CARL VON OSSIETZKY universität OLDENBURG

Fakultät II – Informatik, Wirtschafts- und Rechtswissenschaften

Department für Informatik

Modellbasierte Planung zur Unterstützung der Gefährdungsbeurteilung maritimer Operationen

Dissertation zur Erlangung des Grades eines
Doktors der Ingenieurswissenschaften

Vorgelegt von

Rainer Droste, M.Sc.

Gutachter:
Prof. Dr.-Ing. Axel Hahn
Prof. Dr. Daniela Nicklas

Datum der Disputation:
27. Mai 2016

Zusammenfassung

Maritime und vor allem Offshore-Operationen lassen sich in Bezug auf die Beteiligung vieler unterschiedlicher Akteure und Ressourcen als sehr dynamisch und komplex beschreiben. Unter rauen Umweltbedingungen müssen die beteiligten Akteure mit Unsicherheiten und Risiken während der Durchführung zumeist in kooperativen Prozessen umgehen. In dieser Forschungsarbeit wird ein modellbasierter Ansatz für die Planung von maritimen Operationen, z.B. aus der Offshore-Windindustrie, inklusive der Anbindung von Gefahrenbewertungsmethoden für die Risikominderung, vorgestellt.

Ein Prozessmodell ist die Basis, um zunächst die Verfahrensanweisungen der beteiligten Akteure und der genutzten Ressourcen von Operationen ablauforientiert zu beschreiben. Aufbauend auf dieser Beschreibung wird eine operationsspezifische Analyse der Gefahren und Risiken angeschlossen um operationelle Risiken aufzudecken.

Die prozessorientierte Methodik für die Planung und Analyse maritimer Operationen wird softwareseitig durch eine prototypische Implementierung unterstützt. Dieser Ansatz wird mittels repräsentativer Offshore-Szenarien in Kooperation mit Experten aus der Offshore-Windindustrie in zwei Fallstudien evaluiert und dessen Anwendbarkeit demonstriert.

Abstract

Maritime and especially offshore operations can be described as very dynamic and complex, since the participation of various actors and resources is involved. Under harsh environmental conditions, actors have to deal in cooperative processes with uncertainties and risks during the operation. In this research work a model-based approach will be presented for the planning of maritime operations, e.g. from the off-shore wind industry, including the integration of risk assessment methods for risk reduction.

A conceptual process model is the basis for the description of process-oriented working procedures of the personnel and the used resources. Based on this description, a method for operation-specific analysis of the hazards and failures for operational risks will be introduced.

A prototype supports the process-oriented methodology for planning and analysis of maritime operations. The application of the approach is demonstrated in two case studies and is evaluated in cooperation with experts from the offshore wind domain.

Inhaltsverzeichnis

Verzeichnis der Abkürzungen und Akronyme

ArbSchG	Arbeitsschutzgesetz
AWZ	Ausschließlichen Wirtschaftszone
ARIS	Architektur integrierter Informationssysteme
BAuA	Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
BNatSchG	Bundesnaturschutzgesetz
BPEL	Business Process Execution Language
BPEL4WS	Business Process Execution Language for Web Services
BPML	Business Process Modeling Language
BPMN	Business Process Modeling Notation
BPMN 2.0	Business Process Modelling and Notation
BSH	Bundesamt für Seeschifffahrt und Hydrographie
DIN	Deutsche Institut für Normung e. V.
DistriCT	Distributed Controlling Toolkit
DNV	Det Norske Veritas
ECFA	Events und Causal Analysis
ECFA+	Events and Conditional Factors Analysis
EFRE	Europäischen Fonds für regionale Entwicklung
EnWG	Energiewirtschaftsgesetz
EMF	Eclipse Modeling Framework
EMod	Environment Modeler
(e)EPK	(erweiterte) Ereignisgesteuerte Prozessketten
ESA	European Space Agency
ETA	Event Tree Analysis
FMEA	Failure Mode and Effects Analysis
FT	Fault Tree
FTA	Fault Tree Analysis
GDV	Gesamtverband der Deutschen Versicherungswirtschaft e.V.
GEF	Graphical Editing Framework
GL	Germanischer Lloyd
HAGGIS	Hybrid Architecture for Granularly, Generic and Interoperable Simulations
HAZOP	Hazard and Operability Study
HLA	High Level Architecture
HSE	Health, Safety, and Environment
HSSE	Health, Safety, Security and Environment
IDEF	Integrated Definition

IEC	International Electrotechnical Commission
IMCA	International Marine Contractors Association
ISO	Internationale Organisation für Normung
MES	Multilinear Events Sequencing
MOPhisTo	Maritime Operation Planning Tool
MTO	Man, Technology and Organisation
MTS	Maritime Traffic Simulation
NOGEPA	Netherlands Oil and Gas Exploration and Production Association
OCoP	Offshore Code of Practice
ODF	Operations Data File
OHSAS	Occupational Health and Safety Assessment Series
OMG	Object Management Group
PAAG	Prognose, Auffinden der Ursache, Abschätzen der Auswirkungen, Gegenmaßnahmen
PSA	Persönliche Schutzausrüstung
PWS	Physical World Simulation
ROPE	Risk-Oriented Process Evaluation
RTI	Run-Time Infrastructure
SeeAnlV	Seeanlagenverordnung
SOOP	Forschungsverbund "Sicher Offshore Operationen"
SRÜ	Seerechtsübereinkommens der Vereinten Nationen
STEP	Sequentially Timed Events Plotting Procedure
UML	Unified Modeling Language
WEA	Windenergieanlage
WSV	Wasser- und Schifffahrtsverwaltung des Bundes
XML	Extensible Markup Language

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Momentan zeichnen sich die Prozesse für die Planung, Realisierung und Wartung von Offshore-Windenergie-Operationen durch einen niedrigen Standardisierungsgrad in Deutschland und weiteren europäischen Ländern aus. Mit "nur" 12 Jahren Erfahrung in der kommerziellen Errichtung von Offshore-Windparks ist die Branche noch weit von etablierten internationalen Standards und Verfahren entfernt [Th12]. Der durchschnittliche Zeitaufwand für die Beantragung und die Genehmigung für Offshore-Windparks kann sich von fünf bis zu sieben Jahren hinziehen, je nach Reglement der verschiedenen EU-Mitgliedstaaten [Th12]. Ein wesentlicher Bestandteil für die Genehmigung eines solchen Bauvorhabens ist dabei der Management-Plan bezüglich der Gesundheits-, Sicherheits- und Umweltaspekte (englisch: Health, Safety, and Environment, kurz HSE), um sichere Arbeitsumgebungen für die Arbeitsplätze zu gewährleisten [Ge14]. Initial erstellte, generische Pläne für die Baugenehmigung müssen durch projektspezifische Pläne, Verfahren und Arbeitsanweisungen konkretisiert werden. Dieser Vorgang bringt weitere erforderliche standort-spezifische Analysen und ausführliche technische Beschreibung der Arbeitsabläufe mit sich, um Risikokontroll- und Überwachungsmaßnahmen für verbesserte Betriebssicherheit formulieren zu können. Bedingt durch fehlende Vorgaben der Genehmigungsbehörden für Offshore-Windparks hat sich in der Praxis die Verwendung des Vorgehens des Risikomanagementprozesses etabliert. Nach ISO 31000 ist ein Risikomanagementprozess "die systematische Erfassung und Bewertung von Risiken, sowie die Steuerung von Reaktionen auf festgestellte Risiken. (…) Risikomanagement ist ein systematisches Verfahren, das zur Steuerung aller Risiken in einem Unternehmen angewendet werden kann – zum Beispiel bei Unternehmensrisiken, Kreditrisiken, Finanzanlagenrisiken, Umweltrisiken, versicherungstechnischen Risiken und/oder technischen Risiken" [De11b]. Neben dem wesentlichen Aspekt der Projektorganisation und einem kontinuierlichen Prozess der Identifizierung, Analyse und Bewertung von Risiken ist der HSE-Plan somit ebenfalls ein wichtiges Instrument hinsichtlich der Finanzierung und Absicherung der Offshore Windparks.

1.1 Motivation und Problemstellung

Die Genehmigung für die Errichtung eines Offshore-Windparks erfordert im Wesentlichen die Erstellung eines HSE-Plans, welcher Aspekte bezüglich der Gesundheit, Sicherheit und der Umwelt abdeckt [Th12]. Dies dient ebenfalls der Verbesserung der Sicherheit am Arbeitsplatz und dem Verständnis der Betreibergesellschaft und deren Subunternehmen bezüglich des Umweltschutzes. Die Anforderungen an HSE-Pläne für Offshore-Operationen resultieren aus den nationalen Richtlinien und Vorschriften des Landes in dem die Arbeiten durchgeführt werden. In Deutschland ist für die Genehmigung für neue Windparks und somit auch für die Abnahme

der Sicherheitskonzepte das Bundesamt für Seeschifffahrt und Hydrographie (BSH) zuständig. "Ein Standard existiert derzeit noch nicht, so dass Einzel- und Individualprüfungen notwendig sind" [Bu14b]. Ebenso komplex wie das Genehmigungsverfahren gestaltet sich die Finanzierung solcher Projekte. So resultieren die größten Kosteneinsparungen aus der Minderung der Investitionskosten. In der Branche ist eine Mischfinanzierung aus Eigen- und Fremdkapital üblich. So führen geringere "Marktmargen aufgrund der günstigeren Risikobewertung von Offshore-Projekten im Bereich der Fremdfinanzierung" neben sinkenden projektspezifischen Risiken, die für geringere Risikoaufschläge in der Eigenkapitalfinanzierung sorgen, zu einer möglichen Reduktion von Investitionskosten [St13]. Da keine spezifischen Vorgaben für die Entwicklung und den Inhalt vorliegen, werden internationale Richtlinien für das HSE-Management aus artverwandten Branchen wie der Offshore-Öl- und Gasindustrie [Th10b], [E&94] und Standards wie die ISO 9001 (Qualitätsmanagement), die ISO 14001 für Umweltmanagement oder die OHSAS 18001 [BS00] als Grundlage für diese Forschungsarbeit herangezogen. Neben diesen häufig verwendeten Standards werden weitere operationsspezifische Richtlinien, wie beispielsweise von der NOGEPA [Th11] für Helikopterdeckoperationen oder von der IMCA hinsichtlich des dynamischen Positionierens von Schiffen [Th05] und Verladeoperationen, ausgewertet. Ebenso werden Guidelines in die Recherche einbezogen, wie beispielsweise ein Leitfaden vom Germanischen Lloyd (GL) [Ge02], der ein Verfahren zur qualitativen und quantitativen Risikobewertung für Windparks spezifiziert. In den zu Deutschland gehörenden Meeresnutzungsflächen müssen hierbei folgende Richtlinien als Grundvoraussetzung für die Errichtung von Offshore-Windparks berücksichtigt werden: die Seeanlagenverordnung (SeeAnlV) und das Bundesnaturschutzgesetz (BNatSchG) betreffend des Standortes und der Gründungsstrukturen, sowie der Art der Windenergieanlagen des Offshore-Windparks und das Energiewirtschaftsgesetz (EnWG) bezüglich der Voraussetzungen für die Netzanbindung.

In Deutschland ist die Zuständigkeit für das Genehmigungsverfahren danach getrennt, ob der Windpark im Künstenmeer (bis zwölf Seemeilen; Hoheitsgebiet im Zuständigkeitsbereich des jeweiligen Bundeslandes) oder aber in der ausschließlichen Wirtschaftszone (AWZ) bis 200 Seemeilen und kein Hoheitsgebiet, sondern internationales Gewässer nach internationalen Seerechtsübereinkommens der Vereinten Nationen (SRÜ) verortet ist [Bu14b]. Die Nutzung der Offshore-Windenergie findet in deutschen Gewässern vornehmlich außerhalb der 12-Seemeilen-Zone in der AWZ statt. Da jedoch die Netzanbindung durch das Küstenmeer an die Landanbindung führt, müssen auch für diesen Bereich entsprechende Genehmigungen eingeholt werden. Die Prüfung und Genehmigung für die Errichtung von Offshore-Windparks innerhalb der AWZ obliegt dem BSH unter Hinzuziehung von Fachexpertise der Wasser- und Schifffahrtsverwaltung des Bundes (WSV) und den jeweiligen Landesarbeitsschutzbehörden

der entsprechenden Bundesländer. Neben der Überprüfung hinsichtlich der internationalen Seeschifffahrtswege bzw. Einschränkung dieser Genehmigungsphase, wird primär eine Umweltverträglichkeitsprüfung durchgeführt [ZDN05]. Zusammen mit der Erteilung der Genehmigung werden weitere Auflagen, die vor Baubeginn und Betrieb der Anlagen erfüllt sein müssen, gestellt. Ein wichtiger Teilaspekt ist hierbei, neben dem primären Fokus auf die Umwelt und die Seeschifffahrt, die Vorlage eines Schutz- und Sicherheitskonzeptes für die Sicherheit am Arbeitsplatz für das durchführende Personal. Das Konzept umfasst dabei die Teilaspekte Sicherheitsmanagementsystem und Sicherheitshandbuch mit Verfahrensanweisungen und Notfallplänen [Bu14b]. "Die Schutz- und Sicherheitskonzepte variieren im Umfang und Detaillierungsgrad. Ein Standard existiert derzeit noch nicht" [Bu14b], jedoch haben sich in der Praxis grundlegende Inhalte etabliert [Sc13], [va13].

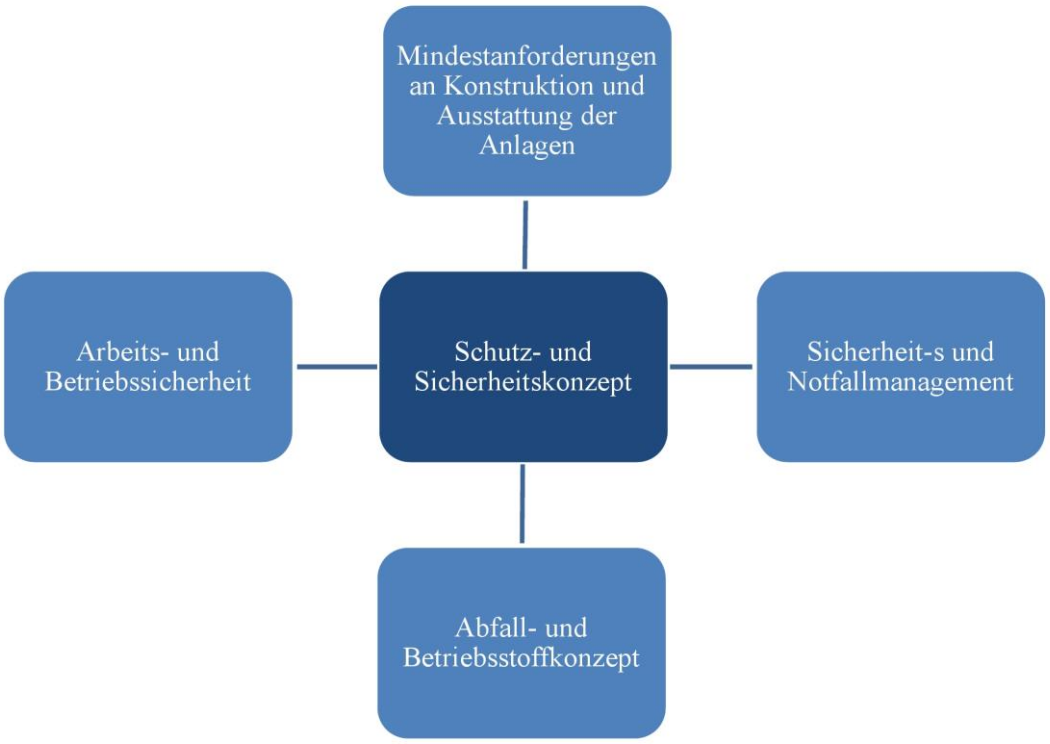


Abbildung 1: Bestandteile des Schutz- und Sicherheitskonzeptes

Abbildung 1 gibt einen Überblick über die in der Praxis üblichen Bestandteile eines Schutz- und Sicherheitskonzeptes in der maritimen Offshore-Wind Domäne. Unter den Bereich der Mindestanforderungen an Konstruktion und Ausstattung der Anlagen fällt beispielsweise das Kennzeichnungskonzept (z.B. Farbgebung der Rotorblätter) für Schiff- und Luftfahrt oder auch das Befeuerungskonzept (z.B. Beleuchtung der WEA). Die Anlagen müssen dabei nach dem aktuellen Stand der Technik ausgestattet sein, sodass die Sicherheit des Schiffs- und Luftverkehrs gewährleistet ist [Bu10], [Bu14a]. Das Sicherheits- und Notfallmanagementsystem

beinhaltet "Methoden und Verfahren zur Gewährleistung der Anlagen-, Arbeits- und Infrastruktursicherheit im Regelbetrieb (Sicherheitsmanagement) sowie Alarm- und Gefahrenabwehrplanungen zum geordneten Umgang mit Krisensituationen (Notfallmanagement)" [Bu10]. Ein weiterer Bestandteil ist das Abfallwirtschafts- und Betriebsstoffkonzept. Danach ist "ein Konzept zur umfassenden und vollständigen Darstellung des Umgangs mit Abfall und Betriebsstoffen bei Bau und Betrieb (…) sechs Monate vor dem geplanten Beginn der Errichtung (…)" vorzulegen [Bu10], [Bu14a]. Der für diese Forschungsarbeit wesentliche Aspekt ist das Konzept zur Arbeits- und Betriebssicherheit.

Es ist ein wichtiger Bestandteil des Schutz- und Sicherheitskonzeptes, das laut Nebenbestimmung Nr. 9 die Arbeitssicherheit bei Errichtung, Betrieb sowie Rückbau von Bau-, Wartungs- und Bedienpersonal gewährleisten soll. Somit soll eine "Gefährdung für Leben und Gesundheit möglichst vermieden und die verbleibende Gefährdung möglichst gering gehalten werden. Bei den Maßnahmen sind der Stand der Technik, Arbeitsmedizin und Hygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse zu berücksichtigen" [Bu10]. Der Schutz des menschlichen Lebens ist von großem öffentlichem Interesse und deshalb seit 2008 Gegenstand der Genehmigung für Offshore-Windparks. Gemäß § 1 Abs. 1 Arbeitsschutzgesetz (ArbSchG) und im Rahmen des Seerechtsübereinkommens findet das Arbeitsschutzgesetz als einziges deutsches Recht in der AWZ Anwendung und gilt somit auch für Offshore-Windenergieanlagen. Dieses wurde entsprechend der Vorgaben der Europäischen Union (nationale Umsetzung der EG-Rahmenrichtlinie 89/391/EWG von 1989) als eine umfassende Rechtsgrundlage geschaffen [GKM13]. Laut den §§ 3,4,5 und 5 ist jeder Arbeitgeber verpflichtet eine "Beurteilung der Arbeitsbedingungen hinsichtlich möglicher Gefährdungen" durchzuführen [Ba13].

1.2 Zieldefinition

Ein in dieser Forschungsarbeit zu entwickelnder Modellierungsansatz hat den Anspruch genau diese Problematik der Erstellung von Gefährdungsbeurteilungen zu lösen. Der Ansatz für die Modellentwicklung zielt darauf hin alle für eine Gefährdungsbeurteilung benötigten Informationen in einem integrierten Modell nach [So12a] zu beschreiben. Es ermöglicht das systematische Beschreiben der Tätigkeiten innerhalb der Prozesse in einer bestimmten Reihenfolge sowie die Zuordnung der beteiligten Akteure, ihre jeweiligen Rollen und die genutzten Ressourcen während einer Operation. Durch die Erweiterung mit Umweltbedingungen, wie z.B. zu hohen Windgeschwindigkeiten, können die Prozesse mit möglichen Gefahren in Beziehung gesetzt werden. Es wird auf eine einfach verständliche Notation zurückgegriffen, die es Domänenexperten (aus dem nautischen Umfeld) ermöglicht, ohne aufwendige Schulung komplexe Szenarien einschließlich der physischen Umwelt und dynamischen Verhaltens zu be-

schreiben. Die hieraus resultierende formale Abbildung von Offshore-Operationen kann in einem weiteren Schritt bezüglich der Gefahren bewertet werden [Dr12], [LBP12]; Die auf Basis des integrierten Modells entstehenden Planungswerkzeuge dienen somit der Unterstützung für Offshore-Domain-Experten bei der Entwicklung der HSE-Pläne für das maritime Umfeld. Es ermöglicht eine detaillierte Planung relevanter Offshore-Manöver und eine Bewertung von Risikosituationen.

Im Systems Engineering wird die Modellbildung eingesetzt, um die System-Umwelt und deren Beziehungsstruktur zu erkennen, die Systeme, deren Bestandteile und dessen Funktionieren zu verstehen und dessen Komplexität beherrschbar zu machen. Unter einem Modell ist eine idealisierte, vereinfachte in gewisser Hinsicht ähnliche Darstellung eines Gegenstands, Systems oder sonstigen Weltausschnitts zu verstehen mit dem Ziel bestimmte Eigenschaften des Vorbilds besser analysieren zu können [He94]. Auch in der (Wirtschafts-) Informatik hat sich die Modellierung als zentrales Instrument zur Beschreibung und Gestaltung von geschäftsbezogenen Arbeiten etabliert [Be95], [WW02].

Ein Modell ist ein System, welches ein anderes System zielorientiert abbildet und dabei eine struktur- und verhaltenstreue Abbildung realisiert [FS13]. Es soll zu einer richtigen aber vereinfachenden und anschaulichen Abbildung eines Wirklichkeitsausschnitts führen und dabei die Prinzipien wie eine schrittweise Verfeinerung, Modularisierung oder Wiederverwendbarkeit berücksichtigen. Modellbeschreibungssprachen schaffen die notwendige Präzision und helfen, Eindeutigkeiten zu schaffen und Missverständnisse zu vermeiden, wie sie bei natürlich-sprachlicher Formulierung auftreten können. In der Wissenschaft und Praxis sind verschiedene Modellierungssprachen entstanden, welche sich konkret mit der Planung, Kontrolle und Steuerung von Geschäftsprozessen, der "zusammengehörige[n] Abfolge[n] von zeitlich und sachlogisch gegliederten Funktionen zum Zwecke einer Leistungserstellung" [FSV05], befassen. Die Formalziele dieser sind z. B. Konstruktionsadäquanz, Wirtschaftlichkeit, systematischer Aufbau, Klarheit oder Vergleichbarkeit. Je nach Modellierungs- und Untersuchungsziel werden die als relevant betrachteten Ausschnitte der Realität im Modell repräsentiert. Dies führt häufig dazu, dass die Abgrenzung zu eng erfolgt und somit der Umwelt realer Systeme, die häufig nicht zu vernachlässigende Einflussfaktoren beinhalten, ein zu geringer Stellenwert beigemessen wird. Beispiele für Modellierungssprachen sind Ereignisgesteuerte Prozessketten (EPK) oder die Business Process Modelling and Notation (BPMN 2.0). Beide bilden Abläufe ähnlich wie Petri-Netze ab mit dem Unterschied, dass die zeitlich und sachlogische gegliederte Abfolge eine Integration weiterer Sichten ermöglicht wird, wie z.B. die Zuweisung von Daten und der Zuordnung der Operationen oder Aktivitäten zu verantwortlichen Elementen (insbesondere Organisationseinheiten). Dabei ist es ebenfalls möglich Kon-

textinformationen zu berücksichtigen. Diese Informationen werden jedoch über textuelle Annotationen eingefügt und werden dadurch weder als Teil der Modellierungsmethodik berücksichtigt, noch aus dem Prozessmodell heraus für eine spätere Analyse nutzbar [WF10].

Auch die ISO empfiehlt in ihrer Normenreihe ISO 9000 ff, welche die Grundsätze für Maßnahmen zum Qualitätsmanagement dokumentiert, die Anwendung eines Konzept basierend auf einem prozessorientierten Ansatz für Managementsysteme, unabhängig von Art oder Größe der Organisation. Dies schließt unter anderem Managementsysteme wie Umwelt (ISO 14000 Familie), Geschäftsrisiko, soziale Verantwortung, Arbeitsschutz und Arbeitssicherheit ein. Dabei werden folgende Vorteile des prozessorientierten Ansatzes genannt [De11c]:

- Abstimmung und Ausrichtung von Prozessen, um die Erreichung beabsichtigter Ergebnisse zu ermöglichen
- Fähigkeit zur Fokussierung der Anstrengungen auf Prozesswirksamkeit und -effizienz
- Kunden oder anderen interessierten Parteien Vertrauen in die beständige Leistung der Organisation zu geben
- Transparenz der Arbeitsabläufe innerhalb der Organisation
- geringere Kosten und Verkürzung der Durchlaufzeiten durch den wirksamen Einsatz der Ressourcen
- verbesserte, beständige und vorhersehbare Ergebnisse
- Schaffung von Möglichkeiten für gezielte und priorisierte Verbesserungsinitiativen;
- Ermutigung der Beteiligung von Personen und die Klarstellung ihrer Verantwortung

Da aufbauend auf dieser Beschreibung eine projekt- und operationsspezifische Analyse der Gefahren und Risiken durchgeführt werden muss, ist es jedoch unumgänglich das gesamte System, demnach alle enthaltenen Objekte samt deren Fähigkeiten, Anfälligkeiten und (physikalischen) Wechselwirkungen untereinander, zu betrachten. Folgende Zielstellung lässt sich für diese Forschungsarbeit herleiten:

Gestaltung und Evaluation einer prozessmodellbasierten Planung kooperativer soziotechnischer Systeme zur Unterstützung der Risikoanalyse und –Bewertung als Bestandteile der Gefährdungsbeurteilung

Im Rahmen dieser Forschungsarbeit wird neben einem durchgängigen Ansatz für die Erstellung von Arbeitsschutz- und Sicherheitskonzepten für die maritime Domäne das Modellierungswerkzeug MOPhisTo (Maritime Operation Planning Tool) entwickelt. MOPhisTo adaptiert und integriert verschiedene prozessorientierte Modelle und Methoden aus unterschiedlichen Domänen, z.B. der Luft- und Raumfahrt, der Automobilindustrie und den Disziplinen

der Informatik, um diese für die Beschreibung kooperativer soziotechnischer Systeme im maritimen Sektor zu übertragen. Als Grundlage für MOPhisTo wird eine Methodik entwickelt, welche es den HSE-Managern ermöglichen soll die Prozesse für die Errichtung, Wartung und Instandhaltung von Offshore-Windparks zu planen und die Gefahrenbewertung für diese durchführen zu können. Dabei sollen projektspezifische Anforderungen wie Standort, eingesetzte Ressourcen und Personal in den Analyseprozess einbezogen werden. Die genannte Zielstellung lässt sich in folgende Teilziele aufschlüsseln:

Z1 *Prozessorientierte Systembeschreibung:* Ausgangspunkt einer jeden Erstellung eines Sicherheitskonzeptes ist die Beschreibung des Systems auf dessen Basis diese durchgeführt werden soll. Es ist eine statische Beschreibung aller Elemente die innerhalb eines konkreten Sicherheitskonzeptes referenziert werden. Durch die Beschreibung von normativen Abläufen einzelner Offshore-Operationen ist eine prozessorientierte Risikobewertung möglich. Das Konzept soll dabei Aspekte zu personenbezogenen Beschreibung von Tätigkeiten in einer sequenziellen Abfolge, die Möglichkeit der Synchronisation und des Informationsaustausches durch Kommunikation enthalten. [Sc13], [Ad12], [Ba13], [Bu96] , [Ge14], [IS15], [PS13].

Z2 *Konzept für die Identifizierung von Gefahren*: Für einzelne Arbeitsschritte müssen in Abhängigkeit zu den spezifischen Anforderungen Gefährdungen und deren Ursachen identifiziert werden, um im Anschluss den Experten die Bewertung der Wahrscheinlichkeit des Eintritts einer Gefährdung, sowie dessen potenziellen Schadensausmaßes zu ermöglichen. [Ad12], [Ba13], [Ge14], [Pi15], [IS15]

Z3 *Quantitative und qualitative Beurteilung der Gefahren*: Eine häufig zum Einsatz kommende und für diese Arbeit relevante Methode ist die Identifikation und Analyse von Risiken per Simulationsverfahren. Bei dieser können durch zwei grundlegenden Verfahren für eine simulationsgestützte Risikoanalyse, der Sensitivitäts- bzw. der Szenarioanalyse, Aussagen über die Auswirkung von Eingangsparametern und deren Zusammenhang bezüglich potenzieller Gefahren getroffen werden. Um eine Identifikation und Analyse von Risiken per Simulationsverfahren zu ermöglichen, muss die Ausführbarkeit der Prozesse gegeben sein. [Go16], [Vi07], [De02], [Ga99], [IS15]

Für die Bewertung der Eintrittswahrscheinlichkeit möglicher Gefahren, einschließlich von unwahrscheinlichen, dennoch existierenden Störfällen, wird eine über die deterministische Betrachtungsweise hinausgehende, quantitative Risikoanalyse eingesetzt. Bei diesen werden die Elemente der Risikogleichung über ein Ranking, Indikatoren oder eine Gewichtungen miteinander kombiniert bzw. ein Risiko rechne-

risch ermittelt. Ein Ziel der modellbasierten Methodik ist es Methoden der Gefährdungsbeurteilungen zu ermöglichen. [Vi07], [Pi15], [IS15] Die Integration von Schutzmaßnahmen zur Minderung der Eintrittswahrscheinlichkeit bzw. das Begrenzen des Schadensausmaßes und eine zugehörige Abschätzung der Wirkung auf diese in die prozessorientierte Bewertungsmethodik müssen möglich sein. [Ge14], [Pi15], [IS15]

Z4 *Durchgängige, integrierte Methodik:* Für die Offshore-Domäne existiert bisher keine vorgeschriebene Methodik für Gefährdungsbeurteilungen. Deshalb sich in diesem Sektor eine Durchführung ähnlich einer Risikoanalyse etabliert. Diese wird angewandt, wenn es sich um ein wirtschaftliches Risiko handelt oder um eines, welches die Umwelt gefährdet (z.B. Kollisionsrisiken etc.). Zudem unterscheidet sich das Vorgehen von der Handhabung in den jeweiligen Unternehmen. So werden beispielsweise häufig nur Vorlagen mit teilweise vorgefertigten Textbausteinen genutzt oder welche, die Bestandteil von Managementsystemen für andere Bereiche darstellen.

Die Erstellung der Gefährdungsbeurteilungen erfolgt meistens in Teamarbeit, bei der die inhaltlichen Schwerpunkte auf die Experten aus den verschiedenen Bereichen verteilt werden. Dabei ist eine enge Kommunikation notwendig, da besonders bei Änderungen stets überprüft werden muss, ob dies Auswirkungen auf andere Bestandteile nach sich zieht. Dies wird dadurch erschwert, dass diese zumeist mit verschiedenen Werkzeugen erzeugt werden. [Sc14], [Hi14], [SW14], [Be14]

Z5 *Werkzeugunterstützung*: Das manuelle Erstellen der Planungs- und Risikodokumentation erfordert einen enormen Zeitaufwand. Interviews zufolge werden jährlich mehrere Wochen alleine für dieses Aufgabenpaket innerhalb von Unternehmen aufgewandt. Die Bewertung liegt zumeist in tabellarischer/textueller Form vor, was eine Wiederverwendung erschwert. [WJ06], [Le14], [Wa01], [Ke07]

1.3 Struktur der Arbeit

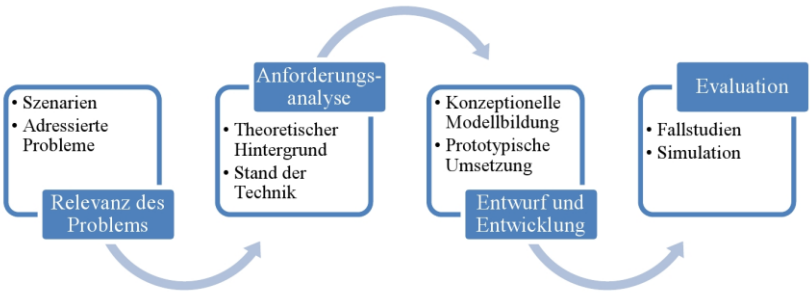


Abbildung 2: Vorgehensmodell der Forschungsarbeit

Die in Abbildung 2 dargestellten Vorgehensschritte definieren die Methode des Forschungsansatzes dieser Arbeit, abgeleitet aus verschiedenen Frameworks und idealisierten Vorgehensmodellen für Designforschungsansätze. [He06], [Pe07]

Dem Vorgehen entsprechend gliedert sich der Aufbau dieser Arbeit grob in vier Kapitel (Abbildung 3): Beginnend wird im ersten Kapitel zunächst der Forschungsgegenstand motiviert und das Problem eingeleitet. Aus diesem abgeleitet folgen das Ziel und der Forschungsbeitrag der Arbeit.

Kapitel 2 befasst sich einleitend mit dem relevanten Stand der Wissenschaft und Technik. Es ist unterteilt in eine Einführung über die bisherigen Verfahren hinsichtlich der Planung und Analyse maritimer Operationen, einen Überblick über Techniken der Prozessmodellierung und darauf aufbauend Verfahren für prozessorientierte Gefährdungsbeurteilungen. Dabei werden die verschiedenen Techniken und Methoden jeweils hinsichtlich ihrer Eignung bzw. ihres möglichen Beitrags für diese Arbeit hin überprüft. Abgeleitet aus der Zielabdeckung wird abschließend in diesem Kapitel der Handlungsbedarf dargestellt.

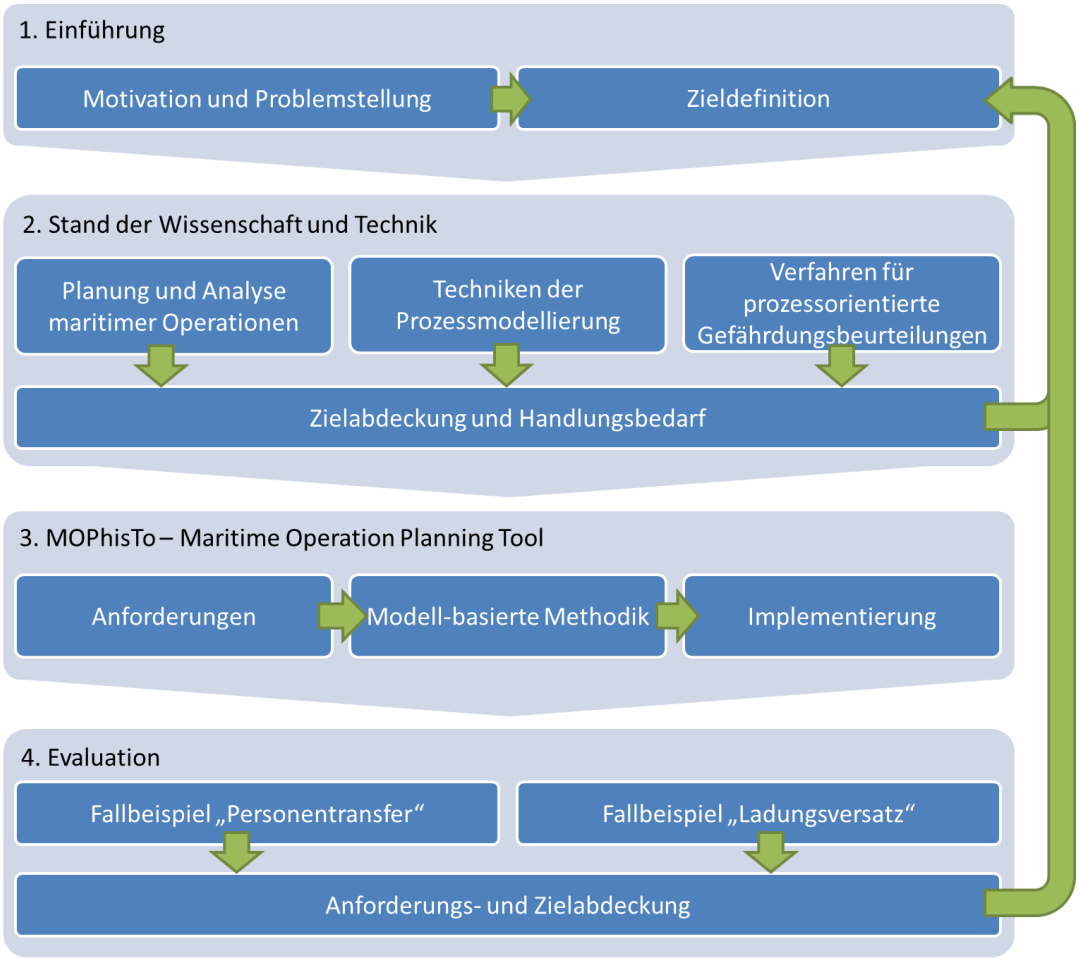


Abbildung 3: Aufbau der Arbeit

Letzteres dient der Anforderungserhebung, dem ersten Abschnitt aus Kapitel 3. Der zweite Abschnitt in Kapitel 3 beschreibt im Detail die modellbasierte Methodik für die Planung und Analyse von Offshore-Operationen. Abgeschlossen wird das Kapitel mit der Darstellung der prototypische Implementierung "MOPhisTo" für die Unterstützung der vorgestellten modellbasierten Methodik.

Mit Hilfe dieser wird die Evaluation in Kapitel 4 durchgeführt. Die zwei selektierten Fallbeispiele "Personentransfer" und "Ladungsversatz" dienen der Überprüfung der Zielerfüllung bzw. Anforderungsabdeckung, der Demonstration der Anwendbarkeit und der Validierung der modellbasierten Methodik.

2 Stand der Wissenschaft und Technik

In diesem Kapitel wird der Stand der Wissenschaft und Technik untersucht. Zunächst wird ein Überblick über die Methoden der Gefährdungsbeurteilung gegeben, welche im deutschen Raum zu tragen kommen. Ergänzt wird Abschnitt 2.1 mit einer Übersicht über identifizierte Techniken der Gefährdungsbeurteilung. Schwerpunkt hierbei sind Werkzeuge und Methoden aus der maritimen Transportwirtschaft, sowie der Offshore-Öl- und Gasindustrie. Zudem wird auf artverwandte Domänen, wie die Luft- und Raumfahrt und die Automobilindustrie, eingegangen. Wie bereits aus Kapitel 1 hervorgeht, haben sich in diesem Sektor prozessorientierte Methoden für eine strukturierte Beschreibung von Systemen durchgesetzt. Dementsprechend widmet sich Abschnitt 2.2 den Techniken der Prozessmodellierung, wobei dort der Schwerpunkt auf verschiedenen Modellierungsansätzen liegt. Dem angeschlossen wird in Abschnitt 2.3 auf Verfahren für prozessorientierte Gefährdungsbeurteilung eingegangen. Das Ziel dieses Kapitels ist neben der Überprüfung hinsichtlich der Abdeckung der in Kapitel 1 vorgestellten Ziele eine Analyse in wie weit diese vorgestellten Ansätze hinsichtlich der Zielerreichung dieser Forschungsarbeit adaptiert bzw. integriert werden können.

2.1 Planung und Analyse maritimer Operationen

Der erste Schritt einer Gefährdungsbeurteilung ist üblicherweise die Definition und Beschreibung des zu betrachtenden Systems. Dieser Schritt ist von entsprechender Bedeutung, da diese Systembeschreibung die Basis der gesamten Risikoanalyse bildet [Kr13]. Eine genaue Systembeschreibung unterstützt dabei nicht nur den Domänenexperten bei der Durchführung der Analyse, sondern vor allem die Personen, die diese im Späteren überprüfen bzw. evaluieren sollen [Vi07]. Dabei sollte eine Systembeschreibung folgende Aspekte beinhalten:

- Beschreibung von technischen Systemen, relevanten Arbeitsschritten und die Betriebsphasen
- Der Zeitraum, auf den sich die Analyse bezieht
- Eine Aufschlüsselung der Personalgruppen, der äußeren Umgebung und den Vermögenswerten, auf die sich die Risikobeurteilung bezieht
- Die Eigenschaften des Systems in Bezug auf die Leistungsfähigkeit Fehler zu tolerieren und der Anfälligkeit für zufällig auftretende Effekte

Der Zweck der Systembeschreibung ist die Analyse ausreichend transparent zu gestalten, so dass andere Personen in der Lage sind diese zu überprüfen und zu beurteilen. Diese Aussagen decken sich mit der im Automotive stark verankerten Definition der ISO Norm für sicherheitsrelevante elektrischer/elektronischer Systeme, nach der in Kraftfahrzeugen zu betrachtenden

Gegenstand als System, eine Anordnung von Systemen oder eine einzelne Funktion verstanden wird [In08]. Die Methoden aus der Praxis werden aus zwei verschiedenen Datenquellen abgeleitet. Neben einer durchgeführten Umfrage, an der sich Service- und Logistikunternehmen sowie Anlagenherstellern ebenfalls Beratungs- und Zertifizierungsdienstleister beteiligt haben, wurde zudem auf eine Reihe von Interviews zurückgegriffen, welche im direkten Gespräch mit Projektpartnern durchgeführt wurden. Eine weitere Quelle sind bereitgestellte Dokumente, welche konkret für die Genehmigungsverfahren für Offshore-Windparks erstellt wurden. In der Praxis werden die Ausarbeitungen hinsichtlich eines Betrachtungsgegenstandes in zwei Aspekte unterteilt: die Beschreibung der Arbeitsabläufe (auch Prozeduren oder Verfahrensanweisungen genannt) und die Risikobewertung dieser. Je nach Unternehmen werden diese Beiden unterschiedlich detailliert ausgeführt, haben jedoch die Gemeinsamkeit, dass diese entweder mit Microsoft Word oder aber mit Microsoft Excel erstellt werden. Bei letzterem sollte hinzugefügt werden, dass dies jedoch nur in Form einer simplen Tabellennutzung erfolgt, also keine besonderen Funktionalitäten genutzt werden, welche eine Tabellenkalkulationssoftware mit sich bringt. Es handelt sich demnach lediglich um unstrukturierte Daten, welche entweder als Fließtext oder aber in Tabellenform dargestellt werden. Da es sich bei diesen um nicht-formale Systembeschreibung handelt, sind diese nach Vinnem nicht geeignet [Vi07].

2.1.1 Methoden der Gefährdungsbeurteilung

Gefährdungsbeurteilungen können je nach Zielstellung in unterschiedlichen Detailierungsgraden ausgeprägt sein. Zumeist ist dies zudem abhängig davon in welchem Grad die Informationen, Daten und deren Quellen vorliegen. Die Methoden werden grundlegend in drei verschiedene Beurteilungsverfahren unterschieden:

- quantitativ
- qualitativ
- semi-quantitativ

Das Ziel der qualitativen Methode ist eine umfassende Auflistung potenzieller Gefahren, welche sich aus den Aufgabenstellungen für die Durchführung von Arbeitsschritten ergibt. Hierfür stehen bereits verschiedene, teilweise auch miteinander kombinierbare, Methoden zur Verfügung. Zu diesen gehören beispielsweise HAZOP oder PAAG [Br01], Checklisten oder auch What-if [Am08] und FMEA [Be06], welche auch bereits in der maritimen Domäne zum Einsatz kommen [Vi07], [De02], [Ga99]. Für die identifizierten Gefahren werden in diesem Verfahren die Vulnerabilität und die möglichen Auswirkungen ermittelt und ggf. mit verhindernden Maßnahmen gegenübergestellt. Eine häufig zum Einsatz kommende und für diese Arbeit

relevante Methode ist die Identifikation und Analyse von Risiken per Simulationsverfahren. Bei dieser können durch zwei grundlegenden Verfahren für eine simulationsgestützte Risikoanalyse, der Sensitivitäts- bzw. der Szenario-Analyse, Aussagen über die Auswirkung von Eingangsparametern und deren Zusammenhang bezüglich potenzieller Gefahren getroffen werden. Für die genauere Betrachtung der Anforderungen bzw. die Evaluation der Eignung der in dieser Arbeit entstehenden Methode wird die Forschungsarbeit von Gollücke [Go16] hinzugezogen. Für die Bewertung der Eintrittswahrscheinlichkeit möglicher Gefahren, einschließlich von unwahrscheinlichen, dennoch existierenden Störfällen, wird eine über die deterministische Betrachtungsweise hinausgehende, quantitative Risikoanalyse eingesetzt. Bekannte Guidelines in diesem Kontext sind das Purple Book [VR05], das LOPA Verfahren [Ce11] oder die aus dem EU-Projekt ARAMIS entstandene Methodologie zur unfallbezogenen Risikoanalysen [Sa05]. In dieser Arbeit werden nicht, wie häufig in der Literatur [To06], [Fe05] diskutiert, die semi-quantitativen Ansätze den qualitativen Ansätzen, sondern den quantitativen Ansätzen zugeordnet. Bei diesen werden die Elemente der Risikogleichung über ein Ranking, Indikatoren oder eine Gewichtungen miteinander kombiniert bzw. ein Risiko rechnerisch ermittelt. Gängige Methoden sind hierbei FTA (Fault Tree Analysis) oder auch die ETA (Event Tree Analysis) [Vi07]. Für die genauere Betrachtung der Anforderungen bzw. die Evaluation der Eignung der in dieser Arbeit entstehenden Methode wird die Forschungsarbeit von Pinkowski hinzugezogen [Pi15]. Für diesen Anwendungszweck sind die wichtigsten Methoden:

- Funktionale Sicherheit nach ISO 26262
- Leitfaden nach Gruber et al
- Offshore Code of Practice (OCoP)
- Vorgehen nach ISO 29400

Zunächst wird die ISO 26262, eine ISO-Norm für sicherheitsrelevante elektrische/elektronische Systeme in Kraftfahrzeugen vorgestellt, in dieser Domäne sind systematische Vorgehen genau für den hier diskutierten Kontext bereits fest verankert. Anschließend wird ein Leitfaden für Gefährdungsbeurteilungen diskutiert welcher sich an Arbeitgeber von kleinen und mittleren Unternehmen (KMU) und an Fachkräfte richtet, um diese bei der Beurteilung der Arbeitsbedingungen zu unterstützen. Des Weiteren werden zwei Methoden speziell für den Offshore-Bereich eingeführt: 1. der "Offshore Code of Practice", welcher durch eine Initiative der europäischen Erst- und Rückversicherern entstanden ist und 2. die ISO 29400, welche um-fassende Anforderungen und Leitlinien für die Planung und Durchführung bietet und darüber hinaus einen besonderen Schwerpunkt auf das Thema Sicherheit setzt.

Funktionale Sicherheit definiert die **ISO 26262** "Road vehicles – Functional safety" als "absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems".

Maier konkretisiert diese Definition, wonach die funktionale Sicherheit die Fähigkeit eines elektrischen oder elektronischen Systems (E / E-Systemen) darstellt beim Auftreten von systematischen Ausfällen (z. B. fehlerhafte Systemauslegung) oder zufälligen Ausfällen (z. B. Alterung von Bauteilen) mit gefahrbringender Wirkung, einen sicheren Zustand einzunehmen bzw. im sicheren Zustand zu bleiben [Ma13]. Abbildung 4 zeigt eine vereinfachte Form des Lebenszyklusmodells der ISO 26262.

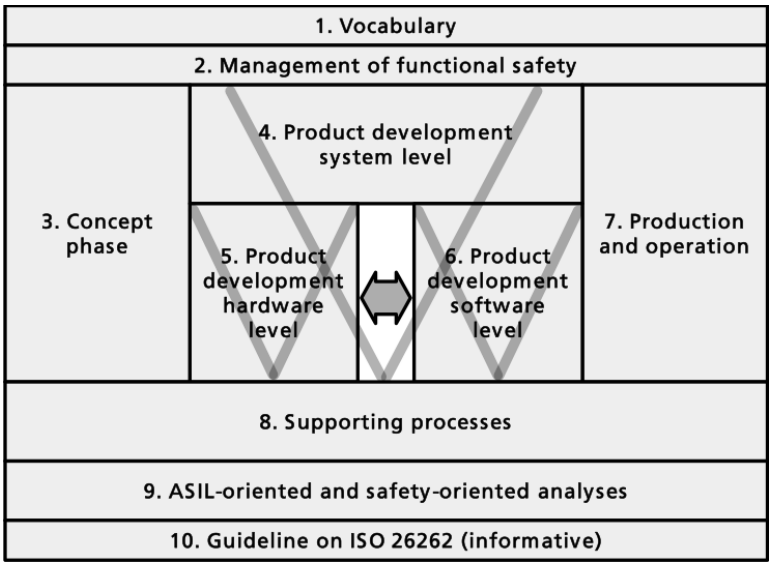


Abbildung 4: Vereinfachtes Lebenszyklusmodell der ISO 26262 [In08]

Das Glossar (1. Vocabulary) erklärt zunächst die die Begriffe und Abkürzungen, die in der Normenreihe verwendet werden. Die ISO 26262 bezieht sich nicht auf die nominale Leistung von E / E-Systemen, selbst wenn die funktionalen Performance-Standards für diese Systeme (z.B. aktive und passive Sicherheitssysteme, Bremssysteme, Adaptive Cruise Control) vorhanden sind. Der zweite Teil im Lebenszyklus der ISO 26262 (2. Management of functional Safte) spezifiziert die Anforderungen an das funktionale Sicherheitsmanagement für Automotive-Anwendungen, einschließlich der projektunabhängigen Anforderungen im Hinblick auf die beteiligten Organisationen (allgemeines Sicherheitsmanagement) und der projektspezifischen Anforderungen in Bezug auf die Managementaktivitäten im Sicherheitslebenszyklus (d.h. Management in der Konzeptphase, der Produktentwicklung und nach der Freigabe für die Produktion). Dieser Teil scheint weniger relevant, da es mehr das klassischen Projektmanagement betrifft um die gesamte (erwartete) Qualität als Ergebnis durch ein gutes Projektmanagement gewährleistet, welches die Verantwortlichkeiten in den frühen Projektphasen definiert. Im dritten Schritt (3. Concept phase) der ISO 26262 werden die Anforderungen für die Konzeptphase für Automobilanwendungen festgelegt:

- *Definition des zu untersuchenden Gegenstandes:* Das primäre Ziel ist die Definition des zu untersuchenden Gegenstandes. Das zweite Ziel ist es ein angemessenes Verständnis dieses Gegenstandes zu vermitteln, um mit diesem weiteren Schritte des Sicherheitslebenszyklus durchzuführen.
- *Initiierung des Sicherheitslebenszyklus*: Das Ziel der Einleitung des Sicherheitslebenszyklus ist es, den Unterschied zwischen einer neuen Entwicklung und einer Änderung an einem bereits bestehenden System deutlich zu machen. Im Falle einer Änderung müssen weitere Aktivitäten für den Sicherheitslebenszyklus definiert werden (ISO 26262-2, Abbildung 2)
- *Gefahrenanalyse und Risikobewertung*: Das Ziel der Gefahrenanalyse und Risikobewertung ist zunächst die Identifizierung und Kategorisierung der Gefahren des Systems und das Formulieren von Sicherheitszielen, um in diesem Zusammenhang Vorkehrungen gegen diese Gefahren zu treffen bzw. unangemessene Risiken zu vermeiden.
- *Funktionales Sicherheitskonzept*: Das Ziel des funktionalen Sicherheitskonzepts ist es die funktionalen Sicherheitsanforderungen der Sicherheitsziele abzuleiten und diese den Elementen des Untersuchungsgegenstands bzw. den externen Risikominderungsmaßnahmen zuzuordnen, um die erforderlichen funktionalen Sicherheiten zu gewährleisten.

Hier wird die Gefahren- und Risikoabschätzung von dem funktionalen Sicherheitskonzept getrennt bzw. Ersteres ist als Input für das Konzept zu verstehen. Die Festlegung der Anforderungen an die Produktentwicklung auf Systemebene für Automobilanwendungen erfolgt in der vierten Phase (4. Product development system level):

- *Spezifikation der technischen Sicherheitsanforderungen*: Das erste Ziel dieser Phase ist es, die technischen Sicherheitsanforderungen zu entwickeln. Die sicherheitstechnische Anforderungsspezifikation verfeinert das funktionale Sicherheitskonzept unter Berücksichtigung des Funktionskonzept und des vorläufigen Architekturdesigns. Das zweite Ziel ist es durch eine Analyse zu verifizieren, ob die sicherheitstechnischen Anforderungen den funktionalen Sicherheitsanforderungen nachkommen.
- *Systemdesign und technisches Sicherheitskonzept*: In diesem Schritt werden das Systemdesign und das technische Sicherheitskonzept entwickelt, welche die funktionalen und technischen Sicherheitsspezifikationen des Untersuchungsgegenstandes erfüllen. Dem angeschlossen erfolgt erneut eine Überprüfung ob das Systemdesign und das technische Sicherheitskonzept mit den technischen Sicherheitsanforderungen übereinstimmen.

