachwissen und Erfahrung, von denen es abhängt, inwieweit das Handeln regel- beziehungsweise wissensbasiert erfolgen kann.

- Zuverlässigkeit, Zeitpunkt und Zeitbedarf für die Personalhandlungen wirken ihrerseits auf den Ereignisablauf und dessen Dynamik zurück: richtiges oder falsches Handeln haben mehr oder minder gravierende Folgen für den Zustand der Anlage beziehungsweise die nachfolgenden Handlungen. Man denke z. B. an Erfolg oder Misserfolg der Erhaltung oder Wiederherstellung sicherheitstechnisch wichtiger Grenzwerte, der Reparatur eines benötigten Systems oder der Zufuhr benötigter Ressourcen. Für Erfolg oder Misserfolg solcher Aktionen kommt es wesentlich auf den Zeitpunkt und die Dauer der betreffenden Aktionen an. Erfolgt eine Aktion zu spät oder dauert ihre Ausführung zu lange, um ihre Wirkung rechtzeitig zu entfalten, fällt diese Handlung unter die Unterlassungsfehler. Erfolgt sie zu früh oder überhastet, kann sie als Ausführungsfehler nachteilige Folgen nach sich ziehen.

Beispiele hierfür sind das vorzeitige Starten von Pumpen, welches bei unzureichender Zufuhr des zu fördernden Mediums zur Kavitation führen kann, sowie ein Komponentenversagen bei manuell eingestellten unzulässig hohen Druck- oder Temperaturgradienten beim Befüllen einer Komponente. Insbesondere bei hochdynamischen Prozessen kann es auch wesentlich auf die stochastischen Variationen ankommen, die den Zeitpunkt und die Dauer der einzelnen Aktionen betreffen und dem menschlichen Handeln intrinsisch sind. Man muss stets damit rechnen, dass es kleinere oder größere Schwankungen zufälliger Art gibt, wann genau eine Person eine Handlung beginnt und wie lange sie für die Ausführung braucht. Die Berücksichtigung solcher Schwankungen ist wichtig, weil sie zusammen zu erheblichen oder sogar unzulässigen Verzögerungen des Handlungsablaufs, Zeitdruck und Stress führen können.

Das Crew-Modul in Verbindung mit MCDET unterstützt die Modellierung, Analyse und Bewertung von Ereignis- und Handlungsabläufen, deren Dynamik durch die vorgenannten drei Punkte beschrieben ist.

3.2.2 Konzept des Crew-Moduls und Entwicklungsstand

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 (sogeannter Basishandlungen) 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. Ausführungszeiten von Basishandlungen können demzufolge Zufallsgrößen sein, die einer aleatorischen Unsicherheit unterliegen.
- Bei der Ausführung menschlicher Maßnahmen sind oftmals mehrere Individuen beteiligt, die miteinander kommunizieren. Durch die Kommunikation werden Informationen über den Zustand des Handlungsablaufs (und ggf. auch über den System- und Prozesszustand) ausgetauscht. 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.

- Sind mehrere Personen am Handlungsablauf beteiligt, so ist zu berücksichtigen, dass
 - Handlungen verschiedener Personen zeitlich parallel ablaufen können oder
 - Handlungen erst dann ausgeführt werden dürfen, wenn bestimmte Bedingungen vorliegen.

Die Bedingungen können System- oder Prozessbedingungen darstellen oder auch durch bestimmte Informationen anderer Personen vorgegeben sein.

- Zufällige Einflüsse 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.

Aufgrund dieser Gegebenheiten sieht das grundlegende Konzept des Crew-Moduls vor, einen komplexen Handlungsablauf, bei dem mehrere Personen beteiligt sind und interagieren können, durch eine Vielzahl von einfachen Basishandlungen zu beschreiben. Die grundlegenden Bausteine des Crew-Moduls bestehen aus Basishandlungen und Handlungslisten.

Für das Crew-Modul wird eine Basishandlung als eine abgeschlossene einfache Einzelhandlung verstanden, die von einem bestimmten Operateur durchgeführt wird. 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 (HL) zu erstellen, die den Ablauf einer bestimmten Teilhandlung beschreiben.
- Angabe der Person, die die Basishandlung durchführt.

- Angabe der Person oder der technischen Komponente, die durch die Basishandlung beeinflusst wird: Die Angabe, welche Person von der Handlung beeinflusst wird, ist wichtig, um den Zeitpunkt zuordnen zu können, wann diese Person durch die Handlung in Anspruch genommen wird oder eine bestimmte Information erhält. Die Angabe der technischen Komponente ist wichtig, um die Zeiten ermitteln zu können, wann die Komponente durch die entsprechende Handlung beeinflusst wird.
- Angabe der Zeit, die die Person für die Ausführung der Basishandlung benötigt: Die Ausführungszeit einer Basishandlung kann entweder als Zufallsvariable oder als konstante Größe spezifiziert werden.
- Kurzbeschreibung der Basishandlung (optional).

Neben den Basishandlungen, die Aktionen von Personen beschreiben, werden im Crew-Modul zusätzlich Verzweigungsvariable verwendet, mit denen angegeben wird, an welcher Stelle des Handlungsablaufs es zu Verzweigungen kommt. Über die Verzweigungsvariable können Abhängigkeiten des Handlungsablaufs von aleatorischen Unsicherheiten (stochastischen Ereignissen) sowie Abhängigkeiten von Prozesszuständen modelliert werden.

Die Basishandlungen, in die ein Handlungsablauf zerlegt worden ist, werden sequenziell zusammengesetzt, um bestimmte Teilhandlungen zu beschreiben. Diese sequenzielle Abfolge von Basishandlungen wird als eine Handlungsliste bezeichnet. Eine Handlungsliste endet dann, wenn der weitere Handlungsablauf von bestimmten Bedingungen abhängt, z. B. Prozesszustände oder zufällige Ereignisse.

Jeder einzelnen Handlungsliste ist eine eindeutige Bedingung zugeordnet. Eine Handlungsliste wird genau dann aktiviert und ausgeführt, wenn im Handlungsablauf die ihr zugeordnete Bedingung erfüllt ist. Durch die eindeutige Zuordnung einer speziellen Bedingung zu jeder Handlungssequenz ist es möglich, Handlungsabläufe z. B. in Abhängigkeit

- vom Prozess- und Systemzustand,
- vom Zustand des bisher erfolgten Handlungsablaufs und
- von stochastischen Einflussfaktoren

zu berücksichtigen.

3.2.3 Überblick der bisherigen Arbeiten zur dynamischen Analyse von Personalhandlungen

Nachfolgend wird kurz der Stand rekapituliert, welchen die Berücksichtigung von Personalhandlungen bis zum aktuellen Vorhaben erreicht hat.

Es wurde ein Konzept entwickelt, wie ein Handlungsablauf zu modellieren ist, um ihn in einer MCDET-basierten dynamischen PSA berücksichtigen zu können (siehe /PES 06/, Kap. 3 und 4). Der Begriff Modellierung bedeutet in diesem Zusammenhang, mit den Informationen über das Ereignis, das Handeln des Personals und die leistungsbestimmenden Faktoren das Vorgehen zu beschreiben, welches das Personal auszuführen hat, um das Ereignis bewältigen zu können. Man spricht auch von einem „Handlungsmodell“. Die Beschreibung des erwarteten Handlungsablaufs geht in ihrem Detaillierungsgrad in der Regel deutlich über denjenigen eines Handlungsmodells für eine klassische Probabilistische Sicherheitsanalyse hinaus, weil sich genauere Aussagen über die Effekte, welche zufällig variierende Zeitpunkte bzw. Zeitdauern der einzelnen Handlungen auf den Ereignisablauf haben, nur gewinnen lassen, wenn der Handlungsablauf möglichst vollständig in einzelne Handlungen zerlegt, deren stochastisch variierende Ausführungszeiten quantifiziert und die zeitliche Abfolge der einzelnen Handlungen korrekt repräsentiert ist. Zu den Handlungen gehören neben dem Ablesen von Anzeigen, der Ausführung von Schalthandlungen, der Kommunikationen im Team usw. auch Wege zum Ort des Handelns und Zeitaufwände für das Zurücklegen solcher Wege. Im Rahmen der Beschreibung des Handlungsablaufs wird das Potenzial für Fehler ermittelt, die aufgrund der Ausprägungen leistungsbestimmender Faktoren zu erwarten sind. Dies schließt die Möglichkeiten ein, Fehler in Abhängigkeit von relevanten leistungsbestimmenden Faktoren zu erkennen und zu beheben.

Das Vorgehen unterscheidet sich nicht grundsätzlich von demjenigen in einer nicht-dynamischen probabilistischen Sicherheitsanalyse. Die Bewertung quantifiziert die Fehler durch Zuordnung von Schätzwerten und Unsicherheitsbändern für Fehlerwahrscheinlichkeiten. Für regelbasiertes Handeln ist vorgesehen, die entsprechenden Tabellen in THERP /SWA 83/ oder ASEP /SWA 87/ zu nutzen. Details dazu finden sich in /PES 06/, Kap. 5).

Das sogenannte Crew-Modul dient in Verbindung mit MCDET dazu, den modellierten Handlungsablauf unter Berücksichtigung von Unsicherheiten und Abhängigkeiten zu simulieren. Aus der Auswertung der Simulationsergebnisse können dann Zeitverteilungen relevanter Handlungen unter der Bedingung bestimmter Ereignisse ermittelt werden. Diese bedingten

Zeitverteilungen können dann als aleatorische Einflussgrößen für eine MCDET-Analyse eines Prozesses verwendet werden.

Leistungsbestimmende Faktoren können sich mehr oder minder schnell ändern. Man denke etwa an das Stressniveau, das nach einem Erfolg oder Misserfolg bei der Reparatur eines benötigten Systems oder der Beherrschung eines technischen Ausfalls ab- oder zunehmen kann. Modellierung, Analyse und Bewertung sehen nicht nur eine Zerlegung des Handlungsablaufs in Einzelhandlungen, sondern auch die Ermittlung und Beurteilung leistungsbestimmender Faktoren für jede dieser Teilhandlungen vor. Auf diese Weise kann der Methoden-anwender Handlung für Handlung den Beitrag der einschlägigen, leistungsbestimmenden Faktoren und Veränderungen dieser Beiträge von einer Handlung zur anderen berücksichtigen. Für den Faktor Stress wurde das methodische Vorgehen konkretisiert und am Beispiel eines Ereignisses mit Brandbekämpfung /FAS 14/, /FAS 18/ vorgestellt.

Die Methodik wurde auch dahingehend weiterentwickelt, dass sie nicht nur regel-, sondern auch wissensbasiertes Handeln erfassen kann /PES 18/. Als Anwendungsfall hat ein Ereignis aus der deutschen Betriebserfahrung gedient, bei welchem das Personal einen „Precursor“ für einen Kühlmittelverluststörfall beherrscht hat. Im Rahmen des entsprechenden Forschungs- und Entwicklungsvorhabens RS1529 ist auch eine einfacher anzuwendende und benutzerfreundlichere Version des Crew-Moduls entwickelt worden.

Grundsätzlich bestehen keine Schwierigkeiten, die Methodik des Crew-Moduls für die Modellierung, Analyse und Bewertung der Personalhandlungen auf die Beherrschung übergreifender Einwirkungen im Rahmen einer dynamischen PSA anzuwenden. Dies zeigt ein Vergleich der Herausforderungen übergreifender Einwirkungen mit den Leistungsmöglichkeiten der Methodik.

Wie für andere Ereignis- und Handlungsabläufe ist für die Modellierung, Analyse und Bewertung ein Szenario festzulegen, welches die Art der Einwirkung und deren möglichen Folgen für die Infrastruktur bzw. die technischen Einrichtungen der Anlage definiert:

- Übergreifende Einwirkungen können ein wissensbasiertes Handeln erfordern, wenn die Einwirkung das Personal vor unerwartete Situationen stellt, die bisheriges Training und vorhandene Prozeduren nicht berücksichtigen. In solchen Fällen kann das Personal auf der Basis seines Fachwissens erkennen, wie es die ihm geläufige Auslegung und Funktionsweise der verfügbaren Anlagenteile und Systeme nutzen kann, um eingetretene Zustände zu beherrschen oder so weit zu verändern, dass eine Verbesserung dieser Zu-

stände eintritt. Wissensbasiertes Handeln dieser Art fällt in den Anwendungsbereich der Methodik.

- Die Auseinandersetzung mit übergreifenden Einwirkungen kann einen erheblichen Einsatz an Personal und materiellen Ressourcen erfordern. Für die Methodik und das Crew-Modul ist das grundsätzlich kein Problem, weil der Handlungsablauf auf die Einzelhandlungen individueller Akteure an bestimmten Orten, zu bestimmten Zeiten und mit bestimmten Mitteln heruntergebrochen wird und diese Einzelhandlungen zu einem realistischen Handlungsmodell zusammengeführt werden. Das Handlungsmodell kann prinzipiell also auch eine Vielzahl seriell oder parallel laufender Handlungen einer großen Zahl von Akteuren repräsentieren.
- Zerstörungen an der Infrastruktur erschweren das Handeln. Der Methodenanwender hat also zu klären, welchen Kategorien leistungsbestimmender Faktoren sich diese Erschwerisse zuordnen lassen, welche Ausprägungen leistungsbestimmender Faktoren vorliegen, auf welche Handlungen die identifizierten leistungsbestimmenden Faktoren mit ihren jeweiligen Ausprägungen wirken und welche Folgen sie für die Handlungszuverlässigkeit und den Zeitablauf des Handelns aller Voraussicht nach haben. Das Herunterbrechen des Handlungsablaufs auf Einzelhandlungen unterstützt eine detaillierte, auf individuelle Handlungen bezogene Untersuchung und Beurteilung leistungsbestimmender Faktoren. Das Handlungsmodell erfasst diese Erkenntnisse für die weiteren Analysen und Bewertungen.
- Die Anwendung des MCDET-Ansatzes erfordert Daten in Form von Wahrscheinlichkeitsverteilungen für die Dauer und die Zuverlässigkeit der Personalhandlungen. Geeignete Daten können der Literatur entnommen und aus Informationen gewonnen werden, die aus Übungserfahrungen des Betreibers sowie Erkenntnissen und Expertenurteilen der MCDET-Anwender stammen. Quelle, Art und Belastbarkeit verwendeter Daten sind genau zu dokumentieren. Dieses Vorgehen unterscheidet sich nicht grundsätzlich von der Bewertung eines Ereignis- und Handlungsablaufs ohne übergreifende Einwirkungen.
- Die Abschätzung der Folgewirkungen übergreifender Ereignisse auf die Infrastruktur und den Stresslevel des Personals sowie das eventuelle Eintreten kaskadierender Effekte sind mit erheblichen Unsicherheiten verbunden. Das Crew-Modul in Verbindung mit MCDET ist besser als jede andere Methodik geeignet, eine Vielzahl verschiedenster Unsicherheiten umfassend und detailliert in der Analyse des Handlungsablaufs zu berücksichtigen.

Die Methodik des Crew-Moduls in Verbindung mit MCDET bietet somit die grundlegenden Voraussetzungen, die für eine Untersuchung der Wirksamkeit von Personalhandlungen unter

den Rahmenbedingungen übergreifender Einwirkungen in Bezug auf Zeit, Zuverlässigkeit und unter Berücksichtigung aleatorischer Unsicherheiten sowie Abhängigkeiten von Systemzuständen erfüllt sein müssen.

Zur Erprobung und Demonstration werden in diesem Vorhaben die zur Verfügung stehenden methodische Ansätze zur dynamischen PSA für Ereignisszenarien unter erschwerenden Randbedingungen durch übergreifende Einwirkungen angewendet. Die Anwendungen dienen auch dazu, Schwachstellen zu erkennen und die Methode entsprechend weiterzuentwickeln.

4 Festlegung eines zu analysierenden Szenarios

Entsprechend den Erkenntnissen aus Untersuchungen und methodischen Weiterentwicklungen in Bezug auf PSA für übergreifende Einwirkungen in den Vorhaben RS1539 des BMWi /ROE 17/ und 4715R01575 des BMU /SPE 18/ haben sich als Ereignisszenarien übergreifender Einwirkungen oder Einwirkungskombinationen bestimmte Szenarien durch hydrologische Einwirkungen mit Überflutungspotenzial als nicht vernachlässigbar herausgestellt. Insbesondere hat sich ergeben, dass das Feuerlöschwassersystem hinsichtlich der freigesetzten Wassermengen im Ringraum das größte Potenzial hat, sicherheitsrelevante Komponenten zu überfluten. Durch redundante und diversitäre Wasserentnahmekquellen (u. a. Brunnenwasser, Flusswasser) gewährleistet das Feuerlöschwassersystem eine zuverlässige Versorgung mit Löschwasser. Um eine Überflutung im Ringraum zu verhindern, durch die sicherheitstechnisch relevante Komponenten beeinträchtigt werden können, ist es erforderlich, die Wasserfreisetzung im Reaktorgebäude-Ringraum möglichst schnell zu unterbinden. Aus diesem Grund kommen menschlichen Handlungen bei solchen Szenarien eine besondere Bedeutung zu.

Entsprechend der Zielsetzung des Vorhabens, menschliche Handlungen unter erschwerten Randbedingungen mit den Methoden der dynamischen PSA zu analysieren, wird unterstellt, dass ein Überflutungsereignis zeitgleich mit der übergreifenden Einwirkung eines Brandes im Ringraum auftritt. Eine solche Ereigniskombination stellt ein extrem seltenes Ereignis dar. Die Annahme ist daher als sehr konservativ zu betrachten.

Bei der Referenzanlage handelt es sich um einen im kommerziellen Betrieb befindlichen Druckwasserreaktor (DWR) eines Kernkraftwerks in Deutschland. Es wird unterstellt, dass in einem Kabelschacht des Reaktorgebäude-Ringraums ein Brand ausbricht und während der Löscharbeiten ein Leck in der Feuerlöschwasserleitung auftritt, welches die Zufuhr des Löschwassers zur Brandbekämpfung unterbricht. Die erschwerende Randbedingung für den Löschvorgang besteht also in der mehr oder minder großen Verzögerung der Löscharbeiten durch die Dauer und den Erfolg der Erkennung, Lokalisierung und Absperrung des Lecks. Ziel ist es, die Auswirkungen dieser Randbedingung auf Zeitverlauf und Wirksamkeit des Löschvorgangs mittels der GRS-Methoden zur dynamischen PSA (Crew-Modul und MCDET) zu untersuchen und zu beurteilen.

Eine schematische Darstellung der für das gewählte Szenario wesentlichen Gegebenheiten findet sich in der Abb. 4.1. Dabei werden insbesondere die Lage des Brandentstehungsortes, der Leckstelle und der Komponenten verdeutlicht, die im Ringraum und auf dem Freigelände der Anlage für Löschvorgang bzw. Leckabspernung von Bedeutung sind. Eine detaillierte Be-

schreibung des ausgewählten Szenarios und seiner sicherheitstechnischen Bedeutung erfolgt direkt nach der grafischen Darstellung.

Es soll an dieser Stelle nochmals hervorgehoben werden, dass es sich bei dem für die Analysen unterstellten Szenario um ein überaus seltenes Ereignis handelt, bei welchem zwei übergreifende Einwirkungen nahezu zeitgleich eintreten und das Anlagenpersonal vor besondere Herausforderungen stellen. Dabei ist es für die durchzuführende Analyse unerheblich, ob die Ereignisse abhängig oder unabhängig voneinander eintreten und mit welcher Eintrittswahrscheinlichkeit dies erfolgt. Vielmehr geht es in der Analyse darum, Zeitverteilungen abzuschätzen, innerhalb der die angenommene Situation vom Anlagenpersonal unter Kontrolle gebracht werden kann. Die Zeitverteilungen können unter der Bedingung verschiedener unsicherer Einflussgrößen berechnet werden, die in der Analyse der Handlungsmaßnahmen berücksichtigt werden. Damit kann der Einfluss unsicherer Größen auf die Zeiten abgeschätzt werden, die das Personal zur erfolgreichen Bearbeitung der angenommenen Situation benötigt. Anhand der ermittelten Zeitverteilungen soll des Weiteren versucht werden, das Gefahrenpotenzial für sicherheitsrelevante Komponenten im Reaktorgebäude-Ringraum abzuschätzen.

Die Analyse kann somit eher als eine 'what if'-Analyse verstanden werden, die eine Abschätzung der Zuverlässigkeit menschlicher Handlungen erlaubt, wenn das Eintreten bestimmter Ereignisse angenommen wird. Diese Art von Analysen können idealerweise dazu verwendet werden, um Konzepte für Notfallmaßnahmen und optimale Maßnamestrategien für bestimmte angenommene Extremsituationen zu entwickeln. Mit der Erstellung solcher Konzepte für Notfallmaßnahmen könnte ein Beitrag geliefert werden, um das Sicherheitsniveau einer Anlage zu verbessern.

Die nachfolgende Abb. 4.1 gibt eine schematische Darstellung der für das Szenario wichtigen Systeme und Komponenten des Reaktorgebäude-Ringraums und des angrenzenden Freigeländes der Referenzanlage wieder.

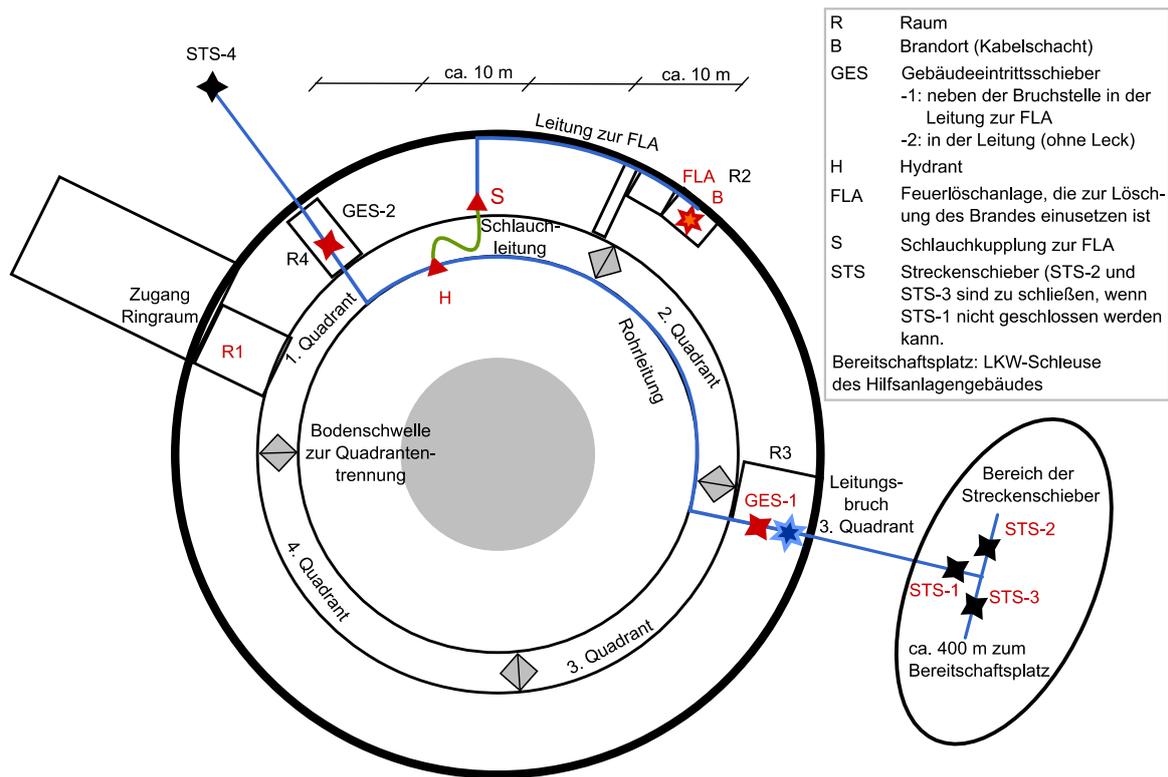


Abb. 4.1 Schematische Darstellung der für das Szenario wichtigen Systeme und Komponenten des Reaktorgebäude-Ringraums und des angrenzenden Freigeländes der Referenzanlage

Nachfolgend findet sich eine genauere Beschreibung des Szenarios und seiner sicherheitstechnischen Bedeutung:

- Weder für den Brand noch für den Leitungsbruch der Feuerlöschwasserleitung im Reaktorgebäude-Ringraum werden spezifische Ursachen unterstellt.
- Der für den Brand unterstellte Kabelschacht enthält Kabel von Messkreisen ebenso wie Kabel zur Ansteuerung oder elektrischen Versorgung sicherheitstechnisch relevanter Komponenten. Der Brand kann somit sicherheitstechnisch wichtige Komponenten und Systeme beeinträchtigen. Der Ort der Leckage wurde entsprechend den folgenden Gesichtspunkten festgelegt:

Wasser aus dem Leck strömt in den dritten Quadranten des Reaktorgebäude-Ringraums. Das Leck ist nur absperrbar, wenn das Personal den Gebäudeeintrittsschieber GES-1 im Reaktorgebäude-Ringraum und die Streckenschieber STS-1 bzw. STS-2 und STS-3 auf dem Freigelände der Anlage schließt. Der Gebäudeeintrittsschieber GES-1 ist ebenso wie der Gebäudeeintrittsschieber GES-2 nach dem Brandalarm von der Warte aus aufgefahren worden, um die Feuerlöschwasserleitung mit Löschwasser zu versorgen. Sollte sich

der Streckenschieber STS-1 beispielsweise wegen Schwergängigkeit nicht schließen lassen, werden durch das Anlagenpersonal die in der Nähe befindlichen Streckenschieber STS-2 und STS-3 vor Ort geschlossen. Das Szenario lässt die Möglichkeit eines Lecks in der Nähe des Gebäudeeintrittsschiebers GES-2 außer Betracht. Die Erkennung eines Lecks am Gebäudeeintrittsschieber GES-2 vor Ort ist von der Leckgröße und Dauer des anstehenden Lecks abhängig, da die Tür zum Treppenhaus geschlossen ist und die Überdruckklappe erst nach entsprechendem Wasseranstieg in Richtung Reaktorgebäude-Ringraum öffnet. In diesem Zusammenhang wird jedoch davon ausgegangen, dass sich die Feuerwehr aufgrund des Brandes längere Zeit in dem Bereich aufhält und somit im Fall eines Lecks an GES-2 den Wassereintritt zeitnah erkennen und die Absperrung veranlassen könnte. Die Schließung der Gebäudeeintrittsschieber kann von der Warte aus, aber auch manuell durch die Feuerwehr vor Ort im Reaktorgebäude-Ringraum erfolgen.

Die Feuerlöschwasserleitung ist gefüllt und steht unter Druck. Aufgrund des Lecks fällt der Druck in der Leitung unter einen kritischen Grenzwert, der deutlich unter den Werten liegt, die mit der Entnahme von Löschwasser für Löschvorgänge, Übungen usw. erreicht werden. Wird der kritische Grenzwert erreicht, erfolgt automatisch ein Start von Feuerlöschwasserpumpen. Letztere sind nicht mit den Druckhaltepumpen zu verwechseln, die den Druck in der Feuerlöschwasserleitung aufrechterhalten, wenn dieser Leitung Löschwasser z. B. über Hydranten entnommen wird. Zwei Feuerlöschwasserpumpen fördern vorzugsweise Brunnenwasser in die Leitung, um den Druck wieder über den Grenzwert anzuheben. Gelingt letzteres nicht, werden automatisch zwei weitere Feuerlöschwasserpumpen zugeschaltet, die Flusswasser mit dem Ziel in die Feuerlöschwasserleitung fördern, den erforderlichen Druck in der Leitung zu erreichen. Eine Abschaltung der Feuerlöschwasserpumpen von Hand wäre durch eine Abschaltung vor Ort im Schaltanlagengebäude möglich. Dies wurde jedoch für die Analyse aufgrund des gleichzeitig auftretenden Brandes nicht in Erwägung gezogen.

Bis zur Schließung der Streckenschieber STS-1 bzw. STS-2 und STS-3 fördern Löschwasserpumpen Wasser in den Ringraum. Solange der Gebäudeeintrittsschieber GES-1 offen ist, fließt außerdem Wasser aus der gefüllten Feuerlöschwasserleitung im Reaktorgebäude-Ringraum in den dritten Ringraumquadranten.

- Aus dem Leck strömt Feuerlöschwasser mit einer Rate von ca. 140 bis 180 kg/s in den dritten Ringraumquadranten. Ist letzterer bis an die Bodenschwellen gefüllt, fließt das Wasser anschließend in die angrenzenden Ringraumquadranten Q2 und Q4, bis das Personal die o. g. Schieber geschlossen hat. Sind der zweite und der vierte Ringraumquad-

rant bis an die Oberkanten der Bodenschwellen gefüllt, wird auch der erste Ringraumquadrant geflutet, solange die Absperrung des Lecks aussteht.

- Eine Überflutung des Ringraums kann zu einer Schädigung sicherheitstechnisch wichtiger Systeme und Komponenten führen. Dazu gehören Reaktorschutz-Messumformer und Pumpen für die Sicherheitseinspeisung, Beckenkühlung, Not- und Nachkühlung sowie Zwischen- und Notzwischenkühlung. Die Absperrung des Lecks dient also nicht nur dazu, die Löschwasserversorgung wiederherzustellen, sondern auch dem Schutz dieser Systeme und Komponenten vor Überflutung.
- Die Analyse wird unter der Annahme durchgeführt, dass die Leckage und der Brand nahezu zeitgleich auftreten. Weitere Überlegungen, mit welcher Wahrscheinlichkeit die beiden Ereignisse gemeinsam auftreten können und ob das Auftreten der beiden Ereignisse korreliert ist, werden im Rahmen dieser Analyse nicht durchgeführt.
- Es wird unterstellt, dass die beiden Ereignisse Brand und Leck zeitlich so nahe beieinander liegen, dass die Leckage die Versorgung mit Löschwasser deutlich beeinträchtigen kann. Bricht die Leitung bereits längere Zeit vor dem Brand, kann das Leck schon abgesperrt sein, wenn die Feuerwehr die Feuerlöschanlage (FLA) mit Löschwasser zu versorgen beginnt. Je später das Leck nach Einleitung des Löschvorgangs eintritt, desto weiter kann die Brandlöschung bereits fortgeschritten sein. Das Szenario sieht deshalb vor, dass das Leck höchstens 3 min vor und höchstens 3 min nach dem Zeitpunkt entsteht, zu dem die Feuerwehr der Feuerlöschanlage (FLA) am Brandort (B) Löschwasser zuführen könnte. Innerhalb dieses Zeitfensters haben alle Zeitpunkte die gleiche Wahrscheinlichkeitsdichte.
- Im vorliegenden Szenario werden keine Ausfälle oder Fehlfunktionen der Mess-, Leittechnik- und Alarmeinrichtungen unterstellt, von denen die Entdeckung des Brandes, die Erkennung der Leckage sowie die Diagnose des Ereignisses durch die Schichtmannschaft in der Warte abhängen. Es gilt ferner die Voraussetzung, dass alle Bedieneinrichtungen bis auf den Streckenschieber STS-1, der schwergängig sein kann, ihre Funktion voll und ganz erfüllen.
- Wochentag und Uhrzeit der Ereigniskombination können unbestimmt bleiben, da sich das benötigte Personal für die anstehenden Handlungen in der Warte und eine ausreichende Zahl von Mitgliedern der Werkfeuerwehr für die Brandbekämpfung und die Absperrung der Leckage ständig am Standort der Referenzanlage befindet (vgl. /KKW 12/, S. 7-2f). Es entstehen somit keine Zeitverluste, beispielsweise durch die Anfahrt von Feuerwehrper-

sonal in Rufbereitschaft, welches sich zu Beginn eines Ereignisses außerhalb der Anlage aufhält.

Die Betrachtung des angenommenen Szenarios endet mit der Wiederherstellung der Löschwasserversorgung und dem erfolgreichen Löschen des Brandes. Es soll untersucht werden, zu welchen Zeitverzögerungen im Löschangriff eine Leckage im Reaktorgebäude-Ringraum führt und welche Einflussfaktoren dafür maßgeblich sind.

5 Beschreibung des Handlungsablaufs zur Beherrschung des Szenarios als Grundlage für eine dynamische Modellierung

Zur Beschreibung eines Handlungsablaufs, die als Grundlage für eine dynamische Modellierung und Analyse dient, sind folgende Aspekte zu berücksichtigen.

- Der Handlungsablauf ist so zu beschreiben, dass Einzelhandlungen (Basishandlungen), die von bestimmten Personen ausgeführt werden, explizit in ihrer zeitlichen Abfolge erläutert werden. In der Erläuterung der Einzelhandlungen sollte vorzugsweise erwähnt werden, welche Person die Handlung ausführt: Dies beinhaltet die von der Person ausgeführte Basishandlung und die für die Ausführung der Basishandlung benötigte Zeit. Die Basishandlungen sollten dabei so einfach gewählt werden, dass sie von einer bestimmten Person ausgeführt wird. D. h., komplexere Aufgaben (Tasks), die von mehreren interagierenden Personen durchgeführt werden, sollten möglichst nicht als Basishandlungen definiert werden.
- Nach dem Konzept des Crew-Moduls zufolge sind zur Beschreibung der Handlungsmaßnahmen die Ausführungszeiten für die zu definierenden Basishandlungen sowie andere aleatorische Unsicherheiten (z. B. menschliche Fehler – sowohl Auslassungs- als auch Ausführungsfehler, Verfügbarkeit von Komponenten, Zugänglichkeit und Verwendbarkeit von benötigten Hilfsmitteln in Abhängigkeit der gegebenen Bedingungen in der Anlage) zu definieren und deren Wahrscheinlichkeiten abzuschätzen. Für Schätzungen von Fehlerwahrscheinlichkeiten regelbasierter Handlungen können die entsprechenden Tabellen in THERP /SWA 83/ oder ASEP /SWA 87/ verwendet werden.
- Des Weiteren können Stressentwicklungen berücksichtigt werden, die sich im Handlungsverlauf unter bestimmten Bedingungen ergeben können. Durch die Zerlegung des Handlungsablaufs in Basishandlungen können den einzelnen beteiligten Personen unterschiedliche Stressverläufe zugeordnet werden. Die Einschätzung der Stressentwicklung kann im Rahmen der eingesetzten Methodik zusätzlich unter Berücksichtigung von Unsicherheiten erfolgen.
- Zur Abschätzung der Wahrscheinlichkeiten für die einzubeziehenden aleatorischen Unsicherheiten und Unsicherheiten bzgl. der Stressentwicklungen werden in der Regel keine Daten aus der Betriebserfahrung vorliegen. Es kann versucht werden,
 - i) anlagenspezifische Informationen einzuholen, die zur Abschätzung der Wahrscheinlichkeiten dienlich sein könnten,

- ii) spezielle Modelle zur Schätzung der entsprechenden Wahrscheinlichkeiten zu entwickeln (ein Beispiel dazu ist in Abschnitt 6.1.2 zu finden),
- iii) subjektive Abschätzungen bzgl. der Wahrscheinlichkeiten durchzuführen, die als subjektiver Vertrauensgrad (Degree of Belief) zu interpretieren sind.

Es hat sich gezeigt, dass es für eine adäquate Beschreibung eines Handlungsablaufs für eine dynamische Analyse vorteilhaft ist, sie von einem Experten für Human Factor (HF) erstellen zu lassen oder diesen zumindest einzubinden.

Der Betreiber der Referenzanlage hat wichtige Informationen bereitgestellt, die in die Modellierung, Analyse und Bewertung des Handlungsablaufs zur Bewältigung des Szenarios eingeflossen sind. Dabei handelt es sich im Wesentlichen um Informationen aus dem Betriebshandbuch (BHB), insbesondere der Brandschutzordnung /KKW 19/, aus der vom Betreiber im Rahmen der (periodischen) Sicherheitsüberprüfung (SÜ) durchgeführten PSA des Betreibers /KKW 12/, aus einer Anlagenbegehung der Referenzanlage sowie aus Diskussionen mit fachkundigen Mitarbeitern des Kraftwerks.

