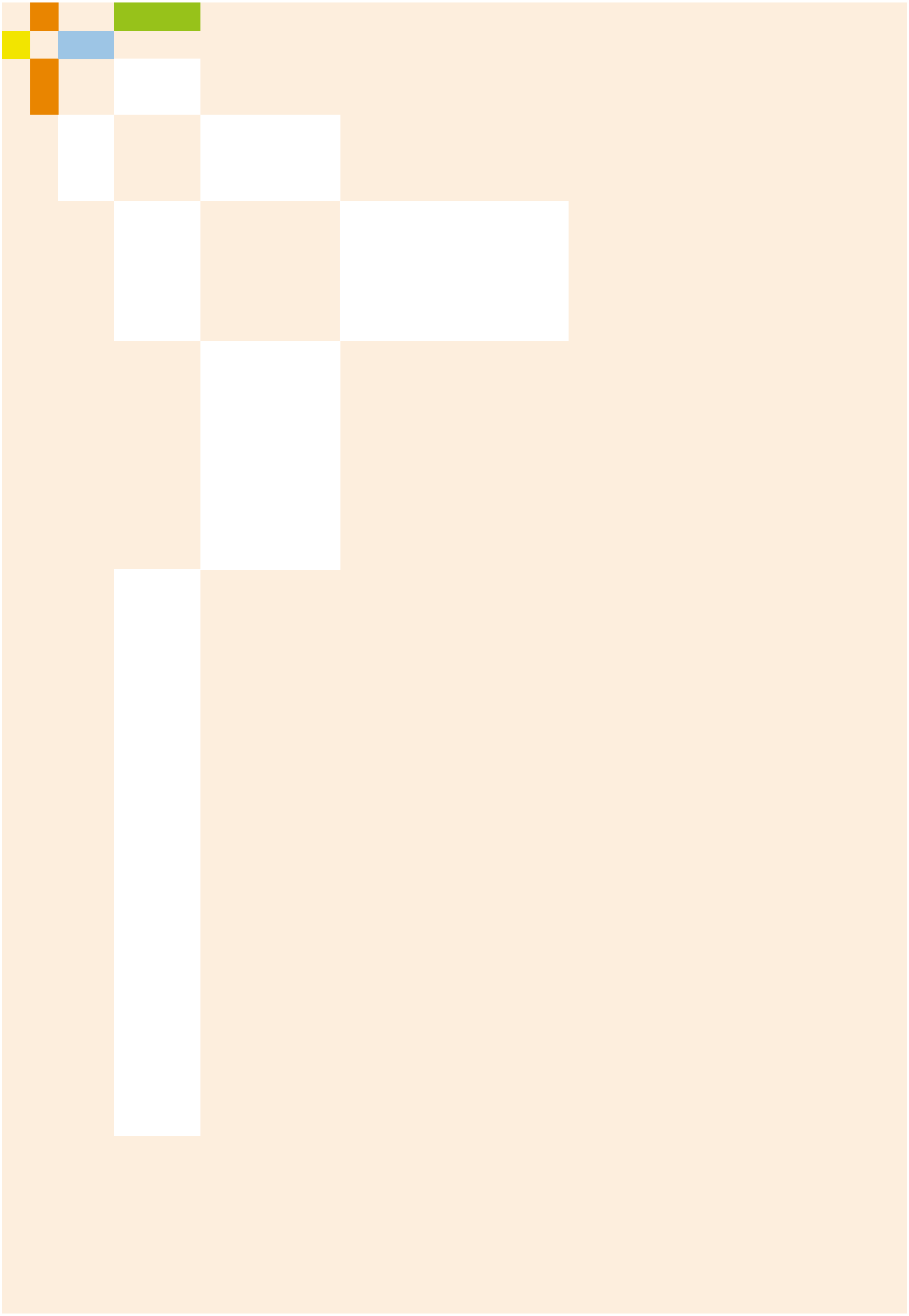
acatech DISKUSSION

Beiträge zu einer Systemtheorie Sicherheit

Jürgen Beyerer, Petra Winzer (Hrsg.)

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN



acatech DISKUSSION

Beiträge zu einer Systemtheorie Sicherheit

Jürgen Beyerer, Petra Winzer (Hrsg.)

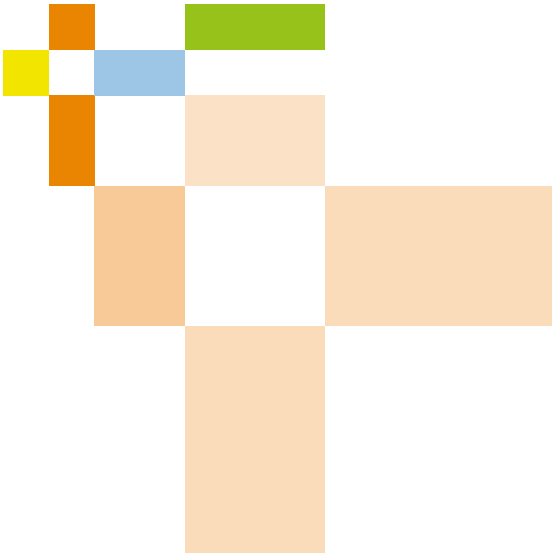
acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Die Reihe acatech DISKUSSION

Diese Reihe dokumentiert Ergebnisse aus Symposien, Arbeitskreisen, Workshops und weiteren Veranstaltungen der Deutschen Akademie der Technikwissenschaften. Die Bände dieser Reihe liegen in der inhaltlichen Verantwortung der jeweiligen Herausgeber und Autoren.

Alle bisher erschienenen acatech Publikationen stehen unter www.acatech.de/publikationen zur Verfügung.

Inhalt



1 Problemstellung und Zielsetzung einer „Systemtheorie Sicherheit“

Prof. Dr.-Ing. habil. Jürgen Beyerer
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
Lehrstuhl für Interaktive Echtzeitsysteme
am Institut für Anthropomatik und Robotik
Karlsruher Institut für Technologie KIT

Sicherheit ist ein fundamentales menschliches Grundbedürfnis, das in der Maslow'schen Bedürfnispyramide direkt auf die physiologischen Bedürfnisse folgt.[1] Sicherheit ist aber auch ein Grundbedürfnis für Unternehmen, Organisationen und unseren Staat.

Dabei ist der deutsche Begriff Sicherheit ziemlich vielschichtig. Er bezieht sich sowohl auf Gefahren durch natürliche Phänomene als auch durch andere Menschen und vom Menschen geschaffene Artefakte und Systeme. Solange es um Sicherheit geht, bei der keine absichtliche Gefährdung durch den Menschen im Spiel ist, spricht man im Englischen spezifischer als im Deutschen von *Safety*. Steckt menschliche Absicht und Intelligenz hinter einer Gefährdung, hat man in der englischen Sprache mit *Security* ebenfalls einen differenzierteren Begriff parat. Im weiteren Sinne bezieht der Begriff Sicherheit auch noch die Zuverlässigkeit (im Englischen: *Reliability*) mit ein. Um diese drei Teilaspekte der Sicherheit adäquat ausdrücken zu können, hat sich der Begriff der „Verlässlichkeit“ etabliert.[2]

Von besonderem gesellschaftlichem Interesse ist die Sicherheit soziotechnischer Systeme.[3] Soziotechnische Systeme sind komplex, und ihre Sicherheit involviert viele Disziplinen: Technik- und Naturwissenschaften, Rechts-, Geistes- und Sozialwissenschaften. Die Motivation für diese Veröffentlichung ist, dass es bislang keine durchgängige, allgemeine Theorie gibt, mit der sich Sicherheit derart komplexer Systeme behandeln lässt und die eine einheitliche, disziplinübergreifende Theorienbasis zur Verfügung stellt. Die Entwicklung einer solchen ganzheitlich angesetzten Theorie erfordert einen gründlichen Diskussionsprozess zwischen den betreffenden Disziplinen und stellt sowohl eine große Kommunikations- als auch eine Abstimmungsherausforderung dar. Die Verfasserinnen und Verfasser dieses Buchs sind der Überzeugung, dass es sich lohnt, eine solche übergreifende Theorie für die Sicherheit in Angriff zu nehmen, und haben sich entsprechend auf den Weg gemacht, erste einschlägige Beiträge zu erarbeiten.

In der Geschichte von Wissenschaft und Technik gibt es viele Beispiele für Gebiete, die erst nach Erscheinen einer grundlegenden Theorie eine rasante Entwicklung genommen haben. Ein schönes Exempel ist die Maxwell'sche Theorie des Elektromagnetismus:[4] Bis James Clerk Maxwell im Jahr 1865 die nach ihm benannten Maxwell-Gleichungen veröffentlichte, gab es eine Vielzahl noch nicht schlüssig miteinander verwobener Einzelerkenntnisse und Teiltheorien von Erfindern und Forschern wie André-Marie Ampère, Charles Augustin de Coulomb, Michael Faraday, Benjamin Franklin, Luigi Galvani, Carl Friedrich Gauß, Hans Christian Ørsted, Alessandro Volta, Wilhelm Eduard Weber und vielen anderen. Maxwell schaffte es schließlich mit seiner Theorie, alle bekannten Phänomene der klassischen Elektrodynamik mit einem kompakten Formelapparat zu beschreiben und sie damit genau zu berechnen. Der Siegeszug der Elektrotechnik wurde zweifellos besonders durch die Bereitstellung dieser grundlegenden Theorie beflügelt.

Ein weiteres Beispiel ist die Regelungstechnik und die dahinterstehende Kybernetik. Zu Beginn des 20. Jahrhunderts war die Regelungstechnik noch stark nach technologischen Ausprägungen gegliedert. Fliehkraftregler zur Drehzahleinhaltung rotierender Kraftmaschinen, Thermostate zur Temperaturregelung, elektrische Regler zur Konstanthaltung von Spannungen und Strömen und so weiter hatten überwiegend eigene Beschreibungsweisen und waren noch nicht in einer kohärenten Wissenschaft aufgegangen. Vor allem in den 40er Jahren des vergangenen Jahrhunderts wurde maßgeblich durch Norbert Wiener und Herrmann Schmidt eine vereinheitlichende Sicht auf die Regelungstechnik entwickelt.[5] Wiener begründete die übergeordnete Lehre der Kybernetik, welche die grundlegenden Gemeinsamkeiten von

1 | Vgl. Maslow 1943.
2 | Vgl. Bertsche et al. 2018.
3 | Unter einem soziotechnischen System versteht man eine organisierte Menge von Menschen und mit diesen verknüpfte Technologien, welche in einer bestimmten Weise strukturiert sind, um ein spezifisches Ergebnis zu produzieren; vgl. Wikipedia 2018.
4 | Vgl. Maxwell 1865.
5 | Vgl. Fasol et al. 2006.

Regelungsvorgängen in Natur und Technik beschreibt, abstrahiert und erklärt.[6] Auf Basis dieser fundamentalen theoretischen Grundlage entwickelte sich dann in der Folgezeit die Regelungstechnik zu einer sehr reichen wissenschaftlichen und technischen Disziplin.

Wie bereits zu Beginn erwähnt, gibt es für die Sicherheit soziotechnischer Systeme bis heute keine Theorie, die alle oben genannten Disziplinen umfasst und eine technologie- und anwendungsdomänenübergreifende Methodik zur Verfügung stellt, mit der eine umfassende formale Problembeschreibung gelingt und komplexe Sicherheitssysteme im soziotechnischen Kontext untersucht, entworfen und verbessert werden können. Die Sicherheitsaspekte Safety, Security und Zuverlässigkeit werden in der Regel unnötigerweise separat betrachtet, sodass mögliche Synergiepotenziale eines ganzheitlichen Ansatzes ungenutzt bleiben.

Um diese methodischen Defizite zu beseitigen, bedarf es einer mathematisch fundierten **Systemtheorie für die Sicherheit**, die von den Spezialitäten der Disziplinen und Technologien abstrahiert, gleichzeitig aber ausdrucksstark genug ist, um die Erfordernisse der involvierten Disziplinen ausreichend abzudecken. Eine solche Theorie muss bemüht sein, über die Disziplinen hinweg einheitliche Begriffe zu definieren und ein gemeinsames Verständnis zu schaffen. Außerdem muss sie auf einem geeigneten Abstraktionsniveau die grundlegenden Wirkungsmechanismen, die in Bezug auf Sicherheit in allen Systemen Geltung besitzen, herausarbeiten. Allerdings ist eine formale Deskription aller sicherheitsrelevanten Eigenschaften, Belange und Mechanismen nur ein erster unverzichtbarer Schritt. Um zielgerichtet und konstruktiv die Sicherheit soziotechnischer Systeme zu analysieren, zu planen, zu verbessern und schließlich zu optimieren, bedarf es auch geeigneter Maße und Metriken, um Sicherheit zu bewerten. Und es braucht einen Kalkül, der über die reine Beschreibung hinaus auch Schlussfolgerungen erlaubt, mit dem man also „rechnen" kann. Bei alledem muss aber auch auf der Beherrschung der Komplexität von aus einer Systemtheorie Sicherheit resultierenden Modellen und Algorithmen, die sich unter anderem aus der Komplexität realer soziotechnischer Systeme ergibt, ein besonderes Augenmerk liegen.

Eine Systemtheorie Sicherheit kann und muss selbstverständlich auf wohl etablierte Gebiete aufsetzen und sollte sich daraus wie aus einem Baukasten bedienen, wie zum Beispiel aus der Informatik, der Systemtheorie, der Spieltheorie, der statistischen Entscheidungstheorie, dem Systems Engineering und der Kybernetik.

Die Förderung der Sicherheitsforschung der letzten Jahre sowohl in Deutschland als auch durch die Europäische Union hat viele sehr gute Ergebnisse hervorgebracht. Sie war aber überwiegend szenario- und anwendungsgetrieben, setzte also gewissermaßen auf eine Bottom-up-Herangehensweise, um konkrete Sicherheitsherausforderungen durch die Forschung zu traktieren. Das Streben nach einer übergreifenden Systemtheorie Sicherheit ergänzt die Sicherheitsforschung um eine wissenschaftliche Top-down-Perspektive und kann zum Synergiestifter zwischen unterschiedlichen speziellen Vorhaben in der Sicherheitsforschung werden.

Im Rahmen des Themennetzwerks Sicherheit der Deutschen Akademie der Technikwissenschaften acatech wurde in den letzten drei Jahren intensiv mit dieser übergeordneten Fragestellung einer Systemtheorie für die Sicherheit gerungen. In einer losen Folge von Workshops wurden von einer interdisziplinär zusammengesetzten Gruppe von Wissenschaftlerinnen und Wissenschaftlern erste Beiträge zu einer generalisierenden Systemtheorie für die Sicherheit in einer konstruktiv kritischen Atmosphäre offenen wissenschaftlichen Dialogs entwickelt. Der vorliegende Band stellt diese frühen Ergebnisse nun der Fachgemeinde der Sicherheitsforschung und der interessierten Öffentlichkeit zur Diskussion.

Im Beitrag von Schlüter und Winzer wird die Rolle des Systems Engineering für die Bereitstellung eines disziplinübergreifenden Denkmodells und eines Vorgehenskonzepts herausgearbeitet.[7] Mit ihrem Generic-Systems-Engineering-Ansatz (GSE-Ansatz) stellen sie allgemein ein mögliches Fundament vor, auf das sich eine Systemtheorie Sicherheit abstützen könnte. An einem konkreten Beispiel werden die Vorteile von GSE dargelegt.

