CARL VON OSSIETZKY universität OLDENBURG

Fakultät II - Informatik, Wirtschafts- und Rechtswissenschaften

Department für Informatik

Dissertation

Prozessgetriebene Risikoanalyse zur Bewertung maritimer Operationen

Dissertation zur Erlangung des Grades eines Doktors der Ingenieurwissenschaften

vorgelegt von

Jan Pinkowski

Gutachter:

Prof. Dr.-Ing. Axel Hahn
Prof. Dr. Martin Fränzle

Datum der Disputation:

11. September 2015

Zusammenfassung

Maritime Operationen wie beispielsweise Arbeiten an Offshore-Bauwerken stellen aufgrund der besonderen Witterungsbedingungen und Distanz zum Festland hohe Herausforderungen an beteiligte Personen, eingesetzte Techniken, Equipment und die Arbeitsabläufe dar. Dabei hat die Sicherheit der durchzuführenden Operation stets die höchste Priorität. Um somit vorab über mögliche Gefährdungen informiert zu sein, werden derartige Vorhaben zuvor geplant und im Hinblick auf mögliche Risiken eingeschätzt. Bestehende Problemstellungen sind jedoch, dass derzeit diese Planung überwiegend informell geschieht. Die dabei eingebrachten Informationen sind darüber hinaus kaum wiederverwendbar, erfordern ein hohes Maß an Erfahrungswissen und ermöglichen kaum eine formalisierte Risikoanalyse mit Berücksichtigung der zugrundeliegenden Arbeitsabläufe.

Um diesen Problemstellungen zu begegnen wurde in dieser Arbeit ein Ansatz zur systematischen und formalisierten Risikoanalyse mit Hilfe graphischer Prozessmodelle zur Planung der Abläufe und Ressourcen einer Operation entwickelt. Innerhalb des systematischen Vorgehens wird dieses Prozessmodell genutzt und um erforderliche Informationen wie beispielsweise Gefährdungen, mögliche Ursachen oder risikomindernde Maßnahmen erweitert. Dabei kann unterstützend eine entwickelte Wissensbasis zur Bereitstellung von Informationen vergangener Planungsvorgänge genutzt werden. Diese Informationen dienen zur Planung der Operation und formalisierten Risikoanalyse mit Hilfe von Fehlerbäumen, die in dem entwickelten Ansatz automatisch erstellt und ausgewertet werden.

Insgesamt wurde der Ansatz vollständig im Rahmen einer prototypischen Implementierung umgesetzt und ermöglicht somit eine durchgängige softwareseitige Unterstützung zur Planung und Analyse maritimer Operationen. Die Evaluierung des Ansatzes erfolgte sowohl qualitativ anhand von Fallbeispielen sowie auf Basis von Bewertungen maritimer Sicherheitsexperten.

Abstract

Due to especially rough weather conditions and large distances to shore, maritime operations represent major challenges for activities to be performed, involved people and used equipment whereas ensuring safety of the operation is the main priority. In order to estimate possible risks of such safety-critical operations, it is necessary to plan an operation beforehand to identify and assess possible hazards and causes. Today the planning of activities and related risks is typically performed informally whereas the specifications are neither reusable nor suitable for risk assessment and require extensive use of knowledge from experience.

In order to overcome these problems, this dissertation introduces an approach to perform a formalized risk analysis based on a graphical process model describing the activities and actors of the planned operation. The process model is thereby systematically enriched with information according to possible hazards and causes which is facilitated by integration of a knowledge base containing information of previously planned operations. Subsequently, this procedure enables to perform an automatic quantitative risk analysis using fault tree analysis whereas the before planned information of activities, hazards and causes are used to automatically construct and analyze fault trees.

The approach has been fully implemented and thereby enables a software-aided tool for planning maritime operations, which has been used for both qualitative and quantitative evaluation by means of case and user studies with maritime experts.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Maritime Operationen wie beispielsweise Arbeiten an Offshore-Bauwerken, sind echte Herausforderungen für die beteiligten Personen, da diese Arbeiten viel witterungsabhängiger sind als vergleichbare Tätigkeiten an Land [Sch09, S. 7]. Dabei hat die Sicherheit maritimer Operationen, in denen nicht nur bei Offshore-Bauwerken eine Vielzahl an Wasserfahrzeugen wie beispielsweise Schlepper, Pontons, Lastkrähne und auch Personen zum Einsatz kommen, höchste Priorität [Sch09, S. 7]. Wie jedoch bei vielen risikoreichen Vorhaben, bleiben auch maritime Operationen nicht vor Unfällen verschont. Unfälle maritimer Operationen unterliegen jedoch der Besonderheit, dass der wie an Land gewohnt direkte und schnelle Zugang zu Rettungsdiensten aufgrund der Distanz stark eingeschränkt ist, sodass im schlimmsten Fall nicht minuten- sondern stundenlang auf Hilfe gewartet werden muss [Lob12]. Zusätzlich erschweren unklare Zuständigkeiten und unterschiedliche Sicherheitskonzepte, die ohnehin durch raue See und Wind riskanten Rettungsmanöver [Lob12]. Demnach sind bereits vor Beginn der maritimen Operationen zunächst im Rahmen des Arbeitsschutzgesetzes Gefährdungsbeurteilungen auszuarbeiten, in denen systematisch mögliche Risiken identifiziert, analysiert und bewertet werden. Diese Dokumente sind ein notwendiger Bestandteil, damit maritime Operationen genehmigt und daraufhin ausgeführt werden können. Insbesondere frühe Phasen zur Konzeption einer maritimen Operation haben dabei das größte Potential Risiken zu eliminieren [Ren13, S. 56], sodass die geplante Operation möglichst ohne Vorfälle durchgeführt werden kann.

Ziel dieser Arbeit ist es einen Ansatz zu entwickeln, um maritime Sicherheitsexperten bei der Erstellung von Gefährdungsbeurteilungen und Durchführung formalisierter Risikoanalysen zu unterstützen, um die Qualität erstellter Gefährdungsbeurteilungen zu erhöhen und somit die Planung sicherer maritimer Operationen zu verbessern. Kapitel 1 führt somit genauer in die Thematik ein und motiviert daher zunächst in Abschnitt 1.1 die Bedeutung und die Herausforderungen. Abschnitt 1.2 geht daraufhin detaillierter auf aktuelle Problemstellungen bei der Erstellung von Gefährdungsbeurteilungen ein, woraufhin im Anschluss in Abschnitt 1.3 die Ziele und Beiträge dieser Ausarbeitung aufgeschlüsselt werden.

1.1 Motivation

Die maritime Branche bietet unter anderem im Rahmen des Ausbaus erneuerbarer Energien ein erhebliches Wachstumspotential [Deu11b, S. 1]. Bei Weiterentwicklungen in dieser Branche hat die Betrachtung von Arbeitsschutz und Schadensfällen sowie Abwehr von Gefahren und Notfallvorsorge eine wachsende Bedeutung [Deu11b, S. 1].

Die Betrachtung dieser Aspekte wird im Rahmen der Projektplanung- und Abwicklung vorgenommen, welche im Vergleich zu anderen Projektphasen als einer der größten Kostenfaktoren prognostiziert wird [Pri12]. Weiterhin sind Risikoeinschätzungen die bei der Projektplanung und -abwicklung vorgenommen werden, aufgrund der damit verbundenen Auswirkungen auf die Finanzierungskosten ein starker Einflussfaktor [Sti13, S. 78]. Durch verbesserte Risikoeinschätzungen und wachsender Erfahrungen können somit finanzielle Risikoaufschläge und Reserven für den Eintrittsfall von Risiken gesenkt werden [Sti13, S. 78]. Hierzu muss eine kontinuierliche Weiterentwicklung der Technik und eine deutlich geringere Fehleranfälligkeit entlang der gesamten Wertschöpfungskette erzielt werden [Sti13, S. 97]. Neben anderen werden Standardisierungen, ausreichende Erfahrungen und technische Weiterentwicklungen als notwendige Randbedingungen im Rahmen der Untersuchung von Kostensenkungspotentialen identifiziert [Sti13, S. 97].

Zum Abschluss der Planung maritimer Operationen werden unter anderem Dokumente wie Gefährdungsbeurteilungen erstellt, in denen im Rahmen von Risikoanalysen und Bewertungen unerwünschte Ereignisse prozessorientiert und somit im Hinblick auf die geplanten Arbeitsabläufe identifiziert und hinsichtlich Ausfallschwere und Häufigkeit eingeordnet werden [Bra02, S. 87]. Die Gefährdungsbeurteilungen selbst werden dabei schriftlich ausgearbeitet und stellen somit ein aufwändiges, kostspieliges jedoch gesetzlich vorgeschriebenes Unterfangen dar [Bunnt], [Küp12]. Traditionellerweise werden die in diesem Rahmen vorgenommenen Risikoanalysen und Bewertungen auf Basis von Expertenmeinungen und deren Erfahrungswissen durchgeführt, was zwar integrale Bestandteile sind, jedoch sollten Analysen und Bewertungen nicht ausschließlich darauf beruhen [Alt10, S. 22]. Dies gilt insbesondere im Hinblick auf die hohe Komplexität maritimer Umgebungen und damit einer Vielzahl an bei der Risikobewertung zu berücksichtigenden Inhalten, sodass derlei Vorhaben schnell ausufern können [Alt10, S. 22], [VdS14]. Darüber hinaus gibt es über die reine Dokumentation und Genehmigung vorgenommener Risikobewertungen im Rahmen von Gefährdungsbeurteilungen den Bedarf das erworbenen Erfahrungswissen sowie Erkenntnisse von Risikoanalysen strukturiert und wiederverwendbar bereitzuhalten, um dieses später zur Verfügung stellen zu können [VdS14, S. 3].

Klassische Ansätze zur Risikoanalyse sind, im Gegensatz zu den Ausführungen für maritime Operationen, nicht prozessorientiert, obwohl sich kritische Aspekte insbesondere auch aus der Zusammenwirkung von Arbeitsabläufen heraus ergeben können [Deu11b, S. 12]. Zusätzlich werden dabei im Gegensatz zum dargestellten Beispiel der maritimen Domäne, anstatt natürlichsprachlicher textueller Beschreibungen stärker Formalisierungen genutzt,

wodurch Risikoeinschätzungen durch entsprechende Analysen und Bewertungen verbessert werden. Da wie erwähnt eine verbesserte Risikoeinschätzung sowie wachsendes Erfahrungswissen diverse Kostensenkungspotentiale in der maritimen Domäne ermöglicht [Sti13, S. 78], stellt sich die Frage, inwiefern entsprechend formalisierte Ansätze zur Risikoanalyse, trotz der erforderlichen prozessorientierten Perspektive zur Beurteilung maritimer Operationen, eingesetzt werden können. Im Rahmen dieser Ausarbeitung wird daher untersucht, wie dennoch mit der prozessorientierten Perspektive eine formalisierte Risikoanalyse zur verbesserten Risikoeinschätzung eingesetzt werden kann. Darüber hinaus ist sowohl innerhalb des Beispiels der maritimen Domäne als auch im Rahmen von formalisierten Ansätzen, Erfahrungswissen notwendig. Ein weiterer Aspekt der Ausarbeitung ist daher, zusätzlich zur Problemstellung der prozessorientierten Perspektive, eine stärkere Verbindung der Aspekte der Formalisierung und der Wiederverwendbarkeit, um somit notwendige Zusammenhänge zur Unterstützung der Risikoanalyse nachvollziehbar und transparent abbilden zu können.

Daher werden im Rahmen dieser Ausarbeitung die genannten Herausforderungen mit einem Lösungsansatz angegangen. Dabei dient die Erstellung von Gefährdungsbeurteilungen für maritime Operationen als Anwendungsfall, indem dafür ein formalisierter Ansatz zur Risikoanalyse integriert in einen prozessorientierten Planungsansatz eingebracht wird. Für dieses Vorgehen wird darüber hinaus die Wiederverwendbarkeit dafür eingebrachter Informationen adressiert, sodass diese für spätere Anwendungen als Anhaltspunkt und Referenz bereitgestellt werden können. Diese Aspekte werden im Rahmen einer softwareseitigen Unterstützung eingebracht, damit mit diesem Ansatz durchgeführte Risikoanalysen für maritime Sicherheitsexperten und weitere beteiligte Personen transparent und nachvollziehbar anwendbar sind.

1.2 Problemstellung

Nachdem zuvor die Bedeutung der Betrachtung von Risiken für Projekte in der maritimen Domäne innerhalb der Motivation herausgestellt wurde, wird in diesem Abschnitt genauer auf die dabei vorherrschenden Problemstellungen eingegangen. Bei der Planung maritimer Operationen als wesentlicher Projektbestandteil sind Gefährdungsbeurteilungen im Rahmen von Schutz- und Sicherheitskonzepten beispielsweise innerhalb maritimer Bauvorhaben zu erstellen. Die Ausarbeitung dieser Dokumente ist gesetzlich vorgeschrieben und wird von maritimen Sicherheitsexperten im Planungsprozess aufwändig in schriftlicher Form erstellt [Bunnt], [Küp12]. Ein bedeutender Faktor um solche Gefährdungsbeurteilungen erstellen zu können, stellt das Erfahrungswissen des jeweiligen Sicherheitsexperten dar, der für die geplante Operation jeweils Gefahren, Folgen, Risiken und mehr identifizieren sowie abschätzen können muss [Alt10, S. 22]. Einige der bekannten Problemstellungen sind dabei, dass

- derzeit in der Branche zu wenig **Erfahrungswissen** vorhanden ist [VdS14],
- es für diese Arbeiten kaum **Formalisierungen** und Tools gibt [Vin07, S. 121]
- existierende verwandte formalisierte Ansätze kaum die erforderliche **prozessorientierte Perspektive** ermöglichen, obwohl eine enge Integration notwendig wäre, da sich kritische Aspekte insbesondere auch aus der Zusammenwirkung von Arbeitsabläufen heraus ergeben können [Deu11b, S. 12],
- derartige maritime Szenarien und Umgebungen eine hohe **Komplexität** und Vielzahl an zu berücksichtigenden Aspekten enthalten [Alt10, S. 22], [MSB09, S. 136]
- vorgenommene Gefährdungsbeurteilungen **transparent** gestaltet werden müssen, um das Schadensrisiko mindern zu können [VdS14, S. 3],
- der Wirkung von eingeplanten **Maßnahmen** hinsichtlich der Reduzierung des Risikos sowie der Relationen von Gefahren zu wenig Beachtung geschenkt wird [Man13, S. 252],
- bisher kein **Standard** existiert, sodass Schutz- und Sicherheitskonzepte in Umfang und Detaillgrad variieren und dadurch Einzel- und Individualprüfungen notwendig sind [Bun14a, S. 16].

Im Rahmen des notwendigen **Erfahrungswissens** ist zu nennen, dass die Branche zum Aufbau und Planung von Offshore-Projekten noch jung ist und somit aufgrund der komplexen Vorhaben bisher nur begrenzt Erfahrungswissen vorhanden ist [VdS14, S. 3]. Da die Branche jedoch starken Wachstumszielen unterliegt und noch viele Potentiale birgt ([VdS14, S. 3], [Bun14b], [MSB09, S. 135]), wird auch das Erfahrungswissen mit dem Verlauf weiterer geplanter und abgeschlossener Projekte anwachsen und dadurch die Qualität zukünftiger Vorhaben steigern. Ein weiterer Faktor, der diese Problemstellung zusätzlich belastet, ist, dass bis zum Jahr 2016 mit einem massiven Zuwachs an neuen Beschäftigten gerechnet wird [Pri12], welche möglicherweise wiederum dem Problem mangelnder Erfahrung unterliegen. Zwar wird ab 2016 ein geringerer Zuwachs der Beschäftigtenzahlen prognostiziert, jedoch liegt dieser bis 2021 weiterhin bei über 20% [Pri12], sodass die Problemstellung voraussichtlich weiter bestehen bleibt. Damit diese aufgelöst werden kann, muss eine Möglichkeit gefunden werden, über den Verlauf verschiedener Projekte und dem Zuwachs und Schwund von Mitarbeiterzahlen hinweg Erfahrungswissen aufzubauen und zum Vorteil für die Erstellung von Gefährdungsbeurteilungen und Planung nutzen zu können.

Im Gegensatz zum Einsatz von Techniken mit denen Informationen für die Beurteilung von Gefährdungen **formalisiert** und **transparent** ausgestaltet werden können, werden

für Gefährdungsbeurteilungen schriftliche Ausarbeitungen angefertigt, die für die Genehmigung der Schutz- und Sicherheitskonzepte genutzt werden. Dennoch werden trotz des hohen Umfangs und der **Komplexität** solcher Vorhaben, diese schriftlichen Ausarbeitungen zur Planung, Analyse und Bewertung genutzt [VdS14], wodurch diese begründeter weise aufgrund ihrer Vielzahl an Auslösern, Faktoren, Konsequenzen etc. im Rahmen einer hohen Zahl an Szenarien schnell ausufern können [Alt10, S. 22]. Diese schriftlichen Ausarbeitungen sind damit zwangsweise aufwändig und besonders im Fall von Änderungen, mit im Dokument verteilt vernetzten Informationen schwer handhabbar. Somit ist es nicht verwunderlich, dass Aspekte wie die Vernetzung von Informationen, wie beispielsweise eingebrachte **Maßnahmen** und Relationen dieser Informationen, zu wenig beachtet werden [Man13, S. 252]. Die fehlende Existenz von **Standards**, die entsprechende Vorgaben über die Form, Inhalt und Verfahrensweise für Gefährdungsbeurteilungen liefern könnte, trägt zudem einen weiteren Teil der genannten Problemstellungen bei, sodass letztendlich die notwendige Konsequenz ist, zu genehmigende Dokumente wie vorgelegte Schutz- und Sicherheitskonzepte Einzel- und Individualprüfungen zu unterziehen [Bun14a, S. 16].

Eine weitere Problemstellung ist, dass das Vorgehen zur Risikoanalyse und Bewertung eine **prozessorientierte Perspektive** zur Abschätzung der Sicherheit von Arbeitsabläufen erfordert. Klassische Techniken zur Risikoanalyse und Bewertung hingegen nehmen kaum diese prozessorientierte Perspektive ein. Zusätzlich nutzen diese, anstatt informeller textueller Beschreibungen, **formalisierte** Ansätze, die für die Risikoanalyse verwendet werden. Als eine solche Technik wird in dieser Ausarbeitung die Fehlerbaumanalyse genauer betrachtet, dessen manueller Einsatz jedoch komplex, zeit- und kostenaufwändig sowie fehleranfällig ist [CACO06], [LST09]. Der Einsatz dieser Technik fördert jedoch andererseits die Präzision und **Transparenz** möglicher Anwendungsfälle [Aul13, S. 24], [Vin07, S. 129], was einige der zuvor aufgeführten Problemstellungen unterstützen könnte. Zudem ist ein weitreichendes Verständnis des betrachteten Anwendungsfalls erforderlich, welches in Form von Fehlerbäumen strukturiert werden kann. Daher ist für die Anwendung einer solchen Technik Erfahrungswissen notwendig, um dieses gezielt einbringen zu können. Dabei hängt es vom jeweiligen Personal ab wie umfangreich das notwendige Wissen vorhanden ist. Eine Form zum übergreifenden Wissensaustausch ist, abgesehen von zu durchsuchenden Dokumenten oder im Gespräch beteiligter Personen, bei denen zusätzlich Problemstellungen wie implizites Wissen und Verständnisschwierigkeiten bestehen, kaum möglich. Um diesen Problemstellungen begegnen zu können, wird daher im Rahmen dieser Ausarbeitung ein Lösungsansatz entwickelt. Für diesen werden dafür zunächst nachfolgend Ziele definiert, die sich an den genannten Problemstellungen orientieren.

1.3 Zieldefinition und Beitrag der Arbeit

Nachdem in den vorangegangenen Abschnitten die Thematik dieser Ausarbeitung motiviert und die Problemstellungen sowohl aus der Anwendung als auch aus technischer Sicht heraus dargelegt wurden, erfolgt in diesem Abschnitt eine genauere Definition von Zielen und Beiträgen, die ein neuer Ansatz anhand der Problemstellungen adressieren sollte. Dabei dienen die identifizierten Problemstellungen und Herausforderungen als Grundlage für die Zieldefinition und Erarbeitung eines Lösungsansatzes sowie im Nachhinein zum Abgleich der Erreichung der gesetzten Ziele.

1.3.1 Zieldefinition

Nachdem im vorangegangenen Abschnitt die Problemstellung der Thematik erläutert wurde, erfolgt in diesem Abschnitt die Definition von Zielen für den zu entwickelnden Lösungsansatz.

Ziel 1 - Formalisierung des Basiswissens Natürlichsprachlich, textuell erfasstes Wissen wie im bisherigen Vorgehen prozessorientierter Anwendungsfälle wie maritime Operationen, kann nur begrenzt maschinenverarbeitbar für Risikoanalysen oder zur Wiederverwendung genutzt werden [ERS10]. Weiterhin ist eine strukturiertere, formalisiertere Form des Wissens erforderlich, um dieses entsprechend verarbeitbar, nachvollziehbar und wiederverwendbar nutzen zu können [ERS10], [Mod06]. Ein neuer Ansatz der im Rahmen dieser Ausarbeitung zu entwickeln ist, soll daher das erforderliche Basiswissen zur prozessorientierten Risikoanalyse sowie zur Wiederverwendung einheitlich formalisieren können.

Ziel 2 - Prozessorientierte Risikobetrachtung Im Rahmen vieler Anwendungsfälle stehen technische Aspekte im Fokus möglicher Risikoanalysen, wohingegen bei der Betrachtung von Abläufen die Arbeitsschritte mit möglichen Ursachen von Gefährdungen und involvierte Personen zu betrachten sind [MKH04]. Eine prozessorientierte Perspektive ist zusätzlich erforderlich, da sich Gefährdungen insbesondere auch durch die Gestaltung der Abläufe und derer Zusammenwirkung heraus ergeben können [Deu11b, S. 12]. Mit Hilfe einer derartigen Perspektive können dann einzelne Tätigkeiten, Bearbeitungsfolgen und involvierte Personen untersucht sowie relevante Gefährdungen identifiziert und Schutzmaßnahmen festgelegt werden [GA12]. Eine prozessorientierte Perspektive für einen Ansatz zur Risikoanalyse soll daher im Rahmen dieser Zieldefinition fokussiert werden, um die genannten Aspekte adäquat mit einbeziehen zu können.

Ziel 3 - Wiederverwendbare Informationen Der initiale Aufwand bei der Durchführung einer formalisierten Risikoanalyse ist zunächst in Bezug auf Zeit und Kosten hoch [CACO06], [LST09]. Dabei werden die jeweils notwendigen Informationen des betrachteten

Anwendungsfalls identifiziert und strukturiert, um im Rahmen der Risikoanalyse darauf aufbauende Ergebnisse zu ermitteln. Bei diesem Vorgehen ist somit zudem Erfahrungswissen notwendig, was mit jedem weiteren Anwendungsfall wächst [MEP+05], [DD08]. Eine Verbesserung der Wiederverwendbarkeit von eingebrachten Informationen über das Erfahrungswissen der beteiligten Personen hinaus, kann somit bei zukünftigen Anwendungsfällen zusätzlich unterstützen, sodass sich dadurch Kosten und Aufwand reduzieren lässt [GLS10]. Ein weiteres Ziel des auszuarbeitenden Ansatzes ist daher, eine Wiederverwendung von vorgenommenen prozessorientierten Risikoanalysen zu ermöglichen und dadurch eingebrachtes Wissen für zukünftige Anwendungsfälle bereitstellen zu können.

Ziel 4 - Unterstützende formalisierte Risikoanalyse Die manuelle Durchführung einer formalisierten Risikoanalyse wie der Fehlerbaumanalyse ist zeit- und kostenaufwändig [CACO06], [LST09]. Zusätzlich müssen im Rahmen komplexer Anwendungsfälle eine Vielzahl unterschiedlicher Aspekte berücksichtigt werden können [Alt10, S. 22]. Eine automatisierte Risikoanalyse soll als Ziel eines Lösungsansatzes dieser Ausarbeitung somit das Vorgehen der Risikoanalyse unterstützen und Orientierungshilfen zur Durchführung bieten, sodass mit entsprechend dokumentierten Ergebnissen eine effiziente Überprüfung von Designalternativen ermöglicht werden kann.

Ziel 5 - Berücksichtigung risikomindernder Maßnahmen Im Rahmen von Risikoanalysen werden Gefährdungen ermittelt und von Sicherheitsexperten eingeschätzt. Bei diesem Vorgehen werden risikomindernde Maßnahmen eingebunden, um dadurch die Einschätzung des Risikos verbessern zu können. Wenig Beachtung wird jedoch dabei der Wirkung der eingeplanten Maßnahmen in Bezug auf die Reduzierung des Risikos geschenkt [Man13, S. 252]. Demnach werden bei der Erarbeitung eines Lösungsansatzes in dieser Ausarbeitung explizit risikomindernde Maßnahmen innerhalb der Risikoanalyse mit berücksichtigt, um deren Effekt gezielt aufschlüsseln zu können.

Ziel 6 - Softwareseitige Unterstützung Damit in das Vorgehen eingebrachte Daten transparent Verknüpft, effektiv aktualisiert sowie die Dokumentation vereinfacht und die Fehleranfälligkeit reduziert werden kann, ist eine softwareseitige Unterstützung notwendig [Vin07, S. 139]. Zur weiteren Effizienz des Vorgehens nach den vorangegangenen Zieldefinitionen ist zusätzlich eine entsprechend durchgängige Unterstützung erforderlich. Innerhalb derer muss ein systematisches Vorgehen ermöglicht werden, in dem Daten transferiert und transparent verwendet werden können.

1.3.2 Beitrag

Die wissenschaftliche Wertschöpfung des hier vorzustellenden Ansatzes wird zusammengefasst als:

„Entwicklung eines Ansatzes zur formalisierten Risikoanalyse einer prozessorientierten Planung, unterstützt durch wiederverwendbare Informationen und Möglichkeit zur automatisierten Analyse“

Im Rahmen dieser Wertschöpfung erbringt diese Ausarbeitung die folgenden Beiträge:

1. **Integrierte Betrachtung von Informationen der Risikoanalyse und prozessorientierten Planung.** Die Risikoanalyse wird als fester Bestandteil der Ablaufplanung von Prozessen am Beispiel maritimer Operationen betrachtet. Dabei wird diese nicht als separates Vorgehen, sondern vielmehr integriert betrachtet, sodass Informationen die in vorangegangenen Planungsschritten ermittelt wurden, auch für die Risikoanalyse weiterer Anwendungen bereitgestellt werden. Diese Informationen werden miteinander vernetzt und in Zusammenhang gebracht, sodass unter anderem Beziehungen von Gefährdungen, Ursachen mit zugrundeliegenden Arbeitsabläufen, risikomindernder Maßnahmen sowie deren Zusammenhang gezielter geplant und analysiert werden können. Weiterhin soll dieses Vorgehen den Anwender unterstützen, sodass Ergebnisse auch mit stärkerer Vernetzung für die Bewertung durch den Anwender übersichtlich, transparent und nachvollziehbar dokumentiert werden können.

2. **Entwicklung eines Ansatzes zur unterstützenden Risikoanalyse.** Mit Hilfe der stärkeren Vernetzung von Informationen, die bei der Ablaufplanung zusammengetragen werden, wird eine formalere, automatisierte Risikoanalyse zur Unterstützung des Vorgehens ermöglicht. Dafür werden Planungsinformationen in Form von Prozessmodellen verwendet, um auf Basis dieser Informationen eine formalisierte Risikoanalyse mit Hilfe von Fehlerbäumen automatisiert durchführen zu können sowie Orientierungshilfen zur Strukturierung der Informationen zu bieten. Als Methode wird dabei die Fehlerbaumanalyse verwendet, in der Fehlerbäume mit Hilfe der Planungsinformationen automatisiert erstellt werden.

3. **Unterstützung der Planung durch Bereitstellung historischer Informationen.** Nachdem eine Planung und Analyse vorgenommen wurde, liegt das darin erworbene und dokumentierte Wissen in Form von Erfahrung des jeweiligen Sicherheitsexperten vor. Aufgrund wiederkehrender und ähnlicher Anwendungsfälle ist dieses Erfahrungswissen für zukünftige Anwendungsfälle nützlich und muss somit abrufbar sein. Ein Beitrag dieser Arbeit ist eine verbesserte, formalisierte Unterstützung zur Wiederverwendbarkeit von Planungsinformationen vergangener Anwendungsfälle. Dabei werden Informationen vergangener Risikoanalysen, wie Gefährdungen, Ursachen und deren Zusammenwirken sowie die vergangenen Wertezuordnungen über Eintritts- und Schadensstufen bereitgestellt und dienen somit als Anhaltspunkt für die Planung zukünftiger Anwendungsfälle.

1.4 Struktur der Arbeit und Methodik

Die vorliegende Ausarbeitung wurde in sechs Kapitel mit entsprechenden Unterkapiteln in Anlehnung an ein typisches ingenieurmäßiges Vorgehen wie in Abbildung 1.1 schematisch dargestellt strukturiert. Dabei hat sich das erste Kapitel der Einleitung, beginnend mit einer Motivation und Problemstellung der Thematik sowie mit der Herausstellung der Ziele und Beiträge dieser Arbeit, gewidmet.

Nachfolgend zu dieser Einleitung, wird in Kapitel 2 der Stand der Wissenschaft und Technik dargelegt, sodass ein Überblick über die aktuelle Situation bei der Planung und Gefährdungsbeurteilung in der maritimen Domäne gegeben wird. Darin enthalten ist die derzeitige Ausgangssituation sowie Ausführungen zum derzeitigen Stand in Bezug auf Schutz- und Sicherheitskonzepte, die bei der Planung maritimer Operationen ausgearbeitet werden. Darüber hinaus werden aufgrund bestehender Problemstellungen, Techniken zur formalisierten und systematischen Risikoanalyse, die verwandten Arbeiten in Bezug auf automatisierte Risikoanalysen sowie Möglichkeiten zur Wiederverwendbarkeit erläutert, woraufhin das Kapitel 2 mit einer Zusammenfassung und der Identifikation des Handlungsbedarfs abschließt. Im Anschluss an den Stand der Technik folgt daraufhin der eigene Ansatz in Kapitel 3, in welchem zunächst im Hinblick auf den zuvor identifizierten Handlungsbedarf

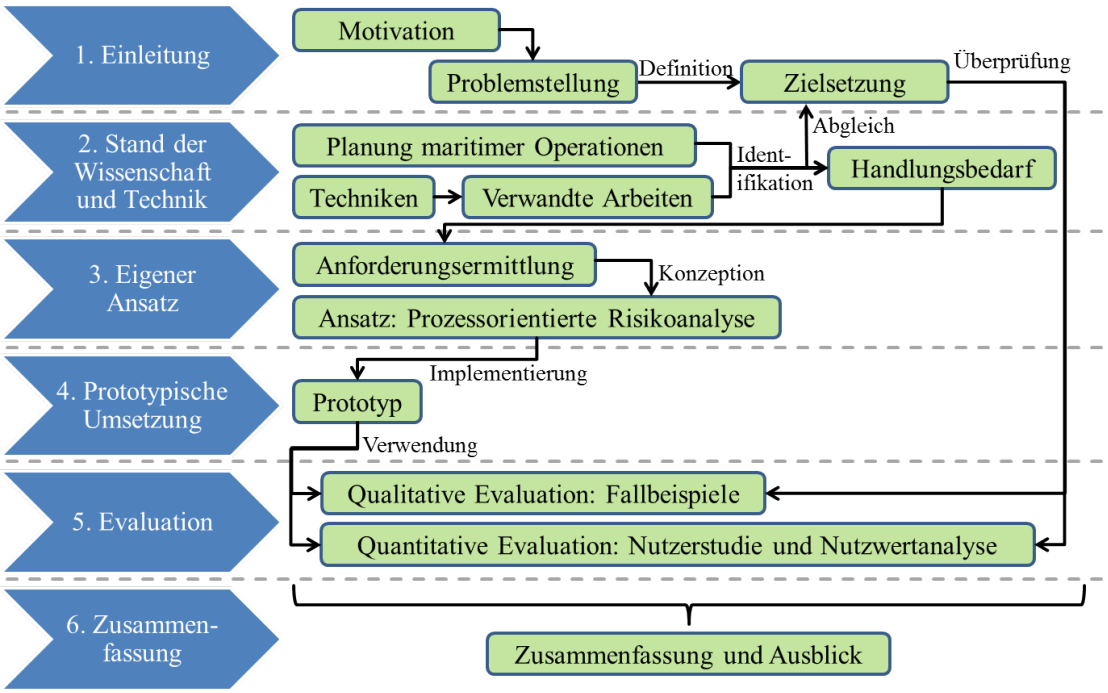

Abbildung 1.1: Schematischer Aufbau der Ausarbeitung

die Anforderungslage für eine Lösungsidee erarbeitet wird. Im übrigen Kapitel wird der eigene Lösungsansatz der prozessorientierten Risikoanalyse im Hinblick auf die ermittelten Anforderungen konzipiert und anhand eines schrittweisen Vorgehens anhand der Schritte Systemdefinition, Gefahrenidentifikation, Risikoanalyse und Risikobewertung erläutert. Anschließend wird in Kapitel 4 die prototypische Umsetzung des Ansatzes und der dabei anhand des zuvor konzipierten Ansatzes implementierte Prototyp beschrieben. Auf Basis der erfolgten prototypischen Umsetzung erfolgt in Kapitel 5 die Evaluation des Ansatzes, welche sich in einen qualitativen und einen quantitativen Teil gliedert. Im Rahmen der qualitativen Evaluation wurden zwei Fallbeispiele ausgewählt, anhand derer die Machbarkeit und praktische Anwendung des Ansatzes demonstriert wird. Zur ergänzenden quantitativen Evaluation wurde eine Nutzerstudie durchgeführt sowie mit Hilfe maritimer Sicherheitsexperten, Daten für eine Nutzerwertanalyse des Ansatzes erhoben und ausgewertet, sodass mit beiden Evaluationsszenarien eine Gegenüberstellung des bisherigen Vorgehens, wie in Kapitel 2 beschrieben, mit dem in dieser Ausarbeitung entwickelten Ansatz ermöglicht wird. Die Ausarbeitung schließt daraufhin in Kapitel 6 mit einer Zusammenfassung sowie einem Ausblick ab.

Kapitel 2

Stand der Wissenschaft und Technik

Mit diesem Kapitel soll ein Überblick über den Stand der Wissenschaft und Technik zum Verständnis und zur späteren Ausarbeitung eines eigenen Lösungsansatzes im Rahmen dieser Ausarbeitung aufgezeigt werden. Dabei umfasst das Kapitel die im Folgenden aufgelisteten Themengebiete und stellt diese jeweils im Rahmen einer Zusammenfassung und Diskussion den zuvor dargelegten Zieldefinitionen dieser Ausarbeitung gegenüber.

- Planung und Gefährdungsbeurteilung maritimer Operationen: Da mit dieser Ausarbeitung die Risikoanalyse und Bewertung maritimer Operationen fokussiert wird, wird im Rahmen des Abschnitts 2.1 in den aktuellen Stand der maritimen Domäne eingeführt und das derzeitige Vorgehen zur Risikoanalyse und Bewertung innerhalb von Gefährdungsbeurteilungen aufgezeigt. Dabei wird sowohl das klassische Vorgehen erläutert sowie auch mögliche Unterstützung durch Software dargestellt und im Rahmen der Zieldefinitionen bewertet.

- Techniken: Auch wenn diese nach dem Abschnitt 2.1 zur Risikobewertung in der maritimen Domäne zufolge kaum für die Gefährdungsbeurteilung verwendet werden, existieren Techniken zur formalisierten und systematischen Risikoanalyse die übergreifend in verschiedenen Domänen etabliert sind. Diese werden in Abschnitt 2.2 aufgeführt und erläutert sowie wiederum im Rahmen der Zieldefinitionen hin bewertet.

- Automatisierte Risikoanalyse: Da die zuvor eingeführten Techniken manuellen Aufwand erfordern, werden als verwandte Arbeiten in Abschnitt 2.3.1 Ansätze dargestellt, die mit Hilfe der Fehlerbaumanalyse eine automatisierte Risikoanalyse zur Reduzierung des Aufwands sowie der Komplexität und Fehleranfälligkeit adressieren.

- Wiederverwendbarkeit von Analysen und Bewertungen: Über den reinen Aufwand hinaus erfordert der Einsatz einer Technik zur Risikoanalyse zusätzlich Erfahrungs-

wissen hinsichtlich des betrachteten Anwendungsfalls. Innerhalb des Abschnitts 2.3.2 werden daher Ansätze aufgezeigt, die dieses Erfahrungswissen nicht nur dem menschlichen Nutzer überlassen, sondern dieses vielmehr unterstützend speichern und bereitstellen, um den initialen Aufwand für zukünftige Anwendungsfälle zu reduzieren.

Im Anschluss an die Ausführungen der vier Themengebiete, werden die dort aufgezeigten Inhalte genutzt, um den Handlungsbedarf, der in dieser Ausarbeitung entsprechend adressiert wird, darzustellen. Dafür erfolgt zum Schluss des Kapitels eine Zusammenfassung und Auflistung des Handlungsbedarfs, welcher im darauffolgenden Kapitel 3 zur Ermittlung von Anforderungen und nachfolgend für die Ausarbeitung eines eigenen Lösungsansatzes verwendet wird.

2.1 Planung und Gefährdungsbeurteilung maritimer Operationen

Dieser Abschnitt behandelt die anwendungsspezifischen Grundlagen der Risikobewertung in der maritimen Domäne und beginnt daher damit, die aktuelle Ausgangssituation zu erfassen und darzustellen. Anschließend wird genauer aufgeführt was unter einem Schutz- und Sicherheitskonzept zu verstehen ist und die erforderlichen Inhalte sowie das Vorgehen zur Erstellung von Gefährdungsbeurteilungen als wesentlicher Bestandteil dessen erläutert. Abschließend wird eine Auswahl an Softwarewerkzeugen erläutert, die bei der Erstellung von Gefährdungsbeurteilung unterstützen sollen. Diese werden am Ende des Abschnitts den Zieldefinitionen dieser Ausarbeitung gegenübergestellt.

2.1.1 Ausgangssituation

Die Bedeutung von Seegebieten im Rahmen wirtschaftlicher Investitionen und Projekten ist in den letzten Jahrzehnten stark gewachsen und zu einem profitablen und vielschichtigen Markt geworden. Dabei ist eine Vielzahl von Anwendungsmöglichkeiten entstanden in denen unterschiedliche Arbeiten auf See stattfinden. Am Beispiel der Offshore-Windindustrie ist zu erkennen, dass bis heute zahlreiche Unternehmen aus verschiedenen Industrie- und Dienstleistungszweigen bereits tätig geworden sind und der Bereich weiterhin erhebliche Wachstumspotentiale für die Zukunft bietet [MSB09, S. 135], [Bun14b]. Unter „Offshore“ versteht man den Bereich im Meer, wobei rechtlich differenziert werden muss, ob es sich um das Küstenmeer (bis zwölf Seemeilen; Hoheitsgebiet im Zuständigkeitsbereich des jeweiligen Bundeslands) oder um die Ausschließliche Wirtschaftszone (AWZ; bis 200 Seemeilen und kein Hoheitsgebiet, sondern internationales Gewässer) handelt [Bun14a, S. 6]. Im Zuge dessen ist auch das Bedürfnis nach Schutz- und Sicherheitskonzepten für Arbeiten in dem Bereich gewachsen [Sch13], [Mul06], [Bra02]. Hierbei gibt es verschiedene Aspekte, die zum einen die Sicherheit beteiligter Personen sowie technische und finanzielle Risiken

beeinflussen [Böt13], zum anderen aber auch eine gesteigerte Komplexität von Prozeduren hinsichtlich höherer Aufwände und Kosten für die Planung, Errichtung, Infrastruktur, Wartung sowie Rettungsmaßnahmen zur Folge haben [Lob12], [Böt13].

Demnach ist es in Deutschland inzwischen verpflichtend, maritime Vorhaben wie den Aufbau von Offshore Windenergieanlagen (OWEA) zu planen und dabei eine Risikobewertung durchzuführen und diese in Form einer Dokumentation für eine Genehmigung zur Verfügung zu stellen, wie beispielsweise in Form von Gefährdungsbeurteilungen wie den sogenannten HSE-Plänen (Health, Safety, Environment) [Tho12]. Inhaltlich bestehen HSE-Pläne aus der Beschreibung von Maßnahmen zur Erreichung von Gesundheits- (engl. Health), Arbeitssicherheit- (engl. Safety) und Umweltaspekten (engl. Environment) [E a94]. Die genehmigende Behörde solcher Vorhaben ist für deutsche Küstengewässer das Bundesamt für Seeschifffahrt und Hydrographie (BSH).

Im europäischen sowie auch internationalen Umfeld sind in diesem Bereich in den letzten Jahren vermehrt Anforderungen für Arbeitssicherheit bei Offshore-Vorhaben entwickelt worden, beispielsweise in Deutschland [Deu11a] oder Großbritannien [Ren10], [Ren13]. Im Jahr 2014 wurde vom BMVI (Bundesministerium für Verkehr und digitale Infrastruktur) das Offshore-Windenergie-Sicherheitsrahmenkonzept (OWE-SRK) [Bun14a] herausgegeben. Dieses dient seitdem für Vorhaben in deutschen Küstengewässern als etablierte Vorgabe und Richtlinie. In diesem gelten folgende Hinweise in Bezug auf ein Schutz- und Sicherheitskonzept:

*In einem **Schutz- und Sicherheitskonzept** soll der Betreiber unter anderem präventive und schadenminimierende Maßnahmen im Zusammenhang mit dem Betrieb des OWP darstellen [Bun14a, S. 22]. Das Schutz- und Sicherheitskonzept wird vom BSH unter Hinzuziehung von Fachexpertise der WSV sowie der Landesarbeitsschutzbehörden geprüft und bedarf der schriftlichen Zustimmung durch die zuständigen Stellen [Bun14a, S. 22].*

Neben allen Präventivmaßnahmen müssen die Anforderungen und Verantwortlichkeiten für den Notfall geklärt werden. Es müssen Szenarien entworfen und Reaktionsmöglichkeiten entwickelt und bewertet werden. Die Rollen und Aufgaben der Beteiligten sind zu definieren. Hierfür müssen die Betreiber der OWP eigene Schutz- und Sicherheitskonzepte vorhalten, die die Arbeits- und Betriebssicherheit ihrer eigenen Anlage sicherstellen [Bun14a, S. 7]. Dieses Konzept und seine Bausteine werden jährlich auf ggf. bestehenden Anpassungsbedarf überprüft, denn sich verändernde Gegebenheiten und neue Herausforderungen erfordern ein flexibles und anpassungsfähiges Instrumentarium [Bun14a, S. 8]. Der in diesem Rahmen vom BSH in Kooperation mit den Klassifikationsgesellschaften Det Norske Veritas (DNV) und Germanischer Lloyd (GL) entwickelte Standard für Konstruktive Ausführung von OWEA [B$^+$07] dient der Rechts- und Planungssicherheit bei der Entwicklung, Konstruktion, Ausführung, dem Betrieb und Rückbau von OWP im Gel-

tungsbereich der Seeanlagenverordnung (SeeAnlV) [B+07]. Im Fokus dieser Ausarbeitung steht das erforderliche Schutz- und Sicherheitskonzept, weshalb dieses in den nachfolgenden Unterabschnitten ausführlicher erläutert wird. Maritime Operationen sind im Hinblick darauf jeweils vom Schutz- und Sicherheitskonzept betroffen und somit der wesentliche Bestandteil bei der, wie im Schutz- und Sicherheitskonzept notwendigen, Betrachtung der Arbeitssicherheit beispielsweise wie im Rahmen maritimer Bauvorhaben.

2.1.2 Schutz- und Sicherheitskonzept

Dieser Abschnitt umfasst die Beschreibung des für die Genehmigung maritimer Operationen notwendigen Schutz- und Sicherheitskonzepts, welches vor Errichtung der ersten Anlage mit einem projektspezifischen Notfallplan bei der Genehmigungsbehörde einzureichen ist [B+07]. Derzeit variieren Schutz- und Sicherheitskonzepte hinsichtlich ihres Umfangs und Detaillierungsgrades [Bun14a, S. 16]. Ein Standard mit entsprechenden Vorgaben existiert derzeit noch nicht, so dass zusätzlich Einzel- und Individualprüfungen dieser Konzepte notwendig sind [Bun14a, S. 16]. Dennoch lässt sich die Arbeits- und Betriebssicherheit als ein wesentlicher Bestandteil dieser Konzepte ableiten [Bun14a]. Innerhalb dieser Ausarbeitung wird der Aspekt der Arbeits- und Betriebssicherheit als Bestandteil des Schutz- und Sicherheitskonzepts fokussiert, in welchem die Arbeitssicherheit in verschiedenen Phasen gewährleistet werden soll [Bun0a], [Bun4f]. Als übergeordnetes Ziel wird im Schutz- und Sicherheitskonzepts der Schutz des menschlichen Lebens und der Gesundheit sowie die Verkehrssicherheit betrachtet [Sch13], [Bun0a]. Nachfolgend werden mit diesem Fokus die inhaltlichen Aspekte des Arbeits- und Betriebssicherheitsanteils aus dem Schutz- und Sicherheitskonzept sowie das Vorgehen genauer erläutert.

Inhalt

Die ständige Genehmigungspraxis für Offshore-Windparkvorhaben in der deutschen ausschließlichen Wirtschaftszone (AWZ) beinhaltet die verbindliche Regelung, dass der Betreiber der Anlage vor Inbetriebnahme des Vorhabens, der Genehmigungsbehörde ein Schutz- und Sicherheitskonzept (SchuSiKo) mit einer projektspezifischen Notfallplanung vorzulegen hat [Pet14]. Darüber hinaus ist das Schutz- und Sicherheitskonzept Bestandteil der Anlagengenehmigung und soll durch Festlegung organisatorischer und technischer Verfahren und Maßnahmen dazu beitragen, die Sicherheit innerhalb und im Umfeld der Anlagen zu gewährleisten, wobei im Vordergrund der Schutz des menschlichen Lebens und der menschlichen Gesundheit sowie die Verkehrssicherheit stehen [Pet14]. Die inhaltlichen Vorgaben dieser notwendigen Schritte für Vorhaben in der deutschen AWZ richten sich dabei nach dem deutschen Arbeitsschutzgesetz (ArbSchG). In diesem wird in §5 Abs. 1 gefordert, „Der Arbeitgeber hat durch eine Beurteilung, der für die Beschäftigten mit ihrer Arbeit verbundenen Gefährdungen, zu ermitteln welche Maßnahmen des Arbeitsschutzes erforder-

lich sind“ [Pet14], [Jur4b]. Diese Gefährdungsbeurteilung bildet im Konzept einer systematischen Prävention die Grundlage für einen wirksamen betrieblichen Arbeitsschutz zur Verhütung von Unfällen bei der Arbeit und arbeitsbedingten Gesundheitsgefahren [Kir04, S. 14]. Demnach sind darin Risiken der auszuübenden Tätigkeiten zu bewerten (Risikobewertung), um die Gefährdung der Beschäftigten bei ihrer Arbeit beurteilen zu können. Das übergreifende Ziel dieser Risikobewertung ist nach [Ren13, S. 56] sicherzustellen, dass alle halbwegs vorhersehbaren Risiken adäquat bewertet wurden. Dabei wird die Risikobewertung als projektbegleitender Prozess über den gesamten Projektlebenszyklus hinweg aufgefasst [Ren13]. Frühe Projektphasen eignen sich dabei in besonderer Weise für die Risikobewertung, da diese das größte Potential haben Risiken eliminieren zu können [Ren13]. Diese bei Risikobewertung vorgenommenen Betrachtungen, Ergebnisse sowie zugrundeliegende Informationen, werden zur Dokumentation im Rahmen der Gefährdungsbeurteilung meist in tabellarischer Form niedergeschrieben. In der Praxis variiert der Detailgrad und Umfang dieser Dokumentation sowie auch die Form, da es diesbezüglich keine konkreten Vorgaben gibt wie diese auszugestalten sind [Bun14a, S. 16]. Gemeinhin werden jedoch identifizierte Gefährdungen einer geplanten Operation zeilenweise aufgeführt und hinsichtlich ihrer Eintritts- sowie Schadensklassifikation eingestuft. Auf Basis dieser Einstufung wird der tatsächliche Risikowert ermittelt sowie anschließend risikomindernde Maßnahmen bestimmt, um die Eintritts- oder Schadensklasse und damit letztendlich den Risikowert zu reduzieren. Ausgewählte risikomindernde Maßnahmen können, wie in Abbildung 2.1 schematisch dargestellt, dabei jeweils auf die Häufigkeits- sowie Schadensklasse wirken, um den Risikowert zu verringern. Diese Maßnahmen werden wiederum textuell in die zeilenweise Dokumentation eingegliedert, woraufhin eine erneute Einstufung hinsichtlich Eintritts- und Schadensklassifikation vorgenommen und daraufhin der Risikowert unter Berücksichtigung der zuvor gelisteten risikomindernden Maßnahmen erneut bestimmt wird. Im Anhang wird in Abbildung 6.1 eine beispielhafte Tabellenstruktur zur Dokumentation einer Gefahrenbewertung, jedoch ohne die beschriebenen Quantifizierungen von Schadensschwere- oder

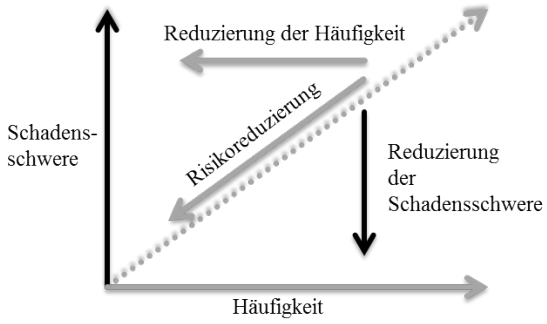

Abbildung 2.1: Risikomindernde Maßnahmen im Risikodiagramm (nach [Bra02])

Häufigkeitsstufen, dargestellt. Wie jedoch bereits erläutert, können die Form sowie auch der Detailgrad dieser Struktur variieren, sodass unterschiedliche Organisationen für diese Struktur verschiedene Vorlagen nutzen. Auch können die Anforderungen der Auftraggeber hinsichtlich verschiedener Anwendungsfälle variieren, sodass demnach eine detailliertere Struktur notwendig ist. Gespräche mit Organisationen die derartige Gefahrenbeurteilungen erstellen, haben ergeben, dass für diese Dokumentation überwiegend interne Vorlagen existieren, die mit Hilfe von Werkzeugen zur Text- bzw. Tabellenverarbeitung, wie Microsoft Word und Excel, individuell ausgefüllt und für das Genehmigungsverfahren weitergereicht werden. Zusätzlich zu der im Anhang in Abbildung 6.1 dargestellten Struktur, können andere Vorlagen abweichen, sodass bspw. eine Verbindung zu möglichen Tätigkeiten oder Operationen über zusätzliche Spalten hergestellt wird.

Ein zusätzliches Hilfsmittel stellt die sogenannte Risikomatrix dar, um Gefährdungen innerhalb von Gefährdungsbeurteilungen durch einen Risikowert, basierend auf Werten zur Einordnung der Schadens- und Häufigkeitsklasse, zu quantifizieren. Durch die Zuordnung von Schadens- und Häufigkeitsklassen, ist mit dieser zweidimensionalen Matrix eine grundsätzliche Einordnung in akzeptable und nicht-akzeptable Regionen hinsichtlich des quantifizierten und berechneten Risikowertes möglich, der zusätzlich innerhalb der Matrix farblich in entsprechende Regionen eingeteilt wird. Eine beispielhafte 5x5 Matrix ist in Abbildung 2.2 dargestellt.

		Schadensklasse				
		1	2	3	4	5
Häufigkeits-klasse	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Abbildung 2.2: Beispiel einer 5x5 Risikomatrix

Für eine unterschiedliche Differenzierung der Betrachtungen sind verschiedene Ausprägungen der Risikomatrix möglich, wie beispielsweise 3x3, 4x4, 7x7 etc. Innerhalb dieser existieren jedoch stets qualitative Abstufungen der Häufigkeits- und Schadensklassen, wie beispielsweise „unbedeutend“ bis „katastrophal“ als Schadensklassen (S), „häufig“ bis „äußerst selten“ als Häufigkeitsklassen (H) [Bra02]. Mit Hilfe dieser Zuordnungen können kritische Ereignisse qualitativ eingeordnet werden, um zwischen akzeptablen und nicht-akzeptablen Ereignissen unterscheiden zu können. Für diese Zuordnung wird, entsprechend Abbildung 2.2, der Risikowert ($R = H * S$) nach [Sch12, S. 13], [Kon05, S. 46]) gebildet. Dieser Wert dient dabei als Indikator für das zugrundeliegende Risiko des gegebenen Ereignisses. Im weiteren Vorgehen einer Risikobewertung können auf diese Weise alle Ereignisse mit Hilfe der Risikomatrix eingeordnet werden. Daraufhin können im Anschluss die Er-

gebnisse gesammelt dargestellt, geordnet und priorisiert werden. Welche Risikowerte bei diesem Vorgehen als akzeptabel bzw. nicht-akzeptabel gelten, muss zuvor zusammen mit der Größe der Risikomatrix festgelegt werden. So können dann, beispielsweise bei einer 5x5 Matrix mit 5 Häufigkeits- sowie Schadensklassen, Risikowerte von 1 bis 3 als akzeptabel angesehen werden und Werte darüber hinaus als kritisch oder nicht-akzeptabel [Bra02]. Dies wird zudem durch eine Farbskala zur Differenzierung unterschiedlicher Risikobereiche bekräftigt. Als rot eingestufte Risikowerte gelten dabei als nicht-, hingegen grüne Bereiche als akzeptabel. Der Bereich dazwischen erfordert zusätzlich besondere Aufmerksamkeit, sodass die dort eingeordneten Risiken nur akzeptiert werden, wenn diese nach dem ALARP (engl. As Low as Reasonably Practicable) [Vin07] Prinzip behandelt und unter Berücksichtigung von risikomindernden Maßnahmen dem Akronym nach „so niedrig, wie vernünftigerweise praktikabel“ gehalten werden.

Erstellung

Mit Hilfe der schematischen Darstellung in Abbildung 2.3 soll das Vorgehen für die Risikobewertung im Rahmen der Erstellung von Gefährdungsbeurteilungen veranschaulicht werden. Der Prozess beginnt dabei mit einem Planungsschritt zur Definition von Akzeptanzkriterien der Risiken des zugrundeliegenden Anwendungsfalls, was sich ggf. auch aus Anforderungen möglicher Auftraggeber heraus ergeben kann. Darüber hinaus kann in diesem Schritt, wie zuvor erläutert, festgelegt werden wie differenziert und in welchem Ausmaß somit die Risikomatrix eingesetzt wird. Diese und weitere Überlegungen für die anschlie-

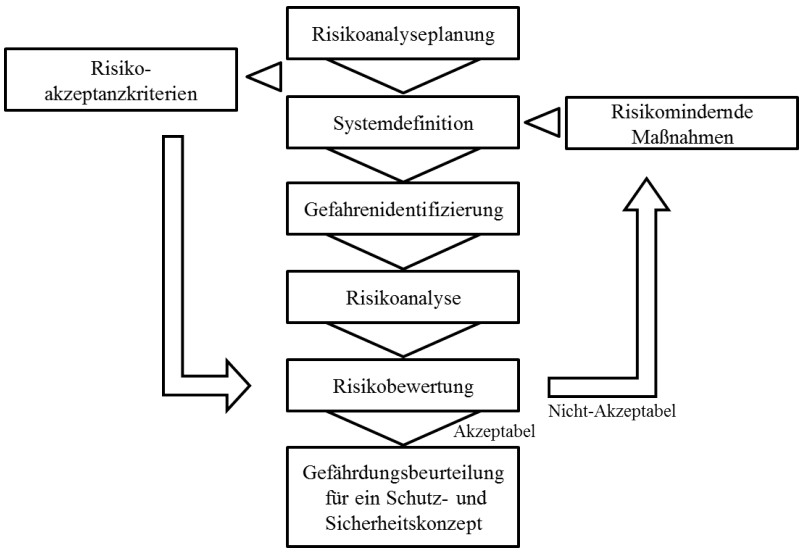

Abbildung 2.3: Vorgehen zur Risiko- bzw. Gefährdungsbeurteilung (eigene Darstellung in Anlehnung an [Vin07, S. 127], [Bra02, S. 87]

ßende Durchführung werden in dem ersten Planungsschritt vorgenommen. Im Anschluss erfolgt der Schritt der **Systemdefinition**, in welchem zunächst der jeweils betrachtete Anwendungsfall beschrieben wird [Kri13, S. 212]. Diese Systemdefinition bildet dabei die grundlegende Basis für die darauffolgenden Schritte und ist somit ein wichtiger Bestandteil dieser [Kri13, S. 212]. Im Rahmen von Gefährdungsbeurteilungen haben sich in der Praxis textuelle Beschreibungen der zu betrachtenden Tätigkeiten und Abläufe für diesen Schritt etabliert. Bei dem darauffolgenden Schritt der **Gefährdungsidentifikation** werden mögliche Gefährdungen und Ursachen des jeweiligen Anwendungsfalls ermittelt, klassifiziert sowie dokumentiert [Vin07, S. 121]. Die anschließende **Risikoanalyse** wird als Prozess der Berechnung des Risikos für zuvor identifizierte Gefährdungen verstanden [Kri13, S. 209]. Dabei werden die zuvor ermittelten Informationen für eine qualitative oder quantitative Analyse genutzt, um somit den Risikowert zu bestimmen. Auf Basis dieser Ergebnisse findet die anschließende **Risikobewertung** statt, wobei somit die zugrundeliegenden Ergebnisse aus der Risikoanalyse genutzt werden [Kri13]. Dabei wird u.a. hinsichtlich der vorherrschenden Akzeptanzkriterien entschieden, ob eine Anpassung des Konzepts erforderlich ist, um die Sicherheit des Konzepts zu verbessern und das Risiko zu reduzieren [Mul06, S. 18], [Kri13, S. 210]. Wird im Schritt der Risikobewertung unter Berücksichtigung der Akzeptanzkriterien festgestellt, dass die vorliegende Gefährdungsbeurteilung nicht ausreichend ist, erfolgt eine erneute Iteration des in Abbildung 2.3 dargestellten Prozesses, ggf. unter Einbeziehung weiterer **risikomindernder Maßnahmen**. Um dabei ein effektives Vorgehen sowie eine sichere Entwicklung und Durchführung komplexer geplanter Vorhaben zu gewährleisten, gelten die folgenden, abfallend priorisierten Schritte [Ren13]:

1. Eliminierung von Gefährdungen
2. Reduzierung der Auswirkung nicht eliminierbarer Gefährdungen
3. Reduzierung der Gefährdung von Personen bspw. durch Einführung von Maßnahmen wie Wachposten
4. Einführung von Schutzsystemen wie beispielsweise Verriegelungen
5. Maßnahmen zur Minderung übriger Risiken beispielsweise durch Schutzausrüstung

2.1.3 Softwareseitige Unterstützung

Einige der Gründe für den Einsatz von Software zur Unterstützung bei der Risikobewertung sind nach Vinnem [Vin07, S. 139]:

- Reduktion der Fehleranfälligkeit durch einheitliche Handhabung der Daten
- Transparente Verknüpfung von Daten
- Vereinfachung der Dokumentation

- Effektive Aktualisierung

Zur softwareseitigen Unterstützung bei der Risikobewertung existieren dafür im Wesentlichen zwei Arten relevanter Software. Zum einen, spezialisierte Software zur detaillierten physikalisch- und statistischen Untersuchung eines einzigen spezifischen Phänomens und zum anderen, Softwarepakete mit denen übergreifende Untersuchungen durchgeführt werden können [Vin07, S. 139]. Die spezialisierten Softwarelösungen sind für eine Vielzahl physikalischer Modellierungsschritte verfügbar, wie beispielsweise Gas-Austritt, Modellierung von Feuer, Explosionen Kollisionen etc. [Vin07, S. 139]. Diese Lösungen sind zwar hinsichtlich ihres Anwendungsbereichs limitiert, können jedoch wichtig sein, um realistische Vorhersagen über Belastungen, Effekte und Reaktionen treffen zu können [Vin07, S. 139]. Für die Erstellung von Gefährdungsbeurteilungen kommen derartige Softwarepakete kaum in Frage, da innerhalb dieser Dokumente nicht nur eine spezifische, sondern eine Vielzahl und somit übergreifende Untersuchung unterschiedlicher Gefährdungen, wie beispielsweise mechanische, elektrische, thermische etc., ermöglicht werden muss [Küp12, S. 22]. Software der zweiten Art entspricht somit mehr den Anforderungen von Gefährdungsbeurteilungen.

Als ein Beispiel einer Software, die bei der Erstellung von Gefährdungsbeurteilungen unterstützen soll, gilt die von der BG ETEM entwickelte Lösung [Ber14, S. 9]. Die „Berufsgenossenschaft Energie Textil Elektro Medienerzeugnisse“ (Abk. BG ETEM), ist überwiegend der zuständige Unfallversicherungsträger für die Errichtung und den Betrieb von Offshore-Windenergieanlagen, da sowohl die Hersteller von Windenergieanlagen als auch die Energieversorgungsunternehmen als Betreiber sowie eine große Zahl von Service- und Wartungsunternehmen Mitgliedsbetriebe der BG ETEM sind [Deu11b, S. 12]. Innerhalb dieser Software können branchenbezogene Musterkataloge verwendet werden, in denen Gefährdungen und Schutzmaßnahmen beschrieben sind [Ber14, S. 9]. Demnach existieren für die Nutzung der Software vordefinierte Bausteine, die der Nutzer für den jeweiligen Anwendungsfall und die Domäne zusammenstellt, um damit die Gefährdungsbeurteilung zu dokumentieren [Ber14, S. 9]. Eine ergänzende Auswahl kommerzieller Beispiele für Software zur Erstellung von Gefährdungsbeurteilungen sind Produkte der HNC-Datentechnik GmbH [Tan14a] (Auditor Plus) und der EcoIntense GmbH [Tan14b] (EcoWebDesk). Diese sollen die Nutzer bei der Erstellung und Verwaltung von Gefährdungsbeurteilungen unterstützen und somit den Arbeitsaufwand verringern sowie die Transparenz erhöhen [Tan14a], [Tan14b]. Jedoch umfasst der Funktionsumfang derartiger Software primär Funktionen zur Dokumentenverwaltung und Erstellung, sodass die Unterstützung bei der Risikoanalyse kaum fokussiert wird. Weitere Beispiele sind RAMSYS [Sea14] sowie BASSnet Risk Manager [BAS14] die als softwareseitige Unterstützung genutzt werden können, jedoch einen vergleichsweise ähnlichen Funktionsumfang besitzen wie die bereits aufgeführten Softwarepakete (siehe Abbildung 2.4).

Zusammenfassung und Diskussion Die erläuterten Softwarepakete wurden in Abbildung 2.4 aufgelistet und hinsichtlich der Zieldefinitionen dieser Ausarbeitung gegenübergestellt. Durch die Gegenüberstellung kann gezeigt werden, dass verfügbare Softwarepakete ähnliche Aufgabengebiete sowie Möglichkeiten bieten diese auszuüben. Demnach kann für diese Softwarepakete gemeinsam zusammengefasst werden, dass in Bezug auf **Ziel 2 - Prozessorientierte Risikobetrachtung** erwartungsgemäß jeder der betrachteten Ansätze diese Perspektive einnimmt, was auch durch die Fokussierung auf Gefährdungsbeurteilungen im Rahmen der Arbeitssicherheit zu erklären ist. Jedoch wird dieses Ziel nur teilweise erfüllt, da zwar die Perspektive eingenommen wird, jedoch eine detaillierte Betrachtung der Prozesse, beispielsweise durch eindeutig definierte Abläufe, Abhängigkeiten und Rahmenbedingungen, nur begrenzt möglich ist. In Bezug zur Zieldefinition nach **Ziel 3 - Wiederverwendbare Informationen** ermöglichen die Ansätze jeweils vordefiniertes Wissen in Form von „Katalogen“ bereitzustellen, aus denen bei der Benutzung der Software selektiert werden kann. Eine umfassende Wiederverwendbarkeit über die vordefinierten Kataloginformationen hinaus, sodass individuell eingepflegte Informationen nutzbar sind, wird jedoch kaum ermöglicht, wodurch das Ziel durch die Softwarepakete nur teilweise erfüllt wird. Dem Softwarepaket RAMSYS fehlt eine derartige Funktionsweise, wohingegen in Auditor Plus darüber hinaus zwar individuell häufig verwendete Textbausteine zusätzlich innerhalb der Kataloge definiert werden, was jedoch für eine bessere Bewertung hinsichtlich der Zieldefinition nicht ausreicht. Bei dem beschriebenen „klassischen Vorgehen“, welches in Abbildung 2.4 vergleichend aufgeführt ist, obliegt der handelnden Person vollständig, ob alte Dokumente oder Dateien nach relevanten Informationen durchsucht und verwendet werden, wodurch diese als Methode das Ziel nicht erfüllt. Abgesehen vom klas-

	Ziel 1 - Formalisierung des Basiswissens	Ziel 2 - Prozessorientierte Risikobetrachtung	Ziel 3 - Wiederverwendbare Informationen	Ziel 4 - Unterstützende formalisierte Risikoanalyse	Ziel 5 - Berücksichtigung risikomindernder Maßnahmen	Ziel 6 - Softwareseitige Unterstützung
Klassisches Vorgehen		(X)			(X)	(X)
BG ETEM		(X)	(X)		(X)	X
Auditor Plus		(X)	(X)		(X)	X
RAMSYS		(X)			(X)	X
EcoWebDesk		(X)	(X)		(X)	X
Risk Manager		(X)	(X)		(X)	X

Abbildung 2.4: Zielerfüllung des klassischen Vorgehens und softwareseitiger Unterstützung bei Gefährdungsbeurteilungen

sischen Vorgehen ist eine durchgängige softwareseitige Unterstützung bei den betrachteten Ansätzen inhärent vorhanden, sodass dies zu einer vollständigen Zielerfüllung nach **Ziel 6 - Softwareseitige Unterstützung** führt. Hinsichtlich der risikomindernden Maßnahmen bei der Planung und Analyse nach **Ziel 5 - Berücksichtigung risikomindernder Maßnahmen** erfüllen sowohl die genannten Ansätze mit softwareseitiger Unterstützung als auch das klassische Vorgehen dieses Ziel nur teilweise. Wie bereits in vorangegangenen Ausführungen erläutert, ist eine Problemstellung des aktuellen Standes der Technik, dass risikomindernde Maßnahmen zwar geplant, jedoch nicht transparent und nachvollziehbar eingepflegt werden können, sodass deren Nutzen und Wirkung individuell aufgeführt werden kann. Diese Problemstellung existiert sowohl im erläuterten klassischen Vorgehen als auch, wie in Abbildung 2.4 ersichtlich, innerhalb kommerziell verfügbarer Softwarepakete.

Die in Abbildung 2.4 mit „X“ für ein Ziel markierten Ansätze entsprechen einer vollständigen Zielerfüllung, wohingegen die mit „(X)“ markierten Ansätze dieses Ziel nur teilweise erfüllen. Keine Markierung entspricht der nicht-Erfüllung eines Ziels.

2.2 Techniken

In diesem Abschnitt werden übergreifende verwandte Ansätze zur Risikoanalyse und Bewertung erläutert, die aufgrund ihrer Ausrichtung und Anwendung relevant sind für die Auswahl eines geeigneten Lösungsansatzes dieser Ausarbeitung. Für diesen Anwendungszweck sind die wichtigsten Techniken nach [Vin07, S. 166 ff], [Uni06, S. 8])

- Fehlerauswirkungs- und Effektanalyse (engl. Failure Mode and Effect Analysis, Abk. FMEA)
- Simulation
- Fehlerbaumanalyse (engl. Fault Tree Analysis, Abk. FTA)
- Ereignisbaumanalyse (engl. Event Tree Analysis, Abk. ETA)

FMEA Die FMEA ist ein strukturierter Ansatz zur Untersuchung eines Systems und dessen Komponenten [Mul06, S. 116]. Systemwissen und identifizierte Einflussfaktoren können mit dieser Technik tabellarisch gesammelt und aufgelistet werden, wodurch die Technik wenig theoretisches Vorwissen sondern eher Erfahrungswissen erfordert [Vin07, S. 169]. Sie basiert somit auf einer textuellen Beschreibung der kausalen Zusammenhänge zwischen Gefahrensituationen, Gefährdungen und technischen Ursachen [Stä11, S. 32], [Slo06]. Diese Informationen werden tabellarisch aufgelistet, wie exemplarisch in Abbildung 2.5 dargestellt, wobei Umfang und Struktur variieren können. Bei der FMEA als eine induktive Methode, wird von bekannten Ursachen ausgehend, auf potentielle Auswirkungen geschlossen

[Stä11, S. 32]. Innerhalb der FMEA können Systemkomponenten jeweils aufgeführt werden, sodass Funktionen sowie mögliche Schwachstellen und Auswirkungen gelistet werden können. Zusätzlich können Einschätzungen getroffen werden, um beispielsweise mit Hilfe von Häufigkeits- oder Schwerestufen zu priorisieren sowie einen Risikowert quantifizieren zu können. Dadurch kann die Kritikalität und Entdeckungswahrscheinlichkeit von potentiellen Fehlermodi ermöglicht werden [Eri05]. Grundsätzlich wird die Methode genutzt, um mögliche Probleme, Fehler, Ursachen etc. frühzeitig identifizieren und eliminieren zu können [Sta03]. Sowohl FMEA als auch Erweiterungen wie FMECA (engl. Failure Mode, Effects and Criticality Analysis), sind strukturierte und standardisierte bottom-up Methoden, die es ermöglichen, potenzielle Fehler bei der Entwicklung eines Produktes bereits während der Planung bzw. im Systementwurf aufzudecken und diesen mittels geeigneter Maßnahmen entgegenzuwirken [Stä11, S. 33], [DIN02]. Dabei können zum einen historische Daten unterstützen, indem entsprechend dokumentierte Informationen zur Hilfe genommen werden [Sta03]. Zum anderen, können Daten anderer Quellen oder Methoden, wie beispielsweise Statistiken, Simulation, FTA etc., in der FMEA ergänzend eingepflegt und dokumentiert werden [Sta03]. Zu Beginn einer FMEA wird das zu betrachtende System in seine Basis-Elemente (z.B. Komponenten) aufgeteilt, welche in einem FMEA-Formblatt gelistet und individuell analysiert werden, indem ihnen dort Soll-Funktionen zugewiesen werden [Stä11, S. 33]. Anschließend werden potenzielle Fehlfunktionen und deren Auswirkungen identifiziert und dokumentiert, woraufhin diese hinsichtlich ihres Risikopotenzials bewertet werden können [Stä11, S. 34].

System														**FMEA No.**
Subsystem														Page
Component														Prepared by
Core team														FMEA Date (org.)
				Existing conditions						Action results				
Component/process	Potential failure mode	Potential effects of mode	Potential causes of mode	Present control mechanisms	Severity	Occurrence	Detection	Risk Priority Number (RPN)	Recommend actions	Action taken	S	O	D	RPN

Abbildung 2.5: Exemplarisches Format einer FMEA Tabelle nach [LLB+11]/[SD14]

Die Durchführung einer vollständigen FMEA ist aufwändig und erfordert detaillierte Kenntnisse des Anwendungsfalls zur Durchführung der Analyse [Sin03, S. 16]. Darüber hinaus können nur einzelne Elemente, wie beispielsweise Ursachen und Gefährdungen, textuell erfasst werden, wodurch nicht genau aufgeschlüsselt werden kann wie diese untereinander, aber auch mit anderen Systemkomponenten oder Faktoren zusammenhängen. Daher können lediglich Einfachfehler erfasst werden, wodurch nie alle Systemgefährdungen identifiziert werden können, da Gefährdungen häufig eine Folge von mehreren Fehlern sind [Stä11, S. 34/35]. Darüber hinaus können menschliche Fehlhandlungen, externe Einflüsse und Schnittstellen nur begrenzt in die Analyse mit einbezogen werden [Stä11, S. 34], [Eri05], [Bra05]. Zudem ist die FMEA im Vergleich zu anderen Verfahren, wie bei-

spielsweise der Fehlerbaumanalyse, eher unsystematisch [Stä11, S. 34], [Eri05], [Bra05]. Zusammenfassend ist die FMEA eine seit vielen Jahren praktizierte und etablierte Technik die inzwischen weitere Arten der Technik selbst, wie beispielsweise zur Untersuchung von Systemen, Komponenten oder Prozessen, umfasst. Für eine ausführliche, über den hier gegebenen Überblick hinausgehende Beschreibung dieser, sei jedoch auf entsprechende Fachliteratur wie Stamatis [Sta03] verwiesen.

Simulation Nach der VDI-Richtlinie 3633 [VDI00] ist eine Simulation, „die Nachbildung eines Systems mit seinen dynamischen Prozessen in einem Modell, um zu Erkenntnissen zu gelangen, die auf die Wirklichkeit übertragbar sind“ [Dor14, S. 47]. Innerhalb dieser, wird zunächst das zu untersuchende System in Form eines Simulationsmodells abgebildet. Ein Simulationsmodell ist ein spezielles, programmiersprachlich abgefasstes Modell zur Behandlung und Auswertung mittels computergestützter Simulation und bildet damit den betrachteten Anwendungsfall mit geeignetem Detailgrad und Abstraktion ab [Dor14, S. 47]. Ein Simulationsmodell muss selbst dynamisches Verhalten erzeugen können und demnach prinzipiell über die gleichen Elemente verfügen wie jedes dynamische System: Es muss eine Wirkungsstruktur aufweisen mit entsprechenden Systemparametern, und es muss auf Einwirkungen aus der Systemumgebung reagieren können [Dor14, S. 47]. Dieses Modell bildet den jeweils problemrelevanten Realitätsausschnitt ab und lässt sich im Rahmen der eigentlichen Ausführung, der Simulation, auswerten und manipulieren, wodurch die Technik für Anwendungsfälle genutzt wird, in denen eine reale Erprobung unmöglich, zu gefährlich oder zu teuer wäre [Dor14, S. 47]. Bei der Ausführung wird das Simulationsmodell somit verarbeitet, um im Nachhinein Eigenschaften des Modells zu untersuchen und somit Rückschlüsse auf den realen Anwendungsfall ziehen zu können. Dabei werden verschiedene Konfigurationen des Simulationsmodells in mehreren Simulationsdurchläufen ausgeführt.

Für den Einsatz eines solchen Verfahrens ist beträchtlicher Aufwand, Zeit, Geld und Expertise [Dor14, S. 49] für die Erstellung eines entsprechenden Simulationsmodells erforderlich, was somit zunächst für eine erhöhte Komplexität des Verfahrens spricht [Buc08, S. 2]. Darüber hinaus ist die Methode schwerfällig, sodass zunächst Hypothesen erhärtet und Modelle formuliert sowie Daten im Nachhinein ausgewertet werden müssen [Dor14, S. 49]. Zur Untersuchung des Modells ist eine hohe Zahl an Simulationsdurchläufen durchzuführen, um eindeutige Ergebnisse zu erlangen, welche jedoch zusätzlich erst von Experten abgeleitet werden müssen, was wiederum fehleranfällig ist [Dor14, S. 49]. Trotz der Nachteile lohnt sich der Einsatz der Simulation in vielerlei Anwendungsfällen. So kann eine mögliche Anwendung beispielsweise zur Untersuchung der Kollisionshäufigkeit im Schiffsverkehr dienen [Bra02, S. 85]. Weiterführende Informationen zur Theorie der statistischen Simulation kann dem Werk von Ripley [Rip09] entnommen werden.