In den nachfolgenden Abschnitten werden der erwartete Handlungsablauf, die Analyse dieses Handlungsablaufs auf Fehler sowie die Quantifizierung der Zeitaufwände der einzelnen Handlungen vorgestellt.

5.1 Modellierung des Handlungsablaufs

Zur besseren Übersicht ist der Handlungsablauf in die folgenden Teilabläufe gegliedert:

- Brandentstehung, Brandalarm und Vorbereitung des Löschvorgangs;
- Bruch der Feuerlöschwasserleitung nahe am Gebäudeeintrittsschieber GES-1 und Erkennung des Lecks von der Warte aus;
- Erkennung des Lecks durch die Feuerwehr im Ringraum (mit Unterstützung bzw. Bekräftigung der Diagnose des Lecks von der Warte aus);
- Absperrung des Streckenschiebers STS-1 in der gebrochenen Löschwasserleitung;
- Absperrung der Streckenschieber STS-2 und STS-3 (im Fall einer Schwergängigkeit des Streckenschiebers STS-1);
- Fortsetzung und erfolgreicher Abschluss der Löscharbeiten.

Die einzelnen Teilabläufe werden in den nachfolgenden Abschnitten beschrieben. Eine dynamische PSA mit dem Crew-Modul erfordert eine detailliertere Beschreibung der Aktionen z. B. der Kommunikation, die zu den beschriebenen Arbeitsschritten gehören. Diese Details können den Handlungslisten entnommen werden, die im Anhang A in Form von Tabellen dargestellt sind.

5.1.1 Brandentstehung, -alarmierung und Vorbereitung des Löschvorgangs

Im Kabelschacht im Reaktorgebäude-Ringraum bricht ein Brand aus (siehe Abb. 4.1; Brandort B). Die Modellierung lässt die Ursache offen. Es könnte sich beispielsweise um einen Kurzschluss handeln. Die Brandmeldeeinrichtungen arbeiten bestimmungsgemäß und nach Ansprechen mindestens zweier Brandmelder auf der zentralen Brandmeldeanlage in der Warte wird vom Schichtleiter Feueralarm mit Rufdurchsage des gemeldeten Brandortes ausgelöst. Es ertönt ein unverkennbarer akustischer Alarm, die Brandmeldeanlage erstellt automatisch einen Ausdruck mit Informationen zum Brandort. Die Brandmeldeanlage erzeugt ein Duplikat des Ausdrucks mit den Informationen zum Brandort. Dieses Duplikat liegt an einem festgelegten Ort außerhalb der Warte für den Einsatzleiter der Werkfeuerwehr zur Abholung bereit.

Bei einem Brandereignis setzt die Brandmeldeanlage, die sich direkt am SL-Arbeitsplatz befindet, entsprechende Meldungen ab. An der Brandschutztafel im Warten-Nebenraum sind die Zustandsinformationen zu den Brandschutzklappen sowie der Feuerlöschwasserversorgung ersichtlich. Von dort aus sind auch die motorbetätigten Gebäudeeintrittsarmaturen anzusteuern. Bei einem Brandereignis überprüft der Schichtleitervertreter ferner die ordnungsgemäße Funktion der automatisch zugeschalteten Feuerlöschwasserpumpen im Warten-Nebenraum (bzw. kann diese bei Bedarf auch jederzeit von Hand einschalten).

Da zwei Brandmelder angesprochen haben, löst der Schichtleiter einen Brandalarm aus und entsendet die erste Löschgruppe an den Brandort, dessen Lage er durchsagt. Wäre der Brand nur von einem Brandmelder angezeigt worden, würde der Schichtleiter einen Brandläufer zur Klärung vor Ort entsenden. Der Schichtleiter lässt die Gebäudeeintrittsschieber GES-1 und GES-2 vom Warten-Nebenraum aus an der Brandschutztafel auffahren. Über die Feuerlöschwasserleitung wird dann von den Druckhaltepumpen Löschwasser in das Feuerlöschwassersystem des Ringraums nachgefördert, sobald die Feuerwehr Löschwasser für die Brandbekämpfung entnimmt. In der Referenzanlage hat der Schichtleiter im Fall von Brandalarmen wie auch von weiteren Alarmen bestimmte Unterlagen zu nutzen. Diese Unterlagen enthalten Anweisungen zum Vorgehen, sie sehen eine Protokollierung bestimmter Informationen vor.

Sofern es die Situation erfordert, kann und wird der Schichtleiter die Bearbeitung unterbrechen.

Die erste Löschgruppe besteht aus dem Einsatzleiter (EL) und acht weiteren Personen, von denen je zwei Personen dem Angriffstrupp, dem Schlauchtrupp und dem Gerätetrupp angehören (AT, ST, GT) sowie dem Melder (ME) und einem Maschinisten (MA). Die Mitglieder der Löschgruppe befinden sich vor dem Löscheinsatz in verschiedenen Teilen der Anlage außerhalb des Kontrollbereichs und begeben sich nach der Durchsage des Schichtleiters zum vorgesehenen Bereitschaftsplatz. Im vorliegenden Szenario ist dies die LKW-Schleuse des Reaktorgebäudes. Auf dem Weg zum Bereitschaftsplatz rüsten sie sich in einem benachbarten, ca. fünfzig Meter entfernten Gebäude mit ihren persönlichen Schutzausrüstungen und Atemschutzgeräten aus. Der Einsatzleiter der Löschgruppe holt am vorgesehenen Ort das Duplikat des Ausdrucks ab, den die Rechnermeldeanlage automatisch erstellt und aus dem insbesondere der Brandort hervorgeht. Die Löschgruppe verfügt somit über eine Informationsquelle zur Lage des Brandorts, die unabhängig von der Durchsage des Schichtleiters ist.

Einsatzleiter sowie Angriffs- und Schlauchtrupp betreten den Ringraum sofort nach dem Eintreffen am Bereitschaftsplatz, ohne auf die vollständige Anwesenheit der Gruppe zu warten. Sie müssen dabei nicht die für den Zutritt zum Kontrollbereich üblichen Schritte durchlaufen, sondern können sich unverzüglich in die Nähe des Brandortes begeben. Nach Informationen des Betreibers zeigt die Übungserfahrung, dass die Feuerwehr 10 bis 15 min nach der Alarmierung am Brandort eintrifft. Die Modellierung des Handlungsablaufs sieht vor, dass der Angriffstrupp der Feuerwehr den Brandort erkundet, während der Schlauchtrupp eine Schlauchverbindung vom Hydranten H zur Schlauchkupplung der Feuerlöschanlage herstellt. Der benötigte Schlauch befindet sich in unmittelbarer Nähe zum Hydranten. Die Schlauchkupplung ist von vergleichbaren Schlauchkupplungen mehrere Meter entfernt, eine farbliche Markierung erleichtert die Unterscheidung benachbarter Schlauchkupplungen. Nach der Herstellung der Schlauchverbindung hat die Löschgruppe nur noch das Ventil am Hydranten zu öffnen, um die Feuerlöschanlage aus der Feuerlöschwasserleitung mit Löschwasser zu versorgen, da die Gebäudeeintrittsschieber GES-1 und GES-2 von der Warte aus aufgefahren worden sind.

Gerätetrupp, Melder und Maschinist verbleiben außerhalb des Kontrollbereichs am Bereitschaftsplatz und warten auf weitere Anweisungen des Einsatzleiters.

5.1.2 Bruch der Feuerlöschwasserleitung und Erkennung des Lecks in der Warte

Die Feuerlöschwasserleitung bricht, während die Vorbereitungsarbeiten zur Bekämpfung des Brandes stattfinden. Der Bruch der Leitung unterbindet die Löschwasserversorgung, solange der Gebäudeeintrittsschieber GES-1 und der Streckenschieber STS-1 offen sind.

Der Leitungsbruch soll im Handlungsablauf als erschwerende Randbedingung der Brandbekämpfung fungieren. Es wurde daher unterstellt, dass der Zeitpunkt für den Bruch und der Zeitpunkt, zu dem die Feuerwehr das Ventil am Hydranten öffnen kann, um der Feuerlöschanlage Löschwasser zuzuführen, eng beieinander liegen. Große Zeitabstände zwischen den Ereignissen hätten den Effekt, dass die Brandlöschung vor Eintritt des Lecks schon sehr weit fortgeschritten ist oder das Leck bereits abgesperrt wurde, bevor sich der Entstehungsbrand zu einem Vollbrand entwickelt hat.

Im vorliegenden Handlungsablauf ist der Zeitpunkt des Bruchs der Feuerlöschwasserleitung mit dem Zeitpunkt gekoppelt, zu welchem die Feuerwehr die Schlauchverbindung zwischen dem Hydranten H und der Feuerlöschanlage hergestellt hat und die Einspeisung des Löschwassers in die Löschanlage durch Öffnung des Ventils am Hydranten H beginnen könnte. Die erschwerende Rahmenbedingung des Bruchs tritt somit ein, wenn die betroffene Handlung gerade bevorsteht oder gerade vollzogen worden ist und eine ununterbrochene Versorgung mit Löschwasser gegeben sein müsste. Für den vorliegenden Handlungsablauf gilt die Annahme, dass der Bruch maximal 3 min vor und maximal 3 min nach dem Öffnen des Ventils am Hydranten eintritt und die Zeitpunkte innerhalb dieser Grenzen gleichverteilt sind.

Für die Löschgruppe äußert sich der Bruch dadurch, dass nach Öffnen des Ventils am Hydranten der Verbindungsschlauch zur Feuerlöschanlage nicht oder nicht weiter gefüllt wird und am Brandort das Löschwasser entweder ausbleibt oder versiegt. Die darauffolgenden Maßnahmen von Einsatzleiter, Angriffstrupp und Schlauchtrupp sind in Abschnitt 5.1.3 erklärt.

Der Druckabfall im Feuerlöschwassernetz (z. B. durch einen Leitungsbruch oder aufgrund von Löschmaßnahmen vor Ort) führt zum automatischen Start der Feuerlöschwasserpumpen. Eine entsprechende Meldung wird abgesetzt. Die Anzeige einer zugehörigen Klasse-2-Meldung beginnt auffällig zu blinken. Auf der Brandschutztafel im Warten-Nebenraum wird angezeigt, welche Meldeeinrichtungen angesprochen haben, dass der Druck in der Feuerlöschwasserleitung auf oder unter einen kritischen Grenzwert abgefallen ist und dass Feuerlöschwasserpumpen nach einem automatischen Start zunächst Brunnenwasser in die Feuerlöschwasser-

leitung fördern. Die Besonderheit des akustischen Alarms schließt Verwechslungen mit anderen Alarmen aus.

Die Modellierung sieht vor, dass der Schichtleiter wie beim Feualarm einen seiner Stellvertreter (SLV) die Anzeigen im Warten-Nebenraum kontrollieren lässt. Nach Rückkehr in die Warte und Bericht erhält der SLV den Auftrag, die Ursache der Anzeigen zu klären. Der Druckabfall in der Feuerlöschwasserleitung deutet auf ein Leck oder eine Wasserentnahme vor Ort hin. Verstärkende Hinweise auf ein bestehendes Leck erfolgen erst aufgrund von Sumpfmeldungen oder der Rückmeldung vor Ort, dass die Löschwassermenge nicht ausreichend ist. Die Schichtmannschaft übt die Diagnose solcher Leckagen immer wieder, wobei Erschwerungen, z. B. in Form verfälschter Anzeigen, zu bewältigen sind. Die Diagnose beruht dabei auf den folgenden Informationen:

- dauerhaft niedriger Druck in der Feuerlöschwasserleitung,
- automatischer Start der Feuerlöschwasserpumpen,
- Meldungen zu den Füllständen in den Sümpfen des dritten Quadranten des Reaktorgebäude-Ringraums,
- keine Anzeige einer erhöhten Radioaktivität im Reaktorgebäude-Ringraum,
- keine Anzeige, die auf Heißwasser im Reaktorgebäude-Ringraum hindeutet.

Die beiden zuletzt genannten Informationen ermöglichen den Ausschluss einer Leckage im Primärkreis bzw. in Komponenten, die Heißwasser führen.

Es wird unterstellt, dass der Schichtleiter und sein Vertreter auf der Grundlage der durchgeführten Untersuchungen nach BHB, der oben genannten Informationen sowie ihrer Übungserfahrung und ihres Wissens über die Anlage erkennen, dass ein Leck in der Feuerlöschwasserleitung im Bereich des dritten Ringraumquadranten vorliegt, dessen Absperrung die Schließung des Gebäudeeintrittsschiebers GES-1, des Streckenschiebers STS-1 und, wenn letzterer in einer Offen-Stellung bleiben sollte, der Streckenschieber STS-2 und STS-3 erfordert. Diese Diagnose wird von den Erkenntnissen der Feuerwehr, die vor Ort die Möglichkeit eines Lecks überprüft hat, bestätigt oder beschleunigt (siehe Abschnitt 5.1.3).

5.1.3 Erkennung des Lecks im Reaktorgebäude-Ringraum durch die Feuerwehr

Der Einsatzleiter meldet der Warte, dass die Versorgung mit Löschwasser gestört ist. Das Betriebshandbuch sieht vor, dass das Schichtpersonal nach möglichen Leckagen sucht. In der vorliegenden Modellierung wird jedoch angenommen, dass der Einsatzleiter der Feuerwehr ein Mitglied des Schlauchtrupps mit der Lecksuche beauftragt, während er selbst am Hydranten und der Angriffstrupp in der Nähe des Brandorts bleiben. Ein Mitglied des Schlauchtrupps entdeckt das Leck über dem dritten Ringraumquadranten Q3 und den Zustrom von Wasser in den Ringraumquadranten. Er erstattet dem Einsatzleiter Bericht und steht für die Schließung des Gebäudeeintrittsschiebers GES-1 mit einer Bedieneinrichtung vor Ort bereit, falls der Schieber von der Warte aus nicht geschlossen worden sein sollte. Der Einsatzleiter meldet der Warte das Leck im Ringraum. Diese Information bestätigt oder beschleunigt die Diagnose des Lecks durch den Schichtleiter und den SLV.

5.1.4 Absperrung der Streckenschieber und Gebäudeeintrittsschieber

Der Schichtleiter lässt den Gebäudeeintrittsschieber GES-1 von der Warte aus schließen. Der stellvertretende Schichtleiter (SLV) setzt sich mit dem Melder in Verbindung und weist ihn im vorliegenden Handlungsablauf an, den Schieber STS-1 bzw., falls dies nicht möglich sein sollte, die Streckenschieber STS-2 und STS-3 zuzufahren. Die Schließmechanismen befinden sich auf dem Freigelände ca. 400 m vom Bereitschaftsplatz entfernt. Die Orte der Streckenschieber sind dem Personal der Feuerwehr genau bekannt. Direkt bei den Streckenschiebern befinden sich Steckschlüssel für die Betätigung des Schließmechanismus.

Der Melder begibt sich zu den Streckenschiebern, holt einen Steckschlüssel, orientiert sich bei Bedarf über die Lage der Schieber, öffnet den entsprechenden Bodendeckel über dem Streckenschieber STS-1 und schließt ihn mittels Steckschlüssel von Hand. Sollte er eine Schwergängigkeit oder andere Anzeichen bemerken, dass der Streckenschieber seine Endstellung nicht erreicht, geht er nacheinander zu den wenige Schritte entfernt liegenden Streckenschiebern STS-2 und STS-3, öffnet die zugehörigen Bodendeckel über den Schließmechanismen und bringt diese von Hand mit dem Steckschlüssel in Zu-Stellung. Anschließend informiert der Melder die Warte über den erfolgreichen Abschluss der Arbeiten.

5.1.5 Fortsetzung und erfolgreiche Beendigung der Löscharbeiten

Sobald der Gebäudeeintrittsschieber GES-1 und die Streckenschieber STS-1 bzw. STS-2 und STS-3 geschlossen sind, steigt der Druck im Feuerlöschwassersystem des Ringraums wieder an. Die Feuerlöschanlage erhält mittels Schlauchverbindung über den Hydranten H Löschwasser. Dafür vorgesehene Löschwasserpumpen fördern Löschwasser über den offenen Gebäudeeintrittsschieber GES-2 nach. Die Brandbekämpfung kann fortgesetzt werden. Der Brand erlischt nach etwa 5 bis 10 min. Der Angriffstrupp kontrolliert den Fortschritt der Löschung und meldet der Warte das Erlöschen des Brandes, nachdem er sich vom Löscherfolg überzeugt hat.

5.2 Untersuchung des Handlungsablaufs auf menschliche Fehlermöglichkeiten

Ziel der Untersuchung ist es, Fehlermöglichkeiten und Faktoren zu bestimmen, die das Auftreten der Fehler fördern oder erschweren. Die Untersuchung des vorliegenden Handlungsablaufs hat die folgenden Ergebnisse erbracht:

- Es ist auszuschließen, dass die Schichtmannschaft in der Warte akustische Alarme überhört, fehlinterpretiert oder nicht weiter beachtet: Die Alarmsignale sind laut, eindeutig und aus zahlreichen Wiederholungen vertraut. Dies gilt sowohl für den Feueralarm als auch für den Alarm nach dem Bruch der Feuerlöschwasserleitung. Der Leitungsbruch löst zudem optische Alarme in Form blinkender Meldungen der Klasse 2 aus. Diese blinken bis zur Quittierung auffällig, haben eine hohe Priorität und fordern die Kontrolle der Anzeigen auf der Brandschutztafel im Warten-Nebenraum.
- Nach Quittierung eines Alarmes besteht prinzipiell die Möglichkeit, dass jede weitere Reaktion unterbleibt (z. B. /SWA 83/, Kap. 11), weil der akustische Alarm verstummt und die optische Anzeige nicht mehr blinkt, sondern in Ruhiglicht erleuchtet ist. Im Handlungsablauf wird diese Möglichkeit ausgeschlossen, da Klasse-2-Meldungen eine hohe Priorität haben und durch eine in Ruhiglicht erleuchtete Anzeige auffallen.
- Verwechslungen des Brandortes mit anderen Gebäudeteilen sind nicht plausibel: Die Brandschutztafel unterstützt die Lokalisierung durch Anordnung und Bezeichnung der Anzeigen. Ein automatisch erstellter Ausdruck der Rechnermeldeanlage enthält Informationen zum Brandort. Sollte der Schichtleiter der Löschgruppe einen vom Brandort abweichenden Gebäudeteil nennen, könnten Mitglieder der Schichtmannschaft, die Ohrenzeugen der Durchsage sind und die korrekte Lage des Brandortes durch die Informationen

auf der Brandmeldeanlage bzw. aus dem Rechnerausdruck kennen, korrigierend eingreifen. Der Einsatzleiter der Löschgruppe holt sich ein Duplikat des automatisch erstellten Rechnerausdrucks mit der Angabe des Brandorts ab. Er verfügt damit über eine Informationsquelle, um den Inhalt der Durchsage des Schichtleiters zum Brandort prüfen und korrigieren zu können. Diese Korrekturmöglichkeit würde nur versagen, wenn der Einsatzleiter den Ausdruck nicht wie vorgesehen und eingeübt abholt oder falsch abliest. Die vorliegende Analyse schließt daher den Fehler aus, dass die Feuerwehr Zeit verliert, weil sie erst einen Gebäudeteil aufsucht, in welchem es nicht brennt.

- Die Feuerlöschanlage kann ihre Funktion nur erfüllen, wenn die Feuerwehr den Schlauch vom Hydranten an die Schlauchkupplung dieser Feuerlöschanlage montiert. Verwechslungen mit anderen Schlauchkupplungen lassen sich ausschließen, weil die räumlichen Abstände zwischen den Kupplungen mehrere Meter betragen und die Schlauchkupplungen zudem farblich unterschiedlich gekennzeichnet sind. Montagefehler würden sich durch austretendes Feuerlöschwasser deutlich manifestieren und eine sofortige Korrektur veranlassen.
- Es ist kaum denkbar, dass die Schließung des Gebäudeeintrittsschiebers nahe der Bruchstelle (GES-1) unterbleibt: Die zügige, korrekte Ausführung dieser Aktion hat eine wesentliche Bedeutung für die Weiterführung der Brandbekämpfung und die Absperrung des Lecks. Entsprechend hoch ist die Konzentration der Person, die den Auftrag zur Schließung erhält, auf die sofortige Ausführung dieses Auftrags.
- Wie das Schließen des Gebäudeeintrittsschiebers, ist das Schließen der Streckenschieber für das Fortführen der Brandbekämpfung unabdingbar. Deshalb erfordert die korrekte, zügige Ausführung dieser Arbeit hohe Priorität und die Aufmerksamkeit des Personals. Die örtliche Lage der Streckenschieber ist aus regelmäßigen Übungen und Begehungen bekannt. Die Tätigkeit des Schließens ist eine Standardaufgabe der Feuerwehr und deshalb sicher auch unter schlechten Randbedingungen durchführbar. Aus diesen Gründen ist nicht von einem Unterlassen oder fehlerhaften Ausführen der Tätigkeit auszugehen.

Zusammenfassend kann somit festgestellt werden, dass Handlungen als sicher anzunehmen sind und deswegen nicht detailliert probabilistisch bewertet werden. Obwohl menschliche Fehlhandlung im beschriebenen Handlungsablauf weitestgehend ausgeschlossen werden können, werden bei der Modellierung des Handlungsablaufs für das Crew-Modul in Kapitel 6 verschiedene aleatorischen Unsicherheiten unterstellt, die den Handlungsablauf beeinflussen können.

5.3 Quantifizierung der Zeitbedarfe der Handlungen

Personalhandlungen werden, wie im vorhergehenden Abschnitt dargelegt, zwar als sicher angenommen, haben aber aufgrund ihrer Ausführungszeiten Einfluss auf den Erfolg des Löschangriffes. Die Dauern der einzelnen Handlungsschritte wurden aufgrund von

- Erfahrungen und Beschreibungen (z. B. Maßnahmen in der Warte),
- systematischen Überprüfungen (z. B. Eintreffen der 1. Löschgruppe am Brandort nach dem Brandalarm),
- analytischen Berechnungen (z. B. aufgrund der zurückzulegenden Wegstrecke) sowie
- weiteren Annahmen

abgeschätzt. Aufgrund der unsicheren Eingangsdaten und unsicheren Randbedingungen in einem Szenario wird generell ein gleichverteilter Bereich zwischen Minimalwert und Maximalwert für eine Handlungsdauer angenommen. Die Zeitverteilungen der einzelnen Handlungen sind im Anhang A dargestellt.

Zusammenfassend lässt sich feststellen, dass das zusätzlich angenommene Ereignis eines Leitungsbruches der Löschwasserleitung im Reaktorgebäude-Ringraum trotz der sicheren Beherrschung der Maßnahmen durch das Personal einen nicht zu vernachlässigenden Einfluss auf den Löscherfolg haben wird, da der eigentliche Löschangriff verzögert wird.

6 Modellierung des beschriebenen Handlungsablaufs zur dynamischen Analyse mit dem Crew-Modul

Mit dem fortschrittlichen methodischen Ansatz zur dynamischen Analyse wird eine detailliertere Modellierung und Analyse der Personalhandlungen bzgl. des angenommenen, in Kapitel 4 beschriebenen Szenarios durchgeführt. Die Ergebnisse der dynamischen Analyse zielen insbesondere darauf ab, Wechselwirkungen und stochastische Einflüsse auf den Handlungsablauf zu berücksichtigen und Wahrscheinlichkeitsverteilungen bzgl. der Zeiten zu ermitteln, wann relevante Handlungen zur Beherrschung des Überflutungsszenarios durch das Personal durchgeführt werden. Ein wesentlicher Aspekt der dynamischen Analyse von menschlichen Handlungen ist die umfangreichere und ausführlichere Berücksichtigung möglicher Unsicherheitsquellen, die einen wesentlichen Einfluss auf den Handlungsablauf haben können.

Durch statistische Auswertungen der Simulationsergebnisse durch das Crew-Modul können sowohl der Einfluss von Abhängigkeiten und Unsicherheiten auf die Zuverlässigkeit von Personalhandlungen quantifiziert als auch Zeitmargen ermittelt werden, die dem Personal der Anlage in bestimmten Situationen zur Verfügung stehen, z. B. bis sicherheitstechnisch relevante Komponenten von der Überflutung betroffen sind.

Der Vorteil der umfangreicheren und detaillierteren Aussagen, die mit den Methoden der dynamischen Analyse erzeugt werden können, besteht darin, dass man einen Kenntnisgewinn bzgl. des komplexen Systemverhaltens unter Unsicherheiten erhält. Durch diesen Kenntnisgewinn können sich Hinweise dazu ergeben, an welchen Stellen angesetzt werden muss, um Verbesserungen des Sicherheitsniveaus der Anlage erzielen zu können.

6.1 Beschreibung der berücksichtigten Unsicherheiten, Abhängigkeiten und Annahmen

Die in der dynamischen Analyse berücksichtigten Unsicherheiten und Abhängigkeiten sind in den nachfolgenden Abschnitten 6.1.1 bis 6.1.7 ausführlich dargestellt.

6.1.1 Unsicherheit bzgl. der Wassereintrittsrates

Für das Szenario wird angenommen, dass das Leck den Leitungsbereich betrifft, der zu einem Wassereintrag in den Quadranten Q3 des Reaktorgebäude-Ringraumes führt. Nach dem postulierten Versagen der Rohrleitung führt die Leckage unmittelbar zu einem Druckabfall auf

< 6,5 bar im Feuerlöschwassersystem und damit zum automatischen Start von zwei Feuerlöschwasserpumpen, die aus dem Brunnen fördern. In /ROE 17/ heißt es dazu:

„... Beim Bruch einer Leitung des Feuerlöschwassersystems ... werden ca. 500 m³/h Wasser in den Ringraum freigesetzt. ...“

Eine Wasserfreisetzung von 500 m³/h entspricht einem Wassereintrag von ca. 140 kg/s. Demgegenüber wurde bei einer Robustheitsanalyse des Anlagenbetreibers der Referenzanlage ein Wassereintritt von 180 kg/s angenommen, was einer Wasserfreisetzung von 648 m³/h entspricht. Dort heißt es:

„Nach dem postulierten Eigenversagen der Rohrleitung führt die Leckage unmittelbar zu einem Druckabfall von < 6,5 bar im Feuerlöschwassersystem und damit zum automatischen Start der beiden Feuerlöschwasserpumpen, die aus dem Brunnen fördern. Die den Analysen zugrundeliegende Leckage von ca. 180 kg/s führt zur Freisetzung einer Wassermenge von etwa 11 m³ pro Minute, die sich durch vorhandene Überströmflächen auch auf den inneren Ringraumbereich verteilt. ...“

Obwohl sich diese beiden Angaben zur Wasserfreisetzung aus den unterschiedlichen Zielsetzungen der Untersuchungen ergeben,

- in dem einen Fall handelt es sich um eine PSA, bei der der Wassereintrag durch den Bruch einer Feuerlöschwasserleitung angegeben wurde,
- im anderen Fall wurde eine Robustheitsuntersuchung durchgeführt, bei der auch andere Ereignisszenarien zugrunde gelegt werden,

ist es dennoch eine realistische Annahme, von einer Unsicherheit bzgl. der Wasserfreisetzung auszugehen. Diese kann sich dadurch ergeben, dass die Wassereintrittsrate von der Größe des Lecks abhängt und das Leck zufallsbedingt mehr oder weniger groß sein kann.

Die Unsicherheit des Wassereintritts wird über eine Gleichverteilung zwischen 140 kg/s und 180 kg/s beschrieben, d. h. $W_{\text{eintritt}} \sim U(140,180)$ kg/s. Dabei werden die Werte aus den beiden vorgenannten Analysen als Orientierung für das Minimum und Maximum der Gleichverteilung zugrunde gelegt.

Die Kenntnis der Wassereintrittsrate ist im Zusammenhang verschiedener Abschätzungen von Bedeutung, beispielsweise zum Einfluss der Wassereintrittsrate

- auf die Karenzzeit, die dem Personal zur Vermeidung der Überflutung sicherheitstechnisch relevanter Komponenten und Systeme zur Verfügung steht, oder
- auf die Zeit, wie schnell die Überflutungshöhen in den Quadranten erreicht sind, bis die Überflutung des betroffenen Quadranten durch die Füllstandsanzeigen in der Warte angezeigt werden (siehe Abschnitt 6.1.2).

Aufgrund der Unsicherheiten der Wassereintrittsrates sind auch die Abschätzungen dieser Zeiten mit Unsicherheiten verbunden.

6.1.2 Unsicherheit der Zeit, wann Überflutungsmeldung für den betroffenen Quadranten an der Reaktorschutztafel angezeigt wird

Der Reaktorgebäude-Ringraum ist in vier Quadranten unterteilt, die durch 0,20 m hohe Bodenschwellen voneinander getrennt sind. Die Volumina der einzelnen Ringraumquadranten bis zur Oberkante der 0,20 m hohen Bodenschwellen betragen:

- Quadrant Q1 (Fläche: 650 m²) – 130 m³,
- Quadrant Q2 (Fläche: 315 m²) – 63 m³,
- Quadrant Q3 (Fläche: 400 m²) – 80 m³,
- Quadrant Q4 (Fläche: 500 m²) – 100 m³.

Aufgrund der sicherheitstechnischen Bedeutung der Ringraumüberwachung zur Beherrschung redundanzübergreifender Überflutungsaustritte werden auslegungsgemäß mehrfach redundante Füllstandsmessungen eingesetzt. Insgesamt kommen zwölf Messfühler (drei Messungen pro Ringraumquadrant, die in einer 2-von-3-Auswahlschaltung verknüpft sind) zum Einsatz. Die 60 cm langen Füllstandsmessungen sind im „inneren Ringraumbereich“ versetzt angeordnet und ragen in eine 30 cm unterhalb des Ringraumbodens befindliche Vertiefung hinein, damit anfallendes Wasser frühzeitig und eindeutig detektiert werden kann. Der zuerst betroffene Ringraumquadrant wird bei Erreichen des Niveaugrenzwertes von $L > 0,34$ m auf der Reaktorschutztafel angezeigt. Bei dieser Höhe ist der Ringraumboden des betroffenen Quadranten flächendeckend mit einem Wasserstand von 4 cm bedeckt.

Der Zeitpunkt, zu welchem die Überflutungsmeldung an der Reaktorschutztafel angezeigt wird, ist abhängig

- vom Quadranten, der vom Wassereintritt zuerst betroffen ist (für das Szenario wurde angenommen, dass Quadrant Q3 zuerst betroffen ist), sowie
- von der Wassereintrittsrate.

In Abhängigkeit von der Größe des Quadranten Q3 und von der Wassereintrittsrate wird bestimmt, wie schnell der Boden des betroffenen Quadranten mit einem Wasserstand von 4 cm bedeckt ist und somit der Niveaugrenzwert $L > 0,34$ m erreicht ist, der auf der Reaktorschutztafel angezeigt wird.

Der Quadrant Q3 hat eine Fläche von 400 m^2 . Für eine Wasserhöhe von 4 cm ist im Quadranten Q3 ein Wasservolumen von $400 \text{ m}^2 \cdot 0,04 \text{ m} = 16 \text{ m}^3$ erforderlich. 16 m^3 Wasser entsprechen einer Masse von ca. $m_{Q3} = 16.000 \text{ kg}$. Die erforderliche Wassermenge für das Volllaufen der Vertiefungen (m) hängt zusätzlich von der Fläche der Vertiefungsschächte ab. Da die Fläche der Vertiefungen nicht bekannt ist, wird eine Unsicherheit der Fläche zwischen 1 m^2 und 3 m^2 angenommen. Für das Volllaufen der drei Vertiefungen in einem Quadranten würde unter Berücksichtigung der Unsicherheiten somit eine zusätzliche Wassermenge zwischen $0,90$ und $2,70 \text{ m}^3$ benötigt, was einer Wassermasse zwischen 900 kg und 2.700 kg entspricht. Die Unsicherheit dieser zusätzlichen Wassermasse wird durch eine Gleichverteilung zwischen 900 und 2.700 kg ausgedrückt, d. h. $m_{\text{Vertiefung}} \sim U(900, 2700) \text{ kg}$. Der Vollständigkeit halber sei hier erwähnt, dass das zusätzliche Volumen der betrieblichen Sümpfe, die Wasser aufnehmen können, in dieser Analyse nicht berücksichtigt wurde.

In Abhängigkeit vom Wert des Wassereintrags W_{eintritt} und dem erforderlichen Wasservolumen, bei dem im Quadranten Q3 eine Wasserhöhe von 4 cm erreicht wird, kann über die Gleichung (6.1) der Zeitpunkt t_{Q3} ermittelt werden, zu dem nach dem Leitungsbruch die Überflutungsmeldung von Quadrant Q3 auf der Reaktorschutztafel angezeigt wird:

$$t_{Q3} = (m_{Q3} + m_{\text{Vertiefung}}) / W_{\text{eintritt}} \quad (6.1),$$

mit $m_{Q3} = 16.000 \text{ kg}$, $m_{\text{Vertiefung}} \sim U(90, 2700) \text{ kg}$, $W_{\text{eintritt}} \sim U(140, 180) \text{ kg/s}$.

Über eine Simulationsrechnung erhält man die in Abb. 6.1 dargestellte Wahrscheinlichkeitsdichte der Zeit t_{Q3} , zu welcher der Wassereintritt für Quadrant Q3 auf der Reaktorschutztafel angezeigt wird.

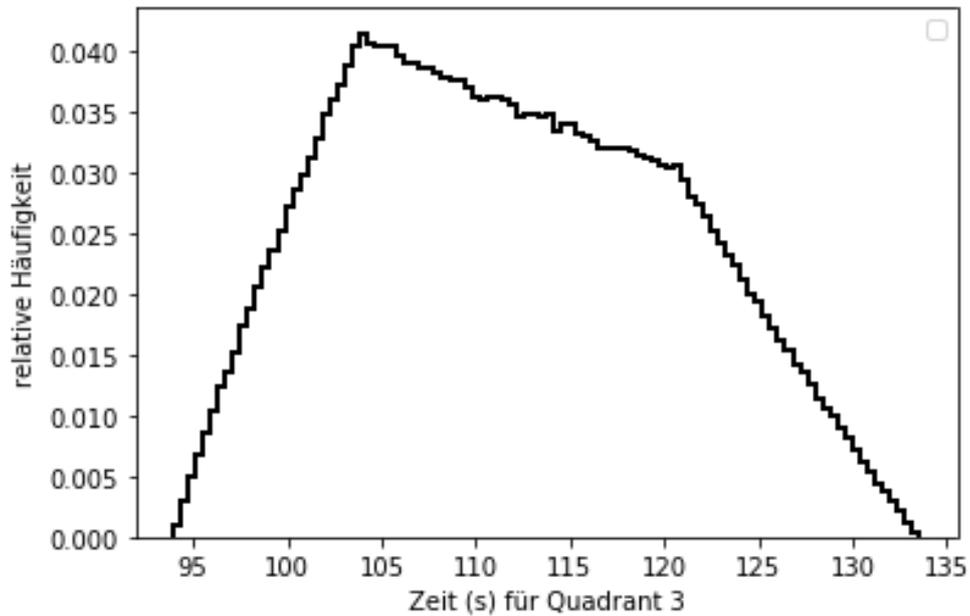


Abb. 6.1 Wahrscheinlichkeitsverteilung der Zeit t_{Q3} , wann der Wassereintritt im Quadranten Q3 durch die redundante Füllstandsmessung an der Reaktorschutztafel angezeigt wird

Um diese Verteilung der Zeiten in der dynamischen Analyse des Handlungsablaufs zu berücksichtigen, können die Simulationswerte entweder direkt aus der empirischen Verteilung oder aus einer Dreiecksverteilung ausgespielt werden, die an die empirische Verteilung approximiert wird. Die Wahrscheinlichkeitsverteilung in Abb. 6.1 kann durch eine Dreiecksverteilung $\text{Triangular}(\text{Min}, \text{Modus}, \text{Max})$ mit den Parametern $\text{Min} = 93$, $\text{Modus} = 105$, $\text{Max} = 135$ approximiert werden. Die approximierte Dreiecksverteilung ist in Abb. 6.2 zusammen mit der empirischen Verteilung dargestellt.