Der Beitrag von Schnieder und Schnieder widmet sich zwei grundlegenden Problemstellungen einer Systemtheorie Sicherheit.[8] Für eine durchgängige, eindeutige Begriffsbildung wird auf Basis der Linguistik ein neues formales Begriffskonzept eingeführt: mittels Klassendiagrammen der Unified Modeling Language (UML). Außerdem werden verschiedene kybernetische Ansätze, probabilistische Modelle und Petrinetze zur Formalisierung von dynamischen Prozessen vorgestellt, mit denen die logische, unsicherheitsbehaftete, temporale Entwicklung sicherheitsrelevanter Abläufe modelliert werden kann.

Im Abschnitt von Bertsche et al. wird der Sicherheitsbegriff weiter gefasst, indem über die Aspekte *Safety* und *Security* hinaus die Zuverlässigkeit von Komponenten, Teilsystemen und

6 | Vgl. Wiener 1948.
7 | Vgl. Schlüter/Winzer 2018.
8 | Vgl. Schnieder/Schnieder 2018.

Systemen miteinbezogen wird.[9] Das führt zum Begriff Verlässlichkeit, der aus Sicht einer sicherheitsbedürftigen Instanz, die hinsichtlich ihrer Gefährdung alle möglichen Ursachen der Beeinträchtigung ihrer Sicherheit gleichermaßen berücksichtigen möchte, eine ganzheitliche Konzeption darstellt.

Die deutsche Begriffsbildung bezüglich Verlässlichkeit geht auf den von J. Laprie geprägten Begriff der Dependability zurück.[10] Als wichtige wegbereitende Arbeiten zur Etablierung des Begriffs Verlässlichkeit in den Technikwissenschaften sind hier auch die weiter zurückliegenden Veröffentlichungen aus der Forschungsgruppe von Eckehard Schnieder[11] zu nennen.

Der Aufsatz von Beyerer und Geisler versucht mit Mitteln der statistischen Entscheidungstheorie und einer Bayes'schen Interpretation von Wahrscheinlichkeit als Grad des Dafürhaltens (Degree of Belief), eine vereinheitlichende Formalisierung Safety- und Security-bezogener Risiken zu schaffen.[12] Mit der Definition eines Rollenkonzepts (Schutzbedürftiger, Gefährder, Schützer) sowie dem Konzept von differenzierten Flanken der Verwundbarkeit wird zusammen mit einer zeitlichen Dynamisierung und einer örtlichen Diskretisierung über Graphen eine methodische Basis vorgeschlagen, mit der soziotechnische Systeme mittels Softwareagenten simuliert werden können.

Müller-Quade beleuchtet in seinem Beitrag die Sicht der Kryptographie auf eine Systemtheorie Sicherheit.[13] Aus dieser Warte spielen vor allem Gefährdungen durch intelligente Angreifer eine Rolle, für die eine probabilistische Modellierung ungeeignet erscheint.

Der Beitrag von Vieweg bringt eine erste juristische Perspektive in die Betrachtungen ein.[14] Neben der Klärung von Begriffen werden einige Risikoszenarien dargestellt und diskutiert. Das Zusammenwirken von Rechtssetzern, Verantwortungsträgern und Entscheidern sowie Behörden und Gerichten in Bezug auf die Sicherheit soziotechnischer Systeme wird als Prozess in einem Regelkreismodell beschrieben und erklärt.

In dem Aufsatz von Raabe wird eine zweite juristische Perspektive auf das Thema Systemtheorie Sicherheit eingenommen.[15] Dabei geht es unter anderem um Risiken für den Datenschutz und die Zusammenhänge mit dem IT-Sicherheitsrecht. Insbesondere wird untersucht, inwieweit abstrakte entscheidungstheoretische Ansätze zur Modellierung solcher Risiken geeignet sind.[16]

In den folgenden Kapiteln geht es dann um spezifische Anwendungen von Ansätzen der Systemtheorie Sicherheit auf konkrete Probleme. Dabei bleibt aber trotz des ausgeprägten Anwendungsbezugs der übergreifende Anspruch der vorliegenden Veröffentlichung im Fokus. Die Beiträge von Lichte und Wolf[17] sowie von Deutschmann und Milbredt[18] befassen sich mit der Sicherheit von Flughäfen. Bei Lichte und Wolf steht die Quantifizierung der Verwundbarkeit (Vulnerabilität) dieser kritischen Infrastrukturen im Vordergrund, wobei Angriffspfade hinsichtlich einer probabilistischen Bewertung der zeitlichen Entfaltung von Gefahren hinsichtlich ihres Risikos beurteilt werden. Eine Perspektive bezüglich der Bewertung der Leistungsfähigkeit von Sicherheitsmaßnahmen auf Basis geeigneter Key-Performance-Indikatoren nimmt der Aufsatz von Deutschmann und Milbredt ein.

Im Beitrag von Labudde wird ein systemtheoretischer Ansatz zur Ausbreitung krimineller Gefahren vorgestellt.[19] Urbane Strukturen werden als Graphen modelliert, auf denen dann ein Wechselwirkungsmodell zwischen Akteuren rechnerisch durchgespielt werden kann. Akteure werden als mobile Softwareagenten modelliert, die sich auf dem Graphen aufhalten und bewegen. Auf dieser Basis können räumliche/zeitliche Simulationen durchgeführt werden, mit denen die Ausbreitung von Kriminalität untersucht und ein Predictive Policing ermöglicht werden kann.

Der Aufsatz von Gleirscher betrachtet die Gefahrenerkennung und -behandlung in autonomen Maschinen.[20] Er stellt eine werkzeugbasierte Vorgehensweise zur Modellierung von Gefahrensituationen und zur Plausibilitäts- und Vollständigkeitsbewertung entsprechender Modelle am Beispiel des automatisierten Fahrens vor.

9 | Vgl. Bertsche et al. 2018.
10 | Vgl. Laprie 1992.
11 | Vgl. Schnieder 2003, Slovak et al. 2005, Schnieder/Slovak 2007 und Müller 2015.
12 | Vgl. Beyerer/Geisler 2018.
13 | Vgl. Müller-Quade 2018.
14 | Vgl. Vieweg 2018.
15 | Vgl. Raabe 2018.
16 | Vgl. Beyerer/Geisler 2018.
17 | Vgl. Lichte/Wolf 2018.
18 | Vgl. Deutschmann/Milbredt 2018.
19 | Vgl. Labudde 2018.
20 | Vgl. Gleirscher 2018.

Im Beitrag von Weyer et al. wird ein umfassendes System für die agentenbasierte Simulation soziotechnischer Systeme vorgestellt.[21] Der Ortsbezug wird durch einen Graphen dargestellt, der eine betrachtete Liegenschaft (Infrastruktur) diskretisiert und als Aktionsfeld für die Agenten dient. Das Simulationssystem SimCo ist dabei eine zunächst semantikfreie Plattform, die erst durch eine konkrete Ausprägung von Agententypen sowie die Anpassung des Graphen an eine spezifische Liegenschaft und Aufgabe spezielle Bedeutung erhält. Hiermit lassen sich Simulationen bezüglich verschiedener soziotechnischer Systeme durchführen, um insbesondere die Beeinflussbarkeit solcher Systeme durch unterschiedliche steuernde Vorgaben zu untersuchen.

Abschließend wenden Arens und Kühne systemtheoretische Ansätze auf Fragen rund um den Schutz und die Sicherheit von Offshore-Windparks an.[22] Da es sich bei solchen Anlagen um kritische Infrastrukturen handelt, müssen Sicherheit und Risiken systematisch untersucht und bewertet werden.

21 | Vgl. Weyer et al. 2018.
22 | Vgl. Arens/Kühne 2018.

Literatur

Arens/Kühne 2018
Arens, U./Kühne, U.: „Schutz und Sicherheit in Offshore-Windparks". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Bertsche et al. 2018
Bertsche, B./Beyerer, J./Goldschmidt, R./Jakobs, E. M./Renn, O./Schlüter, N./Winzer, P./Weyer, J.: „Integrative Theorie der Verlässlichkeit (iTV) für soziotechnische Systeme (STS)". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Beyerer/Geisler 2018
Beyerer, J./Geisler, J.: „Formaler Rahmen für eine einheitliche quantitative Beschreibung des Risikos bezüglich Safety und Security". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Deutschmann/Milbredt 2018
Deutschmann, A./Milbredt, O.: „Globale Bewertung des Sicherheitsniveaus von kritischen Infrastrukturen am Beispiel von Verkehrsflughäfen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Fasol et al. 2006
Fasol, K. H./Lauber, R./Mesch, F./Rake, H./Thoma, M./Töpfer, H.: „Great Names and the Early Days of Control in Germany". In: *Automatisierungstechnik*, 54: 9, München 2006, S. 462–472.

Gleirscher 2018
Gleirscher, M.: „Strukturen für die Gefahrenerkennung und -behandlung in autonomen Maschinen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Labudde 2018
Labudde, D.: „Sicherheit ist die Abwesenheit von Kriminalität – eine Hypothese". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Laprie 1992
Laprie J.-C. (Hrsg.): *Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese*, Wien: Springer-Verlag 1992.

Lichte/Wolf 2018
Lichte, D./Wolf, K.-D.: „Quantitative Analyse der Vulnerabilität am Beispiel Verkehrsflughafen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Maslow 1943
Maslow A.: „A Theory of Human Motivation". In: *Psychological Review*, 50: 4, 1943, S. 370–396.

Maxwell 1865
Maxwell, J. C.: „A Dynamical Theory of the Electromagnetic Field". In: *Royal Society Transactions*, 155, 1865, S. 459–512.

Müller 2015
Müller, J. R.: *Die formalisierte Terminologie der Verlässlichkeit technischer Systeme,* Springer-Verlag 2015.

Müller-Quade 2018
Müller-Quade, J.: „Das Verhältnis der Kryptographie zu einer Systemtheorie Sicherheit". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Raabe 2018
Raabe, O.: „Datenschutz- und IT-sicherheitsrechtliche Risikomodelle". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schlüter/Winzer 2018
Schlüter, N./Winzer, P.: „Bedeutung des Systems Engineering für die Entwicklung einer Systemtheorie der Sicherheit". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schnieder 2003
Schnieder, E.: „Beschreibung der Verlässlichkeit von Verkehrssystemen im Verfügbarkeits-Sicherheits-Diagramm". In: *Signal + Draht*, 95: 10, Oktober 2003, S. 6-9.

Schnieder/Schnieder 2018
Schnieder, E./Schnieder, L.: „Formalisierung von Begriffen der Sicherheit und Sicherheitsmetriken". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schnieder/Slovak 2007
Schnieder, E./ Slovak, R.: „Profund: Ein integrativer Ansatz zum Entwurf verlässlicher Automatisierungssysteme". In: *atp - Automatisierungstechnische Praxis*, 7, Juli 2007, S. 40-44.

Slovak et al. 2005
Slovak, R./ Wegele, S./ Schnieder, E.: „Ein Auswertungsverfahren für Verlässlichkeitsanalysen in der Bahntechnik". In: *Tagungsband 22: Tagung Technische Zuverlässigkeit* (TTZ - 22. Tagung Technische Zuverlässigkeit 07.-08.04.2005 Düsseldorf), Stuttgart: VDI Verlag 2005, S. 213-228.

Vieweg 2018
Vieweg, K.: „Sicherheit – Begriffe, Szenarien, Verantwortlichkeiten und Entscheidungsprozesse aus juristischer Sicht". In: Beyerer, J./ Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Wiener 1948
Wiener, N.: Cybernetics: *Or Control and Communication in the Animal and the Machine*, John Wiley & Sons Inc. 1948.

Wikipedia 2018
Wikipedia: *Soziotechnisches System*. URL: https://de.wikipedia.org/wiki/Soziotechnisches_System [Stand: 24.02.2018].

Weyer et al. 2018
Weyer, J./Adelt, F./Konrad, J./Hoffmann, S.: „Agentenbasierte Simulation des Risikomanagements soziotechnischer Systeme mit dem Simulator SimCo". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

2 Bedeutung des Systems Engineering für die Entwicklung einer Systemtheorie der Sicherheit

PD Dr.-Ing. habil. Nadine Schlüter
Prof. Dr.-Ing. habil. Petra Winzer
Fachgebiet Produktsicherheit und Qualitätswesen
Bergische Universität Wuppertal

1 Einleitung

Um die Sicherheit von Systemen jeglicher Art zu gewährleisten, müssen verschiedenste Wissenschaftsdisziplinen zusammenarbeiten. Dazu benötigen sie ein gemeinsames Denkmodell und ein Vorgehenskonzept. Das Systems Engineering (SE) könnte hierfür eine Basis sein. Doch dazu muss das SE zu seinem universellen Charakter zurückfinden – nur so kann das SE als Rückgrat der Sicherheit für Systeme fungieren.

Dementsprechend wird im Folgenden zunächst das Systems Engineering als Wissenschaftsdisziplin an sich betrachtet, bevor konkret auf seine Vielfalt aufgrund verschiedener fachdisziplinspezifischer Strömungen eingegangen wird. Anschließend wird der Generic-Systems-Engineering-Ansatz (GSE) vorgestellt, dessen Ziel es ist, die fachdisziplinspezifischen Strömungen wieder zu einem interdisziplinären Systems Engineering zusammenzuführen. Zum besseren Verständnis wird die Anwendung des GSE am Beispiel „Messung des Sicherheitsempfindens von Fahrgästen des öffentlichen Personennahverkehrs" erläutert. Abschließend erfolgt ein Fazit.

2 Systems Engineering als Wissenschaftsdisziplin

Die Systemtheorie kann als Grundlage zur Modellierung, Analyse sowie Synthese komplexer Strukturen angesehen werden.[1] Wird sie auf technische Systeme übertragen und mit deren Verbesserungsprozessen verbunden, wird von Systems Engineering (SE) gesprochen. Somit ist das SE Teil der allgemeinen Systemtheorie.[2] Das SE war und ist ein strukturiertes Vorgehen, um die Komplexität von Systemen zu beherrschen.

Das SE verbindet das Denken in Systemen, welches Bestandteil der Systemtheorie ist, mit einem Vorgehenskonzept, das der systematischen Problemlösung dient. Das SE lässt sich wie folgt auch durch seine eigene Begriffskombination definieren, das heißt durch die Begriffe „System" und „Engineering".