Fehlerbaumanalyse Als deduktive Technik geht die Fehlerbaumanalyse (engl. fault tree analysis, Abk. FTA), wie sie in der DIN 25424 [din81], [din90] national und in der IEC 61025 [Int06] international standardisiert ist, von bekannten Auswirkungen aus und ermittelt sukzessiv die zugrundeliegenden unbekannten (Basis-)Ursachen [Stä11, S. 38]. Hieraus wird deutlich, dass die Fehlerbaumanalyse vornehmlich ein Mittel zur Analyse von Gefährdungen auslösenden Ursachen ist, nicht aber ein Werkzeug um Gefährdungen zu identifizieren [Stä11, S. 38], [Lev95]. Die FTA ist daher eine weitere verbreitete Technik zur Analyse und logischer sowie grafischer Strukturierung von Ursache-Wirkungs-Beziehungen. Die Basis für die Fehlerbaumanalyse ist die Erstellung von Fehlerbäumen, die als grafisches Modell verschiedene parallele und sequentielle Kombinationen von Ursachen darstellen, die zu einer Gefahr führen können [RV87], wie exemplarisch in Abbildung 2.6 für den Ausfall eines Kraftstoffsystems dargestellt.

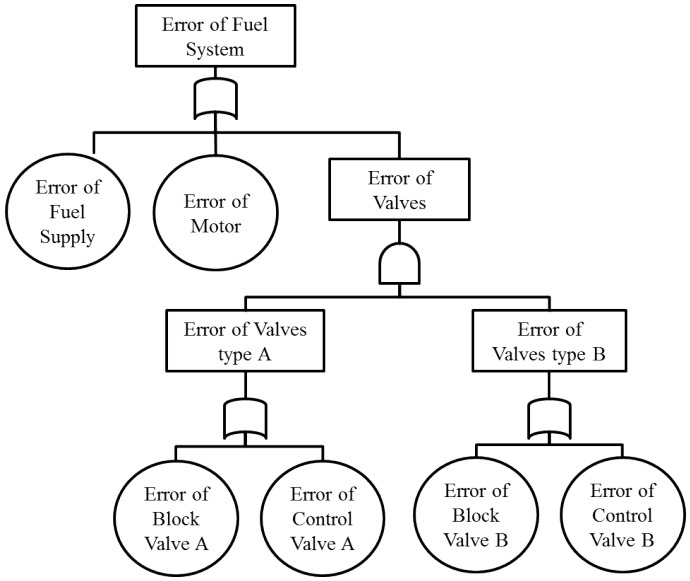

Abbildung 2.6: Exemplarischer Fehlerbaum zur Beschreibung des Ausfalls eines Kraftstoffsystems

Die übergeordnete Gefahr, für die bei der Fehlerbaumerstellung Kombinationen von Ursachen untergeordnet werden, wird in der Terminologie der FTA „Top-Event“ oder unerwünschtes Ereignis (engl. undesired event) genannt. Kombinationen von Ursachen werden mit Hilfe von booleschen Operatoren, den sogenannten „Gates“ strukturiert, die in der grafischen Darstellung mit Hilfe eigener Symbole dargestellt werden (siehe Abbildung 2.7). Darüber hinaus wird zwischen verschiedenen Ursachen bzw. Ereignissen, den sogenannten Events unterschieden, welche wiederum grafisch durch eigene Symbole dargestellt werden

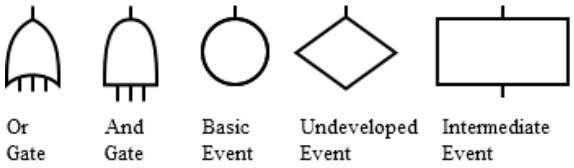

Abbildung 2.7: Auszug der gebräuchlichsten Fehlerbaumsymbole nach [CACO06]

(siehe Abbildung 2.7).

Die Verkettung der einzelnen Symbole zur Erstellung eines Fehlerbaumes erfordert tiefes Wissen über das zu betrachtende System, da somit verschiedene Systembestandteile bzw. Komponenten hinsichtlich ihres Zusammenwirkens verknüpft werden müssen. Eine Hilfestellung können nach dem Fault Tree Handbook [VDF+02] Zuverlässigkeitsblockdiagramme sein, in welchen Komponenten des betrachteten Systems in einem Blockdiagramm dargestellt werden, wie exemplarisch in Abbildung 2.8 dargestellt. In diesem Blockdiagramm werden die Komponenten aufgeführt und miteinander verknüpft, sodass sich daraus eine schematische Struktur des Gesamtsystems, wie exemplarisch für ein Kraftstoffsystem in Abbildung 2.8 mit Komponenten wie Ventilen, Motor und Kraftstoffzufuhr dargestellt, ergibt. Anhand dieser Darstellung lassen sich Pfade im Diagramm identifizieren, bei denen das Zusammenwirken der Komponenten zu einer erfolgreichen Funktion des exemplarisch betrachteten Kraftstoffsystems führt. Für das dargestellte exemplarische Kraftstoffsystem können somit die folgenden beiden erfolgreichen Pfade ermittelt werden:

1. Fuel Supply, Block Valve A, Control Valve A, Motor
2. Fuel Supply, Block Valve B, Control Valve B, Motor

Um mit Hilfe eines solchen Blockdiagramms den Erfolg des Gesamtsystems auswerten zu können, werden die Pfade durchnummeriert und nach den Regeln der booleschen Algebra in konjunktiver Normalform zusammengeführt, sodass das Gesamtsystem erfolgreich ist, wenn $Erfolg = Pfad1 \vee Pfad2$, mit $Pfad1 = FuelSupply \wedge BlockValveA \wedge ControlValveA \wedge Motor$. Gleichermaßen kann somit auch der Misserfolg des Systems ausgedrückt werden, sodass keiner der Pfade erfolgreich ist ($Misserfolg = \neg Erfolg = \neg(Pfad1 \vee Pfad2)$). Wird dies entsprechend der booleschen Algebra umgeformt, kann der Misserfolg des Systems

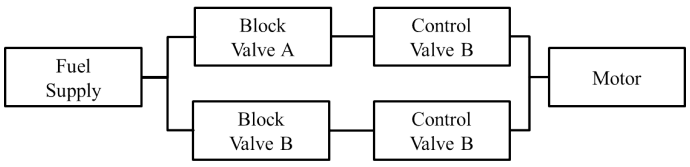

Abbildung 2.8: Exemplarisches Zuverlässigkeitsblockdiagramm eines Kraftstoffsystems nach [VDF+02]

auch als $Misserfolg = \neg FuelSupply \vee \neg Motor \vee ((\neg BlockValveA \vee \neg ControlValveA) \wedge (\neg BlockValveB \vee \neg ControlValveB))$ beschrieben werden. Anschaulicher kann der Misserfolg des Systems jedoch in Form eines Fehlerbaumes dargestellt werden, sodass der Misserfolg bzw. Ausfall des exemplarischen Kraftstoffsystems in Abbildung 2.6, entsprechend der beschriebenen Funktion des Misserfolgs, als Fehlerbaum dargestellt wird. Je nach Umformung des booleschen Ausdrucks kann die Struktur des Fehlerbaums variieren, wobei jedoch die Logik die selbe bleibt. Der Ausfall einer Komponente, wie beispielsweise $\neg FuelSupply$, wird dabei als ein Basic-Event `Error of Fuel Supply` dargestellt. Weitere Verknüpfungen ergeben sich aus den Operatoren, sodass $\vee$ mit Hilfe eines Or-Gates sowie $\wedge$ mit Hilfe eines And-Gates im Fehlerbaum abgebildet wird.

Die Auswertung der Fehlerbäume kann qualitativ oder quantitativ vorgenommen werden, was letztendlich der Analyse im eigentlichen Sinne entspricht. Die Analyse erfolgt Top-Down und dient der Identifizierung der Ursachen eines unerwünschten Ereignisses auf oberster Ebene [Bra05]. Hierbei beschreibt jede Ebene einen identischen Sachverhalt [Lev95], welcher bis hin zur Komponenten-Ebene immer weiter detailliert wird [Stä11, S. 40]. Sämtliche zwischen dem obersten und den Basis-Ereignissen (z.B. Komponentenausfällen) modellierten Ereignisse stellen sogenannte Pseudo-Ereignisse, also Abstraktionen von realen Ereignissen dar [Stä11, S. 40]. Diese ergeben sich durch beliebige Kombinationen von Basis-Ereignissen und spielen zumeist für die formale Analyse der Baumstrukturen eine untergeordnete Rolle [Stä11, S. 40].

Bei der quantitativen Analyse werden im Wesentlichen mit Hilfe boolescher Algebra die Eintrittswahrscheinlichkeiten mit Gates verknüpfter Ursachen berechnet, sodass als Ergebnis die Eintrittswahrscheinlichkeit des Top-Events ermittelt wird. Bei der qualitativen Analyse werden überwiegend Minimal Cutsets ermittelt, die die minimal notwendigen und somit kritischen Kombinationen von Ursachen aufschlüsseln, die zum Auslösen der Gefahr führen können. Dabei wird der zugrundeliegende Fehlerbaum in einen booleschen Ausdruck überführt, welcher soweit vereinfacht wird, dass die relevanten Kombinationen von Ereignissen abzulesen sind [Stä11, S. 40]. Weiterführende Fachliteratur zur Fehlerbaumanalyse stellen die beiden Handbücher Fault Tree Handbook [RV87], [VDF+02] dar.

Ereignisbaumanalyse Im Gegensatz zur FTA wird in der Ereignisbaumanalyse (engl. event tree analysis, Abk. ETA), ausgehend von einer Ursache, untersucht welche Folgen bzw. Auswirkungen diese haben kann. Daher wird die ETA häufig als bottom-up und die Fehlerbaumanalyse als top-down Ansatz betrachtet. Ausgehend von einer Ursache, in der ETA auslösendes Ereignis (engl. initiating event) genannt, werden sukzessive Sequenzen möglicher Folgen identifiziert, die zu einem möglichen Unfallszenario führen können [Eri05, S. 223]. In der ETA werden dabei mögliche Pfade mit Hilfe einer Baumstruktur grafisch dargestellt, dem sogenannten Ereignisbaum (engl. event tree). Ein exemplarischer Event Tree, der diese Pfade ausgehend vom initiating event eines Gaslecks betrachtet, wird in

Abbildung 2.9 dargestellt, wobei die Pfade je nach zutreffen oder nicht-zutreffen übergeordneter Ereignisse verzweigen. Das Ziel der ETA ist es zu bestimmen, ob ein initiating event sich zu einem möglichen Unfall auswirken kann, oder ob es ausreichend Kontrollmechanismen gibt die das verhindern können [Eri05, S. 223]. Somit soll ermittelt werden, ob das Auftreten eines Ereignisses gezwungenermaßen zu einem Schadensereignis führt, oder die Schadensfolgen mittels der im System-Design implementierten Sicherungsmaßnahmen und -prozeduren reduziert bzw. sogar verhindert werden können [Stä11, S. 35]. Ereignisbaumanalysen können auf oberster Gesamtsystemebene durchgeführt werden, wodurch Teilsysteme, Bauteile und Komponenten, Software, Prozesse, Umgebungsbedingungen und menschliche Fehlhandlungen mit abgedeckt werden können [Eri05]. Die ETA kann für verschiedene Anwendungsbereiche eingesetzt werden, sodass diese zum einen zur Identifikation und Optimierung von Schutzeinrichtungen, welche aufgrund ihrer (Un-)Wirksamkeit einen überproportionalen Einfluss auf die Eintrittswahrscheinlichkeit eines bestimmten Schadensereignisses haben, dienen können [Stä11, S. 36]. Zum anderen, kann eine ETA auch dazu verwendet werden verschiedene Unfallszenarien darzustellen, welche aus einem einzigen Initialereignis resultieren können [Stä11, S. 36]. Im Vorgehen der ETA werden ausgehend von einem Initialereignis vorwärtsgerichtet verschiedene resultierende Ereignisse, in Abhängigkeit von getroffenen Maßnahmen bzw. Schutzeinrichtungen identifiziert [Stä11, S. 36]. Dabei werden zunächst von links nach rechts alle getroffenen Maßnahmen der Reihe nach aufgelistet. Dem zugrunde wird der eigentliche Ereignisbaum aufgebaut, in welchem Verzweigungen einzelner Pfade erstellt werden, beispielsweise hinsichtlich des Erfolgs oder Misserfolgs der getroffenen Maßnahmen bzw. des Eintritts oder nicht-Eintritts eines Ereignisses. Zum Abschluss können dann Pfade gesammelt werden, die zu einem gefährlichen Ereignis führen können.

Ein Nachteil der Technik ist, dass stets von einem einzigen Initialereignis ausgegan-

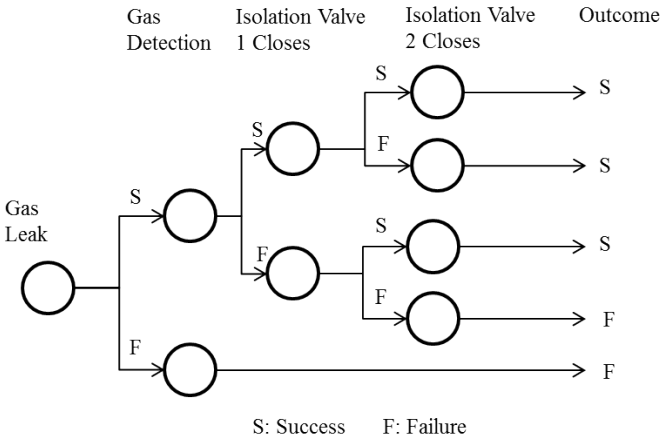

Abbildung 2.9: Exemplarischer Event Tree eines Gaslecks nach [ZK04]

gen wird, sodass deswegen eine Vielzahl von Ereignisbaumanalysen erforderlich wäre, um Konsequenzen von mehreren Initialereignissen bestimmen zu können [Eri05], [Stä11, S. 37].

Zusammenfassung und Diskussion In Abbildung 2.10 werden die erläuterten Techniken hinsichtlich ihrer Zielerfüllung zusammenfassend tabellarisch eingeordnet. Dabei erfüllt die Methode der FMEA die Zieldefinition nach **Ziel 5 - Berücksichtigung risikomindernder Maßnahmen** teilweise, da innerhalb dieser Methode, abhängig von der jeweils verwendeten Tabellenstruktur, risikomindernde Maßnahmen mit eingefügt und bei der Auswertung berücksichtigt werden können. Darüber hinaus deckt sich die Problemstellung mit der des Stands der Technik, sodass die Bewertung der FMEA entsprechend der Bewertung im vorangegangenen Abschnitt, zu einer teilweisen Zielerfüllung führt. Bei den anderen Ansätzen können risikomindernde Maßnahmen nur durch alternative Designs realisiert werden.

Die statistische Simulation ist zwar eine verbreitete Technik zur Risikoanalyse und somit Bestandteil dieses Abschnitts, jedoch sind im Hinblick auf die Komplexität damit durchgeführte Analysen spezifisch und kaum für eine Vielzahl übergreifender Gefährdungen durchführbar. Weiterhin erfordert die Simulation eine Formalisierung notwendigen Wissens, was nach **Ziel 1 - Formalisierung des Basiswissens** zu einer vollständigen Zielerfüllung führt. Für die tatsächliche simulative Untersuchung ist zudem eine softwareseitige Unterstützung notwendig. Da jedoch in diesem Fall nur die Technik als solche bewertet wird, führt dies auch für die übrigen Ansätze nicht zu einer Zielerfüllung.

	Ziel 1 - Formalisierung des Basiswissens	Ziel 2 - Prozessorientierte Risikobetrachtung	Ziel 3 - Wiederverwendbare Informationen	Ziel 4 - Unterstützende formalisierte Risikoanalyse	Ziel 5 - Berücksichtigung risikomindernder Maßnahmen	Ziel 6 - Softwareseitige Unterstützung
FMEA		(X)			(X)	
Simulation	X	(X)			(X)	
FTA	X	(X)			(X)	
ETA	X	(X)			(X)	

Abbildung 2.10: Zielerfüllung der klassischen Techniken

Bei der Methode der FTA ist **Ziel 1 - Formalisierung des Basiswissens** erfüllt, da innerhalb dieser Methode Ursachen einer Gefährdung logisch verknüpft werden können, sodass eine Bewertung der Gefährdung, wie im Fokus von Gefährdungsbeurteilungen, somit transparent und nachvollziehbar ausgestaltet werden kann. Zudem kann dieses Wissen

für anschließende Risikoanalysen verwendet werden. Die ETA und FTA Techniken folgen einem ähnlichen Prinzip, wohingegen die FTA aufzeigt wie ein Fehler zustande kommt und die ETA aufzeigt welche Konsequenzen ein solches Ereignis haben kann [Mul06, S. 120]. Da jedoch für die Durchführung der ETA auch das notwendige Wissen strukturiert dokumentiert werden muss, erfolgt eine Bewertung hinsichtlich **Ziel 1 - Formalisierung des Basiswissens** analog zur FTA, wobei mit der FTA eine vergleichsweise bessere Formalisierung möglich ist [Stä11].

Verschiedene Aspekte zugrundeliegender Prozesse können mit sämtlichen Ansätzen teilweise berücksichtigt werden, sodass **Ziel 2 - Prozessorientierte Risikobetrachtung** teilweise erfüllt wird. So ist beispielsweise in der Simulation die Modellierung von Abläufen erforderlich die mit der Simulation durchlaufen werden müssen, wohingegen in der FMEA eine tabellarische Zuordnung von Prozessschritten erfolgen kann. In der ETA wird der Ablauf ausgehend von einem Initialereignis fortgeführt und in der FTA können explizit Aspekte, wie beispielsweise fehlerhaft durchgeführter Prozessschritte oder Fehlhandlungen, berücksichtigt werden.

Maßnahmen wie nach **Ziel 5 - Berücksichtigung risikomindernder Maßnahmen** gefordert sind mit den Techniken nur bedingt im Rahmen von Designänderungen umsetzbar, weshalb diese nur zu einer teilweisen Zielerfüllung beitragen.

Gemeinhin existieren zwar für sämtliche der aufgeführten Techniken jeweils Softwarepakete die bei der Anwendung der Technik unterstützen, bzw. wie im Fall der Simulation diese erst praktikabel machen, jedoch werden diese in der in Abbildung 2.10 gezeigten Aufstellung nicht berücksichtigt. Hingegen sind nur die Techniken als solche betrachtet worden, weshalb diesen beispielsweise auch eine praktikable Lösung zur Wiederverwendbarkeit fehlt. Dies obliegt somit der Handhabung des jeweiligen Nutzers der Technik, wie gleichermaßen auch die Durchführung der Risikoanalyse.

2.3 Verwandte Arbeiten

Nachdem in den vorangegangenen Abschnitten der derzeitige Stand zur Erstellung von Gefährdungsbeurteilungen für maritime Operationen sowie einige grundlegende Techniken der Risikobewertung erläutert wurden, erfolgt in diesem Abschnitt nun eine Beschreibung von verwandten Arbeiten, die den erläuterten Zieldefinitionen aus Kapitel 1 zur Entwicklung eines Lösungsansatzes hinsichtlich der Aspekte der unterstützenden Risikoanalyse und verbesserter Wiederverwendung nahe kommen. Diese Arbeiten werden daher in diesem Abschnitt zusammengetragen und erläutert sowie im Rahmen der Zieldefinitionen hin untersucht.

2.3.1 Automatisierte Risikoanalyse

Im Rahmen der in Kapitel 1 aufgeführten Problemstellungen und daraus resultierenden Zieldefinitionen und Beiträge dieser Ausarbeitung, ist die Betrachtung einer automatisierten Risikoanalyse sowie einer Technik mit der Risikoanalysen zur Anwendung und Verbesserung der Transparenz für Gefährdungsbeurteilungen notwendig. Im vorangegangenen Abschnitt wurden grundlegende Techniken erläutert, die für eine Risikoanalyse für die in dieser Ausarbeitung betrachteten maritimen Operationen in Frage kommen. Diese Techniken haben gemeinsam, dass sie jeweils manuellen Aufwand und somit Zeit, Kosten und zudem Erfahrungswissen für die Durchführung an sich, als auch für die Anwendung im Anwendungsfall erfordern. Dennoch sind dies wichtige Werkzeuge im Rahmen von verschiedenen Anwendungsfällen von Risikoanalysen.

In Anbetracht des Fokus der maritimen Operationen und der Kapazitäten und Ressourcen maritimer Sicherheitsexperten, erscheint die Durchführung von Simulationen für die vielfältigen Gefährdungen innerhalb von Gefährdungsbeurteilungen kaum praktikabel. Das Verfahren der FMEA ist in der Hinsicht weniger Komplex, erfüllt jedoch nicht den Anspruch nach mehr Transparenz, da in diesem Verfahren kaum aufgeschlüsselt wird, welche Ursachen und in welcher Kombination, einer Gefährdung zugrunde liegen. Weiterhin fokussiert die ETA die Auswirkungen von Gefährdungen, wohingegen die FTA die Ursachen von Gefährdungen betrachtet. Die Identifizierung und Analyse von Ursachen, wie beispielsweise im Rahmen der FTA durchgeführt, bildet jedoch eine entscheidende Basis zur Prävention von Unfällen, wenn mögliche Ursachen dadurch eliminiert oder kontrolliert werden können [Vin07, S. 122]. Weiterhin existieren Ansätze mit denen der Aufwand und die Fehleranfälligkeit der manuellen Erstellung von Fehlerbäumen reduziert werden kann. Diese werden in diesem Abschnitt jeweils als die relevanten verwandten Arbeiten in Bezug zur Risikoanalyse erläutert.

Diese Ansätze adressieren die Problemstellungen der manuellen, informellen und fehleranfälligen Natur bisheriger Verfahren ([JH07]) und ermöglichen daher eine automatisierte Erzeugung von Fehlerbäumen unter Zuhilfenahme zuvor gesammelter und strukturierter Modellinformationen. Dadurch kann die Vernetzung von Gefährdungen transparent gemacht werden ([PL11, S. 193]), was entsprechend zu einer Erfüllung von **Ziel 1 - Formalisierung des Basiswissens** führt. Für diesen Zweck existieren verschiedene Lösungsideen, die sich im Wesentlichen dadurch unterscheiden, dass verschiedene Modellierungssprachen als Grundlage verwendet werden [TLS08, S. 630]. Mit der gewählten Modellierungssprache werden jeweils die notwendigen Informationen und Zusammenhänge des betrachteten Anwendungsfalls modelliert. Auf diese Weise wurde beispielsweise das Hydraulik System eines Airbus 320 von Bieber [BCS02], ein Produktionsbereich der Metallverarbeitung von Liggesmeyer [LR98], oder elektrische Schaltungen von De Vries [DV90] modelliert und als Basis zur Erstellung und Analyse von Fehlerbäumen genutzt. Weitere vergleichbare Ansätze wer-

den nachfolgend, entsprechend der verwendeten Modellierungssprache, zusammenfassend gelistet und anschließend erläutert:

- Chen [Che10], [CACO06] mit Little-Jil [LMW+00]
- Xiang [X+11], [X+10] mit SysML
- Pai [PD02], Lauer [LGP11] mit UML
- Li [L+11], Joshi [JVB07], Dehlinger [DD08] mit AADL (Architecture Analysis and Design Language)
- Papadopoulos [PM01], Tajarrod [TLS08], [LST09] mit Matlab-Simulink
- McKelvin [MEP+05] mit Fault Tolerant Data Flow (FTDF)
- Rae [Rae04], [Rae07] mit hierarchischer Modellierung

Chen [Che10] mit Little-Jil Einen Ansatz liefert Chen im Rahmen seiner Dissertation [Che10], [CACO06]. In diesem werden anhand der Prozessbeschreibungssprache Little-Jil [LMW+00] Prozesse strukturiert abgebildet und somit der betrachtete Anwendungsfall in einem Prozessmodell formalisiert. Dieses Prozessmodell besteht aus der definierten Symbolik, wie in Abbildung 2.11 anhand des exemplarischen Bluttransfusionsprozesses dargestellt, mit welcher das grafische Prozessmodell erstellt wird. Mit dieser Symbolik werden im Wesentlichen in einer Balkendarstellung die betrachteten Aktivitäten bzw. Prozessschritte dargestellt und benannt. Pfeildarstellungen und Verbindungen dieser Prozessschritte kennzeichnen darüber hinaus die Sequenz der Prozessschritte. Im Hintergrund werden mit Bezug auf die Ausführung des Prozesses noch Artefakte und Ressourcen definiert, wobei Artefakte verschiedene Prozessschritte durchlaufen [CCC]. Dabei können Artefakte sowohl innerhalb eines Prozessschrittes verarbeitet sowie auch weitergeleitet oder manipuliert werden [CCC]. Ressourcen spezifizieren sogenannte Agenten und Fähigkeiten, die die Durchführung von Prozessschritten und somit auch Verarbeitung von Artefakten beschreiben. Zur Koordination werden Artefakt- und Ressourcenspezifikationen kombiniert, indem spezifiziert wird, welche Agenten und Fähigkeiten welche Aktivitäten mit welchen Artefakten wann ausführen. Auf Basis dieses Wissens, welches im Prozessmodell strukturiert und somit maschinenlesbar hinterlegt ist, werden Fehlerbäume automatisiert erstellt. Für diesen Zweck werden im Rahmen eines Algorithmus Regeln angewendet, die anhand einer definierten Struktur innerhalb des Prozessmodells entsprechend definierte Fehlerbaumstrukturen erzeugen, welche anschließend zu einem vollständigen Fehlerbaum verbunden werden. Dieses Vorgehen ist integriert in einem Softwarewerkzeug entwickelt worden, sodass ein einzelnes Werkzeug zur Modellierung sowie zur Analyse entstanden ist. Dieser Ansatz wurde innerhalb medizinischer Prozesse angewendet, sodass für eine zuvor manuell festgelegte Gefährdung, wie

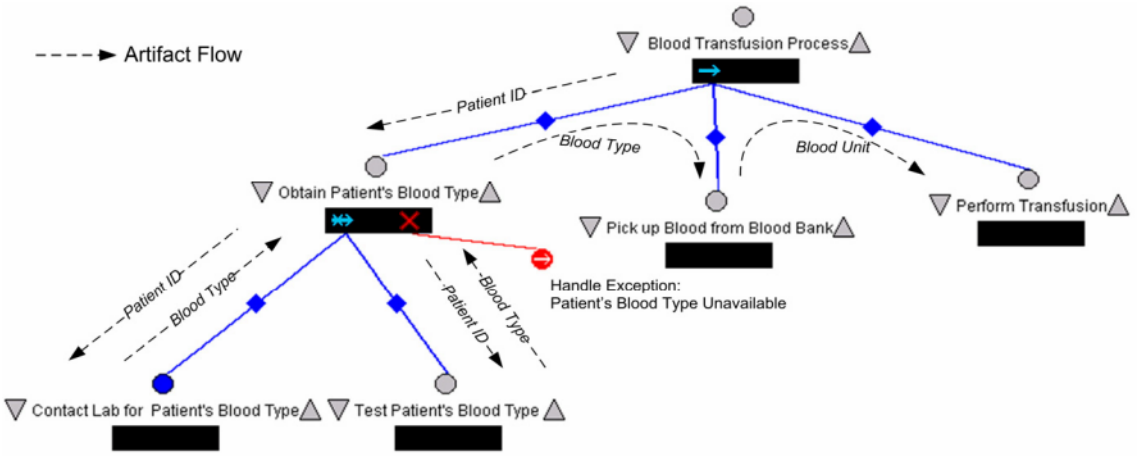

Abbildung 2.11: Mit Little-Jil modellierter Bluttransfusionsprozess nach [CACO06]

beispielsweise „Lieferung der falschen Blutgruppe“, automatisch ein Fehlerbaum anhand des festgelegten Prozessmodells erstellt werden kann. Ein für diesen Anwendungsfall im Prozessmodell definiertes Artefakt wäre somit die zu transportierende Blutkonserve. Da in dem Ansatz jedoch ausschließlich Strukturen der zugrundeliegenden Prozessschritte mit vordefinierten Regeln verarbeitet werden können, ist keine Unterstützung von mehreren Fehlerzuständen bzw. Ursachen eines Schrittes möglich [PBM+08]. Dieser Ansatz erfüllt somit **Ziel 4 - Unterstützende formalisierte Risikoanalyse** und **Ziel 6 - Softwareseitige Unterstützung**. Zudem wird **Ziel 2 - Prozessorientierte Risikobetrachtung** durch den Ansatz teilweise erfüllt, da Prozessmodelle, die die Abläufe des Anwendungsfalls umfassen, als Basiswissen genutzt werden, jedoch lediglich vordefinierte Strukturmuster als Vorlage für die Risikoanalyse dienen. Dadurch ist mit dem Ansatz über die vordefinierten Strukturmuster hinaus, kaum eine Betrachtung tätigkeitsspezifischer Gefährdungen möglich.

Xiang [X+11] mit SysML Im Ansatz von Xiang [X+11], [X+10] wird ein entwickeltes Framework als Lösungsansatz vorgestellt. Mit diesem können anhand von Modellen, die mit der Modellierungssprache SysML [Obj14] erstellt wurden, Fehlerbäume generiert werden. SysML wurde in diesem Ansatz als Modellierungssprache gewählt, da diese als Erweiterung von UML im Hinblick auf die Zielgruppe von IT-Ingenieuren vertrauter anzuwenden erscheint als beispielsweise Modellierungssprachen wie AADL [X+11, S. 7]. Die in dem Ansatz verwendete SysML Notation wurde jedoch zunächst um die Einbringung zusätzlicher Informationen erweitert, sodass Ergänzungen hinsichtlich der Modellierung von Fehlern sowie insbesondere der Abhängigkeiten von Komponenten für den Ansatz zur Fehlerbaumerstellung hinzugekommen sind [AFPR13]. Ein zugrundeliegendes SysML

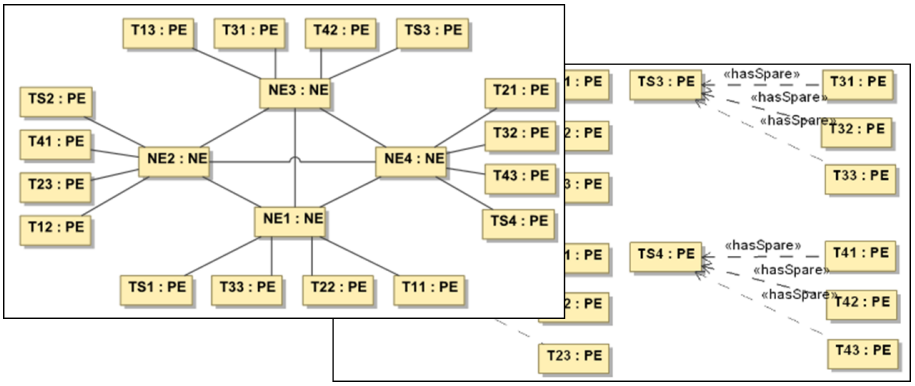

Abbildung 2.12: Konfiguration eines Fault-tolerant Parallel Processors nach [X+11]

Modell wird innerhalb des Ansatzes mit Hilfe des entwickelten Softwarewerkzeugs „CASSI“ eingelesen und in ein internes Datenformat übertragen, welches als Zwischenformat für die Generierung von Fehlerbäumen dient. Mit diesem Zwischenformat werden logische Informationen wie Abhängigkeiten aus dem SysML Modell extrahiert und gespeichert. Für die Generierung selbst wird dieses Zwischenformat erneut verwendet und in eine entsprechende Fehlerbaumstruktur überführt. Dieser Ansatz wurde im Rahmen des Fallbeispiels eines Fault-tolerant Parellel Processors (FTTP) angewendet, wobei die in Abbildung 2.12 dargestellte Konfiguration als Modellgrundlage des Ansatzes dient. Darin enthalten sind Processing-Elemente (PE), Network-Elemente (NE) sowie Elemente die als zusätzliche Redundanzen die Fehlertoleranz bei Ausfall eines PEs erhöhen. Dieses Modell, in welchem die erforderlichen Elemente des Fallbeispiels zusammenhängend dargestellt werden, dient im Rahmen des Ansatzes anschließend dazu die logischen Zusammenhänge zu extrahieren. Ergänzend werden funktionale Zusammenhänge anhand von Sequenzdiagrammen extrahiert, sodass diese kombinierten Informationen und logischen Zusammenhänge daraufhin in einen Fehlerbaum überführt und dargestellt werden können, was an das beschriebene Vorgehen mit Hilfe von Zuverlässigkeitsblockdiagrammen erinnert (siehe Abschnitt 2.2).

Zusammenfassend wird der Ansatz als begrenzt und nur für wenige sicherheitsrelevante Problemstellungen einsetzbar betrachtet [TTV+14]. Ähnlich wie im zuvor erläuterten Ansatz erfüllt der Ansatz von Xiang **Ziel 4 - Unterstützende formalisierte Risikoanalyse** und **Ziel 6 - Softwareseitige Unterstützung**. Darüber hinaus werden durch die Nutzung von Sequenzdiagrammen teilweise auch prozessorientierte Aspekte betrachtet sowie durch die Berücksichtigung von Redundanzen im Rahmen der fokussierten technischen Anwendungsfälle auch eine Form von risikomindernden Maßnahmen, wodurch **Ziel 2 - Prozessorientierte Risikobetrachtung** und **Ziel 5 - Berücksichtigung risikomindernder Maßnahmen** jeweils teilweise erfüllt werden.

Pai [PD02], Lauer [LGP11] mit UML In den Ansätzen von Pai [PD02] und Lauer [LGP11] werden UML Modelle als Grundlage für die Fehlerbaumgenerierung verwendet. Diese Auswahl ist hinsichtlich der Zielgruppe und des Fokus für Softwaresysteme getroffen worden, wobei UML den De-facto-Standard der Modellierungssprachen darstellt [PD02]. Bei Pai werden zunächst UML Modelle zur Beschreibung der Objekt- und Klassenstruktur sowie zur Beschreibung der Ausführung mit dem kommerziellen UML Modellierungswerkzeug Rational Rose erstellt. Anschließend wird die logische Struktur der Objekte und Klassen anhand derer Zusammenhänge bei der Ausführung, ähnlich wie in Abschnitt 2.2 beschrieben, mit einer selbst entwickelten Parseranwendung extrahiert. Die Fehlerbaumerstellung basiert daraufhin auf den so extrahierten Informationen, was konzeptionell an den Ansatz von Xiang erinnert. Zwar wird in dem Ansatz UML als Modellierungssprache genutzt, damit jedoch hauptsächlich eine mögliche Fehlerfortpflanzung modelliert [MPB03]. Weiterhin werden extrahierte Informationen in Form von Blockdiagrammen strukturiert, sodass die darauf aufbauende Erstellung von Fehlerbäumen nach dem klassischen Vorgehen erfolgt [MPB03]. Dieser Ansatz wurde, wie auch der Ansatz von Xiang [X+11], anhand des Fallbeispiels eines Fault-tolerant parallel processors evaluiert.

Im Gegensatz dazu wird im Ansatz von Lauer zwar auch UML als grundlegende Modellierungssprache verwendet, jedoch werden dabei weitere UML Diagramme, über die bei Pai verwendeten Klassendiagramme hinaus, verwendet. Innerhalb dieser werden explizit Informationen über mögliche Fehlerauswirkungen von modellierten Komponenten eingepflegt, die sich der Annahme des Ansatzes nach auf jede der verbundenen Komponenten auswirken. Darüber hinaus ist die Erstellung von Meta-, Komponenten- und Ablaufdiagrammen notwendig, damit eine ausreichende Modellbasis im Rahmen des Ansatzes geschaffen wird. Diese werden mit einem entwickelten Algorithmus durchlaufen, woraufhin Pfade der modellierten Fehlerausbreitung durchlaufen und als Fehlerbaumstruktur, als Ergebnis des Algorithmus, dargestellt werden. Die Darstellung und Analyse wird mit Hilfe des frei verfügbaren Werkzeugs openFTA [Auv14] vorgenommen. Beide Ansätze erfüllen zusammenfassend **Ziel 4 - Unterstützende formalisierte Risikoanalyse**, jedoch ist hinsichtlich der softwareseitigen Unterstützung bei Pai nur das Vorgehen und Ideen sowie in Lauer die Verwendung externer Software aufgeführt worden. **Ziel 6 - Softwareseitige Unterstützung** ist somit durch die vorgestellten Ansätze nicht bzw. nur teilweise erfüllt. Weiterhin ist bei beiden Ansätzen jeweils die Modellierung der zugrundeliegenden Abläufe erforderlich, sodass die rein statische Betrachtung der Objekte und Klassen nicht ausreichend ist, um logische Zusammenhänge zu ermitteln. Somit wird **Ziel 2 - Prozessorientierte Risikobetrachtung** im Rahmen des technischen Fokus der Ansätze jeweils teilweise erfüllt.

Li [L+11], Joshi [JVB07], Dehlinger [DD08] mit AADL Technologisch ein anderer Ansatz, der jedoch konzeptionell wiederum ähnlich ist zu den Ansätzen von Xiang und

Pai, wurde von Li [L+11] auf Basis von AADL Modellen vorgestellt. AADL dient dabei als Modellierungssprache zur Abbildung von Softwaresystemen aus Sicht der Architekturentwicklung, sodass damit Charakteristiken der Struktur, des Verhaltens und von Fehlern des zu entwickelnden Systems abgebildet werden können. In diesem werden im ersten Schritt zunächst notwendige Informationen aus dem zugrundeliegenden AADL Modell extrahiert und in dem Ansatz innerhalb einer strukturierten Datenbank zwischengespeichert. In dieser sind bereits Zusammenhänge der im Modell vorhandenen Komponenten hinterlegt, sodass ausgehend von einer Komponente, Pfade weiterverfolgt werden können die durch einen Ausfall dieser betroffen sind. Diese Datenbank wird im zweiten Schritt genutzt und ausgehend von einem dort gespeicherten Zustand einer Komponente mit einer Tiefensuche traversiert, sodass die dabei abgelaufenen Pfade unmittelbar für die Fehlerbaumerstellung genutzt werden. Der Ansatz von Joshi wurde prototypisch implementiert und nutzt zusätzlich zur Analyse das externe Softwarewerkzeug CAFTA [KG87], ermöglicht jedoch insgesamt keine Betrachtung von sequentiellen Abhängigkeiten von Komponenten [GH08]. In diesem Ansatz wird zunächst die zugrundeliegende Systemarchitektur als AADL Systemmodell, mit darin enthaltenen Systemkomponenten, Typen, Eigenschaften etc. spezifiziert. Darauf aufbauend wird ein Fehlermodell erstellt und dem Systemmodell annotiert, in welchem mögliche Fehler der Komponenten sowie deren Zusammenhänge und Auswirkungen auf andere Komponenten spezifiziert werden. Dies wird im Rahmen der weiteren Verarbeitung in das Zwischenformat eines gerichteten Graphen überführt, welcher als Grundlage für die rekursive Fehlerbaumerstellung anhand der Pfade im Graph dient. Der Ansatz von Dehlinger [DD08] baut auf dem zuvor genannten von Joshi auf, wobei vermehrt dynamische Aspekte bei der Fehlerbaumerstellung adressiert werden, sodass die Erstellung anderer Gates fokussiert wird. Der von Dehlinger vorgestellte Ansatz ist bisher jedoch nur ein Konzept, das auf Basis der Implementierungen und Vorarbeiten aus Joshi erstellt wurde. Die Ideen und Konzepte die im Ansatz von Dehlinger vorgestellt wurden, wurden bisher nicht umgesetzt, sodass **Ziel 4 - Unterstützende formalisierte Risikoanalyse** und **Ziel 6 - Softwareseitige Unterstützung** nach derzeitigem Stand, im Gegensatz zu den Ansätzen von Li und Joshi, jeweils nicht erfüllt werden. Jedoch werden teilweise Aspekte in Bezug auf zugrundeliegende Abläufe bzw. Verhalten des betrachteten Systems berücksichtigt, wodurch **Ziel 2 - Prozessorientierte Risikobetrachtung** teilweise erfüllt wird.

Papadopoulos [PM01], Tajarrod [LST09] mit Matlab-Simulink Die Ansätze von Papadopoulos [PM01] und Tajarrod [TLS08], [LST09] nutzen Matlab-Simulink zur Modellierung der dort betrachteten Systeme. Matlab-Simulink ist dabei gewählt worden, da dies einen verbreiteten Ansatz zur Modellierung und Simulation innerhalb der Anwendung von Systemen des Ingenieurwesens darstellt [TLS08, S. 630]. Als erstes wurde der Ansatz von Papadopoulos zur Erstellung von Fehlerbäumen anhand eines Matlab-Simulink Modells vorgestellt. In diesem Modell wird zunächst eine strukturelle, modulweise Systems-

pezifikation mit Simulink vorgenommen, bei der Module bzw. Komponenten des Systems hinsichtlich ihrer Ein- und Ausgaben miteinander verknüpft werden [Thu04]. Zur Unterstützung der entwickelten Methodik wurde zusätzlich ein Softwarewerkzeug entwickelt, mit dem der Ansatz mit Fokus auf die integrierte Analyse von Hard- und Softwaresystemen umgesetzt wurde. Innerhalb dieses Ansatzes werden im ersten Schritt (siehe Abbildung 2.13) mit Hilfe der Software Simulink von Mathworks, Matlab Modelle zur Beschreibung des adressierten programmierbaren Systems erstellt. Dieses Modell dient nach Abbildung 2.13 als Eingabe für das selbst entwickelte Softwarewerkzeug, wobei dabei das bestehende Modell nochmals mit zusätzlichen Informationen, beispielsweise über die Fehleranfälligkeit, angereichert wird. Das so angereicherte Modell wird mit einer Parser-Anwendung eingelesen und somit für die anschließende Erstellung von Fehlerbäumen bereitgestellt. Die Grobarchitektur und das beschriebene Vorgehen des Ansatzes wird in Abbildung 2.13 grafisch veranschaulicht. Für jedes in der Modellierung erstellte Modul wird eine Analyse durchgeführt, in der untersucht wird, ob und wie sich falsche Moduleingaben zu den Ausgaben fortpflanzen und welche Fehler im Modul entstehen können [Thu04]. Anhand der dabei entstehenden Pfade erfolgt die Erstellung der Fehlerbäume, welche im Dateiformat der Softwareanwendung Fault Tree Plus von Isograph, zur Analyse und Darstellung ausgegeben werden. Ausgehend vom zugrundeliegenden Modell beginnt auch der Ansatz von Tajarrod [TLS08], [LST09] damit das betrachtete Simulink-Modell, mit darin enthaltener Topologie des Systems und Komponenten und Subkomponenten, zu modellieren. Darüber hinaus wird manuell ein Top-Event bzw. eine Komponente innerhalb des Modells festgelegt von der ausgehend die Fehlerbaumerstellung startet. Das Vorgehen dabei erinnert an das der Zuverlässigkeitsblockdiagramme (siehe Abschnitt 2.2), bei der anhand der Topologie des Systems parallel oder sequentiell verknüpfte Komponenten bzw. Subkomponenten und entsprechender Pfade im System für die Fehlerbaumerstellung genutzt werden. Der Ansatz

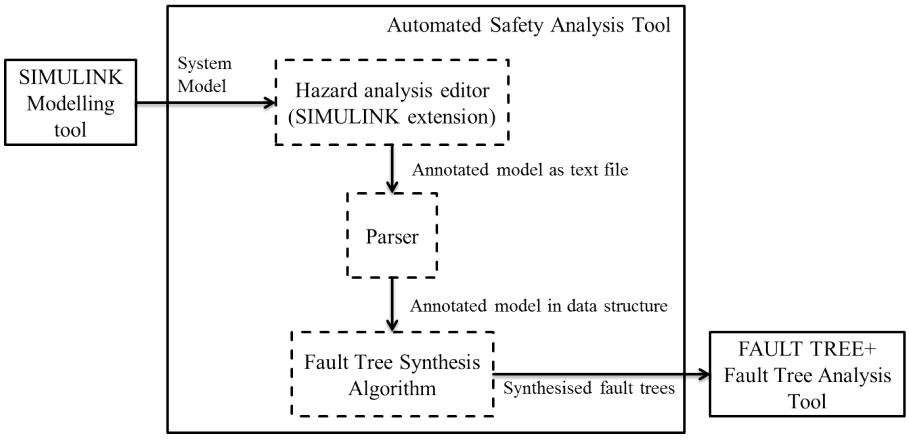

Abbildung 2.13: Architektur des Ansatzes von Papadopoulos [PM01]

wurde anhand eines Nitric Acid Cooler Systems (NAC) [LST09] bzw. eines Mission Avionics System (MAS) [TLS08], mit darin enthaltenen Komponenten zum Fahrzeugmanagement und verschiedenen Steuereinrichtungen etc., exemplarisch angewendet. Wie im klassischen Ansatz der Zuverlässigkeitsblockdiagramme, können jedoch kaum differenzierte Fehlerfälle betrachtet werden, sodass ausschließlich der Ausfall der Komponenten, entsprechend der Systemtopologie verknüpft, in den erstellten Fehlerbäumen aufgeführt werden kann.

Beide Ansätze sind umgesetzt worden, sodass **Ziel 4 - Unterstützende formalisierte Risikoanalyse** erfüllt wird. Darüber hinaus ist im Hinblick auf **Ziel 6 - Softwareseitige Unterstützung** der Ansatz von Tajarrod nicht auf die Anwendung externer Softwarepakete angewiesen, sodass dieses Ziel von Papadopoulos teilweise und von Tajarrod vollständig erfüllt wird. **Ziel 5 - Berücksichtigung risikomindernder Maßnahmen** wird von den Ansätzen jeweils nur teilweise erfüllt, da ausschließlich Änderungen der Systemtopologie, wie beispielsweise durch zusätzliche Redundanzen als Maßnahmen, berücksichtigt werden können. **Ziel 2 - Prozessorientierte Risikobetrachtung** wird ebenfalls teilweise erfüllt, da zwar im Rahmen der Systemtopologien Zusammenhänge der Komponenten bei der Ausführung betrachtet werden, jedoch nicht die Nutzung und Anwendung des Systems.

McKelvin [MEP+05] mit FTDF Als zugrundeliegendes Modell im Ansatz von McKelvin [MEP+05] wird die eigenentwickelte Modellierungssprache FTDF (Fault Tolerant Data Flow) verwendet, mit der im Rahmen hardwarenaher Anwendungsfälle physikalische Mikrocontroller, mit Informationen zu deren Ausführung sowie Verhalten im Fehlerfall, modelliert werden können. Darüber hinaus ist der Ansatz von McKelvin darauf ausgelegt, vorgenommene Arbeiten verifizieren zu können, sodass untersucht werden kann ob das modellierte Verhalten im Fehlerfall sowie berücksichtigte Toleranzen und Zeitaspekte innerhalb vorgegebener Grenzwerte liegen. Die automatische Erstellung von Fehlerbäumen auf Basis solcher Modelle dient dabei als Hilfsmittel derartiger Untersuchungen. Der vorgeschlagene Ansatz von McKelvin wird schematisch in Abbildung 2.14 dargestellt. Analog zu anderen vorgestellten Ansätzen wird dabei, im Hinblick auf die Struktur, Symbolik und Semantik der verwendeten Modellierungssprache, zunächst das zugrundeliegende Modell ausgewertet. Dabei wird zum einen eine Kontrollflussdarstellung, der FTDF-Graph, genutzt, um die Aufgaben einer Steuereinheit, wie beispielsweise die eines invertierten Pendels, zu beschreiben. Ergänzend wird als sogenannter Plattformgraph ein weiteres Modell erstellt, in welchem der verwendete Controller, mit darin enthaltenen Recheneinheiten (ECU) und Kommunikationskanälen (CH), spezifiziert wird. Diese Modelle werden in dem Ansatz zusammengeführt, sodass die Aufgaben entsprechenden Recheneinheiten und genutzten Kommunikationskanälen zugeordnet werden können. Anhand dieser Zuordnung bzw. des dabei entwickelten Modells, wird die Erstellung von Fehlerbäumen vorgenommen. Das gewünschte Top-Event wird dabei zunächst vom Nutzer selbst festgelegt, woraufhin rekursiv den modellierten Zusammenhängen im FTDF gefolgt wird. Dabei verwendete

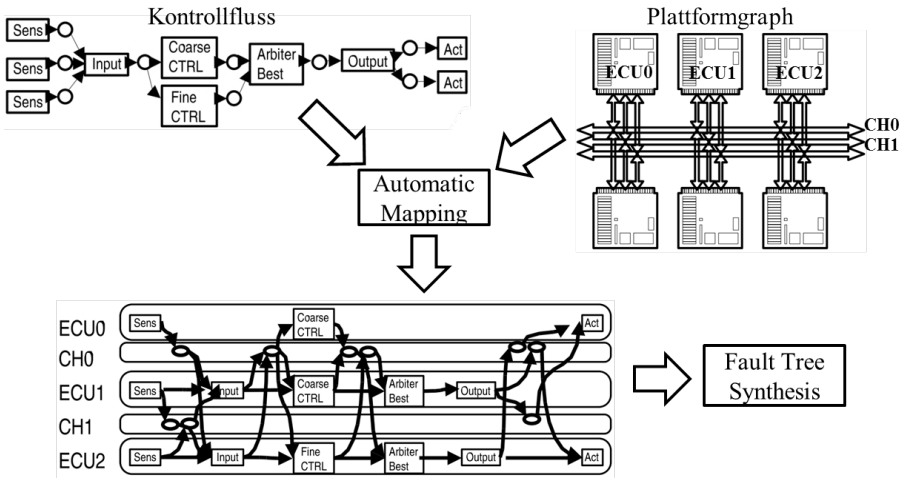

Abbildung 2.14: Schematische Darstellung des Ansatzes von McKelvin [MEP+05]

Hardware wie Recheneinheiten, Kommunikationskanäle, Aktuatoren oder Sensoren werden als Basic-Events im Fehlerbaum übernommen. Deren Zusammenhänge dienen, entsprechend der Aufgabenverteilung, der Erstellung von Gates im Fehlerbaum. Mit diesem Vorgehen können Fehlerbäume erstellt werden, jedoch wird dabei die Modellierung und Berücksichtigung zyklischer Abhängigkeiten nicht unterstützt [GMR11]. Für eine anschließende Auswertung der Fehlerbäume wird in diesem Ansatz auf externe Softwarepakete wie dem Item Toolkit [ITE14] zurückgegriffen. Die Bewertung der Zielerfüllung dieses Ansatzes ist damit analog zu Papadopoulos oder Lauer.

Rae [Rae04], [Rae07] mit hierarchischer Modellierung Im Rahmen der Dissertation von Rae [Rae07] wurde das Softwarewerkzeug „Eucalypt“ zur automatisierten Erstellung von Fehlerbäumen entwickelt. Dieses nutzt als Eingabe eine Reihe hierarchisch strukturierter Modelle, mit denen das jeweils betrachtete System beschrieben und somit das Systemmodell zusammengestellt wird. In diesem werden die Abläufe und das Verhalten der Systemkomponenten, wie beispielsweise Schalter oder Glühbirnen einer elektrischen Schaltung, abgebildet. Solche Elemente können wiederum als Subkomponente mit eigenem Verhalten und weiteren Subkomponenten abgebildet werden, sodass daraus ein hierarchisches Systemmodell entsteht. Mit der Modellierungssprache Communicating Sequential Processes (CSP) [H+85] wird in einer imperativen Sprache somit eine Systemtopologie, wie in Abbildung 2.15 schematisch dargestellt, modelliert. Darüber hinaus wird das mögliche Fehlverhalten einer Komponente spezifiziert, sodass ein Schalter beispielsweise in Ein- oder Aus-Position verklemmt sein kann. Die Erstellung von Fehlerbäumen beginnt nach Abschluss der Modellierung mit der höchsten Hierarchieebene des Modells. Anhand dieser wird das Top-Event festgelegt, woraufhin jede der Subkomponenten und demnach jede

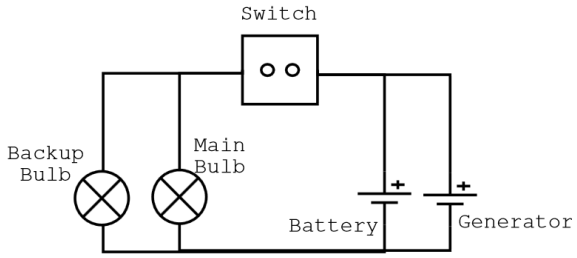

Abbildung 2.15: Anwendungsbeispiel einer elektrischen Schaltung nach Rae [Rae04]

weitere Hierarchiestufe, als Or-Gate sowie jedes darin beschriebene Fehlverhalten der Subkomponente darunterliegend als And-Gate abgebildet wird. Fortlaufend werden auf diese Weise modellierte Fehler der hierarchisch untergeordneten Modelle miteinander verknüpft, wie schematisch in Abbildung 2.16 dargestellt, und dadurch die Fehlerbaumstruktur aufgebaut. Bisherige Anwendungsfälle für den vorgestellten Ansatz sind marine Waffensysteme, Robotik und das Signalsystem eines Bahnübergangs, woran zu sehen ist das überwiegend technische Systeme betrachtet wurden. Darüber hinaus erfordert der Ansatz durch die Nutzung von CSP eine umfangreiche textuelle Beschreibung des Systems als Prozessalgebra. Beim weiteren Ansatz werden zwar somit das Verhalten und die Abläufe des Systems festgelegt, jedoch hat dies kaum Einfluss auf das weitere Vorgehen der Fehlerbaumerstellung und Analyse. Vielmehr werden dafür die hierarchischen Zusammenhänge genutzt, sodass mögliche Änderungen der Abläufe mit den selben Komponenten und hierarchischen Beziehungen keinen Einfluss auf die Fehlerbäume und somit Analyse haben. Der vorgestellte Ansatz von Rae erfüllt somit zusammenfassend nur die Zieldefinitionen nach **Ziel 4 - Unterstützende formalisierte Risikoanalyse** und **Ziel 6 - Softwareseitige Unterstützung**.

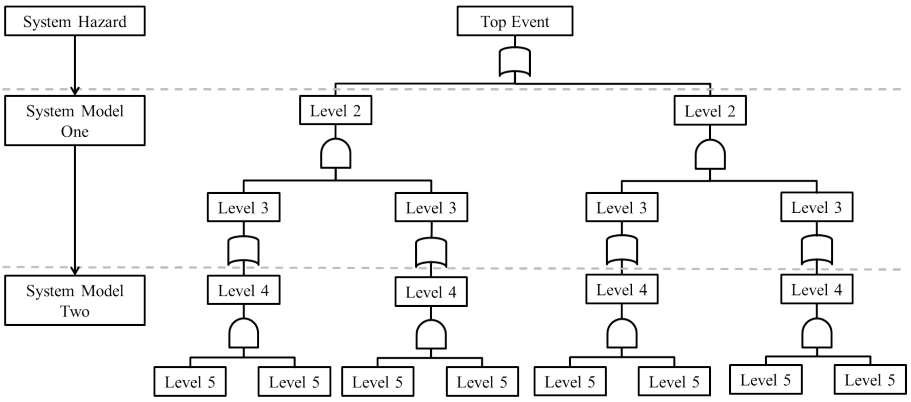

Abbildung 2.16: Schematischer Zusammenhang der hierarchischen Modelle mit daraus resultierendem Fehlerbaum nach Rae [Rae04]

Diskussion und Zusammenfassung Zusammenfassend kann anhand von Tabelle 2.17 eingesehen werden, dass bisher keiner der aufgeführten Ansätze die aufgestellten Zieldefinitionen dieser Ausarbeitung vollständig erfüllt, was gleichzeitig Handlungsbedarf für einen eigenen Lösungsansatz aufzeigt. Aufgrund der Tatsache, dass die identifizierten Ansätze vollständig Gebrauch von der Fehlerbaumanalyse machen sowie die dafür notwendigen Informationen zuvor in einem Modell formalisiert wurden, kann jeder Ansatz jeweils zu einer Verbesserung der Transparenz beitragen und führt jeweils zu einer Zielerfüllung von **Ziel 1 - Formalisierung des Basiswissens**. Erstellte Fehlerbäume werden über Namen und Beschreibungen der Fehlerbaumelemente semantisch mit dem zugrundeliegenden Modell verknüpft, sodass beispielsweise ein Fehlerbaumelement nach einem Modellelement benannt wird, was zusätzlich die Transparenz sowie die Wiedererkennung und den weiteren Verlauf des Entwicklungsprozesses verbessert [Che10], [LST09], [JVB07]. Jedoch sind durch die meisten Ansätze zusätzliche Aufwände notwendig, sodass ein weiterer Entwicklungsschritt erforderlich wird [Jun12].

	Ziel 1 - Formalisierung des Basiswissens	Ziel 2 - Prozessorientierte Risikobetrachtung	Ziel 3 - Wiederverwendbare Informationen	Ziel 4 - Unterstützende formalisierte Risikoanalyse	Ziel 5 - Berücksichtigung risikomindernder Maßnahmen	Ziel 6 - Softwareseitige Unterstützung
Chen	X	(X)		X	(X)	X
Xiang	X	(X)		X	(X)	X
Pai	X	(X)		X	(X)	
Lauer	X	(X)		X	(X)	(X)
Li	X	(X)		X	(X)	X
Dehlinger	X	(X)			(X)	
Joshi	X	(X)		X	(X)	X
Papadopoulos	X	(X)		X	(X)	(X)
Tajarrod	X	(X)		X	(X)	X
McKelvin	X	(X)		X	(X)	(X)
Rae	X			X	(X)	X

Abbildung 2.17: Einordnung der Ansätze zur automatischen Erstellung von Fehlerbäumen zur Risikoanalyse

Betrachtet man **Ziel 2 - Prozessorientierte Risikobetrachtung**, fällt auf, dass in vielen Ansätzen in unterschiedlicher Form eine Berücksichtigung der Abläufe erforderlich ist, um Fehlerbäume überhaupt erstellen zu können. Im Fokus liegen jedoch überwiegend technische Systeme und daher vermehrt Aspekte wie Komponenten, Designs, Architekturen etc. und selten auf der Untersuchung der Prozesse selbst. Im Ansatz von Chen dient explizit

ein Prozessmodell als Grundlage, welches jedoch nur mit Hilfe vordefinierter Strukturmuster für die Risikoanalyse durch Fehlerbäume verwendet werden kann. Somit ist kaum eine Betrachtung von tätigkeitsspezifischen Gefährdungen möglich, da ausschließlich die Strukturen des Prozesses betrachtet werden. Zumeist wird bei den Ansätzen das funktionale Verhalten der jeweiligen Anwendungsfälle abgebildet [Jun12], wohingegen mit der Fehlerbaumanalyse explizit auch menschliches Verhalten mit abgebildet werden kann und auch sollte [Stä11], [Lev95].

Im Hinblick auf **Ziel 3 - Wiederverwendbare Informationen** erfüllt und adressiert keiner der aufgeführten Ansätze diese Zieldefinition. Wohingegen Lauer [LGP11, S. 7] in seinem Ansatz jedoch weiteren Forschungsbedarf hinsichtlich der Verbesserung der Wiederverwendbarkeit erkannt hat. Technologisch ist dafür zumindest der erste Schritt getan, indem die Ansätze ausnahmslos notwendiges Wissen strukturiert in Form verschiedener Modellierungssprachen formalisieren. Zusätzlich sind bereits, wenn auch nicht zur Verbesserung der Wiederverwendbarkeit, innerhalb der Ansätze Technologien mit Potential für eine verbesserte Wiederverwendbarkeit, wie beispielsweise Datenbanken, eingesetzt worden [L+11].

Eine automatisierte Analyse nach **Ziel 4 - Unterstützende formalisierte Risikoanalyse** wird von der überwiegenden Anzahl der vorgestellten Ansätze erfüllt, sodass diese jeweils Algorithmen oder ausimplementierte Lösungsansätze vorgestellt haben. Eine Ausnahme stellt hier der Ansatz von [DD08] dar, in welchem ausschließlich Ideen und ein Konzept beschrieben wurden.

Die Zieldefinition nach **Ziel 5 - Berücksichtigung risikomindernder Maßnahmen** wurde von keinem der Ansätze explizit erfüllt, sodass risikomindernde Maßnahmen ausschließlich im Rahmen von Änderungen des zugrundeliegenden Modells und Designalternativen abgebildet werden können. Eine vollständige Zielerfüllung wäre möglich, wenn explizit risikomindernde Maßnahmen im Ansatz mit eingebracht und berücksichtigt werden. Zwar können jeweils Änderungen des zugrundeliegenden Modells in der Fehlerbaumerstellung und anschließenden Analyse bemerkt und abgebildet werden, jedoch ist dies inhärent durch ein modellbasiertes Vorgehen gegeben und somit nicht ausreichend für eine vollständige Zielerfüllung.

Softwareseitige Unterstützung wird von der überwiegenden Anzahl der dargestellten Ansätze ermöglicht, sodass Ansätze wie [Che10] oder [LST09] vollständig implementiert und ausgewertet wurden. Hingegen sind auch Ansätze identifiziert worden, in denen zwar Implementierungsarbeiten vorgenommen wurden, jedoch keine zentrale softwareseitige Unterstützung ermöglicht wird. Dies führt durch die starke Verteilung von Informationen und Verarbeitungsschritte auf verschiedene Softwarewerkzeuge, nach Tabelle 2.17 zu einer teilweisen Erfüllung nach **Ziel 6 - Softwareseitige Unterstützung**.

Abgesehen vom betrachteten Grad der Zielerfüllung fällt auf, dass einige der An-

sätze nach einer ähnlichen Methodik vorgehen. Ein wesentlicher Unterschied zwischen den Ansätzen stellen dabei die unterschiedlichen Modelle dar, von denen aus der jeweils vorgestellte Ansatz beginnt [LST09]. Die zugrundeliegende Modellierungssprache wird dabei im Hinblick auf die betrachteten Anwendungsfälle, beispielsweise Architekturentwicklung ([L+11],[JVB07], [DD08]), Softwareentwicklung ([PD02], [LGP11]), Systementwicklung ([X+11], [X+10]) etc. sowie der Zielgruppe, beispielsweise IT-Ingenieure [X+11], Sicherheitsingenieure[L+11] etc., für die Nutzung des Ansatzes sorgfältig ausgewählt. Als einziger Ansatz der Abläufe des Anwendungsfalls, wie sie ähnlich auch bei Gefährdungsbeurteilungen betrachtet werden, mit Hilfe von Prozessmodellen beschreibt, wurde der von Chen [Che10], [CACO06] identifiziert. Dieser kann jedoch nur entsprechende Strukturinformationen mit Hilfe vordefinierter Regeln auswerten, wodurch jedoch keine direkt aus den Prozessschritten, über die Regeln hinaus, bestehenden Gefährdungen abgebildet werden können. Somit ist mit diesem Ansatz keine Unterstützung von mehreren Fehlerzuständen bzw. Ursachen eines Schrittes möglich [PBM+08].

Innerhalb der Ansätze werden, nachdem eine entsprechende Modellierungssprache ausgewählt wurde und die notwendigen Informationen in einem Modell abgebildet wurden, die für die Erstellung von Fehlerbäumen relevanten Informationen extrahiert und teilweise zwischengespeichert. Im Rahmen des automatisierten Vorgehens werden daraufhin Fehlerbäume erstellt, die der jeweilige Anwender sodann auswerten und interpretieren kann. Auffallend ist, dass mit den Ansätzen automatisiert erstellte Fehlerbäume von denen manuell erstellter abweichen [Rae04, S. 291], sodass als Ergebnis beispielsweise nur „flache“ Fehlerbäume erstellt werden können [Thu04, S. 68]. Darüber hinaus können kaum Sequenzen von Aktionen in der Fehlerbaumerstellung berücksichtigt werden, sodass der Anwendungsbereich der genannten Ansätze bisher begrenzt ist [KLFL11].

Als weiteres wurde als weiterer Handlungsbedarf im Rahmen der automatisierten Erstellung von Fehlerbäumen identifiziert, dass das eingepflegte und strukturierte Wissen auch wiederverwendet werden können soll [LGP11, S. 7]. Dies ist zusätzlich Bestandteil dieser Ausarbeitung, sodass die verwandten Arbeiten dazu im folgenden Abschnitt dargestellt werden.

2.3.2 Wiederverwendbarkeit von Analysen und Bewertungen

Im vorangegangenen Abschnitt wurden Ansätze betrachtet, die sich mit der Automatisierung von Risikoanalysen beschäftigen. Für diese wurde jeweils eingeordnet, inwiefern diese die Zieldefinitionen dieser Ausarbeitung erfüllen oder nicht-erfüllen. Bei den dort vorgestellten Ansätzen wird im Wesentlichen dem automatisierten Ansatz eine entsprechende Modellstruktur zugrunde gelegt, in der jeweils die Informationen des Anwendungsfalls strukturiert hinterlegt werden. Betrachtet man wiederum das aktuelle Vorgehen bei der Erstellung von Gefährdungsbeurteilungen, wird derartiges Wissen informell beschrieben. Für beide Lösungswege ist Aufwand in Form von Zeit und Kosten erforderlich, um

zum einen die textuelle Beschreibung und zum anderen, die Modellierung vorzunehmen. Dabei gewinnt der jeweilige Nutzer bei der Durchführung an Erfahrung, die bei weiteren Anwendungsfällen eingebracht werden kann und wird. Jedoch werden auch bestehende Dokumente wiederverwendet, beispielsweise über das kopieren und wieder-einfügen (copy-paste), welches das etablierte Verfahren zur Wiederverwendung darstellt, bei dem jedoch das Risiko unzureichender und falscher Wiederverwendung besteht [Kel99], [SH02]. Im Rahmen dieses Abschnitts werden Ansätze untersucht, die eine systematische Wiederverwendbarkeit ermöglichen, was von den im vorangegangenen Abschnitt erläuterten Ansätzen kaum adressiert wird. Die als mit diesem Fokus identifizierten Ansätze werden nachfolgend zusammenfassend gelistet und erläutert:

- Dokas [DI07]
- Dehlinger [DL06]
- Ebrahimipour [ERS10]
- Gomez [GLS10]
- Carter [CS06]

Dokas [DI07] Ein Ansatz, um das in die Fehlerbaumanalyse eingebrachte Wissen wiederverwenden und einfacher zwischen verschiedenen Stakeholdern austauschen zu können, wurde von Dokas [DI07] vorgestellt. Damit dieses Ziel erreicht werden konnte, wurde eine Möglichkeit genutzt dieses Wissen strukturiert zu speichern. Für diesen Zweck sind Ontologien verwendet worden, da sich diese für den Einsatz als wissensbasierte Systeme eignen [DI07]. Damit die Informationen eines Fehlerbaumes in dieser Ontologie abgebildet werden konnten, wurde als Hauptbestandteil des Ansatzes eine entsprechende Klassenstruktur, wie in Abbildung 2.18 dargestellt, in der Ontologie entwickelt, welche die Fehlerbaumelemente sowie erlaubte Eigenschaften von Events und Gates nachbildet. Nach Abschluss dieser Strukturierung konnte diese Ontologie mit Informationen der Fehlerbäume, wie Namen und Beschreibungen sowie auch logische Verknüpfungen durch die Gates abgebildet werden. Dies wurde Anhand des Anwendungsfalls einer Materialrückgewinnungsanlage und dafür manuell erstellten Fehlerbäumen durchgeführt. Mit dem Ansatz wurde gezeigt, dass grundsätzlich eine Abbildung von Zusammenhängen und Informationen eines Fehlerbaumes in Form vom Ontologien ermöglicht werden kann. Offen blieb in dem Ansatz jedoch, wie dieses Wissen gezielt wieder bereitgestellt werden kann. Weiterhin wurde in dem Ansatz nur ein manuelles Befüllen der Ontologie betrachtet, sodass sowohl Fehlerbäume als auch deren Abbild in der Ontologie manuell entwickelt wurden. Die auf diese Weise in die Ontologie eingetragenen Informationen konnten zusätzlich erweitert werden, sodass auch Informationen einer durchgeführten FMEA genutzt werden konnten, was jedoch wiederum nur durch ein manuelles Vorgehen umgesetzt wurde. Die Wiederverwendbarkeit nach **Ziel**

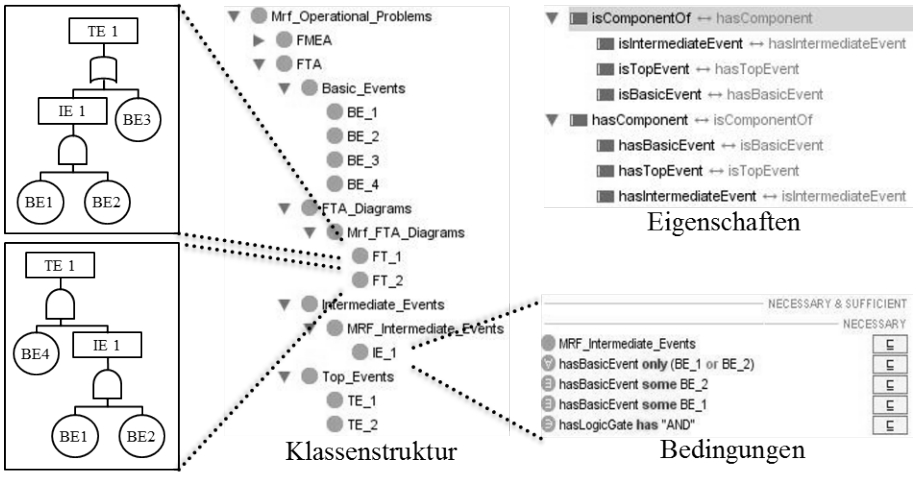

Abbildung 2.18: Auszug der entwickelten Ontologie zur Abbildung von Fehlerbäumen nach Dokas [DI07]

3 - Wiederverwendbare Informationen ist in diesem Ansatz daher teilweise erfüllt, da zwar Fehlerbäume zum Befüllen der Ontologie verwendet werden können, jedoch dies nur in qualitativer Hinsicht ermöglicht sowie eine gezielte Bereitstellung oder automatisierte Einbringung des Wissens kaum adressiert wird. Darüber hinaus wird die Zielerfüllung nach **Ziel 6 - Softwareseitige Unterstützung** ebenfalls mit teilweise bewertet, da der Ansatz auf die Strukturierung innerhalb der Ontologie fokussiert, jedoch das Einpflegen sowie Verwenden der Daten softwareseitig nur begrenzt berücksichtigt wird.

Dehlinger [DL06] Ein weiterer Ansatz zur Verbesserung der Wiederverwendbarkeit wurden von Dehlinger [DL06] vorgestellt. Dieser Ansatz adressiert dabei die Wiederverwendbarkeit innerhalb von Produktlinien für Softwaresysteme, um dabei im Entwicklungsprozess beteiligte Softwareingenieure mit dem entwickelten Softwarewerkzeug PLFaultCAT (Product-Line Fault Tree Creation and Analysis Tool) zu unterstützen. Dieses Softwarewerkzeug baut auf dem quellenoffenen Werkzeug FaultCAT [Bur04] auf und wird für die Visualisierung erstellter Fehlerbäume für eine Produktlinie genutzt. Der entwickelte Ansatz gliedert sich, wie in Abbildung 2.19 schematisch dargestellt, grob in die beiden Phasen Domain Engineering und Application Engineering, wobei durch den Ansatz überwiegend die Phase Application Engineering adressiert wird [DL06, S. 170]. Durch die Phase Domain Engineering wird der entwickelte Ansatz in den Entwicklungsprozess einer Produktlinie eingebettet, sodass diese Phase vollständig manuell durchgeführt wird und zunächst mit der Ermittlung von Anforderungen an die neue Produktlinie beginnt. Darauffolgend werden in Form der Commonality and Variability Analysis sowohl Gemeinsamkeiten als auch mögliche Unterschiede von zu entwickelnden Produkten innerhalb der Produktlinie

festgelegt. Auf Basis dieser Informationen sowie nebenläufigen Untersuchungen möglicher Gefährdungen und Ursachen der Produktlinie beispielsweise durch FMEA, werden manuell Fehlerbäume dieser Produktlinie erstellt. Jedes der in diesen Fehlerbäumen enthaltenen Basic Events wird dabei manuell den festgelegten Gemeinsamkeiten bzw. Unterschieden der Produktlinie zugeordnet. Die resultierenden Fehlerbäume dienen als Eingabe für die Phase Application Engineering, in welcher die zu entwickelnden Produkte innerhalb der Produktlinie betrachtet werden. Exemplarisch kann dabei die Produktlinie einer Wetterstation betrachtet werden, mit den beiden Produkten Wetterstation A und Wetterstation B die zwar sämtliche Gemeinsamkeiten der spezifizierten Produktlinie umfassen, sich jedoch in spezifischen Features unterscheiden. Wetterstation A verfügt dabei beispielsweise über mehrere Windsensoren, wohingegen Wetterstation B stattdessen über einen Not-Aus-Schalter verfügt. Diese Unterschiede und Gemeinsamkeiten werden für diese Produkte im ersten Schritt des Application Engineering erneut manuell zugeordnet. Daraufhin erfolgt die Erstellung von Fehlerbäumen für diese Produkte, wobei im Wesentlichen der zuvor manuell erstellte Fehlerbaum der Produktlinie genutzt wird. Dieser wird anschließend um nicht-relevante Zweige reduziert, sodass beispielsweise Zweige im Zusammenhang mit im Produkt A nicht enthaltenen Features wie Not-Aus-Schalter im Fehlerbaum automatisch entfernt werden.

Die Zielerfüllung nach **Ziel 1 - Formalisierung des Basiswissens** ist in dem Ansatz teilweise gegeben, da zunächst in dem Ansatz einige der notwendigen Informationen einer Produktlinie dokumentiert werden müssen, sodass darüber Gemeinsamkeiten und Unterschiede von Produkten ermittelt werden können. Dies stellt jedoch ein manuelles Vorgehen

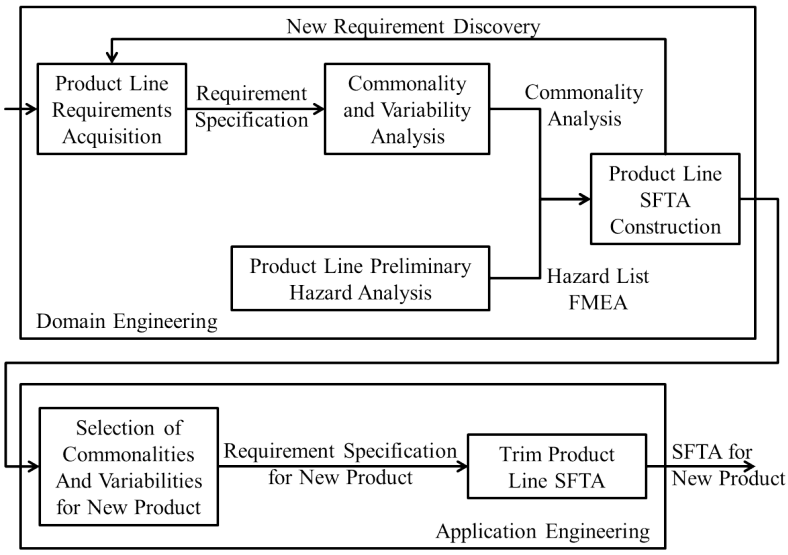

Abbildung 2.19: Schematischer Ablauf des Lösungsansatzes nach Dehlinger [DL06]

dar, in welchem das Basiswissen wiederum informell genutzt wird. **Ziel 3 - Wiederverwendbare Informationen** wird zudem durch den erläuterten Ansatz auch teilweise erfüllt, da die genutzten Fehlerbäume nur im Rahmen von Produkten einer Produktlinie und nicht über Produktlinien hinweg verwendet werden können. Außerdem bleibt offen, inwiefern sich das Vorgehen auf die qualitative und quantitative Analyse sowie deren Wiederverwendung auswirkt und wie die gezielte Bereitstellung des Wissens ausgestaltet wird. Ein Softwarewerkzeug nach **Ziel 6 - Softwareseitige Unterstützung** ist in dem Ansatz implementiert und vorgestellt worden, wodurch dieses Ziel vollständig erfüllt wird. Da zwar im Ansatz innerhalb des Softwarewerkzeugs die Analyse bereits erstellter Fehlerbäume vorgenommen werden kann, jedoch nicht die Erstellung wie in Ansätzen des vorangegangenen Abschnitts automatisiert wird, wird die Zielerfüllung nach **Ziel 4 - Unterstützende formalisierte Risikoanalyse** als teilweise bewertet.