- *Sicherheitsvalidierung*: Das erste Ziel ist es den Nachweis für die Einhaltung der funktionalen Sicherheitsziele zu erbringen und zu zeigen, dass die Sicherheitskonzepte für die funktionale Sicherheit des Systems angemessen sind. Das zweite Ziel ist nachzuweisen, dass die Sicherheitsziele richtig und vollständig in Bezug auf die Fahrzeugebene und im vollen Umfang erfüllt sind.
- *Funktionale Sicherheitsbeurteilung*: Das Ziel der Anforderungen in diesem Abschnitt ist es die Funktionssicherheit, die durch das System erreicht wird, zu beurteilen.

Dieser Abschnitt der Produktenwicklung auf Hardwareebene (5. Product development hardware level) befasst sich mit Empfehlungen, inwieweit ein technisches Sicherheitskonzept von dem funktionalen Konzept abgeleitet werden kann und wie dabei die funktionalen Sicherheitsanforderungen auf den, insbesondere, technischen Teil abgebildet werden können. Analog gibt die ISO in dem sechsten Schritt (6. Product development software level) auch Empfehlungen darüber, nach welchen Kriterien Software entwickelt werden sollte.

Abschnitt sieben der ISO (7. Production and operation) beschreibt die Anforderungen für die Produktion, den Betrieb, den Service (Wartung und Reparatur) sowie die Außerbetriebnahme des Systems.

- *Produktion:* Das erste Ziel der Anforderungen in diesem Abschnitt ist es, einen Produktionsplan für sicherheitsrelevante Produkte zu entwickeln. Das zweite Ziel ist es sicherzustellen, dass die erforderliche Funktionssicherheit während des Produktionsprozesses durch die jeweiligen Produkthersteller oder der Person oder Organisation für diesen Prozess (Fahrzeughersteller, Händler, Zulieferer etc.) gewährleistet wird.
- *Betrieb, Service (Wartung und Reparatur) und Stilllegung*: Das erste Ziel dieser Phase ist es den Umfang der Kundendaten und der Wartungs- und Reparaturanweisungen in Bezug auf die sicherheitsrelevanten Produkten zu definieren, um die erforderliche Funktionssicherheit während des Betriebs des Fahrzeugs zu erhalten. Das zweite Ziel ist es, die Anforderungen in Bezug auf die Schritte zur Behandlung von Sicherheitsfragen vor der Demontage zu schaffen.

In Abschnitt acht (8. Supporting processes) wird auf unterstützende Prozesse eingegangen. Dabei handelt es sich beispielsweise um Abstimmung verteilter Entwicklung über Developer Interface Agreement (DIA), Konfigurations-Management, die Planung von Maßnahmen zur Verifizierung und Validierung, Dokumenten-Reviews und Safety-Assessments oder auch Change Management. Die Bestimmung von Vorschriften und Leitlinien für die Zersetzung von Sicherheitsanforderungen in redundante Sicherheitsanforderungen, um damit eine ASIL

Dekomposition auf die nächste Detailstufe zu ermöglichen, erfolgt im vorletzten Schritt (9. ASIL-oriented and safety-oriented analyses). Zudem sollen in dieser Phase Kriterien für die Koexistenz im von sicherheitsrelevanten Subsystemen mit nicht sicherheitsrelevanten und zudem sicherheitsrelevante Subsysteme mit Zuordnung in verschiedene ASIL Stufen gegeben werden. Der letzte Teil (10. Guideline on ISO 26262) gibt einen Überblick und weitere Erklärungen, wie die ISO zu interpretieren ist, so dass diese möglicherweise eine zusätzliche Informationsquelle.

Vergleicht man das Vorgehen in der Offshore-Branche, finden sich viele Schritte der ISO 26262 darin wieder, allerdings ist die Reihenfolge der Durchführung der Konzepte eine andere. Demnach sind die Konzepte aus diesem Werk durchaus von hoher Relevanz und sollten hinsichtlich einer Übertragung auf die maritime Domäne bzw. mindestens einer Berücksichtigung in der in dieser Forschungsarbeit erstehenden Methodik geprüft werden.

In der Literatur werden verschiedene Vorgehen für eine Gefährdungsbeurteilung eingeführt, welche sich im Kern jedoch sehr stark ähneln [Ad12], [Ba13], [GKM13]. Von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) explizit für die Anwendung in der Praxis vorgeschlagen, wird exemplarisch im Folgenden der Leitfaden für die Gefährdungsbeurteilung nach **Gruber et al** genauer vorgestellt. Die Autoren strukturieren ihr Vorgehen in fünf Phasen (vgl. Abbildung 5).

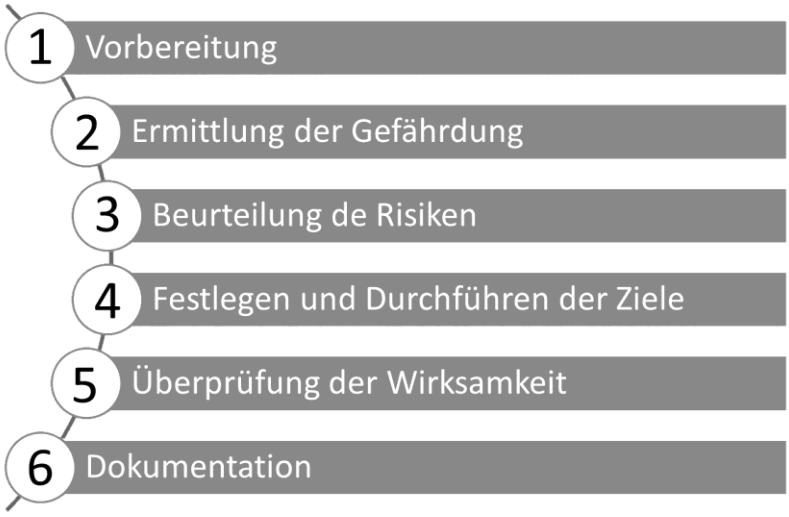


Abbildung 5: Schritte für die Gefährdungsbeurteilung

In der Vorbereitung wird zunächst festgelegt auf welche Art der Tätigkeitsbeschreibung die Gefahrenbeurteilung durchgeführt wird. Es wird dabei zwischen folgenden drei Varianten unterschieden:

- *Unterteilung in ortsfeste und nicht ortsfeste Arbeitsplätze*: Ortsfeste Arbeitsplätze können zum einen arbeitsbereichsbezogen analysiert werden, wodurch die Gefährdungen nur einmal zu erfassen sind. Durch das Ergreifen einer Maßnahme kann die Gefährdung an mehreren Arbeitsplätzen hierbei gleichzeitig abgebaut werden. Zum anderen kann der Fokus der Betrachtung auf die Tätigkeit bzw. den Arbeitsplatz gelegt werden. Auf Basis dieser Betrachtungseinheiten werden die Gefährdungen von Personen beurteilt, die der gleichen Tätigkeit nachgehen. Hier liegen zu-meist keine fest zugewiesenen Arbeitsplätze und/oder häufig wechselnde Arbeitsaufgaben vor. Diese sind jedoch gleichen Gefährdungen ausgesetzt. Für nicht ortsfeste Arbeitsplätze bietet sich eine berufsgruppenbezogene Gefährdungsbeurteilung an. Bei dieser Art der Erfassung wird zunächst die Berufsgruppe festlegt und im Anschluss die konkreten Tätigkeiten zugeordnet.
- *Personenbezogene Gefährdungsbeurteilung*: Die personenbezogene Gefährdungsbeurteilung ist vorzunehmen für Tätigkeiten, die von besonders schutzbedürftigen Personen durchgeführt werden. Zu diesen zählen ebenfalls Leiharbeiter. Hierbei ist der Arbeitgeber (Überlasser) verantwortlich für eine im Vorfeld durchgeführte Gefährdungsbeurteilung in der hervorgehen muss, dass seine Angestellten nebst ihrer körperlichen und geistigen Fähigkeiten durch berufliche Qualifikationen für die Arbeit des Entleihenden geeignet sind.
- *Arbeitsablauforientierte Gefährdungsbeurteilung*: Mit Hilfe der arbeitsablauforientierten Gefährdungsbeurteilung können einzelne Arbeitstätigkeiten, Bearbeitungsfolgen oder Transportabläufe analysiert werden. Aus einer genauen Beschreibung der Arbeitsaufgabe werden die durchzuführenden Tätigkeiten ermittelt und gegeben falls in Teiltätigkeiten untergliedert. Anschließend werden für jeden Teilschritt die relevanten Gefährdungen identifiziert und Schutzmaßnahmen festgelegt.

Bei der Ermittlung der Gefährdung wird zwischen der direkten und indirekten Methode unterschieden. Die direkte Methode wird auch als vorausschauende bzw. präventive Methode aufgeführt. Bei dieser werden Gefährdungen und Belastungen ermittelt, denen die Beschäftigten während der Ausübung der Tätigkeit ausgesetzt sind. Wesentlich ist es die eigentliche Gefahrenquelle zu ermitteln, welche die Gefährdung hervorruft. Ergänzt werden die Bedingungen im Sinne einer Ursachenkette, die Gesundheitsschäden hervorruft. Ebenso sind die Gegebenheiten zu erörtern, bei denen ein Zusammentreffen des Gefährdungsfaktors mit dem Menschen begünstigt wird. Bei der indirekten, auch zurückschauenden Methode, werden Erkenntnisse aus bereits aufgetretenen Ereignissen, d. h. Unfällen und Beinahe-Unfällen, in die Gefährdungsermittlung mit einbezogen. Aus dem Unfallhergang und den ermittelten tatsächlichen Ursachen sind die Gefahrenquellen und die Bedingungen zum Wirksamwerden zu bestimmen.

Die Beurteilung der Risiken bedeutet festzustellen, ob eine Gefahr für die Beschäftigten vorliegt und somit Handlungsbedarf für Arbeitsschutzmaßnahmen besteht. Dabei ist jede ermittelte Gefährdung zu bewerten und zu dokumentieren. Heranzuziehen sind hier Vorgaben aus Gesetzten, Unfallverhütungsschriften, technischen Regelwerken oder gesicherten arbeitswissenschaftlichen Erkenntnissen. Hierbei ist zu beachten, dass ebenfalls Risiken zu bewerten sind, bei denen keine gesetzlichen Vorgaben bzw. Grenzwerte vorliegen. Das Ergebnis der Risikobeurteilung sollte eine Aussage bezüglich des Handlungsbedarfes und der dazugehörenden Dringlichkeit einzelner Gefahren sein. Um das erkannte Risiko zu reduzieren, werden in der vierten Phase (Festlegen und Durchführen der Maßnahmen) die Schutzziele und geeignete Maßnahmen zur Beseitigung oder hinreichenden Begrenzung der festgestellten Gefährdungen festlegt. Dies sind technische, organisatorische und personenbezogene Arbeitsschutzmaßnahmen. Sie sollten die Maßnahmen entsprechend der folgenden Rangfolge treffen:

i. Arbeitsverfahren so gestalten, dass keine Gefährdung vorhanden ist, Gefahrenquellen beseitigen;
ii. Gefährdungen ausschalten oder mindern durch Anwendung von Schutzeinrichtungen, vorzugsweise mit zwangsläufiger Wirkung;
iii. Gesundheitsrisiko minimieren durch Herabsetzung von Intensität bzw. Dauer der Exposition mittels technischer oder arbeitsorganisatorischer Maßnahmen;
iv. Persönliche Schutzeinrichtungen oder Verhaltensregeln anwenden.

Die Überprüfung der Wirksamkeit umfasst die Feststellung der Durchführung der im Schritt 4 gesetzten Maßnahmen, deren Wirksamkeit hinsichtlich der Gefährdungsvermeidung oder -Verringerung. Zudem muss überprüft werden, ob durch die Maßnahmen eventuell neue oder andere Gefährdungen entstanden sind.

Nach ArbSchG muss jeder Arbeitgeber über eine aussagefähige Dokumentation der im Unternehmen durchgeführten Gefährdungsbeurteilung verfügen. Diese Dokumentationspflicht besteht nach § 6 (1) des ArbSchG. Demnach muss der Arbeitgeber über Unterlagen verfügen, die das Ergebnis der Gefährdungsbeurteilung, die darauf gestützten Maßnahmen des Arbeitsschutzes und das Ergebnis ihrer Überprüfung dokumentieren.

Besonders die Vorbereitungsphase aus dem von den Autoren entwickelte Vorgehen zeigt eine hohe Relevanz für diese Forschungsarbeit. Wohingegen sich die weiteren Schritte mit dem in der Praxis üblichen Ablauf decken, wird hier zunächst spezifischer auf die Arbeitsweise eingegangen. Vor allem die "arbeitsablauforientierte Gefährdungsbeurteilung" weißt starke Parallelen mit der in der Motivation dargestellten Art der Ausübung der Arbeiten im maritimen Bereich auf.

In vielen europäischen Ländern, wie z.B. Deutschland, sind neben den gesetzlichen Bestimmungen, weitere Mindestanforderungen für die Sicherheitsbestimmungen am Arbeitsplatz im Zusammenhang mit Offshore-Windparks definiert worden (Deutscher Bundestag, 2011). Auch in Großbritannien hat der Wirtschaftsverband RenewableUK (ehemals BWEA) Gesundheits- und Sicherheitsrichtlinien mit Schwerpunkt auf Offshore- und Onshore-Windparks veröffentlicht [re13]. Im Jahre 2010 erkannte das European Wind Turbine Committee (EWTC) die Notwendigkeit die noch junge Branche der Offshore-Windenergiegewinnung in diesem Punkt zu unterstützen und gründete die Initiative "Offshore Code of Practice" (**OCoP**). Die Initiative der europäischen Erst- und Rückversicherern wird dabei durch den Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) und der Stiftung "Offshore Windenergie" unterstützt. Anfang 2014 wurde erstmalig der OCoP über den GDV herausgegeben und soll als "Leitlinie für das Risikomanagement innerhalb des Errichtungsprozesses von Offshore-Windparkprojekten" verstanden werden [Ge14]. Die inhaltlichen Empfehlungen der Leitlinien bezüglich der Gefahrenbewertung der Offshore-Operationen decken sich weitestgehend mit den Erkenntnissen über den Inhalt der zu erstellenden Dokumenten aus der Praxis, welche durch eine Umfrage bei Projektpartnern im Rahmen des Forschungsprojektes SOOP gewonnen werden konnten [So12b]. Dieser, auch als Risikoverzeichnis bezeichnete Abschnitt eines HSE-Plans beinhaltet dabei die bei der Durchführung einer Risikoanalyse identifizierten Risiken für jeden einzelnen Arbeitsschritt, sowie die entsprechenden Schutzmaßnahmen.

Im Folgenden werden die wesentlichen Bestandteile aufgeführt:

- *Nennung des Prozessschrittes*: Ein Prozessschritt ist beschrieben als eine "Überschrift", die den jeweiligen Kontext möglichst griffig definiert. Sie wird so gewählt, dass eine Abgrenzung zu anderen Schritten deutlich wird.
- *Kurzbeschreibung der Arbeitsschritte*: Eine Beschreibung der zu jedem Prozessschritt zugehörigen Arbeitsschritte.
- *Beschreibung der Gefahren und Einschätzung des Risikos:* Hier werden die wesentlichen Gefahren, die während eines Arbeitsschrittes eintreten können, beschrieben. Für jede Gefahr wird zudem eine Einschätzung bezüglich des potenziellen Risikos ohne jegliche Gefahrenminderung aufgeführt.
- *Beschreibung und Einschätzung der Schutzmaßnahmen:* Mögliche Schutzmaßnahmen zur Minderung der Eintrittswahrscheinlichkeit bzw. das Begrenzen des Schadensausmaßes werden zusammen mit einer zugehörigen Abschätzung der Wirkung auf die jeweilige Gefahr beschrieben.
- *Risiko–Relevanz / und –Status:* Abhängig von der Einschätzung des Risikos und der Wirkung von Schutzmaßnahmen wird für einzelne Gefahren die Relevanz und das Potenzial des Risikos berechnet.

Je nach Unternehmen variiert das erzeugte Dokument bezüglich der Auflistung von Zusatzinformationen, beispielsweise über die eingesetzten Ressourcen oder die Ausbildungsstandards des an den Prozessen beteiligten Personals. Dies hängt auch davon ab, ob dieses Dokument neben der Funktion als Bestandteil der Genehmigungsunterlagen auch für andere Zwecke eingesetzt wird. So werden diese teilweise auch in Form einer Dokumentation für Schulungszwecke bzw. Arbeitsanweisungen eingesetzt.

Eine weitere Gemeinsamkeit zwischen den Erkenntnissen aus der Praxis und dem OCoP ist, dass zum einen eine manuelle Erstellung mittels Microsoft Word und Microsoft Excel genannt wird und zum anderen eine manuelle Erstellung empfohlen wird. Lediglich bei der Berechnung der Relevanz und des Status des Risikos wird jeweils ein Standard eingesetzt, welcher eine automatische Durchführung erlaubt. Die Schritte in dieser Methode decken sich stark mit dem Vorgehen aus dem zuvor vorgestellten Leitfaden für Gefährdungsbeurteilungen.

Viele Neuerungen können demnach nicht festgestellt werden, jedoch ist dieses Werk für die Offshore-Domäne von besonderer Bedeutung, da hiermit eine Referenz für genau diesen Bereich geschaffen wurde und sich Unternehmen daran halten können.

In dem erst kürzlich veröffentlichten internationalen Standard **ISO 29400** "Ships and marine technology - Offshore wind energy - Ports and marine operations" wird auf die Notwendigkeit eines Health, Safety, Security and Environment (HSSE) Plans mit konkreteren Zielvorgaben eingegangen [IS15]. Demnach sollte ein solcher Plan:

- die HSSE-Standards, Prozesse und Verfahren, die für die Arbeit gelten dokumentieren
- die Gefahren und Risiken, die sich auf diese Arbeit beziehen erkennen und bewerten und diese auf ein akzeptables Minimum reduzieren
- dafür dienen, dass Sicherheitsaspekte eine Tragende Rolle bei der Planung und Gestaltung der Arbeit spielen
- minimale Auswirkungen auf die Umwelt gewährleisten
- zum Schutz der Gesundheit der Arbeitskräfte beitragen
- die Sicherheit am Arbeitsplatze insbesondere in Hafenanlagen [..] gewährleisten.

Der Plan muss HSSE-Aktivitäten in allen Phasen der Arbeitsprozesse, von der Planung und Konzeption bis zur Ausführung der Operation, umfassen. Die Gesamtverantwortung für das Risikomanagement sollte bei der Planung von maritimen Operationen klar definiert sein und auf das Projekt angewandt werden, um die Auswirkungen von Gefahren zu reduzieren und das Gesamtrisiko zu begrenzen. Dieses Ziel kann und sollte durch die folgenden Funktionen erreicht werden:

- Identifizierung von potenziellen Gefahren
- Bewertung des Risikopotenzials
- Prävention, um Gefahren zu vermeiden
- Steuerung, um die möglichen Folgen der unvermeidlichen Risiken zu reduzieren
- Maßnahmen, um die Folgen eines Zwischenfalls einzudämmen

Weiterhin wird definiert, dass alle Hafen- und Marineoperationen, einschließlich aller Hauptsysteme, die an solchen Operationen, wie z.B. Verladeoperationen, der Stromerzeugung oder Versorgungssystemen beteiligt sind, einer strengen Gefahrenbewertung unterzogen werden müssen. In die Gefahrenbewertung sollte das an der Ausführung und an der Planung beteiligte Personal von Hafen- und Marineoperationen mit einbezogen werden. Zudem wird empfohlen, eine Analyse der Wirkungsketten durchzuführen, um die Wahrscheinlichkeit und die Folgen potentieller Ereignisse zu bewerten. Dies bildet ebenfalls, falls notwendig, die Grundlage für weitergehende Untersuchungen.

Hierbei werden verschieden Methoden zur Bewertung von Risiken vorgeschlagen, wie beispielsweise die HAZID – Methode, szenario-basierte Risikobewertungen oder auch die Job Safety Analysis (JSA), bei der eine hohe Relevanz für diese Forschungsarbeit identifizierbar ist. Eine JSA sollte folgende Details beinhalten:

- Arbeitsprozesse einer Operation
- Ausrüstung, die in allen Schritten eingesetzt wird
- Identifizierung von Gefahren, die kontrolliert werden müssen
- Vorsichtsmaßnahmen, die getroffen werden müssen und die personelle Verantwortung

Diese Analyse sollte von dem Hafenbetreibern und den Verantwortlichen von den Marineoperationen als Basis für die Darstellung für den Betrieb in den jeweiligen Arbeitsfeldern durchgeführt und dokumentiert werden. Die Ergebnisse der Arbeits- und Sicherheitsanalyse sollten im Anschluss als Arbeitsanweisung dem Personal vorgelegt und deren Inhalt in den unterschiedlichen Operationen in Form von Kick-off Meetings und "Toolbox-talks" übermittelt werden. Der Standard bietet für diese Forschungsarbeit einen sehr fundierten Rahmen, da erkannt wurde, dass in diesem Untersuchungsbereich noch starker Bedarf an Vorgaben und Standards hinsichtlich der Gefährdungsbeurteilung von Hafen- und Marineoperationen besteht.

2.1.2 Techniken der Gefährdungsbeurteilung

Quantitative Risikoanalysen haben traditionell den Fokus auf technische Systeme und deren Eigenschaften. Vernachlässigt wurden dabei zumeist die anderen Bestandteile von Systemen: die menschlichen Akteure und Organisationsstrukturen [Vi07]. Neben der Betrachtung von Techniken, dessen Anwendung in der maritimen Domäne bereits verbreiten sind, wird in diesem Abschnitt ebenfalls ein Exkurs in die Planung der Weltraumforschung gegeben. Es wird dabei jeweils untersucht, inwieweit diese bereits anwendbar auf die Zielstellung dieser Forschungsarbeit sind:

- Events and Conditional Factors Analysis (ECFA+)
- Man, Technology and Organisation (MTO)
- Sequentially Timed Events Plotting Procedure (STEP)
- timeline-basierte Planung (Luft & Raumfahrt)
- VASCO

Die **ECFA+** ist eine Abwandlung der 1978 von Buys und Clark [BC78] vorgestellten Events und Causal Analysis (ECFA). Den Methoden liegt kein expliziertes theoretisches Modell zugrunde, organisationsbezogene Aspekte werden teilweise, interorganitionale Aspekte überhaupt nicht berücksichtigt. Die ECFA– Verfahren dienen vorrangig folgenden 3 Zielstellungen:

- Es ermöglicht die Verifikation von Kausalketten und Ereignisabläufen
- Es bietet eine Struktur für integrierte Untersuchungsergebnisse
- Es unterstützt die Kommunikation während der Untersuchung und nach dessen Abschluss

Abbildung 6 zeigt die schematische Illustration eines Ereignis-Ursachen-Diagramms (Events and Causal Factors Chart), welches den Kern der ECFA – Methoden darstellt.

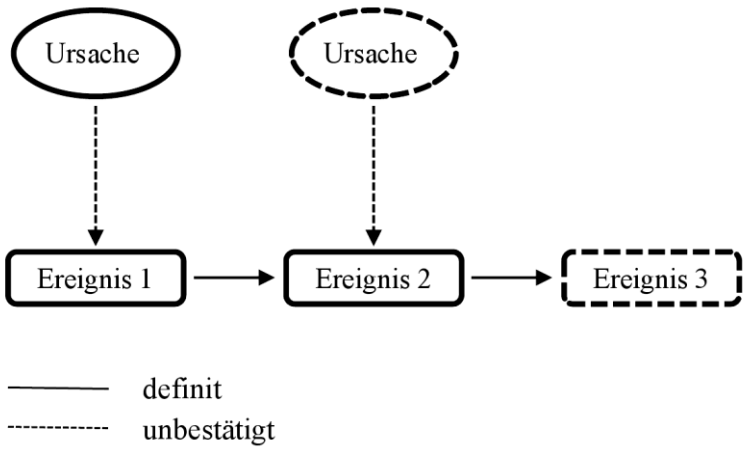


Abbildung 6: Aufbau eines Ereignis-Ursachen-Diagramms

In diesem werden zu dem Unfall beitragende Ereignisse in Form von Rechtecken repräsentiert und durch das Verbinden mit Pfeilen in eine sequenzielle Reihenfolge gestellt. Die durch Ovale dargestellten Ursachen (auch Bedingungen) werden ebenfalls mit Pfeilen den Ereignissen zugeordnet. Beginnend mit dem primär auslösenden Ereignis wird rückwärts die tatsächliche Entstehung des Unfalls beschrieben. Nach den Konventionen von ECFA sollte jedes Ereignisrechteck einem Akteur zugeordnet werden und dessen Handlung beinhalten. Bei Unsicherheiten, durch beispielsweise fehlende Informationen oder Daten, werden die Randlinien sichtbar anders dargestellt (in diesem Fall "gestrichelt"). Da dieses Verfahren keine tieferlegenden Ursachen identifiziert, wird vorgeschlagen diese in Kombination mit anderen Methoden zu verwenden [Ot14].

Auch wenn ECFA+ ursprünglich für die retrospektive Betrachtung von Unfallhergängen konzipiert wurde, kann das Verfahren ebenfalls dafür verwendet werden Arbeitsvorgänge zu Planen und hinsichtlich Risiken zu analysieren, da den Events einem Akteur und dessen Handlung zugeordnet wird (Z1) und Ursachen annotiert werden (Z2). Ein entsprechendes Bewertungskonzept und die Integration von Schutzmaßnahmen (Z3) fehlt jedoch. Hinsichtlich eines durchgängigen Ansatzes ist diese jedoch nicht geeignet, da im Besonderen die Ausführbarkeit (Z4) und generell eine geeignete Werkzeugunterstützung (Z5) nicht gegeben sind.

MTO (Man, Technology and Organisation) wurde ebenfalls ursprünglich als eine Technik für Analyse von (beinahe-) Unfällen und weiteren Zwischenfällen entwickelt. Es baut im Kern auf die Benutzung eines Ereignis-Ursachen-Diagramms auf (vgl. ECFA+), erweitert diese jedoch um eine Änderungsanalyse, welche beschreibt in wie weit die Events von vorherigen Events oder der üblichen Praxis abweichen und eine Hindernisanalyse, bei der technologische und organisatorische Hindernisse, die fehlgeschlagen sind oder vergessen wurden, identifiziert werden. Wesentlich bei dieser Technik ist, dass die Betrachtungsperspektive auf dessen Basis die Analysen durchgeführt werden die drei Aspekte Technologie, Organisation und Arbeitskraft miteinander in Beziehung setzt.

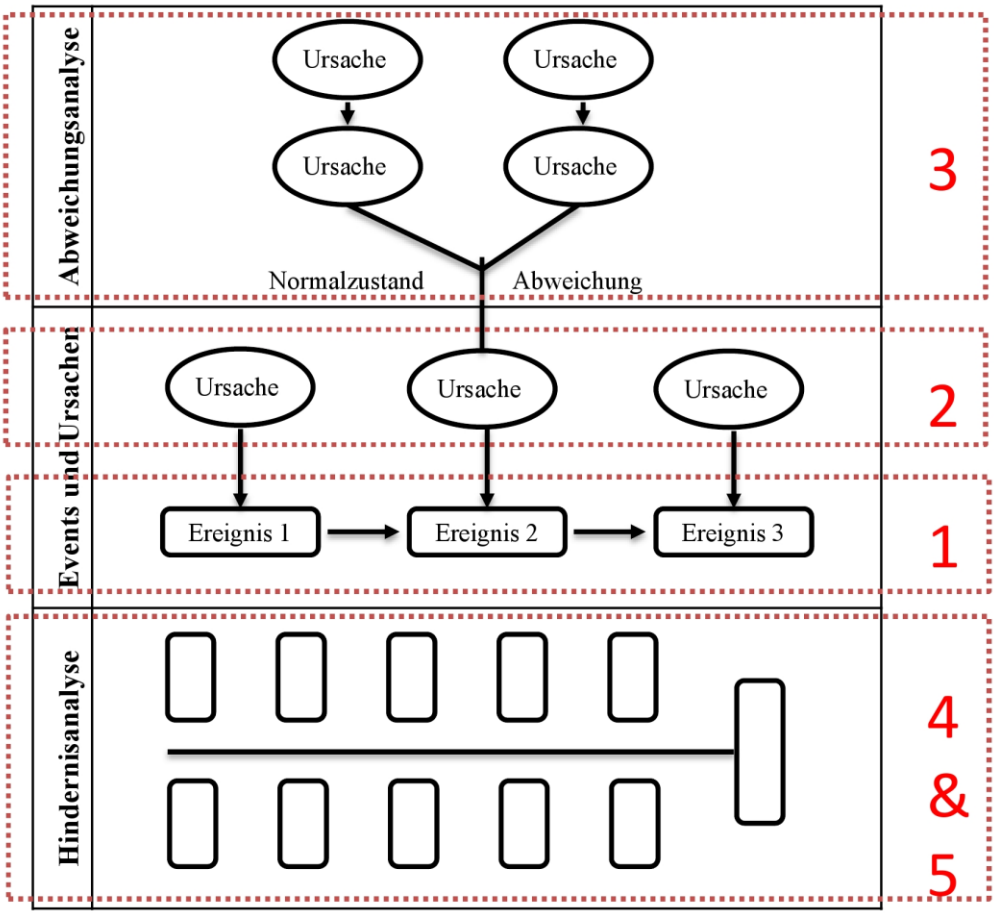


Abbildung 7: Beispielhaftes MTO - Diagramm (Zahlen definieren Bearbeitungsreihenfolge)

Abbildung 7 zeigt ein exemplarisches MTO – Diagramm, welches in folgenden fünf Schritten erzeugt wird:

1. Definition der Eventkette für den zu untersuchenden Prozess
2. Hinzufügen der Ursachen für jedes Event
3. Identifizieren der fehlgeschlagenen Events und Hinzufügen der entsprechenden Ursachenverkettung
4. Hinzufügen von Hindernissen die fehlschlagen bzw. vernachlässigt wurden
5. Identifizieren und Ergänzen von Aktionen die ein erneutes Auftreten verhindern

Das Vorgehen mittels MTO - Diagramm stellt eine Erweiterung der ECFA+ - Methode dar und erfüllt demnach die dort identifizierten Ziele (Z1 & Z2). Neu hinzugekommen ist lediglich die Nachvollziehbarkeit der identifizierten Gefahren. Dies bedeutet auch hier, hinsichtlich eines durchgängigen Ansatzes, dass sich dieses Verfahren als nicht hinreichend herausstellt, da ebenfalls weder die Ausführbarkeit (Z3) noch eine geeignete Werkzeugunterstützung (Z5) gegeben sind.

STEP (Sequentially Timed Events Plotting) wurde 1987 von Hendrick und Brenner [HB87] auf Basis der Multilinear Events Sequencing (MES) Methode [Br75] entwickelt. Der Kern ist

ein Ereignissequenzmodell, welches besagt, dass jeder Unfall aus vielen Teilereignissen besteht. Damit ähnelt es stark der vorgestellten MTO - Technik. Die Einzelereignisse werden dabei sequenziell den verschiedenen ausübenden Akuteren zwischen einem klar definierten Anfangs- und Endzustand zugeordnet. Hierbei differenziert der Analytiker zwischen Akteuren und Reakteuren. Zudem werden für diese jeweils die Kategorien Zeit, Ort, Quelle, Akteur, Handlung, Beschreibung, Ereignisdauer und Bemerkungen festgehalten. In der anschließenden Gefahrenidentifikation werden Ursachen und Bedingungen für Einzelereignisse, sowie Abhängigkeiten zwischen diesen, identifiziert. Das Ergebnis dieser Analyse ist die, in Abbildung 8 konzeptionell illustrierte, graphische Darstellung des Unfalls.

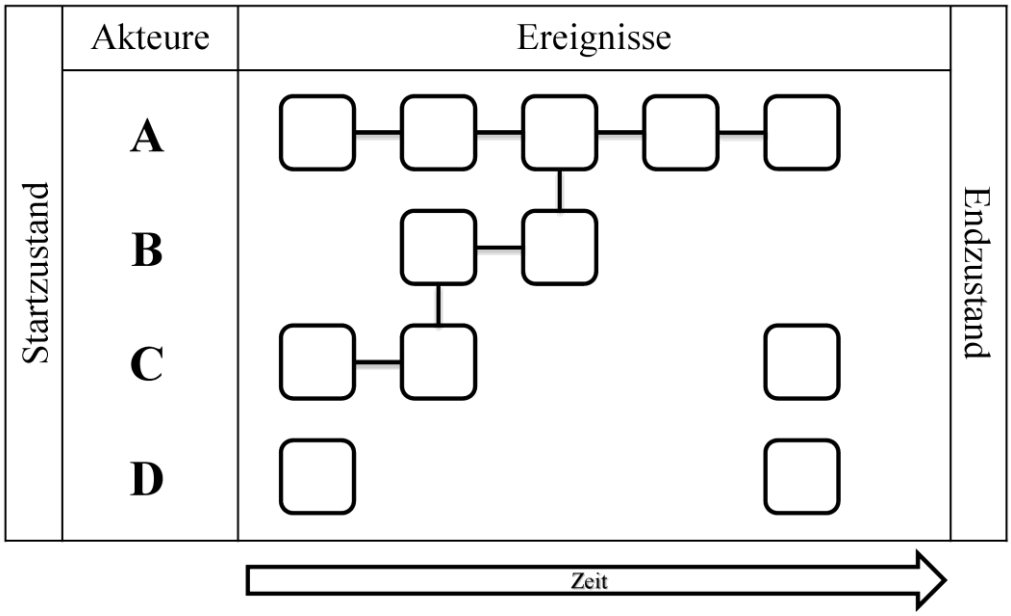


Abbildung 8: Exemplarisches STEP Diagramm

Das STEP – Verfahren ermöglicht ein eindeutigeres Zuordnen von Ereignissen zu Akteuren (Z1) im Vergleich zu den beiden zuvor betrachteten Techniken. Teilweise ist zudem die Kommunikation abgedeckt, da ein Sequenzfluss über verschiedene Akteure hinweg möglich ist, aber auch hier ist eine Ausführung nicht möglich (Z3).

Die Missionsplanung für die Raumfahrt ist ein wichtiges Anwendungsszenario für die Planung und Automatisierung für dynamische Systeme. Dabei spielt die Modellierung von komplexen, operationellen Vorgaben eine wichtige Rolle. Dies beinhaltet insbesondere die Instrumente, deren Subsysteme, Zeit- und Synchronisationsaspekte oder auch die Geometrie. Auch das hohe finanzielle Risiko verlangt stets zuverlässige Planungs- und Betriebspläne, um die Wertgegenstände nicht zu gefährden. Da im Bereich der Automatisierung großes Optimierungspotenzial existiert, sind verschiedene Anwendungen für die Planung von Weltraummissionen

entstanden [Ch12]. Die meisten dieser Systeme setzten auf einen zeitleistenbasierenden Ansatz, bei dem das Gesamtsystem, das Raumfahrzeug und die entsprechenden Bodenstationen durch eine Reihe von Zeitlinien repräsentiert werden.

Jede Zeitleiste stellt entweder die Historie oder aber den vorhergesagten Werte und Aktivitäten des Raumfahrzeuges und der Ressourcen dar. Mit einem solchen zeitleistenbasierte Modellierungsschema werden Aktivitätspläne erzeugt, anhand welcher die Sicherheit verifiziert und den Operationsplan validiert werden kann. Neben der Planung der Aktivitäten werden zudem deren Effekte modelliert, um damit zukünftige Aktivitäten basierend auf der Analyse der Effekte planen zu können. Die meisten zeitleistenbasieren Planungssysteme haben somit die Möglichkeit ein Basissatz an Zuständen, Ressourcen und Zeitabhängigkeiten zu modellieren. In [Ch12] wurde eine Gegenüberstellung über verschiedene Systeme dieser Art veröffentlicht.

Tabelle 1 zeigt eine Analyse der **timeline-basierte Planung** Missionsplanungssysteme hinsichtlich der Funktionalitäten.

System	States, infinite (b)	Resources (b)	Relative timing	Parametric (d) constraints	Search interfaces (e-j)
APSI [Ce09]	Finite , Infinite (by means of parameters)	Yes, depletable and non-depletable	Supported	Yes	e,f,g,h,i,j
ASPEN [Ch00]	Finite, Infinite	Yes, unit, depletable, non-depletable, integral	Yes	Yes	e,f,g,h,i,j
EUROPA	Infinite	Yes	Yes	Yes	e,f,g,h,i,j
flexplan	Supported	Supported	Supported	Supported	All Supported
Mexar2	Finite states	Reusable resources. Cumulative resource, and binary resource	Yes	No	Yes
MUSE	Yes	Yes	No	No	e-j
Pinta/Plato	Yes	Yes	Yes	No	e,f,g,h,j
SKeyP	finite states	Reusable resources. Cumulative resource, and binary resource	Yes	No	Yes
SPIFE	Infinite	Yes	Yes	Yes	e,f,g,i,j
SPIKE	No	Yes	Yes	No	e,f,g,h,i,j

Tabelle 1: Timeline-basierten Missionsplanungssysteme und deren Modellierungs- und Suchfunktionen nach [Ch12]

Folgende Fähigkeiten wurden dabei in fast allen Ansätzen als Basisfunktionalität vorgefunden:

a) lineare, gegeben falls begründete Zeitpunkte für Events bzw. Aktivitäten wie geplante Startzeiten
b) finite und unbestätigte Zustände und (abnutzbare) Ressourcen
c) variable relative Zeiteinschränkungen
d) funktionsparametrischen Abhängigkeiten zwischen Nutzungen und Aktivitätsparametern

Zusätzlich bieten diese Systeme auch im Allgemeinen eine Reihe von Berechnungs-Dienstleistungen wie beispielsweise die Verarbeitung von Abhängigkeiten einer vollständigen oder teilweisen Zeitplanung. Dies beinhaltet typischerweise folgende Aspekte:

e) die Fähigkeit Constraint-Verletzungen bei den oben genannten Einschränkungen zu detektieren
f) eine Aktivität (separiert oder simultan propagiert/modelliert) zu platzieren
g) die Fähigkeit, abzufragen, ob eine bestimmte Platzierung einer Aktivität die Einschränkungen verletzen
h) die Möglichkeit gültige, zeitbezogene Platzierungen einer Tätigkeit ohne Verletzen der Einschränkungen zu tätigen
i) das Vermögen beliebig codierte Constraint-Modellen zu nutzen, um komplexe Beschränkungen und Aktivitäten zu überprüfen: wie zum Beispiel: Manöver, Energieverbrauch, Mobilität oder Thermik
j) überprüfen zu können, ob beim Löschen, Bewegen oder auch beim Dekomponieren von Aktivitäten die erwähnten Constraints noch zutreffen

Auch der bemannten Raumfahrt ist die Automation ein wesentlicher Bestandteil vieler technischer Anlagen, um die Effizienz, Sicherheit und Zuverlässigkeit von Mensch-Maschine-Systemen zu erhöhen. Die Interaktion mit diesen Systemen führen zu neuen Arten von Fehlverhalten, wie beispielsweise Aufmerksamkeitsdefizite, Out-of-the-Loop-Effekte oder der Abbau von Fähigkeiten. Um dieses zu identifizieren wurde im Rahmen des Technologie und Forschungszentrum ESTEC der ESA (European Space Agency) das Forschungsprojekt **VASCO** initiiert, um mit formalen Verifikationstechniken die Probleme der Mensch-Automatisierung zu lösen. Abbildung 9 zeigt die aus dem Projekt entstandene Analysemethode für die Verifikation im sicherheitskritischen Flugbetrieb.

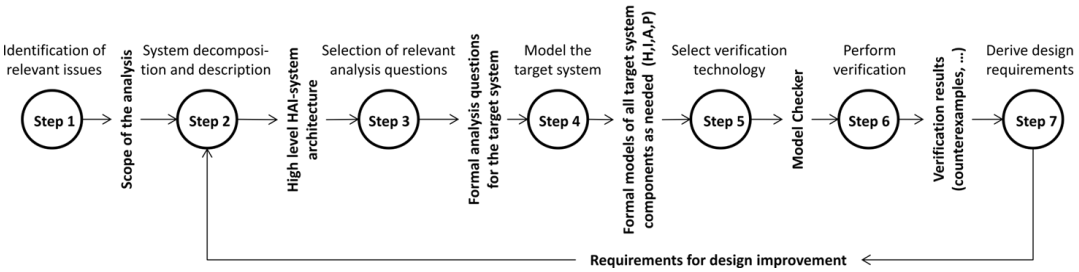


Abbildung 9: Methodologie für die Verifikation

Bei der Betrachtung der sieben Schritte der Methodologie zeigen die Schritte 2 "Systemdekomposition und –Beschreibung" und der vierte Schritt "Modellierung des Zielsystems" eine Relevanz für den Kontext dieser Forschungsarbeit, weshalb im Folgenden eine Beschreibung für diese beiden erflogt.

Als Vorbereitung für die Analyse findet zunächst eine Dekomposition der Mensch-Maschine-Systeme in die einzelnen Komponenten statt:

- Die Mensch- (Operator oder andere Nutzer) und Maschinen-Agenten (automatisierte Systeme)
- Die Prozesse, in welchen die Agenten agieren
- Die Umwelt in der die Prozesse durchgeführt werden
- Die Schnittstellen zwischen allen Komponenten: z.B. Mensch-Mensch, Mensch-Maschine, Maschine-Maschine, ….

Für diesen Schritt wurde in dem Projekt ein Modell entwickelt, mit welchen die eben aufgeführten Komponenten beschrieben werden können (vgl. Abbildung 10).

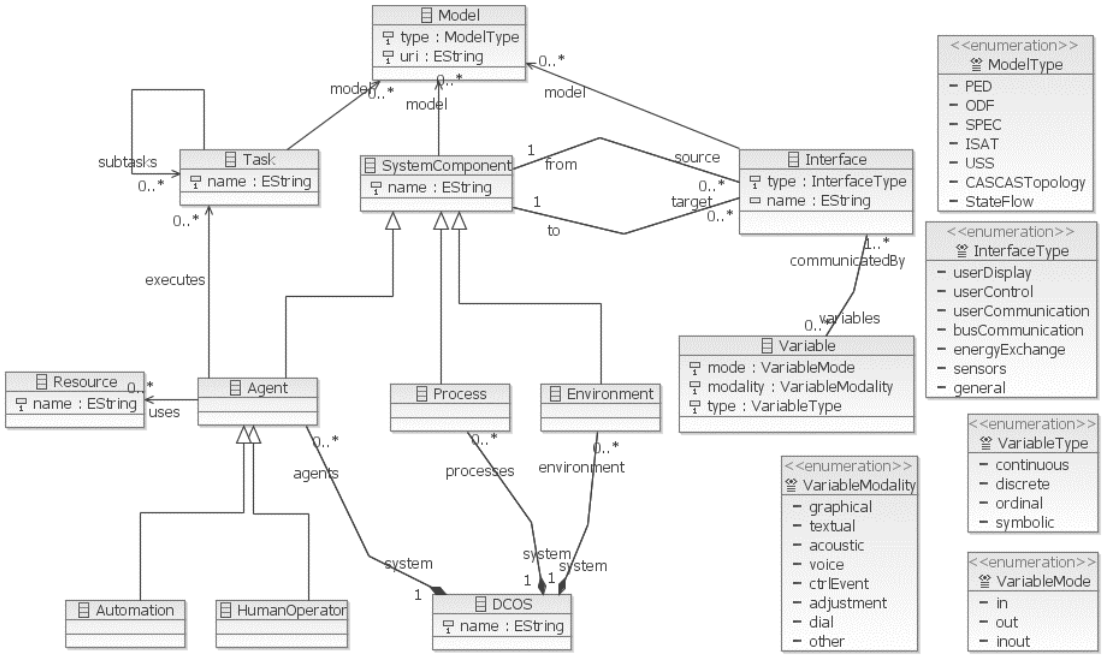


Abbildung 10: Modell für die Beschreibung der Komponenten im Projekt VASCO

Schritt 4 des VASCO – Vorgehens beinhaltet die Identifikation bzw. die Erstellung des Modells passend zu den in Schritt 2 adressierten Komponenten. Für die durch Menschen durchgeführten Aufgaben innerhalb des zu betrachtenden Prozess werden basierend auf den Regelwerken, z.B. für die Flugregeln, die einzelnen Aktivitäten (im Modell mit "Task" bezeichznet) in eine hierarchische Struktur gebracht. Pro Aktivität wird im Anschluss eine Prozedur definiert, welche die genauen Vorgaben enthält wie genau der Mensch die Aktivität auszuführen hat. Für diesen Zweck wird eine Sammlung von ODF (Operations Data File) Prozeduren und Referenz-Informationen eingesetzt. Eine Prozedur ist dabei als ein Set von Instruktionen beschrieben, welches durch Personal mit speziellem Training, wie das Bodenpersonal, aber auch das Personal an Bord, benutzt wird. Neben einer textuellen / graphischen existiert eine XML

(Extensible Markup Language) Repräsentation. Mittels dieser können Checklisten, Ablauflogiken oder auch parallele und gemeinsame Aktivitäten beschrieben werden.

Die timeline-basierten Planungssysteme haben zu den bisher vorgestellten Techniken besonders den Vorteil einer konkreten Ressourcenzuordnung (Z1) und die Möglichkeit der Ausführung (Z3). Eine Werkzeugunterstützung (Z5) ist zwar gegeben, auf Grund der Komplexität der Systeme ist jedoch die Bedienbarkeit für den Anwendungsfall in diesem Kontext nicht geeignet. Letzteres trifft ebenso auf den Analyseansatz auf dem Projekt VASCO zu, welches zudem noch Schwächen in der Darstellung zeigt.

2.2 Techniken der Prozessmodellierung

Nach der DIN ist ein Prozess ein "Satz von in Wechselbeziehung oder Wechselwirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt" [De11a]. Dabei verlangen diese eine Zuordnung von Ressourcen wie Personal oder Material. Ein Geschäftsprozess ist nach [DS03] eine Menge von logisch miteinander verknüpften Aufgaben, mit dem Ziel ein definiertes Geschäftsergebnis zu erreichen. Dies deckt sich mit der Definition von Pall, welche besagt, dass ein Prozess "die logische Organisation von Menschen, Material, Energie, Equipment und Verfahren innerhalb von Arbeitsaktivitäten bestimmt, um ein spezifisches Endresultat (Arbeitsergebnis) zu erreichen" ist [Pa87]. Nach Scheer werden "Geschäftsprozesse (…) aus einer zusammengehörenden Abfolge von Unternehmensverrichtungen zum Zwecke der Leistungserstellung gebildet" [Sc01]. Laut [BS04] ist ein Prozess "die inhaltlich abgeschlossene, zeitliche und sachlogische Folge von Aktivitäten, die zur Bearbeitung eines betriebswirtschaftlich relevanten Objekts notwendig sind."

[St06] identifiziert aus den oben aufgeführten Definitionen im weiteren Sinne folgende Gemeinsamkeit:

- Mit Geschäftsprozessen werden ein Ziel oder auch mehrere Ziele verfolgt, die sich aus den Unternehmenszielen (bzw. der Unternehmensstrategie) ableiten
- Ein Geschäftsprozess lässt sich in Teilaufgaben zerlegen
- Die Teilaufgaben werden von Aufgabenträgern wahrgenommen, die wiederum verschiedenen Organisationseinheiten angehören
- Für die Erfüllung der Geschäftsprozesse sind Unternehmensressourcen notwendig (z.B. Personal, Material, Finanzen),
- Ein Geschäftsprozess (z.B. Auftragsabwicklung) tangiert oft mehrere Abteilungen bzw. Funktionsbereiche (z.B. Beschaffung, Produktion oder Vertrieb) und liegt somit oftmals "quer" zur klassischen Aufbauorganisation

- Geschäftsprozesse benutzen in der Regel Informationsträger (z.B. eine Auftragsbestätigung) zu ihrer Realisierung

Die Geschäftsprozessmodellierung eignet sich für die Kommunikation, Darstellung und Dokumentation von Prozessen und dient ebenfalls als Grundlage für die Analyse und Optimierung dieser [Le95], [MOS09], [BS04].

Im weiteren Verlauf dieser Arbeit wird Prozessmodellierung synonym zu Geschäftsprozessmodellierung benutzt.

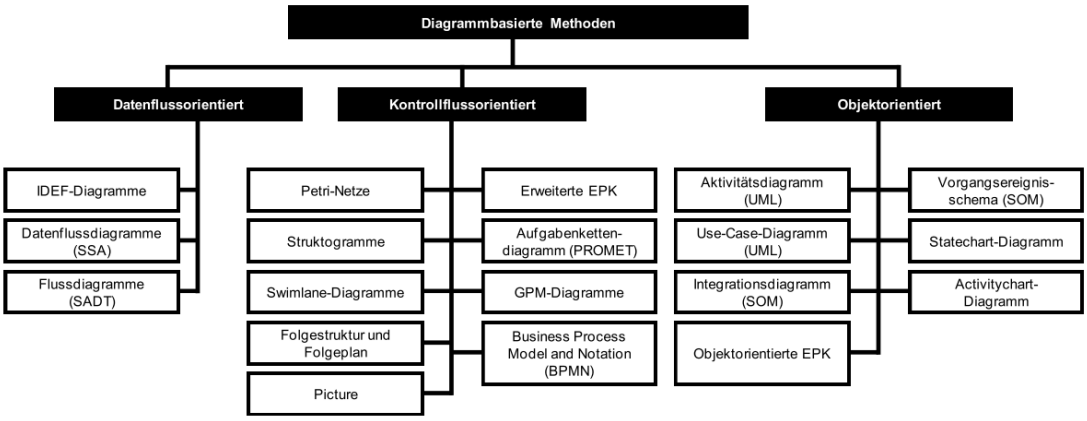


Abbildung 11: Diagrammbasierte Methoden der Geschäftsprozessmodellierung [Ga10]

Es steht eine Vielzahl an verschiedenen Methoden und Sprachen für die Prozessmodellierung zur Verfügung. Abbildung 11 zeigt eine Übersicht über die diagrammbasierten Methoden. In [EOP13] wurden verschiedene Modellierungssprachen aus einer kognitiven und einer technischen Perspektive hin bewertet und analysiert. Die als für den Fokus dieser Arbeit als relevant identifizierten Ansätze werden nachfolgend zusammenfassend gelistet und erläutert. Einführend wird zunächst auf die Petri-Netz-Theorie eingegangen, da Vielzahl an derzeit existierenden Modellierungssprachen für die Gestaltung von Prozessmodellen sich auf die diese Theorie aus dem Jahre 1962 zurückführen lassen:

- (High-Level) Petri-Netze
- (erweiterte) Ereignisgesteuerte Prozesskette (EPK)
- Business Process Modeling and Notation (BPMN 2.0)
- UML-Aktivitätsdiagramm

In seiner Dissertation definierte Carl Adam Petri durch mathematische Formeln eine Methode, um die Modellierung, Analyse und Simulation von verteilten, dynamischen Systemen zu ermöglichen, sowie Nebenläufigkeit und das Wirken zwischen Prozessen abzubilden, die **Petri-Netz-Theorie** [SWD08]. Die Basis-Konstrukte stellen dabei die *Stellen* (Zustände, ggf. mit Marken/Tokens) und *Transitionen* (Zustandsänderungen/-übergänge, Ereignisse) dar.

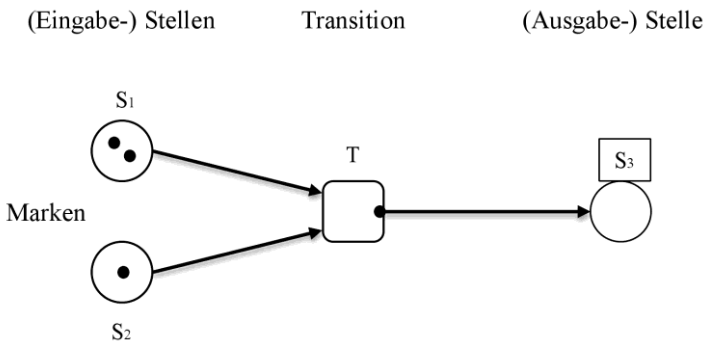


Abbildung 12: Beispiel eines Petri-Netzes

Abbildung 12 zeigt ein Beispiel für eine Transition in einem Petri-Netz, eine Stelle (S) wird als Kreis, eine Transition (T) als Rechteck dargestellt. Durch die Verbindung mit gerichteten Kanten werden diese in eine Ablaufsequenz gebracht. Dabei ist zu beachten, dass nur nicht-gleichartige Konstrukte miteinander verbunden werden können. Die Ausführung einer Transition erfolgt gemäß der Schaltregel, dass jeweils eine Marke von einer Eingabestelle entnommen und jeweils eine Marke den Ausgabestellen hinzugefügt wird. Wird eine Kante zudem gewichtet, entspricht die Anzahl der zu entnehmenden und platzierenden Marken der Größe der Gewichtung. Je nach Auftreten der Konstrukte innerhalb eines Netzes wird dieses als eines der in Abbildung 13 veranschaulichten Strukturelemente verstanden.