Ein System ist ein Artefakt, ein Abbild der Realität in einer sehr abstrakten Form. Es kann nicht ohne Weiteres als ein System erkannt werden, weil es ein gedankliches Konstrukt des Betrachters ist, der sich des systemischen Denkens bedient.[3] Das System ist etwas Zusammengesetztes beziehungsweise Zusammengehöriges, welches durch seine Funktion, sein Verhalten, seine Struktur beziehungsweise seinen Zustand bestimmt wird.[4,5] Handelt es sich um sehr komplexe Systeme, lassen sich diese wiederum in Teilsysteme zerlegen, wie es Weyer und Arens zur Gewährleistung der Sicherheit von soziotechnischen Systemen belegen.[6,7] Die kleinsten Bestandteile des Systems sind die Elemente und deren Wechselbeziehungen. Jedes System hat eine Systemgrenze sowie eine Systemumwelt und kann als Blackbox-System von seiner Umwelt abgegrenzt werden. Diese Systemdefinition ist sehr umfassend, universell und allgemein. Dennoch wird sie zunächst als ausreichend betrachtet, um den Begriff des SE zu erklären, wohl wissend, dass es in der Literatur zahlreiche Systemdefinitionen gibt.[8]

Um Systeme darstellen zu können, sind Modelle erforderlich. Sie sind die vereinfachte Abbildung eines geplanten oder real existierenden Objekts. Sinn und Zweck von Modellen ist es, einen komplexen Sachverhalt auf das Wesentliche abstrahiert

1 | Vgl. Brujin/Herder 2009.
2 | Vgl. Ropohl 2012.
3 | Vgl. Heinrich 2015.
4 | Vgl. Schnieder/Schnieder 2013.
5 | Vgl. Schnieder/Schnieder 2018.
6 | Vgl. Weyer et al. 2018.
7 | Vgl. Arens/Kühne 2018.
8 | Vgl. Luhmann 1980, Ludwig 2001, Hanenkamp 2004, Haberfellner et al. 2012, Schnieder/Schnieder 2013.

wiederzugeben.[9] Ihre Entwicklung erfolgt im SE problemlösungsorientiert, jedoch dienen in den jeweiligen Fachdisziplinen Modelle der Darstellung von Teilaspekten.[10] Da Systeme zunehmend von interdisziplinären Teams analysiert und gestaltet werden, wird die Forderung nach einem transdisziplinären Metamodell immer lauter.[11] Diese Modelle sollten mehrere Funktionen gleichzeitig erfüllen, das heißt Beschreibungs-, Erklärungs-, Prognose-, Gestaltungs- und/oder Optimierungsmodell sein.

Als „Engineering" wird eine Disziplin bezeichnet, welche sich Theorien beziehungsweise strukturierter Tools bedient, um Produkte zu entwickeln beziehungsweise zu verändern. Im Engineering werden die Teildisziplinen nach dem Betrachtungsgegenstand unterschieden. Ausdruck hierfür sind das Mechanical Engineering, das Electrical Engineering, das Software Engineering, das Manufacturing Engineering, das Safety Engineering und das Quality Engineering. Im Sinne der Systemtheorie wären diese Gegenstände bestimmte Systemarten, wie zum Beispiel das Softwaresystem beim Software Engineering. Dagegen entspricht die Sicherheit beim Safety Engineering oder die Qualität beim Quality Engineering spezifischen Aspekten, unter denen die verschiedenen Gegenstände beziehungsweise Systemarten, das heißt das Softwaresystem, aber auch der Antrieb oder die Fabrik, betrachtet werden können.

Werden nun die beiden Begriffe „System" und „Engineering" wieder zusammengefügt, entsteht somit eine Disziplin, die sich Methoden und strukturierter Tools bedient, um Systeme komplex zu gestalten. Nach der Definition des Incose (International Council on Systems Engineering) ist das SE eine Disziplin, die sich zum Ziel gesetzt hat, einen interdisziplinären Prozess zu schaffen, der schrittweise sicherstellt, dass Kunden- und Stakeholder-Anforderungen über den gesamten Lebenszyklus des Systems hinweg zufriedengestellt werden.[12]

Das SE kann die verschiedensten Wissenschaftsdisziplinen miteinander verbinden. Dies wird besonders gefördert durch eine Modifikation des SE, das Model-Based Systems Engineering (MBSE).[13] Das SE unterscheidet sich von den traditionellen, spezifischen Ingenieurdisziplinen dadurch, dass das komplexe System zunächst als Ganzes auch in der Interaktion mit seiner Umgebung, zum Beispiel dem Nutzer oder der Nutzerin des Systems, aber ebenso in der Wechselwirkung mit seinen Teilsystemen beziehungsweise Elementen fachdisziplinübergreifend betrachtet wird. Folglich besteht der Hauptzweck des SE darin, die Aktivitäten der am Problemlösungsprozess Beteiligten zu koordinieren und damit eine Brücke zwischen den Fachdisziplinen zu schlagen.[14]

Das SE wird aber auch als ein verallgemeinerter **Problemlösungsansatz** gesehen.[15] Bahill und Gissing beschreiben das SE als eine Möglichkeit für interdisziplinäre Teams, gemeinsam Probleme zu fixieren, einem System zuzuordnen und sie dann entsprechend zu lösen.

Für das Konzept der Lösungssuche empfiehlt das SE die Anwendung von Methoden, Verfahren und strukturierten Tools. Bezüglich deren Zusammenführung in ein prinzipielles, universelles Lösungskonzept gehen die Meinungen jedoch stark auseinander.[16]

Handelt es sich um komplexere Probleme, die es zu lösen gilt, empfiehlt das SE die Anwendung unterschiedlicher Grundprinzipien des systemischen Denkens und Handelns. Während Haberfellner beim Lösen von Problemen grundsätzlich das Denken vom Großen und Ganzen hin zum Detail fordert,[17] überlassen andere Autorinnen und Autoren das Vorgehen dem jeweiligen Anwendenden.[18]

Der SE-Ansatz erweist sich als universell und somit übertragbar auf jede Problemstellung, das heißt auch auf die Gewährleistung der Sicherheit von Systemen. Da sich alles, was den Menschen umgibt, als System beschreiben lässt, ist es möglich, jedem Problem exakt ein System zuzuordnen. Kritische Stimmen befürchten jedoch aufgrund der Universalität und Abstraktheit des SE-Ansatzes, dass dieser nicht schnell und effizient zu praktikablen Lösungen führt. Das betrifft besonders die Notwendigkeit, das System mit seinen Systemgrenzen, Subsystemen, Elementen und deren Wechselbeziehungen zunächst exakt zu beschreiben beziehungsweise zu definieren. In dieser Zeit könnten – nach Meinung der Kritiker und Kritikerinnen – schon intuitive Lösungen gefunden werden.

9 | Vgl. Schnieder/Schnieder 2013, Mamrot et al. 2014.
10 | Vgl. Schnieder/Schnieder 2018, Bertsche et al. 2018, Lichte/Wolf 2018, Weyer et al. 2018, Arens 2018.
11 | Vgl. Gausemeier et al. 2013, Huber 2014, Albers et al. 2014.
12 | Vgl. Ott 2009.
13 | Vgl. Gausemeier et al. 2013, Alt 2014.
14 | Vgl. Ott 2009.
15 | Vgl. Bahill/Gissing 1998.
16 | Vgl. Bahill/Gissing 1998, Haberfellner/Daenzer 1999, Pahl et al. 2005, Lindemann 2005, Ott 2009, Haberfellner et al. 2012.
17 | Vgl. Haberfellner et al. 2012.
18 | Vgl. Pahl et al. 2005, Lindemann 2005, Ott 2009.

Zusammenfassend kann das SE als eine Wissenschaftsdisziplin verstanden werden, die sich im Wesentlichen eines systemtheoretischen Denkansatzes sowie eines Vorgehenskonzepts in Kombination mit Grundprinzipien bedient, um komplexe Problem- und Aufgabenstellungen transdisziplinär zu lösen.[19] Im humboldtschen Sinn kann von einer Wissenschaftsdisziplin gesprochen werden, wenn diese einen Gegenstand hat und sich einer eigenen methodischen Vorgehensweise bedient, um diesen zu untersuchen.[20] Der Gegenstand des SE ist das System, und die Vorgehensweise ist der Problemlösezyklus zur Lösung von Problemen in diesem System. Dieses universellen Gegenstands und der allgemeingültigen Vorgehensweise zur Problemlösung können sich verschiedenste Wissenschaftsdisziplinen bedienen. Folglich kann das SE auch als eine Art „Dachwissenschaft" betrachtet werden, wie Abbildung 1 verdeutlicht.

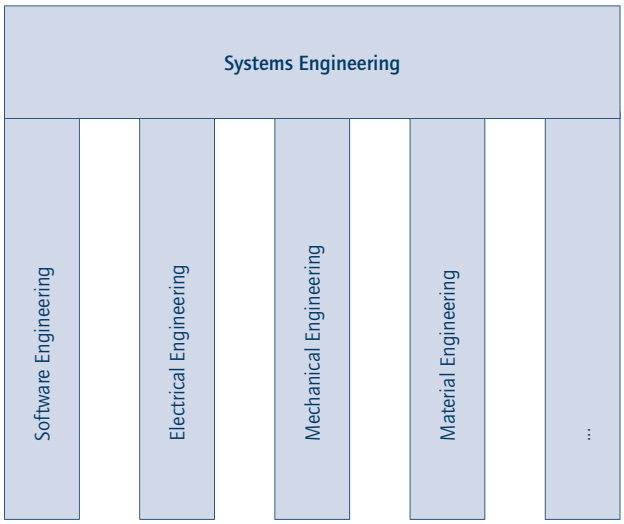


Abbildung 1: SE-Disciplines (Quelle: nach Weilkiens 2007, S. 15)

Das SE kann also als Dachwissenschaft fungieren, wird allerdings nicht immer als solche genutzt. Die Verwendung von SE in einzelnen Fachdisziplinen bringt nämlich nicht zwangsläufig eine Abstimmung von SE-Weiterentwicklungen unter den einzelnen Fachdisziplinen und darüber hinaus mit sich. Wie sich eine solche Vielfalt auf das SE und seine Entwicklung auswirkt, wird daher im folgenden Kapitel näher betrachtet.

3 Systems Engineering und seine Vielfalt

Das SE hat als eigenständige Wissenschaftsdisziplin, wie die Systemtheorie, eine längere Geschichte. In deren Verlauf haben sich bereits unterschiedlichste Ansätze, Konzepte, Methoden und Instrumente in der Praxis zur Lösung mehr oder minder komplexer Problemstellungen bewährt.

Vor diesem Hintergrund erscheint es folglich sinnvoll, die Ursprünge des Systemdenkens und seine Entwicklung sowie die letztendlich daraus resultierenden Auffassungen und Grundannahmen des SE einschließlich der aktuellen Trends zu hinterfragen. Daneben geht es ebenso um die Analyse der methodischen Grundlagen des gegenwärtig praktizierten SE bezüglich der Bewältigung der Komplexität.[21]

Die breite Konzeptvielfalt des SE reicht von universellen Problemlösungsansätzen[22] bis hin zu speziellen SE-Ansätzen, die sich ausschließlich auf

- die Produktentwicklung,[23]
- die Softwareentwicklung,[24]
- die Unternehmensgestaltung[25] oder
- die Erstellung von Sicherheitskonzepten[26]

fokussieren.

Die große Vielfalt der SE-Ansätze, die bereits in der Vergangenheit bestand und auch in der Gegenwart nach wie vor existent ist, zeigt Abbildung 2, aufgeteilt in spezielle und universelle Ansätze.

19 | Vgl. Weilkiens 2007.
20 | Vgl. Winzer 1997.
21 | Vgl. Winzer 2016.
22 | Vgl. Sell 1989, Bahill/Gissing 1998, Haberfellner/Daenzer 1999, Rink 2002, Wulf 2002, Ehrlenspiel 2003, Züst 2004, Lindemann 2005, IEEE 1220-2005, Sage/Rouse 2009, Haberfellner et al. 2012.
23 | Vgl. Pahl et al. 2005, VDI 2221, Schnieder/Schnieder 2013.
24 | Vgl. Fuchs et al. 2001, Sommerville 2007.
25 | Vgl. Schenk 2004, Schuh 2007, Wiendahl et al. 2009.
26 | Vgl. IEC 61508:1998, VDI 2247.

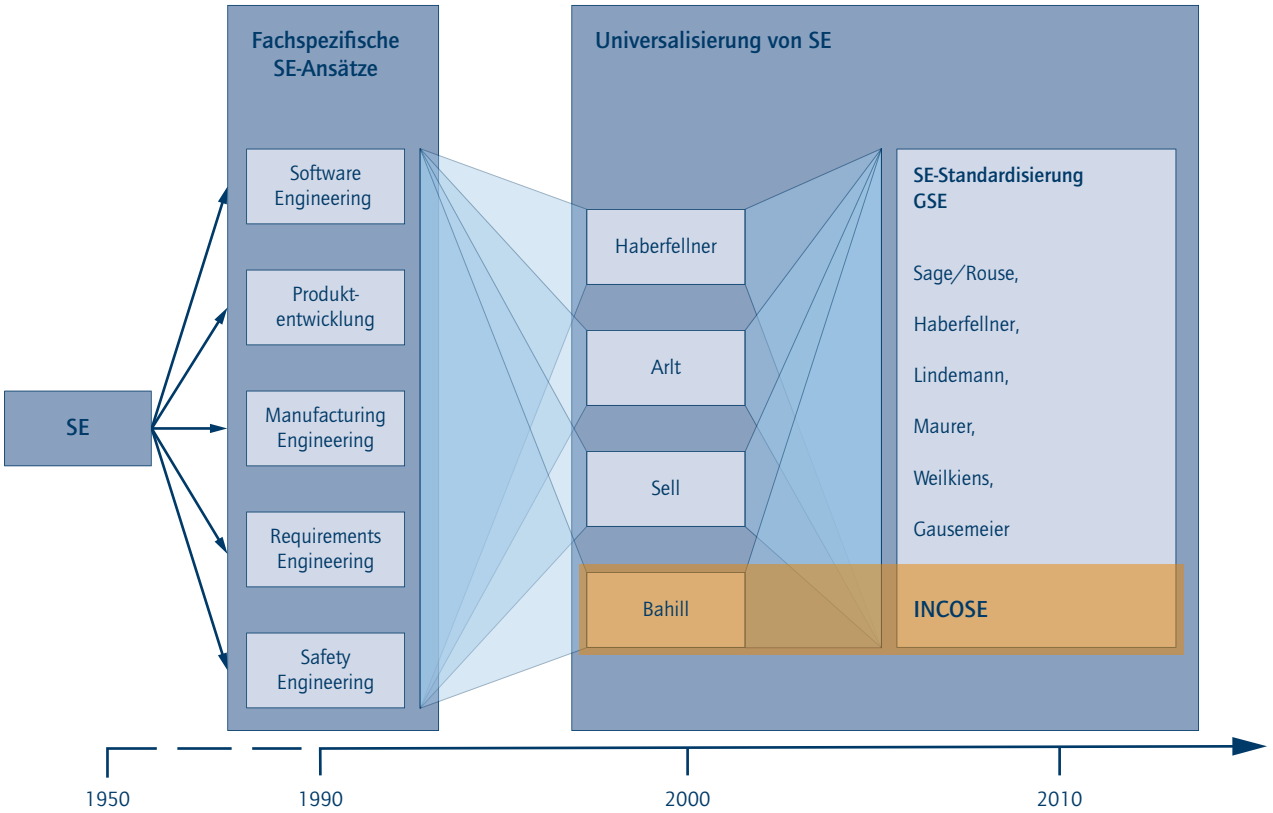


Abbildung 2: SE im Wandel der Zeit (Quelle: nach Sitte/Winzer 2011)

Somit gibt es im SE aktuell zwei wesentliche Gruppierungen. Eine Gruppe verfolgt einen universellen Problemlösungsansatz, während die andere die Nutzung spezifischer SE-Ansätze für die Lösung fachdisziplinspezifischer Fragestellungen favorisiert. Im Folgenden werden daher die universellen Konzepte und anschließend die spezifischen Ansätze bezüglich ihrer transdisziplinären Anwendbarkeit überprüft.