Ebrahimipour [ERS10] Im Gegensatz zum vorherigen Ansatz, wird im Ansatz von Ebrahimipour [ERS10] die Wiederverwendung von Wissen aus einer FMEA betrachtet. In FMEAs wird bisher das für die Risikoanalyse und -bewertung ermittelte Wissen informell in tabellarischer Form dokumentiert und ausgewertet. Durch diese Form der Dokumentation ist eine automatisierte, computergestützte Auswertung nur begrenzt möglich [ERS10]. Daher wird durch den Ansatz eine Modellierung in Form von Ontologien vorgeschlagen, um das vormals informell dokumentierte Wissen strukturiert in Form von Ontologien zu modellieren. Als Werkzeug wird dafür die von der Stanford University entwickelte Software Protègè zur Modellierung der Ontologien verwendet. In dem vorgeschlagenen Ansatz wird zunächst eine Klassenstruktur innerhalb einer Ontologie erstellt, um das Wissen was zuvor textuell erfasst wurde, manuell in die Ontologie übertragen zu können. Die Klassenstruktur richtet sich dabei nach den Zusammenhängen des in Tabellen der FMEA enthaltenen Wissens, sodass entsprechend Klassen zur Abbildung von Aktivitäten sowie von möglichen Ursachen für Gefährdungen in der Ontologie erstellt wurden. Durch diese vorgenommene Strukturierung sollen so die Zusammenhänge des zu untersuchenden Systems und möglichen Gefährdungen und Ursachen in der Ontologie hergestellt werden. Um dieses Wissen wiederverwenden zu können wird die Nutzung von Anfragesprachen wie KIF und JTP vorgeschlagen, sodass mit Hilfe von textuellen Anfragen gezielt Wissen innerhalb der Ontologie gefiltert und selektiert werden kann, was in herkömmlichen Formen der Dokumentation von FMEAs kaum möglich ist.

Der Ansatz unterstützt jedoch nicht bei der Entwicklung dieser Anfragen, sodass diese manuell und individuell vom jeweiligen Nutzer entwickelt werden müssen, was tiefes technisches Verständnis erfordert. Darüber hinaus wird auch das befüllen der Ontologie kaum unterstützt, sodass der Ansatz zunächst einen hohen manuellen Mehraufwand im Vergleich zum bisherigen Vorgehen erfordert. Aufgrund des erheblichen manuellen Aufwandes bei diesem Ansatz sowie fehlender quantitativen Informationen, softwareseitiger

Unterstützung, oder Bereitstellung des Wissens in dem Ansatz, wird zusammenfassend ausschließlich die Zielerfüllung nach **Ziel 3 - Wiederverwendbare Informationen** als teilweise erfüllt bewertet.

Gomez [GLS10] Im Kontrast zum Ansatz zur Wiederverwendbarkeit innerhalb von Produktlinien, wird in Gomez [GLS10] ein alternatives Vorgehen vorgeschlagen. Im Fokus liegen dabei Anwendungsfälle für die Entwicklung eingebetteter Systeme, sodass bei der Entwicklung für ein jeweiliges System eine entsprechende Spezifikation ausgearbeitet wird (`Embedded System Specification`). Diese dient, wie in Abbildung 2.20 dargestellt, in dem Ansatz als Grundlage, um aus dieser die zur Fehlerbaumanalyse relevanten Informationen zu filtern und in einem selbstentwickelten Zwischenmodell (`Intermediate Model`), das als Wissensbasis dient, zu speichern. Das Intermediate Model (IM) eines Systems besteht dabei aus den jeweiligen IMs der einzelnen Komponenten. Innerhalb eines IMs wird unterteilt in Component Information und Dependability Information. Als `Component Information` werden Inhalte, Strukturen, Verhalten und Funktionalität einer Komponente beispielsweise mit Hilfe von UML State Charts, textueller Funktionsbeschreibung, Komponentendiagramme oder Baumdiagramme der Komponentenstruktur dokumentiert. Als `Dependability Information` werden sicherheits- und zuverlässigkeitsrelevante Informationen wie identifizierte Gefährdungen und Ursachen sowie die Arbeitsbedingungen einer Komponente dokumentiert. In der `Fault Tree Analysis Specification` werden Informationen für die durchzuführende Fehlerbaumanalyse spezifiziert, sodass beispielsweise das Top-Event anhand einer im Intermediate Model hinterlegten Gefährdung sowie zu betrachtende Komponenten und Subkomponenten festgelegt werden. Nachdem diese Arbeiten durchgeführt wurden, können darauf aufbauend, anhand der vorgenommenen Spezifikationen und Informationen, Fehlerbäume für jede betrachtete Komponente erstellt werden. Exemplarisch wurden in dem Ansatz bereits notwendige Informationen der Komponente Gasturbine SGT 500 eines Ventilationssystems eingepflegt. Soll der Ansatz nun für eine

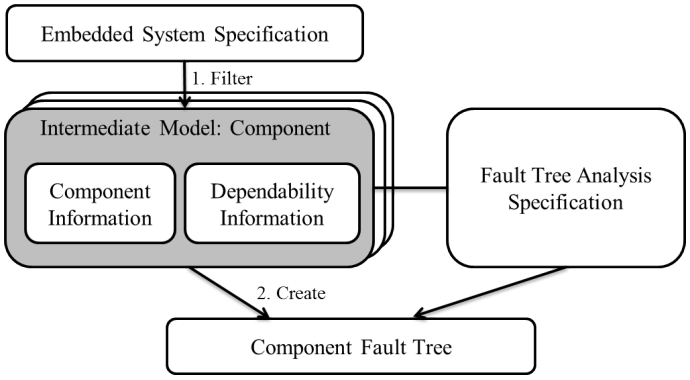

Abbildung 2.20: Schematischer Ablauf des Lösungsansatzes nach Gomez [GLS10]

neue Komponente Gasturbine SGT 400 der selben Produktfamilie angewendet werden, so sollen möglichst viele Informationen anderer Komponenten zur Wiederverwendung genutzt werden. Damit die neue Komponente betrachtet werden kann, muss für diese zunächst ein neues IM erstellt werden. Andere Komponenten des Systems sollen dabei als Orientierungshilfe für die manuelle Suche beispielsweise möglicher Ursachen von Gefährdungen dienen, wobei jedoch wiederum ähnlich wie im Ansatz von Dehlinger [DL06] eine Analyse von Gemeinsamkeiten und Unterschieden (Commonality and Variability) erforderlich ist. Dabei als relevant identifizierte Component und Dependability Informationen sowie auch die FTA Specification können dann übernommen und für die neue Komponente angepasst werden.

Wie am Beispiel zu sehen, adressiert der Ansatz ebenfalls eine Form der Wiederverwendbarkeit innerhalb von Produktlinien, wobei im Kontrast zum Ansatz von Dehlinger [DL06] eine stärker strukturierte und umfangreichere Wissensbasis in Form des Intermediate Model genutzt wird. Darüber hinaus erscheint jedoch der Ansatz von Gomez weniger ausgereift zu sein, sodass eine softwareseitige Unterstützung kaum enthalten ist und somit der manuelle Aufwand weiterhin hoch bleibt. Die im Rahmen des Ansatzes fokussierte Art der Wiederverwendung umfasst somit die Zieldefinition nach **Ziel 3 - Wiederverwendbare Informationen** nur teilweise, da sowohl die Speicherung als auch Bereitstellung von Informationen nur wenig unterstützt wird. Weiterhin wird **Ziel 1 - Formalisierung des Basiswissens** teilweise erfüllt, da zugrundeliegende Informationen umfassend und strukturiert in das Vorgehen einbezogen werden.

Carter [CS06] Zur Verbesserung der Identifikation von Gefährdungen in Konstruktionsprojekten wurde von Carter [CS06] ein Ansatz entwickelt und vorgestellt. In diesem wird versucht Risikoaspekte bereits bei der Planung von Konstruktionsprojekten einzubringen. Für diesen Zweck wurde das Softwarewerkzeug Total-Safety entwickelt und in [CS06] vorgestellt, welches als softwareseitige Unterstützung bei der Planung von Konstruktionsprojekten verstanden werden kann. Dieses Werkzeug entspricht im Wesentlichen einer Webseite mit verschiedenen Formulareingaben durch die man schrittweise geführt wird. Innerhalb eines vorgegebenen Vorgehens fügt der Benutzer von Total-Safety so, im Rahmen verschiedener Formulareingaben wie in Abbildung 2.21 gezeigt, Informationen über das geplante Projekt ein, wie beispielsweise im Projekt stattfindende Tätigkeiten wie „Zement verdichten“ oder genutzte Ressourcen wie „Kipplaster“. Über weitere Formblätter können im Vorgehen, ähnlich wie in Abbildung 2.21 dargestellt, auch Informationen über mögliche Gefährdungen, Ursachen, Schadensfolgen und risikomindernde Maßnahmen eingetragen werden. Technologisch liegt diesem Vorgehen dabei eine Datenbank zugrunde, in welcher die auf diese Weise eingepflegten Informationen gespeichert werden. Weiterhin werden diese Informationen innerhalb des Ansatzes bereitgestellt und unterbreiten dem Nutzer somit Vorschläge auf Basis des vorhandenen Wissens aus der Datenbank. Darüber hinaus dienen die eingepflegten Informationen als Grundlage für eine Risikoanalyse nach dem in

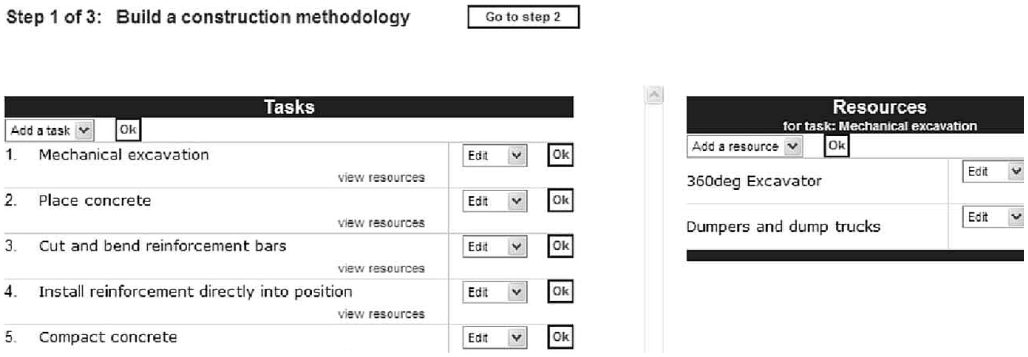

Abbildung 2.21: Screenshot des ersten Formblattes zur Eingabe von Tätigkeiten und Ressourcen nach Carter [CS06]

Kapitel 2.1 beschriebenen klassischen Vorgehen. Eine verbesserte Transparenz von Gefährdungsbeurteilungen kann mit diesem Ansatz durch wenige Zusammenhänge der Informationen untereinander, wie beispielsweise zwischen Tätigkeiten und Gefährdungen, zwar nicht erreicht werden, jedoch können eingepflegte Informationen mit Hilfe des entwickelten Softwarewerkzeugs in Teilen wiederverwendet werden. Dies führt daher zu einer teilweisen Zielerfüllung von **Ziel 3 - Wiederverwendbare Informationen** sowie vollständigen Zielerfüllung nach **Ziel 6 - Softwareseitige Unterstützung**. Hingegen wird **Ziel 4 - Unterstützende formalisierte Risikoanalyse** teilweise erfüllt, sodass die Berechnung selbst automatisiert mit dem Softwarewerkzeug vorgenommen werden kann, jedoch die notwendigen Informationen dafür weiterhin vollständig manuell eingepflegt werden müssen und keine formalisiertere Form als nach dem bisherigen Vorgehen wie in Abschnitt 2.1 möglich ist. Zusätzlich werden risikomindernde Maßnahmen grundsätzlich in den Ansatz mit einbezogen, jedoch besteht dort weiterhin die Problemstellung, analog zum Stand der Technik, der zu geringen Vernetzung und Transparenz dieser, sodass **Ziel 5 - Berücksichtigung risikomindernder Maßnahmen** teilweise erfüllt wird.

Diskussion und Zusammenfassung In Abbildung 2.22 werden die zuvor erläuterten Ansätze nochmals hinsichtlich ihrer Zielerfüllung zusammengefasst dargestellt. Ergänzend dazu ist zu vermerken, dass für das strukturierte Speichern und wieder Abrufen von Informationen verschiedenen Technologien, wie beispielsweise Datenbanken [CS06] und Ontologien [DI07], genutzt werden. Weiterhin nutzen jedoch auch Ansätze eigene Entwicklungen dafür [GLS10], wobei im Kern die genannten Ansätze ganzheitlich eine Möglichkeit nutzen das notwendige Wissen strukturiert zu speichern, um dieses später wiederum filtern und auslesen zu können. Die Ansätze von Dehlinger und Gomez tragen, über die Wiederverwendbarkeit hinaus, indirekt auch zu einer Verbesserung der Transparenz bei, indem innerhalb dieser Ansätze die bereits beschriebene Technik der Fehlerbaumanalyse verwendet wird. Weiterhin unterscheiden sich die genannten Ansätze durch die Fokussie-

rung verschiedener Techniken, wie auf FMEA [ERS10] oder FTA [DL06], [GLS10] sowie dahingehend ob und wie ausgeprägt eine entsprechende softwareseitige Unterstützung innerhalb des Ansatzes ermöglicht wird. Zusammenfassend erfüllt keiner der aufgeführten

	Ziel 1 - Formalisierung des Basiswissens	Ziel 2 - Prozessorientierte Risikobetrachtung	Ziel 3 - Wiederverwendbare Informationen	Ziel 4 - Unterstützende formalisierte Risikoanalyse	Ziel 5 - Berücksichtigung risikomindernder Maßnahmen	Ziel 6 - Softwareseitige Unterstützung
Dokas			(X)			(X)
Dehlinger	(X)		(X)	(X)		X
Ebrahimipour			(X)			
Gomez	(X)		(X)			
Carter			(X)	(X)	(X)	X

Abbildung 2.22: Einordnung der Ansätze fokussiert auf den Aspekt der Wiederverwendbarkeit von Risikoanalysen

Ansätze die Zieldefinitionen dieser Ausarbeitung vollständig. Die Ansätze sind hinsichtlich ihrer Anwendungsfälle und ihres Vorgehens teilweise auf den Einsatz in ihrer Domäne beschränkt, sodass für den Ansatz beispielsweise eine Spezifikation eines zu entwickelnden eingebetteten Systems [GLS10] oder eine Beschreibung der Produktlinie [DL06] erforderlich ist. Der Ansatz von Ebrahimipour ist davon zwar weitgehend unabhängig, ermöglicht im Kern jedoch nur eine alternative zur textuellen Beschreibung, die es jedoch zusätzlich erfordert, dass technische Anfragen formuliert werden damit Informationen gezielt ausgelesen können, was zusätzlich auch ein offener Punkt im Ansatz von Dokas ist.

2.4 Zusammenfassung und Handlungsbedarf der Arbeit

Mit diesem Kapitel wurden zunächst die notwendigen Grundlagen und verwandte Arbeiten dieser Ausarbeitung erläutert. Begonnen wurde damit, den aktuellen Stand der betrachteten Anwendungsdomäne in Abschnitt 2.1 zu erfassen, in dem zunächst die Ausgangssituation erläutert wurde. Weiterhin wurden Gefährdungsbeurteilungen als Bestandteil von Schutz- und Sicherheitskonzepten eingeführt, die in den folgenden Kapiteln dieser Ausarbeitung im Rahmen von Risikoanalyse und Bewertung fokussiert werden. Neben dem dargelegten derzeitigen Vorgehen, existieren einige kommerzielle Werkzeuge die den Anwender bei der Erstellung, Pflege und Verwaltung von Gefährdungsbeurteilungen unterstützen sollen. Exemplarisch wurden diese daher den dieser Ausarbeitung zugrundeliegenden Zieldefinitionen gegenübergestellt, um somit den Grad der bisherigen Zielerfüllung, sowohl des

klassischen Vorgehens als auch hinsichtlich der softwareseitigen Unterstützung aufzeigen zu können. Im Wesentlichen konnte damit verdeutlicht werden, dass kaum Formalisierungen für die Erstellung von Gefährdungsbeurteilungen bzw. dafür notwendige Risikoanalysen existieren. Trotz softwareseitiger Unterstützung ist die informelle, textuelle Beschreibung in natürlicher Sprache vorherrschend, sodass beispielsweise eine intelligente computergestützte Wiederverwendung oder transparente Gefährdungsbeurteilung nur begrenzt möglich ist [ERS10]. Weiterhin können und müssen risikomindernde Maßnahmen innerhalb von Gefährdungsbeurteilungen berücksichtigt werden, jedoch können diese, möglicherweise auch aufgrund mangelnder Formalisierung, nicht ausreichend in die Risikoanalyse und Bewertung, beispielsweise zur Ermittlung der Auswirkungen, eingebracht werden.

Im darauffolgenden Abschnitt 2.2 wurden mögliche Techniken eingeführt mit denen zum einen eine formalisierte Risikoanalyse und Bewertung ermöglicht werden kann sowie zum anderen, ein systematisches Vorgehen zur Risikoanalyse vorgegeben wird. Die aufgeführten Techniken sind dabei jeweils etablierte Verfahren, die in vielerlei Domänen bereits Anwendung gefunden haben. Die Techniken wurden jeweils aufgeführt und erläutert sowie anschließend hinsichtlich der Zieldefinitionen dieser Ausarbeitung abgeglichen. Dabei konnte festgestellt werden, dass keine Technik für sich allein ausreichend ist, um eine breite Zielerfüllung zu erreichen. Vielmehr sind zusätzlich softwareseitige Unterstützung und Erweiterungen notwendig, damit diese umsetzbar sowie praktikabel einsetzbar sind.

Im Weiteren wurden dazu verwandte Arbeiten aufgeführt und erläutert die diese Problemstellungen aufgreifen und somit Erweiterungen dieser Techniken hinsichtlich der Zielerfüllung dieser Ausarbeitung darstellen. Dabei wurden zunächst Ansätze erläutert, die im Rahmen der Fehlerbaumanalyse, welche als Technik in dieser Ausarbeitung fokussiert wird, eine automatisierte Risikoanalyse adressieren. Die dargelegten Ansätze aus dem wissenschaftlichen Umfeld adressieren dabei nur begrenzt erforderliche prozessorientierte Problemstellungen zur Durchführung von Gefährdungsbeurteilungen, sodass überwiegend Anwendungsfälle mit funktionaler Sichtweise wie der Systementwicklung von sowohl Hard- als auch Softwaresystemen adressiert werden. Dennoch ermöglichen diese Ansätze eine Reduzierung der Entwicklungszeit, Fehleranfälligkeit, Entwicklungskosten etc., trotz des zusätzlich gesteigerten Grades an Formalisierung. Der Einsatz der Fehlerbaumanalyse als Technik ermöglicht zusätzlich bereits eine Verbesserung der Transparenz, sodass die Ursachen und entsprechender Verknüpfungen im Fehlerbaum dargestellt und analysiert werden können. Im Vergleich zu den vorangegangenen Ausführungen zum aktuellen Stand der maritimen Domäne bei der Ausarbeitung von Gefährdungsbeurteilungen sowie den Ausführungen zu softwareseitiger Unterstützung und möglichen Techniken, nähern sich die Ansätze zur automatisierten Risikoanalyse durch Fehlerbäume bereits stärker den Zieldefinitionen dieser Ausarbeitung an. Dennoch existieren noch deutliche Diskrepanzen, sodass in den Ansätzen vermehrt technische Systeme betrachtet werden, wohingegen zur Fokussierung von Arbeitsabläufen und deren Sicherheit eine stärkere prozessorientierte Perspektive

erforderlich wäre. Zusätzlich berücksichtigt keiner der identifizierten Ansätze bei der automatisierten Risikoanalyse eine etwaige Wiederverwendbarkeit von Informationen oder risikomindernde Maßnahmen, die jedoch im Rahmen der Zieldefinitionen erforderlich sind.

Nachfolgend wurden daraufhin Ansätze dargelegt, die eine Verbesserung der Wiederverwendbarkeit von Risikoanalysen adressieren. Diese bauen überwiegend auf den erläuterten Techniken auf, sodass die dort für den jeweiligen Anwendungsfall gesammelten Informationen für eine mögliche Wiederverwendung in späteren Anwendungsfällen strukturiert gespeichert wurden. Damit diese Informationen gezielt wieder bereitgestellt werden können sowie der Ansatz und das dort vorgeschlagene Vorgehen praktikabel umgesetzt werden kann, sind teilweise Softwarewerkzeuge entstanden die eine verbesserte Wiederverwendung ermöglichen. Wie jedoch auch im vorangegangenen Abschnitt, werden von den Ansätzen überwiegend technische Systeme betrachtet, was nur begrenzt mit prozessorientierten Problemstellungen, wie beispielsweise im Rahmen von Schutz- und Sicherheitskonzepten für die Arbeitssicherheit, vereinbar ist. Darüber hinaus adressieren die identifizierten Ansätze zwar ganzheitlich das Speichern von Informationen, vernachlässigen jedoch teilweise wie diese praktikabel für spätere Anwendungsfälle wieder bereitgestellt werden können.

Anhand dieser Ausführungen lässt sich der wie folgt aufgelistete Handlungsbedarf ableiten, welcher im nachfolgenden Kapitel dieser Ausarbeitung zur Entwicklung von Anforderungen an einen eigenen Lösungsansatz im Rahmen der genannten Zieldefinitionen führt:

- **Analyse- und prozessübergreifende Betrachtung**: Damit eingebrachte Informationen zur Planung einer Operation durchgängig im Planungsprozess sowie der Analyse und Bewertung verwendet werden können, ist es notwendig, dass diese genauer beschrieben und stärker miteinander vernetzt werden. Dies erscheint insbesondere sinnvoll, da sich Gefährdungen auch durch die Gestaltung und Zusammenwirkung von Arbeitsabläufen ergeben [Deu11b, S. 12], die ansonsten separat geplant werden und so beispielsweise Aspekte wie risikomindernde Maßnahmen oder Relationen von Gefahren zu wenig beachtet werden [Man13, S. 252]. Eine übergreifende Betrachtung dieser Informationen ist daher essentiell zur Realisierung von **Ziel 1** bis **Ziel 3** und wurde von den betrachteten Ansätzen bisher nur in Teilen berücksichtigt.

- **Systematische Planung und Analyse**: Sowohl zur Durchführung einer Risikoanalyse als auch zur gezielten Einbringung notwendiger Informationen zur Abbildung des Anwendungsfalls ist ein systematisches Vorgehen erforderlich. Innerhalb des betrachteten Stands der Technik ist dies bisher kaum übergreifend berücksichtigt worden, sodass diese Aspekte zumeist separat voneinander betrachtet und innerhalb des Vorgehens berücksichtigt worden sind. Damit in einem Lösungsansatz jedoch eine ganzheitliche Unterstützung dieser Aspekte ermöglicht werden kann, ist für sämtliche

Zieldefinitionen **Ziel 1** bis **Ziel 6** ein systematisches Vorgehen mit einer ganzheitlich integrierten Betrachtung dieser Aspekte essentiell [Kri13, S. 281].

- **Integrierte Wiederverwendung**: Ansätze mit Aspekten zur Wiederverwendung werden kaum in die Planung oder Analyse einbezogen und überwiegend gesondert betrachtet. Für eine gezielte Bereitstellung von Informationen im Sinne der Wiederverwendbarkeit ist jedoch eine Integration in ein systematisches Vorgehen erforderlich, sodass durch klare Vorgehensweisen der Aspekt der Wiederverwendbarkeit berücksichtigt und somit sowohl Informationen hinterlegt, als auch bereitgestellt werden können. Darüber hinaus ist eine Integration, sowohl in analyse- als auch prozessübergreifende Aspekte erforderlich, sodass der Kontext der Wiederverwendung ersichtlich wird und damit auch **Ziel 3** adressiert werden kann.

- **Unterstützung bei formalisierter Risikoanalyse**: Die Durchführung einer formalisierten Risikoanalyse ist ein aufwändiges Unterfangen mit hoher Komplexität, weshalb bereits einige Ansätze vorgestellt wurden, dies zu automatisieren. Damit wurde zumeist der manuelle Aufwand auf andere Arbeiten verlagert und der Anwender kaum im Vorgehen unterstützt. Vielmehr sind Orientierungshilfen zur Unterstützung bei der Durchführung solch komplexer Vorhaben erforderlich, welche im Rahmen eines systematischen Vorgehens integriert werden sollten (siehe **Ziel 4**).

- **Unterstützung durch Softwarewerkzeuge**: Wie an den bisherigen Ausführungen erkennbar, ist eine softwareseitige Unterstützung für einen praktikablen Lösungsansatz erforderlich. Dabei sind besonders die Aspekte von **Ziel 3** und **Ziel 4** betroffen, sodass diese kaum ohne eine entsprechende Implementierung umsetzbar sind. Demnach ist die Umsetzung selbst, welche somit auch ein systematisches Vorgehen unterstützen kann, Bestandteil von **Ziel 6**.

Kapitel 3

Eigener Ansatz

In den bisherigen Kapiteln dieser Ausarbeitung wurde die Motivation, Problemstellung und der Stand der Technik dargelegt, um damit die Grundlage zur Entwicklung eines neuen Ansatzes zur prozessorientierten Risikoanalyse zur Bewertung maritimer Operationen zu schaffen. Innerhalb dieses Kapitels wird ein solcher Ansatz entwickelt und beginnt daher nach einem ingenieurmäßigen Vorgehen mit der Ermittlung von Anforderungen anhand des zuvor aus dem Stand der Wissenschaft und Technik identifizierten Handlungsbedarfs. Daraufhin wird ein exemplarisches Fallbeispiel eingeführt, das zur anschaulichen Darstellung der nachfolgenden Arbeiten innerhalb dieses Kapitels genutzt wird. Im Anschluss erfolgt die Beschreibung des entwickelten Ansatzes im Rahmen eines systematischen schrittweisen Vorgehens. Das Kapitel schließt daraufhin mit einer Zusammenfassung ab, in welcher die aufgestellten Anforderungen mit den dafür vorgenommenen Arbeiten dargestellt werden.

3.1 Anforderungsermittlung

Im vorangegangenen Kapitel 2 wurde der aktuelle Stand der Technik dargelegt und der Handlungsbedarf daraus hergeleitet. In diesem Abschnitt sollen darauf aufbauend Anforderungen hergeleitet werden, um daraufhin in den folgenden Abschnitten einen Lösungsansatzes zu erarbeiten. Die Anforderungen richten sich dabei nach den bisherigen Ausführung der Problemstellung und resultierenden Zieldefinitionen sowie des bereits identifizierten Handlungsbedarfs.

Demnach ist in diesem Kontext eine vermehrte Formalisierung des notwendigen Wissens erforderlich. Dies bildet insbesondere eine grundlegende Basis sowohl für Analysen, als auch weiterer Planungs- und Entwicklungsschritte und sorgt somit durch präzise Beschreibungen für eine erhöhte Transparenz und daher für eine verbesserte Nachvollziehbarkeit und Verständlichkeit eingepflegter Informationen [Kri13, S. 212], [Vin07, S. 129]. Zusätzlich wirkt sich eine präzisere Beschreibung des Untersuchungsgegenstandes und Dokumentati-

on der Risikobewertung positiv auf die Präzision und Qualität der Risikobewertung sowie spätere Wiederverwendungen und Aktualisierungen aus [S+02, S. 3], [Vin07, S. 129]. Die Form dieser Beschreibung ist jedoch unter Berücksichtigung des Anwendungsfalls und der Zielgruppe vorzunehmen [X+11, S. 7], [PD02]. Im Kapitel 2 wurde dabei identifiziert, dass bisherige formale Ansätze mit entsprechend formaler Systemdefinition und darauf aufbauender formaler Risikoanalyse häufig funktionale Perspektiven erfüllen [Jun12]. Hingegen ergeben sich für prozessorientierte Anwendungsfälle im Hinblick auf den **Handlungsbedarf „Analyse- und prozessübergreifende Betrachtung“** weitere Anforderungen, die im Folgenden aufgelistet werden:

- *Anforderung 1 - Möglichkeit zur Prozessdefinition.* Als Basis für eine formalisierte Risikoanalyse muss eine Modellgrundlage gefunden werden, mit der das zur Betrachtung des Anwendungsfalls notwendige Wissen formalisiert werden kann (vgl. Abschnitt 2.3). Bisherige Ansätze fokussieren dafür überwiegend technische Anwendungsfälle, weshalb dort funktionale Aspekte berücksichtigt werden [Jun12]. Als Handlungsbedarf wurde daher identifiziert, dass zur Untersuchung von ablauforientierten Problemstellungen entsprechend eine Form zur Definition von Prozessen erforderlich ist [CACO06]. Damit können dann einzelne Tätigkeiten, Bearbeitungsfolgen und involvierte Personen entsprechend formalisiert und strukturiert abgebildet werden.

- *Anforderung 2 - Konzept zur Abbildung risikorelevanter Informationen.* Zusätzlich zur Definition und Abbildung von Abläufen und involvierten Personen müssen relevante Gefährdungen und Schutzmaßnahmen berücksichtigt werden können [GA12]. Zusätzlich sind unerwünschte Ereignisse mit möglichen Kenngrößen und Ursachen relevante Informationen die zu betrachten sind [BB12, S. 39]. Insbesondere die Zusammenhänge dieser Informationen sollten daher in einem Konzept zur Abbildung dieser risikorelevanten Informationen entsprechend abgebildet werden können.

- *Anforderung 3 - Integration von Prozess- und Analysesicht.* Gefährdungen in ablauforientierten Anwendungsfällen können sich durch die Gestaltung der Abläufe und derer Zusammenwirkung heraus ergeben [Deu11b, S. 12]. Die reine Untersuchung dieser Abläufe, auch wenn diese nach Anforderung 1 definiert werden können, ermöglicht jedoch keine ausführliche Betrachtung der dabei enthaltenen Risiken [PBM+08], [CACO06]. Bei der Betrachtung von Abläufen sind daher insbesondere mögliche Ursachen von Gefahren und involvierte Personen zu berücksichtigen, was eine integrierte Betrachtung dieser Aspekte der Prozess- sowie Analysesicht erfordert [MKH04].

Eine formalisierte Systemdefinition bietet einen ersten Grundstein u.a. zur Steigerung der Wiederverwendbarkeit und damit auch der Effektivität des Vorgehens bei der Risikoanalyse und -Bewertung [S+02, S. 3]. Darüber hinaus muss jedoch auch eine technische Grundlage geschaffen werden, damit in das Vorgehen zur Risikobewertung eingebrachtes

Wissen festgeschrieben und bei Bedarf wieder abgerufen werden kann [CS06]. Da mit den vorangegangenen Anforderungen bereits notwendige Aspekte identifiziert wurden, ergeben sich aus dem **Handlungsbedarf „Integrierte Wiederverwendung“** heraus die folgend aufgelisteten zusätzlichen Anforderungen:

- *Anforderung 4 - Konzept zur Speicherung eingebrachter Planungsinformationen.* Damit im Rahmen der Wiederverwendung Informationen erneut genutzt werden können, ist zunächst erforderlich diese Informationen speichern zu können. Ein Beispiel dafür liefern Unfalldatenbanken, welche durch diese Möglichkeit als Ansatz gesehen werden können, um auf historische Daten zugreifen zu können [PSE10]. Eine Speicherung der Informationen erfordert daher eine technische Basis mit der Informationen sukzessive abgelegt und ergänzt werden können [CS06]. Dadurch wird es effizienter Informationen wiederzuverwenden als diese erneut einzupflegen [SPD99, S. 1].

- *Anforderung 5 - Möglichkeit zur Selektion bereitgestellter Informationen.* Zur Vervollständigung des Aspekts der Wiederverwendbarkeit ist die Bereitstellung des gespeicherten Wissens notwendig. Da es jedoch kaum sinnvoll erscheint stets das gesamte gespeicherte Wissen bereitzustellen, ist eine Selektion dessen erforderlich, sodass eine semantikbasierte Wiederverwendung ermöglicht werden kann [KOS12]. Ist dies der Fall kann innerhalb der Suche hinsichtlich der Relevanz des Wissens gefiltert und selektiert werden. Zusätzlich ist im Rahmen der Bereitstellung zu adressieren, dass selektiertes Wissen einem menschlichen Nutzer dargelegt werden muss, sodass dieser durch entsprechend dargestellte Informationen bei der Entscheidungsfindung unterstützt werden muss.

- *Anforderung 6 - Konzept zur Integration von Analyseergebnissen.* Um mit Hilfe einer stärkeren Wiederverwendung das Bild und die Informationen vergangener, gespeicherter Anwendungsfälle zu vervollständigen, sollen zusätzliche Informationen mit in das Vorgehen integriert werden können. Somit sollen Analyseergebnisse die bestehenden Planungsinformationen ergänzen, da diese erst im Rahmen des Vorgehens zur Risikoanalyse ermittelt werden können. Bei einer Speicherung und erneuten Bereitstellung derart erweiterter Planungsinformationen sollen diese somit im Rahmen der Anforderung für eine erhöhte Vergleichbarkeit und als Orientierungshilfe integriert werden, was nach bisherigen Ansätzen kaum möglich ist (vgl. Kapitel 2).

Bisher ist die manuelle Durchführung einer formalisierten Risikoanalyse ein zeit- und kostenaufwändiges Unterfangen ([CACO06], [LST09]) und ist zudem in bisherigen automatisierten Ansätzen beschränkt auf funktionale Aspekte sowie nicht weitreichend entwickelt im Hinblick auf die Durchführung der tatsächlichen Analyse. Gleichermaßen existieren bereits Methoden wie die Fehlerbaumanalyse, mit der die Vernetzung von Gefährdungen

in einem komplexen System transparent gemacht werden können [PL11, S. 193]. Zusätzlich werden die Ergebnisse damit transparent und nachvollziehbar visualisiert und grafisch dokumentiert [DHK+14, S. 480]. Aufgrund der aufwändigen Anwendung einer solchen formalisierten Methode muss jedoch, um einen effizienten Einsatz gewährleisten zu können, eine Basis zur Integration in das Vorgehen zur Planung geschaffen werden [S+02, S. 3]. Damit im Rahmen der Entwicklung eines eigenen Lösungsansatzes die als **Handlungsbedarf „Unterstützung bei formalisierter Risikoanalyse“** identifizierten Problemstellungen adressiert werden können, ergeben sich die folgenden Anforderungen:

- *Anforderung 7 - Konzept zur logischen und hierarchischen Strukturierung.* Zusätzlich zur Betrachtung von ablauf- bzw. prozessorientierten Informationen, ist für die Anwendung einer formalisierten Risikoanalyse die logische Strukturierung von Informationen notwendig, mit der Kombinationen von möglichen Ursachen spezifiziert werden können. Dadurch kann sowohl unterschieden werden, ob der Eintritt einzelner Ursachen ausreichend ist und zu weiteren unerwünschten Ereignissen führen kann, oder ob nur das kombinierte Auftreten derlei Auswirkungen haben kann. Eine hierarchische Strukturierung ist darüber hinaus notwendig zur weiteren Unterteilung und Verschachtelung dieser Informationen. Dies ist jedoch ein aufwändiges Unterfangen [Che10], sodass ein Ansatz zur weiteren gezielten Unterstützung des Anwenders erforderlich ist, um diesem Orientierungshilfen für die Durchführung zu ermöglichen.

- *Anforderung 8 - Konzept zur automatisierten Formalisierung.* Damit eine formalisierte Risikoanalyse durchgeführt werden kann, ist die Anwendung einer entsprechenden Technik erforderlich. Für diese Ausarbeitung ist die Technik der Fehlerbaumanalyse ausgewählt worden, sodass somit für die Analyse Fehlerbäume erstellt werden müssen. Diese sollen im Rahmen der Anforderung mit Hilfe zuvor strukturierter Informationen automatisiert erstellt werden können und somit einen Ansatz zur Formalisierung der Informationen für darauffolgende Analysen ermöglichen.

- *Anforderung 9 - Möglichkeit zur Aufbereitung der Ergebnisse.* Aufbauen auf Anforderungen zur Analyse, Strukturierung und Ergänzung von Wissen, ist eine Form der Dokumentation erforderlich, die als solche genutzt und von den beteiligten Personen verstanden werden kann [Vin07, S. 479, S. 491]. Dadurch sollen beteiligte Personen in die Lage versetzt werden, mögliche Gefährdungen und zu treffende risikomindernde Maßnahmen frühzeitig und insbesondere im Hinblick auf deren Zusammenhänge [Deu11b, S. 12] erkennen zu können [Tho12, S. 60].

Eine weitere, übergreifende und als **Handlungsbedarf „Unterstützung durch Softwarewerkzeuge“** identifizierte Anforderung ist:

- *Anforderung 10 - softwareseitige Unterstützung.* Mit einer einheitlichen, zentralen softwareseitigen Unterstützung soll übergreifend ein effizientes und systematisches

Vorgehen ermöglicht werden, damit das entsprechend eingepflegte Wissen im Rahmen der Anforderungserfüllung maschinenverarbeitbar genutzt werden kann.

3.2 Anwendungsbeispiel: Kranarbeiten

Zum Verständnis des nachfolgend konzipierten Lösungsansatzes wurde ein exemplarischer Anwendungsfall einer repräsentativen Offshore-Operation zur Erläuterung ausgewählt. Dieser Anwendungsfall sind Kranarbeiten, welche wiederkehrende und häufig bei Aufbau- und Wartungsarbeiten stattfindende Aufgabenstellungen beim Materialtransport darstellen. Zur weiteren Verdeutlichung des Szenarios wird in Abbildung 3.1 ein Auszug einer entsprechenden 3D Visualisierung des Anwendungsfalls dargestellt. Für den hier exemplarisch betrachteten Fall kommt dabei ein sogenanntes Jack-Up-Vessel, ein spezielles Schiff für Offshore-Arbeiten, zum Einsatz auf dem sich der Kran und der Kranführer (Abbildung 3.1 c) sowie der Ladeoffizier (Abbildung 3.1 a) und zunächst die Ladung (Abbildung 3.1 b) befindet. Die Ladung soll dabei in der Operation mit Hilfe des Krans, gesteuert vom Kranführer (Abbildung 3.1 c), auf die Offshore-Plattform (Abbildung 3.1 d) umgesetzt werden. Der Ladeoffizier (Abbildung 3.1 a) überwacht dabei den Transport vom Boden aus und steht in Funkkontakt mit dem Kranführer. Der Kranführer sorgt durch die Bedie-

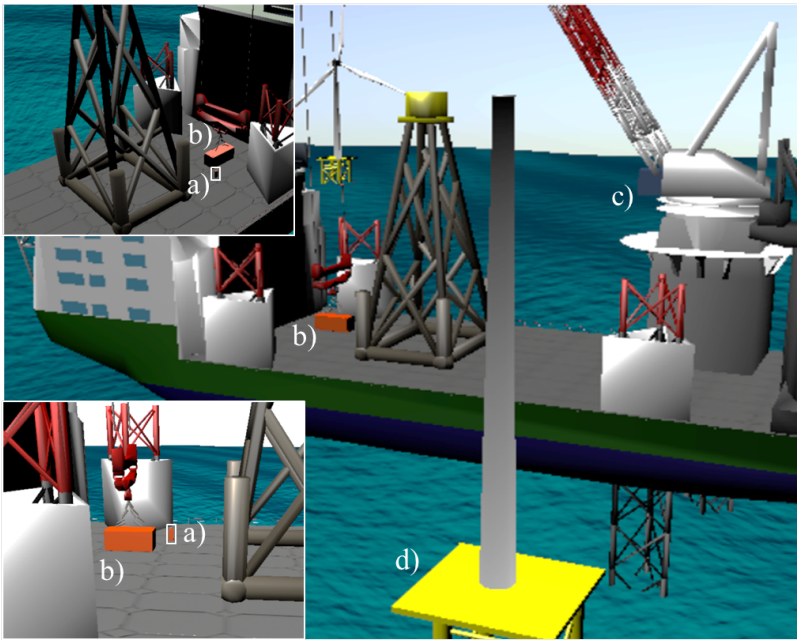

Abbildung 3.1: Visualisierung des Kranarbeiten-Szenarios aus verschiedenen Perspektiven einer 3D-Simulation nach Gollücke [GPL+14], mit einem Ladeoffizier (a) in der Nähe der Ladung (b), einem Kranführer im Führerhaus(c) und einer Offshore-Plattform (d)

nung des Krans für das Anheben und Übersetzen der Ladung. Die Situation wird dabei vom Ladeoffizier beobachtet, sodass sich dieser in der Nähe der Ladung befindet und aus seiner Perspektive per Funk Hinweise an den Kranführer weitergeben kann.

Durch die Handhabung der Ladung birgt diese Operation Potential für Gefährdungen, sodass beispielsweise die Ladung fallen kann. Durch das hohe Gewicht einer solchen Ladung kann diese Gefährdung erhebliche Folgen, wie Personen- und Sachschäden, nach sich ziehen, sodass diese Operation zunächst im Rahmen einer Gefährdungsbeurteilung geplant und hinsichtlich des potentiellen Risikos analysiert und bewertet werden muss.

In diesem Anwendungsbeispiel sind im Wesentlichen zwei Personen involviert, die im Rahmen ihres Aufgabenbereichs verschiedene Tätigkeiten durchführen, welche bei einer Gefährdungsbeurteilung als erstes identifiziert und dokumentiert werden müssen. Darüber hinaus ist es für derlei maritime Operationen notwendig, involvierte Personen sowie deren Tätigkeiten in Zusammenhang mit möglichen Gefährdungen aufzuschlüsseln. Dabei muss ermittelt werden wie risikoreich die geplanten Tätigkeiten sind und welchem Risiko die beteiligten Personen ausgesetzt sind. Darauf aufbauend werden in der Planung risikomindernde Maßnahmen getroffen, um somit das Gesamtrisiko der Operation, sowie das Risiko für die Personen und Tätigkeiten zu reduzieren. Dies dient zum einen zur Genehmigung dieser Operation, sodass diese überhaupt durchgeführt werden darf. Zum anderen, dient es auch der Vorbesprechung, Sensibilisierung und Vorbereitung der involvierten Personen vorab der Durchführung. Der nachfolgend konzipierte Lösungsansatz adressiert diese Inhalte und Anforderungen und wird nachfolgend anhand des Anwendungsbeispiels erläutert. Im Gegensatz zum bisherigen informellen Vorgehen wie in Kapitel 2 beschrieben, nutzt der konzipierte Lösungsansatz dabei eine formalisiertere Herangehensweise zur Planung der Abläufe der Operation, als auch zur Analyse dieser zur Ermittlung der enthaltenen Risiken und setzt dies in einem systematischen Vorgehen um.

3.3 Prozessorientierte Risikoanalyse

In den vorangegangenen Abschnitten wurde zunächst auf Basis verwandter Arbeiten und des Standes der Technik der Handlungsbedarf ermittelt, woraufhin im ersten Abschnitt dieses Kapitels Anforderungen für einen Lösungsansatz aufgestellt wurden. Der dafür entwickelte Lösungsansatz wird zum Überblick schematisch in Abbildung 3.2 skizziert und umfasst dabei die in Kapitel 2 erläuterten Schritte zur Risikoanalyse und Bewertung (siehe Abbildung 2.3). Dieser Lösungsansatz orientiert sich somit an dem Vorgehen zur Risiko- bzw. Gefährdungsbeurteilung nach [Vin07, S. 127], sodass vorzunehmende Arbeiten jeweils in diesem schrittweisen Vorgehen betrachtet werden, um mit dem Lösungsansatz den identifizierten **Handlungsbedarf „Systematische Planung und Analyse“** zu adressieren. Ein integraler Bestandteil des nachfolgend schrittweise erklärten Lösungsansatzes ist das in Abbildung 3.2 skizzierte Vorgehen, welches zusätzlich innerhalb einer softwareseitigen

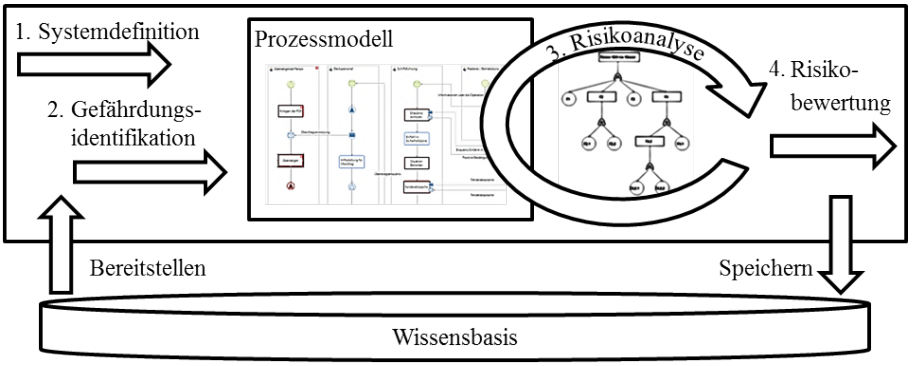

Abbildung 3.2: Schematische Übersicht des Lösungsansatzes

Unterstützung umgesetzt wurde. Innerhalb dieser dient ein Prozessmodell aus dem Ansatz von Droste [DH13], welcher im nachfolgenden Unterabschnitt erläutert wird, zunächst als Mittel zur **Systemdefinition** und formaleren Beschreibung der Abläufe maritimer Operationen, mit der Absicht dieses für Analysen nutzbar zu machen. Dieses Modell wird im Folgeschritt der **Gefährdungsidentifikation** weiter iterativ verfeinert und dabei mit relevanten Informationen angereichert, sodass dieses für eine spätere Risikoanalyse genutzt werden kann. Dabei kann die zugrundeliegende Wissensbasis als zusätzliche Informationsquelle unterstützend genutzt werden, um Informationen vergangener Anwendungsfälle gezielt bereitzustellen. Innerhalb der **Risikoanalyse** werden die in den vorangegangenen Schritten eingebrachten Informationen verwendet, dabei weiter strukturiert und in eine analysierbare, formalisierte Form von Fehlerbäumen überführt und ausgewertet. Der abschließende Schritt der **Risikobewertung** umfasst die manuelle Überprüfung der vorgenommenen Planung sowie das Speichern der in das Vorgehen eingebrachten Informationen in die Wissensbasis. Bei erfolgreicher Planung werden diese Informationen abschließend in diesem Schritt in die Wissensbasis überführt, sodass damit eine gezielte Wiederverwendung ermöglicht werden kann und diese Informationen bei späteren Planungsvorhaben zur erneuten unterstützenden Gefährdungsidentifikation bereitgestellt werden können. Bei nicht erfolgreicher Planung können diese Schritte hingegen zur Umplanung erneut durchlaufen werden, sodass eine alternative oder verfeinerte Planung vorgenommen werden kann. Dies geschieht so lange, bis die Planung und resultierende Ergebnisse der Risikoanalyse den Ansprüchen genügen. In den nachfolgenden Unterabschnitten werden jeweils die erforderlichen Schritte des Vorgehens im Detail erläutert:

1. Systemdefinition
2. Gefährdungsidentifikation
3. Risikoanalyse
4. Risikobewertung

3.3.1 Systemdefinition

Der erste Schritt in Richtung einer Risikoanalyse ist immer zunächst die Definition des betrachteten Systems [Kri13, S. 212]. Diese Systemdefinition bildet dabei die grundlegende Basis für die gesamte Analyse und stellt somit einen wichtigen Bestandteil dar [Kri13, S. 212]. Dieser Schritt sorgt weiterhin dafür, dass durch eine präzise Beschreibung des Systems die Transparenz erhöht wird, sodass beteiligte Personen in der Lage sind eingepflegte Informationen beurteilen und nachvollziehen zu können [Vin07, S. 129]. Während mentale und verbale Modelle die menschliche Vorstellung von Systemen sind und damit immer unpräzise und unvollständig bleiben, stellen formale Modelle hingegen durch exakte Beschreibungen von Elementen und Beziehungen immer eine klar definierte Abbildung eines Sachverhaltes dar [Aul13, S. 24]. Die Formalisierung betrifft hierbei eine einheitliche Modellierungssprache mit präziser Dokumentation und Erläuterung des Modells [Aul13, S. 24]. Diese Modelle ermöglichen somit eine formale Beschreibung eines Ausschnitts der realen Welt und abstrahieren dabei bewusst, indem für den Anwendungsfall des Systems möglicherweise irrelevante Aspekte weggelassen werden. Dieser Vorgang des Modellierens ermöglicht somit auch eine Reduktion der Komplexität eines zu untersuchenden Systems. Die dabei getroffenen Vereinfachungen und Abstraktionen wiederum ermöglichen die Darstellung komplexer Zusammenhänge und so die Erlangung eines Erkenntnisgewinns über ansonsten der Erkenntnis verschlossene Systeme [Aul13, S. 24]. Ein solches Modell bzw. eine solche Modellierungssprache muss demnach gefunden werden, um eine geeignete Beschreibung der Systemdefinition zu ermöglichen. Weiterhin muss diese entsprechend der Zielgruppe ausgewählt und zugeschnitten sein ([X+11, S. 7], [PD02]) und in einen Planungsansatz integriert werden können, sodass die spätere Risikoanalyse auf Grundlage dieses Modells erfolgen kann. Da die Ausarbeitung von Gefährdungsbeurteilungen unterstützt werden soll, ergeben sich somit Inhalte der Systemdefinition aus den notwendigen Informationen einer Gefährdungsbeurteilung, wobei der Untersuchungsgegenstand stets die zu planende und zu analysierende Operation ist. Wesentliche Inhalte die im Rahmen einer Systemdefinition festzulegen sind, sind demnach die an der Operation beteiligten Personen, deren spezifische Tätigkeiten sowie dabei verwendete Ressourcen [Vin07, S. 129], [CS06].

Als Mittel zur Beschreibung stattfindender Arbeitsabläufe, wie beispielsweise einer maritimen Operation, haben sich im Vergleich zu rein textuellen Beschreibungen, formalisierte grafische Ansätze in unterschiedlichen Domänen etabliert, mit denen die Reihenfolge von Tätigkeiten sowie mögliche Verzweigungen und Zusammenhänge mit Personen abbilden lassen. Aspekte wie die Gefährdungen und Ursachen, die Gegenstand der Risikoanalyse sind, werden dabei überwiegend gesondert betrachtet. Mit der Entwicklung des Modellierungswerkzeugs **MOPhisTo** wurde erstmalig ein formalisierter, graphischer Ansatz entwickelt, um eine Systemdefinition gezielt für maritime Operationen vorzunehmen [DH13]. Dabei ermöglicht der Ansatz zusätzlich die Integration von Aspekten zur Risikoanalyse,

sodass diese im Rahmen einer ganzheitlichen Planung und Analyse maritimer Operationen vorgenommen werden kann. Der Ansatz wird demnach als Mittel zur Systemdefinition in dieser Ausarbeitung genutzt und in den nachfolgenden Unterkapiteln erläutert. Nachdem MOPhisTo vorgestellt wurde, führt das darauffolgende Unterkapitel in das zugrundeliegende **Modell** ein. Daraufhin folgt eine Beschreibung des **Vorgehens**, wie dieses Modell zur Systemdefinition genutzt wird, was abschließend durch das **Anwendungsbeispiel** veranschaulicht wird.

MOPhisTo

Mit dem Ansatz von MOPhisTo wurde von Droste [DH13] gezielt ein Ansatz zur Definition des Systems im Rahmen der Planung maritimer Operationen entwickelt, wie schematisch in Abbildung 3.3 dargestellt. Dabei besteht das zu definierende System grundsätzlich aus einer Menge von Elementen, die im Wesentlichen in zwei Typen unterteilt werden können. Zum einen ist ein wesentliches `Element` die betrachtete `Operation` selbst, wobei die darin enthaltenen Arbeitsabläufe graphisch modelliert werden. Zum anderen, können weitere `Elemente` definiert werden, um relevante physikalische Objekte abzubilden, wie beispielsweise involvierte Personen mit deren Qualifikationen. Der Ansatz wurde durch den Anwendungsfokus, die quellenoffene und erweiterbare Implementierung sowie die Möglichkeit zur Kombination mit Aspekten der Risikoanalyse als Alleinstellungsmerkmal gegenüber anderen Ansätzen identifiziert und ausgewählt. Der Ansatz von MOPhisTo wird somit in dieser Ausarbeitung als Mittel zur Systemdefinition verwendet und dient darüber hinaus als Basis zur darauf aufbauenden Entwicklung des Lösungsansatzes dieser Ausarbeitung.

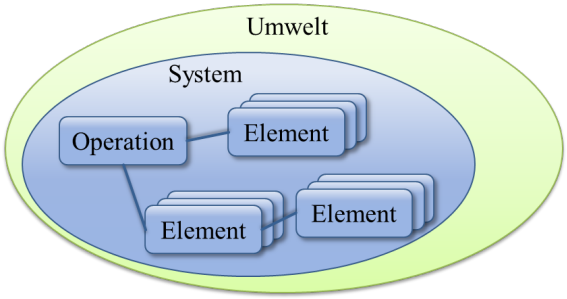

Abbildung 3.3: Schematische Darstellung der Systemdefinition mit MOPhisTo

Eine `Operation` setzt sich zusammen aus den Arbeitsabläufen, bestehend aus einer Reihe von Tätigkeiten die von Personen umgesetzt werden zur Durchführung der Operation. Um somit diese Arbeitsabläufe beschreiben und darstellen zu können, wurde eine Möglichkeit zur graphischen Modellierung als Prozessmodell entwickelt. Diese Prozessmodelle ersetzen die vormals textuelle Beschreibung von Arbeitsabläufen durch grafische Elemente, um somit unter anderem Sequenzen, Verzweigungen und dadurch beispielsweise die

parallele oder sequentielle Bearbeitung von Tätigkeiten darzustellen. Solche Prozessmodelle können domänenübergreifend genutzt werden und gelten gemeinhin als verständliches Hilfsmittel zur Darstellung von Abläufen [MRC07].

Über die graphische Modellierung der Operation hinausgehend werden mit MOPhisTo weitere `Elemente` zur Systemdefinition in Form eines Datenmodells eingepflegt und mit der Operation verknüpft. Die Systemgrenzen zur Umwelt legen sich dadurch fest, dass im System alle für die Planung der Operation erforderlichen Informationen enthalten sein müssen. Darüber hinausgehende Informationen werden automatisch der `Umwelt` zugeschrieben und somit bei der Systemdefinition nicht berücksichtigt. Die erforderlichen Informationen der Systemdefinition können je nach gewünschtem Detailgrad der zu planenden Operation variieren, sodass somit keine allgemeingültige Systemgrenze zur Umwelt festgelegt werden kann. Das `System` umfasst daher stets eine Menge von Elementen, die wiederum selbst ein System sein können, wie beispielsweise ein Lastenkran der wie im Anwendungsbeispiel beschrieben innerhalb einer Operation genutzt wird. Ein `Element` ist Bestandteil eines Systems und kann beispielsweise physikalische Objekte wie handelnde Personen in einer Operation umfassen. Die `Operation` sowie involvierte Personen zählen somit selbst auch zu diesen Elementen, wobei die Operation im Gegensatz zu anderen Elementen in Form eines graphischen Prozessmodells abgebildet wird. Um die somit zur Systemdefinition zu erfassenden Daten handhaben und strukturieren zu können, wurde in MOPhisTo ein Modell entwickelt, um in der Systemdefinition relevante Elemente und darin enthaltene Zusammenhänge einzupflegen. Dieses Modell ist Bestandteil des nachfolgenden Unterabschnitts und wird dort genauer erläutert.

Modell

Das zur Durchführung der Systemdefinition und somit zur Strukturierung der erforderlichen Informationen entwickelte Modell kann zunächst als $M_{sysdef} = (E, R, \Gamma)$ beschrieben werden [KMS05], wobei

- $E = \{e_1, e_2, ..., e_n\}$ eine endliche Menge an Elementen darstellt
- $R = \{r_1, r_2, ..., r_m\}$ eine endliche Menge an Relationen darstellt
- $\Gamma : R \Rightarrow E \times E$ die Funktion zur Abbildung von Relationen zwischen den Elementen definiert

Jedes Element enthält zudem eine endliche Menge an Eigenschaften ($\{p_1, p_2, ..., p_k\}$), wobei jede Eigenschaft p_i einem geordneten Name-Werte-Paar (bspw. $\{name, Ladeoffizier\}$) entspricht. Sämtliche Elemente verfügen dabei zunächst über die Eigenschaften p_{name}, $p_{beschreibung}$, mit $p_{name} = \{name, \emptyset\}$ und $p_{beschreibung} = \{beschreibung, \emptyset\}$.

Eine `Operation` die als graphisches Prozessmodell dargestellt wird, kann zunächst grob als $Operation \in E$ beschrieben werden, die in ihrer graphischen Repräsentation

die nachfolgend erläuterten Unterelemente umfasst. Darin enthalten sind die involvierten Personen ($Actors = \{a_1, a_2, ..., a_i\}$), die als `Actor` innerhalb der `Operation` agieren ($\Gamma : involved\_in \Rightarrow Actors \times Operation$). Jeder Akteur hat dabei einen eigenen, individuellen Arbeitsablauf (`WorkingProcedure`), den dieser durchführt ($\Gamma : performs \Rightarrow Actor \times WorkingProcedure$). Eine `WorkingProcedure` besteht dabei aus Elementen zur Strukturierung des Arbeitsablaufs, genannt `FlowElements`. Ein solches `FlowElement` kann dabei ein `FlowObject` zur Spezifikation von Aktivitäten, Ereignissen und Verzweigungen sein ($FlowObjects = \{Activities, Events, Gateways\}$), oder als `ConnectionObject` die Verbindungen zwischen `FlowObjects` abbilden ($ConnectionObjects = \{SequenceFlow, MessageFlow\}$).

- Aktivitäten bzw. Tätigkeiten die im Rahmen einer `WorkingProcedure` von einem Akteur ausgeführt werden, werden als `Activity` beschrieben ($\Gamma : executed\_in \Rightarrow Activity \times WorkingProcedure$). Eine `Activity` lässt sich dabei in die beiden Ausprägungen `Task` und `SubProcess` unterteilen. Ein `Task` beschreibt dabei eine atomare Tätigkeiten eines Akteurs innerhalb der Operation, wohingegen Tätigkeiten mit weiterer hierarchischer Unterteilung `SubProcess` genannt werden und wiederum eine eigene untergeordnete `WorkingProcedure` beschreiben.

- Mit einem `Event` werden Ereignisse abgebildet, die in einer `WorkingProcedure` ausgeführt werden ($\Gamma : executed\_in \Rightarrow Event \times WorkingProcedure$). Spezielle Ausprägungen von `Events` sind beispielsweise die Kommunikation zwischen Akteuren wie Sende- (`Sending Signal` oder `Sending Message`) und Empfangsereignisse (`Receiving Signal` oder `Receiving Message`) von Nachrichten oder Signalen. Mit Message-Events wird dabei eine gerichtete Kommunikation zwischen zwei `Actors` sowie über Signal-Events eine ungerichtete Kommunikation beschrieben. Weitere Ereignisse markieren den Start (`StartEvent`) und das Ende (`EndEvent`) oder den gezielten Abbruch einer `WorkingProcedure` oder der `Operation`. Für jede `WorkingProcedure` wird durch ein `StartEvent` und `EndEvent` gewährleistet, dass diese einen definierten Start und Endpunkt enthält.

- Als `Gateway` können Verzweigungen innerhalb einer `WorkingProcedure` modelliert werden ($\Gamma : realised\_in \Rightarrow Gateway \times WorkingProcedure$). Grundsätzlich werden dabei als `ForkingGateway` das Öffnen, oder als `JoiningGateway` das Schließen nebenläufiger Pfade abgebildet, wobei durch spezielle Ausprägungen wie dem `AndGateway` die gezielte parallele Ausführung mehrerer Pfade und darin enthaltenen `Activities` und `Events` modelliert wird.

- `ConnectionObject` entspricht einem Element zur Abbildung von Verbindungen innerhalb der Abläufe einer `WorkingProcedure`, sodass mit der speziellen Ausprägung der Sequenzfluss (`SequenceFlow`) zwischen `Activity`, `Event` und `Gateway` Elementen

sowie mit `MessageFlow` ein gerichteter Nachrichtenfluss zwischen `SendingMessage` und `ReceivingMessage` Elementen beschrieben werden kann. Jedes `ConnectionObject` verfügt dabei über die Attribute p_{source} und p_{target}, sodass als p_{source} das Quell- und als p_{target} das Zielelement referenziert wird. `SequenceFlows` finden dabei ausschließlich im Rahmen einer `WorkingProcedure` eines Akteurs statt und eine gezielte Kommunikation zwischen Akteuren nur über `MessageFlows` und entsprechende `Events`.

Zusätzlich zu den wie in Abbildung 3.4 links dargestellten graphischen Elementen, ist zur genaueren Spezifikation der `Operation` die Definition weiterer für die Operation relevanter Elemente erforderlich. In MOPhisTo wird daher im Modell zwischen der Spezifikation der Operation und der Spezifikation dabei relevanter physikalischer Objekte (in Abbildung 3.3 als Element gekennzeichnet) unterschieden. Als weitere relevante Elemente werden die physikalischen Objekte gezählt, die im Rahmen einer Operation und der darin durchgeführten Tätigkeiten genutzt werden. Exemplarisch kann dabei zur Erklärung das Anwendungsbeispiel dienen, sodass zu diesen Elementen beispielsweise der Lastenkran, die involvierten Personen, die Ladung oder das Schiff jeweils im Rahmen der Tätigkeiten genutzt werden. Derlei Elemente können ebenfalls als $E = \{e_1, e_2, ..., e_l\}$ beschrieben werden, sodass das Schiff beispielsweise als $Schiff \in E$ sowie auch für die Operation genutzte konkrete Ausprägungen davon wie das Jack-Up-Vessel (JUV) als Unterelement dessen ($JUV \in Schiff$) mit $p_{type} = \{type$, Jack-Up-Vessel$\}$ und weiteren Attributen spezifiziert werden kann. Im nachfolgenden Unterabschnitt wird der genauere Ablauf der Systemdefinition mit Nutzung des beschriebenen Modells erläutert.

Vorgehen

Das in der Systemdefinition betrachtete System besteht aus einer Menge von Elementen die beschrieben werden müssen. Abbildung 3.4 stellt dafür auf der rechten Seite das Vorgehen schematisch dar und zeigt in der Mitte die dabei verwendeten Modellelemente sowie die verwendete Symbolik zur graphischen Modellierung auf der linken Seite. Unterschieden wird in Abbildung 3.3 zwischen der Operation, als ein spezielles Element das im Rahmen der Prozessmodellierung graphisch in den Schritten (2)-(5) nach Abbildung 3.4 modelliert wird, und anderen Elementen die als physikalische Objekte in Schritt (1) nach Abbildung 3.4 spezifiziert und später mit der Operation verknüpft werden. Der erste Schritt im Vorgehen der Systemdefinition ist nach Abbildung 3.4 (1) somit die Festlegung dieser Elemente, sodass im Rahmen der Systemdefinition definiert wird, welche Elemente als physikalische Objekte, wie Werkzeug, Maschinen, Schutzausrüstung sowie auch involvierte Personen und deren erforderliche Qualifikationen etc., bei der geplanten Operation relevant sind. Diese Elemente werden dabei auch über ihre Attribute wie $p_{name}, p_{beschreibung}$ sowie beliebig weitere wie $p_{type}, p_{size}, p_{qualification\_level}$ etc. detailliert beschrieben.

Im zweiten Schritt (2) erfolgt daraufhin die genauere Spezifikation der geplanten Opera-

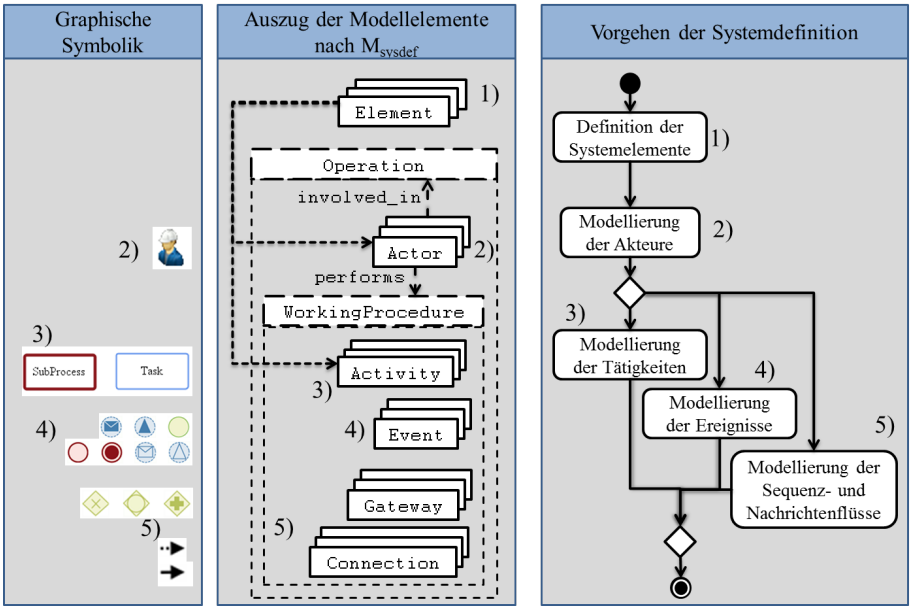

Abbildung 3.4: Schematisches Vorgehen der Systemdefinition

tion, sodass damit begonnen wird Unterelemente wie die Akteure zu definieren. Diese werden dabei zum einen graphisch modelliert, und zum anderen mit den in Schritt (1) festgelegten Elementen verknüpft, sodass beispielsweise dem modellierten Akteur `Ladeoffizier` die Elemente Funkgerät oder Schutzkleidung zugeordnet werden können.

Als weiteres wird im dritten Schritt (3) begonnen die `WorkingProcedures` mit den darin durchzuführenden Tätigkeiten graphisch zu modellieren, sodass `Activities` erstellt werden, die als `Task` bzw. `SubProcess` die einzelnen Tätigkeiten der Operation im Rahmen einer `WorkingProcedure` von einem `Actor` graphisch abbilden. Diesen werden, analog zu Schritt (2), Elementen der Systemdefinition aus Schritt (1) zugeordnet, sodass somit der Zusammenhang von Tätigkeiten und dafür relevanten Systemelementen, wie beispielsweise zu nutzendes Werkzeug, hergestellt und im Modell abgebildet werden kann.

Parallel dazu erfolgt in Schritt (4) die Modellierung von Ereignissen, sodass zur weiteren Spezifikation einer `WorkingProcedure` die Kommunikation sowie Start, Ende oder Abbruch innerhalb einer `WorkingProcedure` mit Hilfe von `Events` definiert wird.

Mit dem parallel stattfindenden Schritt (5) wird zusätzlich der Sequenzfluss in der `WorkingProcedure` zum einen über Verbindungslinien als `SequenceFlow`, zum anderen als `Gateway` beispielsweise zur Modellierung paralleler `Activities` abgebildet. Darüber hinaus wird der Nachrichtenfluss als `MessageFlow` graphisch als gestrichelte Verbindungslinie zwischen zwei Message-Events, wie `SendingMessage` und `ReceivingMessage`, modelliert.

Das Resultat dieses Vorgehens ist eine Systemdefinition der relevanten Systemelemente sowie ein graphisches Prozessmodell, wie exemplarisch in Abbildung 3.5 dargestellt,

zur Spezifikation der Operation als Systemelement, was im nachfolgenden Unterabschnitt anhand des Anwendungsbeispiels Kranarbeiten verdeutlicht wird.

Anwendungsbeispiel

In Abbildung 3.5 wird ein exemplarisches Prozessmodell für das Anwendungsbeispiel Kranarbeiten dargestellt. Dabei wurden zwei Personen bzw. Akteure identifiziert und als Ladeoffizier und Kranführer zunächst nach Schritt (1) als physikalische Objekte mit entsprechenden Attributen wie erforderlichen Qualifikationen definiert und in Schritt (2) graphisch im Prozessmodell modelliert und verknüpft. Innerhalb derer graphischer Umrandung sind die entsprechenden Arbeitsabläufe (`WorkingProcedure`) der Akteure dargestellt, die in den Schritten (3)-(5) modelliert wurden. Die Operation beginnt mit dem Startereignis, welches als oberstes grafisches Element in den Abläufen des Kranführers dargestellt wird und dem Modell nach ein `Event` ist. Zur graphischen Verbindung mit weiteren Elementen wurde,

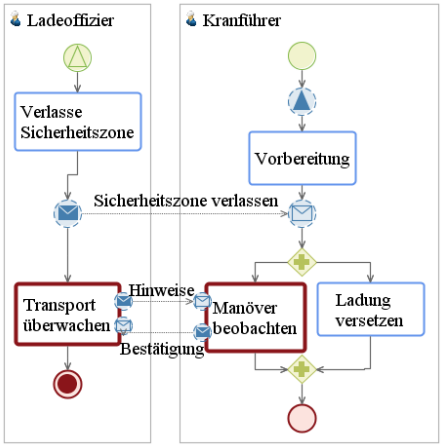

Abbildung 3.5: Darstellung des graphischen Prozessmodells zur Systemdefinition des Anwendungsbeispiels

der Pfeildarstellung folgend, ein `SequenceFlow` genutzt, um den weiteren Ablauf abzubilden. Daraufhin folgt ein (`SendingSignalEvent`) als Dreiecksdarstellung, bei dem ein Signal an den Ladeoffizier gegeben wird, welcher daraufhin seinen Arbeitsablauf mit einem kombinierten Start- und Signalempfangssymbol beginnt. Bei beiden Akteuren findet dem `SequenceFlow` folgend eine einfache Tätigkeit (`Task`) zum Verlassen der Sicherheitszone bzw. zur Vorbereitung für den Transport mit dem Kran statt. Daraufhin erfolgt das direkte Senden einer Nachricht vom Ladeoffizier an den Kranführer (`SendingMessage`) entsprechend des dargestellten Nachrichtenflusses, um dort zu bestätigen, dass die Sicherheitszone verlassen wurde. Anschließend überwacht der Ladeoffizier den Transport (`SubProcess`) und tauscht dabei wiederum Nachrichten durch Ereignisse mit dem Kranführer aus. Die Tätig-

keiten des Kranführers verzweigen durch ein `ForkingAndGateway`, um eine parallele Ausführung der darauffolgenden Tätigkeiten darzustellen. Nach Durchführung der Tätigkeiten wird diese Verzweigung durch ein `JoiningAndGateway` wieder zusammengeführt und der Arbeitsablauf des Kranführers bzw. des Ladeoffiziers daraufhin mit einem `EndEvent` beendet. Bei diesem Prozess sind weitere verbundene Systemelemente die nach Schritt (1) in Abbildung 3.4 definiert wurden, beispielsweise das Funkgerät das in Task „Transport überwachen“, der Kran oder die Ladung selbst die in „Ladung versetzen“ und „Vorbereitung“ als physikalische Objekte genutzt werden.

Die vorgenommene Systemdefinition bildet den ersten Schritt zur Planung der Operation ab. Um darüber hinaus jedoch eine spätere Risikoanalyse und Bewertung der Operation zu ermöglichen, werden im nachfolgenden Schritt zur Gefährdungsidentifikation dafür erforderliche Informationen über mögliche Gefährdungen und Ursachen systematisch ermittelt und eingepflegt.

3.3.2 Gefährdungsidentifikation

Bei dem Schritt der Gefährdungsidentifikation müssen mögliche Gefährdungen und Ursachen für den jeweiligen Anwendungsfall gesucht, klassifiziert und dokumentiert werden [Vin07, S. 121]. Bisher gibt es dabei nach dem Stand der Technik nur wenige Hilfsmittel zur Formalisierung, sodass diesem Vorgang eine systematische und strukturierte Vorgehensweise zugrunde zu legen ist [Vin07, S. 121]. Zudem sollte der Gefährdungsidentifikation eine sorgfältige und präzise Definition des Anwendungsfalls zugrunde liegen [Kri13, S. 302], was in diesem Lösungsansatz der im vorangegangenen Schritt vorgenommenen Systemdefinition entspricht.

Im Rahmen dieser Ausarbeitung werden Informationen der Gefährdungsidentifikation in ein weiteres Modell mit Bezug zur Systemdefinition überführt, um zum einen einen klaren Bezug zum Anwendungsfall und darin entsprechend betroffenen Elementen herstellen zu können. Zum anderen, um eine einheitliche und durchgängige Vorgehensweise im Rahmen von Formalisierungen und Toolunterstützung ermöglichen zu können. Insofern wird die vorgenommene Planung im Schritt der Gefährdungsidentifikation erweitert und mit Informationen über mögliche Gefährdungen und Ursachen strukturiert und systematisch ergänzt. Bei der Gefährdungsidentifikation ist dafür Erfahrungswissen erforderlich, das zum einen vom Sicherheitsexperten selbst kommen kann, zum anderen ist für diesen Fall innerhalb des Lösungsansatzes eine zugrundeliegende Wissensbasis entwickelt worden, die bei diesem Vorhaben auf Basis von Informationen vergangener Anwendungsfälle entsprechende Vorschläge bereitstellen kann. Diese Wissensbasis wird zwar im Schritt der Gefährdungsidentifikation genutzt um Daten bereitzustellen, das Konzept dazu wird jedoch erst im Schritt der Risikobewertung in Abschnitt 3.3.4 erläutert.

Die nachfolgenden Unterkapitel erläutern zunächst das **Modell** zur strukturierten und systematischen Durchführung der Gefährdungsidentifikation, sodass sicherheitskritische

Informationen den im Prozessmodell eingepflegten Elementen zugeordnet werden können. Dieses Modell wurde im Rahmen des Forschungsprojekts SOOP (Sichere Offshore-Operationen[1]), in Anlehnung an das bisherige Vorgehen der maritimen Domäne sowie dem verbreiteten Vorgehen der ISO 26262 für funktionale Sicherheit aus dem Automotive-Bereich [ISO08] entwickelt und in das Werkzeug MOPhisTo integriert.

Darauffolgend wird das **Vorgehen** zur Gefährdungsidentifikation anhand des entwickelten Modells erläutert, sowie daraufhin wie die **Wissensbasis als Informationsquelle** innerhalb der Gefährdungsidentifikation genutzt werden kann. Die Gefährdungsidentifikation schließt dann zur Veranschaulichung mit dem durchgängigen **Anwendungsbeispiel** ab.