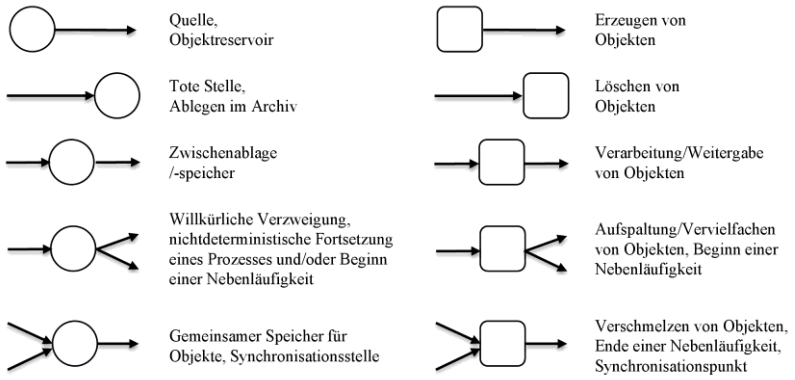


Abbildung 13: Strukturelemente von Petri-Netzen

Bei dem praktischen Einsatz von Petri-Netzen traten oft Probleme mit zu großen und komplexen Modellen auf. Neben dem damit verbundenen sehr hohen Aufwand für die Modellierung fehlte die Möglichkeit Zeit, Kosten und Daten in dem Modell abzubilden. Erst verschiedene Erweiterungen in den 80er Jahren führten zu einem verbreiteten Einsatz dieser Technik in der Praxis. So können durch die Kolorierung der Marken einzelnen Objekten Attribute zugeordnet werden oder durch die Hinzunahme von Zeitaspekten Dauer und Verzögerungen in Abläufen dargestellt werden.

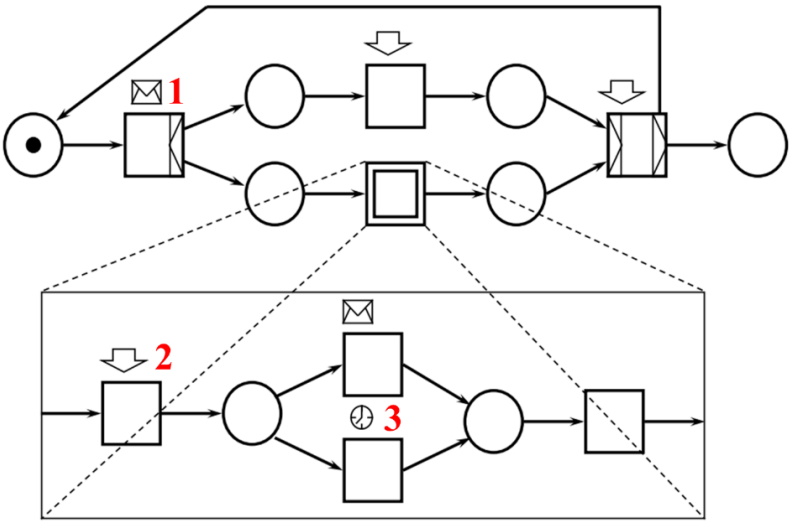


Abbildung 14: Prozessdefinition mittels Petri-Netzen

In der Veröffentlichung [Zh01] wird ein Framework für die Modellierung von militärischen Feldzügen, welche auf einem operationellen Leven basieren, mit Hilfe von kolorierten Petri-Netzen präsentiert. Die Erweiterung um ein Hierarchie-Konzept ermöglicht die Darstellung auf verschiedenen Abstraktionsebenen, indem einzelne Netzelementen durch ein Subnetz ersetzt werden. Abbildung 14 zeigt eine exemplarische Prozessdefinition mit Petri-Netzen, welche bereits Erweiterungen um Aspekte von Workflowsystemen enthalten, wie z.B. die Abbildung von externen Events (1: Nachrichten, Anruf), Nutzeraktionen (2) oder auch Zeitaspekten (3: Dauer, Zeitpunkt) [vv00].

Im Besonderen durch die zuletzt vorgestellte Erweiterung ist eine Abbildung von Prozessen und Arbeitsschritten (Z 1) mittels Petri-Netzen mehr als hinreichend möglich. Lediglich die fehlende visuelle Darstellung konkreter Zuordnung zu verschiedenen Akteuren ist in diesem Kontext als Schwachstelle zu identifizieren. Eine weitere Stärke stellt hier die Ausführbarkeit (Z3) dar, ebenso die stark vertretene Werkzeugunterstützung (Z5). Für eine Verwendung im übergeordneten Ziel dieser Arbeit fehlt jedoch der komplette Kontext bezüglich der Identifizierung und Bewertung von Gefahren und der Ergänzung um Schutzmaßnahmen (Z2).

Die Ereignisgesteuerte Prozesskette (**EPK**) ist eine graphische Modellierungstechnik die 1992 von Keller, Nüttgens und Scheer innerhalb eines Forschungsprojektes der SAP AG entwickelt wurde [KNS92] und darüber hinaus von einer Vielzahl an Unternehmen zur Modellierung, Analyse und Neugestaltung von Geschäftsprozessen genutzt wurde. Die EPK ist ein wesentlicher Bestandteil der Architektur integrierter Informationssysteme (ARIS), welche Scheer erstmals 1991 in einem Buch beschrieben hat [Sc91]. Innerhalb von ARIS dient die EPK der graphischen Beschreibung von komplexen Prozessen, indem der Arbeitsablauf durch eine Folge

von Ereignissen und Funktionen sowie logischen Operatoren beschrieben wird (vgl. Abbildung 15) [Ro96].

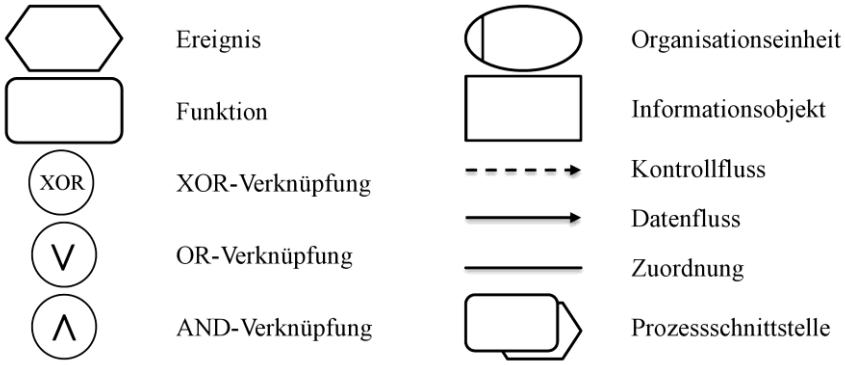


Abbildung 15: Grundelemente einer Ereignisgesteuerten Prozesskette (EPK)

Funktionen sind aktive Prozesselemente, welche eine Aufgabe oder Tätigkeit in einem Unternehmen beschreiben. Sie transformieren dabei Input- in Output-Daten von einem Anfangszustand zu einem resultieren-den Zustand. Seit der Erweiterung (e)EPK kann durch eine Organisationseinheit der Akteur, der die Funktion durchführt, beschrieben werden. Informationsobjekte repräsentieren den Daten-Input und –Output für diese [SS04]. Events sind passive Elemente und stellen wirtschaftliche oder technische Ereignisse dar. Sie stoßen Funktionen an und beschreiben unter welchen Bedingungen diese arbeiten oder zu welchen Zuständen diese führen.

Verknüpfungen werden dazu benutzt um den logischen Ablauf eines Prozesses auszudrücken. Dabei entspricht die AND-Verknüpfung einer Parallelisierung eines Ablaufes, der XOR-Operator dient der Modellierung von Alternativen. Die Verknüpfung mittels OR lässt beide eben beschriebenen Pfade zu. Durch Prozessschnittstellen am Anfang oder am Ende einer EPK können vor- bzw. nachgelagerte Prozesse verknüpft werden.

In Bezug zu der Abbildung von Prozess- und Arbeitsschritten (Z1) verhält es sich bei EPK ähnlich wie bei den zuvor vorgestellten Petri-Netzen: lediglich die fehlende visuelle Darstellung konkreter Zuordnung zu verschiedenen Akteuren ist in diesem Kontext als Schwachstelle zu identifizieren. Auch die Werkzeugunterstützung (Z5) ist in diesem Fall hervorzuheben. Bei EPK handelt es sich jedoch primär um eine Visualisierung von Prozessen, als um eine Sprache für die Ausführung dieser, weshalb es Schwächen bei der Ausführbarkeit (Z3) gibt. Ebenso fehlt hier für eine Verwendung im übergeordneten Ziel dieser Arbeit eine geeignete Unterstützung für die Identifizierung und Bewertung (Z2) von Gefahren und der Ergänzung im Schutzmaßnahmen (Z3).

Mit der Business Process Modeling Notation verfolgte die BPMI (Business Process Management Initiative) zunächst die Entwicklung eines Standards für die Modellierung von WebService- und Geschäftsprozessen [ORM03]. Im Fokus der Entwicklung stand dabei eine verständliche Notation für Fachanwender für das Skizzieren von Prozessen, welche von technischen Entwicklern genutzt werden sollten, um diese in bereits existierende ausführbare Sprachen, wie z.B. BPEL4WS (Business Process Execution Language for Web Services), BPML (Business Process Modeling Language) oder BPEL (Business Process Execution Language), zu transformieren. Der seit 2006 von der OMG (Object Management Group) anerkannte Standard [Al09] wurde initial in der Spezifikation 1.0 im Jahre 2004 von Stephen A. White vorgestellt [Wh04]. Bei der Entwicklung von BPMN wurden die wesentlichen Konzepte von anderen Geschäftsprozessmodellierungssprachen, wie UML-Aktivitätsdiagram, Integrated Definition (IDEF) und EPK vereint [Br08].

Neben der Einführung neuer Diagrammtypen (Choreographie-und Konversationsdiagramm) wurde mit der **BPMN 2.0** (seitdem Business Process Modeling and Notation) die Semantik für das Prozessdiagramm mittels UML spezifiziert. Ebenso wurde eine Ausführungssemantik definiert, inklusive Transformationsregeln in das BPEL Format, sodass die Interpretation und Ausführbarkeit von BPMN Modellen genau beschrieben ist. Mit der Veröffentlichung von BPMN 2.0.1 im Jahr 2013 wurde die Business Process Model and Notation ein ISO / IEC 19510: 2013-Standard. Die Kernelemente der Notation ähneln den Grundkonzepten von EPK, Aktivitäten, Ereignisse und Gateways. Durch die Verwendung von Swimlanes ist jedoch ein genaueres Abbilden der Verantwortlichkeiten möglich. Abbildung 16 zeigt die BPMN 2.0 Notation auf einem Blick, für weiterführende Informationen wird [Gö11] oder [FR14] empfohlen.

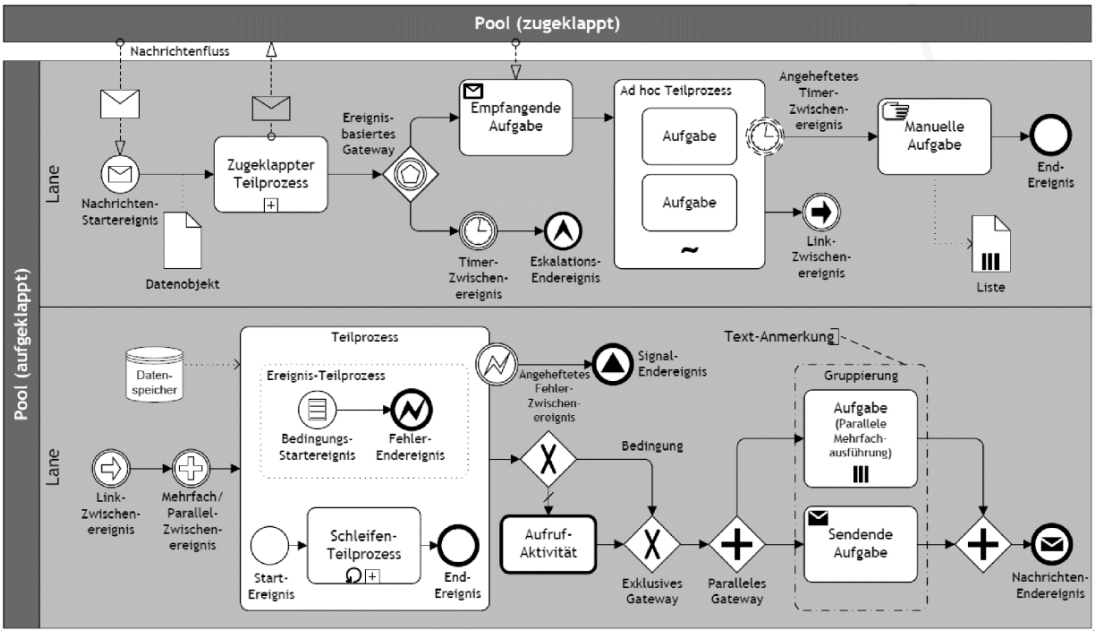


Abbildung 16: BPMN 2.0 Notation auf einen Blick [Ob11]

BPMN 2.0 punktet im Besonderen mit der visuellen Darstellung von Prozess- und Arbeitsschritten (Z1), da das Grundprinzip hierbei bereits eine Zuordnung von diesen zu verschiedenen Akteuren vorgibt. Sowohl die Werkzeugunterstützung (Z5), als auch die Ausführbarkeit (Z3) ist durch die starke Verbreitung von BPMN gegeben. Auch hier fehlen jedoch Grundkonzepte für die Integration von den Gefahren-Aspekten (Z2 & Z3)

Mit dem Aktivitätsdiagramm, einem Verhaltensdiagramm für ablauforientierte Sprachkonzepte der Unified Modeling Language (UML), können verschieden Arten von Abläufen, wie z.B. Geschäftsprozesse, Workflows oder auch Programmabläufe beschrieben werden. Der Fokus, des unter anderem auf Petri-Netzen basierenden Sprachkonzeptes, liegt auf prozedurale Verarbeitungsaspekten, die mittels Kontroll- und/oder Datenflüssen zwischen Aktionen spezifiziert werden.

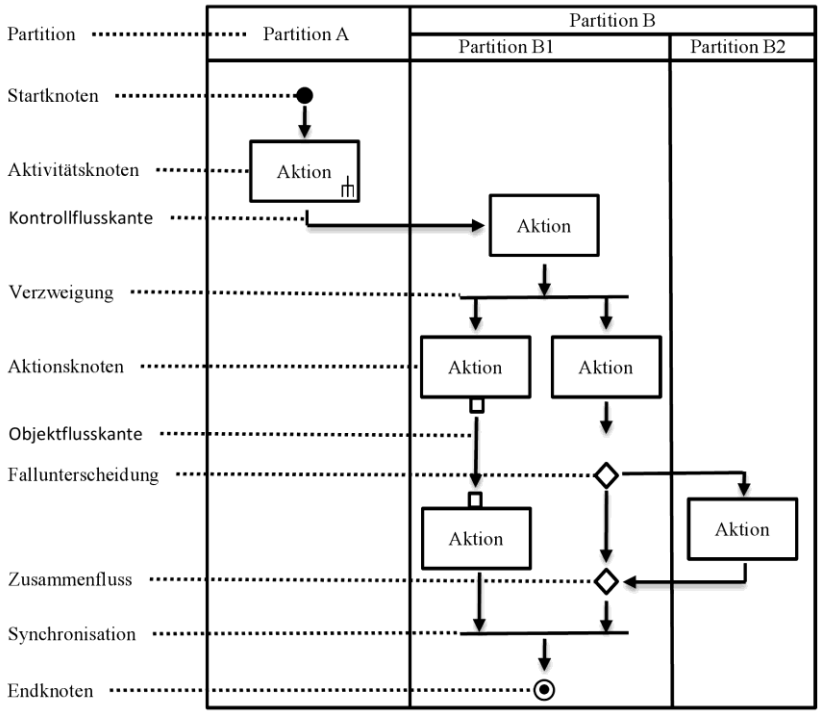


Abbildung 17: Syntax des UML – Aktivitätsdiagrammes

In Abbildung 17 werden die wesentlichen Konzepte der **UML-Aktivitätsdiagramm**-Syntax beschrieben. Das Grundprinzip ist ein gerichteter Graph, bei dem die Aktivitäten die Knoten, die Kontroll- und Datenflüsse die Kanten darstellen. Während die Kontroll- und Datenflüsse die potentiellen Abläufe festlegen, spezifizieren die Aktionen das benutzerdefinierte Verhalten auf verschiedenen fein-granularen Ebenen.

Eine Aktivität wird entweder durch atomaren Aktionen (vgl. Aktionsknoten), oder aber durch die gesamte Verhaltensbeschreibung eines Aktivitätsdiagrammes (vgl. Aktivitätsknoten) beschrieben. Diese können optional mit zusätzlichen Parametern bzw. Vor- und Nachbedingun-

gen ergänzt werden. Gekennzeichnet wird der Beginn eines Ablaufs einer Aktivität durch einen Startknoten (bzw. Initialknoten). Ein Endknoten kennzeichnet hingegen das Ende aller Abläufe einer Aktivität. Die Kanten verbinden Knoten und definieren dadurch die möglichen Abläufe einer Aktivität. Es wird dabei zwischen Kontrollflüssen, welche die reine Reihenfolge zwischen Nachfolger- und Vorgängerknoten ausdrücken und Datenflüssen unterschieden, welche zusätzlich die Datenabhängigkeit zwischen Nachfolger- und Vorgängerknoten beschreiben.

Um nebenläufige Abläufe zu modellieren werden Parallelisierungsknoten eingesetzt. Eine Verzweigung spaltet diese auf, durch eine Synchronisation werden diese wieder zusammengeführt. Fallunterscheidungen können durch Entscheidungsknoten modelliert werden, optional können dort für Kanten Überwachungsbedingungen definiert werden, um das Entscheidungsverhalten zu spezifizieren. Selbiges gilt für Vereinigungsknoten durch den ein Zusammenfluss ermöglicht wird. Wie bei BPMN können Knoten und Kanten innerhalb einer Aktivität gruppiert werden. Diese Gruppierungen werden Partition genannt. Auch hier ist dabei eine Verschachtelung möglich. Weiterführende Informationen über das UML Aktivitätsdiagramm können den Werken von Christoph Kecher [Ke05] bzw. Bernd Österreich [Ös12] entnommen werden.

In Bezug auf die Eignung für die Prozessmodellierung im Kontext dieser Forschungsarbeit stellt sich das UML – Aktivitätsdiagramm gleich geeignet wie BPMN 2.0 dar. Ebenfalls unterstützt diese Modellierungssprache die visuelle Darstellung von Prozess- und Arbeitsschritten (Z 1), auch eine Zuordnung von diesen zu verschiedenen Akteuren ist durch die Partitionierung gegeben. Die Werkzeugunterstützung (Z5) und auch die Ausführbarkeit (Z3) sind durch die starke Verbreitung ebenfalls gegeben. Auch hier fehlen jedoch Grundkonzepte für die Integration von den Gefahren-Aspekten (Z2 & Z3).

Hergeleitet aus den Grundsätzen der ordnungsgemäßen Modellierung [Sc98] wurden in [EOP13] verschiedene Modellierungssprachen aus einer kognitiven und einer technischen Perspektive, im Rahmen eines vom Bundesministerium für Wirtschat und Technologie finanzierten Projekts, analysiert. Die aus den Grundsätzen der Klarheit, Richtigkeit und Vergleichbarkeit hergeleitete und an Carlsson angelehnte kognitive Perspektive veranschaulicht neben dem persönlichen Konsens die visuelle Ausdrucksstärke der Elemente der verschiedenen Notationen. Sie "drückt die Fähigkeit des Modellkonsumenten aus, dass Ergebnismodell zu erfassen und zu verstehen". Die technische Perspektive "betrachtet die Möglichkeiten der Geschäftsprozessmodellierungssprachen, die Anzahl, Bedeutung und mögliche Einsatzmöglichkeiten der Notationselemente" [EOP13].

Die technische Perspektive wird bei der Analyse in folgende Teilperspektiven unterteilt:

- *Funktionell:* Widerspiegelung der ausgeführten Notationselemente wie Aktivitäten und deren Möglichkeiten der Spezifizierung als Teilprozesse
- *Organisatorisch:* Zuordnung von wem Funktionen ausgeführt werden, z.B. Prozessbeteiligte, Organisationseinheiten oder Rollen (sowohl menschlich, als auch technisch)
- *Verhaltensbezogen*: die Möglichkeit sequentielle bzw. parallele Kontrollflüsse von Notationselementen und UND-, ODER- bzw. exklusive ODER-Verknüpfung darzustellen
- *Informell:* Repräsentation von Informationsobjekten, wie Daten, Artefakte, Produkte oder Objekte, welche in einem Prozess erzeugt, benötigt oder verändert werden
- *Unterstützend:* Der Verbreitungsgrat, die Austauschfähigkeit, die Existenz von Modellierungswerkzeugen und die automatische Ausführung der Modellierungssprachen

Bei der folgenden Aufschlüsselung der kognitiven Perspektive richten sich die Autoren nach [Mo07]. Dabei wird auf Grund der Komplexität auf die Untersuchung der kognitiven Integration verzichtet:

- *Unterscheidbarkeit*: Unterscheidbarkeit der Notationselemente, sowohl in ihrer Bedeutung, als auch ihre Ausdrucksstärke
- *Limitierte Wahrnehmung*: die Möglichkeit der Modellierung über mehrere Abstraktionsebenen hinweg
- *Direkte Wahrnehmung*: die spontane bzw. natürliche Interpretation des Ergebnismodells
- *Struktur*: Gruppierung der Notationselemente und der dadurch erreichten Übersichtlichkeit
- *Identifikation*: das Verhältnis zwischen dem Ergebnismodell und des präsentierten Sachverhaltes, sowie die Modellierungskonventionen und deren Bedeutung
- *Ausdrucksfähigkeit*: Anzahl der Notationselemente in Beziehung zu den entschlüsselnden Informationen
- *Einfachheit*: Anzahl der Modellierungskonventionen der einzelnen Modellierungssprachen

Die in Abbildung 15 zusammenfassende Übersicht über die Ergebnisse der Bewertung zeigt, dass sowohl in der kognitiven, als auch in der technischen Dimension sich BPMN als geeignetstes Mittel der Wahl für die Geschäftsprozessmodellierung eignet.

Dimension / Perspektive	Item	EPK	BPMN	UML-Aktivitätsdiagramm
Kognitive Dimension (50%)	Summe	0	2	-1
	Unterscheidbarkeit	o	o	-
	Limitierte Wahrnehmung	o	+	o
	Direkte Wahrnehmung	o	o	o
	Struktur	-	+	-
	Identifikation	o	o	o
	Ausdrucksfähigkeit	+	+	o
	Einfachheit	o	-	+
Technische Dimension (50%)	Summe	-0,8	3	1,2
Funktionelle Perspektive (20%)	Summe	0	2	1
	Aktivität	o	+	o
	Teilprozess	o	+	+
Organisatorische Perspektive (20%)	Summe	-1	2	2
	Intern	-	o	o
	Extern	o	o	o
	Organisationseinheit	o	+	+
	Rolle	o	+	+
	Software	o	o	o
Verhaltensbezogene Perspektive (20%)	Summe	0	3	0
	AND	o	+	o
	OR	o	+	o
	XOR	o	+	o
Informelle Perspektive (20%)	Summe	0	4	1
	Ereignis	o	+	o
	Datenfluss	o	+	+
	Informationsressource	+	+	+
	Softwareressource	-	+	-
Unterstützende Perspektive (20%)	Summe	-1	4	2
	Werkzeugunterstützung	-	+	o
	Austauschbarkeit	-	+	+
	Verbreitungsgrad	+	+	+
	Automatische Ausführbahrkeit	o	+	o
Final Score		-0,4	2,5	0,1

Abbildung 18: Bewertung der kognitiven und technischen Perspektiven [Mo07]

2.3 Verfahren für prozessorientierte Gefährdungsbeurteilung

Wie den Abschlussbemerkungen der in Kapitel 2.2 vorgestellten Techniken der Prozessmodellierung zu entnehmen ist, unterstützen diese in ihrer Reinform keine Konzepte der Gefährdungsbeurteilung, welche jedoch einen wesentlicher Aspekt für die Erreichung der Ziele Z2

& Z3 in dieser Forschungsarbeit darstellen. In diesem Abschnitt werden verschiedene Verfahren für prozessorientierte Gefährdungsbeurteilungen untersucht, welche auf den Techniken auf dem vorausgehenden Kapitel aufbauen:

- Risiko-Detailmodell für (e)EPK
- Risk-extended Business Process Models
- Value-Focused process engineering
- Risikomanagement in der Logistik
- Risk-Oriented Process Evaluation

In [BO02] wurde basierend auf (e)EPK ein prozessorientiertes **Risiko-Detailmodell** vorgestellt. Die Erweiterung des Modells um ein Objekttyp für die Darstellung einzelner Risiken an den jeweiligen Funktionen dient der Abbildung aller notwendigen Informationen für eine Risikoanalyse und -bewertung. Durch die Erweiterung dieses Modells um interorganisationsspezifische Aspekte durch [KKS04] lassen sich Ansprechpartner, sowie die Folgen festhalten, die mit der Realisierung eines Risikos verbunden sind (Abbildung 19).

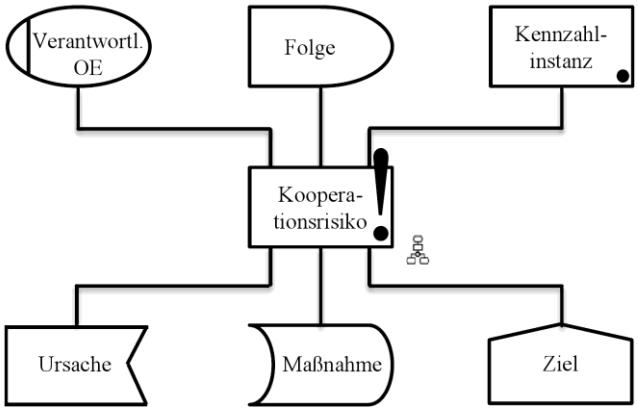


Abbildung 19: Detailmodell für die Analyse und Bewertung von Risiken [KKS04]

Zudem lassen sich Ursachen, (präventive) Maßnahmen zur Minimierung der Eintrittswahrscheinlichkeit, sowie quantitative und qualitative Zielsetzungen dokumentieren. Durch die Verortung der Risiken innerhalb des Prozesses kann neben einer allgemeinen ebenfalls eine prozessorientierte Risikoberechnung durchgeführt werden, indem die Häufigkeit des Ausführens einer Funktion innerhalb eines Prozesses mit der relativen Eintrittswahrscheinlichkeit in Beziehung gebracht wird. Da dies eine Erweiterung zu (e)EPK darstellt gelten auch hier die dort identifizierte, positive Zielabdeckung in Bezug auf die Prozessdarstellung (Z1) und Toolunterstützung (Z5). Dieser Ansatz erweitert diese jedoch zusätzlich für die Ziele bezüglich der Identifikation und Bewertung von Gefahren (Z2) und die Integration von Schutzmaßnahmen (Z3). Es fehlt jedoch ein Konzept für eine ganzheitliche Bewertung des Prozesses. Auch die Schwächen hinsichtlich der Ausführbarkeit sind hier gegeben.

In [Co09] wird ein System, ein Verfahren und ein Werkzeug vorgestellt (**Risk-extended Business Process Models**), welches Risikomanagement-Konzepte in geschäftsprozess-Metamodell integrieren, indem eine Reihe von Metamodell-Erweiterungen zu standardisierten Prozessmodellierungssprachen für die direkte Integration von Risikoinformationen definiert werden. Neben den in Form eines Datenmodells beschriebenen Erweiterungen wird ebenfalls eine Methode beschrieben, wie eine graphische Prozessmodellierung konstruiert werden kann in der operationelle Risikoinformationen im Kontext von Geschäftsprozessen erstellt werden können. Das Ziel der Gesamtmethodik ist die Identifikation und Quantifizierung von Risiken und deren Effekte auf die Prozessobjekte. Exemplarisch wird dies in der Veröffentlichung anhand einer Erweiterung von BPMN in der Version 1.1 demonstriert (vgl. Abbildung 20).

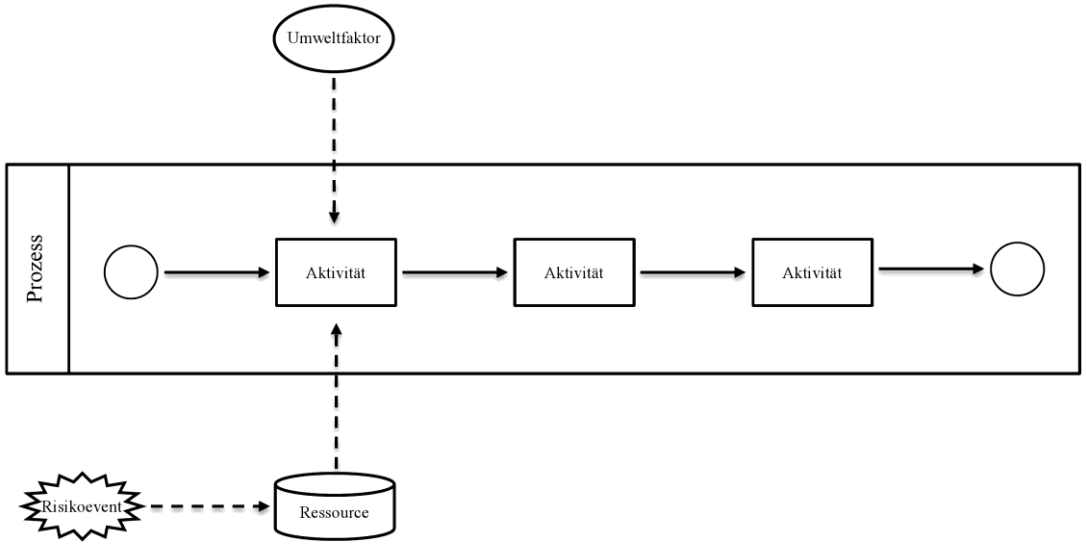


Abbildung 20: Erweiterung von BPMN (v. 1.1) um Risikoinformationen nach [Co09]

Zunächst wird die in dem Prozess durchzuführende Arbeit, wie bei BPMN vorgesehen, durch eine Aneinanderreihung von Aktivitäten mit den zu der Arbeitsbeschreibung spezifischen Attributen beschrieben. Im Folgenden werden Ressourcen und die damit verbundenen Funktionen für die Ausführung dieser Aktivitäten und zusätzlich notwendige Vorbedingungen für diese definiert. Dies beinhaltet ebenfalls messbare Leistungsindikatoren und einem arbeitsbezogenen Qualitätskriterium. Weiter werden potenzielle Risikoereignisse (inklusive einer Frequenz und einem Schweregrad) definiert, die sich auf die Leistungsindikatoren auswirken können und den Ressourcen zugeordnet werden. Im letzten Schritt werden für jede Aktivität externe Faktoren, wie z.B. Umweltfaktoren, als Vorbedingung für die Ausführung definiert.

Diese Art der Risikomodellierung und Modellerweiterung bietet ein strukturiertes Vorgehen für die Identifikation von Risiken innerhalb von Prozessen, indem zunächst mit einem standardisierten Prozessmodell begonnen wird und mittels iterative Durcharbeiten der einzelnen Arbeitsschritte hinsichtlich möglicher Fehler die Ursachen identifiziert werden (inklusive de-

ren tendenziellen Effekte auf die Prozessperformance). Die Methode führt demnach ein Vokabular für die Risikokonzepte und deren mögliche Beziehungen und Kombinationen ein und ermöglicht die Erstellung von systematischen Verfahren, die Ursachen und Auswirkungen der Fehler aufzuzeigen. Weiterhin ermöglicht dieses Verfahren quantitative Modelle für die Bewertung der Risiken, basierend auf einem mit einer Gefahrenbeschreibung erweiterten graphischen Geschäftsprozessmodell. Dieses wurde zudem entworfen, um den Einfluss von Risiken auf die Prozessperformance, beispielsweise durch Bayes'sches Netze oder ereignis-diskrete Simulationen, zu berechnen.

Neu hinzugebracht zu der standardgemäßen Nutzung von BPMN sind in diesem Ansatz die Möglichkeiten der Modellierung von Umweltfaktoren und Risikoaspekte bezüglich eingesetzter Ressourcen, welche die Zielabdeckung von der Prozessmodellierung (Z1) und die Anpassung an spezifische Projekte im Vergleich zu BPMN 2.0 verstärkt und diese um das Ziel der Identifizierung und Bewertung von Gefahren (Z2) erweitert. Da sich diese Erweiterung jedoch auf BPMN 1.1 bezieht und zudem keine semantische bzw. syntaktische Beschreibung hinsichtlich der Ausführung der hinzugefügten Elemente vorliegt, ist weder eine automatische Ausführung des Prozesses selbst, noch eine damit einhergehende Überprüfung der Risiken möglich.

Der werteorientierte, prozesstechnische Ansatz (**Value-Focused process engineering**) nach [Ch06] ergibt sich aus der Integration von existierenden ziel- und prozess-orientierten Modellierungstechniken und wurde erweitert, um eine multidisziplinäre Sicht auf Risiken zu ermöglichen. Es bietet die Möglichkeit die komplementären Ansichten von Risiko- und Prozessmanagement näher zusammen zu bringen. Das wesentliche Ziel des risikoorientierten Prozessmanagements ist es Geschäftsprozessanalytiker bei dem Vergleich verschiedener Prozesskonfigurationen bei der Auswahl der Konfiguration mit geringerem Risiko zu unterstützen. Das Framework vereint die jeweiligen Stärken der Prozessmodellierung und der entscheidungsbasierender Risikomanagement-Ansätze zu einer quantitativen Bewertung der Risiken im Zusammenhang mit folgenden geschäftsspezifischen Belangen:

- Eine ganzheitliche Identifizierung und Darstellung der Risiken innerhalb der Geschäftstätigkeiten
- Dem Verständnis über Zusammenhänge zwischen Risiken, Unternehmensziele und Geschäftsaktivitäten
- Quantifizierung und Analyse der Risiken im Rahmen der Gesamtunternehmensziele zur Erleichterung von Prozess-Design und Evaluierung

Das konzeptuelle Modell baut auf EPK auf, wesentliche Unternehmensziele werden dabei in einem Top-Down Verfahren genauer spezifiziert um relevante Prozessrisiken zu identifizieren. Um sicherzustellen, dass Risikoziele berücksichtigt werden, wird "Risikominimierung von Prozessversagen" als höhergestelltes Ziel in der grundlegenden Ziel-Hierarchie fest verankert. Darüber hinaus kann Geschäftstätigkeit genauer untersucht werden, um weitere relevante Risiken für Aktivitäten zu identifizieren.

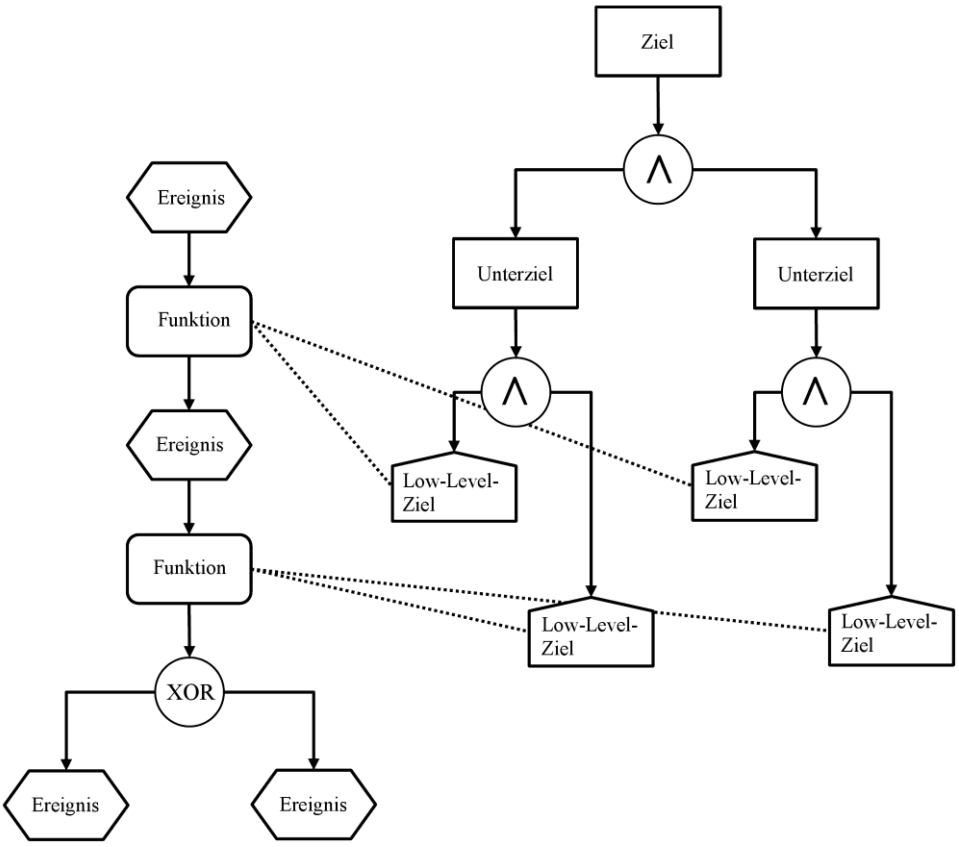


Abbildung 21: Zielhierarchie verbunden mit einem Prozessablauf (EPK) nach [Ch06]

Das Resultat ist eine Zielhierarchie, die mit einem Prozessablauf verbunden ist. Um die relativen Vorteile der verschiedenen Prozesskonfigurationen beurteilen zu können, werden für die einzelnen Ziele Messeinheiten bestimmt. Anschließend wird eine Wertfunktion konstruiert, welche den Präferenzen und Werten des Entscheidungsträgers entspricht. Dies ermöglicht die Berechnung des Nutzens der einzelnen Konfigurationen.

Auch hier gelten wie für die (e)EPK Erweiterung die identifizierten, positiven Zielabdeckung in Bezug auf die Prozessdarstellung (Z1) und Toolunterstützung (Z5). Neben der Integration bezüglich der Identifikation und Bewertung von Gefahren (Z2) existiert eine Konzeption für eine übergeordnete, ganzheitliche Bewertung dieser für den gesamten Prozess. Aber auch hier sind die Schwächen hinsichtlich der Ausführbarkeit gegeben.

Die Grundlage der prozessbezogenen **Risikomanagement in der Logistik** nach [Hu03] ist die Prozessdokumentation mit (e)EPK. Diese wird im Rahmen der Risikoanalyse auf mögliche unerwünschte Ereignisse hin untersucht. Zur Identifikation und Bewertung möglicher Ursachen für diese Ereignisse wird die Fehlerbaumanalyse verwendet (vgl. Abbildung 22).

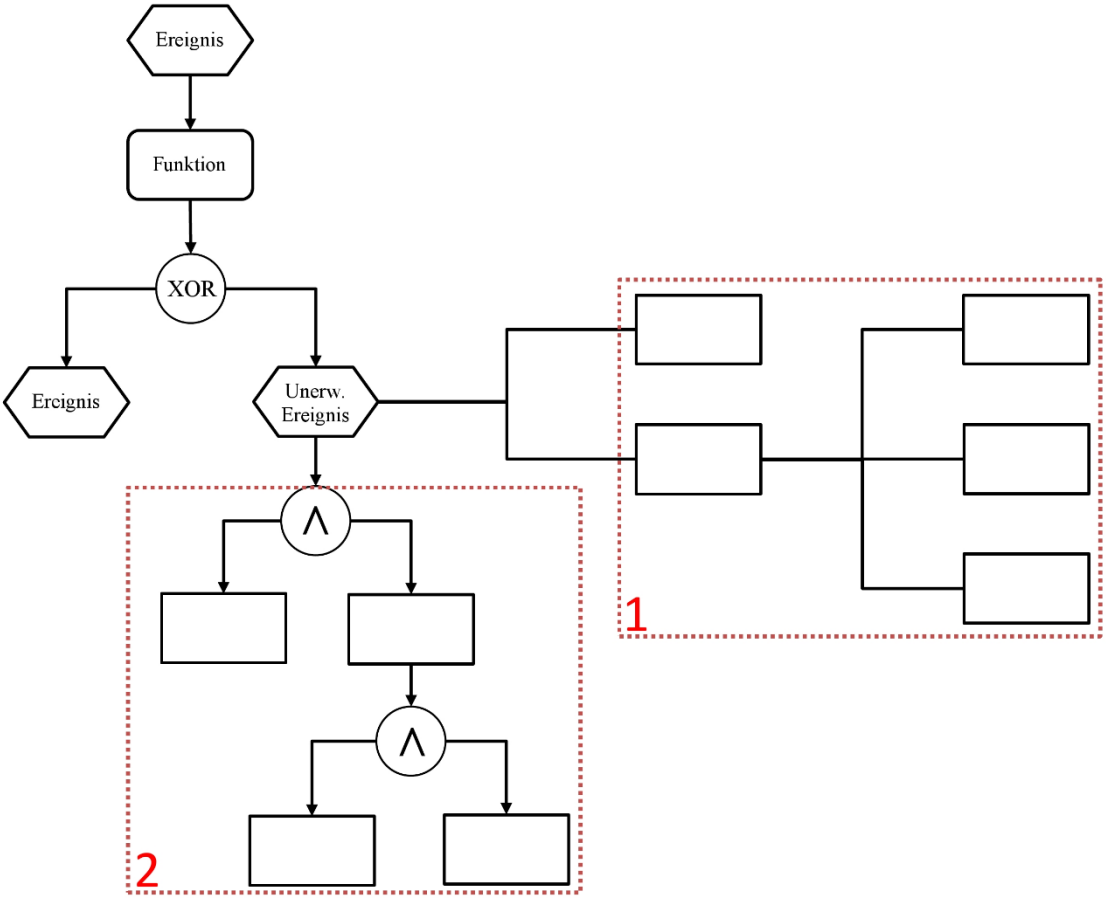


Abbildung 22: prozessbezogene Risikoanalyse nach [Hu03]

Mit diesen können logische Zusammenhänge von Ursachen in einer hierarchischen Anordnung dargestellt werden. Dabei entspricht das oberste Element dieser Hierarchie das unerwünschte Ereignis, für welches über logische Zusammenhänge ("oder" und "und" Gatter) ein Fehlerbaum entwickelt wird, welcher über Zwischenereignisse eine Rückführung des Fehlers auf einzelne Ursachen ermöglicht. Durch die Bestimmung von Wahrscheinlichkeiten für die einzelnen Ursachen kann anschließend durch eine Rechenvorschrift die Eintrittswahrscheinlichkeit für das unerwünschte Ereignis errechnet werden. Neben der Identifikation von Risiken werden mittels Ereignisbaum die Folgen der unerwünschten Ereignisse und der mit diesen verbundenen Konsequenzen dargestellt (vgl. Abbildung 21). Der Aufbau und die spätere Berechnung der Folgen erfolgt dabei äquivalent zu den Fehlerbäumen. Diese Erweiterung von (e)EPK ermöglicht eine dedizierte Untersuchung von Fehlerursachen und möglichen Folgen, die aus diesen für einzelne Funktionen resultieren. Auch hier gelten als eine Erweiterung der Modellierungssprache die erwähnten Zielabdeckungen (Z1, Z5 & Z2). Ein Vorteil gegenüber

den anderen Risiko-Erweiterungen für (e)EPK in Bezug auf die Ausführbarkeit (Z3) bringt dieser Ansatz jedoch auch nicht mit sich.

Die ROPE (**Risk-Oriented Process Evaluation**) Methode kombiniert die Funktionalitäten von Geschäftsprozessmanagement mit Risikomanagement und Business Continuity Managment (Notfallmanagement), um eine ganzheitliche Evaluierung von Geschäftsprozessen, nicht nur hinsichtlich der ökonomischen Effizient, sondern auch hinsichtlich ihrer Robustheit und Sicherheit zu ermöglichen [JTQ07]. Die Basis hierfür ist die Differenzierung von Geschäftsprozessaktivitäten in vier Elemente (Bedingungen, Aktionen, Ressourcen und Umwelt) und einen prozessorientierten Modellierungsansatz von Bedrohungen, präventiver und reaktiver Gegenmaßnahmen, sowie Maßnahmen zur Wiederherstellung (vgl. Abbildung 23).

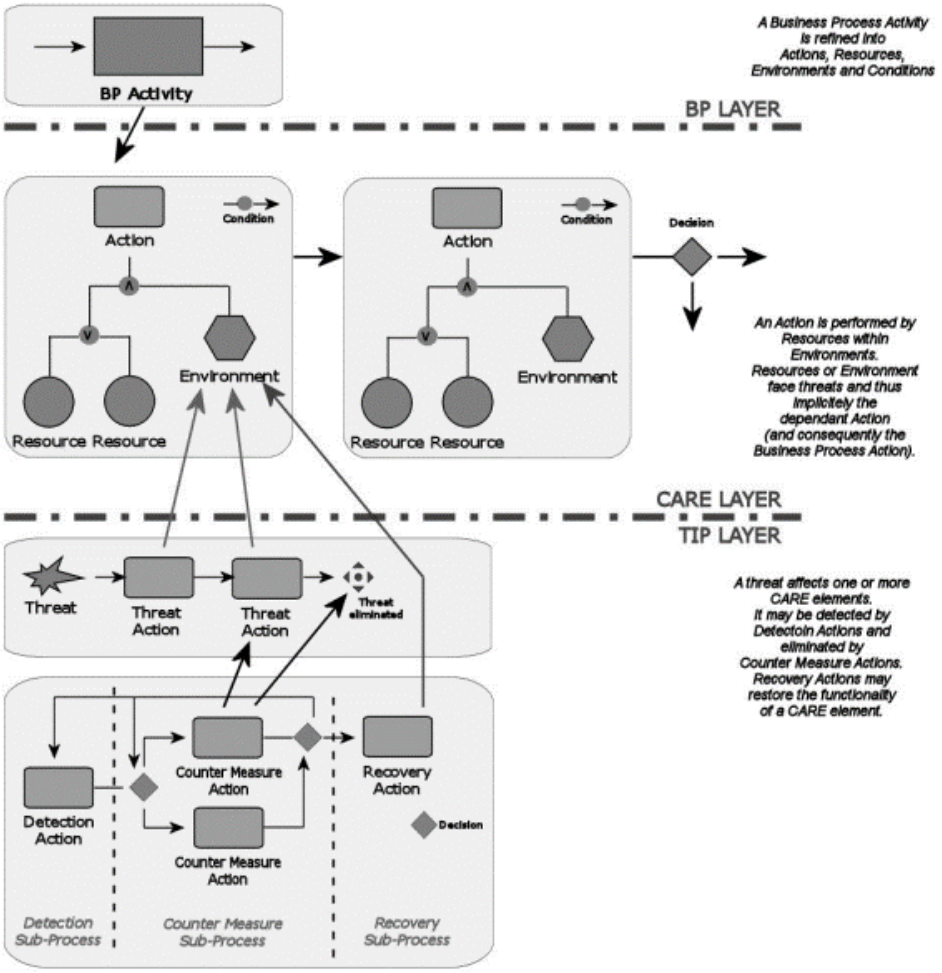


Abbildung 23: ROPE (Risk-Oriented Process Evaluation) Methode [JTQ07]

Für jede Art von Elementen werden nun potenzielle Bedrohungen sowie deren Management- und Wiederherstellungsstrategien identifiziert. Diese werden durch drei verschiedene Sub-Prozesse genauer spezifiziert:

- *Detektion:* Innerhalb dieser Sub-Prozesse wird die Bedrohung erkannt. Die Auswirkungen der Bedrohung sind eng mit der Erfassungszeitpunkt verbunden. Das "Wann" und "Wie" der Entstehung bestimmt die aufzurufenden Gegenmaßnahmen.
- *Gegenmaßnahmen:* Gegenmaßnahmen beeinflussen direkt die Bedrohung, sind diese nicht in der Lage diese zu beenden, wirken sich diese direkt auf das Element der Aktivität aus.
- *Wiederherstellung:* Beschreibt den Prozess, um die Funktionalität eines Elementes wiederherzustellen.

Durch eine Simulation mittels Pfadanalyse können für Bedrohungen alle möglichen Pfade identifiziert werden. Dabei können "Kosten" durch die Ermittlung der Häufigkeit des Auftretens während der Ausführungszeit ermittelt werden. Die Simulation der Bedrohungen zielt auf die Bestimmung und Visualisierung der Auswirkungen von diesen und deren Gegenmaßnahmen auf die kontinuierliche Ausführung eines Geschäftsprozesses ab. Es ermöglicht die Identifizierung der betroffenen Elemente und deren Zustandsänderungen und bestimmt zusätzlich den Zeit- und Kostenaufwand der Bedrohungen, die diesen zugeordnet sind. Im Vergleich zu den bisher vorgestellten Erweiterungen für Prozessmodellierungssprachen für Risikoaspekte, basiert der ROPE Ansatz auf einer generischen Beschreibung einer Geschäftsprozessaktivität. Der Ansatz legt den Schwerpunkt im Besonderen auf die Identifikation und Bewertung von Gefahren (Z2) und deren Ausführbarkeit (Z3). Neben einer geeigneten ausführbaren Prozessmodellierungssprache (Z1) fehlt bei diesem Ansatz jedoch primär die Werkzeugunterstützung (Z5).

2.4 Anforderungsabdeckung und Handlungsbedarf

Die Übersicht über die Verfahren und Techniken für die Erstellung von Gefährdungsuntersuchungen in den maritimen und artverwandten Domänen zeigt neben einer Vielfalt an unterschiedlichsten Techniken im Besonderen die jeweilige Spezialisierung auf einzelne Aspekte. Während vereinzelte Ansätze existieren, welche die menschliche Perspektive mit einbeziehen, liegt der Fokus jedoch stehst primär auf der Beschreibung und Analyse von Systemen. Eine Methode für die ganzheitliche Beschreibung und Gefahrenanalyse für soziotechnische Systeme ist vom Autor nicht gefunden worden. Prozesse erlauben, im Vergleich zur funktionalen Beschreibung eines Systems oder eines Unternehmens, eine systematische Charakteristik, die sowohl vollständig ist und auch den Kontext des Handelns recht gut wiedergibt. Es hat sich gezeigt, dass sich auf diese Art Systeme bzw. Unternehmen analysieren, verstehen, optimieren und gestalten lassen. Dies wird ebenfalls dadurch bekräftigt, dass die Normenreihe ISO 9000 ff im Jahr 2000 auf eine Prozessbeschreibung umgestellt wurde [De11a]. Für eine prozessorientierte Risikoanalyse wurden verschiedene Erweiterungen vorgestellt, welche jedoch nicht

alle notwenigen Aspekte in der Breite abdecken. Keiner der Ansätze ermöglicht eine Beschreibung von Gefahren und deren Ursachen, wie sie für die Zieldomäne erforderlich sind, noch ist ein ganzheitlicher Ansatz für eine qualitative und quantitative Gefahrenbewertung vorhanden.

In den jeweiligen Kurzbeschreibungen der identifizierten verwandten Arbeiten wurde bereits jeweils auf die Zielabdeckung dieser eingegangen. Tabelle 2 fasst diese in einer Darstellung zusammen. Dabei wurde für die einzelnen Bewertungen in drei verschiedenen Abdeckungsgraden differenziert: ein "X" steht für eine überwiegende Erfüllung des Ziels, ein "O" für eine teilweise und "-" für keine Abdeckung.