Die universellen Konzepte des Systems Engineering stellen fachdisziplinübergreifende Problemlösungsansätze dar, welche dem Ziel dienen, das Verständnis des Systems durch Transparenz zu stärken, um so den Lebenszyklus des Systems effizient gestalten zu können.[27] Der Übergang des Systems Engineering hin zum Model-Based Systems Engineering (MBSE) leistet hierzu einen wesentlichen Beitrag. Model-Based Systems Engineering konzentriert sich auf die durchgängige Beschreibung und Analyse technischer Systeme auf Basis ihrer Modellierung.[28] Es fokussiert ein fachdisziplinübergreifendes Systemmodell. Dabei werden verschiedene Modelltypen wie Anforderungs-, Funktions- oder Strukturmodelle miteinander verbunden. Die verteilten Modelle müssen jedoch durchgängig miteinander verknüpft werden; dies kann über Tracelinks erfolgen.[29] Doch bevor solche Tracelinks angelegt werden, müssen sich die Unternehmen darüber im Klaren sein, welche Informationen aus welchen Modellen mit welchen Systemen verknüpft und wie diese Tracelinks genutzt werden sollten. Erst auf dieser Grundlage kann eine Datenintegrationslösung hergestellt werden.[30]

Das Model-Based Systems Engineering findet gegenwärtig in der Industrie keine breite Anwendung. Albers et al. sehen die Ursache hierfür in den unterschiedlichen Abstraktionsgraden der Systemmodellierung.[31] Unterschiedliche Modellierungssprachen sowie differenzierte Modellierungsmethoden erschweren der Praxis das fachdisziplinübergreifende Erstellen des Systemmodells.

27 | Vgl. INCOSE 2007.
28 | Vgl. Dumitrescu et al. 2014, S. 21.
29 | Vgl. Grammel/Kastenholz 2010.
30 | Vgl. ebd.
31 | Vgl. Albers et al. 2014.

Somit ist das modellbasierte Systems Engineering eine Antwort auf die aktuellen Tendenzen der Komplexität, birgt jedoch noch weitere zu lösende Forschungsaufgaben wie:

- die Verknüpfung der verschiedensten Systemmodelle,
- die Interaktion zwischen dem Systemmodell und dem Vorgehenskonzept,
- die umfassende Gewährleistung der Sicherheit von komplexen Systemen und
- die Beschreibung der Art und Weise der Pflege und Dokumentation des Systems Engineering über den Lebenszyklus des Systems.

Ein neuer Zweig bei den universellen Ansätzen des Systems Engineering ist das Systems of Systems Engineering (SoSE). Es beschreibt die Entwicklung, Gestaltung und Transformation von Systemen, welche in komplexe Systeme integriert werden müssen. Somit liegt der Fokus des Systems of Systems Engineering auf der Betrachtung von komplexen Systemen in ihren netzwerkartigen Strukturen, um Zusammenhänge zwischen den Systemen erkennen zu können.[32]

Sahen und Ncube betrachten SoSE als einen dem Systems Engineering übergeordneten Ansatz.[33]

Über ein Top-down-Verfahren werden im Systems-of-Systems-Engineering-Ansatz komplexe Systeme erst in Teilsysteme gesplittet, deren Interaktion analysiert und gestaltet und dann wieder zu einem Gesamtsystem zusammengeführt. Schwerpunkt des Systems of Systems Engineering ist allerdings das Zusammenwirken der Systeme, das System selbst steht nicht im Mittelpunkt. Gleiches gilt für die Interaktion des komplexen Systems mit seiner Umwelt.[34]

SoSE wird sowohl für technische Systeme als auch für komplexe soziotechnische Systeme sowie für Unternehmensnetzwerke oder intelligente Systeme sowie Produktions- und Dienstleistungssysteme genutzt.[35] Es kann festgestellt werden, dass sich der SoSE-Ansatz zwar der Werkzeuge des Systems Engineering bedient, jedoch unterschiedlichste Vorgehensweisen empfiehlt. Es gibt **keine** einheitliche beziehungsweise allgemeingültige Definition des Systems of Systems Engineering.

Verursacht durch die Vielzahl der universellen Systems-Engineering-Ansätze entwickelte sich eine weitere Richtung im Systems Engineering, das Lean Systems Engineering. Ziel des Lean Systems Engineering ist eine Verschlankung des Problemlösungsprozesses. Besonders in der Phase der Anforderungsanalyse wird, so Oppenheim, häufig viel Zeit verschenkt.[36] Aus diesem Grund fokussiert sich das Lean Systems Engineering in der Phase der Anforderungsanalyse darauf, dass Kunde und Auftraggeber gemeinsam die Anforderungen definieren. Somit werden frühzeitig Missverständnisse bezüglich der Anforderungen ausgeräumt, und infolge der Systementwicklung und -gestaltung können dann notwendige Abstimmungen minimiert werden. Das Lean Systems Engineering beschreibt standardisierte Vorgehensweisen und empfiehlt Tools zum Problemlösungsprozess. Dabei kombiniert es die Weisheit des Lean Thinking mit der Schrittfolge des Systems Engineering.[37] Wenn der Lean-Systems-Engineering-Ansatz so erweitert werden könnte, dass Kunde und Auftraggeber gemeinsam das Systemmodell definieren, das heißt nicht nur das Anforderungsmodell, sondern gleichzeitig auch das Funktions-, Struktur- und Prozessmodell, dann wäre eine definierte Basis für den sich anschließenden Problemlösungsprozess geschaffen. Wäre eine Iteration zwischen dem Systemmodell und dem standardisierten Vorgehenskonzept des Lean Systems Engineering vorgesehen, sodass der Problemlösungsprozess transparent und rückverfolgbar gestaltet würde, so könnte das Lean Systems Engineering alle universellen Systems-Engineering-Ansätze in sich vereinen. Dabei müssten aber auch die Datenartefakte der Subsysteme beziehungsweise der verschiedenen Modelle des Systemmodells miteinander verknüpft werden. Diese sogenannten Tracelinks erlauben die Nachverfolgbarkeit (Tracebility), welche für die Rückverfolgung des Lebenszyklus des Systems unabdingbar ist.[38] Grundsätzlich muss die mangelnde Flexibilität zwischen dem Vorgehenskonzept (Problemlösungszyklus) und der Erstellung, Pflege und Dokumentation des Systemmodells bei den universellen Systems-Engineering-Ansätzen bearbeitet und aufgehoben werden.

Allen hier kurz charakterisierten SE-Ansätzen ist gemein, dass sie universell, das heißt in jeder Wissenschaftsdisziplin, angewandt werden können. Somit sind sie durchaus für einen transdisziplinären Problemlösungsansatz geeignet. Jeder der oben genannten SE-Ansätze beansprucht für sich, allgemeingültig zu sein und auf standardisierten Modulen aufzubauen. Genau darin besteht das

32 | Vgl. Keating et al. 2003, Luzeaux/Ruault 2010.
33 | Vgl. Sahen et al. 2009, Ncube et al. 2013.
34 | Vgl. Jamshidi 2009, Dimario 2010.
35 | Vgl. DAG 2010, Jing et al. 2013, Weiss 2013, Lim/Ncube 2013.
36 | Vgl. Oppenheim 2011.
37 | Vgl. ebd.
38 | Vgl. Grammel/Kastenholz 2010.

Problem für die Anwendenden des SE. Welches Vorgehenskonzept sollte ein interdisziplinäres Team nutzen, wenn es die Sicherheit einer komplexen Fabrikanlage gewährleisten möchte?

Damit das SE einen Beitrag zur Gewährleistung der Sicherheit von komplexen Systemen leisten kann, müssen folgende Anforderungen erfüllt sein:

- Denken in Systemen,
- Vorhandensein eines Denkmodells, welches durch die Vertreter und Vertreterinnen aller Fachdisziplinen genutzt werden kann,
- transdisziplinäre Einsetzbarkeit, Transparenz und Rückverfolgbarkeit des Vorgehenskonzepts und
- zielgerichtete Einbindung der Grundprinzipien des systematischen Denkens und Handelns in das Vorgehenskonzept beim Erstellen des Denkmodells.

Diese Anforderungen an das SE dienten als Basis für den Vergleich der verschiedensten Ansätze (siehe Tabelle 1). Es musste festgestellt werden, dass sich eine Vielzahl von Denkmodellen und Vorgehenskonzepten des SE entwickelt haben, die den Anspruch erheben, universell für jegliche Art von Problemen Lösungen entwickeln zu können. Doch die Realität sieht anders aus, wie Tabelle 1 zeigt.

Keiner der hier überprüften universellen Ansätze erfüllt alle Anforderungen.

Einen Überblick über spezifische Denk- und Vorgehensmodelle auf Basis des SE gibt Tabelle 2, wobei auch direkt der Erfüllungsgrad der Anforderungen bezüglich eines disziplinübergreifenden Ansatzes mit angezeigt wird.[39]

Wie in Tabelle 2 ersichtlich, erfüllt auch keiner der spezifischen Ansätze alle Anforderungen.

Somit ist festzustellen, dass sich sowohl die universellen als auch die spezifischen Vorgehensweisen des SE teilweise des Systemdenkens bedienen.[40] Die Mehrzahl der betrachteten universellen

Anforderungen an SE / Quelle	Denken in Systemen	Denkmodell	Vorgehenskonzept			Grundprinzipien des systemischen Denkens und Handelns	Verbindung Denkmodell und Vorgehenskonzept	
			transparent	rückverfolgbar	transdisziplinär		sequentiell	iterativ
Bahill und Gissing 1998	◐	◐	◐	◐	◐	◐	◐	◐
Sell 1989	◐	◐	◐	◐	◐	◐	◐	◐
Haberfellner und Daenzer 1999	◐	◐	◐	◐	◐	◐	◐	◐
Wulf 2002	◐	◐	◐	◐	◐	◐	◐	◐
Ehrlenspiel 2003	◐	◐	◐	◐	◐	◐	◐	
Lindemann 2004	◐	◐	◐	◐	◐	◐	◐	◐
IEEE 1220-2005	◐	◐	◐	◐	◐	◐	◐	
Sage und Rouse 2009	◐	◐	◐	◐	◐	◐	◐	
Haberfellner et al. 2012	◐	◐	◐	◐	◐	◐	◐	◐

Legende: ◑ nicht zutreffend ◐ teilweise zutreffend ● zutreffend

Tabelle 1: Vergleich von universellen Ansätzen auf Basis des SE (Quelle: Winzer 2016, S. 53)

39 | Vgl. Winzer 2016, S. 54.
40 | Vgl. Balzert 1998, Fuchs et al. 2001, Sommerville 2007, Ott 2009.

Anforderungen an SE / Quelle	Denken in Systemen	Denkmodell	Vorgehenskonzept			Grundprinzipien des systemischen Denkens und Handelns	Verbindung Denkmodell und Vorgehenskonzept	
			transparent	rückverfolgbar	transdisziplinär		sequentiell	iterativ
Produktentwicklung								
Pahl et al. 2005	◑	◑	◑	◑	◑	◑	◑	◔
VDI 2221	◑	◑	◑	◑	◑	◑	◔	◔
Schnieder 2013	◑	◑	◑	◑	◑	◑	◑	◔
VDI 2206	◑	◑	◑	◑	◑	◑	◑	◔
Gausemeier et. al 2014	◑	◑	◑	◑	◑	◑	◔	◑
Software Engineering								
IEEE 1220	◑	◑	◑	◑	◑	◑	◑	◔
Sommerville 2007	◑	◑	◑	◑	◑	◑	◑	◔
Fuchs et al. 2001	◑	◑	◑	◑	◔	◑	◑	◔
Balzert 1998	◑	◑	◑	◑	◑	◑	◑	◔
Manufacturing Engineering								
Schenk 2004	◑	◑	◑	◑	◑	◑	◑	◔
Wiendahl 2009	◑	◑	◑	◑	◑	◑	◔	◑
Requirements Engineering								
Ott 2009	◑	◑	◑	◑	◑	◑	◑	◔
Safety Engineering								
ICE 61508	◔	◑	◑	◑	◔	◑	◑	◔
EN ISO 13849-1	◔	◑	◑	◑	◔	◑	◑	◔

Legende: ◔ nicht zutreffend ◑ teilweise zutreffend ◑ zutreffend

Tabelle 2: Vergleich von spezifischen Ansätzen auf Basis des SE (Quelle: Winzer 2016, S. 54)

SE-Ansätze nutzen Denkmodelle und weisen ihre Vorgehenskonzepte als transparent und transdisziplinär sowie zum Teil als rückverfolgbar aus.[41]

Sie nutzen teilweise auch Grundprinzipien des systemischen Denkens und Handelns, wie zum Beispiel die Grundprinzipien der wiederkehrenden Reflexion, vom Ganzen zum Detail oder des diskursiven Vorgehens. Das trifft vereinzelt ebenfalls auf die speziellen Ansätze des SE zu.[42]

41 | Vgl. Bahill/Gissing 1998, Haberfellner/Daenzer 1999, Lindemann 2005, Sommerville 2005, Sage/Rouse 2009, Haberfellner et al. 2012.
42 | Vgl. Schenk 2004, Pahl et al. 2005, Sommerville 2007, Ott 2009.

Die Vielzahl von Denkmodellen und Vorgehenskonzepten, die hier nur auszugsweise und ohne Anspruch auf Vollständigkeit dargestellt werden konnten, erschweren dem potenziellen Nutzer oder der Nutzerin allerdings die Auswahl. Hinzu kommt, dass die Dimensionen der Komplexität in Verbindung mit den höheren Anforderungen an die Gewährleistung der Sicherheit von Systemen heute und in Zukunft transdisziplinäres Denken und Handeln erfordern. Das kann nur auf einer standardisierten Basis erfolgen.

Dazu muss es möglich sein, dass sich die Teams, welche heute immer aus unterschiedlichen Fachspezialisten und -spezialistinnen bestehen, bei der Problemlösung eines gemeinsamen Denkmodells bedienen. Soll zum Beispiel das Schließsystem eines Autos verbessert werden, muss das Team zunächst ein gemeinsames Metamodell, das heißt ein gemeinsames Abbild des Autos, haben. Erst dann kann sich das Spezialteam der Veränderung des Teilsystems „Schließsystem" zuwenden, weil nun klar ist, mit welchen anderen Teilsystemen des Autos das Schließsystem in Verbindung steht. Wird so vorgegangen, kann es nicht passieren, dass sich Türen automatisch öffnen, wenn das Auto unter einer Hochspannungsleitung fährt.

Neben dem gemeinsamen Denkmodell ist auch ein standardisiertes modulares Vorgehen zur Problemlösung notwendig. Veränderungen des Systems sollten so umgesetzt werden, dass sich die verschiedensten Fachspezialisten und -spezialistinnen zunächst gemeinsam darüber verständigen, wie die Problemanalyse und grundsätzlich die Problemlösung aussehen könnten. Erst danach scheint eine fachspezifische Suche nach Lösungsalternativen bei gleichzeitiger Nutzung der Prinzipien des systemischen Denkens und Handelns sinnvoll. Dabei ist die entsprechende Transparenz und Rückverfolgbarkeit zu gewährleisten, damit bei der Zusammenführung der Lösungsalternativen eines komplexen Systems das gesamte Team gemeinsam denken und handeln kann. Folglich ist ein universeller, modularer, standardisierbarer, fachdisziplinübergreifender Problemlösungsansatz erforderlich. Das SE könnte ein solcher sein, wenn es gelingt, über vergleichende Betrachtungen Module aus der Vielzahl der Denkmodelle und Vorgehenskonzepte zu typisieren und standardisiert so zu bündeln, dass für multidisziplinäre Teams eine universelle Problemlösung mithilfe eines vereinheitlichten Denk- und Vorgehensmodells möglich wird. Doch aufgrund der hier nur im Ansatz beschriebenen Vielfalt der Vorgehensweisen des SE kann das bislang nicht gelingen.