Modell

In Erweiterung zum in der Systemdefinition genutzten Modell M_{sysdef}, wird für die Gefährdungsidentifikation analog das Modell $M_{gefident} = (E, R, \Gamma)$ definiert. Mit diesem werden die relevanten Informationen zur Durchführung der Gefährdungsidentifikation strukturiert, sodass dieses die nachfolgend erläuterten Elemente umfasst:

$$
\begin{aligned}
E = \{ \quad & HazardousEvents = \{he_1, he_2, ..., he_l\}, \\
& Exposures = \{e_1, e_2, ..., e_t\}, \\
& OperationalSituations = \{op_1, op_2, ..., op_l\}, \\
& Hazards = \{h_1, h_2, ..., h_i\}, \\
& Causes = \{c_1, c_2, ..., c_b\}, \\
& MitigationMeausures = \{mm_1, mm_2, ..., mm_u\}, \\
& CounterMeasures = \{cm_1, cm_2, ..., cm_k\} \\
\} &
\end{aligned}
$$

Ein Gefährliches Ereignis (`HazardousEvent`) kann dabei endlich oft im Modell vorkommen und beschreibt die Kombination des Auftretens einer Gefährdung (`Hazard`) ($(\Gamma : contains \Rightarrow he_l \times h_i)$ innerhalb einer bestimmten Betriebssituation (`OperationalSituation`) ($\Gamma : occurs\_in \Rightarrow he_l \times op_l$) mit dem Potential zu einem Unfall oder Schaden zu führen [ISO08]. Dabei wird für das `HazardousEvent` eine mögliche Schadensschwere über die Eigenschaft $p_{severity} = \{1, 2, .., 5\}$ definiert, sodass mit steigendem Wert von $p_{severity}$ leichte bis katastrophalen Schäden spezifiziert werden. Diese Einordnung ist abhängig von weiteren Aspekten wie der `OperationalSituation`, da beispielsweise Situationen im Hafenbereich unter Umständen weniger kritisch sein können als Situationen auf offener See. Zu-

[1] https://soop.offis.de/joomla/, http://www.hs-emden-leer.de/forschung-transfer/projekte/soop-sichere-offshore-operationen.html

sätzlich spielen die möglichen Schadensfolgen (`Exposures`) eine wesentliche Rolle, sodass $\Gamma : exposes \Rightarrow he_l \times \subset Exposures$ mögliche Schadensfolgen (`Exposures`) mit dem jeweiligen `HazardousEvent` in Zusammenhang bringt. Darüber hinaus wird mit der Relation $\Gamma : occurs\_in$ auf die für das `HazardousEvent` zu betrachtende `OperationalSituation` in der dieses eintreten kann verwiesen. Da das `HazardousEvent` im Rahmen einer geplanten Operation auftritt, wird dieser Zusammenhang mit dem in der Systemdefinition entwickelten Modell als $\Gamma : part\_of \Rightarrow he_l \times Operation$ ausgedrückt.

Eine Schadensfolge (`Exposure`) beschreibt mit Hilfe der Attribute p_{name} und $p_{beschreibung}$ die Auswirkungen und damit das Gefahrenpotential resultierend aus dem Eintreten des relevanten gefährlichen Ereignisses he_l, was durch die Relation $\Gamma : exposes$ abgebildet wird. Ein `HazardousEvent` kann dabei mehrere `Exposures` haben, sodass auch unterschiedliche Schadensfolgen wie Personen- oder Sachschäden individuell berücksichtigt werden können.

Mit Hilfe der Betriebssituation (`OperationalSituation`) wird durch die Attribute p_{name} und $p_{beschreibung}$ der Umstand in dem ein gefährliches Ereignis auftreten kann definiert [ISO08]. So können verschiedene Situationen im Modell als `OperationalSituation` hinterlegt werden, wie beispielsweise Situationen im Hafenbereich oder auf offener See, um Szenarien zu spezifizieren die im Verlauf einer Operation stattfinden können. Der Zusammenhang zum relevanten `HazardousEvent` wird dabei über $\Gamma : occurs\_in$ hergestellt.

Eine Gefährdung (`Hazard`) entspricht einer potentiellen Schadensquelle ([Ren13, S. 55], [ISO08]), welche über $\Gamma : contains$ individuell in Kontext gesetzt wird, sodass Zusammenhänge zur relevanten `OperationalSituation` als $\Gamma : occurs\_in$ und zu möglichen Folgen als $\Gamma : exposes$ vom `HazardousEvent` nachvollzogen werden können. Um eine Gefährdung h_i genauer aufschlüsseln zu können, werden der Gefährdung mögliche Ursachen (`Causes`) zugeordnet ($\Gamma : caused\_by \Rightarrow h_i \times Causes$), um somit verursachende Faktoren abzubilden. Eine Gefährdung kann somit mehrere mögliche Ursachen assoziieren, sodass somit aufgelistet werden kann, welche Gefährdungen durch welche Ursachen potentiell ausgelöst werden können. Jede Gefährdung wird dabei mit einem `HazardousEvent` in Beziehung gesetzt, in welchem die mögliche Schadensschwere als Attribut, unter Berücksichtigung einer `OperationalSituation`, festgelegt wird.

Eine Ursache (`Cause`) spezifiziert einen möglichen Defekt, Fehler, Störung o.ä. der dazu beitragen kann eine Gefährdung h_i auszulösen ($\Gamma : caused\_by$). Ursachen hängen eng mit stattfindenden Aktivitäten der zugrundeliegenden `Operation` zusammen, sodass diese über die Relation $\Gamma : might\_contain \Rightarrow (Activity \in Operation) \times Causes$ miteinander in Verbindung gesetzt werden. In Erweiterung zu den bestehenden Attributen wird eine Ursache c_b um das Attribut $p_{frequency} = \{1, 2, .., 5\}$ ergänzt. Mit $p_{frequency}$ wird die

Häufigkeit des Eintritts von c_b, wie in der maritimen Domäne üblich (siehe Kapitel 2), eingeordnet. Ein hoher Wert von $p_{frequency}$ steht dabei für häufiges, ein niedriger Wert hingegen für ein selteneres Eintreten des `Cause` c_b. Eine mögliche Wertezuordnung dieses Attributs basiert zumeist auf der subjektiven Einschätzung eines jeweiligen Sicherheitsexperten [Alt10, S. 22]. Diese subjektive Zuordnung ist notwendig, da häufig keine exakten Werte für Eintrittswahrscheinlichkeiten in Operationen vorliegen wie es beispielsweise bei messbaren Maschinenausfällen der Fall ist. In anderen Anwendungsfällen, in denen konkrete Wahrscheinlichkeitswerte beispielsweise durch Statistiken o.ä. vorliegen, werden diese vorwiegend genutzt. Zusammen mit dem Attribut $p_{severity}$ des `HazardousEvent` bilden die $p_{frequency}$ der `Causes` die sogenannten Risikowerte. Diese sind die Werte die die Schadensschwere sowie Häufigkeit und somit den Eintritt einer Gefährdung bzw. Ursache quantifizieren [Sch12], [Bra02]. Auf Basis dieser Werte wird später die Risikoprioritätszahl durch Multiplikation der Schadensschwere und Häufigkeit, wie in Kapitel 2 beschrieben, ermittelt [Fes14, S. 125].

Mit Hilfe risikomindernder Maßnahmen (`MitigationMeasures` und `CounterMeasures`) können Maßnahmen in einer Operation abgebildet werden, um die Risikoprioritätszahl zu verringern. Diese Maßnahmen, wie beispielsweise Schutzkleidung oder Hilfestellungen, können dabei gezielt zur Verringerung der Schadenschwere $p_{severity}$ eines `HazardousEvent` oder der Häufigkeitsstufe $p_{frequency}$ möglicher `Causes` eingesetzt werden. Da diese Maßnahmen, wie auch mögliche Ursachen maßgeblich mit der zugrundeliegenden `Operation` und den darin stattfindenden Aktivitäten zusammenhängen, wird dies über $\Gamma : part\_of \Rightarrow (a_i \in Activities) \times mm_u$ bzw. cm_k im Modell abgebildet. Es kann dabei unterschieden werden zwischen Maßnahmen betreffend der Häufigkeitsstufe (`CounterMeasure`) und der Schadensschwere (`MitigationMeasure`). Eine `MitigationMeasure` enthält somit das Attribut $p_{severityFactor} = \{1, 2, .., 5\}$, bzw. eine `CounterMeasure` zur Beschreibung des jeweiligen Einflusses das Attribut $p_{frequencyFactor} = \{1, 2, .., 5\}$. Diese Attribute wirken jeweils auf das durch die Relation $\Gamma : reduces$ adressierte `HazardousEvent` he_l ($\Gamma : reduces \Rightarrow he_l \times mm_u$) bzw. `Cause` c_b ($\Gamma : reduces \Rightarrow c_b \times cm_k$).

Derlei gesammelte Informationen und dafür getroffene Wertezuordnungen der Attribute dienen dazu weitergehend zu priorisieren und einzuordnen ([Kri13, S. 302]), um damit eingebundene Gefährdungen für die nachfolgende Risikoanalyse klassifizieren zu können [Vin07, S. 121]. Nachfolgend wird zunächst das Vorgehen zum Einpflegen dieser Informationen in Anlehnung an das vorgestellte Modell erläutert.

Vorgehen

Nach dem in Abbildung 3.6 rechts dargestellten Vorgehen kann die Gefährdungsidentifikation sowohl mit Schritt (1), Schritt (2) sowie auch mit beiden Schritten parallel begonnen

werden. Bei Schritt (1) werden zunächst die erforderlichen Gefährdungen, wenn bereits bekannt, modelliert, sodass für diese ein `Hazard` erstellt und über die Attribute p_{name} und $p_{beschreibung}$ sowie die Zuordnung ($\Gamma : contains$) zu einem `HazardousEvent` spezifiziert wird. In Schritt (2) können dann für diesen `Hazard` relevante Ursachen als `Cause` modelliert und ebenfalls über deren Attribute p_{name}, $p_{beschreibung}$ spezifiziert werden. Mit Hilfe der Relation $\Gamma : caused\_by$ erfolgt dabei die Zuordnung eines `Cause` zu einem `Hazard`. Diese Reihenfolge entspricht einem Top-down bzw. deduktiven Vorgehen, bei dem zunächst der `Hazard` und im Hinblick darauf mögliche `Causes` ermittelt und modelliert werden. Dar-

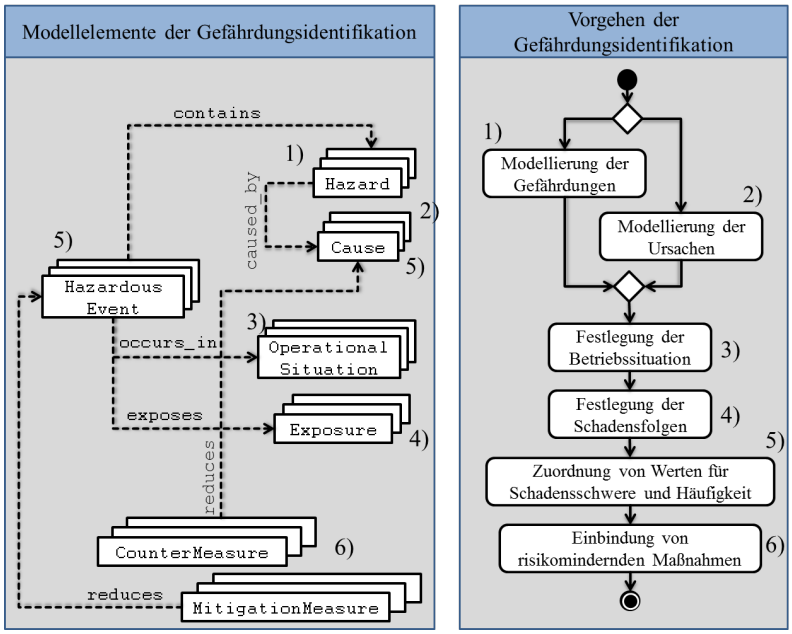

Abbildung 3.6: Schematisches Vorgehen der Gefährdungsidentifikation

über hinaus ist mit dem Ansatz jedoch auch ein bottom-up bzw. induktives Vorgehen möglich, sodass auch zunächst `Causes` in Schritt (2) ermittelt und daraufhin relevante `Hazards` identifiziert und modelliert werden können. Die Ermittlung und Modellierung der `Causes` kann dabei systematisch anhand des in der Systemdefinition entwickelten Prozessmodells erfolgen, sodass die darin enthaltenen Aktivitäten hinsichtlich möglicher Ursachen schrittweise überprüft werden. Identifizierte und modellierte `Causes` einer Aktivität können dann mit Hilfe der Relation $\Gamma : might\_contain$ verknüpft werden. Dieses Vorgehen eignet sich vorzugsweise für Anwendungsfälle in denen die Gefährdungen nicht bereits durch Erfahrungswissen bekannt sind, sodass dafür zunächst systematisch in Schritt(2) mögliche `Causes` und somit von den nominalen Abläufen abweichende Aspekte modelliert werden können. Anschließend kann systematisch überprüft werden, inwiefern sich diese zu möglichen Gefährdungen auswirken können, sodass dadurch neue Gefährdungen identifiziert

und als `Hazards` in Schritt (1) modelliert werden können.

In Schritt (3) wird für jedes enthaltene `HazardousEvent` je eine `OperationalSituation` festgelegt und über die Attribute beschrieben, sodass der Kontext der Gefährdung über die Beschreibung der Situation ersichtlich wird. Schritt (4) umfasst analog zu Schritt (3) die Festlegung der Schadensfolgen, sodass für ein `HazardousEvent` mögliche `Exposures` modelliert und mit Hilfe der Attribute genauer beschrieben werden. Mit den Schritten (3) und (4) wird somit der Umstand der zugrundeliegenden Gefährdung spezifiziert, sodass der Kontext des Auftretens sowie daraus resultierende Folgen beschrieben und dokumentiert werden. Schritt (5) umfasst daraufhin die Quantifizierung der Risikowerte, sodass die Attribute $p_{frequency}$ der `Causes` hinsichtlich der Häufigkeitsklasse sowie $p_{severity}$ der `HazardousEvents` hinsichtlich der Schadensschwere quantifiziert und zugeordnet werden. Die Bestimmung dieser Werte wird durch verschiedene Bedingungen beeinflusst [GLS10, S. 33], sodass über $\Gamma : occurs\_in$ und $\Gamma : exposes$ die Situation des Eintritts und mögliche Schadensfolgen zur genaueren Eingrenzung, neben umfangreichem Erfahrungswissen [Alt10], dienen können.

Abschließend können in Schritt (6) risikomindernde Maßnahmen eingebunden werden, sodass `CounterMeasures` und `MitigationMeasures` erstellt und über $\Gamma : reduces$ relevanten `Causes` oder `HazardousEvents` zugeordnet werden. Mit der Bestimmung des Attributs $p_{frequencyFactor}$ bzw. $p_{severityFactor}$ wird dabei die zuvor zugeordnete $p_{frequency}$ eines `Cause` bzw. $p_{severity}$ eines `HazardousEvents` beeinflusst.

Um nach dieser Vorgehensweise, wie in Abbildung 3.6 dargestellt, Informationen und Zusammenhänge in der Gefährdungsidentifikation ermitteln zu können, ergeben sich verschiedene Informationsquellen aus denen diese auf unterschiedliche Weise gewonnen werden können:

- aus dem Erfahrungswissen des jeweiligen Sicherheitsexperten
- Literaturquellen wie Unfallberichte und Statistiken
- für unbekannte Anwendungsfälle durch erneute systematische Ermittlung beispielsweise durch Fragebögen oder Checklisten
- prozessorientierte Betrachtung der Systemdefinition wie zuvor beschrieben
- anhand der in diesem Ansatz entwickelten Wissensbasis

Das bisherige Vorgehen erfordert umfangreiches Erfahrungswissen des Anwendungsfalls [Alt10, S. 22], wobei zusätzlich Literaturquellen wie Unfallberichte, oder Ansätze zur systematischen Ermittlung beispielsweise durch Fragebögen, Checklisten o.ä. genutzt werden können. Mit dem neu konzipierten Ansatz kommen ergänzende Möglichkeiten hinzu, sodass die prozessorientierte Betrachtung der erfassten Abläufe in der Systemdefinition eine

weitere Grundlage für eine systematische, sowohl induktive als auch deduktive, Ermittlung durch die Schritte (1) und (2) darstellt. Bei dieser sind bereits die beteiligten Personen und deren Arbeitsabläufe erfasst, sodass diese im Rahmen der Gefährdungsidentifikation, fokussiert hinsichtlich möglicher Gefährdungen und Ursachen, hinterfragt und entsprechend dem Konzept zugeordnet werden können. Dies ermöglicht einen zusätzlichen Vorteil gegenüber dem bisherigen Vorgehen, da die Gefährdungsidentifikation dort häufig nicht-systematisch und mit wenig Einbeziehung der zugrundeliegenden Operation vorgenommen wird [Vin13]. Als weiteres kann die Wissensbasis als eine weitere Informationsquelle dienen, um weiteres Erfahrungswissen vergangener Anwendungsfälle unterstützend bereitzustellen. Diese wird daher im nachfolgenden Unterabschnitt beschrieben.

Wissensbasis als Informationsquelle Ein neuer Aspekt der durch den Ansatz hinzukommt ist eine effiziente Wiederverwendung von Informationen, was bisher einen offenen Bereich dargestellt hat [LGP11, S. 7]. Im Rahmen eines Lösungsansatzes werden daher Informationen durch die Wissensbasis unterstützend bereitgestellt, sodass aus vergangenen Anwendungsfällen bekannte, und mit diesem Vorgehen erfasste Informationen über die Zusammenhänge von Gefährdungen, Ursachen, Personen und Tätigkeiten, selektiert und genutzt werden können. Die Wissensbasis bildet damit aus Sicht der bisher aufgeführten Informationsquellen eine übergreifende Möglichkeit Erfahrungswissen des jeweiligen Sicherheitsexperten zu hinterlegen, welches bei der Planung eines Anwendungsfalls beispielsweise in der Systemdefinition oder Gefährdungsidentifikation eingepflegt wurde. Die Wissensbasis, wie schematisch in Abbildung 3.7 dargestellt, umfasst somit Informa-

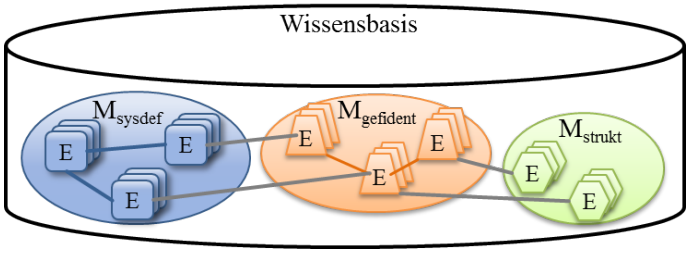

Abbildung 3.7: Schematische Darstellung der Wissensbasis

tionen als Elemente der Systemdefinition (M_{sysdef}), Gefährdungsidentifikation ($M_{gefident}$) sowie des nachfolgend in Kapitel 3.3.3 vorgestellten Modells M_{strukt} und Zusammenhänge dieser Modelle. Diese Informationen können durch die Wissensbasis hinterlegt und bereitgestellt werden. Befindet man sich beispielsweise nach Abbildung 3.6 in Schritt (1) um Gefährdungen zu modellieren, so wird dabei die Wissensbasis durchsucht. Dabei können sämtliche der beschriebenen Relationen der Modelle wie von M_{sysdef} oder $M_{gefident}$ genutzt werden, um möglicherweise relevante Informationen zu finden und bereitstellen zu können. Somit könnte nach Abbildung 3.6 Schritt (1) die Wissensbasis mit Hilfe der Re-

lationen Γ : *contains* und Γ : *part_of* beispielsweise dahingehend durchsucht werden, ob vergleichbare `Operationen` vergangener Anwendungsfälle in der Wissensbasis existieren, um dort betrachtete `Hazards` bereitzustellen. Ist dies der Fall können diese sodann für das aktuelle Vorgehen übernommen werden. Darüber hinaus können wahlweise auch damit zusammenhängende `Causes` durch die Γ : *caused_by* Relation somit erneut für Schritt (2) nach Abbildung 3.6 als Information bzw. Element aus $M_{gefident}$ verwendet werden. Analog dazu verhält es sich mit der Wiederverwendung anderer Informationen, sodass die Wissensbasis dafür eine strukturierte, durchsuchbare Grundlage liefert, um eingepflegtes Wissen bereitzustellen. Ergänzend können, bei fortlaufender Verwendung und sukzessiver Erweiterung der Wissensbasis mit Informationen mehrerer Anwendungsfälle, auch die nach Abbildung 3.6 Schritt (5) zugeordneten Wertestufen unterstützend bereitgestellt werden. Beispielsweise für über mehrere Anwendungsfälle hinweg wiederkehrende `Causes` oder `HazardousEvents` können somit in der Wissensbasis mehrere unterschiedliche Werte von $p_{frequency}$ bzw. $p_{severity}$ vorliegen. Diese können in Form graphischer Werteverläufe dargestellt werden, um somit beispielsweise den Trend als Orientierungshilfe für neue Zuordnungen zu ermöglichen. Jedoch ist bei jeder erneuten Verwendung von Informationen zu überprüfen, ob diese tatsächlich relevant und anwendbar sind.

Diese Möglichkeiten zur Wiederverwendung ergeben sich durch die Strukturierung und zusammenhängenden Betrachtung der Modelle von Systemdefinition und Gefährdungsidentifikation. Weiterhin kann durch diese gemeinsame Betrachtung ermöglicht werden, aus der Wissensbasis relevante Informationen herauszusuchen, sodass beispielsweise verknüpfte Informationen mit ähnlichen, in der Wissensbasis hinterlegten Operationen und darin enthaltenen Tätigkeiten, Akteuren oder Gefährdungen, durchsucht und für zukünftige Anwendungsfälle bereitgestellt werden können. Das weitere Konzept der Wissensbasis, in welchem diese mit Informationen befüllt wird, wird im späteren Abschnitt 3.3.4 - Risikobewertung erläutert.

Anwendungsbeispiel

Für das betrachtete Anwendungsbeispiel der Kranarbeiten bedeutet das erläuterte Konzept, dass zunächst nach Schritt (1) des Vorgehens die relevanten Gefährdungen identifiziert und modelliert werden müssen, entsprechend Abbildung 3.6. Eine bekannte Gefährdung ist dafür das Zusammenstoßen der Ladung, sodass ein `Hazard` mit $p_{name} = \{name,$ Zusammenstoßen der Ladung$\}$ erstellt wird. Nach Schritt (2) müssen dafür nun mögliche Ursachen identifiziert werden, wobei das in der Systemdefinition entwickelte Prozessmodell als Orientierungshilfe für eine systematische Ermittlung dienen kann. Somit werden sukzessive die Tätigkeiten des Kranführers durchgegangen, mögliche `Causes` modelliert und wie in Abbildung 3.8 dargestellt verknüpft. Als Γ : *might_contain* wird dabei jedes `Cause` Element mit einer Tätigkeit innerhalb einer `WorkingProcedure` in Zusammenhang gebracht. Darauffolgend werden im Rahmen von Schritt (3) für jeden modellierten

`Hazard` eine Betriebssituation als `OperationalSituation` festgelegt und mit Hilfe eines `HazardousEvent` kombiniert. Die exemplarisch betrachtete Gefährdung tritt dabei überwiegend in Betriebssituationen mit bereits angehobener bzw. schwebender Last auf, was als p_{name} und $p_{beschreibung}$ der erstellten `OperationalSituation` beschrieben wird. In Schritt (4) werden daraufhin mögliche Schadensfolgen als je eine `Exposure` modelliert und als $\Gamma : exposes$ mit dem relevanten `HazardousEvent` verknüpft. Mögliche Schadensfolgen können für das Anwendungsbeispiel zunächst grob als Personen- oder Sachschäden identifiziert werden, sodass dafür zwei `Exposures` erstellt werden. Darauf folgt in Schritt (5) die Zuordnung von Werten zur Quantifizierung der Schadensschwere und Häufigkeit. Eine Stufe der Schadensschwere wird für jedes erstellte `HazardousEvent` als $p_{severity}$ festgelegt, wobei sich für den Zusammenstoß mit schwebender Last mit möglichen Personen- und Sachschäden eine $p_{severity} = 4$ ergibt. Darüber hinaus werden Häufigkeitsstufen für jede der nach Schritt (2) modellierten `Causes` als $p_{frequency}$, wie in Abbildung 3.8 dargestellt, zugeordnet. Die für dieses Anwendungsbeispiel zugeordneten Werte von $p_{severity}$ und $p_{frequency}$ sind fiktiv gewählt und dienen ausschließlich der Veranschaulichung des Vorgehens.

Im Anschluss werden in Schritt (6) risikomindernde Maßnahmen wie `CounterMeasures`

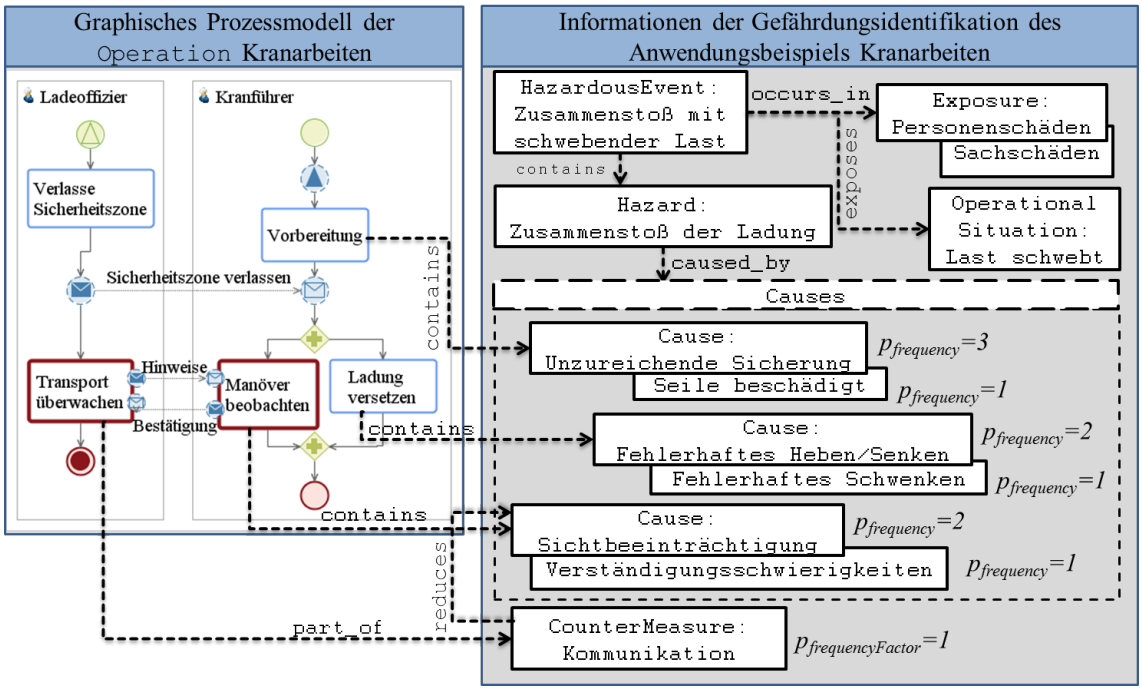

Abbildung 3.8: Schematische Darstellung der in der Gefährdungsidentifikation eingepflegten Informationen mit fiktiven Häufigkeitsstufen und Zusammenhänge zum zugrundeliegenden Prozessmodell des Anwendungsbeispiels

eingebracht, sodass beispielsweise die Sichtbeeinträchtigung des Kranführers durch zusätzliche Kommunikation mit dem Ladeoffizier verbessert werden kann. Somit wird eine `CounterMeasure` erstellt und mit $\Gamma : part\_of$ der Tätigkeit „Transport überwachen“ zugeordnet. Darüber hinaus wird als $\Gamma : reduces$ festgelegt, dass der `Cause` mit $p_{name} = \{name,$ Sichtbeeinträchtigung$\}$ von der `CounterMeasure` durch das Attribut $p_{frequencyFactor} = 1$, wie in Abbildung 3.8 dargestellt, betroffen ist.

Der Aspekt der Wissensbasis könnte in diesem Anwendungsbeispiel, wenn bereits durch Informationen gefüllt, Informationen zur Wiederverwendung bereitstellen. Es können dabei beispielsweise einzelne Gefährdungen und damit verbundene Ursachen erneut genutzt werden. Angenommen in vergangenen Anwendungsfällen sind bereits Kranarbeiten an Land geplant und die dabei eingepflegten Informationen in die Wissensbasis überführt worden, so kann die Wissensbasis dahingehend Informationen ähnlicher Operationen, wie beispielsweise eine weitere Gefährdung mit entsprechenden Ursachen, bereitstellen. Konzeptionell kann mit der Wissensbasis, wie in Abbildung 3.7 schematisch dargestellt, grundsätzlich jedes der in die Modellierung eingebrachten Elemente, deren Verknüpfungen und Attribute, gespeichert, bereitgestellt und damit erneut in späteren Anwendungsfällen genutzt werden.

Durch den Schritt der Gefährdungsidentifikation wurde die Planung der Operation systematisch um erforderliche Informationen über mögliche Gefährdungen und Ursachen ergänzt, wobei unterstützend die Wissensbasis genutzt werden kann. Im nachfolgenden Schritt wird die geplante Operation mit darin enthaltenen Informationen zur Risikoanalyse mit Hilfe von Fehlerbäumen genutzt.

3.3.3 Risikoanalyse

Nachdem die Schritte zur Systemdefinition und Gefahrenidentifikation abgeschlossen, und in diesen die Planung mit den Modellen vervollständigt wurde, folgt der Schritt der Risikoanalyse nach dem in Abbildung 3.9 dargestellten Vorgehen. Dieses Vorgehen findet sich dabei in der Gliederung der nachfolgenden Unterabschnitte wieder. Dabei werden die zuvor erfassten Informationen der Systemdefinition und Gefährdungsidentifikation genutzt und in Schritt (1) **Strukturierung** zunächst strukturiert, sodass im Kontrast zum Stand der Technik Kombinationen von Ursachen berücksichtigt und damit auch Verkettungen betrachtet werden können. Weiterhin wird dabei, aufgrund der ansonsten hohen Zeit- und Kostenaufwände solcher Arbeiten ([CACO06], [LST09]), ein Konzept vorgestellt durch das sowohl eine manuelle als auch eine automatisierte Strukturierung als Orientierungshilfe mit Bezug zu den zugrundeliegenden Abläufen der Systemdefinition ermöglicht wird. Darauffolgend werden diese Vorarbeiten genutzt und darauf aufbauend ein Ansatz konzipiert diese in Schritt (2) **Konstruktion** automatisiert zu formalisieren, sodass diese als Fehlerbaum darstellbar sind. Da sodann Fehlerbäume anhand dieser Informationen erstellt werden können, besteht damit eine formalisierte Struktur die in Schritt (3) der **Berechnung** zur Auswertung der Fehlerbäume genutzt wird. Abschließend erfolgt in Schritt (4)

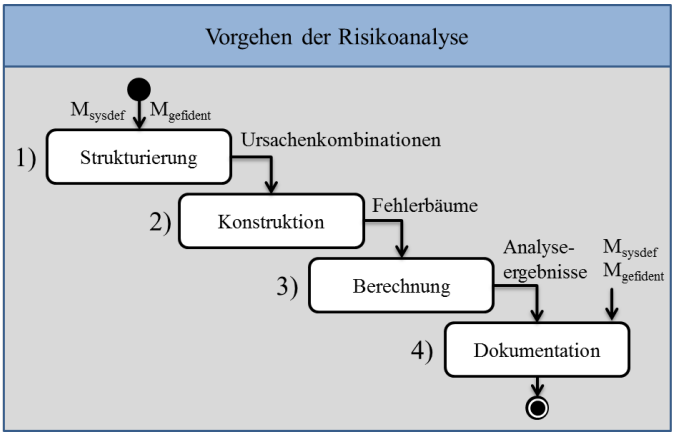

Abbildung 3.9: Abstraktes Vorgehen der Risikoanalyse

mit Hilfe der **Dokumentation** eine zusammenfassende Darstellung der eingepflegten Informationen der Systemdefinition und Gefährdungsidentifikation sowie der Ergebnisse aus der Risikoanalyse, sodass sowohl prozessorientierte als auch risikorelevante Aspekte aufgeführt werden können.

1) Strukturierung

Für den ersten Schritt der Risikoanalyse werden die zugrundeliegenden Informationen, die im Rahmen der Systemdefinition und Gefährdungsidentifikation zusammengetragen wurden, als Vorbereitung für die darauffolgende Konstruktion und Risikoberechnung strukturiert. Diese Informationen liegen zwar vorstrukturiert im Sinne der Prozessmodellierung vor, indem dort Gefährdungen und Ursachen sowie Ursachen mit entsprechenden Elementen des Prozessmodells, wie für die Modelle M_{sysdef} und $M_{gefident}$ beschrieben, miteinander in Beziehung gesetzt wurden. Jedoch bildet dies nur eine Auflistung der Gefährdungen und Ursachen ab, wie sie auch im Stand der Technik gemacht wird, sodass keine Informationen darüber vorhanden sind welche Ursachen tatsächlich eigenständig ausreichend sind die Gefährdung auszulösen bzw. welche Kombinationen weiterer Ursachen dafür notwendig sind. Solche Strukturierungen werden im Rahmen von Sicherheitsanalysen, beispielsweise bei Erstellung von Fehlerbäumen, manuell vorgenommen und werden als zeit- und kostenaufwändig wahrgenommen [CACO06], [LST09]. Um derartige Strukturierungen in diesem Ansatz vornehmen zu können, wird im Folgenden ein Konzept, beginnend mit dem dafür entwickelten Modell und einem systematischen Vorgehen mit Möglichkeit zur unterstützenden automatisierten Strukturierung vorgestellt.

Modell Im vorangegangenen Schritt der Gefährdungsidentifikation und des dort vorgestellten Modells $M_{gefident}$ wurde zunächst als $\Gamma : caused\_by$ ein einfacher Zusammenhang

zwischen `Hazard` und dazu beitragenden `Causes` hergestellt. Um diesen Zusammenhang weiter zu strukturieren und somit auch Kombinationen von `Causes` abbilden zu können, umfasst das Modell zur Strukturierung M_{strukt} die folgenden Elemente:

$$E = \{ \quad CauseStructures = \{cs_1, cs_2, ..., cs_f\}, \\ LogicOperators = \{lo_1, lo_2, ..., lo_g\}, \\ \}$$

Durch diese Elemente wird die logische und hierarchische Strukturierung von Ursachen (`CauseStructure`) mit Hilfe boolescher Operatoren (`LogicOperator`) in Form einer einfachen Baumstruktur ermöglicht, sodass entsprechende Verkettungen von Ursachen in dem Modell abgebildet werden können. Eine erstellte `CauseStructure` kann für je einen `Hazard` als $\Gamma : structures \Rightarrow h_i \times cs_f$ verknüpft werden, wobei $LogicOperator \in CauseStructure$, sodass als Wurzelelement überwiegend ein `LogicOperator` genutzt wird. Alle weiteren über $\Gamma : caused\_by$ zugeordneten `Causes` werden bei der Strukturierung assoziiert, sodass diese jeweils als $\Gamma : associates \Rightarrow cs_f \times c_b \in Causes$ nachvollziehbar sind. Dadurch können zugrundeliegende `Causes` strukturiert, jedoch auch weiterhin unabhängig von der `CauseStructure` genutzt und auch später wiederverwendet werden. Eine vorgenommene Strukturierung kann durch dieses Modell verändert oder gelöscht werden, ohne dass die zugrundeliegenden `Causes` erneut eingepflegt werden müssen. Die booleschen Operatoren dienen darüber hinaus dazu, Ursachen zu kombinieren ($\Gamma : clusters \Rightarrow lo_g \times CauseStructures$) sowie Hierarchieebenen in der Baumstruktur zu ermöglichen. Ein Operator erfordert dabei entsprechend der booleschen Algebra die Existenz mindestens zweier Parameter von `CauseStructure` oder weiterer `LogicOperator`.

Vorgehen Zur Durchführung der Strukturierung mit dem beschriebenen Modell kann im Vorgehen, wie in Abbildung 3.10 dargestellt, zunächst die Möglichkeit nach Schritt (1) zur manuellen Strukturierung vorgenommen werden. Dabei werden die in der Gefährdungsidentifikation ermittelten und modellierten `Causes` eines `Hazard` genutzt. Der Nutzer kann dafür zunächst eine `LogicStructure` erstellen und dieser eine boolesche Funktion, wie beispielsweise $\wedge$ oder $\vee$, zuweisen. Darüber hinaus wird diese `LogicStructure` als Wurzelelement der zu erstellenden Baumstruktur genutzt und über $\Gamma : structures$ dem betrachteten `Hazard` zugeordnet. Darunterliegend werden daraufhin weitere `LogicStructures` erstellt und der ersten über $\Gamma : clusters$ untergeordnet, oder es werden `CauseStructures` anhand der über $\Gamma : caused\_by$ verfügbaren `Causes` erstellt und über $\Gamma : associates$ assoziiert. Durch die weitere Nutzung von Operatoren wird diese Strukturierung um weitere Hierarchieebenen ergänzt. Die logischen Zusammenhänge und hierarchische Strukturierung entsprechen dabei im Wesentlichen dem Vorgehen zur manuellen Erstellung von Fehlerbäumen, bei der diese Überlegungen ebenfalls gemacht werden müssen. Dies ist jedoch wie in

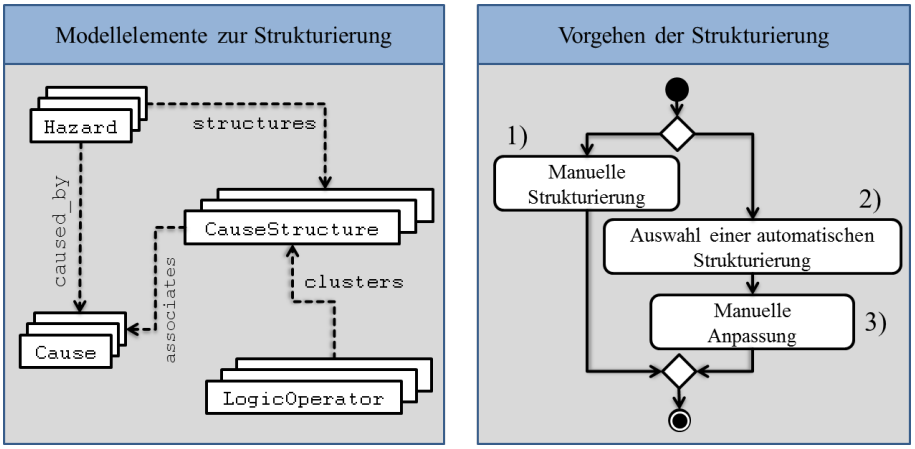

Abbildung 3.10: Vorgehen der Strukturierung

Kapitel 2 beschrieben ein zeitaufwändiges Unterfangen, sodass in diesem Ansatz, wie in Abbildung 3.10 Schritt (2) dargestellt, eine Möglichkeit zur automatischen Strukturierung geschaffen wurde, um den Anwender dabei unterstützen zu können. Diese wird im Detail im nachfolgenden Unterabschnitt erläutert. Die Möglichkeit zur automatischen Strukturierung ist dabei als Orientierungshilfe für die Strukturierung vorgesehen, sodass die damit vorgenommene Strukturierung in Schritt (3) überprüft und auf den Anwendungsfall nach dem Vorgehen wie in Schritt (1) beschrieben angepasst werden kann.

Automatische Strukturierung Wie in Kapitel 2.3.1 erläutert, ist die manuelle Strukturierung aufwändig, sodass bereits Ansätze entwickelt wurden, um in verschiedenen Anwendungsfällen und Domänen eine automatisierte Strukturierung, zur späteren Visualisierung und Analyse als Fehlerbaum, durchführen zu können. Dabei wurde in Kapitel 2 jedoch unter anderem Handlungsbedarf hinsichtlich einer prozessorientierten Perspektive zur tatsächlichen Planung und Analyse von Operationen identifiziert. Jedoch konnte festgestellt werden, dass eine zusammenhängende Modellgrundlage eine erforderliche Basis für einen solchen Ansatz darstellt. Diese Basis wurde mit Hilfe der vorangegangenen Schritte zur Systemdefinition und Gefährdungsidentifikation des Ansatzes und den dort entwickelten Modellen M_{sysdef} und $M_{gefident}$ geschaffen. Auf dieser Basis wird daher in diesem Abschnitt eine Möglichkeit zur automatischen Strukturierung zur weiteren Unterstützung des Nutzers vorgestellt. Der dafür entwickelte Ansatz wird in Abbildung 3.11 schematisch dargestellt und besteht im Kern aus verschiedenen Algorithmen die das Modell M_{strukt} zur Strukturierung erstellen. Erforderlich ist dafür jeweils die Nutzung der bestehenden Informationen, sodass beispielsweise stets $M_{gefident}$ genutzt wird, um die Strukturierung für einen bestimmten `Hazard` und dessen als $\Gamma : caused\_by$ assoziierte `Causes` durchführen zu können. Darüber hinaus haben bestehende Ansätze gezeigt (siehe Kapitel 2), dass auch die

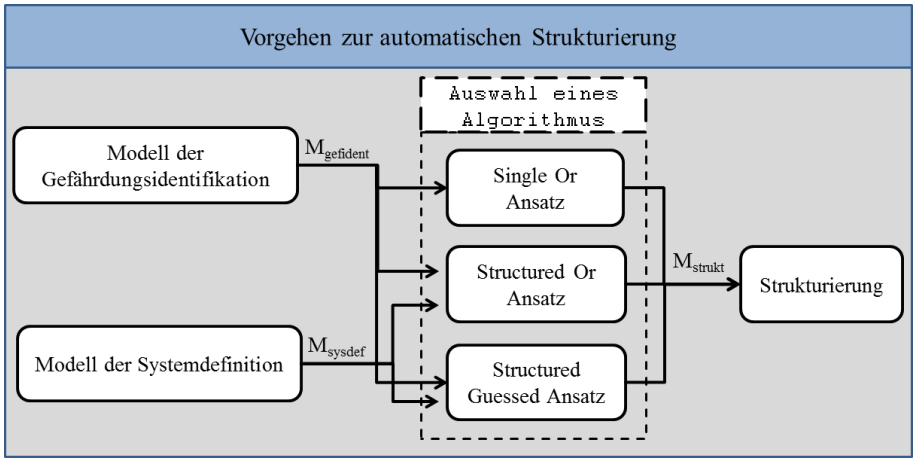

Abbildung 3.11: Schematische Darstellung der automatischen Strukturierung

Verkettung weiterer Systembestandteile, wie beispielsweise in Form der Abläufe, nutzbar sind. Dadurch lassen sich mit Hilfe paralleler oder sequentieller Verkettungen, wie beispielsweise Bestandteil des graphischen Prozessmodells in M_{sysdef}, logische Zusammenhänge für die Strukturierung ableiten. Um dies in einem Lösungsansatz abzubilden, wurden wie in Abbildung 3.11 dargestellt, Algorithmen zur automatischen Strukturierung entwickelt, die nachfolgend erläutert werden. Eine Planung der Arbeitsabläufe wie in M_{sysdef} kann dabei als Hinweis und mögliche Datenquelle für eine Strukturierung dienen, die im Rahmen der weiteren Nutzung durch einen Sicherheitsexperten weiter verfeinert werden kann. Es ist daher anzumerken, dass der jeweilige Nutzer und Sicherheitsexperte stets die Freiheiten hat zu entscheiden, ob eine Strukturierung auf Basis der Arbeitsabläufe den jeweiligen Anwendungsfall adäquat abbildet.

Single Or-Ansatz Einen ersten Ansatz zur einfachen Anwendung kann dafür eine Strukturierung ohne tiefere hierarchische oder logische Zuordnung der eingepflegten Ursachen ermöglichen. Dieses nachfolgend Single Or-Ansatz genannte Vorgehen ähnelt somit dem zuvor beschriebenen bisherigen Vorgehen nach Kapitel 2. Der Single Or-Ansatz kann daher zunächst als eine technologische Brücke verstanden werden, um das Vorgehen wie im aktuellen Stand der Technik beschrieben, für den Anwender abbilden zu können. Mit diesem werden die in das zugrundeliegende Modell $M_{gefident}$ eingepflegten Informationen, mit den als $\Gamma : caused\_by$ zugeordneten `Causes` eines selektierten `Hazard`, gesammelt und mit einem einzigen Or-Operator verknüpft. Dabei ist kaum eine kombinierte Betrachtung von Ursachen möglich, sodass vielmehr eine Auflistung möglicher Ursachen vorgenommen wird, die hier mit dem Single Or-Ansatz nachgebildet wird. Diese Betrachtung ist abgesehen davon, dass die Informationen über mögliche Ursachen einer Gefährdung genutzt werden, losgelöst von den Abläufen des Prozessmodells in M_{sysdef}. Das hat den Nachteil,

dass Änderungen der modellierten Abläufe, beispielsweise durch parallel durchgeführte Sicherheitsmaßnahmen, mit dieser Betrachtungsweise nicht berücksichtigt werden können, was gleichzeitig eine Problemstellung des Stands der Technik widerspiegelt.

Structured Or-Ansatz Mit einem weiteren, genannt Structured Or-Ansatz, wird zusätzlich eine im Vergleich zum Single Or-Ansatz weitergehende Strukturierung ermöglicht, sodass auf Basis der spezifizierten Abläufe des zugrundeliegenden Prozessmodells, hierarchische Beziehungen der `Causes` ermittelt und dargestellt werden können. Dieser nutzt weiterhin nur Or-Operatoren, sodass die zusätzliche Strukturierung kaum Auswirkungen auf eine nachfolgende Analyse hat, jedoch als Zwischenschritt oder Vorarbeit einer manuellen Strukturierung sinnvoll sein kann. Die Strukturierung der durch diesen Algorithmus erzeugten Vorschläge ergeben sich dabei aus der Verteilung von `Causes` eines `Hazard` im Prozessmodell auf unterschiedliche Tätigkeiten die über Γ : *contains* zusammenhängen. Die Tätigkeiten sind im Hinblick auf den Sequenz- bzw. Nachrichtenfluss des Prozessmodells miteinander verknüpft, sodass sich daraus eine Reihenfolge ergibt. Diese wird genutzt, sodass für beginnende Sequenzen, beispielsweise durch Verzweigungen mit `Gateways`, Nachrichtenflüsse durch `Signal-` oder `MessageEvents`, nachfolgende `Causes` entsprechende `CauseStructures` erstellt und mit einem `LogicOperator` verknüpft werden. Des Weiteren dient die hierarchische Modellierung der Abläufe mit enthaltenen Sub-Prozessen die wiederum Sub-Prozesse enthalten können, als weiteres Mittel, um darunterliegende `Causes` eines `Hazard` mit Hilfe von `CauseStructures` und `LogicOperators` zu strukturieren. Dabei wird für jede neue Hierarchieebene durch einen `SubProcess` ein weiterer `LogicOperator` erstellt und darunterliegende `Causes` entsprechend der dort enthaltenen Abläufe verknüpft. Dieses Vorgehen wird durch Algorithmus 1 beschrieben. Änderungen der zugrundeliegenden Abläufe im Prozessmodell, werden somit als Ergebnis dieses Algorithmus innerhalb der ermittelten Strukturierung sichtbar. Dadurch wird ermöglicht, dass Änderungen der zugrundeliegenden Systemdefinitionen direkten Einfluss auf die Risikoanalyse nehmen können, in Form dieses Algorithmus jedoch zunächst nur auf die Hierarchie der Strukturierung.

Structured Guessed-Ansatz Der Structured Guessed-Ansatz funktioniert ähnlich wie der Structured Or-Ansatz, ermöglicht jedoch zusätzlich zur reinen Strukturierung differenziertere Vorschläge hinsichtlich der genutzten `LogicOperators`, sodass Ursachen sowohl verundet als auch verodert werden können. Verzweigungen im Prozessmodell, beispielsweise durch `Gateways` oder Kommunikation, die eine parallele Ausführung nachfolgender Tätigkeiten ermöglichen, werden innerhalb dieses Algorithmus genutzt, um Ursachen der parallel durchgeführten Tätigkeiten mit einem And-Operator zu verknüpfen. Hingegen werden Ursachen von Tätigkeiten die im Ablauf sequentiell durchgeführt werden, durch einen Or-Operator kombiniert. Dieser Ansatz ist daran angelehnt, dass in vielerlei Anwendungsfällen, Parallelitäten bzw. Redundanzen eingeführt werden, um eine Verundung der par-

Algorithm 1 Konzept des Structured Or und Structure Guessed Ansatzes zur Strukturierung

```
1: Gegeben: Selektierte Gefährdung h ∈ Hazard einer op ∈ Operation
2: Ergebnis: CauseStructure cs für h
3:
4: node = StartEvent ∈ FlowObject of op
5: buildStructure(node, ∅)
6:
7: procedure BUILDSTRUCTURE(node ∈ FlowElement, cs ∈ CauseStructure)
8:     if node is forking then
9:         Create and assign LogicOperator to parent cs if existing
10:        for ∀ next FlowObjects of node do
11:            buildStructure(next, LogicOperator)
12:        end for
13:    else
14:        Create and assign LogicOperator to parent cs if existing
15:        for ∀ c if ∃ c : Cause ∈ h.caused_by ∩ node.contains do
16:            Create new cs ∈ CauseStructure associated to c ∧ assign to parent
17:        end for
18:        if node ∈ SubProcess then
19:            Create and assign LogicOperator to parent cs if existing
20:            buildStructure(StartEvent of SubLevel of SubProcess, LogicOperator)
21:            buildStructure(next FlowObject of node, LogicOperator)
22:        else
23:            buildStructure(next FlowObject of node, cs)
24:        end if
25:    end if
26: end procedure
```

allelen Bestandteile zu erreichen, was die Sicherheit des Anwendungsfalls erhöht bzw. das Risiko verringert. Die Ableitung von Und- bzw. Oder-Operatoren anhand paralleler oder sequentieller Zusammenhänge wird dabei bereits vom in Kapitel 2.2 beschriebenen Ansatz mit Hilfe von Blockdiagrammen, sowie von mehreren der in Kapitel 2.3.1 beschriebenen Ansätze genutzt. Darüber hinaus können mit dem hier entwickelten Ansatz differenziertere Fehlerfälle, als beispielsweise der Totalausfall einer Komponente, in Form der eingepflegten `Causes` verwendet werden. Der Structured Guessed-Ansatz nutzt dafür ebenfalls die zugrundeliegenden Zusammenhänge des graphischen Prozessmodells, welches wie in Algorithmus 1 verarbeitet wird und im Gegensatz zum Structured Or-Ansatz Verzweigungen nachfolgender `Causes` mit einem `LogicOperator` verundet.

Da mit Hilfe der zuvor erläuterten Ansätze in der Strukturierung auch Operatoren er-

zeugt werden können, die für die zugrundeliegende Gefährdung nicht relevant sind, muss im Anschluss eine Bereinigung der Strukturierung stattfinden. Dabei werden die beispielsweise durch Verzweigungen, dessen weitere Pfade jedoch keine Ursachen für die Gefährdung enthalten, innerhalb der Strukturierung entfernt. Diese sind dadurch Charakterisiert, dass keine, oder nur einzelne Kind-Elemente vorhanden sind.

Anwendungsbeispiel Zur weiteren Durchführung des Anwendungsbeispiels Kranarbeiten wird, im Rahmen des erläuterten Vorgehens nach Abbildung 3.10, mit Hilfe der automatischen Strukturierung vorgegangen. Somit kann dafür nach Schritt (2) einer der drei vorgestellten Ansätze ausgewählt werden, wobei zum Verständnis hier der Structured Guessed-Ansatz weiter fokussiert wird. Dieser nutzt zur automatischen Strukturierung sowohl die risikorelevanten Informationen, die im Rahmen der Gefährdungsidentifikation als Modell $M_{gefident}$ eingepflegt wurden, sowie die Zusammenhänge des graphischen Prozessmodells zur Abbildung der Operation in der Systemdefinition als M_{sysdef}. Das graphische Prozessmodell des Anwendungsbeispiels Kranarbeiten, wie in Abbildung 3.12 Mitte dargestellt, dient somit als Basis für diesen Ansatz, sodass davon ausgehend Algorithmus 1 mit dem obersten graphischen Element des Kranführers, dem `StartEvent` des Prozesses, beginnt. Dem weiteren Sequenzfluss folgend wird zunächst, aufgrund der Verzweigung

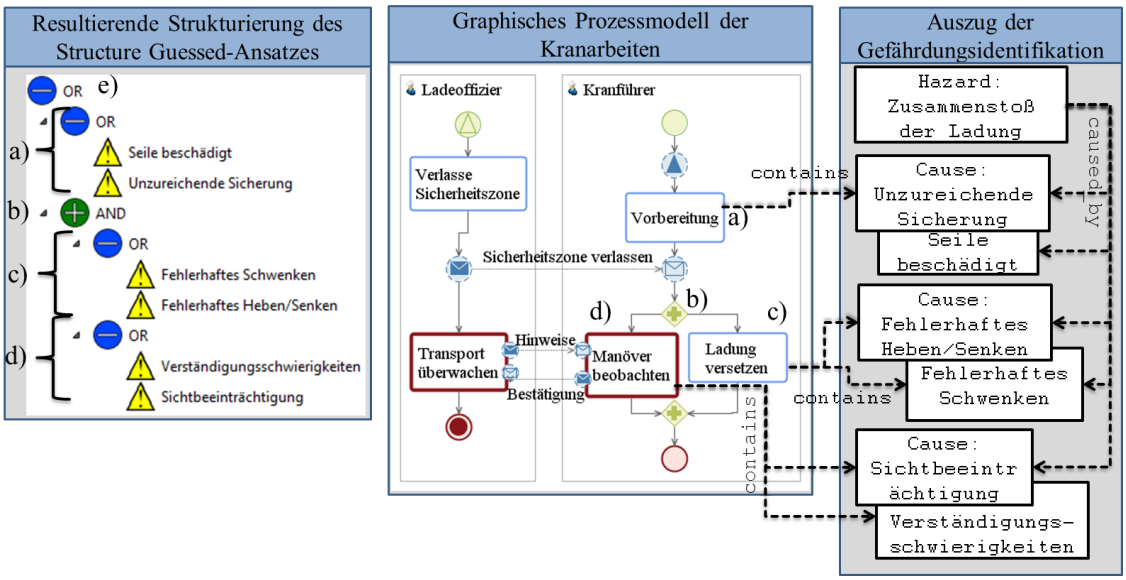

Abbildung 3.12: Schematische Darstellung einer resultierenden Strukturierung für das Anwendungsbeispiel Kranarbeiten

durch das `SendingSignalEvent`, ein `LogicOperator` zur Verundung erstellt, welcher somit das oberste Element der Strukturierung darstellt. Anschließend wird in Schritt (a) initial

ein `Task` mit $\Gamma : contains \cap \Gamma : caused\_by$ und somit möglichen `Causes` des selektierten `Hazard` mit $p_{name} = \{name,$ Zusammenstoß der Ladung$\}$, wie in Abbildung 3.12 rechts dargestellt, gefunden. Diese `Causes` werden dabei vom Algorithmus genutzt und führen zur Strukturierung wie in Abbildung 3.12 links (a) dargestellt, indem diese unter den zuvor erstellten `LogicOperator` verbunden werden. Darüber hinaus wird in (b) durch das `Gateway` im Prozessmodell eine Verzweigung modelliert, die zur Erstellung einer weiteren `LogicStructure` in Form eines Und-Operators führt, wobei daraufhin der Algorithmus für sämtliche Pfade dieser Verzweigung fortgeführt wird. In diesen wird in (c) ein weiterer `Task` sowie in (d) ein `SubProcess` mit relevanten `Causes` identifiziert und für die Strukturierung, wie in Abbildung 3.12 links dargestellt, genutzt.

Die in den Schritten (b)-(d) vorgenommene Strukturierung drückt damit aus, dass sich nur kombiniert `Causes` des Ladung Versetzens und Manöver Überwachens auswirken können. Somit beschreibt die Strukturierung, dass fehlerhafte Manöver wie Heben, Senken oder Schwenken der Ladung sich nicht eigenständig auswirken können, da dies stets durch die Überwachung und Beobachtung rechtzeitig erkannt und korrigiert werden kann. Nur bei nebenher auftretenden Fehlern bei der Beobachtung, sodass fehlerhafte Manöver nicht erkannt werden, führt dies zu weiteren Auswirkungen wie in der Strukturierung als Verundung dargestellt. Entsprechend des Vorgehens nach Abbildung 3.10 kann nach Abschluss dieser automatischen Strukturierung in Schritt (3) eine manuelle Anpassung erfolgen, was beispielsweise für den obersten `LogicOperator` sinnvoll erscheint, sodass dieser in (e) in einen Oder-Operator überführt wird.

Durch den Schritt der Strukturierung konnten die zuvor im Rahmen der Gefährdungsidentifikation ermittelten Informationen für die anschließende Risikoanalyse durch Fehlerbäume vorbereitet werden. Die dabei vorgenommene Strukturierung von Ursachen einer Gefährdung dient somit im nachfolgenden Schritt zur automatisierten Konstruktion von Fehlerbäumen.

2) Konstruktion

Damit die Risikoanalyse im Sinne der Berechnung der Risikowerte erfolgen kann, müssen dafür zunächst die notwendigen Informationen zusammengetragen werden. Vorarbeiten dafür wurden bereits im vorangegangenen Schritt der Strukturierung gemacht. Im Rahmen dieses Unterabschnitts werden daher bereits vorstrukturierte Ursachen einer Gefährdung, wie im vorangegangenen Schritt erstellt, vorausgesetzt. Diese werden, im Gegensatz zum informellen Vorgehen des Stands der Technik, im Schritt der Konstruktion genutzt und automatisch in eine analysierbare, formalisierte Struktur von Fehlerbäumen übertragen. Um dies umzusetzen wird nachfolgend zunächst das Konzept in Form eines dafür entwickelten Modells zur Abbildung von Fehlerbäumen sowie anschließend das Vorgehen anhand eines dafür entwickelten Algorithmus zur automatischen Konstruktion erläutert.

Modell Zur Erstellung von Fehlerbäumen ist ein zusätzliches Konzept erforderlich das zugrundeliegende Informationen der vorangegangenen Schritte nutzen kann, um diese als Fehlerbaum darstellen zu können. Dieses Modell M_{konstr} enthält dabei die folgenden Elemente:

$$\begin{aligned} E = \{ \quad & FaultTrees = \{ft_1, ft_2, ..., ft_y\}, \\ & FaultTreeObjects = \{fto_1, fto_2, ..., fto_z\} \\ & FaultTreeObjectConnections = \{ftc_1, ftc_2, ..., ftc_w\} \\ \} & \end{aligned}$$

Ein Fehlerbaum wird dabei als `FaultTree` abgebildet und besteht demnach grundlegend aus Fehlerbaumobjekten (`FaultTreeObject`) und Elementen zur Verbindung dieser Objekte, den `FaultTreeObjectConnections`. Ein `FaultTree` assoziiert grundlegend ein zuvor im Schritt der Gefährdungsidentifikation modelliertes `HazardousEvent` ($\Gamma : specifies \Rightarrow ft_y \times he_l$), sodass in der Konstruktion dafür je ein Fehlerbaum erstellt wird. `FaultTreeObjects` können weiter als spezielle Objekte wie `FaultTreeEvents` und `FaultTreeGates` im Fehlerbaum unterteilt werden.

Ein `FaultTreeEvent` ist dabei beispielsweise ein `IntermediateEvent`, `Basic-Event`, `TopEvent` etc., wie in Kapitel 2.2 beschrieben. Jedes dieser Events enthält Attribute zur Abbildung von relevanten Kenngrößen, sodass beispielsweise für ein `BasicEvent` als $p_{frequency}$ die Häufigkeitsstufe eines modellierten `Cause` sowie als $p_{mitigatedFrequency}$ dieser Wert unter Berücksichtigung risikomindernder Maßnahmen hinterlegt werden kann. Das `TopEvent` assoziiert zusätzlich den zugrundeliegenden `Hazard` ($\Gamma : defines\_top \Rightarrow fto_z \times h_i$), den dieses als oberstes Element des Fehlerbaumes abbildet [Rae04]. Ein `BasicEvent` hingegen bildet die modellierten `Causes` ab, sodass diese als $\Gamma : defines\_basic \Rightarrow fto_z \times c_b \in Causes$ assoziiert werden. Darüber hinaus ist für die spätere Berechnung und Auswertung eines Fehlerbaumes auch ein Wahrscheinlichkeitswert erforderlich, der als $p_{probability}$ bzw. als $p_{mitigatedProbability}$ unter Einbeziehung risikomindernder Maßnahmen abgebildet wird.

Mit einem `FaultTreeGate` kann hingegen beispielsweise ein `AndGate` oder `OrGate` etc. spezifiziert werden, um boolesche Zusammenhänge zwischen `FaultTreeEvents` darzustellen und eine hierarchische Struktur zu ermöglichen. `FaultTreeObjectConnections` stellen die Verbindungselemente im Fehlerbaum dar, mit welchen `FaultTreeGates` mit entsprechenden `FaultTreeEvents` verbunden werden. Jedes dieser Elemente ftc_w enthält somit die Attribute p_{source} und p_{target}, sodass zwei `FaultTreeObjects` miteinander verbunden werden, wobei auf diese jeweils mit Hilfe der Attribute referenziert wird. Das Vorgehen zur tatsächlichen Konstruktion von Fehlerbäumen anhand der erläuterten Elemente des Modells wird im nachfolgenden Abschnitt erläutert.

Vorgehen Die wesentlichen Schritte zur Erstellung von Fehlerbäumen sind nach Brügge [BB12, S. 39] die in Abbildung 3.13 rechts dargestellt Schritte (1) bis (3). Dabei muss nach Schritt (1) zunächst ein `TopEvent` festgelegt werden, welches durch weitere `FaultTreeObjects` zu einem Fehlerbaum entwickelt wird. Das entwickelte Modell adressiert diesen Schritt, indem aus jeder zugeordneten Gefährdung (`Hazard`) ein entsprechendes `TopEvent` im Fehlerbaum resultiert und als $\Gamma : defines\_top$ referenziert wird. Die notwendige Festlegung von `TopEvents` ergibt sich somit bereits aus den zuvor in der Gefährdungsidentifikation modellierten `Hazards` die somit als relevant identifiziert wurden und daher Bestandteil der Risikoanalyse sind. Das `TopEvent` assoziiert somit einen `Hazard`, der bei der Gefährdungsidentifikation mit möglichen `Causes`, sowie entsprechender Kennzahlen hinsichtlich der Häufigkeit möglicher Ursachen ($p_{frequency}$), spezifiziert wurde. Diese Kennzahlen ergeben somit die Datenquelle für den Schritt (2) zur Erstellung von Fehlerbäumen nach Brügge [BB12, S. 39], welche demnach für den zu erstellenden Fehlerbaum mit Hilfe von $\Gamma : defines\_top$ und $\Gamma : caused\_by$ übernommen und dem Konzept nach als Attribute hinterlegt werden. Dabei ist der Zusammenhang zwischen resultierenden `BasicEvents` und zugrundeliegenden `Causes` als $\Gamma : defines\_basic$ nachvollziehbar, sodass Kenngrößen und Ursachen genutzt werden können, womit der zweite Schritt (2) durch das Modell abgebildet wird. Nach Schritt (2) erforderliche Ursachen können somit anhand der $\Gamma : caused\_by$ Beziehung zwischen einem `Hazard` und dessen `Causes` genutzt werden. Abschließend erfolgt in Schritt (3) die tatsächliche Konstruktion von Fehlerbäumen, die

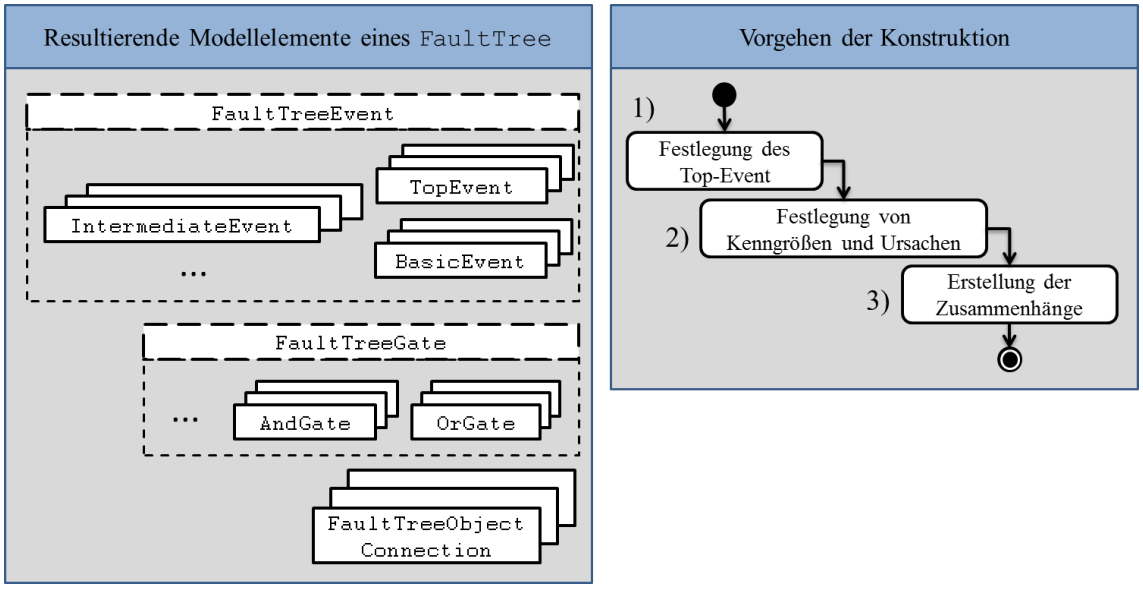

Abbildung 3.13: Schematische Darstellung des Vorgehens zur Konstruktion von Fehlerbäumen sowie daraus resultierenden Modellelementen eines Fehlerbaumes

Algorithm 2 Konzept zur Konstruktion von Fehlerbäumen

Gegeben: $op \in Operation$
Ergebnis: $\exists\ f\ \in\ FaultTree\ for\ \forall\ he\ \in\ HazardousEvent$

for $\forall\ he\ from\ \Gamma : part\_of\ op$ **do**
    Create new FaultTree f and associate to he
    $t = new\ TopEvent\ in\ f\ for\ Hazard\ h\ from\ he$
    $buildTree(t,\ cs \in CauseStructure\ from\ h)$
end for

procedure BUILDTREE($obj\ \in\ FaultTreeObject,\ cs \in\ CauseStructure$)
    if $cs \in\ CauseStructure \wedge \notin LogicStructure$ **then**
        Create $b \in\ BasicEvent\ for\ f$ *connected with parent obj and set attributes*
        for $\forall\ cm \in\ CounterMeasure\ from\ \Gamma : reduces\ of\ associated\ Cause\ by\ cs$ **do**
            Recalculate $p_{mitigatedFrequency}\ of\ b\ from\ cm\ p_{frequencyFactor}$
        end for
    else
        Create $i \in\ IntermediateEvent\ for\ f$ *connected with parent obj*
        Create $g \in\ FaultTreeGate\ from\ cs \in\ LogicStructure\ for\ f$ *connected with* i
        for $\forall\ c \in\ children\ of\ cs$ **do**
            $buildTree(g,\ c)$
        end for
    end if
end procedure

in diesem Ansatz mit Hilfe von Algorithmus 2 automatisch und somit ohne manuellen Aufwand für den Nutzer umgesetzt wurde. Der Algorithmus beginnt für jedes modellierte `HazardousEvent` damit einen Fehlerbaum zu erstellen. Für diesen wird zunächst das `TopEvent` festgelegt und daraufhin, angelehnt an die zuvor vorgenommene Strukturierung, `FaultTreeEvents` und `FaultTreeGates` erstellt und miteinander verbunden. Dabei wird die vorbereitete Strukturierung einer `CauseStructure` rekursiv durchgegangen und enthaltene `CauseStructures`, die keine `LogicStructure` sind und somit direkt einen `Cause` referenzieren, in `BasicEvents` überführt. Für diese `Causes` werden die in der Gefährdungsidentifikation zugeordneten Kenngrößen $p_{frequency}$ übernommen, sodass diese in der formalisierten Struktur des Fehlerbaumes vorhanden sind und für Berechnungen der übergeordneten Gefährdung und damit letztendlich auch für die Ermittlung des übergeordneten Risikowertes genutzt werden können. Falls risikomindernde Maßnahmen vorhanden sind, werden diese bei der Konstruktion mit berücksichtigt, sodass im Hinblick sämtlicher als $\Gamma : reduces$ zugeordneter `CounterMeasures` das Attribut $p_{mitigatedFrequency}$ des `BasicEvent` ermittelt wird. Somit kann bei der späteren Berechnung, in der die Häufigkeitsklasse der Gefährdung ermittelt wird, sowohl die Berechnung ohne sowie mit risikomindernden Maßnahmen

vorgenommen werden, um so die Auswirkung risikomindernder Maßnahmen auf die Häufigkeitsklasse der Gefährdung und den darauf aufbauend ermittelten Risikowert darzustellen. Die jeweils notwendigen booleschen Operatoren, um eine Kombination von Ursachen zu spezifizieren, werden anhand der vorbereiteten Strukturierung ermittelt, sodass eine dort enthaltene `LogicStructure` zur Erstellung eines `FaultTreeGates` mit entsprechender Logik genutzt wird. Darüber hinaus wird dem Format eines Fehlerbaumes entsprechend ein `IntermediateEvent` erstellt und mit dem `FaultTreeGate` verbunden. Dieses Vorgehen setzt sich dabei weiter rekursiv anhand der zugrundeliegenden `CauseStructure` fort, sodass als Ergebnis dieses Vorgehens für jedes modellierte `HazardousEvent` ein Fehlerbaum erstellt und somit die Konstruktion abgeschlossen wurde.

Anwendungsbeispiel Für das Anwendungsbeispiel Kranarbeiten wird im Rahmen des Schrittes Konstruktion der zuvor erläuterte Algorithmus 2 angewendet. Dabei wird, ausgehend vom `HazardousEvent` der in Abbildung 3.14 dargestellte Fehlerbaum erstellt. Das `TopEvent` bezieht sich dabei, wie im Algorithmus beschrieben, auf den zugrundeliegenden `Hazard`, wobei die darunterliegende Fehlerbaumstruktur anhand der zuvor erstellten `CauseStructure` ermittelt wird. Somit resultiert für den obersten `LogicOperator` das unter dem `TopEvent` liegende `OrGate`. Darunterliegend werden rekursiv, anhand der Kind-Elemente des `LogicOperators`, `FaultTreeEvents` und weitere `FaultTreeGates`, wie in Abbildung 3.14 als resultierender Fehlerbaum dargestellt, erzeugt. Die erzeugten `BasicEvents`

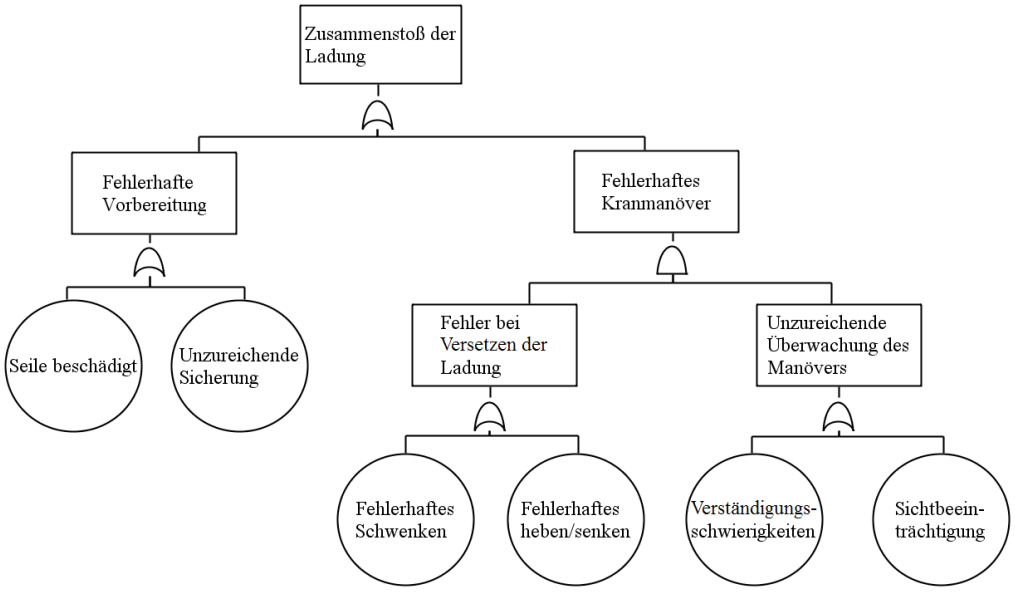

Abbildung 3.14: Automatisiert erstellter Fehlerbaum für das Anwendungsbeispiel Kranarbeiten

enthalten dabei Attribute und Assoziationen zu den zugrundeliegenden `Causes` im Prozessmodell, wie im Abschnitt Gefährdungsidentifikation beschrieben.

Durch die Konstruktion von Fehlerbäumen konnte durch den Ansatz ein weiterer Schritt zur formalisierteren Risikoanalyse vorgenommen werden. Um durch die so erstellten Fehlerbäume Aussagen über die geplante Operation treffen zu können, müssen diese ausgewertet werden, was Gegenstand des nachfolgenden Schrittes der Berechnung ist.

3) Berechnung

Der Schritt der Berechnung entspricht der Analyse der Fehlerbäume im eigentlichen Sinne, indem in diesem Schritt die Eintrittswahrscheinlichkeit bzw. Häufigkeitsstufe der Gefährdung auf Basis der damit über boolesche Operatoren verknüpften Ursachen berechnet wird. Als Grundlage für diesen Schritt dienen somit die in der Konstruktion erstellten Fehlerbäume. Nachfolgend wird dafür das Konzept sowie im Anschluss das Vorgehen beschrieben.

Konzept Die Fehlerbaumanalyse ermöglicht grundsätzlich eine qualitative wie auch quantitative Analyse. In diesem Anwendungsfall wird eine quantitative Analyse verwendet, da in Gefährdungsbeurteilungen wie in Kapitel 2 beschrieben eine quantitative Abschätzung hinsichtlich des Risikos eines Anwendungsfalls getroffen werden muss.

Die Fehlerbaumanalyse nutzt dafür überwiegend Wahrscheinlichkeitswerte für die quantitative Analyse. Bei Gefährdungsbeurteilungen zur Planung beispielsweise maritimer Operationen stehen hingegen kaum Wahrscheinlichkeitswerte zur Verfügung, um den Eintritt aller Gefährdungen und Ursachen einer Operation vollständig beschreiben zu können. Demnach werden Häufigkeitsstufen genutzt, um die Wahrscheinlichkeit des Eintritts eines Ereignisses abschätzen und beschreiben zu können. Diesen Stufen liegen jedoch implizit Wahrscheinlichkeiten zu Grunde, sodass niedrige Stufen für eine geringe Eintritts- bzw. Ausfallwahrscheinlichkeit sprechen sowie hohe Stufen entsprechend für erhöhte Wahrscheinlichkeitswerte. Damit die quantitative Analyse der Fehlerbäume entsprechend im Hinblick auf Gefährdungsbeurteilungen durchgeführt werden kann, werden den impliziten Annahmen

Tabelle 3.1: Wahrscheinlichkeitswerte mit Stufenzuordnung in Anlehnung an [Mul06, S. 36] und [Int02, S. 43])

Stufe	Beschreibung	Häufigkeit (Vorfälle pro Schiff und Jahr)
5	Häufig	$0,1$
4	Vermehrt	10^{-2}
3	Möglich	10^{-3}
2	Gering	10^{-4}
1	Sehr gering	10^{-5}

die den Stufenwerten zugrunde liegen, entsprechende Wahrscheinlichkeitswerte zugeordnet. Einen Ansatz dafür, wie die Größenordnung und Grenzwerte derartiger Wahrscheinlichkeitswerte in der maritimen Domäne zu wählen sind, liefert die IMO (International Maritime Organization) [Int02] bzw. [Mul06, S. 36]. Diese wurden als Anhaltspunkt für die in Tabelle 3.1 vorgenommene Zuordnung von Häufigkeitsstufen genutzt. Diese dargestellten Stufenzuordnungen dienen für diese Ausarbeitung jedoch nur als Vorschlag, der für den praktischen Einsatz der entwickelten Ideen und Werkzeuge jederzeit auf die jeweiligen Anforderungen der Anwendungsfälle angepasst werden kann.

