Hochschule Fulda
University of Applied Sciences

Discussion Papers in Business and Economics

Huth, Michael/Düerkop, Sascha/Romeike, Frank

RIMA-KIL – Risikomanagement für kritische Infrastrukturen in der Logistik

Abschlussbericht

Discussion Paper No 19
4/2017

Herausgeber/Editor:
Hochschule Fulda/Fulda University of Applied Sciences
Fachbereich Wirtschaft/Department of Business
Leipziger Straße 123
36037 Fulda
Deutschland/Germany
www.hs-fulda.de/wirtschaft

ISSN: 2194-7309

Abstract

Das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) publizierte Anfang 2015 die „Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft – Schutz kritischer Infrastrukturen und verkehrsträgerübergreifende Gefahrenabwehr“. Dieses Dokument offenbart erhebliche Erkenntnisdefizite hinsichtlich der Kritikalität logistischer Infrastrukturen durch potenzielle Bedrohungen wie Naturkatastrophen, Unfälle oder terroristische Angriffe. Damit wird deutlich: Deutschland ist auf Risiken, die nach Eintritt einen wesentlichen Einfluss auf die logistische Infrastruktur haben, nur bedingt vorbereitet.

Im Rahmen des Projektes RIMA-KIL „Risikomanagement für kritische Infrastrukturen in der Logistik“ wurden nun verschiedene Ansätze zur Identifizierung und Bewertung von Risiken für die kritische logistische Infrastruktur entwickelt, untersucht und katalogisiert. Das entstandene Methodenset, welches sich Methoden sowohl des Risikomanagements als auch des Operations Research bedient, gibt dem Anwender einen umfassenden Überblick über existierende und praxiserprobte Ansätze. Ferner gibt es in vielen Fällen eine Bewertung über die Anwendbarkeit im logistischen Kontext an.

Mit Hilfe der Methoden, die RIMA-KIL übersichtlich katalogisiert hat, kann ein Entscheider geeignete Tools zur Risikoidentifikation und Risikobewertung umsetzen und vorhandene Risiken so erkennen und proaktiv oder auch reaktiv managen. Auf Basis dieses Erkenntnisgewinns ist es anschließend einem Infrastrukturbetreiber erst möglich das Gesamtnetzwerk entsprechend auszubauen um auch beim Risikoeintritt adäquat vorbereitet zu sein.

Um sowohl praxisrelevante als auch wissenschaftlich innovative Ergebnisse zu erzielen, wurde das Projekt interdisziplinär mit Beteiligten aus Forschung und Praxis durchgeführt. Regelmäßige Koordinationstreffen mit Infrastrukturbetreiber und -nutzern, sowie zahlreiche Präsentationen auf wissenschaftlichen Fachkonferenzen stellten ein ständiges Feedback und somit mögliche Verbesserungen sicher.

Stichworte: Logistik, Infrastruktur, Risikomanagement, Resilienz, Schadenprävention, Risikobewertung

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AH1. ..... Asian Highway 1

AHP ..... Analytic Hierarchy Process

BARM-KIL ..... Best-Practice-Ansätze im Risikomanagement für kritische Infrastrukturen in der Logistik

BBK. ..... Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

BCM ..... Business Continuity Management

BER ..... Flughafen Berlin-Brandenburg

BIA ..... Business Impact Analysis

BMVI. ..... Bundesministerium für Verkehr und digitale Infrastruktur

BSI. ..... Bundesamt für Sicherheit in der Informationstechnik

CDF ..... Cumulative Distribution Fuction / Kumulierte Dichtefunktion

CGA ..... Cross consistency assessment

CIPRNet ..... Critical Infrastructure Preparedness and Resilience Research Network

CNBC ..... Consumer News and Business Channel

CNN ..... Cable News Network

CRMARS ..... Creative Risk Management Approach based on Reverse Thinking

CVT ..... Continuously Variable Transmission / Stufenloses Getriebe

DB ..... Deutsche Bahn

DIN ..... Deutsches Institut für Normung

EN ..... Europäische Norm

ETA ..... Event Tree Analysis / Ereignisbaumanalyse

FCM ..... Fuzzy Cognitive Map

FMEA ..... Fehlermöglichkeits- und Einflussanalyse

FTA ..... Fault Tree Analysis / Fehlerbaumanalyse

GBM ..... Geometrisch Brownsche Bewegung

HAZOP ..... Hazard and Operability

HGrG. ..... Haushaltsgrundsätzegesetz

HOLM. ..... House of Logistics and Mobility

IBSE ..... Interessengemeinschaft zur Bereisung von Straßenbahn- und Eisenbahnstrecken

IDW. ..... Institut der Wirtschaftsprüfer

IEC ..... International Electrotechnical Commission

IHK ..... Industrie- und Handelskammer

ISO ..... International Organization for Standardization

ISO/TS ..... Technical Specification der ISO

KRI ..... Key Risk Indikatoren

LPG ..... Liquid Petroleum Gas

MTPD ..... Maximum Tolerable Period of Disruption

NATO ..... North Atlantic Treaty Organization

NBL ..... Newcomb-Benford's Law

PESTLE ..... Political, Economical, Social, Technological, Legal, Ecological

PIRG ..... Public Interest Research Group

ÖPNV ..... Öffentlicher Personen-Nahverkehr

RAND Corp. ..... Research and Development Corporation

RCA ..... Root Cause Analysis / Fehler-Ursachen-Analyse

RIM ..... Risiko-Idenfikations-Matrix

RIMA-KIL. ..... Risikomanagement für kritische Infrastrukturen in der Logistik

RPZ ..... Risikoprioritätszahl

RSSF ..... Rail Safety and Standards Board des Vereinigten Königreichs

RTO ..... Recovery Time Objective

SWOT ..... Strengths, Weaknesses, Opportunities, Threats

TE ..... Transporteinheiten

USA. ..... Vereinigte Staaten von Amerika

ZE ..... Zeiteinheiten

1 Einleitung

1.1 Ausgangssituation

Das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) publizierte Anfang 2015 die „Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft – Schutz kritischer Infrastrukturen und verkehrsträgerübergreifende Gefahrenabwehr“.[1] Dieses Dokument offenbart (zumindest auf Bundesebene) erhebliche Erkenntnisdefizite hinsichtlich der Kritikalität logistischer Infrastrukturen durch potenzielle Bedrohungen wie beispielsweise Überschwemmungen, aber auch terroristischer Angriffe.[2] Damit wird deutlich: Deutschland ist auf Risiken, die die logistische Infrastruktur betreffen, nur bedingt vorbereitet, weil identifizierte und zukünftige Risiken nicht ausreichend qualifiziert bewertet sind.

Erst die strukturierte, methodisch fundierte und (möglichst) vollständige Identifikation von Risiken sowie deren Bewertung ermöglichen es, logistische Infrastrukturen hinsichtlich ihrer Kritikalität zu beurteilen und zu priorisieren sowie entsprechende Maßnahmen und Maßnahmenpläne zu entwickeln, die Häufigkeit (bzw. die Wahrscheinlichkeit) und/oder Konsequenzen der Risiken reduzieren und die damit eine hohe Verfügbarkeit der Logistik auch als volkswirtschaftliches Versorgungssystem sicherstellen.

Risikoidentifikation und Risikobewertung sind wesentliche Phasen des Risikomanagement-Prozesses, der auf einer Regelkreislogik basiert. Risikomanagement ist seit einigen Jahrzehnten sowohl in Form des betrieblichen Risikomanagements in privatrechtlichen Unternehmen als auch im öffentlichen Bereich etabliert. Die gesetzliche Grundlage des Risikomanagements für den öffentlich-rechtlichen Sektor ist durch § 53 des Haushaltsgrundsätzegesetzes (HGrG) kodifiziert, der seine Entsprechung im Prüfungsstandard 720 des IDW (Institut der Wirtschaftsprüfer) findet. Das oben angeführte Dokument des BMVI macht allerdings deutlich, dass bisher kaum ein systematisches Risikomanagement seitens der Infrastrukturbetreiber stattfindet. Umgekehrt jedoch haben Infrastrukturbetreiber, im Gegensatz zu den betrieblichen Nutzern, alleinig die Möglichkeit, das Logistiknetzwerk so anzupassen, dass es auf potenzielle Realisierungen von Risiken vorbereitet ist.

In den letzten Jahren rückte die Diskrepanz zwischen Notwendigkeit und Anwendung des Risikomanagements für kritische Infrastrukturen stärker in den Fokus zahlreicher Institutionen der öffentlichen Hand So erarbeiteten das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) Konzepte zum „Schutz Kritischer Infrastrukturen“(KRITIS) .[3] Als Teil dieses Projektes führte die KPMG AG Wirtschaftsprüfungsgesellschaft im Auftrag des BSI die „KRITIS-Sektorstudie Transport und Verkehr“ durch und veröffentlichte die Ergebnisse.[4] Vor allem in

[1] Vgl. Bundesministerium für Verkehr und digitale Infrastruktur (2015).
[2] Vgl. dazu auch die kritische Analyse in Huth, Romeike (2015).
[3] Vgl. dazu unter anderem Bundesministerium des Innern (2009) und Bundesministerium des Innern (2011).
[4] Vgl. dazu Bundesamtes für Sicherheit in der Informationstechnik (2015).

dieser Studie werden zwar die Themenkomplexe Transport und Verkehr untersucht, die Logistik jedoch nicht explizit betrachtet. Die Ergebnisse von BBK und BSI lassen sich folgerichtig einerseits als Grundlage für weitere Forschungen nutzen, zeigen aber andererseits auch erneut und sehr präzise die Forschungslücke bezüglich des Risikomanagements in der Logistik auf.

Die Notwendigkeit des Schutzes kritischer Infrastrukturen ist in den vergangenen Jahren, unter anderem auch durch die erhöhte Terrorgefahr in den infrastrukturstarken Nationen, erheblich gestiegen. Die neuerlichen Studien hierzu untermauern dieses gestiegene Interesse an der Thematik. Ferner nährt sich das erhöhte Bewusstsein für die Notwendigkeit eines Risikomanagements für (nicht nur, aber vor allem logistische) Infrastrukturen auch aus direkten Drohungen und Handlungsanweisungen verschiedener Gefährder. Als prominentestes Beispiel sei die sogenannte „Declaration of Jihad" der Terrororganisation Al-Quaida von 2006 erwähnt.[5] Dort heißt es unter der Überschrift „The main mission for which the Military Organization [of Al-Quaeda] is responsible is:" unter anderem "Gathering information about […] the installations" und "Blasting and destroying bridges leading into and out of the cities".[6] Aus diesen konkreten Handlungsanweisungen an den militanten Teil der Al-Quaida folgt unmittelbar die Notwendigkeit sich auf ebendiese Gefahren bzw. Risiken[7] vorzubereiten.

1.2 Zielsetzung

Das Forschungsvorhaben „RIMA-KIL – Risikomanagement für kritische Infrastrukturen in der Logistik" schließt die im vorherigen Abschnitt skizzierte Lücke durch die Entwicklung eines praxisorientierten Vorgehensmodells zur Identifikation und Bewertung von Risiken für logistische Infrastrukturen. Ziel des Projektvorhabens ist es, ein Methodenset zu etablieren, mit dem sich kritische Infrastrukturen in der Logistik identifizieren und bewerten lassen. Das Methodenset dient vor allem öffentlichen Institutionen als Tool, um Risikoanalysen der logistischen Infrastruktur und methodisch-fundierter und standardisierter Form durchführen zu können. RIMA-KIL legt damit die Grundlage für die Risikobewertung der logistischen Infrastrukturen.

Konkretes Ergebnis des Projekts ist eine Übersicht über etablierte und praxiserprobte Risikomanagement-Methoden, wobei jede Methode hinsichtlich ihres spezifischen Einsatzpotenzials für das Risikomanagement kritischer Infrastrukturen in der Logistik bewertet wird.

---

5 Vgl. Al Qaeda (2001).

6 Vgl. Al Qaeda (2001), S. 14.

7 Eine Gefahr, Gefährdungspotenzial bzw. Gefährdung („hazard") besteht immer dann, wenn ein Gegenstand (oder ein chemischer Stoff) oder eine Situation wesentlich so beschaffen ist, dass hiervon eine schädliche Wirkung resultieren kann (inhärente Eigenschaft eines Stoffes oder einer Situation). Ein Risiko existiert nur dann, wenn eine Gefahr und zugleich eine Exposition gegenüber derselben gegeben sind. Nur beide Elemente zusammen bedeuten ein Risiko.

1.3 Vorgehensweise

Der vorliegende Abschlussbericht fasst die Ergebnisse des Forschungsprojekts zusammen und gibt Empfehlungen für die nächsten Schritte auf dem Weg zu einem effektiven Risikomanagement für kritische Infrastrukturen in der Logistik.

Zu Beginn werden in Kapitel 2 die wichtigsten Begriffe und Konzepte, die für das Risikomanagement kritischer Infrastrukturen in der Logistik von Bedeutung sind, inhaltlich abgegrenzt und dargestellt: Notwendig ist,

- kritische Infrastrukturen in der Logistik abzugrenzen,
- Risiken zu charakterisieren, die für kritische Infrastrukturen in der Logistik relevant sind, sowie
- das Konzept des Risikomanagements darzustellen.

Mit diesen notwendigen Grundlagen lassen sich in Kapitel 3 die Methoden auflisten, die für Risikoidentifikation, Risikoanalyse und Risikobewertung eingesetzt werden können. Anschließend werden diese hinsichtlich ihres Einsatz- und Anwendungspotenzials für kritische Infrastrukturen in der Logistik untersucht und bewertet. Die Bewertung basiert auf definierten Kriterien, wie beispielsweise den benötigten Daten oder dem zeitlichen Aufwand für die Anwendung der jeweiligen Methode. Abgeschlossen wird Kapitel 3 mit einer Übersicht über die bewerteten Methoden als wesentliche Entscheidungsgrundlage.

Für einen Methodentyp wurden im Rahmen des Forschungsvorhabens prototypische Implementierungen vorgenommen, um ihr Anwendungspotenzial zu testen. Dabei handelt es sich um netzwerkbasierte Ansätze zur Risikobewertung, bei denen Modelle und Methoden des Operations Research eingesetzt werden. Kapitel 4 dient dazu, diese Ansätze näher zu erläutern und ihr Anwendungspotenzial kritisch zu reflektieren.

Im abschließenden Kapitel 5 werden die gewonnenen Ergebnisse zusammengefasst. Weiterhin werden Empfehlungen für die nächsten Schritte gegeben, ein effektives Risikomanagement für kritische Infrastrukturen in der Logistik zu etablieren.

1.4 Rahmendaten des Forschungsvorhabens „RIMA-KIL – Risikomanagement für kritische Infrastrukturen in der Logistik“

Das Forschungsvorhaben „RIMA-KIL – Risikomanagement für kritische Infrastrukturen in der Logistik“ wurde im Zeitraum März bis November 2016 am House of Logistics and Mobility (HOLM) durchgeführt. Projektpartner waren die Hochschule Fulda, Fachbereich Wirtschaft, sowie die RiskNET GmbH. Assoziierte Partner waren die Contargo Rhein-Main GmbH und Hessen Mobil Straßen- und Verkehrsmanagement. Die nachfolgende Tabelle 1 listet die beteiligten Institutionen sowie die involvierten Ansprechpartner auf.

Institution/Unternehmen	Rolle	Ansprechpartner
Hochschule Fulda[8]	Projektpartner, Projektleitung	Prof. Dr. Michael Huth (Professor für allgemeine Betriebswirtschaftslehre, insbesondere Logistik) Sascha Düerkop (wissenschaftlicher Mitarbeiter) Eugen Kusowenko (studentischer Mitarbeiter)
RiskNET GmbH[9]	Projektpartner	Frank Romeike (Geschäftsführer)
Contargo Rhein-Main GmbH[10]	Assoziierter Partner	Christian Eichmeier (Geschäftsführer) Matthias Krämer (Operations Manager)
Hessen Mobil Straßen- und Verkehrsmanagement[11]	Assoziierter Partner	Matthias Burger (Dezernatsleiter „Steuerung Verkehr“)

Tabelle 1: Beteiligte Institutionen und Ansprechpartner

Das Forschungsvorhaben wurde durch Mittel des HOLM-Innovationsfonds gefördert.[12]

[8] Homepage: https://www.hs-fulda.de/fachbereiche/wirtschaft/.
[9] Homepage: https://www.risknet.de/ bzw. http://www.risknet.eu.
[10] Homepage: http://www.contargo.net/de/.
[11] Homepage: https://mobil.hessen.de/.
[12] Vgl. dazu die Informationen sowie die Projektübersicht auf der Homepage des „House of Logistics and Mobility“ (HOLM): http://www.frankfurt-holm.de/de/services-innovationsfoerderung#node-748.

2 Grundlagen des Risikomanagements kritischer Infrastrukturen in der Logistik

2.1 Abgrenzung kritischer Infrastrukturen in der Logistik

Um den Begriff „kritische Infrastrukturen in der Logistik“ einerseits präzise und andererseits weit genug zu fassen, wird der Begriff für den Rahmen des Projekts im Folgenden explizit definiert. Die Definition soll hierzu aus etablierten Definitionen der Begriffe „Infrastruktur“ und „Kritische Infrastruktur“ abgeleitet werden.

Der Begriff „Infrastruktur“ wird im Folgenden synonym zu dem Begriff „materielle Infrastruktur“, den Jochimsen (1966) in seinem Standardwerk „Theorie der Infrastruktur: Grundlagen der marktwirtschaftlichen Entwicklung“ geprägt hat[13], verwendet. So lässt sich Infrastruktur (eines Landes) definieren als „den Teil der von Menschen erschaffenen Landschaftsstruktur, der durch die immobilen Kapitalgüter repräsentiert wird, deren Outputs der Befriedigung der physischen und sozialen Grundbedürfnisse der Wirtschaftssubjekte dienen; diese Güter und Dienste sind sonst für das einzelne Wirtschaftssubjekt aus Produktions- und Kostengründen nicht verfügbar.“[14]

Basierend auf der obigen Definition des Infrastrukturbegriffes lässt sich der Begriff „kritische Infrastruktur“ diskutieren. Nachdem zahlreiche staatliche Sicherheitskonzeptvorschläge, vor allem in den USA, den Begriff „kritische Infrastruktur“ bereits in den 80er Jahren des vorherigen Jahrhunderts meist durch eine Auflistung aller entsprechenden Infrastrukturen fassten, versuchte sich der „Patriot Act“ 2001 erstmals an einer formalen Definition. Der Patriot Act war ein Sicherheitsdokument, welches unmittelbar nach den Terroranschlägen auf das World Trade Center am 11. September 2001 vom Parlament der USA verabschiedet wurde und darauf abzielte, Terrorakte in den USA und weltweit zu bestrafen und die Gesetzesvollstreckung und seine Fahndungsmethoden zu verbessen.[15] So definierte der Patriot Act den Begriff „Critical Infrastructure“ als “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”[16]

Nahezu wörtlich übernahmen deutsche Behörden diese Definition und übersetzten sie wie folgt: „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“[17] Um diesen abstrakten und weitgefassten Begriff wei-

[13] Jochimsen (1966).
[14] Buhr (2009), S. 40.
[15] Vgl. 107th Congress (2001).
[16] 107th Congress (2001), Sec 1016(b)(2).
[17] Bundesministerium des Innern (2011).

ter zu präzisieren und somit auf die Anwendungen von RIMA-KIL zu spezialisieren, wird folgend der Begriff der „Kritischen Infrastruktur in der Logistik“ eingeführt.

Mit kritischer Infrastruktur in der Logistik ist hier, angelehnt an obige Definition, die Gesamtheit aller Infrastrukturen gemeint, deren Ausfall oder Beeinträchtigung erheblichen Schäden für die Logistik mit sich führt. Dies sind vor allem sämtliche kritischen Teile des Logistiknetzwerkes. Dies umfasst, anders als die reine Transportinfrastruktur als Element der (umfassenderen) logistischen Infrastruktur, sowohl Punkt-Infrastrukturen (beispielsweise Flughäfen) als auch Punkt-Netzwerk-Infrastrukturen (beispielsweise das Bahn-Netzwerk) und Netzwerk-Infrastrukturen (beispielsweise Straßennetzwerk).[18]

2.2 Risiken für kritische Infrastrukturen in der Logistik

2.2.1 PESTLE-Analyse zur Kategorisierung von Risiken

Zur Kategorisierung von externer Risiken für kritische Infrastrukturen in der Logistik bietet sich eine PESTLE-Analyse an. Das Akronym PESTLE steht hierbei für die englischen Kategorie-Begriffe „Political, Economical, Social, Technological, Legal, Ecological“. Durch den hierdurch definierten Rahmen lassen sich externe Risiken für kritische logistische Infrastrukturen entsprechend benennen und kategorisieren.

Wichtig ist zu erkennen, dass mit der PESTLE-Analyse nur externe Risiken identifiziert und kategorisiert werden. Damit sind Risiken gemeint, die von außen auf die Infrastruktur wirken. Daneben müssen jedoch auch interne Risiken betrachtet werden. Beispiele für interne Risiken werden zum Ende dieses Abschnitts exemplarisch genannt.

*2.2.2 **P:** Politische Risiken*

Jegliche Form von Infrastruktur, insbesondere auch logistische Infrastruktur, ist zahlreichen politischen Risiken ausgesetzt. Im Folgenden werden systematisch verschiedene politische Risiken für logistische Infrastrukturen und deren mögliche Auswirkung betrachtet. Zusätzlich werden entsprechende, oft historische, Beispiele aus Hessen und der Gegenwart oder der jüngeren Vergangenheit aufgeführt.

Der Begriff des politischen Risikos ist bis heute nicht scharf und konsenstauglich definiert, wird jedoch üblicherweise weiter unterteilt in „makropolitische Risiken“ und „mikropolitische Risiken“.[19]

Makropolitische Risiken sind hierbei Risiken, die nicht unmittelbar mit dem betrachteten Sektor in Verbindung stehen und neben diesem auch andere Sektoren unmittelbar betreffen. Solche makropolitischen Risiken, die direkte und schwerwiegende Auswirkungen auf die kriti-

[18] Vgl. Buhr (2009).
[19] Sottilotta (2013).

sche logistische Infrastruktur haben, sind vor allem kriegerische Handlungen. Dies umfasst wiederum zum einen Krieg im herkömmlichen Sinne als auch Guerilla-Kriege und Terrorismus.

Bei Kriegen im herkömmlichen Sinne wird die logistische Infrastruktur, insbesondere kritische logistische Infrastruktur, einerseits oft gezielt (etwa mittels Bombardements), aber auch aufgrund von Kollateralschaden zerstört oder stark eingeschränkt. Häufig sind alle Verkehrsmodi hierbei parallel betroffen. So wurden etwa in Frankfurt am Main der Osthafen, der Hauptbahnhof, der Flughafen und nahezu alle Mainbrücken während der alliierten Bombardements zum Ende des zweiten Weltkrieges zerstört.[20]

- Aktuellere Beispiele für die völlige oder teilweise Zerstörung von logistischer Infrastruktur durch kriegerische Handlung finden sich weltweit, darunter auch in Europa. So ist der Flughafen im ostukrainischen Donetsk seit dem 26.05.2014 größtenteils zerstört und bis heute stillgelegt.[21]
- Sämtliche Brücken über den Euphrat in dem gesamten Gouvernement Deir ez-Zoz im Südosten Syriens sind mittlerweile vollständig zerstört und nicht passierbar.[22] Auch der Schienenverkehr in Syrien ist aufgrund des anhaltenden Bürgerkrieges seit Jahren komplett eingestellt.[23]
- Der Hafen von Aden im Jemen, traditionell einer der wichtigsten Hochseehäfen der arabischen Welt, war monatelang nicht schiffbar, da er von sogenannten „Houthi-Rebellen“ besetzt und beschossen wurde. [24]

Auf die ausdrücklichen Aufrufe terroristischer Vereinigungen wie dem sogenannten „Islamischen Staat“ oder „Al-Qaida“, gezielt logistische Infrastruktur anzugreifen, geht der vorliegende Bericht an anderer Stelle ein, da er eine wesentliche Motivation für ein systematisches Risikomanagement für kritische Infrastrukturen in Deutschland darstellt.

Aktuelle Beispiele bestätigen eindrücklich diese Drohungen diverser Terrororganisation, sich insbesondere gegen infrastrukturelle Ziele zu wenden.[25] So betraf der Terroranschlag auf Brüssel vom 22.03.2016 gleich zwei Transportmodi direkt. Sowohl das gesamte U-Bahn-Netz der Stadt als auch der Flughafen wurden nach den Angriffen für einige Tage vollständig gesperrt.[26]

[20] Vgl. Stehen (2003).
[21] Vgl. Ukraine Today (2015).
[22] Vgl. Zaman Alwsl (2016).
[23] Vgl. New York Times (2014).
[24] Vgl. World Maritime News (2015).
[25] Vgl. dazu auch die Beispiele bei Oprach, Bovekamp (2013), S. 91-96.
[26] Vgl. CNN (2016).

Ein Anschlag auf die Brooklyn Bridge in New York war zwar bereits vollständig geplant, konnte jedoch vereitelt werden[27].

Auch maritimer Terrorismus, meist in Form von Piraterie, stellt ein ernstzunehmendes und sehr beträchtliches Risiko für die logistische Infrastruktur da. So wurde etwa der griechische Öltanker „MT Smyrni“ im Jahre 2013 erfolgreich von Piraten gekapert und erst gegen Zahlung von 9,5 Millionen US-Dollar, nach mehr als 10 Monaten in Gefangenschaft, wieder freigegeben.[28]

Ein mikropolitisches Risiko, welches meist nicht unmittelbar mit Gewalt einhergeht, wird etwa durch diplomatische Krisen realisiert. In Hessen sind solche diplomatischen Blockaden spätestens seit der Gründung eines gesamtdeutschen Staates zwar nicht mehr zu beobachten, globalpolitisch spielen sie jedoch weiterhin immer wieder eine Rolle. Da sich solche gezielten Blockaden ausschließlich auf die logistische Infrastruktur beziehen, sind sie als mikropolitische Risiken einzustufen, auch wenn sie mittelbar auch andere Wirtschaftsbereiche betreffen.

So ist etwa das größte Infrastrukturprojekt des asiatischen Kontinents der Geschichte, der „Asian Highway 1 (AH1)“ bis heute nicht vollständig befahrbar, da etwa die Landgrenze zwischen der Demokratischen Volksrepublik im Norden Koreas und der Republik im Süden der koreanischen Halbinsel bis heute nicht passierbar ist.

Auch auf der Schiene gibt es, selbst im Osten Europas, Strecken die für die Durchfahrt komplett gesperrt sind. So ist etwa der traditionell sehr wichtige Schienenkorridor Kars (Türkei–Gyumri (Armenien) – Tiflis (Georgien) aufgrund der anhaltenden Grenzschließungen zwischen der Türkei und Armenien bereits seit Juli 1993 vollständig für jeglichen Güter- und Personenverkehr gesperrt.[29]

In einigen wenigen Fällen werden selbst Flughäfen, obwohl sie meist faktisch in Betrieb sind, aus diplomatischen Gründen teilweise oder vollständig für den Flugverkehr gesperrt. So sind etwa alle Flughäfen auf der Halbinsel Krim, einst wichtige internationale Flugdrehscheiben, für den nach Selbstverständnis internationalen, also außerrussischen, Flugverkehr ebenso gesperrt wie Flughäfen in umstrittenen Gebieten wie Palästina, Zypern oder Bergkarabach.[30]

*2.2.3 **E:** Wirtschaftliche Risiken*

Logistische Infrastruktur im Besitz der öffentlichen Hand ist in der Regel gut vor wirtschaftlichen Risiken geschützt. Im Gegensatz hierzu sind die Teile der logistischen Infrastruktur, die sich teilweise oder ausschließlich in Privatbesitz befinden, immer wieder auch von wirtschaftlichen Risiken bedroht.

---

[27] Vgl. CNN (2003).
[28] Vgl. CNBC (2013).
[29] Vgl. Rail Turkey (2014).
[30] Vgl. Cyprus Mail (2013); Asbarez (2016); Daily Mail (2014).

Insbesondere sind Flughäfen oft erheblichen wirtschaftlichen Risiken ausgesetzt. Das prominenteste Beispiel der jüngeren Vergangenheit ist der Neubau des Berliner Flughafens BER, der die bisherigen drei Berliner Flughäfen teilweise ersetzen sollte. Aufgrund zahlreicher Planungs- und Managementfehler verschob sich die Eröffnung des Flughafens um mittlerweile knapp sechs Jahre.[31] Auch der hessische Flughafen Kassel-Calden ist quasi seit seiner Eröffnung im Jahre 2013 von Insolvenz bedroht.[32]

Auch im Schienenverkehr sind zahlreiche private Akteure im Besitz einzelner Infrastrukturabschnitte oder der Verkehrsmittel, die diese nutzen. Somit unterliegen auch Bahnstrecken immer wieder wirtschaftlichen Risiken. So sind auch Schienenverkehrsnetzwerke immer wieder von wirtschaftlichen Risiken bedroht. Beispielhaft ist die Bahnstrecke Weinheim-Worms zu nennen, welche aufgrund der Reorganisation von Lagerstandorten des Henkel-Konzerns heute stillsteht; Güterverkehr kann daher nicht mehr durchgeführt werden.[33]

Galt die maritime Logistik bisher als „krisensicher“ und wirtschaftlich wenig anfällig, so zeigte die Zahlungsunfähigkeit der südkoreanischen Großreederei „Hanjin Shipping“, dass wirtschaftliche Risiken sich auch auf den Güterverkehr zur See auswirken können. So stapelten sich, als Nachwirkung der Insolvenz von Hanjin, tausende Leercontainer an den Häfen in Europa und Nordamerika und verknappten so die Verfügbarkeit von entsprechenden Containern in Asien.[34] Damit wirkt ein zunächst rein betriebliches Risiko für ein einzelnes Unternehmen anschließend als betriebliches und finanzielles Risiko für Unternehmen innerhalb einer Supply Chain, durch die weiteren Interdependenzen jedoch auch als Risiko für die zugrundeliegende logistische Infrastruktur.

Seltener von wirtschaftlichen Risiken betroffen ist die logistische Straßeninfrastruktur, da diese nahezu ausschließlich, zumindest teilweise, in öffentlicher Hand ist. Vor allem innerhalb der letzten 10 Jahre gab es jedoch vermehrt Pilotprojekte, die versuchten auch Teile der logistischen Straßen-Infrastruktur vollständig zu privatisieren. Die sogenannte „Camino Columbia Toll Road“ war eine der ersten größeren komplett privat getragenen Straßenabschnitte in Nordamerika und diente nur vier Jahre nach seiner Eröffnung im Jahre 2000 bereits als Negativbeispiel für die möglichen wirtschaftlichen Risiken einer Privatstraße. Der Streckenabschnitt in Privatbesitz wurde kurz nach der Gründung der nordamerikanischen Freihandelszone an der texanisch-mexikanischen Grenze erbaut, um das antizipierte gesteigerte Handelsvolumen an der grenzübergreifenden Stadt Laredo vorbei zu leiten. Bereits 2004 musste die Inhabergesellschaft des Straßenabschnitts aufgrund ausbleibender Einnahmen Insolvenz an-

[31] Vgl. Flughafen Berlin (BER) Kosten (2017).
[32] Vgl. Frankfurter Allgemeine Zeitung (2016).
[33] Vgl. IBSE Telegramm 242 (2014), S. 2.
[34] Vgl. Port Technology (2016).

melden. In der Folge wurde der gesamte Streckenabschnitt, nach einer Zwangsversteigerung, vorübergehend für jeglichen Verkehr vollständig gesperrt.[35]

*2.2.4 **S:** Soziale Risiken*

Soziale Risiken betreffen per definitionem zunächst immer Individuen oder Gruppen von Individuen, die durch die Realisierung eines Risikos nicht (mehr) in der Lage sind, ihren sozialen Status zu erhalten. Haben Individuen selbst in der Regel nur wenig Einfluss auf die infrastrukturelle Unversehrtheit, so können soziale Risikorealisierungen Reaktionen von Einzelnen oder Gruppen hervorrufen, die die logistische Infrastruktur unmittelbar einschränken. Insbesondere rufen die Realisierungen von sozialen Risiken eine bestimmte Form von Reaktion hervor, die die logistische Infrastruktur massiv einschränkt: Streik.

Besonders logistische Dienstleistungen durch Luftfracht sind immer wieder massiv durch Streiks beeinträchtigt. So wurde im Februar 2012 der größte deutsche Flughafen in Frankfurt mehrere Tage lang bestreikt. [36] Insgesamt entstanden durch die Hunderte ausgefallener Flüge wirtschaftliche Schäden in Höhe von etwa 5,2 Millionen Euro.[37]

Im Schienengüterverkehr kam es in den letzten Jahren zu zahlreichen Streiks und Arbeitsniederlegungen, die einen wirtschaftlichen Schaden von mehreren hundert Millionen Euro verursachten.[38] Da die Grundursachen der andauernden und wiederholt auftretenden Bahnstreiks bis heute nicht beseitigt sind, ist gerade dieser Transportmodus einem vergleichsweise hohen sozialen Risiko ausgesetzt.

Schlussendlich können auch Streiks auf der Straße, insbesondere, wenn Sie durch Blockaden gestützt werden, erhebliche Folgen für die Funktionalität der Infrastruktur haben. Einer der schwerwiegendsten Streikfälle im Straßenverkehr betraf im Mai 2016 Frankreich. Tagelang blockierten Lastkraftfahrer gezielt Treibstofflager im Land. Parallel wurden auch die Häfen in Calais und Marseille bestreikt, um die Wirkung auf die gesamte Kraftstoffinfrastruktur zu erhöhen. Final führten die anhaltenden Streiks in ganz Frankreich zu Versorgungsengpässen an Tankstellen im ganzen Land.[39]

*2.2.5 **T:** Technologische Risiken*

Zu den technologischen Risiken einer logistischen Infrastruktur können sowohl operative als auch Risiken gezählt werden, die die Steuerung der Infrastruktur betreffen.

---

35 Vgl. US PIRG Education Fund (2009).
36 Vgl. Deutsche Verkehrszeitung (2012).
37 Vgl. Wirtschaftswoche (2016).
38 Vgl. Logistik Heute (2015).
39 Vgl. Südwest Presse (2016).

Operative Risiken umfassen sämtliche Risiken, die durch die Nutzung der logistischen Infrastruktur selbst hervorgerufen werden. Realisiert sich ein solches Risiko, kann (etwa durch einen Unfall) ein kurzeitiger Totalausfall von einzelnen Infrastrukturelementen die Folge sein. In Extremfällen kann jedoch schlimmstenfalls auch eine langfristige Einschränkung oder gar ein langfristiger Ausfall folgen.

Alleine innerhalb der Jahre 2015 und 2016 kam es wiederholt zu schwerwiegenden Unfällen in Hafenanlagen, die die logistische Infrastruktur direkt und nachhaltig schwächten. So waren sämtliche logistischen Aktivitäten am chinesischen Hafen Tianjin nach einer Explosion von Gefahrgut etwa zwei Wochen lang stark eingeschränkt.[40] Auch der Landeshafen Nord in Ludwigshafen, der ebenfalls von einer schweren chemischen Explosion betroffen war, musste nach dem eigentlichen Unfall noch nahezu drei Wochen lang vollständig gesperrt bleiben.[41]

Die Straßenverkehrsinfrastruktur ist insbesondere an kritischen Stellen wie Brücken oder Tunneln immer wieder langfristig durch operationelle technische Risiken beeinträchtigt. So war etwa der Mont-Blanc-Tunnel nach einem Brand, hervorgerufen durch einen entzündeten Lastkraftwagen, im Jahre 1999 über drei Jahre lang gesperrt.[42] Ebenfalls langfristige Folgen hatte ein Verkehrsunfall im baden-württembergischen Backnang: Ein Bagger verkeilte sich unter einer Eisenbahnbrücke und beeinträchtige so die Statik der Brücke nachhaltig. Voraussichtlich ein Jahr lang werden sowohl der Schienenverkehr wie auch der Straßenverkehr unterhalb der Brücke vollständig gesperrt bleiben müssen.[43]

Wie die Steuerung der Infrastruktur durch mangelhafte Planung, etwa von Wartungsarbeiten, selbst technische Risiken hervorrufen kann, hat besonders vehement die Schiersteiner Brücke bei Mainz offenbart. Durch mangelhafte Instandhaltung der Anlage und unsachgemäße Bauarbeiten sackte die Fahrbahn um nahezu 30cm ab und beeinträchtigte den gesamten Straßenverkehr in und um Mainz für Jahre negativ.[44] Aufgrund der Sperrung der Brücke in der Zeit von Februar bis April 2015 und der bis zur Wiedereröffnung um 40 Prozent reduzierten Kapazität für die Rheinquerung rechnete die IHK Frankfurt mit gesamtwirtschaftlichen Kosten von 1,4 Millionen Euro pro Tag.[45]

*2.2.6 **L:** Rechtliche Risiken*

Zu den rechtlichen Risiken zählen zum einen Risiken durch diplomatische Einschränkungen, welche oben bereits ausführlich beschrieben sind, und zum anderen nationale rechtliche Risiken, die etwa die Sperrungen von einzelnen Infrastrukturabschnitten oder ganzen Regionen

[40] Vgl. DB Schenker (2015).
[41] Vgl. Allgemeine Zeitung (2016).
[42] Vgl. Die Welt (2002).
[43] Vgl. Waiblinger Kreiszeitung (2016).
[44] Vgl. Die Welt (2015).
[45] Vgl. Industrie- und Handelskammer Wiesbaden (2015).

betreffen. Ferner führen auch rechtliche Neuerungen, die gerade abseits des Heimatlandes eines logistischen Akteurs oft unerwartet eintreffen, oft zu erheblichen infrastrukturellen Risiken.

*2.2.7 **E:** Umweltrisiken*

Risiken durch die natürliche Umwelt sind vielfältig und häufig sehr schwerwiegend für die Infrastruktur einer Region. Zu Umweltrisiken zählen sämtliche Risiken, die nicht vom Menschen unmittelbar verursacht sind. Insbesondere inkludiert diese Definition aber durchaus auch Folgen des globalen Klimawandels.

Die schwerwiegenden Naturkatastrophen der letzten Jahrzehnte haben oft einen vielfachen Effekt auf die betroffene Bevölkerung, da die humanitäre Situation sich mangels notwendiger Infrastruktur fortlaufend zuspitzt. Besonders schwerwiegende Beispiele wie das Erdbeben in Nepal 2015[46] oder der Taifun Haiyan auf den Philippinen[47] zeigen regelmäßig drastisch auf, wie wichtig ein effektiver Schutz von kritischen Infrastrukturen, auch und insbesondere im Hinblick auf Katastrophen, ist.

Andere Naturereignisse wie der Vulkanausbruch des isländischen Vulkans Eyjafjallajökull im Jahre 2013 rufen zwar keine unmittelbaren humanitären Folgen hervor, blockieren aber große Teile der Infrastruktur und bringen damit logistische Aktivitäten wie den Luftverkehr zum kompletten Stillstand.[48] Solche infrastrukturellen Naturkatastrophenrisiken treten auch in Deutschland regelmäßig auf, vor allem in Form von Hochwasser und Kleinwasser. So ist beispielsweise der Schiffverkehr auf dem Rhein, und somit auch auf dem Main, immer wieder aufgrund von Kleinwasser am Messpunkt Kaub erheblich eingeschränkt.[49]

2.3 Grundlagen des Risikomanagements

Um mit Risiken für logistische Infrastrukturen umzugehen, die Konsequenzen für logistische Prozesse und Prozessketten und damit für die Versorgung von Unternehmen und Endkunden haben können, ist ein Risikomanagement-System erforderlich. Unter Risikomanagement lassen sich – vereinfacht gesprochen –sämtliche Aktivitäten eines Unternehmens im Umgang mit Risiken zusammenfassen; dazu gehören neben der Identifikation und Bewertung von Risiken auch deren Bewältigung und Überwachung.[50]

---

[46] Vgl. The Wall Street Journal (2015).
[47] Vgl. CNN (2013).
[48] Zukunft Mobilität (2010).
[49] Interview mit Christian Eichmeier, Geschäftsführer Contargo GmbH.
[50] Vgl. Gleißner, Romeike (2015), S. 22.

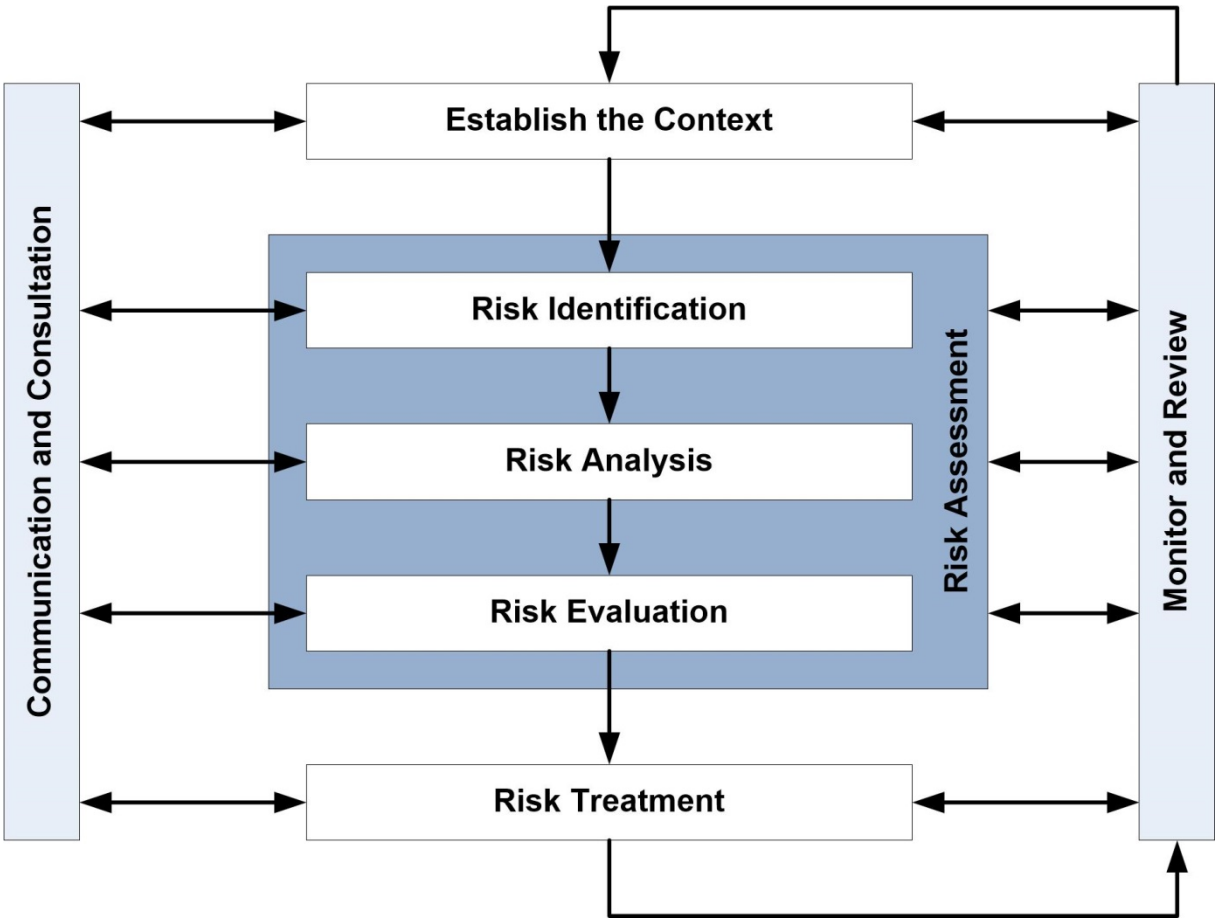


Abbildung 1: Risikomanagement-Kreislauf[51]

Risikomanagement lässt sich durch einen Kreislauf darstellen, der aus mehreren Phasen besteht. Abbildung 1 stellt diesen Kreislauf gemäß dem internationalen Risikomanagement-Standard ISO 31010 dar. Diese Phasen werden nachfolgend skizziert.

- Der Risikomanagement-Kreislauf beginnt damit, die Rahmenbedingungen für das Risikomanagement zu definieren („establish the context“). In dieser auch als „Risikomanagement-Strategie“ bezeichneten Phase wird zum einen die Einbindung des Risikomanagements in die Aufbauorganisation festgelegt, zum anderen aber auch Schwellenwerte für Risiken spezifiziert. Neben einer Definition des externen Zusammenhangs (soziale, kulturelle, politische, rechtliche, regulatorische, finanzielle, technologische, wirtschaftliche, natürliche und wettbewerbsspezifische Gegebenheiten internationaler, nationaler, regionaler oder lokaler Art) liegt ein weiterer Schwerpunkt bei der Erstellung des internen Zusammenhangs (Governance-Struktur, organisatorischer Aufbau, Rollen und Verantwortlichkeiten, Strategien, Ressourcen, Informationssysteme etc.).

[51] Quelle: ISO 31010:2009, S. 12.