Folglich ergeben sich weitere Forderungen an das SE. Dieses muss

- modular aufgebaut,
- standardisierbar und
- universell sein sowie
- spezielle Problemlösungen ermöglichen.

Kann dieser Anspruch schon durch die Modifikation einiger SE-Ansätze erreicht werden, oder muss das SE von Grund auf reformiert werden? Dieser Frage soll im folgenden Kapitel nachgegangen werden.

4 Generic Systems Engineering als mögliche Basis für die Entwicklung einer Systemtheorie der Sicherheit

Das Fazit des dritten Abschnitts belegt, dass sich gerade das SE grundsätzlich dazu eignet, mittels der zielgerichteten Anwendung seines methodischen Vorgehens die Probleme, die aus den neuen Tendenzen der Komplexität entstehen, systematisch und effizient zu bewältigen.

Allerdings zeigt sich ebenso, dass das SE seinen ursprünglichen universellen Ansatz aufgrund der ständig wachsenden Zahl neuer problem- beziehungsweise fachspezifischer Denkmodelle und Vorgehenskonzepte verloren hat. Deshalb erscheint es trotz übergreifender SE-Ansätze eher fraglich, ob aus ihnen ein genereller und generischer, das heißt ein Generic-Systems-Engineering-Ansatz (GSE-Ansatz), gemäß den neuen Anforderungen entwickelt werden kann.

Das Systemdenken muss, so Weilkiens, ein generalisiertes Denkmodell unabhängig von der jeweiligen Fachdisziplin schaffen.[43] Folglich müssen in einem weiter zu entwickelnden generischen SE die Grundbausteine, das heißt das Systemdenken, das Denkmodell und das Vorgehenskonzept (geplantes Vorgehen für die Problemlösung), so verbunden werden, dass eine transdisziplinäre, generelle Nutzung für Problemlösungen jeglicher Art in jeder Branche möglich wird. Das wiederum bedingt eine synergetische Verbindung zwischen dem Denkmodell und dem Vorgehenskonzept, über welche die in den Tabellen 1 und 2 aufgelisteten Ansätze des SE nicht verfügen. Es ist also ein Denkmodell mit entsprechenden Werkzeugen zu entwickeln,

43 | Vgl. Weilkiens 2007.

Sichten	Erläuterung
Anforderungen	Anforderungen sind Erfordernisse oder Erwartungen von Stakeholdern an ein System, welche festgelegt, üblicherweise vorausgesetzt oder verpflichtend sind.
Funktionen	Funktionen beschreiben den Zweck beziehungsweise die Aufgabe, die ein System zu erfüllen hat. Sie geben damit der Umwandlung von Eingaben in Ausgaben eines Systems eine Zielrichtung. Dadurch ermöglichen Funktionen eine Beschreibung davon, „was" ein System oder Teile davon realisieren sollen.
Prozesse	Prozesse beschreiben, wie die Eingaben eines Systems in Ausgaben umgewandelt werden, also das „Wie". Über den Prozess realisiert sich die eingebaute Funktionalität des Systems, das heißt, innerhalb von Prozessen werden bei technischen Systemen durch die Nutzung von Komponenten Funktionen umgesetzt. Erfolgt die Einbindung von Menschen in Prozesse, werden Letztere oftmals auch als Arbeits- oder Geschäftsprozesse bezeichnet (Prozess eines soziotechnischen Systems).
Komponenten	Komponenten sind physische oder logische, einzelne oder zusammengefasste Bestandteile eines Systems.
Personen	Personen beschreiben Menschen. Sie nutzen und realisieren Komponenten und auch Prozesse und stellen Input für die Leistungserbringung zur Verfügung. Somit realisieren sie Funktionen, welche wiederum Anforderungen erfüllen. Im Zusammenhang mit Unternehmensnetzwerken werden Personen den jeweiligen Unternehmen im Netzwerk zugeordnet und durch diese dargestellt.

Tabelle 3: Erläuterung der Sichten für das Systemmodell (Quelle: nach Nicklas 2016)

welches die Komplexität von Systemen allgemein verständlich veranschaulicht. Die Weiterentwicklung des Systems selbst, das heißt seine Genese, muss in dem neuen, generellen Denkmodell, dem GSE-Denkmodell, erkennbar sein.

Das GSE-Denkmodell ist so auszulegen, dass disziplinübergreifend ein einheitliches, möglichst standardisiertes Modell bereitgestellt wird. Dieses muss die Funktionalitäten des Beschreibens, Analysierens, Gestaltens, Optimierens und Prognostizierens erfüllen und zudem eine Kopplung mit den fachspezifischen Methoden zulassen, sodass im Rahmen der einzelnen Schritte des Vorgehenskonzepts mit dem Ziel der Problemlösung die Rückführung der Erkenntnisse aus einzelnen fachspezifischen Methoden und Problemlösungsschritten in das Modell gelingt. Dementsprechend sind für das GSE-Denkmodell die Verwendung des Blackbox-Prinzips, die Nutzung der Hierarchisierung sowie die Verknüpfung von Elementen über Matrizen oder Netzgraphen unumgänglich. Des Weiteren ist bezüglich der Elementarten und ihrer Relationen ein Standard festzulegen, der die Integration fachspezifischer Modellierungen ermöglicht, dabei aber mit einer minimalen Anzahl an Elementarten und Relationen auskommt.

Nicklas, Winzer und Schlüter schlagen hierfür das Demand Compliant Design (DeCoDe) bei technischen Systemen und das Enhanced Demand Compliant Design (e-DeCoDe) für soziotechnische Systeme vor.[44] Die beiden Denkmodelle unterscheiden sich lediglich durch die Elementart „Personen" und nutzen ansonsten die vier weiteren Elementarten „Anforderungen", „Funktionen", „Prozesse" und „Komponenten", die in Tabelle 3 definiert werden.

Durch die standardisierten Elementarten, deren Verknüpfung untereinander und die Betrachtung über den Verlauf der Entwicklungszeit (siehe Abbildung 3) lässt sich die Forderung nach Transparenz und Rückverfolgbarkeit erfüllen.

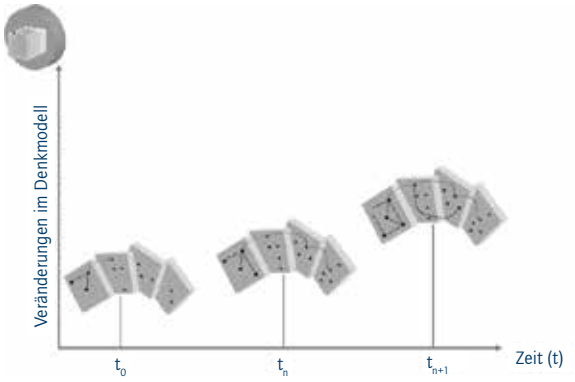


Abbildung 3: Das Prinzip der zeitlichen Veränderung des GSE-Denkmodells (Quelle: Winzer 2016, S. 133)

Doch nur durch eine Interaktion zwischen Modell und Vorgehenskonzept ist es möglich, dass alle beteiligten Personen auf dem aktuellen Stand bezüglich des Systems sind.[45] Die Forderung, dass das Vorgehenskonzept und das Denkmodell kontinuierlich interagieren, ist obligatorisch, da nur so sichergestellt werden kann, dass das Projektteam Entscheidungen auf Basis aktueller Daten und Informationen trifft.

44 | Vgl. Nicklas 2016, Winzer 2016, Schlüter 2017.
45 | Vgl. Schlüter/Winzer 2015.

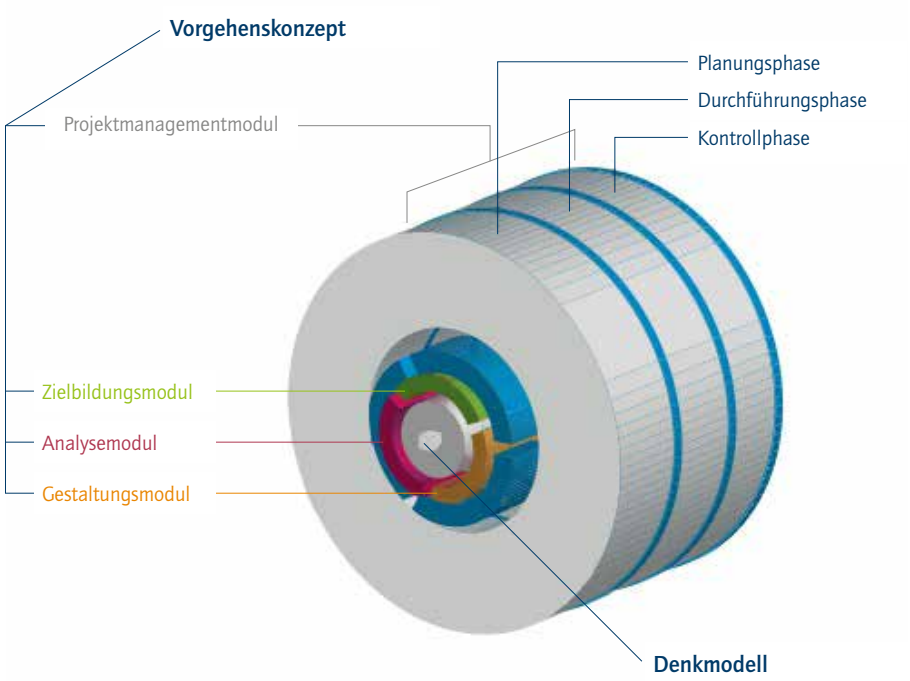


Abbildung 4: Die Genese des GSE-Denkmodells und des GSE-Vorgehenskonzepts (Quelle: Winzer 2016, S. 199)

Aber auch die Transdisziplinarität stellt neben der Transparenz und der Rückverfolgbarkeit spezifische Forderungen an das zu verändernde SE-Vorgehenskonzept. Dies bedeutet, dass das Vorgehenskonzept so zu gestalten ist, dass die fachspezifischen Methoden integrierbar sind und Schnittstellen zwischen ihnen gestaltet werden. Dabei sind die Auswahl und die Kombination der fachspezifischen Methoden problemlösungsorientiert und effizient über ein entsprechendes Projektmanagement zu steuern. Das GSE besteht aus diesem Grund aus einem Ziel-, einem Analyse- und einem Gestaltungsmodul, die durch das Projektmanagementmodul koordiniert werden (siehe Abbildung 4). Alle Module stehen zudem in Verbindung mit dem GSE-Denkmodell, das iterativ nach jedem Schritt innerhalb eines Moduls aktualisiert wird.

Im Zielbildungsmodul werden Methoden und Techniken eingesetzt, die auf Basis des entsprechenden Problems der Zielbildung der anstehenden Arbeiten dienen. Das Analysemodul dient der Identifizierung oder auch Konkretisierung eines Problems. Hier werden Situationen greifbar gemacht, um das Problem und seine Ursachen zu verstehen. Dies umfasst auch das strukturierte Sammeln von Informationen für die Problemlösung. Das GSE-Gestaltungsmodul nutzt das GSE-Denkmodell mit seinen dort hinterlegten Informationen aus dem Ziel- und Analysemodul als Input, um unter Anwendung der Grundprinzipien des systematischen Denkens und Handelns Lösungen zu gestalten. Es bedient sich spezieller fachspezifischer Methoden und Verfahren, die aufgabenspezifisch durchaus auch miteinander kombiniert werden können. Da die Problemlösung aufgrund der im Rahmen des Vorgehenskonzepts neu gewonnenen Erkenntnisse einer gewissen Dynamik unterliegt, ist das Projektmanagementmodul für die zeitlich logische Abfolge der Tätigkeiten zuständig. Mithilfe des Projektmanagementmoduls werden die Methoden und Verfahren der Ziel-, Analyse- und Gestaltungsmodule in zeitlich logischer Folge geplant, realisiert und kontrolliert. Dabei ist es Aufgabe des Projektmanagementmoduls, die Interaktion zwischen dem Denkmodell und den Modulen des Vorgehenskonzepts erfolgreich umzusetzen.[46]

Zum besseren Verständnis des GSE-Denkmodells, der GSE-Module und deren Zusammenwirken wird im folgenden Kapitel aufgezeigt, wie das Problem der Erfassung des Sicherheitsempfindens von Fahrgästen am Bahnhof systematisch gelöst werden kann.

46 | Vgl. Winzer 2013.

5 Anwendungsbeispiel: Messung des Sicherheitsempfindens von Fahrgästen des öffentlichen Personennahverkehrs (ÖPNV)

Im Folgenden wird der Forschungsfrage nachgegangen, wie das Sicherheitsempfinden von Fahrgästen des öffentlichen Personennahverkehrs systematisch gemessen werden kann. Dabei reicht die Messung der Sicherheit von der Prozessleistungsmessung im ÖPNV-Netzwerkverbund über die Überprüfung der Anforderungserfüllung von den im ÖPNV-Netzwerkverbund angebotenen Dienstleistungen bis hin zur Kundenzufriedenheitsmessung bezüglich der Sicherheitsanforderungen.

Hierzu sind folgende Fragen zu lösen:

- Welche Sicherheitsanforderungen sind je nach Prozess und Verantwortlichen zu betrachten?
- Welche Methoden sind zur Überprüfung der Erfüllung von Sicherheitsanforderungen geeignet?
- Wie kann die Erfüllung der Sicherheitsanforderungen bei den Dienstleistungen des ÖPNV-Netzwerkverbunds kontinuierlich gemessen werden?
- Wie werden die Messergebnisse bezüglich der Erfüllung der Sicherheitsanforderungen abgebildet und den jeweiligen Verantwortlichen für den kontinuierlichen Verbesserungsprozess zur Verfügung gestellt?[47]
- Wie kann die Komplexität einer solchen interdisziplinären Aufgabe in einem Unternehmensnetzwerk gelöst werden?

Da Sicherheitsanforderungen eine Teilmenge aller Anforderungen verschiedenster Stakeholder an ein System darstellen, sind Messmethoden, die alle Arten von Anforderungen handhaben können, für diesen Anwendungsfall gefordert. Darüber hinaus kann davon ausgegangen werden, dass Methoden, die unterschiedlichste Stakeholder und ihre Anforderungen verarbeiten können, in diesem Zusammenhang ebenfalls benötigt werden. Dementsprechend werden zur Problemlösung Methoden der Kundenzufriedenheitsmessung zu kombinieren sein, sodass die Dienstleistungsqualität eines komplexen ÖPNV-Netzwerks mit diversen Kundengruppen hinsichtlich der Sicherheit erfasst werden kann.

Der Bedarf an einer solchen Methodik wurde im Rahmen des Projekts VeRSiert[48] deutlich. In diesem Projekt sollte das Sicherheitsempfinden von Fahrgästen des öffentlichen Personennahverkehrs erfasst werden. Es galt, ein Vorgehenskonzept zur ganzheitlichen Erfassung der Kundenzufriedenheit (in diesem Fall Erfassung des Sicherheitsempfindens) in Unternehmensnetzwerken (UNW) zu entwickeln, das durch das GSE sowohl die Komplexität von UNW als auch die unterschiedlichen (UNW-Partner-) Bedürfnisse handhaben kann.[49]

Hierbei werden folgende Methoden im Rahmen des Vorgehenskonzepts eingesetzt (siehe Tabelle 4).