	Z1. Prozessorient. Systembeschreibung	Z2. Identifizierung von Gefahren	Z3. Quan. & qual. Gefährdungsbeurteilung	Z4. Durchgängige, integrierte Methodik	Z 5. Werkzeugunterstützung
Funktionale Sicherheit nach ISO 26262	-	O	-	O	-
Leitfaden nach Gruber et al	O	-	-	O	-
Offshore Code of Practice	-	-	-	O	-
Vorgehen nach ISO 29400	-	-	-	O	-
Events and Conditional Factors Analysis	O	O	-	-	-
Man, Technology and Organisation	O	-	O	-	-
Sequentially Timed Events Plotting Procedure	O	-	O	-	-
timeline-basierte Planung (L&R)	O	X	O	-	O
VASCO	O	-	O	-	O
(High-Level) Petri-Netze	X	O	-	-	O
(erweiterte) Ereignisgesteuerte Prozesskette	X	O	-	-	-
Business Process Modeling and Notation	X	O	-	-	O
UML-Aktivitätsdiagramm	X	O	-	-	O
Risiko-Detailmodell für (e)EPK	X	O	O	O	-
Risk-extended Business Process Models	X	O	X	-	O
Value-Focused process engineering	X	O	O	-	-
Risikomanagement in der Logistik	X	O	O	-	-
Risk-Oriented Process Evaluation	X	-	X	O	O

X = zum größten Teil erfüllt , O = teilweise erfüllt, - = nicht erfüllt

Tabelle 2: Darstellung der Zielabdeckung verwandter Arbeiten

Wie der Tabelle 2 zu entnehmen ist, erfüllt keines der identifizierten, verwandten Arbeiten alle Ziele. Zudem ist festzustellen, dass die Ansätze mit einer quantitativ hohen Zielabdeckung,

die adressierten Ziele nur in einem niedrigeren Level erfüllen. Der sich hieraus ergebende Handlungsbedarf wird in den folgenden drei Eingruppierungen dargestellt:

Prozessorientierte Systembeschreibung

Fast alle Vorgehen für Gefahrenbeurteilungen sind systemorientiert. In den verschiedenen vorgestellten Ansätzen, wie der von Gruber et al oder der ISO 9001, wird zwar eine Prozessorientierung vorgeschlagen, jedoch gehen die Autoren nicht ins Detail, wie genau dies geschehen hat, bzw. was das nun genau bedeutet. Die Techniken der Prozessmodellierung mit teilweise verfügbarer Erweiterung um Aspekte der Gefahrenbeurteilung decken hingegen bedingt diesen Bereich ab. Demnach gibt es Konzepte um personenbezogene Arbeitsabläufe zu beschreiben. Ein wesentliches Manko ist jedoch die fehlende Einbeziehung von Systembestandteilen, wie eingesetzte Ressourcen oder aber Qualifikationen des Personals. Dies ist jedoch notwendig, um eine Aussage über die Gefährdungen während dieser Operationen treffen zu können. Um eine Identifikation und Analyse von Risiken per Simulationsverfahren zu ermöglichen, muss zudem die Ausführbarkeit der Prozesse gegeben sein. Nur durch die Einbeziehung der eben aufgeführten Aspekte ist Ziel **Z1** zu Adressieren.

Gefahrenidentifikation, -analyse und -bewertung

Es gibt verschiedene Vorgehen und Techniken, um für unterschiedliche Arten der Systembeschreibung eine Gefahrenidentifikation durchzuführen. Dies geschieht teilweise auch unter Berücksichtigung personenbezogener Arbeiten. Die Betrachtung geschieht jedoch lose gekoppelt vom Gesamtablauf, d.h. es werden nur einzelne Arbeiten für sich genommen beurteilt und nicht eine Kombination aus mehreren. Viele Gefahren entstehen zudem erst dann, wenn Arbeiten parallel oder aber in einer bestimmten Reihenfolge durchgeführt werden. Wenn eine Aussage über eine komplette Operation getroffen werden soll, fehlt daher auch meistens eine hinreichende Transparenz, um das Erlangen dieser nachvollziehen zu können. Eine Besonderheit in der Offshore-Branche ist zudem der Einfluss der äußeren Umweltbedingungen. Da es sich hier nicht um ein geschlossenes System handelt, sollte bei der Bewertung der Gefahren der äußere Einfluss, wie z.B. Wind oder Wellengang, hinzugezogen werden. Um eine Identifikation und Analyse von Risiken per Simulationsverfahren zu ermöglichen, muss zudem eine eindeutige Beschreibung dieser existieren. Dies ist notwendig um die Ziele **Z2** und **Z3** zu adressieren.

Toolgestützte Methodik

Es wurden verschiedene Ansätze eingeführt, wie eine Gefährdungsbeurteilung durchgeführt werden kann. Problematisch bei diesen ist jedoch die Überführung dieser in die Anwendung. So werden keine konkreten Techniken empfohlen wie einzelne Schritte durchzuführen sind,

was zudem bedingt, dass eine Werkzeugunterstützung nur teilweise vorhanden ist. In der Praxis kommen daher zumeist Microsoft Word oder Microsoft Excel zum Einsatz, welche jedoch hohe Schwierigkeiten bei der Integration der verschiedenen Schritte und ebenfalls der Wiederverwendbarkeit mit sich bringen. Eine integrierte, werkzeugunterstützte Methodik ist daher notwendig um die Ziele **Z4** und **Z5** zu adressieren.

3 MOPhisTo - Maritime Operation Planning Tool

In diesem Kapitel wird die modellbasierte Methodik zur Entwicklung bzw. Planung von sicheren Offshore-Operationen vorgestellt. Der durchgängige Ansatz für die Erstellung von Arbeitsschutz- und Sicherheitskonzepten wird unterstützt durch eine prototypische Implementierung des Modellierungswerkzeugs MOPhisTo. Die Vorschriften und Standards in Bezug auf die Gesundheits- und Sicherheitsaspekte in der Offshore-Industrie bilden dabei die normative Grundlage für den Planungsprozess. Dabei werden die wesentlichen Schritte des HSE-Managements in eine modellbasierte Methode überführt und unterstützen somit die (maritimen) Domänen-Experten bei der Entwicklung von HSE-Plänen für Offshore-Operationen oder anderen maritimen Manövern.

3.1 Methodenübersicht

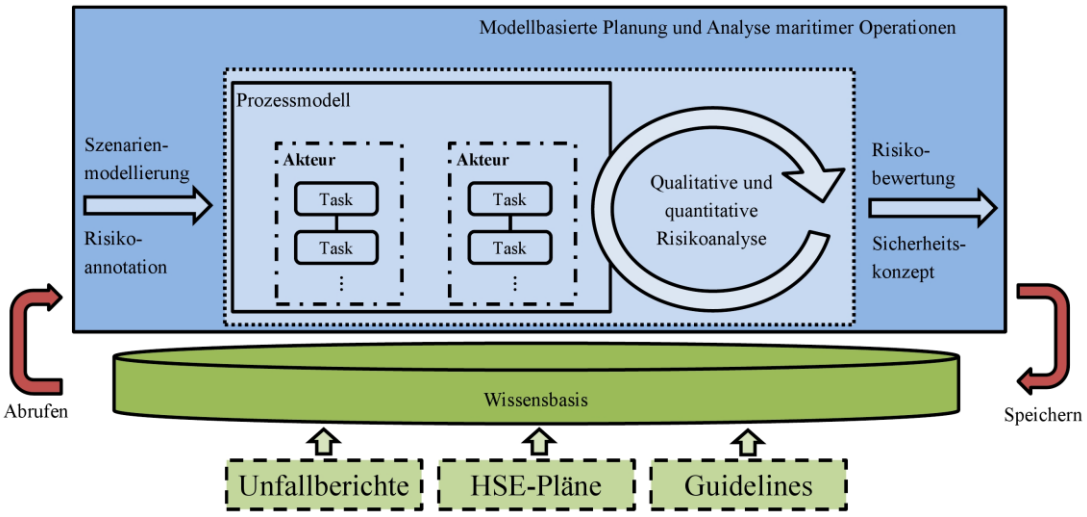


Abbildung 24: Modellbasierte Planung und Analyse maritimer Operationen

Abbildung 24 zeigt eine Übersicht über die Methode für die modellbasierte Planung und Analyse von maritimen Operationen. Ausgangpunkt für ist hierbei eine Beschreibung des Szenarios, welches später analysiert und bewertet werden soll. Darunter versteht sich die Aufschlüsslung der Akteure (z.B. Kapitän oder die Decksbesatzung), eingesetzter Ressourcen (z.B. Schiffe für den Personentransfer, oder die PSA) und Umweltfaktoren (wie Strömung, Wind und Wellengang). Aufbauend auf dieser statischen Beschreibung werden die einzelnen Prozeduren, welche im HSE-Konzept erläutert werden müssen, definiert. Dies geschieht mit Hilfe eines Prozessmodells. So werden für jeden beteiligten Akteur Arbeitsabläufe sequenziell erstellt. Das Modell soll hierbei die Möglichkeit bieten durch Entscheidungsknoten, parallele bzw. unterschiedliche Varianten von Tätigkeiten zu beschreiben und diese durch Kommunikation mit anderen Akuteren im Gesamtablauf zu synchronisieren.

Im weiteren Schritt werden die nun im Ablauf definierten Tätigkeiten, je nach Abhängigkeit zu dem durchführenden Akteur und der eingesetzten Ressourcen, mit möglichen Gefahren und deren Ursachen annotiert. Diese nun existierende Beschreibung des Systems kann nun als Grundlage für eine Bewertung für ein Sicherheitskonzept genutzt werden. Für diese Bewertung stehen verschiedene Verfahren aus dem Bereich der Risikoanalyse bereit. Eine Wissensbasis soll dabei die gesamte Methode unterstützen. Es kann demnach bei allen Schritten auf bereits gesammeltes Expertenwissen zurückgegriffen werden. Dies beinhaltet eine strukturierte Sammlung von Daten aus Unfallberichten, Expertenwissen und vorherigen geplanten Operationen. Die modellbasierte Methode unterstützt Anwender bei der Erstellung von HSE-Plänen, indem sie eine Methodik mit festgelegten Handlungsschritten vorsieht und Werkzeuge bereithält. Basierend auf einer Beschreibung der Umgebung und den dort vorherrschenden Bedingungen kann ein editierbares Prozessmodell entwickelt werden, welches die sequentiellen Abläufe der simulierten maritimen Operation anhand von Tätigkeiten, relevanten Akteuren und deren Interaktion darstellt. Mittels einer lernenden Wissensbasis können Gefährdungen und deren Ursachen den einzelnen Tätigkeiten, sowie Akteuren zugeordnet und mithilfe einer Fehlerbaumanalyse die Eintrittswahrscheinlichkeit für Gefährdungen einer Operation bewertet werden.

Bevor in diesem Kapitel genauer auf die Konzepte der modellbasierten Methodik eingegangen wird werden zunächst im Abschnitt 3.2 die Anforderungen an diese definiert. Für ein besseres Verständnis, wird in dem darauffolgenden Unterkapitel ein Anwendungsbeispiel eingeführt, welches im Verlauf der Beschreibung der Methodik die einzelnen Handlungsschritte veranschaulicht.

3.2 Anforderungen

Für die Erreichung der aufgeführten Ziele werden diese im Weiteren in Form von Anforderungen definiert. Diese werden in die bereits im Handlungsbedarf eingeführten Gruppierungen aufgeteilt: "Prozessorientierte Systembeschreibung", "Gefahrenidentifikation, -analyse und -bewertung" und "Toolgestützte Methodik". Diese dienen im Besonderen dem Aufzeigen des notwendigen Funktionsumfanges des zu entwickelnden Modellierungswerkzeuges für den Domänenexperten.

Prozessorientierte Systembeschreibung

A1 *Ressourceneinsatz:* Ausgangspunkt einer jeden Erstellung eines Sicherheitskonzeptes ist die Beschreibung des Systems auf dessen Basis diese durchgeführt werden soll. Es ist eine statische Beschreibung aller Elemente, die innerhalb eines konkreten Sicherheitskonzeptes referenziert werden [Ad12], [PS13]. Diese sind zumeist abhängig von den projektspezifischen Gegebenheiten, wie den Standort oder den generellen Aufbau des Offshore-Windparks (z.B. Art der Gründungsstrukturen oder Modell der eingesetzten Windkraftanlagen) und den Subunternehmern, die die Tätigkeiten durchführen. Oft definieren diese Gegebenheiten den benötigten Einsatz von Schiffstypen und den dazu gehörenden Einsatzmöglichkeiten. (vgl. **Z1** - Prozessorientierte Systembeschreibung)

A2 *Personaleinsatz:* Durch eine explizite Aufschlüsslung des Personals, welches an der Operation beteiligt ist, kann eine genauere Analyse bezüglich potenzieller Gefahren durchgeführt werden [Ba13]. Hierfür dienlich ist zudem die konkrete Auflistung der Mindestanforderungen an Ausbildungsstandards für die durchgeführten Tätigkeiten. (vgl. **Z1** - Prozessorientierte Systembeschreibung)

A3 *Personenbezogene Beschreiung von Tätigkeiten*: Im Vordergrund eines Schutz- und Sicherheitskonzepts steht der "Schutz des menschlichen Lebens und der menschlichen Gesundheit" [Sc13]. Durch die Beschreibung von normativen Abläufen einzelner Offshore-Operationen ist eine prozessorientierte Risikobewertung möglich. Dabei ist eine "Beurteilung je nach Art der Tätigkeit vorzunehmen" [Bu96], [Sc12]. Somit muss das Konzept Aspekte zu personenbezogenen Beschreibung von Tätigkeiten enthalten [Ad12], [Ba13]. Zudem ist auf die Flexibilität hinsichtlich des Detailgrades zu achten und es sind Konzepte notwendig, um für unterschiedliche Situationen Handlungsalternativen hinterlegen zu können. Der Kontrollfluss der Arbeitsbeschreibung sollte neben sequentiellen, auch kompliziertere Konstrukte, wie z.B. eine bedingte Verzweigung, Nebenläufigkeit, Rücksprünge usw. abbilden können. Auch hinsichtlich Bedingungen sollte das Modell komplexere, kontextbezogene Abläufe ermöglichen, um beispielsweise zeitliche Aspekte oder vor allem Prozessabhängigkeiten zu den Umweltbedingungen zu integrieren. (vgl. **Z1** - Prozessorientierte Systembeschreibung)

A4 *Kommunikation:* Der Austausch von Nachrichten dient neben dem Informationsaustausch der Synchronisation von Arbeitsabläufen an denen mehrere Personen beteiligt sind [Ge14]. (vgl. **Z1** - Prozessorientierte Systembeschreibung)

Gefahrenidentifikation, -analyse und -bewertung

A5 *Konzept zur Risikobeschreibung:* Für die prozessorientierte Risikoanalyse und -bewertung ist eine Annotation relevanter Prozesselemente mit Risikobeschreibungen notwendig. Hierfür ist eine einheitliche Definition unumgänglich. Besonders die von den Praxispartnern bereitgestellten Dokumente weisen in diesem Punkt erhebliche Schwachstellen vor. So wird häufig die eigentlich zu beschreibende Gefahr mit Ursachen und Folgen vermischt [Ad12], [Ba13]. (vgl. **Z2** - Konzept für die Identifizierung von Gefahren)

A6 *Nachvollziehbarkeit (Transparenz):* Es sollte die Möglichkeit bestehen, den Aufbau und die Risikobewertung nachzuvollziehen, um auch prüfen zu können, ob alles seine Richtigkeit hat oder Änderungen vorgenommen werden müssen. Ist die Nachvollziehbarkeit gewährleistet, können auch Redundanzen und Unstimmigkeiten in der Logik des HSE-Plans vermieden werden. Dies würde zu einer größeren Transparenz führen und den Arbeitsaufwand verringern. Dafür sollen in dieser Methodik für einzelne identifizierte Gefahren die entsprechenden Ursachen im System hinterlegt werden [Ad12], [Ba13]. (vgl. **Z2** -Konzept für die Identifizierung von Gefahren)

A7 *Konzept zur Bewertung:* Die Risikobewertung quantifiziert die Gefährdung für einzelne Arbeitsschritte, Akteure und den Gesamtprozess. Das Risiko ist hierbei definiert als eine Kombination der Eintrittswahrscheinlichkeit und der Schadensschwere. Mit dem ermittelten Ergebnis können Schwachstellen in dem Prozess identifiziert werden [Ad12], [Ba13], [Ge14]. (vgl. **Z3** - Quantitative und quantitative Bewertung der Gefahren)

A8 *Betriebssituation:* Wie beschrieben, wird das Risiko lediglich auf der Grundlage der Wahrscheinlichkeit und der Schadensschwere bewertet. Als eine Anforderung wird bereits das konkrete Zuordnen von Ressourcen für Arbeitsschritte eingeführt, welche für eine spezifischere Bewertung dienlich ist. Zudem wurde jedoch ein weiterer Aspekt identifiziert: je nach Situation sollte das Risiko bzw. das darin enthaltene Schadensausmaß unterschiedlich bewertet werden [Ad12]. Ein Beispiel hierfür ist Mann-über-Bord-Manöver. Sollte dieser Fall eintreten, ist nicht nur relevant, ob eine Schutzausrüstung getragen wird, sondern auch, ob dieser Vorfall im Hafen bzw. in Küstennähe, oder innerhalb eines Offshore-Windparks eintritt. Je nachdem variiert der Zeitpunkt des Eintreffens der Rettungskräfte zwischen 10 Minuten und zwei Stunden. Auch die Jahreszeit und der damit zusammenhängende Temperaturunterschied spielt hierbei eine wichtige Rolle. (vgl. **Z1** - Prozessorientierte Systembeschreibung / **Z2** - Konzept für die Identifizierung von Gefahren)

A9 *Ausführbarkeit:* Um eine Identifikation und Analyse von Risiken per Simulationsverfahren zu ermöglichen, muss die Ausführbarkeit der prozessorientierten Systembeschreibung und der annotierten Gefahreninformationen gewährleistet sein. [Go16] . (vgl. **Z3** - Quantitative und quantitative Bewertung der Gefahren)

Toolgestützte Methodik

A10 *Darstellung:* Ein wesentlicher Aspekt der zu entwickelnden Methode ist die Aufschlüsslung der Arbeitsschritte in Abhängigkeit zu der durchführenden Person. In der Praxis werden klassischerweise die Prozessbeschreibungen in Form eines Fließtextes aufgeführt oder teilweise in einer semi-strukturierten Form als Tabelle aufgeführt. Bei Letzteren erfolgt bereits eine Auflistung der an Prozessschritten beteiligten Personen, jedoch keine eindeutige Zuordnung zu den Arbeitsschritten. Das Unterstützungswerkzeug soll demnach eine Darstellungsform für die Prozessbeschreibung integrieren, welche für den Domänenexperten verständlich nutzbar ist [Fv13]. (vgl. **Z5** - Werkzeugunterstützung)

A11 *Wiederverwendbarkeit:* Von einer Wiederverwendbarkeit kann gesprochen werden, wenn eine Methode bzw. ein Tool die Generierung von Modellen und Datenstrukturen unterstützt, die in anderen Anwendungen wiederverwendet werden können [WJ06]. In diesem Kontext ist die Wiederverwendbarkeit für die modellgestützte Methode definiert, dass Teile von projektspezifisch erstellten HSE-Plänen wiederverwendet werden können. Dies erscheint deshalb sinnvoll, weil HSE-Pläne komplex sind und viel Arbeitsaufwand nötig ist, um diese zu erstellen. Durch die Wiederverwendbarkeit von Teilen des HSE-Plans würde man Vorlagen für neue Pläne haben, welches zu Zeitersparnissen führen würden und die Fehlerquote verringern, da die zu verwendenden Teile bereits in der Praxis genutzt und für gut befunden wurden. Bei der bisherigen Erstellung von Gefährdungsbewertungen werden zumeist generische Arbeitspläne als Grundlage benutzt. Erst durch die Integration von projektspezifisch definierten Parametern lassen sich genauere Bewertungsergebnisse erzielen. Eine Verwaltung der generischen Modellierungsartefakte in einem Repository bringt den weiteren Vorteil der zentralen Anpassbarkeit und der damit automatisch nachgelagerten Übernahme in darauf referenzierten Instanzen. Mehrmaliges Ändern, wie es klassischer weise bei unstrukturierten Beschreibungen der Fall ist, entfällt somit [Sc13], [Th12], [Le14]. (vgl **Z4** - Durchgängige Methodik / **Z5** - Werkzeugunterstützung)

A12 *Detailgenauigkeit:* Mit dieser Anforderung ist eine Variation in der Detailgenauigkeit der toolgestützten Methode gemeint. Für die Praxistauglichkeit ist dies von Bedeutung, da Experten geschildert haben, dass es sich aufgrund der Komplexität des HSE-Plans anbietet, die Genauigkeit der Details zu variieren [Le14], [SW14], [Hi14]. Für die Vorlage als Genehmigungsdokument ist ein detaillierter Plan mit allen Prozessanweisungen sinnvoll. Erfahrenen Technikern und Mitarbeitern ist vielmehr eine Darstellung des groben Prozessablaufes als Übersicht wichtig [Le14]. (vgl. **Z1** - Prozessorientierte Systembeschreibung / **Z5** - Werkzeugunterstützung)

A13 *Formale Abbildung:* Grundlage für die Methode ist eine formale Abbildung, um basierend auf den Konzepten eine entsprechende Werkzeugunterstützung zu implementieren. Eine höhere Eindeutigkeit führt zudem zu einem einheitlichen Verständnis, z.B. von Begrifflichkeiten oder Normen und somit zu einer erleichterten Kommunikation [RSD08]. Des Weiteren bedingt Anforderung *A1* die generelle Ausführbarkeit. Sind weiterhin textuelle Beschreibungen der Arbeitsanweisungen, z.B. im Rahmen eines Qualitätsmanagementhandbuchs (vgl. [De11a]), kann aus den Modellierungsartefakten die erforderliche Dokumentation generiert werden. (vgl. **Z1** - Prozessorientierte Systembeschreibung / **Z2** - Konzept für die Identifizierung von Gefahren / **Z4** - Durchgängige Methodik)

A14 *Benutzbarkeit:* Die Benutzbarkeit beschreibt den Aufwand, den ein Benutzer betreiben muss, um ein Softwareprodukt bedienen zu können. Ist das System leicht erlern- und bedienbar, so ist der Aufwand für Schulungen gering und das Produkt weist eine hohe Benutzbarkeit auf [Wa01]. Die Teilmerkmale Verständlichkeit, Erlernbarkeit und Bedienbarkeit konkretisieren die Benutzbarkeit, da das Verhalten und das Konzept des Systems verständlich sein müssen. Ebenso müssen Bedienung, als auch die notwendigen Eingaben erlernbar sein [Ke07]. Die Benutzbarkeit spielt eine wichtige Rolle, denn wenn die Bedienung für den Benutzer umständlich und mühsam ist, besteht kein Grund das Produkt weiter zu nutzen auch wenn alle anderen Qualitätsmerkmale gut sind [Wa01]. (vgl. **Z5** - Werkzeugunterstützung)

3.3 Konzeptionelles Modell

Der Forschungsansatz zielt darauf die Schritte für das HSE-Management in eine modelbasierte Planung zu überführen und somit die (maritimen) Domänen-Experten bei der Entwicklung von HSE-Plänen für Offshore-Operationen oder andere maritime Manöver zu unterstützen. Hierfür wurden prozessorientierte Modellierungskonzepte adaptiert und als Basis für das integrierte Prozess- und Systemmodell genutzt.

Zur normativen Spezifikation des Verhaltens wird ein Prozessmodell verwendet [Dr12], welches auf Konzepten von BPMN 2.0 und dem Aktivitäts-Diagramm der UML basiert. Mit diesem können Operationen beschreiben und strukturiert werden, um die verschiedenen Akteure, die Interaktion zwischen diesen und ihren Aufgaben abzubilden. Ein Prozessschritt beginnt und endet mit Events; Sequenzflüsse ermöglichen die Beschreibung einer zeitlichen Abfolge der verschiedenen Aktivitäten der Teilnehmer. Nachrichtenflüsse beschreiben Herkunft und Ziel von Nachrichten, z. B. Berichte oder Befehle, um die Aktivitäten innerhalb des Prozesses zu synchronisieren. Ressourcen sind einer Aktivität als Objekt aus dem Systemmodell zugeordnet. Das Systemmodell beschreibt die betrachteten Objekte und Umweltbedingungen. Diese sind ebenfalls für die Verwendung im Prozessmodell nutzbar, um Akteure einem spezifischen Abbild innerhalb Systems zuzuordnen. Zum Beispiel kann ein Ladeoffizier zu einem Ladeoffizier-Objekt zugeordnet werden, welches eine Position, maximale Geschwindigkeit und weitere die Analyse relevante Attribute, beispielsweise erworbene Zertifikate oder weitere Qualifikationen, besitzt.

Um das erstellte Prozessmodell hinsichtlich der Risiken zu beurteilen wurden bereits bestehende Konzepte der Offshore-Branche untersucht und zusätzlich die Praxis der Automobilbranche berücksichtigt. Die Erfahrungen im Offshore-Sektor stammen überwiegend aus Öl- und Gasanlagen. Das Wissen nicht jedoch nicht direkt auf den Offshore-Wind-Sektor angewendet werden, es bestehen zwar Gemeinsamkeiten, die meisten Risiken erheblich voneinander abweichen. Die meisten Risiken bestehen hier in Bezug auf Feuer und Explosion bei der Prüfung Öl-und Gas-Anlagen. Dies sind keine primären Risiken, wenn es um Offshore-Windenergieanlagen geht, dies gilt auch für Blowouts oder Leckagen. Neben diesen Unterschieden gibt es jedoch auch Gemeinsamkeiten zwischen diesen Arten von Offshore-Operationen. Dementsprechend wurde Vinnem [Vi07] als Quelle des aktuellen Standes der Praxis in der Risikoanalyse in Betracht gezogen. Im Einzelnen behandelt es die Schritte der QRA, die häufig auf Offshore-Operationen angewendet wird. Der Ansatz basiert auf den Normen IEC 61508 [IE10] und [IE16] IEC 61511. Ein weiterer Ansatz ist die Formal Safety Analysis, die auch für die Offshore-Sicherheitsbewertung verwendet wird [Wa02]. Es basiert auf der Zuweisung von Risiken auf drei Ebenen: unakzeptabel, so niedrig wie sinnvoll praktikabel (as low as reasonably practicable - ALARP) und vernachlässigbar. Da dieses Konzept nicht auf der Quantifizierung beruht und stattdessen eine argumentative Methode zur Risikobewertung verwendet, ist es für den Einsatz mit unserem modellbasierten Ansatz nicht geeignet. Neben diesem Ansatz ist der aktuelle Automotive-Standard von besonderem Interesse. Dieser ist auf die starke Konkurrenz zwischen verschiedenen Herstellern in dieser Branche und der großen Menge der verkauften Einheiten zurückzuführen. Infolgedessen müssen die Prozesse im Au-

tomobilsektor sehr zeit- und kostensparend sein. Um einen kostengünstigen Prozess der Risikobewertung zu erreichen, wird ein spezieller Ansatz angewendet, der in ISO 26262 [In08] definiert ist.

Eines der Konzepte aus dem Automobilsektor, welches ebenfalls im Ansatz dieser Forschungsarbeit verwendet wird, ist das der "gefährlichen Ereignisse". Ihre Verwendung ermöglicht es, Gefahren weiter zu differenzieren, indem eine Situation angeben wird, in welcher diese auftreten. Dies ermöglicht es, die Auswirkungen einer Gefährdung in einer bestimmten Betriebssituation zu bewerten, da die Auswirkungen davon abhängig sein könnten. Ein weiterer Faktor für die Risikobewertung in der Automobilindustrie ist die Kontrollierbarkeit. Die Kontrollierbarkeit einer Gefahr spiegelt die Fähigkeit wieder, Verletzungen oder Schäden durch eine rechtzeitige Reaktion auf ein gefährliches Ereignis zu vermeiden. Dies könnte dadurch erreicht werden, dass Personen, die ein Risiko auslösen könnten, alarmiert werden, dass sie sich dessen bewusst sind und die Möglichkeit haben, vorbeugende Maßnahmen einzuführen. Daher wird die Kontrollierbarkeit eines Risikos als weiteren Bewertungsfaktor in diesem Ansatz berücksichtig, welcher die Risikominderung durch die Einführung von Maßnahmen zur Sensibilisierung eines Risikos unterstützt und damit die Reduktion der Konsequenz ermöglicht.

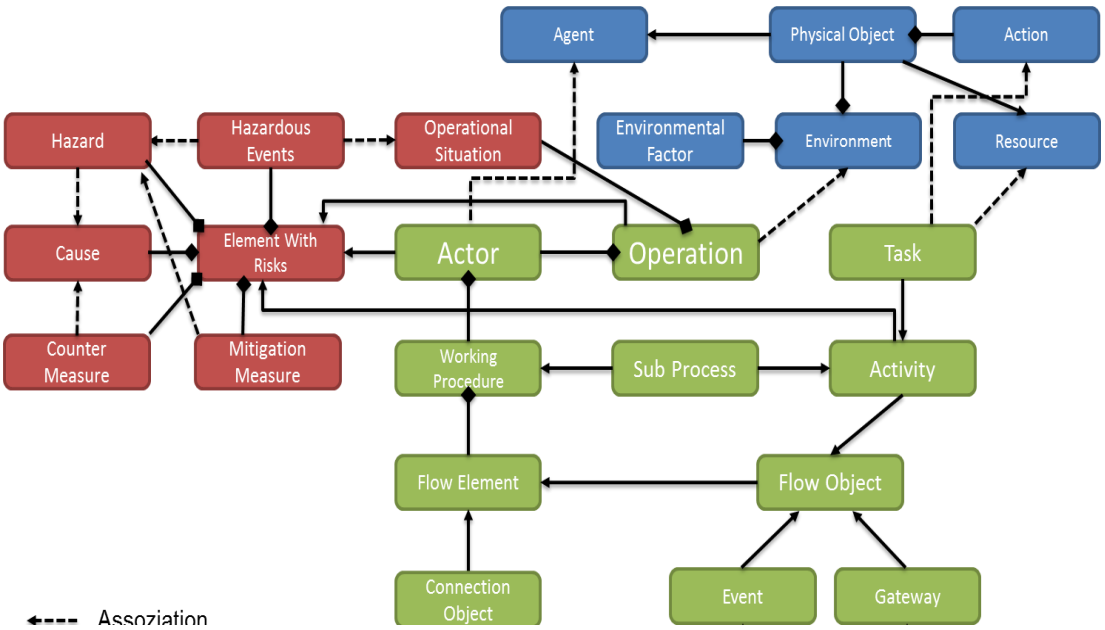


Abbildung 25: Abstrakte Darstellung des MOPhisTo Metamodells

Abbildung 25 zeigt eine abstrakte Darstellung des MOPhisTo Metamodells, auf dessen Syntax im Folgenden eingegangen wird. Diese legt die zugrundeliegende Struktur der Modellierung durch Konzepte, Beziehungen zwischen Konzepten und Integrationsbedingungen fest. Wie der Abbildung zu entnehmen ist, wurde eine Partitionierung in drei Gruppierungen von Metamodell-Elementen vorgenommen: System (blau), Risiko (rot) und Arbeitsablauf (grün).

System: Eine wesentliche Schwachstelle der in den momentan in der Praxis angewandten Methoden der Erstellung von Sicherheitskonzepten in der maritimen Domäne, ist die Nichteindeutigkeit der zu Untersuchenden Elemente, bedingt durch eine fehlende eindeutig definierte, formale Beschreibung. Je nach Erfahrung des Verfassers dieser Konzepte kann daher nicht nur der Detailgrad, mit welchem einzelne Elemente beschrieben werden, variieren, sondern vor allem ein unterschiedliches Verständnis dieser vorherrschen. Um diesem vorzubeugen wird in dem neuen Ansatz bereits bei der Beschreibung der Umgebung auf ein formales Modell eingeführt, mit dem man in der Lage ist Elemente mit ihrer Semantik eindeutig zu beschreiben. Ein System ist definiert durch ein Tupel $X = (Y, N, V, W)$ wobei gilt:

- Y ist eine endliche Menge an `PhysicalObjects`,
- N ist eine endliche Menge an `Actions`,
- V ist eine endliche Menge an `Environments`,
- W ist eine endliche Menge an `EnvironmentalFactors`.

Die Umgebung (`Environment`) bildet die Basis für die Beschreibung eines Szenarios. Diese selbst kann durch eine Karte (`Map`) ausgedrückt werden, in der sich beispielsweise der zu errichtende oder zu wartende Windpark befindet. In dieser Umgebung werden in einer Hierarchie Objekte platziert (`PhysicalObject`), die selbst wiederum durch eine Position und Ausrichtung (`Pose`) und einer Geometrie (`Geometry`) genauer spezifiziert werden. Bei diesen Objekten handelt es sich nicht nur um Ressourcen, sondern auch um das Personal, welches an der Operation beteiligt ist. Dies wird durch die Spezialisierung als ausführendes Objekt (`Agent`) erreicht. Ein solches Objekt kann Aktionen (`Action`) durchführen, was zu einer Veränderung von Objekten in der Umgebung führt. Ein Beispiel hierfür ist das Bewegen von Objekten. Als Einschränkung hierbei gilt, dass eine Aktion nur durchgeführt wird, wenn das ausführende Objekt selbst die notwendigen Fähigkeiten (`Capability`) für die Durchführung besitzt.

Risiko: Für die Darstellung der Risiken und Ursachen, und der Abhängigkeiten zwischen diesen, wird auf die Terminologie aus dem automotive Sicherheitsstandard ISO 26262 zurückgegriffen. Auch wenn dieser zunächst speziell für den Automobilbereich definiert wurde, lassen sich diese Konzepte auch auf die maritime Domäne übertragen, da die ISO 26262 selbst aus einem domänenunabhängigen Sicherheitsstandard, der IEC 61508, abgeleitet wurde. Da sich die wesentlichen Analyse-Konzepte primär auf die Systemanalyse beziehen und weniger auf ablauforientierte Gefährdungsbeurteilungen, werden lediglich die dafür übertragbaren Ansätze übertragen.

Ein Risiko ist ein Tupel $R = (H, C, B, Z, Z^M, Z^C)$ wobei gilt:

- H ist eine endliche Menge an `Hazards`,
- J ist eine endlich Menge an `HazardousEvents`,
- C ist eine endliche Menge an `Causes`,
- B ist eine endliche Menge an `OperationalSituations`,
- $relO: J \in B$ ist eine Relation zwischen einem `HazardousEvent` einer `OperationalSituation` abbildet,
- Z ist eine endliche Menge an `ReductionMeasures`, es kann unterteilt werden in eine endliche Menge an `MitigationMeasures` Z^M und `CounterMeasures` Z^C,
- $relZ^M: Z^M \in H$ ist eine Relation zwischen einem `MitigationMeasures` auf einem `Hazard`,
- $relZ^C: Z^C \in H$ ist eine Relation zwischen einem `CounterMeasures` und einen `Cause`.

Analog zur ISO 26262 werden die Begriffe `HazardousEvent`, `Hazard`, `Failure`, `Fault` und `Error` für eine genauere Strukturierung von Risiken genutzt. Dies stellt bereits eine Verbesserung gegenüber der gegenwärtigen Situation in HSE-Plänen dar, da hierdurch Gefahren und deren Ursachen kategorisiert und feingranularer aufgeschlüsselt werden können. Die tatsächlichen Risiken werden als gefährliche Ereignisse (`HazardousEvent`) beschrieben. Diese setzen sich zusammen aus einer Gefahr (`Hazard`) und einer Betriebssituation (`OperationalSituation`) (Abbildung 26).

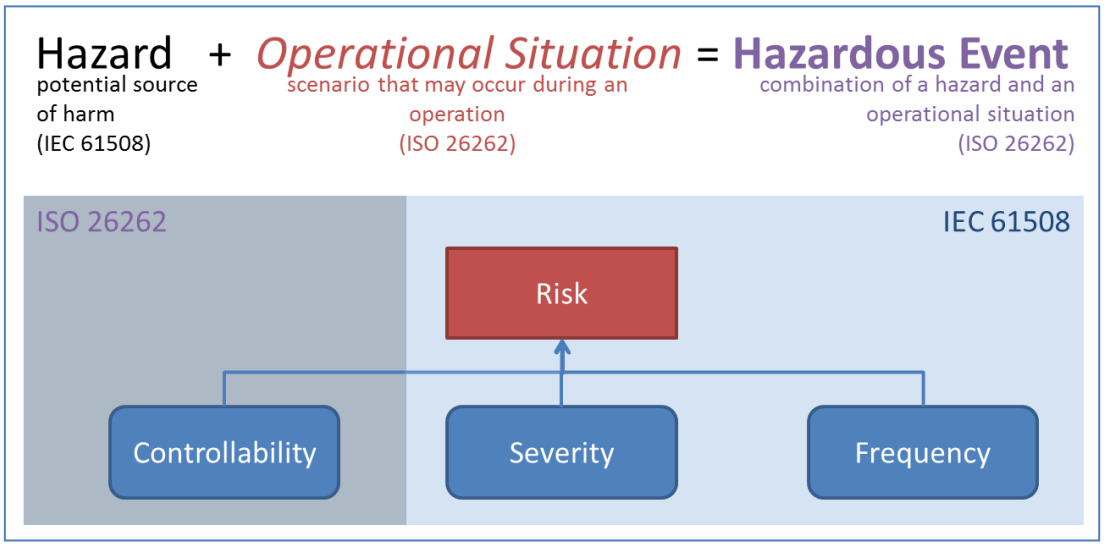


Abbildung 26: Definition gefährlicher Ereignisse

Eine Gefahr beschreibt einen potenziellen Ursprung für ein Risiko, beispielsweise die Verletzung oder der Tod einer Person, die Verschmutzung der Umwelt, oder ein Schaden an einem System. Durch die Kombination mit einer Betriebssituation, in der die Gefahr auftreten

könnte, ist eine genauere Spezifizierung eines Risikos innerhalb einer Operation möglich. So könnte eine Bewertung des Risikos niedriger als üblich in bestimmten Situationen ausfallen und es muss nicht immer vom schlimmsten Fall ausgegangen werden. Durch die Berücksichtigung der Situation erhält man eine genauere Charakterisierung der Gefahr bzw. deren Schadensausmaß (`HazardousEvent: severity`). Der positive Effekt ist es Risiken in einigen Situationen zu vernachlässigen, da die Gefährdung hinreichend gering ist und sich auf die Situationen zu fokussieren, in denen das Risiko in voller Stärke eintreten könnte. Für die initiale Annotation der Gefahrenbeschreibung innerhalb des Prozesses wird zunächst der im deutschen Sprachgebrauch für funktionale Sicherheit für Ursachenbeschreibung von Gefahren gebräuchliche Begriff Fehlerursache (`Cause`) ein unerwünschtes Ereignis verwendet. Die ISO 26262 ist an dieser Stelle genauer und verfeinert diese wie folgt: ein *Fault* stellt eine Ursache für eine Gefahr dar, kann jedoch selbst durch einen *Error*, was einer Abweichung von Soll und Ist beschreibt, ausgedrückt werden. Der `Failure` ist als konkreter Ausfall zu verstehen, der selbst wiederum zu einem `Hazard` führen kann, wenn dieser aus einem Unfall resultiert. Der maritime Experte definiert demnach zunächst lediglich Ursachen für Gefahren, wohingegen der Sicherheitsexperte im Anschluss diese feingranularer in die Fehlerstruktur angelehnt an die ISO 26262 überführen kann. Die Eintrittswahrscheinlichkeit (`Cause frequency`) von Gefahren wird auf Basis der Ursachen errechnet. Neben den Auswirkungen (`Exposure`) von gefährlichen Ereignissen, werden in das Modell Risikoreduktionsmaßnahmen (`Reduction-Measure`) integriert. Minderungsmaßnahmen (`MitigationMeasure`) wirken sich positiv auf die Schadensschwere von gefährlichen Ereignissen aus, Gegenmaßnahmen (`Counter-Measure`) hingegen auf die Eintrittswahrscheinlichkeit von Ursachen, was sich indirekt im Gesamtrisiko wiederspiegelt.

Arbeitsablauf: Für die Art der Modellierung wurden verschiedene Modellierungssprachen analysiert und hinsichtlich ihrer Einsatzmöglichkeit in diesem domänenspezifischen Kontext bewertet. Neben dem wesentlichen Faktor, der formalen Beschreibung von Offshore-Operationen, wurde hierbei zudem auf die graphische Art der Modellierung geachtet. Eine einfache und strukturierte Darstellung soll den Domänenexperten den Zugang zu dem Ansatz erleichtern. Als Basis für das in diesem Ansatz eingeführte Prozessmodell wurden die wichtigsten Konzepte von BPMN 2.0 übernommen und um notwendige Komponenten erweitert, da dies ein guter Kompromiss zwischen Benutzbarkeit und Formalisierung darstellt [Al15].

Durch Nutzung einer BPMN 2.0 ähnlicher Syntax sollen die Arbeitsabläufe in einer bestimmten Reihenfolge anhand von verschiedenen Tätigkeiten, einer Vielzahl von Akteuren, sowie der Interaktion dieser untereinander in einem Prozessmodell dargestellt werden. Alle Tätigkeiten, Akteure, Ereignisse und Nachrichten haben einen definierten Namen und eine Beschreibung. Die zuvor in der Umgebungsbeschreibung hinterlegten Daten werden an dieser

Stelle integriert, so werden beispielsweise Ressourcen zu Tätigkeiten oder Agenten den Akteuren. Das Resultat ist eine formale Beschreibung einer spezifischen Offshore-Operation. Die Detailgenauigkeit der Beschreibung ist dabei flexibel, da der Ersteller selbst entscheiden kann, wie detailliert er einen Arbeitsablauf darstellt und ob mehrere Subprozesse integriert werden sollen. Durch die Verwendung des konzeptionellen Modells können Prozesse mit der Beschreibung aller notwendigen Aktivitäten und Ereignisse, die im Offshore-Betrieb auftreten, darstellt werden. Eine Arbeitsablauf (`WorkingProcedure`) ist ein Tupel $P = (L, A, E, G, T, S, E^S, E^I, E^E, E^{\#_M}, E^{\#_T}, E^{\#_R}, G^F, G^J, G^X, G^M, F)$, wobei gilt:

- L ist eine endliche Menge von `FlowObject` welche sich unterteilt in endliche Mengen von `Activities` A, `Events` E und `Gateways` G,
- A kann unterteilt werden in eine endliche Menge von `Tasks` T und `SubProcesses` S,
- E kann unterteilt werden in Mengen von `StartEvents` E^S, `IntermediateEvents` E^I und `EndEvents` E^E,
- Der Untermengen der Events $E^{\#}$ können wiederum unterteilt werden in eine Menge von Nachrichtenereignissen $E^{\#_M}$, Zeitereignissen $E^{\#_T}$ und Fehlerereignisse $E^{\#_R}$,
- G kann unterteilt werden in eine Menge von `ForkGateways` G^F, `JoinGateways` G^J, `ExclusiveGateways` G^X und `InclusiveGateways` G^M,
- $F \subseteq L \times L$, beschreibt die Kontrollfluss-Relationen, eine endliche Menge an `SequenceFlows` welche die `FlowObjects` verbindet.

Dabei werden die entsprechenden Arbeitsabläufe (`WorkingProcedure`) einer Operation durch die verschiedenen beteiligten Akteure (`Actor`) strukturiert. Ein Arbeitsablauf wird durch verschiedene Konten (`FlowObject`) und Kanten (`ConnectionObject`) beschrieben, um eine sequenzielle Beschreibung zu ermöglichen. Knoten stellen hier Ereignisse (`Event`), Verknüpfungen (`Gateway`) oder Aktivitäten (`Activity`) dar. Ein Ereignis beeinflusst in der Regel die Reihenfolge oder den zeitlichen Ablauf einer Arbeitsanweisung und hat zumeist einen Auslöser oder einen auslösenden Effekt. Es gibt drei Arten von Ereignisse, je nachdem, wann sie in einem Ablauf auftreten: Start-Ereignisse (`StartEvent`), Zwischen-Ereignisse (`IntermediateEvent`) und End-Ereignisse (`EndEvent`). Der Sequenzfluss (`SequenceFlow`) wird verwendet, um den zeitlichen Ablauf für die Aktivitäten, die in einer Operation durchgeführt werden, darzustellen. Jeder Sequenzfluss repräsentiert eine gerichtete Kante zwischen zwei Knoten innerhalb eines Akteurs.

Eine Aktivität (`Activity`) ist ein abstrakter Begriff für die Arbeitsschritte, die während einer Operation durchgeführt werden. Dabei handelt es sich entweder um einen Tätigkeit (`Task`) oder um eine Kapselung von Arbeitsschritten (`SubProcess`), die wiederum durch eine Reihe

von Aktivitäten genauer spezifiziert werden können. Eine Tätigkeit ist eine atomare Aktivität, die nicht auf eine feinere Detaillierung aufgeschlüsselt werden kann. Verknüpfungen werden verwendet um die Divergenz und Konvergenz der Sequenz in einer Verfahrensanweisung zu kontrollieren. So ermöglichen diese Verzweigungen, Gabelungen, Zusammenführen und Verbindungen von Sequenzen.

Die Integration der drei Gruppen ergibt zusammen die MOPhisTo Operation, welche ein Tupel $M = (A, Q, S^{\circ}, mapP, mapT,\ F^{M}, R, Y, mapY)$ ist, wobei gilt:

- A ist eine endliche Menge an `Actors`,
- Q ist eine endliche Menge an `WorkingProcedures` Prozessen,
- $mapA: P \rightarrow A$ ist eine Funktion, die jede `WorkingProcedure` auf einen `Actor` abbildet,
- $S^{\circ} = \cup_{P \in Q} S_P$ ist die endliche Menge an `SubProcesses`,
- $mapP: S^{\circ} \rightarrow Q$ ist eine Funktion, die jeden `SubProcess` auf eine `WorkingProcedure` abbildet,
- $relP: A \rightarrow Y$ ist eine Relation zwischen einem `Actor` und einem `PhysicalObject`,
- $relT: T \rightarrow N$ ist eine Relation zwischen einem `Task` und einer `Action`,
- $HR = \{(P_1 P_2) \in Q \times Q \mid \exists_{s \in S_{P_1}} map(s) = P_2$ ist ein zusammenhängender Graph,
- $F^{M} \subseteq \left(\cup_{P \in Q} \left(T_P \cup e_P^E \cup E_P^{I_M}\right) \times \cup_{P \in Q} \left(T_P \cup e_P^S \cup \varepsilon_P^{I_M}\right)\right) \setminus \cup_{P \in Q} (L_P \times L_P)$ ist eine endliche Menge an `MessageFlows` zwischen `WorkingProcedures`.
- R ist eine endliche Menge an `ElementWithRisks`
- Y ist eine endliche Menge an `PhysicalObjects`

Kanten werden im konzeptionellen Modell nicht nur verwendet, um den Ablauf in einer bestimmten Reihenfolge anzuordnen, sondern ebenfalls um die notwendige Kommunikation zwischen verschiedenen Akteuren abzubilden. Ein Nachrichtenfluss (`MessageFlow`) wird verwendet, um den Austausch von Nachrichten zwischen zwei Akteuren zu ermöglichen. Dies ermöglicht eine Synchronisation von Arbeitsschritten über verschiedene Akutere hinweg.

Um die domänen-spezifischen Bedeutungen der einzelnen Konzepte besser nachvollziehen zu können wird nun im nächsten Abschnitt zunächst ein Anwendungsbeispiel eingeführt.

3.4 Anwendungsbeispiel

Um zu verdeutlichen, wie die modellbasierte Methodik eingesetzt werden kann, wird in diesem Abschnitt das Anwendungsbeispiel "Verladeszenario", d.h. Ladung vorbereiten und anheben, eingeführt (vgl. Abbildung 27).

Abbildung 27: Anwendungsbeispiel für die modellbasierte Methodik (Foto: dpa)

Das Anwendungsbeispiel beinhaltet ein Errichterschiff (Jack-up Vessel) für Offshore-Windenergieanlagen im "aufgejackten" Zustand. Dies bedeutet, dass das Schiff sich durch das Ausfahren von vier Stelzen selbständig aus dem Wasser hebt und dadurch zu einer mit dem Grund verbundenen Arbeitsplattform, einer so genannten self elevating unit, wird. Mittels des Großkrans werden normalerweise die einzelnen Elemente einer solchen Anlage, wie z.B. die Gondel, die Rotorblätter oder aber die Fundamente versetzt und in die Zielposition gebracht. Bevor eine solche Operation startet, müssen zunächst alle beteiligten Personen, z.B. Kranführer und Ladeoffizier, in das Vorhaben eingeführt werden. Je nach Zielort und Beschaffenheit des zu versetzenden Elementes müssen unterschiedliche Vorkehrungen durchgeführt werden, z.B. das Auswählen, Prüfen und Anbringen der passenden Anschlagmittel für ein sicheres Durchführen der Operation. Ebenfalls abhängig von der Ladung trifft der Kranführer seine Vorkehrungen. Dies beinhaltet unter anderem das Anpassen der Kraneinstellungen an das Gewicht. Sobald die Ladung sicher an dem Kranhaken angeschlagen wurde, verlässt der Ladeoffizier die Sicherheitszone und gibt ein entsprechendes Zeichen an den Kranführer. Neben einer Kommunikation mit Sprechfunk, werden mittels Handzeichen die wesentlichen Informationen zwischen diesen beiden Akteuren ausgetauscht. Das eigentliche Versetzen der Ladung geschieht ebenfalls auf Weisung des Ladeoffiziers. Dieser überwacht nicht nur den gesamten Vorgang, sondern gibt dem Kranführer konkrete Anweisungen, wie dieser die Ladung zu versetzen hat.

Während dieser Operation wirken massive Kräfte auf vergleichsweise empfindliche technische Komponenten, wodurch es zu Defekten und Materialermüdung kommen kann. Auch

durch das Schwingen der Ladung, verursacht durch sich ändernde Windbedingungen, kann schnell zur Gefahr von Personal oder andere Gerätschaften führen.

3.5 Modellbasierte Methodik

Dieser Abschnitt beschreibt den Kern des modellbasierten Ansatzes der Planung und Analyse von Offshore-Operationen. Hierdurch wird ein wesentliches Problem, das lose gekoppelte Vorhalten der Informationsbasis der Planung und der Risikoanalyse, wie es zurzeit in der Praxis der maritimen Domäne Anwendung findet, gelöst. Im Folgenden werden die einzelnen Handlungsschritte detailliert dargestellt. Dabei wird jeweils das zugrundeliegende Konzept vorgesellt, das entsprechende Vorgehen beschrieben und mit einem Anwendungsbeispiel verdeutlicht. Die einzelnen Handlungsschritte der Methodik sind in Abbildung 28 dargestellt.

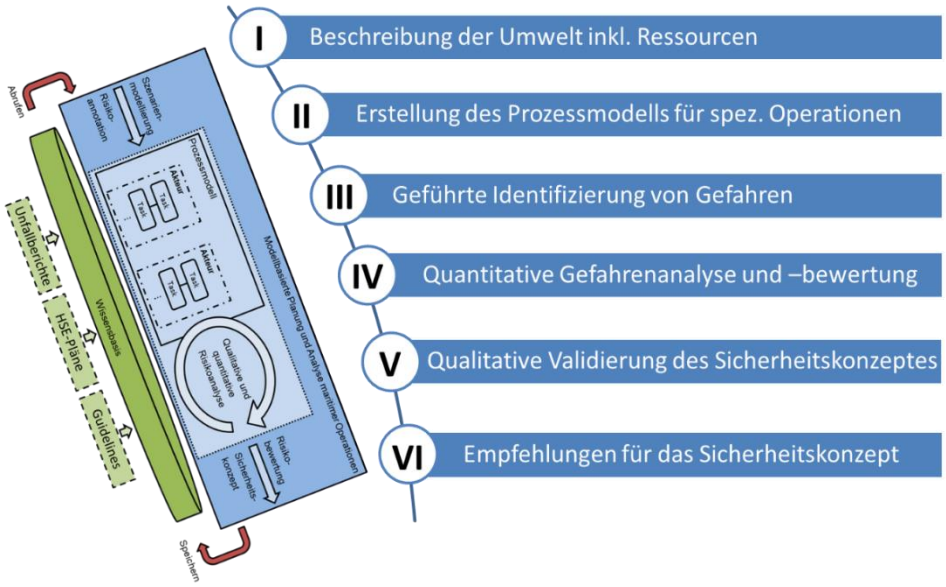


Abbildung 28: Methodik der modellbasierten Methode

Basierend auf einer Beschreibung der Umgebung und Ressourcen kann ein Prozessmodell erstellt werden, welches die einzelnen Akteure und Ressourcen einer Operation darstellt. Jedem Prozessschritt können dann Gefährdungen und Ursachen zugeordnet werden, die qualitativ durch Simulation und quantitativ durch eine Risikobewertung bewertet werden. Das Ergebnis ist ein HSE-Plan, der Empfehlungen für das Sicherheitskonzept enthalten kann.