- Um Risiken wirkungsvoll handhaben zu können, müssen diese bekannt sein. Die Risikoidentifikation („risk identification“) dient dazu, Risiken aufzuspüren. Hierbei sollten Risikoquellen, betroffene Bereiche, Ereignisse und Entwicklungen im Zeitverlauf berücksichtigt werden. Diese Phase führt damit zu einem qualitativen Ergebnis.
- In der Prozessphase der Risikoanalyse („risk analysis“) soll ein besseres Verständnis für ein Risiko generiert werden. Die Risikoanalyse fließt in die Risikobewertung und in Entscheidungen darüber ein, welche Strategien und Methoden der Risikobewältigung für sie am besten geeignet sind. Die Risikoanalyse betrachtet die Ursachen und Quellen der Risiken, ihre positiven und negativen Auswirkungen sowie die Wahrscheinlichkeit ihres Eintretens. Das Risiko wird durch eine Bestimmung der potenziellen Auswirkungen analysiert. Die Risikoanalyse kann je nach Risiko, Zweck der Risikoanalyse und den verfügbaren Informationen, Daten und Ressourcen mit unterschiedlicher Untersuchungstiefe durchgeführt werden. Sie kann je nach Analyseart quantitativer, semi-quantitativer oder qualitativer Natur sein oder eine Kombination davon darstellen.
- In der Risikobewertung („risk evaluation“) werden die bisher erarbeiteten, qualitativen Ergebnisse quantifiziert. Es erfolgt eine Bewertung der Risiken durch potenzielle Schäden oder Schadenszenarien und den damit verknüpften Häufigkeiten beziehungsweise Eintrittswahrscheinlichkeiten. Alle Risiken werden idealerweise mit geeigneten Verteilungsfunktionen beschrieben. Mit Hilfe geeigneter Methoden, beispielsweise einer Sensitivitätsanalyse, lassen sich die Risiken hinsichtlich Relevanz priorisieren. Diese Phasen der Risikoidentifikation, Risikoanalyse und Risikobewertung werden auch als Risikoabschätzung („risk assessment“) bezeichnet. Die Risikoabschätzung bildet den Untersuchungsgegenstand des Forschungsvorhabens „RIMA-KIL“.
- Die im Rahmen der Risikoabschätzung erarbeiteten Informationen, vor allem die bewerteten und priorisierten Risiken, dienen anschließend als Grundlage für die Risikosteuerung („risk treatment“ beziehungsweise „risk mitigation“). Für die Risikosteuerung, das heißt die Handhabung der identifizierten Risiken, bieten sich mehrere Typen risikopolitischer Maßnahmen an (siehe nachfolgende Abbildung 2 unten).
- Die beschriebenen Phasen des Risikomanagement-Kreislaufs werden parallel kontinuierlich überwacht. Durch diese Risikoüberwachung („monitor and review“) wird sichergestellt, dass die Risikomanagement-Phasen korrekt durchgeführt werden, dass die risikopolitischen Maßnahmen richtig umgesetzt werden und die beabsichtigte Wirkung entfalten.
- Parallel zu den Risikomanagement-Phasen ist es sinnvoll, eine effektive Risikokommunikation („communication and consultation“) zu etablieren. Insbesondere die Kommunikation unterstützt Unternehmen beim Aufbau beziehungsweise der Weiterentwicklung einer „gelebten“ Risikokultur.

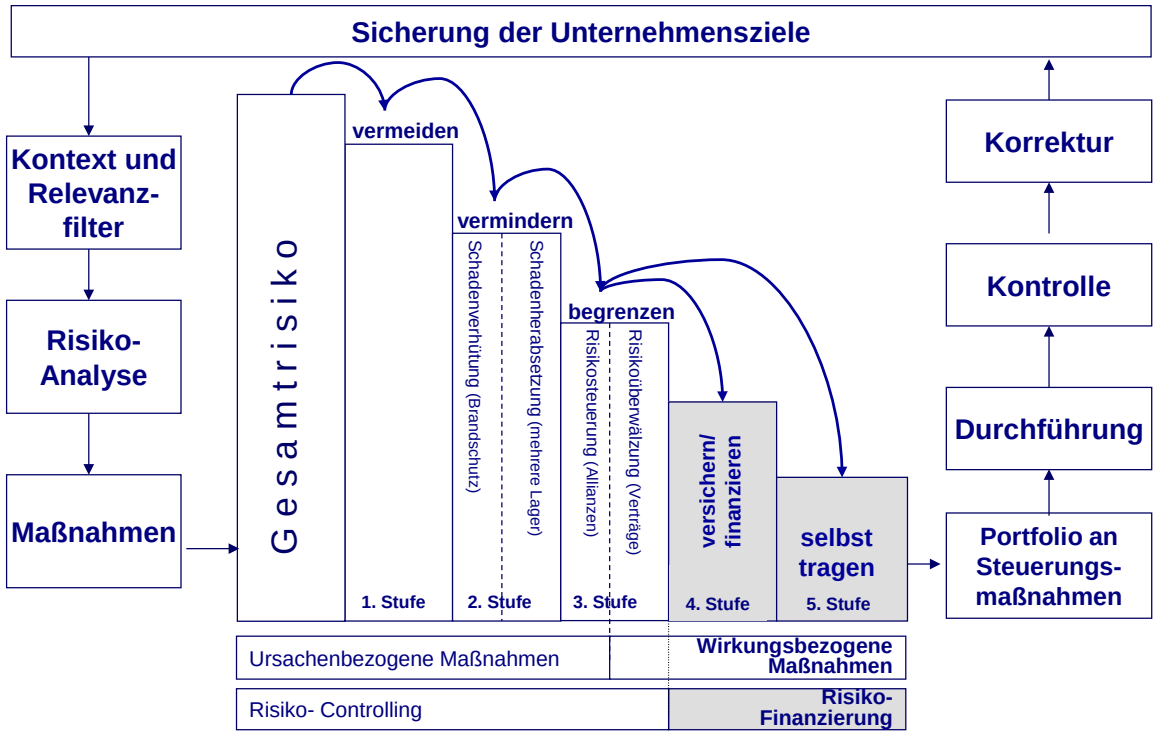


Abbildung 2: Maßnahmen der Risikosteuerung[52]

2.4 Internationale Ansätze zur Identifikation und Bewertung von Risiken für kritische Infrastrukturen in der Logistik

2.4.1 Schutz kritischer Infrastrukturen – politische Ansätze

Wie in Abschnitt 2.1 bereits angedeutet, findet sich Begriff „kritische Infrastrukturen in der Logistik“ bisher kaum Beachtung in der Literatur. Entsprechend sind bisher keinerlei Publikationen erschienen, die sich dem Risikomanagement ebendieser explizit und ausschließlich widmen. Bisherige Literatur und bisherige Ansätze widmen sich bisher vielmehr entweder dem Schutz kritischer Infrastrukturen allgemein oder der Resilienz einer logistischen, aber nicht zwingend kritischen Infrastruktur. Zu beiden Themenkomplexen finden sich zahlreiche politische Strategiepapiere und wissenschaftliche Ansätze, welche im Folgenden zusammengefasst werden.

Das Risikomanagement für kritische Infrastrukturen, insbesondere der logistischen kritischen Infrastruktur, hat seinen konzeptionellen Ursprung in den USA und lässt sich allgemein in drei Phasen einteilen.

In einer ersten Phase führte Präsident Clinton den Begriff „kritische Infrastruktur“ 1996 erstmals formal ein, als er die „Commission on Critical Infrastructure Protection“ gründete, die fortan einen Rahmen für ein Risikomanagement für kritische Infrastrukturen definieren soll-

[52] Quelle: Romeike, Hager (2013), S. 140.

te.[53] Ferner machte der erste Bericht der Kommission erstmals öffentlich auf die Wichtigkeit nationaler Infrastrukturen für den Wohlstand und die Lebensqualität der Amerikaner aufmerksam. Andere nationale Regierungen und internationale Organisation adaptieren den Begriff in dieser ersten systematischen Phase jedoch nicht. Die Weisungen der Kommission und die mediale Wahrnehmung zu dieser Zeit fokussierte meist auf die Sicherung lokaler Infrastruktur und die Ermittlung von Kritikalitäten einzelner Verbindungen innerhalb von Infrastrukturnetzwerken. Die überwiegend betrachteten Risiken bezogen sich daher meist auf Umwelteinflüsse, operationelle Risiken und technologische Risiken.

Die Terroranschläge auf das World Trade Center und das Pentagon am 11. September 2001 rückten die Sicherung der Infrastruktur schlagartig in den Fokus der internationalen und nationalen Politik, vor allem in Nordamerika und Westeuropa. In der folgenden zweiten Phase bezogen sich nahezu alle institutionellen Publikationen und Studien ausschließlich auf das bis dato nahezu unberücksichtigte Risiko durch terroristische Angriffe. Die veränderte Wahrnehmung der Problematik beschreibt etwa Collier (2008) ausführlich am Beispiel der Vereinigten Staaten von Amerika.[54] Den US-amerikanischen Entwicklungen folgend, bildeten in den Folgejahren auch die Vereinten Nationen[55], das Vereinigte Königreich[56], die Europäische Union[57] und andere politische Akteure Institutionen, die sich dem Risikomanagement für kritische Infrastrukturen widmen. Obwohl die meisten dieser institutionellen Einrichtungen hauptsächlich im Hinblick auf terroristische Bedrohungen gegründet wurden, definieren Sie nahezu ausnahmslos ein umfassendes Risikomanagement kritischer Infrastrukturen als Ziel.

Eine dritte Phase des Risikomanagements für kritische Infrastrukturen wurde 2007 durch den „Web War I", einem großangelegten Hacker-Angriff auf sämtliche Internetdienste Estlands, ausgelöst.[58] Die andauernden Attacken führten dazu, dass sämtliche Online-Dienste für etwa eine Woche vollständig offline waren und nur regeneriert werden konnten, indem Estland seine gesamte IT-Infrastruktur für einen Monat von allen internationalen Servern trennte.[59] Als institutionelle Reaktion auf den „Web War I" beschloss die NATO zunächst im April 2008 erstmals eine „Policy of Cyber Defense" und gründete kurz darauf im August 2008 ein Cyberabwehrzentrum (NATO Cooperative Cyber Defence Centre of Excellence).[60] Durch weitere „Cyberangriffe" auf die ehemaligen Sowjetstaaten Litauen 2008, Georgien 2008 und Kasachstan 2009, die allesamt international der Russischen Föderation angelastet wurden,

---

53 Vgl. President's Commission on Critical Infrastructure Protection (1997).
54 Vgl. Collier (2008).
55 2005 gründete der Generalsekretär der Vereinten Nationen das „Counter-Terrorism Implementation Task Force" (CTITF) Büro, dem auch die Arbeitsgruppe „Protection of Critical Infrastructure including vulnerable targets, internet and tourism security" unterstellt ist.
56 2007 gründete das Vereinigte Königreich das „Centre fort he Protection of National Infrastructure (CPNI).
57 2004 gründete die Europäische Union das gemeinsame „European Programme for Critical Infrastructure Protection (EPCIP).
58 Vgl. The Economist (2010).
59 Vgl. Jackson (2013).
60 Vgl. Herzog (2011).

rückte der Themenkomplex „Cybersecurity“ immer mehr in den Fokus der NATO-Bündnispartner und wurde schließlich durch eine Ministerialkonferenz zum Thema „kritische Infrastrukturen und Cybersecurity“ im April 2009 vollständig mit dem Themenkomplex des Schutzes kritischer Infrastrukturen verwoben.[61] Aufgrund der wahrgenommen verminderten Gefahr durch Terror und die ab 2007/2008 wahrgenommen gesteigerte Gefahr durch Angriffe auf die kritische Informationsinfrastruktur, fokussierte sich so die institutionelle Arbeit zum Schutz kritischer Infrastrukturen im Anschluss überwiegend auf den Schutz ebendieser kritischen Infrastruktur.

Aktuelle Entwicklung, insbesondere die Gründung und die Aktivitäten des sogenannten „Islamischen Staates“, fokussieren jedoch die Bemühungen der internationalen Gemeinschaft wieder vermehrt auf ein Risikomanagement bezüglich terroristischer Bedrohungen.[62]

Der Großteil der obigen Ausführung betrachtet die Geschichte des Risikomanagements ausdrücklich aus „westlicher Sicht“ und untersucht hauptsächlich die institutionelle Entwicklung des Schutzes kritischer Infrastrukturen in den USA, in Kanada und in Europa. In anderen Teilen der Welt lässt sich die obige Einteilung in Phasen oft nicht übertragen. So hat etwa die Volksrepublik China bis heute keine offizielle Definition für den Begriff der kritischen Infrastruktur festgelegt und entsprechend keine institutionelle Einrichtung, die sich gezielt mit deren Schutz auseinandersetzt.[63] Andere Staaten bzw. autonome Überseegebiete wie die britischen Jungferninseln[64], fokussieren beim Schutz kritischer Infrastrukturen ausschließlich auf Risiken, die das entsprechende Staatsgebiet besonders bedrohen. Im Fall der britischen Jungferninseln bezieht sich der Schutz kritischer Infrastrukturen allein auf Risiken durch Klimakatastrophen, insbesondere durch Hurrikans.

2.4.2 Schutz kritischer Infrastrukturen – wissenschaftliche Ansätze

Der vermutlich erste Ansatz zum Schutz bzw. zur Zerstörung, einer kritischen Infrastruktur stammt aus dem US-Amerikanischen Thinktank „RAND Corporation“, welcher in den 1950er Jahren nahezu ausschließlich Auftragsforschung für die US Navy durchführte. Der Mathematiker T. E. Harris formulierte, gemeinsam mit dem General a. D. F. S. Ross dort bereits im Jahr 1955[65] erstmals das sogenannte „Maximum Flow Problem“, ein seither klassisches kombinatorisches Optimierungsproblem.

Dieses Problem wird angewandt, um den maximalen eindimensionalen (Waren-) Fluss innerhalb eines Netzwerkes zu bestimmen. Gemeinsam mit zwei anderen Mitarbeitern der RAND Corporation, L. R. Ford jr. und D. R. Fulkerson, entwickelte Harris nicht nur ein effizientes,

[61] Vgl. Bumgarner, Borg (2009).
[62] Vgl. Stock (2017).
[63] Vgl. CIPedia.
[64] Vgl. Penn (2010). S. 52.
[65] Harris, Ross (1955).

exaktes Lösungsverfahren für das Problem, sondern entdeckte und bewies auch das sogenannte „Max-Flow-Min-Cut-Theorem“, welches im Wesentlichen besagt, dass der maximale Fluss in einem Netzwerk genau denselben Wert hat, wie ein minimaler Schnitt eines solchen Netzwerkes. Spätestens, seitdem das erwähnte Paper von Harris und Ross im Jahr 1999 öffentlich freigegeben wurde, wird ersichtlich, inwiefern dieser Zusammenhang für die Autoren eine entscheidende Rolle spielt und welche Motivation diese Forschung vorantrieb. Als „Fallbeispiel“ betrachteten Harris und Ross das Schienennetz der damaligen Sowjetunion und berechneten explizit den maximal möglichen Fluss von Material aus dem Fernen Osten der Sowjetunion in die osteuropäischen Regionen und Satellitenstaaten. Ferner beobachteten die Autoren, dass es einen minimalen Schnitt mit demselben Wert gäbe, und gaben einen Leitfaden an, wie Militärstrategen diesen für ein beliebiges Netzwerk ermitteln könnten. Gemeinsam mit der einführenden Bemerkung, dass „Luftschläge eine effektive Möglichkeit sind, ein Schienennetzwerk lahmzulegen und Truppenverlegungen so zu verhindern“, kommt man heute zu dem Schluss, dass die Auftragsforschung für die US Air Force eine erste Studie zur Aufdeckung von kritischen Infrastrukturen war.[66]

Die frühen Forschungsergebnisse der RAND Corporation begründeten einen kompletten Forschungszweig, der sich am besten als „Suche nach der oder den kritischsten Kanten“ beschreiben lässt. Da eine solche Kritikalitätsbewertung vor allem auch im militärischen Anwendungsbereich, sowohl für gezielte Angriffe als auch zur effektiven Abwehr, relevant ist, wurde die Suche nach kritischen Komponenten vor allem in den Jahrzehnten des kalten Krieges ständig vorangetrieben.[67]

In der Zeit unmittelbar nach dem Ende des kalten Krieges änderten sich die Diktion und der Anwendungsbezug des Forschungsgebietes schlagartig. Von nun an wurde die Suche nach kritischen Komponenten eines Netzwerks vorerst auf rein theoretischer Ebene fortgeführt und die Problematik wurde entsprechend von Wood (1993) als „Network Interdiction Problem“ formal definiert. Erwähnenswerte Beiträge zu diesem Forschungskomplex finden sich ferner etwa bei Washburn und Wood (1995), die erstmals einen Bezug zur Spieltheorie lieferten, bei Cormican et al (1998), die erstmals stochastische Netzwerkstörungen betrachteten, bei Israeli und Wood (2002), die sich mit dem Einfluss von Störungen eines Netzwerkes auf die Lösungen eines kürzeste-Wege-Problems beschäftigten, oder bei Lim und Smith (2007), die sich mit Multicommodity-Fluss-Netzwerken auseinandersetzten.

Innerhalb des letzten Jahrzehnts, ausgelöst durch die gesteigerte politische Aufmerksamkeit, fokussierte sich die Suche nach kritischen Komponenten innerhalb eines Netzwerks dann schlussendlich ausschließlich auf Forschungsbeiträge zum Themenkomplex „kritische Infra-

[66] Vgl. Schrijver (2002), S. 166-169.

[67] Beispiele hierzu finden sich etwa innerhalb des RAND Corporation Think Tanks bei Wollmer (1963), Wollmer (1964), Wollmer (1968) und Fulkerson und Harding (1977), aber erstmals auch außerhalb des Think Tanks, etwa bei Lubore et al (1971), McMasters und Mastin (1970), Ratliff et al (1975), Corley und Chang (1974), Golden (1977), Corley und Sha (1982), Malik et al (1989) und Ball et al (1989).

strukturen“. Den Zusammenhang stellte erstmals Brown et al (2005) und (2006) her. Parallel beschäftigten sich etwa Salmerón et al (2004) und (2009) mit der Suche nach kritischen Komponenten zum Schutz der Energieinfrastruktur. Church und Scaparra (2006) und Scaparra und Church (2008) nutzen dieselben theoretischen Grundlagen um die Kritikalität einzelner Netzwerkkomponenten beim Bau einer neuen Einrichtung einzubeziehen. Weitere Publikationen bezogen sich auf die Kritikalität einzelner Komponenten von Supply Chain Netzwerken, etwa Snyder et al (2006), oder von Telekommunikationssystem, etwa Murray et al (2007). Schlussendlich publizierten Alderson et al (2011) auch erstmals Forschungsergebnisse, die gezielt das Auffinden von kritischen Infrastrukturen innerhalb eines Transportnetzwerkes zum Ziel hatte.

Neben der oben ausführlich beschriebenen überwiegend analytischen Forschung zum Thema kritische Infrastrukturen lassen sich vor allem auch Publikationen aus dem Bereich Risikomanagement selbst dem Themenkomplex „Risikomanagement für kritische Infrastrukturen“ zuschreiben. So schlugen etwa Sarpori et al (2011) ein allgemeines analytisches Vorgehen zum Risikomanagement für kritische Infrastrukturen vor, während Avritzer et al (2014) sehr generisch die Herausforderungen und auch Grenzen des systematischen Risikomanagements für kritische Infrastrukturen aufzeigen.

Hierbei fokussieren sich die allermeisten Beiträge vor allem auf einen konkreten Anwendungsbereich für eine spezielle kritische Infrastruktur. So schlagen Ezell et al (2000) ein generelles Risikomanagement-Framework für Infrastrukturen vor und beziehen sich dabei insbesondere auf die Wasserversorgungsinfrastruktur. Kleiner et al (2006a) und Kleiner et al (2006b) entwickelten eine Risikomanagement-Methode, basierend auf der hier später erläuterten Markov-Methode, die speziell ein Risikomanagement für unterirdische Infrastrukturen, die üblicherweise ein sehr geringeres Ausfallrisiko und drastische Folgen im Falle eines Ausfalles als Charakteristika ausweisen, betreiben.

Ein weiteres intensiv bearbeitetes Forschungsthema beschäftigt sich mit den zahlreichen Interdependenzen zwischen verschiedenen Infrastrukturen. Seit etwa 2000[68] fokussieren sich so zahlreiche Forschungen darauf, Zusammenhänge zwischen verschiedenen kritischen Infrastrukturen aufzudecken, zu modellieren und meist zu simulieren. Diese Analysen und Simulationen, in der Regel beauftragt, gesteuert und finanziert durch nationale Regierungen, dienen häufig nationalen Sicherheitsbehörden zur systematischen Analyse und Beobachtung der aktuellen Gefährdungslage. Ein ausführlicher Überblick über vorhandene Simulationen findet sich etwa bei Pederson et al (2006).

Adar und Wuchner (2005) publizierten einen kurzen Überblick über den aktuellen Stand des Risikomanagements für kritische Infrastrukturen aus Sicht der unternehmerischen Praxis. Sie wiesen insbesondere intensiv darauf hin, dass ein umfassendes Risikomanagement für kriti-

[68] Vgl. Pederson et al. (2006). S. 2.

sche Infrastrukturen zentrale Wichtigkeit für Unternehmen wie staatliche Akteure besitzt, und forderten in der Folge dazu auf, ein nachhaltiges Risikomanagement-Framework zu entwickeln.

In nahezu allen zuvor genannten Forschungsgebieten geht es vor allem um eine betriebswirtschaftliche Sicht auf Risiken und das Risikomanagement selbst. Dies meint, dass vor allem die wirtschaftlichen Konsequenzen einer Risikorealisierung identifiziert, analysiert und bewertet werden. Gerade ein Risikomanagement kritischer logistischer Infrastrukturen hat jedoch immer auch einen großen sozialen Zweck, da nur durch ein präventives Risikomanagement für alle Transportnetzwerke sichergestellt werden kann, dass Risiken bekannt sind und entsprechend langfristig bekämpft werden können. Dies führt, neben wirtschaftlicher Sicherheit, unmittelbar auch zu einer verstärkten Resilienz der entsprechenden Infrastruktur und damit zu einer verbesserten Versorgung der Zivilbevölkerung. Ein spezialisiertes Konzept, im Wesentlichen vorangetrieben von der Weltbank, welches sich ausschließlich auf die Verminderung sozialen Leids durch ein nachhaltiges Risikomanagement bezieht, ist das sogenannte „Social Risk Management“, welches von Holtmann et al (2001) und Holzmann et al (2003) ausführlich beschrieben und von Godfrey et al (2009) kritisch hinterfragt wurde.

Schlussendlich können auch zwei vielbeachtete Publikationen über die wissenschaftliche Fokussierung des Risikomanagements für kritische Infrastrukturen nicht ignoriert werden. So ruft Cardona (2004) explizit dazu auf, das Risikomanagement für kritische Infrastrukturen holistisch zu betrachten und die verschiedenen Forschungsströmungen, die oft wenig kooperieren, zu vereinen und so eine interdisziplinäre Forschung, an der Schnittstelle zwischen Risikomanagement, Netzwerktheorie, Sozialwissenschaften und Sicherheitsforschung zu ermöglichen. Boin und McConnell (2007) zeigen schlussendlich die Grenzen des Risikomanagements für kritische Infrastrukturen auf und schlagen explizit die Brücke zum Themenkomplex Resilience Management, der sich damit befasst wie eine Infrastruktur sich möglichst schnell und verlustarm von einer Risikorealisierung erholen kann.

3 Einsatzpotenzial von Methoden der Risikoidentifikation, Risikoanalyse und Risikobewertung für kritische Infrastrukturen in der Logistik

3.1 Übersicht über Methoden der Risikoidentifikation, Risikoanalyse und Risikobewertung

Wie im vorherigen Kapitel dargestellt, sind Risikoidentifikation, Risikoanalyse und Risikobewertung drei wesentliche Phasen im Risikomanagement. Die Ergebnisqualität dieser drei Phasen beeinflusst maßgeblich eine zielgerichtete und effektive Risikosteuerung. Anders herum besteht die Gefahr, bei einem geringen oder fehlerhaften Methodeneinsatz oder einer niedrigen Datenqualität Ergebnisse zu erhalten, die zu einer falschen Priorisierung der Risiken oder zu falschen oder ineffizienten Maßnahmen zur Risikosteuerung führen.

Vor diesem Hintergrund ist es wichtig, dass Entscheidungsträger eine umfangreiche Methoden-Kompetenz entwickeln, um für bestimmte Fragestellungen im Risikomanagement die jeweils adäquate Methode auszuwählen und einzusetzen. Die Projektergebnisse tragen dazu bei, eine derartige Methoden-Kompetenz aufzubauen.

Die Methoden zur Risikoidentifikation, Risikoanalyse und Risikobewertung lassen sich in Kollektionsmethoden sowie Suchmethoden unterteilen (vgl. Tabelle 2).[69] Kollektionsmethoden sind vornehmlich für Risiken geeignet, die offensichtlich oder bereits bekannt sind (bspw. aufgrund einer bereits früher durchgeführten Risikoidentifikation). In der Praxis erfolgt die Identifikation von Risiken häufig unter Verwendung von Checklisten. Sie lassen sich relativ einfach aus einem bestehenden Risikoinventar extrahieren, dienen jedoch allenfalls als Ausgangspunkt für die Risikoidentifikation.[70]

Auch die SWOT-Analyse dient im Wesentlichen einer strukturierten Darstellung beziehungsweise Zusammenfassung von Ergebnissen, die mit Hilfe anderer Methoden (etwa Brainstorming) erfasst wurden. Auch eine Risiko-Identifikationsmatrix oder ein Self-Assessment unterstützt im Kern die Identifikation offensichtlicher Risiken.

Suchmethoden dagegen lassen sich vor allem für bisher unbekannte Risiken einsetzen. Die Suchmethoden können in analytische Methoden und Kreativitätsmethoden klassifiziert werden. Alle analytischen Suchverfahren sind darauf fokussiert, zukünftige und bisher unbekannte Risikopotenziale zu identifizieren.[71] Einige analytische Suchverfahren wurden ursprünglich für das Qualitätsmanagement entwickelt. Da die Prozessstruktur und Methodik des Risikomanagements einige Parallelen zum Qualitätsmanagement aufweist, liegt es nahe, etablierte Methoden auch auf den Risikoidentifikationsprozess zu übertragen.

---

[69] Vgl. Romeike, Hager (2013), S. 104.
[70] Vgl. Huth, Romeike (2016), S. 74.
[71] Vgl. Romeike, Hager (2013), S. 107 sowie Huth, Romeike (2016), S. 75.

Kreativitätsmethoden hingegen basieren auf kreativen Prozessen, die durch divergentes Denken charakterisiert sind, um relativ flüssig und flexibel zu neuartigen Einfällen und originellen Lösungen zu gelangen. Kreativitätstechniken lassen – im Gegensatz zum rationalen und strukturierten Denken – das Denken chaotisch werden und ermöglichen so vor allem die Identifikation bisher unbekannter Risikopotenziale.

Kollektionsmethoden	**Suchmethoden**	
	Analytische Methoden	**Kreativitätsmethoden**
• Checkliste • Risiko-Identifikations-Matrix (RIM) • Interview, Befragung	• Bow-tie Analysis • Empirische Datenanalyse • Fehlerbaumanalyse (Fault Tree Analysis, FTA) • Fehlermöglichkeits- und Einflussanalyse (FMEA) • Hazard and Operability Study (HAZOP) • Business Impact Analysis (BIA) • Fehler-Ursachen-Analyse • Ishikawa-Diagramm • Ereignisbaumanalyse (Event Tree Analysis) • Markov Analysis • Social Network Analysis	• Morphologische Verfahren • Brainstorming • Brainwriting • Methode 635 • Mind Mapping • KJ-Methode • Flip-Flop-Technik (Kopfstandtechnik) • World-Café • Delphi-Methode • Deterministische Szenarioanalyse • Stochastische Szenarioanalyse

Tabelle 2: Methoden der Risikoidentifikation, -analyse und -bewertung[72]

Tabelle 2 gibt eine Übersicht über Methoden der Risikoidentifikation, -analyse und -bewertung. Diese werden im folgenden Abschnitt dargestellt, erläutert und hinsichtlich ihres Einsatzpotenzials bewertet. Jede Methode wird einheitlich dargestellt. Dabei werden neben einer Beschreibung der Methode und einem Anwendungsbeispiel folgende Eigenschaften verwendet:

- Einsatzzweck,
- Phase des Risikomanagements, in der die Methode eingesetzt werden kann,
- Input bzw. Datenbedarf,
- Output,

[72] Quelle: Eigene Darstellung in Anlehnung an Romeike, Hager (2013), S. 104.

- zeitlicher Aufwand für den Methodeneinsatz,
- personeller Aufwand für den Methodeneinsatz (insbesondere auch benötige Qualifikation),
- Reifegrad des zugrundeliegenden Risikomanagements,
- Stärken und Schwächen der Methode,
- Gesamtbewertung (Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik).

3.2 Abschätzung des Einsatzpotenzials von Methoden der Risikoidentifikation und -bewertung

3.2.1 Kollektionsmethoden

3.2.1.1 Checkliste

3.2.1.1.1 Beschreibung

Eine Checkliste ist eine einfach anzuwendende Methode, um eine Vollständigkeitskontrolle (und damit eine Verifizierung) durchzuführen. Der eigentliche kollektivistische Charakter der Methode besteht in der Erarbeitung der Checkliste selbst. Eine Checkliste listet hierbei (möglichst vollständig) Risiken systematisch auf und ermöglicht es so, einem sachkundigen Experten schnell und übersichtlich die Präsenz von Risiken zu überprüfen.

Besonders attraktiv an der Checkliste ist die Möglichkeit der Wiederverwendung und der stetigen Weiterentwicklung. So können neue Risiken leicht und schnell einer Checkliste hinzugefügt werden und die Checkliste selbst kann regelmäßig durchgegangen werden.

Eine Checkliste kann niemals vollständig sein. Die stochastische und unerwartete Natur eines möglichen negativen Ereignisses in der Zukunft verbietet per definitionem eine vollständige Auflistung aller solcher Ereignisse.

Die Gefahr einer Checkliste ist die vermeintliche Vollständigkeit der Risiken. Wenn der Blick nur auf die Checkliste gerichtet ist, kann damit kann die Motivation eingeschränkt werden, bisher unbekannte Risiken zu identifizieren.

3.2.1.1.2 Phase

☒ Risikoidentifikation

☐ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.1.1.3 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

3.2.1.1.4 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

3.2.1.1.5 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Initial entstehtein hoher Aufwand bei der Erstellung einer Checkliste. Durch die ständige Wiederholbarkeit kann jedoch der Gesamtaufwand pro Durchführung als äußerst niedrig bewertet werden.

3.2.1.1.6 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Zur Erstellung der Checkliste wird weitreichendes Know-how benötigt. Da in der Regel Checklisten fortwährend weiterentwickelt werden und sämtliche Akteure die Möglichkeit erhalten selbst Punkte hinzuzufügen, ist der personelle Aufwand pro Zeiteinheit sehr gering. Die wiederkehrende Überprüfung der Risiken, welche auf der Checkliste aufgeführt werden, erfolgt in der Regel zwar zeitsparend, beansprucht aber durchaus qualifiziertes Fachpersonal.

3.2.1.1.7 Reifegrad des zugrundeliegenden Risikomanagements

☒ Initial

☒ Basic

☐ Evolved

☐ Advanced

☐ Leading

3.2.1.1.8 Stärken und Schwächen

Stärken	Schwächen
• Strukturiertes Verfahren • Lässt sich zeit- und kosteneffizient wiederholt anwenden	• Wird oft statisch verwendet und nicht aktualisiert • Verringert das Bewusstsein für nicht in der Checklist gelistete Risiken • Reduziert die Kreativität der Risikoeigentümer

Tabelle 3: Stärken und Schwächen einer Checklist

3.2.1.1.9 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☐ sehr gut

☒ gut

☐ weniger geeignet

Begründung: Viele Risiken, wie etwa Risiken durch Naturkatastrophen, lassen sich schnell und einfach regelmäßig mit Hilfe einer Checkliste, ggf. unter Hinzuziehung von externen Daten wie etwa Wettervorhersagen oder seismischer Prognosen, durchführen. Nichtantizipierbare, spontane Risiken wie etwa terroristische Angriffe lassen sich durch Checklisten hingegen grundsätzlich nicht aufdecken und werden so systematisch unterschätzt bzw. vernachlässigt.

3.2.1.2 Risikoidentifikations-Matrix (RIM)

3.2.1.2.1 Beschreibung

Eine Risikoidentifikations-matrix (RIM) – nicht zu verwechseln mit einer Risikomatrix oder Risk Map – ist ein einfach anzuwendendes Verfahren, um Risiken zeit- und ressourceneffizient zu sammeln und grob zu bewerten. In einer Risikoidentifikations-Matrix werden die Risikoursachen (Treiber) mit den Auswirkungen in Verbindung gebracht (beispielsweise mit

Scorewerten von 0 = niedrig bis 10 sehr hoch), siehe Tabelle 4. Alle Risikotreiber oder -ursachen (causes) werden horizontal in der Matrix abgebildet. Alle (Risiko-) Wirkungen (effects) werden vertikal in der Matrix abgebildet.

Bspw. Produkt Z		Risikoursachen / Risikotreiber					
		Mensch	Techno-logie	Methode	Material	Organisa-tion	…
Auswirkungen eines Risikoeintritts	Umwelt	4	3	3	0	3	…
	Kunde	3	9	2	5	4	…
	Mitarbeiter	3	3	4	2	2	…
	Finanzen	6	0	5	5	7	…
	…	…	…	…	…	…	…

Tabelle 4: Beispiel Risikoidentifikations-Matrix

Die exemplarische Risikoidentifikations-Matrix zeigt, dass bei den Verbindungen Mensch/Finanzen, Technologie/Kunde sowie Organisation/Finanzen hohe Risiken (hohe Scorewerte) vorliegen. Daher sollten vor allem die Ursachen bzw. Risikotreiber Mensch (auf Finanzen), Technologie (auf Kunde) sowie Organisation (auf Finanzen) reduziert bzw. aktiv gemanagt werden.

3.2.1.2.2 Phase

☒ Risikoidentifikation

☐ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.1.2.3 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

3.2.1.2.4 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

3.2.1.2.5 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

3.2.1.2.6 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☒ niedrig

☒ mittel

☐ hoch

Begründung: Die Aussagekraft einer RIM steht in enger Relation zu der Qualifikation des Konsortiums, welche diese erstellt.

3.2.1.2.7 Reifegrad des zugrundeliegenden Risikomanagements

☒ Initial

☐ Basic

☐ Evolved

☐ Advanced

☐ Leading

3.2.1.2.8 Stärken und Schwächen

Stärken	Schwächen
• Einfache und schnelle Möglichkeit in der Nutzung und zur Identifizierung von Risiken. • Relativ geringer Aufwand.	• Stark reduzierte (fast triviale) Beschreibung von Abhängigkeiten zwischen Ursachen und Wirkungen. • Kreativität wird nicht gefördert, son-

Stärken	Schwächen
	dern tendenziell eher unterdrückt. • (Komplexe) Ursachen- bzw. Wirkungsketten – die in der Praxis regelmäßig existieren – können nicht abgebildet werden.

Tabelle 5: Stärken und Schwächen der Risiko-Identifikationsmatrix

3.2.1.2.9 Gesamtbewertung/Eignung für das Risikomanagement

☐ sehr gut

☒ gut

☒ weniger geeignet

3.2.1.3 Interview, Befragung

3.2.1.3.1 Beschreibung

Ein Interview dient häufig als eine vorgelagerte Stufe des Risikomanagements, vor allem in komplexen Umfeldern. So kann eine Expertenbefragung wichtige Denkanstöße liefern, die bisher nicht betrachtete Risiken in das künftige Risikomanagement einfließen lassen.

Vor allem bei Kollektionsmethoden ist es grundsätzlich ratsam, verschiedene Experten intern und extern zu interviewen, um möglichst breite Erkenntnisse über potenzielle Risiken zu erhalten.

3.2.1.3.2 Phase

☒ Risikoidentifikation

☐ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.1.3.3 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

3.2.1.3.4 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

3.2.1.3.5 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

3.2.1.3.6 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

3.2.1.3.7 Reifegrad des zugrundeliegenden Risikomanagements

☒ Initial

☐ Basic

☐ Evolved

☐ Advanced

☐ Leading

3.2.1.3.8 Stärken und Schwächen

Stärken	Schwächen
• Kosten- und zeiteffizient • Nutzt vorhandenes Know-how, um bekannte Risiken zu erfassen	• Basiert auf dem Wissen einzelner Experten • Bisher unbekannte Risiken werden ggf. nicht identifiziert

Tabelle 6: Stärken und Schwächen eines Interviews

3.2.1.3.9 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☐ sehr gut

☒ gut

☐ weniger geeignet

Begründung: Gerade bei unübersichtlichen und komplexen Systemen wie Infrastrukturen ist es häufig aufwändig, einzelne Schwachpunkte und Risiken zu benennen. Dies gilt jedoch oft nicht für Experten, die quasi täglich mit der entsprechenden Infrastruktur befasst sind. Insofern ist ein Interview eine effektive und zeitsparende Methode, um potenzielle Risiken zu erkennen.

3.2.2 Analytische Methoden

3.2.2.1 Bow-tie Analysis

3.2.2.1.1 Einsatzzweck

Die Bow-tie Analysis wird dazu verwendet, ein Risiko sowie dessen Ursachen und Wirkungen zu identifizieren und in einem einzigen Diagramm strukturiert darzustellen. Da ein Risiko in der Regel eine Vielzahl von Ursachen, aber auch Wirkungen aufweist, hat das Diagramm die Form einer Fliege (im Englischen: bow-tie, siehe Abbildung 3).

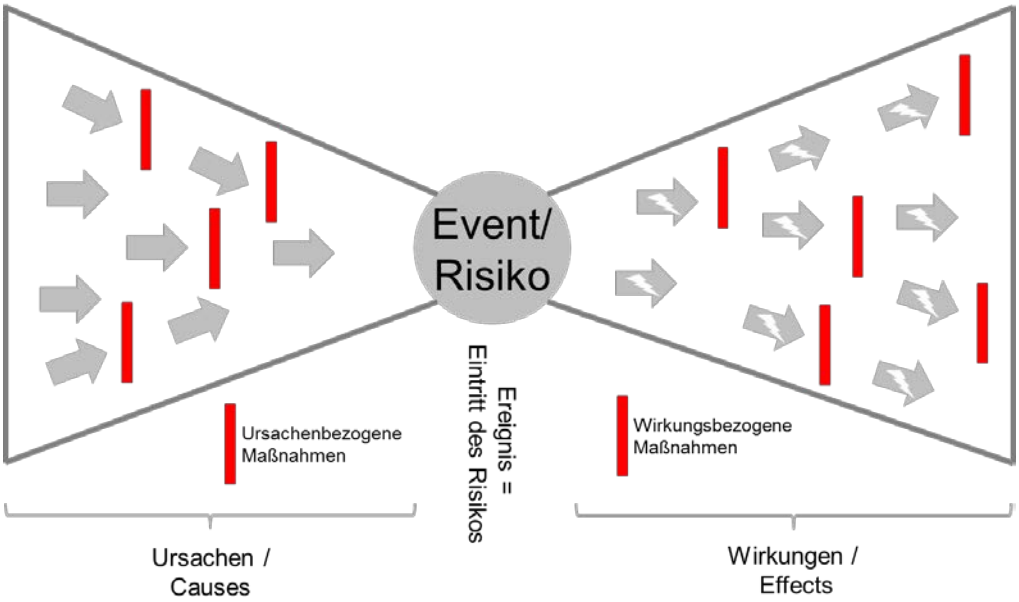


Abbildung 3 Risikomanagement-Rahmen für die Anwendung der Bow-tie Analysis[73]

[73] Quelle: Romeike, Spitzner (2015), S. 134.

Es unterstützt damit die Risikoidentifikation, aber auch die Risikokommunikation und die Entwicklung von Maßnahmen zur Risikosteuerung. Wenn (quantitative) Daten zu Ursachen und Wirkungen verfügbar sind, kann die Bow-tie Analysis auch zur Risikobewertung genutzt werden.

3.2.2.1.2 Beschreibung

Die Bow-tie Analysis hat sich zeitlich auf der Basis vier früheren Methoden entwickelt; diese sind: die Fehlerbaumanalyse, die Ereignisbaumanalyse, Ursache-Wirkungs-Diagrammen sowie der Barrier Analysis.[74] Dementsprechend integriert die Bow-tie Analysis Elemente dieser vier Methoden.

Die Bow-tie Analysis wird aus den folgenden Elementen gebildet:[75]

- Ein „Top Event“: Das zentrale (unerwünschte) Ereignis, für das Ursachen und Wirkungen identifiziert werden sollen.
- Ursachen: Auf der linken Seite des „Top Events“ werden die identifizierten Ursachen für das unerwünschte Ereignis dargestellt. Dies kann mittels eines Ursache-Wirkungs-Diagramms oder mittels einer Fehlerbaumanalyse geschehen.
- Wirkungen: Auf der rechten Seite des „Top Events“ werden die möglichen Wirkungen des unerwünschten Ereignisses dargestellt. Auch hier kann ein Ursache-Wirkungs-Diagramm genutzt werden, alternativ aber auch eine Ereignisbaumanalyse. Die Anwendung von Fehlerbaum- und Ereignisanalyse unter Nutzung quantitativer Daten ermöglicht es, die Bow-tie Analysis auch zur Risikobewertung zu nutzen.[76]
- Schwellen: Sowohl links als auch rechts des „Top Events“ werden sogenannte Barrier platziert. Damit sind Schwellen oder Sperren gemeint, mit denen (dann bereits im Sinne einer Risikobewältigung) versucht wird, den Eintritt des unerwünschten Ereignisses und/oder die Wirkungen zu vermindern oder zu vermeiden.
- Management-System: Teilweise werden die in Verbindungen stehenden Management-Systeme ebenfalls in das Diagramm eingezeichnet.

Es existieren verschiedene Variationen der Bow-tie Analysis, die davon abhängen, zu welchem Zweck die Analyse genutzt werden soll (Risikoidentifikation, Risikobewertung, Risikokommunikation) und aus welchen konkrete Elementen das Diagramm besteht beziehungsweise welche Methoden angewandt werden.

[74] Vgl. Ruijter, Guldenmund (2016), S. 211-212 sowie Romeike, Spitzner (2015), S. 134-135.
[75] Vgl. Ruijter, Guldenmund (2016), S. 213 sowie Romeike, Spitzner (2015), S. 134-135.
[76] Ein derartiger Ansatz wird beispielsweise bei Ferdous et al (2013) dargestellt; er wird durch die Anwendung der Fuzzy-Theorie erweitert.

3.2.2.1.3 AnwendungsbeispielAnwendungsbeispiel

Mokhtari u.a. zeigen beispielhaft, wie die Bow-tie Analysis in einen Risikomanagement-Rahmen integriert werden kann, um die Phasen der Risikoidentifikation, Risikobewertung und Risikobewältigung von Seehäfen und Offshore-Terminals zu unterstützen.[77] Dieser Rahmen wird in der nachfolgenden Abbildung 4 dargestellt.

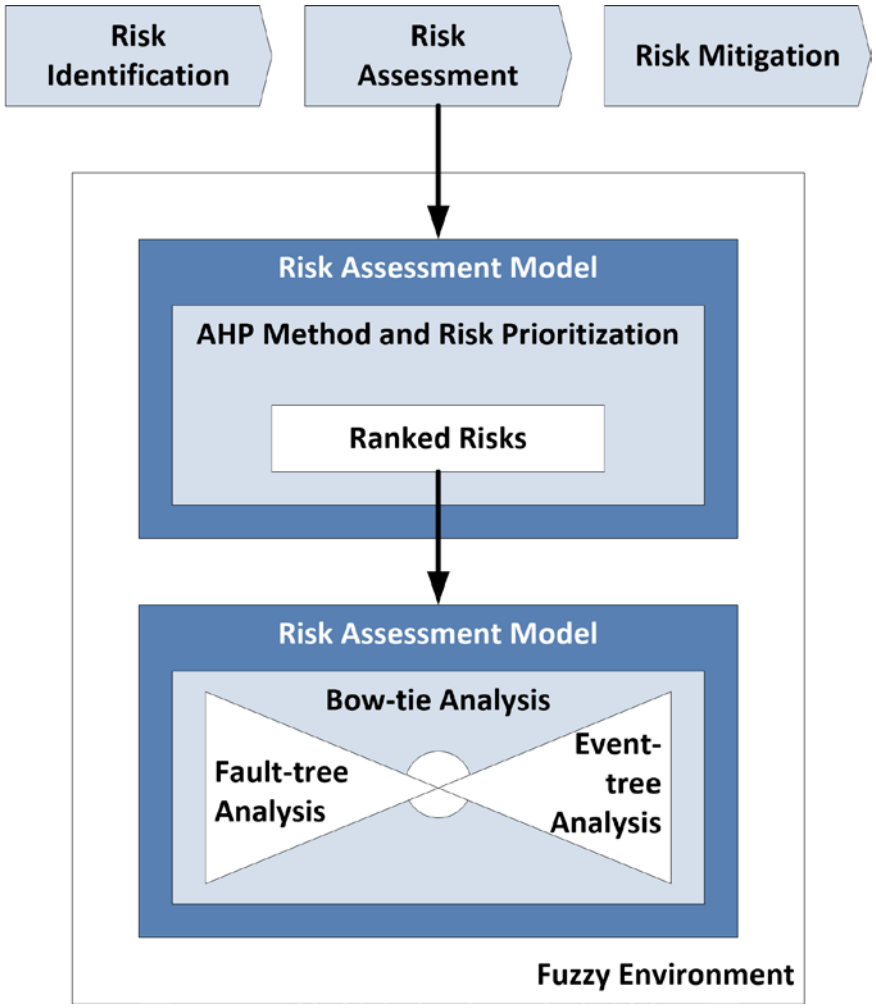


Abbildung 4 Risikomanagement-Rahmen für die Anwendung der Bow-tie Analysis[78]

	Cause	Risk/Event	Effect
Sales	Limited quality of sales people	Might not meet own expectations of trust, quality, reputation and track record	Assuming inappropriate liabilities and risks
		Might not meet customers expectations of trust, quality, reputation and track record	Customer might not purchase again, speak badly about supplier
	Limited quality of product / service	Might not meet customer satisfaction	Customer might not purchase again, speak badly about supplier

[77] Vgl. Mokhtari et al (2011) und Mokhtari et al (2012).

[78] Quelle: Eigene Darstellung in Anlehnung an Mokhtari et al (2011), S. 470 und Mokhtari et al (2012), S. 5091.