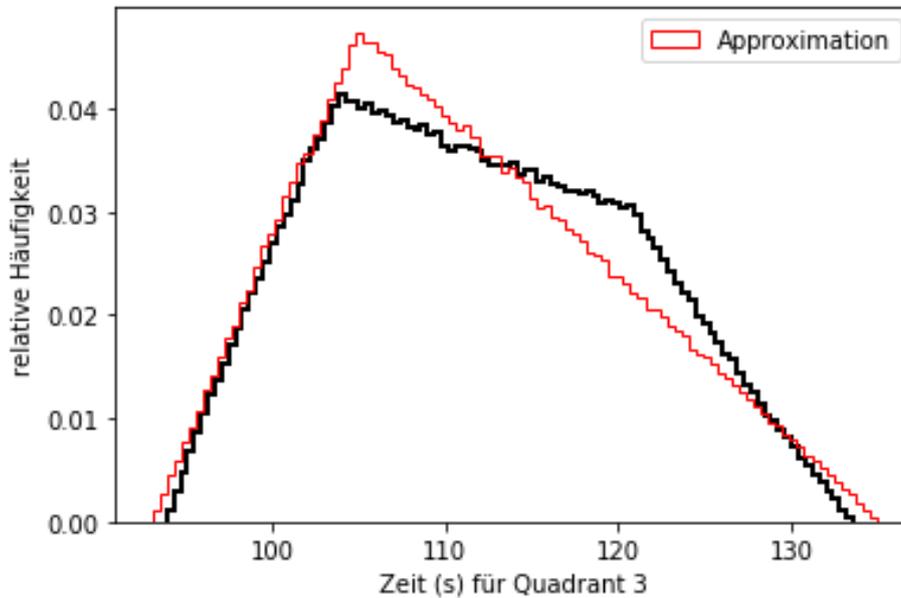


Abb. 6.2 Approximation der Wahrscheinlichkeitsverteilung von t_{Q3} durch die Dreiecksverteilung $t_{Q3} \sim \text{Triangular}(90,105,135)$ s

Der Zeitpunkt, wann für den Quadranten Q3 der Niveaugrenzwert von $L > 0,34$ m nach dem Leitungsbruch erreicht wird und dies auf der Reaktorschutztafel angezeigt wird, liegt zwischen 90 s und 135 s. Diese Zeitverteilung wird im Handlungsmodell berücksichtigt, um zu demonstrieren, in welcher Weise zeitliche Wechselwirkungen berücksichtigt werden können.

6.1.3 Unsicherheit bzgl. des akustischen Alarms zur Signalisierung eines Druckabfalls in der Feuerlöschwasserleitung

Aufgrund der Situation einer übergreifenden Einwirkung wird in dem Modell des Handlungsablaufs die Möglichkeit in Betracht gezogen, dass die Alarmeinrichtung, die einen Druckabfall in der Feuerlöschwasserleitung signalisiert, wegen eines technischen Defekts bei Anforderung nicht verfügbar ist. Dabei wird angenommen, dass ein von der wiederkehrenden Prüfung (WKP) unabhängiger Fehler vorliegen kann. D: h., der Fehler ist auch dann möglich, wenn die WKP vorher ohne Fehler abgeschlossen wurde. Liegt ein solcher Fehler vor, unterbleibt die Alarmierung in der Warte, wenn der Druck in der Feuerlöschwasserleitung abfällt.

Für diese Analyse wird angenommen, dass der Ausfall des Alarms mit der Wahrscheinlichkeit 0,005 vorkommt. Diese Wahrscheinlichkeit soll der Situation Rechnung tragen, dass bei Ereignisabläufen infolge übergreifender Einwirkungen die Wahrscheinlichkeit technischer Defekte erhöht sein kann. Dennoch ist zu betonen, dass dieser Wahrscheinlichkeitswert eine

Annahme ist und durch keine Daten oder Expertenurteil belegt ist. Dieser Wert wird ausschließlich zu Demonstrationszwecken für die in dieser Arbeit durchzuführenden Analyse verwendet.

Für die Unsicherheit bzgl. der Alarmierung nach Druckabfall in der Feuerlöschwasserleitung werden folgende Wahrscheinlichkeiten verwendet:

- $p(\text{Alarm wird ausgelöst}) = 0,995,$
- $p(\text{Alarm wird nicht ausgelöst}) = 0,005.$

6.1.4 Unsicherheit bzgl. des Stressniveaus des Schichtleiter-Stellvertreters durch einen zusätzlichen Alarm

Für die nachfolgenden Betrachtungen wird ausdrücklich darauf hingewiesen, dass die hier beschriebene Vorgehensweise nicht ganz die Situation in der Referenzanlage widerspiegelt. Die hier und in Abschnitt 6.1.5 beschriebenen Unsicherheiten bzgl. des Stressniveaus dienen in erster Linie dazu, die Modellierungsmöglichkeiten bzgl. des Stressverhaltens von Personen und die damit verbundenen Auswirkungen unter Berücksichtigung von Unsicherheiten zu demonstrieren.

Nach dem Brandalarm erfolgt innerhalb einer relativ kurzen Zeit ein zweiter Alarm. Dabei wird angenommen, dass der Schichtleiter-Stellvertreter, der zur Ursachenfindung des Alarms vom Schichtleiter zur Reaktorschutztafel geschickt wird, einen erhöhten Stresszustand entwickeln kann. Der SLV ist besonders gefragt, da er dem Schichtleiter die relevanten Informationen in möglichst kurzer Zeit berichten soll. Ob der SLV einen erhöhten Stresszustand nach dem zweiten Alarm annimmt ist unsicher. Es wird angenommen, dass der Stress des SLV mit einer Wahrscheinlichkeit (Degree of Belief) von 0,4 im normalen oder leicht erhöhten Zustand verbleibt und mit einer Wahrscheinlichkeit von 0,6 eine signifikante Erhöhung aufweist.

- $p(\text{Stress SLV} = \text{normal}) = 0,4,$
- $p(\text{Stress SLV} = \text{hoch}) = 0,6.$

Die Berücksichtigung der Stressentwicklung des SLV und die damit zusammenhängende Unsicherheit erfolgt hauptsächlich zur Demonstration, welche Modellierungs- und Analysemöglichkeiten das Crew-Modul bietet.

6.1.5 Unsicherheit bzgl. der Zeitdauern bis Anzeigen des Überflutungsalarms in Abhängigkeit des Stressniveaus bewertet werden

Es soll an dieser Stelle ausdrücklich erwähnt werden, dass diese Modellierung nicht ganz mit dem Vorgehen in der Referenzanlage übereinstimmt. Die Modellierung wurde insbesondere zu Demonstrationszwecken durchgeführt, in welcher Weise Unsicherheiten bzgl. der Stressentwicklung einer Person und die Abhängigkeit des weiteren Handlungsablaufs vom Stresslevel modelliert werden können.

Der zuerst betroffene Ringraumquadrant wird bei Erreichen des Niveaugrenzwertes von $L > 0,34$ m auf der Reaktorschutztafel in der Warte angezeigt. Bei dieser Höhe ist der Ringraumboden des betroffenen Quadranten flächendeckend mit einem Wasserstand von 4 cm bedeckt.

Wenn aufgrund des Leitungsbruchs der Alarm in der Warte ansteht, hat der SLV die Aufgabe, die Ursache des Alarms zu klären. Aufgrund der guten Ausbildung und des Trainings des Personals wird davon ausgegangen, dass der SLV die entsprechenden Anzeigen, die auf eine Überflutung des Quadranten Q3 im Reaktorgebäude-Ringraum hinweisen, erkennt und auch entsprechend bewertet. Allerdings wird für die Handlungsmaßnahme angenommen, dass der SLV in Abhängigkeit seines Stressniveaus mehr oder weniger Zeit benötigt, um die entsprechenden Anzeigen zu lesen und entsprechend zu interpretieren. Diese Zeit wird hier als Bewertungszeit des Alarms bezeichnet.

Die Bewertungszeiten werden in die drei Kategorien 'schnell', 'verzögert' und 'stark verzögert' kategorisiert. Für Zeiten t_{schnell} , $t_{\text{verzögert}}$ und $t_{\text{stark_verzögert}}$ der einzelnen Kategorien werden folgende Wahrscheinlichkeitsverteilungen angenommen:

- für die Kategorie 'schnell' eine gleichverteilte Zufallszeit zwischen 120 und 150 s, d. h. $t_{\text{schnell}} \sim U(120,150)$ s
- für die Kategorie 'verzögert' eine Zufallszeit $t_{\text{verzögert}} \sim U(150,240)$ s und
- für die Kategorie 'stark verzögert' eine Zufallszeit $t_{\text{stark_verzögert}} \sim U(240,420)$ s.

Die Abhängigkeit der Bewertungszeiten vom Stresslevel des SLV wird über die Wahrscheinlichkeitsgewichtung der jeweiligen Zeitkategorien definiert. Neben der Abhängigkeit der Bewertungszeit vom Stresslevel wird zusätzlich eine zeitliche Wechselwirkung angenommen, die dadurch definiert ist, ob der Schichtleiter-Stellvertreter an der Reaktorschutztafel in der Warte die Anzeigen kontrolliert, bevor oder nachdem die Überflutungsanzeige des dritten Quadran-

ten ansteht. Die Situationen werden mit $t_{SLV} < t_{Q3}$ (SLV erreicht die Reaktorschutztafel, bevor die Überflutungsanzeige ansteht) bzw. $t_{SLV} > t_{Q3}$ (Überflutungsanzeige steht an, bevor der Schichtleiter-Stellvertreter die Reaktorschutztafel erreicht) bezeichnet.

Für das Modell werden folgende Annahmen zugrunde gelegt:

- Der Schichtleiter-Stellvertreter hat ein normales Stressniveau und $t_{SLV} < t_{Q3}$:

In diesem Fall erfolgt die Bewertung des Alarms innerhalb der Zeitkategorie 'schnell' mit einer Wahrscheinlichkeit von 0,7 und mit einer Wahrscheinlichkeit von 0,3 innerhalb der Zeitkategorie 'verzögert'. Dass der SLV bei normalem Stressniveau eine starke zeitliche Verzögerung zur Ursachenfindung aufweist, wird hier ausgeschlossen.

- Der Schichtleiter-Stellvertreter hat ein hohes Stressniveau und $t_{SLV} < t_{Q3}$:

Mit einer Wahrscheinlichkeit von 0,1 erfolgt die Bewertung des Alarms innerhalb der Zeitkategorie 'schnell', mit einer Wahrscheinlichkeit von 0,5 innerhalb der Zeitkategorie 'verzögert' und mit einer Wahrscheinlichkeit von 0,4 innerhalb der Zeitkategorie 'stark verzögert'.

Im Fall von $t_{SLV} < t_{Q3}$ wird angenommen, dass der Schichtleiter-Stellvertreter so lange an der Reaktorschutztafel verweilt, bis die Überflutungsanzeige auf dieser Tafel erscheint und er dies in Abhängigkeit seines Stressniveaus mehr oder weniger schnell registriert.

- Der SLV hat ein normales Stressniveau und $t_{SLV} > t_{Q3}$:

Mit einer Wahrscheinlichkeit von 0,85 erfolgt die Bewertung des Alarms innerhalb der Zeitkategorie 'schnell' und mit einer Wahrscheinlichkeit von 0,15 innerhalb der Zeitkategorie 'verzögert'. Eine starke zeitliche Verzögerung wird in diesem Fall ausgeschlossen.

- Der SLV hat ein hohes Stressniveau und $t_{SLV} > t_{Q3}$:

Mit einer Wahrscheinlichkeit von 0,4 erfolgt die Bewertung des Alarms innerhalb der Zeitkategorie 'schnell', mit einer Wahrscheinlichkeit von 0,4 innerhalb der Zeitkategorie 'verzögert' und mit einer Wahrscheinlichkeit von 0,2 innerhalb der Zeitkategorie 'stark verzögert'.

Zusammenfassend sind die Wahrscheinlichkeitsverteilungen der Bewertungszeiten in Abhängigkeit des Stresslevels des Schichtleiter-Stellvertreters und der Zeit, ob dieser die Reaktorschutztafel erreicht, bevor oder nachdem die Überflutungsanzeige des dritten Quadranten auf der Reaktorschutztafel erscheinen, in Tab. 6.1 aufgeführt.

Tab. 6.1 Wahrscheinlichkeitsverteilungen der Bewertungszeiten in Abhängigkeit des Stressniveaus des SLV und zeitlicher Wechselwirkungen

Stressniveau und Ankunftszeit an der Reaktorschutztafel	Zeitkategorie	Subjektive Wahrscheinlichkeit
Normal und $t_{SLV} < t_{Q3}$	$t_{schnell} \sim U(120,150)$ s $t_{verzögert} \sim U(150,240)$ s $t_{stark_verzögert} \sim U(240,420)$ s	0,70 0,30 0,00
Normal und $t_{SLV} > t_{Q3}$	$t_{schnell} \sim U(120,150)$ s $t_{verzögert} \sim U(150, 40)$ s $t_{stark_verzögert} \sim U(240,420)$ s	0,85 0,15 0,00
Hoch und $t_{SLV} < t_{Q3}$	$t_{schnell} \sim U(120,150)$ s $t_{verzögert} \sim U(150,240)$ s $t_{stark_verzögert} \sim U(240,420)$ s	0,10 0,50 0,40
Hoch und $t_{SLV} > t_{Q3}$	$t_{schnell} \sim U(120,150)$ s $t_{verzögert} \sim U(150,240)$ s $t_{stark_verzögert} \sim U(240,420)$ s	0,40 0,40 0,20

Es sei an dieser Stelle nochmals ausdrücklich betont, dass die Zeiten der Kategorien und die zugeordneten Wahrscheinlichkeiten in Abhängigkeit des Stressniveaus durch eine rein subjektive Abschätzung festgelegt wurden und nicht auf Daten aus der Betriebserfahrung basieren. Falls aus Expertensicht andere Zeiten oder andere Wahrscheinlichkeitsgewichtungen realistischer sind, können diese ohne großen Aufwand im Modell modifiziert werden.

Die Abhängigkeit der Bewertungszeit vom Stressniveau des SLV und von dem Zeitpunkt, zu welchem dieser an der Reaktorschutztafel ankommt, um die Anzeigen abzulesen, wurde allein zu Demonstrationszwecken eingefügt. Damit sollte beispielhaft gezeigt werden, in welcher Weise Unsicherheiten bzgl. der Stressentwicklung einer Person und die Abhängigkeit des weiteren Handlungsablauf vom Stresslevel modelliert werden können. Zu diesem Zweck sollten die subjektiven Abschätzungen zunächst ausreichen.

Im Gegensatz zum 'Black-Box'-Verhalten vieler Human-Factor-Modelle besteht ein Vorteil des erstellte Handlungsmodells für das Crew-Modul darin, dass alle Basishandlungen und deren Ausführungszeiten sowie alle unsicheren Einflussgrößen und deren zugeordnete Wahrscheinlichkeiten explizit dargestellt werden und nachvollziehbar sind. So können alle Abschätzungen von Ausführungszeiten und Wahrscheinlichkeiten unsicherer Einflussgrößen überprüft und falls nötig modifiziert werden.

6.1.6 Verfügbarkeit des Werkzeugs vor Ort

In der Nähe des Ortes, an dem der Streckenschieber STS-1 geschlossen werden muss, befindet sich das dazu notwendige Werkzeug. Im Modell wird die Möglichkeit berücksichtigt, dass sich das benötigte Werkzeug nicht am vorgesehenen Ort befindet. Es könnte beispielsweise von jemandem gebraucht worden sein, der vergessen hat, es wieder zurückzulegen. Da diesbezüglich keine Daten vorliegen, wird eine grobe Abschätzung der Wahrscheinlichkeit unter folgender Annahme vorgenommen.

Annahme: In den letzten zehn Jahren hat sich das betreffende Werkzeug bei wiederkehrenden monatlichen Überprüfungen maximal 1-mal nicht am vorgesehenen Ort befunden. Dementsprechend werden die Ereignisse in Betracht gezogen, dass sich das Werkzeug 0-mal oder 1-mal nicht am vorgesehenen Ort befunden hat. Beiden Ereignissen wird das gleiche Gewicht (Degree of Belief) zugeordnet. Mit dem Bayes'schen Ansatz kann damit eine mittlere Wahrscheinlichkeit von $8,3 \text{ E-}03$ dafür berechnet werden, dass sich das Werkzeug zum Zeitpunkt, zu welchem der Melder vor Ort eintrifft und den Streckenschieber schließen möchte, nicht am vorgesehenen Ort befindet. Damit geht die folgende Unsicherheit in das Modell ein:

- $p(\text{Werkzeug am vorgesehenen Ort nicht verfügbar}) = 8,3 \text{ E-}03$,
- $p(\text{Werkzeug am vorgesehenen Ort verfügbar}) = 9,917 \text{ E-}01$.

6.1.7 Schließzuverlässigkeit des Streckenschiebers

Die Schließzuverlässigkeit des Streckenschiebers bezieht sich darauf, ob sich der Streckenschieber manuell schließen lässt oder nicht. Als Wahrscheinlichkeit, dass sich der Streckenschieber schließen lässt, wird im Modell der Wert 0,99 angenommen. Es wird somit angenommen, dass sich der Schieber mit einer Wahrscheinlichkeit von 0,01 nicht schließen lässt. Falls Daten aus der Betriebserfahrung für die Zuverlässigkeit eines Streckenschiebers erhältlich sind, können die Zuverlässigkeitswerte im Modell leicht modifiziert werden.

6.2 Beschreibung des modellierten Handlungsablaufs für das Crew-Modul

Nachfolgend wird der Handlungsablauf beschrieben, wie er für das Crew-Modul modelliert wurde. Es wird ausdrücklich darauf hingewiesen, dass in dem hier beschriebenen Modell verschiedene Annahmen getroffen wurden, die mit dem Vorgehen in der gewählten Referenzanlage nicht vollständig übereinstimmen.

Für die Modellierung eines Handlungsablaufs im Crew-Modul wird das Mind-Mapping-Tool FreeMind® verwendet. FreeMind® ist eine frei erhältliche Software zum Visualisieren und Strukturieren von Inhalten. Zur benutzerfreundlichen und übersichtlichen Beschreibung und Modellierung eines Handlungsablaufs unter Berücksichtigung von Abhängigkeiten und Unsicherheiten hat sich die Verwendung von FreeMind® für das Crew-Modul bisher am vorteilhaftesten erwiesen.

In diesem Abschnitt wird eine grobe Übersicht des modellierten Handlungsablaufs gegeben. Bei der Beschreibung wird insbesondere darauf Wert gelegt, die Abhängigkeiten des Handlungsablaufs von den im Modell berücksichtigten Unsicherheiten (stochastischen Einflüssen) und zeitlichen Wechselwirkungen zu beschreiben. Die Berücksichtigung stochastischer und zeitlicher Einflüsse wird in der Beschreibung deshalb besonders betont, da sie einen wesentlichen Aspekt der dynamischen Methoden zur Modellierung menschlicher Handlungen ausmachen. Außerdem soll damit beispielhaft verdeutlicht werden, welche Details mit den Methoden modelliert werden können.

Eine grobe Struktur der Handlungslisten (HL), die über die Oberfläche von FreeMind® erstellt wurden, ist in Abb. 6.3 dargestellt. Details zu den Handlungslisten und den darin aufgeführten Basishandlungen, durch die Teilsequenzen von Handlungsabläufen beschrieben werden, sind im Anhang A (Tabellen Tab. A. 1 – Tab. A. 15) aufgeführt.

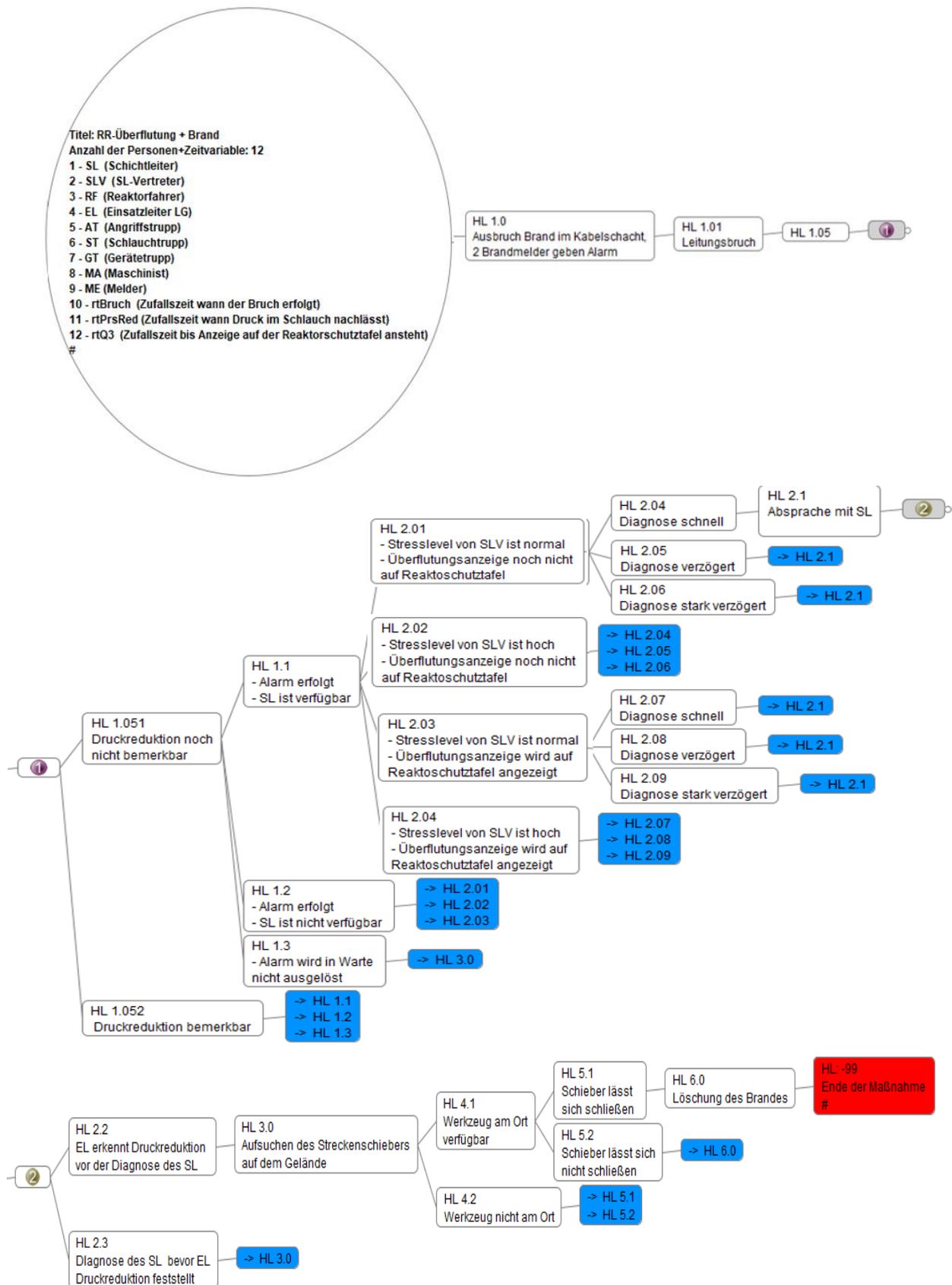


Abb. 6.3 Struktur der Handlungslisten unter Berücksichtigung stochastischer Einflussgrößen und zeitlicher Wechselwirkungen

Der ovale Knoten in Abb. 6.3 stellt den Anfangsknoten des Handlungsablaufs dar, in denen die beteiligten Personen und verschiedene Zeitvariablen definiert sind. Die rechteckigen weißen Knoten beschreiben die Handlungslisten, in denen die Basishandlungen von Teilsequenzen definiert sind. Details zu den Handlungslisten und Basishandlungen sind in Anhang A aufgeführt.

Die Verzweigungen in Abb. 6.3 beschreiben verschiedene Handlungsabläufe, die sich in Abhängigkeit der berücksichtigten Unsicherheiten und zeitlichen Wechselwirkungen ergeben. Die verschiedenen Handlungsabläufe sind in den entsprechenden Handlungslisten durch die Basishandlungen beschrieben.

Die blauen Rechtecke verweisen auf Handlungslisten, mit denen der Handlungsablauf fortgesetzt wird. Das blaue Rechteck mit der Beschriftung => 3.0 weist z. B. darauf hin, dass an dieser Stelle der Handlungsablauf mit der Handlungsliste HL 3.0 fortgesetzt wird, die bereits an anderer Stelle vorkommt und im Detail beschrieben wurde. Gleichbedeutend könnten das blaue Rechteck => 3.0 durch die Handlungsliste HL 3 sowie mit dieser verbundenen nachfolgenden Verzweigungen ersetzt werden. Würde diese Ersetzung für alle in Abb. 6.3 dargestellten blauen Rechtecke erfolgen, wäre zwar die gesamte Komplexität des modellierten Handlungsablaufs offensichtlich, wäre aber völlig unübersichtlich und nicht mehr vernünftig darstellbar.

Die roten Rechtecke beschreiben den Endzustand des Handlungsmodells. Wie aus Abb. 6.3 ersichtlich ist, werden im modellierten Handlungsablauf die Endzustände erreicht, wenn die Handlungsliste HL 5.1 oder HL 5.2 in der Simulation abgearbeitet wurde.

Aus dem Anfangsknoten der Abb. 6.3 ist ersichtlich, dass in dem modellierten Handlungsablauf neun Personen beteiligt sind:

- Schichtleiter (SL),
- Schichtleiter-Stellvertreter (SLV),
- RF (Reaktorfahrer),
- EL (Einsatzleiter der Löschgruppe),
- AT (Angriffstrupp),
- ST (Schlauchtrupp),
- GT (Gerätetrupp),

- MA (Maschinist),
- ME (Melder).

Zusätzlich zu den beteiligten Personen werden drei Zeitvariablen definiert, die innerhalb des Crew-Moduls erfasst und verarbeitet werden. Die Zeitvariable sind Zufallsgrößen, wann bestimmte Ereignisse im Handlungsablauf eintreten.

- Die Zeitvariable t_{Bruch} beschreibt die Zufallszeit, wann der Leitungsbruch erfolgt. Es wurde angenommen, dass der Leitungsbruch 3 min vor bzw. 3 min nach Herstellung der Schlauchverbindung mit dem Hydranten erfolgt. Der Zeitpunkt des Leitungsbruchs ist somit abhängig vom Zeitpunkt der Herstellung der Schlauchverbindung mit dem Hydranten. Wenn der Zeitpunkt der Schlauchverbindung $t_{\text{Verbindung}}$ erreicht ist, wird im Modell die Zufallszeit des Leitungsbruchs durch $t_{\text{Bruch}} = t_{\text{Verbindung}} + r_{\text{Bruch}}$, wobei r_{Bruch} aus einer Gleichverteilung $U(-180,180)$ zwischen - 180 s und 180 s zufällig ausgespielt und im Crew-Modul verarbeitet wird.
- Die Zeitvariable r_{PrsRed} beschreibt den Zufallszeitpunkt, zu welcher der Druckabfall im Schlauch bemerkbar ist. Diese Zeit ist abhängig vom Zeitpunkt t_{Bruch} des Leitungsbruchs. Es wird angenommen, dass es nach dem Leitungsbruch 35 s bis 60 s dauert, bis sich der Druckabfall der Leitung im Schlauch bemerkbar macht, d. h. $t_{\text{DruckRed}} = t_{\text{Bruch}} + r_{\text{PrsRed}}$, wobei r_{PrsRed} aus einer Gleichverteilung $U(35,60)$ zwischen 35 s und 60 s zufällig ausgespielt wird.
- Die Zeitvariable r_{Q3} beschreibt die Zufallszeit, bis die Überflutungsanzeige für den Quadranten Q3 auf der Reaktorschutztafel ansteht. Die Zeit t_{AnzQ3} , wann die Anzeige auf der Reaktorschutztafel erscheint, ist abhängig vom Zeitpunkt des Leitungsbruchs und von Unsicherheiten bzgl. der Wassereintrittsrates und des Volumens an Wasser, das bis zum Erreichen der redundant ausgelegten Füllstandsanzeigen bei 4 cm Wasserhöhe benötigt wird. Die Herleitung und Berechnung der Zeitverteilung wird in Abschnitt 6.1.2 beschrieben.

Nach dem Anfangsknoten wird in Abb. 6.3 die Ablaufstruktur der verschiedenen Handlungslisten dargestellt. In der in Abb. 6.3 dargestellten Ablaufstruktur sind innerhalb der einzelnen Handlungslisten (HL) stichwortartig die Situationen angedeutet, für die die jeweiligen Teilsequenzen von Handlungen durchgeführt werden. In HL 5.1 ist z. B. der Handlungsablauf beschrieben, der durchgeführt wird, wenn sich der Streckenschieber STS-1 schließen lässt. HL 5.2 beschreibt den Handlungsablauf für den Fall, dass sich der Streckenschieber STS-1 nicht schließen lässt.

Die Handlungsabläufe in den einzelnen Handlungslisten werden durch Basishandlungen beschrieben, die für die einzelnen Handlungslisten im Anhang A (Tabellen Tab. A. 1 – Tab. A. 15) ausführlich beschrieben werden. Beispielhaft wird der Inhalt der Handlungsliste HL 1.0, wie er für das Crew-Modul in der Oberfläche eingegeben wurde, in Abb. 6.4 dargestellt.

```

HL 1.0 // Ausbruch Brand im Kabelschacht, 2 Brandmelder geben Alarm
Bed: & HLcont = 0
/SL / - / 10 20 // SL hört Alarm und sieht blinkende Klasse 2 Meldung
/SL / - / 5 15 // SL unterbricht Tätigkeit und quittiert Alarm
/SL / SLV / 10 40 // SL weist SLV an BS-Tafel im W-Nebenr zu kontrollieren
/SLV / - / 10 20 // SLV geht in Warten-Nebenraum zu den Anzeigen der Melder
/SL / - / 20 40 // SL holt Unterlagen die im Brandfall auszufüllen sind
/SLV / - / 40 60 // SLV erkennt, dass Brand im Kabelschacht vorliegt
/SLV / SL / 30 60 // SLV kehrt in Warte zurück und informiert SL
/SL / RF / 5 15 // SL gibt RF Anweisung , GES1+2 zu öffnen
/RF / - / 10 20 // RF öffnet GES1 + 2
/SL / - / 120 180 // SL löst Brandalarm über Funkanlage aus
/SL / EL / 0 0 // Durch Brandalarm werden EL,AT,ST, und GT alarmiert
/SL / AT / 0 0 //
/SL / ST / 0 0 //
/SL / GT / 0 0 //
/EL / - / 300 600 // AT, ST holt Schutzausrüstung und begibt sich zum RR
/EL / AT / 0 0 //
/AT / ST / 0 0 //
/GT / -3 / 300 600 // GT holt Ausrüstung und geht zum Bereitschaftsplatz außerhalb des RR
/GT / MA / 0 0 // MA und ME begeben sich mit GT zum Ber.platz
/GT / ME / 0 0 //
/EL / ST / 30 40 // EL+ST begeben sich in die Nähe des Hydranten
/EL / -1 / 0 0 // Zeit wann EL und ST am Hydranten im RR sind
/AT / -2 / 30 50 // AT begibt sich zum Brandort, erkennt Brand im Kabelschacht und informiert EL
/EL / ST / 180 240 // EL+ST stellen Schverb zw. Hydrant und Kupplung der Löschanlage her
/EL / -4 / 0 0 // Zeitpunkt wann Schlauchverbindung hergestellt
if -4 & tBruch = 0 then tBruch = EL //Referenz_Zeit für Bruch
/rBruch / - / -180 180 // Zufallszeit für Brucheintritt zum Zeitpunkt wann Schverb hergestellt ist
/rPrsRed / - / 35 60 // Zufallszeit bis Druckabfall nach Bruch erkennbar ist
/rQ3 / - / 90 135 // Tr(90,105,135): Zufallszeit bis Überfl-Anz für Q3 auf der Reaktoschutztafel ansteht
#

```

Abb. 6.4 Basishandlungen der Handlungsliste HL 1.0

Die Inhalte der Handlungslisten folgen einer bestimmten Struktur:

- In der ersten Zeile wird die Identifikationsnummer einer Handlungsliste (HL) angegeben (z. B. HL 1.0). Optional kann nach dem Zeichen ‘//’ eine kurze Beschreibung gegeben werden, was die jeweilige Handlungsliste beinhaltet.
- In der Zeile, die mit dem Key-Word ‘Bed:’ beginnt, wird die Bedingung zur Aktivierung der Handlungsliste angegeben. In der Bedingung werden z. B. die Nummer derjenigen Handlungsliste angegeben, die durch die aktuelle Handlungsliste fortgesetzt wird, die Zustände von unsicheren Größen, die zur Ausführung der Handlungsliste gegeben sein müssen oder auch Zeitabhängigkeiten, die zur Ausführung der jeweiligen Handlungsliste erfüllt sein müssen. Die Bedingung HLcont = 0 gibt z. B. an, dass noch keine Handlungsliste vorliegt, bei welcher der Handlungsablauf fortzusetzen ist. D: h., HL 1 ist die erste Handlungsliste, die zur Ausführung kommt. HLcont ist eine Variable des Crew-Moduls, die die

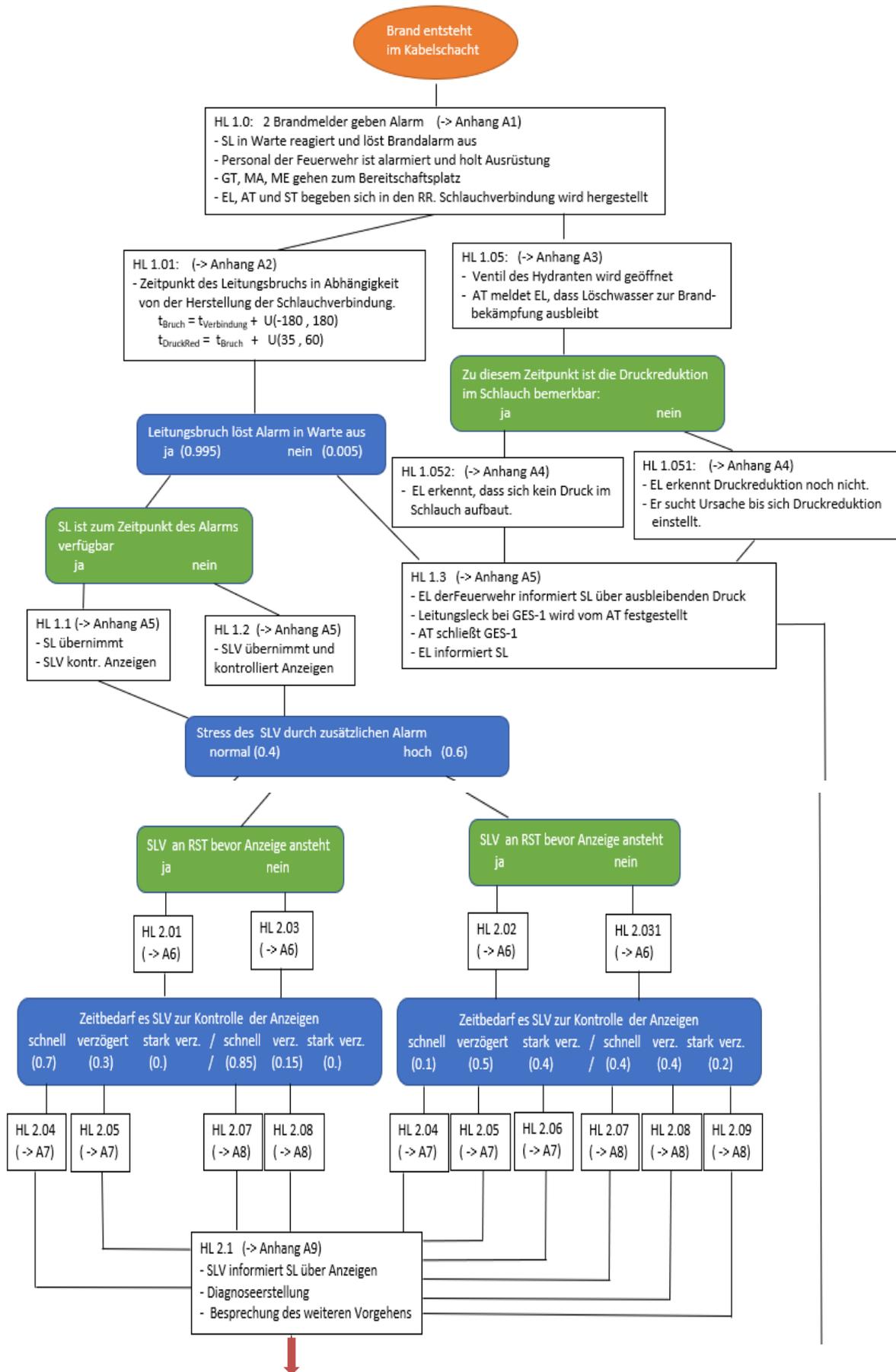
Nummer derjenigen Handlungsliste angibt, auf der die aktuelle Handlungsliste aufsetzt und fortgeführt wird. HLcont muss obligatorisch in jeder Bedingung einer Handlungsliste spezifiziert werden.