Beschreibung der Umwelt inklusive Ressourcen

Der Kern sowohl für die Beschreibung von Abläufen, als auch der Definition von potentiellen Gefahren innerhalb dieser, bildet das Umgebungsmodell. Es dient der formalen Beschreibung aller relevanten Elemente einer Operation. Es enthält dabei nicht nur die durch die in dem Ablauf der Operation verbrauchten bzw. erzeugten Ressourcen bzw. Arbeitsmittel (vgl. An-

forderung **A1**) oder Informationen, die Aufschlüsselung des eingesetzten Personals (vgl. Anforderung **A2**), sondern zusätzlich die Beschreibung der Umgebung mit allen relevanten Systembestandteilen und Umweltfaktoren. Letzteres können dabei auch die Beschreibung des zu errichtenden Windparks, oder aber die Schiffe bzw. Offshore-Installationen bei einem Personentransfermanövers sein.

Im ersten Schritt wird die Umgebung der zu planenden maritimen Operation beschrieben, indem dafür relevante Ressourcen, Akteure und Objekte ausgewählt und in einer Szene positioniert werden können. Der jeweilige Standort und die dort vorherrschenden Umweltbedingungen können in die Beschreibung mit einbezogen werden.

Verschiedenste Arten von Parametern wie die Krankapazität, die Länge des Schiffes oder die Höhe der Windenergieanlage können bei der Umweltbeschreibung hinzugezogen werden. Dabei können auch Angaben zu verschiedenen Schiffstypen, z.B. Jack-Up Vessel oder Transportschiffe, eingegeben und für zukünftige Szenarien verwendet werden. Für Akutere, wie z.B. Ladeoffiziere, können die Rollen definiert werden. So können die zur Verfügung stehenden Fähigkeiten und deren Qualifikationen beachtet werden.

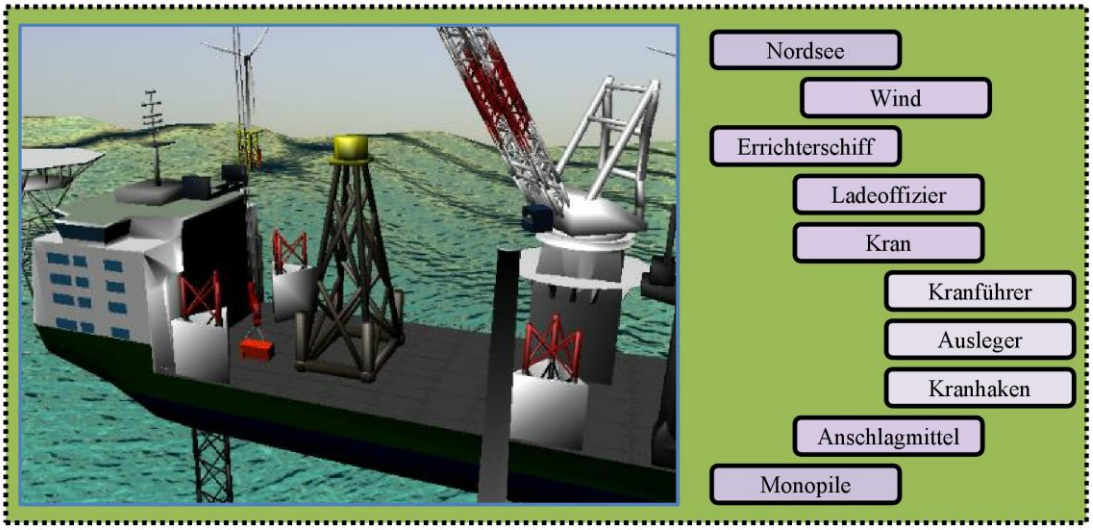


Abbildung 29: Beschreibung der Umwelt inklusive Ressourcen

Abbildung 29 zeigt das Anwendungsszenario in Kombination mit exemplarischen, hierarchisch angeordneten Elementen.

Erstellung des Prozessmodells für spezifische Operationen

Das Prozessmodell dient der Erzeugung von normativen Abläufen einzelner Offshore-Operationen und bildet damit den Kern der prozessorientierten Risikobewertung. Das Konzept dieses Partialmodells enthält dabei Aspekte zu personenbezogenen Beschreibung von Tätigkeiten (vgl. Anforderung **A3**) in einer sequenziellen Abfolge, der Möglichkeit der Synchronisation

und der Informationsaustausches durch Kommunikation (vgl. Anforderung **A4**) und der Darstellung von Handlungsalternativen (vgl. Anforderung **A3**).

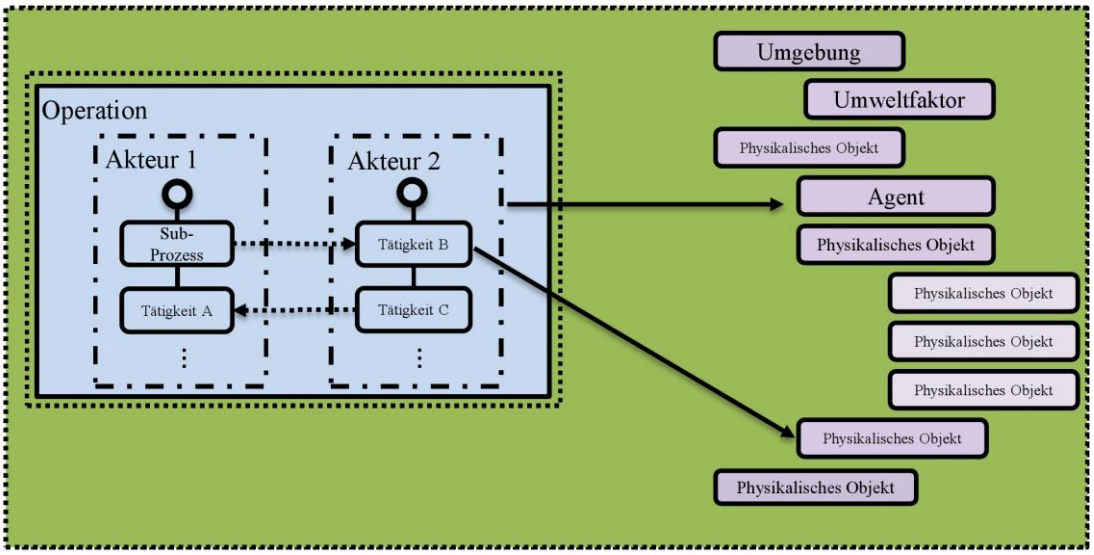


Abbildung 30: Integration des Prozesses in die Systembeschreibung

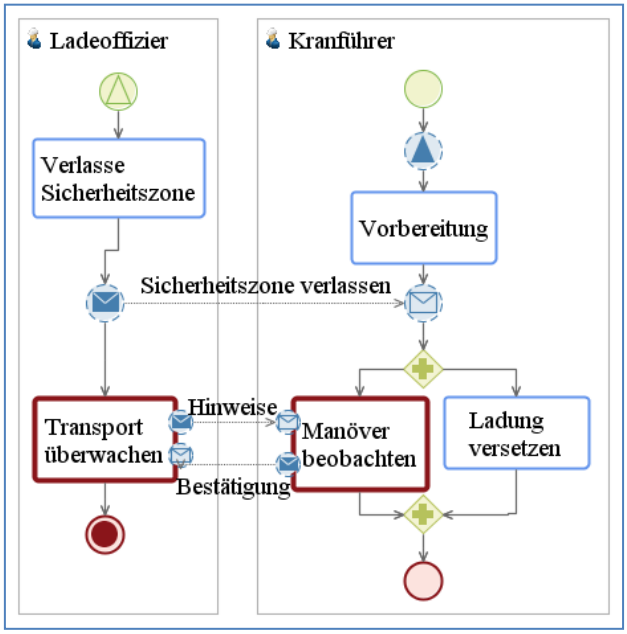


Abbildung 31: Erstellung des Prozessmodells für spezielle Operationen

Abbildung 31 zeigt den im Anwendungsszenario Arbeitsprozedur in Form eines Prozessmodells. Zunächst gibt der Kranoffizier ein Signal an den Ladeoffizier, woraufhin dieser die Sicherheitszone verlässt und der Kranführer mit seinen Vorbereitungen beginnt. Sobald der Kranführer die Nachricht vom Ladeoffizier bekommt, dass dieser sich in einem sicheren Bereich befindet, starten beider Akteure gleichzeitig mit der Durchführung der Verladung. Dabei beobachtet der Ladeoffizier stets den Transport und gibt dem Kranführer die notwendigen Hinweise und Anweisungen wie dieser den Kran steuern soll. Nach jeder Nachricht erfolgt

immer eine Bestätigung um sicherzugehen, dass die Kommandos korrekt bei der Gegenstelle eingegangen sind. Der Prozess endet mit einer erfolgreichen Versetzung der Ladung.

Assistierte Identifizierung von Gefährdungen und deren Ursachen

Um eine Gefahrenbewertung für einen Prozess durchführen zu können, muss dieses mit potentiellen Gefahren und deren Ursachen annotiert werden. Dies geschieht durch die Integration des Gefahrenmodells. Risikobeschreibungen werden hierbei mit den Tätigkeiten und / oder den durchführenden Personen verknüpft (vgl. Anforderung **A5**). Das Konzept sieht für die verschiedenen Gefahrenelemente einen spezifischen Bewertungsansatz (vgl. Anforderung **A7**). Dies ist, neben der Eintrittswahrscheinlichkeit von Ursachen, die Schadensschwere von Gefährdungen. Diese Annotation ermöglicht verschiedene Arten der Analyse, wie beispielsweise Model Checking, statische Analysen oder Simulation. Für die Beschreibung von Gefahren und Ursachen und die Darstellung von Abhängigkeiten zwischen diesen wird die Terminologie aus vorhandenen Sicherheitsstandards benutzt.

Nachdem das Prozessmodell erstellt worden ist, können potentielle Gefahren der Operation und Ursachen für jeden einzelnen Prozessschritt und/oder Akteur hinzugefügt werden (vgl. Anforderung **A6**). Für die Terminologie der Risikobegriffe erfolgt eine Orientierung an der ISO 26262 für funktionale Sicherheit, die vorwiegend in der Automobilbranche verwendet wird. Potentielle Gefahren können hier beispielsweise die Verletzung einer Person, eine Person über Bord, oder der Ausfall eines Systems sein. Die zugeordnete operationale Situation charakterisiert die vorherrschenden Umweltbedingungen, z.B. Wetterbedingungen, Wassertemperatur, Standort, die dann mit der Gefahrenquelle in ein Verhältnis gesetzt werden können (vgl. Anforderung **A8**). So unterscheiden sich beispielsweise die Auswirkungen der Gefahr "Man-über-Bord" je nachdem, ob diese in der Nordsee mit kälteren Wassertemperaturen und hohem Wellengang, oder bei wohltemperierten Bedingungen in der Karibik, eintritt. Aus diesem Grund spielt die operationale Situation eine wichtige Rolle. Eine Gefahr kann durch einen oder mehrere Ursachen ausgelöst werden, d.h. die gewünschte Funktion wird nicht so ausgeführt wie gefordert. Beispielsweise kann eine Person sich nicht an Anweisungen halten oder ein Kran nicht die gewünschte Funktion erfüllen. Aus einem bereits bestehenden Gefährdungs- und Ursachenkatalog können Vorschläge für den jeweiligen Prozessschritt übernommen werden, die von einer lernenden Wissensbasis bereitgestellt werden. Die bereits existierenden Daten werden sowohl aus Unfallberichten als auch aus den bereits modellierten Prozessmodellen extrahiert und in der Wissensbasis hinterlegt. Es ist möglich, jederzeit neue Gefahren und Ursachen hinzuzufügen, um die Wissensbasis zu erweitern und den Katalog somit weiter zu füllen.

Das Prozessmodell wird mit potenziellen Risiken für die weitere Analyse mit Annotationen versehen werden. Die Annotation der Risiken hat mehrere Vorteile. Es erlaubt Risiken der gesamten Operation, speziell den Akuteren oder auch deren Tätigkeiten zuzuweisen. Auf diese Weise kann bereits bei der Planung von diesen Tätigkeiten auf spezifische Risiken eingegangen werden. Die ermöglicht es das aus der Analyse resultierendes Sicherheitskonzept für verschiedene Zielgruppen zu strukturieren. Beispielsweise mit Schwerpunkt auf die Akteure, z.B. zu verwenden als Arbeitsanweisung für Techniker in denen speziell für deren Tätigkeiten die entsprechenden Risiken aufgezeigt werden, oder die gesamte Operation. Letztere wird zumeist von HSE-Manager und Zertifiziere bevorzugt. Des Weiteren ermöglicht die Annotation weitere Analyse der Operation, dabei soll jede Art der formalen Analyse, Modellüberprüfung, statische Analyse oder Simulation durchführbar sein. Abschließend ermöglicht es zudem zu beurteilen, ob die Ursachen einer Gefahr korrekt identifiziert wurden.

Abbildung 32 zeigt ein Beispiel für eine Annotation der prozessorientierten Systembeschreibung mit Instanzen der eingeführten Beschreibung von Gefahren und deren Ursachen. Deutlich zu erkennen ist hierbei die prozesszentrische Integration aller wesentlichen Bestandteile, welche als Grundlage für eine transparente Gefährdungsbeurteilung dienen, da hierdurch ein nachvollziehbarer Zusammenhang zwischen den Gefahren, den Akteuren und der eingesetzten Ressourcen in konkreten Arbeitsschritten ermöglicht wird (vgl. Anforderung **A6**).

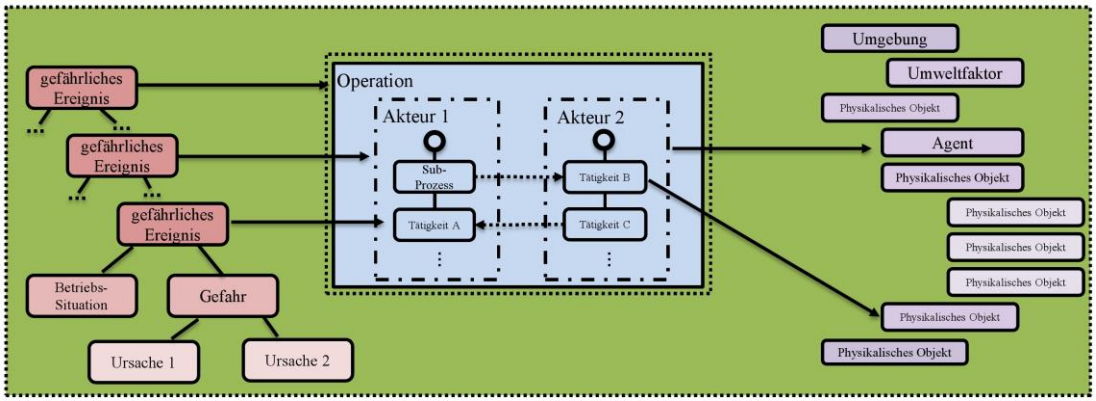


Abbildung 32: Annotation der prozessorientierten Systembeschreibung mit Gefahren und Ursachen

Im Anwendungsszenario könnte ein gefährliches Ereignis wie folgt aussehen: während des Versetzens der Ladung besteht die Gefahr eines Zusammenstoßes mit dem Ladeoffizier. Dies kann durch verschiedene Ursachenkombinationen geschehen. So kann beispielsweise ein fehlerhaftes Anschlagmittel versagen, oder aber die Anweisungen an den Kranführer werden falsch entgegengenommen, was in einer entsprechenden Fehlversetzung resultiert. Je nach operationaler Situation, beispielsweise starke oder schwache Windverhältnisse, können die beim Eintreten einer Ursache entstehenden Kräfte und somit der daraus resultierende Schaden noch zusätzlich verstärkt werden.

Quantitative Risikoanalyse und -bewertung

Die quantitative Risikobewertung ermittelt die Gefährdung für einzelne Arbeitsschritte, Akteure und den Gesamtprozess, indem mithilfe einer FTA die Gefahren und Ursachen logisch miteinander verknüpft werden. Der Experte muss die Wahrscheinlichkeit für das Eintreten der Gefahr und der Ursachen zwar selbst definieren, erhält aber durch den Fehlerbaum eine logische Übersicht über die Zusammenhänge (vgl. Anforderung **A7**). Somit kann der Experte selbst, aber auch andere Beteiligte nachvollziehen, wie ein bestimmter Wert bei der Risikobewertung zustande kommt. Für genauere theoretische Grundlagen zu Fehlerbäumen und deren Aufbau bzw. generell der quantitativen Risikobewertung wird auf die Forschungsarbeit [Pi15] verwiesen. Heutzutage ist die FTA ist eine der wichtigsten Techniken im Bereich der Wahrscheinlichkeits-Risikobewertung und der Zuverlässigkeitsanalysen von Systemen. Ursprünglich für die Anwendung in der Atomenergie entwickelt, wird FTA in immer mehr Bereichen eingesetzt, in denen Systemanalysen notwendig sind [SC02].

Ein Fehlerbaum (FT) ist eine grafische, logisch strukturierte Darstellung von unerwünschten Ereignissen und deren mögliche Ursachen. Es kann eingesetzt werden, um alle Kombinationen von Basis-Ereignissen zu charakterisieren, die zu einem so genannten "Top-Event" führen können. Die logische Struktur des Baumes beschreibt demnach die Kombination von Basis-Ereignissen, den Blättern eines Fehlerbaumes, welche die zu einem Top-Event, dem Wurzelelement, führen. Ausgehend von entwickelten Fehlerbäumen können Methoden sowohl für die qualitative, als auch quantitative Systemanalyse angewandt werden. Die Gefährdungsanalyse ist in der Offshore-Domäne ein wichtiger Faktor. Als ein Bestandteil dessen gewinnt die FTA immer mehr Aufmerksamkeit [Vi07], [ZDN13], [Su12]. Da Fehlerbäume in der Regel händisch erstellt werden, erfordert dies erfahrene Ingenieure mit hinreichenden Kenntnissen über das System und weiteren notwendigen Details. Manuell erzeugte Fehlerbäume sind demnach zeit- und kostenintensiv. Zudem ist man dort auf die Expertise des Erstellers angewiesen und zudem ist dieses Vorgehen fehleranfällig, da menschliches Versagen zu Unvollständigkeit führen kann. Das hier eingeführte Vorgehen, basierend auf den in den vorherigen Abschnitten eingeführten Planungsprozess, adressiert genau dies. Zum einen werden wiederverwendbare Prozessmodelle und nicht textuelle Prozessbeschreibungen genutzt und zum anderen wird das Vorgehen für die Gefahrenbewertung optimiert. Für jedes im Prozessmodell annotierte gefährliche Ereignis werden logisch strukturierte Fehlerbäume, basierend auf den identifizierten Ursachen erzeugt. Da die Ursachen konkreten Aktivitäten oder Personal zugeordnet werden, können diese Verortungen bei der Instanziierung der Fehlerbaumstrukturen berücksichtigt werden. Der Prozessverlauf dient dabei als wesentliche Informationsquelle. Wenn z.B. Aktivitäten gleichzeitig durchgeführt werden, kann daraus geschlossen werden, dass ebenfalls die dort hinterlegten, einer gemeinsamen Gefahr zugeordneten, Ursachen zeitgleich auftreten müssen.

Abbildung 33 zeigt eine mögliche Fehlerbaumstruktur für das Beispielszenario. Ein "Zusammenstoß der Ladung" ist in diesem Fall das gefährliche Ereignis. Dem Beispiel ist zu entnehmen, dass das Eintreten dieser Gefahr entweder durch eine "fehlerhafte Vorbereitung" oder durch ein "fehlerhaftes Kranmanöver" resultieren kann. Im Prozess sind dies zwei nacheinander durchgeführte Aktivitäten. Letztere Ursache kann hingegen nur durch ein zeitgleiches Auftreten eines "Fehler(s) beim Versetzen der Ladung" und einer "unzureichende(n) Überwachung des Manövers" eintreten. Bei einem Abgleich mit dem im Beispiel eingeführten Prozess kann auch dort eine Parallelität der Ausführung der entsprechenden Aktivität entnommen werden.

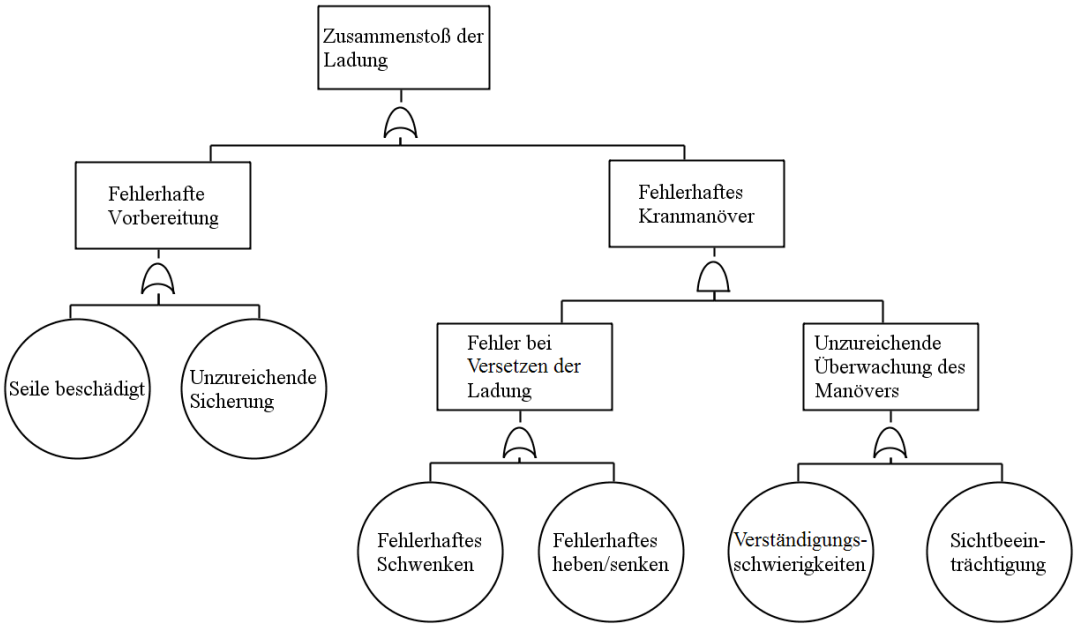


Abbildung 33: Beispiel für eine Fehlerbaumstruktur

In seiner Dissertationsschrift geht Pinkowski genauer auf die verschiedenen Möglichkeiten einer prozessorientierten, automatischen Erzeugung von Fehlerbaumstrukturen basierend auf der hier vorgestellten modellbasierten Methode der prozessorientierten Systembeschreibung und der angeschlossenen Identifizierung und Annotation potenzieller Gefahren und deren Ursachen ein [Pi15].

Qualitative Validierung durch Simulation

Aufgrund des Modellansatzes der Methode kann eine qualitative Validierung durch verschiedene Simulationsläufe überprüft werden. Dabei wird untersucht, ob die Abhängigkeiten zwischen Gefahr und Ursache zutreffen. Hierbei kann auch eine unterschiedliche Parametrisierung verwendet werden. Dieser Schritt der modellbasierten Methodik nimmt in der praktischen Durchführung für sich stehend einen umfangreichen Stellenwert ein. In dieser Arbeit wird kurz

auf die wesentlichen Aspekte eingegangen, für eine genauere Beschreibung wird auf die Forschungsarbeit von Gollücke [Go16] verwiesen. Ein wesentliches Ziel der simulationsbasierten Analyse ist, neben der Möglichkeit der Quantifizierung der durch Fehlerbaum entstandenen resultierenden Gefahren- und Ursachenkombinationen, eine qualitative Validierung des bisherigen Status der Gefährdungsbeurteilung. Dies bedeutet, dass mit diesem Verfahren gezielt untersucht wird, ob zusätzliche kritische Situationen eintreten können oder aber auch neue Ursachenkombinationen, die zu diesen führen, identifiziert werden können. Um das Auftreten von Gefahren und deren Ursachen während der Simulationszeit zu identifizieren, ist eine formalisierte Beschreibung dieser notwendig. Dies wird durch die für diesen Zweck entwickelte "Hazard Description Language (HDL)" erreicht. Die Sprache ermöglicht den Experten die Gefahren und Ursachen in einer naturnahen Sprache zu formalisieren. Bei der Entwicklung dieser Sprache wurde ebenfalls darauf geachtet, dass diese kompatibel zur Object Constraint Language (OCL) ist. OCL ist eine weit verbreitete und hervorragend evaluierte Sprache, für die bereits etliche Implementierung für den Einsatz in einer Simulationsumgebung existieren [WK03], [CW02]. Die HDL-Muster werden die automatisch in OCL-Ausdrücke transformiert, HDL kann somit als Schnittstelle zur Beschreibung Gefahren und Ursachen mittels OCL gesehen werden, ohne die Notwendigkeit von tieferen Kenntnissen über diese Sprache. Die Gefahr "Ladeoffizier kollidiert mit der Ladung" wird beschrieben durch "distance between Lift Supervisor and Cargo equals 0cm", die Ursache "Ladeoffizier befindet sich unterhalb der Ladung” durch "position.x of Lift Supervisor equals position.x of Cargo and position.y of Lift Supervisor equals position.y of Cargo and position.z of Cargo is more than height of Lift Supervisor”. Ein ausführlicheres Beispiel befindet sich im Anhang (Abbildung 63)

Die Identifizierung ist wichtig, da die Fehlerbäume auf Fehler und Vollständigkeit überprüfen werden sollen. Genauer gesagt, durch die Identifizierung von Ereignissen kann in jedem Simulationsschritt evaluiert werden, ob das zugehörige Top-Ereignis eingetreten ist. Ist dies der Fall ist, wird der Fehlerbaum hinsichtlich Abweichungen zwischen den automatisch identifizierten Fehlern und den im Vorfeld durch den Experten beschriebenen Fehlerbaum untersucht. Sollte eine Ursache aus dem Fehlerbaum nicht erfasst worden sein, kann dies bedeuten, dass diese nicht notwendig für das Eintreten der Gefahr ist. Auf diese Weise kann beurteilt werden, ob die Fehlerbaumstruktur korrekt ist oder ggf. einen Defekt aufweist. Auf der anderen Seite wird geprüft, ob Fehler auftreten, die nicht in der aktuellen Fehlerbaumstruktur für das Top-Ereignis identifiziert wurden. Wenn dies der Fall ist, müssen die detektierten Fehler der Fehlerbaumstruktur hinzugefügt werden. Dieser Vorgang wird mit den geänderten Strukturen erneut durchgeführt, bis keine weiteren Gefahren oder Ursachen außerhalb dieser gefunden werden. Dies erlaubt eine möglichst, bis zu einem gewissen Level, genaue Abschätzung der

Risiken, abhängig von den Grenzen der Simulation. Eine Voraussetzung für die simulationsbasierte Analyse ist neben der Formalisierung der Gefahren und Ursachen, und damit einer Überprüfbarkeit dieser, die Integration dieser Aspekte in die Simulationsumgebung und die dazugehörigen Abläufe. Die Simulationsumgebung basiert auf der prozessorientierten Systembeschreibung. Dieser werden neben den Aktivitäten, welche die Agenten durchführen sollen, ebenfalls die Informationen über die Objekte der Umgebung entnommen (vgl. Anforderung **A9**). Der Simulationsumgebung liegt ein physikalisches Modell zugrunde, wodurch Effekte wie z.B. Wind bei der Steuerung des Krans durch den Kranführer berücksichtigt werden können.

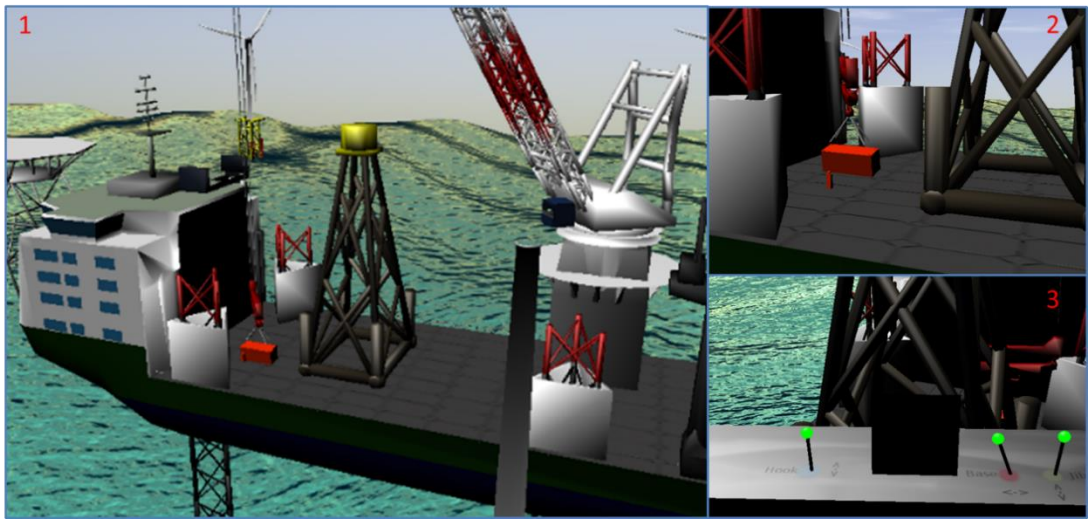
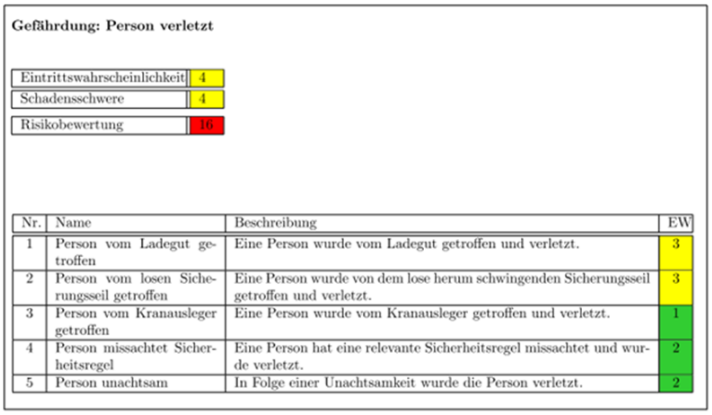


Abbildung 34: Qualitative Validierung durch Simulation

Abbildung 34 zeigt die 3D-Umgebung der Simulation, sie besteht aus dem Errichterschiff (1), der zu transportierenden Ladung und dem Ladeoffizier (2) und der Krankanzel (3).

Empfehlungen für das Sicherheitskonzept

Das Ergebnis der vorherigen Schritte ist die automatische Generierung eines textuellen HSE-Plans mit der grafischen Darstellung der einzelnen Prozesse, der Beschreibung der Ursachen, deren Eintrittswahrscheinlichkeit sowie der Schadensschwere und der daraus ermittelten Risikobewertung. Abbildung 35 zeigt ein Beispiel, wie die Bewertung einer potenziellen Gefahr und deren Ursachen aufbereitet werden kann.



Gefährdung: Person verletzt

Eintrittswahrscheinlichkeit	4
Schadensschwere	4
Risikobewertung	16

Nr.	Name	Beschreibung	EW
1	Person vom Ladegut getroffen	Eine Person wurde vom Ladegut getroffen und verletzt.	3
2	Person vom losen Sicherungsseil getroffen	Eine Person wurde von dem lose herum schwingenden Sicherungsseil getroffen und verletzt.	3
3	Person vom Kranausleger getroffen	Eine Person wurde vom Kranausleger getroffen und verletzt.	1
4	Person missachtet Sicherheitsregel	Eine Person hat eine relevante Sicherheitsregel missachtet und wurde verletzt.	2
5	Person unachtsam	In Folge einer Unachtsamkeit wurde die Person verletzt.	2

Abbildung 35: Beispiel einer Bewertung einer Gefahr

Die Risikobewertung ergibt sich aus der für die Gefahr bewertete Schadensschwere und der aus den zugehörigen Ursachen errechneten Eintrittswahrscheinlichkeit. Um das Risiko für eine Gefahr zu reduzieren, können geeignete Schutzmaßnahmen entwickelt werden, sodass eine neue Risikobewertung durchgeführt werden muss. Als finaler Schritt erfolgen Empfehlungen für das Sicherheitskonzept. Es ist hierbei möglich, eine detaillierte Version des HSE-Plans inklusive Schaubilder der einzelnen Prozesse zu erstellen, um Verständnisprobleme von relativ neuen bzw. ungeübten Mitarbeitern zu vermeiden oder für bereits geschulte Mitarbeiter einen abstrakteren HSE-Plan zu erstellen.

3.6 Implementierung

Dieses Unterkapitel beschäftigt sich mit der prototypischen Implementierung für die Unterstützung der vorgestellten modellbasierten Methodik - MOPhisTo. Sie wurden mit Hilfe der Eclipse IDE, dem Eclipse Modeling Framework (EMF) und dem Graphical Editing Framework (GEF) in einer Java-Umgebung implementiert. Bei der Entwicklung der Werkzeuge wurde darauf geachtet diese möglichst modular zu gestalten. So ist für jede in der Methodik vorgestellte Phase ein eigenes Plug-In Projekt entwickelt worden, um vorab die Möglichkeiten für eine Erweiterung bzw. einen Austausch dieser Module zu gewährleisten. Um die Durchgängigkeit der Methodik über alle Module zu gewährleisten, liegt dem Prototyp eine Implementierung des integrierten Modells zugrunde (vgl. Anforderung **A13**). Spätere Erweiterung oder ein Austausch einzelner Komponenten ist, solange sie konform zu diesem Modell sind, ohne großen Aufwand möglich und eine weiteres verwenden der entwickelten Methodik ist gegeben. Um die qualitative Validierung durch Simulation zu ermöglichen, wurde während der Entwicklung von Beginn die Anforderung der Ausführbarkeit berücksichtigt (vgl. Anforderung **A9**). Im Rahmen dieser Forschungsarbeit sind zwei Komponenten für die Unterstützung der Methodik entstanden: MOPhisTo, ein Werkzeug für die Planung und Analyse von

maritimen Operationen und MASCaS, einer multi-Agent Simulationskomponente für die Ausführung der normativ geplanten Prozesse innerhalb der HAGGIS-Simulationsumgebung [Ha14].

Zunächst wird kurz das virtuelle Testbed HAGGIS eingeführt. Das virtuelle Testbed HAGGIS bietet durch verschiedene Modellierungs- und Simulationskomponenten einen Rahmen, um die notwendigen Methoden für die Systemspezifikation und formalen Risikoanalysen Umzusetzen, wie sie für die Methodik dieser Forschungsarbeit notwendig sind.

Für die Sicherstellung der Interoperabilität innerhalb des HAGGIS – Frameworks ist das HAGGIS Datenmodell entstanden [DHS14].

1: Universal	Unit, Graph, Math, 3D Geometry, …
2: Engineering	Physics, Geography, …
3: Application	TrafficSystem, Vehicles, Sense, HMI, Environment, …
4: Domain	Maritime, …

Abbildung 36: Ebenen des HAGGIS Datenmodells

Das HAGGIS - Modell ist hierbei in vier verschiedene Ebenen unterteilt, welche jeweils für sich wiederum in einzelne Pakete strukturiert sind (vgl. Abbildung 36):

1. *Universal*: Die Universal-Schicht enthält Konzepte und Datentypen, die eine allgemeine Bedeutung für alle Schichten unterhalb dieser darstellt. Diese sind gruppiert in die Pakete Einheiten, Graphentheorie, Mathematik und 3D-Geometrie. Hiermit lassen sich Konzepte wie Zeit, Punkte, Winkel oder auch Posen im Raum ausdrücken.
2. *Engineering:* In die zweite Schicht werden ingenieurspezifische Elemente eingeordnet, mit denen sich beispielsweise physikalische Körper oder aber auch geographische Aspekte beschreiben lassen.
3. *Application:* Die Anwendungsschicht umfasst alle Konzepte und Datentypen für unterschiedlichen Anwendungsfelder. In den Paketen dieser Schicht lassen sich Verkehrsnetze, Fahrzeuge, Sensoren und ebenfalls Umweltphänomene wie z.B. Wind, Wellen und Strömungen wiederfinden.
4. *Domain:* In dieser Schicht werden Modellpakete mit Elementen für die verschiedenen Domänen wie z.B. die Maritime-, Luftfahrt- oder Automobilindustrie verankert. Das Paket "Maritime" realisiert zum Beispiel weitere Konzepte und Datentypen wie Schiffsbrücke, Offshore-Kran oder auch das Deckspersonal.

Auf Basis dieser in diesem Modell definierten Elemente kann ein beliebig komplexes System definiert werden. So kann beispielsweise aus verschiedenen Elementen ein Objekt wie ein Schiff erzeugt werden, welches aus einem Rumpf, einem Deck und einer Brücke besteht. Das HAGGIS – Datenmodell dient als Grundlage für die Beschreibung der Umwelt und der Ressourcen der modellbasierten Methodik.

Abbildung 37 zeigt einen Ausschnitt der für diesen Kontext wesentlichen Klassen aus dem Umgebungsmodell.

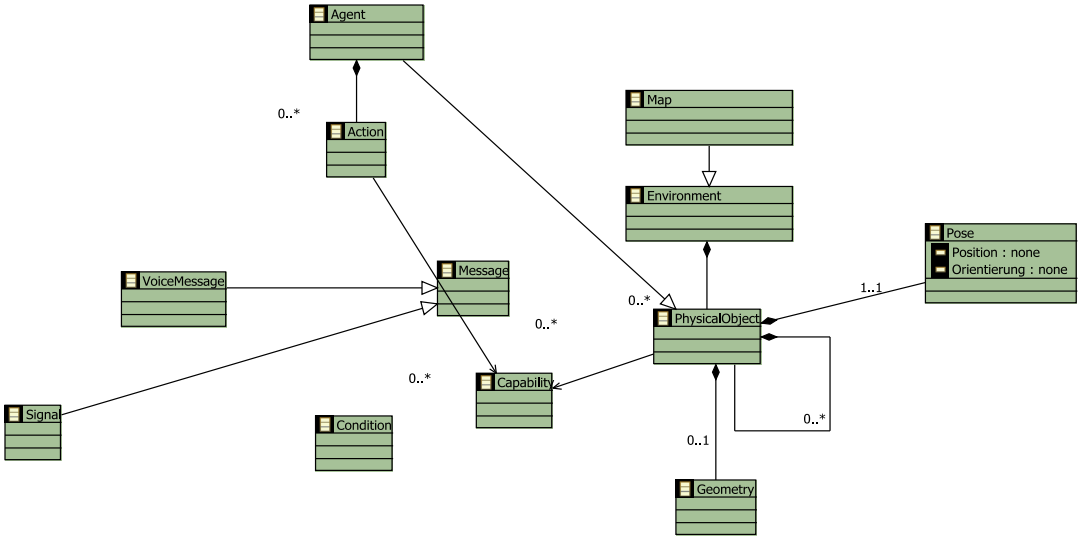


Abbildung 37: Umgebungsmodell

Die Komponente EMod – Environment Modeler – dient der Instanziierung der Umgebung der zu analysierenden Szenarien. Mit dieser ist der Anwender in der Lage eine Szene der Operation zu erstellen, in der alle Akteure und physikalischen Objekte, welche in der Analyse untersucht werden sollen, abgebildet werden. Zugleich werden hier die notwendigen Objektinformationen für eine Analyse in einer 3D-Simulation hinterlegt.

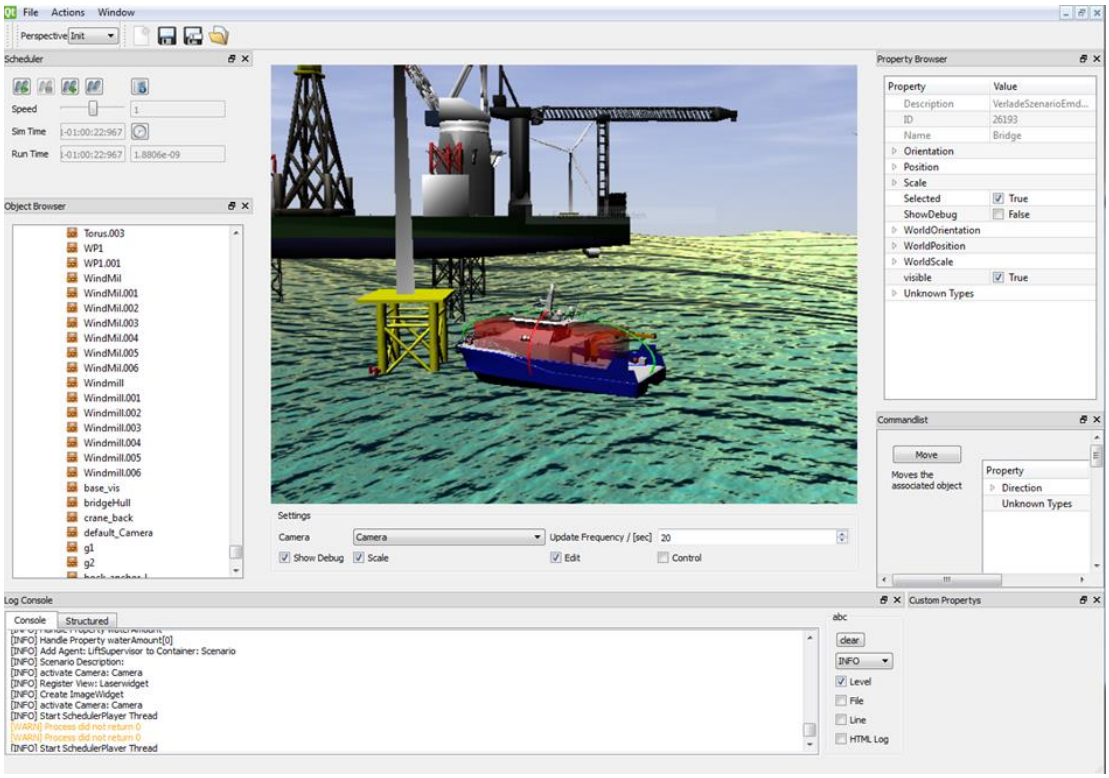


Abbildung 38: EMod - Environment Modeler - Beschreibung der Umwelt inklusive Ressourcen

Abbildung 38 zeigt einen Screenshot von EMod: mittig zu sehen ist eine 3D-Darstellung des Szenarios, auf der linken Seite eine Auflistung aller physikalischen Objekte, rechts die Möglichkeiten Objektparameter zu konkretisieren.

Mithilfe des Prozesseditors können die Abläufe der maritimen Operationen systematisch beschrieben werden. Durch die Nutzung einer an BPMN 2.0 angelehnten Syntax, inklusive einer graphischen Notation zur visuellen Darstellung, können die Arbeitsabläufe in einer bestimmten Reihenfolge anhand von verschiedenen Tasks, d.h. Aufgaben, einer Vielzahl von Akteuren, ihren zugehörigen Rollen sowie der Interaktion der Akteuren untereinander, in einem Prozessmodell dargestellt werden (vgl. Anforderung **A10**).

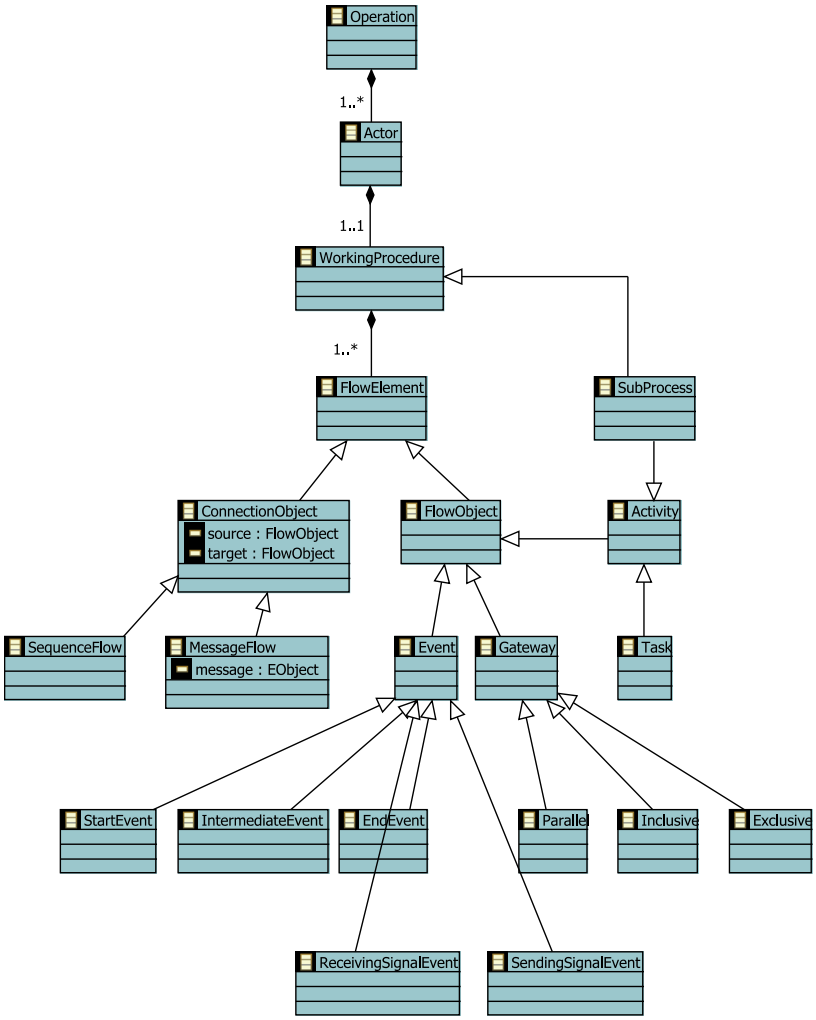


Abbildung 39: Prozessmodell

Abbildung 39 zeigt einen Ausschnitt der für diesen Kontext wesentlichen Klassen aus dem Prozessmodell. Die zuvor in der Umweltbeschreibung hinterlegten Daten werden an dieser Stelle genutzt, um konkreten Akteuren oder Anlagen zugeordnet werden zu können. Das Resultat ist eine formale Beschreibung einer spezifischen Offshore-Operation. Die Detailgenauigkeit der Beschreibung ist dabei flexibel, da der Ersteller selbst entscheiden kann, wie detailliert er einen Prozess darstellt und ob mehrere Subprozesse integriert werden sollen (vgl. Anforderung **A12**). In Abbildung 40 ist ein beispielhafter Prozess dargestellt, welcher den Überstieg einer Person von einem Schiff zu einer Dritteinheit, beispielsweise. zu einer Offshore-WEA, darstellt. Alle Aktivitäten, Akteure, Rollen und Nachrichten haben einen definierten Namen und eine Beschreibung.

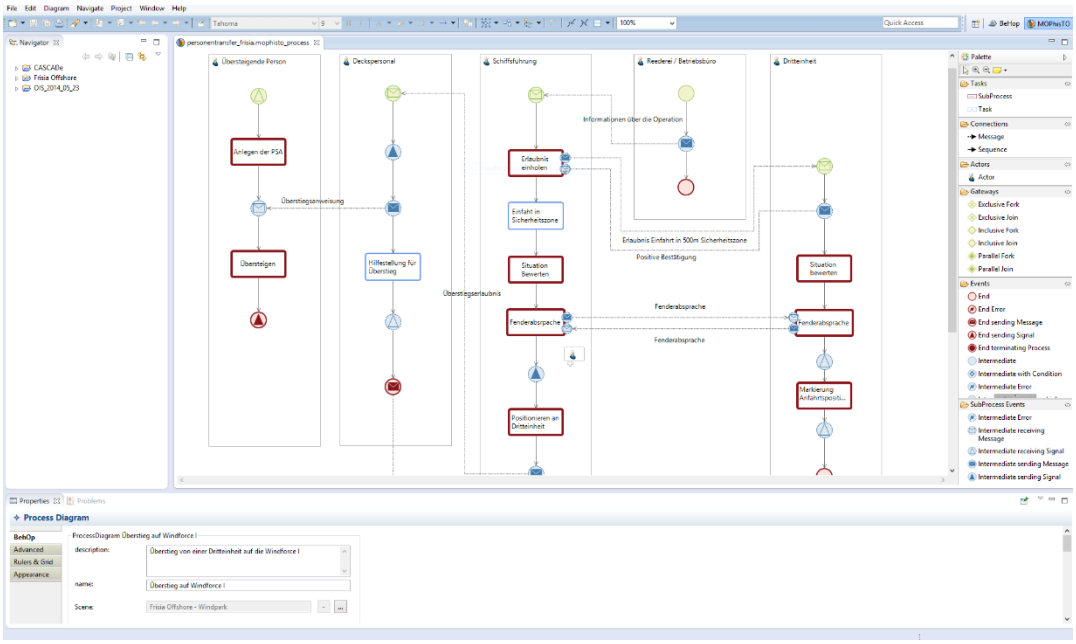


Abbildung 40: MOPhisTo - Prozesseditor

Als Basis zur Erstellung eines Prozesses bietet MOPhisTo fünf Typen von Prozesselementen, welche weiterhin anhand des gezeigten Beispielprozesses erläutert werden. Die fünf "Bahnen", die durch große Rechtecke umrahmt dargestellt werden, repräsentieren jeweils grafisch die Arbeitsprozedur (`WorkingProcedure`) eines Akteurs (`Actor`), z.B. eine übersteigende Person oder Deckspersonal, welche mit beliebig vielen andere Akteure in der Operation in Beziehung stehen können. In einer "Bahn" können verschiedene Flussobjekte (`FlowObject`) angeordnet werden. Diese werden unterteilt in Ereignisse (`Event`), Entscheidungspunkt (`Gateway`) und Aktivitäten (`Activity`). Eine Arbeitsprozedur eines Akteurs enthält dabei mindestens einen Anfang (`StartEvent`) und ein Ende (`EndEvent`). Eine Aktivität ist in Form eines kleinen Rechtecks dargestellt und bezeichnet die Tätigkeit, die in einer Operation ausgeführt wird. Es kann sich entweder um eine atomare Beschreibung einer Tätigkeit handeln (`Task`), oder um eine Aktivität, die in weitere Teilprozesse (`SubProcess`) untergliedert ist. Für die Ausführung des Prozesses beschreiben die Tätigkeiten die Manipulation eines Objektes in der Simulationsumgebung. Welches Objekt manipuliert wird ist dabei in der Tätigkeit durch eine Referenz in der eingebundene EMod-Datei vorgegeben. Ein Subprozess referenziert eine Datei des Typs .mophisto_subprocess. Diese stellt ein eigenständiges Diagramm mit Prozesselementen dar. Ein solches Subprozess-Diagramm enthält dabei keinen Akteur, da dieser bereits im ‚Main'-Prozess modelliert ist, in dem sich das hier beschriebene Prozesselement befindet. Um Nachrichten, Signale oder Abbruchbedingungen aus Subprozessen heraus zu verschicken, werden diese durch Events an dem zugehörigen Element in dem Hauptprozess annotiert.

Ereignisse werden in Form von Kreisen dargestellt und definieren entweder den Start- oder Endzeitpunkt einer Sequenz oder dienen der Darstellung von Interaktion zwischen Akteuren. Die Interaktion erfolgt in Form von Kommunikation, indem Nachrichten übertragen werden. Die Nachrichten werden global definiert und können wiederverwendet werden. Durch die Interaktion können Prozesse synchronisiert werden, indem ein Teilprozess nur angestoßen wird, wenn eine bestimmte Nachricht, z.B. ein Handzeichen, erhalten wird. Je nach Ausprägung des Events werden verschiedene Farben und kleine Symbole verwendet, bspw. startet ein Prozess mit einem grünen Kreis, eine Interaktion wird durch einen blauen Kreis, z.B. mit einem Brief für eine Nachricht, dargestellt und den Endzeitpunkt stellt ein roter Kreis dar.