Vorgehen Auf Basis einer derartigen Stufenzuordnung wie in Tabelle 3.1 vorgeschlagen, kann die quantitative Analyse erfolgen. Erstellte Fehlerbäume werden dabei entsprechend der Berechnungsgrundlage, unter Berücksichtigung der erforderlichen stochastischen Unabhängigkeit der Ereignisse, berechnet (siehe Fault Tree Handbook [RV87, V1-3ff]):

$$P(A \cap B) = P(A) \cdot P(B)$$
$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Dabei wird für die Berechnung jeweils der Wert nach der vorgeschlagenen Stufenzuordnung, wie in Tabelle 3.1 dargestellt, für das Attribut $p_{frequency}$ genutzt und entsprechend das Attribut $p_{probability}$ gesetzt. Initial ergeben sich somit aufgrund der Zugehörigkeit zu einem `Cause` ausschließlich für die `BasicEvents` Werte, wobei diese im Rahmen der Berechnung für alle weiteren `FaultTreeObjects` bestimmt werden. Im Vorgehen kann ausgehend von den `BasicEvents` die Berechnung für jedes `FaultTreeObject` stattfinden und die Ergebnisse als Attribute hinterlegt werden. Als weiteres können bei der Berechnung risikomindernde Maßnahmen mit einbezogen werden, sodass dafür analog die Attribute $p_{mitigatedProbability}$ bzw. $p_{mitigatedFrequency}$ genutzt werden können. Nachdem die Häufigkeitsstufen aller Gefährdungen bzw. `TopEvents` berechnet wurden, erfolgt unter Einbeziehung der Schadensklasse des entsprechenden `HazardousEvent` der Gefährdung, die Berechnung des Risikowertes über die Multiplikation von $p_{frequency}$ und $p_{severity}$, wie in Kapitel 2 beschrieben.

Anwendungsbeispiel Nachdem zunächst die Konstruktion des Fehlerbaumes für das Anwendungsbeispiel im vorangegangenen Abschnitt erläutert wurde, wurde in diesem Abschnitt die Auswertung des Baumes in Form der Berechnung der Werte beschrieben. In Abbildung 3.15 wird dafür der erstellte Fehlerbaum mit den ergänzten berechneten sowie aus den `Causes` resultierenden Werten, die als Attribute hinterlegt sind, dargestellt. Dabei werden die aus den `Causes` resultierenden Häufigkeitsstufen als $p_{frequency}$ der `BasicEvents` aufgeführt. Der anhand dieses Wertes ermittelte Wahrscheinlichkeitswert zur Berechnung des Fehlerbaumes wird als Attribut $p_{probability}$ hinterlegt und resultiert bei den `BasicEvents` aus deren $p_{frequency}$ und wird bei den übrigen `Events` auf Basis derer darunterliegender

Sub-Fehlerbäume mit darin enthaltenen Zusammenhängen berechnet. Zusätzlich wurde für den `Cause` bzw. das `BasicEvent` „Sichtbeeinträchtigung“ eine risikomindernde Maßnahme als `CounterMeasure` einbezogen. Diese reduziert durch das Attribut $p_{frequencyFactor}$ die $p_{frequency}$ des `BasicEvents`, woraus sich die $p_{mitigatedFrequency}$ und die daraus abgeleitete $p_{mitigatedProbability}$ ergibt. Diese Werte werden anhand der Berechnungsvorschriften genutzt, um den Fehlerbaum zu berechnen und somit sukzessive von den `BasicEvents` ausgehend Werte für $p_{probability}$ und im Fall von modellierten risikomindernden Maßnahmen $p_{mitigatedProbability}$ zu ermitteln. Mit Hilfe der Fehlerbaumanalyse und der vorgenommenen Berechnung konnten nun risikomindernde Maßnahmen in Form einer `CounterMeasure` in das Vorgehen mit einbezogen werden. Durch die Darstellung als Fehlerbaum, in welchem die Zusammenhänge logisch und hierarchisch veranschaulicht werden, können die Ergebnisse, wie in Abbildung 3.15 dargestellt, eingesehen werden. Durch diese Zusammenhänge kann auch der Effekt bzw. die Auswirkungen auf hierarchisch höher liegende `FaultTreeEvents` durch die risikomindernden Maßnahmen betrachtet werden, wie im rechten Teilbaum von Abbildung 3.15 dargestellt. Bei der Berechnung der Werte für das `TopEvent` haben somit Ergebnisse des linken Teilbaumes aufgrund des `OrGates` und der zugrundeliegenden Berechnungsvorschrift einen höheren Einfluss, sodass somit die getroffene risikomindernde

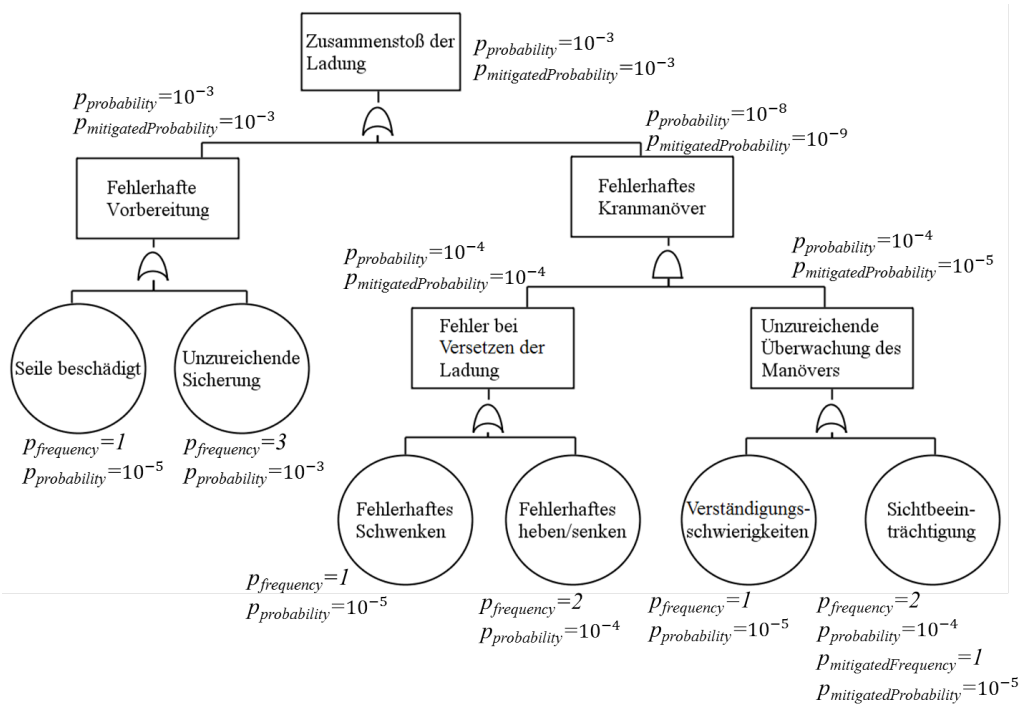

Abbildung 3.15: Fehlerbaum für das Anwendungsbeispiel Kranarbeiten mit berechneten Attributen

Maßnahme letztendlich kaum zur Risikominderung der eigentlichen Gefährdung beiträgt. Die vorgenommenen Arbeiten zur Konstruktion und Berechnung der Fehlerbäume können durch diese Möglichkeiten einen wesentlichen Beitrag zur gezielten Einbringung von risikomindernden Maßnahmen als auch zur Veranschaulichung der zugrundeliegenden Zusammenhänge von Gefährdungen und Ursachen leisten.

Durch die vorgenommene Berechnung konnten zuvor erstellte Fehlerbäume ausgewertet und Ergebnisse anhand der graphischen Darstellung betrachtet werden. Um jedoch auch im Hinblick auf vergleichsweise komplexere Operationen mit einer Vielzahl an möglichen Gefährdungen und Ursachen für die spätere Risikobewertung eine praktikable Möglichkeit zur Einsichtnahme zu ermöglichen, erfolgt im nachfolgenden Schritt der Dokumentation eine Aufbereitung dieser zugrundeliegender Informationen.

4) Dokumentation

Damit die Risikoanalyse abgeschlossen werden kann, müssen die darin erarbeiteten Ergebnisse zusammengefasst und verständlich dokumentiert werden, um somit die Komplexität für die anschließende Bewertung und Entscheidungsfindung für den Anwender im akzeptablen Bereich zu halten. Das Ziel ist somit mit Hilfe der Dokumentation die Risiken zu präsentieren und dadurch eine Basis zur Entscheidungsfindung u.a. über risikomindernde Maßnahmen zu ermöglichen [Vin07, S. 478]. Auf Basis dieser Dokumentation erfolgt sodann die Risikobewertung, sodass die im Schritt der Dokumentation aufgearbeiteten Informationen als Eingabe für die Risikobewertung dienen [Vin07, S. 479]. Die Form der Dokumentation sollte in Art einer Gefährdungsbeurteilung erfolgen, sodass diese als solche genutzt und von den beteiligten Personen verstanden werden kann [Vin07, S. 479, S. 491]. Dafür eignen sich graphische und textuelle Formen der Ergebnisdarstellung, sodass auch Nicht-Experten diese Dokumentation leicht verstehen können [Vin07, S. 491]. In den nachfolgenden Unterabschnitten wird zur Umsetzung einer solchen Dokumentation das entsprechende Konzept und Vorgehen beschrieben und daraufhin mit Hilfe des Anwendungsbeispiels veranschaulicht.

Konzept Eine mögliche Ergebnisdarstellung muss so dokumentiert sein, dass die Risikowerte der Gefährdungen, Häufigkeits- und Schwereklassen sowie der Einfluss von risikomindernden Maßnahmen und der Bezug zu Tätigkeiten oder Akteuren der geplanten Operation eingesehen werden können. Diese Informationen müssen dafür zum einen aus dem zugrundeliegenden Prozessmodell entnommen werden, da dieses den aktuellen Stand der Planung umfasst. Zum anderen sind die erstellten und ausgewerteten Fehlerbäume eine weitere Datenquelle aus der die Analyseergebnisse gewonnen werden können. Durch die Vernetzung dieser Informationen können diese jeweils genutzt und gemeinsam abgerufen und dargestellt werden. Zur Dokumentation dienen daher konzeptionell die in den vorangegangenen Schritten zusammengetragenen Informationen als Datenquelle. Dabei wird

sowohl das Prozessmodell mit den dort modellierten Akteuren, deren Arbeitsabläufe und Tätigkeiten sowie Informationen der Gefährdungsidentifikation und die erstellten Fehlerbäume und deren Ergebnisse genutzt. Der Ansatz zur Dokumentation dieser Informationen orientiert sich an dem bisherigen Vorgehen wie in Kapitel 2 beschrieben. Demnach werden diese Informationen in eine strukturierte tabellarische Form überführt, in der zunächst die zugrundeliegenden Abläufe mit entsprechenden Beschreibungen dokumentiert werden. Diese wird, entsprechend der konzeptionellen Zusammenhänge, um Aspekte aus der Gefährdungsidentifikation erweitert, sodass Abläufe mit Gefährdungen und Ursachen gemeinsam dokumentiert und betrachtet werden können. Darüber hinaus erfolgt, nach der Dokumentation der Arbeitsabläufe eines Akteurs, eine Zusammenfassung spezifischer Gefährdungen, Ursachen und Maßnahmen die den jeweiligen Akteur betreffen.

Abgesehen von dieser Dokumentation der Abläufe, werden Informationen, Ergebnisse und Zusammenhänge der Risikoanalyse dokumentiert. Diese Dokumente müssen für maritime Sicherheitsexperten in gewohnter Weise handhabbar sein, sodass diese beliebig verändert und verteilt werden können. Eine in der maritimen Domäne für diesen Zweck verwendete Form der Dokumentation wird mit Hilfe der Risikomatrix (siehe Abschnitt 2.1) vorgenommen [Bra02, S. 88]. Mit der Risikomatrix können alle analysierten Ereignisse aus der formalisierten Risikoanalyse in verdichteter Form dargestellt werden [Bra02, S. 88]. Sie zeigt die untersuchten Gefahren und Ursachen auf und ermöglicht das Ordnen entsprechend ihres ermittelten Risikos und die Trennung von akzeptablen bzw. nicht-akzeptablen Ereignissen [Bra02, S. 88]. Dies bildet zudem die Grundlage für die darauffolgende Risikobewertung, sodass mit einer übersichtlichen Dokumentation der jeweilige Leser in der Lage ist, diese zu verstehen und entsprechend Gefährdungen einzusehen sowie gezielt frühzeitig Maßnahmen zur Verbesserung treffen kann [Tho12, S. 60].

Vorgehen Da sämtliche Informationen für den Schritt der Dokumentation strukturiert vorliegen, entsprechend der erläuterten Konzepte, wird die Dokumentation automatisch vorgenommen. Dafür wird zunächst das zugrundeliegende Prozessmodell mit den dort modellierten Abläufen, ähnlich wie mit Algorithmus 1, sukzessive durchgegangen. Im Zuge dessen werden die Informationen wie Namen und Beschreibungen der Aktivitäten und Kommunikation eines Akteurs, sowie per Γ : *contains* mit den spezifischen Aktivitäten des Akteurs zusammenhängende `Causes`, tabellarisch dokumentiert (vgl. Abbildung 3.16 (a)), um eine gemeinsame Perspektive von prozess- und risikorelevanten Informationen zu ermöglichen. Eine zusammenfassende Darstellung von Gefährdungen, Ursachen, Schadensfolgen etc. erfolgt dabei abschließend zur Dokumentation der Arbeitsabläufe eines Akteurs (vgl. Abbildung 3.16 (b)), sodass diese Informationen für jeden Akteur zentral dokumentiert und eingesehen werden können. Über die akteurspezifische Dokumentation (vgl. Abbildung 3.16 (a)-(b)) erfolgt ebenfalls automatisch eine detaillierte Dokumentation der Gefährdungen selbst, in welcher gezielt Informationen der Gefährdungsidentifikation

und der Risikoanalyse für die Dokumentation genutzt werden (vgl. Abbildung 3.16 (c)). Dabei erfolgt je Gefährdung die Darstellung der Risikoberechnung anhand der Attribute $p_{severity}$ und $p_{frequency}$, bei dem die Ergebnisse der Berechnung der jeweiligen Fehlerbäume genutzt wird. Darüber hinaus werden Schadensfolgen und risikomindernde Maßnahmen, sowie sämtliche beitragenden Ursachen zur Gefährdung mit und ohne Einbeziehung risikomindernder Maßnahmen inklusive deren $p_{frequency}$ bzw. $p_{mitigatedFrequency}$, aufgeführt.

Anwendungsbeispiel Ein Auszug der Dokumentation des Anwendungsbeispiels nach dem beschriebenen Vorgehen wird in Abbildung 3.16 dargestellt. Diese wurde dem Ansatz entsprechend automatisiert, mit Hilfe der zugrundeliegenden Informationen der vorangegangenen Schritte, erzeugt. Der erste Teil der resultierenden Dokumentation fasst den modellierten Prozess zusammen und dokumentiert dabei jeweils die Arbeitsabläufe eines Akteurs, wobei Abbildung 3.16 (a) auszugsweise die resultierende Dokumentation des Kranführers darstellt. Zusätzlich werden dazu parallel die bei der Gefährdungsidentifikation für Aktivitäten des Kranführers eingebrachten möglichen Ursachen aufgeführt, wie beispielsweise bei der Aktivität zum Versetzen der Ladung die Ursachen zum fehlerhaften Schwenken oder Heben. Somit wird eine gemeinsame Einsicht in sowohl den geplanten Ab-

a) Dokumentation der Arbeitsabläufe des Akteurs

1.1.2 Actor: Kranführer

No.	Name	Description	Causes
	...		
3	Vorbereitung		- Seile beschädigt - Unzureichende Sicherung
4	Receive message from: Ladeoffizier	- Sicherheitszone verlassen	
5.1	Parallele Ausführung	- Anzahl: 2	
5.1.1	Ladung versetzen		- Fehlerhaftes Schwenken - Fehlerhaftes Heben/Senken
5.2.1	Manöver beobachten		- Sichtbeeinträchtigung - Verständigungsschwierigkeiten
6	End of operation	The operation is completed for this actor.	

b) Risikozusammenfassung des Akteurs

Risk summary for actor: Kranführer

Hazards	Exposures	Causes	Measures
- Zusammenstoß der Ladung	- Personenschäden - Sachschäden	- Seile beschädigt - Unzureichende Sicherung - Fehlerhaftes Schwenken - Fehlerhaftes Heben/Senken - Sichtbeeinträchtigung - Verständigungs-schwierigkeiten	- Kommunikation

c) Gesamtdokumentation einer Gefährdung

2 Risk Assessment

2.1 Hazard: Zusammenstoß der Ladung

Operational Situation: Last schwebt

Frequency	3
Severity	4
Risk	12

2.1.1 Exposures

No.	Name	Description
1	Personenschäden	-
2	Sachschäden	-

2.1.2 Mitigation Measures

No.	Name	Description
1		-

2.1.3 Causes of Hazard

No.	Name	Freq.	CounterMeasures	Mitigated Freq.
1	Seile beschädigt	1		1
2	Unzureichende Sicherung	3		3
3	Fehlerhaftes Schwenken	1		1
4	Fehlerhaftes Heben/Senken	2		2
5	Verständigungsschwierigkeiten	1		1
6	Sichtbeeinträchtigung	2	Kommunikation (1)	1

Abbildung 3.16: Auszug aus der zusammenfassenden Dokumentation des Kranführers (links) und der Gefährdung Zusammenstoß der Ladung (rechts) aus dem Anwendungsbeispiel Kranarbeiten

lauf als auch mögliche Ursachen einer Gefährdung gewährleistet. Für jeden Akteur wird in der Art jeweils eine solche Beschreibung erstellt. Zusätzlich erfolgt zum Abschluss der

Tätigkeitsbeschreibung eines Akteurs eine, wie in Abbildung 3.16 (b) dargestellte, Zusammenfassung seiner spezifischen Gefährdungen, Schadensfolgen, möglichen Ursachen und risikomindernden Maßnahmen, um die gemeinsame Perspektive zu vervollständigen und einen schnellen Einblick zu ermöglichen. Als zweiten Teil dieser Dokumentation, werden eingebrachte Gefährdungen detailliert aufgeführt und sowohl die Ergebnisse der Berechnung des Risikowertes dargestellt als auch mögliche Schadensfolgen, risikomindernde Maßnahmen und entsprechend bewertete Ursachen (siehe Abbildung 3.16 (c)). Im Rahmen der in der maritimen Domäne üblichen farblichen Abgrenzung einer Risikomatrix, werden vorgenommene Bewertungen in dieser Auflistung ebenfalls farblich hinterlegt. Eine solche Auflistung erfolgt nach dem Vorgehen der Dokumentation systematisch für jede eingebrachte Gefährdung der geplanten Operation. Weiterhin sind die dafür aufgeführten Detailinformationen ebenfalls bezogen auf die gesamte Operation, sodass diese für eine übergreifende Risikobewertung durch den Anwender im nachfolgenden Abschnitt genutzt werden können.

3.3.4 Risikobewertung

Die Risikobewertung ist das Vorgehen in dem die Ergebnisse der Risikoanalyse verwendet werden [Kri13, S. 209]. Dabei werden diese Ergebnisse dahingehend betrachtet, ob diese akzeptabel oder nicht-akzeptabel sind [Kri13, S. 210], [Vin07, S. 127]. Insofern erfolgt eine manuelle Überprüfung, ob die Ergebnisse und somit die in den Schritten zur Systemdefinition, Gefährdungsidentifikation und Risikoanalyse geplante maritime Operation den Akzeptanzkriterien genügt. Ein häufig angewandtes Prinzip dabei ist ALARP (engl. As Low As Reasonably Practicable) [Vin07, S. 63], was so viel bedeutet wie, dass das betrachtete Risiko so gering wie vernünftigerweise praktikabel sein soll. Dies ist zwar ein verbreitetes Prinzip, jedoch ist dieses unpräzise, da es der subjektiven Einschätzung des jeweiligen Sicherheitsexperten obliegt, was als vernünftigerweise praktikabel gilt [Kri13, S. 248]. Dennoch erfolgt diese Überprüfung manuell durch den jeweiligen Sicherheitsexperten oder einer Gruppe von Sicherheitsexperten, in der hinsichtlich der Akzeptanz oder Nicht-Akzeptanz entschieden wird. Bei Vorliegen nicht-akzeptabler Ergebnisse wird daraufhin entschieden, beispielsweise welche risikomindernden Maßnahmen ergriffen werden müssen, um somit Änderungen der Systemdefinition und der nachfolgenden Schritte einzupflegen, bis eine erneute Risikobewertung auf Basis der Risikoanalyse erfolgen kann.

Wenn jedoch die vorgenommene Planung den Akzeptanzkriterien genügt, wird diese beispielsweise für Verfahren zur Genehmigung, Vorbesprechungen, Schulungen etc. genutzt. Bei erneuter Planung anderer Anwendungsfälle ist wiederholt das Erfahrungswissen des Nutzers erforderlich, um wiederum in der Systemdefinition die Operation zu Planen und daraufhin aufgrund seiner Erfahrung mit anderen Anwendungsfällen und der Domäne eine entsprechende Gefährdungsidentifikation vorzunehmen. Traditionelle Ansätze zur Risikobewertung basieren daher umfassend auf Erfahrungswissen [Alt10, S. 22]. Die Wieder-

verwendung ist dabei bisher, wie im Handlungsbedarf identifiziert, eine Herausforderung, sodass bestenfalls das dafür notwendige Erfahrungswissen beim Nutzer vorhanden oder zumindest soweit ausgeprägt ist, dass entsprechend Unterlagen anderer Anwendungsfälle hinzugezogen werden können, damit beispielsweise eine ausreichend vollständige Gefährdungsidentifikation erfolgen kann. In dem hier vorgestellten Ansatz soll dieser Schritt durch die entwickelte Wissensbasis unterstützt werden. Daher werden zum Abschluss des Schrittes der Risikobewertung, bei Vorliegen einer zufriedenstellenden Gefährdungsbeurteilung, die enthaltenen Informationen des Anwendungsfalls durch einen im Folgenden vorgestellten Ansatz der Wissensbasis persistent gespeichert, sodass diese Informationen erneut bereitgestellt werden können. In den nachfolgenden Abschnitten werden das dafür notwendige Modell zum Speichern dieser Informationen sowie das Vorgehen erläutert.

Modell Eine formalere Systemdefinition bietet einen ersten Grundstein zur Steigerung der Wiederverwendbarkeit und damit letztendlich der Effektivität des Vorgehens zur Risikobewertung [S$^+$02, S. 3]. Darüber hinaus muss jedoch auch eine technische Grundlage geschaffen werden, damit das in das Vorgehen zur Risikobewertung eingebrachte Wissen gespeichert und bei Bedarf wieder abgerufen werden kann [CS06]. In diesem Abschnitt wird daher der Ansatz einer Wissensbasis konzipiert, um Wissen, das in den verschiedenen Schritten des systematischen Vorgehens eingebracht wurde, speichern zu können damit dieses erneut wieder bereitgestellt werden kann. Das dafür notwendige Model $M_{wissensb}$ umfasst die folgenden Elemente zum strukturierten Speichern dieser Informationen:

$$\begin{aligned} E = \{ \quad & KBElements = \{ke_1, ke_2, ..., ke_a\}, \\ & KBParameters = \{kp_1, kp_2, ..., kp_b\}, \\ & KBRelations = \{kr_1, kr_2, ..., kr_c\}, \\ \} & \end{aligned}$$

Die Wissensbasis (KnowledgeBase, Abk. KB) besteht dabei aus Elementen (`KBElement`) und Relationen zwischen diesen Elementen (`KBRelations`). `KBElement` stellt dabei ein generisches Element dar, mit dem grundsätzlich jedes Element der zuvor entwickelten Modelle M_{sysdef}, $M_{gefident}$ oder M_{strukt} abgebildet werden kann. Damit wird ermöglicht, dass jedes der Elemente bzw. der eingepflegten Informationen aus den Schritten des systematischen Vorgehens, in der Wissensbasis mit Hilfe des Modells abgebildet und strukturiert gespeichert werden kann. Somit können beispielsweise ein `Actor` oder ein `Task` aus M_{sysdef}, ein damit zusammenhängender `Cause` aus $M_{gefident}$ mit sämtlichen Attributen, oder eine dafür entwickelte `CauseStructure` aus M_{strukt} jeweils als `KBElement` in der Wissensbasis gespeichert werden.

Eine `KBRelation` ist ein generisches Element mit dem die Zusammenhänge zwischen gespeicherten `KBElements` nachgebildet werden, sodass beispielsweise der als Γ : *contains*

beschriebene Zusammenhang eines `Task` mit enthaltenen `Causes` sowie sämtliche weitere Zusammenhänge der zuvor erläuterten Modelle jeweils als `KBRelation` ausgedrückt und gespeichert werden können. Dies ist insbesondere für die spätere Bereitstellung von Informationen ein wichtiger Aspekt, sodass auch zusammenhängende Informationen bereitgestellt und vor allem gezielt nach relevanten Informationen durchsucht werden können.

Mit Hilfe eines `KBParameter` kann ein `KBElement` um weitere Informationen ergänzt werden. Ein Beispiel dafür sind mögliche Analyseergebnisse, wie die im vorangegangenen Schritt der Risikoanalyse ermittelte Häufigkeitsstufe einer Gefährdung. Diese Werte, wie auch zugeordnete Werte zur Schadensschwere, können als `KBParameter` auch fortlaufend hinterlegt werden. Für wiederkehrende Gefährdungen, die in der Wissensbasis hinterlegt und verwendet werden, kann so der Werteverlauf vergangener Anwendungsfälle als Orientierungshilfe ergänzt werden, um beispielsweise die Tendenz und den Verlauf eines Wertes aufzuzeigen. Durch die Bereitstellung dieser so gespeicherten Informationen werden somit Schritte wie die Gefährdungsidentifikation oder Risikoanalyse zukünftiger Anwendungsfälle zusätzlich unterstützt.

Vorgehen Die Durchführung der Risikobewertung selbst stellt überwiegend manuellen Aufwand zur Überprüfung der vorgenommenen Planung dar. Wird eine Planung dabei als ausreichend bewertet, können im Rahmen des entwickelten Lösungsansatzes die im Vorgehen der Planung eingepflegten Informationen mit Hilfe der Wissensbasis strukturiert gespeichert werden. Dabei entsteht für den Nutzer durch diesen zusätzlichen Schritt kein weiterer Mehraufwand, da Informationen der Schritte Systemdefinition, Gefährdungsidentifikation und Risikoanalyse bereits wie beschrieben strukturiert vorliegen. Die Speicherung dieser Informationen in der Wissensbasis kann somit automatisch vorgenommen werden. Dabei wird zunächst vom Modell M_{sysdef} der Systemdefinition ausgegangen und dort enthaltene Elemente mit sämtlichen Attributen jeweils als ein `KBElement` gespeichert. Systematisch werden daraufhin alle Zusammenhänge zwischen den Elementen aus M_{sysdef} als ein `KBRelation` Element gespeichert. Dabei ergeben sich bereits Zusammenhänge zu weiteren Informationen, die beispielsweise im Rahmen der Gefährdungsidentifikation in M_{sysdef} eingepflegt wurden. Für diese werden wiederum `KBElements` und `KBRelations` erstellt, sowie daraufhin mit damit zusammenhängenden Elementen weiter verfahren, bis somit abschließend sämtliche Informationen der vorgenommenen Planung in der Wissensbasis hinterlegt wurden. Eine Besonderheit ergibt sich dabei hinsichtlich der `KBParameter`, welche als fortlaufende Liste beispielsweise die als Attribute von `Causes` zugeordneten Werte speichern und bei erneuter Verwendung und Speicherung dieser `Causes` diese Liste erweitern können.

Als Abschluss der Risikobewertung kann somit das erworbene Planungswissen gespeichert werden, sodass dieses unterstützend im Rahmen der softwareseitigen Unterstützung für zukünftige Anwendungsfälle bereitgestellt wird. Dabei ist das Wissen der Prozess- sowie Analysesicht miteinander vernetzt, woraus sich zusätzlich für die Wiederverwendung

analysebezogener Informationen ein Kontext der Prozesssicht erschließen lässt. Dieser kann zur gezielten Suche und Bereitstellung von Informationen genutzt werden, sodass beispielsweise für wiederkehrende Tätigkeiten oder Akteure die Wissensbasis durchsucht wird, um damit zusammenhängende Informationen zu erhalten.

Anwendungsbeispiel Nach Abschluss der Schritte des systematischen Vorgehens, wird die vorgenommene Planung des fiktiven Anwendungsbeispiels in die Wissensbasis gespeichert. Dafür wird die gesamte geplante Operation, mit allen darin enthaltenen und verknüpften Informationen in die Wissensbasis überführt. Abbildung 3.17 stellt dabei schematisch einen Auszug der enthaltenen `KBElements` dar. Dem Vorgehen nach, beginnend bei der Operation, wird diese als ein `KBElement` aufgefasst und gespeichert. Sukzessive werden die entsprechenden Unterelemente wie die Akteure der Operation, im Anwendungsbeispiel der Ladeoffizier und der Kranführer, ebenfalls als jeweils solch ein `KBElement` gespeichert. Mit Hilfe der `KBRelations` wird der Zusammenhang der Akteure und der Operation nachgebildet, sodass dieser, wie im Anwendungsbeispiel geplant, erhalten bleibt. Für die Akteure werden analog dazu deren spezifische Tätigkeiten, als jeweilige Unterelemente des Akteurs, in die Wissensbasis überführt und auf gleiche Weise miteinander verknüpft. Nach diesem Vorgehen werden sukzessive weitere Informationen der Operation, wie Gefährdungen, mögliche Ursachen, risikomindernde Maßnahmen sowie vorgenommene Strukturierungen jeweils in die Wissensbasis überführt, sodass diese Informationen, wie auszugsweise in Abbildung 3.17 schematisch dargestellt, in der Wissensbasis enthalten sind. Zusätzliche Informationen zur weiteren, über die Planung hinausgehenden Anreicherung, werden in diesem Vorgehen als weitere `KBParameter` eines Elements ergänzt. Für das Anwendungs-

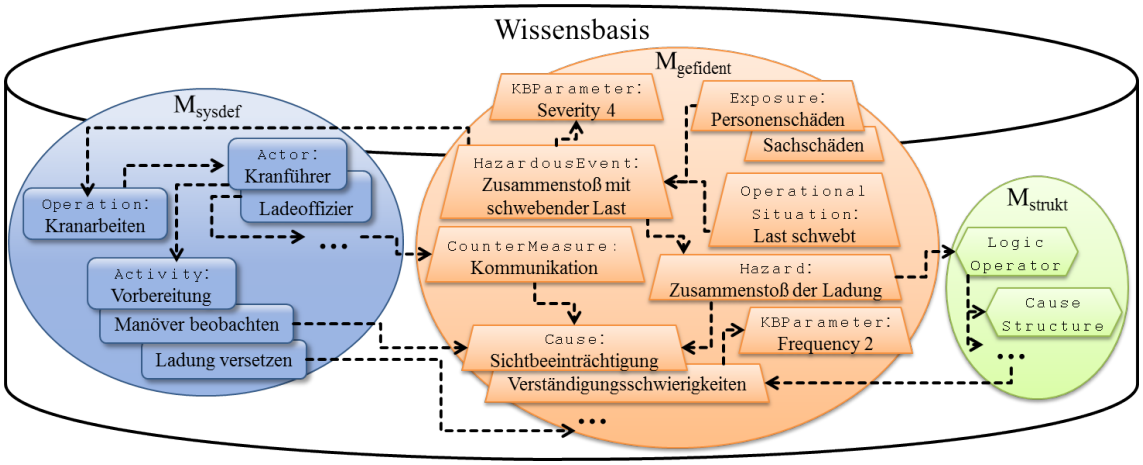

Abbildung 3.17: Auszugsweise schematische Darstellung der resultierenden `KBElements` der Wissensbasis für das Anwendungsbeispiel Kranarbeiten

beispiel bedeutet dies, dass beispielsweise ermittelte Häufigkeitsstufen der Ursachen oder der Gefährdung als ein Parameter des Elements der Gefährdung sowie auch die zugeordnete Schadensstufen ergänzt werden können. Beide Parameter werden fortlaufend, bei wiederholter Verwendung von Elementen wie einer Gefährdung, ergänzt, sodass für diese mehrere `KBParameter` zur Abbildung zugeordneter Schadensstufen bzw. ermittelter Häufigkeitsstufen hinterlegt werden. Diese wird als zusätzliche Orientierungshilfe bei späterer Wiederverwendung dieser Elemente grafisch dargestellt.

3.4 Zusammenfassung

Mit diesem Kapitel wurde anhand der vorangegangenen Ausführungen der Kapitel 1 und 2 ein eigener Lösungsansatz im Hinblick auf die Zieldefinitionen und des identifizierten Handlungsbedarfs entwickelt und vorgestellt. Dafür wurden zu Beginn des Kapitels zunächst technische Anforderungen ermittelt, die an einen Lösungsansatz zu stellen sind. Darauffolgend wurde der eigene Lösungsansatz anhand des schrittweisen Vorgehens zur Risikoanalyse und Bewertung erläutert. In diesem sind die wesentlichen Aspekte des Lösungsansatzes in die folgenden Schritte unterteilt worden:

- Systemdefinition
- Gefährdungsidentifikation
- Risikoanalyse
- Risikobewertung

Im Schritt der **Systemdefinition** wurde erläutert, welche Inhalte für eine prozessorientierte Planung einer Operation innerhalb der Systemdefinition zu definieren sind. Weiterhin ist daraufhin der bestehende Ansatz von MOPhisTo ausgewählt worden, mit dem diese Inhalte adäquat abgebildet sowie die zugrundeliegenden in Abschnitt 3.1 aufgestellten Anforderungen adressiert werden konnten. Dieser Ansatz wurde mit seiner graphischen Darstellung und Symbolik innerhalb der Systemdefinition erläutert sowie das graphische Prozessmodell zur Beschreibung der Operation des Anwendungsbeispiels vorgestellt.

Im Anschluss wurde der Schritt zur **Gefährdungsidentifikation** eingeführt sowie ein strukturiertes Modell der in diesem Schritt einzupflegenden Informationen vorgestellt. Darüber hinaus wurde das Vorgehen, wie diese Informationen innerhalb des Lösungsansatzes gemeinsam mit den zugrundeliegenden Informationen der Systemdefinition eingepflegt und verwendet werden können, vorgestellt. Als ein weiterer Aspekt im Schritt der Gefährdungsidentifikation wurde die Einbringung der notwendigen Informationen betrachtet, welche mit Hilfe des Lösungsansatzes manuell eingepflegt, jedoch auch durch eine zugrundeliegende

Wissensbasis als weitere Informationsquelle unterstützend bereitgestellt werden können.

Der Schritt der **Risikoanalyse** nutzt darauffolgend die in den vorangegangenen Schritten zusammengetragenen und strukturierten Informationen. Diese werden dabei zunächst hierarchisch sowie logisch, als Vorbereitung für die Fehlerbaumanalyse strukturiert, was manuell, automatisiert oder in einem kombinierten Vorgehen vorgenommen werden kann. Auf Basis dieses Schrittes erfolgt dann die automatisierte Erstellung von Fehlerbäumen, indem relevante Informationen vorangegangener Schritte in die analysierbare Form von Fehlerbäumen überführt, darauffolgend ausgewertet und die Ergebnisse dokumentiert werden.

Anschließend erfolgt der abschließende Schritt der **Risikobewertung**, welcher überwiegend manuellen Aufwand zur Überprüfung und Entscheidung erfordert. Wurde jedoch entschieden, dass auf Basis der vorliegenden Ergebnisse die vorgenommene Planung mit den darin eingepflegten und vernetzten Informationen ausreichend ist, so kann dieses Wissen im Rahmen des Lösungsansatzes in einer Wissensbasis gespeichert werden. Dieses in der Wissensbasis hinterlegte Wissen ist erneut nutzbar, sodass dieses in anderen Anwendungsfällen, beispielsweise im Schritt der Gefährdungsidentifikation, gezielt bereitgestellt und erneut genutzt werden kann.

Nachdem der entwickelte Lösungsansatz erläutert wurde, erfolgt abschließend eine zusammenfassende Auflistung, welche technischen Anforderungen durch welche konzeptionellen Aspekte des Ansatzes zusammen mit den einzelnen Schritten des Vorgehens adressiert werden:

- *Anforderung 1 - Möglichkeit zur Prozessdefinition.* Im Rahmen der Anforderung 1 wurde im Schritt der Systemdefinition eine Möglichkeit zur Modellierung gefunden, mit der die notwendigen Informationen eines Anwendungsfalls mit darin enthaltenen Arbeitsabläufen und Personen abgebildet werden können. Die Verwendung des bestehenden Ansatzes von MOPhisTo im Rahmen der Systemdefinition ermöglicht daher die geforderte Möglichkeit zur Prozessdefinition mit dafür notwendigen Informationen, sodass die Anforderung damit erfüllt wird.
- *Anforderung 2 - Konzept zur Abbildung risikorelevanter Informationen.* Im Schritt der Gefährdungsidentifikation wurde ein Modell entwickelt und vorgestellt, mit dem erforderliche Begrifflichkeiten und Zusammenhänge zwischen Gefährdungen, Ursachen, Folgen etc. konzeptionell zusammengebracht werden können. Dieses wird dafür genutzt derartige Informationen zu strukturieren und im Rahmen des schrittweisen Vorgehens innerhalb der Arbeiten der Gefährdungsidentifikation abbilden zu können.
- *Anforderung 3 - Integration von Prozess- und Analysesicht.* Mit der Systemdefinition

wird ein erster Bestandteil zur Anforderungserfüllung beigetragen, da mit dieser eine entsprechende Datengrundlage zur Integration geschaffen wurde. Darauf aufbauend ermöglicht die Gefährdungsidentifikation das Einpflegen weiterer, für die Analyse erforderlicher Informationen. Durch diese Datengrundlage kann die erforderliche Analysesicht durch das erarbeitete Konzept verstärkt berücksichtigt werden. Mit Hilfe des Schrittes zur Risikoanalyse wird die Anforderung weiter vervollständigt, sodass in diesem Schritt Informationen sowohl aus Prozess- als auch Analysesicht zur Strukturierung genutzt, ausgewertet und dokumentiert werden können. Zusätzlich wird diese Anforderung bei der Betrachtung der Wiederverwendbarkeit im Rahmen der Risikobewertung berücksichtigt, sodass sowohl analysespezifische als auch prozessspezifische Informationen im Verbund gespeichert und später bereitgestellt werden können. Dadurch ist eine integrierte Sicht über sämtliche Schritte des systematischen Vorgehens gegeben, wodurch die Anforderung erfüllt wird.

- *Anforderung 4 - Konzept zur Speicherung eingebrachter Planungsinformationen.* Als letzter Schritt des Vorgehens wird in der Risikobewertung entschieden, auf Basis der zugrundeliegenden eingepflegten Informationen und Ergebnisse, ob die Planung abgeschlossen werden kann oder nicht. Die bis zu diesem Schritt eingepflegten Informationen werden im Rahmen des Lösungsansatzes wiederverwendet, um diese erneut in anderen Anwendungsfällen zu nutzen oder als Orientierungshilfe bereitstellen zu können. Für diesen Zweck wurde eine Wissensbasis konzipiert mit der das gesammelte Wissen entsprechend der Anforderung strukturiert gespeichert wird, wodurch diese Anforderung erfüllt ist.

- *Anforderung 5 - Möglichkeit zur Selektion bereitgestellter Informationen.* In dem Lösungsansatz wurde eine Möglichkeit beschrieben eingepflegtes Wissen aus vergangenen Anwendungsfällen durch eine zugrundeliegende Wissensbasis erneut zu nutzen. Um dem Nutzer nicht stets die gesamte Wissensbasis bereitzustellen, kann im Rahmen des Lösungsansatzes sowohl manuell, als auch anhand der Verknüpfung von Informationen automatisiert gefiltert werden, woraufhin die Selektion erfolgen kann. Für ein selektiertes Element wie beispielsweise eine Gefährdung, können daraufhin relevante Informationen wie vorgenommene Wertezuordnungen als Orientierungshilfe eingesehen sowie damit zusammenhängende Detailinformationen oder Unterelemente übernommen und daher erneut verwendet werden.

- *Anforderung 6 - Konzept zur Integration von Analyseergebnissen.* Über die Wiederverwendung innerhalb des Vorgehens eingepflegter Informationen hinaus, wurde eine Möglichkeit geschaffen mit Hilfe zusätzlicher Parameter und Relationen weitere Informationen zu ergänzen. Durch dieses Konzept können auch erst im Vorgehen ermittelte Informationen wie Ergebnisse der Analyse ergänzend im Rahmen der Wiederverwendbarkeit als weitere Orientierungshilfe genutzt werden.

- *Anforderung 7 - Konzept zur logischen und hierarchischen Strukturierung.* Mit dem im Lösungsansatz beschriebenen systematischen Vorgehen sind Möglichkeiten zur logischen und hierarchischen Strukturierung aufgezeigt und konzipiert worden. Diese Anforderung wird insbesondere durch den Schritt der Risikoanalyse adressiert, da Aspekte zur Strukturierung bei der Fehlerbaumanalyse erforderlich sind. Eine Möglichkeit ist dies manuell vorzunehmen und so die für die Risikoanalyse notwendigen Informationen losgelöst von der übrigen Planung zu strukturieren. Eine weitere Möglichkeit stellen die konzipierten automatisierten Ansätze dar. Darin werden zugrundeliegende Planungsinformationen, im Sinne der als Prozessmodell definierten Abläufe, verwendet. Mit diesen können Vorschläge als Orientierungshilfe erzeugt werden, die zusätzlich manuell angepasst werden können, wodurch ein kombiniertes Vorgehen ermöglicht wird. Durch die so konzipierten Ansätze werden unterschiedliche Möglichkeiten zur unterstützenden Strukturierung ermöglicht, wodurch die Anforderung erfüllt wird.

- *Anforderung 8 - Konzept zur automatisierten Formalisierung.* Als eine weitere Unterstützung, vorbereitend zur Risikoanalyse, wurde ein Konzept zur automatisierten Strukturierung entwickelt, um mögliche Ursachen einer Gefährdung verketten zu können, sodass als Orientierungshilfe Kombinationen von Ursachen dargestellt werden können. Ergänzend dazu konnten mit einem weiteren Konzept zur Formalisierung derart vorbereiteter Informationen Fehlerbäume automatisiert erstellt werden.

- *Anforderung 9 - Möglichkeit zur Aufbereitung der Ergebnisse.* Eine Aufbereitung der Ergebnisse wird zum Abschluss des Schritts der Risikoanalyse beschrieben, sodass diese Ergebnisse gemeinsam mit zugrundeliegenden Planungsinformationen eingesehen und als Grundlage für die Risikobewertung genutzt werden können. Weiterhin werden dabei bereits eingebrachte Wertezuordnungen entsprechend der Darstellung der Risikomatrix aufbereitet. Eine gezielte Zusammenfassung der Ergebnisse der Risikoanalyse und eine integrierte Dokumentation und Darstellung der dafür notwendigen Informationen, integriert mit Informationen der Systemdefinition, führen zu einer Erfüllung der Anforderung.

Da in diesem Kapitel zunächst der Lösungsansatz konzeptionell beschrieben wurde, konnte Anforderung 10 - softwareseitige Unterstützung bisher nicht erfüllt werden. Daher wird der erläuterte Lösungsansatz im nachfolgenden Kapitel 4 im Rahmen einer prototypischen Umsetzung implementiert, um somit die Anforderung zu adressieren sowie eine spätere Evaluation des Ansatzes zu ermöglichen.

Kapitel 4

Prototypische Umsetzung

In vorangegangenen Abschnitten dieser Ausarbeitung wurde zunächst der Stand der Technik in Kapitel 2 aufgeführt sowie daraus der Handlungsbedarf der Arbeit ermittelt. Auf dieser Grundlage wurde in Kapitel 3 eine Lösungsidee auf Basis der Anforderungen entwickelt und vorgestellt. Diese Lösungsidee erstreckt sich über mehrere Schritte zur Risiko- bzw. Gefährdungsbeurteilung hinweg. Damit daraus ein durchgängiger Lösungsansatz entsteht, wurden die Ausführungen des vorangegangenen Abschnitts im Rahmen von Implementierungsarbeiten umgesetzt. Dabei ist ein Softwarewerkzeug entstanden, welches die bekannten Schritte zur Gefährdungsbeurteilung abbildet und den Anwender bei der Durchführung des Ansatzes unterstützt. Die dafür vorgenommenen Implementierungsarbeiten werden daher in den folgenden Unterabschnitten anhand des bekannten Vorgehens zur Gefährdungsbeurteilung erläutert. Darüber hinaus dienen diese vorgenommenen Implementierungsarbeiten zur Überprüfung der Umsetzbarkeit der Lösungsidee sowie als Grundlage für die spätere Evaluation des Ansatzes in Kapitel 5.

4.1 Überblick

Als Umsetzung zu den in Kapitel 3 beschriebenen Konzepten ist ein Softwarewerkzeug entstanden, in dem diese implementiert wurden. Die dabei von dieser Ausarbeitung adressierten Komponenten werden in Abbildung 4.1 als Übersicht dargestellt. Mit dieser Umsetzung wird der Anwender bei der Durchführung des systematischen Vorgehens mit Systemdefinition, Gefährdungsidentifikation, Risikoanalyse und Risikobewertung unterstützt, sodass die notwendigen Informationen dieser Schritte in eine durchgängig genutzte Modellstruktur eingepflegt werden. Zur Systemdefinition nach Abbildung 4.1 (a) wird dafür der Prozessmodelleditor mit Umsetzung durch MOPhisTo genutzt, in welchem das vorgestellte Modell M_{sysdef} als Datenmodell implementiert und daraus das Softwarewerkzeug MOPhisTo als graphischer Editor zur Abbildung von Operationen mit Akteuren und Arbeitsabläufen etc. erzeugt wurde. Als weiteres wurde zur Umsetzung der Gefährdungsidentifikation nach

Abbildung 4.1 (b) das Sicherheitskonzept in einem Datenmodell anhand von $M_{gefident}$ umgesetzt. Dieses ergänzt den Prozessmodelleditor MOPhisTo um Eingabemasken zum Einpflegen von erforderlichen Informationen der Gefährdungsidentifikation.

Der Schritt der Risikoanalyse wird nach Abbildung 4.1 (c) durch mehrere Komponenten im Analysekonzept adressiert. Als ersten Teilschritt dafür wurde in Erweiterung zum Sicherheitskonzept, die Strukturierung nach M_{strukt} als Datenmodell umgesetzt, sodass zuvor eingepflegte Gefährdungen und Ursachen manuell und mit möglicher Unterstützung durch automatisierte Strukturierungsvorschläge strukturiert werden können. Darüber hinaus wurden erforderliche Zusammenhänge zur Erstellung von Fehlerbäumen nach M_{konstr} in einem entsprechenden Datenmodell umgesetzt sowie daraus ein grafischer Editor zur Visualisierung der Fehlerbäume und Einsichtnahme in mögliche Zusammenhänge und Ergebnisse erstellt. Die zuvor in Kapitel 3 entwickelten Algorithmen zur Strukturierung und Konstruktion mit Hilfe der Modelle M_{strukt} und M_{konstr} wurden im Analysekonzept sowie auch die Berechnung erstellter Fehlerbäume entsprechend umgesetzt. Der graphische Feh-

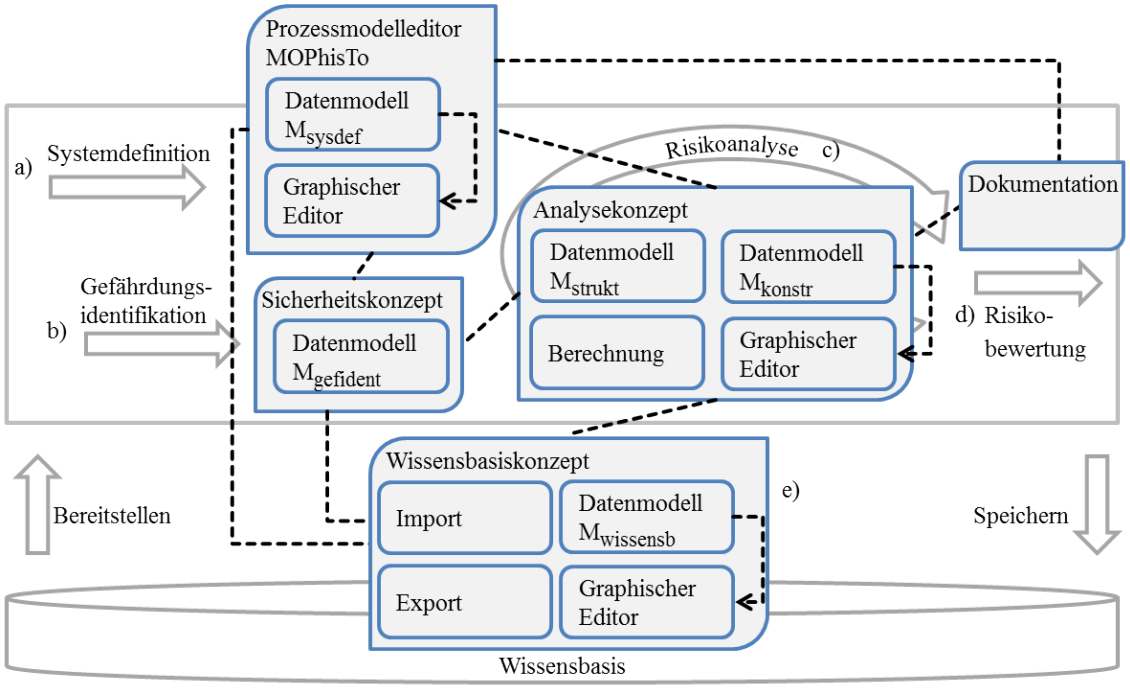

Abbildung 4.1: Schematische Übersicht und Einordnung der prototypischen Umsetzung in das bisherige Vorgehen

lerbaumeditor ermöglicht dabei zusätzlich auch eine Erstellung von Fehlerbäumen, losgelöst vom übrigen Vorgehen. Für sämtliche in dem Editor dargestellten Fehlerbäume wurden zusätzlich Exportfunktionalitäten umgesetzt, um diese Fehlerbäume in weiteren, beispiels-

weise kommerziellen Anwendungen nutzen zu können. Zum Abschluss der Risikoanalyse und Vorbereitung der Risikobewertung, implementiert die Komponente Dokumentation Funktionalitäten zum Auslesen der Informationen des modellierten Prozesses und ausgewerteter Fehlerbäume. Im Rahmen der Risikobewertung können die eingepflegten Informationen der Planung in der Wissensbasis gespeichert werden. Die Wissensbasis setzt dabei das zuvor entwickelte Modell $M_{wissensb}$ in einem Datenmodell um, woraufhin wiederum ein grafischer Editor zur Einsichtnahme in den bestehenden Datenumfang entwickelt wurde. Darüber hinaus wurden dort Funktionalitäten zum Import sowie zum Export und damit gezieltes Ein- und Auslesen von Informationen umgesetzt.

Die Implementierungsarbeiten sind mit Hilfe von Ecore sowie des Eclipse Modeling Frameworks (EMF)[1] vorgenommen worden. Mit diesen wurden zunächst sämtliche der vorgestellten Datenmodelle als Ecore UML Modelle umgesetzt. Auf dieser Grundlage wurde Quellcode generiert, mit dem diese Daten in einer softwareseitigen Unterstützung abgebildet und beispielsweise in Form von graphischen Editoren oder Eingabemasken genutzt werden konnten. Die darauffolgenden Implementierungsarbeiten sind mit der Programmiersprache Java vorgenommen und im Rahmen eines einzigen Softwarewerkzeugs mit Plug-In Architektur implementiert worden. Demnach sind alle nachfolgend erläuterten Funktionen und Darstellungen auf diese Weise umgesetzt worden.

4.2 Systemdefinition

Die Systemdefinition soll eine präzise Definition des Anwendungsfalls ermöglichen, sodass diese für alle beteiligten Personen beim Vorgehen der Planung Transparent ist und somit verstanden und nachvollzogen werden kann [Vin07, S. 129]. Dabei sind in der Systemdefinition u.a. Beschreibungen der relevanten Aktivitäten und Personen enthalten [Vin07, S. 129]. Für diesen Zweck ist ein Werkzeug entstanden, mit welchem grafische Prozessmodelle zur Planung von Abläufen erstellt und editiert werden können. Ein Bildschirmabbild dieses Werkzeugs ist in Abbildung 4.2 dargestellt. Innerhalb dieses Werkzeugs können Aktivitäten, Personen sowie weitere Aspekte eines zu planenden Ablaufs mit einer definierten **Symbolik** (Abbildung 4.2 rechts) abgebildet werden. Aktivitäten können dabei hierarchisch modelliert und Kommunikation, beispielsweise als Austausch von Nachrichten innerhalb des Ablaufs, abgebildet werden. Weiterhin kann die zeitliche Abfolge von Aktivitäten als Sequenzfluss modelliert werden, sowohl mit parallelen als auch mit sequentiellen Pfaden. Diese Aktivitäten werden einem Akteur zugeordnet, welcher als vertikale Umgrenzung Raum für mehrere auszuübende Aktivitäten bzw. Tätigkeiten bietet. Dieses Softwarewerkzeug ist im Rahmen angrenzender Forschungsarbeiten von Droste [DH13] entstanden. Es bietet neben der Nutzung der Symbolik zur grafischen Modellierung in der **Prozess-**

[1] http://www.eclipse.org/modeling/emf/

modellsicht zudem eine Projekt- und eine Eigenschaftssicht. In der **Eigenschaftssicht** können dabei zusätzliche Informationen von in der Prozessmodellsicht selektierten Elementen angezeigt und manipuliert werden. So können beispielsweise in der Eigenschaftssicht eines `Tasks` sowohl dessen Name und Beschreibung als auch darin getroffene risikomindernde Maßnahmen und enthaltene Ursachen für Gefährdungen bearbeitet oder relevante weitere Elemente der Systemdefinition, wie beispielsweise Ausrüstung etc. als Ressourcen, hinterlegt werden. Die **Projektsicht** dient hingegen der Verwaltung verschiedener Projekte, indem dort Dateien unter entsprechenden Projektnamen abgelegt, referenziert und sortiert werden können.

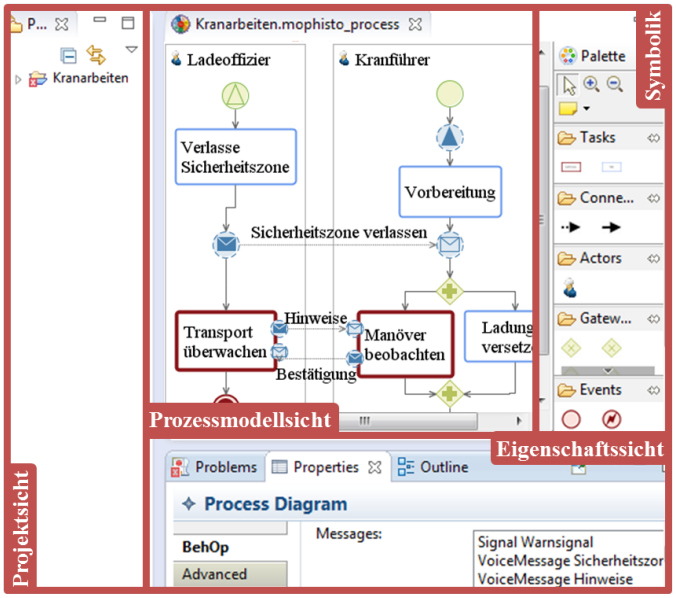

Abbildung 4.2: Werkzeug zum editieren des Prozessmodells

4.3 Gefährdungsidentifikation

Der Schritt zur Gefährdungsidentifikation sollte strukturiert und systematisch ablaufen, sodass in diesem Gefährdungen und mögliche Ursachen gefunden sowie klassifiziert und dokumentiert werden können [Vin07, S. 121]. Als dabei unterstützende Maßnahmen werden u.a. Erfahrungswissen aus ähnlichen Projekten und Operationen sowie Studien und Statistiken betrachtet [Vin07, S. 121]. Damit innerhalb des in dieser Ausarbeitung entwickelten Lösungsansatzes eine durchgängige, softwareseitige Unterstützung und damit das geforderte strukturierte und systematische Vorgehen ermöglicht werden kann, wurden die Implementierungsarbeiten zur Gefährdungsidentifikation entsprechend in den Prozessmodelleditor integriert. Dabei sind grundsätzlich folgende Funktionen integriert worden, die

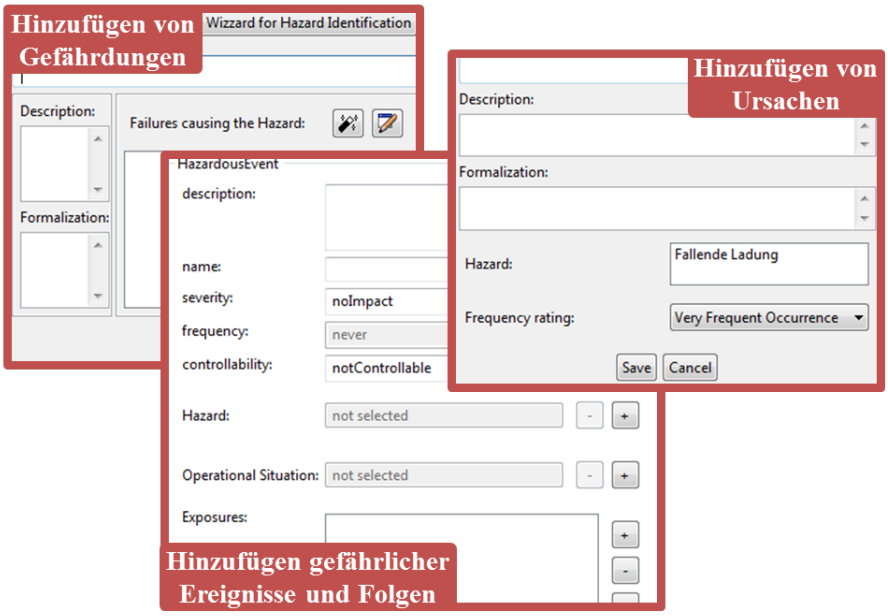

Abbildung 4.3: Eingabemasken zum Einpflegen der Informationen für die Gefährdungsidentifikation

für den Benutzer sowohl an geeigneter Stelle mit Bedienung der rechten Maustaste innerhalb des grafischen Prozessmodells als auch jeweils über die **Eigenschaftssicht** erreicht werden können:

- Hinzufügen neuer Gefährdungen und Ursachen
- Zuordnung von Häufigkeitsklassen für Ursachen ($p_{frequency}$)
- Zuordnung von Schwereklassen für Gefährdungen ($p_{severity}$)
- Hinzufügen von gefährlichen Ereignissen, Betriebssituationen und möglichen Schadensfolgen
- Nutzung von Informationen vergangener Anwendungsfälle aus der Wissensbasis

Zur Eingabe und Bearbeitung neuer oder bestehender Gefährdungen und Ursachen existieren innerhalb der Software entsprechende Eingabemasken, wie in Abbildung 4.3 dargestellt, in denen diese Informationen sowohl mit Namen und Beschreibungen sowie auch mit entsprechenden Werten bezüglich Frequency und Severity versehen werden können. Zusätzlich können in darin Informationen miteinander verknüpft werden, sodass beispielsweise für eine neu eingepflegte Ursache die Referenz zur entsprechenden Gefährdung festgelegt werden muss. Für die Übernahme von Informationen aus der Wissensbasis ist eine gesonderte Funktion implementiert worden, die aus der Eingabemaske zum Hinzufügen einer

neuen Gefährdung heraus aufrufbar ist. Diese Funktion, mit entsprechend implementierter grafischer Oberfläche, ist in Abbildung 4.4 dargestellt. Mit dieser Funktion lässt sich

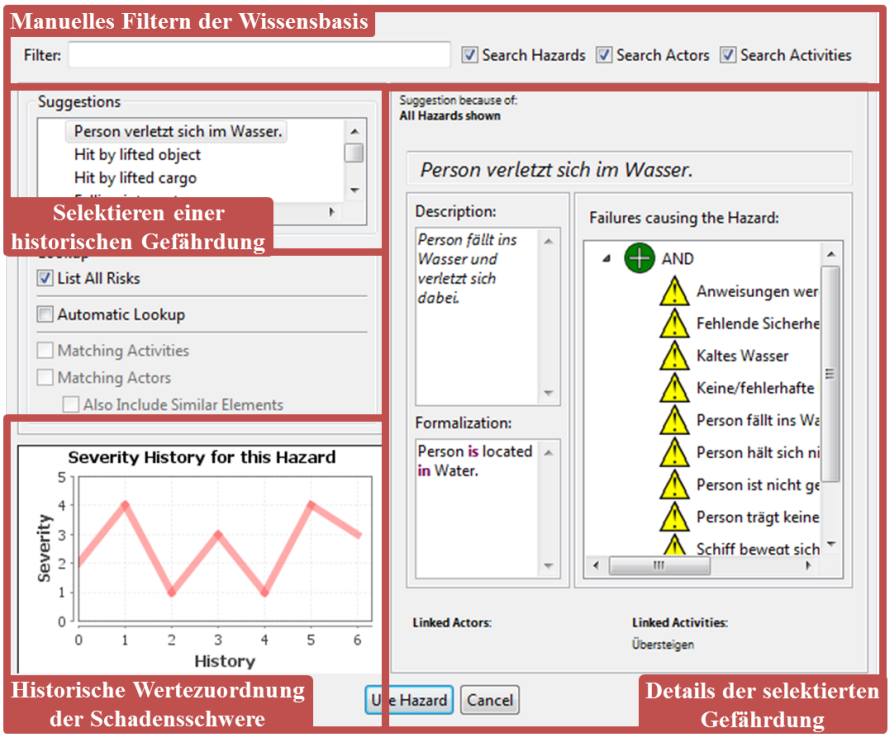

Abbildung 4.4: Eingabemaske zur Darstellung und Selektion von aus der Wissensbasis bereitgestellten Daten zur unterstützenden Gefährdungsidentifikation

die zugrundeliegende Wissensbasis automatisch sowie manuell durchsuchen bzw. filtern und nähere Informationen, wie beispielsweise der Kurvenverlauf der bisher verwendeten Severity bzw. Frequency-Stufe die jeweils als `KBParameter` hinterlegt sind, oder zuletzt zugeordnete Kombinationen von Ursachen einer selektierten Gefährdung anzeigen. Zudem wird der Benutzer bei Übernahme einer Gefährdung aus der Wissensbasis für jede der zugeordneten Ursachen aufgefordert, diese an passender Stelle der aktuellen Planung einzubetten. Zusätzlich wird für jede der Ursachen aus der Wissensbasis, die Informationen der bisher verwendeten Frequency-Stufen dieser Ursache als Orientierungshilfe in einem Kurvenverlauf visualisiert.

4.4 Risikoanalyse

Nach dem Abschluss der Schritte der Systemdefinition und Gefährdungsidentifikation, in welchen das zugrundeliegende Prozessmodell aufgebaut sowie mit Informationen über Ge-

fährdungen und mögliche Ursachen angereichert wurde, kann der Schritt der Risikoanalyse beginnen. Der erste Teilschritt umfasst dabei die Strukturierung der Daten, sodass diese miteinander in Beziehung gesetzt werden und somit erstmals Kombinationen möglicher Ursachen einer Gefährdung betrachtet werden. Dieser Schritt kann sowohl vollständig manuell als auch automatisiert durch Vorschläge zur Orientierungshilfe vorgenommen werden, woraufhin die so erstellte Basisstruktur anschließend im Schritt der Konstruktion in die Form der Fehlerbäume für die Analyse überführt wird. Diese werden anschließend im Schritt der Berechnung ausgewertet sowie darauffolgend innerhalb der Dokumentation für die anschließende Risikobewertung vorbereitet.

4.4.1 Strukturierung

Der Schritt der Strukturierung ist der erste Schritt der Risikoanalyse, in welchem das zugrundeliegende Prozessmodell, mit entsprechend angereicherten und vernetzten Informationen der Gefährdungen, Ursachen und Prozessmodellelementen, verwendet wird. Diese Informationen werden dabei als Vorbereitung für die Konstruktion der Fehlerbäume und somit für den Schritt der Berechnung verwendet. Dabei werden im Rahmen dieser Vorbereitung boolesche Operatoren eingefügt, um die Vernetzung von Gefahren und Ursachen genauer zu spezifizieren. Dieser Vorgang ist für jede der zu betrachtenden Gefährdungen erforderlich. Für eine softwareseitige Unterstützung innerhalb der integrierten Softwareumgebung wurden zwei Möglichkeiten entwickelt, zum einen zur Unterstützung des manuellen Vorgehens, zum anderen ein darauf aufbauendes automatisiertes Vorgehen, die beide nachfolgend erläutert werden.

Manuelles Vorgehen Im Rahmen des manuellen Vorgehens können boolesche Operatoren und damit einhergehende hierarchische Strukturen vom Benutzer vollständig manuell erstellt werden. Dieser Vorgang ähnelt der herkömmlichen Verfahrensweise zur Erstellung von Fehlerbäumen, in denen das Einfügen boolescher Operatoren und Strukturierung die wesentlichen Schritte darstellen. Für diesen Vorgang wurde innerhalb der softwareseitigen Unterstützung ein Werkzeug (siehe Abbildung 4.5) entwickelt, dass den Benutzer bei diesem Vorgehen unterstützt. Zuvor eingebrachte Ursachen einer ausgewählten Gefährdung werden in der **Selektionssicht** (Abbildung 4.5 links) aufgelistet und können so vom Benutzer selektiert und in die Struktursicht (Abbildung 4.5 rechts) in eine Hierarchieebene überführt werden. Zusätzlich können zur logischen Verknüpfung boolesche Operatoren in der **Operatorsicht** (Abbildung 4.5 unten links) ausgewählt und ebenfalls in die Struktursicht überführt werden, wodurch eine Baumstruktur resultiert.

Automatisiertes Vorgehen Ergänzend zum manuellen Vorgehen, kann die hierarchische Struktur mit enthaltenen booleschen Operatoren in diesem Ansatz auch automatisiert

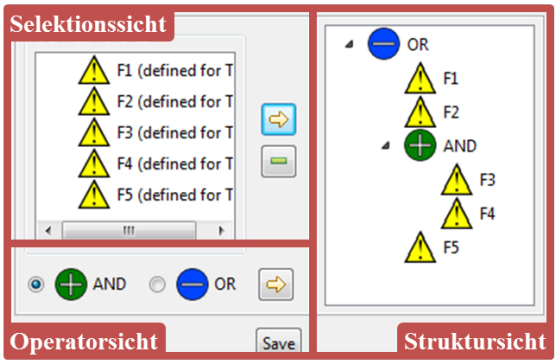

Abbildung 4.5: Werkzeug zur manuellen Strukturierung und Zuordnung boolescher Operatoren

zur Unterstützung vorgeschlagen werden. Dabei dient die vorgenommene Planung des Anwendungsfalls in Form des Prozessmodells als Grundlage. Innerhalb dieses Prozessmodells dienen modellierte Sequenzen und Parallelitäten der geplanten Arbeitsabläufe dazu, hierarchische Strukturen und boolesche Operatoren für die Risikoanalyse abzuleiten. Wie im vorangegangenen Kapitel 3 beschrieben, wird dieses Vorgehen als Vorschlagsystem genutzt, mit dem automatisch eine Basisstruktur geschaffen wird, die vom Anwender anschließend nach Bedarf angepasst werden kann. Somit muss der Anwender nicht vollends eigenständig diesen Schritt ohne Anhaltspunkte oder Vorarbeiten, wie im manuellen Vorgehen beschrieben, vornehmen, sondern erhält über die automatische Strukturierung eine Basis und Orientierungshilfe zum Beginn seiner Arbeiten. Damit dem Anwender eine Auswahl ermöglicht werden kann, sodass auch flexible Anforderungen der jeweiligen Anwendungsfälle, beispielsweise hinsichtlich des Detaillierungsgrades, berücksichtigt werden können, wurden unterschiedliche Algorithmen entwickelt und in Kapitel 3 erläutert. Abbildung 4.6

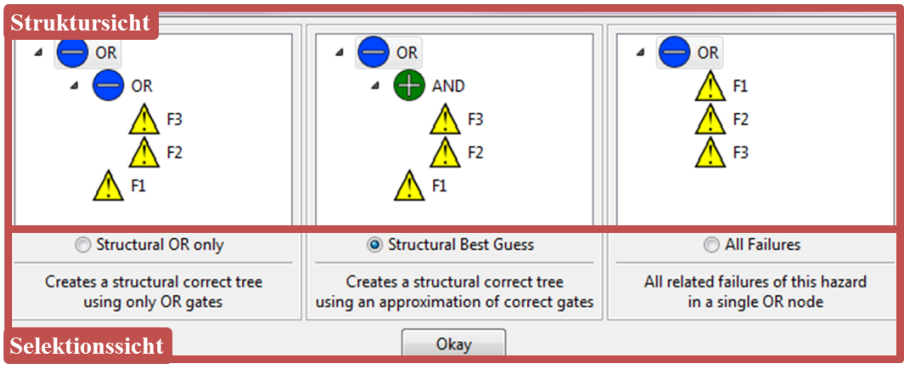

Abbildung 4.6: Darstellung und Auswahl der Ergebnisse der Algorithmen zur automatisch erstellten Strukturierung

zeigt dabei drei der implementierten Algorithmen, die dort innerhalb der **Struktursicht** (Abbildung 4.6 oben) hinsichtlich ihrer Resultate betrachtet sowie in der **Selektionssicht** (Abbildung 4.6 unten) entsprechend selektiert werden können.

Nachdem einer der Algorithmen in der **Selektionssicht** aus Abbildung 4.6 ausgewählt wurde, werden dessen Ergebnisse entsprechend übernommen, um die Kombinationen von Ursachen der selektierten Gefährdung zuzuordnen. Diese dienen jedoch zunächst als Basisstruktur, sodass diese im Nachhinein stets wie im manuellen Vorgehen beschrieben, beliebig manipuliert werden können, um beispielsweise Ursachen zu entfernen oder mit Hilfe des Werkzeugs in Abbildung 4.5 umzustrukturieren oder einzelne boolesche Operatoren mit geringem Aufwand zu verändern.

4.4.2 Konstruktion

Im vorangegangenen Schritt der Strukturierung ist eine Basisstruktur manuell, oder mit Hilfe der vorgestellten Algorithmen, erstellt worden. Diese dient dem Schritt der Konstruktion, in dem die tatsächlichen Fehlerbäume der Gefährdungen erstellt werden. Dieser Schritt wird durch den Benutzer angestoßen, indem dieser die Funktion der Risikoanalyse in der **Prozessmodellsicht** nach Abbildung 4.2 anwählt und somit die Umsetzung von Algorithmus 2 angestoßen wird. Daraufhin wird für jedes `HazardousEvent` ein Fehlerbaum erstellt. Somit von der Gefährdung ausgehend, wird in diesem Ansatz die Basisstruktur rekursiv durchiteriert und die booleschen Operatoren jeweils in `FaultTreeGates` sowie die spezifizierten Ursachen in `FaultTreeEvents` des Fehlerbaumes überführt, wie zuvor in Kapitel 3 als Algorithmus 2 konzipiert. Bei der Erstellung werden zu den Ursachen selbst, die in der Basisstruktur vorliegen, auch die im Schritt der Gefährdungsidentifikation eingepflegten Werte der Frequency von Ursachen für die Events übernommen. Auf diese wirken zudem, wie im Prozessmodell spezifiziert, risikomindernde Maßnahmen. Diese werden als zusätzliche Daten in den resultierenden Events hinterlegt, sodass sich für diese sowohl je ein reduzierter sowie normaler Wert der Frequency ergibt. Diese Informationen und der erstellte Fehlerbaum werden dann, wie in Abbildung 4.7 dargestellt, mit Hilfe des dafür entwickelten Editors visualisiert.

4.4.3 Berechnung

Direkt nach der Erstellung der Fehlerbäume erfolgt die quantitative Analyse. Diese wird auf Basis der Struktur eines zuvor erstellten Fehlerbaumes und den entsprechend quantifizierten Elementen vorgenommen, sodass das Ergebnis der Berechnung sowohl die durch risikomindernde Maßnahmen reduzierte als auch normale Frequency des `TopEvents` ist. Für die Berechnung bzw. quantitative Analyse wurden bekannte Algorithmen von Rauzy [Rau93] mit Hilfe binärer Entscheidungsdiagramme sowie ein eigener vereinfachter Ansatz mit einem rekursiven bottom-up Algorithmus entsprechend der Berechnungsvorschriften

(siehe Fault Tree Handbook [RV87, V1-3ff], [Mar12], [Moh13]) implementiert. Zur Durchführung der Berechnung werden jeweils die zugeordneten Wertestufen, wie zuvor beschrieben, in Wahrscheinlichkeitswerte überführt. Der zugrundeliegende Fehlerbaum wird daraufhin ausgewertet, sodass jeweils beide Frequency Werte des `TopEvents` ermittelt werden. Die vorgenommenen Implementierungsarbeiten sind zusätzlich mit Hilfe von Fehlerbäumen für Benchmark-Tests ([Lim13], [Rau93]) mit bekannten Ergebnissen validiert worden. Für die integrierte Visualisierung und Verarbeitung nah an der Modellierung der zugrun-

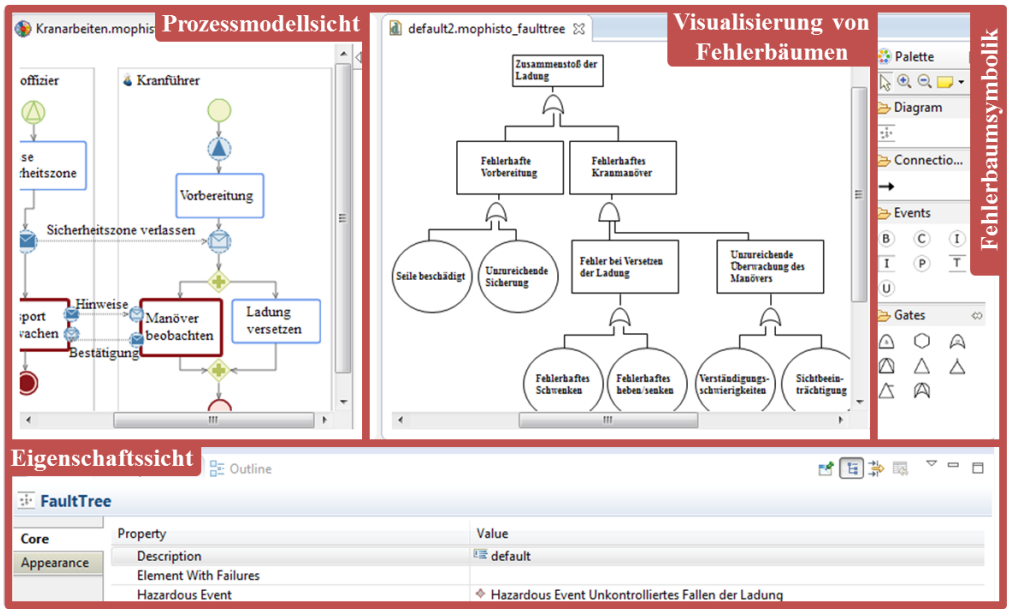

Abbildung 4.7: Integrierte Darstellung von Fehlerbaumeditor und Prozessmodelleditor

deliegenden Prozesse, wurden alle beschriebenen Funktionen in eine einheitliche Softwareumgebung integriert. Innerhalb dieser **Visualisierung** werden mit Hilfe des erstellten Fehlerbaumeditors demnach alle erstellten Fehlerbäume dargestellt. Zusätzlich können mit diesem Werkzeug manuell Fehlerbäume erstellt und manipuliert werden, sodass per Drag & Drop die **Fehlerbaumsymbolik** (siehe Abbildung 4.7 rechts) dafür genutzt werden kann. Darüber hinaus können darin die Analyseergebnisse erstellter Fehlerbäume sowie auch Zusammenhänge von `BasicEvents` und `Causes`, `HazardousEvent` und `FaultTree` etc. in einer eigenen **Eigenschaftssicht** eingesehen und nachvollzogen werden. Die so dargestellten Fehlerbäume werden dabei automatisch innerhalb der zuvor erläuterten **Projektsicht** als eigene Datei im Projekt gespeichert. Aus der **Visualisierung** heraus lassen sich zusätzlich selektierte Fehlerbäume in andere bekannte Dateiformate anderer Software zur Bearbeitung und Auswertung von Fehlerbäumen, wie beispielsweise OpenFTA [Auv14] oder fault tree plus [Iso14], exportieren.