Schritt des Vorgehenskonzepts	Ausgewählte Methode(n)	Literaturverweis(e)
Orientierende Analyse	Blackbox-Ansatz Sampling Sekundäranalyse	Haberfellner 2002 Schlüter und Sochacki 2012 Schlüter und Sochacki 2012
Erweitertes Service Blueprint	Erweitertes Service Blueprint	Schlüter 2013
Kundenkontaktpunkte	Erweitertes Service Blueprint	Schlüter 2013
Leistungsclustermerkmale	Erweitertes Service Blueprint	Schlüter 2013
Leistungscluster	DeCoDe e-DeCoDe	Sitte und Winzer 2011 Nicklas et al. 2016
Datenbankaufbau	DeCoDe e-DeCoDe	Sitte und Winzer 2011 Nicklas et al. 2016
Befragung	Cards & Lights	Schlüter 2013
Datenauswertung	Interpolation DeCoDe e-DeCoDe	Bollhöfer und Mehrmann 2004 Sitte und Winzer 2011 Nicklas et al. 2016

Tabelle 4: Eingesetzte Methoden im Rahmen des Vorgehenskonzepts zur Messung des Sicherheitsempfindens in UNW (Quelle: nach Schlüter 2017)

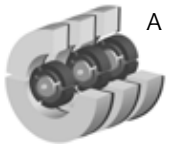
47 | Vgl. Schlüter 2017.

48 | Vgl. BMBF-Projekt VeRSiert – Sicherheit im ÖPNV bei Großveranstaltungen: Vernetzung von Verkehrsunternehmen, Einsatzkräften, Veranstaltern und Fahrgästen des ÖPNV.

49 | Vgl. Schlüter 2013.

Entsprechend den einzelnen Schritten des Vorgehenskonzepts wird die Anwendung der Methoden im Rahmen der GSE-Module und ihre Interaktion mit dem GSE-Denkmodell in den nachfolgenden Unterkapiteln dargelegt, um abschließend die Durchführung kritisch reflektieren und evaluieren zu können.

Schritt 1: Orientierende Analyse

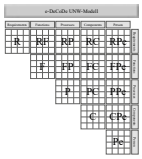


Die orientierende Analyse diente der Bestimmung der UNW-Partner, der zu berücksichtigenden Kundengruppen, der Aufnahme der Prozesse sowie der Erfassung der Netzwerktypologie[50] und wurde mit den Ansprechpersonen der Kölner Verkehrsbetriebe (KVB) sowie des Nahverkehrs Rheinland (NVR) durchgeführt.

Als Ergebnis stellte sich heraus, dass es sich beim ÖPNV-Unternehmensnetzwerk um ein heterarchisches Unternehmensnetzwerk mit Netzwerkmanagement handelt.[51]

Die Befugnisse des Netzwerkmanagers sind allerdings beschränkt. Im Tätigkeitsbereich „Kundenzufriedenheit", in dem auch das Sicherheitsempfinden von Fahrgästen angesiedelt ist, sind die Netzwerkpartner selbst verantwortlich und tauschen keine Informationen aus. Daraus resultiert, dass ein Abgleich von Daten zum Sicherheitsempfinden oder eine koordinierte Erhebung dessen weder entlang der horizontalen noch entlang der vertikalen Wertschöpfungskette stattfindet. Sowohl die eingeschränkten Befugnisse innerhalb des Netzwerks als auch die Konkurrenzsituation der einzelnen Partner am Markt führen zu einer nur bedingt transparenten Kommunikations- und Prozessstruktur des Netzwerks. Dies spiegelt sich unter anderem darin wider, dass die Kundenkontaktpunkte eines einzelnen Partners zur Befragung der Fahrgäste zwar für die Erhebung des eigenen Leistungsniveaus genutzt werden können, nicht aber für die Erhebung der Leistungen anderer Partner. Eine netzwerkumfassende, koordinierte Messung des Sicherheitsempfindens ist somit bislang nicht möglich.[52]

Das bedeutet, dass die partnerbezogenen Prozesse und Leistungen des Netzwerks bei einzelnen Unternehmensnetzwerkpartnern dokumentiert und unter Wahrung der Geheimhaltungspflicht koordiniert werden müssen.[53]

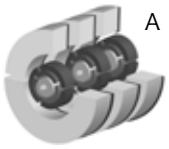


Die Erkenntnisse der orientierenden Analyse wurden zudem in e-DeCoDe abgebildet, wobei zunächst die Netzwerkebene mit den einzelnen Partnern und die zwischen ihnen vorhandenen Kommunikationswege bezüglich Kundenzufriedenheitsmessungen dargestellt wurden, wie Abbildung 5 zeigt.[54]

Auf Basis der Erkenntnisse der orientierenden Analyse ist für das weitere Vorgehen die Nutzung eines Leistungsclusters geboten, das die Geheimhaltung der Befragungsergebnisse gegenüber den beteiligten Netzwerkpartnern ermöglicht (für weiterführende Informationen siehe Handlungsleitfaden in Schlüter 2013). Zudem sind damit einhergehende getrennte Prozesserhebungen sowie Geheimhaltungsregelungen zu berücksichtigen.

Im Folgenden wird dies am Beispiel der Kundengruppenstrukturen weibliche und männliche Fahrgäste und der Untergruppe Fußballfan veranschaulicht. Ziel war es, nachvollziehen und belegen zu können, ob sich das Sicherheitsempfinden von weiblichen und männlichen Fußballfans, die den ÖPNV nutzen, von der größeren, unspezifischen Kundengruppe unterscheidet.[55]

Schritt 2: Erweitertes Service Blueprinting



Auf Basis der erfassten Partnerstrukturen werden in der zweiten Systemebene zunächst die Prozesse der fokussierten Kundengruppen für das Szenario „Benutzung der U-Bahn und Ausstieg am Kölner Hauptbahnhof" bei der KVB erhoben (Schlüter 2013). Dies erfolgt mithilfe des erweiterten Service Blueprinting.[56]

Für die Erstellung des erweiterten Service Blueprint wurden zunächst die Kunden- sowie die Unternehmensprozesse vom Netzwerkpartner KVB erfasst. Anschließend wurden die Prozesse der anderen Unternehmensnetzwerkpartner, die in diesem Szenario relevant sind, ergänzt, sodass ein umfassendes Abbild sowohl der Kunden- als auch der Netzwerkprozesse entstand.[57]

Hierbei stellte sich heraus, dass neben den Prozessen anderer Unternehmensnetzwerkpartner auch Prozesse von Externen

50 | Vgl. Schlüter 2013.
51 | Vgl. ebd.
52 | Vgl. ebd.
53 | Vgl. ebd.
54 | Vgl. ebd.
55 | Vgl. ebd.
56 | Vgl. ebd.
57 | Vgl. ebd.

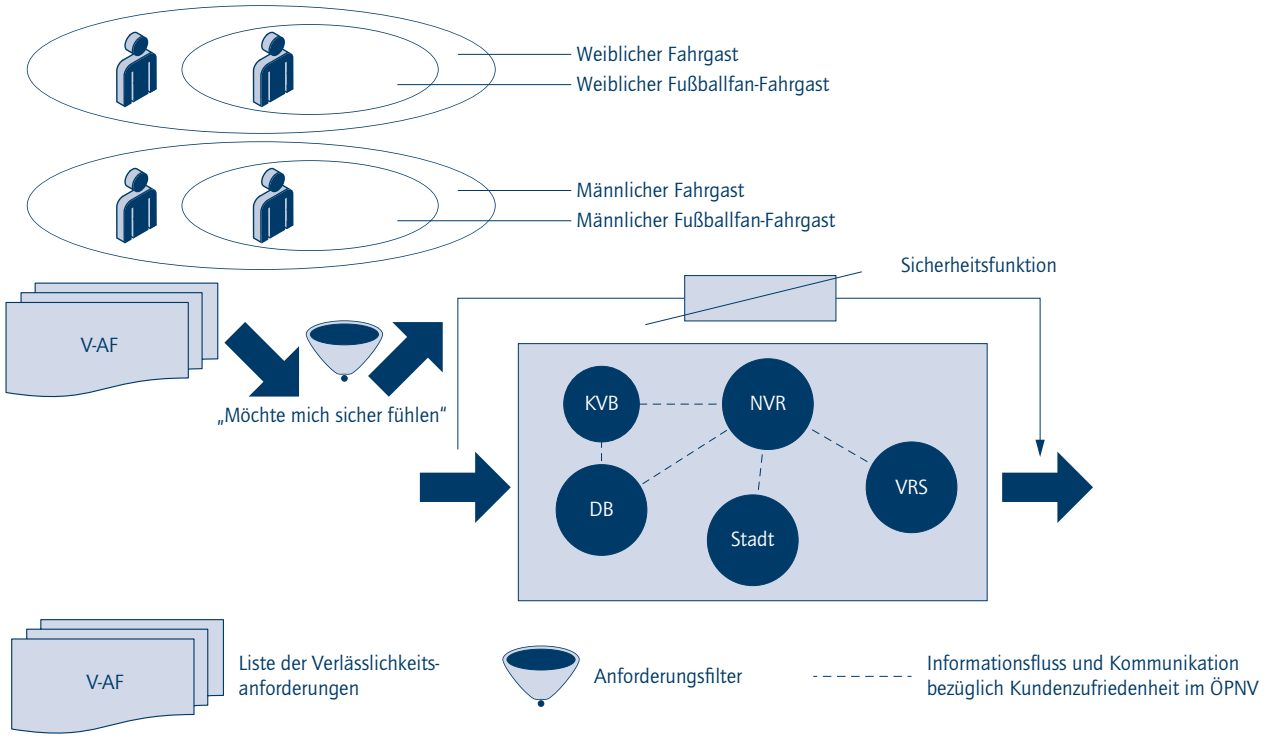


Abbildung 5: Abbildung des UNW mit Kundengruppen und Informationsfluss bezüglich Kundenzufriedenheit als Ergebnis der orientierenden Analyse (Quelle: Schlüter 2017, S. 98)

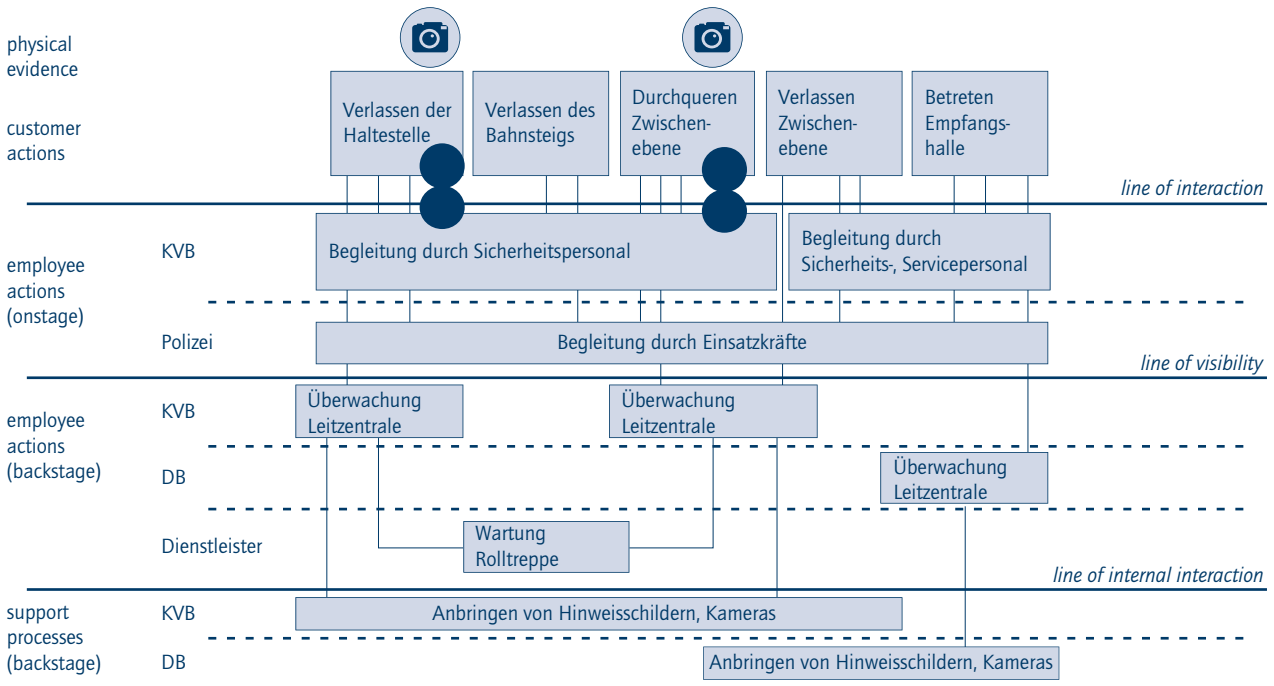
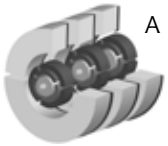


Abbildung 6: Ausschnitt Service Blueprinting „Benutzung der U-Bahn und Ausstieg am Kölner Hauptbahnhof“ (Quelle: nach Schlüter 2013)

relevant sind. In diesem Fall sind es die Polizei und die Rettungskräfte, die nach dem Ende des Bundesligafußballspiels des 1. FC Köln zwischenzeitlich sowohl am U-Bahnsteig des Kölner Hauptbahnhofs als auch an der Zwischenebene anwesend sind (siehe Abbildung 6). Dementsprechend wurde die Systemdefinition um die entsprechenden Externen, die ebenfalls Einfluss auf die Verlässlichkeit des ÖPNV-Systems haben, erweitert, und die Erkenntnisse wurden im e-DeCoDe-basierten UNW-Modell aktualisiert.[58]

Durch die Nutzung des erweiterten Service Blueprint wurden somit alle relevanten Prozesse bezüglich „Sicherheitsempfinden des Fahrgastes" sowie deren Verantwortliche erfasst. Die Erkenntnisse wurden umfassend im UNW-Systemmodell abgebildet.[59]

Schritt 3: Kundenkontaktpunkte und Leistungsmerkmale



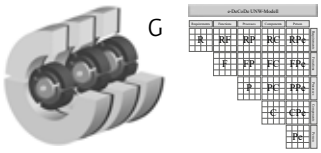
Im nächsten Schritt sind die erhobenen Kundenprozesse auf Kundenkontaktpunkte mit den Prozessen des UNW zu untersuchen. Es wurden Kundenkontaktpunkte in der Bahn, am Kundeninformationsschalter und am Bahnsteig identifiziert. Da im Projekt VeRSiert[60], das unter anderem das Sicherheitsempfinden in Bezug auf die Personendichte erheben sollte, die nötige Kameratechnik zur Erfassung der Anzahl der Personen vor Ort nur in der Zwischenebene der U-Bahn-Haltestelle Kölner Hauptbahnhof verfügbar war, wurde dieser Kontaktpunkt im Folgenden weiter betrachtet.[61]

Ebenso durch das Projekt vorgegeben waren die Leistungsmerkmale, die mit der Kundenbefragung zu messen sind. Hierzu wurden für die Befragung zwei Fragen an den Kunden gestellt:[62]

- Fühlen Sie sich bei der derzeitig herrschenden Personendichte wohl?
- Fühlen Sie sich bei der derzeitig herrschenden Personendichte sicher?