- Nach der Bedingung folgt eine Liste von Basishandlungen, die durch die verschiedenen Personen ausgeführt werden. Eine Basishandlung wird als eine 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. Einsatzleiter informiert Schichtleiter, dass der Brand gelöscht ist). Jeder Basishandlung sind Attribute zugeordnet, die eine nähere Beschreibung der Basishandlung erlauben. Die Definition der Basishandlungen ist bisher auf folgende Attribute beschränkt:
 - Person, welche die Handlung ausführt,
 - Person oder technische Komponente, welche durch die Basishandlung beeinflusst wird,
 - Ausführungszeit der Basishandlung,
 - kurze Beschreibung der Basishandlung (optional).

Die einzelnen Verzweigungen in Abb. 6.3 ergeben sich aus den berücksichtigten unsicheren Größen und aus den zeitlichen Wechselwirkungen, die für den Handlungsablauf modelliert worden sind. Die im Modell berücksichtigten unsicheren Größen sind im vorhergehenden Abschnitt 6.1 erläutert.

Die Besonderheit der Modellierung eines Handlungsablaufs mit den in der GRS entwickelten Methoden zur dynamischen PSA besteht darin, dass stochastische Einflüsse (aleatorische Unsicherheiten), zeitliche Wechselwirkungen, Abhängigkeiten von Prozess- bzw. Systemzuständen aber auch Unsicherheiten bzgl. Stressentwicklungen und Stressauswirkungen berücksichtigt werden können. Um diese Möglichkeiten zu demonstrieren, wurden in das Handlungsmodell zusätzlich Unsicherheiten bzgl. der Stressentwicklung und Stressauswirkung, sowie verschiedene zeitliche Wechselwirkungen eingebunden. Auch wenn durch sie zunächst keine signifikanten Auswirkungen auf den Handlungsablauf zu erwarten sind, wurden sie dennoch modelliert, um zu zeigen, welche Modellierungsmöglichkeiten die fortschrittlichen Methoden zur dynamischen PSA bieten.

Um die modellierten Abhängigkeiten des Handlungsablaufs besser zu veranschaulichen, wurde das in Tab. 6.5 dargestellte Ablaufdiagramm erstellt.



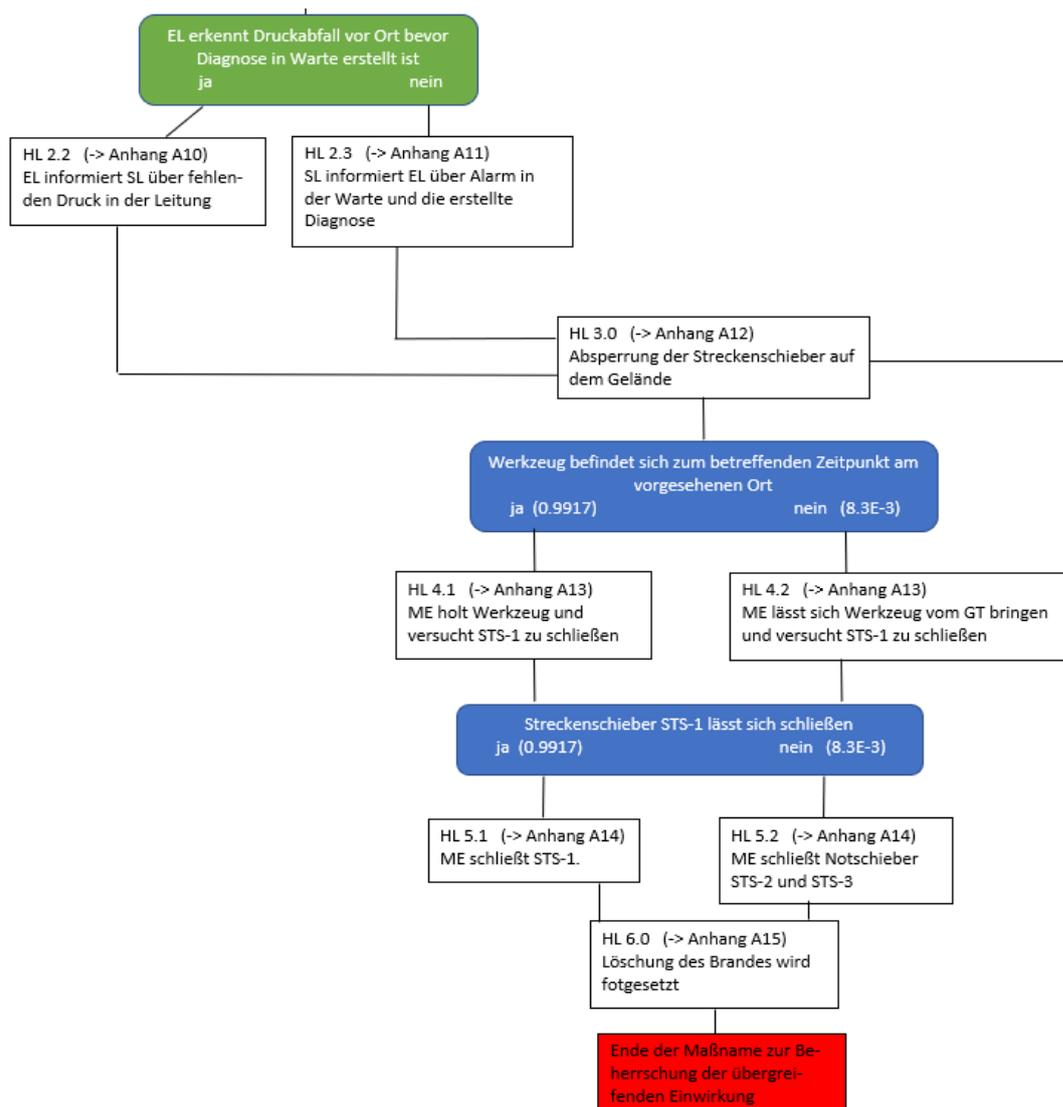


Abb. 6.5 Ablaufdiagramm der Notfallmaßnahme in Abhängigkeit von Unsicherheiten, Systemzuständen und zeitlichen Wechselwirkungen

Durch das Ablaufdiagramm der Notfallmaßnahme in Tab. 6.5 soll die modellierte Abhängigkeitsstruktur des Handlungsablaufs veranschaulicht werden. Dabei werden die Handlungslisten aufgeführt, die sich in Abhängigkeit der verschiedenen Situationen aus den berücksichtigten Unsicherheiten und zeitlichen Wechselwirkungen ergeben. Die blauen Knoten beschreiben die stochastischen Einflussgrößen (aleatorische Unsicherheiten), die grünen Knoten die Abhängigkeiten des Handlungsablaufs aufgrund zeitlicher Wechselwirkungen.

In HL 1.0 werden die Aktionen des Anlagenpersonals beschrieben, die durch den Brandalarm ausgelöst werden (siehe Anhang A, Tab. A. 1). In HL 1.01 wird der Leitungsbruch in Abhängigkeit von dem Zeitpunkt modelliert, zu welchem die Schlauchverbindung zum Hydranten hergestellt ist (siehe Anhang A, Tab. A. 2). Für die Modellierung wurde angenommen, dass

der Bruch der Feuerlöschwasserleitung 3 min vor bzw. 3 min nach der Herstellung der Schlauchverbindung erfolgt. Aufgrund des Leitungsbruchs sollte in der Warte ein Alarm ausgelöst werden. Im Handlungsmodell wird die Möglichkeit berücksichtigt, dass nach dem Leitungsbruch der Alarm in der Warte nicht ausgelöst wird. Diese Unsicherheit wird Abb. 6.5 durch den blauen Knoten angezeigt, welcher der HL 1.01 folgt.

In Abhängigkeit davon, ob der Alarm in der Warte ausgelöst wird oder nicht, erfolgen unterschiedliche Handlungsabläufe. Wenn der Alarm ausgelöst wird, hängen die weiteren Abläufe von der Situation ab, ob der Schichtleiter zum Zeitpunkt des Alarms verfügbar ist oder nicht. Diese Situation, ob der Schichtleiter verfügbar ist oder nicht, wird nicht durch die Angabe einer Wahrscheinlichkeit bestimmt, sondern durch die Zeit, wie lange der Schichtleiter durch andere Aufgaben beschäftigt ist. Die Abhängigkeit des weiteren Handlungsablaufs ist deshalb durch eine zeitliche Wechselwirkung gekennzeichnet. Ist der Schichtleiter verfügbar, wird HL 1.1 ausgeführt. Falls er noch beschäftigt und nicht verfügbar ist, werden die Basishandlungen der HL 1.2 aktiviert. HL 1.1 und HL 1.2 werden in Anhang A, Tab. A. 5 detailliert beschrieben.

Falls der Alarm in der Warte nicht ausgelöst wird, werden die Basishandlungen der HL 1.3 (siehe Anhang A, Tab. A. 5) aktiviert.

In HL 1.05 (siehe Anhang A, Tab. A. 3) wird der Ablauf bis zum Erkennen, dass Löschwasser ausbleibt, modelliert. Danach erfolgt der weitere Ablauf in Abhängigkeit davon, ob sich zu diesem Zeitpunkt die Druckreduktion im Schlauch schon bemerkbar macht oder nicht. Falls sie sich bemerkbar macht, wird HL 1.052 ausgeführt, ansonsten HL 1.051. Der Unterschied, der sich an dieser Stelle im Handlungsablauf ergibt, besteht nur in einer gewissen zeitlichen Verzögerung, wann der Einsatzleiter den Druckabfall in der Leitung erkennt. Obwohl diese Verzögerung keine besondere Relevanz im Handlungsablauf hat, wurde sie dennoch eingebaut, um die Modellierungsmöglichkeiten des Crew-Moduls zu demonstrieren.

Die restlichen Handlungslisten, die den weiten Handlungsablauf beschreiben, sind ausführlich in den Tabellen Tab. A. 1 bis Tab. A. 15 in Anhang A beschrieben.

6.3 Probabilistische Auswertung und Diskussion der Simulationsergebnisse

Eine Zielsetzung in dieser Arbeit besteht unter anderem darin, die Modellierungs- und Analysemöglichkeiten der GRS-Methoden zur dynamischen PSA am Beispiel übergreifender Einwirkungen unter erschwerten Bedingungen zu demonstrieren. Das in Abschnitt 6.2 beschriebene Modell dient dabei als Anwendungsbeispiel einer Notfallmaßnahme bei übergreifenden

Einwirkungen. Bei der Maßnahme wurden stochastische Einflüsse, Unsicherheiten bzgl. der Stressentwicklung und Stressauswirkung sowie zeitliche Wechselwirkungen im Handlungsablauf berücksichtigt. In Bezug auf die Auswertung der Simulationsergebnisse wurde in erster Linie auf die Ermittlung der Zeitverteilungen unter bestimmten Bedingungen eingegangen. Zusätzlich können aber auch Mittelwert oder mittlere Quantile der Zeiten über die Stichprobe der dynamischen Ereignisbäume mit ihren zugehörigen ein- oder zweiseitigen 90 %-, 95 %- und 99%-Konfidenzintervallen berechnet werden, um den Schätzfehler aufgrund des Stichprobenumfangs zu ermitteln. Dies erfolgte jedoch in der nachfolgend dargestellten Auswertung nicht, da hier zunächst demonstriert werden soll, wie die Unsicherheiten der Ausführungszeiten relevanter Handlungen abgeschätzt werden können, die man dann als aleatorische Unsicherheiten in einer MCDET-Analyse verwenden kann.

Mit dem Crew-Modul wurden in Verbindung mit MCDET 2.400 Simulationen des Handlungsablaufs durchgeführt. Dabei wurden 100 dynamische Ereignisbäume im Rahmen einer Monte-Carlo-Simulation erzeugt, in denen Ausführungszeiten der Basishandlungen und andere aleatorische Unsicherheiten zufällig ausgespielt wurden. In jedem der 100 dynamischen Ereignisbäume wurden 24 verschiedene Sequenzen gerechnet. Die 24 Sequenzen ergeben sich aus den möglichen Kombinationen der im Modell definierten diskreten Zufallsvariablen und zeitlichen Wechselwirkungen. Einen Überblick dazu liefert das Ablaufdiagramm in Tab 6.5.

Ein wesentlicher Aspekt der Auswertung einer dynamischen Analyse mit dem Crew-Modul ist die Ermittlung von Zeitverteilungen, wann relevante Handlungen ausgeführt worden sind. Diese Zeitverteilungen liefern neben der Wahrscheinlichkeit, dass bestimmte Handlungen ausgeführt werden, auch die Wahrscheinlichkeiten dafür, dass die Handlungen in bestimmten Zeitintervallen ausgeführt werden. Ein weiterer wesentlicher Aspekt besteht darin, dass über die Ermittlung bedingter Wahrscheinlichkeitsverteilungen die Auswirkung stochastischer Einflussgrößen auf die Zeitverteilungen quantifiziert werden kann. Dies soll im Folgenden anhand einiger ausgewählter Beispiele veranschaulicht werden.

Für die Löschung des Brandes ist es bei einem gleichzeitig erfolgten Bruch in der Feuerlöschwasserleitung notwendig, dass der Gebäudeeintrittsschieber GES-1 und der Streckenschieber STS-1 auf dem Gelände abgesperrt werden. Diese beiden Aktionen sind somit von erheblicher Bedeutung, da durch die Absperrungen zum einen die Überflutung im Ringraum gestoppt wird. Zum anderen sind diese Aktionen notwendig, damit sich durch die Absperrungen der Druck in der Feuerlöschwasserleitung wieder aufbauen und die Löschung des Brandes fortgeführt werden kann. In den Auswertbeispielen soll demonstriert werden, wie die Auswirkungen von unsicheren Einflussgrößen auf die Ausführungszeiten wichtiger

Handlungen quantifiziert werden können. Für die Auswertbeispiele werden dafür Fragestellungen zugrunde gelegt, in denen die Zeitverteilungen in Abhängigkeit der berücksichtigten unsicheren Größen ermittelt und miteinander verglichen werden, z. B.:

- Zeitdauer, bis GES-1 nach Leitungsbruch geschlossen wird in Abhängigkeit davon, ob nach dem Bruch der Leitung Alarm ausgelöst wird oder nicht, und von der Stressentwicklung des Schichtleiter-Stellvertreters.
- Zeitpunkt, zu dem STS-1 abgesperrt wird in Abhängigkeit vom Alarm, vom Stress des Schichtleiter-Stellvertreters, ob das notwendige Werkzeug zum Schließen des Streckenschiebers vor Ort verfügbar ist und davon, ob sich STS-1 schließen lässt oder nicht.

Eine wichtige Eigenschaft der verwendeten GRS-Methodik zur dynamischen PSA, die in den Auswertbeispielen besonders herausgestellt werden soll, ist die Möglichkeit zur Erzeugung bedingter Wahrscheinlichkeitsverteilungen und deren Verwendung zur Quantifikation der Auswirkungen stochastischer Einflussgrößen. Dies soll beispielhaft an einigen der oben genannten Fragestellungen demonstriert werden.

Eine Annahme für den Handlungsablauf bestand darin, dass der Leitungsbruch in Abhängigkeit vom Zeitpunkt der Herstellung der Schlauchverbindung erfolgt. Die Abhängigkeit bestand darin, dass der Leitungsbruch zu einer Zufallszeit zwischen 0 und 3 min vor oder nach der Herstellung der Schlauchverbindung erfolgt. Unter Berücksichtigung dieser Abhängigkeit ergeben sich die in Abb. 6.6 dargestellten Verteilungen der Zeitpunkte, wann die Schlauchverbindung mit dem Hydranten hergestellt ist und der Leitungsbruch erfolgt.

Aus den Verteilungen in Abb. 6.6 ist abzulesen, dass nach dem Brandalarm die Schlauchverbindung mit dem Hydranten zwischen ca. 14 und 20 min hergestellt wird. Da der Leitungsbruch zu einem zufälligen Zeitpunkt zwischen 0 und 3 min vor oder nach der Herstellung der Schlauchverbindung erfolgt, ist es plausibel, dass die Zeitverteilung des Leitungsbruchs eine größere Streuung aufweist und zwischen etwa 12 und 22,5 min nach dem Beginn des Brandes erfolgt. Die Verteilungen wurden hauptsächlich zur Überprüfung der Plausibilität bzgl. der Abhängigkeiten der simulierten Zeiten dargestellt. Die 5 %-, 50 %- und 95 %-Quantile der Zeitverteilung des Leitungsbruchs sind in Tab. 6.2 angegeben.

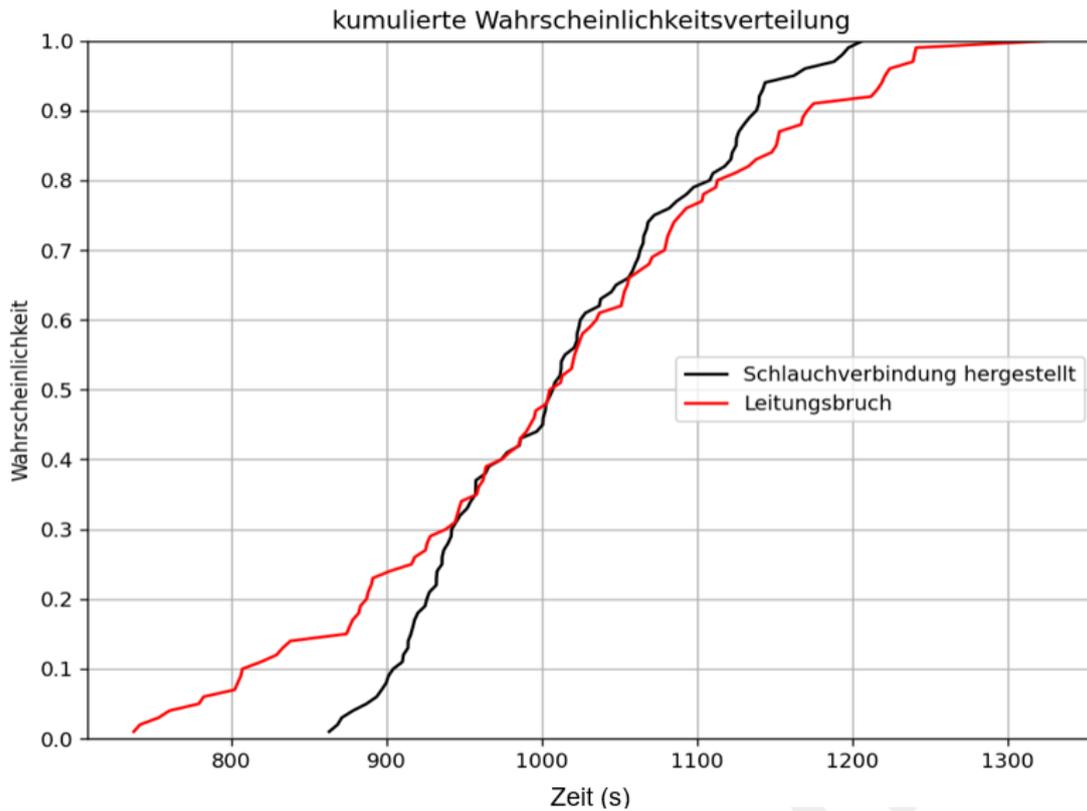


Abb. 6.6 Kumulierte Verteilungsfunktion der Zeiten, wann ein Leitungsbruch nach Auslösung des Brandalarms erfolgt und die Schlauchverbindung zum Hydranten hergestellt ist

Wie oben bereits erwähnt, ist es nach dem Bruch in der Feuerlöschwasserleitung wichtig, dass der Gebäudeeintrittsschieber GES-1 und der Streckenschieber STS-1 auf dem Gelände möglichst schnell abgesperrt werden. Abb. 6.7 zeigt die kumulierten Verteilungsfunktionen bzgl. der Zeitdauern, bis GES-1 und STS-1 nach dem Leitungsbruch durch das Personal abgesperrt werden können.

Man erkennt anhand der Tatsache, dass sich die kumulierten Wahrscheinlichkeiten der Zeitpunkte des Leitungsbruchs (vgl. Abb. 6.6) sowie bzgl. der Zeitdauern, bis GES-1 abgesperrt ist (siehe Abb. 6.7, schwarze Kurve) zu 1 aufsummieren, dass der Leitungsbruch als auch die Absperrung von GES-1 mit Sicherheit eintritt. Dies entspricht den Annahmen, die für die Modellierung getroffen wurden. Etwas anders stellt sich die Situation bzgl. der Absperrung des Streckenschiebers STS-1 dar. Hier wurde die Möglichkeit in Betracht gezogen, dass sich der Streckenschieber mit einer Wahrscheinlichkeit von 0,01 nicht schließen lässt. Dies drückt sich in der kumulierten Verteilungsfunktion dadurch aus, dass sich die Wahrscheinlichkeit für die Absperrung von STS-1 nur auf 0,99 aufsummiert, wie in Abb. 6.7 an der

blauen Kurve zu erkennen ist. Anhand der blauen Kurve kann beispielsweise die Aussage gemacht werden, dass mit einer Wahrscheinlichkeit von 0,99 der Streckenschieber STS-1 innerhalb von 30 min nach dem Leitungsbruch abgesperrt werden kann.

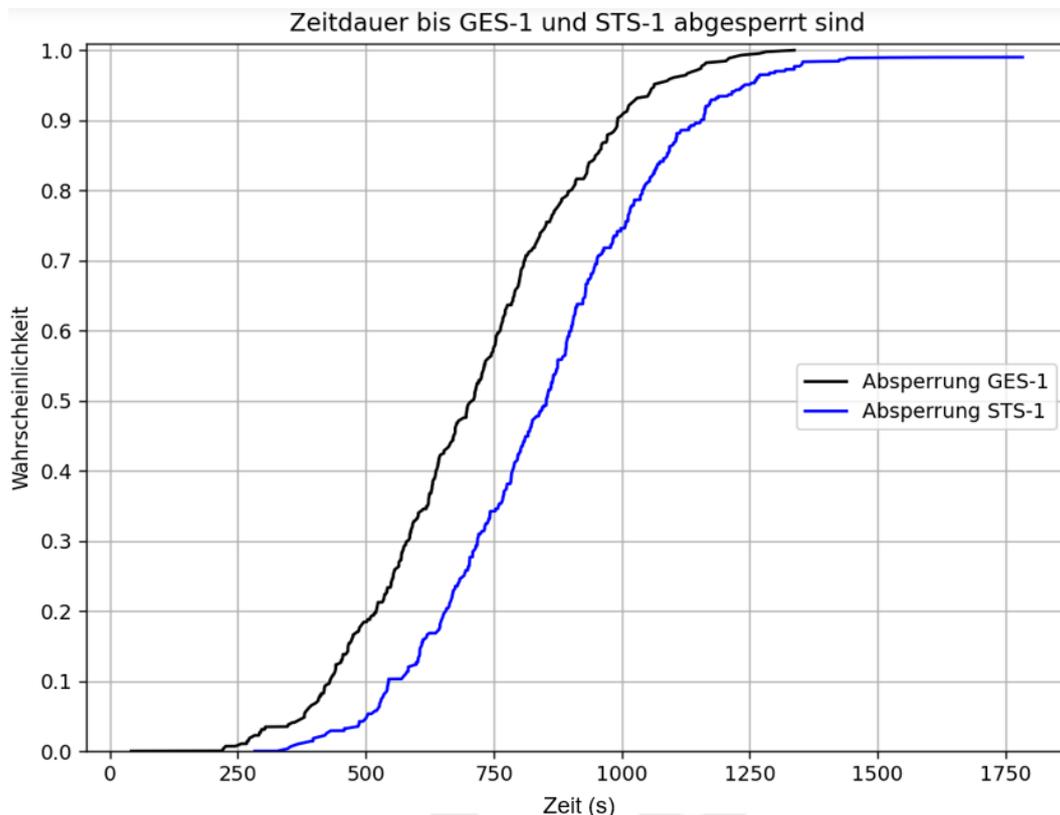


Abb. 6.7 Kumulierte Verteilungsfunktionen der Zeitspannen, bis GES-1 und STS-1 nach dem Leitungsbruch abgesperrt werden

Aus den kumulierten Verteilungsfunktionen lassen sich zwar verschiedene statistische Kenngrößen berechnen sowie die Variation der Zeiten erkennen, wann das Leck eingetreten ist bzw. wann GES-1 oder der Streckenschieber STS-1 abgesperrt wurden. Oftmals interessieren aber auch die Zeitspannen, die zwischen zwei Zeitpunkten liegen. Aus dem Vergleich der Verteilungen, wie z. B. in Abb. 6.7, lassen sich solche Zeitspannen, wie beispielsweise die Zeitspanne zwischen der Absperrung von GES-1 und der Absperrung von STS-1, nicht ermitteln. Dazu müssen die Abhängigkeiten der beiden Zeitpunkte bzgl. jeder Sequenz berücksichtigt werden. Das Crew-Modul und die Auswerteroutinen des Post-Processing wurden so weiterentwickelt, dass auch diese Zeitabhängigkeiten bzgl. jeder gerechneten Sequenz von Handlungsabläufen berücksichtigt und ausgewertet werden können.

In Abb. 6.8 ist die Wahrscheinlichkeitsverteilung der Zeitdifferenz zwischen den Absperrzeiten von GES-1 und STS-1 unter Berücksichtigung der Zeitabhängigkeiten in den einzelnen Se-

quenzen angegeben. Aus der Verteilung der Zeitdifferenz der Absperrzeiten erkennt man, dass die Absperrung von STS-1 länger dauert als die Absperrung von GES-1.



Abb. 6.8 Wahrscheinlichkeitsverteilung der Zeitdauer, bis STS-1 nach der Schließung von GES-1 abgesperrt wird

Aus den Verteilungsfunktionen in Abb. 6.6 und Abb. 6.7 können verschiedene probabilistische Aussagen abgeleitet und probabilistische Kenngrößen ermittelt werden, wie z. B. der Mittelwert und die 5 %-, 50 % und 95 %-Quantile. In Tab. 6.2 werden diese Kenngrößen für den

- Zeitpunkt des Leitungsbruchs,
- Zeitdauer bis zur Absperrung von GES-1 nach Leitungsbruch,
- Zeitdauer bis zur Absperrung von STS1-1 nach Leitungsbruch,
- Zeitdauer zwischen Absperrung von GES-1 und STS-1

angegeben.

Tab. 6.2 Mittelwert und Quantile der Zeiten, wann der Leitungsbruch erfolgt, den Zeitdauern, wann GES-1 sowie STS-1 nach dem Eintritt des Leitungsbruchs abgesperrt werden können, sowie der Zeitdauer zwischen der Absperrung von GES-1 und STS-1

Quantil	Zeitdauer bis zur Absperrung von GES-1 (nach Abb. 6.7)	Zeitdauer bis zur Absperrung von STS-1 (nach Abb. 6.7)	Zeitdauer zwischen Absperrung von GES-1 und STS-1 (nach Abb. 6.8)	Zeitpunkt des Leitungsbruchs (nach Abb. 6.6)
5 %	380 s	502 s	72 s	779 s
50 %	708 s	853 s	142 s	1005 s
95 %	1063 s	1240 s	191 s	1221 s
Mittelwert	709 s	837 s	135 s	1006 s

Aus den Verteilungsfunktionen in Abb. 6.7 kann abgelesen werden, dass nach dem Leitungsbruch die Absperrung des Streckenschiebers STS-1 mit einer Wahrscheinlichkeit von 90 % zwischen ca. 8 und 20,5 min gelingt und die Absperrung von GES-1 mit einer Wahrscheinlichkeit von 90 % zwischen ca. 6 und 18 min. Mit einer Wahrscheinlichkeit von ca. 5 % kann STS-1 eher als 12 min geschlossen werden. Allerdings können mit einer Wahrscheinlichkeit von 5 % auch Zeiten bis ca. 30 min auftreten, bis der Streckenschieber nach dem Leitungsbruch geschossen werden kann.

Aus der Wahrscheinlichkeitsverteilung in Abb. 6.8 erkennt man, dass sich der größte Anteil (ca. 99 %) der Zeitdauern zwischen der Absperrung von GES-1 und STS-1 in dem Bereich zwischen knapp 1 min und 4 min bewegt. Allerdings erkennt man auch, dass mit einer geringen Wahrscheinlichkeit (ca. 1 %) Zeitdauern zwischen den Absperrungen auftreten, die größer als 4 min sind und bis zu 8,5 min in Anspruch nehmen.

In solchen Situationen interessiert oftmals die Frage, durch welche Einflüsse eine solch hohe Variation verursacht wird. Bei derartigen Untersuchungen zeigt sich ein wesentlicher Vorteil der GRS-Methoden zur dynamischen PSA. Wie in den vorhergehenden Abschnitten 6.1 und 6.2 erläutert, wurde der Handlungsablauf unter Berücksichtigung von Unsicherheiten und zeitlichen Abhängigkeiten modelliert und simuliert. Aus den Simulationsergebnissen können nun die Einflüsse bestimmter unsicherer Größen ausgewertet und quantifiziert werden. Dies soll zunächst am Beispiel der in Abb. 6.7 dargestellten Verteilung der Zeitdauer zwischen dem Leitungsleck und der Absperrung von STS-1 demonstriert werden.

Eine unsichere Größe, die im Handlungsmodell berücksichtigt wurde, besteht darin, ob nach dem Bruch der Feuerlöschwasserleitung ein Alarm in der Warte ausgelöst wird oder nicht. Es soll nun untersucht werden, ob diese Unsicherheit einen Einfluss auf die Zeit hat, die benötigt wird, um nach dem Eintritt des Lecks den Streckenschieber STS-1 abzusperren. Um den Einfluss stochastischer Variablen auf eine Prozessgröße zu quantifizieren, werden bedingte Wahrscheinlichkeitsverteilungen berechnet und miteinander verglichen. Im zu untersuchenden Beispiel werden die bedingten Wahrscheinlichkeitsverteilungen der Zeitdauern in Abhängigkeit davon ermittelt, ob der Alarm in der Warte nach Leitungsbruch ausgelöst wird oder nicht.

Diese Ereignisse treten mit sehr unterschiedlichen Wahrscheinlichkeiten auf. Die Wahrscheinlichkeit, dass ein Alarm ausgelöst wird, wurde im Modell mit 0,995, und die Wahrscheinlichkeit, dass der Alarm nicht ausgelöst wird, mit 0,005 angenommen. Um die Wahrscheinlichkeitsverteilungen der Ereignisse unabhängig von ihren Eintrittswahrscheinlichkeiten miteinander vergleichen zu können, werden die bedingten Wahrscheinlichkeitsverteilungen ermittelt, die in Form einer kumulierten Verteilungsfunktion in Abb. 6.9 dargestellt sind.

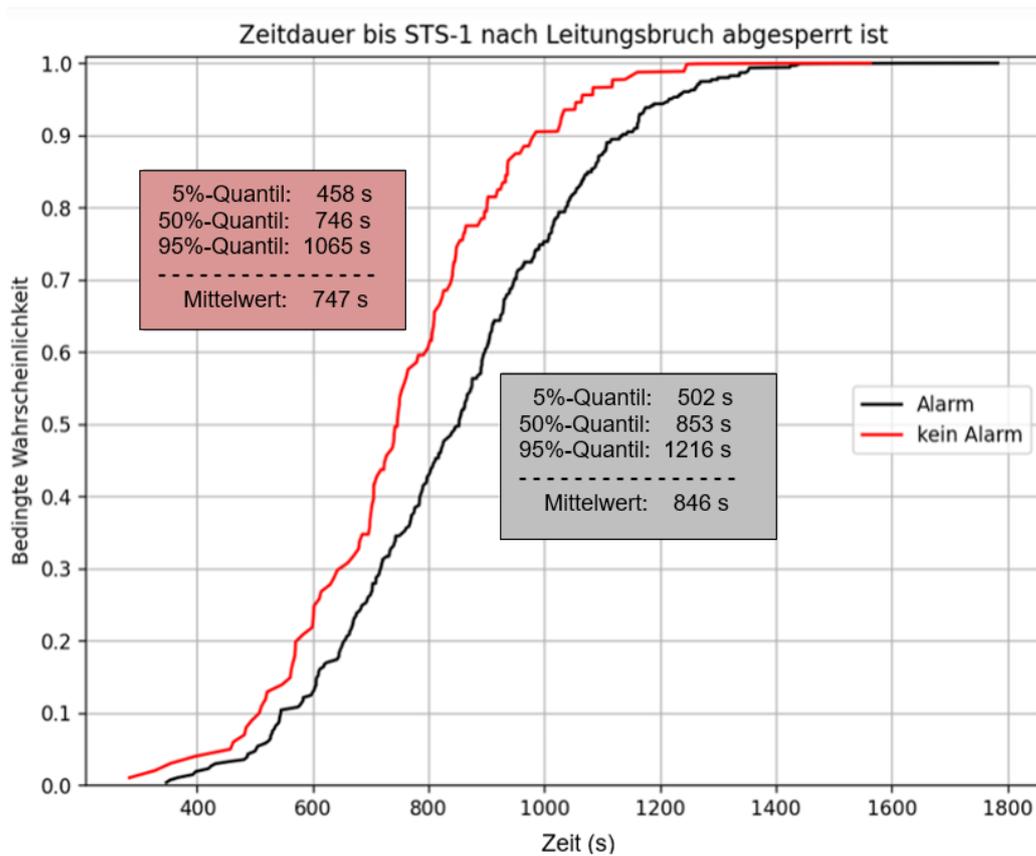


Abb. 6.9 Bedingte Verteilungsfunktion der Zeitdauern zwischen Eintritt des Lecks und Absperrung von STS-1 in Abhängigkeit von der Auslösung des Alarms

Aus den bedingten Verteilungen in Abb. 6.9 erkennt man, dass es bei der Auslösung des Alarms in der Warte gegenüber der Situation, in welcher der Alarm nicht ausgelöst wird, etwas länger dauert, bis der Schieber STS-1 nach dem Leitungsbruch abgesperrt ist. Dies liegt in erster Linie an den Zeitspannen, die für die Kontrollen der Anzeigen auf der Reaktorschutz- und der Brandschutztafel erforderlich sind, sowie an der Diagnosefindung und Kommunikation zwischen Schichtleiter, Schichtleiter-Stellvertreter und Einsatzleiter. Wenn der Alarm nicht ausgelöst wird, jedoch der Einsatzleiter der Feuerwehr den Druckabfall bemerkt und dem Schichtleiter in der Warte meldet, liegen dem Personal in der Warte wesentliche Informationen vor, die eine schnellere Kontrolle der Anzeigen und Diagnosefindung ermöglichen. Dies gilt allerdings nur für den Fall, dass sich die Feuerwehr aufgrund des Brandes im Ringraum des Reaktorgebäudes befindet.