4.4.4 Dokumentation

Nachdem die vorangegangenen Schritte zur Risikoanalyse abgeschlossen wurden, stehen dem Nutzer sämtliche Informationen für die anschließende Risikobewertung bereit. Jedoch müssen diese zunächst im Rahmen des Schrittes zur Dokumentation in eine übersichtliche und verständliche Form gebracht werden. Dadurch werden ein verbessertes Verständnis der Gefahren selbst sowie auch deren Kritikalität und entsprechend im Voraus zu treffender Maßnahmen ermöglicht [Tho12, S. 60]. Für diesen Zweck ist eine Möglichkeit implementiert worden sowohl in der Prozessmodellierung eingepflegte Informationen über entsprechende Arbeitsabläufe, handelnde Personen etc. sowie Resultate der Risikoanalyse in einem Microsoft Word Dokument zusammenzufassen und zu speichern. Dieses Dokument kann inner-

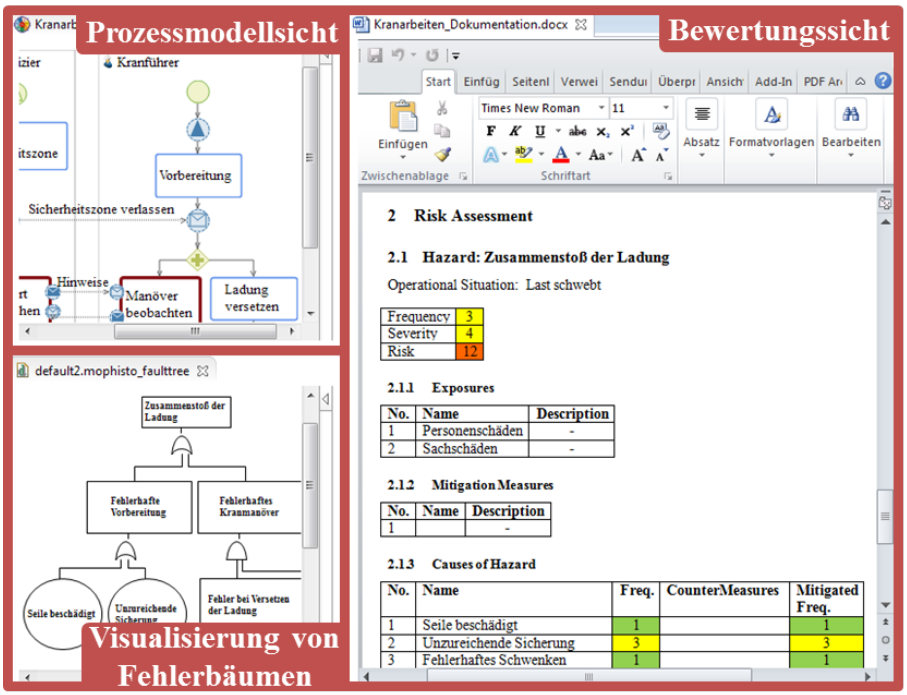

Abbildung 4.8: Zusammenfassende Dokumentation der Modellinformationen und Analyseergebnisse integriert als Bewertungssicht in der Gesamtsoftware

halb der entwickelten Softwareumgebung integriert, geöffnet und wie in der **Bewertungssicht** in Abbildung 4.8 dargestellt, betrachtet werden. Die Funktion kann über die zuvor erläuterte **Projektsicht** für ein erstelltes Prozessmodell aufgerufen werden, woraufhin ohne weitere Interaktion mit dem Benutzer ein entsprechendes Word Dokument innerhalb des selektierten Projekts automatisch erstellt wird. Für eine tabellarische Zusammenfassung der modellierten Arbeitsabläufe wird dabei das zugrundeliegende Prozessmodell durchiteriert und Textelemente der Tätigkeiten, Akteure, Nachrichten etc. übernommen, chrono-

logisch geordnet und mit entsprechend verknüpften Gefährdungen, Ursachen, Maßnahmen etc. versehen. Aufgrund der internen Verknüpfung der Prozessmodelldatei mit der Fehlerbaumdatei wird in dieser Auswertung, nach Abschluss der Iteration des Prozessmodells, die Zusammenfassung der Risikoanalyse in ähnlicher Form automatisch angestoßen. Dabei werden alle erstellten Fehlerbäume genutzt und die entsprechend abgebildeten Gefährdungen jeweils aufgelistet. Für jede Gefährdung ergibt sich dabei eine Gesamtbewertung des Risikos, basierend auf den Ergebnissen der Fehlerbaumanalyse sowie der Zuordnung der Schadensschwere. Zusätzlich zu dieser Gesamtbewertung, einsehbar in der **Bewertungssicht**, werden für jede Gefährdung detailliert Schadensfolgen, mögliche Ursachen sowie darauf wirkende risikomindernde Maßnahmen und deren Effekt als eigenes Kapitel in der erstellten Dokumentation aufgelistet. Weiterhin werden jeweils Analyseergebnisse sowie auch zugeordnete Werte sowohl textuell als auch mit entsprechender Farbkodierung (grün, gelb, rot) der Risikomatrix (siehe Kapitel 2), sowohl als ursprünglicher Wert sowie unter Berücksichtigung risikomindernder Maßnahmen, dargestellt.

4.5 Risikobewertung

Innerhalb der Risikobewertung werden die Ergebnisse der Risikoanalyse genutzt und hinsichtlich ihrer Akzeptanz oder nicht-Akzeptanz hin überprüft [Kri13, S. 210], [Vin07, S. 127/209]. Dies obliegt jedoch der subjektiven Einschätzung der jeweiligen Person, weshalb dieser Schritt überwiegend ein manueller Vorgang ist [Kri13, S. 248]. Ein zusätzlicher Schritt, der im Rahmen der prototypischen Umsetzung der Lösungsideen dieser Ausarbeitung implementiert wurde, ist der Aspekt der Wiederverwendbarkeit. Im Schritt der Gefährdungsidentifikation konnte bereits dargestellt werden, wie dieses Wissen innerhalb eines Anwendungsfalls bereitgestellt werden kann. Im Schritt der Risikobewertung ist es somit notwendig, nach erfolgter Planung dieses Wissen für spätere Anwendungsfälle zu speichern. Dafür wurde das in Kapitel 3 entwickelte Konzept der Wissensbasis in ein entsprechendes Datenmodell überführt, in welchem die erforderliche Generalisierung der Elemente und Relationen abgebildet wird. Aus diesem Datenmodell heraus wurde eine einfache Editoranwendung erzeugt, um eingepflegte Informationen einsehen und manipulieren zu können. Zusätzlich wurden Funktionalitäten entwickelt, ein durch Planung einer Operation entwickeltes Prozessmodell mit darin verknüpften Informationen wie Gefährdungen, Ursachen, risikomindernden Maßnahmen sowie auch vorgenommenen Strukturierungen, in die Wissensbasis zu überführen. Dafür wird eine Prozessmodelldatei in der **Projektsicht** selektiert und daraufhin die Funktion zum Exportieren ausgewählt. Die vorliegenden Informationen werden daraufhin automatisch in die Wissensbasis überführt.

4.6 Zusammenfassung

Mit Hilfe der vorgenommenen und erläuterten Implementierungsarbeiten konnten die in Kapitel 3 entwickelten Ideen und Konzepte prototypisch umgesetzt werden, sodass durch diese Umsetzung Anforderung 10 - softwareseitige Unterstützung erfüllt werden konnte. Dabei wurde anlog zum vorgeschlagenen Vorgehen aus Kapitel 3 vorgegangen und die resultierende Implementierung jeweils schrittweise anhand von Bildschirmausschnitten präsentiert. Im Schritt der Systemdefinition wurde somit das bestehende grafische Werkzeug MOPhisTo zur Prozessmodellierung verwendet und im Rahmen der darauf folgenden Schritte erweitert. Im Schritt der Gefährdungsidentifikation wurden Werkzeuge dargestellt, mit denen u.a. Gefährdungen und Ursachen in ein zugrundeliegendes Prozessmodell sowohl rein manuell, als auch mit Hilfe der Wissensbasis, eingepflegt werden können. In der Risikoanalyse konnten daraufhin Schritte zur manuellen sowie zur automatisierten Strukturierung dieser Informationen und darauf aufbauend zur Konstruktion und Berechnung der Fehlerbäume mit anschließender Dokumentation erläutert werden. Zum Abschluss wurde aufgezeigt, wie eingebrachte Informationen im Sinne der späteren Wiederverwendung, strukturiert gespeichert werden können. Diese dargestellten Arbeiten zur prototypischen Umsetzung sollen im nachfolgenden Kapitel dazu dienen, den Ansatz zu evaluieren.

Kapitel 5

Evaluation

In den beiden vorangegangenen Kapiteln wurde ein Lösungsansatz anhand eines systematischen Vorgehens entwickelt und umgesetzt. Für eine notwendige Evaluation des Ansatzes wird die beschriebene prototypische Umsetzung mit folgender Zielvorstellung genutzt:

- **Demonstration der praktischen Anwendung:** Als ein wesentliches Ziel der Evaluation soll die praktische Anwendung des entwickelten Ansatzes demonstriert werden. Dabei wird anhand des schrittweisen systematischen Vorgehens die Anwendung des Lösungsansatzes anhand ausgewählter realer Problemstellungen mit Hilfe der vorgenommenen Umsetzung beschrieben.
- **Überprüfung der Zielerfüllung:** Mit Hilfe der praktischen Anwendung des Lösungsansatzes wird als weiteres Ziel der Evaluation die Erfüllung der in Abschnitt 1.3 aufgestellten Zielvorstellungen untersucht.
- **Untersuchung der Machbarkeit und Grenzen:** Um den entwickelten Lösungsansatz kritisch zu hinterfragen ist ein letztes Ziel der Evaluation die Machbarkeit und Grenzen des Ansatzes zu untersuchen.

Um die praktische Anwendung und Machbarkeit der Durchführung des Ansatzes zu demonstrieren wurden zwei reale Fallbeispiele (Personentransfer, Lotsenwesen) ausgewählt anhand derer der Lösungsansatz angewendet wird. Beide Fallbeispiele werden dafür zunächst in ihrer jeweiligen Ausgangssituation beschrieben, woraufhin die Durchführung des Ansatzes anhand des bekannten systematischen Vorgehens mit den Schritten zur Systemdefinition, Gefährdungsidentifikation, Risikoanalyse und Risikobewertung erläutert wird. Dadurch wird eine **qualitative Evaluation** des Ansatzes vorgenommen, indem dabei eine systematische Bearbeitung der Fallbeispiele mit Hilfe des Ansatzes erfolgt, sodass das Zusammenwirken der einzelnen Aspekte im Rahmen des schrittweisen Vorgehens erläutert wird. Im Anschluss erfolgt jeweils eine Zusammenfassung der Ergebnisse und Einordnung der Zielerfüllung durch die Umsetzung des Ansatzes.

Nachdem mit der Durchführung der Fallbeispiele die Machbarkeit des Ansatzes gezeigt wurde, wird zur Vervollständigung der Evaluation des Ansatzes eine **quantitative Evaluation** mit Hilfe einer Nutzerstudie durchgeführt. Dadurch wird ein Vergleich des in dieser Ausarbeitung entwickelten Ansatzes mit dem bisherigen Vorgehen ermöglicht. Zur weiteren Belegung dieser Ergebnisse wurde als viertes Evaluationsszenario gezielt die praktische Eignung des Ansatzes mit Hilfe von maritimen Sicherheitsexperten untersucht, um somit die Machbarkeit und Grenzen des Ansatzes aus Sicht der Praxis zu reflektieren. Das Vorgehen dieser Untersuchung und die gewonnenen Erkenntnisse und Ergebnisse werden somit zum Abschluss des Szenarios erläutert.

5.1 Fallbeispiel: Personentransfer

Die Evaluation des entwickelten Lösungsansatzes beginnt mit dem Fallbeispiel des Personentransfers. Dieses wurde als einer der wiederkehrenden Anwendungsfälle der maritimen Domäne identifiziert, in dem Personen von Schiffen auf Offshore-Plattformen oder andere Schiffe übersteigen müssen [Sch09, S. 9]. Der Personentransfer stellt somit eine repräsentative maritime Operation dar, für die eine vorhergehende Planung und Gefährdungsbeurteilung erforderlich ist. Im Rahmen der Evaluation des Ansatzes ist dieses Fallbeispiel somit ausgewählt worden, um die praktische Anwendung des Ansatzes zu demonstrieren sowie die Machbarkeit und Grenzen des Ansatzes anhand eines repräsentativen Fallbeispiels zu demonstrieren und dabei die Zielerfüllung des Ansatzes zu untersuchen. Weiterhin wird dabei die folgende praktische Fragestellung durch das Fallbeispiel adressiert:

Eignet sich der entwickelte Lösungsansatz zur Durchführung einer Gefährdungsbeurteilung zum Erkenntnisgewinn über Abläufe und Risiken der geplanten maritimen Operation?

In den nachfolgenden Unterabschnitten wird zur Beantwortung dieser Fragestellung zunächst die aktuelle Ausgangssituation des Fallbeispiels erläutert. Daraufhin wird die Durchführung des Fallbeispiels anhand des systematischen Vorgehens des Ansatzes schrittweise erläutert und zum Abschluss die Ergebnisse und Zielerfüllung durch den Ansatz beschrieben. Teile der Ergebnisse der exemplarischen Anwendung dieses Fallbeispiels wurden bereits in [LDP+14] veröffentlicht und präsentiert.

5.1.1 Ausgangssituation

Beim Aufbau von Offshore-Wind Plattformen ist eine häufig auftretende Operation die des Personentransfers. Diese ist ein wesentlicher Bestandteil im Rahmen von Installations- oder Wartungsarbeiten, um das notwendige Personal zum Einsatzort zu befördern. Die Operation des Personentransfers umfasst dabei grundlegend den Transport und das Übersteigen einer Person auf die entsprechende Plattform. Dieser Prozess wird als kritisch eingestuft,

da dieser maßgeblich von Wetterbedingungen abhängig ist und zudem hohen finanziellen Einfluss durch mögliche Stillstandszeiten oder menschliche Fehler hat [GAAR14]. Derartige maritime Operationen gelten somit als Herausforderungen für beteiligte Personen, da die Arbeiten witterungsabhängiger sind als vergleichbare Tätigkeiten an Land [Sch09, S. 7]. Kommt es zu Unfällen, ist der wie an Land gewohnt direkte und schnelle Zugang zu Rettungsdiensten aufgrund der Distanz beschränkt, sodass der Einsatz von Notfall- und Rettungsmaßnahmen erheblich mehr Zeit in Anspruch nehmen kann [Lob12]. Um somit die Sicherheit zu erhöhen sind derartige Prozesse Bestandteil von vorbereitenden Trainingsmaßnahmen [RK13]. Ein entsprechendes Bewusstsein über das Vorgehen, mögliche Gefährdungen und Ursachen einer solchen Operation ist daher notwendig bei der Durchführung, sodass sich diese Operation als ein Fallbeispiel zur Evaluation eignet, indem dafür eine entsprechende Planung mit Gefährdungsbeurteilung erforderlich ist.

5.1.2 Durchführung des Fallbeispiels

Die Durchführung des Ansatzes anhand des Fallbeispiels Personentransfer wird nach dem bisher verwendeten systematischen Vorgehen strukturiert. Dafür werden zunächst im Schritt der Systemdefinition die erforderlichen Personen und deren Arbeitsabläufe im Anwendungsfall mit Hilfe von MOPhisTo abgebildet. Anschließend werden im Schritt der Gefährdungsidentifikation ausgewählte mögliche Gefährdungen und Ursachen beim Personentransfer den modellierten Abläufen hinzugefügt. Im Schritt der Risikoanalyse werden die eingepflegten möglichen Ursachen daraufhin zunächst strukturiert, woraufhin Fehlerbäume erstellt und ausgewertet werden. Auf Basis der aus diesen Informationen resultierenden Dokumentation erfolgt der abschließende Schritt zur Risikobewertung. Unterstützend zur Durchführung des Fallbeispiels mit Hilfe des entwickelten Lösungsansatzes werden Informationen realer, abgeschlossener Planungsvorhaben maritimer Operationen mit Personentransfer genutzt. Aus diesen textuellen Beschreibungen werden die entsprechenden Arbeitsabläufe sowie mögliche Gefährdungen, Ursachen und Bewertungen angelehnt, um das Fallbeispiel praxisnah zur späteren Überprüfung durch maritime Sicherheitsexperten abbilden zu können.

Systemdefinition

In Anlehnung an abgeschlossene Planungen und Gefährdungsbeurteilung maritimer Operationen mit Personentransfer, sind im Rahmen der Systemdefinition die Abläufe der Operation in Form eines graphischen Prozessmodells, wie in Abbildung 5.1 dargestellt, modelliert worden. Als die beteiligten Personen (`Actors`) wurden dabei die Folgenden identifiziert:

- Übersteigendes Personal (engl. Offshore Personnel)
- Bootsmann (engl. Boatswain)

- Schiffsführung (engl. Ship's Command)
- Deckspersonal (engl. Ship's Crew)

Diese Akteure sind jeweils als eigener, grafisch abgegrenzter Bereich im Prozessmodell abgebildet und mit entsprechenden Abläufen (`WorkingProcedure`) mit Tätigkeiten und Kommunikation modelliert worden. Zusätzlich sind den Akteuren, die gleichermaßen als physikalische Objekte wie in Kapitel 3.3.1 beschrieben Bestandteil der Systemdefinition sind, für die Durchführung der Offshore-Operation erforderliche Qualifikationen hinzugefügt worden, wie die erforderliche Sicherheitsschulung ($p_{qualification} = \{qualification$, Basic Safety Offshore Training$\}$) und bescheinigte Gesundheitsüberprüfung ($p_{qualification} = \{qualification$, Occupational Health Screening G 41$\}$).

Die Abläufe des Prozesses beginnen zunächst bei der Schiffsführung, indem der Sicherheitsbereich befahren wird (**Task: Enter safety zone**) und die Situation vor Ort im Hinblick auf die Durchführbarkeit der Operation überprüft wird (**Task: Assess situation**). Ist die Operation in der aktuellen Situation durchführbar, gibt die Schiffsführung

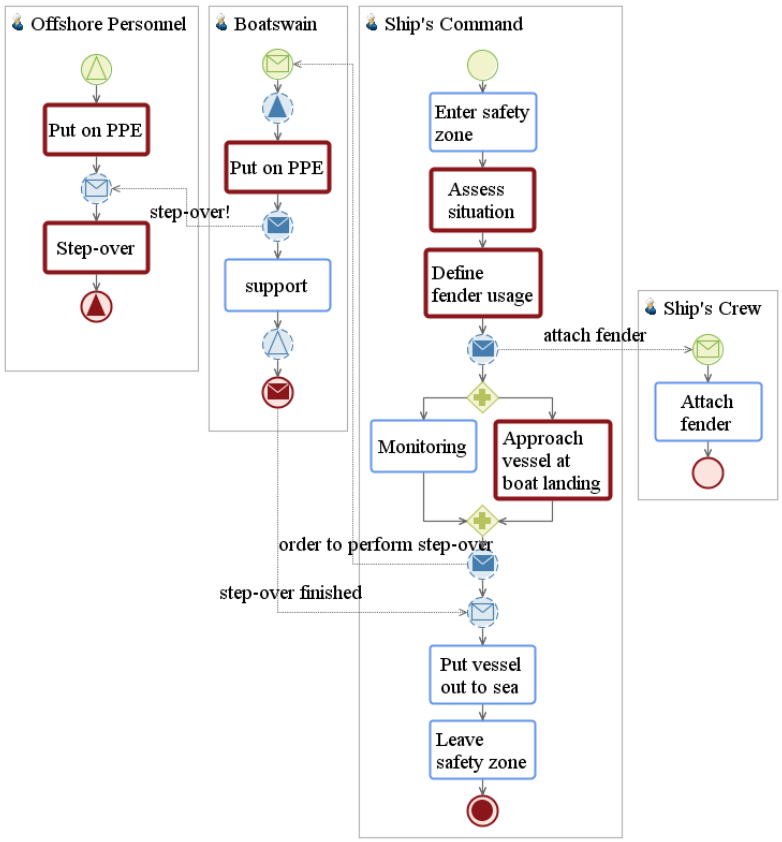

Abbildung 5.1: Graphisches Prozessmodell der Abläufe des Fallbeispiels Personentransfer

die Benutzung der Fender vor (**Task: Define fender usage)** und kommuniziert dies an die Decksbesatzung, welche die Vorgaben umsetzt (**Task: Attach fender**). Anschließend erfolgt die Anfahrt an die Plattform (**Task: Approach vessel at boat landing**), welche parallel überwacht werden muss (**Task: Monitoring**). Ist dies geschehen wird dem Bootsmann mitgeteilt, dass das Übersteigen stattfinden kann, welcher wiederum das Personal entsprechend informiert. Beide Akteure bereiten sich darauf vor und ziehen die erforderliche Schutzkleidung an (**Task: Put on PPE**). Nach der Aufforderung des Bootsmannes kann das Personal übersteigen (**Task: Step-over**), wobei der Bootsmann Hilfestellung leistet (**Task: Support**). Ist dies geschehen legt das Schiff wieder ab (**Task: Put vessel out to sea**) und verlässt den Sicherheitsbereich (**Task: Leave safety zone**). Im Schritt der Systemdefinition wurden somit die stattfindenden Abläufe graphisch abgebildet (siehe Abbildung 5.1) und sowohl Tätigkeiten (`Tasks`) den jeweiligen Akteuren (`Actors`) zugeordnet als auch Kommunikation dieser eingepflegt. Das entwickelte graphische Prozessmodell dient somit als Grundlage für die nachfolgenden Schritte des systematischen Vorgehens.

Gefährdungsidentifikation

Nachdem die Modellierung der Abläufe in der Systemdefinition beendet ist, folgt der Schritt zur Gefährdungsidentifikation mit der Modellierung von Gefährdungen und Ursachen sowie darüber hinaus der Festlegung von Betriebssituationen, Schadensfolgen, risikomindernden Maßnahmen und entsprechenden Kenngrößen hinsichtlich der Häufigkeit und Schadensschwere. Für dieses Vorgehen können, wie in Kapitel 3.3.2 beschrieben, verschiedene Informationsquellen genutzt werden. Da das Fallbeispiel des Personentransfers eine Art Standard-Operation darstellt, die beim Aufbau von Windkraftenergieanlagen und anderen Offshore Bauten regelmäßig stattfindet, sind dafür relevante Informationen zur Gefährdungsidentifikation aus vorangegangenen, in der Literatur dokumentierten, Planungen bekannt. Wären diese Gefährdungsbeurteilungen in der Vergangenheit mit dem entwickelten Lösungsansatz umgesetzt worden, so könnte die Wissensbasis diese Informationen bereitstellen, die jedoch aufgrund der initialen Anwendung des Ansatzes im Rahmen des Fallbeispiels zunächst als leer angenommen wird.

Somit dienen dokumentierte Informationen aus abgeschlossenen Gefährdungsbeurteilungen als Informationsquelle und werden im Rahmen des Lösungsansatzes, wie in Kapitel 3.3.2 beschrieben, manuell eingepflegt. Anhand dieser Informationen lassen sich wie folgt die zwei wesentlichen Gefährdungen (`Hazards`) im Fallbeispiel identifizieren:

- Zusammenstoßen von Schiffen mit der Plattform
- Sturz beim Übersteigen

Diese Informationen wie die identifizierten `Hazards` wurden dabei jeweils als Elemente von $M_{gefident}$ modelliert und Elementen des Prozessmodells zugeordnet, wie schematisch in Abbildung 5.2 für Zusammenstoß und in Abbildung 5.3 für Sturz dargestellt.

Zusammenstoß Die Gefährdung des Zusammenstoßens von Schiffen mit der Plattform besteht zumeist vor Anlegen des jeweiligen Schiffes an die Offshore-Plattform. Relevante Bestandteile dieser Gefährdung hängen somit überwiegend mit dem vorderen Teil des zugrundeliegenden Prozesses zusammen, weshalb dieser Auszug des Prozesses in Abbildung 5.2 links dargestellt wird. Die entsprechende Betriebssituation lässt sich somit als `OperationalSituation` wie in Abbildung 5.2 rechts dargestellt beschreiben. Kombiniert

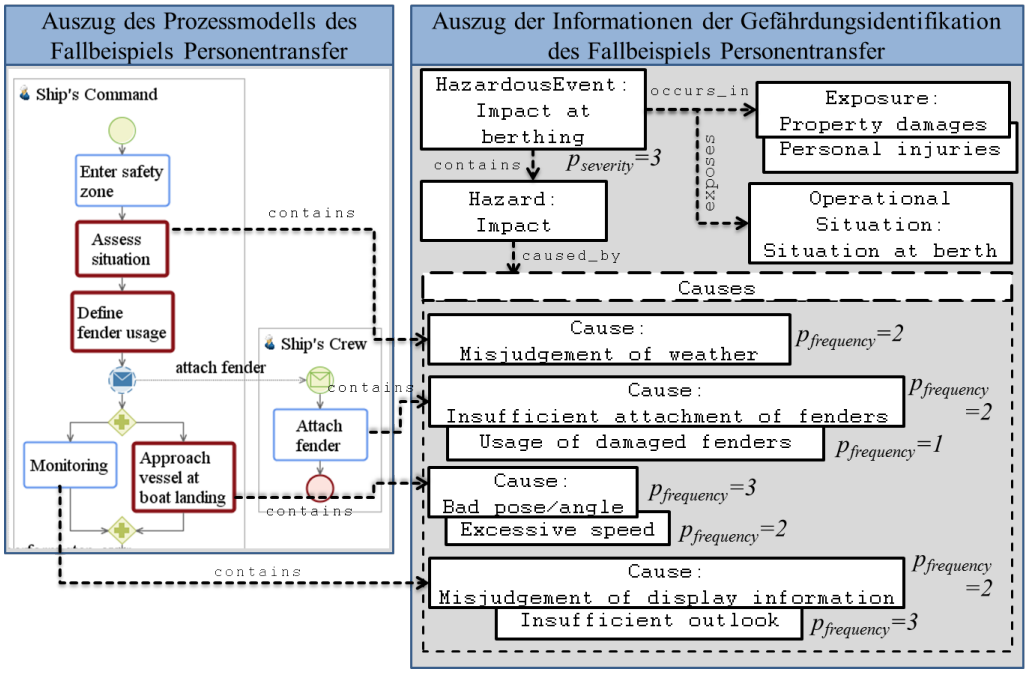

Abbildung 5.2: Schematische Darstellung der in der Gefährdungsidentifikation für die Gefährdung Zusammenstoß eingepflegten Elemente und Zusammenhänge

mit möglichen Personen- oder Sachschäden, die als `Exposures` modelliert wurden, ergibt sich mit der `OperationalSituation` das `HazardousEvent` für die Gefährdung des Zusammenstoßes. Mögliche Ursachen die als `Causes` modelliert werden, ergeben sich durch die systematische Betrachtung der relevanten Aktivitäten im Prozessmodell. Eine frühzeitige Ursache im Prozess kann somit die Fehleinschätzung des Wetters einen wesentlichen Beitrag zur Gefährdung Zusammenstoß sein, die als `Cause` modelliert und mit dem zugrundeliegenden Prozesselement als Γ : *contains* in Zusammenhang gebracht wird. Denn obwohl die Bewertung der Situation (**Task: Assess situation**) bereits Bestandteil einer Tätigkeit im Prozess ist, kann das Wetter entgegen der Bewertung umschlagen und somit eine mögliche Ursache ergeben [Bri14]. Als weiteres kann die Anfahrt an die Plattform (**Task: Approach Vessel**) wesentliche Ursachen durch beispielsweise eine zu hohe Geschwindigkeit oder einen schlechten Anfahrtswinkel beitragen. Die Anfahrt wird dabei zwar kontinuier-

lich Überwacht (**Task: Monitoring**), jedoch hält dies wiederum bekannte Ursachen bereit, sodass auch ein schlechter Ausblick oder Fehleinschätzungen der Lage bei dieser Aktivität zum Zusammenstoß führen können. Als letzte der als relevant identifizierten Aktivitäten birgt das Festmachen der Fender (**Task: Attach fender**) die Möglichkeit Ursachen für einen Zusammenstoß zu ermöglichen, indem dort möglicherweise falsche oder beschädigte Fender verwendet werden [Bri14], sodass diese nicht wie beabsichtigt als Schutzkörper zum Halten des Abstands oder als Stoßdämpfer dienen können.

Sturz Im späteren Teil des Prozesses bzw. der Operation, wie als Auszug in Abbildung 5.3 links dargestellt, kann die weitere Gefährdung des Sturzes verortet werden, welche eine wiederkehrende Herausforderung beim Überstieg darstellt [Bri14]. Diese Gefährdung kann erst in einer Betriebssituation auftreten, bei der das Schiff bereits an einer Plattform angelegt ist und der Überstieg beginnen kann. Somit findet die Betriebssituation und Kontext dieser Gefährdung auf See nach erfolgtem Anlegen des Schiffes an der entsprechenden Plattform im Rahmen der Übersteigen-Prozedur statt, was als `OperationalSituation` entsprechend dokumentiert wird. Nach dem beschriebenen Vorgehen in Kapitel 3.3.2 sind dafür nun Ursachen zu identifizieren und zu modellieren sowie dabei mit Elementen des Prozessmodells in Zusammenhang zu bringen. Mögliche Ursachen für diese Gefährdung können sich dabei beispielsweise bereits durch die Schutzausrüstung (**Task: Put on PPE**) ergeben, die zwar zum einen die Sicherheit beim Übersteigen erhöht, jedoch zum anderen auch Defekt oder falsch angelegt sein und somit zur Gefährdung beitragen kann. Weitere Ursachen werden durch den tatsächlichen Überstieg (**Task: Step-Over**) ermöglicht, sodass hierbei das Ausrutschen oder Stolpern in der Gefährdung Sturz enden können. Für den Eintrittsfall derlei Ursachen bzw. zur Vermeidung derer, finden zusätzliche Hilfestellungen beim Überstieg (**Task: Support**) statt. Jedoch ist eine wiederkehrende Problematik das Weglassen von Tätigkeiten [BM05], sodass das Fehlen oder die falsche Durchführung dieser Hilfestellungen jeweils weitere Ursachen darstellen, die wie die zuvor aufgeführten Ursachen als entsprechende `Causes`, wie in Abbildung 5.3 dargestellt, modelliert wurden. Darüber hinaus sind, wie bei Gefährdungsbeurteilungen erforderlich, Kenngrößen zur Bestimmung der Häufigkeit und Schadensschwere definiert worden. Diese sind entsprechend des Lösungsansatzes als Attribute $p_{frequency}$ bzw. $p_{severity}$, wie in Abbildung 5.3 dargestellt, in Anlehnung an abgeschlossene Gefährdungsbeurteilungen dieses Fallbeispiels, ausgewählt und für die jeweiligen `Causes` bzw. das `HazardousEvent` eingepflegt worden. Risikomindernde Maßnahmen zur Reduktion der Häufigkeit (`CounterMeasure`) und der Schadensschwere (`MitigationMeasure`) konnten zusätzlich mit ihrem spezifischen Einfluss auf `Causes` und `HazardousEvents` berücksichtigt werden, womit die erforderlichen Informationen zur Gefährdungsidentifikation für Gefährdungsbeurteilungen mit Hilfe des Lösungsansatzes vollständig abgebildet und eingepflegt werden konnten.

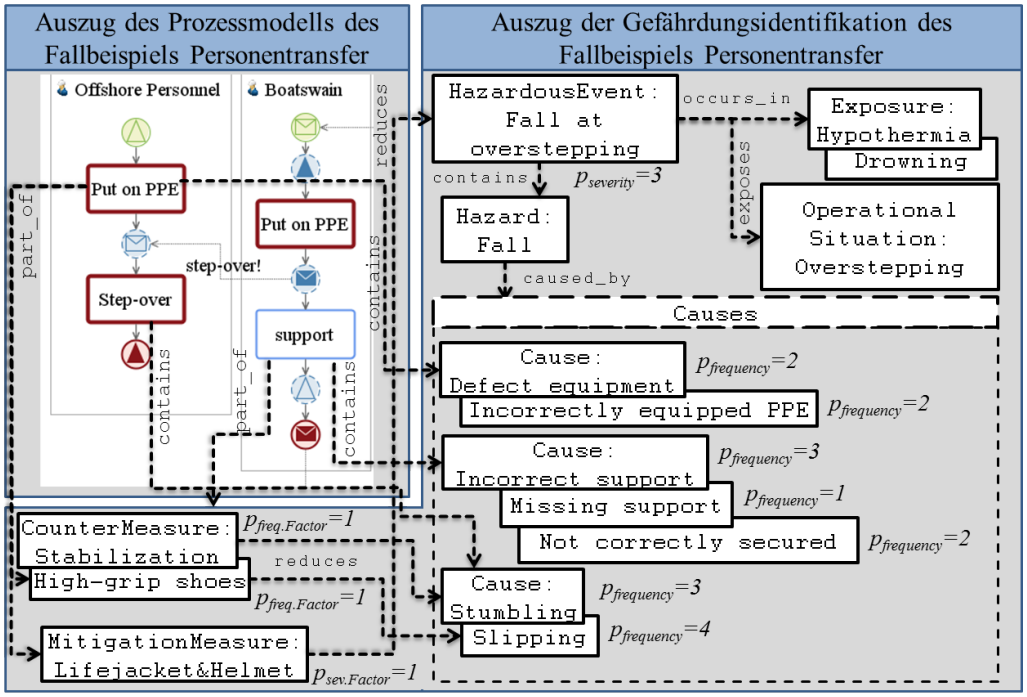

Abbildung 5.3: Schematische Darstellung der in der Gefährdungsidentifikation für die Gefährdung Sturz eingepflegten Elemente und Zusammenhänge

Risikoanalyse

In den vorangegangenen Schritten wurde vorgestellt, wie erforderliche Informationen zur Gefährdungsbeurteilung des Fallbeispiels im Rahmen der Systemdefinition und Gefährdungsidentifikation mit dem entwickelten Lösungsansatz eingepflegt werden können. Damit nun auf Basis dieser Informationen eine Risikoanalyse stattfinden kann, folgen wie in Kapitel 3.3.3 beschrieben, Schritte zur weiteren Strukturierung, Konstruktion von Fehlerbäumen, Auswertung der Bäume durch den Schritt der Berechnung sowie abschließend eine zusammenfassende Dokumentation der Risikoanalyse. Diese Schritte werden in den nachfolgenden Unterabschnitten im Rahmen des Fallbeispiels Personentransfer erläutert.

Strukturierung Im ersten Schritt zur Risikoanalyse werden die in den vorangegangenen Schritten eingepflegten `Causes` weiter strukturiert. Wie in Kapitel 3.3.3 beschrieben, kann dies manuell mit dem in Abbildung 4.5 dargestellten Werkzeug vorgenommen werden oder als Basisstruktur Ergebnisse der implementierten Algorithmen, wie in Abbildung 4.6 dargestellt, ausgewählt werden. Eine derartige Strukturierung wird dabei für jeden `Hazard` des Fallbeispiels und somit für Zusammenstoß und Sturz vorgenommen. Aufgrund der Möglichkeit zur automatischen Strukturierung in welcher die logischen und hierarchischen

Zusammenhänge als Orientierungshilfe erstellt werden, wird für die Gefährdungen jeweils der Strukturvorschlag des Structure Guessed-Algorithmus verwendet, sodass sich daraus die in Abbildung 5.4 dargestellten Strukturierungen ergeben.

Für die Gefährdung **Zusammenstoß** ergibt sich somit die in Abbildung 5.4 links dargestellte Struktur von möglichen Ursachen (`CauseStructures`). Als in der Hierarchie am höchsten stehende Ursache wird die fehlerhafte Wettereinschätzung aufgeführt (Abbildung 5.4 a), was damit eine übergeordnete Ursache darstellt und durch die übergeordnete Veroderung mit weiteren Ursachen bereits zu der Gefährdung führen kann. Die Position dieser Ursache in der Hierarchie ergibt sich dadurch, dass diese Ursache als erste relevante für diese Gefährdung im Prozess aufgeführt wird und somit entsprechend nach Algorithmus 1 chronologisch als erste aufgeführt wird, was in diesem Fall auch semantisch plausibel erscheint. Weitere Ursachen werden in der Hierarchie verundet eingebracht (Abbildung 5.4 b), was aus den parallel stattfindenden Aktivitäten der Schiffsbesatzung zum Anbringen der Fender sowie aus den Aktivitäten zum gezielten Anlegen des Schiffes an der Plattform resultiert. Somit können beispielsweise eine falsche Verwendung der Fender (Abbildung 5.4 c), beispielsweise an falscher Stelle, zu hoch oder zu tief angebracht, in Kombination mit einer zu hohen Geschwindigkeit und schlechter Sicht, zu der Gefährdung Zusammenstoß mit der Plattform führen. Andererseits können möglicherweise eingetretene Ursachen der Schiffsführung durch korrekt angebrachte Fender durch deren Funktion als Schutzkörper ausgeglichen werden, sodass kein unbeabsichtigter Zusammenstoß eintritt.

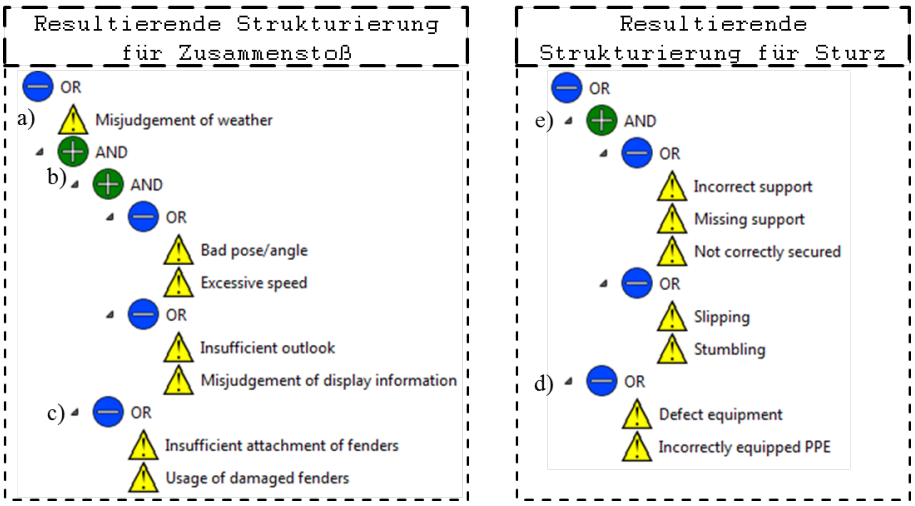

Abbildung 5.4: Resultierende Strukturierungen für Zusammenstoß (links) und Sturz (rechts) des Fallbeispiels Personentransfer

Für die Gefährdung **Sturz** ergibt sich die in Abbildung 5.4 rechts dargestellte Strukturierung. Diese resultiert zunächst nach Algorithmus 1 aus der Veroderung der einzelnen

Sequenz zum Anziehen der Schutzkleidung des Personals und der dort entsprechend eingebrachten Ursachen (Abbildung 5.4 d). Ein weiterer Bestandteil dieser Sequenz ist die anschließend parallele Durchführung von Hilfestellung und Übersteigen, was eine Verundung der für diese Tätigkeiten eingebrachten Ursachen in der Strukturierung ergibt (Abbildung 5.4 e). Nach dieser Struktur kann somit falsch angelegte oder defekte Schutzkleidung bereits zu der Gefährdung Sturz führen, da so die darin enthaltenen Überstiegshilfen, wie Gurte zur Befestigung, verwendet werden, jedoch dem Gewicht der Personen nicht standhalten können. Weiterhin kann die Gefährdung durch fehlende oder falsche Hilfestellungen und ein gleichzeitiges Ausrutschen oder Stolpern des Personals stattfinden. Im Gegenzug kann das Ausrutschen oder Stolpern einer Person möglicherweise durch korrekte Hilfestellungen kompensiert werden, sodass es nicht zum Sturz kommt.

Konstruktion Nachfolgend zum Schritt der Strukturierung erfolgt die Erstellung von Fehlerbäumen für die jeweils betrachteten Gefährdungen des Fallbeispiels. Die Abbildung 5.5 zeigt daher die aus der Anwendung von Algorithmus 2 resultierenden Fehlerbäume der Gefährdungen Zusammenstoß (links) und Sturz (rechts). Als Basis für die Konstruktion wurden dafür jeweils die zuvor in Abbildung 5.4 dargestellten Strukturierungen genutzt. Die Konstruktion wurde durch Einsatz von Algorithmus 2 (siehe Kapitel 3.3.3) nach Aufruf der entsprechenden Funktion in der prototypischen Umsetzung, ohne weitere Interaktion mit dem Nutzer automatisiert vorgenommen. Dabei sind die logischen Operatoren (`LogicOperators`) der vorgenommenen Strukturierungen entsprechend in `FaultTreeGates` des Fehlerbaumes überführt sowie die jeweiligen Ursachen (`Causes`) als `BasicEvents` eingepflegt worden. Das `TopEvent` des Fehlerbaumes wurde jeweils entsprechend der betrachteten Gefährdung Zusammenstoß bzw. Sturz erstellt. Weiterhin wurden bei der Konstruktion im Prozess eingepflegte risikomindernde Maßnahmen mit berücksichtigt, sodass beispielsweise die Hilfestellung sowie die Schutzausrüstung als solche sich positiv auf die Häufigkeitsklassen der Ursachen von Stolpern und Ausrutschen auswirken. Diese Zusammenhänge wurden bei der Konstruktion für die jeweiligen Elemente im Fehlerbaum übernommen, sodass sowohl die neutralen ($p_{frequency}$) als auch die Werte mit berücksichtigten risikomindernden Maßnahmen ($p_{mitigatedFrequency}$) eingesehen werden können. Dies veranschaulicht das `BasicEvent` Slipping, welches entsprechend des Konzepts den ursprünglichen `Cause` assoziiert und daher den dort hinterlegten ursprünglichen Wert als $p_{frequency} = 4$ übernimmt. Als weiteres Attribut dieses Events wird die $p_{mitigatedFrequency}$ im Algorithmus als Wert unter Berücksichtigung der relevanten risikomindernden Maßnahmen ermittelt. Die Ermittlung dieses Wertes erfolgt über die vorgenommene Zuordnung von Maßnahmen ($\Gamma : reduces$) und deren Einflussfaktor $p_{frequencyFactor}$ auf eine Ursache (`Cause`), welcher mit der ursprünglichen $p_{frequency}$ verrechnet und im `BasicEvent` hinterlegt wird. Im Fall dieses Events hat das Sicherheitsschuhwerk als Maßnahme und Teil der Schutzausrüstung einen $p_{frequencyFactor} = 1$ (siehe Abbildung 5.3), woraus sich die $p_{mitigatedFrequency} = 3$ für

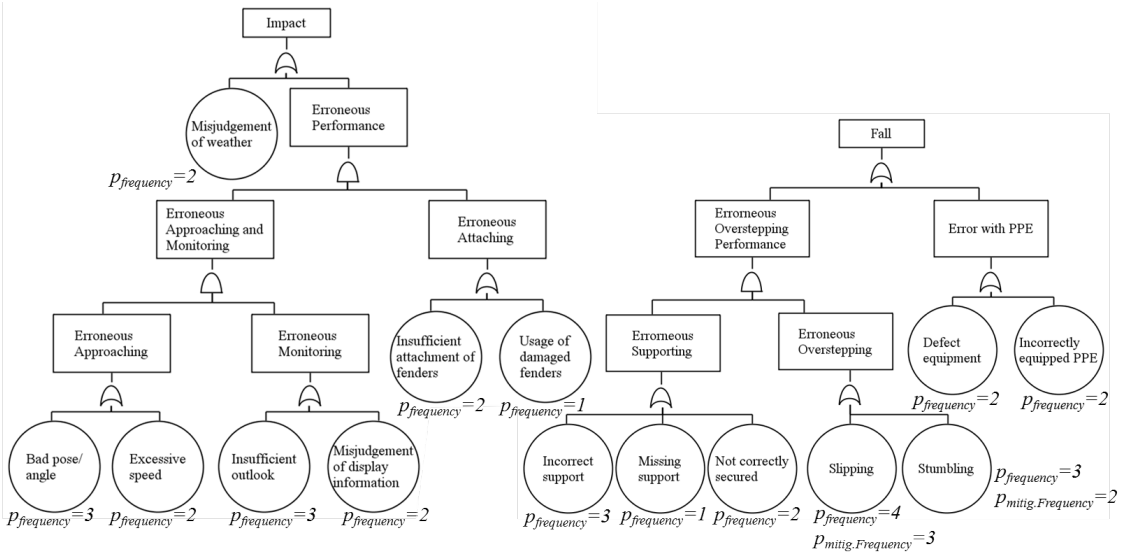

Abbildung 5.5: Aus der Konstruktion resultierende Fehlerbäume für die Gefährdung Zusammenstoß (links) und Sturz (rechts) des Fallbeispiels Personentransfer

das `BasicEvent` ergibt.

Berechnung Direkt im Anschluss an die Konstruktion wird die Auswertung der Fehlerbäume als Schritt der Berechnung angestoßen. Dabei wird die Häufigkeitsstufe $p_{frequency}$ bzw. Eintrittswahrscheinlichkeit $p_{probability}$ der Gefährdung ermittelt, indem im Rahmen der Fehlerbaumanalyse der Wert für das jeweilige `TopEvent` berechnet wird. Diese Berechnung wird dabei sukzessive für alle Fehlerbaumelemente durchgeführt, sodass innerhalb der Fehlerbaumeditoranwendung, wie in Abbildung 4.7 dargestellt, diese Ergebnisse in der Fehlerbaumdarstellung bzw. der Eigenschaftssicht für alle `FaultTreeObjects` eingesehen werden können. Dabei wurden die jeweils als $p_{frequency}$ zuvor zugeordneten Häufigkeitsstufen der Ursachen, wie in Kapitel 3.3.3 beschrieben, zur Berechnung in $p_{probability}$ Werte der entsprechenden Events im Fehlerbaum überführt. Über die Werte von $p_{probability}$ wurde daraufhin die Berechnung entsprechend der Berechnungsgrundlagen für Fehlerbäume durchgeführt (siehe Kapitel 3.3.3).

Dokumentation Zum Abschluss des Schrittes der Risikoanalyse werden die ermittelten Ergebnisse und in die Planung eingebrachte Informationen zusammenfassend dokumentiert. Dafür wird der wie in der prototypischen Umsetzung beschriebene Funktionsumfang genutzt, um somit eine Dokumentation des Fallbeispiels im Rahmen der Gefährdungsbeurteilung zu erstellen. Abbildung 5.6 zeigt einen Auszug dieser Dokumentation, welche mit

Hilfe der vorgenommenen prototypischen Umsetzung automatisiert erstellt wurde. Diese Dokumentation beginnt mit der Benennung des Akteurs, Auflistung dessen Attribute wie die in der Systemdefinition als $p_{qualification}$ zugeordneten Qualifikationen sowie darauffolgend mit der systematischen Auflistung der spezifizierten Abläufe (Abbildung 5.6 a). Ergänzt wurde die dort vorgenommene Dokumentation der Arbeitsabläufe um die entsprechend eingepflegten Informationen der Gefährdungsidentifikation, sodass schnell ein Überblick über die jeweils für den Akteur relevanten Informationen gewonnen werden kann. Diese Form der Dokumentation wurde systematisch für jeden der beteiligten Akteure erstellt. Im Anschluss an die Dokumentation der jeweiligen Abläufe des Akteurs, erfolgt zusätzlich eine spezifische Zusammenfassung der relevanten Gefährdungen des Akteurs (Abbildung 5.6 b). Dabei werden die Gefährdungen mit möglichen Folgen und die durch den Akteur beigetragenen und getroffenen risikomindernde Maßnahmen und Ursachen personenspezifisch aufgeschlüsselt. Eine gesonderte übergreifende Dokumentation der Gefährdungen erfolgt im Anschluss an die Dokumentation der Akteure und deren Abläufe (Abbildung 5.6 c). Für die Dokumentation der Gefährdungen werden dabei die erstellten und ausgewerteten Fehlerbäume genutzt, sodass je Fehlerbaum bzw. Gefährdung ein Kapitel in der Dokumentation erstellt wird (Abbildung 5.6 c). Innerhalb eines solchen Kapitels

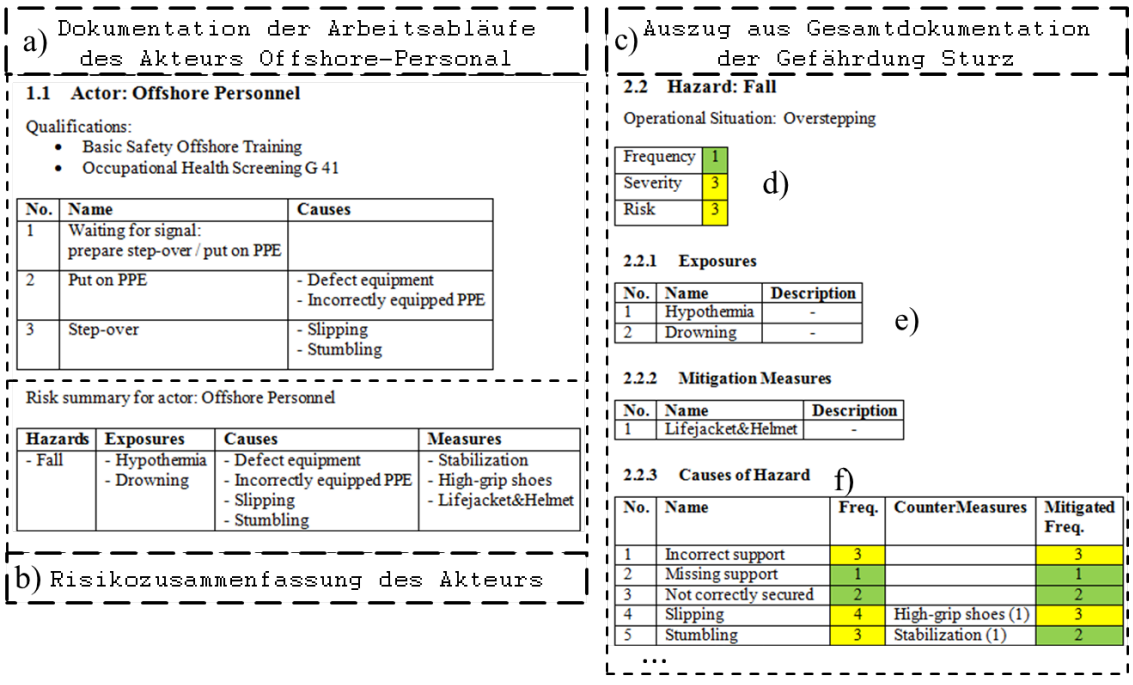

Abbildung 5.6: Auszug aus der zusammenfassenden Dokumentation der Akteure (links) und der Gefährdungen (rechts) des Fallbeispiels Personentransfer

wird zunächst die Zusammenfassung des Risikos dargestellt, bei der die durch den Fehlerbaum ermittelte Häufigkeitsstufe der Gefährdung mit der entsprechenden Schadensschwere verrechnet wird (Abbildung 5.6 d). Darunter werden die möglichen Folgen der Gefährdung aufgelistet (Abbildung 5.6 e). Darauf folgt eine Auflistung der zugeordneten Ursachen mit den dafür ermittelten Wertestufen, darauf wirkenden risikomindernden Maßnahmen und daraus resultierende neue Wertestufen, wie beispielsweise für die Ursache Slipping zuvor erläutert (Abbildung 5.6 f). Durch die so automatisch erstellte Dokumentation konnten zuvor nach dem Vorgehen eingepflegte Informationen zusammenfassend und systematisch dokumentiert werden, sodass diese für eine Gefährdungsbeurteilung genutzt werden können. Durch die textuelle, tabellarische Form der Dokumentation wurde diese angelehnt an die gängige Praxis bei Gefährdungsbeurteilungen, sodass dieses Vorgehen mit einer solchen Präsentation der Ergebnisse für die Domäne zur Planung maritimer Operationen wie Personentransfer geeignet erscheint.

Risikobewertung

Die als abschließender Schritt zur Risikoanalyse erstellte Dokumentation wird für die Risikobewertung im Rahmen der Gefährdungsbeurteilung genutzt. In dieser werden zusammenfassend die bei der Planung gesammelten und eingepflegten Informationen zusammen mit Ergebnissen der Risikoanalyse dargestellt. Auf dieser Basis kann somit konzeptionell entschieden werden, ob das ermittelte Risiko des zugrundeliegend geplanten Fallbeispiels akzeptabel ist bzw. ob eine Umplanung erfolgen muss. Da die Risikobewertung somit ein manuelles Vorgehen ist, wurde für diesen Schritt im Rahmen dieser Ausarbeitung eine Risikobewertung durch maritime Sicherheitsexperten fokussiert, um zu überprüfen ob sich das Vorgehen und Ergebnisse des Ansatzes zur Gefährdungsbeurteilung eignen. Im Sinne des Fallbeispiels wurden dafür die zuvor erläuterten Schritte exemplarisch durchgeführt, um die Machbarkeit und Durchführung des Ansatzes zu demonstrieren. Die daraus resultierenden Ergebnisse wurden daraufhin maritimen Sicherheitsexperten zur Bewertung vorgelegt. Zwar stellen diese Ergebnisse keinen Anspruch auf Vollständigkeit, jedoch konnten maritime Sicherheitsexperten daran die grundsätzliche Machbarkeit und Eignung für eine mögliche Risikobewertung erkennen. Dabei wurde zum einen der in dieser Ausarbeitung entwickelte Ansatz vorgestellt sowie zum anderen die für das Fallbeispiel des Personentransfers vorgenommenen und in den vorangegangenen Abschnitten erläuterten Arbeiten dargelegt. Demnach konnten die maritimen Sicherheitsexperten im Rahmen der Risikobewertung einsehen, inwiefern das mit diesem Ansatz umgesetzte Fallbeispiel die bestehenden Sicherheitskonzepte abbilden kann. Dabei konnte festgestellt werden, dass der hier entwickelte Ansatz in der Lage ist das entwickelte Fallbeispiel plausibel abzubilden und die daraus resultierende Form der Dokumentation für eine Risikobewertung genutzt werden kann. Zusätzlich wurde dabei der Mehrwert des Ansatzes mit einer detaillierteren, formalisierten Risikoanalyse innerhalb eines systematischen Vorgehens, nah an den zugrundeliegenden

Abläufen im Vergleich zum bisherigen Vorgehen, von den Experten positiv bemerkt. Weitere Ausführungen zur Evaluation mit Hilfe von maritimen Sicherheitsexperten folgen in Abschnitt 5.4, in welchem weitergehend die praktische Eignung des Ansatzes untersucht und bewertet wurde.

Überführung in die Wissensbasis Angenommen ein vorliegendes Sicherheitskonzept mit entsprechender Dokumentation wird als ausreichend erachtet, so ist nach dem in dieser Ausarbeitung entwickelten Vorgehen der nächste Schritt das eingepflegte und strukturierte Wissen zu speichern, um dieses für spätere Anwendungsfälle bereitstellen zu können. Durch Entwicklung der Wissensbasis werden diese Informationen, wie beispielsweise Ursachen der Gefährdung, Zuordnungen von Ursachen und Tätigkeiten, betroffene Akteure, vorgenommene Strukturierungen etc., wie zuvor in Kapitel 3 anhand der Abbildungen 3.7 und 3.17 veranschaulicht, verwendet. Diese können dadurch in zukünftigen Anwendungsfällen eingesehen und erneut zur Unterstützung weiterer Vorhaben genutzt werden. Wird dieses Konzept weitergehend für verschiedene Fallbeispiele genutzt, so werden wiederholt involvierte Akteure, wie beispielsweise der Bootsmann, in der Wissensbasis mit mehreren Operationen verknüpft. Gleichermaßen ergeben sich weitere Zusammenhänge durch wiederholt auftretende Aktivitäten, Maßnahmen, Ursachen oder Gefährdungen. Somit kann beispielsweise auch die Gefährdung Sturz innerhalb der Wissensbasis auf mehrere Operationen verweisen, in denen diese Gefährdung bei der Planung anderer Fallbeispiele betrachtet und genutzt wurde. Zugeordnete bzw. ermittelte Werte wie Severity oder Frequency werden als zusätzliche Parameter für jede der Gefährdungen gelistet und werden bei weiterer Verwendung der Gefährdung fortlaufend erweitert. Auch können sich für eine Gefährdung gleichermaßen unterschiedliche Strukturierungen ergeben, die in der Wissensbasis hinterlegt sind. All diese Informationen sind erneut abrufbar, sobald diese in der Wissensbasis hinterlegt wurden, sodass diese entsprechend durchsucht und gezielt bereitgestellt werden können in späteren Anwendungsfällen. Bei der Betrachtung dieses Fallbeispiels wurde die Wissensbasis jedoch zunächst als leer angenommen, um eine initiale Anwendung des Ansatzes demonstrieren zu können, sodass zum Abschluss der Risikobewertung ausschließlich die zuvor erläuterten Informationen des Fallbeispiels darin enthalten sind.

5.1.3 Zusammenfassung und Zielerfüllung

In diesem Abschnitt wurde der in dieser Ausarbeitung entwickelte Ansatz an einem ersten Fallbeispiel angewendet. Dafür wurde der Personentransfer als ein wiederkehrender Prozess, bei dem eine Gefährdungsbeurteilung erforderlich ist, aus der maritimen Domäne ausgewählt. Entgegen dem bisherigen Vorgehen mit überwiegend informeller Handhabung der Informationen wie im Stand der Technik, wurde dieses Fallbeispiel mit seinen zugrundeliegenden Abläufen innerhalb der Systemdefinition in einem Prozessmodell strukturiert und graphisch abgebildet. Dieses Prozessmodell wurde daraufhin im Schritt der Gefährdungsi-

dentifikation hinsichtlich der bei der Operation bestehenden Gefährdungen Zusammenstoß und Sturz sowie für diese Gefährdungen mögliche Ursachen in Form des dafür entwickelten Modells strukturiert ergänzt. Die somit zusammengetragenen Informationen des Fallbeispiels wurden darauffolgend für eine Risikoanalyse verwendet, in welcher die eingebrachten Ursachen einer Gefährdung zunächst mit Hilfe der implementierten Algorithmen logisch und hierarchisch strukturiert wurden. Diese Strukturierung wurde für die automatisierte Konstruktion und Auswertung von Fehlerbäumen verwendet, um für den Schritt der Risikoanalyse eine formalisierte Grundlage ermöglichen zu können. In einer zusammenfassenden Dokumentation wurden diese Ergebnisse und weitere eingebrachte Informationen zur Darstellung und anschließenden Risikobewertung im Rahmen der Gefährdungsbeurteilung aufbereitet. Zum Abschluss wurden der Ansatz und die Dokumentation zur Beantwortung der zu Beginn genannten Fragestellung maritimen Sicherheitsexperten zur Überprüfung vorgelegt. Der Ansatz und die daraus erzeugte zusammenfassende Dokumentation, mit den enthaltenen Informationen der Planung und Ergebnissen der Risikoanalyse, wurden dabei als geeignet empfunden, wodurch die zu Beginn gesetzte Fragestellung beantwortet werden konnte. Zusätzlich wurde dabei der Mehrwert des Ansatzes mit einer detaillierteren, formalisierten Risikoanalyse innerhalb eines systematischen Vorgehens im Vergleich zum bisherigen Vorgehen positiv begutachtet. Detailliertere Informationen zu der Befragung von maritimen Sicherheitsexperten, durch die die Fragestellung beantwortet und die Eignung des Ansatzes nachgewiesen werden konnte, folgen in Kapitel 5.4. Darüber hinaus wurden die eingepflegten Informationen des Vorgehens in die Wissensbasis zur möglichen Wiederverwendung in späteren Anwendungsfällen gespeichert.

Mit diesem erläuterten Vorgehen wurde der erarbeitete Ansatz am Fallbeispiel Personentransfer angewendet. Im Folgenden wird die Erfüllung der zu Beginn der Ausarbeitung gesteckten Ziele, im Rahmen der Umsetzung durch das Fallbeispiel, hinsichtlich der Erfüllung oder nicht-Erfüllung hin bewertet.

- Ziel 1 - Formalisierung des Basiswissens: Für die Modellierung der Abläufe und Personen dieses Anwendungsfalls wurde der entwickelte Prozessmodelleditor MOPhisTo verwendet, wodurch eine Formalisierung des Basiswissens ermöglicht und somit das Ziel **erfüllt** wurde.

- Ziel 2 - Prozessorientierte Risikobetrachtung: Aufbauend auf die modellierten Abläufe des Anwendungsfalls konnten mit dem entwickelten Ansatz relevante Gefährdungen und Ursachen fokussiert auf die Abläufe des Anwendungsfalls eingebracht werden. Das Ziel wurde somit **erfüllt**, da prozessorientierte als auch Aspekte zur Risikobetrachtung somit gemeinsam betrachtet und im Vorgehen verarbeitet werden konnten.

- Ziel 3 - Wiederverwendbare Informationen: In diesem Abschnitt wurde die initiale Anwendung des Ansatzes für das Fallbeispiel Personentransfer betrachtet. Eingebrachte Informationen und Ergebnisse konnten abschließend zum Anwendungsfall in

die Wissensbasis gespeichert werden. Da für eine echte Wiederverwendung jedoch auch eine weitere Nutzung der gespeicherten Informationen erforderlich ist, wird das Ziel nur **teilweise** erfüllt, da dies mit dem Fallbeispiel nicht demonstriert wurde.

- Ziel 4 - Unterstützende formalisierte Risikoanalyse: Im Rahmen der Risikoanalyse konnten mit den implementierten Algorithmen automatisierte Strukturierungsvorschläge als Orientierungshilfe erzeugt, übernommen und manuell angepasst werden. Darauffolgend kann diese Strukturierung automatisch in die formalisierte Struktur von Fehlerbäumen überführt und ausgewertet werden. Das Ziel wurde somit **erfüllt**.

- Ziel 5 - Berücksichtigung risikomindernder Maßnahmen: Innerhalb der Systemdefinition konnten risikomindernde Maßnahmen mit eingepflegt sowie gezielt hinsichtlich ihres Effekts mit möglichen Ursachen verknüpft werden. Weiterhin konnten diese Informationen automatisch innerhalb der Risikoanalyse verwendet und ausgewertet werden, wodurch das Ziel **erfüllt** wird.

- Ziel 6 - Softwareseitige Unterstützung: Im Rahmen der Ausführungen dieses Fallbeispiels ist durchgängig die in der prototypischen Umsetzung beschriebene Implementierung verwendet und mit Abbildungen dargestellt worden. Die erforderlichen Schritte des systematischen Vorgehens dieses Ansatzes sind somit ganzheitlich softwareseitig unterstützt worden, wodurch das Ziel **erfüllt** wird.

Zusammenfassend konnten die aufgestellten Zieldefinitionen, abgesehen vom Aspekt der Bereitstellung von Informationen aus der Wiederverwendbarkeit welcher nicht demonstriert wurde, erfüllt werden. Zwar konnten die eingepflegten Informationen dieses Fallbeispiels in der Wissensbasis gespeichert werden, jedoch war diese zu Beginn des Fallbeispiels leer, sodass hiermit eine initiale Anwendung des Ansatzes demonstriert wurde. Weiterhin lässt sich vermerken, dass die im Fallbeispiel automatisiert vorgenommenen Strukturierungsvorschläge nicht die Semantik möglicher Ursachen im Prozess berücksichtigen, sondern nur eine chronologische Strukturierung von Ursachen im Hinblick auf die zugrundeliegende Prozessmodellstruktur ermöglichen. Dadurch können Ursachen die frühzeitig im Prozessmodell hinterlegt werden, einer höheren Hierarchieebene in der Strukturierung zugeordnet werden als Ursachen die später im Prozess eingepflegt sind. Dies liefert für den hier beschriebenen Anwendungsfall zwar plausible Ergebnisse, jedoch ist eine zusätzliche Überprüfung durch den jeweiligen Sicherheitsexperten ratsam da in anderen Anwendungsfällen möglicherweise eine andere Semantik gewünscht ist als die vorgeschlagene. Daher besteht durchgehend die Möglichkeit derlei Strukturierungen manuell anzupassen, wodurch die durch die Algorithmen erstellten Strukturvorschläge als Orientierungshilfen zu verstehen sind.

5.2 Fallbeispiel: Lotsenwesen bei Hafenmanövern

Zur weiteren Vervollständigung der qualitativen Evaluation des Ansatzes dient das Fallbeispiel des Lotsenwesens. Im Rahmen dieses Fallbeispiels sollen mit dem Ansatz sicherheitskritische Operationen, wie die Interaktion von Lotsen und Schleppern beim Manövrieren, untersucht werden. Innerhalb dieser Operationen werden Schiffsunfälle überwiegend durch menschliche Faktoren verursacht, wobei Ursachen wie Fehleinschätzungen und unzureichende Sicht die Hauptgründe sind [HFM06, S. 402]. Hilfsmittel wie Displays der Schiffsbrücke und teilweise auch sogenannte Portable Pilot Units unterstützen dabei den Lotsen bei der Durchführung seiner Tätigkeiten mit der visuellen Darstellung und Handhabung von notwendigen Informationen. Im Rahmen des Fallbeispiels soll mit dem entwickelten Lösungsansatz untersucht werden, inwiefern ein neuer Augmented Reality Ansatz zur Visualisierung von Informationen, entwickelt von Ostendorp [MCO15], als weiteres Hilfsmittel den Lotsen bei seinen Tätigkeiten unterstützen kann. Die zugrundeliegende Fragestellung des Fallbeispiels, die mit dem entwickelten Lösungsansatz zu beantworten ist, wird somit wie folgt zusammengefasst:

Kann durch einen alternativen Ansatz zur Visualisierung von Informationen die Risikosituation innerhalb von Lotsenoperationen bei Hafenmanövern verbessert werden?

In den nachfolgenden Unterabschnitten wird der in dieser Ausarbeitung entwickelte Ansatz anhand des Fallbeispiels Lotsenwesen angewendet, um diese Fragestellung zu beantworten und somit den Ansatz zu evaluieren. Dafür wird zunächst die aktuelle Ausgangssituation des Lotsenwesens zur Einführung in die Thematik skizziert. Darauf folgt die Durchführung des Fallbeispiels mit Beschreibung der Anwendung des entwickelten Ansatzes. Die Durchführung wird dabei, wie in den Kapiteln zuvor, systematisch in Schritte zur Systemdefinition, Gefährdungsidentifikation, Risikoanalyse und Risikobewertung mit jeweiligen Unterschritten gegliedert. Zum Abschluss erfolgt eine Zusammenfassung und Einordnung der Zielerfüllung des Ansatzes im Hinblick auf das durchgeführte Fallbeispiel.

5.2.1 Ausgangssituation

Die Navigation auf See erfordert im Gegensatz zur Navigation im Hafenbereich unterschiedliche Fähigkeiten und Wissen [Fri08, S. 2]. Die meisten Schiffskollisionen und Grundberührungen passieren im Hafenbereich, da dort die Navigation durch Land, Flachwasser, andere Fahrzeuge und Brücken, Stege, Pier etc. limitiert wird [Fri08, S. 2]. Da somit das sichere Befahren des Hafenbereichs häufig eine besondere Ortskenntnis notwendig macht, können und müssen Schiffe teilweise einen Lotsen aufnehmen [Ohn12, S. 222]. Der Lotse ist dabei in allen nautischen Belangen der kompetente und sachkundige Ansprechpartner u.a. mit Kenntnis über Besonderheiten und Schwierigkeiten des Lotsreviers [Hen, S. 153], sodass die

durch den Lotsen beratenen Kapitäne diesem in der Regel die nautische Führung des Schiffes übergeben [Bun14c]. Dabei sind die Lotsen einer großen Bandbreite unterschiedlicher technischer Hilfsmittel, wie Assistenzsysteme verschiedener Hersteller und Sprachen, Besatzungen, Schiffen etc., ausgesetzt [Lot14]. Zusätzlich werden Schiffe ökonomisch bedingt kontinuierlich größer, sodass Hafenmanöver somit eine immer größere Herausforderung darstellen [MCO15]. Um somit notwendige Informationen zur Navigation und Überwachung der Hafenmanöver visuell bereitzustellen, nutzen Lotsen häufig eine sogenannte Portable Pilot Unit (PPU). Die PPU, häufig als Laptop oder Tablet-System realisiert, stellt somit zwar eine Quelle für zusätzliche Informationen dar, jedoch zwingt diese gleichzeitig den Lotsen dazu den Blick auf das Display zu lenken, obwohl der direkte Blick aus der Schiffsbrücke heraus die wichtigste Informationsquelle bei Lotsenoperationen darstellt [MCO15].

Im Ansatz von Ostendorp [MCO15] wurde daher ein Ansatz mit Smart Glasses vorgestellt, bei dem notwendige Informationen als Augmented Reality Lösung auf einer Brille visualisiert werden, sodass der Blick des Lotsen weniger abgelenkt wird. Zusätzlich wurden dabei alternative graphische Visualisierungen vorgeschlagen, um den Aufwand zur Verarbeitung der Informationen und somit auch dadurch resultierende Fehler, wie Fehleinschätzungen und übersehene Informationen, zu reduzieren. Im Rahmen des MANVIP (Managing Vessels in Port Waters) Projekts wurde diese Möglichkeit zur Unterstützung der Lotsen mit Hilfe des in dieser Ausarbeitung umgesetzten Lösungsansatzes hinsichtlich der zuvor genannten Fragestellung untersucht. Die dabei angewendeten Schritte des systematischen Vorgehens werden in den nachfolgenden Unterabschnitten erläutert.

5.2.2 Durchführung des Fallbeispiels

Die Durchführung des Fallbeispiels orientiert sich, wie in den Kapiteln zuvor, an den Schritten zur Systemdefinition, Gefährdungsidentifikation, Risikoanalyse und Risikobewertung mit jeweiligen Unterschritten. Dabei werden zunächst in der Systemdefinition die wesentlichen Abläufe und Aktivitäten des Lotsen im Fallbeispiel graphisch modelliert. Darauf folgt der Schritt der Gefährdungsidentifikation, in welchem mögliche Gefährdungen und damit zusammenhängende Ursachen identifiziert und eingepflegt werden, wofür die dem Ansatz zugrundeliegende Wissensbasis genutzt wird, um derlei Informationen abgeschlossener Anwendungsfälle wiederverwenden zu können. Zur Ermittlung der notwendigen Kenngrößen der Ursachen wurden maritime Experten befragt, die die Häufigkeit der Ursachen jeweils im Hinblick auf das bisherige Vorgehen sowie auf den Smart Glasses Ansatz hin bewertet haben. In der Risikoanalyse wurden diese Ursachen zunächst strukturiert und anschließend zur Konstruktion und Auswertung von Fehlerbäumen genutzt, sodass die dabei ermittelten Ergebnisse zur Gegenüberstellung der beiden Ansätze verwendet werden konnten. Das Vorgehen schließt mit dem Schritt der Risikobewertung ab, indem im Rahmen des Vorgehens eingepflegte Informationen in die Wissensbasis für eine spätere Wiederverwendung überführt werden.