	Cause	Risk/Event	Effect
	Sales process		
	Contracting process	Contracting process design and operating effectiveness might be inadequate	...
	Customer require-ments	Quality and detail of customer re-quirements might be bad	...
	Offer schedule	Potentially no adequate offer schedule	...
	Offer team and contract team	Potentially no adequate ofer team or no necessary resources for the con-tract phase	...
	Risk Management	Potentially no adequyte risk manage-ment procedures in place	...
	Interface bid team and contract team	Potentially no close co-operation between bid and contract execution team	...
	Compliance - Export Control	Proposals might not be in line with the legal requirements/restrictions for export control/war good export	...
	Customer Finance - Customer credit status	Credit line might not be proporly defined and monitored for each customer	...
Finance and control	Assuming inappropriate liabilities and risks	Business case might be endangered	Not meeting financial targets
HR	Company under stress due to unrealistically high growth targets	Might not be enough focus on quality and integrity of sales force	Limited quality of sales people
	Company rather saturated		
	Company under stress due to unrealistically high growth targets	Might not be enough focus on quality of engineers	Limited quality of development engineers
	Engineer resource plan-ning process		
Development	Limited quality of devel-opment engineers	Might not meet expectations of technical expertise	Limited quality of product / service
	Development process	Development process design and operating effectiveness might be inadequate	
Strategic	Investors and analysists pressure on company	Executive management might adopt stategy for short term growth	Company under stress due to unrealistically high growth targets

Tabelle 7: Ursachen, Ereignisse und Effekte in tabellarischer Übersicht

Die Anwendung der Bow-tie Analysis wird begleitet durch den Einsatz der Analytic Hierarchy Process Method (AHP) für die Priorisierung der Risiken (siehe Abbildung 4). Für die Top-Risiken wird anschließend die Bow-tie Analysis angewandt, um Ursachen und Wirkungen zu identifizieren sowie eine Bewertung durchzuführen. Die Ursachen werden mittels der Fehlerbaumanalyse, die Wirkungen mittels der Ereignisbaumanalyse erarbeitet.

Kjølle, Utne und Gjerde stellen den Ablauf einer Risikoanalyse für kritische Infrastrukturen im Elektrizitätsbereich dar. Sie betonen die gute Eignung der Bow-tie Analysis als Rahmenmodell für die Risikoanalyse.[79]

3.2.2.1.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☒ Risikobewertung

☐ Risikosteuerung

3.2.2.1.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Für die Risikoidentifikation ist es sinnvoll (und ausreichend), Expertenschätzungen zu nutzen. Gleichzeitig können Kreativitätsmethoden genutzt werden, um die Bow-tie Analysis durchzuführen.

3.2.2.1.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: In Abhängigkeit von der Zielsetzung der Analyse, aber auch des Methodeneinsatzes und der Datenverfügbarkeit ist der Output eher qualitativ (für die Risikoidentifikation) oder quantitativ (für die Risikobewertung). Der qualitative Output, vor allem in Form von Ursachen-Szenarien, wird häufig in einer sinnvoll-simplifizierten Form dargestellt.[80]

[79] Vgl. Kjølle et al (2012), S. 81.
[80] Vgl. Mokhtari et al (2011), S. 466.

3.2.2.1.7 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☒ mittel

☐ hoch

Begründung: Der zeitliche Aufwand für die Durchführung der Bow-tie Analysis hängt von der Zielsetzung ab: Die Risikoidentifikation kann mit einem relativ geringen Zeitaufwand durchgeführt werden; für die Risikobewertung sind sowohl Datenbedarf, aber auch der Zeitaufwand für die Durchführung deutlich höher.

3.2.2.1.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☒ niedrig

☐ mittel

☒ hoch

Begründung: Der personelle Aufwand für die Durchführung der Bow-tie Analysis hängt von der Zielsetzung ab: Die Risikoidentifikation kann auch von Fach-/Domänenexperten durchgeführt werden, die nur ein geringes Methodenwissen einbringen.[81] Für die Risikobewertung sind neben des Fach- oder Domänenwissens vor allem auch profunde Kenntnisse in Fehlerbaum- und Ereignisbaumanalyse notwendig.

3.2.2.1.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☒ Basic

☒ Evolved

☐ Advanced

☐ Leading

3.2.2.1.10 Stärken und Schwächen

Stärken	Schwächen
• Strukturiertes Verfahren • Klare – auch grafische – Gliederung von Ursachen, Ereignissen und Effekten • Grafische Darstellung auch zur Risikokommunikation geeignet • Gute Verbindungsmöglichkeiten zu an-	• Komplexe Ursache-Wirkungszusammenhänge können nur sehr eingeschränkt abgebildet werden (komplexe Feedback-Loops und nicht lineare Abhängigkeiten). • Wirkungen bilden oft die Ursache für

[81] Vgl. dazu auch die Einschätzung bei Lewis, Smith (2010), S. 8.

Stärken	Schwächen
deren – vor allem analytischen – Methoden • Maßnahmen (Barrier) können in der Bow-Tie Analysis abgebildet werden.	andere „Top Events“. Dies kann im Bow-Tie-Diagramm nicht abgebildet werden.

Tabelle 8 Stärken und Schwächen der Bow-Tie Analysis

3.2.2.1.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

3.2.2.2 Empirische Datenanalyse

3.2.2.2.1 Einsatzzweck

Die empirische Datenanalyse untersucht historische Daten auf potenzielle Manipulationen oder unbeabsichtigte Fehler. Die empirische Datenanalyse zählt zu den „Data-Mining-Methoden“, die der explorativen Datenanalyse zugeordnet werden können. Hierbei wird – beispielsweise im Kontext Risikomanagement – mit Hilfe numerischer und statistischer Verfahren das Ziel verfolgt, Muster beziehungsweise Strukturen oder Besonderheiten in den Daten zu erkennen. Durch eine solche Analyse können beispielsweise gezielte oder unbeabsichtigte Manipulationen an Eingangsdaten empirisch nachgewiesen werden und Anwender so davor schützen, solche fehlerbehafteten Daten weiter zu verwenden. Die empirische Datenanalyse trägt damit zu einer möglichst hohen Qualität der genutzten Daten bei.

3.2.2.2.2 Beschreibung

Die quantitative und qualitative Datenanalyse wird heute vor allem in der angewandten Statistik angewendet. Die Methodik der Datenanalyse eignet sich beispielsweise

- zur Analyse von großen Stichproben,
- zur Objektivierung und Quantifizierung von statistischen Erhebungen,
- zum Testen von Hypothesen oder zur Überprüfung statistischer Zusammenhänge (beispielsweise Assoziationsanalyse oder Regressionsanalyse),
- zum Erkennen von Mustern und Strukturen in Daten (beispielsweise dichtebasierte Ausreißer-Erkennung oder Clusteranalyse) oder

- zum Vergleich von Daten beziehungsweise empirischen Ergebnissen über die Zeit (beispielsweise Zeitreihenanalyse).

Als ein Anwendungsbeispiel untersucht die empirische Datenanalyse beispielsweise die Häufigkeit der Anfangsziffern von Datensätzen. Gemäß dem Benfordschen Gesetz (auch Newcomb-Benford's Law, NBL) sind die ersten Ziffern „natürlicher" Datensätze stets mit absteigender und immer gleicher Wahrscheinlichkeit verteilt. So treten beispielsweise Zahlen mit der Anfangsziffer 1 etwa 6,5-mal so häufig auf wie solche mit der Anfangsziffer 9. So tritt in etwa 30 Prozent aller Fälle die 1 als führende Ziffer der einzelnen Daten auf. Absteigend verteilen sich die Leitziffern gemäß Abbildung 5. Ursprünglich entdeckt hat diese empirische Ziffernverteilung der Astronom und Mathematiker Simon Newcomb (1881). Der Physiker Frank Benford (1883–1948) entdeckte diese Gesetzmäßigkeit in den 1930er Jahren wieder und veröffentlichte sie in Benford(1938).

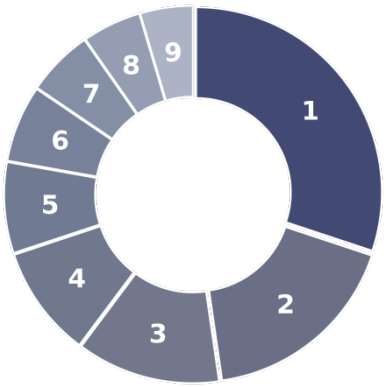


Abbildung 5 Empirische Verteilung von Ziffern nach dem Benfordschen Gesetz[82]

Führende Ziffer	Wahrscheinlichkeit
1	30,1 %
2	17,6 %
3	12,5 %
4	9,7 %
5	7,9 %
6	6,7 %
7	5,8 %
8	5,1 %
9	4,6 %

Tabelle 9: Empirische Verteilung von Ziffern nach der Wahrscheinlichkeit log10(n+1) – log10(n)

[82] Quelle: Wikimedia (2008).

Treten in einem untersuchten Datensatz deutlich abweichende Verteilungen der Leitziffern auf, so liegt der Verdacht nahe, dass der Datensatz manipuliert wurde oder fehlerbehaftet ist. Wird eine solche Verteilungsanomalie, meist computergestützt oder vollautomatisiert, ermittelt, werden die Daten einer genaueren manuellen Prüfung unterzogen um die vermeintliche „Datenverunreinigung“ genauer zu beleuchten und gegebenenfalls zu korrigieren.

Bei der Anwendung des Benfordschen Gesetzes ist es wichtig, dass die Datensätze einer bestimmten Struktur folgen. Dies gilt vor allem dann, wenn die Mantissen der Logarithmen des Datensatzes in den Grenzen von 0 bis 1 gleichverteilt sind. In der Praxis gilt dies für viele Datensätze, vor allem wenn diese umfangreich sind und einigermaßen weit verteilt (dispergiert) sind. Umfangreiche und unabhängige Datensätze (vgl. ein Risiko- oder Versicherungsportfolio) folgt häufig einer Normalverteilung. Die Gesetzmäßigkeit des Gesetzes basiert auf den gleichverteilten Mantissen der Logarithmen der Zahlenwerte des Datensatzes. So gilt das Benfordsche Gesetz beispielsweise für Datensätze in Steuererklärungen, Buchhaltungssystemen etc. und wird dort auch in der Praxis angewendet.

Wie groß nun tatsächlich die Differenz zwischen der empirischen und der theoretisch zu erwartenden Verteilung sein muss, damit ein Verdacht auf Manipulation bestätigt und eventuell weiterverfolgt wird, kann in der Praxis mit Hilfe bekannter mathematisch-statistischer Anpassungstests (beispielsweise dem Chi-Quadrat-Test oder dem Kolmogorow-Smirnow-Test) analysiert werden.

3.2.2.2.3 Anwendungsbeispiel

Die Anwendung einer empirischen Datenanalyse ist vor allem an logistischen Umschlagpunkten sinnvoll, da hier eine (gezielte) Datenmanipulation am wahrscheinlichsten ist. So ist es etwa denkbar, dass einzelne Akteure gezielt die Daten eines Hafens manipulieren um die Operationen entsprechend zu stören oder zu lenken. Solche Manipulationen können durch eine empirische Datenanalyse ganz konkret aufgedeckt werden und nach einer angeschlossenen manuellen Analyse entsprechend behoben werden. Finanzämter und Wirtschaftsprüfer nutzen bereits seit vielen Jahren die empirische Datenanalyse, um Unregelmäßigkeiten im Rechnungswesen zu identifizieren. So wurden beispielsweise die „kreativen“ Bilanzmanipulation der US-Konzerne Enron und Worldcom mit Hilfe des Benfordschen Gesetzes erkannt. Auch Marktpreise folgen in der Regel dem Bernfordschen Gesetz und könnten daher für Logistikunternehmen ein Mehrwert stiftendes Analyseinstrument sein.

3.2.2.2.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.2.2.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☐ Expertenschätzung

Beschreibung: Der Input muss eine möglichst große, und somit aussagekräftige, Datenbasis sein, welche aus „natürlichen Daten“ besteht. Natürliche Daten sind hierbei vollständig randomisierte Zahlen, die nicht strukturell gewisse Leitziffern besitzen.

3.2.2.2.6 Output

☐ eher qualitativ

☐ qualitativ und quantitativ

☒ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Der Output ist unmittelbar zunächst eine Verteilung der Leitziffern innerhalb des Datensatzes. Hieraus abgeleitet lässt sich oft ein Teilbereich der Daten isolieren, indem die Verteilung ungewöhnlich und vermutlich manipuliert ist – dieser Teil kann als potenzielle Schwachstelle als qualitativer Output verstanden werden.

3.2.2.2.7 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: In der Regel wird eine empirische Datenanalyse vollautomatisiert auf große Datensätze angewendet und bedarf somit, nach einer Implementierungsphase, keines weiteren Aufwandes.

3.2.2.2.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Da die Verifikation zunächst vollständig Computer basiert erfolgt, wird kein Personal benötigt. Erst bei einer folgenden Tiefenanalyse wird die Expertise von qualifiziertem Personal benötigt.

3.2.2.2.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☐ Evolved

☒ Advanced

☒ Leading

Erläuterung: Die empirische Datenanalyse ist eine mittlerweile vielfach evaluierte und gut entwickelte Methode, die zum Standardprüfprozedere zahlreicher Akteure (etwa Wirtschaftsprüfer, Steuerfahnder oder Betrugsexperten) zählt.

3.2.2.2.10 Stärken und Schwächen

Stärken	Schwächen
• Kann schnell und einfach als „Routine-Plausibilitätscheck“ umgesetzt werden • Geringer Ressourceneinsatz	• Nur für komplett zufällige, ganzzahlige Datensätze plausibel anwendbar • Ergebnis ist rein binär: „Korrekt“ oder „Manipuliert“

Tabelle 10: Stärken und Schwächen der empirischen Datenanalyse

3.2.2.2.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

Begründung: Die „Entdeckungswahrscheinlichkeit“ des Verfahrens ist zwar gering, aber die Anwendung so einfach und problemlos, da vollständig automatisiert, dass die Methode an sämtlichen logistischen Knotenpunkten umgesetzt werden sollte.

3.2.2.3 Fehlerbaumanalyse

3.2.2.3.1 Einsatzzweck

Die Fehlerbaumanalyse (engl. Fault Tree Analysis, FTA) wird eingesetzt um Ausfallwahrscheinlichkeiten von komplexen Systemen, nicht einzelner Komponenten, zu ermitteln. Der Hauptzweck ist somit das Risiko eines Gesamtsystems als Ableitung der Risiken einzelner Komponenten zu bewerten und zu quantifizieren.

3.2.2.3.2 Beschreibung

Die Fehlerbaumanalyse ist im Kern eine Top-Down-Fehleranalyse, die – ausgehend von dem binären (1 = defekt, 0 = nicht defekt) Zustand eines Top-Ereignisses – untersucht, welche binären Zustände tieferliegender Systemteile plausibel sind. Wird also der Defekt des Gesamtsystems auf der obersten Ebene des Fehlerbaums angenommen, so prüft die Fehlerbaumanalyse, ob dieser Ausfall zwangsläufig den Ausfall eines oder mehrerer tieferliegender Systemteile als Ursache haben muss. Diese Abhängigkeiten werden, unter Benutzung der Boolschen Algebra, bis zu den elementaren Teilen des Systems herunter propagiert. Somit werden mit Hilfe der Fehlerbaumanalyse die logischen Verknüpfungen von Teilsystemausfällen auf allen kritischen Pfaden ermittelt, welche insgesamt zu einem Systemausfall des gesamten Systems führen kann.

Die Fehlerbaumanalyse und seine grafische Darstellung sind durch die DIN 25424 (beziehungsweise international durch IEC 61025 und EN 61025) standardisiert. Entsprechend konsistent werden sowohl die grafische Repräsentation als auch die eigentliche Boolsche Berechnungsmethode in zahlreichen verschiedensten Unternehmen und Branchen angewendet.

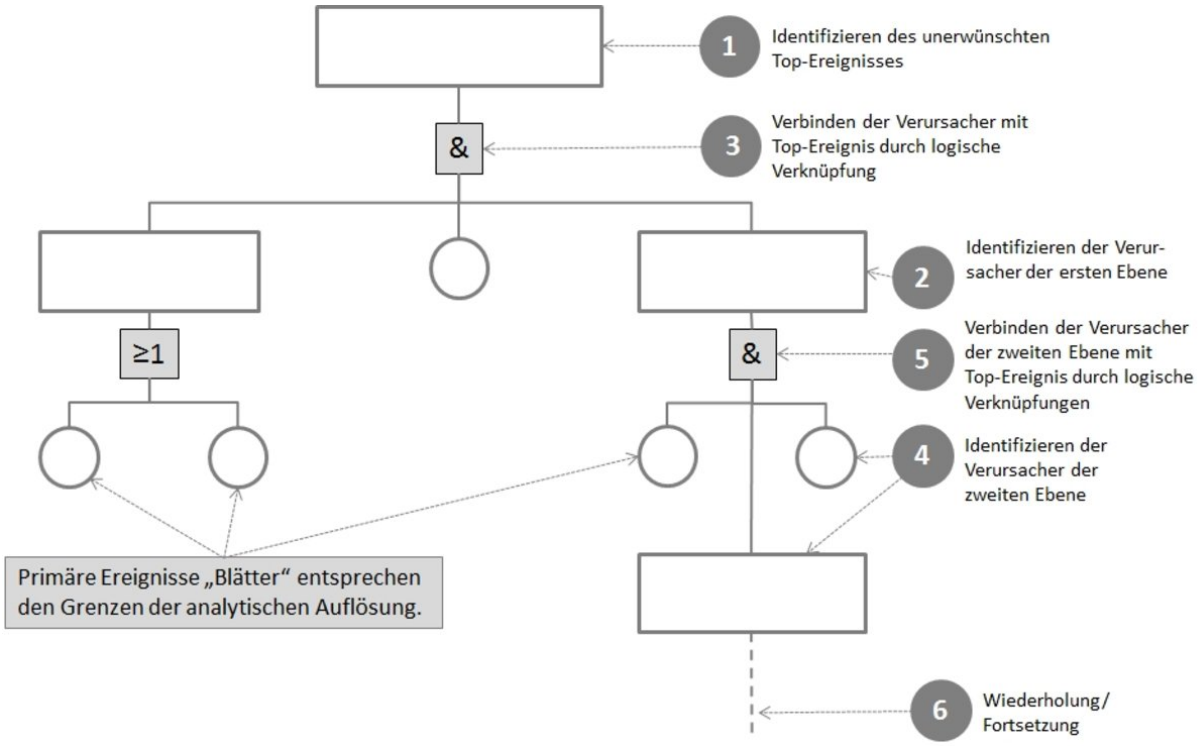


Abbildung 6 Exemplarischer Fehlerbaum[83]

3.2.2.3.3 Anwendungsbeispiel

Für die Fehlerbaumanalyse gibt es eine Vielzahl von Anwendungsbeispielen aus unterschiedlichen Fachgebieten. Giannopoulos, Filippini und Schimmer bezeichnen die Fehlerbaumanalyse mit Fokus auf das Risikomanagement kritischer Infrastrukturen als die wesentliche Methode zur Identifikation der Verwundbarkeiten eines Systems.[84] Fehlerbaumanalyse sei vor allem für die Analyse geeignet für einzelne Elemente der kritischen Infrastruktur geeignet.

Sherwin, Medal und Lapp beschreiben die Anwendung der Fehlerbaumanalyse für eine konkrete Fragestellung im Rahmen des Supply Chain Risk Management:[85] Dabei geht es um Verspätungsrisiken in Supply Chains, die durch geringe Stückmengen, aber erhebliche Werte (für Bauteile und Komponenten) charakterisiert sind. Das Besondere an der Anwendung ist, neben der Nutzung der Stücklisten als Grundlage für die Nutzung der Fehlerbaumanalyse, dass verschiedene Szenarien für die Abmilderung der Auswirkungen sowie die damit verbundenen Kosten berücksichtigt werden. Die Anwendung der Fehlerbaumanalyse führt damit nicht nur zur Identifikation und Bewertung von Risiken, sondern bereits zur proaktiven Bewertung risikoreduzierenden Maßnahmen.

Gerde und Kjølle zeigen, wie die Fehlerbaumanalyse als ein Element von mehreren im Rahmen eines umfangreichen Risikoidentifikationsprozesses genutzt werden kann, bei dem unter-

[83] Quelle: Romeike, Hager (2003), S. 264 sowie RiskNET – The Risk Management Network.
[84] Vgl. Giannopoulos et al (2012).
[85] Vgl. Sherwin et al (2016).

schiedliche Methoden miteinander kombiniert werden. Konkret geht es dabei um die Risikoidentifikation von Energiesystemen, bei der die Fehlerbaumanalyse einen Beitrag zur übergeordneten Bow-tie Analysis leistet.[86]

3.2.2.3.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☒ Risikobewertung

☐ Risikosteuerung

3.2.2.3.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☐ Expertenschätzung

Beschreibung: Der Input muss eine möglichst detaillierte Systembeschreibung, zum Beispiel in Form einer Explosionszeichnung, sein. Weitere quantitative Daten und/oder historische Daten, sowie Experteneinschätzungen, sind im Prinzip nicht notwendig.

3.2.2.3.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Man unterscheidet zwischen der qualitativen und der quantitativen Fehlerbaumanalyse. Bei der qualitativen Fehlerbaumanalyse wird ausschließlich bestimmt, welches Bauteil oder welche Fehlermeldung den Defekt des Gesamtsystems verursachen könnte. Bei der quantitativen Fehlerbaumanalyse werden neben den rein Boolschen Aussagen auch explizite Rechnungen über die Wahrscheinlichkeiten und deren Fortpflanzungen durch das System durchgeführt um quantitative Erkenntnisse, in Form von Ausfallwahrscheinlichkeiten als Output, zu gewinnen.

[86] Vgl. Gerde, Kjølle (2011).

3.2.2.3.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Die erstmalige Implementierung der Methode ist enorm aufwendig, da tiefes Wissen über die Struktur des Systems als Input benötigt wird, die initial oft nicht vorliegen. Ist der eigentliche Fehlerbaum hingegen einmal implementiert, im Idealfall sowohl qualitativ als auch quantitativ, so ist der Aufwand der Methodenpflege sehr gering. Lediglich die Richtigkeit des Systemaufbaus und eventueller Wahrscheinlichkeiten muss überwacht und gegebenenfalls angepasst werden.

3.2.2.3.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Gerade in der Implementierungsphase der Fehlerbaumanalyse ist tiefgreifendes Fachwissen erforderlich, um den Systemaufbau genau zu beschreiben. Insbesondere Wirkungszusammenhänge sind hierbei häufig nur bei hoch qualifizierten Mitarbeitern zu erfragen.

3.2.2.3.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☒ Evolved

☒ Advanced

☐ Leading

Erläuterung: Aufgrund seiner vielseitigen, da qualitative und quantitativen, Ausrichtung und seiner Branchenunabhängigkeit ist die Fehlerbaumanalyse ein ausgereiftes Verfahren. Dies drückt sich auch durch die zahlreichen Standardisierungen, national wie international, aus.

3.2.2.3.10 Stärken und Schwächen

Stärken	Schwächen
• Baumstruktur ermöglicht klar strukturierte systematische Untersuchung • Kann als Methode für die Ursachenanalyse im Rahmen der Bow-Tie Analysis genutzt werden • DIN-Standardisierung sowie internationaler Standard IEC 61025 (EN 61025)	• Ermittelt „nur“ die Ausfallwahrscheinlichkeiten • Ausgiebiges Strukturwissen erforderlich

Tabelle 11: Stärken und Schwächen der Fehlerbaumanalyse

3.2.2.3.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

Begründung: Da Logistiknetzwerke, wie etwa Straßennetzwerke, oft hochkomplexe und vielverzweigte Systeme sind, ergibt eine Fehlerbaumanalyse in der Analyse von Risiken in der Logistik viel Sinn. Nur durch eine konsequente deduktive Schlussfolgerungskette, wie sie die Fehlerbaumanalyse durchführt, ist oft die eigentliche Ursache eines resultierenden Risikos zu ermitteln.

3.2.2.4 Fehlermöglichkeits- und Einflussanalyse (FMEA)

3.2.2.4.1 Einsatzzweck

Die Fehlermöglichkeits- und Einflussanalyse (FMEA), im Englischen: Failure Mode and Effects Analysis, ist eine analytische Methode zur Messung der Zuverlässigkeit eines Systems und zur Ermittlung potenzieller Schwachstellen. Gleichzeitig deckt sie – zumindest ansatzweise – auch die Risikosteuerung ab, weil für identifizierte Risiken Maßnahmen und Verantwortlichkeiten definiert werden können. Aus militärischen Einsatzzwecken kommend, wird die FMEA heute unter anderem von Lieferteilen für von Serienteilen der Automobilindustrie, gem. ISO/TS 1694921, genutzt.

3.2.2.4.2 Beschreibung

Im Rahmen der Risikoidentifikation und -bewertung ermittelt die FMEA die sogenannte Risikoprioritätszahl RPZ als Produkt der drei Faktoren P, W und Z. Diese RPZ dient als Maß zur

Risikobewertung. Hierbei symbolisiert P (probability) die Wahrscheinlichkeit, dass ein gewisses Risiko auftritt, W die Entdeckungswahrscheinlichkeit und Z die Fehlerfolge.[87]

Da üblicherweise alle drei Faktoren auf den Bereich 1-10 normiert werden, eignet sich das Verfahren insbesondere zur Quantifizierung von qualitativ bewerteten Risiken.[88] Bedingt durch dieses Vorgehen, lassen sich die Ergebnisse lediglich als grobe Einschätzung eines Risikos verstehen. Eine hohe RPZ deutet demnach auf die Notwendigkeit weiterer Maßnahmen hin, während Risiken mit niedriger RPZ vernachlässigt werden können. Die multiplikative Verknüpfung der drei Faktoren muss jedoch kritisch gesehen werden: Insbesondere bei „Low-probability high-consequence risks", wie sie im Bereich der kritischen Infrastrukturen vorkommen, kann die RPZ bei extrem niedrigen P- oder W-Werten insgesamt niedrig sein und damit fälschlicherweise eine geringe Dringlichkeit suggerieren.

Durch die Aggregation von Risiken an einzelnen Stellen eines größeren Systems, dessen Grenzen klar definiert sein müssen, erlaubt FMEA insbesondere auch die Ableitung eines Maßes für die Verlässlichkeit eines komplexen Systems. Im Kontext des Risikomanagements kritischer logistischer Infrastrukturen ermöglicht es FMEA so, durch Analyse aller Netzwerkkomponenten eine Gesamtrisikobewertung für eine Infrastruktur zu erstellen.

Die FMEA ist letztendlich weniger eine Methode zur Risikoidentifikation, sondern mehr ein Mittel zu einer (möglichst) ganzheitlichen Dokumentation, Bewertung und Steuerung identifizierter Risiken.

3.2.2.4.3 Anwendungsbeispiel

Ein Anwendungsbeispiel liefern etwa Arvanitoyannis und Varzakas, die 2008 eine Case Study zur Durchführung der ISO 22000 am Beispiel der industriellen Verarbeitung von Lachs veröffentlichten[89]. Die konkreten Arbeitsschritte der Lachsverarbeitung wurden hierbei zunächst mittels eines Flussdiagramms entsprechend in Beziehung zueinander gesetzt (siehe Abbildung 7). Anschließend wurden für sämtliche kritischen Prozessteile (Anlieferung, Blutentfernung, Filetieren, Kühlung, Verpackung, Distribution), welche ausnahmslos im Rahmen der Qualitätsanalyse bereits überprüft werden, durch eine FMEA-Analyse hinsichtlich Auftrittswahrscheinlichkeit von Schadstoffen, Entdeckungswahrscheinlichkeit dieser und Fehlerfolge bewertet. Diese Bewertungen basierten dabei sowohl auf historischen, analytischen Daten, als auch auf qualitativen Daten, welche durch Expertenbefragungen gewonnen wurden. Schlussendlich wurden die Ergebnisse, also die resultierenden Risikoprioritätszahlen, mit den Vorgaben und Schwellwerten des Unternehmens abgeglichen. Überschritt die RPZ einen gewissen Schwellwert, so implizierte dies direkt, dass regulative Maßnahmen seitens

[87] Vgl. Bojar (2012).
[88] Vgl. Kim, Kim (2016).
[89] Arvanitoyannis, Varzakas (2008).

des Managements nötig waren, um die Risikowahrscheinlichkeit oder dessen Auswirkungen zu reduzieren.

Obwohl das hier aufgezeigte Beispiel keinen direkten Zusammenhang zum Risikomanagement von kritischen Infrastrukturen in der Logistik aufweist, so zeigt es doch gut auf, wie sich die FMEA-Methode auch im Kontext der Infrastrukturanalyse nutzen lässt, indem entsprechende Netzwerke ähnlich dem hier aufgezeigten Ablaufplan analysiert werden.

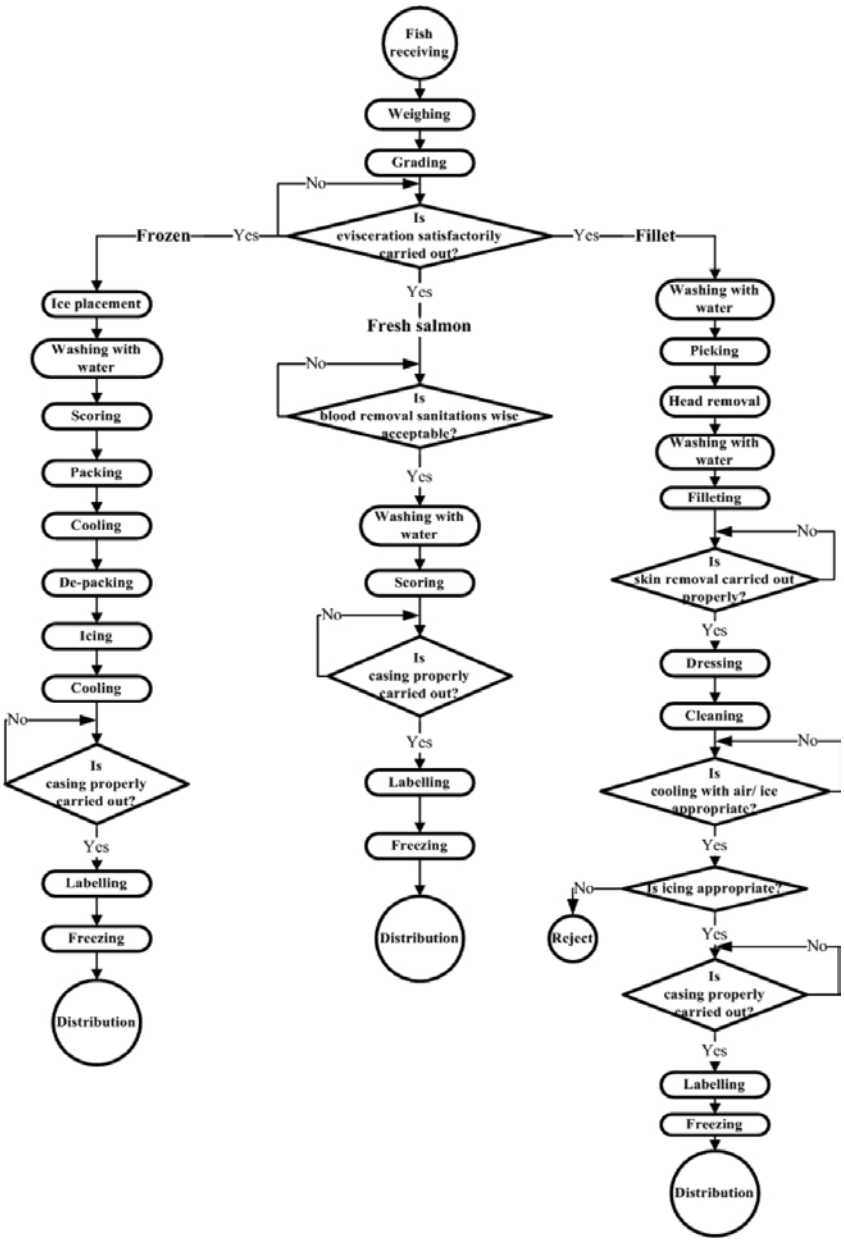


Abbildung 7: Flussdiagramm zur Lachsverarbeitung[90]

[90] Vgl. Arvanitoyannis, Varzakas (2008).

3.2.2.4.4 Phase

☐ Risikoidentifikation

☐ Risikoanalyse

☒ Risikobewertung

☐ Risikosteuerung

3.2.2.4.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Als Input können sowohl historische Daten, als auch Expertenschätzungen zur Ermittlung der einzelnen Faktoren genutzt werden.

3.2.2.4.6 Output

☐ eher qualitativ

☐ qualitativ und quantitativ

☒ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Output der FMEA ist das mit einer kritischen Infrastruktur verbundene Risikoinventar. Für jedes Risiko ergibt sich als weiterer Out die Risikoprioritätszahl RPZ. Sie ist eine quantitative Bewertung des Risikos. Da diese Kennzahl häufig auf qualitativen Inputs („Ratings“) innerhalb eines normierten Zahlenbereichs basiert, kann der Output nicht als absolutes Risikomaß missverstanden werden, sondern sollte ausschließlich zum Abgleich miteinander oder mit einem externen Schwellwert dienen. Die Kritikpunkte zur RPZ im Rahmen des Risikomanagements kritischer Infrastrukturen wurden oben bereits erläutert.

3.2.2.4.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Da in einer ersten Phase zunächst das System komplett und inklusive aller Wirkungsbeziehungen abgebildet wird, fällt bereits vor der eigentlichen Durchführung der Me-

thode ein beträchtlicher Arbeitsaufwand an. Für die Analyse müssen schlussendlich alle Einzelteile eines Systems explizit untersucht werden, welches erneut mit einem großen Aufwand verbunden ist.

3.2.2.4.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Da die Methode unter anderem auf „Rankings“, also Experteneinschätzungen, zurückgreift und ein tiefes Verständnis aller Wirkungszusammenhänge voraussetzt, müssen nahezu alle hochqualifizierten System- und Teilsystemexperten in den Prozess mit eingebunden werden.

3.2.2.4.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☐ Evolved

☒ Advanced

☐ Leading

3.2.2.4.10 Stärken und Schwächen

Stärken	Schwächen
• Das System wird vollumfassend betrachtet und schrittweise in kleinste Komponenten zerlegt • Klare Regulierung durch ISO-Vorschrift	• Die Multiplikation der ordinalskalierten Merkmale P, W und Z ist streng mathematisch nicht definiert. Daher ist auch die RPZ eher kritisch zu bewerten. • Viele Risiken (vor allem schwankungsorientierte) können nicht mit Hilfe P, W und Z bewertet werden. • Es ist nicht sichergestellt, dass ähnlichen Risiken dieselben RPZ zugeordnet werden. • Zeit- und Ressourcenverbreich hoch • Großer Datenbedarf und Systemkenntnisse erforderlich

Tabelle 12: Stärken und Schwächen der Fehlermöglichkeits- und Einflussanalyse

3.2.2.4.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☐ sehr gut

☒ gut

☐ weniger geeignet

Begründung: Aufgrund der Analyse von Risiken an Einzelstellen eines Systems bzw. Netzwerkes und der Propagierung dieser Risiken auf ein Gesamtnetzwerk, eignet es sich gut, um ein komplexes und vielfach verflochtenes System, wie es logistische Infrastrukturen üblicherweise sind, zu untersuchen. Die eigentliche Identifikation von Risiken wird allerdings nicht methodisch unterstützt; die Risikoprioritätszahl suggeriert eine Quantifizierung, die aufgrund der multiplikativen Verknüpfung kritisch zu sehen ist.

3.2.2.5 Hazard and Operability Analysis (HAZOP)

3.2.2.5.1 Einsatzzweck

Die Hazard analysis and operability (HAZOP) Analyse wird zur Analyse genutzt, wie ein Prozess von dem geplanten Ablauf abweicht. Insbesondere untersucht eine HAZOP Analyse sowohl mögliche Fehlfunktionen von einzelnen Komponenten eines größeren Systems als auch die Auswirkungen auf das Gesamtsystem. Unter Einbeziehung eines interdisziplinären Expertenteams wird die HAZOP-Analyse meist bereits in der Designphase eines Systems

angewandt, um verschiedenste potenzielle Schwächen im Aufbau frühzeitig, also schon vor Inbetriebnahme, zu erkennen und durch entsprechende Einwürfe der Experten zu beheben.[91]

3.2.2.5.2 Beschreibung

Die HAZOP-Analyse wurde ursprünglich von dem ehemaligen britischen Chemiekonzern ICI entwickelt, um als Risikomanagement-Methode während des Baus eines neuen Werkes genutzt zu werden. So beschreibt etwa Lawley (1974), einer der damaligen Operations Manager von ICI, erstmals die HAZOP-Analyse als prozessorientiertes Verfahren, welches Abweichung vom Normalbetrieb anhand von verschiedenen Messungen erfassen will und die Folgen für das Gesamtsystem bewertet. [92] Insbesondere basiert die gesamte Methode auf der Annahme, dass ein Risiko ausschließlich entsteht, wenn eine Abweichung von der geplanten Norm beobachtet wird.

In der Folge wurde die HAZOP-Analyse stets weiterentwickelt und resultierte in einer dreiphasigen Methode:[93]

- In einer ersten Phase werden der Grund und das Ziel der Analyse definiert. Der Leiter der bevorstehenden Studie sammelt hierbei detaillierte Informationen über das zu untersuchende System und schlägt eine Dekomposition in Systemteile und Teilprozesse vor. Ferner legt der Studienleiter die genaue Zusammensetzung des Teams zusammen und erstellt einen Projektmanagementplan.
- In einer zweiten Phase treffen sich die Mitglieder der Studie, und der Leiter führt zunächst tiefgehend in das System und dessen Modell ein. Alle Studienmitglieder besprechen gemeinsam jede Komponente und jeden Teilprozess des Systems und beschreiben die einzelnen Prozesse und deren wichtigsten Kennzahlen im Detail. Besonders wird hierbei die Abweichung eines Systemparameters untersucht und die Auswirkungen auf das Gesamtsystem in diesem Fall.
- In der finalen Phase schlagen Mitglieder der Studie Änderungen an den Komponenten ihres Kompetenzbereiches vor. Der Studienleiter sammelt diese und ruft gegebenenfalls zu einem weiteren Meeting auf.

3.2.2.5.3 Anwendungsbeispiel

Ein AnwendungsbeispielAnwendungsbeispielder HAZOP-Analyse im Kontext Infrastruktur liefert Rail Safety and Standards Board (RSSF) des Vereinigtes Königreiches mit der Studie „Understanding human factors and developing risk reduction solutions for pedestrian cros-

[91] Vgl. Dunjó (2010).
[92] Lawley (1974).
[93] Vgl. Rossing (2010).

sings at railway stations".[94] Die Studie beschäftigte sich intensiv mit einem klassischen Thema des Schienenverkehrs, nämlich Passagieren, die Gleise betreten. Ziel der Studie war einerseits die Risiken und vor allem die menschlichen Faktoren, die zu Unglücken hierdurch führen, zu untersuchen und andererseits die Entwicklung von Lösungen, die dieses Risiko vermindern. Hierzu hat zunächst eine Forschungsgruppe, die die Funktion des „Studienleiters" übernahm, aktuelle Sicherheitsvorschriften studiert und zahlreiche Feldbesuche durchgeführt. Aufbauend auf den dadurch gewonnenen Erkenntnissen über das Gesamtsystem „Bahnhof", wurde ein detailgetreues Modell entwickelt und mit einem großen Team von Experten diskutiert. Durch die Heterogenität des Expertenteams wurde eine große Anzahl verschiedener Faktoren für potenzielle Risiken, inklusive Architektur, Design, Farbgebung und Zugausstattung, bedacht und detailliert analysiert. Aufbauend auf dem Feedback der Experten erstellte eine Kommission zahlreiche Vorschläge zur Reduktion von Risiken in diesem Teilbereich, von denen am Ende 24 Vorschläge der Expertenrunde erneut vorgelegt wurden. Aufbauend auf diesen finalen Erkenntnissen diskutieren nun die zuständigen Bahnhofsbetreiber, welche der Maßnahmen schlussendlich umgesetzt werden.

3.2.2.5.4 Phase

☐ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☒ Risikosteuerung

3.2.2.5.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Zur Beschreibung des Gesamtsystems und der Dekomposition durch den Studienleiter werden zahlreiche detaillierte Daten über das System und sämtliche Komponenten benötigt. Dies beinhaltet insbesondere historische und quantitative Daten über das System und seine Prozesse. Schlussendlich schätzen zahlreiche Experten aus allen betroffenen Bereichen die genauen Risiken und deren Auswirkung ab.

[94] RSSB (2009).

3.2.2.5.6 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Der Output besteht bei der HAZOP-Analyse nicht aus einem Risiko, einer Einschätzung dessen oder einer Bewertung eines Risikos. Vielmehr ist der Output ein neues System, welches eine „risikobewusstere“ Variante des ursprünglichen Systems beschreibt. Durch einen unter Umständen iterativ angewandten Prozess entsteht so, zumindest formal, final ein „risikoloses“ System.

3.2.2.5.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Insbesondere die erste Phase erfordert einen erheblichen zeitlichen Aufwand, da das oftmals komplexe Gesamtsystem detailgetreu modelliert werden muss. Üblicherweise werden hierzu über Monate aufwändige 3D-Modelle erzeugt, mittels deren eine sehr präzise Analyse möglich ist. Durch die iterative Vorgehensweise ist ferner auch der Aufwand der anderen Akteure, also der Experten, a priori nicht abschätzbar.

3.2.2.5.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Der personelle Aufwand ist extrem hoch, da in der Regel Experten für jedes Teil des Systems hinzugezogen werden. Ferner werden meist auch externe Experten eingeladen an der eigentlichen Analyse mitzuwirken.

3.2.2.5.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☐ Evolved

☒ Advanced

☒ Leading

Erläuterung: Die HAZOP-Methode gilt in vielen Branchen, darunter auch beim Einsatz für Infrastrukturprojekte, als State-of-the-Art-Methode, da durch Einbeziehung eines großen Know-how-Pools eine Vielzahl unterschiedlichster Risikoursachen betrachtet werden.

3.2.2.5.10 Stärken und Schwächen

Stärken	Schwächen
• Gründliche und langfristig bewährte Analysemethode • Ermittelt nicht nur einzelne Schwachstellen, sondern „kritischen Pfad“	• Extrem Zeit- und Ressourcen-aufwendig • Nahezu ausschließlich qualitative Ergebnisse

Tabelle 13: Stärken und Schwächen der HAZOP-Analyse

3.2.2.5.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

Begründung: Die HAZOP-Analyse wird bereits ausführlich im Bereich Infrastrukturgroßprojekte genutzt und eignet sich hervorragend hierfür.

3.2.2.6 Business Impact Analysis

3.2.2.6.1 Einsatzzweck

Die Business Impact Analysis (BIA) wird üblicherweise als Teil des Business Continuity Managements implementiert, um die kritischen Geschäftsprozesse einer Unternehmung zu identifizieren. Insbesondere dient die BIA dazu, durch eine Analyse aller Prozessabhängigkeiten zu identifizieren, welche Abläufe im Gesamtprozess besonders funktions- und erfolgskritisch

sind und welche Ressourcen folglich für den Betrieb dieser kritischen Prozesse im Normal- und Notbetrieb eingeplant werden müssen. Schließlich soll die BIA auch die „Maximum Tolerable Period of Disruption“ (MTPD), also die maximal tolerable Ausfallszeit, und die „Recovery Time Objective“ (RTO), also die angestrebte Wiederanlaufzeit, für sämtliche Teilprozesse ermitteln.

3.2.2.6.2 Beschreibung

Die BIA wird üblicherweise in drei Phasen oder sechs Schritte unterteilt:

- In der ersten Phase („Scope und Konzeption“) wird in einem ersten Schritt der Umfang der geplanten Analyse festgelegt. Hierbei wird insbesondere definiert, welche Geschäftsbereiche in welchem Detaillierungsgrad analysiert werden sollen. In einem zweiten Schritt wird einerseits das genaue Bewertungsschema, und damit das Konzept, definiert und andererseits eine Methodik zur Datenerhebung und -speicherung festgelegt. Zuletzt werden über die gesamte Phase hinweg Fragebögen erstellt und an die einzelnen Geschäftsbereiche verteilt, um die eigentliche Analyse auch von den einzelnen Geschäftsbereichen mit-definieren zu lassen.
- In der zweiten Phase, der Erhebungsphase, wird in einem ersten Schritt die Analyse der einzelnen Prozesse selbst durchgeführt. Hierzu wird ein Projektplan definiert, ein Interview-Kalender erstellt, und die retournierten Fragebögen werden ausgewertet, um potenzielle Risiken und Schwachstellen in den einzelnen Prozessen aufzudecken. Im zweiten Schritt dieser Hauptphase werden die Ergebnisse der eigentlichen Analyse nach einer Qualitätssicherung dokumentiert und präsentiert.
- In der dritten Phase („Analyse und Entscheidung“) werden die kritischen Geschäftsprozesse anhand der gewonnen Ergebnisse zunächst in einem ersten Schritt identifiziert. In einem zweiten Schritt werden darauf basierend Anforderung an die kritischen Geschäftsprozesse und an die Ressourcen des Unternehmens abgeleitet. Schlussendlich wird auf Basis dieser Erkenntnisse ein Maßnahmenkatalog entwickelt.[95]

3.2.2.6.3 Anwendungsbeispiel

Radeschütz (2011) betrachtet in ihrer Dissertationsschrift „Business Impact Analysis“ ein exemplarisches Beispiel, welches sowohl den Input als auch den Output einer Business Analyse detailliert aufzeigt. [96] Das Beispiel beschreibt die Geschäftsprozesse eines Leihwagenunternehmens (vgl. Abbildung 8) und resultiert, nach einer umfangreichen BIA, in einer Empfehlung für einen optimierten Ablaufplan (vgl. Abbildung 9).

[95] Vgl. BCM News (2010).
[96] Vgl. Radeschütz (2011).