Wie aus dem Vergleich der Verteilungen jedoch ersichtlich, sind die Unterschiede in den Zeiten nicht gravierend. Im Mittel handelt es sich um ca. 1 – 2 min Zeitverzögerung bis zur Absperrung des Streckenschiebers STS-1, die durch die unsichere Größe der Alarmauslösung nach Leitungsbruch verursacht wird.

Einen größeren Einfluss könnte man jedoch vermuten, den die Stressentwicklung des Schichtleiter-Stellvertreter SLV auf die Zeitdauer hat, bis STS-1 abgesperrt werden kann. Diese Einflüsse werden nachfolgend untersucht.

Im Modell wurde angenommen, dass mit dem hohen Stresslevel eine höhere Wahrscheinlichkeit verbunden ist, dass der SLV bei der Kontrolle der Anzeigen mehr Zeit benötigt. Im Folgenden soll die Auswirkung auf die Zeitdifferenz zwischen Leitungsbruch und Absperrung des Streckenschiebers STS-1 unter den Bedingungen untersucht werden, dass der Stresslevel des SLV normal bzw. hoch ist.

In Abb. 6.10 wird mittels der bedingten Verteilungsfunktionen dargestellt, inwieweit der Faktor Stress die Zeiten beeinflusst, bis der Streckenschieber nach dem Leitungsbruch abgesperrt werden kann. Der Vergleich der bedingten Verteilungen zeigt, dass der Stress des SLV, so wie er für den Handlungsablauf modelliert wurde, einen ähnlich geringen Effekt auf die Zeiten hat, wie die Unsicherheit, ob der Alarm nach dem Leitungsbruch ausgelöst wird oder nicht (vgl. Abb. 6.9). Gegenüber normalem Stress erhöhen sich bei hohem Stress die Zeiten, bis der Streckenschieber nach dem Leitungsbruch abgesperrt ist, im Mittel um etwa 1,5 min. Des Weiteren lassen sich aus den bedingten Verteilungen z. B. folgende probabilistische Aussagen ableiten:

- Unter der Bedingung, dass der Schichtleiter-Stellvertreter hohen Stress entwickelt, erfolgt die Abspernung des Streckenschiebers nach dem Leitungsbruch mit einer Wahrscheinlichkeit von 95 % in einem Zeitraum von etwa 6 bis 21 min. Unter der Bedingung, dass der Stresslevel auf normalem Niveau, erfolgt die Abspernung von STS-1 mit einer Wahrscheinlichkeit von 95 % in einem Zeitraum zwischen ca. 6 und 18,5 min.
- Die bedingte Wahrscheinlichkeit dafür, dass die Abspernung innerhalb von 10 min gelingt, beträgt bei normalem Stress 0,18 und bei hohem Stress 0,1.
- Die bedingte Wahrscheinlichkeit, dass die Abspernung in einem Zeitraum zwischen 10 min und 15 min gelingt, beträgt bei normalem Stress ca. 0,53 und bei hohem Stress ca. 0,44.

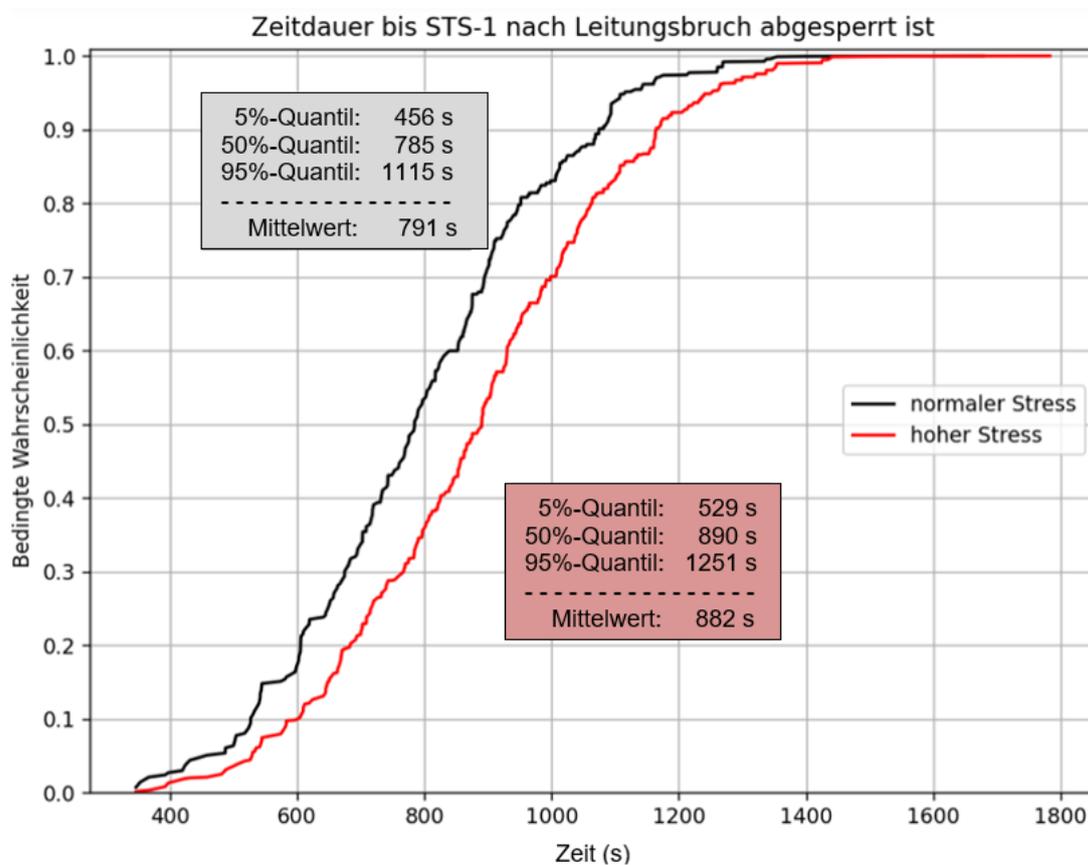


Abb. 6.10 Bedingte Verteilungsfunktion der Zeitdauern zwischen Eintritt des Lecks und Abspernung von STS-1 in Abhängigkeit von der Stressentwicklung des SLV

Aus den bedingten Verteilungen in Abb. 6.10 erkennt man auch, dass sich mit einer Wahrscheinlichkeit von 1% Zeiten ergeben, die deutlich höhere Werte aufweisen als die angegebenen 95 %-Quantile der beiden Stressniveaus. Dies erkennt man daran, dass sich die Verteilungen im oberen 1 %-Bereich weit zu hohen Zeitwerten hin ausdehnen. Zwar treten diese

sehr hohen Zeitwerte nur mit sehr kleinen Wahrscheinlichkeiten auf. Es kann dennoch grundsätzlich wichtig sein zu untersuchen, durch welche Einflüsse diese hohen Absperrzeiten verursacht werden, um ggf. sicherheitstechnische Verbesserungen durchführen zu können.

Weitere stochastische Größen, die im Handlungsmodell berücksichtigt wurden, betreffen die Unsicherheit, ob das Werkzeug vor Ort zum Öffnen der Abdeckung und zum Schließen des Schiebers verfügbar ist oder es sich aus irgendwelchen Gründen nicht vor Ort befindet. Abb. 6.11 zeigt die entsprechenden bedingten Verteilungsfunktionen der Absperrzeiten des Streckenschiebers STS-1 nach Leitungsbruch. Eine andere Darstellung ist durch die dazugehörigen bedingten Wahrscheinlichkeitsverteilungen in Abb. 6.12 angegeben.

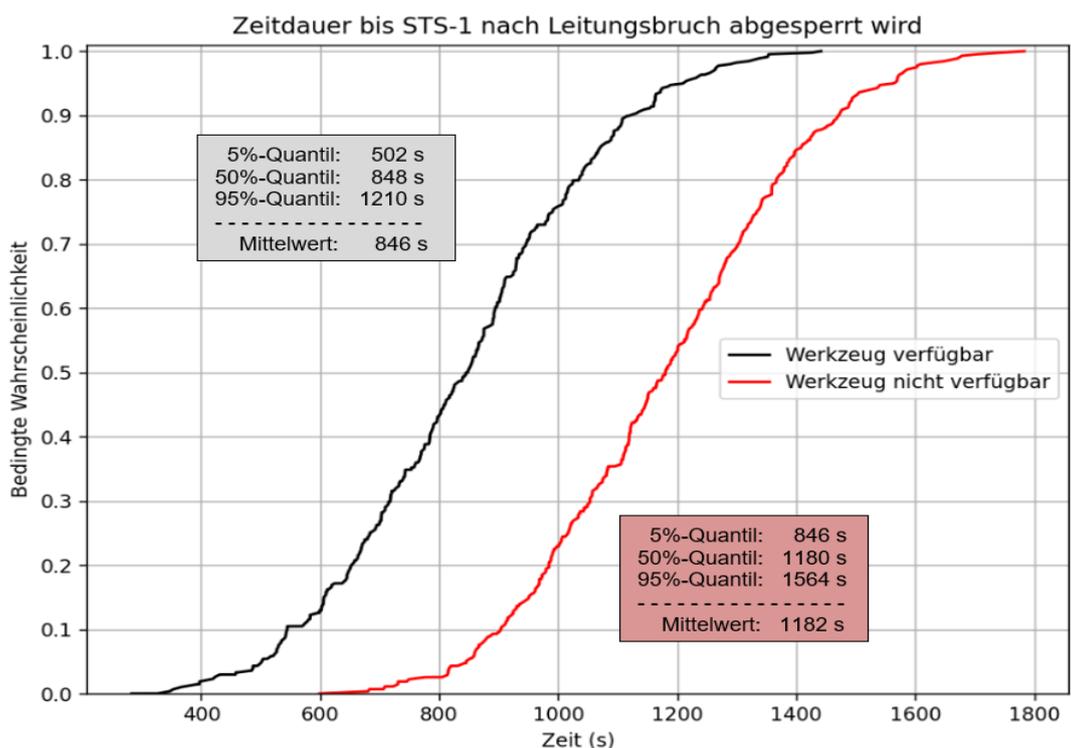


Abb. 6.11 Bedingte Verteilungsfunktion der Zeitdauern zwischen Leitungsbruch und Absperrung von STS-1 abhängig von der Verfügbarkeit des Werkzeugs

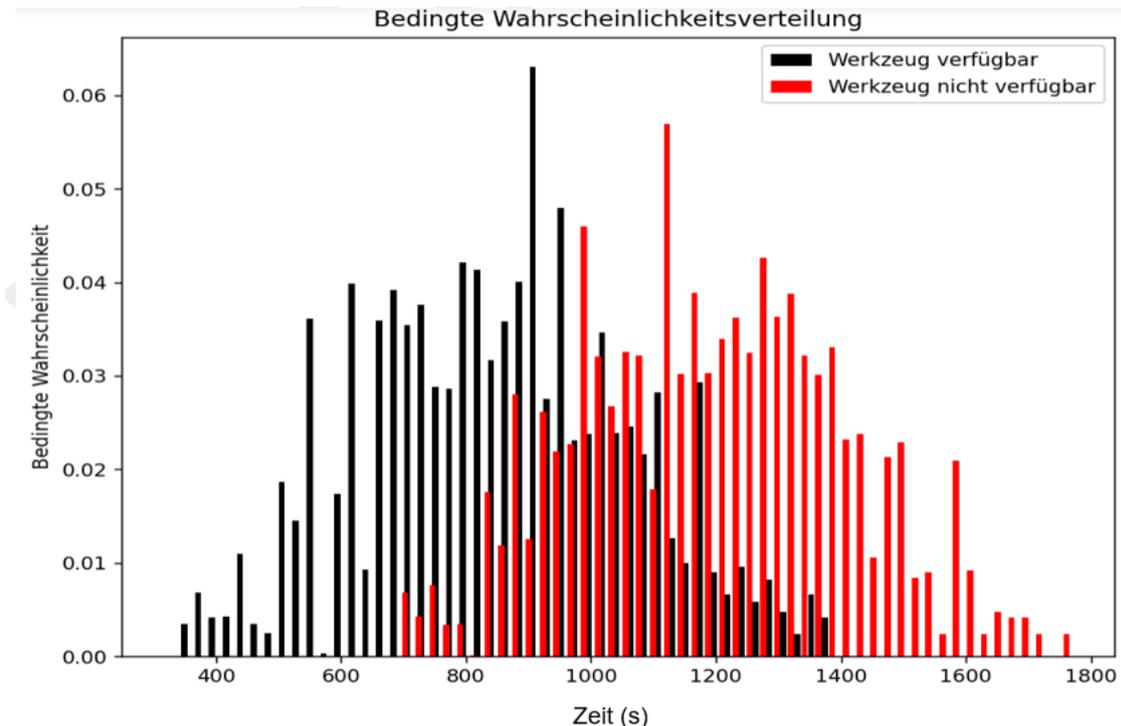


Abb. 6.12 Bedingte Wahrscheinlichkeitsverteilung der Zeitdauern zwischen Leitungsbruch und Absperrung von STS-1 abhängig von der Verfügbarkeit des Werkzeugs

Die Verzögerung der Absperrung des Streckenschiebers STS-1 infolge der Situation, dass sich das erforderliche Werkzeug nicht vor Ort befindet, beträgt knapp 6 min. Im Fall, dass sich das Werkzeug vor Ort befindet, wird der Streckenschieber STS-1 mit einer Wahrscheinlichkeit von 95 % in einem Zeitraum zwischen ca. 6 und 20 min abgesperrt. Die Wahrscheinlichkeit, dass die Absperrung unter der gegebenen Bedingung länger als 20 min dauert, beträgt ca. 5%, d. h.

$$p(\text{Absperrung von STS-1} > 20 \text{ min} \mid \text{Werkzeug vor Ort verfügbar}) = 0,05.$$

Befindet sich das Werkzeug nicht vor Ort, erfolgt die Absperrung mit einer Wahrscheinlichkeit von 95 % in einem Zeitraum zwischen ca. 11 und 26 min. In diesem Fall beträgt die bedingte Wahrscheinlichkeit, dass die Absperrung länger als 20 min dauert, ca. 0,47, d. h.

$$p(\text{Absperrung von STS-1} > 20 \text{ min} \mid \text{Werkzeug nicht vor Ort verfügbar}) = 0,47.$$

Es soll hier nochmals betont werden, dass sich diese Aussagen auf die bedingten Wahrscheinlichkeitsverteilungen beziehen. Mit den Wahrscheinlichkeiten, dass das erforderliche Werkzeug vor Ort verfügbar ($p = 0,9917$) bzw. nicht verfügbar ist ($p = 0,0083$), können dann anhand

der Gleichung $P(A|B) \cdot P(B) = P(A \text{ und } B)$ z. B. die Wahrscheinlichkeiten folgender Ereignisse berechnet werden:

- $p(\text{Werkzeug vor Ort verfügbar und Zeit der Absperrung von STS-1} > 20 \text{ min}) = 0,046,$
- $p(\text{Werkzeug vor Ort nicht verfügbar und Zeit der Absperrung von STS-1} > 20 \text{ min}) = 0,0039.$

Aus diesen Werten kann man erkennen, dass die Wahrscheinlichkeit in beiden Fällen relativ gering ist, dass die Absperrzeit von STS-1 länger als 20 min dauert. Wenn man sich jedoch auf die Wahrscheinlichkeiten der bedingten Verteilungen bezieht, erkennt man, dass die Verfügbarkeit des Werkzeugs vor Ort einen relevanten Einflussfaktor bzgl. des Absperrzeitpunktes des Streckenschiebers darstellt. Aus der bisherigen Auswertung zeigt sich, dass die Verfügbarkeit des für die Absperrung erforderlichen Werkzeugs vor Ort bisher den größten Einfluss auf den Zeitpunkt hat, wann der Streckenschieber nach dem Leitungsbruch abgesperrt wird.

Abschließend soll zusätzlich der Einfluss untersucht werden, der sich aus der Unsicherheit ergibt, ob sich der Streckenschieber schließen lässt oder nicht. Die Wahrscheinlichkeit, dass sich der Streckenschieber STS-1 nicht schließen lässt, wurde im Modell mit 0,01 angenommen. In diesem Fall müssen die beiden Notschieber STS-2 und STS-3 geschlossen werden.

Die bedingten Verteilungsfunktionen, die in Abb. 6.13 dargestellt sind, zeigen die Absperrzeiten der Streckenschieber in Abhängigkeit der Verfügbarkeit des Werkzeugs und der Zuverlässigkeit an, dass sich der Streckenschieber STS-1 schließen lässt. Die Bedingungen beschreiben dabei die folgenden Situationen:

- **Bedingung 1:** Das erforderliche Werkzeug ist vor Ort verfügbar und der Streckenschieber STS-1 lässt sich schließen.
- **Bedingung 2:** Das erforderliche Werkzeug muss beschafft werden, da vor Ort nicht verfügbar und der Streckenschieber STS-1 lässt sich schließen.
- **Bedingung 3:** Das erforderliche Werkzeug ist vor Ort verfügbar und Absperrung über Notschieber.
- **Bedingung 4:** Das erforderliche Werkzeug muss beschafft werden, da vor Ort nicht verfügbar und Absperrung über Notschieber.

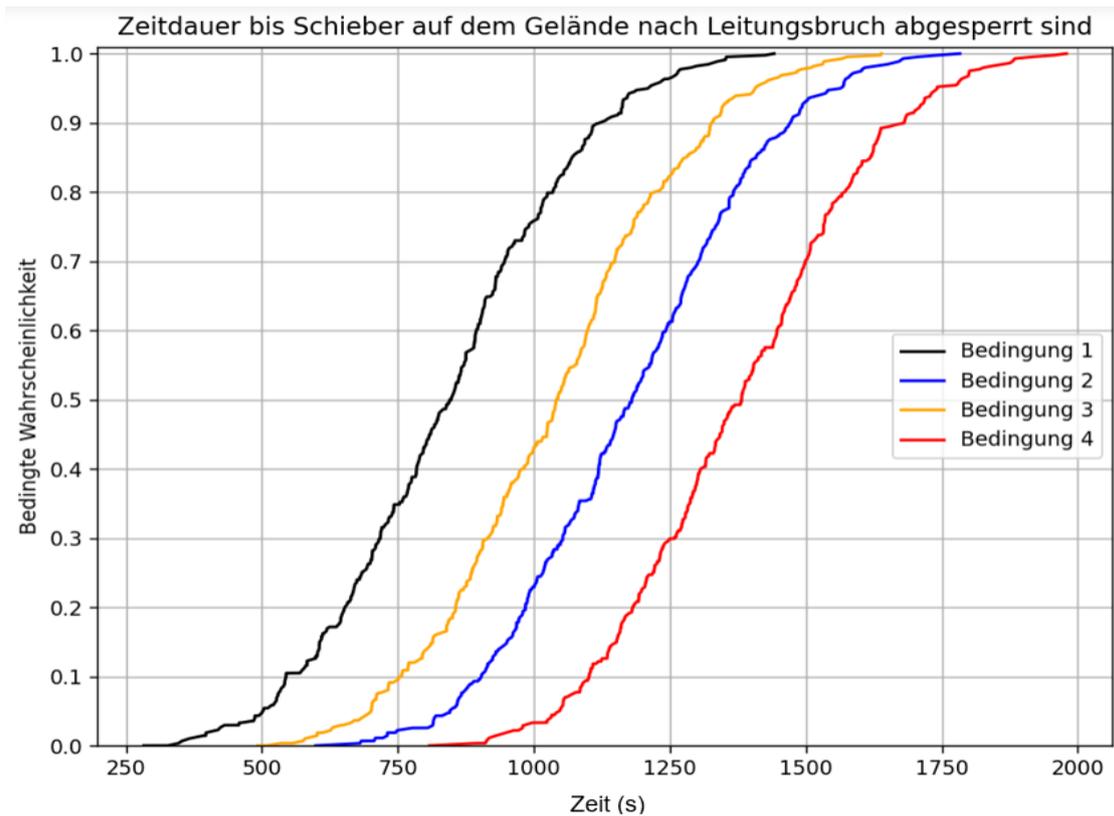


Abb. 6.13 Bedingte Verteilungsfunktionen der Absperrzeit der Streckenschieber in Abhängigkeit von der Verfügbarkeit des Werkzeugs vor Ort und der Zuverlässigkeit, dass sich STS-1 schließen lässt

Mittelwerte, zweiseitige Konfidenzintervalle sowie die 5 %-, 50 %- und 95 %-Quantile der Absperrzeiten von STS-1 bzgl. der bedingten Verteilungen sind in Tab. 6.3 angegeben.

Tab. 6.3 Mittelwert, zweiseitige 95%-Konfidenzintervalle und Quantile der Absperrzeit (s) der Streckenschieber in Abhängigkeit von der Verfügbarkeit des Werkzeugs vor Ort und der Zuverlässigkeit, dass sich STS-1 schließen lässt

Quantil	Absperrzeit unter Bedingung 1	Absperrzeit unter Bedingung 2	Absperrzeit unter Bedingung 3	Absperrzeit unter Bedingung 4
5 %	502 s	846 s	700 s	1047 s
50 %	848 s	1180 s	1042 s	1382 s
95 %	1210 s	1563 s	1407 s	1741 s
Mittelwert	843 s	1182 s	1043 s	1382 s
95 %-Konfidenzintervall	(421, 1265)	(758, 1606)	(618, 1467)	(956, 1808)

Wie zu erwarten, werden die schnellsten Absperrzeiten dann erreicht, wenn das für die Absperrung erforderliche Werkzeug vor Ort verfügbar ist und sich der Streckenschieber STS-1 schließen lässt (Bedingung 1). In diesem Fall dauert es im Mittel ca. 14 min, bis STS-1 nach dem Leitungsbruch geschlossen werden kann. Mit einer Wahrscheinlichkeit von 90 % dauert es in diesem Fall zwischen ca. 8 und 20 min, bis der Streckenschieber STS-1 nach dem Leitungsbruch abgesperrt werden kann.

Entsprechend ist zu erwarten, dass sich die längsten Zeiten bis zur Absperrung dann ergeben, wenn das für die Absperrung erforderliche Werkzeug vor Ort nicht verfügbar ist und sich der Schieber STS-1 nicht schließen lässt (Bedingung 4). Unter dieser Bedingung dauert es im Mittel ca. 23 min, bis die Notschieber nach Leitungsbruch geschlossen werden. Mit einer Wahrscheinlichkeit von 90 % dauert es in diesem Fall zwischen ca. 18 und 29 min, bis die Notschieber nach dem Leitungsbruch abgesperrt werden können.

Was nicht ohne Weiteres zu erwarten war ist die Tatsache, dass sich das fehlende Werkzeug vor Ort stärker auf die Absperrzeiten auswirkt als das Ereignis, dass sich der Streckenschieber STS-1 nicht schließen lässt. Noch weniger konnte vorhergesagt werden, welchen Einfluss die verschiedenen Ereigniskombinationen auf die Absperrzeiten haben. Durch die hier angewendete Methodik ist es möglich, die Auswirkung stochastischer Einflussfaktoren auf relevante Ergebnisgrößen (z. B. Zeitdauer bis Streckenschieber nach Leitungsbruch abgesperrt werden kann) probabilistisch zu quantifizieren.

Anhand der 95 %-Konfidenzintervalle und der Mittelwerte der bedingten Verteilungen kann man erkennen, dass sich die mittleren Absperrzeiten unter den Bedingungen 1 und 4 signifikant unterscheiden. Dies erkennt man daran, dass der Mittelwert der Verteilung unter Bedingung 1 nicht im 95 %-Konfidenzintervall der Bedingung 4 liegt und umgekehrt. Durch statistische Tests auf Verteilungsunterschiede könnte auch überprüft werden, ob sich die Verteilungen insgesamt und nicht nur die Mittelwerte signifikant unterscheiden. Dieser Test wurde jedoch an dieser Stelle nicht durchgeführt.

Bisher wurde nur auf die Wahrscheinlichkeiten der bedingten Verteilungen, wie sie in Abb. 6.13 dargestellt sind, eingegangen. Die Wahrscheinlichkeiten, mit denen die Situationen der Bedingungen 1 – 4 auftreten, sind jedoch sehr unterschiedlich, wie die nachfolgenden Werte zeigen:

- $p(\text{Bedingung 1}) = 9,818 \text{ E-}01,$
- $p(\text{Bedingung 2}) = 9,917 \text{ E-}03,$

- $p(\text{Bedingung 3}) = 8,22 \text{ E-}03$,
- $p(\text{Bedingung 4}) = 8,30 \text{ E-}05$.

Auch wenn die Eintrittswahrscheinlichkeit, dass das für die Absperrung erforderliche Werkzeug vor Ort nicht verfügbar ist und sich STS-1 nicht schließen lässt, mit $8,3 \text{ E-}05$ sehr gering ist, kann die Erkenntnis dennoch wichtig sein, dass diese Ereigniskombination zu einer signifikanten Erhöhung der Zeitdauern führt, bis die geborstene Feuerlöschwasserleitung abgesperrt werden kann. An dieser Stelle könnte man ansetzen, sich über Maßnahmen Gedanken zu machen, wie man diese Ereignisse, die zu den signifikanten Verzögerungen der Leitungsabsperrung führen, ausschließen kann. Auch wenn diese Ereignisse nur mit geringer Wahrscheinlichkeit auftreten, hilft eine solche Analyse diejenigen Ereignisse zu identifizieren, die unabhängig von ihren Eintrittswahrscheinlichkeiten sicherheitstechnisch relevante Auswirkungen haben können.

Abschließend wird kurz diskutiert, wie sich die probabilistischen Ergebnisse der dynamischen PSA bzgl. des zugrundeliegenden Szenarios anwenden lassen. In Bezug auf eine Überflutung des Reaktorgebäude-Ringraums können anhand der Ergebnisse in Tab. 6.3 beispielsweise folgende Schlüsse gezogen werden.

In Abschnitt 6.1.1 wurde beschrieben, mit welcher Mengenrate Wasser in den Ringraum strömt, wenn ein Bruch der Feuerlöschwasserleitung an der angenommenen Stelle eintritt. Unter Berücksichtigung bestehender Unsicherheiten wurde angenommen, dass nach einem Leitungsbruch Wasser mit einer Rate zwischen 140 und 180 kg/s in den Ringraum strömt, wobei die Werte zwischen 140 und 180 kg/s als gleichverteilt angenommen wurden. Über die in Abb. 6.13 ermittelten bedingten Zeitverteilungen kann nun berechnet werden, welche Überflutungshöhen unter den jeweiligen Bedingungen im Reaktorgebäude-Ringraum erreicht werden und ob dadurch sicherheitstechnisch relevante Komponenten betroffen sind.

In der Tab. 6.4 wurden die Überflutungshöhen berechnet, die bzgl. der vier oben genannten Bedingungen aufgrund des einströmenden Wassers erreicht werden. Als Referenzzeit, wie lange Wasser in den Ringraum einströmt, werden aus den jeweiligen Zeitverteilungen diejenigen Absperrzeiten gewählt, die mit einer Wahrscheinlichkeit von 95 % nicht überschritten werden. Dabei handelt es sich um die in Tab. 6.3 aufgeführten 95 %-Quantile der jeweiligen Verteilungen. Diese konservative Festlegung der Absperrzeiten dient zur Abschätzung, ob es in dem Modell überhaupt zu sicherheitstechnisch relevanten Überflutungen kommen kann und welche Sicherheitsmargen selbst mit den konservativ gewählten Zeiten noch eingehalten wer-

den können. Die unter den Bedingungen 1 – 4 in den Ringraum eintretenden Wassermengen und Überflutungshöhen in den jeweiligen vier Quadranten sind in Tab. 6.4 aufgeführt.

Tab. 6.4 In den Ringraum eingetretene Wassermenge und Wasserhöhe in den vier Quadranten in Abhängigkeit der Wassereintrittsrate und der Absperrzeit

	Bedingung 1	Bedingung 2	Bedingung 3	Bedingung 4
95 %-Quantil der Absperrzeit	1210 s	1563 s	1407 s	1741s
Wassereintrittsrate	140 – 180 kg/s			
In den Ringraum eingetretene Wassermenge	170 – 218 m ³	219 – 281 m ³	200 – 253 m ³	244 – 313 m ³
Wasserhöhe				
- Quadrant Q3	20 – 20 cm			
- Quadrant Q4	9 – 13,8 cm	13,9 – 20 cm	12 – 17,3 cm	16,4 – 20 cm
- Quadrant Q2	14 – 20 cm	20 – 20 cm	19 – 20 cm	20 – 20 cm
- Quadrant Q1	0 – 0,9 cm	1 – 5,8 cm	0 – 3,5 cm	2,9 – 10,8 cm

Die Berechnung der in Tab. 6.4 angegebenen Werte werden am Beispiel der Bedingung 1 erläutert. Für die restlichen Bedingungen erfolgen die Berechnungen analog:

- Unter der Bedingung 1 wurde ein Absperrzeitpunkt von $t = 1210$ s als 95 %-Quantil ermittelt. Während dieser Zeit strömt eine Wassermenge zwischen 170 m³ und 218 m³ zunächst in den vom Leck betroffenen Quadranten Q3 ein.
- Bei einer Wasserhöhe von $0,20$ m (Höhe der Bodenschwellen) ist im Quadranten Q3 eine Wassermenge von 80 m³ enthalten. Ab dieser Wassermenge läuft das zusätzlich einströmende Wasser zu gleichen Teilen in die Quadranten Q2 und Q4 über, d. h. jeweils 45 m³ bis 69 m³ in beide Quadranten. Bis zu der Höhe der Bodenschwellen hat Quadrant Q2 ein Volumen von 63 m³ und Quadrant Q4 ein Volumen von 100 m³. Wenn beispielsweise 69 m³ Wasser in den Quadranten Q2 fließen, laufen noch 9 m³ vom Quadranten Q2 in den Quadranten Q1 über.
- Die berechneten Wasserhöhen in den Quadranten hängen von der Menge des übergelaufenen Wassers und von der Fläche der Quadranten ab (siehe Abschnitt 6.1.2). Damit ergeben sich durch das übergelaufene Wasser in die benachbarten Quadranten die in Tab. 6.4 berechneten Wasserhöhen, die sich in den einzelnen Quadranten vom Zeitpunkt des

Bruchs in der Feuerlöschwasserleitung bis zur Absperrung des Gebäudeeintrittsschiebers GES-1 und der Streckenschieber auf dem Gelände ergeben.

Im Reaktorgebäude-Ringraum befinden sich Komponenten von Sicherheitssystemen, die bei großen Wasserfreisetzungen im Ringraum beeinträchtigt werden können. Bei Überflutungserignissen im Ringraum ist eine räumliche Trennung von Komponenten verschiedener Redundanten nicht gegeben, sodass bei Freisetzung großer Wassermengen ein redundanzübergreifender Verlust von Systemfunktionen möglich wäre. Eine weitere Frage, die aus den Analyseergebnissen abgeleitet werden kann, bezieht sich auf die Zeitmarge, die vom Zeitpunkt der Absperrung der Streckenschieber verbleibt, bis sicherheitstechnisch relevante Komponenten von der Überflutung betroffen wären, wenn die Absperrung nicht gelingen würde.

Die am tiefsten angeordneten, sicherheitstechnisch relevanten Komponenten einschließlich ihrer Einrichtungen zur Energie- und Medienversorgung und der erforderlichen Instrumentierung und Steuerung sind:

- die Sicherheitseinspeisepumpen (JND; Unterkante des Pumpenmotors 0,4 m über dem Ringraumboden),
- die Zusatzborierpumpen (JDH; Unterkante des Pumpenmotors 0,64 m über dem Ringraumboden).
- die redundant und diversitär ausgelegten Messumformer, die sich auf einer Höhe von 0,74 m über dem Ringraumboden befinden.

Die maximal zulässige Fluthöhe bei Überflutung des Reaktorgebäude-Ringraumes beträgt somit 0,40 m zum Funktionserhalt der HD-Sicherheitseinspeisepumpen. Zum Schutz der Zusatzborierpumpen darf eine maximale Fluthöhe von 0,64 m nicht überschritten werden. Da die Messumformer höher angeordnet sind als die Zusatzborierpumpen, ist der Schutz der Zusatzborierpumpen auch abdeckend für die Messumformer.

Die Gesamtfläche des Reaktorgebäude-Ringraums beträgt 1.865 m^2 . Das zulässige Wasservolumen, das im Ringraum freigesetzt werden darf, beträgt somit für die Sicherheitseinspeisepumpen 738 m^3 , für die Zusatzborierpumpen insgesamt 1.182 m^3 und für die Messumformer 1.366 m^3 . Die nicht sicherheitstechnisch relevante Ringraumabsaugung befindet sich bei 0,35 m über dem Ringraumboden, was einem zulässigen Wasservolumen von ca. 646 m^3 entspricht.

Die Zeitmargen, die zum Zeitpunkt der Absperrung zur Verfügung stehen würden, bis sicherheitstechnisch relevante Komponenten von der Überflutung betroffen wären, wenn die Absperrung nicht gelingen würde, sind in Tab. 6.5 aufgeführt.

Tab. 6.5 Zeitmarge vom Zeitpunkt der Absperrung der Streckenschieber bis zur potenziellen Überflutung sicherheitstechnisch relevanter Komponenten

	Bedingung 1	Bedingung 2	Bedingung 3	Bedingung 4
95 %-Quantil der Absperrzeit	1210 s	1563 s	1407 s	1741 s
Wassereintrittsrate	140 – 180 kg/s			
Sicherheitseinspeisepumpen (0,4 m)	67 – 48 min	61 – 42 min	64 – 45 min	59 – 39 min
Zusatzborierpumpen (0,64 m)	120 – 89 min	114 – 83 min	117 – 86 min	111 – 80 min
Messumformer (0,74 m)	142 – 106 min	136 – 100 min	139 – 103 min	133 – 97 min

Die Angaben in Tab. 6.5 sind folgendermaßen zu lesen:

Unter Bedingung 1 (Werkzeug ist vor Ort verfügbar und Streckenschieber STS-1 lässt sich schließen) kann der Streckenschieber mit einer Wahrscheinlichkeit von 0,95 innerhalb 1.210 s (ca. 20 min) nach Leckageeintritt geschlossen werden. Wäre zu diesem Zeitpunkt die Absperrung des Streckenschiebers nicht möglich gewesen, würden dem Anlagenpersonal bei einer Wassereintrittsrate von 140 kg/s eine Zeitmarge von ca. 67 min verbleiben, Gegenmaßnahmen einzuleiten, um eine Überflutung der Sicherheitseinspeisepumpen zu verhindern. Bei einer Wassereintrittsrate von 180 kg/s würde die Zeitmarge 48 min betragen.

Eine der Maßnahmen, die in diesem Fall ergriffen wird, besteht darin, die Notschieber zu schließen. Dies ist die Situation, die in der Bedingung 3 beschrieben ist. In diesem Fall wird die Zeit bis zur Absperrung von ca. 23 min mit einer Wahrscheinlichkeit von 0,95 nicht überschritten. Könnten auch die Notschieber nicht geschlossen werden, würden dem Personal in Abhängigkeit der Wassereintrittsrate noch 45 bis 64 min verbleiben, um die Sicherheitseinspeisepumpen vor einer Überflutung zu schützen.

Unter dem wenig wahrscheinlichen, ungünstigen Szenario der Bedingung 4 (Werkzeug vor Ort ist nicht verfügbar und Streckenschieber STS-1 lässt sich nicht schließen) betragen die Zeit-

margen, um die Sicherheitseinspeisepumpen vor Überflutung zu schützen, zwischen ca. 39 und 59 min in Abhängigkeit von der Einspeiserate des Wassers in den Ringraum.