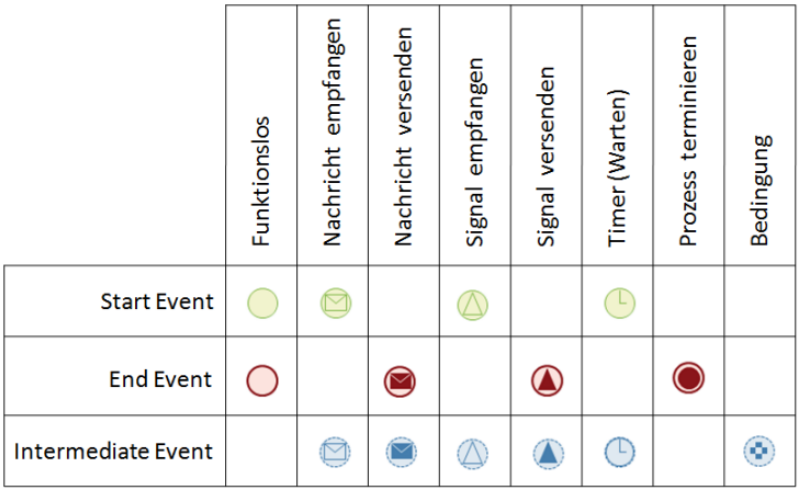


Abbildung 41: Funktionen der Events

Die Symbole für Entscheidungspunkte haben die Form eines Diamanten. Für jeden Entscheidungspunkt existieren im MOPhisTo - Prozessdiagramm zwei Typen. Zum einen eine Gabelung (`ForkGateway`), welche den Prozess in mehrere Prozessbahnen aufteilt, zum anderen für eine Zusammenführung (`JoinGateway`), welches die Prozessbahnen wieder zusammenführt. Ein exklusiver Entscheidungspunkt (`ExclusiveGateway`) hält mindestens zwei nachfolgende Prozessbahnen. Welche Prozessbahn ausgeführt wird, ist durch eine im Entscheidungspunkt modellierte Bedingung vorgeschrieben. Wichtig ist, das stets nur eine einzige der nachfolgenden Prozessbahnen ausgeführt wird. Bei einem inklusiven Entscheidungspunkt (`InclusiveGateway`) verhält es sich ähnlich wie bei dem exklusiven Derivat. Für jede nachfolgende Prozessbahn ist eine Bedingung modelliert. Jedoch werden beim Inklusiven alle Prozessbahnen ausgeführt deren Bedingung zutreffen und nicht nur eine einzige wie beim Exklusiven. Werden mehrere Prozessbahnen gleichzeitig ausgeführt, muss außerdem gewartet werden, bis die Ausführung aller Prozessbahnen erfolgt und in einer gemeinsamen Zusammenführung endet, vorausgesetzt die Prozessbahnen enden nicht in einem End-Ereignis. Ein paralleler Entscheidungsknoten (`ParallelGateway`) enthält keine Bedingung. Stattdessen

werden alle nachfolgenden Prozessbahnen parallel ausgeführt. Wie bei dem inklusiven Entscheidungspunkt muss auch hier darauf gewartet werden, dass alle Prozessbahnen die Zusammenführung erreicht haben, bis die weitere Ausführung des Prozesses erfolgen kann.

Um die einzelnen Flussobjekte miteinander zu verbinden, werden Verbindungen (`Connections`) verwendet, die Sequenzflüsse (`SequenceFlow`) in Form von durchgezogenen Linien und einfache Nachrichtenfluss (`MessageFlow`) durch gestrichelte Linien darstellen. Ein Sequenzfluss bildet die Verbindung zwischen zwei Prozesselementen. Wenn vom "nächsten Prozesselement" die Sprache ist, ist dabei gemeint, dass vom ausgehenden Prozesselement zum nächsten Prozesselement eine solche Verbindung existiert. Ein Nachrichtenfluss verbindet ein sendendes mit einemempfangenden Ereignis. Die Nachricht oder das Signal wird dabei direkt in einen solchen Fluss modelliert.

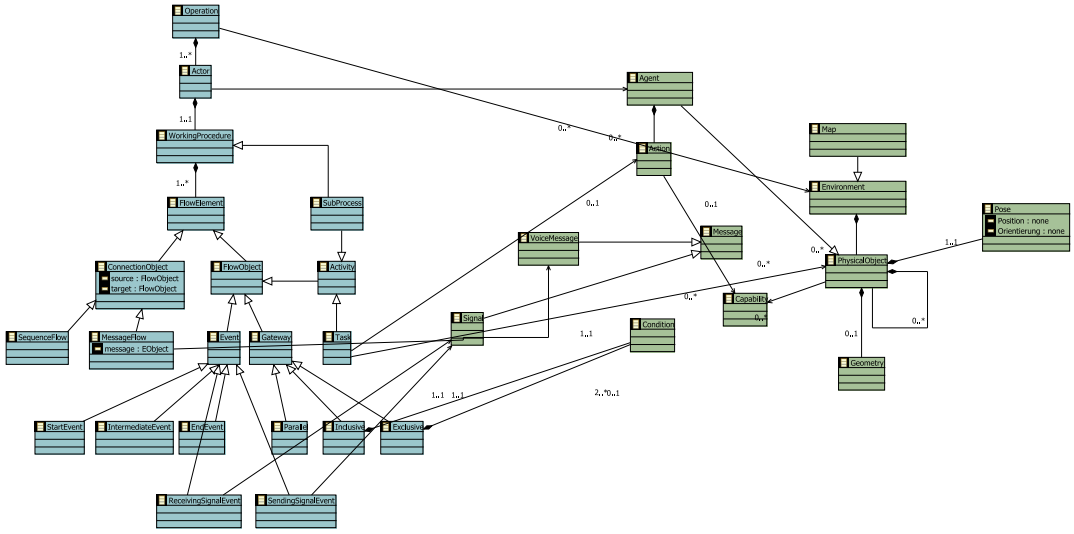


Abbildung 42: Integration der Umgebungsbeschreibung in den Prozess

Abbildung 42 zeigt die Integration der Umgebung in die prozessorientierte Modellbeschreibung. Einer Operation wird stets eine konkrete Umgebung zugeordnet, in der diese durchgeführt wird. Durch diese lose Kopplung wird erreicht, dass geplante Operationen für verschiedene Umgebungen angepasst werden können, andererseits für eine Umgebung mehrere Operationen geplant werden können.

Akteure werden in dieser durch Agenten (`Agent`) repräsentiert. Durch diese Integration ergeben sich ebenfalls die dadurch identifizierten Aktionen aus der Umgebung die für einen spezifischen Akteur in Form von Tätigkeiten planbar sind, eingeschränkt durch die dem Agenten zugewiesenen und den von der Aktion benötigten Fähigkeiten. Den Tätigkeiten können neben der Aktion ebenfalls Ressourcen die für die Durchführung dieser notwendig sind zugeordnet werden. Wie bereits erwähnt werden sind Bedingungen den verschiedenen Ereignissen zugeordnet, die Nachrichten (`Message`) den Nachrichtenflüssen. Signale (`Signal`) werden ebenfalls durch entsprechende Ereignisse in den Prozess integriert.

Ein gefährliches Ereignis (`HazardousEvent`) wird stets der gesamten Operation untergeordnet. Dies gilt ebenso für die Gefahr (`Hazard`) und der Betriebssituation (`OperationalSituation`). Die Ursachen (`Cause`) für die Gefahr werden entweder einem Akteur, oder einer konkreten Tätigkeit innerhalb von diesem, zugeordnet. Über die im Prozessschritt vorgestellte Verschachtelung von Aktivitäten mittels Subprozesse kann dies in beliebiger Prozesstiefe geschehen. Ursachen einer zugehörigen Gefahr können über mehrere Akteure verteilt werden. Minderungsmaßnahmen (`MitigationMeasure`) und Gegenmaßnahmen (`CounterMeasure`) werden innerhalb des Prozesses den Tätigkeiten, müssen demnach aktiv durchgeführt werden, um den entsprechenden Effekt auf den jeweiligen Risikofaktor einzuwirken. Abbildung 48 stellt die Integration der Gefahrenbeschreibung in das Prozessmodell dar.

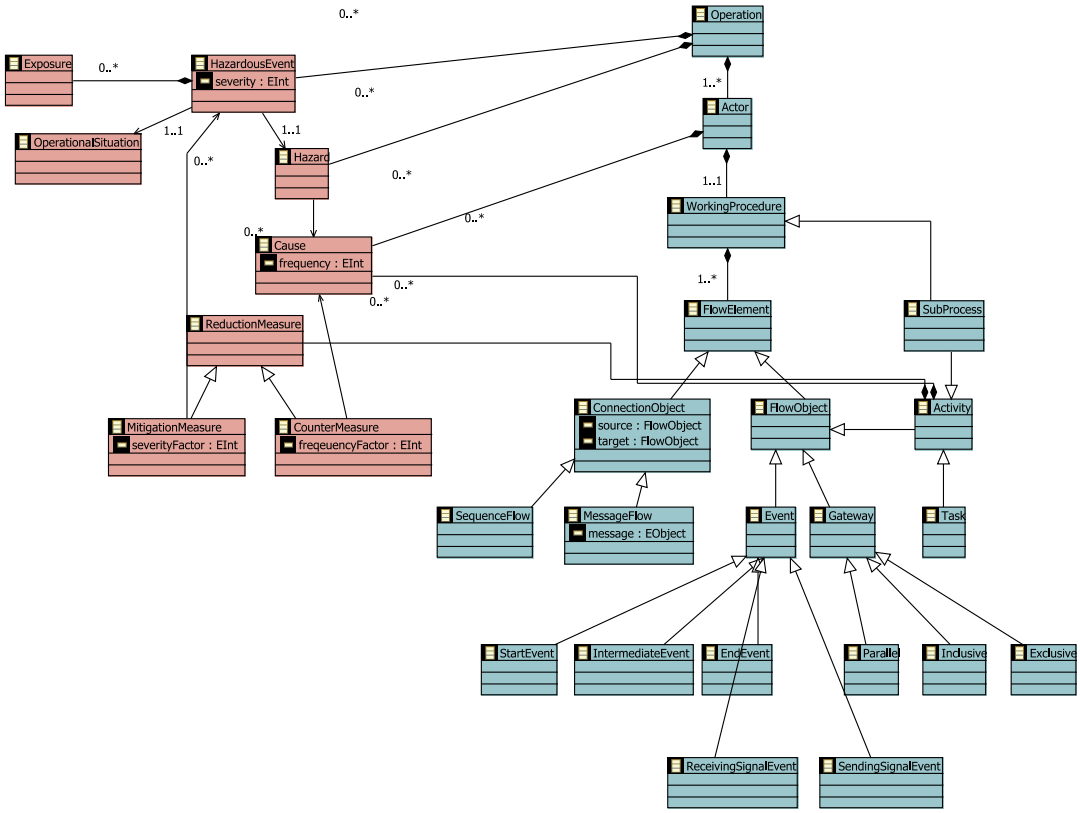


Abbildung 43: Integration der Gefahrenbeschreibung in den Prozess

Die Funktionalität der Gefahrenannotation wurde direkt in den Prozesseditor von MOPhisTo integriert. Die einfache und manuelle Art ist es die entsprechenden Prozesselemente zu selektieren und im Eigenschaftenfenster in der entsprechenden Rubrik die Eintragungen vornehmen. In den dort hinterlegten Dialogen werden neben der Konkretisierung dieser (z.B. Eintrittswahrscheinlichkeit oder Schadensschwere) ebenfalls die Möglichkeit gegeben die Zuordnung inklusive der Struktur von Gefahren und deren Ursachen gegeben. Um diesen Vorgang für die Domänenexperten zu unterstützen ist in der Methode eine Wissensbasis integriert, welche durch verschiedene Quellen befüllt wird (vgl. Anforderung **A11**). Neben den Analyseer-

gebnissen aus Unfallberichten und Guidelines sind im Besonderen historisch geplante Prozesse und mit denen einhergehend die Gefahrenbewertungen Input für diese. Die Nutzung dieser Wissensbasis ermöglicht die Identifikation möglicher Gefahren und Ursachen über mehrere Faktoren und liefert gefilterte Listen potentieller Risiken. Bei der Überführung von Wissen in diese Datenbasis wird dieses generalisiert und mit semantischen Informationen angereichert. Für die Benutzung innerhalb der Methodik wurde der "Hazard Identifcation Wizzard" entwickelt, welcher neben einfachen textbasierten Vergleichen ebenfalls die Semantik berücksichtigt (vgl Abbildung 44). Abhängig von dem im Prozess selektierten Element und von der Parametrisierung der Suche werden Vorschläge für Gefahren und deren Ursachen gegeben. Verglichen werden dabei beispielsweise ähnliche Prozessschritte oder die Akteure. Die Wissensbasis kann, soweit bereits hinterlegt, ebenfalls die historisch definierten Ursachenstrukturen und die Bewertungen von der Schadensschwere oder den Eintrittswahrscheinlichkeiten anzeigen.

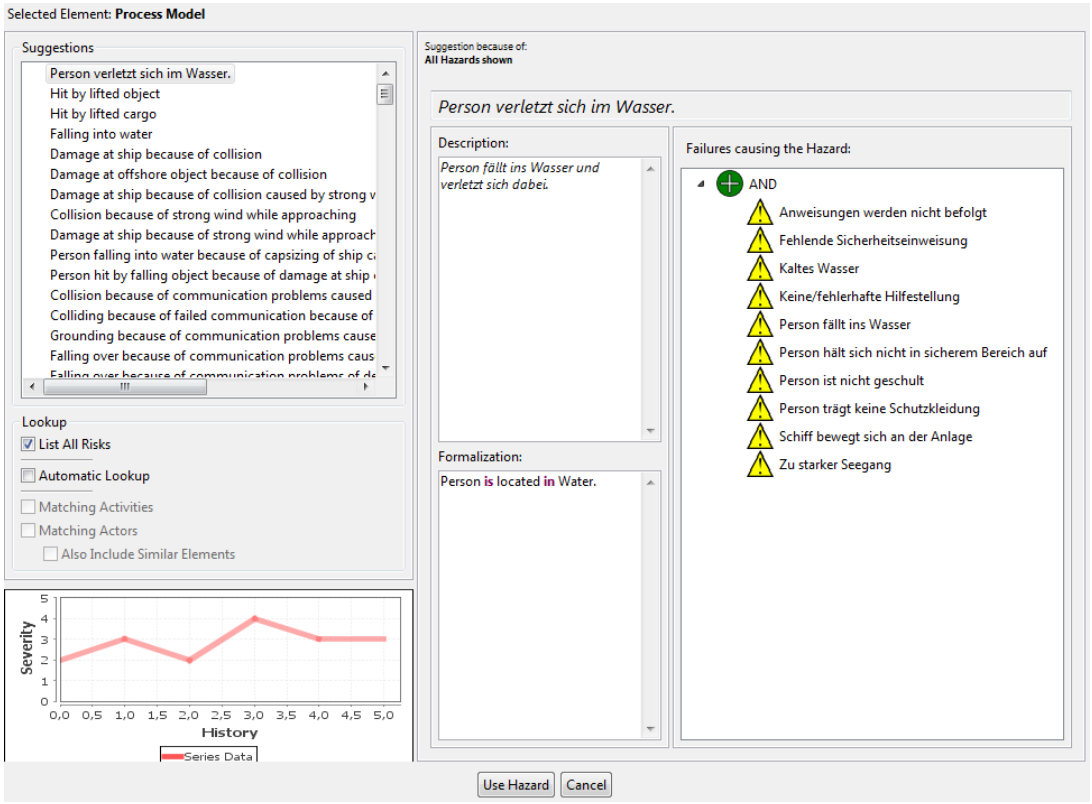


Abbildung 44: MOPhisTo - Hazard Identification Wizzard

Dieser Dialog dient lediglich zur Unterstützung und kann bzw. darf dem Experten nicht die Verantwortung für die gewissenhafte Identifikation von Gefahren und Ursachen abnehmen. Wenn demnach Daten aus der Wissensbasis wiederverwendet werden müssen diese demnach stets durch den Experten individuell geprüft und bestätigt werden.

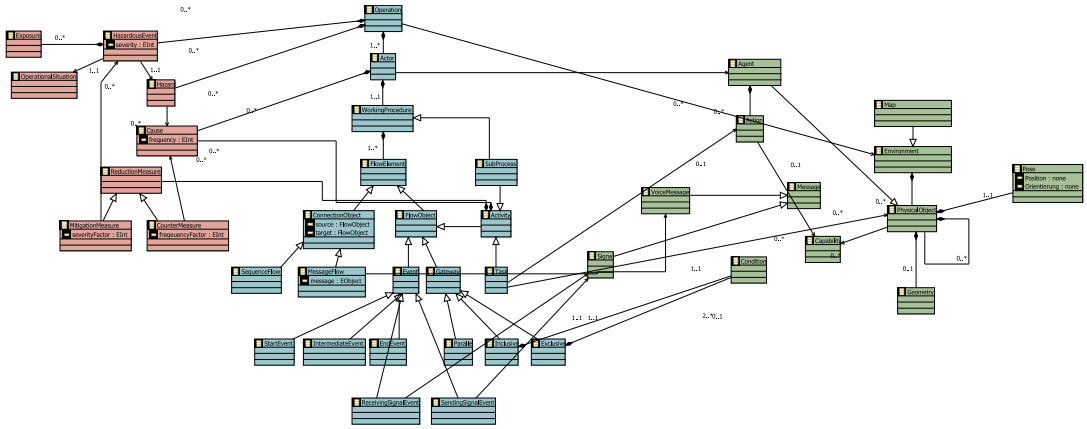


Abbildung 45: Integriertes Modell

Abbildung 45 zeigt eine Gesamtübersicht über das integrierte, prozessorientierte Modell. Hier wird sichtbar, wie über das gesamte Modell hinweg eine ganzheitliche Bewertung der Arbeitsanweisungen möglich ist. So können Arbeitsprozesse einer Operation und die Ausrüstung, die in jeden Schritten eingesetzt wird, beschrieben werden. Neben der Identifizierung und Integration von potenziellen Gefahren werden ebenfalls deren Vorsichtsmaßnahmen bzw. Gegenmaßnahmen, die für diese getroffen werden, konkret in den Prozess eingeplant werden. Durch die Zuordnung der Tätigkeiten zu verschieden Akteuren wird ebenfalls die die Verantwortung des an diesen involvierten Personals deutlich [IS15].

Für den Schritt der quantitativen Gefährdungsbeurteilung wurde im Rahmen der Dissertation von Pinkowski [Pi15] ein Modul für die automatische Erzeugung und Darstellung von Fehlerbäumen innerhalb von MOPhisTo entwickelt. Das Modul verwendet dabei die in dem vorhergehenden Schritt annotierten Gefahrenbeschreibungen und die Struktur des Prozessmodells, um die Fehlerbaumstruktur zu generieren.

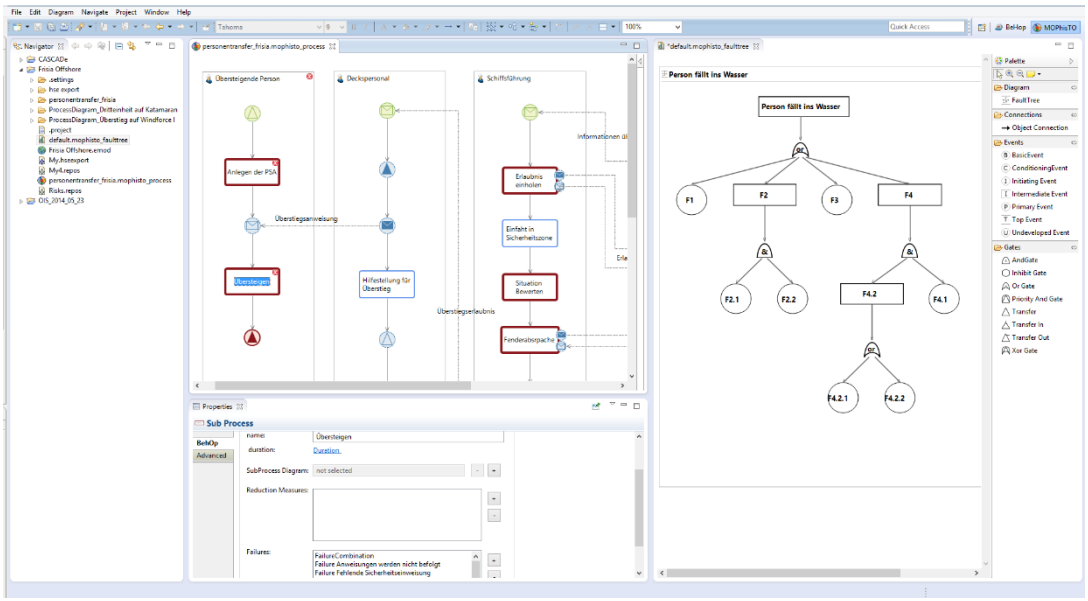


Abbildung 46: MOPhisTo - Fehlerbaumeditor

Im rechten Abschnitt zeigt Abbildung 46 einen aus dem Prozessmodell (links) generierten Fehlerbaum. Durch das den beiden Modulen gemeinsam zugrundeliegende Modell wird nicht nur die Integrität sichergestellt. Es ermöglicht ebenfalls eine werkzeugseitige Unterstützung. So können beispielsweise zu den Fehlerbaumelementen gehörende Prozessmodell-Elemente hervorgehoben werden. Neben der Modifizierung von automatisch generierten Fehlerbäumen können Domänenexperten mit dem Fehlerbaumeditor neue Strukturen erstellen.

Für die Umsetzung der qualitativen Gefahrenbeurteilung wurde auf das Simulationsframewok HAGGIS zurückgegriffen. Das Framework bietet neben verschiedenen Co-Simulationen und Steuerungskomponenten eine zentrale Instanz für Sicherstellung der Interoperabilität. In dem Simulationskern wird neben der zeitlichen Taktung ein gemeinsamer Speicher für die Objektverwaltung der Simulationsumgebung bereitgestellt. Zu den für diese Forschungsarbeit relevanten Co-Simulationen gehören die Maritime Traffic Simulation (MTS) und die Physical World Simulation (PWS). MTS ist eine flexibel einsetzbare maritime Verkehrssimulation, welche bei der Umsetzung, dem Ausführen und Beobachten des Verhaltens von mehreren Schiffe unter nahezu realistischen Bedingungen unterstützt. Für jedes dieser Schiffe ist ein dynamisches Modell, welches das Verhalten in Abhängigkeit zu den Umwelteinflüssen wie Wellen, Strömungen oder auch Wind beschreibt, hinterlegt. Die PWS ist eine Mehrkörpersimulation für die Berücksichtigung physikalischer Wechselwirkungen von starren Körpern innerhalb der simulierten Umgebung [SDH12].

Für die Kommunikation zwischen den Komponenten wird dabei HLA – RTI eingesetzt. Die High Level Architecture (HLA) ist eine Kommunikationsschnittstelle für verteilte Simulationen. Die Kommunikation zwischen den Simulationen wird dabei von einer Run-Time Infrastructure (RTI) geregelt. Die ausgetauschten Objekte werden dabei mit dem HAGGIS Datenmodell beschrieben. Für die Ausführung des im MOPhisTo Prozesseditor definierten, normativen Verhaltens wurde ein Interpreter MASCaS für die Prozessmodelle entwickelt. Das Grundkonzept von MASCaS ist die Erstellung einer Multi-Agenten-Simulation, welche das im Prozess beschriebene Verhalten der Akteure ausführt. Für das Aufsetzen und Steuern von Simulationsläufen innerhalb von HAGGIS wird das Distributed Controlling Toolkit (DistriCT) eingesetzt (vgl. Abbildung 47).

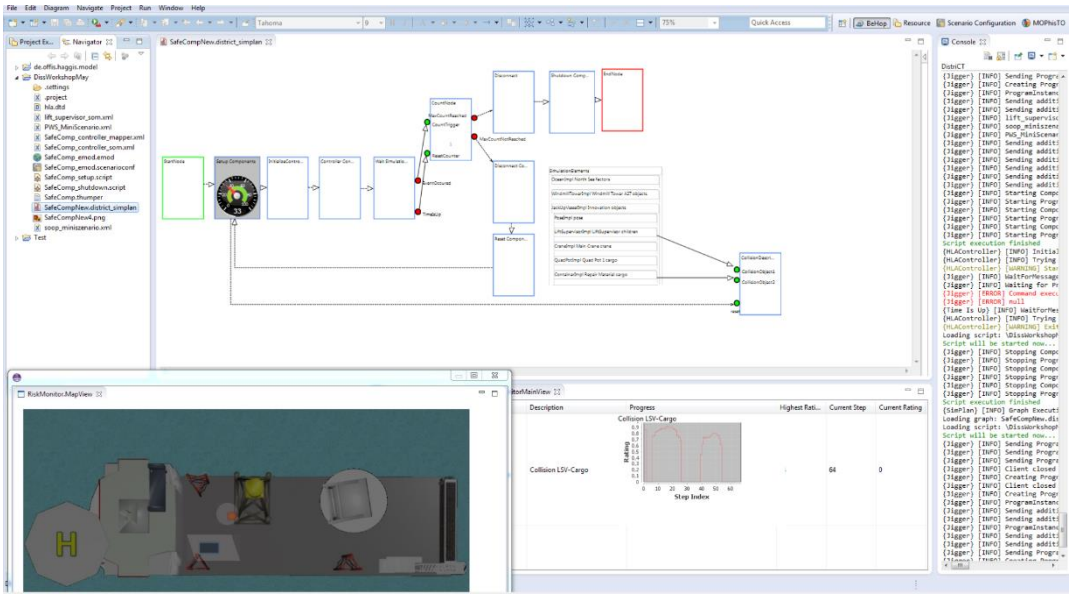


Abbildung 47: DistriCT - Qualitative Validierung durch Simulation

Mit DistriCT können die verschiedenen Komponenten entsprechend des modellierten Szenarios konfiguriert, gestartet und gestoppt werden. Dies kann beispielsweise benutzt werden, um bewusst Fehler zu injizieren oder eine systematische Parameterexploration durchzuführen. Während der Simulation können neben dem Systemstatus ebenfalls logische oder physikalische Zusammenhänge zu gefährlichen Situationen erfasst werden. Mittels dieser kann gezielt ein Simulationslauf in Richtung kritischer Situationen gesteuert oder auch seltene Ereignisse gesucht werden. Zudem führt es zu einer Reduktion der erforderlichen Simulationsläufe [Go16] . Die Erkenntnisse der Simulationsläufe werden anschließend von dem Experten genutzt, um ggf. neue Risikoaspekte in das Modell zu integrieren, oder aber Parameter anzupassen.

Als finaler Schritt erfolgt die Empfehlung für das Sicherheitskonzept, basierend auf den Informationen aus dem integrierten Modell. Die Erstellung eines textuellen HSE-Plans, inklusive der Arbeitsanweisungen, der Beschreibung Gefahren und Ursachen, inklusive deren Eintrittswahrscheinlichkeit, sowie der Schadensschwere und der daraus ermittelten Risikobewertung, erfolgt dabei automatisiert (vgl. Anforderungen **A10**, **A14**). Es ist hierbei möglich, eine detaillierte Version des HSE-Plans inklusive Schaubilder der einzelnen Prozessabschnitte, um Verständnisprobleme von relativ neuen bzw. ungeübten Mitarbeitern zu vermeiden, oder für bereits geschulte Mitarbeiter eine abstraktere Version zu erstellen (vgl. Abbildung 48).

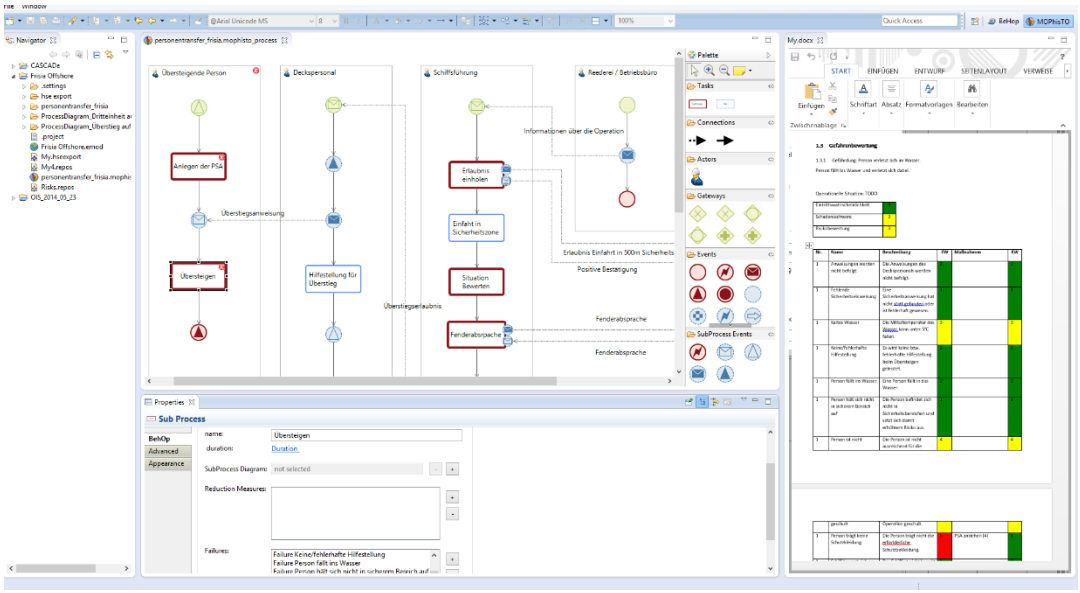


Abbildung 48: MOPhisTo - HSE-Plan Export nach Microsoft Word

4 Evaluation

Die sich aus der Motivation und den existierenden Konzepten und Ansätzen heraus ergebenen Anforderungen wurden in den im vorgegangenen Kapitel beschriebenen Lösungsansatz überführt. Darauf aufbauend resultierte abschließend eine prototypische Umsetzung, welche für die Evaluation folgender Ziele eingesetzt wurde:

- Überprüfung der Zielerfüllung bzw. Anforderungsabdeckung
- Demonstration der Anwendbarkeit
- Validierung der modellbasierten Methodik

Durchgeführt wurde die Evaluation im Rahmen des Forschungsprojekts SOOP. Die Arbeitsziele des EFRE geförderten maritimen Innovationsverbundes sind die Steigerungen des Personen- und Umweltschutzes, der Prozesssicherheit und der Effizienz bezüglich Kostenreduktion bei Offshore-Operationen mittels eines integrierten IT-gestützten Missions- und Risikomanagements. Dabei liegt der Fokus auf der Unterstützung der Planungsphase von Offshore-Operationen, des Trainings und der Durchführung durch integrierte Modellierungs- und Assistenzsysteme. Abbildung 49 zeigt im Überblick das Vorgehensmodell für die sichere Gestaltung und Durchführung von Offshore-Operationen.

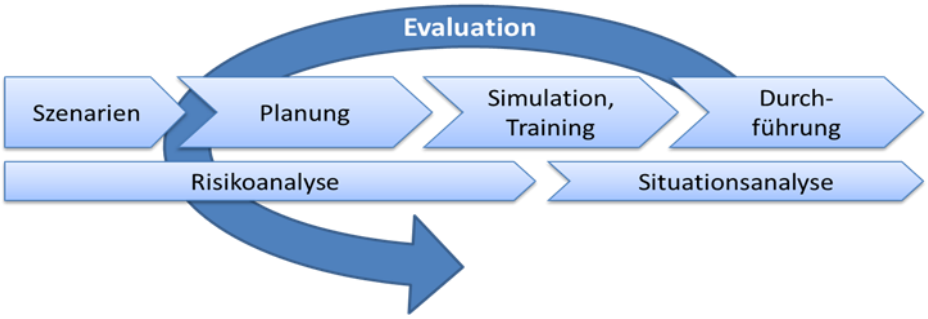


Abbildung 49: SOOP Vorgehensmodel

Ausgehend von den Szenarien "Übersteigen" & "Ladungsversatz" werden Referenzoperationen entwickelt, die als Basis für verschiedene gleichartige Missionen verwendet werden können. Für eine konkrete Operation erfolgt zunächst eine Planungsphase, in der die Operation in Zeit und Raum unter Verwendung von Standardbausteinen und Verhaltensmodellen für Menschen, Material und Umwelt beschrieben wird. Hierbei werden sowohl der optimale Ablauf einer Operation als auch mögliche Fehlerursachen und Risikosituationen modelliert. Die entworfenen Planungs- und Verhaltensmodelle werden für Simulationen und formale Risikoanalysen genutzt, die bereits im Vorfeld helfen, mögliche Gefahren zu identifizieren und zu vermeiden. Anschließend werden die verifizierten Planungsmodelle in Simulatoren für Training und Optimierung genutzt.

Die tatsächliche Durchführung der Operation unterstützt ein sensorgestützter Missionsassistent, der die Ist-Situation mit der aus Simulation und Planung bekannten Soll-Situation der Operationen vergleicht. Der Missionsassistent erstellt auf Basis der Sensordaten ein Operationsbild und prüft, in wie weit dieses innerhalb des vorgesehenen Operationskorridors liegt. Die Daten kommen aus einem verteilten Sensornetzwerk, das Sensordaten aggregiert und bereitstellt. Wenn während der Durchführung kritische Situationen erkannt werden, erzeugt der Missionsassistent Warnungen und Analysen, so dass die verantwortlichen Personen geeignet auf die kritische Situation reagieren können.

Das Übersteige-Szenario wurde ausgewählt, um die Evaluation der ersten Phasen von SOOP durchzuführen. Dies beinhaltet die Szenario-Definition und Planungsphase der Operation und eine anschließende Risikoanalyse. Mittels des Verladeszenarios werden verstärkt die Aspekte der Simulation und die Funktion des Missionsassistenten evaluiert.

Anhand dieser beider Szenarien wird im Folgenden untersucht in wie weit sich die entwickelte modellbasierte Methodik für die Planung und Gefährdungsbeurteilung maritimer Operationen eignet.

4.1 Fallbeispiel "Personentransfer"

Das erste Fallbeispiel behandelt den Transfer einer Person von einem Schiff auf eine Offshore-Windenergie-Anlage. Es evaluiert den Einsatz der modellbasierten Methodik anhand eines Vorganges, der in allen Phasen des Lebenszyklus eines Offshore-Windparks durchgeführt wird, und somit repräsentativ für die Domäne ist. Das Fallbeispiel deckt somit eine große Gruppe von Domänen-Experten ab, die inhaltlich mit dem Szenario vertraut sind. Die Fragestellung für die Evaluation am Beispiel "Personentransfer" lautet wie folgt:

Eignet sich das prozessorientierte Planungsmodell für die Durchführung einer quantitativen Risikoanalyse und -Bewertung maritimer Operationen?

Nach einer kurzen Einführung in das Fallbeispiel, wird im Detail auf den Anwendungskontext eingegangen. Dieser bildet die Ausgangslage für die spätere Durchführung, welche in einem zweistufigen Verfahren behandelt wird. Zunächst wird der Ansatz der quantitative Risikoanalyse und -bewertung nach Pinkowski [Pi15] angewandt. Anschließend erfolgen eine Evaluation der Gesamtmethodik, Planung und Gefahrenbewertung der Operation, und dessen Ergebnisse anhand einer Nutzwertanalyse mit Unterstützung von Domänen-Experten. Abgeschlossen wird das Fallbeispiel durch eine Zusammenfassung und einer anschließenden Diskussion.

4.1.1 Durchführung

Im Folgenden werden die Schritte der in Kapitel 3.3 eingeführten Methodik auf das Fallbeispiel "Personentransfer" angewandt, wobei in diesem Fall die qualitative Validierung durch Simulation vernachlässigt wird. Dabei werden die in Abschnitt 3.6 dargestellten prototypischen Implementierungen eingesetzt und dabei eine entsprechende Instanz des integrierten Modells erzeugt.

Der Personentransfer kann je nach Schiff und Gegebenheit auf unterschiedliche Arten erfolgen [Th10a]. Der Transfer von Personal auf und von Windkraftanlagen ist durch die Umweltbedingungen maßgeblich beeinflusst. Die Art von Operationen wird in der Seefahrt zwar häufig durchgeführt (z.B. Lotsenübergabe), ist hier aber besonderen Einflüssen ausgesetzt. In diesem Fallbeispiel wird die gängigste Variante, nämlich der Transfer mit einem Crew Boot, gewählt. Ein Crew Boot ist ein größeres Schiff, welches häufig für Versorgungsfahrten und Personentransfers zum Einsatz kommt. Es wird an die windgeschützte Seite der Offshore-WEA manövriert und drückt sich langsam mit dem Bug voraus gegen die Plattform. Dabei steht ein Einweiser am Bug mittels Funk o.ä. im permanenten Kontakt zur Brücke stehen. Diese Boote sind oft mit passgenauen Gummi-Manschetten ausgerüstet, sodass diese Boote stabiler an der Plattform liegen. Manche Boote und Plattformen besitzen sog. 'Surfer', dies sind Einrichtungen am Boot und an der Plattform, die stabil ineinander greifen und das Übersetzen von Personen erleichtern. Es gelten bei diesem Vorgang dieselben Gefahren wie bei einem Transfer mit einem kleinen Boot, sodass unbedingt Schutzausrüstung getragen werden sollte und Assistenzkräfte beim Transfer helfen müssen. Nach dem Transfer entfernt sich das Boot langsam rückwärts und geht auf Abstand zur Plattform.

Beschreibung der Umwelt inklusive Ressourcen

Umweltbedingungen, wie beispielsweise das Wetter und der Wellengang, spielen eine zentrale Rolle für alle Tätigkeiten der Offshore-Industrie. Sie nehmen großen Einfluss auf die Arbeit und die Anlagen auf offener See. Neben den örtlichen Faktoren, z.B. Lage des Offshore-Windparks und damit einhergehend weiten Rettungswegen, sind die Umweltbedingungen wesentlich für die Differenzierung der Risiken unter verschiedenen Betriebssituationen.

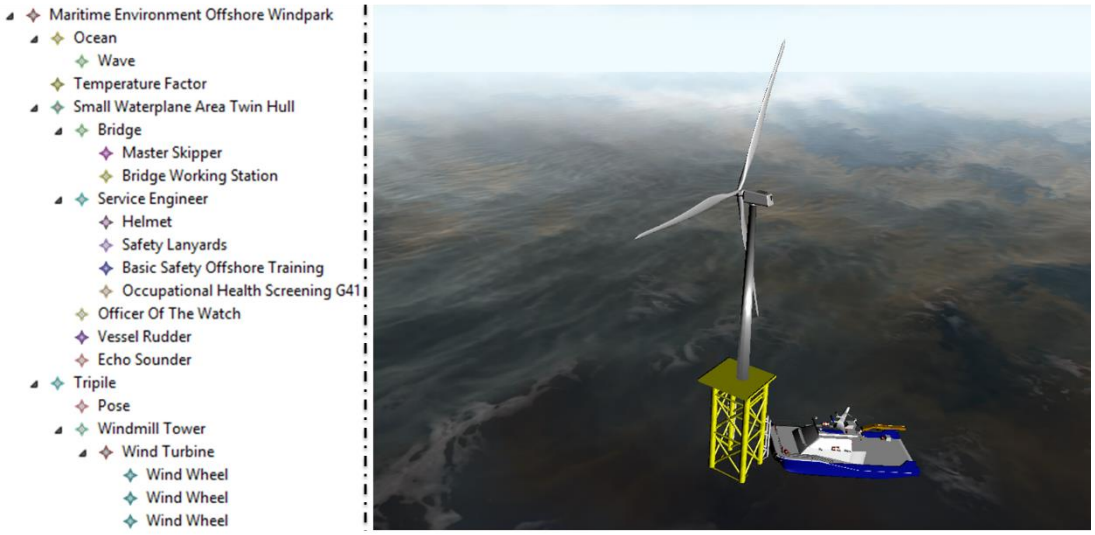


Abbildung 50: Beschreibung des Szenarios "Übersteigen"

Abbildung 50 beschreibt das Szenario "Übersteigen". Bei den hierarchisch aufgeführten Elementen handelt es sich lediglich um einen Ausschnitt. Das komplette Modell kann aus komplexitätsgründen nicht vollständig abgebildet werden. In der folgenden Beschreibung werden die exemplarisch selektierten Elemente der Abbildung referenziert.

Für den Vorgang des Personaltransfers mittels Crew Boot werden folgende Umweltbedingungen berücksichtigt:

- Windgeschwindigkeit und -richtung
- Strömungsstärke und -richtung
- Gezeiten
- Wellenhöhe und -richtung `(EnvironmentalFactor: Wave)`
- Sichtweite (über Wasser) und -verhältnisse (z.B. Nebel, Regen),
- Temperatur
- Gischt-Bildung

Das Crew Boot (`PhyiscalObject: Small Waterplane Area Twin Hull`) ist ein zentrales Element des Szenarios. Es besteht aus vielen verschiedenen Komponenten wie z.B. Rumpf, Brücke (`PhyicalObject: Bridge`), Hauptdeck und ggf. spezifischen Besonderheiten hinsichtlich der Bauart, welche Einfluss auf die Durchführung und die Sicherheit der Operation nehmen. Weiterhin ist in einem Schiff viel Technik verbaut, welche relevante Informationen enthalten, die ebenfalls in dem Modell abgebildet werden. Dazu gehören unter anderem Primärantrieb, Sekundär-Antriebe (schwenkbare Düsen/Propeller), Kommunikationssysteme, Navigationssysteme, Sensoren (für Wind/Regen/Temperatur), Radar oder Echolot (`PhysicalObject: Echo Sounder`).

Die Personen an Bord nehmen eine gesonderte Rolle ein. Sie erfüllen viele Funktionen und kommunizieren miteinander. Sie stehen in einer Befehlskette und sind auch für bestimmte Handlungen verantwortlich. Obwohl das Personal geschult ist, kann menschliches Versagen nicht völlig ausgeschlossen werden. Der Kapitän (`Agent: Master`) ist die oberste Autorität an Bord eines Schiffes und verantwortlich für die Operationen. Er hat die Befehlsgewalt und somit stehen seine Entscheidungen über die der anderen Crew-Mitglieder. Die Assistenzkräfte (`Agent: Officer Oft The Watch`) unterstehen dem Kapitän und sind entsprechend eingewiesen. Sie unterstützen den Transfer von übersetzenden Personen. Die zu übersetzende Person (`Agent: Service Engineer`) ist an allen Übersetzungsvorgängen beteiligt. Sie sollte eingewiesen sein und dem Transfer zugestimmt haben, da sie das größte Risiko trägt. Zudem wird eine Mindestanzahl an Zertifikaten wie z.B. Basis-Sicherheitstraining für Offshore-Arbeiten (`offshoreQualification: Basic Safety Offshore Training`) vorausgesetzt. Die Schutzausrüstung für die Personen ist sehr wichtig und sollte je nach Risiko gewählt werden. Das beinhaltet Sicherheitshelm (`PhysicalObject: Helmet`), Sicherheitsschuhe, evtl. Schwimmweste, Sicherheitsbrille, Sicherheits-Handschuhe, Sicherheitsleinen (`PhysicalObject: Saftey Lanyards`), evtl. Überlebensanzug, Pfeife und Sender. Über die Kommunikationsmittel verständigen sich die einzelnen Personen und koordinieren die Operation. Eine standardisierte Kommunikation ist empfehlenswert. Es gibt mehrere Arten von Kommunikationen: Routine (z.B. Anmeldung), Operation (z.B. beim Transfer) und Notfall. Diese Arten der Kommunikation sind nach Prioritäten gegliedert. Es gibt verschiedene Kommunikationsmöglichkeiten und während einer Operation sollten mehrere zur Verfügung stehen, um bei Ausfall Alternativen zu besitzen. Zu den Kommunikationsmitteln zählen Funk (VHF/UHF), Schiffstelefon / Gegensprechanlagen, Mobilfunknetz, Satelliten-Telefon, Handsignale, Lichtsignale und Pfeifsignale. Die Wahl des Kommunikationsmittels beeinflusst ebenfalls die Operation, da, wenn hand- und nicht sprachaktiviert, dem Nutzer nur eine Hand zur Verfügung steht. Die Plattform auf welche die Person übersetzt, ist ein weiteres Objekt dieses Szenarios. Da das Schiff sich in unmittelbarer Nähe befindet, besteht das Risiko der Kollision. Die Plattform kann von unterschiedlicher Bauart (z.B. Höhe, Länge, Breite, Gewicht) sein und darum eine Vielzahl von Eigenschaften besitzen. Sie wird sehr stark von Umweltbedingungen beeinflusst und dementsprechend ist auch mit der Gefahr des Materialversagens an stark beanspruchten Stellen zu rechnen. Auch weitere besondere Eigenschaften der Plattform, wie z.B. Geländer oder Leitern (evtl. rutschig, vereist oder zerbrechlich), und auch der konkrete Übersetzpunkt (evtl. rutschig oder vereist - gute Ausleuchtung?) müssen berücksichtigt werden.

Erstellung des Prozessmodells

Die zu übersetzende Person (`Actor: Offshore Personnel`) und weitere beteiligte Personen müssen ihre Einweisung erhalten, eine Aufklärung über die Gefahren und Risiken bekommen und sich mit dem nötigen Sicherheits-Equipment ausrüsten. Weiterhin sollten Checklisten, welche z.B. die Überprüfung des Transfer-Equipments, der Kommunikationsmittel (z.B. `PhysicalObject: UHF`…) usw. beinhalten abgearbeitet werden. Der Kapitän muss sein Schiff und die Operation mindestens eine Stunde vor Ankunft bei der für den Sektor des Windparks zuständigen Aufsicht anmelden und eine Übereinkunft mit dem Ziel über Ablauf, Kommunikation (Mittel, Frequenz usw.) und der zu erfüllenden Checklisten treffen. In der Regel wird eine Offshore-Anlage von einer Sicherheitszone mit dem Radius von 500m umgeben, welche nur von Errichterschiffen und Schiffen für die Versorgung der Anlage befahren werden darf. Ab hier startet das Anwendungsszenario "Übersteigen" (vgl. Abbildung 51).

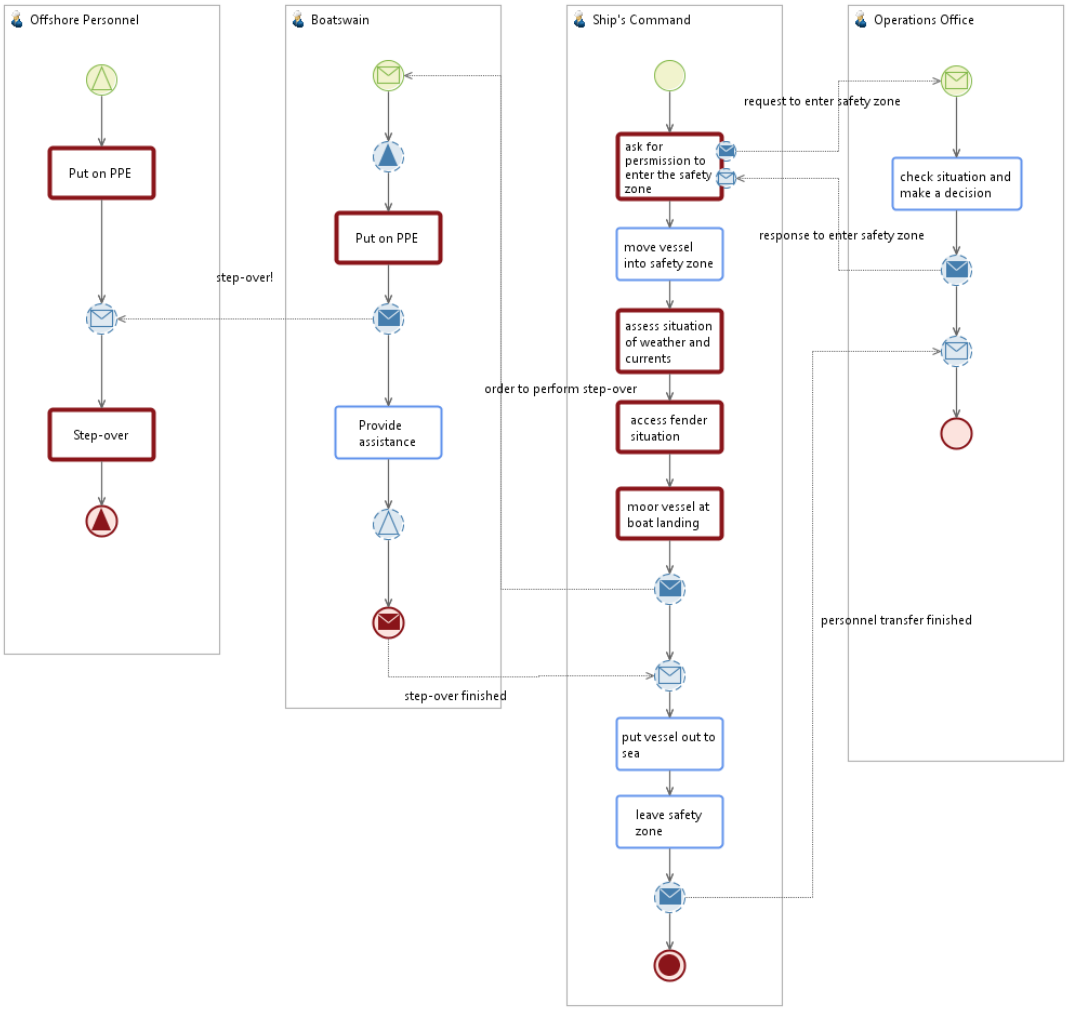


Abbildung 51: Anwendungsszenario "Übersteigen"

Vor Eintritt in diese Zone muss der Schiffsführer (`Actor: Ship's Command`) bei der für den Windpark verantwortlichen Instanz (`Actor: Operations Office`) um Erlaubnis bitten

diese Zone befahren zu dürfen (`SubProcess: ask for persmision to entert he safety zone`). Um die Erlaubnis für die Einfahrt in die besagte Zone zu erhalten, müssen vorab die erforderlichen Checklisten erfüllt worden sein. Ist diese Erlaubnis erteilt, darf sich das Schiff mit langsamer Fahrt der Anlage nähern (`Task: move vessel into safety zone`). Zirka 50 m vor der Plattform sollte das Schiff halten und für einen gewissen Zeitraum (10-15min) die Rahmenbedingungen (Wetter, Seegang, Lage) des Transfers erfassen (`SubProcess: asses situation of wather and currents`). Sind diese erfasst und entsprechen diese den Voraussetzungen für einen sicheren Transfer wird mit dem Manöver begonnen. Während des Manövers sollte eine reibungslose Kommunikation zwischen Brücke und dem auf dem Schiff stehenden Einweiser (`Actor: Boatswain`) stehen. Dabei ist zu beachten, dass vor Beginn jedes Transfers, die Checklisten für die Art des Transfers (bezüglich des Equipments und des Vorgangs) erfüllt werden müssen. Der Schiffsführer manövriert nun das Boot an die windgeschützte Seite der Anlage und fährt mit dem Bug voraus langsam gegen die Plattform. Dabei sollte ein Einweiser am Bug mittels Funk o.ä. im permanenten Kontakt zur Brücke stehen. Das Schiff wird mit langsamer Fahrt vorwärts gegen die Plattform gepresst und befindet sich anschließend in einer stabilen Lage. In diesem Moment kann die zu übersetzende Person auf die Plattform steigen. Dabei sollte die Person unbedingt von Assistenzkräften unterstützt werden, da sich die rutschige Plattform weiterhin mit dem Schiff bewegt. Diese Methode birgt ein hohes Risiko. Zusätzlich sind die beteiligten Personen den Umweltbedingungen (z.B. starker Wind) ausgeliefert, sodass unbedingt eine entsprechende Schutzausrüstung getragen werden sollte. Nach dem Transfer entfernt sich das Schiff langsam rückwärts, geht auf Abstand zur Anlage und verlässt die Sicherheitszone.

Identifizierung von Gefährdungen

Die größte Gefahr in diesem Szenario ist, dass die übersetzende Person oder eine Assistenzkraft über Bord geht. Dies kann aus vielerlei Gründen geschehen und je nach Art der Durchführung des Transfers ist das Risiko dafür unterschiedlich hoch. Es reicht beispielsweise eine ruckartige Bewegung des Schiffes oder ein falscher Tritt auf rutschigem oder vereistem Untergrund. Laut [Th10a] sollten Vorkehrungen getroffen werden, um das Risiko über Bord zu gehen zu minimieren und bei einem tatsächlichen Unfall mit dementsprechenden Notfallmaßnahmen zu reagieren. So ist im Vorfeld eine gute Einweisung und Sicherheitsbelehrung für alle Personen erforderlich und die aktiv beteiligten Personen sollten mit entsprechender Schutzausrüstung, insbesondere mit einer Schwimmweste, oder in kälteren Gewässern mit einem Überlebensanzug ausgestattet sein. Das Verletzungsrisiko bei diesem Transfer ist ebenfalls hoch. Personen können stürzen oder sich Gliedmaßen z.B. zwischen Schiff und Anlage einklemmen. Hier spielt wieder die richtige Schutzausrüstung eine große Rolle. Ein weiteres

Risiko ist ein Wetterumschwung während des Transfers. Dadurch kann der Wellengang stark zunehmen, die Sichtverhältnisse können schlechter werden und Regen und Wind werden zu einem großen Sicherheitsrisiko. Der Kapitän sollte die sich wechselnden Umweltverhältnisse berücksichtigen und dementsprechend handeln. So sollte gegebenenfalls auf eine andere Art des Transfers zurückgegriffen, der gesamte Vorgang verschoben oder gar abgebrochen werden.