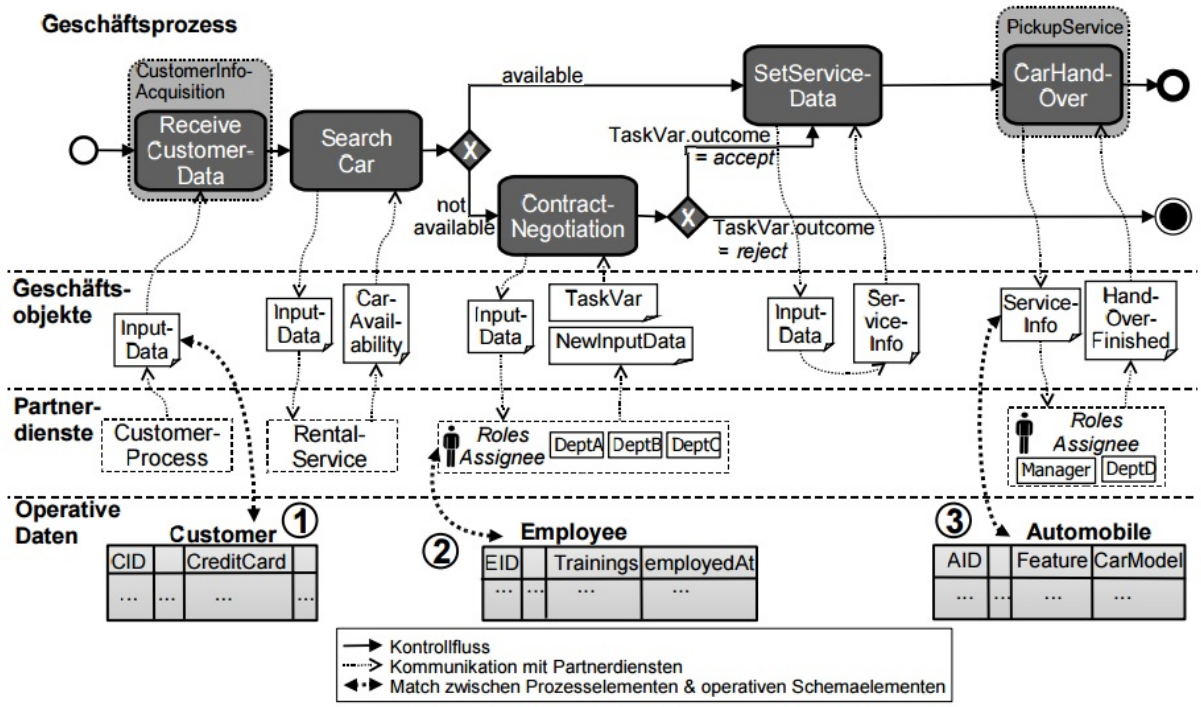


Abbildung 8: Geschäftsprozesse bei einem Leihwagenunternehmen[97]

Im ursprünglichen Unternehmensaufbau lassen sich die Prozessabläufe wie folgt zusammenfassen: Nach Eingang einer Kundenanfrage wird ein entsprechender Leihwagen, durch Abfrage des Bestandes einzelner Verleiher vor Ort, gesucht. Wird ein passendes Fahrzeug für den gewünschten Zeitraum gefunden, so werden Service (Wäsche, Wartung etc.) und Hand-Over-Prozesse entsprechend eingeplant. Ist kein passendes Fahrzeug verfügbar, versucht ein verfügbarer Mitarbeiter aus einer beliebigen Abteilung den Kunden zu überzeugen ein anderes Fahrzeug oder einen anderen Mietzeitraum zu wählen. Scheitern diese Verhandlungen wird die Kundenanfrage abgelehnt. Stimmt der Kunde zu, werden Service und Hand-Over entsprechend geplant. Im Laufe der BIA zeigen Experten der Geschäftsbereiche auf, dass besonders zwei Prozesse kritisch für den Geschäftsbereich sind. So berichten die Kundenbetreuer, dass wohlhabende Privatkunden häufig umfassende Wünsche haben und durch die standardisierte Abfertigung daher oft bereits früh im Prozess verloren werden. Insbesondere scheitern die bisher zufällig ausgewählten Mitarbeiter aus verschiedensten Bereichen und ohne entsprechende Qualifikation häufig an der Nachverhandlung mit vermögenden Kunden. Ferner berichtet die Abteilung der Instandsetzung der Fahrzeuge, dass Sportwägen stark überdurchschnittlich oft von Pannen oder Unfällen betroffen sind.

[97] Quelle: Radeschütz (2011).

Aufgrund der ermittelten Schwachstellen schlägt der Studienleiter verschiedene Maßnahmen vor, die gemeinsam mit den entsprechenden Experten entwickelt wurden. Einerseits empfiehlt er, dass vermögende Kunden, die man etwa an einer Platin-Kreditkarte identifizieren kann, von Beginn an persönlich betreut werden. Hierzu werden entsprechende Kunden zu dem neuen Geschäftsprozess „Special Service“ vermittelt, der gemeinsam mit dem Kunden versucht eine kundenzufriedenstellende Konfiguration des Leihangebotes zu ermitteln und bei Erfolg eine entsprechende Buchung durchführt. Dieser Special Service wird hierbei von Beginn an von Mitarbeitern mit ausgeprägten Kommunikations-Qualifikationen durchgeführt. Ferner, wird der Bereich „Hand-Over“ aufgespalten. Das Hand-Over von Sportwägen soll künftig von gut qualifizierten Experten durchgeführt werden, die Kunden entsprechend auf die besonderen Bedürfnisse von Sportwägen hinweisen. Die Ergebnisse der BIA und den vorgeschlagenen neuen Ablaufplan zeigt Abbildung 9.

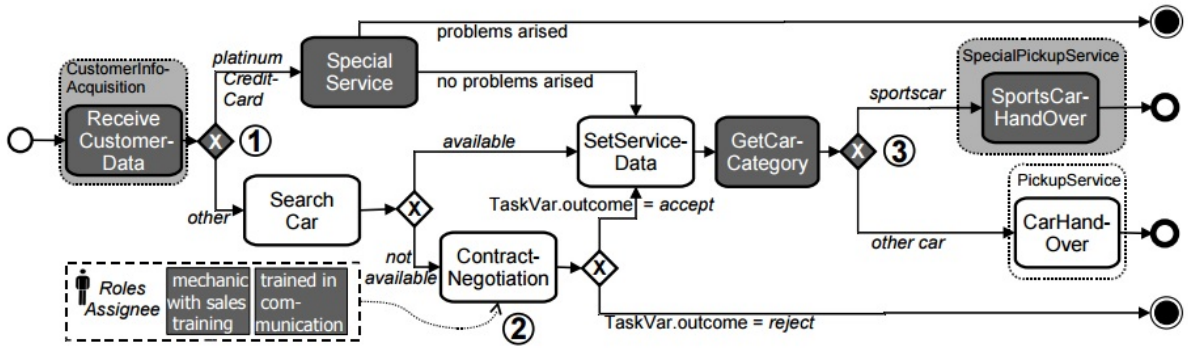


Abbildung 9: Optimierte Geschäftsprozesse desselben Leihwagenunternehmens[98]

3.2.2.6.4 Phase

☒ Risikoidentifikation

☐ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.2.6.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☒ Expertenschätzung

[98] Quelle: Radeschütz (2011).

Beschreibung: Prinzipiell basiert die Business Impact Analyse vor allem auf Experteneinschätzungen. Diese bedienen sich dabei häufig auch quantitativer Daten, um eine präzisere und validere Einschätzung abzugeben. Der genaue Daten- und Experteneinsatz wird innerhalb der Analyse in Phase eins detailliert geplant und kann daher stark variieren.

3.2.2.6.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Der Output der BIA lässt sich in zwei wesentliche Teile aufteilen: Einerseits werden für einzelne Teilprozesse oft quantitative Werte als Output des Verfahrens erhoben (vgl. MTPD, RTO im Teil „Einsatzzweck“). Andererseits ist Hauptziel der BIA die Identifizierung der kritischen Prozesse innerhalb eines Geschäftsmodells. Die reine Kritikalität ist hierbei als qualitativer (und damit subjektiver) Output zu verstehen.

3.2.2.6.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Eine BIA erfordert einen sehr geringen zeitlichen Aufwand für jeden Teilprozess einer Unternehmung. Lediglich die Koordinierung und die Dokumentation der Ergebnisse führt zu einem hohen Aufwand.

3.2.2.6.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☒ mittel

☒ hoch

Begründung: Der Großteil einer BIA wird von einer koordinieren Stelle innerhalb eines Unternehmens/Systems durchgeführt. Diese Stelle kann hierbei sowohl eine externe Koordinierungseinheit sein, als auch eine Fachkraft innerhalb des Unternehmens mit mittlerer Qualifikation, da kein tiefgreifendes System- oder Prozess-Verständnis von dem Koordinator ver-

langt wird. Da Teil der BIA immer eine Experteneinschätzung ist, wird selbstverständlich auch hochqualifiziertes Personal benötigt, um einzelne Prozesse detailliert zu durchdringen und zu analysieren.

3.2.2.6.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☒ Evolved

☒ Advanced

☐ Leading

Erläuterung: Die BIA gehört zu den Standardmethoden des Business Continuity Managements (BCM), welches heute in vielen Unternehmen fester Bestandteil der Managementebene ist. Andererseits taugen die oft vagen und subjektiven Erkenntnisse einer BIA oft nicht dazu den Bereich Risikomanagement vollständig abzudecken.

3.2.2.6.10 Stärken und Schwächen

Stärken	Schwächen
• Umfangreiches Verfahren, welches zahlreiche hilfreiche Outputs liefert • Impliziert direkte Handlungsempfehlungen	• Experten aus allen relevanten Ebenen müssen involviert werden • Eine BIA ist immer ein langfristig Projekt und Bedarf einer eigenen „Steuerungseinheit“

Tabelle 14: Stärken und Schwächen der Business Impact Analysis

3.2.2.6.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☐ sehr gut

☐ gut

☒ weniger geeignet

Begründung: Zum einen ist eine Zerlegung einer logistischen Infrastruktur in klar abgegrenzte Teilprozesse nur schwer oder gar nicht möglich. Zum anderen ist zunächst unklar, welcher Akteur ein Interesse daran haben könnte, die Koordination einer BIA für eine Infrastruktur zu leiten. Übernimmt der Infrastrukturbetreiber selbst diese Aufgabe, so wird es diesem kaum möglich sein, valide Expertenschätzungen über einzelne kritische Bereiche der Infrastruktur

zu erhalten, da keiner der Teilinfrastruktur-Betreiber offensichtliche Schwächen offenbaren möchte.

3.2.2.7 Fehler-Ursachen-Analyse

3.2.2.7.1 Einsatzzweck

Die Fehlerursachenanalyse (im Englischen: Root Cause Analysis, kurz: RCA) ist eine Methode, die entwickelt wurde, um die Ursachen von Ereignissen, die die Sicherheit, die Gesundheit, die Umwelt, die Qualität oder die Zuverlässigkeit beeinflussen, detailliert zu analysieren. Somit ist die Fehlerursachenanalyse ein Tool, welches dabei hilft, nicht nur zu ermitteln, was genau wie passiert, sondern auch, warum ein Ereignis eintrifft.

Das Hauptargument für eine tiefgehende Ursachenanalyse ist die Überzeugung, dass nur durch ein detailliertes Verständnis von Fehlerursachen künftige Wiederholungen eines Fehlers vermieden werden können. Schlussendlich dienen die gewonnenen Erkenntnisse über Fehlerursachen der Erstellung von Maßnahmenkatalogen um die Auslösung einer solchen Fehlerursache künftig unwahrscheinlicher zu machen.[99]

3.2.2.7.2 Beschreibung

Die RCA besteht in der Regel aus vier Phasen, die Rooney und Vanden Heuvel (2004) wie folgt zusammenfassen:

1. Datenerhebung: In der Initialphase der Analyse werden alle verfügbaren Daten über einen aufgetretenen Fehler gesammelt.
2. Kausalanalyse: In der zweiten Phase der Analyse werden Kausalzusammenhänge grafisch, etwa in Form eines Ereignisbaumes, dargestellt. Dank dieser strukturierten Darstellung können die Analysten in Folge die gesammelten Daten den einzelnen Teilprozessen zuordnen und eventuell fehlende Datensätze klar definieren. Um die erste Phase effektiv und zielführend durchzuführen, werden Datenbedarfe, die bei der Erstellung der Kausalketten auftreten, immer wieder an Phase 1 kommuniziert.
3. Ursachenanalyse: In Phase 3 der RCA werden die Grundursachen auf Basis der kausalen Zusammenhänge ermittelt. Hierzu kommt vor allem die sogenannte Grundursachenkarte als Tool zur Anwendung, welche tieferliegende Gründe für jeden Kausalzusammenhang aufzeigt.
4. Maßnahmendefinition und Implementierung: Im letzten Schritt werden Maßnahmen zur Anpassung des Systems und der Ressourcenallokation definiert. Aufgrund der Er-

[99] Vgl. Rooney, Vanden Heuvel (2004).

mittlung der Grundursachen in den vorigen Phasen können gezielte Maßnahmen implementiert werden, die künftigen Risikorealisierungen vorbeugen.

3.2.2.7.3 Anwendungsbeispiel

Ein interessantes, wenn auch nicht infrastrukturbezogenes Anwendungsbeispiel für eine klassische Fehlerursachenanalyse liefern etwa Weeks et al. (2004)[100]. Sie untersuchen ugandische Entbindungsstationen in Krankenhäusern und die häufigsten dort auftretenden Negativereignisse. Beispielhaft zeigt Abbildung 10 die Ergebnisse der RCA für das Ereignis „Hebamme kommt zu spät zur Arbeit“ auf. Durch wiederholte Kausalrückführungen können so am Ende, in Spalte 3, die Grundursachen für das Ereignis ausgemacht werden. Auf Basis dieser Erkenntnisse können dann wiederum Entscheidungen definiert und der Klinikleitung vorgelegt werden. Die Grafik folgt einer sehr systematischen und strengen „Why-Why-Why-Policy“, die darauf abzielt solange kausale Ursachen zu erforschen, bis eine sogenannte Grundursache ermittelt werden kann.

Die bereits erwähnte Studie liefert außerdem allgemeine Erkenntnisse über die Durchführung eines RCA. So deutet sie explizit auf die Wichtigkeit der Einbeziehung von Experten aus allen Fachbereichen, in diesem Fall sowohl das Gesundheitsministerium als auch erfahrene Mitarbeiter und Verwalter der Station, hin. Ferner betonen die Autoren mehrfach, dass die eigentliche Kausalanalyse, also Phase 2 aus obigem Modell, stets im Fokus stehen muss. Während RCA’s in der Anwendung oft bereits innerhalb der Datenerhebungsphase im Sande verlaufen, sichert eine vollständige Fokussierung auf Phase 2 den Erfolg der Analyse. In diesem Fall wurden Daten folglich stets, in Form eines Pull-Prozesses, dann ermittelt, wenn diese für die nächste „Why-Ebene“ wichtig waren.

[100] Weeks et al. (2004).

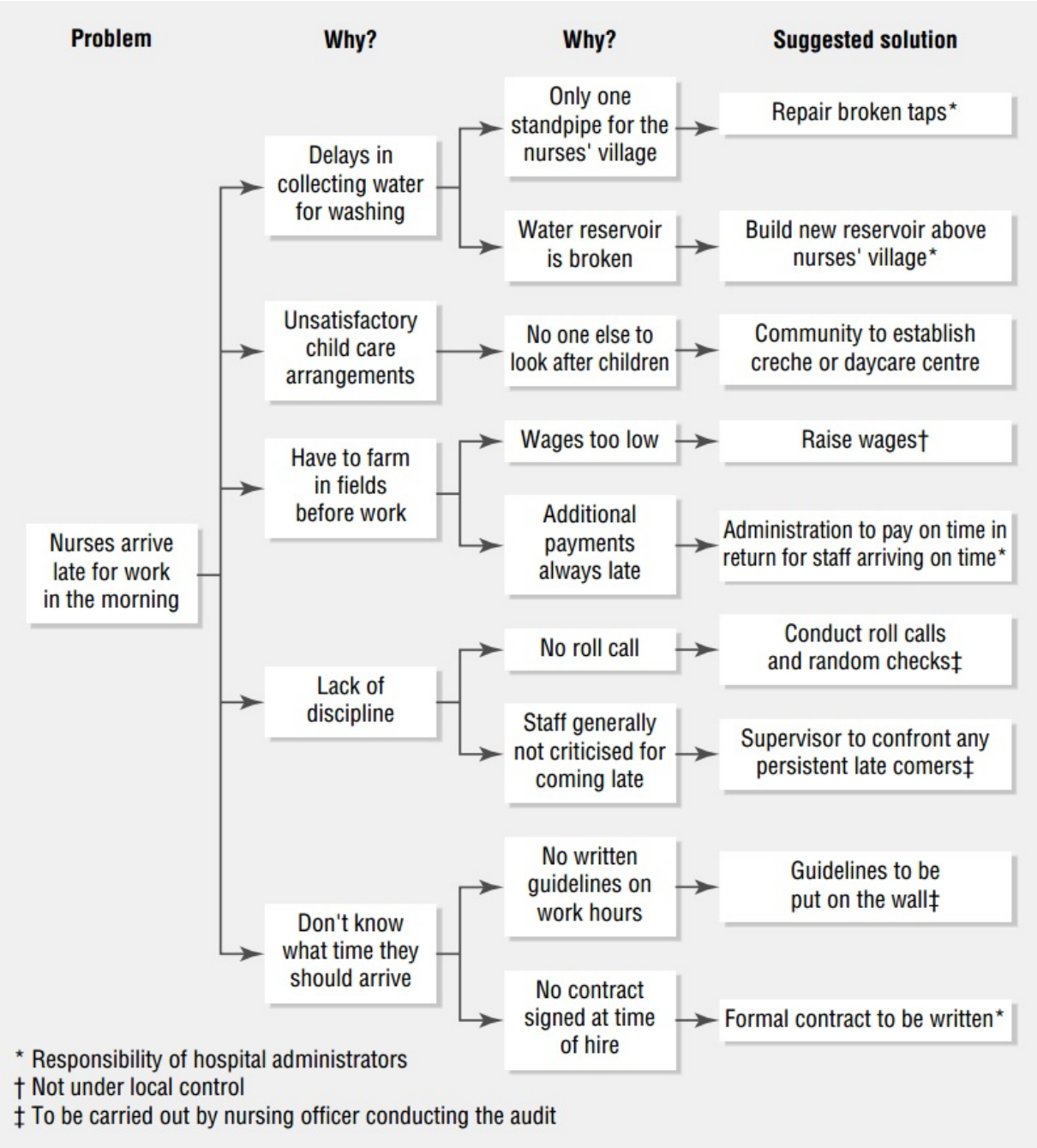


Abbildung 10: RCA für das Ereignis "Hebamme kommt zu spät zur Arbeit"[101]

3.2.2.7.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

[101] Quelle: Weeks et al. (2004).

3.2.2.7.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Bei der RCA werden sowohl umfangreiche quantitative Daten, insbesondere bei technischen Prozessen, benötigt, als auch Experteneinschätzungen aus allen betroffenen Bereichen.

3.2.2.7.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Der finale Output der RCA besteht aus einem Maßnahmenkatalog, deren Durchführbarkeit im Folgenden von einer Management-Ebene überprüft wird. Als Nebenprodukt liefert die RCA aber auch eine ausführliche Kausalkette, die zahlreiche andere negative Phänomene darstellt. Folglich ermittelt die RCA neben den qualitativen Handlungsempfehlungen auch quantitative Kenntnisse über den Gesamtprozess.

3.2.2.7.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Üblicherweise ist die Datenbeschaffungsphase die aufwendigste Phase des Verfahrens. Alleine die Sicherung, Aufbereitung und Präsentation aller benötigten Daten kann jedoch extrem aufwendig sein, vor allem bei komplexen, technischen Vorgängen.

3.2.2.7.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Bei der RCA kommen in der Regel mehrere Bereiche eines Unternehmens zum Einsatz. In den meisten Fällen reicht jedoch die Expertise der Mitarbeiter mittlerer Qualifikation vollkommen zur Bewertung der Kausalzusammenhänge aus.

3.2.2.7.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☒ Basic

☐ Evolved

☐ Advanced

☐ Leading

3.2.2.7.10 Stärken und Schwächen

Stärken	Schwächen
• Systematische Entwicklung eines „Risikopfades“ • Durch „Why-Why-Why-Analyse“ gut kommunizierbar • Exzellenter Ausgangspunkt für die Analyse und das Auffinden adäquater Frühwarnindikatoren (Key Risk Indikatoren, KRI). • In der Praxis sehr weit verbreitet; viele Good-/Best-Practice-Beispiele aus unterschiedlichen Branchen.	• Hoher zeitlicher Aufwand • Zugriff auf Experten aller Bereiche notwendig • Oft existiert nicht nur eine Ursache für ein auftretendes Problem, sondern mehrere Ursachen. Komplexe Ursachensysteme können mit der Fehler-Ursachen-Analyse nicht abgebildet werden.

Tabelle 15: Stärken und Schwächen der Fehlerursachenanalyse

3.2.2.7.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

Begründung: Aufgrund der strengen Kausalzusammenhangsketten scheint das Verfahren sehr gut zur Untersuchung von Risiken für kritische Infrastrukturen geeignet zu sein. Insbesondere lassen sich durch ausführliche und breit angelegte Untersuchung die kritischen Teile einer Infrastruktur selbst ermitteln.

3.2.2.8 Ishikawa-Diagramm

3.2.2.8.1 Einsatzzweck

Ein Ishikawa-Diagram, oder Fischgräten-Diagramm, ist eine grafische Darstellung von Wirkungsursachen, die ein einzelnes Ereignis beeinflussen. Eine Ishikawa-Analyse, die zugrundeliegende systematische Erstellung eines Ishikawa-Diagramms, ist somit ein Tool um Geschäftsprozesse und deren Effizienz zu untersuchen. Insbesondere dient eine Ishikawa-Analyse dazu Abhängigkeiten von Ereignissen aufzuzeigen.

3.2.2.8.2 Beschreibung

Die Ishikawa-Analyse, sowie das Ishikawa-Diagramm als dessen Ergebnis, wurden von dem japanischen Statistiker Kaoru Ishikawa 1986 entwickelt.[102] Die Ishikawa-Analyse sucht in einer klar strukturierten Form für Ursachen für ein zuvor klar definiertes Endereignis. Dieses Endereignis bildet entsprechend den „Kopf“ eines stilisierten Fischskelettes; daher wird es im englischen Sprachgebrauch häufig als „Fishbone Diagram“ bezeichnet. Die einzelnen Gräten bilden hierbei die sechs potenziellen Ursachenkategorien: Mensch, Maschine, Material, Umwelt, Methode und Prozess. In einer zweiten Ursachenfindungsebene werden in der Folge die einzelnen Gräten durch eine „Five-Why-Analyse“[103] weiter verzweigt. Hierbei wird etwa zunächst hinterfragt, welche menschlichen Faktoren das betrachtete Endereignis beeinflussen. Identifiziert man hierbei etwa die Ursache „Mitarbeiter ist kurzzeitig abwesend“ so wird eine entsprechend kleinere „Untergräte“ an die Gräte „Menschen“ angefügt. Diese Untergräte wird in der weiteren Analyse dann analog weiterverzweigt.[104]

3.2.2.8.3 AnwendungsbeispielAnwendungsbeispiel

Ein AnwendungsbeispielAnwendungsbeispielfindet sich, neben der bereits erwähnten Case Study für die Risikoidentifikation in einem Krankenhaus von Bose (2012), bei Canale et al (2005).

[102] Vgl. Ishikawa (1986).
[103] Siehe auch Beschreibung der Root-Cause-Analysis.
[104] Für eine Beschreibung der Ishikawa-Analyse siehe z.B. auch Bose (2012).

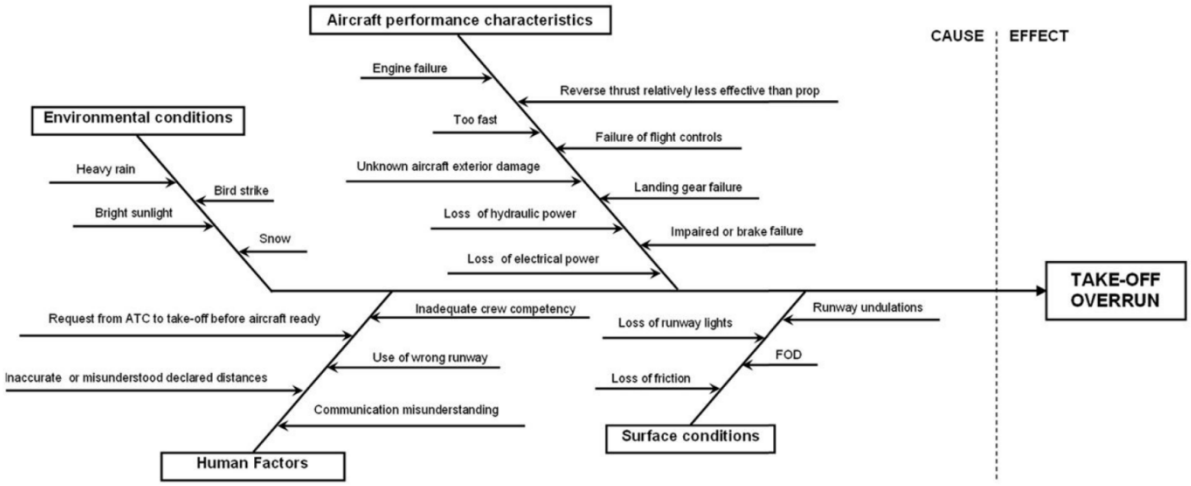


Abbildung 11: Ishikawa-Diagramm zum Endereignis "Take-off overrun"[105]

Den Richtlinien des Aviation Safety Network folgend untersuchen die Autoren insgesamt neun verschiedene mögliche Unglücksereignisse an einem Flughafen und identifizieren die Ursachen jeweils mittels eines Ishikawa-Diagramms. Beispielhaft sei hier das Endereignis „Take-Off Overrun“ genannt, also das Verlassen der Landebahn bei einem Start. In diesem speziellen Fall wurden die möglichen Ursachen für dieses Ereignis als menschliches Versagen, ein Problem mit dem Flugzeug, Umweltbedingungen und Defekte an der Landebahn identifiziert. Entsprechend wurden hier nur die vier relevanten „Hauptgräten“ definiert, welche im Folgenden durch eine „Why-Why-Analyse“ weiter verzweigt wurden.

Das Ergebnis, die grafische Darstellung, zeigt übersichtlich mögliche Risiken auf. Durch ebendiese übersichtliche Darstellung lassen sich künftig bei Starts die ermittelten Risiken leicht überprüfen und eventuell beheben.

Andererseits zeigt das Ergebnis auch die Schwächen der Ishikawa-Analyse und des Ishikawa-Diagramms auf. So sind alle Ursachen, also die Risiken selbst, gleichwertig repräsentiert. Eine Abstufung oder Hervorhebung von besonders folgenreichen oder besonders wahrscheinlich ist nicht möglich.[106] Ferner führt die sehr strukturierte Vorgehensweise zwar dazu „übliche Risiken“ zu ermitteln, schränkt jedoch das Aufdecken ungewöhnlicher Risiken gleichermaßen ein.[107]

[105] Quelle der Abbildung ist Canale et al (2005).
[106] Vgl. Ruhm (2004).
[107] Vgl. Straker (2010) und Watson (2004).

3.2.2.8.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.2.8.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

3.2.2.8.6 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Das Ergebnis ist eine grafische Repräsentation von Ursachen-Wirkungs-Relationen für vordefinierte Endereignisse.

3.2.2.8.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Vor allem die „Why-Why-Analyse“ muss regelmäßig wiederholt werden und ist oft sehr zeitintensiv.

3.2.2.8.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Da eine Ishikawa-Analyse lediglich auf Experteneinschätzungen basiert, wird fachreichendes Systemwissen verlangt um diese durchzuführen. Vor allem die „Five-Why-Analyse“ verlangt, aufgrund ihres iterativen Charakters, sehr gute und tiefgehende Kenntnisse des Systems in allen Teilen.

3.2.2.8.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☒ Basic

☐ Evolved

☐ Advanced

☐ Leading

3.2.2.8.10 Stärken und Schwächen

Stärken	Schwächen
• Strukturierte Vorgehensweise • Intuitiv-verständliche grafische Darstellung	• Zeitlich und personell aufwändiges Verfahren • Keine Gewichtung oder Priorisierung/Bewertung der Risiken • Nicht-lineare und komplexe Ursache-Wirkungsketten können nicht abgebildet werden

Tabelle 16: Stärken und Schwächen der Ishikawa-Analyse

3.2.2.8.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☐ sehr gut

☒ gut

☐ weniger geeignet

3.2.2.9 Ereignisbaumanalyse

3.2.2.9.1 Einsatzzweck

Die Ereignisbaumanalyse (engl.: Event Tree Analysis, ETA) ist ein induktives Verfahren zur Ermittlung eines möglichen Verhaltens und dessen Folgen innerhalb eines Systems.[108] Hierbei wird von einem Ereignis ausgegangen, welches möglicherweise ein Risiko beeinflussen

[108] Vgl. Liu (2012), S.70.

kann. Schließlich werden mögliche Folgen analysiert. Die betrachteten Ereignisse können hierbei sowohl interne Ereignisse sein (wie der Ausfall einer Komponente), aber auch externe Ereignisse, wie eine Naturkatastrophe.

ÜblicherweiseerfolgtenAnalyse und Verzweigung hierbei binär. Das Grundereignis löst hierbei jeweils einen Zustand 1 (intakt) oder 0 (defekt) eines Prozesses aus. Abhängig von dem Status dieses Prozesses wird die Folge für weitere Prozesse ermittelt. Durch dieses induktive Vorgehen ermittelt die ETA schlussendlich einen binären Vektor der den Zustand jeder einzelnen Komponente des Gesamtsystems beschreibt.

Trotz struktureller und grafischer Ähnlichkeiten unterscheidet sich die ETA grundlegend von der Fehlerbaumanalyse (FTA), welche ein deduktives Vorgehen verfolgt. Während bei der FTA ausgehend von einem Fehler eine Ursache deduktiv gesucht wird, sucht die ETA ausgehend von einem möglichen Versagen einer Komponente nach möglichen Auswirkungen.[109]

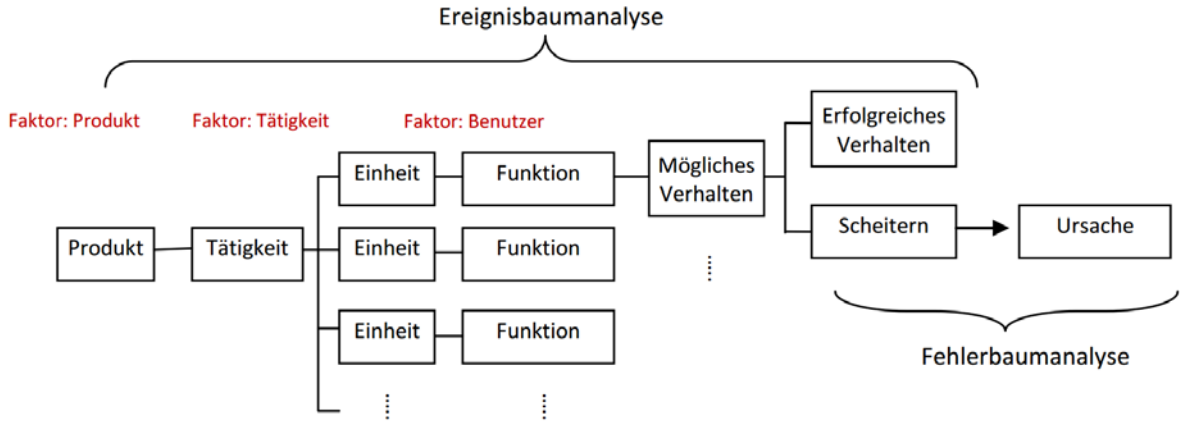


Abbildung 12: Zusammenhang Ereignisbaumanalyse und Fehlerbaumanalyse[110]

3.2.2.9.2 Beschreibung

Der erste Schritt einer jeden Ereignisbaumanalyse ist die klare Definition eines oder mehrerer sogenannter Initiatoren. Diese Initiatoren sind hierbei – zumindest im Rahmen des Risikomanagements – Unglücke, deren Folgen untersucht werden sollen und die die Wurzel des finalen Ereignisbaums darstellen.[111] Ausgehend von diesem Initiator werden induktiv Folgen ermittelt und in einer Baumstruktur dargestellt. Ist etwa der Initiator das Ereignis „Springflut“, so könnten die Folgeereignisse beispielsweise entweder „Frühwarnsystem wurde ausgelöst“ oder „Frühwarnsystem wurde nicht ausgelöst“ sein. Entsprechend entstehen, in diesem Fall zwei, Teilpfade, die anschließend weiter verzweigt werden. Hierbei wird häufig, jedoch nicht immer, binär verzweigt. So lässt etwa die Folge „Wasserstand“ offensichtlich mehr als zwei

[109] Vgl. Liu (2012), S.71.
[110] Quelle: Liu (2011), S. 71.
[111] Vgl. Andrews, Dunnett (2000)

mögliche Ausprägungen zu. Die Blätter des Ereignisbaumes bilden am Ende per Konstruktion mögliche Endzustände. Der Pfad zu diesen erlaubt es ferner die Wahrscheinlichkeit des Eintretens eines solchen Endzustandes zu berechnen, indem die Wahrscheinlichkeiten der einzelnen Teilpfade multipliziert werden.

3.2.2.9.3 Anwendungsbeispiel

Ferdous et al (2011) untersuchten in Form einer Case Study explizit das Grundereignis „schwerwiegender Austritt von LPG-Gas an einer Pipeline“ und seine Folgen durch eine Ereignisbaumanalyse. Ziel der Autoren war, neben der grafischen Darstellung unten vor allem eine quantitative Studie durchzuführen, die abschätzen sollte, wie genau die ermittelten Wahrscheinlichkeiten der Endszenarien sind. Folgend der untenstehenden Grafik und den dort aufgezeigten Wahrscheinlichkeiten kommen sie etwa zu dem Schluss, dass mit einer Wahrscheinlichkeit von 0,9 * 0,9 = 0,81 (= 81 %) ein Feuerball entsteht, wenn eine größere Menge Gas an einer Pipeline austritt.

Gerade die stochastische Auswertung der Folgen des Gasaustritts innerhalb der Energieinfrastruktur bietet aber auch Grund zur Kritik an der Ereignisbaumanalyse. So scheint vor allem die Annahme der stochastischen Unabhängigkeit einzelner Folgeereignisse in der Realität selten gegeben zu sein und andererseits sind genaue Eintrittswahrscheinlichkeit in der Praxis nahezu nie vorhanden, insbesondere bei eher seltenen Risiken in Infrastrukturen.[112]

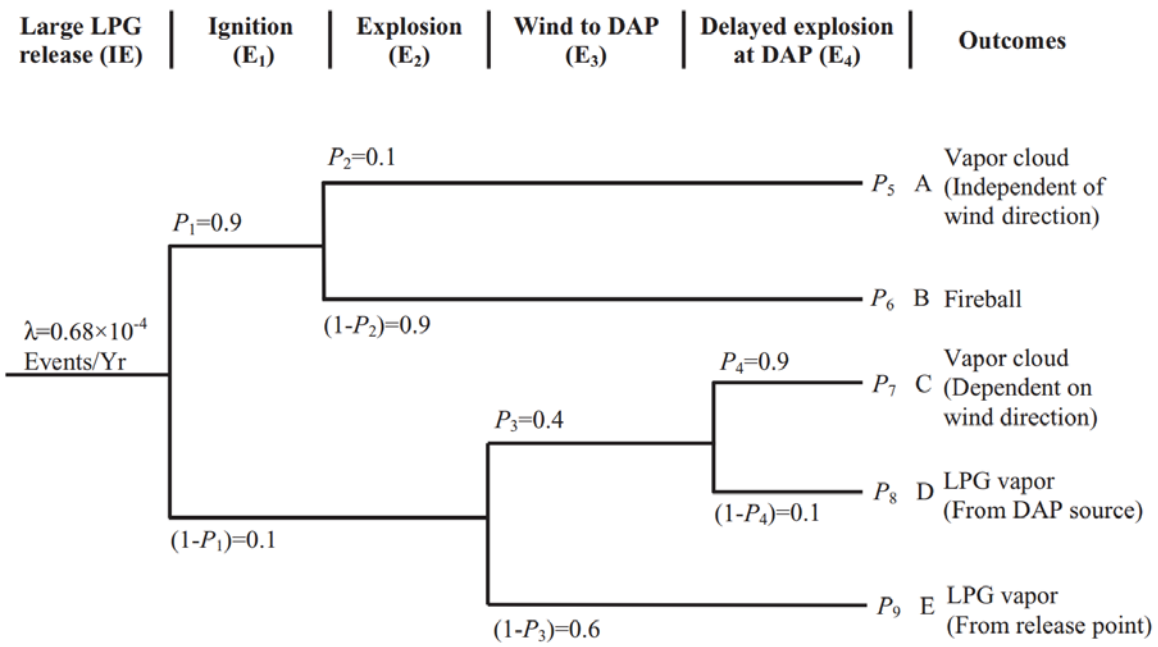


Abbildung 13: Ereignisbaumanalyse[113]

[112] Vgl. Ferdous et al (2011), S. 106.
[113] Quelle: Ferdous et al (2011), S.89.

3.2.2.9.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.2.9.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Einerseits fließt Expertenwissen in den Aufbau des Baumes selbst direkt ein. Andererseits fließen, in Form von Wahrscheinlichkeiten, auch quantitative Daten in die Analyse ein.

3.2.2.9.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Der reine Aufbau der Baumes zeigt qualitativ die Wirkungszusammenhänge nach dem Eintreffen eines Unglückes auf. Die aufmultiplizierten Wahrscheinlichkeiten liefern ferner eine quantitative Aussage über die Eintrittswahrscheinlichkeit jedes Endzustandes.

3.2.2.9.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Die Erstellung eines einzelnen Ereignisbaumes ist in der Regel zeiteffizient möglich. Nutzt man die Ereignisbaumanalyse jedoch für eine umfassende Gesamtanalyse der Auswirkungen verschiedener Risiken auf das Gesamtsystem und seine Teile, so werden zahlreiche Ereignisbäume erstellt.

3.2.2.9.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Vor allem für die Auswertung der Eintrittswahrscheinlichkeiten sind statistische Kenntnisse notwendig. Ferner wird tiefgreifende Strukturexpertise benötigt um einen Ereignisbaum möglichst vollumfänglich zu erstellen.

3.2.2.9.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☒ Evolved

☐ Advanced

☐ Leading

3.2.2.9.10 Stärken und Schwächen

Stärken	Schwächen
• Einzelne Ereignisbäume bieten sehr übersichtliche Struktur • Liefert qualitative und quantitative Erkenntnisse	• Vollumfängliche Analyse erfordert eine Vielzahl einzelner Bäume, was der Übersicht abträglich ist • Sammelt überwiegend bereits bekanntes Strukturwissen • Komplexe Abhängigkeiten oder Wirkungsketten sowie Iterationen können nicht abgebildet werden

Tabelle 17: Stärken und Schwächen der Ereignisbaumanalyse

3.2.2.9.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

Begründung: Da logistische Infrastrukturen in aller Regel in vielfacherweise miteinander verwoben sind, entstehen sehr schwer identifizierbare Wirkungszusammenhänge. Diese kann eine ETA durch die strukturierte Vorgehensweise aufzeigen und anschaulich darstellen.

3.2.2.10 Markov-Analyse

3.2.2.10.1 Einsatzzweck

Die Markov-Analyse (benannt nach dem russischen Mathematiker Andrei Andrejewitsch Markow, 1856-1922) wird im Kontext des Risikomanagements angewendet, um zufällige Zustandsänderungen eines Systems zu modellieren (Random Walk), falls man davon ausgehen darf, dass die Zustandsänderungen nur über einen begrenzten Zeitraum hinweg Einfluss aufeinander haben oder sogar gedächtnislos sind. So können beispielsweise Ausfallwahrscheinlichkeiten oder Verfügbarkeitswahrscheinlichkeiten analytisch ermittelt werden. Mit Hilfe der so ermittelten Wahrscheinlichkeiten kann in der Folge ein System stochastisch auf Schwachstellen, also Elemente mit hoher Ausfallwahrscheinlichkeit, untersucht werden.

Aufgrund der rechnerischen Komplexität und den ausführlichen benötigten Daten, die in der Regel aus langfristigen Analysen des Systems gewonnen werden müssen, um aussagekräftig zu sein, wird die Markov-Analyse hauptsächlich auf sich durchgehend wiederholende Prozesse angewandt, die komplex aufgebaut sind und zufälligen Einflüssen ausgeliefert sind. Markov-Prozesse kennzeichnen einen stochastischen Prozess. Hierbei wird zwischen kontinuierlichen und diskreten Prozessen unterschieden. Handelt es sich um einen diskreten Prozess, so wird dieser auch als Markov-Kette bezeichnet. Eine Markov-Kette ist eine Folge von Zufallsexperimenten, bei der die Wahrscheinlichkeit in Schritt n einen bestimmten Zustand anzunehmen lediglich vom Zustand in Schritt (n-1) abhängt und nicht von der weiter zurückliegenden „Vorgeschichte“ des Prozesses.

Eine Stärke der Markov-Analyse ist, dass sie eine präzise Aussage über Ausfallwahrscheinlichkeiten (etwa in Ratingmodellen) auch dann ermöglicht, wenn starke Abhängigkeiten zwischen den einzelnen Teilprozessen bestehen.[114] In diesem Kontext sind Markov-Ketten ein in der Praxis häufig verwendetes Modell zur Beschreibung von Systemen, deren Verhalten durch einen zufälligen Übergang von einem Systemzustand zu einem anderen Systemzustand gekennzeichnet ist.

3.2.2.10.2 Beschreibung

Um einen Markov-Prozess auf seine Verlässlichkeit hin zu prüfen, muss dieser zunächst in Form einer Markov-Kette modelliert werden. Eine solche Markov-Kette kann dabei etwa die zeitliche Entwicklung von Objekten oder Systemen beschreiben, die zu jedem Zeitpunkt jeweils nur eine von endlich vielen Zuständen annehmen können.

Als Datenbasis für die Modellierung der Markov-Kette werden hierzu folgende Komponenten als Input benötigt:

1. Die Menge der endlich-vielen möglichen Zuständen, genannt Zustandsraum.

[114] Vgl. Weber et al. (2012).

2. Die Wahrscheinlichkeiten, dass das Objekt, beziehungsweise das System, sich im zum Ausgangszeitpunkt in einem bestimmten Zustand befindet. Diese Wahrscheinlichkeiten, die in Summe eine Wahrscheinlichkeit von 1 ergeben müssen, definieren die Anfangsverteilung.
3. Eine Matrix, welche Übergangswahrscheinlichkeiten enthält, also die Wahrscheinlichkeit, dass Zustand i zu j im nächsten zeitdiskreten Schritt wird.

Die Gesamtheit der Daten aus 1 bis 3 nennt man Markov-Kette.[115] Der Begriff der Kette rührt daher, dass der Zustand des Systems zu jedem beliebigen Zeitpunkt ausschließlich von dem Zustand in der unmittelbaren Vorgängerperiode abhängt. Die entsprechende Wahrscheinlichkeit lässt sich folglich aus der Matrix der Übergangswahrscheinlichkeiten ableiten.

Es wird angenommen, dass die Menge der möglichen Zustände endlich viele Elemente s_1, …, s_L enthält. Eine Markov-Kette wird durch eine Migrationsmatrix beschrieben, deren i-te Zeile die Wahrscheinlichkeiten angibt, in einem Schritt von Zustand s_i in die Zustände s_1, …, s_L zu migrieren. Die Migrationsmatrix hat daher die Dimension LxL.

Ein Beispiel für eine Markov-Kette sind die Ratingmigrationen von Unternehmen. Ein Unternehmen hat beispielsweise das Rating 4 zu Beginn eines Jahres und wird dann mit gewissen Wahrscheinlichkeiten zum Jahresende hin in Rating 1-L migrieren. Dieses Vorgehen lässt sich auch auf Infrastrukturinvestitionen übertragen, um beispielsweise die zeitliche Entwicklung von (kritischen) Infrastrukturprojekten zu evaluieren.

Mit Hilfe der Modellierung des Prozesses lassen sich so stationäre Wahrscheinlichkeiten ermitteln, also die Wahrscheinlichkeit, dass ein bestimmter Zustand in einer bestimmten Zeitperiode eintritt. So kann man etwa bei einem komplexen System präzise die Wahrscheinlichkeit eines Ausfalls berechnen, indem man diesen als einen möglichen Zustand definiert.

3.2.2.10.3 Anwendungsbeispiel

Klassische Beispiele für Markov-Ketten sind durch sogenannte „zufällige Irrfahrten“ gegeben, die auch als „Random Walk“ bezeichnet werden.[116]

Zahlreiche finanzmathematische Bewertungs- und Risikomodelle – beispielsweise die Black/Scholes-Formel sowie das Varianz-Kovarianz-Modell – bauen auf einem Random Walk (und damit einer Markov-Kette) auf. In Anlehnung an eine Parabel von Murray kann dieser zufällig gewählte Pfad wie der Weg eines „Betrunkenen“ betrachtet werden.[117] Wenn der Betrunkene auf seinem Heimweg eine Teilstrecke zurückgelegt hat, ist ungewiss, welche Richtung er als nächstes einschlagen wird und welche Entfernung er dann in dieser Richtung

[115] Vgl. Putermann (1990).
[116] Vgl. Romeike/Eicher (2017).
[117] Vgl. Kim/Malz/Mina (1999), S. 87 ff.

hinter sich lässt. Die insgesamt von dem „Betrunkenen“ zurückgelegte Wegstrecke setzt sich aus mehreren Teilschritten zusammen, die jeder für sich betrachtet bezüglich der Richtung und Länge ebenso zufällig und unabhängig vom vorherigen Schritt sind wie die daraus entstehende Gesamtentfernung vom Ursprungspunkt.[118] Random Walks können auf unterschiedliche Weise generiert werden, zum Beispiel als echter Zufallsprozess, als Prozess mit bestimmten Mustern in der zeitlichen Entwicklung der Volatilitätscluster sowie mit oder ohne Trends.

Eine solche Stochastizität lässt sich auch relativ einfach auf Infrastrukturprojekte und deren Entwicklung über die Zeit (Nutzungsdauer über die Zeit etc.) übertragen.