Systemdefinition

Zur genaueren Definition des betrachteten Fallbeispiels werden im ersten Schritt des systematischen Vorgehens die Abläufe des Fallbeispiels aus Sicht des Lotsen modelliert. Dabei wird das in der prototypischen Umsetzung beschriebene Werkzeug zur Prozessmodellierung mit entsprechender graphischer Symbolik verwendet. Das dabei resultierende graphische Prozessmodell der obersten Ebene (Level 0), mit darin enthaltenen Aktivitäten des Lotsen wie Vorbereitung, Planung, Übersteigen, Einweisung, Navigation im Fahrwasser, Manövrierung, Festmachen und Ausstieg, wird in Abbildung 5.7 (Level 0) dargestellt. Zur weiteren Verfeinerung wurden Sub-Prozesse genutzt, um somit als weitere Ebenen die Aktivitäten detaillierter zu modellieren, die im Rahmen der Hafenmanöver stattfinden. Diese sind das Manövrieren (**Manoeuvring**) und Festmachen (**Mooring Operation**), die wie in Abbildung 5.7 (Level 1) dargestellt, als Sub-Prozesse die Abläufe des Fallbeispiels aus Sicht des Lotsen detaillierter beschreiben. Dabei umfasst das Manövrieren (Level 1 - Manoeuvring) zunächst Aktivitäten zur Vorbereitung des Schleppereinsatzes, wie die Anpassung der Geschwindigkeit, Position und der manuellen Steuerung (**Adjust speed** bis **Change steering mode**). Anschließend werden in einem weiteren Sub-Prozess die Schlepper verbunden (**Connection of tugs**), sodass darauf jeweils nebenläufig die Führung der Schlepper- und Eigenschiffsmanöver (**Guide tug/ship manoeuvring**) stattfindet. Diese werden dem Schema folgend weiter, wie in den Abbildungen 5.8 und 5.9 dargestellt, als eigene Sub-Prozesse verfeinert, sodass sich das Führen der Schlepper und des Eigenschiffs jeweils in Aktivitäten zur Überwachung (**Monitor tug activities**/**Monitor own ship information**) und Kommandierung (**Give tug orders**/**Perform precision manoeuvring**) unterteilen (siehe Abbildung 5.8 (Level 2)) [HFM06, S. 403]. In Abbildung 5.9 Level 3 bzw. 4 werden die für das Fallbeispiel betrachteten atomaren Aktivitäten zum Überwachen bzw. Kommandieren erforderlicher Informationen darstellt, wobei insbesondere die

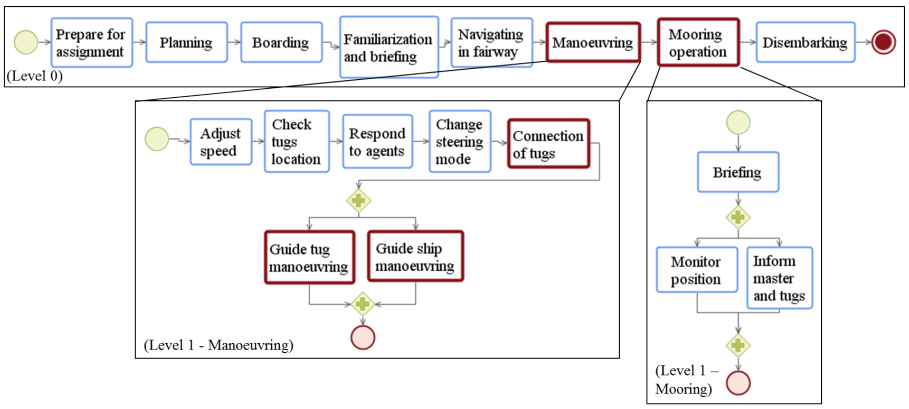

Abbildung 5.7: Oberste (Level 0) und erste Sub-Ebenen (Level 1) des Lotsenprozesses

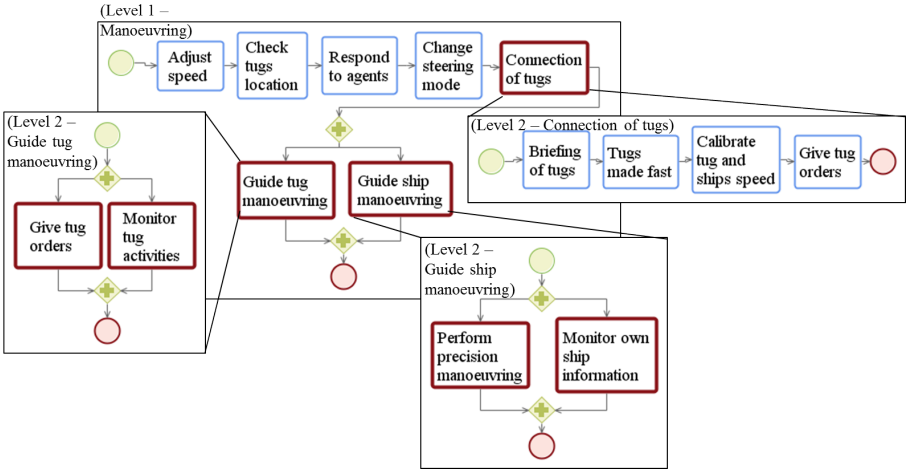

Abbildung 5.8: Erste (Level 1) und zweite Sub-Ebenen (Level 2) des Lotsenprozesses

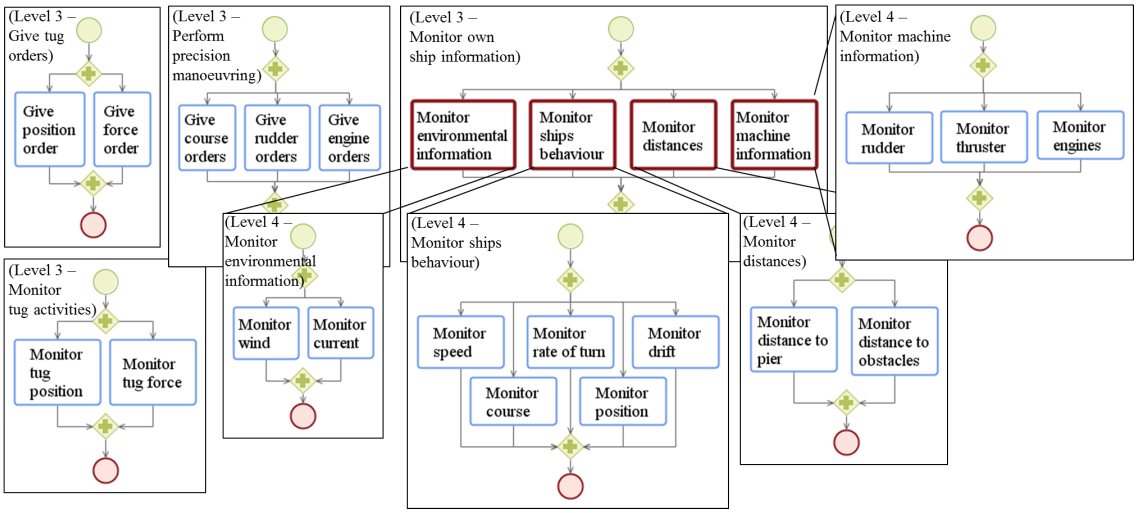

Abbildung 5.9: Dritte (Level 3) und vierte Sub-Ebenen (Level 4) des Lotsenprozesses

Überwachung der Informationen des Eigenschiffs (Level 3 - Monitor own ship information) eine Vielzahl an Informationen umfasst. Die Überwachung dieser Informationen umfasst Aktivitäten, wie in Abbildung 5.9 (Level 4) dargestellt, wofür u.a. auf der Schiffsbrücke befindliche Displays, Portable Pilot Units (PPUs) sowie der Blick aus der Schiffsbrücke erforderlich sind.

Gefährdungsidentifikation

Nachdem die Modellierung der Abläufe in der Systemdefinition abgeschlossen ist, folgt der Schritt zur Gefährdungsidentifikation mit der Modellierung von Gefährdungen und Ursachen sowie darüber hinaus der Festlegung von Betriebssituationen, Schadensfolgen, risikomindernde Maßnahmen und entsprechende Kenngrößen hinsichtlich der Häufigkeit und Schadensschwere. Für dieses Vorgehen können, wie in Kapitel 3.3.2 beschrieben, verschiedene Informationsquellen genutzt werden. Aus der Literatur als Informationsquelle sind dafür bereits Gefährdungen dieses Fallbeispiels bekannt, wie beispielsweise Grundberührungen, Kollisionen und Zusammenstöße mit statischen Objekten wie Bojen etc. [AS06], [TC00], [HFM06] oder Personenschäden durch Sturz beim Übersteigen [Ham14], reißende Seile beim Festmachen oder Ablegen. Aufgrund der Arbeiten im vorangegangenen Fallbeispiel des Personentransfers können zusätzlich durch die Wissensbasis als weitere Informationsquelle die dort hinterlegten Informationen inklusive der Gefährdungen, Ursachen etc., wie in Abbildung 5.10 dargestellt, bereitgestellt werden. Gefährdungen und daraus möglicherweise resultierende Unfälle werden überwiegend vom Faktor Mensch verursacht [BM05], [HFM06], [GHS02]. Nachfolgend werden aufgrund der erheblichen Relevanz dieses Faktors in der Praxis sowie für die zu beantwortende Fragestellung dieses Fallbeispiels, Ursachen dieses Faktors verstärkt betrachtet. Exemplarisch werden dafür anschließend die folgenden Gefährdungen im Vorgehen behandelt:

- Sturz
- Kollision

Die Gefährdung Sturz hat zwar kaum Einfluss auf die übergeordnete Fragestellung, stellt wie zuvor erläutert jedoch eine realistische Gefährdung im Fallbeispiel dar. Zusätzlich wurde diese Gefährdung bereits im vorangegangenen Fallbeispiel betrachtet, sodass hier die Möglichkeit der Wiederverwendung besteht und diese Gefährdung somit zur Veranschaulichung dieses Vorgehens im Rahmen der Evaluation des Ansatzes genutzt wird. Als zur Beantwortung der Fragestellung dient somit die Gefährdung Kollision, die in der Praxis eine relevante Gefährdung im Fallbeispiel darstellt und eng mit zugrundeliegenden Hilfsmitteln zur Visualisierung entsprechend der Fragestellung zusammenhängt.

Sturz Für die Gefährdung Sturz wird, wie in Abbildung 5.10 dargestellt, durch die prototypische Umsetzung mit Hilfe der Wissensbasis angeboten, die im vorangegangenen Fallbeispiel eingepflegten Informationen wiederzuverwenden. Bei der Gefährdungsidentifikation kann, wie in Kapitel 4 beschrieben, die Wissensbasis automatisch sowie auch manuell durchsucht und relevante Gefährdungen, wie beispielsweise Sturz nach Abbildung 5.10 (a), selektiert werden. Die Gefährdung Sturz wird als einzige aus den Vorschlägen für dieses Fallbeispiel aus der Wissensbasis wie in Kapitel 4 beschrieben selektiert, sodass Detai-

linformationen wie mögliche Ursachen und deren Kombination angezeigt und übernommen werden (siehe Abbildung 5.10 (b) und (c)). Eine `OperationalSituation` wird nach Übernahme der Gefährdung erneut festgelegt, da Gefährdungen wie Stürze mit teilweise tödlichem Ausgang in diesem Fallbeispiel überwiegend beim Übersteigen vom Lotsenboot auf das zu lotsende Schiff bekannt sind [Ham14]. Eine entsprechende Betriebssituation findet somit auf See, vor Einfahrt in die Hafengewässer statt. Als zusätzliche Orientierungshilfe zur weiteren Betrachtung dieser Gefährdung wird außerdem der Werteverlauf der zuletzt genutzten Wertestufen der Schadensschwere dieser Gefährdung innerhalb vergangener Anwendungsfälle dargestellt (siehe Abbildung 5.10 (b)). Da mit dem Fallbeispiel Personentransfer eine initiale Anwendung demonstriert und somit die Wissensbasis als leer angenommen wurde, enthält die Wissensbasis und somit auch der Werteverlauf der Gefährdung nur einen einzigen historischen Wert der Schadensschwere, der als `KBParameter` in der Wissensbasis vorliegt. Bei Übernahme der selektierten Gefährdung werden die in Abbildung 5.10 (c) in der bestehenden Strukturierung enthaltenen `Causes` sowie die Strukturierung selbst ebenfalls übernommen Die `Causes` werden dabei zur Erfüllung der Relation Γ : *contains* entsprechenden Elementen im Prozessmodell wie dem Lotsen als Akteur sowie dessen Tätigkeit zum Übersteigen (**Task: Boarding**) zugeordnet, wobei diese hinsichtlich

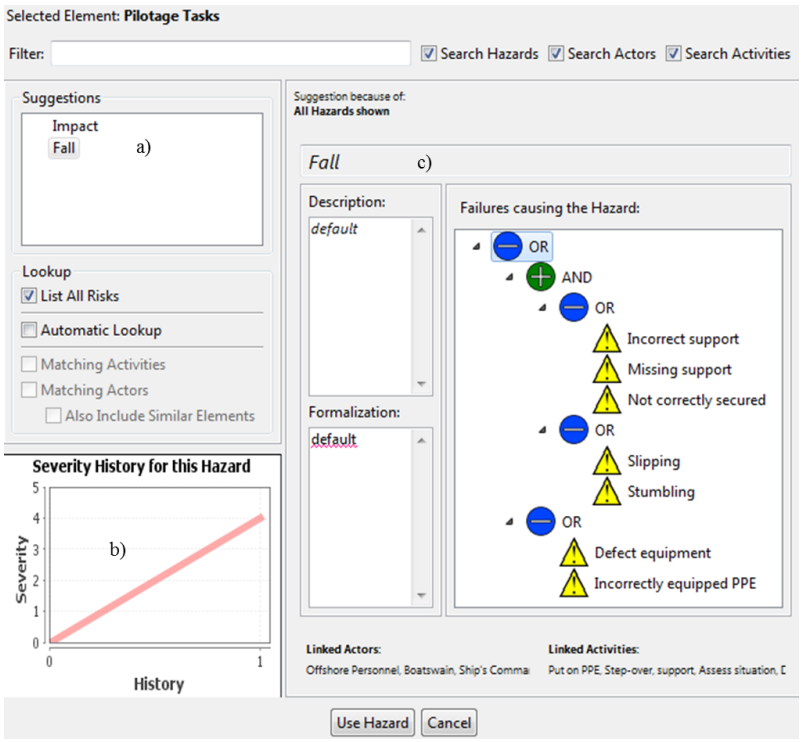

Abbildung 5.10: Bildschirmauszug der durch die prototypische Implementierung angebotenen Wiederverwendung der Gefährdung Sturz aus der Wissensbasis

ihrer Attribute erneut konfiguriert werden können. Hinsichtlich des Attributes $p_{frequency}$ dienen dabei die als `KBParameter` in der Wissensbasis hinterlegten Attributwerte vergangener Verwendungen des `Cause` als Orientierungshilfe, ähnlich wie in Abbildung 5.10 (b) dargestellt. Da durch die Wissensbasis nicht nur die Ursachen, sondern gleichzeitig deren Kombination bereitgestellt und genutzt werden können, ist für die Gefährdung Sturz keine erneute Strukturierung im nachfolgenden Schritt der Risikoanalyse erforderlich, jedoch mit dem Ansatz möglich.

Kollision Aufgrund der erhöhten Schwierigkeit durch die Nähe zum Land, andere Fahrzeuge und Brücken, Stege etc. finden somit Berührungen mit dynamischen oder statischen Objekten, die als Gefährdung Kollision beschrieben werden, vermehrt bei Manövern im Hafenbereich statt [Fri08, S. 2], sodass dies als `OperationalSituation` im Rahmen des Vorgehens abgebildet wird. Da diese Situation ebenfalls den Einsatz von Schlepperfahrzeugen und Lotsen erfordert, stellt diese Gefährdung einen wesentlichen Beitrag zur Beantwortung der zuvor genannten Fragestellung dar. Die Betrachtung dieser Gefährdung wird somit, wie im manuellen Vorgehen zur Gefährdungsidentifikation in Kapitel 3.3.2 beschrieben, umgesetzt, sodass die dafür eingepflegten und in Zusammenhang gebrachten Informationen zusammenfassend in Abbildung 6.2 im Anhang dargestellt werden. Da im Hinblick auf die mit dem Lösungsansatz zu beantwortende Fragestellung die notwendigen Informationen im Rahmen des Lotsenprozesses betrachtet werden müssen, wird für die Ermittlung von Ursachen das in Kapitel 3.3.2 beschriebene systematische Vorgehen genutzt, bei dem das Prozessmodell als Grundlage für eine systematische Ermittlung dient. Dabei werden die Aktivitäten des Lotsenprozesses sukzessive hinsichtlich möglicher Ursachen überprüft. Anhaltspunkte für mögliche Ursachen liefern dabei u.a. die Untersuchungen von Grech [GHS02], wobei die Untersuchung einer Vielzahl an Unfallberichten ergeben hat, dass sich in diesem Kontext eine Vielzahl der verursachenden Faktoren auf menschliche Fehler bei der Wahrnehmung und Interpretation von Informationen zurückführen lassen. Daraus folgernd können analog zum beschriebenen Vorgehen innerhalb von Tätigkeiten zur Überwachung (Monitoring) von Informationen wiederkehrende Ursachen als Fehleinschätzung (engl. Misjudgement) und Übersehen (engl. Overlooking) dieser Information identifiziert und eingepflegt werden. Für jeden `Task` im Prozessmodell (in Abbildung 5.9 Level 4 und Level 3 - Monitor tug activities) mit p_{name} = "*Monitor x*" erfolgt somit eine Zuordnung per Γ : *contains* der beiden identifizierten `Causes`. Diese werden als `Cause` mit p_{name} = "*Misjudgement of x*" und p_{name} = "*Overlooked x*" beschrieben, wobei x der jeweils in der Tätigkeit zu überwachenden Information wie beispielsweise Rate of Turn (Abbildung 5.9 Level 4 - Monitor ships behaviour) entspricht. Darüber hinaus können Tätigkeiten zur Kommunikation auf der Schiffsbrücke und mit den Schleppern weitere Ursachen enthalten, sodass für Tätigkeiten zum Geben von Kommandos mit p_{name} = "*Give y orders*") entsprechend weitere `Causes` modelliert werden müssen [BM05],

[GHS02]. Diese werden als `Causes` mit $p_{name} =$ "*Inappropriate y order*" modelliert und per Γ : *contains* mit der zugrundeliegenden Tätigkeit zum Geben von Kommandos in Zusammenhang gebracht, wobei y die jeweils zu kommandierende Information darstellt, wie beispielsweise ein neuer Schiffskurs (Abbildung 5.9 Level 3 - Perform precision manoeuvring). Eine tabellarische Zusammenfassung dieser Zuordnungen wird in Abbildung 6.2 im Anhang dokumentiert.

Darüber hinaus wurden im Rahmen einer Befragung maritimer Experten mit Erfahrung im Bereich des Lotsenwesens sowie Hafenlotsen selbst, durch deren Einschätzungen Kenngrößen der $p_{frequency}$ für sämtliche `Causes` ermittelt sowie gleichermaßen die ermittelten `Causes` validiert. Dabei wurde zunächst für jeden `Cause` der Wert $p_{frequency}$ unter Betrachtung des aktuellen Stands der Technik ermittelt und dokumentiert. Anschließend wurde der Ansatz von Ostendorp [MCO15] mit alternativen Visualisierungsentwürfen der Informationen vorgestellt, sodass daraufhin die $p_{frequency}$ erneut bewertet wurde. Die vorgenommenen Bewertungen im Hinblick auf den Stand der Technik wurden jeweils den `Causes` als $p_{frequency}$ zugeführt, wohingegen die ermittelten Unterschiede der Bewertungen hinsichtlich Verbesserung oder Verschlechterung durch Aspekte des neuen Ansatzes als risikomindernde Maßnahmen (`CounterMeasures`) mit entsprechendem $p_{frequencyFactor}$ modelliert wurden. Risikomindernde Maßnahmen die durch den neuen Ansatz bereitgestellt wurden, sind u.a. die numerische Visualisierung der Kräftewirkung der Schlepper, Visualisierung gegebener Kommandos und deren Status der Umsetzung sowie Nutzung einer Brille als Darstellungsmedium anstatt der Nutzung eines Tablets wie im Stand der Technik mit PPUs. Beispielsweise wurde somit im Stand der Technik der `Cause` mit $p_{name} =$ "*Misjudgement of tug forces*" im Schnitt mit der höchst möglichen $p_{frequency}$ bewertet, da bisher dafür keine unterstützende Visualisierung existiert. Hingegen hat die Bewertung ergeben, dass mit Hilfe der durch den neuen Ansatz eingebrachten `CounterMeasure` zur zusätzlichen Visualisierung der numerischen Schlepperkräfte in Tonnen, eine Reduktion der $p_{frequency}$ des `Causes` um drei Stufen erwartet wird, was als $p_{frequencyFactor} = 3$ der `CounterMeasure` modelliert wurde.

Risikoanalyse

Im den vorangegangenen Schritten wurden zunächst die zugrundeliegenden Abläufe und Tätigkeiten des Fallbeispiels in Form eines Prozessmodells in der Systemdefinition abgebildet. Daraufhin wurden weitere Informationen im Rahmen der Gefährdungsidentifikation zum einen mit Hilfe der Wissensbasis, zum anderen manuell eingepflegt, um die Fragestellung hinsichtlich der Risikosituation und Visualisierungen bei der Durchführung des Fallbeispiels zu adressieren. Damit in diesem Abschnitt auf Basis dieser Informationen eine Risikoanalyse stattfinden kann, werden diese Informationen, wie in Kapitel 3.3.3 beschrieben, genutzt. Dabei folgen Schritte zur weiteren Strukturierung, Konstruktion von Fehlerbäumen, Auswertung der Bäume durch den Schritt der Berechnung, sodass abschlie-

ßend vergleichende Ergebnisse für den Stand der Technik und den neuen Ansatz zur Verfügung stehen. Diese Schritte werden in den nachfolgenden Unterabschnitten im Rahmen des Fallbeispiels erläutert.

Strukturierung Im Gegensatz zu den für die Gefährdung Sturz übernommenen Informationen, für die durch die Wiederverwendung keine erneute Strukturierung erforderlich ist, muss die im vorangegangenen Schritt eingepflegte Gefährdung Kollision und damit zusammenhängende Ursachen zu Beginn der Risikoanalyse strukturiert werden. Dafür wird erneut die Unterstützung durch die implementierten Algorithmen genutzt und aufgrund der darin enthaltenen logischen und hierarchischen Strukturierung die Ergebnisse des Structure Guessed-Algorithmus für das Vorgehen der Strukturierung, wie in Kapitel 3.3.3 beschrieben, verwendet. Die dabei jeweils im Prozess genutzten `Gateways` zur Modellierung paralleler Abläufe, wie beispielsweise zur Überwachung und Kommandierung der Schlepper wie in Abbildung 5.8 (Level 2 - Guide tug manoeuvring) dargestellt, werden in der Strukturierung als `LogicOperator` verundet, wie in Abbildung 5.11 (a) dargestellt. Hingegen die hierarchischen Zusammenhänge durch die Nutzung von Sub-Prozessen sowie die Modellierung sequentieller Abläufe werden mit einem `LogicOperator` verodert abgebildet. Im Rahmen der manuellen Anpassung, wie im Vorgehen zur Strukturierung in Kapitel 3.3.3 beschrieben, wurde die aus dem Algorithmus resultierende Struktur angepasst, sodass die logischen Zusammenhänge überprüft und korrigiert wurden. So wurde beispielsweise die aus den in Abbildung 5.9 (Level 3 - Monitor tug activities) dargestellten Abläufen durch den verwendeten Algorithmus eine Verundung als resultierender logischer Zusammenhang

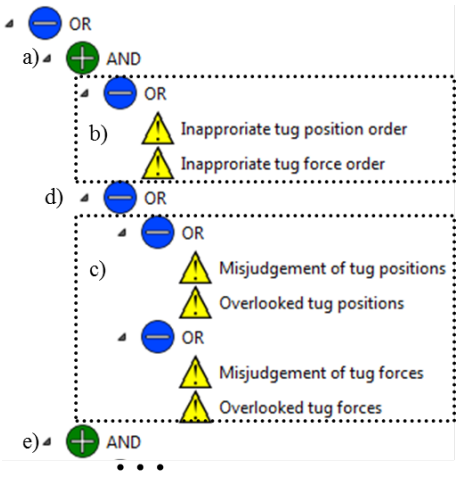

Abbildung 5.11: Auszug der aus dem Vorgehen zur Strukturierung resultierenden Struktur der mit Abläufen der Schleppermanövrierung zusammenhängenden Ursachen

vorgeschlagen, wohingegen der logische Zusammenhang einer Veroderung realistischer erscheint. Die nach diesem Vorgehen resultierenden Zusammenhänge sind exemplarisch in Abbildung 5.11 (b) und (d) dargestellt. Aus den `Causes` einzelner `Tasks` resultierende Strukturen sind wie in Abbildung 5.11 (c) dargestellt aus der Strukturierung des Algorithmus übernommen worden. Der Übersichtlichkeit halber stellt Abbildung 5.11 nur einen die Abläufe der Schleppermanövrierung betreffenden Auszug der resultierenden Strukturierung dar. Die aus dem Vorgehen resultierende Gesamtstrukturierung, die sich an Abbildung 5.11 (e) anschließt und die Strukturierung in Bezug zur Manövrierung des Eigenschiffs darstellt, wird in Abbildung 6.3 im Anhang dokumentiert.

Konstruktion Nachdem wie zuvor erläutert die Strukturierung unterstützt durch die genutzten Algorithmen vorgenommen worden ist, wird diese im Schritt der Konstruktion in eine analysierbare Struktur eines Fehlerbaumes überführt. Dies wird sequentiell für alle im Prozessmodell spezifizierten gefährlichen Ereignisse bzw. darin enthaltenen Gefährdungen vorgenommen, sodass je gefährlichem Ereignis ein Fehlerbaum erstellt wird. Für dieses exemplarische Fallbeispiel ergibt sich somit je ein Fehlerbaum für Kollision und Sturz.

Die Gefährdung Sturz wurde dabei bereits im vorangegangenen Fallbeispiel erläutert und entsprechend im Vorgehen des Ansatzes behandelt. Dabei wurde die Gefährdung mit dafür vorgenommener Strukturierung der möglichen Ursachen zum Abschluss des Vorgehens in der entwickelten Wissensbasis gespeichert. Diese Informationen wurden in der Gefährdungsidentifikation und Strukturierung des Fallbeispiels Lotsenwesen erneut genutzt und somit mit Hilfe der Wissensbasis wiederverwendet. Für den Schritt zur Konstruktion der Fehlerbäume ergibt sich somit hinsichtlich der Gefährdung Sturz dieselbe Ausgangssituation wie im vorangegangenen Fallbeispiel erläutert, sodass die vorliegende Strukturierung und daraus resultierende Fehlerbaumstruktur bereits in Abbildung 5.5 (rechts) dargestellt wurde. Das Vorgehen und die Ergebnisse des Schrittes zur Konstruktion werden demnach in diesem Abschnitt nicht erneut aufgeführt.

Hingegen wurde die Gefährdung Kollision im Fallbeispiel Lotsenwesen neu eingebracht, sodass diese fokussiert im Hinblick auf die Konstruktion betrachtet wird. Aus Sicht des Nutzers ist für die Konstruktion der Fehlerbäume kein zusätzlicher Aufwand notwendig, da dies in der prototypischen Implementierung, wie in Kapitel 4 beschrieben, automatisch vorgenommen wird. Die betrachtete Gefährdung Kollision dient dabei zur Erstellung des Top Ereignisses (`TopEvent`) des Fehlerbaumes. Die darunterliegende Fehlerbaumstruktur ergibt sich aus der zuvor erläuterten Strukturierung, wobei entsprechende Operatoren der Strukturierung wie Und bzw. Oder in die jeweiligen `FaultTreeGates` des Fehlerbaumes sowie die eingepflegten Ursachen in `BasicEvents` überführt werden. `IntermediateEvents` sind für eine valide Fehlerbaumstruktur zusätzlich notwendig und werden daher mit jedem `FaultTreeGate` erstellt, spielen jedoch im Hinblick auf die eigentliche Analyse eine untergeordnete Rolle [Stä11, S. 40]. Benennungen der erstellten `IntermediateEvents` leiten sich

aus den Attributen p_{name} der `LogicOperators` ab, welche wiederum aus den entsprechenden Attributen des jeweiligen `Gateways` oder anderen Prozesselementen wie `SubProcess` abgeleitet werden.

Der aus diesem Vorgehen resultierende Gesamtfehlerbaum wird in Abbildung 6.4 im Anhang gezeigt, sodass Abbildung 5.12 hingegen einen Auszug davon darstellt, der sich aus dem zuvor erläuterten Auszug der Strukturierung nach Abbildung 5.11 des vorangegangenen Abschnitts ergibt. Darin enthalten sind die zugeordneten Attribute $p_{frequency}$ und $p_{mitigatedFrequency}$ der `BasicEvents` die wie in Kapitel 3.3.3 bzw. Algorithmus 2 beschrieben ermittelt wurden.

Für Fehler bei der Kommandierung von Schlepperposition und Kraft wurde somit Anhand der zuvor erläuterten Befragung Werte im Hinblick auf den derzeitigen Stand der Technik von $p_{frequency} = 4$ bzw. 5 ermittelt, sodass durch die Experten ein verhältnismäßig häufiges Auftreten dieser Ereignisse vermerkt wurde. Im Hinblick auf den Ansatz von Ostendorp erfolgt dort eine zusätzliche Visualisierung der gegebenen Kommandos und deren Status der Umsetzung durch den Schlepper, die auf der Brille dargestellt und somit gleichzeitig mit Blick aus dem Fenster eingesehen werden können. Diese als `CounterMeasure` modellierten Maßnahmen wurden im Rahmen der Befragung hinsichtlich ihres Einflusses mit $p_{frequencyFactor} = 3$ bzw. 4 bewertet, was aus Sicht der Experten zu einer deutlichen

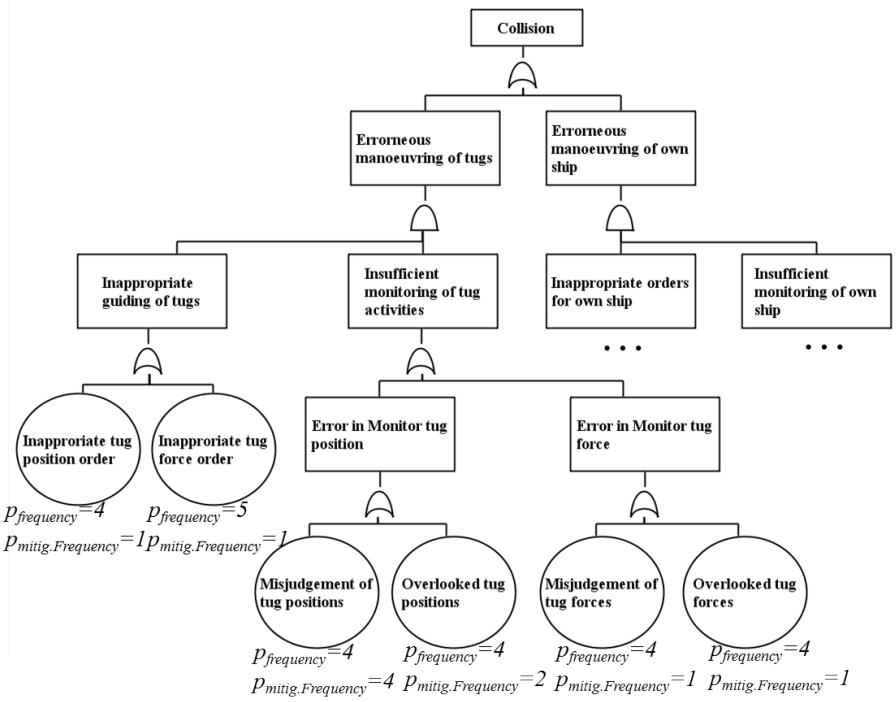

Abbildung 5.12: Auszug des resultierenden Fehlerbaums der Gefährdung Kollision

Verringerung der Häufigkeit der zugrundeliegenden Ursachen als $p_{mitigatedFrequency}$ führt. Analog dazu ergeben sich die weiteren Werte der $p_{frequency}$ aus der Einschätzung der Experten für den aktuellen Stand der Technik sowie der Einfluss mit Verbesserung oder Verschlechterung durch den neuen Ansatz als $p_{mitigatedFrequency}$ bzw. $p_{frequencyFactor}$ der `CounterMeasures`. Ursachen hinsichtlich des Übersehens von Informationen wurden dabei überwiegend aufgrund der Nutzung der Brille als Darstellungsmedium besser bewertet, da der Blick mit dem Ansatz nicht mehr zur Überwachung verschiedener Monitore abgelenkt werden muss. Eine weitere positive Bewertung ergibt sich für die Ursache der Fehleinschätzung von Schlepperkräften, die im derzeitigen Stand der Technik nur indirekt durch Wellenschlag, Rauch- und Geräuschentwicklung des Schleppers überwacht und eingeschätzt werden können. Mit dem neuen Ansatz hingegen erfolgt erstmals eine direkte numerische Darstellung der Kräftewirkung, was in der Differenz der $p_{frequency}$ und $p_{mitigatedFrequency}$ dieser Ursache ersichtlich wird.

Berechnung Nachdem die Konstruktion eines Fehlerbaumes abgeschlossen ist, wird im Schritt der Berechnung die eigentliche Analyse durchgeführt, sodass die Häufigkeitsstufe bzw. Wahrscheinlichkeit des `TopEvents` bestimmt werden kann. Das `TopEvent` entspricht in diesem Fallbeispiel der betrachteten Gefährdung der Kollision. Auf Basis der `BasicEvents` wird entsprechend der bekannten Berechnungsvorschriften (siehe Kapitel 3.3.3) diese Berechnung sukzessive vorgenommen. Für diesen Schritt ist keine weitere Interaktion mit dem Nutzer notwendig, sodass die Berechnung automatisiert und direkt im Anschluss an die Konstruktion des Fehlerbaumes erfolgt. Das bedeutet, dass zum Zeitpunkt der graphischen Darstellung des resultierenden Fehlerbaumes, wie in Abbildung 4.7 dargestellt, die Berechnung bereits vorgenommen wurde. Somit können die Ergebnisse der Berechnung in diesem Fehlerbaum bereits innerhalb der Fehlerbaumeditoranwendung, wie in der prototypischen Umsetzung beschrieben, eingesehen werden.

Für das `TopEvent` ergibt sich dabei ein Wert der $p_{probability}$ in der Größenordnung von $p_{frequency} = 4$ bei der Betrachtung des bisherigen Vorgehens im Lotsenwesen. Hingegen führt die Berechnung anhand der durch den neuen Ansatz ermittelten $p_{mitigatedFrequency}$ zu einem $p_{probability}$ Wert des `TopEvents` in der Größenordnung von $p_{frequency} = 1$, sodass sich auf Grundlage der Einschätzung der Experten die Häufigkeit von Kollisionen im Hinblick auf die zugrundeliegenden Ursachen durch Nutzung des neuen Ansatzes reduziert. Darüber hinaus können in den `IntermediateEvents` weitere Zwischenergebnisse eingesehen werden, wie beispielsweise die Reduktion der Häufigkeit zur fehlerhaften Manövrierung von Schleppern von $p_{frequency} = 4$ auf $p_{mitigatedFrequency} = 1$.

Dokumentation Abschließend werden die Ergebnisse sowie die verknüpften Informationen der zugrundeliegenden Planung zusammenfassend dokumentiert. Dafür wird die Funktionalität der prototypischen Umsetzung genutzt, um damit innerhalb der softwareseitigen

Unterstützung ein Word Dokument mit Dokumentation des Fallbeispiels zu erstellen. In diesem werden die eingebrachten Informationen der Planung und Analyse aufgeführt und entsprechend aufbereitet dargestellt. Diese beginnt dabei mit einer Tätigkeitsbeschreibung der Akteure, in welcher tabellarisch die Tätigkeiten sowie die möglichen Ursachen aufgeführt werden. Im Anschluss an die Beschreibung jedes Akteurs folgt eine Zusammenfassung seiner spezifischen Gefährdungen, Ursachen etc. Nachdem in der Dokumentation somit alle Akteure, deren Tätigkeiten und spezifische Gefährdungen, Ursachen etc. aufgelistet wurden, erfolgt eine für die gesamte geplante Operation übergreifende Auflistung der in dem Prozess definierten Gefährdungen mit Betriebssituation sowie bekannten Ursachen, welche für das Fallbeispiel Lotsenwesen und die darin enthaltene Gefährdung Kollision in Abbildung 6.5 im Anhang dargestellt wird. Dabei werden die Analyseergebnisse zusammenfassend dargestellt sowie daraufhin sämtliche Folgen und Ursachen sowohl mit als auch ohne Berücksichtigung risikomindernder Maßnahmen aufgeführt. Die Form der Dokumentation ist damit analog zu der in Abbildung 5.6 dargestellten und wird automatisch mit Hilfe der prototypischen Umsetzung erzeugt, weshalb diese im Anhang eingesehen und hier nicht erneut erläutert wird.

Risikobewertung

Im Schritt der Risikobewertung erfolgt eine manuelle Überprüfung der Ergebnisse und somit der geplanten maritimen Operation. Um diesen Schritt zu unterstützen wurde mit dem entwickelten Ansatz zum Abschluss der Risikoanalyse eine zusammenfassende Dokumentation erzeugt. Das betrachtete exemplarische Fallbeispiel hat zwar keinen Anspruch auf Vollständigkeit, jedoch konnte im vorangegangenen Fallbeispiel mit Hilfe maritimer Sicherheitsexperten gezeigt werden, dass der Ansatz für ein solches Vorhaben geeignet erscheint. Weitere Ausführungen dazu, in denen die praktische Eignung des Ansatzes mit Hilfe maritimer Experten evaluiert wird folgt in Kapitel 5.4. Damit die in den vorangegangenen Schritten gesammelten Informationen für zukünftige Fallbeispiele wiederverwendet werden können, werden diese zum Abschluss in die Wissensbasis überführt. Dieser Schritt geschieht, nach manuellem Aufruf der Funktion, wie in der prototypischen Umsetzung beschrieben automatisch, sodass keine weitere Interaktion notwendig ist. Die Gefährdung Kollision kommt dabei als eine neue Gefährdung in der Wissensbasis hinzu, sodass hierfür das Vorgehen wie im vorangegangenen Fallbeispiel erläutert stattfindet. Die Gefährdung Sturz ist hingegen bereits in der Wissensbasis vorhanden und muss insofern nicht erneut hinzugefügt werden. Hingegen wird die bestehende Gefährdung erweitert, insofern zusätzliche Aspekte wie beispielsweise weitere Ursachen, Maßnahmen etc. hinzugekommen wären. Beispielsweise wurde die Gefährdung Sturz im Fallbeispiel für einen weiteren Akteur verwendet, sodass dieser Zusammenhang in der Wissensbasis der bestehenden Gefährdung hinzugefügt wird. Gleichermaßen verhält es sich, wären Ursachen anderen Aktivitäten bzw. zusätzliche Ursachen neuer Aktivitäten ergänzt worden. Als weiteres werden die Gefähr-

dung und die jeweiligen Ursachen um weitere Parameter hinsichtlich Schadensschwere und Häufigkeitsklasse erweitert, sodass sich daraus ein historischer Werteverlauf nachbilden lässt.

5.2.3 Zusammenfassung und Zielerfüllung

In diesem Abschnitt wurde der entwickelte eigene Ansatz mit Hilfe der dafür umgesetzten prototypischen Implementierung für das Fallbeispiel des Lotsenwesens angewendet. Dafür wurde zunächst der Prozess mit den spezifischen Abläufen der beteiligten Personen im Schritt der Systemdefinition erfasst und entsprechend modelliert. Anschließend wurden Kollision und Sturz als die wesentlichen Gefährdungen innerhalb dieses Anwendungsfalls identifiziert und mögliche Ursachen dafür ermittelt und eingepflegt. Dabei wurde die Gefährdung Sturz und dazugehörige Ursachen mit Hilfe der entwickelten Wissensbasis systematisch wiederverwendet und im Vorgehen berücksichtigt. Die im Rahmen der Systemdefinition und Gefährdungsidentifikation zusammengetragenen Informationen wurden dann im Schritt der Risikoanalyse entsprechend strukturiert, ausgewertet und dokumentiert, sodass diese zum Abschluss dem Schritt der Risikobewertung und damit einer weiteren Vervollständigung der Wissensbasis zugeführt werden konnten.

Zur Beantwortung der übergeordneten Fragestellung wurden mit Hilfe von Expertenbefragungen zunächst Kenngrößen hinsichtlich der Häufigkeit der betrachteten Ursachen im Hinblick auf den aktuellen Stand der Technik ermittelt. Ergänzend wurden im entwickelten Lösungsansatz risikomindernde Maßnahmen, die durch einen alternativen Ansatz zur unterstützenden Visualisierung hinzukommen, ergänzt und anhand der Bewertung durch die Experten berücksichtigt. Mit Hilfe der anschließenden Fehlerbaumanalyse wurden diese Kenngrößen verrechnet, sodass der Stand der Technik mit dem alternativen Ansatz gegenübergestellt werden und der Einfluss des Ansatzes ermittelt werden konnte. Die erstellte Dokumentation fasst diese Ergebnisse zusammen und zeigt dabei eine Verbesserung durch den alternativen Ansatz auf, sodass mit Hilfe des entwickelten Lösungsansatzes die zugrundeliegende Fragestellung beantwortet werden konnte.

Die Erfüllung der zu Beginn in Abschnitt 1.3 gesetzten Ziele wird im Folgenden aufgeführt und zusammengefasst:

- Ziel 1 - Formalisierung des Basiswissens: Innerhalb der zentralen Prozessmodellierung wurde eine Basis geschaffen erforderliches Wissen in Bezug auf die zugrundeliegenden Abläufe mit beteiligten Personen, deren Tätigkeiten und Zusammenhänge durch Nutzung der Prozessmodellierung zu formalisieren. Das Ziel wurde somit **erfüllt**.

- Ziel 2 - Prozessorientierte Risikobetrachtung: Als ein zentraler Bestandteil des Ansatzes wird eine Form der Prozessmodellierung verwendet, mit der Prozesse strukturiert abgebildet werden können. In diese Struktur konnten zusätzliche Informationen über mögliche Gefährdungen, Ursachen und darauf wirkende risikomindernde Maßnahmen

eingebracht und als Grundlage für eine darauf aufbauende Risikoanalyse genutzt werden. Das Ziel wurde somit **erfüllt**, da sich Änderungen der Prozesse unmittelbar in der Risikoanalyse widerspiegeln lassen bzw. die Ergebnisse der Risikoanalyse eine Überarbeitung der Prozesse nach sich ziehen kann.

- Ziel 3 - Wiederverwendbare Informationen: Im Rahmen dieses Fallbeispiels konnte die zugrundeliegende Wissensbasis verwendet werden, um relevante Gefährdungen und Ursachen eines zuvor gespeicherten Fallbeispiels erneut zu nutzen, wodurch der initiale Aufwand diese Informationen einzupflegen reduziert werden konnte. Weiterhin wurden über die reine Nutzung hinaus, bestehende Informationen innerhalb der Wissensbasis durch erneute Verwendung innerhalb des Vorgehens ergänzt. Das Ziel wurde somit **erfüllt**.

- Ziel 4 - Unterstützende formalisierte Risikoanalyse: Durch die Verwendung der etablierten Technik der Fehlerbaumanalyse konnte ein Verfahren zur formalisierten Risikoanalyse in den Ansatz integriert werden. Zusätzlich wurde in dem Ansatz sowohl eine Möglichkeit zur manuellen als auch automatisierten Strukturierung der für diese Analyse notwendigen Informationen entwickelt und verwendet. Die Erstellung und Analyse von Fehlerbäumen konnte somit automatisiert sowie vorbereitend als Orientierungshilfe mögliche Strukturierungsvorschläge erzeugt werden, wodurch das Ziel **erfüllt** wurde.

- Ziel 5 - Berücksichtigung risikomindernder Maßnahmen: Das übergeordnete Ziel eines solchen Planungsansatzes ist, wie im Fallbeispiel des Lotsenwesens, die möglichen Risiken zu reduzieren. Risikomindernde Maßnahmen wie sie in diesem Fallbeispiel durch alternative Visualisierungen eingebracht wurden, sind dafür das wesentliche Hilfsmittel. Diese konnten in dem vorgestellten Ansatz bei der Modellierung sowie darauf aufbauenden Analyse berücksichtigt werden, sodass deren Einfluss auf individuelle Ursachen sowie auch das Gesamtrisiko eingesehen werden kann. Das Ziel wurde somit **erfüllt**.

- Ziel 6 - Softwareseitige Unterstützung: Der vorgestellte Ansatz ist im Rahmen der prototypischen Umsetzung implementiert worden. Diese Implementierung ist für die Durchführung dieses Fallbeispiels konsequent genutzt worden, wodurch das Ziel **erfüllt** wurde.

Zusammenfassend lässt sich feststellen, dass die aufgestellten Zieldefinitionen mit dem entwickelten Lösungsansatz erfüllt werden konnten. In dem Vorgehen können einzelne Aspekte wie die Abläufe, Tätigkeiten, Gefährdungen und Ursachen gezielt fokussiert und systematisch eingepflegt werden. Die darauffolgende Strukturierung für die Risikoanalyse bietet daraufhin eine erste Orientierungshilfe wie diese Informationen verknüpft werden

können, was bereits in dieser frühen Planungsphase zu einer Überprüfung und ggf. Änderung des Konzepts führen kann. Zwar ist diese Strukturierung automatisiert möglich, jedoch sollte dabei stets der jeweilige Sicherheitsexperte die Möglichkeit haben dies zu hinterfragen und zu ändern. Für das Fallbeispiel des Lotsenwesens sind primär personen- bzw. tätigkeitsbezogene Ursachen aufgeführt und untersucht worden. Zusätzlich können in dem Vorgehen analog dazu beispielsweise technische Ursachen wie Maschinenausfälle etc. betrachtet werden. Für diese ist jedoch insbesondere für die automatisierte Strukturierung darauf zu achten, dass diese an geeigneten Positionen verknüpft werden. Denn im Gegensatz zu tätigkeitsbezogenen Ursachen können technische Ursachen möglicherweise auch außerhalb einer spezifischen Tätigkeit auftreten, wodurch diese ggf. manuell verknüpft werden müssen. So kann sich beispielsweise ein Fehler der Steuerung des eigenen Schiffes bereits allein als eine Ursache zur Kollision herausstellen ohne mit möglichen Wahrnehmungsschwierigkeiten anderer Tätigkeiten kombiniert werden zu müssen. Eine übergreifende korrekte und vollständige Erfassung und Strukturierung ist jedoch kaum möglich, sodass das Ergebnis wie auch die Strukturierung und Fehlerbäume stets vom Fokus, der Perspektive und von den jeweiligen Personen und Anwendungsfällen abhängt.

5.3 Vergleich mit bisherigem Vorgehen

Im Rahmen der in den vorangegangenen Abschnitten vorgenommenen Evaluation durch Fallbeispiele wurde eine qualitative Untersuchung des Ansatzes vorgenommen. In der qualitativen Evaluation wurde dabei eine systematische Bearbeitung der Fallbeispiele mit Hilfe des Ansatzes dargestellt, sodass das Zusammenwirken der einzelnen Aspekte im Rahmen des schrittweisen Vorgehens erläutert wurde. Um diese Ergebnisse zu ergänzen und die Evaluation somit zu vervollständigen, wird in diesem Abschnitt der Ansatz zusätzlich durch eine quantitative Erhebung mit der folgenden Zielvorstellung evaluiert:

- das bisherige Vorgehen mit dem neuen Ansatz quantitativ gegenüberzustellen
- den Ansatz durch Anwendung durch andere Personen zu evaluieren
- Tendenzen und Anhaltspunkte über die Benutzbarkeit und Erlernbarkeit des Ansatzes zu erhalten
- die Akzeptanz des Ansatzes durch Anwender zu überprüfen

Im Rahmen dieser Evaluation wurde daher auf Basis der vorgenommenen Implementierungsarbeiten eine Nutzerstudie durchgeführt. Dabei wurden den Probanden Aufgaben zur Lösung mit dem bisherigen Vorgehen nach Kapitel 2 als auch mit dem neuen Ansatz gestellt und im Anschluss ausgewertet, um so beide Ansätze quantitativ gegenüberstellen zu können. Die Probanden hatten dabei unterschiedliches Vorwissen und umfassten

einen Personenkreis von Informatik-Studenten, Fachinformatikern sowie Hochschulabsolventen mit und ohne Promotion. Insgesamt haben 23 Probanden unter jeweils vergleichbaren Arbeitsbedingungen an der Studie im geplanten Umfang von 75 Minuten je Proband teilgenommen. Das Vorgehen der Studie sowie die Rahmenbedingungen und Ergebnisse werden in den nachfolgenden Unterabschnitten näher erläutert. Des Weiteren ist anzumerken, dass innerhalb der Studie beide Ansätze ausschließlich in Betrachtung ihres manuellen Vorgehens untersucht wurden. Der Aspekt der Wiederverwendbarkeit wurde somit nicht mit untersucht, da diese Funktionalität im bisherigen Vorgehen nicht vorhanden ist. Somit haben die Probanden mit einem „ungelernten“ System gearbeitet, sodass eine mögliche Begünstigung der softwareseitigen Umsetzung durch unterstützte Wiederverwendung von Informationen im Rahmen der Studie nicht berücksichtigt wurde.

5.3.1 Vorgehen und Durchführung

Mit Hilfe der vorangegangenen Implementierung, die zur Überprüfung der Umsetzbarkeit des entwickelten Ansatzes dient, wurden im Rahmen einer Nutzerstudie Ergebnisse zur Bewertung und damit quantitativen Evaluation des Ansatzes erhoben. Die Studie wurde konzipiert, um einen Vergleich des bisherigen Ansatzes, wie in Kapitel 2.1 beschrieben, und des neu entwickelten Ansatzes zu ermöglichen. Dabei wurde die zuvor in Kapitel 4 beschriebene prototypische Umsetzung als Anwendung des neu entwickelten Ansatzes genutzt. Die an der Studie teilnehmenden Probanden wurden dabei zunächst in das Vorgehen der Studie eingeführt und anhand eines Beispielszenarios mit dem Vorgehen und den beiden zu nutzenden Ansätzen vertraut gemacht. Im darauffolgenden Studienablauf wurden den Probanden gleichwertige Aufgaben zur Lösung mit dem bisherigen als auch dem neuen Ansatz gestellt.

Aufgaben zur Lösung mit dem bisherigen Ansatz umfassten dabei typische Arbeiten zur Planung und Aufstellung von Sicherheitskonzepten wie in Kapitel 2.1 beschrieben:

- textuelle Beschreibung der Aktivitäten
- Identifikation und Bewertung von Risiken

Um vergleichbare Ergebnisse zu erhalten, umfassten die Aufgaben zur Lösung mit dem neuen Ansatz gleichwertige Arbeiten, welche jedoch entsprechend mit Hilfe des neuen Ansatzes zu lösen waren. Abschließend wurde von jedem der Probanden je ein Fragebogen ausgefüllt. In diesem wurden Fragen nach dem System Usability Scale (SUS) von John Brooke [Bro96] zur Überprüfung der Benutzbarkeit und dem Vergleich beider Ansätze, sowohl positiv als auch negativ formuliert, vorbereitet. Nach Einhaltung und Auswertung der nach dieser Methode erhobenen Daten kann eine Tendenz der zu vergleichenden Ansätze hinsichtlich deren Benutzbarkeit erzielt werden. Zusätzlich wurden in einer abschließenden Befragung Anmerkungen der Probanden aufgenommen und dokumentiert.

5.3.2 Rahmenbedingungen

Für die Durchführung der Studie wurden für jeden Probanden die gleichen Rahmenbedingungen hergestellt, sodass keine abweichenden Störeinflüsse die Studienergebnisse verfälschen konnten. Dafür wurden einheitliche Räumlichkeiten und technische Infrastruktur bereitgestellt und ein störungsfreies Arbeitsklima gewährleistet. Zur Gegenüberstellung beider Ansätze wurde eine einheitliche, mit beiden Ansätzen gleichermaßen zu lösende Aufgabenstellung vorbereitet. Notwendige Einführungen und Erklärungen wurden vorab ermöglicht und anhand von Beispielen verdeutlicht. Des Weiteren wurde kein Teilnehmer bevorzugt oder zusätzlich bei der Bearbeitung unterstützt. Für die Bearbeitung der Aufgaben wurden jeweils die selben Softwarewerkzeuge bereitgestellt und es gab keine Möglichkeiten für die Probanden ihre Lösungen hinsichtlich Korrektheit zu überprüfen, zu korrigieren oder untereinander zu vergleichen. Diese einheitliche Verfahrensweise ermöglicht es, in der Bewertung ausschließlich die beiden Ansätze hinsichtlich der gelösten Aufgaben miteinander zu vergleichen und andere Einflüsse auszuschließen.

5.3.3 Auswertung und Ergebnisse

In diesem Abschnitt werden die Resultate der nach dem zuvor beschriebenen Vorgehen durchgeführten Nutzerstudie ausgewertet. Dafür wurde die von den Probanden jeweils benötigte Zeit, gelöste Aufgaben sowie der Fragebogen nach dem System Usability Scale (SUS) für die Auswertung genutzt. In den anschließenden Unterabschnitten werden daher die Aspekte Bearbeitungszeit, Benutzbarkeit, Erlernbarkeit und Einschätzung der Probanden im Rahmen der Auswertung genauer erläutert.

Bearbeitungszeit

Um den erforderlichen Aufwand zum Lösen der gestellten Aufgaben mit Hilfe des bisherigen mit dem neuen Ansatz vergleichen zu können, wurden im Rahmen der Studie die Bearbeitungszeiten der jeweiligen Aufgaben ermittelt und dokumentiert. Zeiten für vorbereitende Maßnahmen, wie Erklärungen, Lesen der Aufgabenstellung etc., wurden dabei nicht mit einbezogen, sodass eine reine Bewertung der erforderlichen Zeit zur Bearbeitung der Aufgabe vorgenommen wurde. Die auf diese Weise ermittelte durchschnittliche Bearbeitungszeit über alle Probanden mit dem bisherigen (links) und dem neuen Ansatz (rechts) wird in Abbildung 5.13 dargestellt.

Insgesamt benötigten die Teilnehmer damit im Schnitt 48:02 Minuten, wovon 25:24 Minuten zur Bearbeitung mit dem bisherigen und 22:38 Minuten für die Bearbeitung mit dem neuen Ansatz benötigt wurden. Im Rahmen der Studie war somit durchschnittlich 02:46 Minuten und damit ca. 10% weniger Bearbeitungszeit zum Lösen der Aufgaben mit dem neuen Ansatz erforderlich. Im bisherigen Ansatz entfielen dabei 04:40 Minuten auf den Schritt zur Gefährdungsidentifikation und 10:35 Minuten auf die Risikoanalyse, womit

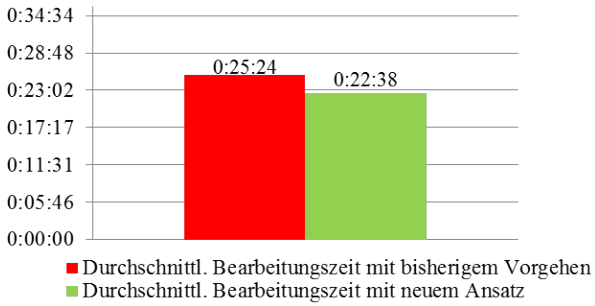

Abbildung 5.13: Gegenüberstellung der durchschnittlichen Gesamtbearbeitungszeiten mit dem bisherigem Vorgehen (links) und dem neuen Ansatz (rechts)

diese beiden Schritte mit 15:15 Minuten den überwiegenden Aufwand (ca. 60%) mit dem bisherigen Ansatz ausmachten. Im Gegensatz dazu entfielen für die Gefährdungsidentifikation und Risikoanalyse im neuen Ansatz nur ca. 25% der Gesamtzeit auf diese Arbeiten, sodass der überwiegende Aufwand bei der Systemdefinition anfiel. Dennoch hat die Gefährdungsidentifikation mit dem neuen Ansatz im Durchschnitt 05:07 Minuten und damit im Vergleich mit der gleichen Aufgabe, gelöst mit dem bisherigen Ansatz, rund 27 Sekunden bzw. ca. 9% länger beansprucht. Dies wurde auch von den Probanden wahrgenommen und kommuniziert, sodass im Gegensatz zur sukzessiven Auflistung im bisherigen Ansatz, im neuen Ansatz eine stärkere Interaktion mit der prototypischen Implementierung notwendig war, was entsprechend auch in der gemessenen Bearbeitungszeit sichtbar ist.

Trotz des teilweisen Mehraufwands mit dem neuen Ansatz, konnten insgesamt die gestellten Aufgaben tendenziell in kürzerer Zeit gelöst werden als mit dem bisherigen Vorgehen. Demnach kann geschlussfolgert werden, dass beide Ansätze im Hinblick auf die erforderliche Bearbeitungszeit bei initialer Anwendung zur Lösung einer Aufgabe vergleichbar aufwändig sind. Wohingegen zu erwarten ist, dass bei weiterer Anwendung des neuen Ansatzes und durch dadurch steigenden Mehrwert der Wissensbasis die erforderliche Bearbeitungszeit mit dem neuen Ansatz sinkt. Innerhalb dieser Untersuchung sollte jedoch ein neutraler Vergleich beider Ansätze stattfinden, sodass beide Ansätze hinsichtlich ihrer initialen Anwendung betrachtet wurden.

Benutzbarkeit

Zur Untersuchung der Benutzbarkeit des neuen Ansatzes wurde im Anschluss an die Bearbeitung der gestellten Aufgaben von den Probanden jeweils ein Fragebogen ausgefüllt. Dieser enthielt die nach dem System Usability Scale (SUS) nach John Brooke [Bro96] geforderten Aussagen, welche von den Probanden anhand ihrer zuvor gemachten Erfahrungen beim Lösen der Aufgaben, mit Abstufungen zwischen starkem Zuspruch (++) und starker

Ablehnung (- -) bewertet wurden.

Insgesamt wurden auf diese Weise 10 Fragen beantwortet, die in der Auswertung maximal 100 Punkte ergeben. Für diese Wertung wurde jeweils der vorgenommenen Zuordnung der Probanden hinsichtlich ihrer Zustimmung oder Ablehnung ein Wert von 0 bis 4 zugeteilt. Zusammengenommen ergab sich so für den neuen Ansatz, repräsentiert durch die vorgenommene prototypische Umsetzung, ein durchschnittlicher Wert von 68. Dieser für die prototypische Umsetzung ermittelte Wert wird nach Bangor [BKM09] im oberen Grenzbereich zur Akzeptanz, mit Potential zur Verbesserung, eingeordnet (siehe Abbildung 5.14). Diese Einordnung bestätigt den prototypischen Charakter der Umsetzung und zeigt zudem bereits die Tendenz zu einer akzeptabel benutzbaren Lösung auf. Mit diesem Ergebnis kann zusätzlich bestärkt werden, das die vorgenommene prototypische Umsetzung dem Nachweis der Machbarkeit und Umsetzbarkeit des entwickelten Ansatzes genügt.

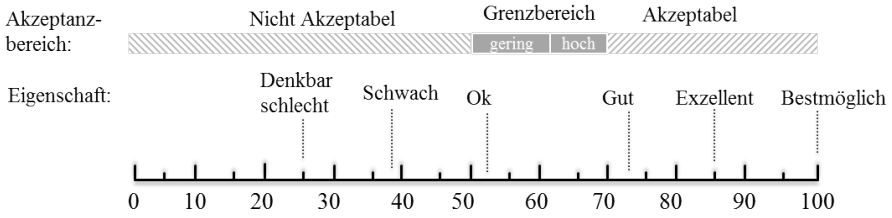

Abbildung 5.14: Skala zur Einordnung eines nach dem System Usability Score (SUS) ermittelten Wertes (eigene Darstellung in Anlehnung an [BKM09])

Erlernbarkeit

Im Rahmen der Durchführung mit Hilfe des SUS und den Fragebögen konnten einige der mit Zuspruch und Ablehnung bewerteten Aussagen hinsichtlich der Erlernbarkeit des neuen Ansatzes ausgewertet werden. Die eigenen Fähigkeiten der Person sowie das notwendige Vorwissen wurden dafür in die Auswertung mit einbezogen und durch die Probanden entsprechend eingeordnet. Daraus ergab sich im Durchschnitt über alle Probanden ein Wert von 61 Punkten (siehe Abbildung 5.15). Die Auswertung der Erlernbarkeit ergab außerdem, dass Probanden die vor der Studie angegeben haben kein Vorwissen zu haben, einen Erlernbarkeitswert von 58 erreicht haben. Hingegen kamen Probanden mit einem geringen Vorwissen auf 63 Punkte und Probanden mit mittlerem Vorwissen auf rund 75 Punkte. Dabei fällt auf, dass der Erlernbarkeitswert offenbar geringer ausfällt, je weniger Vorwissen von den Probanden in die Studie eingebracht wurde. Möglicherweise konnten ungelernte Probanden, die im Anschluss der Studie vorgenommenen Einschätzungen hinsichtlich Hilfestellungen und Vorwissen, genauer abschätzen da deren ersten Erfahrungen mit dem genutzten neuen Ansatz erst vollständig im Rahmen der Studie erworben wurden. Hingegen lagen die ersten Erfahrungen bei Probanden mit geringem und mittlerem Vorwissen wei-

ter zurück, sodass Einschätzungen ob Hilfestellungen oder wie viel Vorwissen notwendig war, nicht mehr so gut abgeschätzt werden konnte und somit möglicherweise eine optimistischere Schätzung erfolgt ist, als bei ungelernten Probanden deren erste Erfahrungen innerhalb der Studie gemacht wurden. Das Ergebnis ist nach der SUS Skala im mittleren Grenzbereich einzuordnen und bestätigt damit, dass der neue Ansatz Einarbeitungs- und Lernaufwand zur Verwendung erfordert.

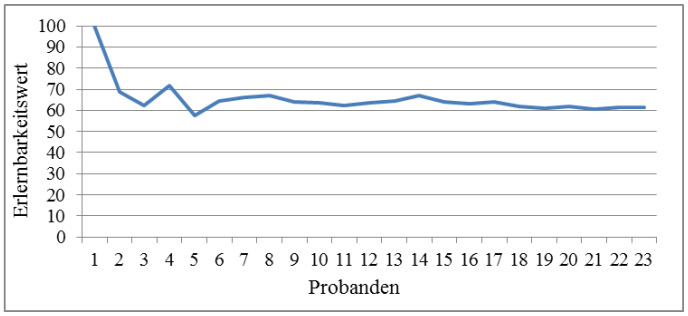

Abbildung 5.15: Verlauf der nach dem SUS ausgewerteten durchschnittlichen Erlernbarkeit über alle Probanden

Einschätzung der Probanden

Im Rahmen der abschließenden Bearbeitung des Fragebogens haben die Probanden jeweils 15 Aussagen hinsichtlich ihrer Zustimmung oder Ablehnung bewertet. Zehn dieser Aussagen bezogen sich auf die Auswertung der Benutzbarkeit und Erlernbarkeit nach dem SUS. Weitere fünf Aussagen wurden ergänzt, um eine vergleichende Bewertung der beiden verwendeten Ansätze durch die Probanden zu ermöglichen. Die dabei getroffenen Angaben der Probanden sind in Abbildung 5.16 dargestellt. Ersichtlich ist, dass die Probanden im Durchschnitt der Aussage „Ich fand den bisherigen Ansatz einfacher zu verstehen“ eher nicht zugestimmt haben, sodass ihnen der neue Ansatz offenbar leichter gefallen ist. Ein Grund dafür kann die Unterstützung des Ansatzes durch die prototypische Implementierung sein, wodurch die Nutzer sich durch die Software bei der Bearbeitung der Aufgaben besser unterstützt gefühlt haben könnten. Dies unterstreicht auch die Bewertung der Aussage „Ich fand die Gefährdungsidentifikation und Risikoanalyse im neuen Ansatz einfacher umzusetzen“, der die Probanden deutlich zugestimmt haben. Zusätzlich würden die Probanden offenbar den neuen Ansatz bevorzugen, da sie die Aussage „Ich würde den bisherigen Ansatz bevorzugen“ deutlich abgelehnt haben. Die Probanden empfanden weiterhin, dass der neue Ansatz, unterstützt durch die genutzte prototypische Umsetzung, mehr Interaktionsmöglichkeiten bietet im Vergleich zum bisherigen Ansatz. Außerdem empfanden die Probanden den neuen Ansatz als weniger zeitaufwändig als den bisherigen, was auch in der Auswertung der Bearbeitungszeiten messbar war.

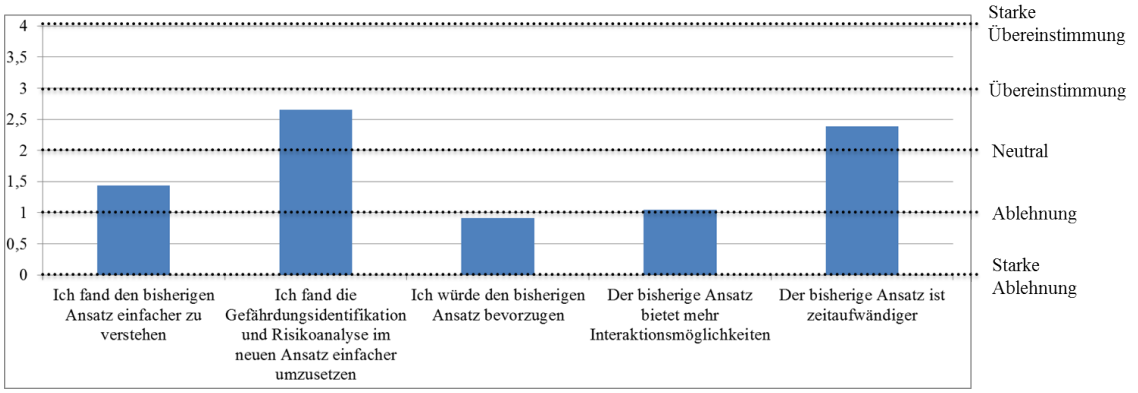

Abbildung 5.16: Durchschnittliche Bewertung der Probanden zum Vergleich der benutzten Ansätze

5.3.4 Zusammenfassung und Diskussion

Als erste Maßnahme zur quantitativen Evaluation des in dieser Ausarbeitung entwickelten Ansatzes wurde eine Nutzerstudie konzipiert und durchgeführt, um Daten für eine quantitative Gegenüberstellung des neuen Ansatzes mit dem bisherigen Vorgehen zu ermöglichen. Innerhalb dieser Studie haben 23 Probanden Aufgaben mit Hilfe beider Ansätze gelöst, wobei jeweils die Bearbeitungszeiten dokumentiert wurden. Zum Abschluss der Studie wurde von jedem der Probanden ein Fragebogen ausgefüllt, der nach dem System Usability Scale (SUS) von John Brooke [Bro96] zur Auswertung der Benutzbarkeit und Erlernbarkeit genutzt wurde. Darüber hinaus wurden vergleichende Aussagen der in der Studie angewendeten Ansätze aufgenommen und für eine Gegenüberstellung aus Sicht der Probanden vorgenommen.

Insgesamt wurde mit der Studie gezeigt, dass der zeitliche Aufwand beim manuellen Vorgehen beider Ansätze vergleichbar hoch ist. Jedoch wird erwartet, dass sich der Aufwand bei kontinuierlicher Anwendung des neuen Ansatzes, durch wachsende Erfahrung mit dem Ansatz sowie durch die steigende Möglichkeit zur Wiederverwendung bestehender Informationen der Wissensbasis, weiter reduziert. Hinsichtlich der ausgewerteten Benutzbarkeit und Erlernbarkeit des Ansatzes ist anzumerken, dass nur wenige Probanden Erfahrungen wie von maritimen Sicherheitsexperten in die Studie einbringen konnten. Die ermittelten Ergebnisse können daher nur als Tendenz zu verstehen sein, sodass im nachfolgenden Kapitel 5.4 ergänzend untersucht wird, inwiefern sich der Ansatz aus Sicht von maritimen Sicherheitsexperten eignet. Weiterhin könnte sich im Hinblick auf die vorgenommene Einschätzung der starke technische Hintergrund der Probanden möglicherweise positiv ausgewirkt haben, sodass die vorgenommene prototypische Umsetzung stärkeres Interesse geweckt haben könnte als die im bisherigen Ansatz genutzten Werkzeuge zur Text-

verarbeitung. Somit wäre eine begünstigende Bewertung durch Einsatz der prototypischen Umsetzung, und nicht des neuen Ansatzes an sich, denkbar. Die ermittelten Ergebnisse der Einschätzung der Probanden soll daher als weiterer Aspekt im nachfolgenden Abschnitt mit Hilfe von maritimen Sicherheitsexperten untersucht werden, ob diese die Einschätzung der Probanden teilen oder ob deren Einschätzungen abweichen.

5.4 Untersuchung der praktischen Eignung des Ansatzes

Nachdem in den vorangegangenen Abschnitten der vorgestellte Ansatz mit zwei Fallbeispielen sowie einer Nutzerstudie evaluiert wurde, folgt im diesem Abschnitt zur weiteren Bekräftigung der Ergebnisse eine Evaluation durch maritime Sicherheitsexperten. Dies soll die quantitative Evaluation des entwickelten Ansatzes erweitern sowie die bisherigen Ergebnisse aus Sicht von maritimen Sicherheitsexperten widerspiegeln und somit gleichermaßen die vorgenommenen Arbeiten weitergehend aus Sicht der Praxis untersuchen. Dafür wurden maritime Sicherheitsexperten mit mehrjähriger Erfahrung in der Planung und Analyse maritimer Operationen ausgewählt, der entwickelte Ansatz vorgestellt und von diesen bewertet und diskutiert. Die vorgenommene Bewertung durch die maritimen Sicherheitsexperten wurde anschließend einer Nutzwertanalyse zugeführt, in der das bisherige Vorgehen und der neue Ansatz erfasst und gegenüberstellend quantitativ bewertet wurde. Das Vorgehen im Rahmen dieser Untersuchung wird im nachfolgenden Unterabschnitt beschrieben, woraufhin anschließend auf die Durchführung sowie die Ergebnisse, sowohl der Nutzerstudie als auch der persönlichen Gespräche, eingegangen wird.

5.4.1 Vorgehen und Durchführung

Zur Untersuchung der praktischen Eignung (Praxistauglichkeit) wurden fünf maritime Sicherheitsexperten befragt, um die Perspektive aus Sicht der Praxis bei der Evaluation des neuen Ansatzes mit einzubeziehen. Um ein gemeinsames Verständnis gewährleisten zu können, wurde das wiederkehrende und somit für die Experten vertraute Fallbeispiel des

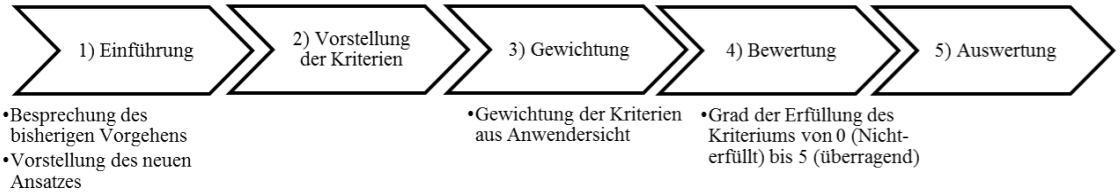

Abbildung 5.17: Schematisches Vorgehen zur Untersuchung der Praxistauglichkeit mit Hilfe maritimer Sicherheitsexperten

Personentransfers, wie in Kapitel 5.1 beschrieben, verwendet. Das Vorgehen zur Untersuchung der Praxistauglichkeit ist schematisch in Abbildung 5.17 visualisiert und wird in den nachfolgenden Unterabschnitten schrittweise erläutert.

1) Einführung Zur Einführung in das weitere Vorgehen wurde den maritimen Experten zunächst im persönlichen Gespräch der neue Ansatz auf Basis der prototypischen Umsetzung anhand des bekannten Fallbeispiels präsentiert und erläutert. Gleichermaßen wurde dabei das bisherige Vorgehen der Experten zum Vergleich erhoben, welches in Kapitel 2.1 beschrieben ist. Meinungen und Aussagen der Experten wurden ab dem Schritt zur Einführung über das gesamte Vorgehen hinweg fortlaufend dokumentiert, um im Nachgang zur Durchführung die Ergebnisse entsprechend zu belegen zu können.

2) Vorstellung der Kriterien Vorbereitend zum weiteren Vorgehen wurde der Begriff der Praxistauglichkeit in Kriterien, wie in Tabelle 5.1 dargestellt, unterteilt, um eine differenziertere Betrachtung der Fragestellung nach praktischer Eignung zu ermöglichen. Diese Kriterien setzen sich aus Qualitätsmerkmalen von Software, der Benutzbarkeit sowie Übertragbarkeit und aus der Praxis per Fragebögen und Vorgesprächen abgeleiteten Aspekten zusammen[1], um den Ansatz hinsichtlich dieser gezielt untersuchen und bewerten zu können. Diese Kriterien wurden den Experten vorgestellt und erläutert, sodass diese für die nachfolgenden Schritte von den Experten selbstständig bearbeitet werden konnten. Unterstützend stand den Experten dabei eine schriftliche Beschreibung und Aufstellung der Kriterien bereit.

Tabelle 5.1: Ermittelte Kriterien zur Untersuchung der Praxistauglichkeit

Aktualität	Manueller Aufwand	Benutzbarkeit
Schnittstellen	Darstellung	Sprache
Detailgenauigkeit	Transparenz	Eindeutigkeit
Übertragbarkeit	Flexibilität	Wiederverwendbarkeit

3) Gewichtung Nachfolgend zur Vorstellung der in Tabelle 5.1 dargestellten Kriterien, wurde eine Gewichtung der einzelnen Kriterien aus Anwendersicht vorgenommen. Die 12 Kriterien wurden dafür von den maritimen Sicherheitsexperten, jeweils nach deren Einschätzung in eine individuell gewichtete Rangfolge zur Unterscheidung unterschiedlich wichtiger Kriterien, sortiert.

4) Bewertung Anschließend wurden die Kriterien im Einzelnen in Bezug auf das bisherige Vorgehen und den neu vorgestellten Ansatz betrachtet. Dafür wurde für jedes Kriterium

[1] vgl. [Pet14]

je Ansatz eine Bewertung durchgeführt, bei der die maritimen Sicherheitsexperten bewertet haben, inwiefern das Kriterium durch den neuen und den bisherigen Ansatz erfüllt oder nicht-erfüllt wird. Ein nicht-erfülltes Kriterium für einen Ansatz wurde dabei mit einem Wert von 0 bewertet, ein überragend erfülltes Kriterium hingegen mit einem Wert von 5. Darüber hinaus gab es die Abstufungen ausreichend (1), befriedigend (2), gut (3), sehr gut (4).

5) Auswertung Nach Abschluss der Bewertung lagen somit Informationen über die Gewichtung der Kriterien sowie der von jedem der Experten bewertete Erfüllungsgrad des Kriteriums für jeden der beiden Ansätze vor. Zur weiteren Arbeit und Auswertung der Ergebnisse wurden zunächst die vorgenommenen Gewichtungen der Experten, zur Durchführung der nachfolgenden Nutzwertanalyse, in eine aggregierte Gesamtgewichtung der Kriterien überführt. Abbildung 5.18 stellt das Resultat dieser Maßnahme als abfallende Reihenfolge der Kriterien dar. Die jeweiligen Nutzwerte der Kriterien ergeben sich daraufhin durch die Verrechnung der vorgenommenen Bewertung der Experten mit dem ermittelten Gewichtungswert des Kriteriums. Die Ergebnisse dieser Auswertung sowie einige der in den Gesprächen gesammelten Aussagen und Meinungen der Experten werden im nachfolgenden Abschnitt erläutert.

5.4.2 Ergebnisse

Nachdem im Rahmen des zuvor beschriebenen Vorgehens die erforderlichen Daten zur Durchführung der Nutzwertanalyse erhoben wurden, werden in diesem Abschnitt die ermittelten Ergebnisse beschrieben. Dabei werden die durch die von den Experten vorgenommenen Gewichtungen und Zuordnungen hinsichtlich des Erfüllungsgrades der Kriterien genutzt, um die Nutzwerte zu berechnen. Für jedes Kriterium ergibt sich nach diesem Vorgehen ein Nutzwert der das Kriterium für das bisherige Vorgehen beziffert sowie ein Nutzwert der dies entsprechend für den neuen Ansatz darstellt. Jeder dieser Nutzwerte, wie in Abbildung 5.18 dargestellt, beschreibt somit die Eignung des jeweiligen Ansatzes hinsichtlich eines Kriteriums, wobei ein höherer Nutzwert eine bessere, ein niedriger Nutzwert eine geringere Eignung durch den jeweiligen Ansatz beschreibt. Im Rahmen des vorgestellten Vorgehens wurden zusätzlich zur Erhebung der erforderlichen Daten für die quantitative Auswertung, die vorgenommenen Aussagen und Begründungen für die getätigte Auswahl dokumentiert, sodass in diesem Abschnitt sowohl die Nutzwerte als auch das Meinungsbild der maritimen Experten erläutert wird.

Abbildung 5.18 stellt die ermittelten Ergebnisse der quantitativen Auswertung durch die Nutzwertanalyse, der Gewichtung nach abfallend, über alle Kriterien zusammenfassend für beide betrachteten Ansätze dar. Demnach sind Aktualität und Transparenz als die beiden wichtigsten Kriterien identifiziert worden sowie nah folgend die Wiederverwendbarkeit, Aufwand und Detailgenauigkeit. In der Abbildung werden weiterhin die beiden Ansätze

hinsichtlich ihrer Nutzwerte quantitativ gegenübergestellt, sodass der bisherige Ansatz insgesamt mit einem Nutzwert von 1150 und der neue Ansatz mit einem Nutzwert von 1780 über alle Kriterien bewertet wurde und demnach hinsichtlich dieses Ergebnisses für maritime Experten als geeignet erscheint.