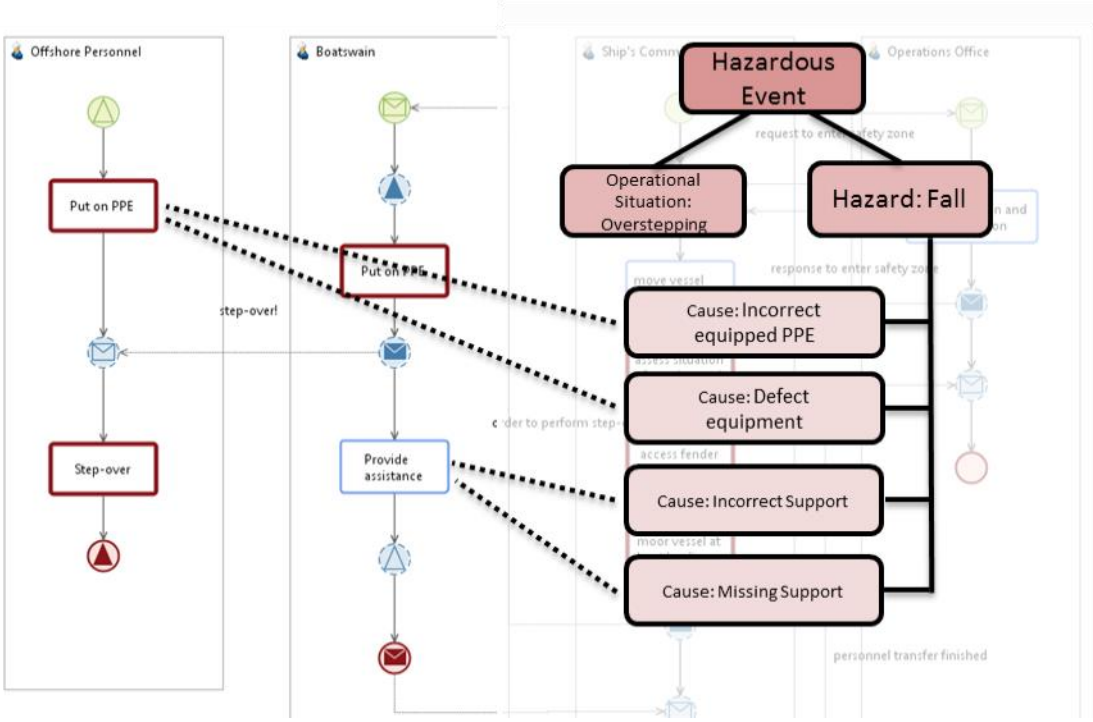


Abbildung 52: Identifizierung von Gefahren und Ursachen und deren Verortung im Prozess

Abbildung 52 zeigt exemplarisch die Identifizierung der Gefahr "Sturz" (`Hazard: Fall`) und die Betriebssituation "Überstieg" (`OperationalSituation: Overstepping`). Die möglichen Gefahren und Ursachen werden innerhalb der Prozessbeschreibung ergänzt. Sie ergeben sich zum aus der Tätigkeitsbeschreibung, oder aber aus der Verwendung von Hilfsmitteln. Ersteres ergibt sich beispielsweise aus der Tätigkeit "Hilfestellung geben" (`Task: Provide assistance`), aus der sich die möglichen Ursachen der "falschen Unterstützung" (`Fault: Incorrect Support`) bzw. der "fehlenden Unterstützung" (`Cause: Missing Support`) ergeben. Ein Beispiel für eine Hilfsmittel bezogene Gefahrenursache ergibt sich aus der Tätigkeit "Anlegen der persönlichen Schutzausrüstung" (`Task: Put on PPE`). In dieser wird neben der möglichen Ursache des "falschen Anlegen der Ausrüstung" (`Cause: Incorrect equipped PPE`) die "defekte Ausrüstung" (`Cause: Defect equipment`) aufgeführt. Während der Annotation der Ursachen wird bereits eine Zuordnung zu einer möglichen Gefahr vorgenommen.

Quantitative Risikoanalyse und –Bewertung

Die Verortung der Ursachen innerhalb des Prozesses in Kombination mit der erwähnten Zuordnung zu Gefahren nutzt Pinkowski in seinem Ansatz um konkrete Zusammenhänge abzuleiten. Das Resultat spiegelt sich in einem strukturierten Fehlerbaum wieder (vgl. Abbildung 53). Dies ermöglicht eine differenzierte Betrachtung der Fehlerursachen hinsichtlich der Eintrittswahrscheinlichkeit. Demnach müssen gewisse Ereignisse die zu Gefahrenursachen führen gleichzeitig eintreten.

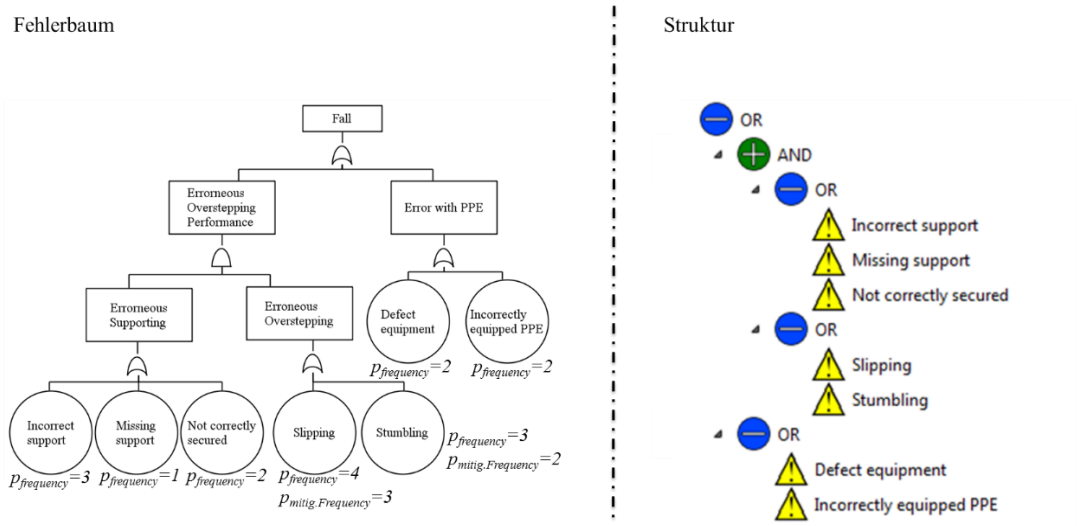


Abbildung 53: Auszug aus der Gesamtdokumentation und dem zugehörigen Fehlerbaum zu der Gefährdung "Sturz" [Pi15]

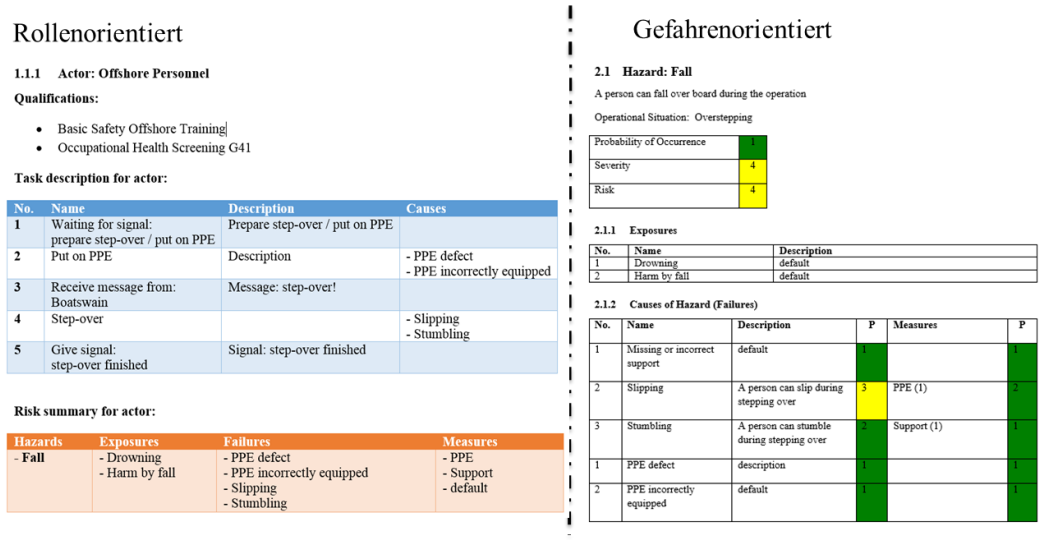
Nach Erstellung aller Gefährdungsstrukturen wird eine automatische Berechnung der Gefahren vorgenommen, welche diese in den Berechnungsvorschriften berücksichtigt. Die Berechnung des Risikos ergibt sich dabei aus der eingeführten Berechnung der Wahrscheinlichkeit des Eintritts multipliziert mit dem Schadensausmaß welches für die Gefahr während der identifizierten Betriebssituation zugeordnet wird. Eingeplante Schutzmaßnahmen werden in diesem Schritt ebenfalls berücksichtigt. Diese wirken sich entweder auf die Eintrittswahrscheinlichkeit oder die Schadensschwere aus. Das Tragen von "Schwimmweste und Helm" (`Mitigation Measure: Lifejacket&Helmet`) verringert dabei die Schadensauswirkungen bei einem Sturz. Auf die gleiche Weise verringern die "High-Grip-Schuhe" (`Counter Measure: High-grip shoes`) das Risiko auszurutschen (`Cause: Slipping`) und wirken sich dadurch positiv aus die Eintrittswahrscheinlichkeit aus.

Erstellung des Sicherheitskonzepts

Wie zu Beginn der Durchführung eingeführt, wurde die Information der vorgegangenen Schritte stets in dem integrierten Modell gespeichert. In dem finalen Schritt werden nun diese

dem Adressaten entsprechend aufbereitet. Je nach Anwendungszweck können diese beispielsweise als Einführung für das Offshore-Personal als Vorbereitung für den Überstieg während der Überfahrt zum Windpark oder aber als Bestandteil des HSE-Konzeptes für die Genehmigungsbehörden oder auch Rückversicherer aufbereitet werden. Abbildung 54 zeigt auf der linken Seite eine mögliche Darstellung für die Rolle "Offshore-Personal". Diese enthält eine tabellarische Erläuterung aller durchzuführenden Schritte und eine Zusammenfassung über mögliche Gefahren und Risiken. Auch weitergehende Informationen die bei der Beschreibung des Systems im Modell hinterlegt wurden, können hier dargestellt werden. So werden hier exemplarisch die notwendigen Qualifikationen für den Akteur aufgelistet.

Rechts dargestellt sind detaillierte Informationen über die Gefahr "Sturz". Neben der Berechnung des Risikos, der entsprechenden Ursachen und entgegenwirkenden Maßnahmen, werden hier ebenfalls mögliche Folgen aufgeführt.



Rollenorientiert

1.1.1 Actor: Offshore Personnel

Qualifications:

- Basic Safety Offshore Training
- Occupational Health Screening G41

Task description for actor:

No.	Name	Description	Causes
1	Waiting for signal: prepare step-over / put on PPE	Prepare step-over / put on PPE	
2	Put on PPE	Description	- PPE defect - PPE incorrectly equipped
3	Receive message from: Boatswain	Message: step-over!	
4	Step-over		- Slipping - Stumbling
5	Give signal: step-over finished	Signal: step-over finished	

Risk summary for actor:

Hazards	Exposures	Failures	Measures
- **Fall**	- Drowning - Harm by fall	- PPE defect - PPE incorrectly equipped - Slipping - Stumbling	- PPE - Support - default

Gefahrenorientiert

2.1 Hazard: Fall

A person can fall over board during the operation

Operational Situation: Overstepping

Probability of Occurrence	1
Severity	4
Risk	4

2.1.1 Exposures

No.	Name	Description
1	Drowning	default
2	Harm by fall	default

2.1.2 Causes of Hazard (Failures)

No.	Name	Description	P	Measures	P
1	Missing or incorrect support	default	1		1
2	Slipping	A person can slip during stepping over	3	PPE (1)	2
3	Stumbling	A person can stumble during stepping over	2	Support (1)	1
1	PPE defect	description	1		1
2	PPE incorrectly equipped	default	1		1

Abbildung 54: Exemplarische Ausgabe des Sicherheitskonzeptes

4.1.2 Validierung durch Experten

Das Ergebnis der prozessorientierten Systemmodellierung mit anschließender quantitativen Risikoanalyse und Risikobewertung in der zweiten Phase wird mit Domänen-Experten hinsichtlich einer Nutzwertanalyse überprüft. Auf diese Weise soll die Praxistauglichkeit ermittelt werden. Die qualitative Analysemethode von Zangemeister [Za71] bzw. der Überarbeitung dieser durch Bechmann [Be76] dient der strukturierten Analyse, welche das Ziel hat anhand von Nutzwerten eine Rangfolge von Handlungsalternativen zu erstellen. In diesem Fall wurde die in dieser Arbeit vorgestellte modellbasierte Methodik mit den Techniken der Domänen-Experten evaluiert. Die Nutzwerte ergeben sich aus dem Produkt von Zielerfüllungsfaktoren und Gewichtungsfaktoren, die von den verschiedenen Experten bewertet wurde. Die Methode

mit dem größten Gesamtnutzwert entspricht dabei am besten den definierten Kriterien. Die Bewertungskriterien setzen sich aus Qualitätsmerkmalen von Software und einer Auswertung eines Fragebogens, in dem HSE-Experten das aktuelle Vorgehen in den ihren Unternehmen schildern, zusammen. Die Gewichtung der Kriterien wurde von verschiedenen Experten, die sich in ihrer täglichen Arbeit mit der Erstellung von Gefährdungsbeurteilungen in der maritimen Domäne beschäftigen, vorgenommen. Ein entscheidender Auswahlfaktor für die Experten ist ebenfalls der inhaltliche Bezug zu dem Fallbeispiel "Personentransfer". Die Durchführung der Evaluation erfolgt in drei Schritten (vgl. Abbildung 55):

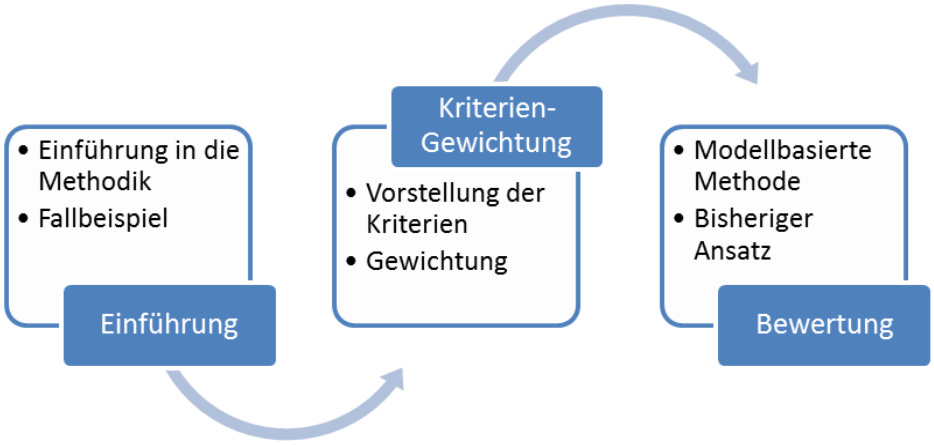


Abbildung 55: Drei Phasen der Evaluation durch Domänen-Experten

Einführung

In persönlichen Gesprächen wurde zunächst die modellbasierte Methodik mittels Präsentation eingeführt. Dabei wurde von den Experten das jeweilige bisherige Vorgehen innerhalb der Firma zu den einzelnen Schritten dargestellt. Anschließend wurde anhand der prototypischen Umsetzung die konkrete Anwendung der "neuen" Methodik demonstriert. Für ein besseres Verständnis ist dabei das Fallbeispiel "Personentransfer" unternehmensspezifisch angepasst. Dafür stellten die Experten die vorhandenen Dokumentationen aus deren Häusern vorab bereit. Dies führte nicht nur zu einem besseren Kontextverständnis, sondern diente vor allem der Vergleichbarkeit der Ergebnisse beider Ansätze.

Kriterien-Gewichtung

Zu Beginn der zweiten Phase der Evaluation ist zunächst das Verständnis über die zwölf Kriterien hinsichtlich der Praxistauglichkeitsbewertung aufgebaut worden. Dies geschah neben der Bereitstellung einer schriftlichen Erläuterung mittels Dialog, um alle Unklarheiten, wie z.B. die Abgrenzung zusammenhängender Kriterien, zu beseitigen. Nachfolgend wurde von den Experten die individuelle Gewichtung dieser Bewertungskriterien durchgeführt. Im Folgenden werden die zwölf Kriterien kurz dargestellt.

- *Aktualität:* Damit ein vollständiger und richtiger HSE-Plan erstellt werden kann, müssen die Daten, die dem HSE-Experten vorliegen, aktuell sein. Mit diesem Kriterium soll identifiziert werden, ob die Methoden dabei unterstützen die Aktualität der Daten und somit des HSE-Plans zu gewährleisten.
- *Benutzbarkeit:* Das Qualitätsmerkmal Benutzbarkeit bzw. Usability beschreibt den Aufwand, den ein Benutzer betreiben muss, um ein Softwareprodukt bedienen zu können. Ist das System leicht erlern- und bedienbar, so ist der Aufwand für Schulungen gering und das Produkt weist eine hohe Benutzbarkeit auf. [Wa01], [BVW07], [Ho08]
- *Darstellung:* Mit diesem Kriterium soll identifiziert werden, welche Möglichkeiten der Darstellung die beiden Methoden zulassen und worin sie sich unterscheiden. Dabei soll zum einen darauf eingegangen werden, ob eine textuelle und/oder eine grafische Darstellung ermöglicht werden und mit welcher Genauigkeit die Darstellung erfolgen kann.
- *Detailgenauigkeit:* Mit der Bewertung dieses Kriteriums soll identifiziert werden, ob und inwieweit die Methoden eine Variation in der Detailgenauigkeit unterstützen. Für die Praxistauglichkeit kann dies von Bedeutung sein, da Experten geschildert haben, dass es sich aufgrund der Komplexität des HSE-Plans anbietet, die Genauigkeit der Details zu variieren. Für die Vorlage als Genehmigungsdokument ist ein detaillierter Plan mit allen Prozessanweisungen sinnvoll. Für erfahrene Techniker und Mitarbeiter ist vielmehr eine Darstellung des groben Prozessablaufes als Übersicht von Wichtigkeit.
- *Eindeutigkeit*: Anhand des Kriteriums Eindeutigkeit soll festgestellt werden, ob die Verwendung der Methoden im Unternehmen zu einer erhöhten Eindeutigkeit führen kann oder nicht. Eine höhere Eindeutigkeit führt zu einem einheitlichen Verständnis, z.B. von Begrifflichkeiten oder Normen und somit zu einer erleichterten Kommunikation. Es soll hierbei auch festgestellt werden, ob eine erhöhte Eindeutigkeit überhaupt notwendig ist, da sie möglicherweise bereits existiert.
- *Flexibilität:* Mit dem Kriterium Flexibilität soll geprüft werden, ob die Methoden die Möglichkeit bieten flexibel auf veränderte Anforderungen zu reagieren oder dies nur schwer ermöglichen. Bei den HSE-Projekten kommt es immer wieder vor, dass sich Parameter, z.B. aus Kundensicht oder auch Umweltbedingungen, ändern. Einige Teile des HSE-Plans und auch die Risikobewertung müssen möglicherweise abgeändert werden. Je nachdem wie flexibel eine Methode ist, desto weniger Aufwand können die Änderungen für den HSE-Experten bedeuten.
- *Manueller Aufwand:* Mit Hilfe dieses Kriteriums soll herausgearbeitet werden, wie groß der Aufwand bei der jeweiligen Methode eingeschätzt wird, um einen HSE-

Plan zu erstellen. Je höher der manuelle Aufwand ist desto unkomfortabler ist die Erstellung für den HSE-Experten.

- *Schnittstellen:* Mithilfe von Schnittstellen kann ein Datenaustausch stattfinden, wobei zwischen Softwareschnittstellen, Datenbankschnittstellen, Hardwareschnittstellen, sowie Benutzerschnittstellen unterschieden wird.
- *Sprache:* Anhand des Kriteriums der Sprache soll identifiziert werden, inwieweit die beiden Methoden praxistauglich sind, indem herausgearbeitet wird, welche Sprachen von Bedeutung sind und warum.
- *Transparenz:* Ein HSE-Plan ist häufig ein komplexes Konstrukt und wird zum Teil von mehreren Experten erstellt. Für die Genehmigung eines Offshore-Windparks muss dieser detailliert vom BSH geprüft werden. Anhand dieses Kriteriums der Transparenz soll eingeordnet werden, inwieweit die Methoden die Möglichkeit bieten, den HSE-Plan nachvollziehbar zu gestalten.
- *Übertragbarkeit:* Weist ein Softwareprodukt eine hohe Übertragbarkeit bzw. Portabilität auf, so ist der Aufwand gering es in eine andere Hardware- oder Betriebssystemumgebung zu übertragen und zu integrieren. Dieses Qualitätsmerkmal beschreibt somit den Grad der Plattformunabhängigkeit eines Softwareprodukts. Mi Hilfe der Teilmerkmale Anpassbarkeit und Installierbarkeit wird dies noch einmal verdeutlicht. [Wa01], [BVW07], [Ho08]
- *Wiederverwendbarkeit:* Von einer Wiederverwendbarkeit kann gesprochen werden, wenn eine Methode bzw. ein Tool die Generierung von Modellen und Datenstrukturen unterstützt, die in anderen Anwendungen wiederverwendet werden können [WJ05]. In dem hier vorliegenden Kontext sollen anhand des Kriteriums Wiederverwendbarkeit die Methoden und Tools dahingehend untersucht werden, inwieweit sie geeignet sind, Teile der HSE-Pläne wiederzuverwenden.

Tabelle 3 zeigt das Ergebnis der Erhebung der Gewichtungsfaktoren durch die Sicherheitsexperten, geordnet nach der errechneten Bedeutung (je höher die Zahl, desto bedeutender das Kriterium). Hierfür ordnete jeder Experte die jeweiligen Kriterien in eine Rangliste ein, wobei das wichtigste Kriterium mit einer 12, das Unwichtigste mit einer 1 bewertet wurde.

Kriterium / Experte	Nr. 1	Nr.2	Nr. 3	Nr. 4	Nr. 5	G_i
Aktualität	9	11	10	10	8	12
Transparenz	5	10	7	6	12	10
Manueller Aufwand	11	6	9	1	10	9
Detailgenauigkeit	3	8	5	9	11	9
Wiederverwendbarkeit	10	2	12	8	3	9
Darstellung	12	7	4	4	5	8
Flexibilität	4	5	11	3	7	8
Eindeutigkeit	8	12	1	2	6	7
Sprache	6	4	6	11	2	7
Benutzbarkeit	2	9	3	5	9	7
Schnittstellen	1	1	8	12	1	6
Übertragbarkeit	7	3	2	7	4	6

Tabelle 3: Ergebnis der Erhebung der Gewichtungsfaktoren durch Domänen-Experten

Der Gewichtungsfaktor G_i berechnet sich anschließend aus dem Durchschnitt im Verhältnis zu der Summe aller Ziffern ($\sum_{12}^{1} G_i = 78$). Der Tabelle zu entnehmen ist, dass die Aktualität (12) und Transparenz (10) nach Gewichtung der Sicherheitsexperten die größte Bedeutung zugeordnet wird. Dem folgen der manuelle Aufwand, die Detailgenauigkeit und die Wiederverwendbarkeit (jeweils 9).

Bewertung

In der Bewertungs-Phase wird mittels der Nutzwertanalyse beurteilt, wie weit die beiden Ansätze der bisher im Unternehmen angewandte und der vorgestellte modellbasierte Ansatz, die jeweiligen Kriterien erfüllen. Bei dieser werden sowohl neben einer Bewertung in Form eines Zielerfüllungsfaktors ebenfalls Informationen aus den persönlichen Gesprächen mit berücksichtigt. Der Zielerfüllungsfaktor drückt eine subjektive Punktzahl aus, die aussagt, in wie weit der jeweilige Ansatz einem Kriterium erfüllt (vgl. Tabelle 4)

Erfüllung des Kriteriums	Zielerfüllungsfaktor
Nicht erfüllt	0
Ausreichend	1
Befriedigend	2
Gut	3
Sehr gut	4
Überragend	5

Tabelle 4: Übersicht über die Zielerfüllungsfaktoren und deren Bedeutung

Nach der Ermittlung der Zielerfüllungsfaktoren für das jeweilige Kriterium konnte über die Berechnung der Teilnutzwerte der abschließende Gesamtnutzwert für beide Alternativen berechnet werden. Dafür wurde das Produkt aus Gewichtungs- mit Zielerfüllungsfaktor über alle Kriterien hin aufsummiert. Abbildung 56 zeigt die errechneten Gesamtnutzwerte beider Ansätze und deren prozentuale Abweichung (sortiert nach Bedeutung der Kriterien).

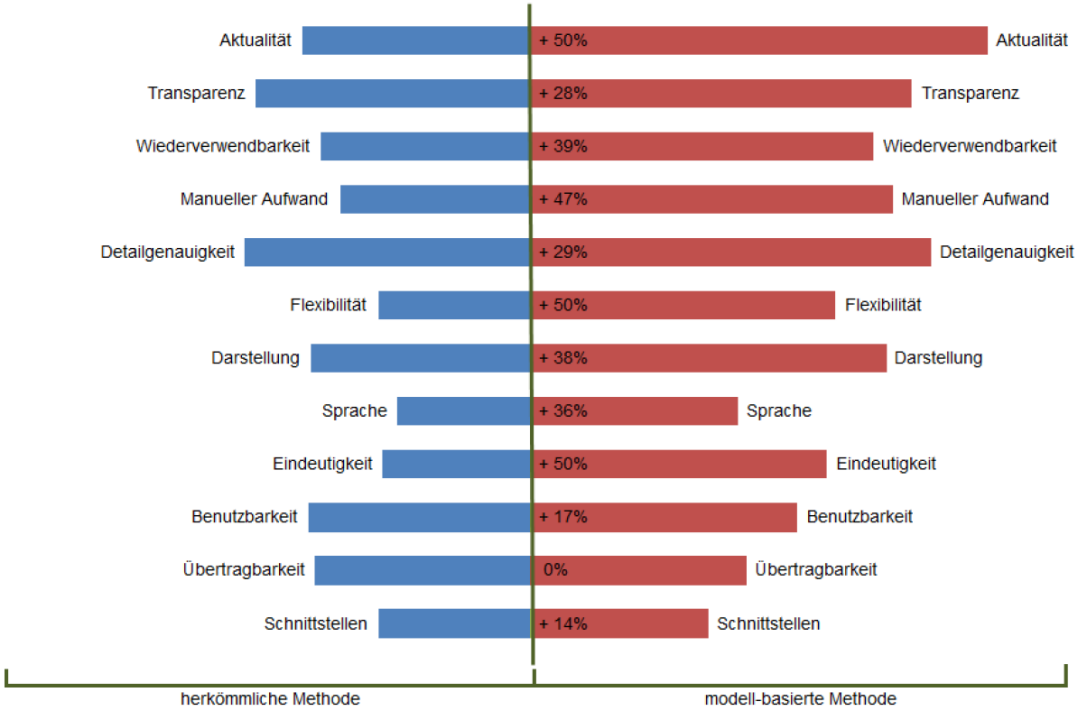


Abbildung 56: Gesamtnutzwerte beider Methoden und deren prozentuale Abweichung

Wie der Auswertung zu entnehmen ist, wird das von den Experten als wichtigstes eingeschätzte Kriterium, nämlich die ***Aktualität***, für die in dieser Arbeit vorgestellten Methode im Vergleich zum herkömmlichen Vorgehen in der Praxis doppelt so gut bewertet.. Interessant dabei ist, dass in den persönlichen Gesprächen mit den Experten deutlich geworden ist, dass die Aktualität selbst von dem Nutzer und nicht der Methode selbst abhängt. Dies beruht wahrscheinlich auf einer Annahme, dass sich Pläne mit der modellbasierte Methode einfacher aktualisieren lassen. Hinsichtlich der Wichtigkeit folgt nach der Aktualität die ***Transparenz***. Hier wurde ebenfalls die neue Methode durchgängig besser eingeschätzt. Es ist von den Experten besonders die Nachvollziehbarkeit von Risiken hinsichtlich deren Verortung im Ablauf und damit einhergehend deren Strukturierung als Begründung genannt worden. Dies unterstütze zudem kollaborative Arbeiten an Sicherheitskonzepten, eine Auswirkung auf die Bewertung der Risiken wurde jedoch nicht identifiziert. Auch in Bezug auf die ***Wiederverwendbarkeit***, eines der drittwichtigsten Kriterien, wird die modellbasierte Methode höher bewertet, wobei hier mit knapp 40 Prozent Vorsprung wieder ein deutlicher Abstand zu erkennen ist. Dies ist besonders durch die Auswirkungen der Wiederverwendbarkeit auf den ***manuellen Aufwand***

begründet. Auch in diesem Punkt konnte die modellbasierte Methode die Experten überzeugen. Hervorgehoben wurde hier die Funktionalität des Prozessmodells, trotz des initial höheren Aufwandes, d.h. Einarbeitung in die Methode und Tools. Die Bewertung der ***Detailgenauigkeit*** ist dagegen bei beiden Methoden ähnlich, sodass sich die modellbasierte nur um rund 30 Prozent von der herkömmlichen Methode abhebt. Dies liegt vermutlich daran, dass, ähnlich wie bei der Aktualität, noch immer der Experte maßgeblich für die Detailtiefe ist und nicht die verwendete Methode. Für die fünf Kriterien, die relativ wichtig für die praktische Anwendung sind, lässt sich deshalb sagen, dass die modellbasierte Methode besser bewertet wird, außer in Bezug auf die Transparenz und die Detailgenauigkeit. Hervorzuheben bei den weiteren Kriterien ist die Bewertung der ***Eindeutigkeit***. In den persönlichen Gesprächen ist der Eindruck entstanden, dass Eindeutigkeit für die Unternehmen wichtig ist, in der Einordnung der Wichtigkeit spiegelt sich dies jedoch nicht wieder. Die modellbasierte Methode wird genau wie bei Aktualität und Flexibilität um 50 Prozent besser bewertet.

4.1.3 Zusammenfassung

Das Anwendungsbeispiel "Personentransfer" wurde in Kooperation mit verschiedenen maritimen Unternehmen durchgeführt und evaluiert. Die Expertengruppe setzte sich zusammen aus Spezialisten für die Durchführung von Operationen wie beispielsweise ein Personentransfer und Experten für die Erstellung und Evaluierung von HSE-Plänen. Die Durchführung der Evaluation erfolgte in zwei Phasen. Zunächst ist im ersten Schritt die prozessorientierten Systembeschreibung hinsichtlich Gefahren und Ursachen annotiert und anschließend das Verfahrens der prozessorientierten, quantitativen Risikoanalyse und –Bewertung nach Pinkowski [Pi15] angewandt worden. Das ganzheitliche Ergebnis wurde in der zweiten Phase mit Domänen-Experten hinsichtlich der Praxistauglichkeit mittels einer Nutzwertanalyse überprüft. Dazu wurde zunächst ein Kriterienkatalog mit zwölf Kriterien entwickelt. Diese setzen sich zusammen aus Qualitätsmerkmalen von Software und einer Auswertung eines Fragebogens in dem HSE-Experten das aktuelle Vorgehen in ihren Unternehmen schildern. Insgesamt lässt sich feststellen, dass die modellbasierte Methode bei den wichtigen Kriterien (Aktualität, Manueller Aufwand, Flexibilität) deutlich besser abgeschnitten hat als die herkömmliche Methode. Je unwichtiger ein Kriterium von den Experten eingeschätzt wurde, desto indifferenter ist die Bewertung ausgefallen. Eine Ausnahme ist die Eindeutigkeit, die trotz geringer Wichtigkeit eine Abweichung von 50 Prozent aufweist.

Zusammenfassend kann durch die zweistufige Evaluierung die Fragestellung, ob sich das prozessorientierte Planungsmodell für die Durchführung einer quantitativen Risikoanalyse und -Bewertung maritimer Operationen eignet, positiv beantwortet werden.

4.2 Fallbeispiel "Ladungsversatz"

Zur Vervollständigung der Evaluation der modellbasierten Methodik wird diese in einem weiteren Fallbeispiel, dem "Ladungsversatz", mit Fokus auf die simulationsbasierte Analyse untersucht. Kranarbeiten auf See sind stets verbunden mit Gefahren für Mensch und Technik. Wind, Seeschlag, Nässe, Bewuchs und Sonneneinstrahlung bedrohen zu jeder Zeit technische Einrichtungen. Nicht nur bei der Errichtung der Anlagen, sondern auch bei Wartung ist vor Ort unter schwierigen Bedingungen zu arbeiten. Das in dem Fallbeispiel betrachtete Szenario "Ladungsversatz", dessen primärer Ablauf Kranarbeiten auf See beinhaltet, ist ein wiederkehrender und häufig beim Aufbau und bei Wartungsarbeiten stattfindender Arbeitsschritt. Durch die Vielzahl der Risiken und ihre hohe Kombinationsmöglichkeit wird das Wartungspersonal vor sich ständig wechselnde Aufgaben gestellt. Offshore-Operationen, wie die im Szenario skizzierte Errichtung und Wartung von Windkraftanlagen, tragen somit ein erhebliches Sicherheitsrisiko in sich. Die Fragestellung für die Evaluation am Beispiel "Ladungsversatz" lautet wie folgt:

Eignet sich das prozessorientierte Planungsmodell für die Durchführung einer simulationsbasierten Risikoanalyse und Bewertung maritimer Operationen?

Nach dieser kurzen Einführung in das Fallbeispiel, wird im Detail auf die Durchführung eingegangen. Es wird detailliert die Instanz "Ladungsversatz" des prozessorientierten Planungsmodell eingeführt, bestehend aus dem Prozessmodell der spezifischen Operation, der Inklusion der benutzten Ressourcen und der Einflussfaktoren hinsichtlich verschiedener Betriebssituationen. Der nach der Identifizierung durchgeführten quantitativen Risikobewertung folgt eine simulationsbasierte Analyse und Bewertung. In dieser wird die Strukturierung der Gefahrenbeschreibung untersucht und noch nicht identifizierte Ursachen aufgedeckt. Abgeschlossen wird das Fallbeispiel durch eine Zusammenfassung und einer anschließenden Diskussion.

4.2.1 Durchführung

Beschreibung der Umwelt inklusive Ressourcen

Die Umweltbedingungen, wie das Wetter und der Wellengang, gelten für alle Tätigkeiten der Offshore-Industrie und haben somit ebenfalls einen großen Einfluss auf die durchgeführten Kranarbeiten und der darin involvierten Materialien. Hinsichtlich der Umweltbedingungen sollten folgende Faktoren betrachten werden: Windgeschwindigkeit, Windrichtung, Strömungsstärke/-richtung, Gezeiten, Wassertiefe, durchschnittliche Wellenhöhe, Wellenrichtung, Sichtweite (über Wasser), Temperatur, Sichtverhältnisse (z.B. Nebel, Regen), Sonneneinstrahlung (Sicht blenden) und die Gischt-Bildung. Besonders Windgeschwindigkeit und

Windrichtung wirken sich auf die verschiedensten Verlade-Objekte aus. Neben Containern, werden sowohl einzelne Elemente einer Anlage bis hin zu einem komplett zusammengebauten Rotor versetzt. Dies beding, dass der Ladeoffizier viele Aspekte zu berücksichtigen hat und individuell die passenden Kräne, sowie das geeignete Verlade-Equipment je nach Verlade-Objekt und Umweltbedingungen selektieren muss. Spezifische Faktoren sind dabei das Gewicht und die Verankerungsmöglichkeiten der Ladung, deren Gewichtsverteilung, Windangriffsfläche und Dichte.

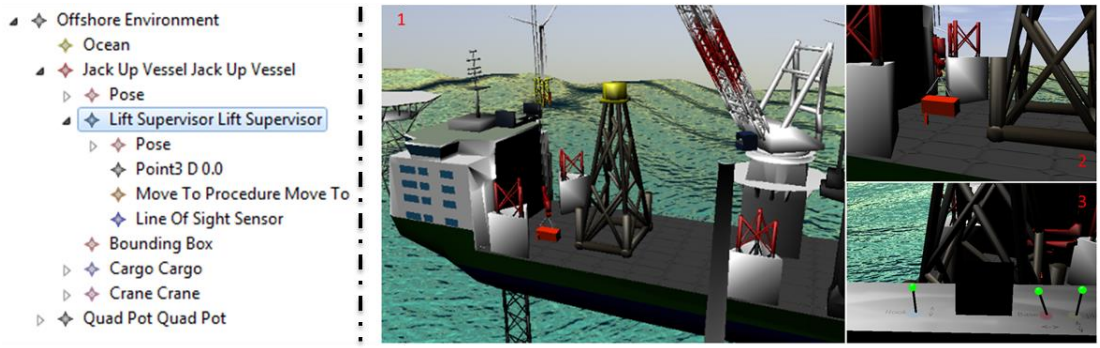


Abbildung 57: Beschreibung der Umwelt inklusive Ressourcen für das Fallbeispiel "Ladungsversatz"

Das Verlade-Equipment dient der Befestigung mit dem Kranhaken. Neben einfachen Schlaufen, oder Ketten kommen aber auch Stahl-Konstrukte, die um das Objekt gebaut, sind zum Einsatz. Das Equipment ist unbedingt mittels Checklisten zu überprüfen. Die Richtseile dienen den Assistenzkräften zur Stabilisierung der Ladung. Mit diesen kann das Objekt geringfügig manövriert und im Gleichgewicht gehalten werden. Die in der Operation involvierten Kräne müssen zwingend vor der Operation auf ihre Funktionstüchtigkeit und Sicherheit hinsichtlich des konkreten Anwendungszweckes überprüft werden. Das beinhaltet ebenfalls Art und Aufbau des Krans, bei dem folgende Komponenten und Eigenschaften relevant sind: Basis, Motor, evtl. drehbarer Kopf, Führerhaus, Hydraulikarm, Winde, Kette, Haken, evtl. Gegengewicht, max. Reichweite, max. Hubgewicht, Assistenzsysteme (Sensoren Wind/Bewegung, Closed circuit television system – Kameraunterstützung) und Kommunikationsmittel.

Auch die Kommunikation der Assistenzkräften und des Ladeoffiziers sind essenziele Bestandteile und Risikofaktoren in diesem Szenario. Daher sollte auch diese vor Operation ausführlich getestet werden. Ein Ausfall der Kommunikation während der Operation bedingt eine Unterbrechung dieser, bis eine alternative Kommunikationsmöglichkeit eingerichtet worden ist. Alle Personen dieses Szenarios sollten permanent miteinander in Kontakt stehen. Wie bei dem Personentransfer-Szenario gibt es auch hier drei unterschiedliche Arten der Kommunikation: Funk (VHF/UHF), Schiffstelefon, Mobil-Netz, Satelliten-Telefon, Handsignale, Lichtsignale, Pfeifsignale.

Erstellung des Prozessmodells

Die Steuerung des Krans erfolgt durch den Kranfahrer auf konkrete Anweisung des Ladeoffiziers. Bei seiner Arbeit wird er dabei von verschiedenen Assistenzsystemen unterstützt. Der Ladeoffizier ist verantwortlich für diese Operation und deswegen auch die befehlshabende Person in diesem Szenario. Neben dem Kranführer folgen auch die Assistenzkräfte seinen Anweisungen. Er ist somit Hauptverantwortlicher für den gesamten Ladungsversatz, trifft Entscheidungen und führt Kommunikation mit allen beteiligten Personen. Das Assistenzpersonal ist für das Befestigen des Hakens am Verlade-Objekt, sowie für das Stabilisieren mittels Richtleinen zuständig. Vor Beginn des Ladungsversatzes müssen alle Beteiligten Personen, wie Kranführer, Ladeoffizier, Anschläger, Kapitän, etc., in die Operation eingewiesen werden. Anschließend werden die erforderlichen Checklisten von den jeweilig verantwortlichen Personen durchgeführt. Dies schließt die Überprüfung des Kranes (`PhysicalObject: Crane`), der Kommunikationsmittel, des Verlade-Equipments, der Ladung und der Umweltbedingungen des Zielortes. Wie Abbildung 58 zu entnehmen ist übernimmt der Ladeoffizier (`Actor: Lift Supervisor`) während des gesamten Vorganges die Verantwortung. Sind die Checklisten erfolgreich durchgeführt worden und lassen die Windverhältnisse (es zu, kann die Verladung beginnen. Dafür werden entsprechend der Ladung (`PhysicalObject: Cargo`) zunächst Einstellungen (z.B. Kraneinstellungen) vom Kranführer (`Actor: Crane Operator`) vorgenommen.

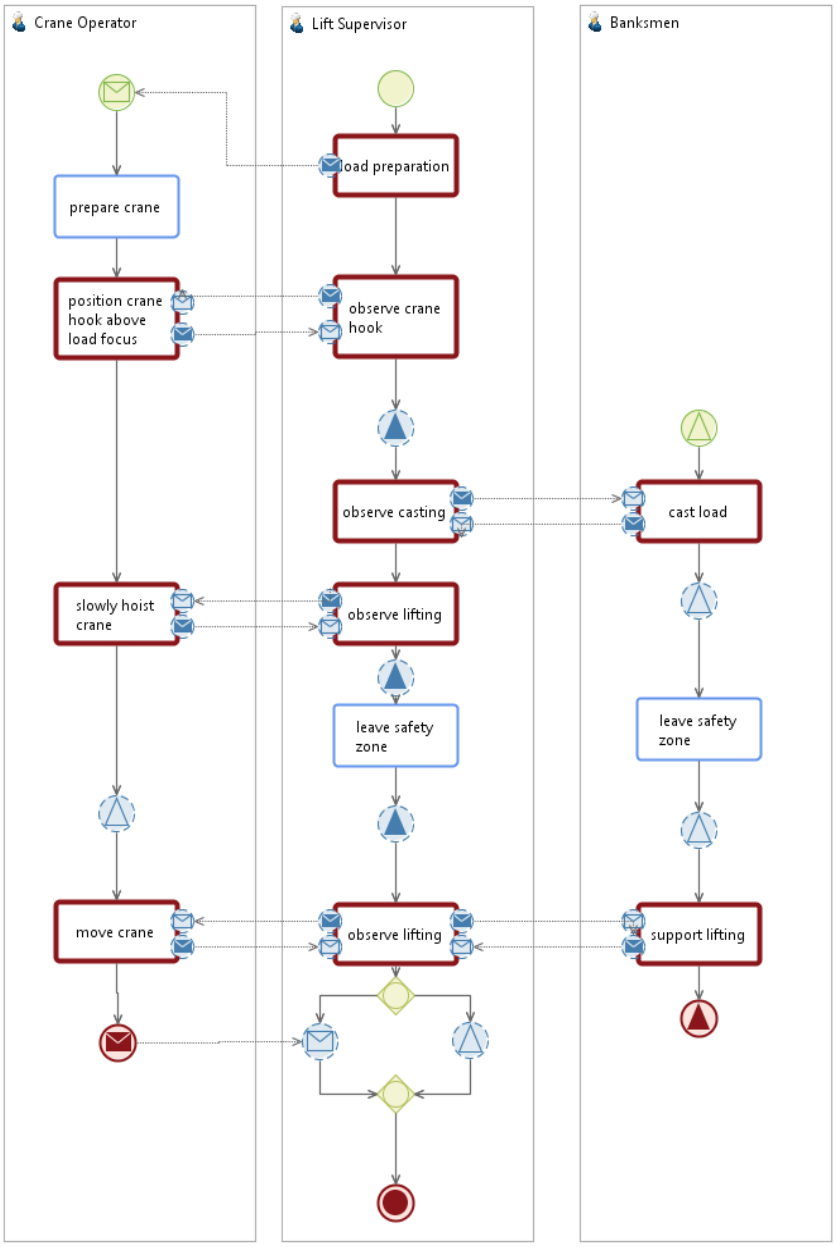


Abbildung 58: Anwendungsszenario "Ladungsversatz"

Anschließend fährt der Kranführer, entsprechend den Anweisungen des Ladeoffiziers, den Kran an eine geeignete Position. Diese kann je nach Umgebung und Art des zu verladenden Objekts unterschiedlich sein. Befinden sich die Kräne in entsprechender Position, müssen diese evtl. noch zusätzlich verankert bzw. stabilisiert werden. Anschließend wird vom Kranführer, wie vorgesehen, der Ausleger über das zu verladende Objekt gesteuert und der Haken herabgelassen. Nun befestigen die Anschläger unter Aufsicht des Ladeoffiziers die Ladung am Kranhaken. Dabei kommt spezielles Verlade-Equipment, sogenannte Anschlagmittel, zum Einsatz, welche für das Material geeignet ist. Manche Ladungen besitzen Ladevorrichtungen (z.B. Ösen), andere müssen mit Ketten und Gurten umschlungen und an den Haken befestigt

werden. Flügel für Windenergieanlagen sind an bestimmten Stellen mit für den Transport vorgesehenen Stahl-Konstrukten versehen, an denen die Haken befestigt werden können. Ist die Ladung angeschlagen und vom Ladeoffizier überprüft worden, gibt dieser das Signal an den Kranführer. Für das nun folgende Manöver ist eine gute Kommunikation zwischen den beteiligten Personen sehr wichtig. Der Ladeoffizier muss dem Kranführer die richtige Anweisung geben, damit die Ladung gleichmäßig und sicher angehoben werden kann. Auch die Anschläger (`Actor: Banksmen`), die die schwebende Ladung von unten mit Richtseilen ausrichten, müssen vom Ladeoffizier die richtigen Kommandos erhalten. Geschehen dabei Fehler oder versteht ein Teilnehmer die Anweisung des Aufsehers nicht richtig, muss dieser sofort Alarm geben. Der Hebe-Vorgang wird daraufhin unterbrochen und die letzten Anweisungen werden wiederholt.

Nachdem die Abnahme des Ladeoffiziers bezüglich der Anschlagmittel positiv verlaufen ist, kann mit der Operation fortgefahren werden. Um sicherzustellen, dass die Ladung ordnungsgemäß angeschlagen ist und der Haken sich mittig über der Ladung befindet, wird zunächst vom Kranführer verlangt auf Vorspann zu gehen. Dieser Schritt ist wichtig, da bei falschem Anschlagen bzw. bei einem existierenden Versatz zwischen Haken und Ladung, die Ladung nach Anheben ins Schwingen geraten kann. Ist auch dieser Vorgang erfolgreich absolviert und haben Ladeoffizier und Anschläger die Sicherheitszone verlassen, beginnt die eigentliche Versetzung. Während des Schwenkens halten die Assistenzkräfte das Objekt mit ihren Richtseilen in ausgeglichener Position. In diesem Teil der Operation ist es grundsätzlich zu vermeiden, dass sich Personen direkt unter der schwebenden Last befinden. Erreicht die Ladung die Zielposition, lässt der Kranführer unter den Anweisungen des Ladeoffiziers die Ladung langsam ab. Assistenzkräfte unterstützen dabei wieder mit Richtseilen und helfen dabei das Objekt korrekt abzustellen.

Identifikation von Gefährdungen und quantitative Risikoanalyse und –Bewertung

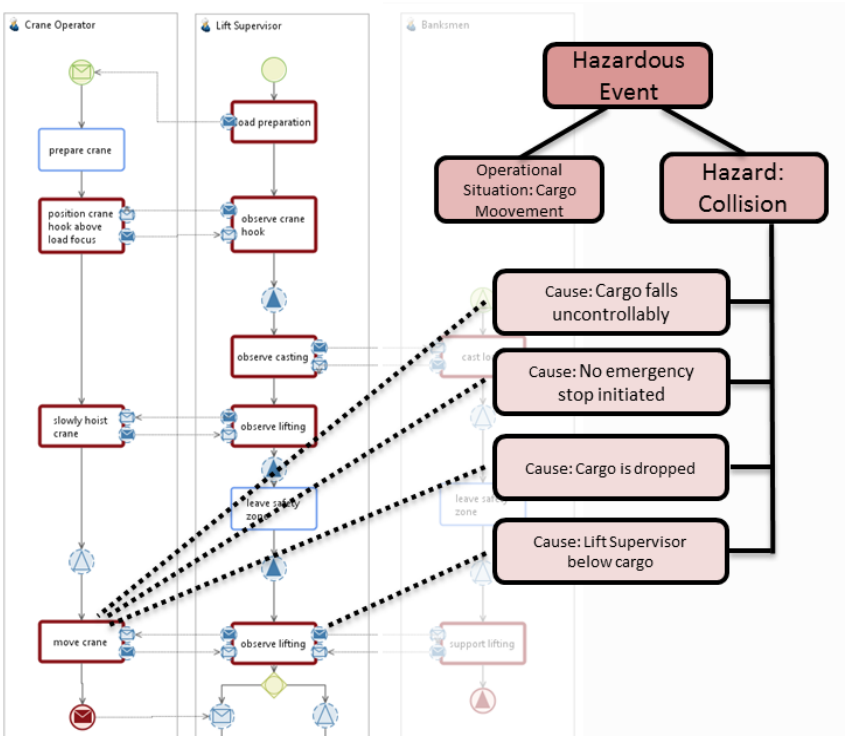


Abbildung 59: Identifizierung von Gefahren und Ursachen und deren Verortung im Prozess

Abbildung 59 zeigt exemplarisch die Identifizierung der Gefahr "Kollision" (`Hazard: Collision`) und die Betriebssituation "Ladungsversatz" (`Operational Situation: Cargo Movement`). Die möglichen Gefahren und Ursachen werden innerhalb der Prozessbeschreibung ergänzt. Innerhalb des Subprozesses "bewege Kran" (`Sub Process: move crane`) werden dabei drei mögliche Ursachen für eine Kollision verortet:

- "Unkontrollierbarer Sturz der Ladung" (`Cause: Cargo falls uncontrollably`)
- "Not-Aus nicht betätigt" (`Cause: No emergency stop initiated`)
- "Ladung ist gestützt" (`Cause: Cargo is dropped`)

Zudem wird bei dem Sub-Prozess "Ladung beobachten" die mögliche Fehlerursache "Ladeoffizier befindet sich unterhalb der Ladung" (`Cause: Lift Supervisor below cargo`) identifiziert. Die quantitative Risikoanalyse und -bewertung erfolgt wie im vorhergehenden Fallbeispiels "Personentransfer" mittels der Methode von Pinkowski [Pi15]. Das Ergebnis der Strukturierung bzw. die daraus entstehenden Fehlerbäume sind ein wesentlicher Input für die simulationsbasierte Analyse.

Simulationsbasierten Risikoanalyse und Bewertung

Um eventuell noch nicht betrachtete Ursachen für Gefahren zu identifizierte bzw. die Struktur der Gefahren zu überprüfen, wird die simulationsbasierte Analysemethode von Gollücke angewandt. In einem ersten Schritt werden hierfür zunächst eine Parameter Exploration und die notwendigen Simulatoren generiert. Diese beschreiben verschiedene Abläufe von Simulationsgängen, dabei wird auf die in den ersten beiden Schritten entstandene Modell-Instanz des Szenarios zurückgegriffen. Aus der Analyse des Prozessmodells ergeben sich die Simulator-Instanzen für die Ausführung der Agenten, um das Verhalten der Beteiligten Akteure zu übernehmen. Ein Simulator repräsentiert das Verhalten des Ladeoffiziers, wie beispielsweise die Bewegung dessen auf dem Schiffsdeck. Hierfür werden für die Ausführung des Subprozesses "Ladung beobachten" (`SubProcess: observe lifting`) verschiedene Beobachtungspfade errechnet, welche eine freie Sicht auf die Ladung und den Kranführer gewährleisten. Währen der Simulation wählt der Agent abhängig eines vorgegebenen Wahrscheinlichkeitswertes einen spezifischen Pfad. Durch einen weiteren Simulator werden Umwelteinflüsse und die Kranbewegungen berücksichtigt. Dort werden physikalische Effekte, wie zum Beispiel, die Kollision von Objekten oder Soft Body Effekte, wie das Schwingen des Kranseils, simuliert. Umwelteinflüsse sind Partikeleffekte wie Regen oder Schnee. Die Simulationskomponente bietet zusätzlich eine integrierte Visualisierung, welche für Testzwecke oder eine manuelle Beobachtung genutzt werden kann. Währen der Ausführung der verschiedenen Simulationsläufe wird durch eine weitere Komponente das Auftreten von Gefahren und Ursachen beobachtet. Das Ergebnis der simulationsbasierten Analyse sind Ursachen die zu einer Gefahr geführt haben, welche im initialen manuellen Identifizierungsschritte nicht berücksichtigt wurden.