In Abbildung 14 wird gezeigt, wie sich die in einem Random Walk zurückgelegte Entfernung S von seinem ursprünglichen Standpunkt aus den einzelnen Schritten S_1 bis S_6 zusammensetzen könnte. Der Random Walk startet vom Ausgangspunkt A_0 beginnend in eine zufällige Richtung und legt dabei eine Strecke S_1 zufälliger Länge zurück. An dem nächsten Punkt A_1 angekommen, wird wieder eine Strecke S_2 zufälliger Länge in eine zufällige Richtung beschritten. Nach sechs Schritten wird der Punkt A_6 erreicht. Die einzelnen Schritte S_i eines Random Walk lassen sich mit Hilfe von Vektoren beschreiben. In Abbildung 14 ist jeder Schritt ein zweidimensionaler Vektor. Der erste Schritt S_1 wäre beispielsweise ein Vektor mit den Elementen $x = 2$ und $y = 3$. Werden vom Punkt A_0 beginnend aus zwei Einheiten nach rechts und drei Einheiten nach oben zurückgelegt, wird der Punkt A_1 erreicht. Bei einem negativen x und y würde die Bewegung genau in die entgegengesetzte Richtung führen. Entsprechend lassen sich die restlichen Schritte S_2 bis S_6 als Vektoren ausdrücken. Die Summe der sechs Schritt-Vektoren S_i ergibt den Random Walk, welcher selbst einen Vektor S darstellt und die Bewegung von A_0 nach A_6 beschreibt. Jeder Vektor S kann deshalb als eine Summe von n einzelnen Schritt-Vektoren S_i aufgefasst werden oder selbst ein Schritt-Vektor eines übergeordneten Random Walks sein. Diese Eigenschaft wird als Selbstähnlichkeit bezeichnet. Weil die Länge und Richtung der einzelnen Vektoren vom Zufall abhängig ist, ist auch der daraus entstehende Random Walk ein Zufallsprozess.

[118] Vgl. Romeike/Hager (2010).

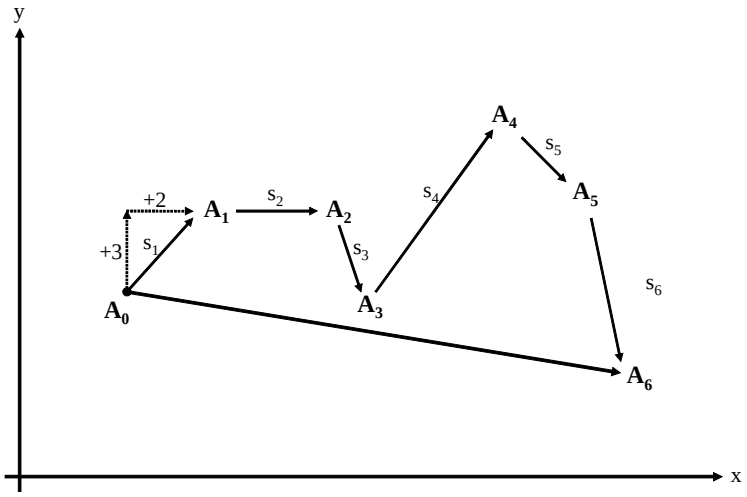


Abbildung 14: Beispiel für einen Random Walk[119]

Für statistische Aussagen sind viele Random Walks mit der gleichen Anzahl n von Schritten (Vektoren) notwendig, denn erst bei einer großen Anzahl von zufälligen Bewegungen kann etwas über deren mittlere Entfernung vom Ursprungspunkt ausgesagt werden. Dabei hängt die mittlere Entfernung von der Anzahl n der Schritt-Vektoren S_i ab, denn der Summen-Vektor S wird umso länger, je mehr Schritt-Vektoren S_i vorhanden sind.

In diesem Kontext ist das Wurzelgesetz von großer Relevanz: Standardabweichung (S) = σ(S) ~ $\sqrt{n}$

Auf dem Fundament von Random Walk und Wurzelgesetz beruhen zahlreiche Simulation im Risikomanagement. Die Standardparametrisierung von stochastischen Simulationen (Monte Carlo Simulation) enthält häufig eine Normalverteilung für den Random Walk, kombiniert mit der Skalierung der Volatilität auf einen längeren Planungshorizont mit Hilfe des Wurzelgesetzes.

Abbildung 15 zeigt beispielhaft eine von vielen möglichen Realisationen eines Zufallsprozesses (beispielsweise Preisentwicklung über die Zeit; in diesem Fall 30 Zeiteinheiten).

[119] Quelle: Romeike/Hager (2010), S. 11.

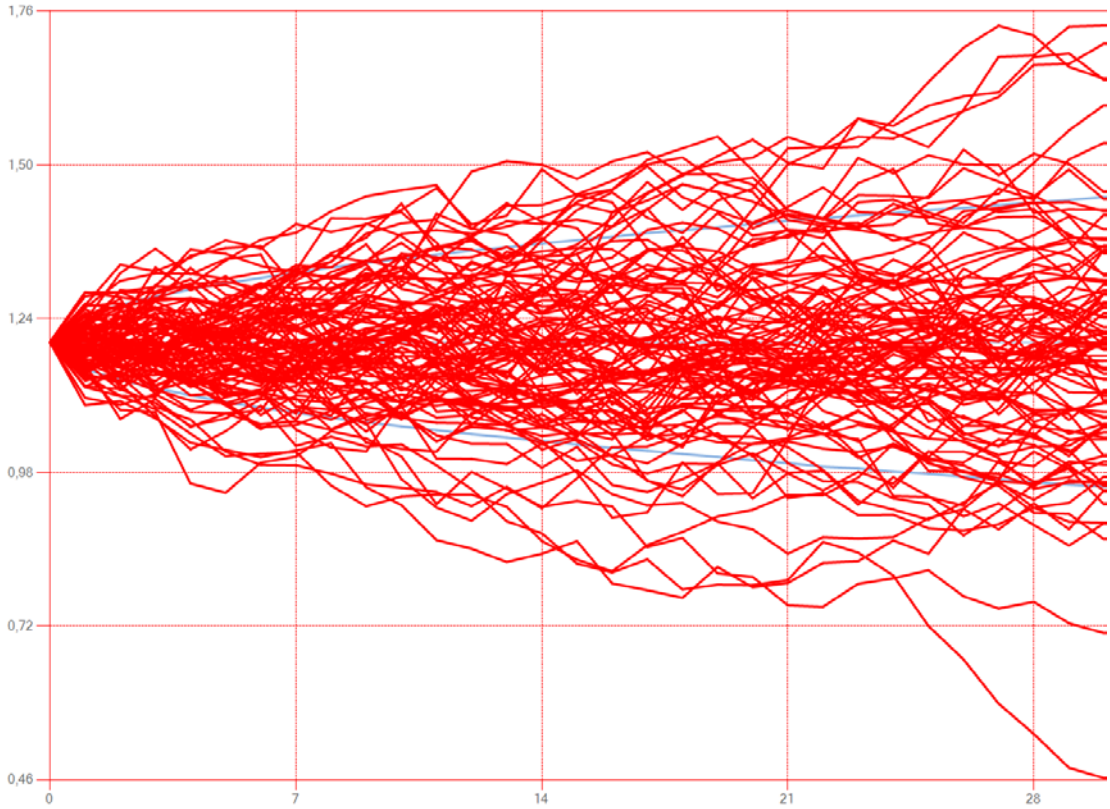


Abbildung 15: Random Walk für die zukünftige Entwicklung des Dieselpreises[120]

Um einen Random Walk für die Entwicklung eines Risikofaktors unterstellen zu dürfen bedarf es einer Reihe von Annahmen. Insbesondere müssen die einzelnen Schritte unabhängig voneinander sein. Statt einer Normalverteilung können alternativ verteilte Zufallszahlen verwendet werden, statt dem Random Walk sind alternative Zufallsprozesse denkbar. Die Annahmen und Prämissen ändern sich, aber ob diese Annahmen in der Realität erfüllt werden muss der Risikomanager entscheiden.[121]

3.2.2.10.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☒ Risikobewertung

☒ Risikosteuerung

[120] Quelle: RiskNET – The Risk Management Network sowie Romeike/Eicher (2017).
[121] Vgl. Romeike/Hager (2010).

3.2.2.10.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☒ Expertenschätzung

3.2.2.10.6 Output

☐ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☒ rein quantitativ

Beschreibung des Outputs: Das Ergebnis ist eine Wahrscheinlichkeit zwischen 0 und 1 dafür, ob ein System (oder eine Komponente) in einer bestimmten Periode ausfällt.

3.2.2.10.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☒ mittel

☒ hoch

Begründung: Der methodische und zeitliche Aufwand der Methode ist hoch.

3.2.2.10.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Zur Durchführung einer Markov-Analyse wird hochqualifiziertes Personal mit tiefgreifenden analytischen Kenntnissen im Bereich der Stochastik benötigt.

3.2.2.10.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☐ Evolved

☒ Advanced

☒ Leading

Erläuterung: Markov-Ketten liegen vielen stochastischen Prozess-Simulationen (beispielsweise Wiener Prozess oder GBM) zu Grunde. Markov-Ketten werden vor allem im Bereich der Finanzmarktmodellierung und bei Ratingmodellen intensiv genutzt. In der Versicherungsmathematik werden diskrete Markov-Ketten verwendet zur Berücksichtigung biometrischer Risiken (Invalidisierungswahrscheinlichkeiten, Sterbewahrscheinlichkeiten etc.). Auch im Bereich von Infrastrukturprojekten ist eine Anwendung möglich, um beispielsweise die zeitliche Entwicklung einer Infrastrukturinvestition abzubilden.

3.2.2.10.10 Stärken und Grenzen

Stärken	Grenzen
• Zufällige Zustandsänderungen eines Systems können relativ einfach modelliert werden (siehe auch GBM-Modellierung). • Relativ leichte Modellierung von stochastischen Netzen. • Das Grundprinzip von Markov-Ketten ist leicht verständlich und kommunizierbar. • Sehr effiziente Algorithmen bei geringem Aufwand (insbesondere bei Verwendung stochastischer IT-Werkzeuge).	• Große Rechenkomplexität. • Hohe mathematische/stochastische Fachkompetenz erforderlich. • In der Praxis können beispielsweise mit einem Random Walk nur sehr begrenzt extreme Stressszenarien abgebildet werden.

Tabelle 18: Stärken und Grenzen der Markov-Analyse

3.2.2.10.11 Gesamtbewertung/Eignung für das Risikomanagement

☒ sehr gut

☒ gut

☐ weniger geeignet

Begründung: Für Risiken in Bereich von Infrastrukturrisiken ist eine Anwendung der Markov-Analyse sinnvoll anwendbar, um beispielsweise die Frage zu beantworten, wie lange die Infrastruktur der Gesellschaft zur Verfügung steht. Alterungseffekte sollten hierbei nicht berücksichtigt werden beziehungsweise sollten durch Investitionen in Wartung und Instandhaltung eliminiert werden.

3.2.2.11 Social Network Analysis

3.2.2.11.1 Einsatzzweck

Die Social Network Analysis ist eine mathematische Methode, die einzelne Akteure und Interaktionen zwischen diesen innerhalb eines Netzwerks untersucht. Die Methode versucht, das Verhalten der Mitglieder eines Netzwerkes zu verstehen und vorherzusagen und auf Basis dieser Vorhersagen und Erkenntnisse die eigentliche Entscheidungsfindung der einzelnen Akteure zu verstehen.[122]

Die Social Network Analysis wird üblicherweise in den Sozialwissenschaften angewandt, um Dynamiken innerhalb einer Personengruppe besser zu verstehen und so systemkritische Akteure zu identifizieren. Insbesondere wird die Social Network Analysis auch in der Kriminalistik verwendet, um die verwundbarsten und kritischsten Akteure einer „Zelle“ zu identifizieren und so durch die Verhaftung einzelner Akteure die gesamte Zelle maximal zu schwächen.[123]

Die Anwendung lässt sich auch auf logistische Netzwerke übertragen, um die kritischen und störungsanfälligen Akteure oder Knotenpunkte einer Infrastruktur zu identifizieren.

3.2.2.11.2 Beschreibung

Die Social Network Analysis im engeren Sinne wird stets auf eine bereits bestehende Menge von Akteuren angewendet und kann als eine mathematische Methode zur „Verbindung der Knoten“[124] verstanden werden. Die Akteure selbst werden hierbei zunächst als Knoten eines Netzwerks modelliert. Die Kanten dieses Netzwerks werden anschließend als Hauptaufgabe der Social Network Analyse erstellt. Jede Kante zwischen zwei Akteuren A und B symbolisiert hierbei eine Beziehung zwischen A und B in einer beliebigen Form, beispielsweise Warenaustausch oder Kommunikation.

Hierzu werden die Intensitäten der Verbindungen gemessen bzw. beobachtet, zum Beispiel in Form der Höhe des Warenflusses oder in Form der Häufigkeit von Interaktionen. Anhand

---

[122] Vgl. Renfro, Deckro (2001).
[123] Vgl. Koschade (2006) .
[124] Vgl. Krebs(2002).

dieser Beobachtung wird das „soziale“ Netzwerk durch Hinzufügen von Kanten unterschiedlicher Stärke modelliert.

In einem zweiten Schritt kann das entstandene Netzwerk auf Schwachpunkte untersucht werden. Hierbei werden verschiedene graphentheoretische Konzepte verwendet, um die Knoten des Graphs zu bewerten. Insbesondere werden hierzu der Knotengrad, die „Betweenness-Zentralität“ und die Nähe der einzelnen Knoten gemessen, um deren Kritikalität für das Gesamtnetzwerk zu quantifizieren.

Anhand der Ergebnisse einer solchen Analyse lassen sich für die Funktionalität kritische Knoten, und somit Akteure, identifizieren. Entfällt ein solcher, kritischer Knoten, sind die Auswirkungen auf das gesamte Netzwerk besonders schwerwiegend, da etwa verschiedene Teilbereiche überhaupt nicht mehr oder nur noch über bedeutend längere Wege miteinander vernetzt sind.

3.2.2.11.3 Anwendungsbeispiel

Choi und Hong (2002)[125] modellierten in Ihrer Arbeit die kompletten Supply Chains verschiedener Produkte aus der Automotive-Branche als „Soziales Netzwerk“, wobei Verbindungen zwischen Knoten in diesem Fall Warenflüsse darstellen. Beispielhaft sei das Zuliefernetzwerk für das Modell „Accord“ des Autoherstellers Honda dargestellt (vgl. Abbildung 16)

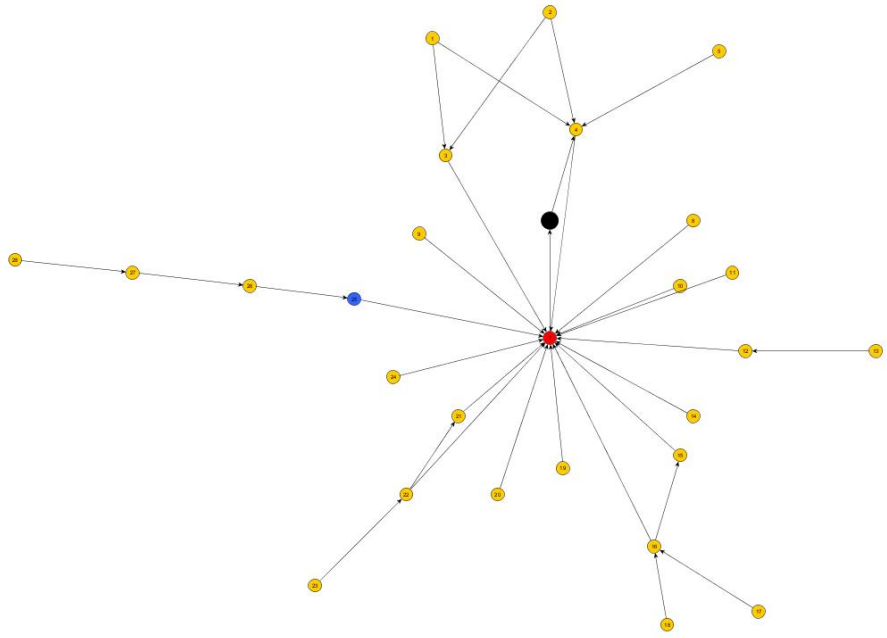


Abbildung 16: Social Network der Produktion des Honda Accord[126]

[125] Vgl. Choi, Hong (2002).
[126] Quelle: Kim et al (2011), S. 200.

Bemerkenswert ist vor allem, dass Honda (in Abbildung 16 schwarz hervorgehoben) selbst auf den ersten Blick nicht sonderlich kritisch oder zentral für die Lieferkette zu sein scheint. (Bei anderen Szenarien in der Automotive-Industrie war diese Dezentralität des eigentlichen Herstellers sogar noch ausgeprägter.) Vielmehr scheint der Zulieferer CVT (in Abbildung 16 rot hervorgehoben) der kritischste Akteur in diesem Materialflussnetzwerk zu sein. Eine qualitative Analyse verschiedener Zentralitätskonzepte bestätigt diesen Eindruck und ermittelte etwa für CVT eine Betweenness-Zentralität[127] von 13, während Emhart (in Abbildung 16 blau hervorgehoben), ein weiterer Zulieferer mit der insgesamt zweithöchsten Betweenness-Zentralität, lediglich einen Wert von 2 erreicht. Folglich ist vor allem der Zulieferer CVT enorm wichtig für die Funktionalität des Produktionsnetzwerks. Umgekehrt ist Honda offenbar stark abhängig von der Zuverlässigkeit der Zulieferers CVT und wäre bei Ausfall dessen, etwa durch Streik, nicht in der Lage, weiter das Modell „Accord“ zu produzieren.

Diese Analyse, basierend auf den unidirektionalen Materialflüssen innerhalb des Netzwerks, ermittelt also eindeutig den Knoten CVT als kritischsten Punkt innerhalb des „Social Networks“. Dies impliziert ein erhebliches Risiko beim Zulieferer CVT, deren Insolvenz oder Unproduktivität aus anderen Gründen, nur schwerlich abgefangen werden könnte.

3.2.2.11.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☒ Risikobewertung

☐ Risikosteuerung

3.2.2.11.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☐ Expertenschätzung

Beschreibung: Zur Darstellung und Modellierung des Netzwerkes werden historische Daten, vor allem über vorige Interaktionen zwischen einzelnen Knoten, benötigt.

[127] Die Betweenness-Zentralität eines Knotens v ist die Anzahl der kürzesten Wege im Graphen die durch den Knoten v laufen. Hierbei werden alle kürzesten Wege zwischen zwei beliebigen Knoten im Graphen berücksichtigt.

3.2.2.11.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Der Output ist zunächst eine Menge von Knotenbewertungen, welche die Kritikalität eines einzelnen Knotens quantitativ beschreiben. Aus diesen Bewertungen lassen sich wiederum qualitative „Rankings“ ableiten.

3.2.2.11.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Üblicherweise ist die Konstruktion des „sozialen Netzwerkes“ sehr arbeits- und zeitintensiv, da Daten langfristig und detailliert beobachtet werden müssen.

3.2.2.11.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Für die Konstruktion des Netzwerkes werden gut qualifizierte Experten benötigt, die Warenflüsse oder Transaktionshäufigkeiten beobachten und strukturieren können.

3.2.2.11.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☐ Evolved

☒ Advanced

☒ Leading

Erläuterung: Die Social Network Analysis wird bisher hauptsächlich in den Sozialwissenschaften und mit Bezug auf menschliche Akteure betrieben. In diesem Bereich hat sie sich seit einiger Zeit etabliert und wird regelmäßig zur Beobachtung von komplexen menschlichen Gruppen benutzt. Die Anwendung im Risikomanagement ist hingegen relativ neu und entsprechend wenig verbreitet.

3.2.2.11.10 Stärken und Schwächen

Stärken	Schwächen
• Zahlreiche Verfahren aus der Graphentheorie lassen sich auf das fertige Netzwerk anwenden • Netzwerk-Struktur liefert eine sehr intuitve Darstellung für Infrastukturen • Auch komplexe Netzwerke lassen sich (grafisch) abbilden.	• Bisher kaum im Risikomanagement-Kontext erprobt • Modellaufbau sehr komplex und aufwendig • Empirische Daten für die Modellierung erforderlich.

Tabelle 19: Stärken und Schwächen der Social Network-Analyse

3.2.2.11.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

Begründung: Aufgrund der natürlichen Analogie zwischen einem sozialen Netzwerk und einem logistischen Infrastrukturnetzwerk bietet sich die Methode zur Anwendung im Risikomanagement für kritische Infrastrukturen in der Logistik an.

3.2.3 Kreativitätsmethoden

3.2.3.1 Morphologische Verfahren

3.2.3.1.1 Einsatzzweck

Ein morphologisches Verfahren (oder eine morphologische Analyse) ist eine Methode, um für eine bestimmte Problemstellung sämtliche möglichen Zusammenhänge der beeinflussenden Parameter zu identifizieren und zu analysieren.[128] Die Methode kann im Risikomanagement dazu genutzt werden, die Kombination von Ursachen, aber auch Auswirkungen für ein spezifisches Risiko zu identifizieren und zu analysieren. Sie gilt als nicht-quantitative Methode, bei der diskrete, voneinander unabhängige Variablen genutzt werden. Sie verwendet zur struktu-

[128] Vgl. Ritchey (2011a), S. 84 sowie Romeike, Hager (2013), S. 109.

rierten Darstellung den morphologischen Kasten (häufig auch Zwicky-Box, benannt nach dem Schweizer Astrophysiker Fritz Zwicky, 1898-1974).

3.2.3.1.2 Beschreibung

Die morphologische Analyse[129] wird in mehreren, in der Regel vier, Schritten durchgeführt:[130]

1. Beschreiben Sie die Fragestellung bzw. das Problem.
2. Sammeln Sie Parameter, die für die Beantwortung relevant sind. Zunächst werden die wichtigsten Dimensionen eines Problems (hier: eines Risikos) identifiziert und definiert. Für jede dieser Dimensionen werden anschließend die möglichen Ausprägungen oder Zustände identifiziert und festgelegt, die eine Dimension annehmen kann; sie werden als Variablen oder Parameter bezeichnet.
3. Sammeln Sie Ausprägungen pro Parameter. Die Anzahl der Ausprägungen kann je Parameter unterschiedlich sein.Damit ist das morphologische Feld aufgestellt, für das im nächsten Schritt Konfigurationen untersucht werden, die eine bestimmte Kombination von Ausprägungen oder Zuständen je Dimension repräsentieren. Da die Anzahl der Konfigurationen selbst bei einer geringen Anzahl an Variablen erhebliche Ausmaße annehmen kann, ist es sinnvoll, das Feld zu reduzieren. Hierzu dient das cross-consistency assessment (CGA), bei dem durch einen paarweisen Vergleich eruiert wird, ob ein Variablenpaar existieren kann oder nicht. Die Größe des morphologischen Felds kann mit der CGA üblicherweise um 90 bis 95 Prozent reduziert werden.
4. Kombinieren Sie die unterschiedlichen Ausprägungen der Parameter miteinander! Die verbleibenden Konfigurationen können dann als interaktives Referenzmodell für die detaillierte Analyse genutzt werden. Insbesondere durch Einsatz geeigneter Software kann jede Variable (oder Kombinationen von Variablen) als Input oder als Output genutzt werden, um sich die mit dieser Variable verbundenen weiteren Variablen anzeigen zu lassen.

Sinnvollerweise wird die morphologische Analyse durch Gruppen (einzeln oder getrennt) durchgeführt.

3.2.3.1.3 AnwendungsbeispielAnwendungsbeispiel

Ritchey verdeutlicht die Anwendung der morphologischen Analyse im Rahmen der Gefahrenanalyse für Nukleartransporte.[131] Dabei stand folgende Frage im Fokus der Untersuchung:

[129] In der englischsprachigen Literatur wird die morphologische Analyse auch als „general morphological analysis“ (GMA) bezeichnet.
[130] Vgl. Ritchey (2011b), S. 12-14.

„What are the most important factors involving the transport of nuclear material and nuclear waste, as concerns conditions and regulations for protective measures, and how do these factors relate to each other?“[132] Jeder im ersten Schritt identifizierte Parameter mit einer bestimmten Ausprägung kann als primärer Auslöser fungieren; die Analyse zeigt dann, welche der anderen Parameter mit welchen Ausprägungen als besonders relevant (oder als wahrscheinlich) gelten.

Die Methode wurde von Ritchey im Rahmen des Risikomanagements auch auf andere Fragestellungen angewandt, beispielsweise auf die Evaluierung von unterschiedlichen Großrisiken (Naturkatastrophe, Pandemie, Terrorismus).[133] Auch die Analyse von Risiken für Nuklearanlagen wurde mittels der morphologischen Analyse untersucht.[134]

In Tabelle 20ist exemplarisch ein morphologischer Kasten (Zwicky-Box) dargestellt.

Parameter	**Ausprä-gung 1**	**Ausprä-gung 1**	**Ausprä-gung 1**	**Ausprä-gung 1**	**Ausprä-gung 1**	**Ausprä-gung 1**	**Ausprä-gung 1**	**Aus-prä-gung 1**	**…**
Art der Transportmittel	Bahn	Lkw	Flugzeug	Schiff	…				
Transportbehälter	Uranhexafluorid-Tank	CASTOR Transportbehälter	Transnucléaire Behälter (Frankreich)	Excellox Behälter (UK)					
…									

Tabelle 20: Morphologischer Kasten am Beispiel eines Nukleartransports

Der morphologische Kasten ist ein Ordnungsschema und beflügelt die eigene Kreativität, in dem die enthaltenen Elemente beliebig kombiniert werden.

3.2.3.1.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

---

[131] Vgl. Ritchey (2009).
[132] Ritchey (2009), S. 4.
[133] Vgl. Ritchey (2006).
[134] Vgl. Ritchey (2003).

3.2.3.1.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Der konkrete Input kann auch im Rahmen des Gruppenprozesses erarbeitet werden.

3.2.3.1.6 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Das Ergebnis des morphologischen Verfahrens sind sämtliche möglichen Kombinationen von Parametern, die ein Risiko beeinflussen.

3.2.3.1.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Ritchey beschreibt die Rahmenbedingungen zur Anwendung der Methode.[135] Insgesamt geht Ritchey von einem zeitlichen Aufwand von zwei bis zehn Workshop-Tagen aus.

3.2.3.1.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Ritchey beschreibt die Rahmenbedingungen zur Anwendung der Methode.[136] Dabei geht er von einem Gruppenprozess aus, wobei eine Gruppe aus nicht mehr als sechs bis

[135] Vgl. Ritchey (2011b), S. 14.
[136] Vgl. Ritchey (2011b), S. 14.

sieben Experten bestehen sollte. Die Gruppenarbeit sollte dazu moderiert werden; Ritchey schlägt zwei Moderatoren vor.

3.2.3.1.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☒ Basic

☒ Evolved

☐ Advanced

☐ Leading

3.2.3.1.10 Stärken und Schwächen

Stärken	Schwächen
• Strukturierte Vorgehensweise • Alle möglichen Kombinationen für Risiken, Ursachen und/oder Wirkungen werden (theoretisch) erfasst. • Methodik fördert den „Blick über den Tellerrand“.	• Zeitlich und personell aufwändiges Verfahren • Aufwändige Bewertung bzw. Filterung der Ergebnisse notwendig • Qualität der Ergebnisse hängt stark von der Moderation und der Erfahrung des Moderators ab. • Aufwändige Bewertung beziehungsweise Filterung der Ergebnisse notwendig. • Qualität der Ergebnisse ist abhängig von der Kompetenz, Vorstellungskraft, Kreativität und dem Enthusiasmus der Teilnehmer. • Methodik kann keine radikalen Ergebnisse produzieren („Black Swans“), da die definierten Dimensionen die Kreativität einschränken.

Tabelle 21: Stärken und Schwächen morphologischer Verfahren

3.2.3.1.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☒ gut

☐ weniger geeignet

3.2.3.2 Brainstorming

3.2.3.2.1 Einsatzzweck

Brainstorming („using the brain to storm a problem“[137]) ist eine Kreativitätsmethode, die zu einer Vielzahl von – in der Regel neuen – Aspekten führen soll. Unter die Ergebnisse eines Brainstormings fallen neue Ideen oder Konzepte. Im Bereich des Risikomanagements fallen unter diese Aspekte unerwünschte Ereignisse, Ursachen, aber auch Wirkungen – und damit alle Elemente von Risiken.

Inzwischen wird Brainstorming oftmals als Oberbegriff für eine Klasse von Kreativitätsmethoden angesehen.

3.2.3.2.2 Beschreibung

Brainstorming als Methode ist einfach durchzuführen. Methoden-Kenntnisse sind praktisch nicht notwendig. Brainstorming lässt sich wie folgt umsetzen:[138]

- Vorbereitung: Im Rahmen der Vorbereitung wird die Teilnehmergruppe zusammengestellt; sie sollte aus 5 bis 7 Personen bestehen.[139] Bei kleineren Gruppen ist oft das assoziative Potenzial für einen ausreichenden Ideenfluss zu gering. Ist die Gruppe größer, ist mit kommunikativen Störungen zu rechnen.[140] Noch wichtiger als die Gruppengröße ist die Heterogenität der Gruppe hinsichtlich ihrer Interdisziplinarität. Weiterhin wird die zugrundeliegende Fragestellung erläutert. Sinnvoll ist es, auch die Regeln zu erklären. Ebenfalls ist es sinnvoll, einen Protokollanten zu ernennen.
- Risikoidentifikation und -analyse: Die Teilnehmer nennen mögliche Risiken, mögliche Ursachen und/oder mögliche Wirkungen. Hier werden in der Praxis ergänzend andere Methoden eingesetzt, beispielsweise der morphologische Kasten oder die KJ-Methode. Die Begriffe werden dokumentiert. Somit lassen sich eigene Ideen mit bereits genannten Aspekten kombinieren. Ziel dieser Phase ist, innerhalb einer definierten Zeit (maximal 30 Minuten) möglichst viele Aspekte zu identifizieren.
- Ergebnisanalyse: Die dokumentieren Ergebnisse werden gruppiert und sortiert, anschließend bewertet. Eventuell werden Aspekte aussortiert.

Wichtig ist jedoch, vor allem Fehler in der Vorgehensweise zu vermeiden, indem bestimmte Regeln eingehalten werden:

- Das Ziel ist, möglichst viele Aspekte zu sammeln.

---

[137] Vgl. Romeike, Hager (2013), S. 109.
[138] Vgl. dazu auch Chapman, Ward (1997), S. 120 sowie Romeike, Hager (2013), S. 109-110.
[139] Chapman und Ward dagegen sprechen von einer Gruppengröße von 6 bis 12 Teilnehmern; vgl. Chapman, Ward (1997), S. 120.
[140] Vgl. Romeike, Hager (2013), S. 109.

- Eine Beurteilung oder Bewertung der Aspekte ist nicht erlaubt (diese erfolgt später in der Ergebnisanalyse).
- Auch vermeintlich unsinnige (weil inhaltlich anscheinend entfernte) Aspekte sind erlaubt. Freie Äußerung aller Ideen.

Johnston weist darauf hin, dass – obwohl Kreativität auf Individuen bezogen werden muss – bei Risikoanalysen im Infrastrukturbereich eine Gruppenarbeit unausweichlich ist, diese dann jedoch wieder die individuelle Kreativität fördern sollte.[141] Weiterhin listet er eine Vielzahl von Hinweisen auf, die insbesondere im Bereich der Infrastruktur-Risikoanalyse zu einem effektiven Brainstorming beitragen sollen.[142]

3.2.3.2.3 Anwendungsbeispiel

Explizite und detaillierte Anwendungsbeispiele sind in der wissenschaftlichen Literatur kaum zu finden. Dies liegt vor allem daran, dass Brainstorming häufig in Kombination mit anderen Methoden (zum Beispiel der Bow-tie-Analysis oder der morphologischen Analyse) durchgeführt wird.

Explizit genannt wird Brainstorming als Methode zur Risikoidentifikation bei Berle, Asbjørnslett und Rice: Dort wird eine Verwundbarkeitsanalyse für ein Seeverkehrssystem für Flüssiggas durchgeführt. Im Rahmen dieser Analyse erfolgt die Risikoidentifikation auf Basis von historischen Daten und dem Einsatz des Brainstormings mit „Praktikern".[143] Ebenso wird Brainstorming explizit bei Romeike/Hager als Verfahren für die Risikoidentifikation genannt.[144]

3.2.3.2.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☒ Risikobewertung

☒ Risikosteuerung

[141] Vgl. Johnston (2012), S. 30.
[142] Vgl. Johnston (2012), S. 30-31.
[143] Vgl. Berle et al (2011), S. 702.
[144] Vgl. Romeike, Hager (2013), S. 109.

3.2.3.2.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Für das Brainstorming sind in der einfachsten Form keine Daten notwendig. Das Ergebnis ergibt sich aus dem Wissen und der Kreativität der Teilnehmer.

3.2.3.2.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Die Ergebnisse eines Brainstormings sind, je nach Fokus der Fragestellung, unerwünschte Ereignisse und/oder deren Ursachen und/oder deren Wirkungen. Ein Brainstorming kann auch für die Risikosteuerung eingesetzt werden, indem mögliche risikopolitische Maßnahmen erarbeitet werden. Die Ergebnisse des Brainstormings können in anderen Methoden weiterverarbeitet werden, beispielsweise mittels der Bow-Tie Analysis, die als Rahmen für das Brainstorming fungieren kann.[145]

3.2.3.2.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Das eigentliche Brainstorming benötigt nur den Zeitaufwand für die Vorbereitung und die Durchführung. Diese beiden Phasen können in weniger als einer Stunde durchgeführt werden. Die Ergebnisanalyse, die auch getrennt von den ersten beiden Phasen erfolgen kann, dauert möglicherweise, auch aufgrund von Diskussionen zur Bewertung, länger.

[145] Vgl. Lewis, Smith (2010), S. 8 und 17.

3.2.3.2.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Für die Durchführung des Brainstormings ist nahezu kein Methodenwissen notwendig (wohl jedoch Fachwissen). Die Qualität der Ergebnisse hängt stark von der Zusammensetzung des Brainstorming-Teams ab (Interdisziplinarität, heterogenes Spektrum von Laien und Experten). Es kann grundsätzlich ohne Methodenschulung durchgeführt werden.

3.2.3.2.9 Reifegrad des zugrundeliegenden Risikomanagements

☒ Initial

☒ Basic

☒ Evolved

☒ Advanced

☒ Leading

Erläuterung: Brainstorming definiert nicht den Reifegrad des Risikomanagements; es kann sowohl auf einer niedrigen, aber auch auf einer hoch-professionellen Stufe des Risikomanagements eingesetzt werden.

3.2.3.2.10 Stärken und Schwächen

Stärken	Schwächen
• Einfach umzusetzendes Verfahren (einfache Regeln, kein Expertenwissen notwendig) • Auch kurzfristig einsetzbar	• Gefahr, dass Regeln nicht eingehalten werden und damit die kreative Leistung eingeschränkt wird, zum Beispiel durch „Zerreden“ einer Idee

Tabelle 22 : Stärken und Schwächen des Brainstormings

3.2.3.2.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

3.2.3.3 Brainwriting

3.2.3.3.1 Einsatzzweck

Brainwriting ist eine dem Brainstorming sehr ähnliche Kreativitätsmethode. Der Unterschied zwischen Brainstorming und Brainwriting liegt in der Art und Weise, wie risikorelevante Aspekte genannt und festgehalten werden: Während beim Brainstorming diese Aspekte verbal genannt und in der Regel durch einen Moderator festgehalten werden, formulieren beim Brainwriting die Teilnehmer ihre Ideen schriftlich; eine Diskussion findet erst zum Ende statt.[146] In einer abgewandelten Form („Kummerkasten-Ansatz“) erfolgt die Sammlung der Informationen, beispielsweise identifizierten Risiken, in einer anonymisierten Form.

3.2.3.3.2 Beschreibung

Die Vorgehensweise beim Brainwriting entspricht grundsätzlich derjenigen des Brainstormings. Abweichend zum Brainstorming ist kein Protokollant zu ernennen. Die wesentliche Änderung ist, dass die risikorelevanten Aspekte unmittelbar von den Teilnehmern aufgeschrieben werden. Hierfür bietet sich eine definierte Struktur an, etwa die Erfassung der Risiken in einer Risikomatrix oder in einer Top-10-Tabelle. In der Praxis des Risikomanagements bietet sich eine Anonymisierung der Ergebnisse an, damit Risikoinformationen ohne jegliche Hemmschwelle, blockierende Einflüsse aus der Gruppe oder der Angst vor persönlichen Konsequenzen kommuniziert und diskutiert werden (siehe „Kummerkasten-Ansatz“).

3.2.3.3.3 AnwendungsbeispielAnwendungsbeispiel

Explizite und detaillierte Anwendungsbeispiele sind in der wissenschaftlichen Literatur – wie beim Brainstorming – kaum zu finden; die Begründung entspricht derjenigen des Brainstormings.

3.2.3.3.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☒ Risikobewertung

☒ Risikosteuerung

[146] Vgl. Spang, Gerhard (2016), S. 434.

3.2.3.3.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Für das Brainstorming sind in der einfachsten Form keine Daten notwendig. Das Ergebnis ergibt sich aus dem Wissen und der Kreativität der Teilnehmer.

3.2.3.3.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Die Ergebnisse eines Brainwritings sind, je nach Fokus der Fragestellung, unerwünschte Ereignisse und/oder deren Ursachen und/oder deren Wirkungen. Ein Brainwriting kann auch für die Risikosteuerung eingesetzt werden, indem mögliche risikopolitische Maßnahmen erarbeitet werden. Die Ergebnisse des Brainwritings können in anderen Methoden weiterverarbeitet werden, beispielsweise mittels der Bow-tie Analysis, die als Rahmen für das Brainwriting fungieren kann.[147]

3.2.3.3.7 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Das eigentliche Brainwriting benötigt nur den Zeitaufwand für die Vorbereitung und die Durchführung. Diese beiden Phasen können in weniger als einer Stunde durchgeführt werden. Die Ergebnisanalyse, die auch getrennt von den ersten beiden Phasen erfolgen kann, dauert möglicherweise, auch aufgrund von Diskussionen zur Bewertung, länger.

[147] Vgl. Lewis, Smith (2010), S. 8 und 17.

3.2.3.3.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Für die Durchführung des Brainwritings ist nahezu kein Methodenwissen notwendig. Es kann ohne Schulung durchgeführt werden.

3.2.3.3.9 Reifegrad des zugrundeliegenden Risikomanagements

☒ Initial

☒ Basic

☒ Evolved

☒ Advanced

☒ Leading

Erläuterung: Brainwriting definiert – analog zu Brainstorming – nicht den Reifegrad des Risikomanagements; es kann sowohl auf einer niedrigen, aber auch auf einer hoch-professionellen Stufe des Risikomanagements eingesetzt werden.

3.2.3.3.10 Stärken und Schwächen

Stärken	Schwächen
• Einfach umzusetzendes Verfahren (einfache Regeln, kein Expertenwissen notwendig) • Auch kurzfristig einsetzbar • Durch eine „Anonymisierung“ der Inhalte werden auch „kritische“ Themen dokumentiert und diskutiert („Kummerkasten-Ansatz“) • Inhalte werden nicht zerredet; kein Risiko von „Groupthink“, das heißt Anpassung der individuellen Meinung an die erwartete Gruppenmeinung.	• Keine explizite Interaktion, zum Beispiel verbaler Austausch, während der Kreativphase. Dies kann die Kreativität stören. • Qualität der Ergebnisse ist abhängig von der Kompetenz, Vorstellungskraft, Kreativität und dem Enthusiasmus der Teilnehmer. • Ergebnisse sind nicht wertfrei.

Tabelle 23: Stärken und Schwächen des Brainwritings

3.2.3.3.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

3.2.3.4 Methode 635

3.2.3.4.1 Einsatzzweck

Die Methode 635 zählt zu den Brainwriting-Techniken (siehe oben) und ist ein Ansatz, in möglichst kurzer Zeit eine recht große Anzahl an Ideen (oder im Risikomanagement: Risiken, Ursachen und/oder Wirkungen) zu erarbeiten, die in einem nächsten Schritt analysiert und bewertet werden.[148] Im Rahmen der Anwendung führen die Teilnehmer die Ideen von anderen Teilnehmern fort. So erzeugen sie innerhalb einer kurzen Zeit 108 unterschiedliche Ansatzpunkte (6 Teilnehmer x 3 Ideen x 6 Reihen) für risikorelevante Aspekte.

3.2.3.4.2 Beschreibung

Die Methode 635 hat ihren Namen von der Anzahl der Teilnehmer (6), der Anzahl der „Ideen“ (jeweils 3) und der Anzahl, wie oft jedes „Arbeitsblatt“ weitergegeben wird (5 mal).

1. Schritt: Jeder Teilnehmer erhält ein vorbereitetes Arbeitsblatt mit drei Spalten und sechs Zeilen.
2. Schritt: Der Moderator definiert die Zeitspanne für das Ausfüllen sowie die anschließende Weitergabe der Arbeitsblätter (beispielsweise 3 bis 5 Minuten).
3. Schritt: Jeder der 6 Teilnehmer verfasst 3 Ideen (beziehungsweise Risiken) und trägt diese in die Felder der ersten Zeile des Arbeitsblattes ein.
4. Schritt: Nach Ablauf der definierten Zeitspanne werden die Arbeitsblätter im Uhrzeigersinn an den nächsten Teilnehmer weitergegeben.
5. Schritt: Jeder Teilnehmer sollte die bereits genannten Ideen aufgreifen, ergänzen oder weiterentwickeln. Die neuen (drei) Ideen trägt er in die nächste freie Zeile ein.
6. Schritt: Die Arbeitsblätter werden so lange im Uhrzeigersinn weitergegeben, bis auch die letzte Zeile des Arbeitsblattes ausgefüllt ist.

Nach Abschluss sind insgesamt 6 x 3 x 6 = 108 Ideen bzw. risikorelevante Aspekte erarbeitet worden, die im nächsten Schritt gefiltert und bewertet werden.

[148] Vgl. Romeike, Hager (2013), S. 110.

Die Methode 635 baut damit nicht auf einen unmittelbaren und gleichzeitigen Austausch von Gedanken aller Teilnehmer, sondern auf die sukzessive Erweiterung von Gedankengängen.

3.2.3.4.3 Anwendungsbeispiel

Zur Identifikation von Risiken, etwa im Bereich Supply-Chain-Risiken kann die Methode 6-3-5 ohne großen Aufwand eingesetzt werden.[149] In Tabelle 24 ist exemplarisch ein Formblatt der Methode 6-3-5 skizziert. Das Vorgehen im Risikomanagement sollte wir nachfolgend skizziert durchgeführt werden:

1. Bestimmen Sie innerhalb der Gruppe einen Zeitnehmer
2. Jeder Teilnehmer erhält ein Formular mit einer Tabelle (3 Spalten, 6 Zeilen). Jeder Teilnehmer trägt in jeder Spalte der ersten Zeile je ein Risiko ein (insgesamt also drei Risiken)
3. Nach zwei Minuten werden die Blätter gleichzeitig und im Uhrzeigersinn weitergereicht.
4. Der nächste Teilnehmer soll nun versuchen, die bereits genannten Risiken aufzugreifen, zu ergänzen, weiterzuentwickeln oder evtl. ein neues Risiko zu formulieren.
5. Es gelten die Regeln des Brainwritings, das heißt jedes Risiko ist gleichwertig und es gibt keine Diskussionen zu den einzelnen Vorschlägen.
6. Am Ende erfolgt durch alle Teilnehmer eine Konsolidierung und Klassifikation der identifizierten Risiken (Streichung von Dubletten, Konsolidierung etc.)

Supply-Chain-Risiken (Methode 6-3-5)		
Risiko	**Risiko**	**Risiko**
1. Versorgungsrisiken	2. Prozess- u. Steuerungsrisiken	3. Umfeldrisiken
4. Insolvenz Lieferant	5. Sabotage	6. Terroranschlag
7 …	8 …	9 …
10 …	11 …	12 …
13 …	14 …	15 …
16 …	17 …	18 …

Tabelle 24: Arbeitsblatt der Methode 6-3-5 (6 Teilnehmer x 18 Ideen = 108 Ideen)

[149] Vgl. Romeike/Eicher (2017).

3.2.3.4.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.3.4.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Für die Methode 635 sind keine Daten notwendig. Das Ergebnis ergibt sich aus dem Wissen und der Kreativität der Teilnehmer.

3.2.3.4.6 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Die Ergebnisse der Methode 635 sind, je nach Fokus der Fragestellung, unerwünschte Ereignisse und/oder deren Ursachen und/oder deren Wirkungen. Die Ergebnisse können in anderen Methoden weiterverarbeitet werden, beispielsweise mittels der Bow-tie Analysis.

3.2.3.4.7 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Die Methode 635 kann – ohne Vorbereitung und Ergebnisanalyse – innerhalb einer halben Stunde durchgeführt werden. Die Ergebnisanalyse dauert mutmaßlich, auch aufgrund von Diskussionen zur Bewertung, länger.

3.2.3.4.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Für die Durchführung der Methode 635 ist nahezu kein Methodenwissen notwendig. Sie kann ohne Schulung durchgeführt werden.

3.2.3.4.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☒ Basic

☒ Evolved

☒ Advanced

☒ Leading

3.2.3.4.10 Stärken und Schwächen

Stärken	Schwächen
• Einfach umzusetzendes Verfahren • Auch kurzfristig einsetzbar • Sukzessive Weiterführung von Ideen • Durch eine „Anonymisierung“ der Inhalte werden auch „kritische“ Themen dokumentiert und diskutiert („Kummerkasten-Ansatz“) • Inhalte werden nicht zerredet; kein Risiko von „Groupthink“, das heißt Anpassung der individuellen Meinung an die erwartete Gruppenmeinung.	• Keine explizite Interaktion, zum Beispiel verbaler Austausch, während der Kreativphase. Dies kann die Kreativität stören. • Redundanzen möglich, im ungünstigsten Fall insgesamt nur drei Ideen. • Qualität der Ergebnisse ist abhängig von der Kompetenz, Vorstellungskraft, Kreativität und dem Enthusiasmus der Teilnehmer. • Ergebnisse sind nicht wertfrei.

Tabelle 25: Stärken und Schwächen der Methode 635

3.2.3.4.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

3.2.3.5 Mind Mapping

3.2.3.5.1 Einsatzzweck

Das Mind-Mapping (auch Gedankenlandkarte oder Gedächtnislandkarte) dient dazu, ausgehend von einem zentralen Risiko, möglichst sämtliche Ursachen und/oder Wirkungen und/oder Maßnahmen zu identifizieren, die mit dem Risiko in Verbindung stehen. Durch die besondere Form der Anordnung entsteht ein bildhafter Überblick bzw. eine Gedankenkarte – die Mind Map. Durch die grafische Darstellungsform werden beide Gehirnhälften angesprochen; damit soll die geistige Leistung verbessert werden.