Durch die Verwendung zweier unterschiedlicher Adjektive ist es möglich, eine unterschiedliche Ausprägung des Sicherheitsempfindens zu erheben. Weitere Einflussfaktoren auf das Sicherheitsempfinden wurden im Rahmen des Projekts aufgrund der begrenzten finanziellen, technischen und personellen Ressourcen nicht berücksichtigt, können aber durch das strukturierte und systematische Vorgehen jederzeit ergänzt werden.[63]

Schritt 4: Leistungscluster



Der nächste Schritt ist nun das Erstellen des Leistungsclusters gemäß Typ C[64], das die Prozesse, die Kundenkontaktpunkte, die Leistungen, die Merkmale und die Verantwortlichkeiten miteinander verknüpft, um somit die anschließende Auswertung der Befragungsdaten zu ermöglichen. Dabei wurden die Daten für das Leistungscluster im e-DeCoDe-Systemmodell des UNW abgebildet. Ziel hierbei ist eine einheitliche und standardisierte Informationsbasis für die nächsten Schritte.

Hierzu waren die bereits vorhandenen Daten bezüglich der Prozesse und Verantwortlichkeiten um die Leistungsmerkmale zu ergänzen und entsprechend zu verknüpfen. So wurden die für das Leistungscluster C relevanten Informationen (Prozesse, Kundenkontaktpunkte, Leistungen, Merkmale und Verantwortlichkeiten), wie in Abbildung 7 dargestellt, im e-DeCoDe-Systemmodell des UNW ergänzt und vernetzt.[65]

Bei der Erstellung des Leistungsclusters wurden zunächst die Leistungen der KVB und – der Vollständigkeit halber – die Leistungen der anderen Unternehmensnetzwerkpartner, die für die zu berücksichtigenden Szenarien relevant sind, aus dem e-DeCoDe-Modell entnommen und im Leistungscluster hinterlegt. Anschließend erfolgte die Auflistung der Merkmale und Indikatoren der Leistungen. Durch die daraus entstehende Matrix, die der e-DeCoDe-Matrix „Anforderung-Person" entspricht, konnten die einzelnen Leistungen in der Prozess-Matrix mit den Indikatoren verknüpft werden. An jedem dieser Verknüpfungspunkte konnten nun Fragen zum Erfüllungsgrad der Leistung bezüglich

58 | Vgl. Schlüter 2013.
59 | Vgl. ebd.
60 | Nähere Informationen zum Projekt unter www.versiert.info.
61 | Vgl. Schlüter 2013.
62 | Vgl. ebd.
63 | Vgl. ebd.
64 | Leistungsclustervariante, die speziell für jeden UNW-Partner bereitgestellt wird, um unter anderem Geheimhaltungsvereinbarungen nicht zu verletzen (Schlüter 2013).
65 | Vgl. Schlüter 2013.

der Sicherheit hinterlegt werden. Eine weitere Vernetzung erfolgte mit potenziell zur Befragung geeigneten Kundenkontaktpunkten, den Kundengruppen, den Zeitpunkten der Befragung und der Verantwortlichkeit durch die Unternehmensnetzwerkpartner[66] (Schlüter 2013). Die Notwendigkeit von separat für jeden Partner erstellten Leistungsclustern ohne Zugriff auf Leistungscluster anderer Partner ergab sich dabei aus den Geheimhaltungsbedingungen des UNW (siehe Abbildung 8).

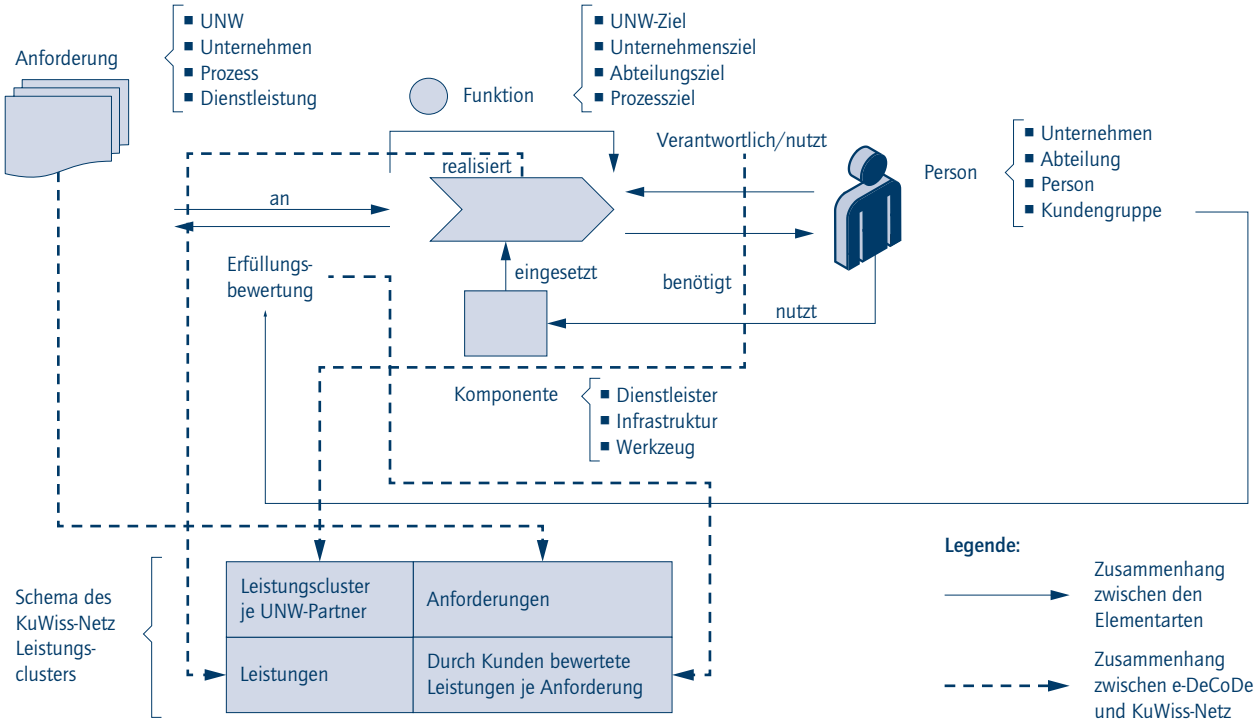
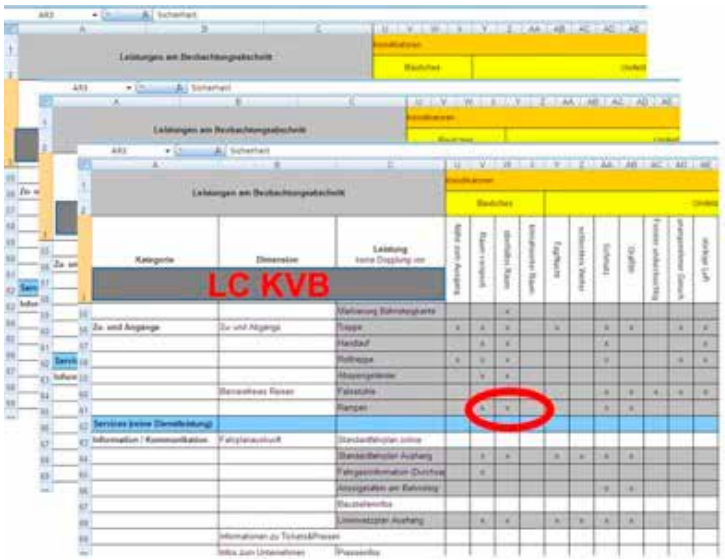


Abbildung 7: e-DeCoDe-Input für das Leistungscluster (Quelle: Schlüter 2017, S. 102)



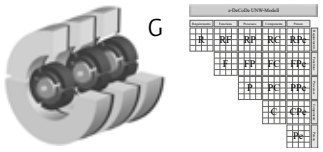
Attribute	Inhalt
ProzessID	34
UNWP	KVP
Ort	Köln Hbf
Zeit	15:30
Datum	16.04.2010
Event	BL-Spiel
Kundengruppe	Fan
Merkmal	Personendichte
Indikator	Sicherheitsgefühl

Abbildung 8: Beispielhafter Ausschnitt des implementierten Leistungsclusters (Quelle: nach Schlüter 2013, S. 71)

66 | Vgl. Schlüter 2013.

Da das Leistungscluster an sich bereits umfangreiche Dimensionen beinhaltet, ohne dass Befragungsdaten oder gar entsprechende Auswertungsmöglichkeiten durch die Hinterlegung von mathematischen Funktionen zur multi-kriteriellen Analyse weiter berücksichtigt werden, wurde zudem ein Softwaretool entwickelt, welches die Auswertung von Befragungsdaten ermöglicht. Dieses Tool wird im folgenden Schritt vorgestellt (Schlüter 2013).

Schritt 5: Datenbank



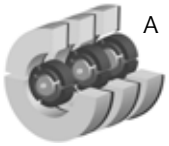
Das Softwaretool stellt die Nutzeroberfläche einer Datenbank dar, welche Leistungscluster mit den entsprechend benötigten Funktionen zum Anlegen von Clustern, Verknüpfungen von Verantwortlichkeiten, Kundenkontaktpunkten und Kundengruppen abbildet (siehe Abbildung 9).[67]

Abbildung 9: Screenshot der Software Cards & Lights – clWeb v1.0 (Quelle: nach Schlüter 2013)

Das Softwaretool kann Metadaten den einzelnen Zweigen der Baumstrukturen (je ein Baum für Unternehmensnetzwerkpartner, Kundengruppen, Prozesse, Kundenkontaktpunkte, Verantwortung etc.) zuweisen und diese mit Attributen belegen. Im Rahmen der Auswertung stehen die Attribute dann zur Verfügung. Zur besseren Übersicht wurden die Metadaten, die einen Überblick über die diversen Baumstrukturen beziehungsweise Dimensionen des Leistungsclusters geben, ebenfalls in einer Baumstruktur organisiert.[68]

Die Baumstruktur entspricht dabei der Hierarchie einer e-DeCoDe-Matrix, sodass die Software die nötigen Daten aus e-DeCoDe nutzen kann. Zudem können die Ergebnisse der Befragungsauswertung später wieder in e-DeCoDe überführt werden.[69]

Schritt 6: Befragung



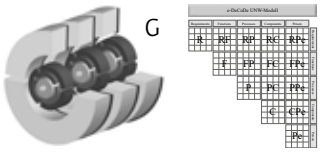
Ziel der Befragung war die Erhebung der subjektiv empfundenen Sicherheit des Fahrgastes. Dabei kann das Vorgehen prinzipiell auch für andere subjektive Empfindungen genutzt werden, die anschließend den in der Situation gemessenen Leistungsmerkmalen der Verlässlichkeit gegenübergestellt werden.

Die Befragungen zur Erhebung des Sicherheitsempfindens der Fahrgäste wurden am Kundenkontaktpunkt U-Bahnsteig Kölner Hauptbahnhof mit der Poll-Cards-Befragungstechnik durchgeführt, um den Anforderungen der Befragung (hohe Anzahl an Personen innerhalb von Sekunden befragen, ohne diese von der Weiterreise abzuhalten) zu entsprechen. Durch die Toolbox mit unterschiedlichsten fachspezifischen Befragungsmethoden setzt das Vorgehenskonzept dabei bereits die vom GSE geforderte zielgerichtete Methodenauswahl je konkrete Problemstellung innerhalb des Zielbildungsmoduls um.[70]

Insgesamt wurden sechs Befragungen durchgeführt. Hierbei wurden den U-Bahn-Fahrgästen nach Verlassen der U-Bahn Befragungskarten mit der Aufschrift „Fühlen Sie sich bei der aktuell vorherrschenden Personendichte sicher?" beziehungsweise „... wohl?" ausgehändigt, die von den Befragten in der Zwischenebene in eine Urne mit den Farben Rot (= Nein), Gelb (= Enthaltung) und Grün (= Ja) eingeworfen wurden. Durch Leerung der Urnen in festgelegten Zeitintervallen, die auf den Fahrplan der U-Bahnen abgestimmt waren, konnten die Befragungsergebnisse den einzelnen U-Bahnlinien und Kundengruppen (beispielsweise Fußballfan, wenn es sich um eine direkt vom Stadion kommende Einsatzbahn handelte) sowie den Kameramessdaten bezüglich der vorherrschenden Personendichte zugeordnet werden. Alle Messdaten wurden im Softwaretool hinterlegt, um im nächsten Schritt die Auswertung zu ermöglichen.[71]

67 | Vgl. Schlüter 2013.
68 | Vgl. ebd.
69 | Vgl. ebd.
70 | Vgl. ebd.
71 | Vgl. ebd.

Schritt 7: Datenauswertung



Die Auswertung der Messdaten erfolgt je Messtag und je Kundengruppencluster mittels der im Softwaretool hinterlegten multi-kriteriellen Auswertung. Insgesamt wurden Erkenntnisse bezüglich des unterschiedlichen Sicherheitsempfindens in Abhängigkeit von der vorherrschenden Personendichte für unter anderem Fußballfans analysiert.[72] Ein Beispiel für die Auswertung zeigt Abbildung 10.

Die Ergebnisse wurden vom Softwaretool in e-DeCoDe übertragen und dem für den genutzten Kundenkontaktpunkt verantwortlichen Partner, der KVB, präsentiert. Anschließend wurde das e-DeCoDe-Modell aktualisiert, sodass es für zukünftige Projekttätigkeiten auf dem neuesten Stand ist.[73]

Zwischenfazit

Auch wenn die Verknüpfung der Leistungscluster der einzelnen Unternehmensnetzwerkpartner in der Software aus Zeitgründen nicht mehr erfolgte, konnte mithilfe der systematischen Vorgehensweise des DyNamic-Ansatzes zur Messung des Sicherheitsempfindens dennoch erreicht werden, dass netzwerkpartnerübergreifende Kundenanforderungen und Leistungen der Verlässlichkeit, den betreffenden Verantwortlichen und den Kundenkontaktpunkten unter Berücksichtigung der Geheimhaltung zugeordnet werden konnten. In Zukunft ist somit eine detaillierte Analyse der Zusammenhänge von Ursache (Leistungserbringung) und Wirkung (Sicherheitsempfinden/Kundenzufriedenheit) trotz der Komplexität und Intransparenz von UNW möglich.[74]

Dabei können Kundenanforderungen aller Art aus dem Themenbereich Sicherheit oder darüber hinaus bezüglich ihres Erfüllungsgrads beim Kunden überprüft werden. Dies ist durch die systematische Vorgehensweise vom Abstrakten zum Detail über die Prozessebenen des zu betrachtenden Systems möglich.