Das Kriterium der **Aktualität** vorgenommener Planungen wurde durch die Experten am höchsten gewichtet und erhielt im bisherigen Ansatz einen Gesamtnutzwert von 108. Hingegen wurde die Aktualität im neuen Ansatz mit einem Nutzwert von 216 und damit um 50% besser bewertet als im bisherigen Ansatz. Anhand der Nutzwerte dieses Kriteriums ergibt sich somit eine Bewertung, die im neuen Ansatz doppelt so gut ausfällt im Vergleich zum bisherigen Vorgehen. Auffallend ist jedoch, dass in den Gesprächen deutlich geworden ist, dass die Aktualität auch maßgeblich vom jeweiligen Experten abhängt und nicht vom Ansatz selbst. Eine dennoch bessere Bewertung des neuen Ansatzes hängt möglicherweise damit zusammen, dass dieses Kriterium möglicherweise durch eine stärkere softwareseitige Unterstützung sowie durch die Bereitstellung von Informationen aus der Wissensbasis als besser erfüllt bzw. weniger aufwändig empfunden wird. Darüber hinaus wurde die Nachvollziehbarkeit einer vorgenommenen Planung für andere beteiligte Personen als Kriterium der **Transparenz** ähnlich hoch gewichtet und durch den neuen Ansatz als um 28% eher geeignet bewertet, aufgrund rein textueller, informeller Darstellungen im bisherigen Vorgehen wodurch die Übersichtlichkeit und Nachvollziehbarkeit erschwert wird. Hingegen können im neuen Ansatz in der laufenden Planung Zusammenhänge zwischen Gefährdungen, Ursachen und risikomindernden Maßnahmen sowie frühere Bewertungen im Vorgehen eingesehen werden, was laut den Experten zur besseren Bewertung geführt hat.

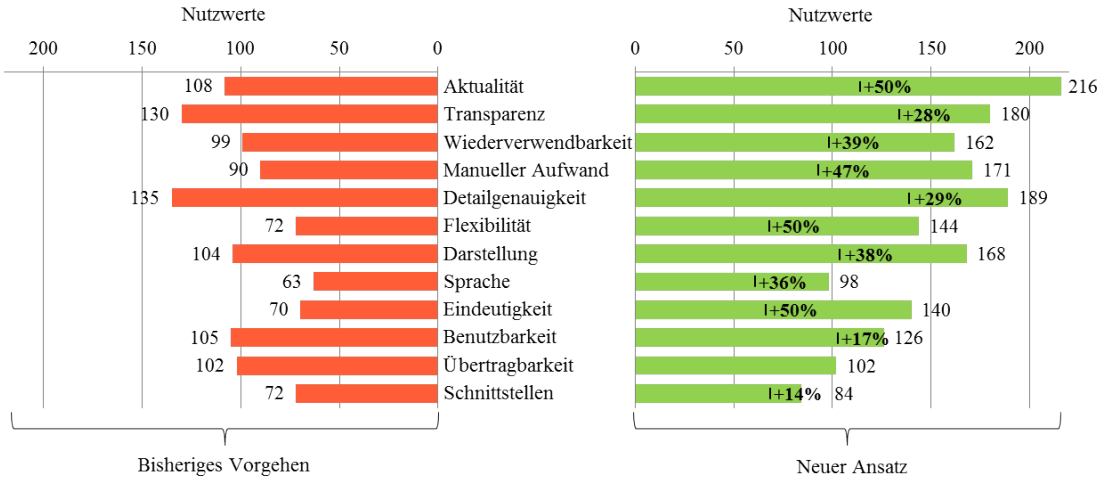

Abbildung 5.18: Ergebnisse der resultierenden Nutzwerte mit absteigender Gewichtung der Kriterien

Weitere hoch gewichtete Kriterien sind die **Wiederverwendbarkeit** und der **manuelle Aufwand**, die mit 39% bzw. 47% besser bewertet wurden im Vergleich zum bisherigen Vorgehen. Die Wiederverwendung im bisherigen Vorgehen bleibt vollständig dem Nutzer überlassen und wird daher laut den Experten als mühsam empfunden, was auch die Bewertung von 99 Punkten wiederspiegelt. Laut den Experten ist der neue Ansatz komfortabler zu handhaben, sodass einzelne Informationen beliebig oft wiederverwendet werden können, was insbesondere auch für eine schnelle Einbeziehung neuer Mitarbeiter und Nutzung wiederkehrender, bereits geprüfter oder in andere Sprachen übersetzter Informationen vorteilhaft ist. Insgesamt wird der Initial- und Folgeaufwand zur Planung maritimer Operationen als Kriterium des **manuellen Aufwands** mit dem neuen Ansatz durch softwareseitige Unterstützung und modellzentrische Handhabung um 47% besser bewertet im Vergleich zum bisherigen Vorgehen, bei welchem der Großteil der Informationen informell erfasst werden muss und zudem Inhalte teilweise auf verschiedene Dokumente verteilt sind. Trotz des somit als geringer empfundenen manuellen Aufwands, wurde von den Experten dennoch angemerkt, dass der Lernaufwand des neuen Ansatzes zu Beginn als höher eingeschätzt wird im Vergleich zu verbreiteten Werkzeugen zur Textverarbeitung. Dies bestärkt die gemachten Erfahrungen und Ergebnisse der Nutzerstudie aus Kapitel 5.3, wobei anzumerken ist, dass weitere Kriterien wie beispielsweise Wiederverwendbarkeit möglichen Einfluss auf die Bewertung des manuellen Aufwands des Gesamtansatzes haben können.

Mit den Kriterien der **Detailgenauigkeit** und **Flexibilität** wurde die Möglichkeit zur Variation und Flexibilität eines Ansatzes hinsichtlich unterschiedlicher Anforderungen für Gefährdungsbeurteilungen bewertet. Diese Kriterien hängen zwar maßgeblich vom jeweiligen Experten ab, welcher entscheidet welche Informationen wie detailliert eingepflegt werden, jedoch wird der neue Ansatz aufgrund des strukturierten und logischen Aufbaus als unterstützend empfunden, um verschieden detaillierte Planungen hinsichtlich unterschiedlicher Anforderungen durchzuführen. Im bisherigen Ansatz wird dies als kaum komfortabel umsetzbar empfunden, da die Komplexität der Dokumente hoch ist und bereits das Finden von betroffenen Stellen als aufwändig empfunden wird.

Kriterien wie **Darstellung** oder **Sprache**, die Möglichkeiten zur Visualisierung und Dokumentation bzw. zur mehrsprachigen Planungen beschreiben, wurden von den Experten als weniger wichtig eingeordnet und durch den neuen Ansatz als jeweils besser erfüllt bewertet. Zwar schätzen die Experten die vielen Freiheitsgrade des bisherigen Vorgehens, merkten jedoch auch die begrenzte Möglichkeit zur Darstellung von Zusammenhängen wie beispielsweise Abläufen oder Gefährdungen und Ursachen sowie die zusätzlich hohe Komplexität informeller, textueller Beschreibungen an. Die prototypische Umsetzung des neuen Ansatzes ermöglicht unterstützende Darstellungsformen von Prozessmodell und Fehlerbaum sowie eine daraus resultierende textuelle Dokumentation, ist jedoch durch die Umsetzung dieser spezifischen Technologien gleichermaßen auch beschränkt. Überwiegend wird mit dem bisherigen Ansatz in deutscher oder englischer Sprache gearbeitet, wobei je-

doch auch je nach Projekt und Anforderungen auch andere Sprachen hinzukommen können, bei denen dann teilweise Übersetzungsbüros hinzugezogen werden müssen. Der bisherige Ansatz an sich ermöglicht demnach durch die Textverarbeitung eine hohe Flexibilität und überlässt somit die Ausformulierung und teilweise Übersetzung dem jeweiligen Experten. Von den Experten wurde angemerkt, dass durch die verbesserte Wiederverwendbarkeit in dem neuen Ansatz gleichzeitig sich der Aspekt der Sprache verbessert, da sowohl Elemente in deutscher als auch bereits übersetzte in anderer Sprache vorgehalten und verwendet werden können, um den Experten zu unterstützen. Der Initialaufwand im neuen Ansatz, zum befüllen einer entsprechend mehrsprachigen Wissensbasis wird als hoch eingeschätzt, hingegen der Folgeaufwand als entsprechend gering diese zu nutzen. Dem gegenüber ist der Aufwand beim bisherigen Vorgehen jedes Mal gleich.

Hinsichtlich der **Eindeutigkeit** wurde bewertet, wie gut ein Ansatz den Anwender dabei unterstützt, die Planung mit Begrifflichkeiten, Strukturen etc. zum Verständnis durch Dritte auszugestalten. Entgegen dem bisherigen Vorgehen gibt der neue Ansatz durch die prototypische Umsetzung eine Terminologie und erforderliche Zusammenhänge vor, wodurch die Eindeutigkeit der somit vorgenommenen Planung verstärkt wird. Dabei wurde zusätzlich angemerkt, dass nach einiger Zeit durch die Wissensbasis ein Bestand an definierten und dokumentierten Begrifflichkeiten zur Verfügung steht, der für jeden neuen Prozess einheitlich verwendet werden kann. Als Kriterium der **Benutzbarkeit** wird die zuvor in Abschnitt 5.3 erläuterte Untersuchung durch Einschätzung der maritimen Experten abgeglichen. Der prototypischen Umsetzung durch den neuen Ansatz standen die Experten erwartungsgemäß zunächst skeptisch gegenüber und merkten einen initial erforderlich höheren Lernaufwand an. Hingegen wurde gleichermaßen teilweise Vorwissen der Experten im Rahmen der Prozessmodellierung sowie weitere Möglichkeiten identifiziert, bei denen die prototypische Implementierung den Nutzer in seiner Handlungsweise unterstützt. Das Kriterium Benutzbarkeit wurde insgesamt mit dem neuen Ansatz um 17% besser bewertet, was als Ergebnis auch der in Abschnitt 5.3 ermittelten Tendenz durch die Nutzerstudie entspricht, sodass beide Ansätze eindeutig benutzbar sind, jedoch der neue Ansatz das Kriterium geringfügig besser erfüllt.

Als die beiden Kriterien mit der geringsten Gewichtung wurden die **Übertragbarkeit** und die **Schnittstellen** identifiziert. Mit diesen wurden technische Aspekte der Software bewertet, um zu überprüfen wie gut sich ein Ansatz auf anderen Systemen einsetzen lässt, bzw. welche Schnittstellen zu anderen Softwaresystemen bestehen. Bei beiden Kriterien kam eine ähnliche Bewertung der beiden Ansätze heraus, wobei im Rahmen der Bewertung dieser beiden technischeren Kriterien aufgefallen ist, dass die befragten Personen eher Experten ihrer Domäne und weniger in Bezug auf derlei technische Aspekte sind. Somit sind die vorgenommenen Bewertungen dieser beiden letzten Attribute vermutlich wenig aussagekräftig.

5.4.3 Zusammenfassung

Zur weiteren Unterstützung der quantitativen Evaluation des entwickelten Ansatzes wurden in diesem Kapitel, mit Hilfe maritimer Sicherheitsexperten, Daten bezüglich des bisherigen Vorgehens und des neu entwickelten Ansatzes erhoben. Diese Daten umfassten eine Gewichtung und Einschätzung der Experten in Bezug auf verschiedene Kriterien, deren Erfüllungsgrad beider Ansätze somit gegenübergestellt wurde. Nach Erhebung dieser Daten wurde darauf aufbauend eine Nutzwertanalyse durchgeführt, um den tatsächlichen Nutzwert und damit die Eignung des jeweiligen Ansatzes hinsichtlich der Kriterien nach Einschätzung der Experten zu ermitteln. Die Auswertung hat ergeben, dass für den neu entwickelten Ansatz ein höherer Nutzwert resultiert als mit dem bisherigen Vorgehen, woraus geschlussfolgert werden kann, dass sich dieser Ansatz aus Sicht der Experten für den praktischen Einsatz eignet und den Werten nach zu Urteil deutliche Vorteile hat.

Während der Durchführung dieser Evaluation standen die Experten dem neuen Ansatz kritisch gegenüber, sodass eine notwendige Einarbeitungszeit angemerkt wurde. Zusätzlich zu dieser erwartungsgemäßen Skepsis gegenüber dem neuen Ansatz wurden dennoch von den Experten verschiedene positive Aspekte des Ansatzes bemerkt die im Folgenden zusammengefasst werden:

- Fokussiertere Arbeitsweise durch explizit erforderliche Zusammenhänge, grafische Darstellungen und Verbindung von prozessorientierten und Risikoaspekten
- Automatisierte Risikoanalyse wird als sehr hilfreich erachtet, da mit geringem Aufwand Designänderungen durchgeführt werden können
- Einsatz der Fehlerbaumanalyse schafft stärkere Transparenz, sodass vorgenommene Arbeiten von anderen beteiligten Personen besser nachvollzogen werden können und dient somit als geeignete Diskussionsgrundlage mit Aufschlüsselung von Ursachen und Gefährdungen
- Die Wissensbasis unterstützt in mehrfacher Hinsicht, sodass ungelerntes Personal leichter von bestehendem Erfahrungswissen profitieren kann. Außerdem wird auch erwartet, dass dadurch generell die Qualität der Arbeiten steigt, da durch die Mehrfachnutzung der Informationen diese verfeinert und hinterlegt werden können.
- Die Einbeziehung von risikomindernden Maßnahmen in den Planungsablauf wurde positiv bemerkt, sodass im Gegensatz zum bisherigen Vorgehen explizit aufgeführt wird worauf diese wirken und welchen Effekt sie haben, sodass zukünftig damit auch besser priorisiert werden kann, beispielsweise um Maßnahmen für besonders kritische Ursachen zu treffen.
- Eine hohe und praktikable Möglichkeit zur Wiederverwendung wird als sehr sinnvoll erachtet, sodass diese besonders für wiederkehrende Aspekte und Überschneidun-

gen zwischen Anwendungsfällen, beispielsweise durch ähnliche Arbeiten, Personen, Schiffen, Trainingsstufen etc., relevant wird. Auch können somit bereits in andere Sprachen übersetzte, durch andere Institutionen überprüfte Informationen auf diese Weise vorgehalten und beliebig oft verwendet werden.

Als weiteres wurde angemerkt, dass der Ansatz möglicherweise als zu detailliert für die tägliche Arbeit empfunden werden könnte. Wohingegen gleichermaßen festgestellt wurde, dass zwar die Möglichkeit für detaillierte Arbeiten in beiden Ansätzen vorhanden ist, jedoch es der handelnden Person obliegt inwieweit dies genutzt wird. Trotz des vermutet höheren Initialaufwandes mit dem neuen Ansatz wurde dieser dennoch durch die Experten besser bewertet als das bisherige Vorgehen, wodurch dieser trotz entsprechender Skepsis als geeignet erscheint.

5.5 Zusammenfassung

Nachdem in den vorangegangenen Kapiteln ein eigener Ansatz entwickelt und umgesetzt wurde, wurde dieser in diesem Kapitel qualitativ und quantitativ evaluiert. Für die **qualitative Evaluation** wurde der Ansatz anhand der Fallbeispiele Personentransfer und Lotsenwesen angewendet und systematisch erläutert. Im Rahmen des systematischen Vorgehens wurden dabei die Fallbeispiele mit Hilfe der Schritte Systemdefinition, Gefährdungsidentifikation, Risikoanalyse und Risikobewertung ausgearbeitet. Im ersten Fallbeispiel des **Personentransfers** wurde dabei eine initiale Anwendung des Ansatzes demonstriert, sodass zunächst der Ansatz ohne Nutzung der Wissensbasis behandelt wurde. Im Verlauf der Durchführung des Fallbeispiels wurden in den Schritten zur Systemdefinition und Gefährdungsidentifikation notwendige Informationen zur Abbildung des Fallbeispiels manuell eingebracht und entsprechend in Zusammenhang gebracht. Diese Informationen der auf diese Weise vorgenommenen Planung des Fallbeispiels wurden daraufhin der Risikoanalyse zugeführt, sodass zum Abschluss des Fallbeispiels diese Informationen und ermittelte Ergebnisse der Risikoanalyse, wie die Strukturierung der Ursachen und berechnete Werte, in die Wissensbasis überführt werden konnten. Im zweiten Fallbeispiel des **Lotsenwesens** wurde daraufhin eine weitere Anwendung des Ansatzes vorgenommen, in der wiederum nach dem bekannten Vorgehen vorgegangen wurde. Im Unterschied zum ersten Fallbeispiel, konnte in diesem jedoch zusätzlich zum beschriebenen manuellen Vorgehen die durch das erste Fallbeispiel befüllte Wissensbasis ergänzend genutzt werden. Dadurch konnte im Schritt der Gefährdungsidentifikation unterstützend eine für das Fallbeispiel des Lotsenwesens relevante Gefährdung aus der Wissensbasis gewonnen werden, sodass diese nicht manuell eingepflegt werden musste. Weiterhin konnte dies zudem den Schritt der Risikoanalyse unterstützen, indem für diese Gefährdung eine bestehende Strukturierung genutzt wurde. Anhand dieser Fallbeispiele wurde der entwickelte Ansatz qualitativ evaluiert, das Vorgehen erläutert und die Machbarkeit und Durchführung des Ansatzes demonstriert.

Weiterhin wurden die durch die Anwendung der Fallbeispiele erfüllten Ziele dieser Ausarbeitung in Abschnitt 5.1.3 und 5.2.3 abgeglichen.

Ergänzend zu diesem Vorgehen wurde im Rahmen der **quantitativen Evaluation** eine Nutzerstudie, zum Vergleich des bisherigen Vorgehens mit dem entwickelten Ansatz, durchgeführt sowie Daten mit Hilfe von maritimen Sicherheitsexperten für eine Nutzwertanalyse erhoben und ausgewertet. In der **Nutzerstudie** konnte die Tendenz aufgezeigt werden, dass beide Ansätze vergleichbar aufwändig durchzuführen sind sowie der neu entwickelte Ansatz bevorzugt eingesetzt wird. Dies konnte mit Hilfe maritimer Sicherheitsexperten und einer **Nutzwertanalyse** zusätzlich bekräftigt werden, sodass der entwickelte Ansatz als geeignet erscheint und besonders im Hinblick auf eine längerfristige Anwendung Vorteile hat. Die weitere Zielerfüllung der Ausarbeitung im Hinblick auf die quantitative Evaluation wird im Folgenden zusammengefasst:

- Ziel 1 - Formalisierung des Basiswissens: Die stärkere Formalisierung des Ansatzes im Vergleich zum bisherigen Vorgehen wurde sowohl im Rahmen der Nutzerstudie als auch mit Hilfe von maritimen Experten evaluiert, wobei besonders durch die Experten die Zielerfüllung zur Formalisierung hervorgehoben wurde und das Ziel als **erfüllt** betrachtet werden kann
- Ziel 2 - Prozessorientierte Risikobetrachtung: In der Nutzerstudie ist der Ansatz mit der prozessorientierten Herangehensweise praktisch angewendet worden, was zu einer positiven Endbewertung geführt hat. Zusätzlich konnte durch maritime Sicherheitsexperten bestätigt werden, dass das Ziel durch den Ansatz **erfüllt** wurde.
- Ziel 3 - Wiederverwendbare Informationen: Wiederverwendbarkeit wurde in der Nutzerstudie nicht evaluiert, jedoch konnte dieses Ziel durch die Experten als eines der wichtigsten und sehr gut umgesetzten Ziele evaluiert werden, wodurch dieses Ziel als **erfüllt** betrachtet wird.
- Ziel 4 - Unterstützende formalisierte Risikoanalyse: Die Ergebnisse der Nutzerstudie zeigen eine benutzbare Umsetzung des Ansatzes im Rahmen des Ziels an, was zusätzlich durch Auswertung der erhobenen Daten durch die Experten bestärkt wird, sodass der Ansatz als Unterstützung und stärkere Formalisierung einzupflegender Informationen und das Ziel als **erfüllt** empfunden wird.
- Ziel 5 - Berücksichtigung risikomindernder Maßnahmen: Durch Untersuchung der Praxistauglichkeit wurde besonders die Strukturierung und Transparenz des Ansatzes hervorgehoben, sodass risikomindernde Maßnahmen und deren Effekt explizit aufgeschlüsselt und nachvollzogen werden können, wodurch das Ziel **erfüllt** wird.
- Ziel 6 - Softwareseitige Unterstützung: Mit Hilfe der prototypischen Umsetzung ist die softwareseitige Unterstützung in beiden Szenarien zur quantitativen Evaluation positiv bewertet worden, sodass das Ziel als **erfüllt** gilt.

Insgesamt konnten somit alle vorgenommenen Zieldefinitionen mit Hilfe verschiedener Evaluationsszenarien beantwortet werden. Besonders die Nutzerstudie hat jedoch gleichermaßen auch aufgezeigt, dass im Rahmen der prototypischen Umsetzung noch Potential für Verbesserungen besteht. Dennoch wurde der Ansatz auch von maritimen Sicherheitsexperten, als die Anwender eines solchen Ansatzes, positiv bewertet.

Kapitel 6

Zusammenfassung und Ausblick

Einen wesentlichen Bestandteil zur Durchführung maritimer Aufgaben wie beispielsweise Aufbau, Installation und Wartung von Offshore-Windenergieanlagen stellen vorbereitende Planungsmaßnahmen dar. Innerhalb dieser stellt die Planung maritimer Operationen die Praxis vor diverse Herausforderungen, sodass die Komplexität und Menge derartiger Arbeiten stetig wächst und entsprechend viel Erfahrungswissen erfordert, um solch ein Vorhaben im Hinblick auf die besonders kritischen Einsatzbedingungen adäquat durchzuführen. Dafür fehlt es zudem an Systematik und Formalisierung bei derlei Vorgehen, sodass die maritimen Sicherheitsexperten bei der Durchführung kaum unterstützt werden, um strukturiert relevante Gefährdungen, Ursachen und risikomindernde Maßnahmen identifizieren und abschätzen zu können.

Innerhalb dieser Arbeit wurden diese Problemstellungen in den vorangegangenen Kapiteln adressiert und ein Lösungsansatz dafür entwickelt. Dabei wurde anhand eines systematischen Vorgehens zunächst ein entsprechendes Konzept entwickelt, anschließend prototypisch umgesetzt und daraufhin qualitativ anhand zweier Fallbeispiele sowie quantitativ durch eine Nutzerstudie und eine Nutzwertanalyse mit Hilfe maritimer Sicherheitsexperten evaluiert. Dieses Kapitel schließt somit die vorliegende Arbeit zusammenfassend ab und gibt einen Ausblick über mögliche Erweiterungen und zukünftige Arbeiten.

6.1 Zusammenfassung

Im Rahmen der vorliegenden Ausarbeitung wurde ein Ansatz zur formalisierten Risikoanalyse für prozessorientierte Anwendungen, wie die Planung maritimer Operationen, entwickelt. Basierend auf einer strukturierten Systemdefinition werden innerhalb eines systematischen Vorgehens erforderliche Informationen miteinander vernetzt und können somit für eine Risikoanalyse sowie eine stärkere Wiederverwendbarkeit genutzt werden.

In Kapitel 2 dieser Ausarbeitung wurde für das Vorhaben zunächst der Stand der

Technik erhoben, in welchem zu Beginn das derzeitige Vorgehen und Rahmenbedingungen zur Risikobewertung von Operationen in der maritimen Domäne dargestellt wurden. Als Bestandteil davon wurde der Begriff der Schutz- und Sicherheitskonzepte eingeführt und anhand des Vorgehens beschrieben. Erweitert wurde dies um weitere Ausführungen bezüglich der derzeitigen technischen Umsetzungen und Möglichkeiten zur Unterstützung. Ergänzend wurden Techniken für eine stärkere Formalisierung eines Ansatzes erläutert und bewertet, woraufhin verwandte Arbeiten aufgeführt worden sind, die diese für bestimmte Problemstellungen anwenden und anpassen. Sämtliche Ansätze wurden hinsichtlich der übergeordneten Zielvorstellungen bewertet und daraufhin der Handlungsbedarf ermittelt.

Im Anschluss wurde in Kapitel 3 ein eigener Ansatz konzipiert, in welchem zunächst im Hinblick auf den identifizierten Handlungsbedarf und die übergeordneten Zielvorstellungen, Anforderungen ermittelt wurden. Im Rahmen eines schrittweisen, systematischen Vorgehens wurde daraufhin der entwickelte Ansatz mit Konzepten und jeweiligem Vorgehen beschrieben und anhand eines durchgehenden Anwendungsbeispiels veranschaulicht. Auf Basis der zur Systemdefinition verwendeten Software MOPhisTo und dort innerhalb eines Prozessmodells geplanten Abläufen, wurde im darauffolgenden Schritt ein Konzept zur strukturierten Integration von Informationen der Gefährdungsidentifikation entwickelt. In diesem können neue Informationen sowohl manuell als auch unterstützt durch gespeicherte Informationen vergangener Anwendungsfälle eingebracht werden. Darauffolgend konnten eingepflegte Informationen zur weiteren Strukturierung und aufbauenden Formalisierung genutzt werden, sodass im Rahmen einer Fehlerbaumanalyse die Risikoanalyse einer geplanten Operation durchgeführt werden kann. Mit Hilfe einer entwickelten Wissensbasis wird abschließend zu diesem Vorgehen ermöglicht, eingebrachte Informationen strukturiert zu speichern, sodass diese für zukünftige Anwendungsfälle erneut bereitgestellt werden können. Die prototypische Umsetzung dieses entwickelten Ansatzes wurde zudem in Kapitel 4 beschrieben.

In Kapitel 5 wurde der entwickelte Ansatz im Hinblick auf verschiedene Szenarien evaluiert. Zunächst wurden im Rahmen einer qualitativen Evaluation zwei Fallbeispiele behandelt und die Machbarkeit und Durchführung des Ansatzes demonstriert. Mit Hilfe dieser Fallbeispiele und der Anwendung des Ansatzes konnte bereits die Erfüllung der übergeordneten Ziele nachgewiesen werden. Zusätzlich wurde der Ansatz quantitativ evaluiert, sodass die Zielvorstellungen zur Ergänzung auch durch die Anwendung eines größeren Personenkreises nachgewiesen werden konnte. Dafür wurde zum einen eine Nutzerstudie durchgeführt, in der im Rahmen der Anwendung durch mehrere Probanden Daten zum Vergleich des neu entwickelten und des bisherigen Ansatzes, wie in Kapitel 2 beschrieben, erhoben werden konnten. Zum anderen wurde der Ansatz ergänzend maritimen Sicherheitsexperten, als reale Anwender des Ansatzes, vorgestellt und in einer Befragung Daten

zur Durchführung einer Nutzerstudie erhoben und ausgewertet. Die qualitative und quantitative Evaluation hat somit ergeben, dass der Ansatz positiv zu bewerten ist und die aufgestellten Zielvorstellungen erfüllt.

6.2 Ausblick

Mit der qualitativen und quantitativen Evaluation des Ansatzes konnte gezeigt werden, dass gestellte Zielvorstellungen erfüllt werden können. Dennoch konnten weitere Arbeiten identifiziert werden, die im Rahmen weiterer Forschungsvorhaben den Ansatz sinnvoll erweitern könnten:

- **Simulative Ergänzung**: Für den in dieser Ausarbeitung gewählten Ansatz wird die Fehlerbaumanalyse verwendet, um eine Möglichkeit zur formalisierten Strukturierung und Auswertung zu bieten. Dabei muss stets abgewägt werden, welche Strukturen betrachtet und wie quantitative Abschätzungen zu treffen sind. Wurden alle erforderlichen Informationen betrachtet und richtig zusammengesetzt?, Ist die vorgenommene Quantifizierung zu optimistisch/pessimistisch?, sind dabei aufkommende Fragestellungen. Ein Ansatz der Antworten darauf und damit eine stärkere Evidenz für die Planung liefern kann, würde eine sinnvolle Erweiterung darstellen. Eine erste Lösungsidee dafür wird mit Hilfe von Simulation in der andauernden Forschung von Gollücke [GPL+14] entwickelt.

- **Erweiterung der Informationsquellen**: Im Verlauf derartiger Planungsvorhaben, wie beispielsweise für maritime Operationen, ist viel Erfahrungswissen über die Domäne und den betrachteten Anwendungsfall erforderlich. Überwiegend wird dies vom jeweiligen Experten gefordert der die entsprechende Planung durchführt. Ein erster Ansatz den Experten dabei zu unterstützen wurde mit der Integration der Wissensbasis in das Vorgehen ermöglicht. Diese wächst zwar mit jeder Durchführung bzw. jedem Anwendungsfall, jedoch existieren weitere Informationsquellen, wie beispielsweise Statistiken und Unfallberichte, die zu einer sinnvollen Erweiterung der Wissensbasis dienen können. Ein Ansatz der dieses Wissen, welches häufig unstrukturiert und nur in textueller Form vorliegt, formalisiert und strukturiert, um dieses in der Wissensbasis zu hinterlegen, wäre ein weiteres interessantes Forschungsvorhaben.

Literaturverzeichnis

[AFPR13] Andrews, Zoe ; Fitzgerald, John ; Payne, Richard ; Romanovsky, Alexander: Fault modelling for systems of systems. In: Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on IEEE, 2013, S. 1–8

[Alt10] Altiok, Dr. T.: Model-based risk. In: Cargo Security International - Maritime and Port Security (2010), S. pp. 22–24

[AS06] Antao, Pedro ; Soares, C G.: Fault-tree models of accident scenarios of RoPax vessels. In: International Journal of Automation and Computing 3 (2006), Nr. 2, S. 107–116

[Aul13] Aull, F.: Modell zur Ableitung effizienter Implementierungsstrategien für Lean-Production-Methoden. Utz, Herbert, 2013 (Forschungsberichte IWB). http://books.google.de/books?id=QkDw3-9lz8EC. – ISBN 9783831642830

[Auv14] Auvation: OpenFTA. http://www.openfta.com/, 2014. – [Online; Zugriff: 21.10.2014]

[B+07] Bellmer, Horst u. a.: Standard - Konstruktive Ausführung von Offshore-Windenergieanlagen. Bundesamt für Seeschifffahrt und Hydrographie, 2007

[BAS14] BASSnet: Risk Manager. http://www.bassnet.no/portfolio-item/risk-manager/, 2014. – [Online; Zugriff: 14.10.2014]

[BB12] Brüggemann, H. ; Bremer, P.: Grundlagen Qualitätsmanagement: Von den Werkzeugen über Methoden zum TQM. Vieweg+Teubner Verlag, 2012 http://books.google.de/books?id=sCA-ZDlTkjsC. – ISBN 9783834813091

[BCS02] Bieber, Pierre ; Castel, Charles ; Seguin, Christel: Combination of Fault Tree Analysis and Model Checking for Safety Assessment of Complex System. Version: 2002. http://dx.doi.org/10.1007/3-540-36080-8_3. In: Bondavalli, Andrea (Hrsg.) ; Thevenod-Fosse, Pascale (Hrsg.): Dependable

Computing EDCC-4 Bd. 2485. Springer Berlin Heidelberg, 2002. – DOI 10.1007/3–540–36080–8_3. – ISBN 978–3–540–00012–9, 19-31

[Ber14] Berufsgenossenschaft ETEM - Energie Textil Elektro Medienerzeugnisse: Gefährdungsbeurteilung - Nur eine Richtung zählt! http://www.bgetem.de/redaktion/medien-service/dokumente-und-dateien/etem/pdf/etem-3-2014-ausgabe-elektro-feinmechanik, 2014. – [Online; Zugriff: 25.09.2014]

[BKM09] Bangor, Aaron ; Kortum, Philip ; Miller, James: Determining what individual SUS scores mean: Adding an adjective rating scale. In: Journal of usability studies 4 (2009), Nr. 3, S. 114–123

[BM05] Baker, CC ; McCafferty, DB: Accident database review of human element concerns: What do the results mean for classification? In: Proc. Int Conf. Human Factors in Ship Design and Operation, RINA Feb, 2005

[Böt13] Böttcher, Jörg: Handbuch Offshore-Windenergie. 2013

[Bra02] Braasch, Wolfram: Risikoanalysen für Offshore-Installationen. In: Schiff und Hafen (2002), Nr. 6, S. 85–90

[Bra05] Braband, Jens: Ein semi-quantitativer Ansatz zur Risikoanalyse in der Eisenbahnautomatisierung. In: Signal + Draht 10 (2005)

[Bri14] Brinkmann, Martina: Die Nordsee ist unberechenbar - der Überstieg von einem Transferschiff auf eine Windkraftanlage kann für Monteure lebensgefährlich werden. http://www.tuhh.de/zeit-beilage/startseite/ueberstieg.html, 2014. – [Online; Zugriff: 05.12.2014]

[Bro96] Brooke, John: SUS-A quick and dirty usability scale. In: Usability evaluation in industry 189 (1996), S. 194

[Buc08] Buchholz, Peter: Modellgestützte Analyse und Optimierung. http://ls4-www.cs.tu-dortmund.de/download/LehreMaterialien/MAO2011/MAO_7.pdf, 2008. – [Online; Zugriff: 01.09.2014]

[Bun0a] Bundesamt für Seeschifffahrt und Hydrographie: Standard Schutz- und Sicherheitskonzept für Offshore-Windparks. 2010a

[Bun4f] Bundesamt für Seeschifffahrt und Hydrographie: Genehmigungsbescheid ÖWP West". http://www.bsh.de/de/Meeresnutzung/Wirtschaft/Windparks/Genehmigungsbescheide/Nordsee/OWP_West/Genehmigungsbescheid_OWP_West.pdf, 2014f. – [Online; Zugriff: 08.07.2014]

[Bun14a] Bundesministerium für Verkehr und digitale Infrastruktur: Offshore-Windenergie - Sicherheitsrahmenkonzept (OWE-SRK). 2014

[Bun14b] Bundesministerium für Wirtschaft und Energie: Offshore-Windenergie - Wirtschaft. http://www.offshore-windenergie.net/wirtschaft. Version: August 2014

[Bun14c] Bundesverband der See- und Hafenlotsen e.V.: Die Aufgaben eines Lotsen. http://bshl.de/ueberlotsen/berufsbild/index.html, 2014. – [Online; Zugriff: 18.11.2014]

[Bunnt] Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA): Warum mache ich eine Gefährdungsbeurteilung? http://www.gefaehrdungsbeurteilung.de/de/einstieg/warum, Jahr unbekannt. – [Online; Zugriff: 27.08.2014]

[Bur04] Burgess, M: Fault tree creation and analysis tool: user manual. 2004

[CACO06] Chen, Bin ; Avrunin, George S. ; Clarke, Lori A. ; Osterweil, Leon J.: L.J.: Automatic Fault Tree Derivation from Little-JIL Process Definitions. In: Springer-Verlag LNCS, 2006, S. 150–158

[CCC] Christov, Stefan C. ; Chao, Tiffany Y. ; Clarke, Lori A.: Generating Natural-language Process Descriptions from Formal Process Models.

[Che10] Chen, Bin: Improving processes using static analysis techniques, University of Massachusetts - Amherst, dissertation, 2010. http://scholarworks.umass.edu/dissertations/AAI3445153/

[CS06] Carter, Gregory ; Smith, Simon D.: Safety hazard identification on construction projects. In: Journal of Construction Engineering and Management 132 (2006), Nr. 2, S. 197–205

[DD08] Dehlinger, Josh ; Dugan, Joanne B.: Analyzing dynamic fault trees derived from model-based system architectures. In: Nuclear Engineering and Technology: An International Journal of the Korean Nuclear Society 40 (2008), Nr. 5, S. 365–374

[Deu11a] Deutscher Bundestag: Keine zusätzlichen Sicherheitsanforderungen bei Offshore-Windanlagen. Berlin : PuK 2 Parlamentskorrespondenz, 2011 (Drucksache 17/5441)

[Deu11b] Deutscher Bundestag: Sicherheit und Arbeitsschutz bei Offshore-Windenergieanlagen. http://dipbt.bundestag.de/dip21/btd/17/054/1705441.pdf, 2011. – [Online; Zugriff: 19.09.2014]

[DH13] Droste, Rainer ; Hahn, Axel: Modellbasierte Planung und Analyse von Offshore-Operationen. In: Tagungsband zum Doctoral Consortium der WI 2013 (2013), S. 74

[DHK+14] Drews, G. ; Hillebrand, N. ; Kärner, M. ; Peipe, S. ; Rohrschneider, U.: Praxishandbuch Projektmanagement - inkl. eBook und Arbeitshilfen online. Haufe Lexware GmbH, 2014 (Haufe Fachbuch). http://books.google.de/books?id=6atqAwAAQBAJ. – ISBN 9783648050903

[DI07] Dokas, Ioannis M. ; Ireland, C: Ontology to support knowledge representation and risk analysis for the development of early warning system in solid waste management operations. In: Proceedings of the International Symposium on Environmental Software Systems, 2007

[din81] Fehlerbaumanalyse: DIN 25424. Methode und Bildzeichen. 1981 (Bd. 1). https://books.google.de/books?id=FuizjwEACAAJ

[din90] Fehlerbaumanalyse: Fault tree analysis : DIN 25424. Handrechenverfahren zur Auswertung eines Fehlerbaumes. Beuth, 1990 (DIN-Normen: Deutsches Institut für Normung Bd. 2). https://books.google.de/books?id=6uUumAEACAAJ

[DIN02] DIN, EN: 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer/elektronischer Systeme. In: Berlin: Beuth-Verlag (2002)

[DL06] Dehlinger, Josh ; Lutz, Robyn R.: Plfaultcat: A product-line software fault tree analysis tool. In: Automated Software Engineering 13 (2006), Nr. 1, S. 169–193

[Dor14] Dornes, N.: Alternative Risikomodellierungs-, Risikoanalyse- und Bewertungsmethode: Risikomanagement ohne komplexe mathematische Modelle. Disserta Verlag, 2014 http://books.google.de/books?id=GG-yBAAAQBAJ. – ISBN 9783954256662

[DV90] De Vries, Ronald C.: An automated methodology for generating a fault tree. In: Reliability, IEEE Transactions on 39 (1990), Nr. 1, S. 76–86

[E a94] E and P Forum: Guidelines for the Development and Application of Health, Safety and Environmental Management Systems. London : E&P Forum, 1994

[Eri05] Ericson, C.A.: Hazard Analysis Techniques for System Safety. Wiley, 2005 http://books.google.de/books?id=8ErpVtkp7ZYC. – ISBN 9780471739418

[ERS10] Ebrahimipour, V ; Rezaie, Kamran ; Shokravi, S: An ontology approach to support FMEA studies. In: Expert Systems with Applications 37 (2010), Nr. 1, S. 671–677

[Fes14] Festag, Sebastian: Umgang mit Risiken: Qualifizierung und Quantifizierung XXVII. Sicherheitswissenschaftliches Symposion der GfS (Juni 2013 in Wien). Beuth Verlag GmbH, 2014 (Beuth Forum). http://books.google.de/books?id=3KFhAgAAQBAJ. – ISBN 9783410242659

[Fri08] Fritelli, John: Ship navigation in harbors: Safety issues. CRS Report for Congress http://research.policyarchive.org/19247.pdf, 2008. – [Online; Zugriff: 04.02.2015]

[GA12] Grewer, A. ; Adolph, L.: Ratgeber zur Gefährdungsbeurteilung: Handbuch für Arbeitsschutzfachleute. Baua, Bundesanstalt für Arbeitssschutz und Arbeitsmedizin, 2012 http://books.google.de/books?id=ssK6lgEACAAJ. – ISBN 9783882617177

[GAAR14] Greiner, S ; Albers, H ; Albers, H ; Renz, T: Low-risk Processes, Customized for Operation of Offshore Wind Farms. In: DEWI Magazin (2014), Nr. 44, S. 58–63

[GH08] Grunske, Lars ; Han, Jun: A comparative study into architecture-based safety evaluation methodologies using AADL's Error Annex and failure propagation models. In: High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE IEEE, 2008, S. 283–292

[GHS02] Grech, Michelle R. ; Horberry, Tim ; Smith, Andrew: Human error in maritime operations: Analyses of accident reports using the Leximancer tool. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting Bd. 46 SAGE Publications, 2002, S. 1718–1721

[GLS10] Gómez, Carolina ; Liggesmeyer, Peter ; Sutor, Ariane: Variability management of safety and reliability models: an intermediate model towards systematic reuse of component fault trees. In: Computer Safety, Reliability, and Security. Springer, 2010, S. 28–40

[GMR11] Glukhikh, Mikhail ; Moiseev, Mikhail ; Richter, Harald: An Approach for the Reliability Analysis of Automotive Control Systems. In: DEPEND 2011, The Fourth International Conference on Dependability, 2011, S. 51–56

[GPL+14] Gollücke, Volker ; Pinkowski, Jan ; Läsche, Christoph ; Gerwinn, Sebastian ; Hahn, Axel: Simulation-based Completeness Analysis and Adaption of

Fault Trees. In: SIMUL 2014, The Sixth International Conference on Advances in System Simulation, 2014

[H+85] Hoare, Charles Antony R. u. a.: Communicating sequential processes. Bd. 178. Prentice-hall Englewood Cliffs, 1985

[Ham14] Hamburger Abendblatt: Lotse stürzt beim Übersteigen in die Elbe, 20.02.2012, Brunsbüttel. http://www.abendblatt.de/region/article2192646/Lotse-stuerzt-beim-Uebersteigen-in-die-Elbe.html, 2014. – [Online; Zugriff: 19.11.2014]

[Hen] Henriksen, A.: Seeunfalluntersuchung und Berechtigungsentzug. Duncker & Humblot http://books.google.de/books?id=HJswlkwd0AoC. – ISBN 9783428485765

[HFM06] Hetherington, Catherine ; Flin, Rhona ; Mearns, Kathryn: Safety in shipping: The human element. In: Journal of safety research 37 (2006), Nr. 4, S. 401–411

[Int02] International Maritime Organisation (IMO): Guidelines for Formal Safety (FSA) for use in the IMO Rule-Making Process, MSC/Circ. 1023 and MEPC/Circ. 392. http://www.imo.org/OurWork/HumanElement/VisionPrinciplesGoals/Documents/1023-MEPC392.pdf, 2002. – [Online; Zugriff: 04.09.2014]

[Int06] International Electrotechnical Commission and others: IEC 61025: Fault tree analysis (FTA). In: International Standard (2006)

[ISO08] ISO: ISO 26262 Road vehicles - Functional safety. 2008

[Iso14] Isograph Ltd: Fault Tree Plus. http://www.isograph.com, 2014. – [Online; Zugriff: 28.10.2014]

[ITE14] ITEM: ToolKit. http://www.itemuk.com/toolkit.html, 2014. – [Online; Zugriff: 21.10.2014]

[JH07] Joshi, Anjali ; Heimdahl, Mats Per E.: Behavioral fault modeling for model-based safety analysis. In: High Assurance Systems Engineering Symposium, 2007. HASE'07. 10th IEEE IEEE, 2007, S. 199–208

[Jun12] Junglas, Marco: Methodische Entwicklung hochintegrierter mechatronischer Systeme unter funktionalen, zuverlässigkeits-und sicherheitstechnischen Aspekten-Analyse und Quantifizierung, Universität Duisburg-Essen, Fakultät für Ingenieurwissenschaften» Maschinenbau und Verfahrenstechnik» Institut für Mechatronik und Systemdynamik, Diss., 2012

[Jur4b] Juris GmbH: Arbeitsschutzgesetz. http://www.gesetze-im-internet.de/bundesrecht/arbschg/gesamt.pdf, 2014b. – [Online; Zugriff: 13.08.2014]

[JVB07] Joshi, Anjali ; Vestal, Steve ; Binns, Pam: Automatic generation of static fault trees from aadl models. In: Workshop on Architecting Dependable Systems of The 37th Annual IEEE/IFIP Int. Conference on Dependable Systems and Networks, Edinburgh, UK, 2007

[Kel99] Kelly, Timothy P.: Arguing safety: a systematic approach to managing safety cases. University of York, 1999

[KG87] Koren, JM ; Gaertner, J: CAFTA: a fault tree analysis tool designed for PSA. In: Probabilistic safety assessment and risk management PSA'87. Vol. 2. 1987

[Kir04] Kirchberg, S.: Ratgeber zur Ermittlung gefährdungsbezogener Arbeitsschutzmaßnahmen im Betrieb. Handbuch für Arbeitsschutzfachleute. 4. Auflage. Bremerhaven: Wirtschaftsverlag NW Verlag für neue Wissenschaft GmbH 2001, 2004 http://www.uni-stuttgart.de/zv/sicherheitswesen/dokumente/ratgeber_gefaehrdung.pdf

[KLFL11] Kuntz, Matthias ; Leitner-Fischer, Florian ; Leue, Stefan: From probabilistic counterexamples via causality to fault trees. Springer, 2011

[KMS05] Kagdi, Huzefa ; Maletic, Jonathan I. ; Sutton, Andrew: Context-free slicing of UML class models. In: Software Maintenance, 2005. ICSM'05. Proceedings of the 21st IEEE International Conference on IEEE, 2005, S. 635–638

[Kon05] Kontovas, Christos A.: Formal Safety Assessment - Critical Review and Future Role, NATIONAL TECHNICAL UNIVERSITY OF ATHENS - School of Naval Architecture and Marine Engineering, Diploma Thesis, 2005

[KOS12] Koschmider, Agnes ; Oberweis, Andreas ; Schoknecht, Andreas: SemReuse–Semantikbasierte Wiederverwendung von Geschäftsprozessmodellen1. (2012)

[Küp12] Küppers, Martin: See und Sicherheit - Der Weg zur Gefährdungsbeurteilung. In: SicherheitsProfi - Das Magazin der Berufsgenossenschaft für Transport und Verkehrswirtschaft (2012), S. pp. 22–23

[Kri13] Kristiansen, S.: Maritime Transportation: Safety Management and Risk Analysis. Taylor & Francis, 2013 http://books.google.de/books?id=ra7bAAAAQBAJ. – ISBN 9781136077586

[L+11] Li, Yue u. a.: A method for constructing fault trees from AADL models. In: Proceedings of the 8th international conference on Autonomic and trusted computing. Berlin, Heidelberg : Springer-Verlag, 2011 (ATC'11). – ISBN 978–3–642–23495–8, 243–258

[LDP+14] Läsche, Christoph ; Droste, Rainer ; Pinkowski, Jan ; Gerwinn, Sebastian ; Hahn, Axel: Model-Based Risk Assessment of Offshore Operations. In: Proceedings 33rd International Conference on Ocean, Offshore and Arctic Engineering (2014), S. 1–10

[Lev95] Leveson, N.: SafeWare: System Safety and Computers. Addison-Wesley, 1995 (Computer Science and Electrical Engineering Series). http://books.google.de/books?id=ZrZQAAAAMAAJ. – ISBN 9780201119725

[LGP11] Lauer, Christoph ; German, Reinhard ; Pollmer, Jens: Fault tree synthesis from UML models for reliability analysis at early design stages. In: ACM SIGSOFT Software Engineering Notes 36 (2011), Nr. 1, S. 1–8

[Lim13] Limnios, N.: Fault Trees. Wiley, 2013 (ISTE). http://books.google.de/books?id=ZvPViVpG2ksC. – ISBN 9781118614068

[LLB+11] Liu, Hu-Chen ; Liu, Long ; Bian, Qi-Hao ; Lin, Qin-Lian ; Dong, Na ; Xu, Peng-Cheng: Failure mode and effects analysis using fuzzy evidential reasoning approach and grey theory. In: Expert Systems with Applications 38 (2011), Nr. 4, S. 4403–4415

[LMW+00] Lemer, Barbara S. ; McCall, Eric K. ; Wise, Alexander ; Cass, Aaron G. ; Osterweil, Leon J. ; Jr., Stanley M. S.: Using Little-JIL to Coordinate Agents in Software Engineering. In: Proceedings of the 15th IEEE international conference on Automated software engineering. Washington, DC, USA : IEEE Computer Society, 2000 (ASE '00). – ISBN 0–7695–0710–7, 155–

[Lob12] Lobenstein, Caterina: 100 Kilometer bis zur Klinik. In: Die Zeit (2012), Januar. http://www.zeit.de/2012/01/C-Windpark, Abruf: 08. August 2014

[Lot14] Lotsenbrüderschaft Emden: Die Lotsen auf der Ems. http://www.emspilots.de/default.aspx?id=4, 2014. – [Online; Zugriff: 18.11.2014]

[LR98] Liggesmeyer, P. ; Rothfelder, M.: Improving system reliability with automatic fault tree generation. In: Fault-Tolerant Computing, 1998. Digest of Papers. Twenty-Eighth Annual International Symposium on, 1998. – ISSN 0731–3071, S. 90 –99

[LST09] Latif-Shabgahi, G. ; Tajarrod, F.: A New Approach for the Construction of Fault Trees from System Simulink. In: Availability, Reliability and Security, 2009. ARES '09. International Conference on, 2009, S. 712–717

[Man13] Manuele, Fred A.: On the practice of safety. John Wiley & Sons, 2013

[Mar12] Marchanka, Aliaksandr: Analysis of ISO26262 standard application in development of steer-by-wire systems. Göteborg, Schweden, Chalmers University of Technology, University of Gothenburg, Department of Computer Science and Engineering, Diplomarbeit, 2012

[MCO15] Marie-Christin Ostendorp, Andreas L. Jan Charles Lenk L. Jan Charles Lenk: Smart Glasses to support Maritime Pilots in Harbor maneuvers. In: Proceedings of the 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015), 2015

[MEP+05] Mckelvin, Mark L. ; Eirea, Gabriel ; Pinello, Claudio ; Kanajan, Sri ; Sangiovanni-vincentelli, Alberto L.: A Formal Approach to Fault Tree Synthesis for the Analysis of Distributed Fault Tolerant Systems. In: Procs. of the 5th ACM International Conference on Embedded Software, 2005, S. 237–246

[MKH04] Marx, Marcus ; Knetsch, Thomas ; Hauptmanns, Ulrich: Analysis of occupational hazards using fault trees. Version: 2004. http://dx.doi.org/10.1007/978-0-85729-410-4_9. In: Spitzer, Cornelia (Hrsg.) ; Schmocker, Ulrich (Hrsg.) ; Dang, VinhN. (Hrsg.): Probabilistic Safety Assessment and Management. Springer London, 2004. – DOI 10.1007/978–0–85729–410–4_9. – ISBN 978–1–4471–1057–6, 52-57

[Mod06] Modarres, M.: Risk Analysis in Engineering: Techniques, Tools, and Trends. Taylor & Francis, 2006 http://books.google.de/books?id=ErjFzRWSne8C. – ISBN 9781574447941

[Moh13] Mohr, Dominik: Seminar Sicherheit und Softwareengineering, Lehrstuhl 14, Technische Universität Dortmund. 2013

[MPB03] Majzik, István ; Pataricza, András ; Bondavalli, Andrea: Stochastic dependability analysis of system architecture based on UML models. In: Architecting dependable systems. Springer, 2003, S. 219–244

[MRC07] Mendling, Jan ; Reijers, Hajo A. ; Cardoso, Jorge: What makes process models understandable? In: Business Process Management. Springer, 2007, S. 48–63

[MSB09] Madlener, Reinhard ; Siegers, Lena ; Bendig, Stefan: Risikomanagement und-controlling bei Offshore-Windenergieanlagen. In: Zeitschrift für Energiewirtschaft 33 (2009), Nr. 2, S. 135–146

[Mul06] Mullai, Arben ; Ojala, Lauri (Hrsg.) ; Suominen, Mikko (Hrsg.): Risk Management System - Risk Assessment Frameworks and Techniques / DaGoB (Safe and Reliable Transport Chains of Dangerous Goods in the Baltic Sea Region) Project Office, Turku School of Economics, Turku, Finland. 2006 (DaGoB Publication Serie 5:2006 5:2006). – Forschungsbericht. – ISBN 951–564–393–7

[Obj14] Object Management Group (OMG): Systems Modeling Language (SysML). http://www.omg.org/spec/SysML/1.3/, 2014. – [Online; Zugriff: 21.10.2014]

[Ohn12] Ohne Author: Seemannschaft: Handbuch für Segler und Motorbootfahrer. Bod Third Party Titles, 2012 http://books.google.de/books?id=ChNEJIw5gzOC. – ISBN 9783864443244

[PBM+08] Pock, Michael ; Belhadaoui, Hicham ; Malassé, Olaf ; Walter, Max u. a.: Efficient generation and representation of failure lists out of an information flux model for modeling safety critical systems. In: The European Safety and Reliability Conference, ESREL 2008, 2008, S. 1829–1837

[PD02] Pai, G.J. ; Dugan, J.B.: Automatic synthesis of dynamic fault trees from UML system models. In: Software Reliability Engineering, 2002. ISSRE 2003. Proceedings. 13th International Symposium on, 2002. – ISSN 1071–9458, S. 243 – 254

[Pet14] Petry, C.: Untersuchung und Bewertung der Praxistauglichkeit einer modell-basierten Methode zur Erstellung von HSE-Plänen. Germany, Carl-von-Ossietzky Universität Oldenburg, Masterarbeit, November 2014

[PL11] Ponn, J. ; Lindemann, U.: Konzeptentwicklung und Gestaltung Technischer Produkte. Springer, 2011 (VDI-Buch). http://books.google.de/books?id=7OofBAAAQBAJ. – ISBN 9783642205804

[PM01] Papadopoulos, Yiannis ; Maruhn, Matthias: Model-based synthesis of fault trees from matlab-simulink models. In: Dependable Systems and Networks, 2001. DSN 2001. International Conference on IEEE, 2001, S. 77–82

[Pri12] PricewaterhouseCoopers International Limited: Prognose zum Umsatzes der deutschen Offshore-Windenergieindustrie im Jahr 2016. http://www.pwc.de/de/energiewende/

offshore-windenergie-kommt-gewaltig-in-fahrt.jhtml?linktransform=no, 2012. – [Online; Zugriff: 23.09.2014]

[PSE10] Psarros, George ; Skjong, Rolf ; Eide, Magnus S.: Under-reporting of maritime accidents. In: Accident Analysis & Prevention 42 (2010), Nr. 2, S. 619–625

[Rae04] Rae, P. A.; L. A.; Lindsay: A Behaviour-Based Method for Fault Tree Generation. In: Proceedings of the 22nd International System Safety Conference 22 (2004)

[Rae07] Rae, Andrew: Behaviour-Based Methodology for Fault Tree Generation, School of Information Technology and Electrical Engineering, Diss., 2007

[Rau93] Rauzy, Antoine: New algorithms for fault trees analysis. In: Reliability Engineering and System Safety 40 (1993), Nr. 3, S. 203–211

[Ren10] RenewableUK: Guidelines for Onshore and Offshore Wind Farms - Health & Safety in the Wind Energy Industry Sector. London : RenewableUK, 2010

[Ren13] RenewableUK: Guidelines for Onshore and Offshore Wind Farms - Health & Safety in the Wind Energy Industry Sector. London : RenewableUK, 2013

[Rip09] Ripley, B.D.: Stochastic Simulation. Wiley, 2009 (Wiley Series in Probability and Statistics). http://books.google.de/books?id=rmGfsJxRDqgC. – ISBN 9780470317389

[RK13] Richter, Jan ; Korte, Holger: Towards an Implementation for Offshore Operation Simulations. In: Control Applications in Marine Systems Bd. 9, 2013, S. 362–367

[RV87] Roberts, N.H. ; Vesely, W.E.: Fault Tree Handbook. U.S. Government Printing Office, 1987 http://books.google.de/books?id=x9t9qjLFm9sC. – ISBN 9780160055829

[S+02] Stølen, Ketil u. a.: Model-based risk assessment–the CORAS approach. In: 1st iTrust Workshop, 2002

[Sch09] Schaper, Rolf: Baustelle Offshore - Einer der größten Windparks der Welt entsteht nordöstlich von Fehmarn. In: BG BAU (2009), Nr. Ausgabe 4, S. S.6–9

[Sch12] Schmauder, Prof. Dr.-Ing. M.: Fachtagung Arbeitsschutz 2012, TÜV NORD Akademie, Hamburg. http://www.tuev-nord.de/cps/rde/xbcr/tng_de/gefaehrdungsbeurteilung_2.pdf, 2012. – [Online; Zugriff: 21.09.2014]

[Sch13] Schnegelsberg, Sybille: Schutz- und Sicherheitskonzept für Arbeiten an Offshore-Windenergieanlagen, Fachtagung Windenergie 14./15.3.2013 in Rheinsberg, März 2013

[SD14] Shafiee, Mahmood ; Dinmohammadi, Fateme: An FMEA-based risk assessment approach for wind turbine systems: a comparative study of onshore and offshore. In: Energies 7 (2014), Nr. 2, S. 619–642

[Sea14] Seashore: Risk Assessment and Management System. http://www.seashore.de/page/de/produkte/ramsys.php, 2014. – [Online; Zugriff: 14.10.2014]

[SH02] Smith, Shamus P. ; Harrison, Michael D.: Improving hazard classification through the reuse of descriptive arguments. In: Software Reuse: Methods, Techniques, and Tools. Springer, 2002, S. 255–268

[Sin03] Sinnerbrink, Holger: Gefahrenanalyse mittels FMEA. http://www2.cs.uni-paderborn.de/cs/ag-schaefer/Lehre/Lehrveranstaltungen/Seminare/AEIzS/Abgaben/Folien/4_FMEA_HSinnerbrink.pdf, 2003. – [Online; Zugriff: 01.09.2014]

[Slo06] Slovak, Roman: Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs, TU Braunschweig, dissertation, 2006

[SPD99] Snoeck, Monique ; Poels, Geert ; Dedene, Guido: Reusing business models. In: DTEW Research Report 9934 (1999), S. 1–21

[Sta03] Stamatis, D.H.: Failure Mode and Effect Analysis: FMEA from Theory to Execution. ASQ Quality Press, 2003 http://books.google.de/books?id=TTxI8jbTkVwC. – ISBN 9780873895989

[Stä11] Ständer, Tobias: Eine modellbasierte Methode zur Objektivierung der Risikoanalyse nach ISO 26262. 2011

[Sti13] Stiftung Offshore-Windenergie: Kostensenkungspotenziale der Offshore-Windenergie in Deutschland. http://de.statista.com/statistik/studie/id/17163/dokument/potenziale-der-deutschen-offshore-windindustrie-2013/, 2013. – [Online; Zugriff: 23.09.2014]

[Tan14a] Tandem Media: Auditor plus - Die umfassende Software für Arbeits- und Umweltschutz-Management. http://www.tandem-piazza.org/produktreport/73393/

hnc-software-arbeits-und-umweltschutz-management.htm, 2014. – [Online; Zugriff: 04.10.2014]

[Tan14b] Tandem Media: EcoWebDesk - Die praxisnahe Software für Arbeitssicherheit und Umweltmanagement. http://www.tandem-piazza.org/produktreport/73112/ecointense-software-arbeits-und-umweltschutzmanagement.htm, 2014. – [Online; Zugriff: 04.10.2014]

[TC00] Trbojevic, Vladimir M. ; Carr, Barry J.: Risk based methodology for safety improvements in ports. In: Journal of Hazardous Materials 71 (2000), Nr. 1, S. 467–480

[Tho12] Thomsen, K. E.: Offshore Wind: A Comprehensive Guide to Successful Offshore Wind Farm Installation. Amsterdam : Elsevier Science & Technology, 2012

[Thu04] Thums, A.: Formale Fehlerbaumanalyse. 2004 http://books.google.de/books?id=qPFOywAACAAJ

[TLS08] Tajarrod, F ; Latif-Shabgahi, G: A novel methodology for synthesis of fault trees from MATLAB-Simulink model. In: World Academy of Science, Engineering and Technology 41 (2008), S. 630–636

[TTV+14] Tippenhauer, Nils O. ; Temple, William G. ; Vu, An H. ; Chen, Binbin ; Nicol, David M. ; Kalbarczyk, Zbigniew ; Sanders, William H.: Automatic Generation of Security Argument Graphs. In: arXiv preprint arXiv:1405.7475 (2014)

[Uni06] United Nations: Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment. http://unctad.org/en/Docs/sdtetlb20054_en.pdf, 2006. – [Online; Zugriff: 23.09.2014]

[VDF+02] Vesley, Dr W. ; Dugan, Dr J. ; Fragole, J ; Minarik II, J ; Railsback, J: Fault tree handbook with aerospace applications. In: NASA Office of Safety and Mission Assurance, NASA Headquarters, Washington DC 20546 (2002)

[VDI00] VDI Richtlinie: 3633: Simulation von Logistik. In: Materialfluß-und Produktionssystemen, Grundlagen, Beuth (2000)

[VdS14] VdS: Entwurf Offshore Code of Practice. http://www.vds-industrial.de/fileadmin/compliance/3549/VdS_3549_2014-01-29_OCoP_Konsultationsentwurf_2.pdf, 2014

[Vin07] Vinnem, Jan E.: Offshore Risk Assessment. London : Springer Series in Reliability Engineering, 2007

[Vin13] Vinnem, J.E.: Offshore Risk Assessment vol 2.: Principles, Modelling and Applications of QRA Studies. Springer London, 2013 (Springer Series in Reliability Engineering). https://books.google.de/books?id=3N65BAAAQBAJ. – ISBN 9781447152132

[X+10] Xiang, Jianwen u. a.: Automatic static fault tree analysis from system models. In: 2010 IEEE 16th Pacific Rim International Symposium on Dependable Computing, 2010, S. 241–242

[X+11] Xiang, Jianwen u. a.: Automatic synthesis of static fault trees from system models. In: Secure Software Integration and Reliability Improvement (SSIRI), 2011 Fifth International Conference on IEEE, 2011, S. 127–136

[ZK04] Zhang, N ; Kezunovic, M: Verifying the protection system operation using an advanced fault analysis tool combined with the event tree analysis. In: Proc. 2004 36th Annual North American Power Symposium (NAPS2004) Citeseer, 2004, S. 133–139

Anhang

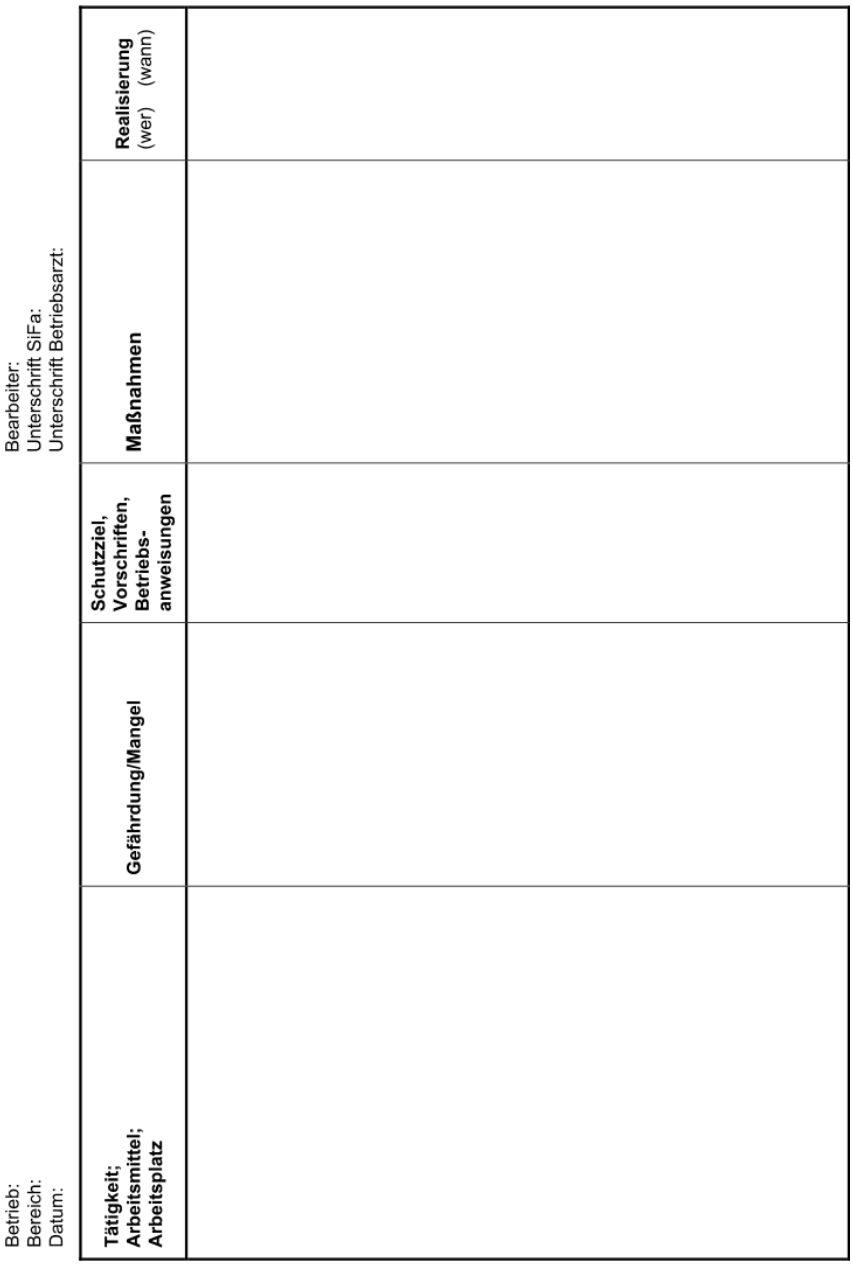

Abbildung 6.1: Exemplarisches Formblatt zur Dokumentation der Gefährdungsbeurteilung nach [Kir04, S. 376]

Activity/SubProcess	Possible Cause	Task
Monitor Tug Activities	Misjudgement of tug positions	Monitor tug position
	Overlooked tug positions	Monitor tug position
	Misjudgement of tug forces	Monitor tug force
	Overlooked tug forces	Monitor tug force
Monitor Environmental Information	Misjudgement of wind	Monitor wind
	Overlooked wind	Monitor wind
	Misjudgement of current	Monitor current
	Overlooked current	Monitor current
Monitor Own Ship Behaviour	Misjudgement of ships speed	Monitor speed
	Overlooked ships speed	Monitor speed
	Misjudgement of ships course	Monitor course
	Overlooked ships course	Monitor course
	Misjudgement of rate of turn	Monitor rate of turn
	Overlooked rate of turn	Monitor rate of turn
	Misjudgement of own position	Monitor position
	Overlooked own position	Monitor position
	Misjudgement of drift effect	Monitor drift
	Overlooked drift effect	Monitor drift
Monitor Distances	Misjudgement of distance to pier	Monitor distance to pier
	Overlooked distance to pier	Monitor distance to pier
	Misjudgement of distance to obstacles	Monitor distance to obstacles
	Overlooked distance to obstacles	Monitor distance to obstacles
Monitor Machine Information	Misjudgement of rudder information	Monitor rudder
	Overlooked rudder information	Monitor rudder
	Misjudgement of thruster information	Monitor thruster
	Overlooked thruster information	Monitor thruster
	Misjudgement of engine situation	Monitor engines
	Overlooked engine situation	Monitor engines
Give Tug Orders	Inappropriate tug position order	Give position order
	Inappropriate tug force order	Give force order
Perform Precision Manoeuvring	Inappropriate ship course order	Give course orders
	Inappropriate ship rudder order	Give rudder orders
	Inappropriate ship engine order	Give engine orders

Abbildung 6.2: Zusammenfassende Tabelle der im Fallbeispiel Lotsenwesen betrachteten Ursachen zur Gefährdung Kollision

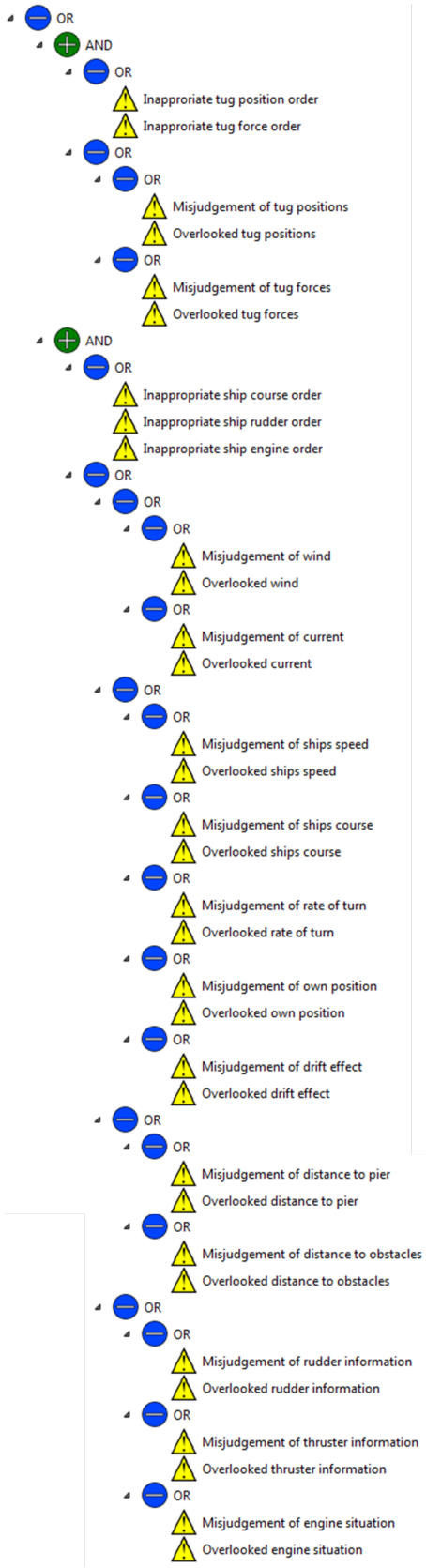

Abbildung 6.3: Aus dem Vorgehen zur Strukturierung mit Hilfe des Structure-guessed Algorithmus resultierende Gesamtstruktur der Gefährdung Kollision für das Fallbeispiel Lotsenwesen

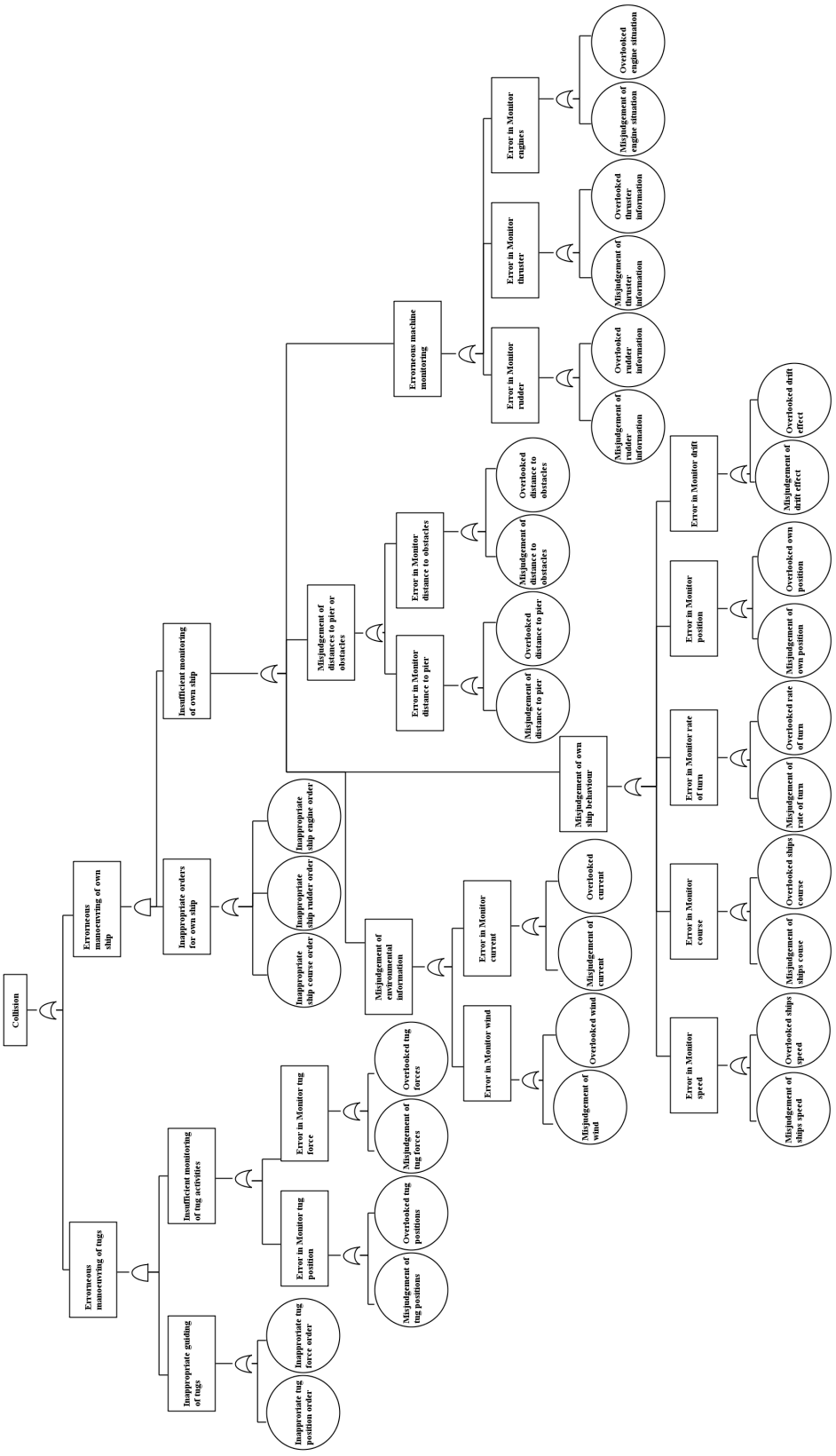

Abbildung 6.4: Resultierender Fehlerbaum der Gefährdung Kollision für das Fallbeispiel Lotsenwesen

1.1 Hazard: Collision

Operational Situation: Manoeuvring in Port Waters

Frequency	1
Severity	4
Risk	4

1.1.1 Exposures

No.	Name	Description
1	Property damages	-
2	Capsizing	-

1.1.2 Causes of Hazard

No.	Name	Freq.	CounterMeasures	Mitigated Freq.
1	Misjudgement of tug positions	4	-	4
2	Overlooked tug positions	4	Position visualization on smart glasses (2)	2
3	Misjudgement of tug forces	4	Numerical force visualization (3)	1
4	Overlooked tug forces	4	Force visualization on smart glasses (3)	1
5	Misjudgement of wind	4	Wind visualization integrated on sea map (3)	1
6	Overlooked wind	3	Wind visualization on smart glasses (2)	1
7	Misjudgement of current	4	Visualization of current on sea map (1)	3
8	Overlooked current	3	Current visualization on smart glasses (0)	3
9	Misjudgement of ships speed	4	Speed visualization integrated on sea map (3)	1
10	Overlooked ships speed	4	Speed visualization on smart glasses (3)	1
11	Misjudgement of ships course	4	Course visualization integr. on sea map (1)	2
12	Overlooked ships course	4	Course visualization on smart glasses (3)	1
13	Misjudgement of rate of turn	4	ROT visualization integrated on sea map (2)	2
14	Overlooked rate of turn	4	ROT visualization on smart glasses (2)	2
15	Misjudgement of own position	4	Pos. visualization + actual outlook (3)	1
16	Overlooked own position	2	Pos. visualization on smart glasses (1)	1
17	Misjudgement of drift effect	4	Wheel effect visualization (2)	2
18	Overlooked drift effect	4	Wheel effect visualizat. on smart glasses (3)	1
19	Misjudgement of distance to pier	3	Dist. visualization integrated on sea map (2)	1
20	Overlooked distance to pier	3	Dist. visualization on smart glasses (2)	1
21	Misjudgement of distance to obstacles	4	Stopping distance visualization (3)	1
22	Overlooked distance to obstacles	3	Stopping dist. vis. on smart glasses (2)	1
23	Misjudgement of rudder information	4	Rudder vis. integrated on sea map (3)	2
24	Overlooked rudder information	4	Rudder visualization on smart glasses (2)	2
25	Misjudgement of thruster information	3	Thruster vis. integrated on sea map (0)	3
26	Overlooked thruster information	4	Thruster visualization on smart glasses (3)	1
27	Misjudgement of engine situation	3	Engine situation indicator integration (1)	2
28	Overlooked engine situation	4	Engine indicator icon on smart glasses (3)	1
29	Inappropriate tug position order	4	Visualizat. of given orders and execution (3)	1
30	Inappropriate tug force order	5	Visualizat. of tugs force, position, towage (4)	1
31	Inappropriate ship course order	4	-	4
32	Inappropriate ship rudder order	4	-	4
33	Inappropriate ship engine order	4	-	4

Abbildung 6.5: Resultierende Dokumentation der Gefährdung Kollision als Auszug der Gesamtdokumentation des Fallbeispiels Lotsenwesen