3.2.3.5.2 Beschreibung

Beim Mind-Mapping wird mit einem weißen Blatt (oder generell: einer leeren) Fläche begonnen. In die Mitte dieser Fläche wird der zentrale Begriff geschrieben. Beim Risikomanagement wird dies in der Regel ein Objekt sein (zum Beispiel eine kritische logistische Infrastruktur) oder ein bereits identifiziertes Risiko. Anschließend werden zu diesem zentralen Begriff möglichst viele Schlüsselwörter gesucht:

- Wenn als Ausgangssituation eine kritische logistische Infrastruktur aufgeführt ist, könnten sämtliche Risiken aufgeführt werden, die für diese Infrastruktur relevant sind. Die einzelnen Mind-Map-Äste bilden alternativ die Risikoarten oder auch die Ursachen oder Wirkungen der Risiken ab. Alternativ können auch Maßnahmen zur Risikosteuerung abgebildet werden.
- Wenn als Ausgangssituation dagegen ein bereits bekanntes Risiko aufgeschrieben wurde, könnten als Schlüsselbegriffe beispielsweise sämtliche Ursachen, Wirkungen und/oder Maßnahmen aufgeführt werden, die mit diesem Risiko in Verbindung stehen.

Die identifizierten Begriffe lassen sich anschließend sortieren und gruppieren. Sie werden anhand verschiedener Zweige und bei Bedarf unter Zuhilfenahme weiterer Symbole grafisch um den zentralen Begriff angeordnet. Die Anordnung kann dann zu einer vielschichtigen Hierarchie von Zweigen führen. Einzelne Begriffe lassen sich auch verbinden, um Beziehungen zwischen Begriffen zu verdeutlichen. Hierbei lassen sich auch komplexe Abhängigkeiten abbilden, etwa in Form von so genannten konzeptuellen Karten (conceptual maps), semantischen Netzen oder Ontologien. Möchte man die Darstellung nicht auf eine Baumstruktur beschränken, lassen sich logische und sonstige Zusammenhänge auch mit Hilfe einer kognitiven Karte (auch mental map) oder Fuzzy Cognitive Maps (FCMs) strukturieren und visualisieren.

3.2.3.5.3 AnwendungsbeispielAnwendungsbeispiel

Sääskilahti und Särelä beschreiben den Einsatz sowie Stärken und Schwächen von Mind Maps im Rahmen der Risikoidentifikation (in dem Fall allerdings in Host-

Identitätsprotokollen).[150] Sie heben auf der einen Seite die Stärke eines Mind Maps (bzw. der entsprechenden Vorlage) für die Identifikation, konkret aber auch für die Durchführung von Interviews und die entsprechende unmittelbare Dokumentation der Ergebnisse hervor. Sie weisen insbesondere auf die Vorteile im Vergleich zu Checklisten hin.

Hristova, Schlegel und Obermeier nutzen dagegen eine Mind Map eher zur – sich an die Risikoidentifikation anschließenden – Visualisierung und Kommunikation der identifizierten Risiken (vgl. auch Abbildung 17).[151]

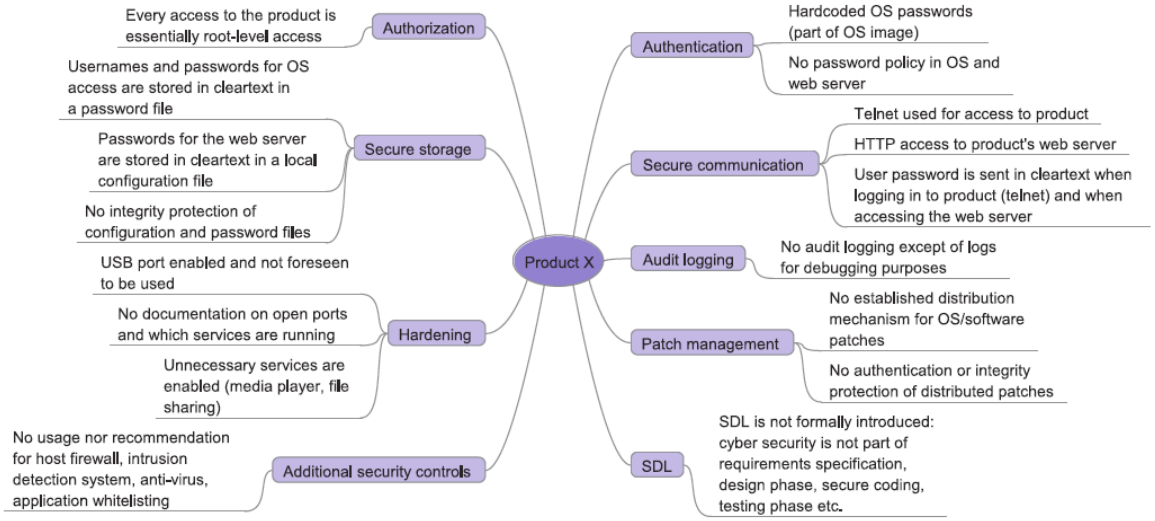


Abbildung 17 Beispiel für eine Mind Map zur Identifikation von Sicherheitslücken[152]

3.2.3.5.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.3.5.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

[150] Vgl. Sääskilahti, Särelä (2010).
[151] Vgl. Hristova et al (2014).
[152] Vgl. Hristova et al (2014), S. 269.

Beschreibung: Für die Anwendung des Mind-Mapping sind keine Daten notwendig. Das Ergebnis ergibt sich aus dem Wissen und der Kreativität der Teilnehmer.

3.2.3.5.6 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Das Ergebnis des Mind-Mapping ist eine sogenannte Mind Map. Die Teilnehmer eines Mind-Mapping-Workshops arbeiten damit unmittelbar an einem Ergebnisdokument. Gleichzeitig werden aber Mind Maps auch kritisch für Dokumentationszwecke gesehen, die für Außenstehende, das heißt für bei der Risikoidentifikation und Risikoanalyse nicht involvierte Personen, eher schwer zu verstehen seien.[153] Andererseits kann eine Mind Map auch gut als Kommunikationsbasis der wesentlichen Ergebnisse verwendet werden.[154]

3.2.3.5.7 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Der zeitliche Aufwand für die Erstellung einer Mind Map kann variiert werden. Damit kann auch bei eingeschränkter zeitlicher Verfügbarkeit gut mit dem Mind-Mapping gearbeitet werden.

3.2.3.5.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Für die Durchführung des Mind-Mapping ist nahezu kein Methodenwissen notwendig. Ein Mind-Mapping kann ohne Schulung durchgeführt werden.

[153] Vgl. Sääskilahti, Särelä (2010), S. 216.
[154] Vgl. Hristova et al (2014), S. 268.

3.2.3.5.9 Reifegrad des zugrundeliegenden Risikomanagements

☒ Initial

☒ Basic

☐ Evolved

☐ Advanced

☐ Leading

3.2.3.5.10 Stärken und Schwächen

Stärken	Schwächen
• Einfach umzusetzendes Verfahren • Visualisierung von Ergebnissen • Auch Beziehungen zwischen Einzelaspekten werden deutlich • Mind-Maps prägen sich gut ein; Konzentration auf das Wesentliche. • Risiko, den „(Risiko-)Wald vor lauter Bäumen“ nicht mehr zu sehen, wird reduziert (das Wichtigste steht näher im Zentrum, das weniger Wichtiges steht mehr am Rande).	• Zunehmende Komplexität bei großen Mindmaps • Die mono-hierarchische Struktur führt dazu, dass komplexe Ontologien stark vereinfacht dargestellt werden (etwa bei Abhängigkeiten zwischen Risiken). Alternative: Cognitive Maps.

Tabelle 26: Stärken und Schwächen des Mind Mappings

3.2.3.5.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☐ sehr gut

☒ gut

☐ weniger geeignet

Begründung: Mind Maps eignen sich vor allem dazu, im Rahmen der Risikoidentifikation Interviews zu strukturieren und ihre Ergebnisse unmittelbar (das heißt „real-time“) zu dokumentieren. Somit kann eine Mind Map als Ergebnisdokument weiterverwendet werden. Möglicherweise haben jedoch Personen, die nicht in die Risikoidentifikation involviert waren, Probleme, die Ergebnisse zu verstehen.

3.2.3.6 KJ-Methode

3.2.3.6.1 Einsatzzweck

Die von dem japanischen Anthropologen Jiro Kawakita entwickelte KJ-Methode ist eine Kreativitätsmethode, bei der im Rahmen von zwei Phasen Risiken, Ursache, Wirkungen und/oder

mögliche risikopolitische Maßnahmen identifiziert werden. Die Methode wird an einer Pinnwand oder einer Tafel durchgeführt, an der zunächst Stichworte gesammelt und dann in einer zweiten Phase nach Themen strukturiert werden. Die erste Phase erfolgt individuell, die zweite Phase als Teamarbeit. Das Ergebnis der Methode ist eine „Risiko-Landschaft“, bei der die Beziehungen zwischen den Stichworten und den Kategorien oder Themen explizit dargestellt werden.

3.2.3.6.2 Beschreibung

Die KJ-Methode wird in mehreren Schritten durchgeführt:[155]

1. Im ersten Schritt werden sämtliche Stichworte, die den Teilnehmern zu einem Oberthema (zum Beispiel einem bestimmten Risiko oder einer kritischen logistischen Infrastruktur) auf Karten oder selbstklebende Haftzettel geschrieben. Dieser Schritt wird von jedem Teilnehmer individuell durchgeführt.
2. Die Karten werden anschließend gemischt und – im Team – sortiert und gruppiert. So genannte „einsame Wölfe“, die (noch) zu keiner Gruppe passen, werden zunächst aussortiert und bilden eine eigene Gruppe. Zusätzlich werden für die Kartengruppen Bezeichnungen gefunden und aufgeschrieben, die zu einer Charakterisierung der Gruppen führen.
3. Im dritten Schritt werden die Kartengruppen neu angeordnet. Dabei wird eine Landschaft mit den Gruppen gebildet. Vor allem lassen sich zwischen den Gruppen bzw. den einzelnen Karten Pfeile eintragen (oder ankleben), die Ursache-/Wirkungs-Zusammenhänge verdeutlichen.
4. Ein expliziter Schritt innerhalb der KJ-Methode ist die Erläuterung der Ergebnisse (also der Kartenlandschaft). Dabei müssen die vorhandenen Daten berücksichtigt werden, während gleichzeitig die Landschaft beschrieben (aber nicht interpretiert) werden sollte.

[155] Vgl. Scupin (1997), S. 235-236.

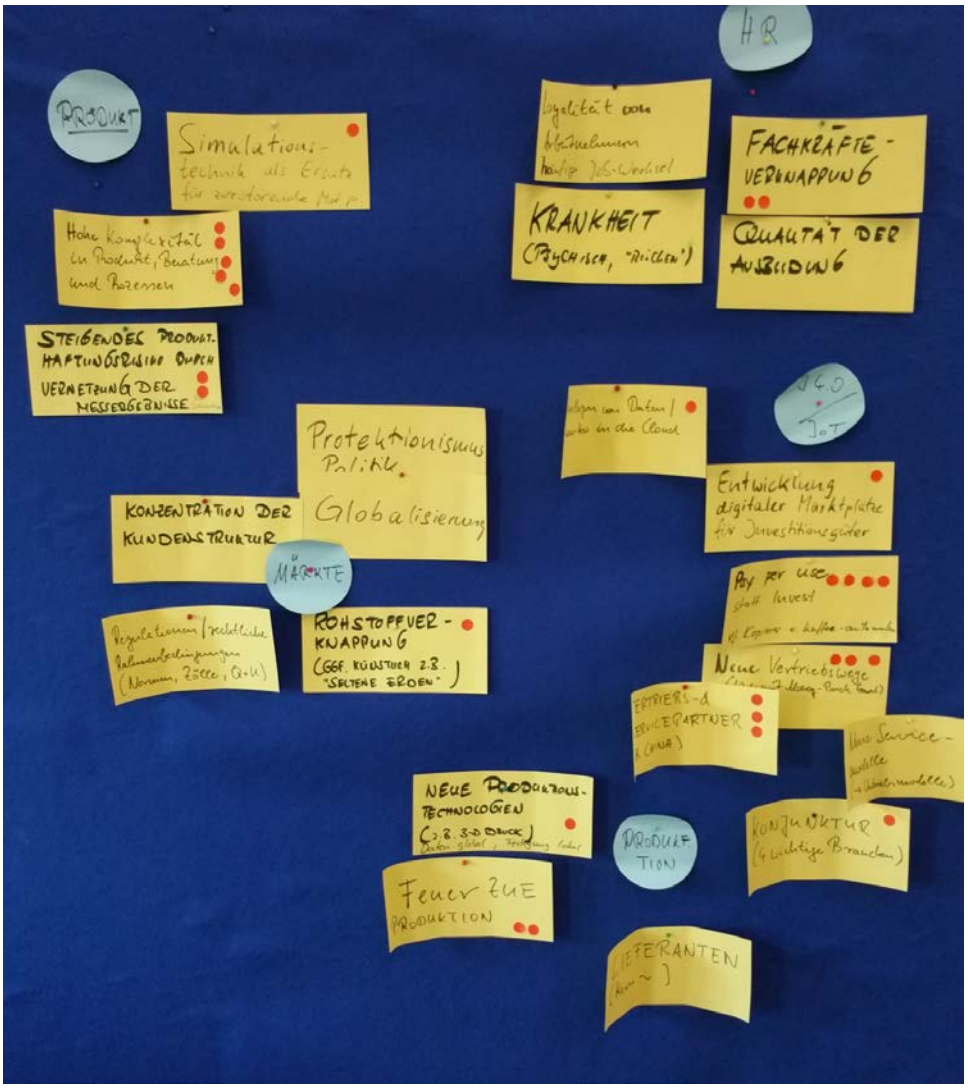


Abbildung 18 Einsatz der KJ-Methode im Rahmen einer Risikoanalyse[156]

3.2.3.6.3 Anwendungsbeispiel

Schieg beschreibt die Anwendung der KJ-Methode im Rahmen der Post-Mortem-Analyse in Konstruktionsprojekten. Dabei betont Schieg, dass die KJ-Methode vor allem zu einem tieferen Verständnis der Ursache-/Wirkungs-Zusammenhänge führe.[157] Auch im Risikomanagement ist die Analyse und höhere Transparenz der Ursache-/Wirkungs-Zusammenhänge von einer besonderen Relevanz.

Kado, Horiuchi und Seki betonen, dass die KJ-Methode gut mit einem Brainstorming zu verbinden sei: Dabei kann die KJ-Methode genutzt werden, um die im Rahmen des Brainstormings identifizierten Begriffe zu ordnen, zu gruppieren und in Kausalketten zu bringen.[158]

---

[156] Quelle: RiskNET GmbH.
[157] Vgl. Schieg (2007), S. 149.
[158] Vgl. Kado et al (2003), S. 20.

3.2.3.6.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.3.6.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Für die Anwendung der KJ-Methode sind keine Daten notwendig. Das Ergebnis ergibt sich aus dem Wissen und der Kreativität der Teilnehmer.

3.2.3.6.6 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Neben einer Auflistung von Risiken, Ursachen oder Wirkungen führt die KJ-Methode auch zu Kausalketten. Damit lassen sich durch Anwendung der KJ-Methode Ursache-/Wirkungs-Zusammenhänge identifizieren und darstellen.

3.2.3.6.7 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

3.2.3.6.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Für die Anwendung der KJ-Methode ist nahezu kein Methodenwissen notwendig.

3.2.3.6.9 Reifegrad des zugrundeliegenden Risikomanagements

☒ Initial

☒ Basic

☒ Evolved

☐ Advanced

☐ Leading

3.2.3.6.10 Stärken und Schwächen

Stärken	Schwächen
• Einfach umzusetzendes Verfahren • Strukturierung von Ergebnissen • Primär Visualisierungsmethodik, daher erfolgt in der Praxis regelmäßig eine Kombination mit anderen Methoden (beispielsweise Brainstorming) • Zusammenhänge (etwa Ursache-Wirkungsketten) können einfach und pragmatisch visualisiert werden. • Gewisse Standardisierung der Dokumentation (Karten, Pinnwand etc.), damit eine Vergleichbarkeit der Ergebnisse möglich ist.	• Meta-Plan-Tafeln und Verbrauchsmaterialien werden benötigt. • Durch die Auswahl der Teilnehmer erfolgt eine Einflussnahme auf das Ergebnis. • Qualität der Ergebnisse ist abhängig von der Kompetenz, Vorstellungskraft, Kreativität, Teamfähigkeit, Kommunikationsfähigkeit und dem Enthusiasmus der Teilnehmer. • Die Teilnehmer beeinflussen sich gegenseitig (Groupthink).

Tabelle 27: Stärken und Schwächen der KJ-Methode

3.2.3.6.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

3.2.3.7 Flip-Flop-Technik (Kopfstandtechnik)

3.2.3.7.1 Einsatzzweck

Die Kopfstandtechnik (auch als Flip-Flop- oder Umkehrtechnik, im Englischen als „reverse thinking“ bezeichnet) dient dazu, Risiken zu identifizieren, indem die eigentliche Kernfrage umgekehrt wird. Die Methode geht auf den englischen Arzt und Kognitionswissenschaftler Edward de Bono (geb. 1933) zurück. Mit der Umkehr der ursprünglichen Aufgabenstellung soll die Fragestellung ungewöhnlich sein, wodurch die Teilnehmer provoziert und angeregt werden sollen. Damit sollen – im Gegensatz zu einer „konventionellen“ Vorgehensweise – unerwartete Ergebnisse erzielt werden.

3.2.3.7.2 Beschreibung

Die Kopfstand-Technik läuft üblicherweise in mehreren Phasen ab:

1. Ausgehend von der Aufgabe oder Fragestellung wird diese Aufgabe umgekehrt und damit auf den Kopf gestellt. Beispiel aus der Praxis für die Kopfstand-Methode: „Was müssen wir als Unternehmen tun, damit wir scheitern und insolvent werden?“
2. Anschließend versuchen die Teilnehmer für diese umgekehrte Aufgabenstellung Lösungen zu entwickeln.
3. Die entwickelten Lösungen sind dann wiederum auf den Kopf zu stellen, um zu Lösungsansätzen für die eigentliche Fragestellung zu gelangen.

3.2.3.7.3 Anwendungsbeispiel

Sawaguchi entwickelt einen Ansatz, der auf der Kopfstand-Technik basiert:[159] Dieser als CRMART („Creative Risk Management Approach based on Reverse Thinking“) bezeichnete Ansatz fokussiert nicht auf die (Ex-post-) Analyse von Risiken oder Ausfällen, sondern auf die kreative Entwicklung möglicher Risiken. Der Kern des Ansatzes liegt in der Umkehrung der wesentlichen Frage, die bei klassischen Ansätzen der Risikoidentifikation „How Risk(s) Occurred?“ lauten könnte, bei CRMART dagegen umgekehrt wird; sie lautet dann: „How We Create Risk(s)?“ Dieser Ansatz wird auf ein Beispiel im Bereich von Organisations- und Informationsrisiken angewandt.

Bei einer Anwendung im Risikomanagement wäre es sinnvoll, sich vor allem auch mit potenziellen Worst-case-Szenarien zu beschäftigen. Die Fragestellung wäre: „Was müssen wir als Unternehmen tun, damit das Worst-Case-Szenario eintritt?“

[159] Vgl. Sawaguchi (2015).

3.2.3.7.4 Phase

☒ Risikoidentifikation

☐ Risikoanalyse

☐ Risikobewertung

☒ Risikosteuerung

3.2.3.7.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

Beschreibung: Sawaguchi weist darauf hin, dass mit der Kopfstand-Technik die Menge der benötigten historischen Daten gering ist.[160]

3.2.3.7.6 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

3.2.3.7.7 Zeitlicher Aufwand für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

3.2.3.7.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☒ niedrig

☐ mittel

☐ hoch

Begründung: Für die Durchführung der Kopfstand-Technik ist kein Methodenwissen notwendig. Sie kann ohne Schulung durchgeführt werden. Es kann jedoch schwierig sein, konkrete

[160] Vgl. Sawaguchi (2015), S. 581.

„umgekehrte“ Lösungen (oder Anti-Lösungen) zu finden, wenn die umgekehrte Fragestellung abstrakt oder komplex ist.

3.2.3.7.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☒ Evolved

☒ Advanced

☐ Leading

3.2.3.7.10 Stärken und Schwächen

Stärken	Schwächen
• Unkonventionelle Methode; sie soll unerwartete Ergebnisse möglich machen	• Abstraktionsfähigkeit und „Umdenken“ der Teilnehmer notwendig • Für einzelne Fragestellung wird ein „Kopfstand“ schwierig zu erarbeiten sein

Tabelle 28: Stärken und Schwächen der Kopfstand-Technik

3.2.3.7.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☒ gut

☐ weniger geeignet

Begründung: Die Eignung der Kopfstand-Technik hängt auch von der Aufgabenstellung ab. Sie kann – je nach Aufgabenstellung – zu Lösungen (bspw. zu identifizierten Risiken oder zu möglichen risikopolitischen Maßnahmen) führen, die auf konventionellen Art und Weise nicht erarbeitet worden wären.

3.2.3.8 World-Café

3.2.3.8.1 Einsatzzweck

Ein World-Café ist eine Workshop-Methode, bei der eine Gruppe von Teilnehmern in sich mischenden Gruppen an Tischen bestimmte Fragestellungen diskutiert; beispielsweise die Frage nach Risiken für bestimmte Arten logistischer Infrastrukturen. Durch die vorbereiteten

Fragen, die jeweils kleinen Gruppen und die intendiert-positive Atmosphäre sollen die Fragestellungen aus unterschiedlichen Perspektiven diskutiert und beantwortet werden. Es kann damit die Risikoidentifikation und die Erarbeitung von risikosteuernden Maßnahmen, ggf. auch die Risikoanalyse unterstützen.

3.2.3.8.2 Beschreibung

Ein World-Café, das für Teilnehmergrößen von 12 bis 2.000 Personen durchgeführt werden kann, lassen sich drei Phasen unterscheiden:

1. In der Vorbereitungsphase ist – neben dem physischen Aufbau des World-Cafés (Tische, „Tischdecken" zum Beschreiben, beispielsweise Flipchart-Papier, Stifte) – vor allem die Vorbereitung der Fragestellungen wichtig. Sie sollten einfach formuliert sein, so dass sie für die Teilnehmer einladend wirken. Daneben sind die „Spielregeln" bzw. die Etikette zu spezifizieren. Für jeden Tisch ist ein Gastgeber zu benennen.
2. In der Durchführungsphase, die zwischen 45 und 180 Minuten dauert, ordnen sich Teilnehmer einem Tisch zu, an dem eine oder zwei konkrete Fragestellungen diskutiert. Die Teilnehmerzahl an einem Tisch sollte vier bis maximal sechs betragen. Der Gastgeber erörtert die Fragestellung sowie die ggf. bereits vorher erarbeiteten Ergebnisse und unterstützt den Dialog, ohne jedoch zu moderieren. Die Teilnehmer nutzen die Tischdecke, um (Zwischen-) Ergebnisse zu dokumentieren. Nach einer vorher festgelegten Zeitdauer wechseln die Teilnehmer an einen anderen Tisch.
3. Nachbereitungsphase: Nach der Diskussionsrunde werden die Ergebnisse (die Tischdecken) als Galerie ausgehängt. Auch eine Zusammenfassung der Ergebnisse sowie eine Priorisierung können sinnvoll sein.

3.2.3.8.3 Anwendungsbeispiel

Hoffmann erläutert den Einsatz eines World-Cafés, um Indikatoren und risikopolitische Maßnahmen für vorab spezifizierte Risikoursachen zu diskutieren und zu erarbeiten. Für 15 teilnehmende Unternehmen wurden vier Tische gebildet. Jede der vier Diskussionsrunden dauerte 30 Minuten, wobei die Teilnehmer nach einer Runde an einen anderen Tisch wechselten. Im Anschluss an das World-Café wurden die Ergebnisse durch die Vergabe von Punkten gewichtet.[161]

Saint-Marc u.a. beschreiben den Einsatz des World Cafés für die Risikoabschätzung im Eisenbahnwesen. Dabei wurden vorab Komponentenbäume für unterschiedliche Teilsysteme im Eisenbahnwesen an den verschiedenen Tischen verteilt, so dass an jedem Tisch über eine an-

[161] Vgl. Hoffmann (2012), S. 87-88.

dere Domäne diskutiert wurde. Die Ergebnisse wurden unmittelbar in die Baumstrukturen eingetragen.[162]

3.2.3.8.4 Phase

☒ Risikoidentifikation

☐ Risikoanalyse

☐ Risikobewertung

☒ Risikosteuerung

3.2.3.8.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

3.2.3.8.6 Output

☒ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

Beschreibung des Outputs: Der Output des World Café sind dokumentierte Ergebnisse der verschiedenen Diskussionsrunden an den einzelnen Tischen. In der Regel ist der Output nicht (zwangsläufig) vorgegeben-strukturiert, sondern hängt von dem Diskussionsverlauf und den dabei gewonnenen Ergebnissen ab.

3.2.3.8.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Der Aufwand für Vorbereitung, Durchführung und Nachbereitung ist (relativ) hoch. Zeitlich wird ein World Café die Dauer eines Tages nicht überschreiten.

[162] Vgl. Saint-Marc et al (2016), S. 5.

3.2.3.8.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☒ mittel

☐ hoch

Begründung: Die Methode eignet sich vor allem für mittlere bis große Gruppengrößen; Evers spricht dabei von mittleren Gruppengrößen bei 20 bis 30 Teilnehmern und von großen Gruppen bei mehr Teilnehmern.[163] Dementsprechend ist der Aufwand für Vorbereitung, Durchführung und Nachbereitung (relativ) hoch. Andererseits erfordert die Durchführung eines World Cafés keine besonderen fachlichen Qualifikationen.

3.2.3.8.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☒ Basic

☒ Evolved

☒ Advanced

☒ Leading

3.2.3.8.10 Stärken und Schwächen

Stärken	Schwächen
• Vielfältiges Know-how wird gebündelt. • Durch Wechsel von einem Café in eine anderes und die damit verbundene Durchmischung der Teilnehmer können sich produktive Gruppen ergeben, die auch neuartige Risiken benennen können. • Teilnehmer benötigen keine spezielle Methodenkenntnis.	• Relativ aufwändiges Verfahren • Die Qualität des Outputs kann variieren; sie hängt maßgeblich vom Diskussionsverlauf ab.

Tabelle 29: Stärken und Schwächen des World-Cafés

[163] Vgl. Evers (2012), S. 18.

3.2.3.8.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☐ sehr gut

☒ gut

☐ weniger geeignet

3.2.3.9 Delphi-Methode

3.2.3.9.1 Einsatzzweck

Mit der Delphi-Methode, die als mehrstufiges Befragungsverfahren konzipiert ist, sollen Expertenmeinungen erfasst und – durch die Bereitstellung von anonymisierten (Zwischen-) Ergebnissen – fortgeführt und verfeinert werden. Damit sollen sich beispielsweise Risiken, deren Ursachen, aber auch Wirkungen und mögliche risikopolitische Maßnahmen identifizieren und entwickeln lassen.

3.2.3.9.2 Beschreibung

Die Delphi-Methode ist als mehrstufiges Verfahren konzipiert. In einer ersten Runde erhalten die Teilnehmer der Delphi-Studie, die ein Expertenwissen aufweisen sollten, einen Fragen- oder Thesenkatalog, den sie schriftlich beantworten. Für eine zweite (und auch spätere Fragenrunden) werden die Antworten der vorherigen Runde teilweise anonymisiert einzeln aufgeführt, teilweise auch zusammengefasst und durch statistische Maße verdeutlicht.

Durch die schriftliche Beantwortung und die Anonymisierung der Antworten sollen Störeinflüsse, die beispielsweise bei einer Gruppendiskussion entstehen können, eliminiert werden.

3.2.3.9.3 Anwendungsbeispiel

Liu et al. beschreiben die Konzeption, die Durchführung und die Resultate einer Delphi-Befragung zu IT-Risiken in China. Dabei gehen Sie auch auf Schwächen dieses Ansatzes ein: Dazu zählt auf der einen Seite, dass das Expertengremium, das im Rahmen der Delphi-Methode befragt wird, statistisch nicht repräsentativ ist. Auf der anderen Seite zählt dazu, dass sich mögliche Zwischenergebnisse durchaus durch eine sehr kleine (im Sinne von: zu kleine) Gruppe von Experten ergeben können.[164]

Markmann, Darkow und von der Gracht führen für eine Delphi-Studie zu Supply-Chain-Risiken durch.[165]

[164] Vgl. Liu, S. et al (2010).
[165] Vgl. Markmann et al (2013).

3.2.3.9.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☐ Risikobewertung

☐ Risikosteuerung

3.2.3.9.5 Input/Datenbedarf

☐ Quantitative/historische/empirische Daten

☒ Expertenschätzung

3.2.3.9.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

3.2.3.9.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

Begründung: Aufgrund der mehrstufigen Erhebungsdesigns ist der Zeitaufwand für die Delphi-Methode hoch. Auch wenn Markmann, Darkow und von der Gracht von einem geringen Zeitaufwand sprechen, so ist der von ihnen skizzierte zeitliche Rahmen von drei Monaten als eher umfangreich zu bewerten.[166]

3.2.3.9.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☐ mittel

☒ hoch

[166] Vgl. dazu Markmann et al (2013), S. 1827.

Begründung: Die Teilnehmer der Delphi-Methode werden gemeinhin als Experten bezeichnet. Dementsprechend sollte zumindest ein vertieftes Domänenwissen vorhanden sein, um die Fragen beantworten zu können. Methodische Kenntnisse bezüglich der Delphi-Methode sind für die Teilnehmer nicht notwendig. Die ausführende Stelle der Befragung benötigt dagegen entsprechendes Methoden-Know-how.

3.2.3.9.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☐ Evolved

☐ Advanced

☐ Leading

3.2.3.9.10 Stärken und Schwächen

Stärken	Schwächen
• Anonymisiert • Mehrstufiges Verfahren, welches unterschiedlichste Experten miteinbezieht	• Expertengremium statistisch nicht repräsentativ • Zwischenergebnisse entstehen durch Analyse einer sehr kleinen Gruppe

Tabelle 30: Stärken und Schwächen der Delphi-Methode

3.2.3.9.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☐ sehr gut

☒ gut

☐ weniger geeignet

3.2.3.10 Szenarioanalyse (deterministisch)

3.2.3.10.1 Einsatzzweck

Die (deterministische) Szenarioanalyse ist im betriebswirtschaftlichen Kontext und im Risikomanagement eine weit verbreitete Methode, die insbesondere im Bereich Strategie/Unternehmensentwicklung als Instrument der Entscheidungsvorbereitung und -

unterstützung etabliert ist.[167] Sie wird vorrangig bei zukunftsorientierten Fragestellungen eingesetzt, kann aber auch bei der Auswahl einer Alternative bei einer unmittelbar anstehenden Entscheidung wirkungsvoll unterstützen (vgl. Abbildung 19). Szenarios werden häufig in Form eines Szenariotrichters dargestellt. Die Trichterform basiert darauf, dass die Unsicherheit zunimmt, je weiter potenzielle Szenarien in der Zukunft liegen. Die Grundidee ist, einen alternativen Zustand zu beschreiben und anhand dieser Beschreibung Konsequenzen auf eine zu untersuchende Fragestellung abzuleiten.[168] In aller Regel werden die so erhaltenen Kenntnisse verwendet, um darauf aufbauend zu konkreten Handlungsempfehlungen zu gelangen.

Die Szenarioanalyse wurde im Jahr 1967 von Herman Kahn und Anthony J. Wiener in die Wirtschaftswissenschaften eingeführt. Sie definieren Szenario als „a hypothetical sequence of events constructed for the purpose of focussing attention on causal processes and decision points".[169] Kahn und Wiener weiter: "They answer two kinds of questions: (1) Precisely how might some hypothetical situation come about, step by step? and (2) What alternatives exist, for each actor, at each step, for preventing, diverting, or facilitating the process"[170]. Kahn wollte – nach den Erfahrungen des Zweiten Weltkriegs – mit Hilfe von Szenarien eingetretene Denkpfade verlassen und unvorstellbare und undenkbare („think the unthinkable") Entwicklungen bei den Analysen berücksichtigen.

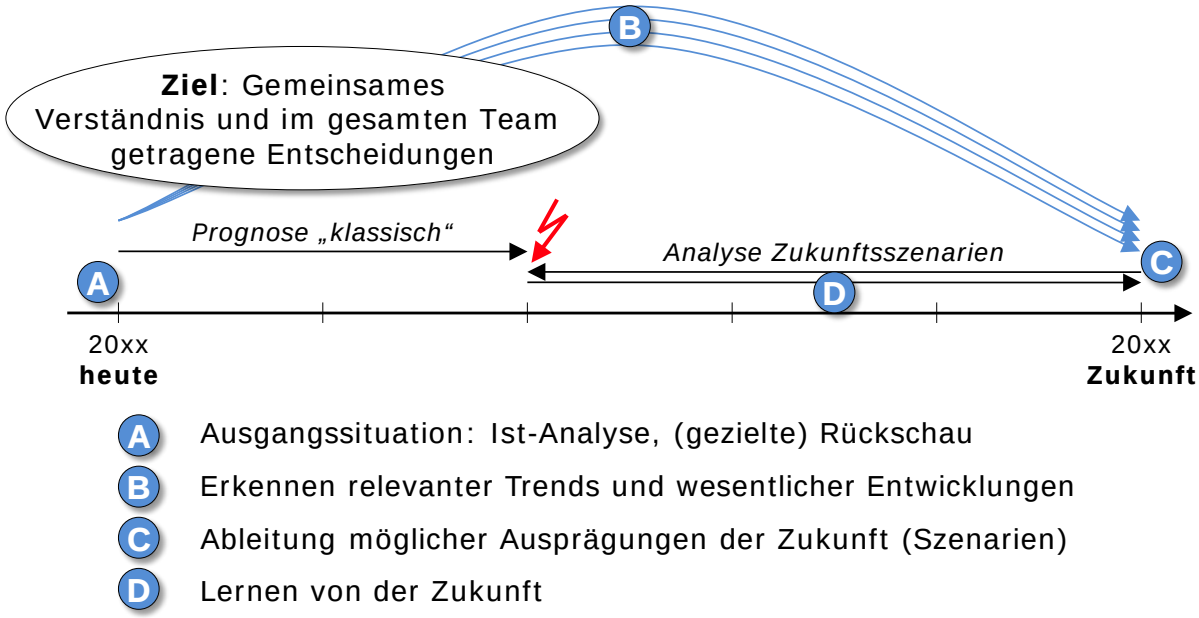


Abbildung 19: Formale Grundidee der (deterministischen) Szenarioanalyse[171]

[167] Die nachfolgenden Ausführungen basieren auf Romeike/Eicher (2017) sowie Romeike/Spitzner (2013), S. 94 ff.
[168] Vgl. Romeike/Spitzner (2013), S. 94.
[169] Kahn/Wiener (1967), S. 6.
[170] Kahn/Wiener (1967), S. 6.
[171] Quelle: Romeike/Eicher (2017).

3.2.3.10.2 Beschreibung

In Abbildung 20 ist ein aus acht Schritten bestehendes Vorgehensmodell dargestellt.[172]

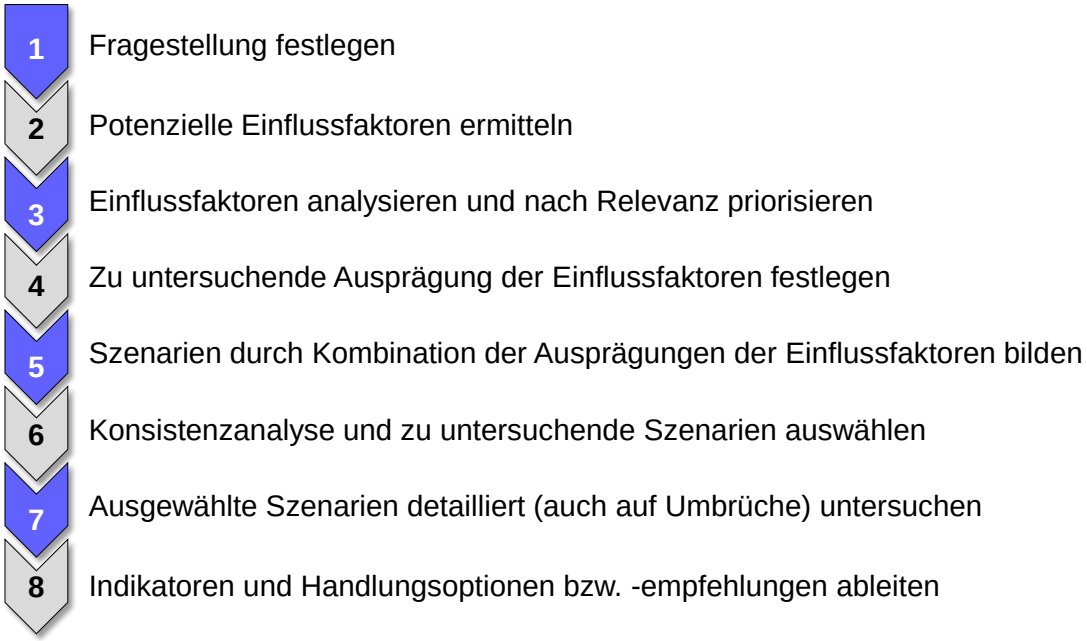


Abbildung 20: Berücksichtigung von Risiken im Planungsprozess

Der erste Schritt, das Festlegen der zu untersuchenden Fragestellung, dient insbesondere zwei wichtigen Aspekten: Klarheit zu erlangen, was genau zu untersuchen ist, sowie dem gemeinsamen Verständnis darüber im Team.[173] Bei dem zweiten Aspekt geht es auch darum, eine gemeinsame Sprache zu finden, was in einem interdisziplinär oder sogar intersektoral zusammengesetzten Team nicht ganz einfach, aber sehr wichtig ist. Nur das gemeinsame Verständnis sichert, dass in der weiteren Analyse das Team in die gleiche Richtung arbeitet.

Einflussfaktoren beschreiben relevante Sachverhalte in Bezug auf die zu untersuchende Fragestellung (zweiter Schritt). Sie sind dadurch gekennzeichnet, dass sie veränderlich sind und diese Veränderung jeweils wichtig in Bezug auf die Fragestellung ist. Das Identifizieren von Einflussfaktoren beginnt häufig als interne Analyse unter dem Einsatz von Kreativitätstechniken. Gegebenenfalls können hier Strukturvorgaben – etwa die klassische PESTLE-Analyse (siehe Abschnitt 2.2.1) – bei der Sammlung potenzieller Einflussfaktoren helfen. Basierend auf diesen Ergebnissen helfen vertiefende Literaturrecherchen und Experteninterviews, die ermittelten Einflussfaktoren zu verifizieren und zu ergänzen. Im Ergebnis dieses Schrittes sollte zu den Einflussfaktoren ein gemeinsames Verständnis vorherrschen, Duplikate sollten

[172] Die nachfolgenden Ausführungen basieren auf Romeike/Spitzner (2013), S. 95 ff.
[173] Vgl. Romeike/Spitzner (2013), S. 95.

ebenso wie Ober- und Unterbegriffe eliminiert sein. Um in der späteren Analyse Missdeutungen zu vermeiden, sind Einflussfaktoren wertfrei zu beschreiben.

Im dritten Schritt sind die Einflussfaktoren entsprechend ihrer Wichtigkeit in Bezug auf die Fragestellung zu priorisieren. Ziel ist es, sich in der weiteren Analyse auf die wichtigsten Einflussfaktoren zu konzentrieren. Als Faustregel sollten hiernach nicht mehr als zwanzig Einflussfaktoren üblich bleiben. Dadurch wird die Komplexität der weiteren Analyse reduziert. Ohne diese Priorisierung besteht die Gefahr, in die Komplexitätsfalle zu tappen und an der Analyse zu scheitern. Als Instrumente kommen hier die Einflussfaktorenanalyse, auch Vernetzungsmatrix oder Papiercomputer von Vester bzw. Vester'sche Einflussmatrix genannt, oder auch eine Einfluss-Unsicherheitsanalyse zum Einsatz.

Im vierten Schritt werden die als realistisch erscheinenden Ausprägungen je Einflussfaktor für die weitere Szenarioanalyse festgelegt. Quellen für diese Festlegung sind Studien, Experteninterviews, Extrapolationen, Gruppendiskussionen und Intuition.

Mögliche Szenarien werden anschließend in einem fünften Schritt durch Kombination verschiedener Ausprägungen der Einflussfaktoren gebildet. Für diese ist zu untersuchen, ob sie in sich möglichst konsistent sind, das heißt, ob die Ausprägungen der Einflussfaktoren sich nicht widersprechen. Dies kann mit einer paarweisen Analyse oder mit Hilfe einer Konsistenzmatrix erfolgen (sechster Schritt). Aus den konsistenten Szenarien werden dann diejenigen ausgewählt, die im Folgenden detailliert zu untersuchen sind.

Die ausgewählten Szenarien werden in Hinblick auf die zu untersuchende Fragestellung analysiert und die sich aus ihnen ergebenden Konsequenzen abgeleitet. Oft ist es ratsam, Störereignisse wie beispielweise externe Schocks oder Trendbrüche mit in diese Analyse aufzunehmen, um so ein Gefühl für die Sensitivität beziehungsweise Stabilität der Szenarien zu erhalten (siebter Schritt). Änderungen im Ausmaß einer Katastrophe sollten bei dieser Sensitivitätsanalyse jedoch außen vor bleiben, da mit ihnen häufig eine Veränderung des gesamten Gefüges verbunden ist, also die getroffenen Annahmen und berücksichtigen Wirkungszusammenhänge nicht mehr gelten. Basierend auf den Konsequenzen werden Handlungsoptionen gesammelt und diese ebenfalls auf ihren Einfluss hin untersucht. Ergebnis sind dann konkrete Handlungsempfehlungen für die untersuchte Fragestellung (achter Schritt). Insbesondere für negative Szenarien ist es zudem ratsam, Indikatoren zu identifizieren, die den Eintritt des Szenarios ankündigen. All diese Ergebnisse werden in einem sogenannten Szenario-Steckbrief zusammengefasst.

3.2.3.10.3 Anwendungsbeispiel

Konkrete Anwendungen dieser flexiblen Simulationsmethode im betriebswirtschaftlichen Kontext sind beispielsweise:[174]

- Analyse alterativer beziehungsweise zukünftiger Zustände. Hierbei geht es darum, mögliche Entwicklungen zu identifizieren, die dahinterstehenden Annahmen zu explizieren und besonders relevante Entwicklungen zu erkennen. Auswirkungen externer und interner Einflüsse werden analysiert. Darüber hinaus werden in diesem Prozess häufig auch Unsicherheiten, Wissenslücken und Dilemmata aufgedeckt, die im Rahmen der Entscheidungsfindung zu berücksichtigen sind.
- Zielbildung und Entscheidungsunterstützung. Existieren lediglich vage Zielvorstellungen, können diese mit Hilfe der Szenarioanalyse konkretisiert werden. Im Fokus der Analyse stehen Fragen wie: Wohin soll es gehen? Was soll konkret erreicht werden? Wie soll dieses Ziel geschafft werden? Dazu sind in aller Regel alternative Handlungsoptionen zu entwickeln und zu bewerten, um Entscheidungsprozesse aktiv und wirkungsvoll zu unterstützen.
- Kommunikation von Sach- oder Problemlagen. Szenarien eignen sich auch hervorragend, einzelne Entscheider oder auch breite Bevölkerungsschichten über Themen und Problemlagen zu informieren (beispielsweise Auswirkungen der Digitalisierung auf die Gesellschaft oder Auswirkungen der Elektromobilität auf die Automobilindustrie etc.). Szenarien schaffen es durch ihre bildhafte und gegebenenfalls pointierte Darstellung eines möglichen Zustands, einen Sachverhalt greifbar und verständlich zu machen. Interne wie öffentliche Debatten lassen sich dadurch anreichern. Ausführungen und Erläuterungen können mit Hilfe von Szenarien konkret und bildlich anstelle von vage und abstrakt vermittelt werden.

Daher ist die (deterministische) Szenarioanalyse auch sehr gut auf Fragestellungen im Bereich der kritischen Infrastruktur anwendbar.

3.2.3.10.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☒ Risikobewertung

☒ Risikosteuerung

[174] Vgl. Romeike/Spitzner (2013), S. 98 ff.

3.2.3.10.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☒ Expertenschätzung

3.2.3.10.6 Output

☐ eher qualitativ

☒ qualitativ und quantitativ

☐ eher quantitativ

☐ rein quantitativ

3.2.3.10.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☒ mittel

☒ hoch

Der zeitliche Aufwand hängt sehr stark von der Komplexität der Fragestellung ab. Insgesamt dürfte der Aufwand bei Fragestellungen im Kontext kritischer Infrastruktur eher als hoch einzuschätzen sein.

3.2.3.10.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☒ mittel

☒ hoch

Der personelle Aufwand hängt sehr stark von der Komplexität der Fragestellung und von de Zusammensetzung des „Szenarioteams“ ab.

3.2.3.10.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☐ Evolved

☒ Advanced

☒ Leading

3.2.3.10.10 Stärken und Schwächen

Stärken	Schwächen
• Eine Szenarioanalyse erlaubt den Einbezug qualitativer Aspekte und quantitativer Daten in die Analyse, sie fördert das Denken in Alternativen. • Häufig werden durch die Betrachtung aus verschiedenen Perspektiven Zusammenhänge sichtbar, die auf den ersten Blick nicht offensichtlich sind, darüber hinaus erweitert die meist interdisziplinäre Zusammenarbeit die Sichtweise des Analyseteams. • Die Szenarioanalyse kann leicht mit weiteren Methoden der Erkenntnisgewinnung kombiniert werden, beispielsweise Prognosen, Umfragen oder Delphi-Verfahren. • Die Szenarioanalyse „zwingt“ die Teilnehmer zu einem strukturierten Vorgehen bei der Analyse zukünftiger Szenarien. • Komplexität kann mit Hilfe der Einflussfaktorenanalyse sowie der Konsistenzmatrix reduziert werden.	• Erforderlich für den Einsatz der Szenarioanalyse ist die Fähigkeit komplex und vernetzt zu denken. • Die Qualität der Szenarien ist unter anderem abhängig von Kompetenz, Vorstellungskraft, Kreativität, Teamfähigkeit, Kommunikationsfähigkeit oder Enthusiasmus der Teilnehmer der Szenarioanalyse; hierin liegen vielfältige Möglichkeiten für ein Scheitern. • Die Ergebnisse der Analyse sind – je nach Stärke der subjektiven Beeinflussung durch die Teilnehmer – nicht wertfrei und daher keine gesicherten Erkenntnisse, sie sind stets angreifbar. • Die Anwendung der Methode ist zeit- und arbeitsintensiv, damit in der Regel auch mit hohen Kosten verbunden.