Die anderen Werte sind analog zu interpretieren, wobei für die höher gelegenen Komponenten die Zeitmargen, um Überflutungen zu verhindern, entsprechend größer sind. Aus den Werten in Tab. 6.5 ist zu erkennen, dass die unterschiedlichen Situationen, die in den Bedingungen spezifiziert sind, geringere Auswirkung auf die Zeitmargen haben als die Höhen, in denen die jeweiligen Komponenten angeordnet sind.

Die Zeiten, die vom Leckageeintritt bis zur Absperrung der Streckenschieber mit einer Wahrscheinlichkeit von 95 % nicht überschritten werden, stellen keine unmittelbare Gefahr bzgl. der Überflutung sicherheitstechnisch relevanter Komponenten im Ringraum dar. Dies ist beispielsweise an den Zeitmargen zu erkennen, die bis zur Überflutung sicherheitstechnisch relevanter Komponenten bestehen. Auch für die als ungünstigste Situation angenommene Bedingung 4, die lediglich mit einer sehr geringen Wahrscheinlichkeit von 0,0085 eintritt, besteht noch eine Zeitmarge zwischen ca. 39 und 59 min (abhängig von der Wassereintrittsrate), bis die am niedrigsten angeordneten Sicherheitseinspeisepumpen von der Überflutung betroffen sind.

Anders ist die Situation bzgl. des Brandszenarios zu beurteilen, das als erschwerende Situation zeitgleich zum Leck in der Feuerlöschwasserleitung angenommen wurde. Die Zeiten, die bis zur Absperrung der Streckenschieber benötigt werden, stellen zugleich diejenigen Zeitpunkte dar, ab denen die Löschung des Brandes fortgesetzt werden kann.

In Abb. 6.14 wird die Zeitverteilung zwischen Eintritt des Brandes und der Absperrung der Streckenschieber unter der wahrscheinlichsten Bedingung ($p = 0,982$) dargestellt, dass sich das Werkzeug auslegungsgemäß vor Ort befindet und der Streckenschieber STS-1 absperrbar ist.

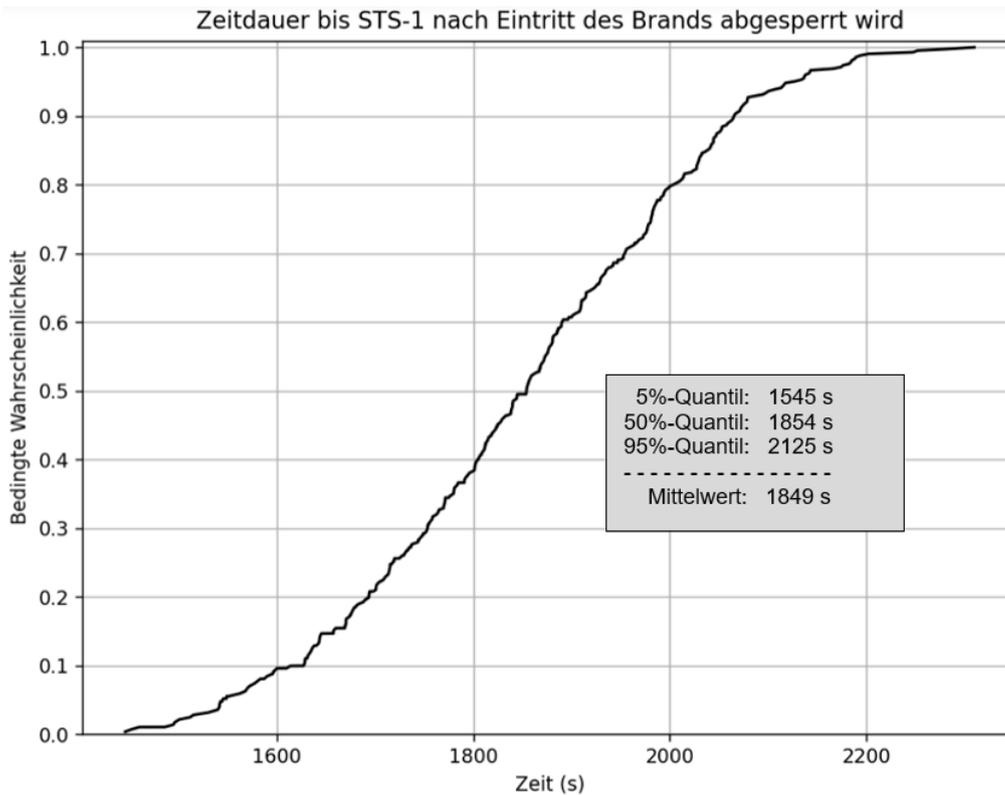


Abb. 6.14 Verteilung der Zeit von Brandentstehung bis zur Absperrung von STS-1

Unter der Bedingung, dass sich das zur Absperrung erforderliche Werkzeug vor Ort befindet und der Streckenschieber STS-1 absperrbar ist, ergibt sich eine mittlere Zeitspanne von ca. 30,5 min, bis nach der Brandentstehung der Streckenschieber STS-1 abgesperrt und damit die Bekämpfung und Löschung des Brandes beginnen kann. Mit einer Wahrscheinlichkeit von 0,9 liegen die Zeiten zwischen 26 und 35 min. Mit einer Wahrscheinlichkeit von 5 % werden Zeitspannen erreicht, die zwischen 24 und 26 min liegen. Auch wenn nur die kürzesten Zeiten bis zur Leckabsperrung in Betracht gezogen werden, betragen die Zeitverzögerungen, bis mit der Löschung des Brandes beginnen kann, mehr als 24 min. Diese Zeitverzögerung bei der Löschung des Brandes kann durchaus sicherheitstechnisch relevante Auswirkungen haben. Bei unabhängiger Betrachtung ist das angenommene Szenario, d. h. das zeitgleiche Eintreten eines Brandes und einem Leck in der Feuerlöschwasserleitung, allerdings wenig wahrscheinlich.

Um beurteilen zu können, ob die Verzögerungszeiten des Löschanfangs signifikante Auswirkungen auf Schädigungen sicherheitstechnisch relevanter Komponenten haben, müsste eine Brandsimulation durchgeführt werden, wobei die ermittelten bedingten Zeitverteilungen als aleatorische Unsicherheiten in den Brandsimulationen berücksichtigt werden.

7 Zusammenfassung und Ausblick

In Ergänzung zur konventionellen PSA sind in den letzten Jahren vermehrt fortschrittliche Methoden der dynamischen PSA entwickelt worden, die mittlerweile für Anwendungen zur Verfügung stehen. In der GRS wurde das Crew-Modul entwickelt, mit dem ein Handlungsablauf, der sich durch die arbeitsteilige Ausführung von Handlungen durch die Schichtmannschaft ergibt, als ein dynamischer Ablauf modelliert und simuliert werden kann. Um die Abhängigkeiten von Handlungsabläufen von stochastischen Einflussgrößen berücksichtigen zu können, wird das Crew-Modul in Verbindung mit der in der GRS entwickelten Methode MCDET (*Monte Carlo Dynamic Event Tree*) eingesetzt, die aus einer Kombination von Monte-Carlo-Simulation und dynamischer Ereignisbaummethode besteht. Dabei kann der Einfluss beliebiger stochastischer (aleatorischer) Einflussgrößen sowie epistemischer Unsicherheiten in Abhängigkeit vom Prozesszustand in der Analyse analysiert werden.

Solche Wechselwirkungen sind insbesondere auch bei Ereignissen infolge übergreifender Einwirkungen oder auch Einwirkungskombinationen zu erwarten, bei denen Notfallmaßnahmen durch das Anlagenpersonal unter erschwerenden Randbedingungen durchzuführen sind. Erschwerende Bedingungen, die im Fall übergreifender Einwirkungen auftreten können, ergeben sich insbesondere dann, wenn mehrere übergreifende Einwirkungen in Kombination auftreten oder zu kaskadierenden Ereignisketten führen, deren Beherrschung das Personal vor besondere Herausforderungen stellt.

Das Crew-Modul wurde in Verbindung mit MCDET für eine Handlungsmaßnahme angewendet, die unter erschwerten Randbedingungen für ein ausgewähltes Beispiel übergreifender Einwirkungen durchgeführt wurde. Als Ereignisszenarien übergreifender Einwirkungen bzw. Einwirkungskombinationen haben sich aus vorangegangenen Untersuchungen der GRS bestimmte Szenarien infolge hydrologischer Einwirkungen mit Überflutungspotenzial als nicht zu vernachlässigend herausgestellt. Insbesondere hat sich ergeben, dass das Feuerlöschwassersystem hinsichtlich der freigesetzten Wassermengen im Ringraum das größte Potenzial hat, sicherheitstechnisch relevante Komponenten zu überfluten. Um eine Überflutung im Reaktorgebäude-Ringraum zu verhindern, durch die sicherheitstechnisch relevante Komponenten beeinträchtigt werden können, ist es erforderlich, die Wasserfreisetzung im Ringraum möglichst schnell zu unterbinden. Aus diesem Grund kommt menschlichen Handlungen bei solchen Szenarien eine besondere Bedeutung zu.

Entsprechend der Zielsetzung des Vorhabens, menschliche Handlungen unter erschwerten Randbedingungen mit den Methoden der dynamischen PSA zu analysieren, wurde angenom-

men, dass ein Überflutungsereignis zeitgleich zu der übergreifenden Einwirkung eines Brandes im Ringraum stattfindet. Für das Szenario wurde unterstellt, dass in einem Kabelschacht des Reaktorgebäude-Ringraums ein Brand ausbricht und während der Löscharbeiten ein Leck in der Feuerlöschwasserleitung entsteht, welches die Zufuhr des Löschwassers zur Brandbekämpfung unterbricht. Die erschwerende Randbedingung für den Löschvorgang besteht also in der mehr oder minder großen Verzögerung der Löscharbeiten durch die Dauer und den Erfolg der Erkennung, Lokalisierung und Absperrung des Lecks.

Das Crew-Modul wurde auf das angenommene Szenario angewendet. Ein wesentlicher Aspekt der dynamischen Analyse von menschlichen Handlungen ist die umfassendere und detailliertere Berücksichtigung möglicher Unsicherheitsquellen, die einen wesentlichen Einfluss auf den Handlungsablauf haben können. Unsicherheiten, die im Handlungsmodell berücksichtigt wurden, betreffen Unsicherheiten in Bezug auf

- die Wassereintrittsrate,
- die Auslösung des akustischen Alarms nach Leitungsbruch,
- die Zeit, wann nach Auslösung des Alarms die Überflutungsanzeigen in der Warte anstehen,
- die Entwicklung des Stressniveaus durch den zusätzlichen Alarm nach Leitungsbruch,
- die Zeitdauern in Abhängigkeit des Stressniveaus, bis Anzeigen in der Warte für die Diagnose erkannt und interpretiert werden,
- die Verfügbarkeit des zur Absperrung der Streckenschieber vor Ort erforderlichen Werkzeugs,
- die Schließzuverlässigkeit des Streckenschiebers STS-1.

Die Besonderheit der dynamischen Modellierung eines Handlungsablaufs besteht darin, Abfolgen von Handlungen unter Berücksichtigung zeitlicher Einflüsse, Abhängigkeiten von System- und Prozesszuständen sowie zufälligen Einflussfaktoren modellieren zu können.

Es wurde demonstriert, dass der Faktor Stress als dynamische Größe in das Handlungsmodell unter Berücksichtigung von Unsicherheiten eingebunden werden kann. Auch können die Auswirkungen hoher Stresslevel nicht nur über erhöhte Fehlerwahrscheinlichkeiten bestimmter Handlungen, sondern z. B. auch durch Stress verursachte zeitliche Verzögerungen oder auch fehlerhafte Handlungen, die den Anlagenzustand verschlimmern (Englisch: Errors of Commission, EoC) modelliert werden.

Des Weiteren wurde gezeigt, dass sich hoher Stress unter bestimmten Bedingungen nicht global auf alle beteiligten Personen beziehen muss, sondern auch nur einzelne Personen betreffen kann. Im Modell wurde beispielsweise angenommen, dass sich hoher Stress nur beim Schichtleiter-Stellvertreter einstellt, da dieser bei der Diagnosefindung und aufgrund der in Kombination auftretenden Ereignisse Brand und Überflutung besonders in Anspruch genommen ist.

Mit dem Crew-Modul wurden in Verbindung mit MCDET 2.400 Simulationen des Handlungsablaufs durchgeführt. Dabei wurden 100 dynamische Ereignisbäume im Rahmen einer Monte-Carlo-Simulation erzeugt, in denen Ausführungszeiten der Basishandlungen und andere aleatorische Unsicherheiten zufällig ausgespielt wurden. In jedem der 100 dynamischen Ereignisbäume wurden 24 verschiedene Sequenzen gerechnet. Die 24 Sequenzen ergeben sich aus den möglichen Kombinationen der im Modell definierten diskreten Zufallsvariablen und zeitlichen Wechselwirkungen.

Für die Löschung des Brandes ist es bei einem gleichzeitigen Bruch der Feuerlöschwasserleitung notwendig, dass der Gebäudeeintrittsschieber GES-1 und der Streckenschieber STS-1 auf dem Gelände abgesperrt werden. Diese beiden Aktionen sind von erheblicher Bedeutung, da durch die Absperrungen zum einen die Überflutung im Ringraum gestoppt wird. Zum anderen kann durch die Absperrungen der Druck in der Feuerlöschwasserleitung wieder aufgebaut und die Löschung des Brandes fortgeführt werden. Da die Absperrungen der beiden Schieber GES-1 und STS-1 nicht nacheinander, sondern parallel durch den Angriffstrupp der Feuerwehr bzw. den Melder durchgeführt werden und notwendigerweise beide Absperrungen ausgeführt werden müssen, ist für die Fortführung der Löschung relevant, welche der beiden Absperrungen später durchgeführt wird. Durch die Verteilung der Zeitdifferenzen zwischen der Absperrung von GES-1 und STS-1 konnte gezeigt werden, dass die Absperrung des Streckenschiebers STS-1 durch den Melder später erfolgt als die des Gebäudeeintrittsschiebers GES-1, der durch den Angriffstrupp der Feuerwehr geschlossen wird. Relevant für das Überflutungsszenario und die Brandlöschung ist somit der Zeitpunkt, wann der Streckenschieber STS-1 bzw. die Notschieber STS-2 und STS-3 abgesperrt werden.

Es wurde untersucht, welche Auswirkungen verschiedene stochastische Einflussgrößen (Auslösung des Alarms, Stresserhöhung und damit verbundene Verzögerungen in der Diagnosefindung, Verfügbarkeit des zur Absperrung erforderlichen Werkzeugs vor Ort, Schließbarkeit des Streckenschiebers) auf die Zeitspanne haben, bis die Überflutung im Ringraum gestoppt werden kann.

Die Untersuchungen haben gezeigt, dass es mit der angewendeten Methodik der dynamischen PSA möglich ist, die Auswirkung stochastischer Einflussfaktoren auf Ergebnisgrößen (z. B. Absperrzeit des Streckenschiebers bzw. der Notschieber auf dem Gelände) zu quantifizieren. So konnte beispielsweise gezeigt werden, dass es zu einer signifikanten Verzögerung der Absperrung des Leitungslecks kommt, wenn das benötigte Werkzeug vor Ort nicht verfügbar ist und sich der Streckenschieber STS-1 nicht schließen lässt. Dem gegenüber hat sich gezeigt, dass das im Modell angenommene hohe Stressniveau des Schichtleiter-Stellvertreters oder die Alarmauslösung nach dem Leitungsbruch nur eine geringfügige Erhöhung der Absperrzeit zur Folge hat.

Im Reaktorgebäude-Ringraum befinden sich Komponenten von Sicherheitssystemen, die bei großen Wasserfreisetzungen in diesem Gebäude beeinträchtigt werden können. Weitere Fragestellungen, die beispielsweise aus den probabilistischen Ergebnissen abgeleitet werden können, beziehen sich auf die Überflutungshöhen in den jeweiligen Quadranten des Ringraums oder auf die Zeitmargen, die vom Zeitpunkt der Absperrung der Streckenschieber verbleiben würden, bis die am tiefsten angeordneten, sicherheitstechnisch relevanten Komponenten einschließlich ihrer Einrichtungen zur Energie- und Medienversorgung und der erforderlichen Instrumentierung und Steuerung von der Überflutung betroffen wären.

Es konnte gezeigt werden, dass selbst unter den ungünstigsten wenig wahrscheinlichen Ereigniskombinationen sicherheitstechnisch relevante Komponenten nicht von der Überflutung betroffen sind. Die Zeitmargen bis zur Überflutung der am tiefsten gelegenen Sicherheitseinspeisepumpen betragen – ab dem Zeitpunkt der Absperrung gerechnet – mit einer Wahrscheinlichkeit von 95 % mindestens 39 – 59 min. Ab dem Zeitpunkt des Leckageeintritts gerechnet, betragen die Zeitmargen bis zur Überflutung der am tiefsten gelegenen sicherheitstechnisch relevanten Komponenten mit einer Wahrscheinlichkeit von 95 % mindestens 68 – 88 min. Die Variation der Zeitmargen hängt von der Wassereintrittsrate ab, die als unsichere Größe in einem Intervall zwischen 140 kg/s und 180 kg/s angenommen wurde.

Der Vorteil der umfangreicheren und detaillierteren Aussagen, die mit den Methoden der dynamischen Analyse erzeugt werden können, besteht darin, dass man einen Kenntniskern bzgl. des komplexen Systemverhaltens unter Unsicherheiten erhält. Dieser Kenntniskern besteht in erster Linie darin, dass man die Auswirkungen unsicherer Einflussgrößen auf die Zeiten relevanter Handlungen (beispielsweise der Zeitpunkt, zu dem der Streckenschieber STS-1 abgesperrt wird, Zeitverzögerung der Brandlöschung) und daraus abgeleiteter Größen (u. a. Überflutungshöhe in den Quadranten des Reaktorgebäude-Ringraums oder Zeitmargen, bis sicherheitstechnisch relevante Komponenten von der Überflutung betroffen sind) quantifi-

zieren kann. Durch diesen Kenntnisgewinn können sich Hinweise darüber ergeben, an welchen Stellen angesetzt werden muss, um Verbesserungen des Sicherheitsniveaus der Anlage erzielen zu können.

Neben den umfassenderen und detaillierten Analysemöglichkeiten sind mit der in diesem Vorhaben angewendeten Methodik folgende weitere Vorteile verbunden:

- Die Modellierung der Handlungsabläufe sowie die Annahmen bzgl. der Zeiten und Wahrscheinlichkeiten, die in das Modell eingehen, sind transparent und im Einzelnen nachvollziehbar. Falls für verschiedene Teile des Modells fundiertere Informationen und Abschätzungen vorliegen, können diese Teile leicht modifiziert werden.
- Durch die ausführlichen Überlegungen und Antizipationen, die zur Modellierung der Handlungsabläufe notwendig sind, werden Abhängigkeiten und mögliche, unsichere Einflussgrößen erkannt, an die man bei grober Betrachtung nicht denken würde, die jedoch einen nicht unerheblichen Effekt auf die Ausführung der Handlungsmaßnahme haben können.
- Auswirkungen stochastischer Einflussgrößen können quantifiziert werden, wodurch sich ihre Relevanz und sicherheitstechnische Bedeutung fundierter abschätzen lässt.

Es ist beabsichtigt, die Methodik der dynamischen PSA vermehrt für unterschiedliche, komplexe, zeitlich veränderliche Szenarien und Fragestellungen anzuwenden, um aus diesen Anwendungen zu lernen und sinnvolle Weiterentwicklungen dieses Analysewerkzeugs durchführen zu können.

Literaturverzeichnis

- /ADO 12/ Adolfsson, Y., et al. (eds.): In IDPSA – Integrated Deterministic-Probabilistic Safety Assessment, 2nd Workshop, KTH, Stockholm, Schweden, November 19-21, 2012.
- /CHA 07/ Chang, Y. H., A. Mosleh: Cognitive Modeling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents – Part 1: Overview of the IDAC Model, Reliability Engineering & System Safety, 92 (8) S. 997 – 1013, Elsevier, 2007, <https://doi.org/10.1016/j.ress.2006.05.014>.
- /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., W. Preischl: Quantitative Bewertung wissensbasierter Handlungen in einer probabilistischen Sicherheitsanalyse, Technischer Fachbericht, GRS-A-3579, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, 2010, <http://www.grs.de/publikation/grs-A-3579>.
- /FAS 14/ Faßmann, W.: Methode für die Analyse und Bewertung der Wechselwirkung zwischen Stress und der Zuverlässigkeit wissensbasierten Handelns in der probabilistischen Sicherheitsanalyse, Technischer Fachbericht, GRS-332, ISBN-978-3-944161-12-9, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, Juni 2014, <http://www.grs.de/publikation/grs-332>.
- /FAS 18/ Faßmann, W., J. Peschke: Beurteilung der menschlichen Zuverlässigkeit in PSA für übergreifende Einwirkungen, GRS-516, ISBN 978-3-947685-01-1, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, August 2018, <http://www.grs.de/publikation/grs-516>.
- /HOF 01/ Hofer, E., et al.: Methodenentwicklung zur simulativen Behandlung der Stochastik in probabilistischen Sicherheitsanalysen der Stufe 2, GRS-A-2997, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Dezember 2001.

- /IZQ 08/ Izquierdo, J. M., et al.: SCAIS (Simulation Code System for Integrated Safety Assessment): Current Status and Applications, in: Proceedings of ESREL 2008 and 17th SRA Europe, Valencia, Spanien, September 2008.
- /KKW 12/ Kernkraftwerksbetreiber der Referenzanlage: Sicherheitsüberprüfung nach AtG – Probabilistische Sicherheitsanalyse – Brand (LB), 2012.
- /KKW 19/ Kernkraftwerksbetreiber der Referenzanlage: Betriebshandbuch – Betriebsordnungen – Brandschutzordnung (Sicherheitsspezifikation), 2019.19
- /KLO 06/ Kloos, M., J. Peschke: MCDET – A Probabilistic Dynamics Method Combining Monte Carlo Simulation with the Discrete Dynamic Event Tree Approach, Nuclear Science and Engineering, 153, S. 137 – 156, 2006.
<https://www.ans.org/pubs/journals/nse/article-2601/>.
- /LIU 12/ Liu, P.: Task Complexity Measure for Emergency Operating Procedures Based on Resource Requirements in Human Information Processing, Paper 27-Mo2-2, in: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012), ISBN: 978-1-62276-436-5, Curran Associates, Inc., Red Hook, NY, USA, 2012.
- /MOH 12/ Mohagegh, Z.: Hybrid Incorporation of Physical and Social Failure Mechanisms in Probabilistic Risk Assessment, Paper 16C-Fr2-4, in: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012), ISBN: 978-1-62276-436-5, Curran Associates, Inc., Red Hook, NY, USA, 2012.
- /NEA 19/ OECD Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK): Dynamic PSA – Preparing for the Future, Task Proposal, Paris, 2019.

- /OSB 18/ Osborn, D., et al.: Level 2 Probabilistic Risk Assessment Using Dynamic Event Tree Analysis, in: Aldemir, T. (Ed.), Advanced Concepts in Nuclear Energy Risk Assessment and Management, Volume 1, ISBN: 978-81-3225-60-6 World Scientific Publishing Co Pte Ltd., Singapur, Juni 2018, <https://doi.org/10.1142/10587>.
- /PES 06/ Peschke, J., et al.: Methodenentwicklung für die Berücksichtigung menschlicher Eingriffe im Rahmen einer dynamischen PSA der Stufen 1 und 2, GRS-A-3340, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Juni 2006.
- /PES 14/ Peschke, J., et al.: Methodenentwicklung zur Analyse von Personalhandlungen im Rahmen probabilistischer Dynamikanalysen am Beispiel von Brandereignisabläufen mit Brandbekämpfung, Technischer Fachbericht, GRS-331, ISBN 978-3-944161-11-2, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Juni 2014, <https://www.grs.de/publikation/grs-331>.
- /PES 18/ Peschke, J., et al.: MCDET Methode zur Integralen Deterministisch-Probabilistischen Sicherheitsanalyse, GRS-520, ISBN 978-3-947685-05-9, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, September 2018, <https://www.grs.de/publikation/grs-520>.
- /RAB 14/ Rabiti, C., et al.: RAVEN, a New Software for Dynamic Risk Analysis, in: Proceedings of 12th International Probabilistic Safety Assessment and Management Conference (PSAM12), Honolulu, HI, USA, Juni 2014, http://www.diegomandelli.com/papers/2014/PSAM/RAVEN/PSAM12-RAVEN_Overview_jjc_aa.pdf.
- /ROE 17/ Röwekamp, M., et al.: Methoden zur Bestimmung des standort- und anlagenspezifischen Risikos eines Kernkraftwerks durch übergreifende Einwirkungen / Estimation of the Site and Plant Specific Risk of a Nuclear Power Plant from Hazards, Technischer Fachbericht / Technical Report, GRS-A-3888, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Juni 2017.

- /SPE 18/ Sperbeck, S., et al.: Informationstool Hazards Library – Analysehilfsmittel zur Bereitstellung von Informationen und Daten zur systematischen Durchführung von PSA für übergreifende Einwirkungen, GRS-A-3914, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, April 2018.
- /SWA 83/ Swain, A. D., H. E. Guttman: Handbook on Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, NUREG/CR-1278, United States Nuclear Regulatory Commission (NRC), Washington, DC, USA, August 1983.
- /SWA 87/ Swain, A. D.: Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, U.S. Nuclear Regulatory Commission (NRC), Washington, DC, USA, 1987.

Abbildungsverzeichnis

Abb. 4.1	Schematische Darstellung der für das Szenario wichtigen Systeme und Komponenten des Reaktorgebäude-Ringraums und des angrenzenden Freigeländes der Referenzanlage	25
Abb. 6.1	Wahrscheinlichkeitsverteilung der Zeit t_{Q3} , wann der Wassereintritt im Quadranten Q3 durch die redundante Füllstandsmessung an der Reaktorschutztafel angezeigt wird	43
Abb. 6.2	Approximation der Wahrscheinlichkeitsverteilung von t_{Q3} durch die Dreiecksverteilung $t_{Q3} \sim \text{Triangular}(90,105,135)$ s	44
Abb. 6.3	Struktur der Handlungslisten unter Berücksichtigung stochastischer Einflussgrößen und zeitlicher Wechselwirkungen. Details zu den Handlungslisten siehe Anhang A, Tabellen Tab. A. 1 – Tab. A. 15	51
Abb. 6.4	Basishandlungen der Handlungsliste HL 1.0.....	54
Abb. 6.5	Ablaufdiagramm der Notfallmaßnahme in Abhängigkeit von Unsicherheiten, Systemzuständen und zeitlichen Wechselwirkungen.....	57
Abb. 6.6	Kumulierte Verteilungsfunktion der Zeiten, wann ein Leitungsbruch nach Auslösung des Brandalarms erfolgt und die Schlauchverbindung zum Hydranten hergestellt ist.....	61
Abb. 6.7	Kumulierte Verteilungsfunktionen der Zeitspannen, bis GES-1 und STS-1 nach dem Leitungsbruch abgesperrt werden	62
Abb. 6.8	Wahrscheinlichkeitsverteilung der Zeitdauer, bis STS-1 nach der Schließung von GES-1 abgesperrt wird	63
Abb. 6.9	Bedingte Verteilungsfunktion der Zeitdauern zwischen Eintritt des Lecks und Absperrung von STS-1 in Abhängigkeit von der Auslösung des Alarms	65
Abb. 6.10	Bedingte Verteilungsfunktion der Zeitdauern zwischen Eintritt des Lecks und Absperrung von STS-1 in Abhängigkeit von der Stressentwicklung des SLV	67
Abb. 6.11	Bedingte Verteilungsfunktion der Zeitdauern zwischen Leitungsbruch und Absperrung von STS-1 abhängig von der Verfügbarkeit des Werkzeugs.....	68
Abb. 6.12	Bedingte Wahrscheinlichkeitsverteilung der Zeitdauern zwischen Leitungsbruch und Absperrung von STS-1 abhängig von der Verfügbarkeit des Werkzeugs	69

Abb. 6.13	Bedingte Verteilungsfunktionen der Absperrzeit der Streckenschieber in Abhängigkeit von der Verfügbarkeit des Werkzeugs vor Ort und der Zuverlässigkeit, dass sich STS-1 schließen lässt.....	71
Abb. 6.14	Verteilung der Zeit von Brandentstehung bis zur Absperrung von STS-1	78

Tabellenverzeichnis

Tab. 6.1	Wahrscheinlichkeitsverteilungen der Bewertungszeiten in Abhängigkeit des Stressniveaus des SLV und zeitlicher Wechselwirkungen.....	48
Tab. 6.2	Mittelwert und Quantile der Zeiten, wann der Leitungsbruch erfolgt, den Zeitdauern, wann GES-1 sowie STS-1 nach dem Eintritt des Leitungsbruchs abgesperrt werden können, sowie der Zeitdauer zwischen der Absperrung von GES-1 und STS-1	64
Tab. 6.3	Mittelwert, zweiseitige 95%-Konfidenzintervalle und Quantile der Absperrzeit (s) der Streckenschieber in Abhängigkeit von der Verfügbarkeit des Werkzeugs vor Ort und der Zuverlässigkeit, dass sich STS-1 schließen lässt.....	71
Tab. 6.4	In den Ringraum eingetretene Wassermenge und Wasserhöhe in den vier Quadranten in Abhängigkeit der Wassereintrittsrate und der Absperrzeit	74
Tab. 6.5	Zeitmarge vom Zeitpunkt der Absperrung der Streckenschieber bis zur potenziellen Überflutung sicherheitsrelevanter Komponenten.....	76
Tab. A. 1	Brandalarm und Aufsuchen des Brandortes → Handlungsablauf für HL 1.0.....	95
Tab. A. 2	Zufallszeiten für Leitungsbruch, Druckreduktion und Überflutungsanzeige in Abhängigkeit der Zeit, wann die Schlauchverbindung zum Hydranten hergestellt ist → Handlungsablauf für HL 1.01	100
Tab. A. 3	Angriffstrupp stellt fest, dass kein Wasser zur Löschung ankommt → Handlungsablauf für HL 1.05	102
Tab. A. 4	Abhängigkeit des Handlungsablaufs vom Zeitpunkt, zu dem sich die Druckreduktion im Schlauch bemerkbar macht → Handlungsablauf für HL 1.051 und HL 1.052.....	103
Tab. A. 5	Abhängigkeit des Handlungsablaufs von der Unsicherheit, ob ein Alarm ausgelöst wird oder nicht, und der Verfügbarkeit des Schichtleiters → Handlungsablauf für HL 1.1, HL 1.2 und HL 1.3	104
Tab. A. 6	Definition der Unsicherheit, wann der SLV die Überflutungsanzeige erkennt und die Diagnose erstellt → Handlungsablauf für HL 2.01, HL 2.02, HL 2.03 und HL 2.031 (Fortsetzung von HL 1.1 und HL 1.2).....	108

Tab. A. 7	Bewertung der Anzeigen in Abhängigkeit vom Stress → Handlungsablauf für HL 2.04, HL 2.05 und HL 2.06 (Fortsetzung von HL 2.01 und HL 2.02).....	110
Tab. A. 8	Bewertung der Anzeigen in Abhängigkeit vom Stress → Handlungsablauf für HL 2.07, HL 2.08 und HL 2.09 (Fortsetzung von HL 2.03 und HL 2.031)	112
Tab. A. 9	Diagnose und weiteres Vorgehen → Handlungsablauf für HL 2.1 (Fortsetzung von HL 2.04 – HL 2.09).....	114
Tab. A. 10	Einsatzleiter erkennt Druckabfall, bevor Diagnose in Warte erstellt ist → Handlungsablauf für HL 2.2 (Fortsetzung von HL 2.1)	115
Tab. A. 11	Diagnose des SL liegt vor, bevor der Einsatzleiter den Druckabfall in der Leitung feststellt → Handlungsablauf für HL 2.3 (Fortsetzung von HL 2.1).....	117
Tab. A. 12	Absperrung der Streckenschieber auf dem Gelände → Handlungsablauf für HL 3.0 (Fortsetzung von HL 2.2 bzw. HL 2.3).....	119
Tab. A. 13	Unsicherheit bzgl. des Werkzeugs vor Ort → Handlungsablauf für HL 4.1 bzw. HL 4.2 (Fortsetzung von HL 3.0)	120
Tab. A. 14	Unsicherheit, ob sich der Streckenschieber STS-1 schließen lässt → Handlungsablauf für HL 5.1 bzw. HL 5.2 (Fortsetzung von HL 4.1 bzw. HL 4.2)	122
Tab. A. 15	Fortführung der Brandlöschung → Handlungsablauf für HL 6 (Fortsetzung von HL 5.1 bzw. HL 5.2).....	124

Abkürzungsverzeichnis

AT	Angriffstrupp
B	Brandort
BMU	Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit
BMWi	Bundesministerium für Wirtschaft und Energie
BST	Brandschutztafel
CFD	Computational Fluid Dynamics
CSNI	Committee on the Safety of Nuclear Installations
DWR	Druckwasserreaktor
EL	Einsatzleiter
EoC	Error(s) of Commission
FLA	Feuerlöschanlage
GES	Gebäudeeintrittsschieber
GT	Gerätetrupp
H	Hydrant
HF	Human Factor
IDPSA	Integrated deterministic probabilistic safety assessment
LKW	Lastkraftwagen
MA	Maschinist
MCDET	Monte Carlo Dynamic Event Tree
ME	Melder
NEA	Nuclear Energy Agency
NFM	Notfallmaßnahme(n)
NRC	Nuclear Regulatory Commission
OECD	Organisation for Economic Cooperation and Development
OSU	Ohio State University
PSA	Probabilistische Sicherheitsanalyse
p(...)	Wahrscheinlichkeit (Englisch: probability) für ...
R	Raum
RST	Reaktorschutztafel
RF	Reaktorfahrer
SBO	Station Black-out
SL	Schichtleiter
SLV	Schichtleiter-Stellvertreter
SNL	Sandia National Laboratories
SSC	Bauliche Anlagenteile, Systeme und Komponenten (Englisch: Structures, Systems and Components)

ST	Schlauchtrupp
STS	Streckenschieber
SÜ	Sicherheitsüberprüfung
WGRISK	Working Group on Risk Assessment
WKP	Wiederkehrende Prüfung

A Anhang: Beschreibung des Handlungsablaufs für eine dynamische PSA

Tab. A. 1 Brandalarm und Aufsuchen des Brandortes → Handlungsablauf für HL 1.0

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
T < 0	E: Im Kabelschacht K des Ringraums bricht ein Brand aus.	In der Nähe des Kabelschachts K befinden sich viele sicherheitstechnisch relevante Systeme.
T = 0	<p>E: Aufgrund der vertikalen Anordnung der Kabel lösen annähernd zeitgleich zwei Brandmelder aus. Die Brandmeldeanlage spricht an und löst in der Warte automatisch einen akustischen Alarm aus. In der Warte steht eine rot blinkende Meldung der Klasse 2 an.</p> <p>Auf der Brandschutztafel im Warten-Nebenraum gehen die Meldelampen der beiden Brandmelder an, die wegen des Brandes angesprochen haben. Die Rechnermeldeanlage erstellt die Unterlage („Alarmausdrucke“) für den Löscheinsatz.</p>	<p>Ein Versagen der Brandmeldeeinrichtungen wird nicht unterstellt.</p> <p>Die Unterlage für den Löscheinsatz liegt in der Warte und an mehreren dafür vorgesehenen Orten auf dem Anlagengelände vor.</p>
<p>Min = 10 s Max = 20 s</p>	<p>Handlungsablauf zu HL 1.1:</p> <p>Der SL hört den Brandalarm und sieht die blinkende Klasse-2-Meldung. Er weiß aufgrund dieser Informationen, dass die Brandschutztafel im Warten-Nebenraum zu kontrollieren ist.</p>	<p>Es ist auszuschließen, dass alle Mitglieder der Schichtmannschaft den Alarm überhören oder nicht beachten: der Alarm ist laut genug und eindeutig, ebenso die Klasse-2-Meldung mit ihrer hohen Priorität. Das Vorgehen bei Brandalarmen ist klar geregelt und gut eingeübt.</p> <p>Aufgrund der Annahme, dass zwei Brandmelder auslösen, entfällt eine Branderkundung durch einen Anlagenwärter. Es erfolgt eine sofortige Einleitung der Brandbekämpfung von der Warte aus.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 5 s Max = 15 s	Der Schichtleiter SL unterbricht seine aktuelle Tätigkeit und lässt den Alarm quittieren.	Es ist nicht plausibel, dass nach dem Quittieren der Meldung jede weitere Aktion unterbleibt, weil die übrigen Mitglieder der Schichtmannschaft eine Durchsage des SL zum Eintreten des Brandfalls erwarten. Zudem steht nach wie vor die Klasse-2-Meldung gut sichtbar an. Auch hat die Rechnermeldeanlage einen Ausdruck mit Informationen zum Brandort erzeugt. Deshalb wird kein Fehler entsprechend THERP Tab. 11-13 (1) unterstellt. Infolge der Quittierung gehen optische Alarmlampen vom Zustand „blinkend“ in den weniger auffälligen Zustand „Ruhiglicht ein“ über.
Min = 10 s Max = 40 s	Der SL prüft, welchen Mitarbeiter in der Warte er von einer laufenden Aufgabe abziehen kann. Er sieht, dass einer seiner Stellvertreter (SLV) verfügbar ist, und beauftragt diesen, die Anzeigen auf der Brandschutztafel im Warten-Nebenraum zu kontrollieren. Der SLV soll klären, welche Brandmelder in welchem Gebäudeteil angesprochen haben.	
Min = 10 s Max = 20 s	Der SLV sucht den Warten-Nebenraum auf, erkennt, auf welchem Bereich der Brandschutztafel Anzeigen anstehen, und begibt sich zu diesem Bereich.	Die Brandschutztafel im Warten-Nebenraum zeigt in schematischer Darstellung an, in welchen Gebäudeteilen sich welche Brandmelder befinden. Sie unterstützt dadurch die Lokalisierung des Brandortes. Die Meldeeinrichtungen der angesprochenen Brandmelder sind erleuchtet und fallen auf, weil kein weiterer Brand vorliegt und deshalb nur diese Anzeigen erleuchtet sind. Daher ist ein Verwechslungsfehler auszuschließen. Ein Unterlassungsfehler ist auszuschließen, weil der SLV auf seine Aufgabe konzentriert ist.
Min = 20 s Max = 40 s	Parallel dazu holt der SL die Unterlagen, die er im Brandfall auszufüllen hat.	Die Unterlagen für den SL unterstützen die korrekte Erfüllung der Aufgaben im Brandfall. Sie beugen Auslassungs- und Verwechslungsfehlern vor. Die Nutzung der Unterlagen ist verbindlich. Vereinfachend werden die einzelnen Arbeitsschritte des SL, die mit der Nutzung der Unterlage für den Brandfall verbunden sind, nicht weiter modelliert.
Min = 40 s Max = 60 s	Der SLV erkennt anhand der Anzeigen, dass Brandmelder im Bereich B angesprochen haben und ein Brand im Kabelschacht K vorliegt. Er kontrolliert sorgfältig die übrigen Anzeigen zu den Brandmeldern in den Gebäudeteilen, die an K angrenzen. Der SLV stellt fest, dass der Brand	Ein Unterlassungsfehler ist auszuschließen, weil der SLV auf seine Aufgabe konzentriert ist. Die Gebäude-Eintrittsschieber müssen geöffnet sein, damit das Feuerlöschwassersystem im Ringraum mit Löschwasser versorgt werden kann.