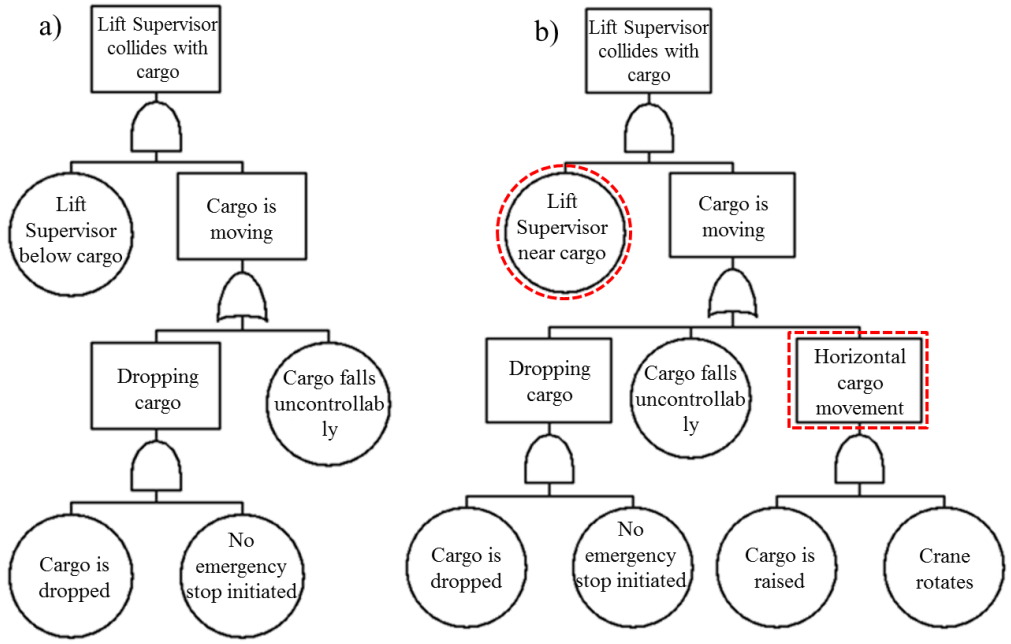


Abbildung 60: Fehlerbäume des Verladeszenarios. a) vor b) nach der simulationsbasierten Analyse

In Abbildung 60 wird das Ergebnis der Fehlerbaumstruktur vor der Analyse (a) und nach der simulationsbasierten Analyse (b) dargestellt. Eine neue Erkenntnis ist hierbei, dass die Gefahr nicht nur eintritt, wenn sich der Ladeoffizier unterhalb der Ladung, sondern auch wenn er sich in der Nähe befindet (`Cause: Lift Supervisor near cargo`). Des Weiteren wurde erkannt, dass eine Rotation des Krans (`Cause: Horizontal cargo movement`) während des Anhebens der Ladung ebenfalls zu einer möglichen Kollision führt.

4.2.2 Zusammenfassung

Im Fallbeispiel "Ladungsversatz" wurde die Systembeschreibung erstellt, das Verhalten mittels Prozessbeschreibung ergänzt und anschließend um potenzielle Gefahrenbeschreibungen erweitert. Dem folgte ebenfalls das Verfahren der prozessorientierten, quantitativen Risikoanalyse und –Bewertung nach Pinkowski [Pi15]. Demnach wurde auch in diesem Fallbeispiel die generelle Anwendbarkeit der Methodik demonstriert. Der eigentliche Fokus folgte im Anschluss, indem demonstriert wurde, dass sich die Modellbeschreibung eignet, um die bis zu diesem Punkt entstandene, quantitative Bewertung, durch eine qualitative, simulationsbasierte Analyse zu erweitern. Es konnte durch die Anwendung des Konzeptes und der Werkzeuge nach Gollücke [Go16] die Ausführbarkeit demonstriert werden. In diesem erfolgte zunächst eine statische Auswertung des Prozessverhaltens und der Gefahrenbeschreibung. Darauf aufbauend sind verschiedene Simulationspläne entstanden, durch dessen Ausführung nebst neuen Ursachen für Gefahren überarbeitete Fehlerbaumkonstruktionen identifiziert werden konnten.

Eine simulationsbasierte Analyse auf Basis des Planungsmodells wurde demonstriert, weshalb die auch in diesem Fallbeispiel die eingehende Hypothese bestätigt wurde.

4.3 Anforderungs- und Zielabdeckung

Um die Praxistauglichkeit der Methodik zu zeigen, wurde das erste Fallbeispiel "Personentransfer" zusätzlich mit einer Expertengruppe evaluiert. In dem zweiten Fallbeispiel wurde demonstriert, dass das Modell ebenfalls durch eine simulationsbasierte Analyse untersucht werden kann, dessen Ergebnis eine qualitative Validierung eines Sicherheitskonzeptes ermöglicht.

Bevor Aussagen über die Zielabdeckung getroffen werden, wird im Folgenden zunächst auf die Anforderungsabdeckung eingegangen.

Prozessorientierte Systembeschreibung

Konzeptionell wurde der Aspekt der Abbildung der in einer Operation eingesetzten Ressourcen im ersten Schritt der entwickelten Methodik "Beschreibung der Umwelt inklusive Ressourcen" verortet. Die formale Beschreibung dieser erfolgt im Umgebungsmodell, durch dessen Semantik die Beschreibung der Elemente eindeutig erfolgt und somit der bisher vorherrschenden Problematik der Nichteindeutigkeit von Begrifflichkeiten entgegengewirkt wird. Als Bestandteil des integrierten Modells und somit der Basis für die Umsetzung des Prototypen wurde unter dessen Verwendung in der Evaluation, gilt die Anforderung **A1** als erfüllt. Vielmehr wurde ebenfalls die Anwendbarkeit des Konzeptes in beiden Fallbeispielen demonstriert. Ebenso wie die Ressourcen, wird das Personal für die Operation im ersten Schritt der Methodik definiert. Auch die sich aus dieser Anforderung ergebenen Modellierungskonstrukte sind Bestandteil des Umgebungsmodells. Die Adressierung und Evaluation dieser Anforderung erfolgten synchron zu der Vorhergegangenen. Demnach gilt auch die Anforderung **A2** als erfüllt. Im zweiten Schritt wurden die Arbeitsschritte durch das Prozessmodell abgebildet. Dabei wurden die einzelnen Handlungsschritte in Form von einzelnen Aktivitäten und Subprozessen modelliert. Der Kontrollfluss auf oberster Ebene beschränkte sich in diesem Fallbeispiel auf eine rein sequentielle Darstellung. Komplexere Verzweigungen und kontextbezogene Kontrollflüsse sind in verschiedenen Subprozessen abgebildet. So wird beispielsweise in dem Subprozess "access situation of weather and currents" des ersten Fallbeispiels Bezug auf die Umweltbedingungen genommen. Nebenläufigkeit bzw. parallele Arbeiten von verschiedenen Akteuren wurden über die Synchronisation durch Nachrichten und Signalen beschrieben. Die Anforderungen **A3** und **A4** gelten demnach als erfüllt.

Gefahrenidentifikation, -analyse und -bewertung

Im dritten Schritt der Durchführung wurden zunächst die Gefahren und deren Ursache identifiziert und der prozessorientierten Systembeschreibung hinzugefügt. Die notwendige Transparenz wurde dabei durch die direkte Verknüpfung der Gefahren und Ursachen und deren Verortung innerhalb des Prozessmodells geschaffen. Für jedes Element wurden dabei die für die spätere Berechnung notwendigen Risikoparameter (Eintrittswahrscheinlichkeit, Schadensschwere und Kontrollierbarkeit) definiert. Zudem sind die verschiedenen Betriebssituationen, welche für die Gefahren relevant sind im Modell hinterlegt. Die Anforderung **A5**, **A6** & **A8** gelten somit als erfüllt. Die Bewertung der Risiken erfolgte in dem Fallbeispiel nach dem Ansatz von Pinkowski [Pi15]. In Abhängigkeit von dem Prozessmodell wurden die Strukturen und somit die Basis für die Berechnung des Risikos erstellt. Dem angeschlossen erfolgte die Bewertung der Risiken mittels Fehlerbaumanalyse. Die Anforderung **A7** gilt somit als erfüllt. Es konnte gezeigt werden, dass für einzelne Arbeitsschritte in Abhängigkeit zu den spezifischen Anforderungen Gefährdungen und deren Ursachen identifiziert wer-den können, um im Anschluss den Experten die Bewertung der Wahrscheinlichkeit des Eintritts einer Gefährdung sowie deren potenzielles Schadensausmaß zu ermöglichen. Basierend auf der prozessorientierten Systembeschreibung und der dort integrierten Risikokonstrukte konnte gezeigt werden, wie unter Verwendung der Co-Simulationsumgebung HAGGIS neue Fehlerkombinationen erzeugt, bzw. vorhandene überprüft werden konnten. Die Ausführbarkeit des Modells wurde somit demonstriert, woraus sich ableiten lässt, dass die Anforderung **A9** adressiert und erfüllt wurde.

Toolgestützte Methodik

Die Darstellung der Abläufe in der toolgestützten Methode wurde mittels eines graphischen Prozessmodells umgesetzt. Grundsätzlich wurde die Visualisierung zwar von den Experten dieser Aspekt bezogen auf die Gesamtheit aller Aspekte der modellbasierten Methode als weniger wichtig eingeordnet, jedoch im Vergleich zu dem klassisch textuellen oder tabellarischen Vorgehen besser bewertet. Wird das Kriterium der Darstellung jedoch im Kontext der automatischen Erstellung des Sicherheitskonzepts betrachtet, erschließt sich der erst eigentliche Mehrwert. Die Visualisierung unterstützt die sonst nur textuell verfassten Arbeitsanweisungen. So werden neben dem Gesamtüberblick über die relevanten Tätigkeiten auch die Kommunikationspunkte mit anderen Akteuren aufgezeigt. Die Anforderung **A10** gilt daher als erfüllt. Die Basis, sowohl für die die prozessorientierte Systembeschreibung, die Gefahrenidentifikation, -analyse und -bewertung, als auch für das daraus resultierende Sicherheitskonzeptes bildet die formale Abbildung aller relevanten Aspekte in dem hier entwickeltem Modell und der mit diesem eingehenden Vorteile, wie z.B. der Wiederverwendbarkeit einzelner Modellierungskonstrukte und der flexiblen Detailgenauigkeit. Da die gesamte Umsetzung von MO-PhisTo auf dem integrierten Modell basiert und die Evaluation der gesamten Methodik mit

diesem Werkzeug erfolgreich durchgeführt wurde, gilt somit die Anforderung **A13** als erfüllt. Ein Bestandteil von MOPhisTo ist das Repository, in welches abgeleitet aus spezifischen Operationen und deren Bewertung, generische Prozess- und Gefahrenelemente, sowie deren Relationen abgelegt werden. Die Wiederverwendbarkeit wurde in der Evaluation erfolgreich angewandt, womit die Anforderung **A11** als erfüllt gilt. Während der Durchführung des ersten Fallbeispiels zusammen mit den Domänenexperten wurde der Aspekt der Benutzbarkeit ausgiebig diskutiert. Als negativ betrachtet wurde generell der Aufwand für anfallende Schulungen. Die Werkzeuge Microsoft Word bzw. Microsoft Excel, meistens eingesetzt für die Anwendung der momentanen Methode in der Praxis, wird laut den Experten entweder während der Ausbildung, oder aber in einer späteren Fortbildung erlernt. Einige Experten, die bereits durch anderweitige Tätigkeiten Erfahrungen mit Prozessmodellierung besitzen, gehen davon aus, dass der zusätzliche Aufwand für eine Einführung in MOPhisTo grundsätzlich kein Hindernis darstelle, jedoch sollte dies durch weitergehende Studien gezeigt werden. Ein großes Potential wurde in der Integration aller relevanten Aspekte einer Gefährdungsbeurteilung in ein Werkzeug identifiziert. Das Problem der losen Koppelung von Ablaufbeschreibungen in Microsoft Word und der Beschreibung und Bewertung der Gefahren in Microsoft Excel, zumeist durchgeführt von verschiedenen Personen, wird durch MOPhisTo gelöst. Anforderung **A14** gilt somit nur teilweise als erfüllt. Die von den Experten geschildert Notwendigkeit einer variablen Detailgenauigkeit spiegelt sich im Besonderen bei der automatischen Generierung der Pläne wieder. Für die Vorlage als Genehmigungsdokument ist ein detaillierter Plan mit allen Prozessanweisungen sinnvoll. Für erfahrene Techniker und Mitarbeiter ist vielmehr eine Darstellung des groben Prozessablaufes als Übersicht von Wichtigkeit. Genau dies wurde durch das Werkzeug abgedeckt und von den Experten in der Evaluation bestätigt. Die Anforderung **A12** gilt somit als erfüllt.

Zusammenfassend kann durch die Evaluation gezeigt werden, dass eine Beschreibung des Systems als Ausgangsbasis für eine Erstellung eines Sicherheitskonzeptes inklusive personenbezogener Beschreibungen von Tätigkeiten in einer sequenziellen Abfolge, der Möglichkeit der Synchronisation und der Informationsaustausches durch Kommunikation möglich ist, wonach das Ziel **Z1** - Prozessorientierte Systembeschreibung - als erfüllt gilt. Es konnte gezeigt werden, dass für einzelne Arbeitsschritte in Abhängigkeit zu den spezifischen Anforderungen Gefährdungen und deren Ursachen identifiziert werden können, um im Anschluss den Experten eine Bewertung der Wahrscheinlichkeit eines Eintritts einer Gefährdung sowie deren potenzielles Schadensausmaß zu ermöglichen. Demnach wurde ebenfalls dieses Ziel **Z2** - Konzept für die Identifizierung von Gefahren - erfüllt. Bei der Durchführung beider Anwendungsbeispiele wurde eine quantitative Beurteilung der identifizierten Gefahren durchgeführt, auch unter Berücksichtigung von risikomindernder Maßnahmen. Bei dem zweiten Szenario wurde

ebenfalls die qualitative Beurteilung mittels Simulation angewandt. Das Ziel **Z3** - Quantitative und qualitative Beurteilung der Gefahren - wurde demnach erfüllt. Die Sicherheitsuntersuchung für das Anwendungsbeispiel wurde durchgängig mit EMod und MOPhisTo und dementsprechend mit dem dahinterliegenden integrierten Modell durchgeführt. Damit gelten beide Ziele **Z4** - Durchgängige, integrierte Methodik - und **Z5** - Werkzeugunterstützung - als erfüllt.

5 Zusammenfassung und Ausblick

Der Beschluss der Bundesregierung, bis zum Jahr 2035 den Anteil der erneuerbaren Energien im Strombereich bis zu 60% auszubauen, erhöht den Druck auf die Branche. Bis 2050 soll allein die Windenergie rund die Hälfte aller erneuerbaren Energien ausmachen. Aufgrund der Windverhältnisse eignen sich dafür besonders Offshore-Standorte. Die Wetterbedingungen auf hoher See (zu starker Wind, Regen oder hoher Wellengang) stellen jedoch eine Gefährdung für das Personal dar. In den letzten Jahren ist es deshalb immer wieder zu Unfällen gekommen. Die Versorgung und Rettung von Verletzten ist aufgrund der Komplexität auf hoher See erschwert.

Das frühzeitige Erfassen und Analysieren potenzieller Risiken dient der Reduktion von Unfällen. Im Rahmen des Genehmigungsprozesses für Offshore-Windparks müssen die Betreibergesellschaften Pläne bezüglich Gesundheits-, Arbeitssicherheits- und Umweltschutzregelungen vorlegen, welche die entsprechenden Gefahren und deren Ursachen aufzeigen. Bisher werden die Prozesse der Operationen von den Offshore-Unternehmen zumeist textuell bzw. mit sehr allgemeiner kommerzieller Software für Arbeitsschutz- und Umweltmanagement erstellt.

Die Forschungsarbeit verfolgt das Ziel der Entwicklung einer modellbasierten Methodik für eine computer-gestützte Analyse der Health & Safety Aspekte, um die Planung und Gefahrenbewertung zu unterstützen. Das Konzept der prozessorientierten Systembeschreibung und einer darauf aufbauenden evidenzbasierten Risikoanalyse und Prozessverbesserung ermöglicht eine leichtere Dokumentation und Wiederverwendung. So sind Pläne projektspezifisch anpassbar und bei Beantragung, der Einbindung von Dienstleistern, für Versicherungen und während der Schulung einsetzbar. Das erste Kapitel dieser Arbeit beschäftigt sich mit dem derzeit wenig standardisiertem Vorgehen bei der Erstellung eines HSE-Planes. Die daraus resultierenden Erkenntnisse dienen als Motivation für die Ausarbeitung einer toolgestützten Methodik für einen prozessmodellbasierten Planungsansatz für kooperative sozio-technische Systeme für die Unterstützung der Risikoanalyse und -bewertung.

Im zweiten Kapitel wird der Stand der Wissenschaft und Technik untersucht. Nach einem Überblick über die Methoden der Gefährdungsbeurteilung, welche im deutschen Raum zu tragen kommen, folgte eine Übersicht über identifizierte Techniken der Gefährdungsbeurteilung. Schwerpunkt hierbei sind Werkzeuge und Methoden aus der maritimen Transportwirtschaft sowie der Offshore-Öl- und Gasindustrie. Zudem wird auf artverwandte Domänen wie die Luft- und Raumfahrt und die Automobilindustrie eingegangen. Anschließend widmete sich das Kapitel den Techniken der Prozessmodellierung. Dem angeschlossen wurde auf Verfahren

für prozessorientierte Gefährdungsbeurteilung eingegangen. Abgeschlossen wurde der Überblick über den Stands der Wissenschaft und Technik mit der Überprüfung der Methoden und Techniken hinsichtlich der Abdeckung der in Kapitel 1 vorgestellten Ziele, sowie einer Analyse, in wie weit diese hinsichtlich der Zielerreichung dieser Forschungsarbeit adaptiert bzw. integriert werden konnten.

Die in dieser Forschungsarbeit entstandene toolgestützte Methodik zur Entwicklung bzw. Planung von sicheren Offshore-Operationen, als ein Beispiel für komplexe maritime, wurde im dritten Kapitel vorgestellt und detailliert Erläutert. Die Vorschriften und Standards in Bezug auf die Gesundheits- und Sicherheitsaspekte in der Offshore-Industrie bildeten dabei die normative Grundlage für den Planungsprozess. Dabei wurden die wesentlichen Schritte des HSE-Managements in eine modellbasierte Methode überführt, um somit die (maritimen) Domänen-Experten bei der Entwicklung von HSE-Plänen für Offshore-Operationen oder anderen maritimen Manövern zu Unterstützen. Abgeschlossen wurde das Kapitel mit der Darstellung der prototypische Implementierung "MOPhisTo" für die Unterstützung der vorgestellten modellbasierten Methodik. Um die Durchgängigkeit der Methodik über alle Module zu gewährleisten, liegt dem Prototyp eine Implementierung des integrierten Modells zugrunde. Spätere Erweiterung oder ein Austausch einzelner Komponenten ist, solange sie konform zu diesem Modell sind, ohne großen Aufwand möglich und eine weiteres verwenden der entwickelten Methodik ist gegeben.

Die Evaluation in Kapitel 5 erfolgt mittels zweier Fallbeispiele: "Personentransfer" und "Ladungsversatz". Diese dienen der Überprüfung der Zielerfüllung bzw. Anforderungsabdeckung, der Demonstration der Anwendbarkeit und der Validierung der modellbasierten Methodik. Auf Basis der Befragung von Experten kann die Aussage getroffen werden, dass die modellbasierte Methode als praxistauglich zu bezeichnen. Ein weiterer Aspekt, der für die Praxistauglichkeit spricht, ist die Aussage von der Mehrheit der Experten, dass die Methode auch auf andere Domänen übertragbar sei und nicht zwingend nur zur Erstellung von HSE-Plänen und Gefährdungsbeurteilungen im Bereich der Offshore-Industrie genutzt werden muss. Demnach können für eine Vielzahl von Anwendungsfällen Prozessmodelle und Gefährdungsbeurteilungen erstellt werden.

Durch die Evaluation konnte gezeigt werden, dass basierend auf dem Planungsmodell eine Erstellung einer Gefährdungsbeurteilung durch quantitative Risikoanalyse und Risikobewertung, ergänzt durch eine qualitative Validierung möglich ist. Es konnten jedoch noch weitere Arbeiten identifiziert werden, welche den in dieser Arbeit vorgestellten Ansatz durch weiterer Forschungsvorhaben erweitern könnten:

- ***Übertragbarkeit:*** die toolgestützte Methodik selbst keinerlei offshore-spezifischen Aspekte enthält, kann der Ansatz auf andere Domänen übertragen werden. Im Rahmen eine Übertragung sollten im Speziellen die ersten beiden Phasen der Methodik überprüft werden. Die Modellierung der Prozesse und der Systemumgebung wurden in der Evaluierung lediglich mit einem offshore-spezifischen Kontext durchgeführt. Die Einführung dieser Methodik in eine neue Domäne könnte entsprechende Anpassungen bzw. Erweiterungen des Modells mit sich bringen. Die Risikoanalyse und –Bewertung wurde selbst aus dem Automotive- in den Offshore-Wind-Sektor in dieser Arbeit übertragen. Ob sich das prozessorientierte Verfahren auch für Gefährdungsbeurteilungen innerhalb eines anderen Kontextes eignet (z.B. innerhalb von Gebäuden, Werkstätten oder Fabriken) muss noch durch weitere Fallstudien gezeigt werden.

- ***Automatisierter Vergleich***: Eine mögliche Erweiterung der toolgestützten Methodik wäre ein automatischer Vergleich verschiedener Prozessvarianten, um den Experten unterschiedlichen Auswirkungen hinsichtlich des Risikopotenzials aufzuzeigen. So wurde im Rahmen des Forschungsprojekts COSINUS (Kooperative Schiffsführung für nautische Sicherheit) untersucht in wie weit sich die prozessorientierte Systembeschreibung als Art der Darstellung hinsichtlich des Informationsgehaltes eignet. Ziel des Vorhabens war die Entwicklung eines Systemansatzes für die kooperative Schiffsführung (inklusive vorrauschauender Gefahrenvermeidung und kooperativer Entscheidungsunterstützung) zwischen den Nautikern an Land und auf See für eine sichere, effiziente und damit leichte Verkehrsabwicklung. Das wurde anhand einer Integration der technischen Systeme auf den Schiffsbrücken und in der Verkehrszentrale, sowie neuer Mensch-Maschine-Schnittstellen für die vorrausschauende Darstellung von Lagebildern umgesetzt. Der Einsatz der prozessorientierten Systembeschreibung diente in dem Projekt dem Verständnis und als Ausgangsbasis für Vorgaben bezüglich der Verkehrsabwicklung und der kooperative Entscheidungsfindung für die sichere Schiffsführung. Dies beinhaltet beispielsweise Anforderungen an die Kommunikation zwischen land- und seeseitiger Systeme unter Einbeziehung dezentraler Datenquellen. Dies umfasst neben der Analyse und Definition, welche Daten über welche Kommunikationskanäle mit welchen Datenraten ausgetauscht werden sollen, auch die Anforderungen an die Datenschnittstellen, die Datenvalidierung, die Informationsfusion, die Qualitätsmetriken und die semantischen Kompressionsverfahren, um den Daten- und Informationsaustausch über existierende schmalbandige sowie zukünftige breitbandige Kommunikationskanäle zu realisieren. Die Modellierung selbst ist dabei in einen zweistufigen Prozess unterteilt, bei dem zunächst die normativen Abläufe modelliert werden (vgl. Abbildung 61). Als darauffolgender Schritt wird auf Basis dieses Prozessmodells der Prozess der kooperativen Operation abgeleitet und model-

liert (vgl. Abbildung 62). Die Ergebnisse beider Szenarien werden einer Expertengruppe zum Review bereitgestellt. Diese setzt sich aus nautischen Experten sowohl von Land- als auch von Seeseite zusammen. Darunter befinden sich Hersteller für Schiffsbrücken und Überwachungssysteme für den Schiffsverkehr und Ausbilder für die Berufsschifffahrt. Das Resultat zeigt zwei durch Experten validierte Prozesse, mit dem gemeinsamen Ziel der kooperativen Schiffsführung während eines Anlegemanövers durch Unterstützung verschiedener Systemkomponenten. Ein automatisierter Vergleich würde entsprechende Unterschiede hinsichtlich der Risiken zwischen beiden Prozessen aufzeigen.

- ***Prozessoptimierung:*** Ähnlich wie bei der Optimierung von Prozessen hinsichtlich eines effektiveren Ressourceneinsatzes, kann basierend auf den Erkenntnissen einer durchgeführten Risikoanalyse- und Bewertung ein Prozess durchgeführt werden. So können unter Verwendung von historischem Wissen einzelne Prozessabschnitte hinsichtlich ihrer Risiken hin optimiert werden. Ein Beispiel wäre hierbei das Übersetzen von Personen. Nach [Th10a] gibt es vier Verschiedene Typen des Personentransfers. Der Subprozess "Step-Over" aus dem ersten Fallbeispiel der Evaluation (4.1 Fallbeispiel "Personentransfer"), würde in einer Optimierungsphase mit den äquivalenten Prozessabschnitten alternativer Überstiegs-Varianten verglichen werden.

Literaturverzeichnis

[Ad12] Adolph, L.: Ratgeber zur Gefährdungsbeurteilung. Handbuch für Arbeitsschutzfachleute. Baua, Bundesanstalt für Arbeitssschutz und Arbeitsmedizin, Dortmund[u.a.], 2012.

[Al09] Allweyer, T.: BPMN 2.0 - Business Process Model and Notation. Einführung in den Standard für die Geschäftsprozessmodellierung. Books on Demand GmbH, Norderstedt, 2009, c 2009.

[Al15] Allweyer, T.: BPMN 2.0 - Business Process Model and Notation. Einführung in den Standard für die Geschäftsprozessmodellierung. Books on Demand, Norderstedt, 2015.

[Am08] American Institute of Chemical Engineers: Guidelines for Hazard Evaluation Procedures. John Wiley & Sons, Inc, Hoboken, NJ, USA, 2008.

[Ba13] Barthelmes, H.: Handbuch Industrial Engineering. Vom Markt zum Produkt. Hanser, München, 2013.

[BC78] Buys, J. R.; Clark, J. L.: Events and Causal Factors Charting. DOE 76-45/14. (SSDC-14), 1978.

[Be06] DIN EN 60812:2006-11: Analysetechniken für die Funktionsfähigkeit von Systemen - Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (IEC 60812:2006), 2006.

[Be14] Bethmann, R. Bethmann, R.: Beantworteter Fragebogen zur Evaluierung der Nutzung von HSE-Tools in Unternehmen der maritimen Branche - REETEC GmbH - Fachkraft für Arbeitssicherheit, 2014.

[Be76] Bechmann, A.: Die Nutzwertanal[y]se. Untersuchungen zur Theorie und Praxis eines Planungsinstrumentes. Inst. für Landschaftspflege und Naturschutz der Techn. Univ. Hannover, Hannover, 1976.

[Be95] Becker, J.: Strukturanalogien in Informationsmodellen. In (König, W. Hrsg.): Wirtschaftsinformatik ’95. Physica-Verlag HD, Heidelberg, 1995; S. 133–150.

[BO02] Brabänder, E.; Ochs, H.: Analyse und Gestaltung prozessorientierter Risikomanagementsysteme mit Ereignisgesteuerten Prozessketten. In (Nüttgens, M.; Rump, F. J. Hrsg.): EPK 2002 - Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten, Bonn, 2002.

[Br01] Gefaehrdungs- und Betreibbarkeitsuntersuchung (HAZOP). Leitfaden. BS IEC 61882:2001, 2001.

[Br08] Briol, P.: BPMN. The business process modeling notation pocket handbook. Patrice Briol, [United States?], 2008.

[Br75] Brenner, L.: Accident investigation: multilinear events sequencing method: Journal of Safety Research 7, 1975; S. 67–73.

[BS00] BSI: Occupational health and safety management systems. Guidelines for the implementation of OHSAS 18001. British Standards Institution, London, 2000.

[BS04] Becker, J.; Schütte, R.: Handelsinformationssysteme. Domänenorientierte Einführung in die Wirtschaftsinformatik. mi-Wirtschaftsbuch, München, 2004.

[Bu10] Bundesamt für Seeschifffahrt und Hydrographie (BSH): Standard Schutz- und Sicherheitskonzept für Offshore-Windparks. Entwurf, 2010.

[Bu14a] Bundesamt für Seeschifffahrt und Hydrographie (BSH): Genehmigungsbescheid "OWP West", 2014.

[Bu14b] Bundesministerium für Verkehr und digitale Infrastruktur (BMVI): Offshore Windenergie – Sicherheitsrahmenkonzept. Stand April 2014, 2014.

[Bu96]: Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit. Arbeitsschutzgesetz - ArbSchG, 1996.

[BVW07] Becker, J.; Vering, O.; Winkelmann, A.: Softwareauswahl und -einführung in Industrie und Handel. Vorgehen und Erfahrungen bei ERP- und Warenwirtschaftssystemen ; mit 21 Tabellen. Springer, Berlin [u.a.], 2007.

[Ce11] Center for Chemical Process Safety (CCPS): Layer of Protection Analysis. Simplified Process Risk Assessment. Wiley-AIChE, s.l., 2011.

[Ch06] Churliov, L. et al.: Integrating Risks in Business Process Models with Value focused Process Engineering. In (Ljungberg, J.; Andersson, M. Hrsg.): Proceedings of the 14th European Conference on Information Systems, 2006.

[Ch12] Chien, S. A. et al.: A Generalized Timeline Representation, Services, and Interface for Automating Space Mission Operations. In (SSC; Deutsches Zentrum für Luft- und Raumfahrt (DLR) Hrsg.): SpaceOps 2012 - the 12th International Conference on Space Operations, 2012.

[Co09] Cope, E. W. et al. Cope, E. W. et al.: System and Method for creating and expressing risk-extended business process model, 2009.

[CW02] Clark, T.; Warmer, J. B.: Object modeling with the OCL. The rationale behind the Object Constraint Language. Springer, Berlin, New York, 2002.

[De02] Det Norske Veritas (DNV): Marine risk assessment. Health and Safety Executive, Sudbury, 2002.

[De11a] Deutsches Institut für Normung: ISO 9000 Einführungs- und Unterstützungspaket. Leitfaden zum Konzept und zur Anwendung des prozessorientierten Ansatzes für Managementsysteme. erstellt durch ISO/TC 176/SC 2 „Qualitätsmanagementsysteme“, 2011.

[De11b] Deutsches Institut für Normung: Risikomanagement -Grundsätze und Leitlinien (ISO 31000:2009). Risk management - principles and guidelines (ISO 31000:2009) = Mangement du risque - principes et lignes directrices (ISO 31000:2009). Beuth, Berlin, 2011.

[De11c] Deutsches Institut für Normung: Leitfaden zum Konzept und zur Anwendung des prozessorientierten Ansatzes für Managementsysteme. erstellt durch ISO/TC 176/SC 2 „Qualitätsmanagementsysteme“, 2011.

[DHS14] Dibbern, C.; Hahn, A.; Schweigert, S.: Interoperability In Co-Simulatons Of Maritime Systems. In (ECMS Hrsg.): 28th Conference on Modelling and Simulation, 2014; S. 71–77.

[Dr12] Droste, R. et al.: Model-Based Risk Assessment Supporting Development of HSE Plans for Safe Offshore Operations. In (Hutchison, D. et al. Hrsg.): Formal Methods for Industrial Critical Systems. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012; S. 146–161.

[DS03] Davenport, T. H.; Short, J. E.: The new industrial engineering. Information technology and business process redesign. In Operations management, 2003; S. 97–123.

[E&94] Guidelines for the Development and Application of Health, Safety and Environmental Management Systems, London, 1994.

[EOP13] Erek, K.; Opitz Nicky; Pröhl, T.: Geschäftsprozessmodellierung. Kriterien und Methoden der Prozessmodellierung für ein Management-Cockpit. Projektbericht. Universitätsverlag der TU Berlin, Berlin, 2013.

[Fe05] Fell, R. et al.: A framework for landslide risk assessment and management: Landslide Risk Management. Taylor and Francis, London, 2005.

[FR14] Freund, J.; Rücker, B.: Praxishandbuch BPMN 2.0. Hanser, München, 2014.

[FS13] Ferstl, O. K.; Sinz, E. J.: Grundlagen der Wirtschaftsinformatik. Oldenbourg, München, 2013.

[FSV05] Fink, A.; Schneidereit, G.; Voß, S.: Grundlagen der Wirtschaftsinformatik. Physica-Verl, Heidelberg, 2005.

[Fv13] Frank, U.; van Laak, B. L.: Anforderungen an Sprachen zur Geschäftsprozessmodellierung, Koblenz, 2013.

[Ga10] Gadatsch, A.: Grundkurs Geschäftsprozess-Management. Methoden und Werkzeuge für die IT-Praxis ; eine Einführung für Studenten und Praktiker. Vieweg + Teubner, Wiesbaden, 2010.

[Ga99] Garrik, J.: Risk Assesment Methodologies Applicable to Marine Systems, Washington, D.C., 1999.

[Ge02] Richtlinie zur Erstellung von technischen Risikoanalysen für Offshore-Windparks, Hamburg, 2002.

[Ge14] Offshore Code of Practice (OCoP), 2014.

[GKM13] Gruber, H.; Kittelmann, M.; Mierdel, B.: Leitfaden für die Gefährdungsbeurteilung. DCV, Bochum, 2013.

[Gö11] Götz, M.: BPMN 2.0 Tutorial - Kompakte Einführung in die BPMN 2.0, 2011.

[Go16] Golluecke, V.: Bewertung von Simulationszuständen für eine gezielte Analyse risikoreicher Systeme, Oldenburg, 2016.

[Ha14] Hahn, A.: Test Bed for Safety Assessment of New e-Navigation Systems*. In International Journal of e-Navigation and Maritime Economy, 2014, 1; S. 14–28.

[HB87] Hendrick, K.; Benner, L.: Investigating accidents with STEP. Dekker, New York, 1987.

[He06] Hevner, A. R. et al.: Design science in information systems research: Information systems the state of the field. Wiley, Chichester [u.a.], 2006; S. 191–232.

[He94] Hesse, W. et al.: Terminologie in der Softwaretechnik - Ein Begriffssystem für die Analyse und Modellierung von Anwendungssystemen. Teil 2: Tätigkeits- und ergebnisbezogene Elemente: Informatik-Spektrum. Springer-Verlag, 1994; S. 96–105.

[Hi14] Hintermaier, U. Hintermaier, U.: Antwort auf die Frage, wie HSE-Pläne erstellt werden - Siemens – HSE Coordinator Offshore, 2014.

[Ho08] Hoffmann, D. W.: Software-Qualität. Springer, Berlin, Heidelberg, 2008.

[Hu03] Huth, M.: Risikomanagement in der Logistik (Teil 2). Prozesskettenbezogene Risikoanalyse. In RiskNET - The Risk Management Network, 2003; S. 55–67.

[IE10] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, Geneva, Switzerland, 2010.

[IE16] IEC 61511. Functional safety - Safety instrumented systems for the process industry sector. International Electrotechnical Commission, Geneva, 2016.

[In08] ISO DIS 26262; Road vehicles - Functional safety, 2008.

[IS15] ISO 29400:2015. Ships and marine technology -- Offshore wind energy -- Port and marine operations, 2015.

[JTQ07] Jakoubi, S.; Tjoa, S.; Quirchmayr, G.: Rope: A Methodology for Enabling the Risk-Aware Modelling and Simulation of Business Processes: ECIS 2007 Proceedings, 2007.

[Ke05] Kecher, C.: UML 2.0. Das umfassende Handbuch ; [inkl. DIN-A2-Poster mit Struktur- und Verhaltensdiagrammen ; aktuell zum UML-Standard 2.0 ; alle Diagramme und Notationselemente ; Praxisbeispiele in C# und Java 5 ; inkl. CD mit UML-Tools]. Galileo Press, Bonn, 2005.

[Ke07] Kelter, U.: Software-Qualitätsmodelle, 2007.

[KKS04] Klein, R.; Kupsch, F.; Scheer, A.-W.: Modellierung inter-organisationaler Prozesse mit ereignisgesteuerten Prozessketten. In Veröffentlichungen des Instituts für, 2004.

[KNS92] Keller, G.; Nüttgens, M.; Scheer, A.-W.: Semantische Prozeßmodellierung auf der Grundlage „Ereignisgesteuerter Prozeßketten (EPK)“. Heft 89, 1992.

[Kr13] Kristiansen, S.: Maritime Transportation: Safety Management and Risk Analysis. Taylor and Francis, 2013.

[LBP12] Läsche, C.; Böde, E.; Peikenkamp, T.: A Method for Guided Hazard Identification and Risk Mitigation for Offshore Operations. In (Hutchison, D. et al. Hrsg.): Computer Safety, Reliability, and Security. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012; S. 37–48.

[Le14] Legde, M. Droste, R.; Petry, C. M.; Pinkowski, J.: Vorstellung der toolgestützen Methode für die Erstellung von HSE - Plänen. DNV - GL, Hamburg, 2014.

[Le95] Lehner, F.: Grundfragen und Positioniereung der Wirtschaftsinformatik. In (Lehner, F.; Hildebrand, K.; Maier, R. Hrsg.): Wirtschaftsinformatik - Theoretische Grundlagen. Hanser, Wien, 1995; S. 1–71.

[Ma13] Maier, C.: Integriertes Modell zur Entwicklung von funktional sicheren Produkten in der Automobilbranche, 2013.

[Mo07] Moody, D.: What makes a good diagram? improving the cognitive effectiveness of diagrams in is development: Advances in Information Systems Development, 2007, 2007; S. 481–492.

[MOS09] Mevius, M.; Oberweis, A.; Stucky, W.: Neue Ansätze bei der Modellierung eines kennzahlenbasierten Managements von Geschäftsprozessen. In Controlling Zeitschrift für erfolgsorientierte Unternehmenssteuerung, 2009, 21.

[Ob11] Object Management Group (OMG): BPMN 2.0 - Business Process Model and Notation. http://www.bpmb.de/images/BPMN2_0_Poster_DE.pdf.

[ORM03] Owen, M.; Raj, J.; Martin Owen and Jog Raj, Popkin Software: BPMN and Business Process Management. Introduction to the New Business Process Modeling Standard, 2003.

[Ös12] Österreich, B.: Analyse und Design mit der UML 2.5. Objektorientierte Softwareentwicklung ; [inkl. Poster mit UML-Notationsübersicht]. z. Oldenbourg, München, 2012.

[Ot14] Otegui, J. L.: Failure analysis. Fundamentals and applications in mechanical components. Springer, Cham, 2014.

[Pa87] Pall, G. A.: Quality process management. Prentice-Hall, Englewood Cliffs NJ, 1987.

[Pe07] Peffers, K. et al.: A design science research methodology for information systems research. In Journal of management information systems, 2007, 24; S. 45–77.

[Pi15] Pinkowski, J.: Prozessgetriebene Risikoanalyse zur Bewertung maritimer Operationen. Dissertation, Oldenburg, 2015.

[PS13] Pfeiffer, T.; Sauer, J.: Arbeitsschutz von A-Z 2014. Haufe-Lexware, Freiburg im Breisgau, 2013.

[re13] Offshore Wind and Marine Energy Health and Safety Guidelines. 2013: Issue 1, 2013.

[Ro96] Rosemann, M.: Komplexitätsmanagement in Prozeßmodellen. Methodenspezifische Gestaltungsempfehlungen für die Informationsmodellierung. Gabler Verlag, Wiesbaden, 1996.

[RSD08] Rosemann, M.; Schwegmann, A.; Delfmann, P.: Notwendigkeit einer Vorbereitung der Prozessmodellierung. In (Becker, J. Hrsg.): Prozessmanagement. Ein Leitfaden zur prozessorientierten Organisationsgestaltung. Springer, Berlin [u.a.], 2008; S. 45–104.

[Sa05] Salvi, O.: EU-Project ARAMIS (Accidental Risk Assessment Methodology for Industries in the framework of the SEVESO II directive), 2005.

[Sc01] Scheer, A.-W.: ARIS - Modellierungsmethoden, Metamodelle, Anwendungen. Springer, Berlin [u.a.], 2001.

[SC02] Stamatelatos, M.; Caraballo, J.: Fault tree handbook with aerospace applications. Office of safety and mission assurance NASA headquarters, Washinton, D.C., 2002.

[Sc12] Schnegelsberg, S.: Sicherheitsaspekte in offshore – Windparks aus Sicht des Arbeitsschutzes, Emden, 2012.

[Sc13] Schnegelsberg, S.: Schutz-und Sicherheitskonzept für Arbeiten an Offshore-Windenergieanlagen, Rheinsberg, 2013.

[Sc14] Schnegelsberg, S. Schnegelsberg, S.: Gefährdungsbeurteilung in der Offshore-Domäne, 2014.

[Sc91] Scheer, A.-W.: Architektur integrierter Informationssysteme. Grundlagen der Unternehmensmodellierung. Springer, Berlin, 1991.

[Sc98] Schütte, R.: Grundsätze orddnungsmässiger referenzmodellierung. Konstruktion konfigurations- und anpassungsorientierter Modelle. Gabler, Wiesbaden, 1998.

[SDH12] Schweigert, S.; Droste, R.; Hahn, A. Hrsg.: Multi-Agenten basierte 3D Simulation für die Evaluierung von Offshore Operationen (accepted paper), 2012.

[So12a] Sobiech, C. et al.: Model based Development of Health, Safety, and Environment Plans and Risk Assessment for Offshore Operations. In (Bruzzone, G.; Caccia, M. Hrsg.): Manoeuvring and Control of Marine Craft. Elsevier, IFAC, 2012; S. 49–54.

[So12b] Sobiech, C. et al.: Project Soop: Safe Offshore Operations: International Symposium Information on Ships ISIS 2012, 2012.

[SS04] Schmelzer, H. J.; Sesselmann, W.: Geschäftsprozessmanagement in der Praxis. Produktivität steigern, Wert erhöhen, Kunden zufrieden stellen. Hanser, München, 2004.

[St06] Staud, J. L.: Geschäftsprozessanalyse. Ereignisgesteuerte Prozessketten und objektorientierte Geschäftsprozessmodellierung für Betriebswirtschaftliche Standardsoftware (German Edition). Springer, Dordrecht, 2006.

[St13] Kostensenkungspotenziale der Offshore-Windenergie in Deutschland, Berlin, Germany, 2013.

[Su12] Sutton, I. S.: Offshore safety management. Implementing a SEMS program. William Andrew, Waltham, MA, 2012.

[SW14] Schneider, P.; Wallenstein, M. Schneider, P.; Wallenstein, M.: Antwort auf die Frage, wie HSE-Pläne erstellt werden - OWS, Oldenburg, 2014.

[SWD08] Spath, D.; Weisbecker, A.; Drawehn, J. Hrsg.: Business process management tools 2008. Eine evaluierende Marktstudie zu aktuellen Werkzeugen. Fraunhofer IRB Verl, Stuttgart, 2008.

[Th05] The International Marine Contractors Association (IMCA): FMEA management guide. IMCA M 178, 2005.

[Th10a] The International Marine Contractors Association (IMCA): Guidance on the Transfer of Personnel to and from Offshore Vessels. IMCA SEL 025, IMCA M 202, 2010.

[Th10b] The International Association of Oil & Gas Producers (OGP): HSE management - guidelines for working together in a contract environment, London, 2010.

[Th11] The Netherlands Oil and Gas Exploration and Production Association (NOGEPA): Helideck Operations and Precedures Manual, 2011.

[Th12] Thomsen, K. E.: Offshore wind. A comprehensive guide to successful offshore wind farm installation. Elsevier, Amsterdam, 2012.

[To06] Natural Hazard Management. Research Report, 2006.

[va13] van Leusen, S.: Zulassungsverfahren für Offshore-Windparks in der deutschen AWZ, 2013.

[Vi07] Vinnem, J. E.: Offshore Risk Assessment. Principles, Modelling and Applications of Qra Studies. Springer, Dordrecht, 2007.

[VR05] Guideline for quantitative risk assessment - "Purple book". CPR 18E, 2005.

[vv00] van der Aalst, W.; van Hee, K.: Workflow Management. Models, methods and systems, Eindhoven, 2000.

[Wa01] Wallmüller, E.: Software-Qualitätsmanagement in der Praxis. Software-Qualität durch Führung und Verbesserung von Software-Prozessen. Hanser, München, 2001.

[Wa02] Wang, J.: Offshore safety case approach and formal safety assessment of ships. In Journal of Safety Research, 2002, 33; S. 81–115.

[WF10] Wagner, D.; Ferstl, O. K.: Erhöhte Abbildungstreue von Geschäftsprozessmodellen durch Kontextsensitivität. In (Engels, G. Hrsg.): Modellierung 2010. 24. - 26. März 2010, Klagenfurt, Österreich. Ges. für Informatik, Bonn, 2010; S. 117–132.

[Wh04] White, S. A.: Introduction to BPMN. In IBM Cooperation, 2004, 2; S. 0.

[WJ05] Weiß, G.; Jakob, R.: Agentenorientierte Softwareentwicklung. Methoden und Tools ; mit 78 Tabellen. Springer, Berlin, 2005.

[WJ06] Weiß, G.; Jakob, R.: Agentenorientierte Softwareentwicklung. Springer, Dordrecht, 2006.

[WK03] Warmer, J. B.; Kleppe, A. G.: The object constraint language. Getting your models ready for MDA. Addison-Wesley, Boston, MA, 2003.

[WW02] Wand, Y.; Weber, R.: Research Commentary. Information Systems and Conceptual Modeling—A Research Agenda: Information Systems Research, 2002; S. 363–376.

[Za71] Zangemeister, C.: Nutzwertanalyse in der Systemtechnik. Eine Methodik zur multidimensionalen Bewertung und Auswahl von Projektalternativen. Zugl.: Berlin (West), Techn. Univ., Diss., 1970. Wittemann, München, 1971.

[ZDN05] Zeiler, M.; Dahlke, C.; Nolte, N.: Offshore-Windparks in der ausschließlichen Wirtschaftszone von Nord- und Ostsee, 2005.

[ZDN13] Zhang, H.; Duan, M.; Ni, Mingchen, Hu, Yianwei: Risk Analysis of Oil/Gas Leakage of Subsea Production System Based on Fuzzy Fault Tree: International Journal of Energy Engineering (IJEE). World Academic Publishing, 2013; S. 79–85.

[Zh01] Zhang, L. et al.: Model-based Operational Planning Using Coloured Petri Nets, 2001.

Anhang

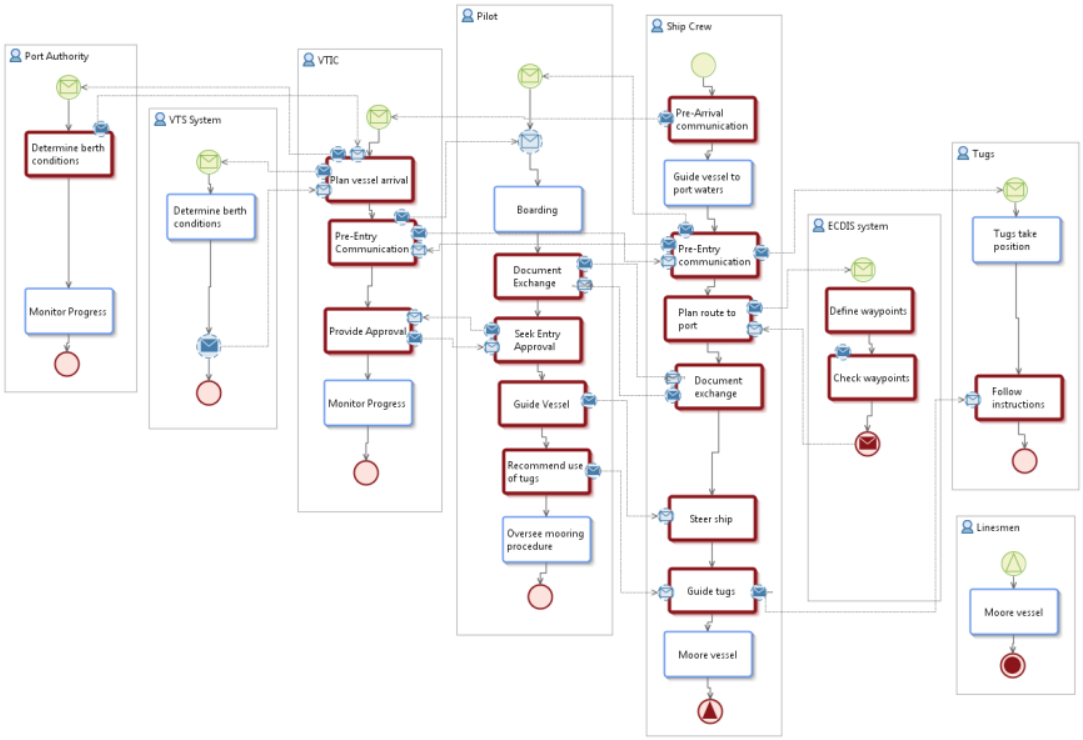


Abbildung 61: Klassisches Anlegemanöver

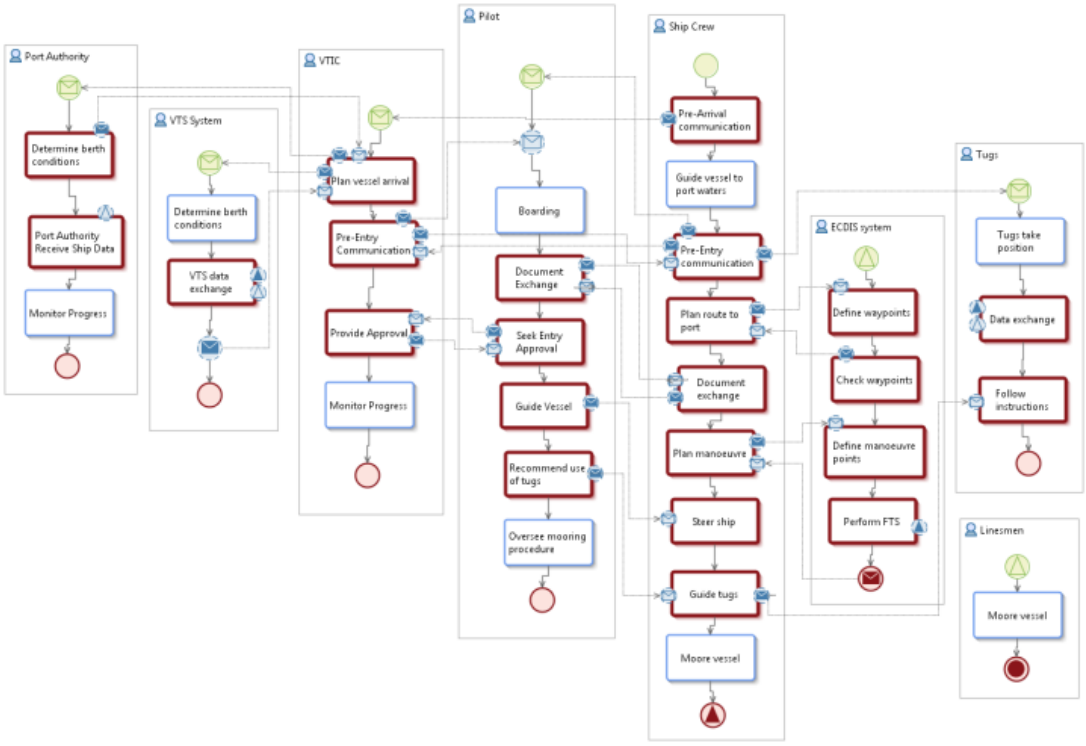


Abbildung 62: Kooperatives Anlegemanöver

The LiftSupervisor is too close to the Cargo.

```
distance between LiftSupervisor and Cargo hooked on Crane is
    lower than 1 meter and Cargo is "swinging".
```

Alternative using status macros:

```
status macro for Cargo named "hooked": Cargo is hooked on Crane
    .
distance between LiftSupervisor and "hooked" Cargo is lower
    than 1 meter and Cargo is "swinging".
```

LiftSupervisor is hit by Cargo.

```
position of LiftSupervisor equals the position of Cargo hooked
    on Crane.
```

Equipment of Ship is hit by Cargo.

```
position of Object at Ship equals position of Cargo hooked on
    Crane.
```

LiftSupervisor stands under Cargo.

```
LiftSupervisor is under Cargo lifted on Crane.
```

Abbildung 63: Hazard Description Language (HDL) – Beispiel

Eidesstattliche Erklärung

Hiermit versichere ich, Rainer DROSTE, dass ich die von mir vorgelegte Arbeit mit dem Titel, 'Modellbasierte Planung zur Unterstützung der Gefährdungsbeurteilung maritimer Operationen' selbstständig verfasst habe, dass ich die verwendeten Quellen, Internet-Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Datum	Rainer DROSTE