Tabelle 31: Stärken und Schwächen der (deterministischen) Szenarioanalyse

3.2.3.10.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

Durch das „Lernen aus der Zukunft“ ist die Szenarioanalyse sehr gut für Fragestellungen im Bereich der kritischen Infrastruktur geeignet. Insbesondere bisher unbekannte Szenarien können mit Hilfe dieser Methode evaluiert und diskutiert werden.

3.2.3.11 Stochastische Szenarioanalyse (Monte-Carlo-Simulation)

3.2.3.11.1 Einsatzzweck

Die stochastische Szenarioanalyse (Monte-Carlo-Simulation) basiert auf der Idee, die Eingangsparameter einer Simulation als Zufallsgrößen zu betrachten.[175] So können analytisch nicht oder nur aufwendig lösbare Probleme mit Hilfe der Wahrscheinlichkeitstheorie (die Teil der Stochastik ist, die Wahrscheinlichkeitstheorie und Statistik zusammenfasst) numerisch gelöst werden. Generell lassen sich zwei Problemgruppen unterscheiden, bei denen die Stochastische Szenarioanalyse angewendet werden kann. Mit ihrer Hilfe können einerseits Problemstellungen deterministischer Natur, die eine eindeutige Lösung besitzen, bearbeitet werden. Auf der anderen Seite sind aber auch Fragen, die sich der Gruppe stochastischer Problemstellungen zuordnen lassen, für eine Monte-Carlo-Simulation ein geeignetes Anwendungsfeld. Die Basis für die Simulation bildet eine sehr große Zahl gleichartiger Zufallsexperimente.

Aus einer betriebswirtschaftlichen Sicht können alle Fragen untersucht werden, die

- entweder aufgrund der Vielzahl ihrer Einflussgrößen nicht mehr exakt analysiert werden (können) und bei denen daher auf eine Stichprobe für die Analyse zurückgegriffen wird;
- oder bei denen die Eingangsparameter Zufallsgrößen sind (Auch die Optimierung von Prozessen oder Entscheidungen bei nicht exakt bekannten Parametern gehören zu dieser Gruppe).

Die Anwendung der stochastischen Szenarioanalyse ist breit gefächert und reicht unter anderem von der Stabilitätsanalyse von Algorithmen und Systemen, der Aggregation von Einzelrisiken eines Unternehmens zu einem unternehmerischen Gesamtrisiko, der Vorhersage von Entwicklungen, die selbst durch zufällige Ereignisse beeinflusst werden (stochastische Prozesse), der Optimierung von Entscheidungen, die auf unsicheren Annahmen beruhen bis zur Modellierung komplexer Prozesse (Wetter/Klima, Produktionsprozesse, Supply-Chain-Prozesse, Rekonstruktionsverfahren in der Nuklearmedizin) oder der Schätzung von Verteilungsparametern.

[175] Die nachfolgenden Ausführungen basieren auf Romeike/Eicher (2017) sowie Romeike/Spitzner (2013), S. 94 ff.

3.2.3.11.2 Beschreibung

Das Vorgehen bei einer stochastischen Simulation (Monte-Carlo-Simulation) wurde von Metropolis und Ulam in einem Artikel beschrieben, der im Jahre 1949 im Journal of the American Statistical Association erschienen ist. Darin beschreiben beide Wissenschaftler das Vorgehen bei der Monte-Carlo-Methode durch zwei Schritte: „(1) production of ‚random' values with their frequency distribution equal to those which govern the change of each parameter, (2) calculation of the values of those parameters which are deterministic, i.e., obtained algebraically from the others"[176].

An diesem durch Metropolis und Ulam beschriebenen Vorgehen hat sich in den letzten 60 Jahren nicht viel geändert (vgl. Abbildung 21).

Abbildung 21: Grundsätzliches Vorgehen der stochastischen Szenarioanalyse

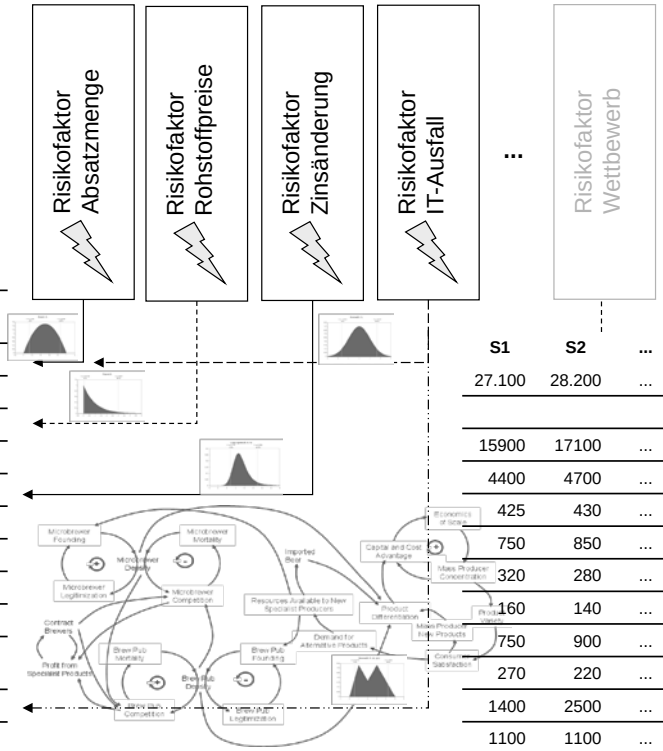
3.2.3.11.3 Anwendungsbeispiel

Die stochastische Szenarioanalyse kann im Kontext kritischer Infrastrukturrisiken beispielsweise für die Risikoaggregation sowie die Analyse einer kumulierenden Wirkungen der Risiken verwendet werden.

Im Rahmen einer stochastischen Szenarioanalyse werden zunächst die Wirkungen der relevanten Einzelrisiken bestimmten Positionen, etwa der Plan-Gewinn-und-Verlust-Rechnung oder der Plan-Cash-flow-Rechnung, zugeordnet. Beispielsweise wird sich eine ungeplante Erhöhung der Kupferpreise oder anderer Rohstoffpreise auf die Position „Materialaufwand" auswirken. Eine Voraussetzung für die Bestimmung des „Gesamtrisikoumfangs" mittels Risi-

[176] Vgl. Metropolis/Ulam (1949)

koaggregation stellt die Zuordnung von Risiken zu Positionen der Unternehmensplanung dar. Dabei können Risiken beispielsweise als Schwankungsbreite um einen Planwert modelliert werden (beispielsweise +5 % / -2 % Absatzmengenschwankung) oder auch als ereignisorientierte Risiken (Häufigkeit sowie Schadensausmaß). Die in Abbildung 22 beispielhaft aufgeführten Szenarien S_1 bis S_n zeigen dabei die unterschiedlichen Zukunftspfade der Outputvariablen – basierend auf den modellierten Risiken (Inputfaktoren) – auf.



Erträge	IST 2017 in T€	PLAN 2018 in T€	S1	S2	...	Sn
Umsatzerlöse	25.000	28.000	27.100	28.200	...	29.500
Aufwendungen						
Materialeinsatz	15.600	17500	15900	17100	...	17900
Personalkosten	4.500	4600	4400	4700	...	4800
Zinsaufwand	418	418	425	430	...	410
Verkaufsprovisionen	750	800	750	850	...	810
Kundenskonto	280	300	320	280	...	300
Hilfs- und Betriebsstoffe	140	150	160	140	...	150
Stromkosten	680	850	750	900	...	710
Instandhaltung Maschinen	265	265	270	220	...	310
sonstiger Aufwand	550	550	1400	2500	...	450
Abschreibungen	1.100	1100	1100	1100	...	1100
Gewinn (vor Steuern)	717	1.467	1.625	-20	...	2.560

Abbildung 22: Berücksichtigung von Risiken im Planungsprozess[177]

Ein Blick auf die verschiedenen Szenarien der Simulationsläufe veranschaulicht, dass bei jedem Simulationslauf andere Kombinationen von Ausprägungen der Risiken resultieren. Damit erhält man in jedem Schritt einen simulierten Wert für die betrachtete Zielgröße (beispielsweise Gewinn oder Cashflow). Die Gesamtheit aller Simulationsläufe beziehungsweise simulierten Gewinn- und Verlustrechnungen (oder Bilanzen oder Cash-Flow-Rechnungen) liefert eine „repräsentative Stichprobe“ aller möglichen Risiko-Szenarien des Unternehmens. Aus den ermittelten Realisationen der Zielgröße ergeben sich aggregierte Wahrscheinlichkeitsverteilungen (Dichtefunktionen), die dann für weitere Analysen genutzt werden (vgl. Abbildung 23 und Abbildung 24).

[177] Quelle: Romeike/Hager (2013), S. 133.

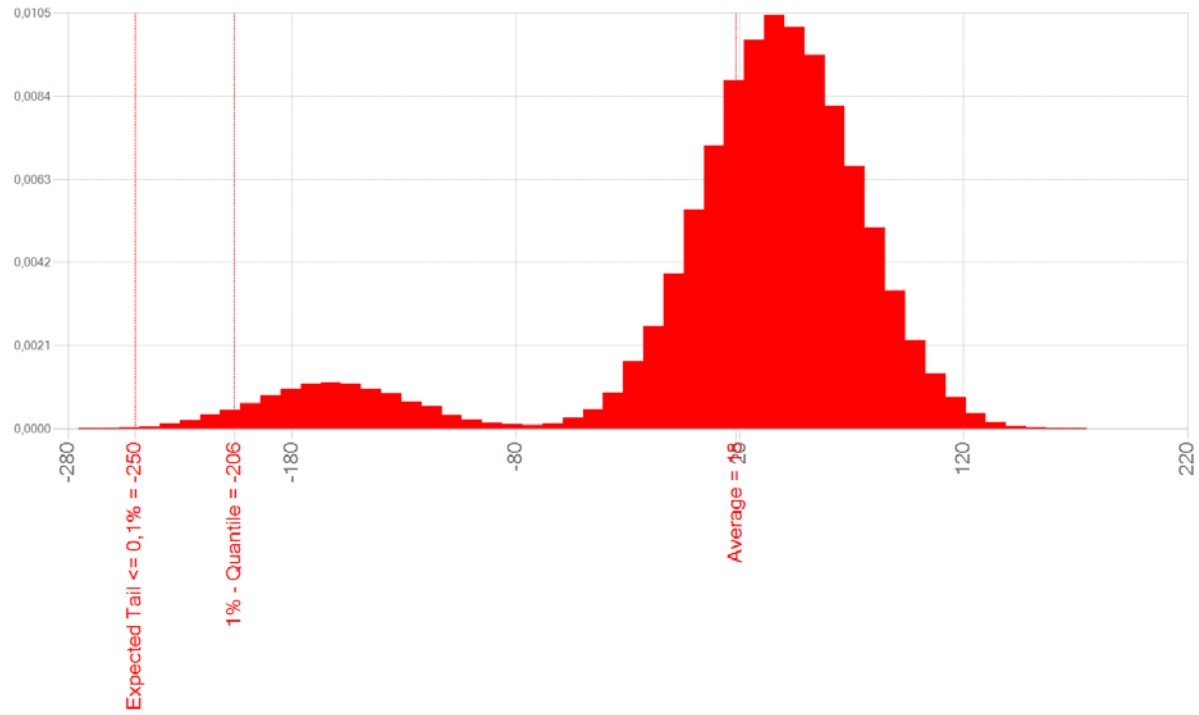


Abbildung 23: Histogramm basierend auf 100.000 simulierten Szenarien[178]

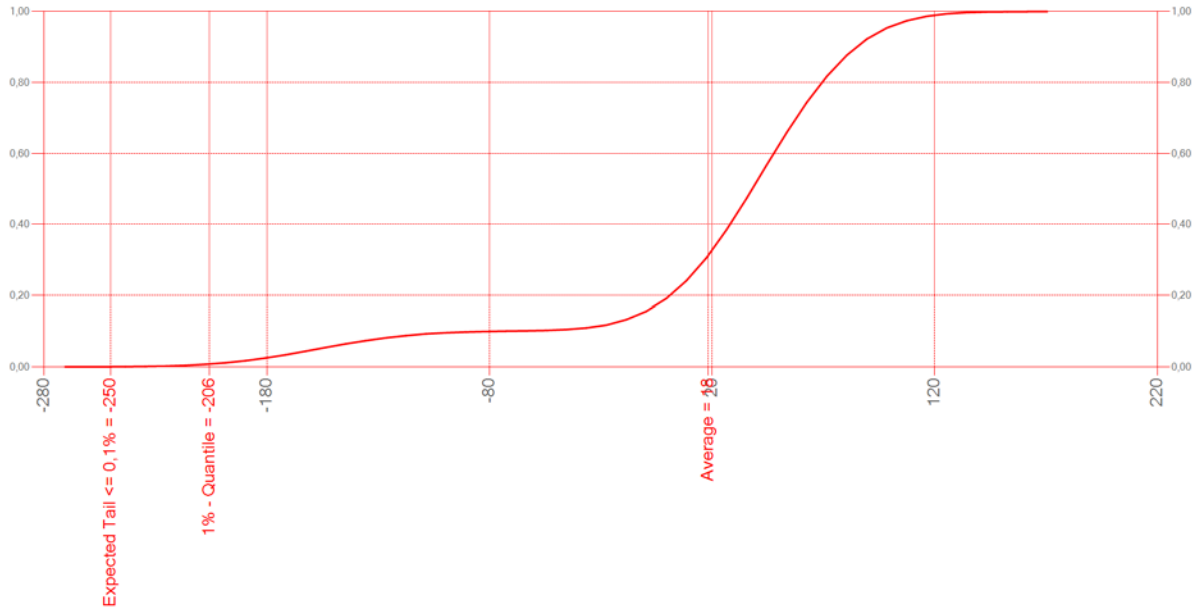


Abbildung 24: Kumulierte Dichtefunktion (CDF, Cumulative Distribution Function) basierend auf 100.000 simulierten Szenarien[179]

[178] Quelle: Romeike/Eicher (2017).
[179] Quelle: Romeike/Eicher (2017)..

Ein komplettes Umsetzungsbeispiel zur Risikoaggregation und zur Umsetzung einer Szenariooplanung (Bandbreitenplanung, Korridorplanung) finden Sie bei Romeike/Spitzner[180] sowie Romeike/Stallinger[181].

3.2.3.11.4 Phase

☒ Risikoidentifikation

☒ Risikoanalyse

☒ Risikobewertung

☒ Risikosteuerung

3.2.3.11.5 Input/Datenbedarf

☒ Quantitative/historische/empirische Daten

☒ Expertenschätzung

3.2.3.11.6 Output

☐ eher qualitativ

☐ qualitativ und quantitativ

☐ eher quantitativ

☒ rein quantitativ

3.2.3.11.7 Zeitlicher Aufwand für den Methodeneinsatz

☐ niedrig

☒ mittel

☒ hoch

Der zeitliche Aufwand hängt sehr stark von der Komplexität der Fragestellung ab. Insgesamt dürfte der Aufwand bei Fragestellungen im Kontext kritischer Infrastruktur eher als hoch einzuschätzen sein.

[180] Vgl. Romeike/Spitzner (2013), S. 265 ff.
[181] Vgl. Romeike/Stallinger (2012).

3.2.3.11.8 Personeller Aufwand (Qualifikation etc.) für den Methodeneinsatz

☐ niedrig

☒ mittel

☒ hoch

Der personelle Aufwand hängt sehr stark von der Komplexität der Fragestellung ab. Insgesamt dürfte der personelle Aufwand bei Fragestellungen im Kontext kritischer Infrastruktur eher als hoch einzuschätzen sein, da unterschiedliche Experten bei der Erstellung des „stochastischen Modells“ involviert sein werden.

3.2.3.11.9 Reifegrad des zugrundeliegenden Risikomanagements

☐ Initial

☐ Basic

☒ Evolved

☒ Advanced

☒ Leading

3.2.3.11.10 Stärken und Schwächen

Stärken	Schwächen
• Einfach anwendbare Berechnungsmethode zur Berücksichtigung von Unsicherheiten. • In der Regel deutlich höhere Transparenz und Erkenntnisse (etwa im Entscheidungsprozess) als in klassischen Verfahren. • Kann Volatilitätsclustering, fat tails, nichtlineare Exposures und Extremszenarios in der Risikoberechnung berücksichtigen • Bei vielen Fragestellungen (beispielsweise der Risikoaggregation) die einzige praktikable Methode. • Die Methode kann beliebige Verteilungen simulieren.	• Nicht selten sind Wahrscheinlichkeitsverteilungen und deren Parameter nur geschätzt (Expertenschätzungen), größere Fehler in diesen Schätzungen führen zu nicht validen oder sogar falschen Ergebnissen.

Tabelle 32: Stärken und Schwächen der stochastischen Szenarioanalyse

3.2.3.11.11 Gesamtbewertung/Eignung für das Risikomanagement kritischer Infrastrukturen in der Logistik

☒ sehr gut

☐ gut

☐ weniger geeignet

Bei der stochastischen Szenarioanalyse (Monte-Carlo-Simulation) handelt es sich um eine etablierte und fundierte Methode im Risikomanagement. Im Kontext Risikoaggregation existiert keine alternative Methode. Auch zur Analyse von Risiken im Bereich von kritischen Infrastrukturrisiken handelt es ich um eine flexible und höchst effiziente Methode, die auch sehr gut mit anderen Methoden (Brainstorming, deterministische Szenarioanalyse etc.) kombiniert werden kann.

4 Netzwerkbasierte Ansätze zur Risikobewertung kritischer Infrastrukturen in der Logistik

4.1 Bedeutung netzwerkbasierter Ansätze zur Risikobewertung

Die im vorherigen Kapitel dargestellten und bewerteten Methoden stellen das Handwerkzeug dar, um grundsätzlich, aber im Speziellen auch für kritische Infrastrukturen in der Logistik, Risiken zu identifizieren, sie zu analysieren und zu bewerten. Die Toolbox mit Methoden des Risikomanagements ist aber immer noch von generischer Natur. Das bedeutet: In der Regel müssen die dargestellten Methoden noch an spezifische Rahmenbedingungen angepasst werden (zum Beispiel an die Art der kritischen Infrastruktur oder an die Prozesse, die die Infrastruktur nutzen).

Bereits in Abschnitt 2.4 wurden Forschungsansätze vorgestellt, die die Spezifika der logistischen Infrastruktur explizit berücksichtigten. Dabei ging es vor allem um den Netzwerk-Charakter der logistischen Infrastruktur.

Der Netzwerk-Charakter soll in diesem Kapitel aufgegriffen werden, um zwei methodische Ansätze vorzustellen, bei denen einzelne Elemente oder die logistische Infrastruktur als Ganzes bewertet werden kann. Diese Methoden basieren auf der Annahme, dass einzelne Risiken und deren Ursachen bereits identifiziert sind. Die Auswirkungen sind insofern bekannt, als davon ausgegangen wird, dass sie – zumindest temporär – ein oder mehrere Elemente der logistischen Infrastruktur unbenutzbar machen. Auf Basis dieses temporären Ausfalls von Knoten und/oder Kanten der Infrastruktur stellt sich die Frage nach den weiteren Auswirkungen. Diese sind, aufgrund der Komplexität eines Netzwerks, nicht unmittelbar ersichtlich. Der Auswahl einer Kante oder eines Knotens kann möglicherweise durch die Nutzung anderer Kanten oder Knoten kompensiert werden; andererseits ist das Netzwerk möglicherweise bereits so ausgelastet, dass alternative Kanten oder Knoten nicht verfügbar sind.

Im Folgenden werden daher zwei netzwerk-basierte Ansätze vorgestellt, die auf Basis von Methoden des Operations Research, eine Bewertung von Risiken für die logistische Infrastruktur ermöglichen. Es sind – trotz des expliziten Infrastrukturbezugs – abstrakte Methoden, die zunächst viele Details logistischer Prozesse nicht abbilden; nur so wird die grundsätzliche Vorgehensweise deutlich. Für eine konkrete Umsetzung sind deutlich mehr Spezifika zu berücksichtigen; diese lassen sich aber problemlos integrieren. Die generelle Methodik bleibt davon nicht betroffen.

4.2 Ansatz 1

4.2.1 Grundidee

Ein multimodales Logistiknetzwerk, wie das Logistiknetzwerk Hessens, wird durchgehend von einer Vielzahl verschiedener Akteure genutzt. In der Realität sind dies, zumindest in eini-

gen uni- oder multimodalen Teilnetzwerken, Logistikdienstleister, private Nutzer und der öffentliche Nahverkehr (ÖPNV).

Im Gegensatz zu einer Supply Chain, in der eine höhere betriebliche Managementebene in der Regel das gesamte Netzwerk regulieren kann, kann ein solches, offenes Netzwerk nie vollständig gesteuert werden. Um eine valide Risikobewertung zu erstellen, muss daher das Verhalten aller Nutzer des Netzwerks geschätzt beziehungsweise simuliert werden. Auch die Verhaltensänderungen nach der Realisierung eines Risikos muss entsprechend unterstellt werden.

Die Risikobewertung, also die Messung des Schadensausmaßes, kann dann als der Kostenzuwachs des Gesamtnetzwerkes nach der Realisierung eines Risikos verstanden werden. Um diese zu quantifizieren müssen die Gesamtkosten des Netzwerkes zweimal, und zwar vor und nach dem Eintritt des Risikos, bewertet werden.

4.2.2 Annahmen

Um eine Risikobewertung eines (Teil-) Netzwerkes zu ermöglichen, werden folgende Annahmen getroffen:

- Das Netzwerk besteht aus endlich vielen wohldefinierten Punkten, die im folgenden „Gemeinden“ genannt werden.
- Für jede Gemeinde ist die Nettonachfrage beziehungsweise das Nettoangebot in Transporteinheiten (TE) bekannt.
- Für jede Verbindung zwischen zwei Gemeinden ist eine maximale Kapazität in TE pro Zeiteinheit (ZE) bekannt.
- Für jede Verbindung zwischen zwei Gemeinden sind die Nutzungskosten der Verbindung in TE bekannt.

Ferner sei das Netzwerk geschlossen, also jede TE, die von einer Gemeinde *v* innerhalb des Netzwerkes angeboten wird, in einer Zielgemeinde *w* innerhalb des Netzwerkes nachgefragt. Im Gegensatz zu den obigen Annahmen schränkt diese Bedingung das Netzwerk nicht real ein, da jedes nicht-geschlossene Netzwerk leicht in ein geschlossenes Netzwerk überführt werden kann. Hierzu werden Dummy-Gemeinden eingeführt, welche die externe Nachfrage und das externe Angebot symbolisieren. Schließlich folgen alle Nutzer des Netzwerks einem ökonomischen, also profitmaximierenden Handeln. Die obigen Annahmen implizieren unter anderem, dass private Nutzer und Nutzer des öffentlichen Verkehrs in folgendem Modell nicht abgebildet werden können. Um die beanspruchte Kapazität dieser nicht-logistischen Nutzer implizit doch zu beachten wird die Kapazität aller Verbindungen innerhalb des Netzwerkes um die durchschnittliche private und öffentliche Nutzung reduziert.

4.2.3 Netzwerkkonstruktion

Das logistische Netzwerk der beobachteten Region kann als Graph $G = (V, E)$ modelliert werden. Jeder Knoten $v \in V$ repräsentiert dann eine Gemeinde innerhalb des Netzwerkes und jede Kante $e = (v, w) \in E \subseteq V \times V$ repräsentiert eine einzelne Direktverbindung zwischen zwei Gemeinden. Insbesondere sind ist der Graph nicht schlicht, da zwar keine Schlingen, sehr wohl aber Mehrfachverbindungen zwischen Gemeinden existieren können. Beispielhaft seien die Gemeinden Frankfurt und Hanau erwähnt, die per Schiene, per Wasserstraße und per Autobahn direkt miteinander verbunden sind. Somit existieren drei Kanten zwischen den beiden Knoten, die Frankfurt beziehungsweise Hanau repräsentieren.

Ferner sei $b(v)$ die Nettonachfrage bzw. das Nettoangebot der Gemeinde $v \in V$ pro Zeiteinheit. Anbietende Gemeinden haben hierbei einen positiven Wert, während Gemeinden mit mehr Bedarf als Angebot einen negativen Wert zugewiesen bekommen. Durch die Annahme der Geschlossenheit des Netzwerks gilt, dass Bedarf und Angebot sich ausgleichen und es damit keine überschüssige Nachfrage und kein überschüssiges Angebot gibt:

$$\sum_{\forall v \in V} b(v) = 0$$

Abschließend besitzt jede Kante eine nicht-negative maximale Kapazität pro Zeiteinheit $u(e)$ und Nutzungskosten $c(e)$.

4.2.4 Problemdefinition

Basierend auf dem oben definierten Netzwerk lässt sich ein geeignetes Optimierungsproblem definieren, welches die Gesamtkosten des Netzwerks minimiert. Diese Kosten repräsentieren, zumindest annähernd und unter den obigen Annahmen, das Gesamtverkehrsaufkommen innerhalb des Netzwerkes. In der Realität verhalten sich die Nutzer des Netzwerkes hingegen üblicherweise egoistisch und sind einzig an der Minimierung ihrer eigenen Kosten, nicht an der Minimierung der Gesamtkosten des Netzwerkes, interessiert. Sollte jedoch die Kapazität auf einem beliebigen, vielgenutzten, Teilnetzwerk eine knappe Ressource darstellen, so werden sogar egoistisch agierende Nutzer auf die „nächstbessere“ Route ausweichen. Auf diesem Wege nähert sich schlussendlich das reale Verkehrsaufkommen, zumindest langfristig, der errechneten optimalen Lösung schrittweise an.

Ein zweiter Kritikpunkt an obigem Modell könnte sein, dass es keine Differenzierung zwischen unterschiedlichen Gütern bzw. Güterklassen vornimmt. Dies bedeutet praktisch, dass jedes Angebot von Gut „A“ jede Nachfrage von Gut „B“ theoretisch befriedigen könnte, solange die Mengen in TE übereinstimmen. Um doch verschiedene Güter bzw. Güterklassen unterscheiden zu können, oder um sicherzustellen, dass Unternehmen „X“ nicht die Nachfrage von Unternehmen „Y“ befriedigen kann, könnten für jedes Gut beziehungsweise jede Gü-

terklasse und für jedes Unternehmen eigene Netzwerke definiert werfen. Um daraus eine vollumfängliche Lösung des Gesamtproblems abzuleiten, könnte zunächst das zugrundeliegende Problem für ein erstes (priorisiertes) Gut und Unternehmen gelöst werden. Der Kapazitätsverbrauch dieses priorisierten Guts und Unternehmens wird anschließend an jeder einzelnen Kante des Graphen von der Gesamtkapazität abgezogen. Auf dem so entstandenen Graphen entsprechen also die Kantengewichte nun der „Restkapazität“ nach der Nutzung durch das priorisierte Gut und Unternehmen. Sukzessive können so, nach Priorisierung sortiert, alle Güter beziehungsweise Güterklassen und Unternehmen eingearbeitet werden.

Das resultierende, zu lösende, Optimierungsproblem ist in der Literatur bekannt als „Minimum Cost Flow Problem“ oder „Minimal Cost Flow Problem“ und kann wie folgt als lineares Optimierungsproblem dargestellt werden:

$$\min \sum_{e \in E} c(e) \cdot f(e)$$

$$\sum_{e \in N^+(v)} f(e) - \sum_{e \in N^-} f(e) = b(v) \qquad \forall v \in V$$

$$0 \leq f(e) \leq u(e) \qquad \forall v \in V$$

Hierbei bezeichnet $f(e)$, für alle $e \in E$, die Entscheidungsvariablen des Modells. Ferner bezeichnet $N^+(v)$ die Menge aller positiven Nachbarn eines Knotens $v \in V$ und analog $N^-(v)$ die Menge aller negativen Nachbarn eines Knotens $v \in V$.

Die Zielfunktion minimiert die Gesamtkosten des Netzwerks. Die erste Nebenbedingung garantiert, dass jede Lösung tatsächlich einen Fluss innerhalb des Netzwerks repräsentiert, welche die Gesamtheit an Nachfrage und Angebot erfüllt. Die zweite Nebenbedingung sichert, dass die Kapazitätsrestriktion auf jeder einzelnen Kante erfüllt wird.

4.2.5 Lösung des Problems

Das zuvor definierte Optimierungsproblem kann, zum Beispiel mit dem „Mean Cycle Cancelling“-Algorithmus, in Polynomialzeit gelöst werden. Jede Lösung des Problems besteht einerseits aus den exakten Verkehrsmengen auf allen Kanten des Netzwerks und andererseits aus einem Zielfunktionswert, welcher die minimalen Gesamtkosten des Netzwerkes angibt. Dieser Zielfunktionswert kann als eine quantitative Bewertung des Gesamtnetzwerkes verstanden werden. Realisiert sich ein Risiko, kann das Netzwerk durch die Löschung der defekten Knoten und/oder Kanten beziehungsweise durch die Herabsetzung der Kapazität im Falle einer Einschränkung, an die neue Situation angepasst werden. Sei nun $\acute{G} = (\acute{V}, \acute{E})$ das resultierende Teilnetzwerk mit $\acute{E} \subseteq E$ und $\acute{V} \subseteq V$. Der Lösungsraum des Minimum Cost Flow

Problems auf $\acute{G}$ ist ein Unterraum des Lösungsraumes desselben Problems auf G. Insbesondere gilt somit für den Zielfunktionswert folgende Ungleichung:

$$\Delta MCFP := MCFP(\acute{G}) - MCFP(G) \geq 0$$

Diese Differenz der beiden Zielfunktionswerte kann als die „Preis“ des Risikos, welches hier realisiert wurde, verstanden werden. Mit Hilfe dieser „Risikokosten“ und der gemeinsamen Wahrscheinlichkeitsverteilung $P(\acute{V}, \acute{E})$ aller betroffenen Kosten und Kanten ist es dann möglich, dass Risiko wie folgt zu bewerten:

$$Risk(\acute{V}, \acute{E}) = P(\acute{V}, \acute{E}) \cdot \Delta MCFP$$

4.3 Ansatz 2

4.3.1 Grundidee

In der Praxis ist es den einzelnen Akteuren in der Regel nicht möglich, umfassende Infrastrukturdaten und Transportdaten zu erfassen. Dies impliziert, dass auch die Umsetzung des zuvor vorgestellten Ansatzes für zahlreiche Anwender, insbesondere für Nutzer des Netzwerks, nicht praktikabel ist. Um ein valide Risikobewertung auch aus Unternehmersicht zu ermöglichen bedarf es daher eines Ansatzes, der darauf abzielt, die Daten eines Akteurs, etwa eines Logistikdienstleisters, direkt zu nutzen.

Hierzu wurde ein alternativer Ansatz entwickelt, der dezidiert die wesentlich detaillierteren, aber weniger umfassenden Daten berücksichtigt. Erneut werden hierzu die Gesamtkosten aller logistischen Aktivitäten vor und nach der Realisierung eines Risikos berechnet und verglichen. Im Unterschied zum vorigen Risikobewertungsansatz wird jedoch nicht das Gesamtnetzwerk nach der Risikorealisierung re-optimiert, sondern es werden lediglich diejenigen logistischen Aktivitäten, die über betroffene Teilinfrastrukturen geroutet waren, neu geplant.

4.3.2 Annahmen

Um eine Risikobewertung eines (Teil-) Netzwerkes vorzunehmen, werden zunächst folgende Annahmen getroffen:

- Das Netzwerk besteht aus endlich vielen wohldefinierten Punkten, die im folgenden „logistische Punkte“ genannt werden.
- Für jede Verbindung zwischen zwei logistischen Punkten sind die Nutzungskosten bekannt.
- Sämtliche Transportaufträge, die das untersuchte Netzwerk, oder einen Teil dessen, nutzen, sind a priori bekannt. Ferner sei angenommen, dass gar das genaue Routing eines jeden Auftrags bereits bekannt ist. Konkret bedeutet dies, dass für jede Trans-

porteinheit die genaue Abfolge von genutzten Einzelverbindungen, von der Quelle bis zur Senke, bekannt ist.

4.3.3 Netzwerkkonstruktion

Das logistische Netzwerk der betrachteten Region wird als (ungerichteter) Graph $G = (V, E)$ wie folgt modelliert. Jeder Knoten $v \in V$ repräsentiert einen logistischen Punkt. Ein solcher, logistischer Punkt kann jede Art eines physisch existierenden Ortes sein, an dem logistische Aktivitäten stattfinden. Anders ausgedrückt ist V die Menge aller logistischen Orte, an denen logistische Objekte versandt, empfangen, weitergeleitet, gelagert, (wieder-) verpackt und/oder etikettiert werden. Diese Definition schließt sowohl logistische Punkte in Privatbesitz, wie etwa Lager eines Unternehmens, ebenso ein wie logistische Punkte der öffentlichen Hand, wie etwa Häfen, Bahnhöfe oder ähnliche.

Jede Kante $e \in E$ repräsentiert eine physische Verbindung zwischen zwei logistischen Punkten und ist so selbst Teil der logistischen Infrastruktur. Eine einzelne Kante repräsentiert hierbei stets ausschließlich eine unimodulare Verbindung, etwa eine Straße, eine Schienentrasse oder eine Wasserstraße. Dies impliziert, dass der Graph G nicht schlicht ist, da mehrere Verbindungen zwischen zwei logistischen Punkten existieren können, welche verschieden Transportmodi repräsentieren.

Die Informationen über alle aktuellen Aufträge und deren Routings werden genutzt um für jeden Knoten $v \in V$ eine Matrix A_v zu definieren, für welche im Weiteren sämtliche risikoverbundenen Kosten bewertet werden sollen. Diese Matrix speichert die Auftragsdaten, indem es sämtliche Quelle-Senke-Beziehungen und Transportquantitäten sämtlicher logistischer Prozesse, welche über den Knoten $v \in V$ laufen, enthält. Dies bedeutet insbesondere, dass nur ein Bruchteil aller Aufträge in jeder knotenspezifischen Matrix gespeichert wird und somit ein expliziter Auftrag üblicherweise in mehreren solcher Matrizen gespeichert wird. Wenn die Menge $O_v = \{(v_1, w_1), \dots, (v_n, w_n)\}$ alle Quelle-Senke-Beziehungen aller Aufträge, die via Knoten v geroutet wurden, enthält, so lässt sich die Matrix A_v elementweise wie folgt definieren:

$$(a_v)_{i,j}) = \begin{cases} q_{i,j}, \text{falls } (v_i, w_j) \in O_v \\ 0, \text{sonst} \end{cases}$$

Hierbei ist $q_{i,j} = q(v_i, w_j)$ die Transportmenge, die von v_i nach w_j transportiert werden muss.

4.3.4 Problemdefinition und Lösung

Um ein bestimmtes Risikoereignis für einen bestimmten logistischen Infrastrukturpunkt $v \in V$ zu bewerten, werden erneut zunächst die Kosten berechnet, die entstehen, wenn alle

Aufträge der Menge O_v unter „Normalbedingungen“ durchgeführt werden. Diese Kosten können aufgrund der bekannten Routings, Transportmengen und Wegekosten leicht berechnet werden.

Anschließend können die Teile des Netzwerkes identifiziert werden, die durch die Risikorealisierung beeinträchtigt wurden. Ohne Einschränkung der Allgemeinheit seien ausschließlich logistische Punkte (und keine Verbindungen) beeinträchtig. Die Teilmenge aller beeinträchtigten logistischen Punkte werde im Folgenden mit $R \subseteq V$ bezeichnet. Insbesondere bedeutet dies, dass das Gesamtnetzwerk nach der Risikorealisierung dem induzierten Subgraphen von $V \backslash R$ entspricht, also $\hat{G} \coloneqq G[V \backslash R] = (\hat{V}, \hat{E})$, mit $\hat{V} = V \backslash R$ und $\hat{E} = \{e = (v, w) \in E \mid v, w \in \hat{V}\}$. Die Gesamtkosten zur Erfüllung aller Aufträge im post-Risiko-Netzwerk können dann berechnet werden, indem die Kosten der kürzesten Wege aller Aufträge im post-Risiko-Netzwerk berechnet werden.

Abschließend können die Gesamtkosten vor und nach der Realisierung des Risikos verglichen und diese Differenz als Bewertung des Risikos interpretiert werden.

Ohne Beschränkung der Allgemeinheit wird im Folgenden ein Risiko untersucht, welches ausschließlich einen logistischen Punkt v^* beeinträchtigt. Ferner sei angenommen, erneut ohne Beschränkung der Allgemeinheit, dass dieser logistische Punkt durch die Risikorealisierung vollständig zerstört wird. Um die Gesamtkosten aller logistischen Aktivitäten im Netzwerk vor und nach der Risikorealisierung zu vergleichen, müssen lediglich die Gesamtkosten aller Aktivitäten verglichen werden, die durch den betroffenen Knoten v^* geroutet waren. Für jedes Quelle-Senke-Tupel (i, j) mit $(a_{v^*})_{i,j} > 0$ berechnen sich hierzu die Kosten $C_{i,j}$ dieses Auftrages, indem die Transportquantitäten mit jeder Kostenbewertung multipliziert werden und die so gewonnen Gesamttransportkosten pro Kante aufsummiert werden. Somit können die Gesamtkosten aller logistischen Aktivitäten, die durch v^* geroutet waren, im intakten Netzwerk wie folgt berechnet werden:

$$C_{v^*}^{\text{pre}} = \sum_{(i,j):(a_{v^*})_{i,j}>0} C_{i,j}$$

Um eine Risikobewertung für das Risiko “Komplettausfall von v^*“ berechnen zu können, müssen außerdem die Gesamtkosten aller über v^* gerouteten Aufträge im post-Risiko-Netzwerk berechnet werden. Hierzu werden alle logistischen Aktivitäten, die ursprünglich über den nun defekten logistischen Punkt v^* geroutet waren, neu geroutet, indem für alle (i, j) mit $(a_{v^*})_{i,j} > 0$ der kürzeste Weg von v_i nach w_j im defekten Netzwerk $\hat{G}$ berechnet wird. Durch aufsummieren der logistischen Kosten aller benutzten Kanten, multipliziert mit den Transportquantitäten $(a_{v^*})_{i,j}$, ergeben sich die Gesamtkosten der Erfüllung dieses Auftrages $\hat{C}_{i,j}$. Die Gesamtkosten aller logistischen Aktivitäten, die über den Knoten v^* geroutet waren, im post-Risiko-Netzwerk ergeben sich daher zu:

$$C_{v^*}^{\text{post}} = \sum_{(i,j):(a_{v^*})_{i,j}>0} \hat{C}_{i,j}$$

Abschließend kann nun das Risiko mit der Differenz der beiden Gesamtkosten bewertet:

$$\Delta C_{v^*} = C_{v^*}^{\text{post}} - C_{v^*}^{\text{pre}}$$

4.4 Vergleich beider Ansätze und kritische Würdigung

Grundsätzlich versuchen beide Ansätze, dieselbe Frage zu beantworten: Wie kann ein potenzielles Risiko in einem logistischen Netzwerk quantitativ bewertet werden? In beiden Fällen werden, auf sehr unterschiedliche Weise, die Gesamtkosten vor und nach der Risikorealisierung miteinander verglichen. Die Differenz darf hierbei keineswegs als absoluter Kostenwert missverstanden werden, sondern soll vielmehr eine relative Vergleichbarkeit von mehreren potenziellen Risiken ermöglichen, also eine Abschätzung ermöglichen, ob es sich um ein „eher gravierendes“ oder ein „eher kleineres“ Risiko handelt. Kombiniert mit einer Abschätzung einer Häufigkeit oder einer Eintrittswahrscheinlichkeit ergibt sich so für Entscheidungsträger die Möglichkeit, ein logistisches Netzwerk, insbesondere die kritischen logistischen Infrastrukturen, explizit auf die schwerwiegendsten Risikoszenarien vorzubereiten. Eine solche Vorbereitung wird üblicherweise durch eine Erweiterung des Netzwerkes, etwa durch den Aufbau von Alternativen, realisiert. Um anschließend abzuschätzen inwiefern ein potenziell erweitertes Netzwerk weiterhin anfällig für Risiken ist, können selbstverständlich dieselben, zuvor vorgestellten, Verfahren verwendet werden.

Andererseits identifizieren beide Ansätze keine Risiken, schätzen die Eintrittswahrscheinlichkeiten von Risiken ab oder schlagen konkrete Erweiterungen vor. All diese Problemstellungen müssen isoliert, vor- oder nachgelagert, gelöst werden um die kritische logistische Infrastruktur optimal vorzubereiten.

Betrachtet man solche Verfahren im Hinblick auf seinen Nutzen zur Terrorabwehr, so ergibt sich neben dem Nutzen der Risikobewertung auch eine Abschreckung gegenüber potenziellen Angreifern. Schon durch die Illusion einer robusteren Vorbereitung auf Anschläge, welche etwa durch eine Veröffentlichung von Ergebnissen gegeben sein könnte, könnten potenzielle Angreifer andere, schlechter vorbereitete, Ziele ins Visier nehmen, da sie einen größeren Schaden für die Gesellschaft antizipieren.

Trotz der gemeinsamen Fragestellung, die beide Ansätze beantworten wollten, basieren die Ansätze auf unterschiedlichen Ausgangssituationen. Während der erste Ansatz Daten zur gesamten logistischen Infrastruktur, all seinen Nutzern und deren Transporten benötigt, versucht der zweite Ansatz, mit möglichst wenig Datenbedarf auszukommen, indem nur die explizit betroffenen Knoten näher untersucht werden. In diesem Sinne kann der erste Ansatz als ein eher volkswirtschaftlicher Ansatz verstanden werden, der vor allem von Infrastrukturbetreibern umsetzbar ist. Im Gegensatz hierzu kann der zweite Ansatz als ein unternehmerischer

Ansatz verstanden, den jeder Besitzer (mindestens) eines eigenen logistischen Punktes selbstständig verfolgen kann, ohne auf „Fremddaten“ angewiesen zu sein. Dennoch ist es beim zweiten Ansatz sinnvoll, ihn aus der Perspektive einer übergeordneten Institution zu verfolgen.

Unterscheidet man verschiedene Anwendungsgebiete so ergeben sich, folgerichtig, sehr unterschiedliche Stärken und Schwächen der beiden Ansätze. Während der „volkswirtschaftliche“ Ansatz sich nahezu ausschließlich auf Risikoszenarien anwenden lässt, in denen die Infrastruktur für einen langen Zeitraum beeinträchtigt ist, so kann der „unternehmerische Ansatz“ auch gut auf kurzzeitige Störungen und Defekte angewandt werden. Der Hauptgrund hierzu ist, dass der erste Ansatz den global optimalen Zustand aller Verkehrsflüsse innerhalb eines Netzwerkes, vor und nach der Risikorealisierung, bewertet. Unmittelbar nach der Risikorealisierung wird sich jedoch ein neues globales Optimum nicht absehbar einstellen, da zunächst alle Akteure kurzfristig versuchen mit der neuen Situation zu arbeiten. Folgerichtig wird sich ein neues, globales Optimum nur sehr langsam einpendeln. Da der zweite Ansatz ausschließlich aktuelle (etwa tagesaktuelle) Aufträge betrachtet, erlaubt es eine wesentlich schnellere Adaption an eine neue Gesamtsituation. Langfristig können bei diesem Ansatz neue Aufträge anschließend direkt optimal durch das post-Risiko-Netzwerk geroutet werden.

Selbst wenn der zweite Ansatz auf einzelne Infrastrukturelemente (wie zum Beispiel einen Hafen) fokussiert, dient er nicht primär dem Hafenbetreiber zur Entscheidungsunterstützung, sondern vielmehr einem übergeordneten Entscheidungsträger, beispielsweise einer Landesbehörde. Um diesen Punkt zu verdeutlichen, soll ein einfaches Beispiel betrachtet werden: Wenn der Hafen Hanau aufgrund eines realisierten Risikos temporär nicht genutzt werden kann, werden die logistischen Flüsse – soweit möglich – auf andere Infrastrukturelemente ausweichen (bzw. umgeleitet werden), zum Beispiel auf den Hafen Frankfurt. Abgesehen von Kosten für die Wiederherstellung der Einsatzfähigkeit bedeutet das Risiko für den Hafen Hanau einen Umsatzverlust in Höhe von 100 % für den Zeitraum der Nichtnutzung. Auf der anderen Seite würde der Umsatz des Hafens Frankfurt aufgrund der zusätzlich abgewickelten logistischen Prozesse deutlich steigen; damit ist die Realisierung des Risikos in Hanau eine wesentliche Chance für den Hafen Frankfurt. Die Bewertung der Auswirkungen für beide Häfen ist trivial und von geringem Wert. Ein übergeordneter Entscheidungsträger auf Landesebene dagegen kann für sämtliche Infrastrukturelemente (in diesem Beispiel für alle Häfen) die Folgen einer Risikorealisation „durchspielen“ und damit für jedes mögliche Szenario die (Gesamt-) Kosten als unmittelbare Konsequenzen des realisierten Risikos ermitteln. Auf Basis der Szenarien und bewerteten Risiken lassen sich Prioritäten ermitteln und Risikosteuerungsmaßnahmen gemäß der Priorisierungen gezielt umsetzen.

5 Fazit und Ausblick

5.1 Wesentliche Projektergebnisse

Kritische Infrastrukturen sind bereits seit Jahren ein relevantes Thema in der Sicherheitsforschung. Häufig bezogen sich bisherige Forschungsaktivitäten aber auf Informations- und Kommunikationsinfrastrukturen oder auf energiebezogene Infrastrukturen. Auch der Bereich Verkehr wurde bereits untersucht. Die Logistik, die einen engen Bezug zum Thema Verkehr aufweist, war bisher jedoch von einer expliziten Berücksichtigung in der Sicherheitsforschung ausgenommen. Dies änderte sich durch unterschiedliche Entwicklungen in der jüngeren Vergangenheit, bei denen die logistische Infrastruktur erheblich beeinträchtigt wurde. Hierzu zählen beispielsweise Naturkatastrophen, aber auch terroristische Aktionen. Die Logistik als Versorgungssystem ist jedoch ein wesentliches Rückgrat einer Volkswirtschaft; dies gilt vor allem für hochentwickelte Volkswirtschaften wie auch Deutschland. Dementsprechend gravierend können die Auswirkungen sein, wenn die logistische Infrastruktur durch realisierte Risiken beeinträchtigt wird.