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 30 s Max = 60 s	<p>noch auf den Kabelschacht K begrenzt ist.</p> <p>Der SLV kehrt in die Warte zurück und erstattet dem SL Bericht.</p>	<p>Der SL steht ggf. nicht sofort für die Entgegennahme des Berichts zur Verfügung stehen, weil er seine laufenden Arbeiten (z. B. ein Telefonat) unterbrechen bzw. zu einem vorläufigen Abschluss bringen muss. Die Zeitverteilung schließt eine eventuelle Wartezeit für den SLV ein.</p>
Min = 10 s Max = 20 s	<p>Zwischenzeitlich öffnet der Reaktorfahrer RF auf Anweisung des SL die beiden Gebäudeeintritts-Schieber GES-1 und GES-2 von Hand.</p>	<p>Eine Unterlassung wird ausgeschlossen, da die Aufmerksamkeit des Personals allein auf den Brandalarm konzentriert ist.</p>
Min = 120 s Max = 180 s	<p>Der SL löst den Brandalarm über die Sprechfunkanlage aus, nennt den Brandbereich (B) und entsendet eine Löschgruppe zur Brandbekämpfung.</p> <p>Alle Mitglieder der Löschgruppe hören die Durchsage und verlassen daraufhin ihren jeweiligen Aufenthaltsort, um ihre persönliche Schutzausrüstung aufzunehmen.</p>	<p>Eine Unterlassung der Durchsage wird als unplausibel ausgeschlossen. Das Vorgehen ist hochgradig geübt, die Aufmerksamkeit des SL und des SLV sind darauf konzentriert.</p> <p>Bei der Benennung des Brandortes ist ein Unterlassungsfehler auszuschließen, weil in solchen Fällen sicher sofort die Nachfrage kommt, wo der Brandort sei.</p> <p>Eine fehlerhafte Durchsage zum Brandort von Seiten des SL wird vernachlässigt: Der SL wird zum einen sorgfältig darauf achten, den Brandort zutreffend zu benennen. Zum anderen gibt es zwei Möglichkeiten, den Fehler zu erkennen und zu korrigieren:</p> <ul style="list-style-type: none"> • Der SLV hat den Brandort ermittelt, hört die falsche Durchsage, veranlasst den SL zu einer Korrektur der Durchsage und achtet genau darauf, dass die Wiederholung der Durchsage eine korrekte Information zum Brandort enthält. • Der EL holt am vorgesehenen Ort die Unterlage für den Löscheinsatz ab, aus der auch der korrekte Ort des Brandes hervorgeht. Der EL könnte im Fall einer Unklarheit zum Brandort in der Warte nachfragen. Den zugehörigen Zeitaufwand deckt die Zeitspanne von fünf bis zehn min ab, in denen sich der EL und die Löschgruppe für den Einsatz ausrüsten und bereit machen.
Min = 300 s Max = 600 s	<p>Die Mitglieder der Löschgruppe holen die persönliche Schutzausrüstung (PSA) und die Atemgeräte am Aufbewahrungsort (ca. 50 m vom vorgesehenen Sammelpunkt für den anstehenden Einsatz entfernt) ab.</p>	<p>Es entfallen Schritte, die beim Zutritt zum Kontrollbereich üblicherweise zu durchlaufen sind. Die Feuerwehr hat im Einsatzfall schnellen Zutritt zum Kontrollbereich.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>EL, AT und ST gehen unabhängig voneinander zum „Zugang Ringraum“. Der EL holt sich am vorgesehenen Ort die Unterlage für den Löscheinsatz ab. EL, Angriffstrupp (AT) und Schlauchtrupp (ST)</p> <ul style="list-style-type: none"> • nehmen Dosimeter auf. • legen PSA und PA an. • betreten den Ringraum. <p>MA, ME und GT fahren bzw. gehen zum Bereitschaftsplatz vor dem Reaktorgebäude</p>	<p>Vereinfachend wird angenommen, dass der Einsatzleiter (EL), der Angriffstrupp (AT) und der Schlauchtrupp (ST) den Brandort gemeinsam aufsuchen.</p> <p>Die Mitglieder des Gerätetrupps (GT) bleiben am Bereitschaftsplatz außerhalb des Ringraums in Bereitschaft.</p>
<p>Min = 30 s Max = 40 s</p> <p>Min = 30 s Max = 50 s</p>	<p>EL und ST begeben sich zum Ort des Hydranten.</p> <p>Der AT begibt sich so nahe an den Brandort, wie es möglich ist, und stellt fest, dass es im Kabelschacht K brennt und dass der Brand noch auf den Kabelschacht beschränkt ist. Der AT kehrt zurück und informiert den EL.</p>	
<p>Min = 180 s Max = 240 s</p>	<p>Der ST stellt eine Schlauchverbindung zwischen dem Hydranten H und der Schlauchkupplung S der Löschanlage her. Es wird kontrolliert, dass der Schlauch korrekt montiert ist. Gleichzeitig dazu begibt sich AT mit dem Schlauch zum Brandort, um die Brandbekämpfung zu beginnen.</p>	<p>Der dazu notwendige Schlauch befindet sich direkt neben dem Hydranten H. Eine Verwechslung der Hydranten H mit einem benachbarten Hydranten hätte keine Folgen, da die Hydranten alle gleichermaßen mit Löschwasser versorgt werden.</p> <p>Eine Verwechslung der Schlauchkupplung S mit derjenigen anderer Löschanlagen wird ausgeschlossen:</p> <ul style="list-style-type: none"> • Benachbarte Kupplungen sind 2 – 5 m entfernt. • Die Kupplungen sind auch farblich unterschiedlich gekennzeichnet. <p>Ein an falscher Kupplung angeschlossener Schlauch würde auffallen, sobald die Löschanlage in Betrieb genommen wird. Der AT wird dann zusammen mit dem ST den Schlauch unverzüglich an der richtigen Kupplung S anschließen.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>Modellierung von HL 1.0 im Crew-Modul:</p> <pre> HL 1.0 // Ausbruch Brand im Kabelschacht, 2 Brandmelder geben Alarm Bed: & HLcont = 0 /SL / - / 10 20 // SL hört Alarm und sieht blinkende Klasse 2 Meldung /SL / - / 5 15 // SL unterbricht Tätigkeit und quittiert Alarm /SL / SLV / 10 40 // SL weist SLV an BS-Tafel im W-Nebenr zu kontrollieren /SLV / - / 10 20 // SLV geht in Warten-Nebenraum zu den Anzeigen der Melder /SL / - / 20 40 // SL holt Unterlagen die im Brandfall auszufüllen sind /SLV / - / 40 60 // SLV erkennt, dass Brand im Kabelschacht vorliegt /SLV / SL / 30 60 // SLV kehrt in Warte zurück und informiert SL /SL / RF / 5 15 // SL gibt RF Anweisung, GES1+2 zu öffnen /RF / - / 10 20 // RF öffnet GES1+2 /SL / - / 120 180 // SL löst Brandalarm über Funkanlage aus /SL / EL / 0 0 // Durch Brandalarm werden EL,AT,ST, und GT alarmiert /SL / AT / 0 0 // /SL / ST / 0 0 // /SL / GT / 0 0 // /EL / - / 300 600 // AT, ST holt Schutzausrüstung und begibt sich zum RR /EL / AT / 0 0 // /AT / ST / 0 0 // /GT / -3 / 300 600 // GT holt Ausrüstung und geht zum Bereitschaftsplatz außerhalb des RR /GT / MA / 0 0 // MA und ME begeben sich mit GT zum Ber.platz /GT / ME / 0 0 // /EL / ST / 30 40 // EL+ST begeben sich in die Nähe des Hydranten /EL / -1 / 0 0 // Zeit wann EL und ST am Hydranten im RR sind /AT / -2 / 30 50 // AT begibt sich zum Brandort, erkennt Brand im Kabelschacht und informiert EL /EL / ST / 180 240 // EL+ST stellen Schverb zw. Hydrant und Kupplung der Löschanlage her /EL / -4 / 0 0 // Zeitpunkt wann Schlauchverbindung hergestellt if -4 & tBruch = 0 then tBruch = EL // Referenz_Zeit für Bruch /rtBruch / - / -180 180 // Zufallszeit für Brucheintritt zum Zeitpunkt wann Schverb hergestellt ist /rtPrsRed / - / 35 60 // Zufallszeit bis Druckabfall nach Bruch erkennbar ist /rtQ3 / - / 90 135 // Tr(90,105,135): Zufallszeit bis Überfl-Anz für Q3 auf der Reaktoschutztafel ansteht # </pre>	<p>Die HL 1.0 wird als erste auszuführende Handlungsliste aktiviert. Dies wird spezifiziert durch: Bed: & HLcont = 0. D. h., es gibt keine vorher ausgeführte Handlungsliste.</p>

Tab. A. 2 Zufallszeiten für Leitungsbruch, Druckreduktion und Überflutungsanzeige in Abhängigkeit der Zeit, wann die Schlauchverbindung zum Hydranten hergestellt ist → Handlungsablauf für HL 1.01

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>Handlungsablauf zu HL 1.01: E: Zufällig und unabhängig vom bisherigen Ereignis- und Handlungsablauf bricht die Feuerlöschwasserleitung. Der Bruch erfolgt zufällig 3 min vor bzw. nach Herstellung der Schlauchverbindung zum Hydranten. Aus dem Leck strömen 140 – 180 kg/s Löschwasser in den Ringraumquadranten Q3 (so lange, bis das Leck abgesperrt ist). Der Druck im Feuerlöschwassersystem fällt unter den Grenzwert G. Dieser Druckabfall führt zu einem</p> <ul style="list-style-type: none"> • automatischen Start von Feuerlöschwasserpumpen, welche Feuerlöschwasser nachfördern, • charakteristischen Alarm in der Warte, • einer Klasse-2-Meldung „Druck tief“ im Feuerlöschwassersystem, ebenfalls in der Warte. <p>Im Feuerlöschwassersystem des Ringraums fällt der Druck mehr oder minder bald nach dem Zeitpunkt des Bruchs ebenfalls ab. Am Hydranten H steht Feuerlöschwasser mit zunehmend geringerem Druck an.</p>	<p>Die Annahmen zu Zeitpunkt und Zeitfenster des Bruchs sind von Seiten der Ersteller des vorliegenden Handlungsablaufs festgelegt worden. Der Bruch liegt noch vor dem Gebäudeeintrittsschieber GES-1 der Feuerlösch-Wasserleitung innerhalb des Ringraums. Das Leck kann nur durch Schließung der Streckenschieber STS-1 (bzw. STS-2 UND STS-3) auf dem Freigelände der Anlage und des Gebäudeeintritts-Schiebers GES-1, der zur Vorbereitung des Löschens geöffnet worden ist, abgesperrt werden. Das Feuerlöschwassersystem im Ringraum ist gefüllt und steht unter Druck. Zum Zeitpunkt des Bruchs hält sich niemand so nahe an der Bruchstelle auf, dass letztere sofort entdeckt und gemeldet werden kann.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>Modellierung von HL 1.01 im Crew-Modul:</p> <pre data-bbox="436 391 1160 678"> HL 1.01 // Zeitpunkt des Leitungsbruchs in Abhängigkeit von der Zeit, wann Schlauchverbindung hergestellt ist Bed: & HLcont = 1.0 /EL / -21 / 0 0 // Zeitpunkt des Bruchs: Schverb - U(-180,180) if -21 then tBruch += rtBruch & tPrsRed = tBruch & tPrsRed += rtPrsRed & tAnzqQ3 = tBruch & tAnzqQ3 += rtQ3 & EL = tBruch /EL / b_AlarmBruch / 0 0 // akustischer Alarm nach Bruch: 1 - funktioniert 2 - fällt aus (p=5.E-3) # </pre> <p>In der if-Anweisung werden die Zufallszeiten zugeordnet.</p> <p>Nach der Zuordnung des zufälligen Zeitpunkts des Leitungsbruchs wird die Verzweigungsvariable b_AlarmBruch im Modell definiert.</p>	<p>Die HL 1.01 wird aktiviert, wenn</p> <ul style="list-style-type: none"> - die vorhergehende Handlungsliste HL 1.0 ist <p>Dies wird spezifiziert durch: Bed: & HLcont = 1.0</p> <p>Der Zeitpunkt $t_{\text{Verbindung}}$, an dem die Schlauchverbindung hergestellt ist, dient als Referenzzeit, wann der Bruch in der Feuerlöschwasserleitung erfolgt.</p> <p>Es wird angenommen, dass der Leitungsbruch zu einer zufälligen Zeit in dem Intervall 3 min vor und 3 min nach $t_{\text{Verbindung}}$ erfolgt, d. h. $t_{\text{Bruch}} \sim U(t_{\text{Verbindung}} - 180 \text{ s}, t_{\text{Verbindung}} + 180 \text{ s})$, wobei $U(a, b)$ eine Gleichverteilung zwischen a und b beschreibt.</p> <p>Es wird angenommen, dass sich nach einer gleichverteilten Zufallszeit zwischen 35 und 60 s nach dem Bruch eine Druckreduktion bemerkbar macht, d. h. $t_{\text{PrsRed}} = t_{\text{Bruch}} + U(35, 60)$.</p> <p>Nach Abschnitt 6.1.2 wird der Zeitpunkt t_{Q3}, wann die Überflutungsanzeige für den Quadrant Q3 auf der Reaktorschutztafel nach t_{Bruch} ansteht, aus der Dreiecksverteilung zwischen 90 und 135 s bei einem Modalwert von 105 s zufällig ausgespielt, d. h. $t_{\text{Q3}} = t_{\text{Bruch}} + \text{Triangular}(90, 105, 135) \text{ s}$.</p> <p>Durch die Verzweigungsvariable b_AlarmBruch wird die aleatorische Unsicherheit definiert, ob nach dem Leitungsbruch ein Alarm in der Warte ausgelöst wird oder nicht. Es wird angenommen, dass der Alarm mit einer Wahrscheinlichkeit von</p> <ul style="list-style-type: none"> - $p = 0,995$ ausgelöst, und - $1 - p = 0,005$ nicht ausgelöst wird.

Tab. A. 3 Angriffstrupp stellt fest, dass kein Wasser zur Löschung ankommt → Handlungsablauf für HL 1.05

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
<p>Min = 10 s Max = 15 s</p> <p>Min = 30 s Max = 60 s</p> <p>Min = 20 s Max = 40 s</p>	<p>Handlungsablauf zu HL 1.05:</p> <p>Ein Mitglied des ST öffnet auf Anweisung des EL das Ventil am Hydranten H, um dem Schlauch über die Löschanlage Wasser zuzuführen.</p> <p>Zwischenzeitlich wartet der AT in der Nähe des Brandortes darauf, dass die Löschanlage Wasser abgibt.</p> <p>Der AT informiert den EL, dass kein Wasser kommt.</p>	<p>Der AT weiß, dass der EL und der ST die Schlauchverbindung herstellen. Er wartet eine gewisse Zeit auf das Löschwasser, das infolge des Bruchs nicht kommt. Wie lange er wartet, ist zufällig und wird durch die angegebenen Gleichverteilung zwischen 30 und 60 s ausgedrückt.</p> <p>Nach einer gewissen zufälligen Wartezeit informiert der AT den EL.</p>
	<p>Modellierung von HL 1.05 im Crew-Modul:</p> <pre data-bbox="436 837 1160 1005"> HL 1.05 // Bed: & HLcont = 1.01 / EL / ST / 10 15 // EL gibt Anw. und Ventil des Hydranten wird geöffnet / AT / - / 30 60 // AT wartet auf Wasser / AT / EL / 20 40 // AT ruft EL an und informiert dass kein Wasser kommt # </pre>	<p>Die HL 1.051 wird aktiviert, wenn die vorhergehende Handlungsliste HL 1.01 ist.</p> <p>Dies wird spezifiziert durch: Bed: & HLcont = 1.01</p> <p>Ansonsten werden in HL 1.05 die Basishandlungen spezifiziert, die oben beschrieben wurden.</p>

Tab. A. 4 Abhängigkeit des Handlungsablaufs vom Zeitpunkt, zu dem sich die Druckreduktion im Schlauch bemerkbar macht → Handlungsablauf für HL 1.051 und HL 1.052

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
<p>5 s</p> <p>5 s</p>	<p>Handlungsablauf zu HL 1.051: E: Die Druckreduktion macht sich noch nicht bemerkbar: In diesem Fall wird angenommen, dass der EL die Ursache des ausbleibenden Wassers untersucht, bis sich die Druckreduktion bemerkbar macht.</p> <p>Danach wird angenommen, dass der EL sofort erkennt, dass kein Druck in der Leitung ist.</p> <p>Handlungsablauf zu HL 1.052: E: Druckreduktion macht sich bereits bemerkbar: Es wird angenommen, dass EL sofort erkennt, dass kein Druck in der Leitung ist.</p>	<p>Wenn der EL die Information vom AT erhält, ist der weitere Handlungsablauf abhängig davon, ob sich zu diesem Zeitpunkt die Druckreduktion durch den Leitungsbruch schon bemerkbar macht oder noch nicht.</p>
	<p>Modellierung von HL 1.051 und 1.052 im Crew-Modul:</p> <pre data-bbox="421 911 1144 1106"> HL 1.051 // Zeitpunkt wann sich Druckreduktion bemerkbar macht ist noch nicht erreicht Bed: & HLcont = 1.05 & EL < tPrsRed /EL /-23 / 0 0 // EL wird Zeit zugewiesen wann sich DruckRed einstellt if -23 then EL = tPrsRed /EL /-5 / 5 5 // EL erkennt dass kein Druck in der Leitung ist # </pre> <pre data-bbox="421 1118 1061 1246"> HL 1.052 // Zeitpunkt wann sich Druckreduktion bemerkbar macht ist erreicht Bed: & HLcont = 1.05 & EL >= tPrsRed /EL /-5 / 5 5 // EL erkennt dass kein Druck in der Leitung ist # </pre>	<p>Die HL 1.051 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 1.05 ist und • wenn der EL informiert wird, bevor sich Druckreduktion einstellt. <p>Dies wird durch die Bedingung Bed: & HLcont = 1.05 & EL < tPrsRed spezifiziert.</p> <p>Durch die if-Anweisung wird dem EL die Zeit tPrsRed zugeordnet, zu der sich die Druckreduktion bemerkbar macht.</p> <p>Die HL 1.052 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 1.05 ist und • EL informiert wird, nachdem die Druckreduktion bemerkbar ist. <p>Dies wird durch die Bedingung Bed: & HLcont = 1.05 & EL ≥ tPrsRed spezifiziert.</p>

Tab. A. 5 Abhängigkeit des Handlungsablaufs von der Unsicherheit, ob ein Alarm ausgelöst wird oder nicht, und der Verfügbarkeit des Schichtleiters → Handlungsablauf für HL 1.1, HL 1.2 und HL 1.3

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>E: Der akustische Alarm ist von Meldeeinrichtungen ausgelöst worden, die sich im Feuerlöschwassersystem (Drucküberwachung) befinden.</p> <ul style="list-style-type: none"> • Der Druck in der Feuerlöschwasserleitung liegt unter dem Grenzwert G. • Die Brunnenwasser-versorgten Feuerlöschwasser-Pumpen sind automatisch angelaufen und fördern. Die anderen Feuerlöschwasserpumpen (Flusswasser) werden zeitverzögert zugeschaltet, wenn der erforderliche Druck in der Feuerlöschwasserleitung nicht wieder erreicht wird. 	<p>Der Alarm in der Warte wird ausgelöst. Der Alarm unterscheidet sich von allen anderen Alarmen deutlich. Die Bedeutung des Alarms ist gut bekannt. Er kann mehrmals pro Woche ausgelöst werden, wenn bestimmte Grenzwerte, z. B. wegen Druckschwankungen im Feuerlöschwassersystem, ansprechen, die bei Übungen üblich sind.</p> <p>Die Schichtmannschaft in der Warte</p> <ul style="list-style-type: none"> • hört den charakteristischen Alarm, der durch Erreichen des Grenzwertes G (Druck in der Feuerlöschwasserleitung) ausgelöst wird, • sieht die auffällig blinkende Klasse-2-Meldung „Druck tief“ im Feuerlöschwassersystem und • weiß, dass in dieser Situation die Brandschutztafel zu kontrollieren ist.
<p>Min = 5 s Max = 20 s</p> <p>Min = 10 s Max = 40 s</p> <p>Min = 10 s Max = 20 s</p> <p>Min = 20 s Max = 45 s</p>	<p>Handlungsablauf zu HL 1.1:</p> <p>Der SL unterbricht seine aktuelle Tätigkeit, und lässt den Alarm quittieren.</p> <p>Der SL prüft, welcher Mitarbeiter in der Warte für die Kontrolle der Brandschutztafel abkömmlich ist, sieht, dass einer seiner Stellvertreter (SLV) verfügbar ist und beauftragt ihn, die Anzeigen auf der Brandschutztafel zu kontrollieren.</p> <p>Der SLV begibt sich zur Brandschutztafel.</p> <p>Der SLV kontrolliert die Anzeigen auf der Brandschutztafel. Zu diesem Zeitpunkt wird angenommen, dass der SLV durch den zusätzlichen Alarm einen erhöhten Stress entwickeln kann.</p>	<p>Erfolgt dann, wenn der SL zum Zeitpunkt des Alarms verfügbar ist.</p> <p>Nach Quittierung verstummt der Alarm, die Meldung steht in Ruhiglicht an. Wie bei dem Brandalarm wird die Möglichkeit, dass nach der Quittierung jede weitere Aktion unterbleibt als unplausibel außer Acht gelassen. Die gesamte Schichtmannschaft erwartet nun die Kontrolle der Brandschutztafel und würde den SL darauf hinweisen, wenn diese Kontrolle unterbliebe.</p> <p>Ein Ausfall der Anzeigen auf der Brandschutztafel wird nicht unterstellt. Ablesefehler sind unplausibel:</p> <ul style="list-style-type: none"> • Der SLV wendet seine volle Aufmerksamkeit der Brandschutztafel zu, die Kontrolle ist seine einzige Aufgabe.

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
		<ul style="list-style-type: none"> Die Anzeigen sind übersichtlich angeordnet, nicht zu verwechseln und eindeutig. <p>Eine Abschaltung der Feuerlöschwasserpumpen von Hand ist möglich, aber wirkungslos: Die Automatik schaltet die Pumpen so lange sofort wieder zu, als der Druck unter dem Grenzwert G liegt.</p>
	<p>Modellierung von HL 1.1 im Crew-Modul:</p> <pre style="border: 1px solid black; padding: 5px;"> HL 1.1 // Alarm funktioniert + SL ist zum Zeitpunkt des Bruchs verfügbar Bed: & HLcont >= 1.051 & HLcont <= 1.052 & b_AlarmBruch = 1 & SL <= tBruch / SL / -30 / 0 0 // SL ist verfügbar wenn Br-Alarm einsetzt und kann Bearbeitung übernehmen if -30 then SL = tBruch // SL wird die Zeit des Bruchs zugewiesen / SL / - / 5 20 // SL unterbricht Tätigkeit und lässt Alarm quittieren / SL / SLV / 10 40 // SL prüft welcher Mitarbeiter frei ist; weist SLV an RS-Tafel zu kontrollieren / SLV / - / 10 20 // SLV begibt sich zur RS-Tafel / SLV / b_stresSLV / 0 0 // Stress durch zusätzlichen Alarm 1 - normal (0,4) 2 - hoch (0,6) # </pre>	<p>HL 1.1 wird aktiviert, wenn</p> <ul style="list-style-type: none"> die vorhergehende Handlungsliste 1.051 oder 1.052 ist und Alarm in der Warte ausgelöst wird (b_AlarmBruch = 1) und der SL zum Zeitpunkt des Alarms nicht beschäftigt ist (SL < tBruch). <p>Wenn der SL verfügbar ist, wird ihm der Zeitpunkt des Bruchs zugewiesen, zu dem auch der Alarm stattfindet. Ab diesem Zeitpunkt fängt der SL mit den entsprechenden Handlungen an.</p> <p>Durch die Verzweigungsvariable b_stresSLV wird die Unsicherheit berücksichtigt, ob der SLV nach dem zusätzlichen Alarm einen hohen Stress entwickelt oder nicht. Zur Stressentwicklung des SLV werden folgende Wahrscheinlichkeiten angenommen (siehe Abschnitt 6.1.4):</p> <ul style="list-style-type: none"> Stress normal mit Wahrscheinlichkeit 0,4, Stress hoch mit Wahrscheinlichkeit 0,6.
<p>Min = 5 s Max = 15 s</p> <p>Min = 10 s Max = 20 s</p> <p>Min = 20 s Max = 45 s</p>	<p>Handlungsablauf zu HL 1.2:</p> <p>Der SLV unterbricht seine Tätigkeit und quittiert den Alarm.</p> <p>Der SLV begibt sich zur Brandschutztafel.</p> <p>Der SLV kontrolliert die Anzeigen auf der Brandschutztafel. Zu diesem Zeitpunkt wird angenommen, dass der SLV durch den zusätzlichen Alarm einen erhöhten Stress entwickeln kann.</p>	<p>Erfolgt dann, wenn SL zum Zeitpunkt des Alarms nicht verfügbar ist.</p> <p>Der SLV weiß, dass der SL mit anderen Aufgaben beschäftigt ist und nicht zur Verfügung steht. Deshalb wird angenommen, dass der SLV sofort die Bearbeitung des Alarms übernimmt.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>Modellierung von HL 1.2 im Crew-Modul:</p> <pre data-bbox="421 363 1146 655"> HL 1.2 // Alarm funktioniert und SL ist zum Zeitpkt des Bruchs nicht verfügbar Bed: & HLcont >= 1.051 & HLcont <= 1.052 & b_AlarmBruch = 1 & SL > tBruch /SLV/ -31 / 0 0 // SLV übernimmt die Bearbeitung des Alarms da SL nicht verf if -31 then SLV = tBruch /SLV/ - / 5 15 // SLV unterbricht Tätigkeit und quittiert Alarm /SLV/ - / 10 20 // SLV begibt sich zur RS-Tafel /SLV/ - / 20 45 // SLV kontrolliert Anzeigen der RST /SLV/ b_stresSLV/ 0 0 // Stress durch zusätzlichen Alarm 1 - normal (0.4) 2 - hoch (0.6) # </pre>	<p>HL 1.2 wird aktiviert, wenn</p> <ul data-bbox="1191 336 1917 424" style="list-style-type: none"> • die vorhergehende Handlungsliste HL 1.051 oder 1.052 ist und • Alarm in der Warte ausgelöst wird (b_AlarmBruch = 1) und • SL zum Zeitpunkt des Alarms beschäftigt ist (SL > tBruch). <p>Der SLV wird Zeitpunkt des Bruchs zugewiesen, zu dem auch der Alarm stattfindet. Ab diesem Zeitpunkt fängt der SLV mit den entsprechenden Handlungen an. Die Unsicherheit der Stressentwicklung vom SLV ist analog zu HL 1.1.</p>
<p>Min = 60 s Max = 180 s</p> <p>Min = 45 s ax = 60 s</p> <p>Min = 60 s Max = 90 s</p> <p>Min = 10 s Max = 20 s</p> <p>Min = 15 s Max = 25 s</p> <p>Min = 10 s Max = 20 s</p> <p>Min = 60 s Max = 120 s</p> <p>Min = 20 s Max = 45 s</p>	<p>Handlungsablauf zu HL 1.3:</p> <p>Der EL ruft den SL in Warte an und meldet Druckabfall. Das weitere Vorgehen wird zwischen EL und SL abgesprochen.</p> <p>Der EL weist den AT an, sich zum GES-1 zu begeben, der sich dorthin begibt.</p> <p>Der AT erkennt Wassereintritt in Q3 und findet Leitungsleck in der Nähe von GES-1.</p> <p>Der AT informiert den EL über das Leck in Q3.</p> <p>Der EL ruft den SL in der Warte an und informiert den SL über das Leck.</p> <p>Der EL weist den AL an, GES-1 vor Ort schließen zu lassen.</p> <p>Der AT schließt GES-1 und wartet, bis GES-1 komplett zugefahren ist.</p> <p>Parallel dazu weist der SL den SLV an, den Streckenschieber SLS-1 auf dem Gelände schließen zu lassen.</p>	<p>Erkennung des Lecks durch die Feuerwehr im Ringraum, wenn nach dem Leitungsbruch der Alarm in der Warte nicht ausgelöst wird.</p> <p>In HL 1.051 bzw. HL 1.052 hat der EL erkannt, dass kein Druck in der Leitung ist.</p> <p>Verschiedene Möglichkeiten werden in Betracht gezogen.</p> <p>In der Zeitspanne ist die Wegzeit vom Brandort bis zum Quadranten Q3 enthalten.</p> <p>In dieser Zeitspanne wird berücksichtigt, dass der AT eine gewisse Zeit nach dem Leck suchen muss.</p> <p>Sie sind sich einig, GES-1 schließen zu lassen.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>Modellierung von HL 1.3 im Crew-Modul:</p> <pre> HL 1.3 // Alarm wird in Warte nicht ausgelöst Bed: & HLcont >= 1.051 & HLcont <= 1.052 & b_AlarmBruch = 2 / EL / SL / 60 180 // EL ruft SL in Warte und meldet Druckabfall. Beratung des weiteren Vorgehens. / EL / AT / 45 60 // EL schickt AT zu GES-1, der sich dorthin begibt. / AT / -6 / 60 90 // AT findet Leck in der Nähe von GES-1 und erkennt Wassereintritt in Q3. / AT / EL / 10 20 // AT informiert EL über das Leck in Q3 / EL / SL / 15 25 // EL informiert SL / EL / AT / 10 20 // EL weist AT an GES-1 vor Ort zu schließen / AT / -7 / 60 120 // AT schließt GES-1 und wartet bis GES-1 komplett zu ist / SL / SLV / 20 45 // SL weist SLV an Streckenschieber auf dem Gelände schließen zu lassen # </pre>	<p>HL 1.3 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 1.051 oder HL 1.052 ist und • der Alarm in der Warte nicht ausgelöst wird (b_AlarmBruch = 2).

Tab. A. 6 Definition der Unsicherheit, wann der SLV die Überflutungsanzeige erkennt und die Diagnose erstellt → Handlungsablauf für HL 2.01, HL 2.02, HL 2.03 und HL 2.031 (Fortsetzung von HL 1.1 und HL 1.2)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>Handlungsablauf zu HL 2.01, 2.02, 2.03 und 2.031: Unterschiede zwischen HL 2.01, HL 2.02, HL 2.03 und HL 2.031 bestehen im Zustand des Stressniveaus des SLV und in den Zeiten, wann der SLV an der Reaktorschutztafel ankommt. Abhängig davon werden die Unsicherheiten spezifiziert, wie schnell SLV die Anzeigen registriert und die Überflutung des Q3 korrekt bewertet.</p>	<p>Es wird angenommen, dass der SLV auf jeden Fall eine korrekte Bewertung der Anzeigen durchführt, nur in unterschiedlicher Zeit, die vom Stress und von der Zeit abhängt, wann er an der RST ankommt.</p>
	<p>Modellierung von HL 2.01 im Crew-Modul:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>HL 2.01 // SLV steht vor der Anzeige AnzQ3 an der RST. Sein Stresslevel ist normal Bed: &HLcont >= 1.1 & HLcont <= 1.2 & b_stresSLV = 1 & SLV < tAnzQ3 /SLV / b_detAnzQ3 / 0 0 // SLV erkennt Anzeige 1-schnell (0.7) 2-verzögert (0.3) 3-stark verzögert (p=0) #</p> </div>	<p>HL 2.01 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 1.1 oder 1.2 ist und • der SLV normalen Stress hat ($b_stresSLV = 1$) und • der SLV an der RST ankommt, bevor die Überflutungsanzeige für Quadrant Q3 an der RST erscheint ($SLV < t_{AnzQ3}$). <p>Mit der Verzweigungsvariable $b_detAnzQ3$ werden die Unsicherheiten modelliert, in welcher Zeit SLV die Überflutungsanzeige erkennt und Diagnose erstellt. Die angenommenen Unsicherheiten sind in Abschnitt 6.1.5 erläutert.</p>
	<p>Modellierung von HL 2.02 im Crew-Modul:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>HL 2.02 // SLV steht vor der Anzeige AnzQ3 an der RST. Sein Stresslevel ist hoch. Bed: &HLcont >= 1.1 & HLcont <= 1.2 & b_stresSLV = 2 & SLV < tAnzQ3 /SLV / b_detAnzQ3 / 0 0 // SLV erkennt Anzeige 1-schnell (0.1) 2-verzögert (0.5) 3-stark verzögert (p=0.4) #</p> </div>	<p>HL 2.02 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 1.1 oder 1.2 ist und • SLV hohen Stress hat ($b_stresSLV = 2$) und • SLV an RST ankommt, bevor Überflutungsanzeige für Quadrant Q3 an der RST erscheint ($SLV < t_{AnzQ3}$). <p>Unsicherheiten sind in Abschnitt 6.1.5 erläutert.</p>
	<p>Modellierung von HL 2.03 im Crew-Modul:</p>	<p>HL 2.03 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 1.1 oder 1.2 ist und • SLV normalen Stress hat ($b_stresSLV = 1$) und • Überflutungsanzeige für Quadrant Q3 ansteht, bevor der SLV an der RST ankommt ($SLV > t_{AnzQ3}$). <p>Unsicherheiten sind in Abschnitt 6.1.5 erläutert.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>HL 2.03 // Anzeige Q3 steht auf der RST bereits an, wenn SLV dort ankommt. Normaler Stress Bed: & HLcont >= 1.1 & HLcont <= 1.2 & b_stresSLV = 1 & SLV > tAnzQ3 / SLV / b_detAnzQ3 / 0 0 // SLV erkennt Anzeige 1-schnell (0.85) 2-verzögert (0.15) 3-stark verzögert (p=0.) #</p>	
	<p>Modellierung von HL 2.031 im Crew-Modul:</p> <p>HL 2.031 // Anzeige Q3 steht auf der RST bereits an, wenn SLV dort ankommt. Hoher Stress. Bed: & HLcont >= 1.1 & HLcont <= 1.2 & b_stresSLV = 2 & SLV > tAnzQ3 / SLV / b_detAnzQ3 / 0 0 // SLV erkennt Anzeige 1-schnell (0.4) 2-verzögert (0.4) 3-stark verzögert (p=0.2) #</p>	<p>HL 2.031 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 1.1 oder 1.2 ist und • SLV hohen Stress hat (b_stresSLV = 2) und • Überflutungsanzeige für Quadrant Q3 ansteht, bevor der SLV an der RST ankommt (SLV > t_{AnzQ3}). <p>Unsicherheiten sind in Abschnitt 6.1.5 erläutert.</p>

Tab. A. 7 Bewertung der Anzeigen in Abhängigkeit vom Stress → Handlungsablauf für HL 2.04, HL 2.05 und HL 2.06 (Fortsetzung von HL 2.01 und HL 2.02)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
<p>Min = 120 s Max = 150 s</p>	<p>Handlungsablauf zu HL 2.04: Der SLV kontrolliert die rechnerbasierten und konventionellen Anzeigen in der Warte.</p> <p>Der SLV beobachtet die Anzeigen eine Zeitlang, um sich von der Stabilität des Ist-Zustands zu überzeugen. Bei schneller Ausführung wird dafür ein Zeitbedarf zwischen 120 und 150 s angenommen.</p>	<p>Der SLV erkennt und diagnostiziert schnell.</p> <p>Während der SLV prüft, erscheint die Überflutungsanzeige. Ab diesem Zeitpunkt kann der SLV die Überflutung erkennen, wenn er die Anzeige registriert. Er erkennt weiter:</p> <ul style="list-style-type: none"> • Im Ringraum wird <u>kein</u> Anstieg der Radioaktivität angezeigt, der Anstieg der Füllstände geht also nicht auf Wasser aus einem Leck im Primärkreis zurück. • Melder im Ringraum, die bei Heißwasser ansprechen würden, haben <u>nicht</u> angesprochen, d. h. es liegt kein Leck in Komponenten im Reaktorgebäude vor, die Heißwasser führen. • Der Druck in der Feuerlöschwasserleitung bleibt permanent unter dem Grenzwert G. <p>Der Fehler, dass die Kontrollen komplett unterbleiben, ist unplausibel, da der SLV auf diese Aufgaben konzentriert ist. Für Heißwasser und Radioaktivität: keine Anzeige erhöhter Werte, da Meseinrichtungen nicht beaufschlagt werden. Daher keine Plausibilität der Möglichkeit, irrtümlich einen erhöhten Wert festzustellen.</p>
	<p>Modellierung von HL 2.04 im Crew-Modul:</p> <pre data-bbox="421 1129 1099 1313"> HL 2.04 // SLV identifiziert Überflutung schnell wenn Anzeige ansteht Bed: & HLcont >= 2.01 & HLcont <= 2.02 & b_detAnzQ3 = 1 /SLV/ -33 / 0 0 // Während SLV prüft erscheint AnzgQ3. Zeit wird SLV zugeordnet if -33 & SLV <= tAnzgQ3 then SLV = tAnzgQ3 /SLV / - / 120 150 // SLV kontr rechnbas und konv Anzeigen. Dabei erkennt er AnzgQ3 # </pre>	<p>HL 2.04 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 2.01 oder 2.02 ist und • schnelle Bewertung der Anzeigen vorliegt (b_detAnzQ3 = 1) <p>Zuordnung der Zeit, wann die Anzeige auf der RST erscheint.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 150 s Max = 240 s	<p>Handlungsablauf zu HL 2.05:</p> <p>Der SLV kontrolliert die rechnerbasierten und konventionellen Anzeigen in der Warte zeitverzögert.</p> <p>Der SLV beobachtet die Anzeigen eine Zeitlang, um sich von der Stabilität des Ist-Zustands zu überzeugen. Bei verzögerter Ausführung wird dafür ein Zeitbedarf zwischen 150 und 240 s angenommen.</p>	<p>Der SLV erkennt und bewertet die Anzeigen zeitverzögert.</p> <p>Ansonsten ist der Handlungsablauf analog zu HL 2.04.</p>
	<p>Modellierung von HL 2.05 im Crew-Modul:</p> <pre data-bbox="421 608 1167 804"> HL 2.05 // SLV identifiziert Überflutung verzögert wenn Anzeige ansteht Bed: & HLcont >= 2.01 & HLcont <= 2.02 & b_detAnzQ3 = 2 /SLV / -33 / 0 0 // Während SLV prüft erscheint AnzgQ3. Zeit wird SLV zugeordnet if -33 & SLV <= tAnzgQ3 then SLV = tAnzgQ3 /SLV / - / 150 240 // SLV kontr rechnbas und konv Anzeigen. Dabei erkennt er AnzgQ3 # </pre>	<p>HL 2.05 wird aktiviert, wenn</p> <ul data-bbox="1211 584 1944 639" style="list-style-type: none"> • die vorhergehende HL 2.01 oder 2.02 ist und • verzögerte Bewertung der Anzeigen vorliegt (b_detAnzQ3 = 2) ist. <p>Zuordnung der Zeit, wann die Anzeige auf der RST erscheint.</p>
Min = 240 s Max = 420 s	<p>Handlungsablauf zu HL 2.06:</p> <p>Der SLV kontrolliert die rechnerbasierten und konventionellen Anzeigen in der Warte stark zeitverzögert.</p> <p>Der SLV beobachtet die Anzeigen eine Zeitlang, um sich von der Stabilität des Ist-Zustands zu überzeugen. Bei stark verzögerter Ausführung wird dafür ein Zeitbedarf zwischen 240 und 420 s angenommen.</p>	<p>Der SLV erkennt und bewertet die Anzeigen stark zeitverzögert.</p> <p>Im Fall, dass der SLV normalen Stress aufweist, wird angenommen, dass die Kontrolle der Anzeigen nicht stark zeitverzögert ist. Ansonsten ist der Handlungsablauf analog zu HL 2.04.</p>
	<p>Modellierung von HL 2.06 im Crew-Modul:</p> <pre data-bbox="421 1139 1167 1326"> HL 2.06 // SLV identifiziert Überflutung stark verzögert wenn Anzeige ansteht Bed: & HLcont >= 2.01 & HLcont <= 2.02 & b_detAnzQ3 = 3 /SLV / -33 / 0 0 // Während SLV prüft erscheint AnzgQ3. Zeit wird SLV zugeordnet if -33 & SLV <= tAnzgQ3 then SLV = tAnzgQ3 /SLV / - / 240 420 // SLV kontr rechnbas und konv Anzeigen. Dabei erkennt er AnzgQ3 # </pre>	<p>HL 2.06 wird aktiviert, wenn</p> <ul data-bbox="1211 1115 1883 1198" style="list-style-type: none"> • die vorhergehende Handlungsliste HL 2.01 oder 2.02 ist und • stark verzögerte Bewertung der Anzeigen vorliegt (b_detAnzQ3 = 3). <p>Zuordnung der Zeit, wann die Anzeige auf der RST erscheint.</p>

Tab. A. 8 Bewertung der Anzeigen in Abhängigkeit vom Stress → Handlungsablauf für HL 2.07, HL 2.08 und HL 2.09 (Fortsetzung von HL 2.03 und HL 2.031)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 120 s Max = 150 s	<p>Handlungsablauf zu HL 2.07:</p> <p>Der SLV kontrolliert die rechnerbasierten und konventionellen Anzeigen in der Warte schnell. Der SLV beobachtet die Anzeigen eine Zeitlang, um sich von der Stabilität des Ist-Zustands zu überzeugen.</p> <p>Bei schneller Ausführung wird dafür ein Zeitbedarf zwischen 120 und 150 s angenommen.</p>	<p>SLV erkennt und bewertet Anzeigen schnell.</p> <p>Wenn der SLV an der RST ankommt, steht die Überflutungsanzeige bereits an.</p> <p>Der Unterschied zu HL 2.04 besteht in der Wahrscheinlichkeitsbewertung, mit der die Zeitverteilung der schnellen Ausführung zu Anwendung kommt. Ansonsten ist der Handlungsablauf analog zu HL 2.04.</p>
	<p>Modellierung von HL 2.07 im Crew-Modul:</p> <pre data-bbox="421 751 1167 890"> HL 2.07 // SLV identifiziert Überflutung schnell Bed: & HLcont >= 2.03 & HLcont <= 2.031 & b_detAnzQ3 = 1 / SLV / - / 120 150 // SLV kontr rechnbas und konv Anzeigen. Dabei erkennt er AnzgQ3 # </pre>	<p>HL 2.07 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 2.03 oder 2.031 ist und • schnelle Bewertung der Anzeigen vorliegt (b_detAnzQ3 = 1).
Min = 150 s Max = 240 s	<p>Handlungsablauf zu HL 2.08:</p> <p>Der SLV kontrolliert die rechnerbasierten und konventionellen Anzeigen in der Warte zeitverzögert. Der SLV beobachtet die Anzeigen eine Zeitlang, um sich von der Stabilität des Ist-Zustands zu überzeugen. Bei verzögerter Ausführung wird dafür ein Zeitbedarf zwischen 150 und 240 s angenommen.</p>	<p>Der SLV erkennt und bewertet die Anzeigen zeitverzögert.</p> <p>Wenn SLV an RST ankommt, steht die Überflutungsanzeige bereits an. Der Unterschied zu HL 2.05 besteht in der Wahrscheinlichkeitsbewertung, mit der die Zeitverteilung der verzögerten Ausführung zu Anwendung kommt. Ansonsten ist der Handlungsablauf analog zu HL 2.05.</p>
	<p>Modellierung von HL 2.08 im Crew-Modul:</p> <pre data-bbox="421 1198 1167 1337"> HL 2.08 // SLV identifiziert Überflutung verzögert Bed: & HLcont >= 2.03 & HLcont <= 2.031 & b_detAnzQ3 = 2 / SLV / - / 150 240 // SLV kontr rechnbas und konv Anzeigen. Dabei erkennt er AnzgQ3 # </pre>	<p>HL 2.08 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 2.03 oder 2.031 ist und • eine verzögerte Bewertung der Anzeigen vorliegt (b_detAnzQ3 = 2).

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 240 s Max = 420 s	<p>Handlungsablauf zu HL 2.09:</p> <p>Der SLV kontrolliert die rechnerbasierten und konventionellen Anzeigen in der Warte stark zeitverzögert.</p> <p>Der SLV beobachtet die Anzeigen eine Zeitlang, um sich von der Stabilität des Ist-Zustands zu überzeugen.</p> <p>Bei stark verzögerter Ausführung wird dafür ein Zeitbedarf zwischen 240 und 420 s angenommen.</p>	<p>Der SLV erkennt und bewertet die Anzeigen stark zeitverzögert.</p> <p>Im Fall, dass der SLV normalen Stress aufweist, wird angenommen, dass die Kontrolle der Anzeigen nicht stark zeitverzögert ist.</p> <p>Wenn der SLV an der RST ankommt, steht die Überflutungsanzeige bereits an.</p> <p>Der Unterschied zu HL 2.05 besteht in der Wahrscheinlichkeitsbewertung, mit der die Zeitverteilung der stark verzögerten Ausführung zu Anwendung kommt. Ansonsten ist der Handlungsablauf analog zu HL 2.06.</p>
	<p>Modellierung von HL 2.09 im Crew-Modul:</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>HL 2.09 // SLV identifiziert Überflutung stark verzögert Bed: & HLcont >= 2.03 & HLcont <= 2.031 & b_detAnzQ3 = 3 /SLV / - / 240 420 // SLV kontr rechnerbas und konv Anzeigen. Dabei erkennt er AnzgQ3 #</pre> </div>	<p>HL 2.09 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die die vorhergehende Handlungsliste HL 2.03 oder 2.031 ist und • eine stark verzögerte Bewertung der Anzeigen vorliegt (b_detAnzQ3 = 3).

Tab. A. 9 Diagnose und weiteres Vorgehen → Handlungsablauf für HL 2.1 (Fortsetzung von HL 2.04 – HL 2.09)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 120 s Max = 150 s	<p>Handlungsablauf zu HL 2.1: Der SLV meldet dem SL das Ergebnis seiner Kontrollen. Sie erstellen Diagnose und diskutieren das weitere Vorgehen.</p>	<p>Zur korrekten Diagnose gehört auch die Erkenntnis, welche weiteren Schritte die Meisterung des Ist-Zustands erfordert.</p> <p>Es ist unplausibel, dass Bericht, Feststellung des Ist-Zustands und Anweisung zum Absperrern der Schieber unterbleiben oder fehlerhaft sind: die Aufmerksamkeit von SL bzw. SLV ist auf diese Aufgaben konzentriert, der Wassereintrag in den Ringraum hat eine zu hohe sicherheitstechnische Bedeutung.</p> <p>Es wird eine Überflutung des Ringraums durch Bruch der Feuerlöschwasserleitung und Ausströmen des Feuerlöschwassers in den Ringraum-Quadranten Q3 diagnostiziert. Damit steht fest, dass der Streckenschieber STS-1 auf dem Anlagengelände, der die gebrochene Leitung absperrt, vor Ort von Hand zu schließen ist. Ebenso hat der offene Gebäudeeintrittsschieber GES-1 geschlossen zu sein, damit kein Wasser aus dem unter Druck stehenden Feuerlöschwassersystem im Ringraum über das Leck austritt.</p>

Tab. A. 10 Einsatzleiter erkennt Druckabfall, bevor Diagnose in Warte erstellt ist → Handlungsablauf für HL 2.2 (Fortsetzung von HL 2.1)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 60 s Max = 120 s	<p>Handlungsablauf zu HL 2.2: EL ruft in der Warte an und meldet SL den festgestellten Druckabfall. Sie besprechen weiteres Vorgehen.</p>	<p>I In HL 1.051 bzw. HL 1.052 stellen AT und EL während der Brandbekämpfung fest, dass in der Wasserleitung kein Druck ist. Wenn sie dies erkennen, bevor die Diagnose des Leitungsbruchs in der Warte erstellt ist, ruft der EL in der Warte an und informiert den SL.</p>
Min = 5 s Max = 5 s	Der SL weist den EL an, GES-1 vor Ort zu schließen zu lassen.	Die Anweisung beinhaltet auch, dass Streckenschieber STS-2 und STS-3 in unmittelbarer Nähe zu schließen sind, falls sich der Streckenschieber STS-1 nicht schließen lassen sollte.
Min = 15 s Max = 30 s	Unmittelbar danach weist SL den SLV an, Streckenschieber STS-1 auf dem Gelände schließen zu lassen.	Die Wegezeit von AT vom Brandort bis zum Ort des GES-1 ist in der Zeitabschätzung berücksichtigt.
Min = 45 s Max = 60 s	Parallel dazu weist EL den AT an, sich zu GES-1 zu begeben und diesen zu schließen. AT begibt sich zum Ort des GES-1.	Es wird angenommen, dass die Suche nach dem Leck etwas Zeit in Anspruch nehmen wird. Den Wassereintritt wird dagegen vom AT recht schnell bemerkt werden.
Min = 60 s Max = 90 s	AT findet das Leck in der Leitung, welches sich in der Nähe von GES-1 befindet. Außerdem bemerkt er den Wassereintritt in den Quadranten Q3.	
Min = 60 s Max = 120 s	Der AT schließt GES-1 und wartet, bis GES-1 komplett geschlossen ist.	
Min = 10 s Max = 20 s	Der AT informiert den EL über das Leck in Q3 und dass GES-1 abgesperrt wurde.	
Min = 15 s Max = 25 s	Der EL informiert den SL über Leck und dass GES-1 abgesperrt wurde.	

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>Modellierung von HL 2.2 im Crew-Modul:</p> <div style="border: 1px solid black; padding: 5px;"> <p>HL 2.2 // EL erkennt dass kein Druck in der Ltg ist bevor Diagnose des Alarms erstellt ist Bed: & HLcont = 2.1 & EL < SL / EL / SL / 60 120 // EL ruft SL in Warte an und meldet Druckabfall. Beratung des weiteren Vorgehens. / SL / EL / 5 5 // SL weist EL an, GES-1 vor Ort zu schließen / SL / SLV / 15 30 // SL weist SLV an Streckenschieber auf dem Gelände schließen zu lassen / EL / AT / 45 60 // EL schickt AT zu GES-1, der sich dorthin begibt. / AT / -7 / 60 90 // AT findet Leck in der Nähe von GES-1 und erkennt Wassereintritt in Q3. / AT / -8 / 60 120 // AT schließt GES-1 und wartet bis GES-1 komplett zu ist / AT / EL / 10 20 // AT informiert EL über das Leck und das GES-1 geschlossen wurde. / EL / SL / 15 25 // EL informiert SL, dass GES-1 abgesperrt ist #</p> </div>	<p>HL 2.2 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 2.1 ist und • EL den Druckabfall in der Leitung bemerkt, bevor SL die Diagnose in der Warte erstellt hat (EL < SL). <p>Die aktuelle Zeit vom EL wird in HL 1.051 bzw. HL 1.052, die vom SL in HL 2.1 ermittelt.</p>

Tab. A. 11 Diagnose des SL liegt vor, bevor der Einsatzleiter den Druckabfall in der Leitung feststellt → Handlungsablauf für HL 2.3 (Fortsetzung von HL 2.1)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 40 s Max = 70 s	Handlungsablauf zu HL 2.3: SL ruft EL an und informiert diesen über den Alarm und die erstellte Diagnose. Sie besprechen weiteres Vorgehen.	Wenn die Diagnose in der Warte erstellt ist, bevor EL der Feuerwehr den Druckabfall in der Leitung feststellt, wird SL den EL unmittelbar über den Alarm und die erstellte Diagnose informieren.
Min = 45 s Max = 60 s	Der EL weist den AT an, sich in den Quadranten Q3 zu begeben, um die Situation vor Ort zu kontrollieren. Der AT begibt sich in den Quadranten Q3.	Die Wegezeit von AT vom Brandort bis zum Quadranten Q3 ist in der Zeitabschätzung berücksichtigt.
Min = 60 s Max = 90 s	Der AT findet das Leck in der Leitung, welches sich in der Nähe von GES-1 befindet. Außerdem bemerkt er den Wassereintritt in den Quadranten Q3.	Es wird angenommen, dass der AT weiß, dass GES-1 in der gegebenen Situation abzusperren ist.
Min = 60 s Max = 120 s	Der AT schließt GES-1 und wartet, bis GES-1 komplett geschlossen ist.	Die Anweisung beinhaltet auch, dass Streckenschieber STS-2 und STS-3 in unmittelbarer Nähe zu schließen sind, falls sich der Streckenschieber STS-1 nicht schließen lassen sollte.
Min = 10 s Max = 20 s	Der AT informiert den EL über das Leck in Q3 und dass GES-1 abgesperrt wurde.	
Min = 15 s Max = 25 s	Der EL informiert den SL über das Leck und dass GES-1 abgesperrt wurde.	
Min = 15 s Max = 30 s	Unmittelbar danach weist der SL den SLV an, Streckenschieber SLS-1 auf dem Gelände schließen zu lassen.	

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>Modellierung von HL 2.3 im Crew-Modul:</p> <pre> HL 2.3 // Diagnose in Warte liegt vor, bevor EL den Druckabfall in der Leitung feststellt Bed: & HLcont = 2.1 & SL <= EL /SL / EL / 40 70 // SL informiert EL über Alarm und die erstellte Diagnose / EL / AT / 45 60 // EL schickt AT in den Quadrant 3, der sich dorthin begibt / AT / -7 / 60 90 // AT findet Leck in der Nähe von GES-1 und erkennt Wassereintritt in Q3. / AT / -8 / 60 120 // AT schließt GES-1 und wartet bis GES-1 komplett zu ist / AT / EL / 10 20 // AT informiert EL über das Leck in Q3 / EL / SL / 15 25 // EL informiert SL /SL / SLV / 15 30 // SL weist SLV an Streckenschieber auf dem Gelände schließen zu lassen # </pre>	<p>HL 2.3 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 2.1 ist und • der SL die Diagnose in der Warte erstellt hat, bevor der EL den Druckabfall in der Leitung bemerkt, bevor (SL ≤ EL) ist. <p>Die aktuelle Zeit vom EL wird in HL 1.051 bzw. HL 1.052, die vom SL in HL 2.1 ermittelt.</p>

Tab. A. 12 Absperrung der Streckenschieber auf dem Gelände → Handlungsablauf für HL 3.0 (Fortsetzung von HL 2.2 bzw. HL 2.3)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
<p>Min = 75 s Max = 90 s</p> <p>Min = 8 s Max = 16 s</p> <p>Min = 15 s Max = 30 s</p> <p>Min = 120 s Max = 360 s</p>	<p>Handlungsablauf zu HL 3.0:</p> <p>Der SLV ruft am Sammelplatz der Feuerwehr vor der Zufahrt zum Kontrollbereich an. Dort steht der Gerätetrupp (GT) in Bereitschaft. Der SLV instruiert den ME, auf dem Freigelände den Streckenschieber STS-1 der Feuerlöschwasserleitung zu schließen. Der SLV lässt sich die Instruktion wiederholen, um zu kontrollieren, dass sie richtig verstanden worden ist.</p> <p>Parallel dazu weist der SL den RF an, den Zustand ZU des Gebäudeeintrittsschieber GES-1 zu kontrollieren und zu schließen, falls letzterer offen sein sollte.</p> <p>Der RF führt diese Anweisung aus und meldet den Vollzug.</p> <p>Der ME begibt sich vor Ort zum Streckenschieber STS-1 und begibt sich zum Ort, wo sich das erforderliche Werkzeug (Steckschlüssel) befindet. Dieser Aufbewahrungsort ist in der Nähe des zu schließenden Schiebers. An dieser Stelle wird die aleatorische Unsicherheit berücksichtigt, dass sich das erforderliche Werkzeug nicht am vorgesehenen Ort befindet. Die Wahrscheinlichkeit dazu wird mit 8.3 E-03 abgeschätzt.</p>	<p>Die Unterlassung oder fehlerhafte Ausführung der Aktionen des SLV, SL, RF und ME ist zu vernachlässigen, da die Aufmerksamkeit des Personals darauf konzentriert ist.</p> <p>Die ersatzweise Schließung zweier weiterer Streckenschieber in unmittelbarer Nähe (STS-2 und STS-3) wird als Vorgehen festgelegt, wenn der Streckenschieber STS-1 sich nicht schließen lassen sollte.</p> <p>Eine Annahme von Fehlern bei dieser Ausführung ist nicht plausibel, der erhaltenen Instruktion, da die Tätigkeit gut bekannt, die Lage der zu betätigten Komponente zur Schließung des Schiebers klar und das Vorgehen zur Schließung vertraut sind. Die Annahmen zu den Wahrscheinlichkeiten sind in Abschnitt 6.1.6 erläutert.</p>
	<p>Modellierung von HL 3.0 im Crew-Modul:</p> <pre data-bbox="416 1043 999 1276"> HL 3.0 // Aufsuchen des Streckenschiebers auf dem Gelände Bed: & HLcont >= 2.2 & HLcont <= 2.3 Bed: & HLcont = 1.3 /SLV/ ME / 75 90 // SLV ruft am Sammelplatz der FW an und instruiert ME Streckenschieber zu schließen /SL/ RF / 8 16 // SL weist RF an Zustand von GES-1 zu kontrollieren /RF / - / 15 30 // RF kontrolliert GES-1. /ME / - / 120 240 // ME begibt sich vor Ort zum STS-1 und geht zum Ort wo Werkzeug aufbewahrt wird /ME / b_Wrkz / 0 0 // Werkzeug am vorgesehenen Ort 1 - ja (p=0.9917) 2 - nein (p=8.3E-3) # </pre>	<p>HL 3.0 wird aktiviert, wenn</p> <ul style="list-style-type: none"> die vorhergehende Handlungsliste HL 2.2 oder HL 2.3 ist. <p>Mit der Verzweigungsvariablen b_Wrkzg wird die Unsicherheit berücksichtigt, ob das notwendige Werkzeug sich zum betreffenden Zeitpunkt am vorgesehenen Ort befindet oder nicht. Eine Erläuterung dazu ist in Abschnitt 6.1.6 zu finden.</p>

Tab. A. 13 Unsicherheit bzgl. des Werkzeugs vor Ort → Handlungsablauf für HL 4.1 bzw. HL 4.2 (Fortsetzung von HL 3.0)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
<p>Min = 10 s Max = 20 s</p> <p>Min = 15 s Max = 30 s</p>	<p>Handlungsablauf zu HL 4.1: ME nimmt Werkzeug am vorgesehenen Ort auf und begibt sich zur Abdeckung des Schiebers.</p> <p>Der ME öffnet Abdeckung mit Werkzeug. An dieser Stelle wird die Unsicherheit berücksichtigt, ob sich STS-1 schließen lässt oder nicht (siehe Abschnitt 6.1.7).</p>	<p>Das Werkzeug befindet sich am vorgesehenen Ort.</p> <p>Die Abdeckung ist normalerweise relativ schnell zu öffnen. Es kann jedoch passieren, dass die Öse der Abdeckung verdreht ist oder das Werkzeug etwas verbogen ist, wodurch das Öffnen etwas länger dauert.</p>
	<p>Modellierung von HL 4.1 im Crew-Modul:</p> <pre data-bbox="416 647 1171 834"> HL 4.1 // Wrkzg am Ort (p=0.9917) Bed: & HLcont = 3.0 & b_Wrkzg = 1 / ME / - / 10 20 // ME nimmt Werkzeug und geht zur Abdeckung des Schiebers / ME / - / 15 30 // ME öffnet Abdeckung mit Werkzeug / ME / b_relSchieber / 0 0 // Schieber lässt sich schließen 1 - ja (p=0.99) 2 - nein (p=0.01) # </pre>	<p>HL 4.1 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 3.0 ist und • sich das Werkzeug zum Schließen des Streckenschiebers am vorgesehenen Ort befindet (b_Wrkzg = 1).
<p>Min = 20 s Max = 45 s</p> <p>Min = 40 s Max = 150 s</p> <p>Min = 150 s Max = 300 s</p> <p>Min = 15 s Max = 30 s</p>	<p>Handlungsablauf zu HL 4.2: ME ruft bei Gerätetrupp (GT) an und fragt nach erforderlichem Werkzeug.</p> <p>Eine Person des GT besorgt das erforderliche Werkzeug.</p> <p>Eine Person des GT begibt sich zum Ort des Schiebers und übergibt dem ME das Werkzeug.</p> <p>Der ME öffnet Abdeckung mit Werkzeug. An dieser Stelle wird die Unsicherheit berücksichtigt, ob sich STS-1 schließen lässt oder nicht (siehe Abschnitt 6.1.7).</p>	<p>Das Werkzeug befindet sich nicht am vorgesehenen Ort. In dieser Zeitabschätzung wird berücksichtigt, dass ME im näheren Umfeld eine gewisse Zeit nach Werkzeug sucht.</p> <p>Bei der Zeitverteilung wird angenommen, dass die Besorgung des Werkzeugs etwas mehr Zeit in Anspruch nimmt, da es in der Gerätschaft erst gesucht werden muss.</p> <p>Die Wegstrecke kann etwas länger sein, wenn das Werkzeug an anderer Stelle besorgt werden muss.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
	<p>Modellierung von HL 4.2 im Crew-Modul:</p> <pre> HL 4.2 // Werkzeug nicht am Ort (p=8.3E-3) Bed: & HLcont= 3.0 & b_Wrkzg = 2 / ME / GT / 20 45 // ME ruft bei GT an und fragt nach erforderlichem Werkzeug / GT / - / 40 150 // Person des GT besorgt erforderliches Werkzeug / GT / ME / 150 300 // GT begibt sich zum Ort des Schiebers und übergibt Werkzeug / ME / - / 15 30 // ME öffnet Abdeckung mit Werkzeug / ME / b_reiSchieber / 0 0 // Schieber lässt sich schließen 1 - ja (p=0.99) 2 - nein (p=0.01) # </pre>	<p>HL 4.2 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 3.0 ist und • sich das Werkzeug zum Schließen des Streckenschiebers nicht am vorgesehenen Ort befindet (b_Wrkzg = 2).

Tab. A. 14 Unsicherheit, ob sich der Streckenschieber STS-1 schließen lässt → Handlungsablauf für HL 5.1 bzw. HL 5.2 (Fortsetzung von HL 4.1 bzw. HL 4.2)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
<p>Min = 15 s Max = 40 s</p> <p>Min = 20 s Max = 40 s</p> <p>Min = 15 s Max = 30 s</p>	<p>Handlungsablauf zu HL 5.1: Der ME schließt STS-1.</p> <p>ME ruft den SL in der Warte an und informiert ihn über die Absperrung von STS-1.</p> <p>Der SL informiert den EL am Brandort, dass STS-1 abgesperrt ist.</p>	<p>STS-1 lässt sich schließen. In der Zeitabschätzung wird berücksichtigt, dass das Schließen etwas schwergängig sein kann.</p>
	<p>Modellierung von HL 5.1 im Crew-Modul:</p> <pre data-bbox="421 783 1171 979"> HL 5.1 // Schieber lässt sich schließen (p=0.99) Bed: & HLcont >= 4.1 & HLcont <= 4.2 & b_relSchieber = 1 /ME /-9/ 15 40 // ME schließt den Schieber /ME /SL / 20 40 // ME ruft SL in Warte an und meldet Schließung des Schiebers /SL /EL / 15 30 // SL informiert EL, dass Streckenschieber zu # </pre>	<p>HL 5.1 wird aktiviert, wenn</p> <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 4.1 oder HL 4.2 ist und • sich der Streckenschieber STS-1 schließen lässt (b_relSchieber = 1).
<p>Min = 45 s Max = 120 s</p> <p>Min = 20 s Max = 40 s</p> <p>Min = 20 s Max = 40 s</p>	<p>Handlungsablauf zu HL 5.2: Der ME versucht eine gewisse Zeit vergeblich, den Schieber zu schließen.</p> <p>Der ME geht zum Ort der beiden Notschieber.</p> <p>Der ME öffnet die Abdeckung des 1. Notschiebers.</p>	<p>STS-1 lässt sich nicht schließen. Diese Zeit, in der ME versucht den Schieber zu schließen, kann mehr oder weniger Zeit in Anspruch nehmen. Der ME weiß, dass er nun die Notschieber STS-2 und STS-3 zu schließen hat.</p> <p>Die Notschieber befinden sich in der Nähe von STS-1. Es wird angenommen, dass sich die Notschieber auf jeden Fall schließen lassen.</p> <p>Wegen der räumlichen Nähe der Notschieber decken die Handlungszeiten auch die wenigen Schritte zwischen den Notschiebern ab.</p>

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 15 s Max = 40 s Min = 20 s Max = 40 s Min = 15 s Max = 40 s Min = 20 s Max = 40 s Min = 15 s Max = 30 s	/ ME / - / 15 40 // ME schließt 1. Notschieber. Der ME öffnet die Abdeckung des 2. Notschiebers. Der ME schließt den 2. Notschieber. Der ME ruft den SL in der Warte an und informiert ihn über die Absperrung von STS-1. Der SL informiert den EL am Brandort, dass STS-1 abgesperrt ist.	
	Modellierung von HL 5.2 im Crew-Modul: <div style="border: 1px solid black; padding: 5px;"> <pre> HL 5.2 // Schieber lässt sich nicht schließen (p=0.01) Bed: & HLcont >= 4.1 & HLcont <= 4.2 & b_relSchieber = 2 / ME / - / 45 120 // ME versucht gewisse Zeit vergeblich Schieber zu schließen / ME / - / 20 40 // ME geht zum Ort der beiden Notschieber / ME / - / 20 40 // ME öffnet Abdeckung des 1. Notschiebers / ME / - / 15 40 // ME schließt 1. Notschieber / ME / - / 20 40 // ME öffnet Abdeckung des 2. Notschiebers / ME / -10 / 15 40 // ME schließt 2. Notschieber / ME / SL / 20 40 // ME ruft SL in Warte an und meldet Schließung des Schiebers / SL / EL / 15 30 // SL informiert EL, dass Streckenschieber zu # </pre> </div>	HL 5.2 wird aktiviert, wenn <ul style="list-style-type: none"> • die vorhergehende Handlungsliste HL 4.1 oder HL 4.2 ist und • sich der Streckenschieber STS-1 nicht schließen lässt (b_relSchieber = 2).

Tab. A. 15 Fortführung der Brandlöschung → Handlungsablauf für HL 6 (Fortsetzung von HL 5.1 bzw. HL 5.2)

Zeitpunkt	Ereignis (E) / Personalhandlung (H)	Erläuterungen
Min = 300 s Max = 600 s	Handlungsablauf zu HL 6.0: EL, ST und AT setzen die Löschung des Brandes fort	Der Gebäudeeintrittsschieber GES-1 ist ZU. Der GES-2 geöffnet. Es wird Wasser in das Feuerlöschwassersystem gefördert und die Brandbekämpfung kann fortgesetzt werden.
Min = 20 s Max = 40 s	Der EL meldet dem SL die erfolgreiche Löschung des Brandes.	Der Brand erlischt. Ende der Notfallmaßnahme.
	Modellierung von HL 6.0 im Crew-Modul: <div style="border: 1px solid black; padding: 5px; display: inline-block;"> HL 6.0 // Brandlöschung Bed: & HLcont >= 5.1 & HLcont <= 5.2 / EL / -10 / 300 600 // Löschung des Brandes / EL / SL / 60 120 // EL meldet SL erfolgreiche Löschung des Brandes # </div> <div style="background-color: red; color: white; padding: 5px; display: inline-block; margin-left: 20px;"> HL -99 // Ende der Notfallmaßnahme Bed: & HLcont = 6.0 # </div>	HL 6.0 wird aktiviert, wenn <ul style="list-style-type: none"> die vorhergehende Handlungsliste HL 5.1 oder HL 5.2 ist.

**Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH**

Schwertnergasse 1
50667 Köln

Telefon +49 221 2068-0

Telefax +49 221 2068-888

Forschungszentrum
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