Der Fokus des vorliegenden Projekts dient damit dazu, das Risikomanagement für kritische Infrastrukturen in der Logistik zu professionalisieren, das heißt das Risikomanagement zu unterstützen, zu fördern und zu verbessern.

Wichtig für eine derartige Professionalisierung des Risikomanagements ist zunächst, die Risiken (oder Arten von Risiken) zu kennen, die für kritische Infrastrukturen in der Logistik relevant sein können. Diese wurden anhand einer PESTLE-Analyse transparent gemacht. Auch wenn die anhand der PESTLE-Analyse beispielhaft aufgeführten Risiken nicht explizit dazu beitragen, das Risikomanagement zu professionalisieren, sind sie doch für eine Sensibilisierung von Betreibern und Nutzern der logistischen Infrastrukturen relevant. Denn erst wenn ein möglichst umfassendes Bild der Risiken existiert, wird häufig die Notwendigkeit für ein Risikomanagement erkannt.

Die erste Phase eines effektiven Risikomanagements ist die Risikoidentifikation. Damit verbunden werden häufig (je nach Abgrenzung der einzelnen Phasen) die Risikoanalyse sowie die Risikobewertung. Zusammengefasst werden diese Phasen auch als Risikoabschätzung bezeichnet. Die Risikoabschätzung ist für das Risikomanagement von eminenter Bedeutung. Einfach gesagt gilt für das Risikomanagement der Satz: „Garbage in – garbage out.“ Mit anderen Worten: Die Qualität der Ergebnisse aus der Risikoabschätzung ist für die Handhabung der Risiken (die Risikosteuerung) wesentlich. Wenn bei der Risikoabschätzung – zum Beispiel aufgrund einer schwachen methodischen Fundierung, zu oberflächlicher Betrachtung oder anderen Gründen – Fehler gemacht werden, wirken sich diese Fehler unweigerlich auf die Priorisierung von Risiken sowie die Entwicklung und Anwendung von risikopolitischen Maßnahmen aus. Risiken, deren Bedeutung unterschätzt wird oder die gar „übersehen“ wer-

den (das heißt, die bei der Identifizierung nicht erkannt werden), können zu gravierenden Folgeschäden führen.

Aus diesem Grund ist es von besonderer Bedeutung, den „Werkzeugkoffer“ für Risikoidentifikation, -analyse und -bewertung zu kennen und zielgerichtet einsetzen zu können. Das „Handwerkzeug“ sind die entsprechenden Methoden. Im Rahmen des Forschungsvorhabens wurden diese Methoden strukturiert (quasi in der Werkzeugkiste in unterschiedliche Fächer einsortiert) dargestellt (eine Art Bedienungsanleitung für die jeweiligen Werkzeuge) und bewertet. Die Darstellung zielte auf den Einsatzzweck und die Vorgehensweise bei der Anwendung der Methode. Die Bewertung berücksichtigte unter anderem den zeitlichen sowie den personellen Aufwand für den Einsatz, aber auch Aspekte wie die Art der benötigten Input- sowie der erzeugten Output-Daten. Letztendlich wurde eine Abschlussbewertung für das Einsatzpotenzial jeder Methode getroffen.

Mit diesen Ergebnissen haben Entscheidungsträger eine Übersicht, anhand derer sie für den jeweiligen spezifischen Kontext die richtige(n) Methode(n) auswählen können, das heißt diejenige(n) Methode(n), die sich unter Kosten- und Zeitkriterien sowie des Untersuchungsgegenstandes (zum Beispiel der Art der logistischen Infrastruktur) am sinnvollsten einsetzen lassen.

Daneben wurden im Rahmen des Forschungsvorhabens auch zwei quantitative Ansätze entwickelt, wie Risiken in Netzwerken bewertet werden können. Diese Ansätze, die auf den Grundlagen des Operations Research aufbauen, ermöglichen es Entscheidungsträgern, anhand der Auswirkungen von Risiken auf logistische Prozessketten die „Kosten“ eines Risikos zu ermitteln. Mit diesen Bewertungsinformationen lassen sich Risiken – und dadurch auch die damit verbundenen risikopolitischen Maßnahmen – priorisieren.

Mit diesen Ergebnissen liefert das Projekt konkrete Ansatzpunkte, die zu einer Professionalisierung des Risikomanagements für kritische Infrastrukturen in der Logistik beitragen können.

5.2 Erfolgsfaktoren für ein effektives Risikomanagement kritischer Infrastrukturen in der Logistik

Ein wesentlicher Grundstein für ein effektives Risikomanagement ist der Einsatz von Methoden zur Risikoidentifikation, -analyse und -bewertung. Aus empirischen – oftmals branchenspezifischen – Erhebungen ist bekannt, dass der Reifegrad des Risikomanagements oft noch niedrig ist. Das heißt beispielsweise, dass Risikomanagement als rückwärtsgerichtete „Risikobuchhaltung“ verstanden wird (bei der die „Entdeckung“ neuer Risiken praktisch nur durch die Risikorealisierung erfolgt) und dass ein Methodeneinsatz bei der Risikoabschätzung nahezu nicht erfolgt. In der Logistikbranche dominieren als Methoden Brainstorming und Check-

listen; viele andere Methoden sind jedoch entweder nicht bekannt oder werden nicht eingesetzt.[182]

Ob das Risikomanagement für kritische Infrastrukturen in der Logistik (vor allem auch der Methodeneinsatz zur Identifikation, Analyse und Bewertung von Risiken) einen höheren Reifegrad aufweist, ist bislang unklar. Erste Gespräche, die allerdings nicht repräsentativ sind und daher keine Verallgemeinerung zulassen, gaben jedoch keinen Anlass zur Hoffnung auf ein professionelles Risikomanagement. Diese Thematik wird ab 2017 in einem nachfolgenden Projekt („BARM-KIL - Best-Practice-Ansätze im Risikomanagement für kritische Infrastrukturen in der Logistik“) untersucht.

Wichtig für ein effektives Risikomanagement sind hinsichtlich des Methodeneinsatzes vor allem drei Aspekte:

- Auf der einen Seite muss das Wissen über den „Werkzeugkoffer“ des Risikomanagers, das heißt über die verfügbaren Methoden, vorhanden sein. Die Methoden müssen bekannt sein, ihre Anwendung (möglichst) geübt. Ein Risikomanager muss Anforderungen, Rahmenbedingungen sowie Stärken und Schwächen kennen. Erst mit diesem grundsätzlichen Know-how lässt sich die richtige Methode für den richtigen Einsatzzweck zielgerichtet auswählen. Die mögliche Diskrepanz zwischen Wunsch und Wirklichkeit lässt sich durch entsprechende Schulungsmaßnahmen deutlich reduzieren.
- Auf der anderen Seite müssen Institutionen (und zwar privatwirtschaftliche Unternehmen wie auch öffentliche Institutionen) stärker für die Notwendigkeit und die Sinnhaftigkeit des Risikomanagements sensibilisiert sein. Dass eine „Risikobuchhaltung“ als administrativer Aufwand angesehen wird, ist beinahe verständlich. Wichtig ist jedoch, die Bedeutung von Risiken für kritische Infrastrukturen in der Logistik für die jeweilige Institution klarzumachen sowie die daraus abgeleitete Notwendigkeit und Wirksamkeit, Risiken zu identifizieren, zu analysieren und zu bewerten, um dann geeignete risikopolitische Maßnahmen ergreifen zu können. Hier gilt es daher, eine stärkere Sensibilisierung der Institutionen für ein proaktives Risikomanagement zu erreichen.
- Unternehmen sollten erkennen, dass ein methodisch fundiertes Risikomanagement die Robustheit (beziehungsweise Resilienz) erhöht, da „Überraschungen“ reduziert werden und die Planbarkeit erhöht wird. Dies wiederum ist im Interesse der Kapitalgeber, der Arbeitnehmer, Lieferanten und Kunden.

[182] Vgl. Lohre, Huth, M. (2015), S. 311.

Literatur- und Quellenverzeichnis

107th Congress (2001). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act). Act. H. R. 3162

Al Qaeda (2001). Declaration of Jihad. Veröffentlichung des US Department of Justice. bereitgestellt durch Federation of American Scientists. Online verfügbar: http://fas.org/irp/world/para/aqmanual.pdf (Zugriff am 28.10.2016).

Adar, E., Wuchner, A. (2005). Risk management for critical infrastructure protection (CIP) challenges, best practices & tools. First IEEE International Workshop on Critical Infrastructure Protection. S. 8 ff.

Alderson, D.L., Brown, G.G., Carlyle, W.M., Wood, R.K. (2011). Solving Defender-Attacker-Defender Models for Infrastructure Defense. S. 28-49 in: Wood K, Dell R (eds). Operations Research, Computing and Homeland Defense. Hanover, MD: Institute for Operations Research and the Management Sciences

Allgemeine Zeitung (2016). Nach BASF-Unglück: Betroffener Hafen wieder freigegeben. Online verfügbar: https://www.az-online.de/deutschland/nach-basf-unglueck-betroffener-hafen-wieder-freigegeben-zr-6934829.html (Zugriff: 05.11.2016).

Andrews, J. D., Dunnett, S. J. (2000). Event-tree analysis using binary decision diagrams. IEEE Transactions on Reliability. Vol. 49 (2). S. 230-238.

Arvanitoyannis, I., Varzakas, T. (2008). Application of ISO 22000 and Failure Mode and Effect Analysis (FMEA) for Industrial Processing of Salmon: A Case Study. Critical Reviews in Food Science and Nutrition. No. 48. S.411–429.

Asbarez (2016). Artsakh Determined to Open Stepanakert Airport for 'People's Right to Free Movement'. Online verfügbar: http://asbarez.com/141373/artsakh-determined-to-open-stepanakert-airport-for-peoples-right-to-free-movement/ (Zugriff: 31.10.2016)

Avritzer, A., Di Giandomenico, F., Remke, A., Riedl, M. (2012). Assessing dependability and resilience in critical infrastructures: challenges and opportunities. Resilience assessment and evaluation of computing systems. S. 41-63.

Ball, M. O., Golden, B., L., Vohra, R. V. (1989). Finding the Most Vital Arcs in a Network. Operations Research Letters. Vol. 8 (2). S. 73-76.

Baumann, S., Erber, I., Gattringer, M. (2016). Selection of risk identification instruments. ACRN Oxford Journal of Finance and Risk Perspectives. Vol. 5 (2). S. 27-41.

BCM News (2010). Kochbuch für eine Business Impact Analyse". Online verfügbar: http://www.bcm-news.de/wp-content/uploads/kochbuch-fuer-eine-bia.pdf (Zugriff: 10.02.2016)

Behrends, E. (2000). Introduction to Markov chains (Vol. 228). Braunschweig/Wiesbaden: Vieweg.

Benford, F. (1938). The Law of Anomalous Numbers. Proceedings of the American Philosophical Society. Philadelphia. S. 551–572.

Berle, Ø., Asbjørnslett, B. E., Rice, J. B. (2011). Formal Vulnerability Assessment of a maritime transportation system. Reliability Engineering & System Safety. Vol. 96 (6). S. 696–705.

Bhaskar, V., Lallement, P. (2010). Modeling a supply chain using a network of queues. Applied Mathematical Modelling. Vol. 34 (8). S. 2074–2088.

Boin, A., McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. Journal of Contingencies and Crisis Management. Vol. 15 (1). S. 50-59.

Bojar, P. (2012). Application of FMEA method for assessment of risk in land transportation of hazardous materials. Journal of KONES Powertrain and Transport. Vol. 19 (3). S. 44

Bose, T. K. (2012). Application of Fishbone Analysis for Evaluating Supply Chain and Business Process - A Case Study on the St James Hospital. International Journal of Managing Value and Supply Chains. Vol. 3(2). S. 17-24.

Brown, G. G., Carlyle, W. M., Salmeron, J., Wood, K. (2005). Analyzing the vulnerability of critical infrastructure to attack and planning defenses. INFORMS Tutorials in Operations Research. Institute for Operations Research and the Management Sciences, Hanover, MD. S. 102-123

Brown, G. G., Carlyle, W. M., Salmerón, J., Wood, K. (2006). Defending Critical Infrastructure. Interfaces. Vol. 36 (6). S. 530–544.

Buhr, W. (2009), Infrastructure of the Market Economy. Volkswirtschaftliche Diskussionsbeiträge. Discussion Paper No. 132-09. Fachbereich Wirtschaftswissenschaften. Wirtschaftsinformatik und Wirtschaftsrecht. Universität Siegen.

Buffett, S. (2005). A Markov Model for Inventory Level Optimization in Supply-Chain Management. Advances in Artificial Intelligence. 18th Conference of the Canadian Society for Computational Studies of Intelligence. Victoria, Canada. Springer. Heidelberg.

Bumgarner, J., Borg, S. (2009). Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008. US-CCU Special Report.

Bundesamtes für Sicherheit in der Informationstechnik (2015). KRITIS-Sektorstudie Transport und Verkehr. Online verfügbar: http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_TuV.pdf?__blob=publicationFile (Zugriff am 28.10.2016).

Bundesministerium des Innern (2009). Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Online verfügbar: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf;jsessionid=F15594BE8C3E483D72DA07CB14FF2D3B.2_cid364?__blob=publicationFile (Zugriff am 28.10.2016).

Bundesministerium des Innern (2011). Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. Online verfügbar: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Leitfaden_Schutz-Kritis.pdf?__blob=publicationFile (Zugriff am 28.10.2016).

Bundesministerium für Verkehr und digitale Infrastruktur (2015). Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft – Schutz kritischer Infrastrukturen und verkehrsträgerübergreifende Gefahrenabwehr. Online verfügbar: http://www.bmvi.de/SharedDocs/DE/Anlage/Presse/baer_sicherheitsstrategie_15-01-2015.pdf?__blob=publicationFile (Zugriff am 28.10.2016).

Buzan, T., Buzan, B. (2002). Das Mind-Map-Buch. Die beste Methode zur Steigerung ihres geistigen Potentials. Moderne Verlagsgesellschaft. München.

Canale, S., Distefano, N., Leonardi, S. (2005). A risk assessment procedure for the safety management of airport infrastructures. III Convegno Internazionale SIIV (People, Land, Environment and Transport Infrastructures). Bari, Italy. S. 2-8.

Cardona, O. D. (2004). The need for rethinking the concepts of vulnerability and risk from a holistic perspective: a necessary review and criticism for effective risk management. Mapping vulnerability: Disasters, development and people. S. 17.

Chapman, C., Ward, S. (1997). Project Risk Management – Processes, Techniques and Insights. John Wiley & Sons. Chichester.

Choi, T. Y., Hong, Y., 2002. Unveiling the structure of supply networks: case studies in Honda, Acura, and DaimlerChrysler. Journal of Operations Management. Vol. 20 (5), S. 469-493.

Church R. L., Scaparra, M. P. (2006). Protecting Critical Assets: The r-interdiction Median Problem with Fortification. Geographical Analysis. Vol. 39 (2). S. 129-146.

CIPedia. Wiki-Projekt des CIPRNet der Europäischen Union. Online verfügbar: www.cipedia.eu (Zugriff: 04.03.2017).

Clemens, P. L. (2002). Event tree analysis. JE Jacobs Sverdrup. Online verfügbar: http://kspt.icc.spbstu.ru/media/files/2011/course/depend/01_EventTree.pdf (Zugriff 12.03.2017)

CNBC (2013). Pirates Release Tanker and 26 Crew Seized Last Year. Online verfügbar: http://www.cnbc.com/id/100543040 (Zugriff: 26.10.2016).

CNN (2003). Ohio trucker joined al Qaida jihad. Online verfügbar: http://edition.cnn.com/2003/LAW/06/19/alqaeda.plea/ (Zugriff: 23.03.2017).

CNN (2013). Typhoon Haiyan: No medicine, little aid at Tacloban clinic. Online verfügbar: http://edition.cnn.com/2013/11/13/world/asia/typhoon-haiyan/ (Zugriff 05.11.2016).

CNN (2016). Brussels travel: Flights suspended, transit limited. Online verfügbar: http://edition.cnn.com/2016/03/22/europe/brussels-explosions-transport-flights-metro-suspended/ (Zugriff: 31.10.2016).

Collier, S., Lakoff, A. (2008). The vulnerability of vital systems: How ‘critical infrastructure’ became a security problem. The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation, S. 40-62.

Corley, H. W., Chang, H., (1974). Finding the n Most Vital Nodes in a Flow Network. Management Science. Vol 21 (3). S. 362-364.

Corley, H. W., and Sha, D. Y. (1982). Most Vital Links and Nodes in Weighted Networks. Operations Research Letters. Vol 1 (4). S. 157-160.

Cormican, K. J., Morton, D. P., Wood, R. K. (1998). Stochastic Network Interdiction. Operations Research. Vol. 46 (2). S. 184-197.

Cyprus Mail (2013). Bold plan to regenerate derelict Nicosia airport. Online verfügbar: http://cyprus-mail.com/2013/09/22/bold-plan-to-regenerate-derelict-nicosia-airport/ (Zugriff 31.10.2016).

Daily Mail (2014). Inside the ruins of Gaza’s airport. Online verfügbar: http://www.dailymail.co.uk/news/article-2730465/Inside-ruins-Gaza-s-airport-Photographs-transport-hub-named-honour-Yasser-Arafat-open-just-three-years-destroyed-neglect-war.html (Zugriff: 31.10.2016).

DB Schenker China (2015). Explosions in industrial area in Tianjin impacts port operations. Online verfügbar: http://www.dbschenker.com.cn/log-cn-en/news_media/news/9842348/explosion_in_tianjin.html (Zugriff: 05.11.2016).

De Souza, E., Ochoa, P.M. (1992). State space exploration in Markov models. Performance Evaluation Review. Vol. 20 (1). S. 152-166.

Deutsche-Verkehrszeitung (2012). Streik am Flughafen Frankfurt verschärft. Online verfügbar: http://www.dvz.de/rubriken/single-view/nachricht/streik-am-flughafen-frankfurt-verschaerft.html (Zugriff: 05.11.2016).

Die Welt (2002). Montblanc-Tunnel drei Jahre nach Großbrand wieder eröffnet. Online verfügbar: https://www.welt.de/print-welt/article378424/Montblanc-Tunnel-drei-Jahre-nach-Grossbrand-wieder-eroeffnet.html (Zugriff: 05.11.2016).

Die Welt (2015). Baumängel an der A643-Brücke - Zehntausende im Stau. Online verfügbar: https://www.welt.de/regionales/hessen/article137342084/Baumaengel-an-A643-Bruecke-Zehntausende-im-Stau.html (Zugriff: 05.11.2016).

Dudgeon, P. (2001). Breaking Out of the Box: The Biography of Edward de Bono. Headline. London, UK.

Dunjó, J., Fthenakis, V., Vílchez, J. A., Arnaldos, J. (2010). Hazard and operability (HAZOP) analysis. A literature review. Journal of hazardous materials. Vol. 173 (1). S. 19-32.

Evers, M. (2012). Participation in Flood risk Management – An introduction and recommendations for implementation. Karlstad, Sweden. Online verfügbar: http://www.diva-portal.org/smash/get/diva2:442763/fulltext01.pdf (Zugriff 09.03.2017).

Ezell, B. C., Farr, J. V., Wiese, I. (2000). Infrastructure risk analysis model. Journal of infrastructure systems. Vol. 6 (3). S. 114-117.

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., Veitch, B. (2011). Fault and event tree analyses for process systems risk analysis: uncertainty handling formulations. Risk Analysis. Vol. 31 (1). S. 86-107.

Ferdous, R., Khan, F., Sadiq, R., Amyotte P., Vetch, B. (2013). Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach. Process Safety and Environmental Protection. Vol. 91. S. 1-18.

Flick, U. (1995). Qualitative Forschung. Theorie, Methoden, Anwendung in Psychologie und Sozialwissenschaften. Rowohlt Taschenbuchverlag. Hamburg.

Flughafen Berlin (BER) Kosten (2017). Online verfügbar: https://www.flughafen-berlin-kosten.de/ (Zugriff 10.3.2017).

Frankfurter Allgemeine Zeitung (2016). Gewagte Prognosen. Online verfügbar: http://www.faz.net/aktuell/rhein-main/bilanz-zum-flughafen-kassel-calden-nach-3-jahren-14160787.html (Zugriff: 31.10.2016).

Fulkerson, D. R., Harding, G. C. (1977). Maximizing the Minimum Source-Sink Path Subject to a Budget Constraint. Mathematical Programming. Vol. 13 (1). S.116-118.

Giannopoulos, G., Filippini, R., Schimmer, M. (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. JRC Technical Notes.

Gjerde, O., Kjølle, G.H., Detlefsen, N. K., Brønmo, G. (2011). Risk and vulnerability analysis of power systems including extraordinary events. 2011 IEEE Trondheim PowerTech. S. 1-5.

Gleißner, W., Romeike, F. (2015). Grundlagen des Risikomanagements. in: Gleißner, W./Romeike, F. (Hrsg.): Praxishandbuch Risikomanagement: Konzepte – Methoden – Umsetzung. Erich Schmidt Verlag. Berlin 2015. S. 19-43.

Gleißner, W. (2017). Grundlagen des Risikomanagements – Mit fundierten Informationen zu besseren Entscheidungen. 3. Auflage. Vahlen Verlag. München.

Godfrey, P. C., Merrill, C. B., Hansen, J. M. (2009). The relationship between corporate social responsibility and shareholder value: An empirical test of the risk management hypothesis. Strategic management journal. Vol. 30 (4). S. 425-445.

Golden, B. (1977). A Problem in Network Interdiction. Naval Research Logistics Quarterly. Vol. 25 (4). S. 711-713.

Harris, T. E., Ross, F. S. (1955). Fundamentals of a method for evaluating rail net capacities (No. RM-1573). RAND CORP Santa Monica, USA.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security. Vol. 4 (2).

Higgins, J. M., Wiese, G. G. (1996). Innovationsmanagement. Kreativitätstechniken für den unternehmerischen Erfolg. Springer Verlag. Berlin.

Hoffmann, P. (2012). Innovative Supply Risk Management, in: Bogaschewsky, R. u.a. (Hrsg.). SupplyManagement Research – Aktuelle Forschungsergebnisse 2012. Wiesbaden. Springer Gabler. S. 79-104.

Holzmann, R., Jørgensen, S. (2001). Social risk management: A new conceptual framework for social protection, and beyond. International Tax and Public Finance. Vol. 8 (4). S. 529-556.

Holzmann, R., Sherburne-Benz, L., Tesliuc, E. (2003). Social risk management: The World Bank's approach to social protection in a globalizing world. Washington DC, USA: World Bank.

Hristova, A., Schlegel, R., Obermeier, S. (2014). Security Assessment Methodology for Industrial Control System Products. The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems. S. 264-269.

Huth, M., Romeike, F. (2015). Schutz kritischer Infrastrukturen und verkehrsträgerübergreifende Gefahrenabwehr. in: RISIKO MANAGER. Nr. 4. S. 10-13.

IBSE Telegramm 242 (2011). Strecke 3578 Weinheim (Bergstr)-Viernheim. S.2.

Industrie- und Handelskammer Wiesbaden (2015). IHK-Resolution zur Verkehrsinfrastruktur im Raum Mainz – Wiesbaden. Online verfügbar: https://www.ihk-wiesbaden.de/presse/journalisten/Pressemeldungen/IHK-Resolution-zur-Verkehrsinfrastruktur/2586458 (Zuggriff am 22.11.2016).

Ishikawa, K. (1986). Guide to Quality Control. Tokyo, Japan: Asian Productivity Organization.

Israeli, E., Wood, R. K. (2002). Shortest-Path Network Interdiction. Networks. Vol. 40 (2). S. 97-111.

Jackson, C. M. (2013). Estonian cyber policy after the 2007 attacks: Drivers of change and factors for success. New Voices In Public Policy, Vol. 7 (1).

Jochimsen, R. (1966). Theorie der Infrastruktur: Grundlagen der marktwirtschaftlichen Entwicklung. Mohr Siebeck Verlag.

Johnston, R. G. (2012). Physical vulnerability assessment. Critical Infrastructure Security – Assessment, Prevention, Detection, Response. WIT Press. Southampton,Boston. S. 21-36.

Kado, K., Horiuchi, T., Seki, T. (2003). Application of FMECA to Project Risk Identification Process. Journal of the Society of Project Management. Vol. 5 (2). S. 19-25.

Kahn, H., Wiener, A. J. (1967). The Year 2000: A Framework for Speculation on the Next Thirty-Three Years. MacMillan. New York, USA.

Kähler, W.-M. (2006). Statistische Datenanalyse: Verfahren verstehen und mit SPSS gekonnt einsetzen. 4. Auflage. Vieweg Verlag. Wiesbaden.

Kim E.S., Kim H.S. (2015), A reliability model of truck transportation using FMEA and FTA. Proceedings of the World Congress on Mechanical, Chemical, and Material Engineering. S. 256-3

Kim, Y., Choi, T. Y., Yan, T., Dooley, K. (2011). Structural investigation of supply networks: A social network analysis approach. Journal of Operations Management. Vol. 29 (3). S. 194-211.

Kjølle, G. H., Utne, I. B., Gjerde, O. (2012). Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety. Vol. 105. S. 80-89.

Kleiner, Y., Sadiq, R., & Rajani, B. (2006a). Modelling the deterioration of buried infrastructure as a fuzzy Markov process. Journal of Water Supply: Research and Technology-AQUA. Vol. 55 (2). S. 67-80.

Kleiner, Y., Rajani, B., & Sadiq, R. (2006b). Failure risk management of buried infrastructure using fuzzy-based techniques. Journal of Water Supply: Research and Technology-AQUA. Vol. 55 (2). S. 81-94.

König, E., Zedler, D. (Hrsg.) (1995). Bilanz qualitativer Forschung. Bd. 1: Grundlagen qualitativer Forschung; Bd. 2: Methoden. Deutscher Studien Verlag. Weinheim.

Koschade, S. (2006). A Social Network Analysis of Jemaah Islamiyah: The Applications to Counter-Terrorism and Intelligence. Studies in Conflict and Terrorism. Vol. 29 (6). S. 559-575.

Krebs, V. (2002). Mapping Networks of Terrorist Cells. Connections. Vol. 24 (3). S. 43-52.

Kuckartz, U. (Hrsg.) (2007). Qualitative Datenanalyse: computergestützt. methodische Hintergründe und Beispiele aus der Forschungspraxis. 2. Auflage. VS Verl. für Sozialwissenschaften. Wiesbaden.

Lawley, H.G. (1974). Operability Studies and Hazard Analysis. Chemical Engineering Progress. Vol. 70 (4). S. 45-56.

Lewis, S, Smith, K. (2010). Lessons Learned from Real World Application of the Bow-tie Method. Online verfügbar: http://www.risktec.co.uk/media/43525/bow-tie%20lessons%20learned%20-%20aiche.pdf (Zugriff 09.03.2017).

Lim, C., Smith, J. C. (2007). Algorithms for Discrete and Continuous Multicommodity Flow Network Interdiction Problems. IIE Transactions. Vol. 39 (1). S. 15-26.

Liu, H. L. (2012). Arbeitswissenschaftliches Modell zur nutzerorientierten Gestaltung technischer Produkte für Menschen mit krankheitsbedingten Einschränkungen am Beispiel von Sanitärprodukten. Dissertationsschrift. Online verfügbar: https://www.depositonce.tu-berlin.de/bitstream/11303/3579/1/Dokument_51.pdf (Zugriff 12.03.2017)

Logistik Heute (2015). GDL-Streik: Schäden in Millionenhöhe erwartet. Online verfügbar: http://www.logistik-heute.de/Logistik-News-Logistik-Nachrichten/Markt-News/12980/Gueterzuege-bleiben-noch-bis-Freitag-stehen-GDL-Streik-Schaeden-in-Millionen (Zugriff: 01.11.2016).

Lohre, D., Huth, M. (2015). Besonderheiten des Logistik-Risikomanagements bei Logistikdienstleistern. in: Huth, M./Romeike, F. (Hrsg., 2015): Risikomanagement in der Logistik: Konzepte - Instrumente - Anwendungsbeispiele. Springer Gabler. Wiesbaden. S. 301-314.

Lubore, S. H., Ratliff, H. D., Sicilia, G. T. (1971). Determining the Most Vital Link in a Flow Network. Naval Research Logistics Quarterly. Vol. 18 (4). S. 497-502.

Malik, K., Mittal, A. K., Gupta, S. K. (1989). The k Most Vital Arcs in the Shortest Path Problem. Operations Research Letters. Vol. 8 (4). S. 223–227.

McMasters, A. W., Mastin, T. M. (1970). Optimal Interdiction of a Supply Network. Naval Research Logistics Quarterly. Vol. 17 (3). S. 261-268.

Metropolis, N. C., Ulam, S. (1949). The Monte Carlo Method, Journal of the American Statistical Association. Vol. 44 (247). S. 335-341.

Mokhtari, K., Ren, J., Roberts, C., Wang, J. (2011). Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals. Journal of Hazardous Materials. Vol. 192 (2). S. 465-475.

Mokhtari, K., Ren, J., Roberts, C., Wang, J. (2012). Decision support framework for risk management on sea ports and terminals using fuzzy set theory and evidential reasoning approach. Expert Systems with Applications. Vol. 39 (5). S. 5087–5103.

Murray, A. T., Matisziw, T. C., Grubesic, T. H. (2007). Critical Network Infrastructure Analysis: Interdiction and System Flow. Journal of Geographical Systems. Vol. 9 (2). S. 103-117.

Newcomb, S. (1881). Note on the Frequency of the Use of different Digits in Natural Numbers. American journal of mathematics. Baltimore. S. 39–40.

New York Times (2014). Once Bustling, Syria's Fractured Railroad Is a Testament to Shattered Ambitions. Online verfügbar: http://www.nytimes.com/2014/05/26/world/middleeast/damascus-syria-hejaz-railway-station.html (Zugriff: 31.10.2016)

Oprach, M., Bovekamp, B. (2013). Hybrid Threats and Supply Chain Safety Management. in: M. Essig u.a. (Hrsg.): Supply Chain Safety Management: Security and Robustness in Logistics. Springer. Berlin/Heidelberg 2013. S. 89-100.

Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M. (2006). Critical infrastructure interdependency modeling: a survey of US and international research. Idaho National Laboratory. S. 25-27.

Penn, A. B. (2010). The Virgin Islands Climate Change Green Paper. Conservation and Fisheries Department and Ministry of Natural Resources and Labour.

Port Technology (2016). Empty Hanjin Containers congesting ports. Online verfügbar: https://www.porttechnology.org/news/empty_hanjin_containers_congesting_ports (Zugriff: 30.10.2016).

President's Commission on Critical Infrastructure Protection (1997). Critical Foundations – Protecting America's Infrastructures. Online verfügbar: https://fas.org/sgp/library/pccip.pdf (Zugriff 24.02.2017).

Putermann, M. L. (2005). Markov Decision Processes: Discrete Stochastic Dynamic Programming. Wiley & Sons. Hoboken.

Radeschütz, S. N. (2011). Business Impact Analysis - Konzept und Realisierung einer ganzheitlichen Geschäftsanalyse. Dissertation. Universität Stuttgart

Rail Turkey (2014). 10 Things to Know About Baku-Tbilisi-Kars Railway Project. Online verfügbar: https://railturkey.org/2014/10/20/baku-tblisi-kars-railway/ (Zugriff: 31.10.2016).

Ratliff, D. H, Sicilia, G. T., Lubore, S. H. (1975). Finding the n Most Vital Links in Flow Networks. Management Science. Vol. 21 (5). S. 531-539.

Renfro, R., Deckro. R. (2001). A Social Network Analysis of the Iranian Government. 69th MORS Symposium. S. 4.

Ritchey, T. (2003). Nuclear Facilities and Sabotage: Using Morphological Analysis as a Scenario and Strategy Development Laboratory. Online verfügbar: http://www.swemorph.com/pdf/inmm-r2.pdf (Zugriff 09.03.2017).

Ritchey, T. (2006). Modelling Multi-Hazard Disaster Reduction Strategies with Computer-Aided Morphological Analysis. Online verfügbar: http://swemorph.com/pdf/multi.pdf (Zugriff 09.03.2017).

Ritchey, T. (2009). Threat Analysis for the Transport of Radioactive Material. Online verfügbar: http://www.swemorph.com/pdf/ma-patram1.pdf (Zugriff 09.03.2017).

Ritchey, T. (2011a). Modeling Alternative Futures with General Morphological Analysis. World Future Review. Vol. 3 (1). S. 83-94.

Ritchey, T. (2011b). Wicked Problems – Social Messes: Decision Support Modelling with Morphological Analysis. Springer Verlag. Berlin, Heidelberg.

Rohrbach, B. (1969). Kreativ nach Regeln – Methode 635, eine neue Technik zum Lösen von Problemen. Absatzwirtschaft 12. Heft 19. S. 73-76.

Romeike, F., Hager, P. (2010). Gute Frage: Was ist ein „Random Walk“. Risk, Compliance & Audit. Vol. 6. S. 11-12.

Romeike, F., Stallinger, M. (2012). Bandbreiten- bzw. Korridorplanung – Integration von Risikomanagement und Unternehmensplanung. Risk, Compliance & Audit. Vol. 6. S. 12-21.

Romeike, F., Hager, P. (2013). Erfolgsfaktor Risiko-Management 3.0 – Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel. 3. Auflage. Springer Gabler. Wiesbaden.

Romeike, F., Spitzner, J. (2013). Von Szenarioanalyse bis Wargaming – Betriebswirtschaftliche Simulationen im Praxiseinsatz. Wiley Verlag. Weinheim.

Romeike, F., Spitzner, J. (2015). Einsatz von Simulationsmethoden im Logistik-Risikomanagement. Risikomanagement in der Logistik. Springer/Gabler Verlag. Wiesbaden. S. 127-158.

Romeike, F., Eicher, A. (2017). Risikomanagement (Studienwissen kompakt). Springer Verlag. Wiesbaden.

Rooney, J.J., Vanden Heuvel, L.N. (2004). Root Cause Analysis For Beginners. Quality progress. Vol 37 (7). S. 45-56.

Rossing, N.L. (2010). A functional HAZOP Methodology. Computers and Chemical Engineering. Vol. 34. S. 244–253.

RSSB (2009). Understanding human factors and developing risk reduction solutions for pedestrian crossings at railway stations. Online verfügbar: https://www.rssb.co.uk/library/research-development-and-innovation/research-brief-T730.pdf (Zugriff am 08.02.2017)

Ruhm, K. H. (2004). Cause and Effect Diagram. Internet Portal "Measurement Science and Technology". Online verfügbar: www.mmm.ethz.ch/dok01/d0000538.pdf (Zugriff 11.03.2017).

Ruijter, A. de, Guldenmund, F. (2016). The bowtie method: A review. Safety Science. Vol. 88. S. 211-218.

Sääskilahti, J., Särelä, M. (2010). Risk Analysis of Host Identity Protocol – Using Risk Identification Method Based on Value Chain Dynamics Toolkit. ECSA '10 – Proceedings of the Fourth European Conference on Software Architecture. Copenhagen, Denmark. S. 213-220.

Saint-Marc, C., Capoccioni, C.P., Saussine, G., Chenier, D., Davoine, P.A., Villanova-Olivier, M. u.a. (2016). IDISFER, an Ontology to Model Extreme Floods-Related Processes. Conference Paper: World Congress on Railway Research. Mailand, Italy. Online verfügbar: https://www.researchgate.net/profile/Cecile_Saint-Marc/publication/308966999_IDISFER_an_Ontology_to_Model_Extreme_Floods-Related_Processes/links/57fb488208ae91deaa633c7f.pdf (Zugriff 09.03.2017).

Salmerón, J., Wood, K., Baldick, R. (2004). Analysis of Electric Grid Security under Terrorist Threat. IEEE Transactions on Power Systems. Vol. 19 (2). S. 905–912.

Salmerón, J., Wood, K., Baldick, R. (2009). Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids. IEEE Transactions on Power Systems. Vol. 24 (1). S. 96-104.

Sapori, E., Sciutto, M., Sciutto, G. (2014). A Quantitative Approach to Risk Management in Critical Infrastructures. Transportation Research Procedia, Vol. 3.. S. 740-749.

Sawaguchi, M. (2015). Research on the Efficacy of Creative Risk Management Approach based on Reverse Thinking. Procedia Engineering. Vol. 131. S. 577-589.

Scaparra, M. P., Church, R. L. (2008). A Bilevel Mixed-Integer Program for Critical Infrastructure Protection Planning. Computers and Operations Research. Vol. 35 (6). S. 1905-1923.

Schieg, M. (2007). Post-mortem analysis on the analysis and evaluation of risks in construction project management. Journal of Business Economics and Management. Vol. 8 (2). S. 145-153.

Schrijver, A. (2002). Combinatorial optimization: polyhedra and efficiency (24. Auflage). Springer Science & Business Media.

Scupin, R. (1997). The KJ Method: A Technique for Analyzing Data Derived from Japanese Ethnology. Human organization. Vol. 56 (2). S. 233-237.

Seifert, J. (2005). Cognitive map, Mnemo-Technik und Mind Mapping. Raumeindrücke mental verorten, Wissensstrukturen visualisieren, Vorstellungsräume zum Lernen nutzen. ALFA-FORUM. Zeitschrift für Alphabetisierung und Grundbildung. Vol. 60. S. 32–34.

Serfozo, R. (2009). Basics of Applied Stochastic Processes. Springer Verlag. Heidelberg.

Sherwin, M. D., Medal, H., Lapp, S. A. (2016). Proactive cost-effective identification and mitigation of supply delay risks in a low volume high value supply chain using fault-tree analysis. International Journal of Production Economics. Vol. 175. S. 153-163.

Snyder, L. V., Scaparra, M. P., Daskin, M. S., Church, R. L. (2006). Planning for Disruptions in Supply Chain Networks, Tutorials. In: Johnson, M.P., Norman, B., Secomandi, N. (Hrsg.). Operations Research: Models, Methods, and Applications for Innovative Decision Making. Institute for Operations Research and Management Science.

Sottilotta, C. E. (2013). Political risk: concepts, definitions. Challenge, Working Paper Series, LUISS School of Government. Rome, Italy.

Spang, K., Gerhard, M. (2016). Risikomanagement. Projektmanagement von Verkehrsinfrastrukturprojekten. Springer Vieweg. Berlin, Heidelberg. S. 419-453.

Stehen, J. (2003). Liste der Flugangriffe auf Frankfurt am Main im 2. Weltkrieg. Institut für Stadtgeschichte. Online verfügbar: http://www.ffmhist.de/ffm33-45/portal01/portal01.php?ziel=t_hm_lkluftangriffe (Zugriff am 31.10.2016).

Stock, J. (2017). United Nations Security Council open debate on the protection of critical infrastructure against terrorist attacks. Statement by Interpol. Online verfügbar: https://www.interpol.int/content/download/34261/450506/version/1/file/Statement%20by%20Secretary%20General%20to%20the%20UNSC.pdf (Zugriff: 24.02.2017).

Straker, D. (2010). Cause-Effect Diagram. Online verfügbar: http://syque.com/quality_tools/toolbook/cause-effect/cause-effect.htm (Zugriff 11.03.2017)

Südwest Presse (2016). Streik und Straßenblockaden legen Teile des Landes lahm. Online verfügbar: http://www.swp.de/ulm/nachrichten/politik/streik-und-strassenblockaden-legen-teile-des-landes-lahm-13020619.html (Zugriff: 05.11.2016).

The Economist (2010). War in the fifth domain. Online verfügbar: http://www.economist.com/node/16478792 (Zugriff: 03.03.2017).

The Wall Street Journal (2015). Nepal Earthquake Response Challenges Logistics Experts. Online verfügbar: http://www.wsj.com/articles/nepal-earthquake-response-challenges-logistics-experts-1430343036 (Zugriff: 05.11.2016).

Ukraine Today (2015). Cyborgs vs. Kremlin. http://cyborgs.uatoday.tv/ (Zugriff am 31.10.2016).

US PIRG Education Fund (2009). Private Roads, Public Costs. Online verfügbar: http://www.uspirg.org/sites/pirg/files/reports/Private-Roads-Public-Costs-Updated_1.pdf (Zugriff: 30.10.2016).

Vesely, W. E., Goldberg, F. F., Roberts, N. H., Haasl, D. F. (1981). Fault tree handbook (No. NUREG-0492). Nuclear Regulatory Commission Washington DC.

Waiblinger Kreiszeitung (2016). Nach Unfall: S4 bleibt monatelang gesperrt. Online verfügbar: http://www.zvw.de/inhalt.backnang-baggertransport-bleibt-an-eisenbahnbruecke-haengen.b0c78359-c7e9-45d9-99d3-9ecb000fd0a4.html (Zugriff: 05.11.2016).

Washburn, A., Wood, K. (1995). Two-Person Zero Sum Games for Network Interdiction. Operations Research. Vol. 43 (2). S. 243-251.

Watson, G. (2004). The Legacy Of Ishikawa. Quality Progress. Vol. 37 (4). S. 54-47.

Weber, P., Medina-Oliva, G., Simon, C., Iung, B. (2012). Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence. Vol. 25 (4). S. 671-682.

Weeks, A. D., Alia, G., Ononge, S., Mutungi, A., Otolorin, E. O., Mirembe, F. M. (2004). Introducing criteria based audit into Ugandan maternity units. Quality and Safety in Health Care. Vol. 13(1). S. 52-55.

Wikimedia (2008). Diagramm zur Benford-Verteilung. Online verfügbar: https://upload.wikimedia.org/wikipedia/de/8/84/Benford.svg (Zugriff 11.03.2017)

Wirtschaftswoche: (2016). GdF muss für Streikkosten aufkommen. Online verfügbar: http://www.wiwo.de/unternehmen/dienstleister/flughafenstreik-in-frankfurt-gdf-muss-fuer-streikkosten-aufkommen/13930392.html (Zugriff: 05.11.2016).

Wollmer, R. D. (1963). Some Methods for Determining the Most Vital Link in a Railway Network. RAND Memorandum, RM-3321-ISA.

Wollmer, R. D. (1964). Removing Arcs from a Network. Operations Research. Vol. 12 (6). S. 934-940.

Wollmer, R. D. (1968). Stochastic Sensitivity Analysis of Maximum Flow and Shortest Route Networks. Management Science. Vol. 14 (9). S. 551-564.

Wood, R. K. (1993). Deterministic Network Interdiction, Mathematical and Computer Modelling. Vol. 17 (2). S. 1-18.

World Maritime News (2015). Port of Aden Reopens for Business. Online verfügbar: http://worldmaritimenews.com/archives/169231/port-of-aden-reopens-for-business/ (Zugriff: 31.10.2016).

Zaman Alwsl (2016). U.S. air strikes destroy last Euphrates bridges in Deir Ez Zor. Online verfügbar: https://en.zamanalwsl.net/news/18649.html (Zugriff: 31.10.2016).

Zukunft Mobilität (2010). Eyjafjallajökull – Die Auswirkungen in Europa und der ganzen Welt. Online verfügbar: http://www.zukunft-mobilitaet.net/849/analyse/eyjafjallajoekull-fazit-schaden-flugverkehr-global/ (Zugriff: 23.02.2017).

Zwicky, F. (1966). Entdecken, Erfinden, Forschen im morphologischen Weltbild. Droemer/Knaur Verlag. München, Zürich.

Index

Bisherige Beiträge/Previous Papers

- No 18: Skauradszun, Dominik: Synthetische Sekundärinsolvenzverfahren und „echter“ Rechtsschutz, 2016.
- No 17: Huth, Michael/Lohre, Dirk: Risikomanagement in der Speditions- und Logistikbranche: Bestandsaufnahme zu Verbreitung und Reifegrad, 2015.
- No 16: Kreipl, Claudia: Compliance Management: Ein Konzept (auch) für kleine und mittelständige Unternehmen, 2015.
- No 15: Anja Thies; Stefanie Deinert; Michael Huth: Soziale Nachhaltigkeit bei Gewinnung und Bindung von Berufskraftfahrerinnen und -fahrern in der Logistikbranche, 2015.
- No 14: Kohler, Irina; Dehmel, Lisa: Wertschöpfung durch Unternehmenskommunikation – Evaluation der Erfolgswirkung durch Kommunikations-Controlling, 2015.
- No 13: Kohler, Irina; Ingerl, Carina: Beitrag des Controllings zur Umsetzung von Corporate Governance in Familienunternehmen, 2015.
- No 12: Slapnicar, Klaus W.: Wirtschaftsrecht à jour, 2015.
- No 11: Kohler, Irina: Fuldaer Supply Chain Management-Dialog: Trends und Herausforderungen im Supply Chain Controlling, 2014.
- No 10: Hillebrand, Rainer: Germany and the eurozone crisis: evidence for the country's "normalisation"?, 2014.
- No 9: Irina Kohler; Carina Ingerl: Unternehmensnachfolge und Family Business Governance im Mittelstand: Eine empirische Studie zur Nachfolgeproblematik in der Region Fulda, 2014.
- No 8: Neuert, J.: Business Management Strategies and Research Development, 2013.
- No 7: Huth, M.; Goele, H.: Potenzial der Ersatzteillogistik von produzierenden Unternehmen in der Region Berlin/Brandenburg, 2013.
- No 6: Kreipl, Claudia; Preißing, Dagmar; Huth, Michael; Lohre, Dirk; Och, Dominik; Neuert, Josef: Contributions to Applied International Business Management Research, 2013.
- No 5: Boelsche, Dorit: Performance measurement in humanitarian logistics, 2013.
- No 4: Conrad, Peter; Hummel, Thomas R.: Transitions: Individuelle Handhabung und Verarbeitungsformen institutionellen Wandels, 2012.
- No 3: Hummel, Thomas R.; Turovskaya, Maria S.: Project Studies in Specific Business, Legal and Economic Topics: video conference presentations, 2011.

- No 2: Hans, Lothar: Zur Konzeption eines Verwaltungscontrollings, 2011.
- No 1: nicht veröffentlicht/not published.

Alle Beiträge stehen auf der Homepage des Fachbereichs Wirtschaft als Download zur Verfügung: www.hs-fulda.de/wirtschaft.

The papers can be downloaded from the homepage of the Faculty of Business: www.hs-fulda.de/wirtschaft.