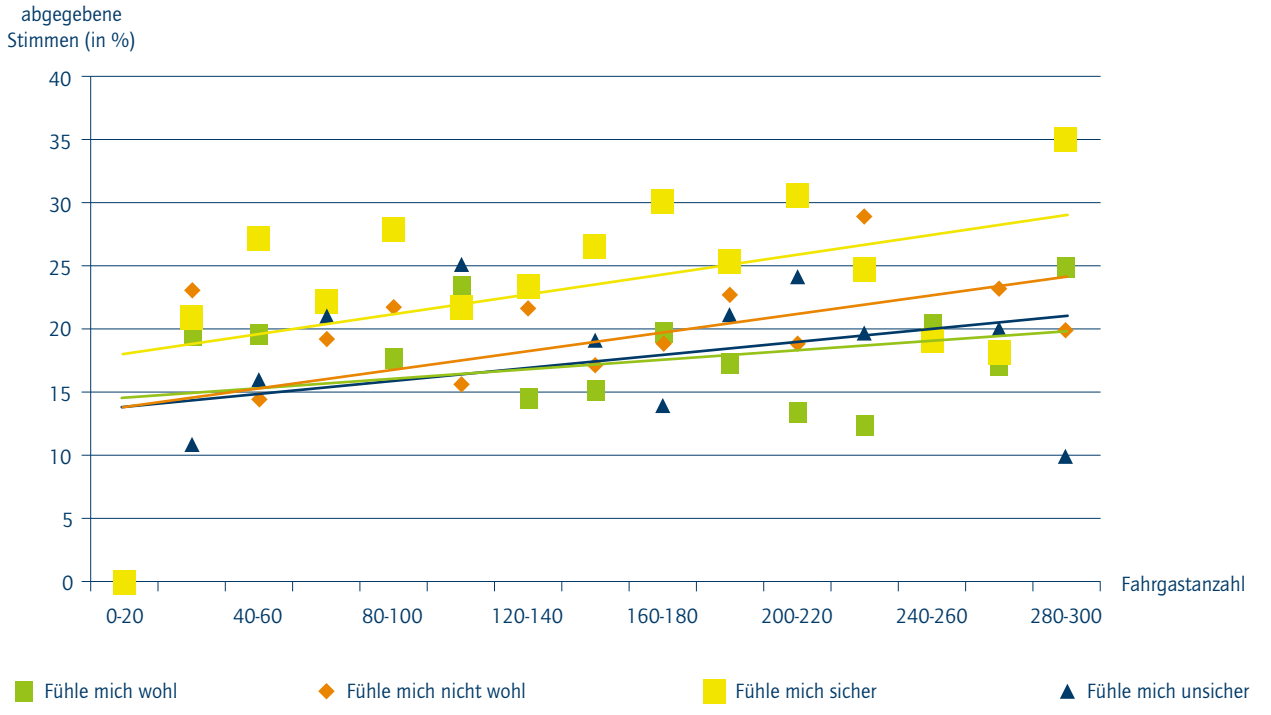


Abbildung 10: Sicherheitsempfinden von Fahrgästen am Kölner Hauptbahnhof (23.05.2009, N = 4.397, n = 169) (Quelle: nach Schlüter 2013)

72 | Vgl. Schlüter 2013.
73 | Vgl. ebd.
74 | Vgl. ebd.

Durch die kontinuierliche Hinterlegung neu gewonnener Erkenntnisse aus dem Vorgehenskonzept in das e-DeCoDe-Denkmodell werden alle Informationen für das Projektteam bereitgestellt. Für die Nutzung der gewonnenen Befragungsdaten ist allerdings die Verwendung von Software mit entsprechend implementierten Nutzungsrechten empfehlenswert, um die Geheimhaltungsbedingungen eines solchen Projekts zu erfüllen. Das bedeutet, dass e-DeCoDe mit dem Gesamtabbild des Netzwerks nur vom Projektteam genutzt wird, während begrenzte Sichten auf das System, die aus dem e-DeCoDe-Modell gespeist werden, für die jeweiligen UNW-Partner mittels des Softwaretools bereitgestellt werden.

6 Fazit

Das Systems Engineering ist eine Wissenschaftsdisziplin, die sich in den letzten Jahrzehnten stark den fachspezifischen Bedürfnissen angepasst hat. Diese Diversitätsentwicklung hat allerdings zur Konsequenz, dass keine Basis für einen fachdisziplinübergreifenden Lösungsansatz bei komplexen Problemen existiert – dies ist jedoch gerade für das komplexe und interdisziplinäre Forschungsthema der Sicherheit gefragt. Dementsprechend wurde im vorliegenden Beitrag das Generic Systems Engineering vorgestellt. Es wird aufgezeigt, warum es entwickelt wurde und wie es Interdisziplinarität, die Handhabung von Komplexität und eine einheitliche Modellierung von Systemen ermöglichen kann. Veranschaulicht wurde dies am Beispiel „Messung des Sicherheitsempfindens im ÖPNV".

Doch ist das gewählte Beispiel nur ein kleiner Bestandteil des umfassenden Themenfelds der Sicherheit, wie dieser acatech Band zeigt. Infolgedessen ist zu prüfen, ob das Generic Systems Engineering auch als Rückgrat für eine Systemtheorie der Sicherheitswissenschaften geeignet ist beziehungsweise ob es zu einer solchen weiterentwickelt werden kann. Erste Anwendungsbeispiele für des Generic Systems Engineering zeigen, wie auch in diesem Artikel im Abschnitt 5 an einem Beispiel illustriert, dass Sicherheit und Zuverlässigkeit von Systemen in interdisziplinären Teams sehr zielorientiert und systematisch mithilfe des Generic Systems Engineering gestaltet werden können. Auch ist zu prüfen, ob das GSE eine mögliche Basis sein kann, um die von Bertsche et al. gestellten Forschungsfragen bei der Gewährleistung der Verlässlichkeit von soziotechnischen Systemen zu lösen.[75]

Doch während das GSE ein systematisches und zielgerichtetes Vorgehen zur Lösung von Problemen in interdisziplinären Teams ermöglicht, sind konkrete Detailfragen bezüglich der problemspezifischen Vorgehenskonzepte weiter zu erforschen. Im präsentierten Beispiel wurden alle befragten Fahrgäste als Menschen betrachtet, die es zu beschützen gilt. Beyerer fordert hingegen, bei der Modellierung der Sicherheit von Systemen die Rolle des Menschen im System beziehungsweise in seinem Umfeld genauer zu definieren.[76] Der Mensch kann

a) der zu Beschützende (Safety) im System und

b) der Gefährder (Security) für das System und sein Umfeld sein.[77]

Der Fall a) erfordert ein ganz anderes systemtheoretisches Vorgehen als der Fall b), obwohl das System mit den gleichen Elementen beschrieben werden kann. Die Rolle des Systemelements „Mensch", welche sich in den Fällen a) und b) ändert, erfordert jeweils andere Lösungskonzepte.[78] Raabe erweitert dieses Rollenkonzept des Menschen um den Entscheider und den Verantwortlichen,[79] und Labudde spricht von einem Multi-Agenten-System.[80] Folglich muss in der weiteren Forschungsarbeit im Rahmen der Systemtheorie der Sicherheit geklärt werden, welche definierten Rollen der Mensch in diesem soziotechnischen System einnehmen kann und wie dies zu modellieren ist, um gezielte Prognosen beziehungsweise Veränderungen ableiten zu können.

Auch bezüglich der Modellierung ergibt sich weiterer Forschungsbedarf. So ist zu hinterfragen, wie ein Modell zu gestalten ist, wenn davon auszugehen ist, dass ein interdisziplinäres Team die Sicherheit von soziotechnischen Systemen gewährleisten soll. Labudde schlägt zwei standardisierte Sichten – die Ebene der mobilen Agenten und die Ebene der fixierten Objekte – vor.[81] Weyer et al. fordern die Beschreibung von technischen, sozialen sowie organisatorischen Aspekten,[82] und Schlüter/Winzer favorisieren im vorliegenden Beitrag fünf Sichten zur

75 | Vgl. Bertsche et al. 2018.
76 | Vgl. Beyerer/Geisler 2018.
77 | Vgl. Beyerer/Geisler 2018, Lichte/Wolf 2018, Arens/Kühne 2018.
78 | Vgl. ebd.
79 | Vgl. Raabe 2018.
80 | Vgl. Labudde 2018.
81 | Vgl. ebd.
82 | Vgl. Weyer et al. 2018.

standardisierten Abbildung von Systemen, nämlich die Anforderungs-, die Funktions-, die Komponenten-, die Prozess- und die Personensicht. Das Modell darf aber nicht nur eine Analysefunktion haben, sondern muss auch gleichzeitig Optimierungs-, Bewertungs-, Gestaltungs- und Prognosefunktionen erfüllen. Dazu ist es auch erforderlich, die Beschreibungstiefe dieses Modells zu fixieren.[83]

Soll die Sicherheit eines Systems gewährleistet werden, so muss der Begriff der Sicherheit zunächst geklärt und einheitlich definiert werden.[84]

Dies ist die Voraussetzung, um die verschiedensten sicherheitsrelevanten Anforderungen, die an ein System gestellt werden, vergleichend und interdisziplinär betrachten zu können. Dazu sind noch zu erarbeitende Metriken der Sicherheit eine grundlegende Voraussetzung.[85] Aber auch unterschiedliche Rechtsauffassungen (sicherheitsrechtliche Anforderungen an ein System) bedürfen eines Abgleichs.[86] Viewegs Forderung, dass neben der begrifflichen Klärung auch eine Transparenz des methodischen Vorgehens zur Gewährleistung der Sicherheit von Systemen erforderlich ist, ist unbedingt zu unterstützen. Da interdisziplinäre Teams dies gewährleisten müssen, darf dieses methodische Vorgehen nicht fachspezifisch sein. Insofern ist zu prüfen, ob das GSE diesem Anspruch genügt.

Da die Systeme, für die Sicherheit zu gewährleisten ist, unterschiedlich komplex sein können, muss das Denkmodell es zudem gestatten, bestimmte Elemente des Systems in unterschiedlicher Genauigkeit und über mehrere Ebenen zu modellieren.[87] Hieraus ist abzuleiten, dass es für ein interdisziplinäres Systems Engineering essenziell ist, dass systemtheoretischen Prinzipien wie „vom Groben zum Detail", die die Handhabung von Komplexität ermöglichen, gefolgt wird und diese nicht fachspezifischen Bedürfnissen zum Opfer fallen. Nur wenn die Rückkehr zu einem interdisziplinären, systemtheoretisch fundierten und modellbasierten Ansatz für das weite Themenfeld der Sicherheit gelingt, wird es möglich sein, die komplexen Aufgabenstellungen der Zukunft für alle Beteiligten zufriedenstellend zu lösen.

83 | Vgl. Schnieder/Schnieder 2018.
84 | Vgl. Bertsche et al. 2018, Schnieder/Schnieder 2018, Raabe 2018, Vieweg 2018.
85 | Vgl. Schnieder/Schnieder 2018.
86 | Vgl. Vieweg 2018, Raabe 2018.
87 | Für sehr komplexe Systeme siehe Beitrag von Weyer et al. 2018; für einfache Systeme siehe Beitrag von Gleirscher 2018.

Literatur

Albers et al. 2014
Albers, A./Matthiesen, S./Urosac, N./Moeser, G./Schmidt, S./Lüpcke, R.: „Abstraktionsgrade der Systemmodellierung – von der Sprache zur Anwendung". In: Maurer, M. S./Abulawi, J./Schulze, S. (Hrsg.): *Tag des Systems Engineering* (Bremen 12. bis 14. November 2014), München: Hanser 2014, S. 183–192.

Alt 2014
Alt, U.: „Modellbasiertes Systems Engineering und seine Technologien als Schlüssel für Industrie 4.0". In: Maurer, M. S./Abulawi, J./Schulze, S. (Hrsg.): *Tag des Systems Engineering* (Bremen 12. bis 14. November 2014), München: Hanser 2014, S. 3–10.

Arens/Kühne 2018
Arens, U./Kühne, U.: „Schutz und Sicherheit in Offshore-Windparks". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Bahill/Gissing 1998
Bahill, T./Gissing, B.: „Re-evaluating Systems Engineering Concepts Using Systems Thinking". In: IEEE (Hrsg.): *IEEE Transactions on Systems Man and Cybernetics Part C* (Application and Reviews), Part C, 1998, S. 516–527.

Balzert 1998
Balzert, H.: *Lehrbuch der Software-Technik*, Heidelberg: Spektrum Akad. Verlag 1998.

Bertsche et al. 2018
Bertsche, B./Beyerer, J./Goldschmidt, R./Jakobs, E. M./Renn, O./Schlüter, N./Winzer, P./Weyer, J.: „Integrative Theorie der Verlässlichkeit (iTV) für soziotechnische Systeme (STS)". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Beyerer et al. 2010
Beyerer, J./Geisler, J./Dahlem, A./Winzer, P.: „Sicherheit – Systemanalyse und Design". In: Winzer, P./Schnieder, E./Bach, F.-W. (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven* (acatech DISKUTIERT), Heidelberg: Springer Verlag 2010, S. 39–72.

Beyerer/Geisler 2018
Geisler, J./Beyerer, J.: „Formaler Rahmen für eine einheitliche quantitative Beschreibung des Risikos bezüglich Safety und Security". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Brujin/Herder 2009
Brujin, J. A./Herder, P. M.: *System and Actor Perspectives on Sociotechnical Systems. IEEE Transactions On Systems Man And Cybernetics Part A-Systems And Humans*, 39: 5, 2009, S. 981–992.

DAG 2010
DAG: Defense Acquisition Guidebook 2010. URL: https://dag.dau.mil [Stand: 11.03.2013].

Dalhöfer/Rall 2009
Dalhöfer, J./Rall, K.: *Komplexitätsbewertung indirekter Geschäftsprozesse*, Aachen: Shaker 2009.

Dimario 2010
Dimario, M. J.: *Systems of Systems Collaboration Formation* (Systems Research Series), Vol. 1.1, Singapur: World Scientific Publishing Co. Pteltd. 2010.

Dumitrescu et al. 2014
Dumitrescu, R./Fechtelspeter, Ch./Kühn, A.: „Systematische Berücksichtigung von Fertigungsanforderungen im Model-Based Engineering". In: Maurer, M. S./Abulawi, J./Schulze, S. (Hrsg.): *Tag des Systems Engineering* (Bremen, 12. bis 14. November 2014), München: Hanser 2014, S. 21–32.

Ehrlenspiel 2003
Ehrlenspiel, K.: *Integrierte Produktentwicklung; Denkabläufe, Methodeneinsatz, Zusammenarbeit*, München: Hanser Verlag 2003.

Fuchs et al. 2001
Fuchs, M./Lersch, F./Pollehen, D. (Hrsg.): *Neues Rollenverständnis für die Entwicklung verteilter Systemverbunde in der Karosserie- und Sicherheitstechnik* (VDI-Berichte), Düsseldorf 2001.

Gausemeier et al. 2013
Gausemeier, J./Gaukstern, T./Tschirner, C.: „Systems Engineering Management Based on a Discipline-Spanning System Model". In: Paredis, C. J. J./Bishop, C./Bodner D. (Hrsg.): *Conference on Systems Engineering Research, Proceedings*, Elsevier B.V. 2013.

Gleirscher 2018
Gleirscher, M.: „Strukturen für die Gefahrenerkennung und -behandlung in autonomen Maschinen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Grammel/Kastenholz 2010
Grammel, B./Kastenholz, S.: „A Generic Traceability Framework for Facet-Based Data Extraction in Model-Driven Software Development". In: *ECMFA-TW Proceedings*, New York: ACM 2010, S. 7–14.

Haskin et al. 2011
Haskin, C./Krueger, M./Forsberg, K./Walden, D./Hameling, R. D.: *Systems Engineering Handbook V3.2.2*, TP-2002-002-03.2.2. INCOSE, San Diego, USA 2011.

Haberfellner et al. 2012
Haberfellner, R./Vössner, S./Weck, O./Fricke, E.: *Systems Engineering. Grundlagen und Anwendung*, Zürich: Orell Füssli 2012.

Haberfellner/Daenzer 2002
Haberfellner, R./Daenzer, W. F.: *Systems Engineering – Methodik und Praxis*, Zürich: Verlag Industrielle Organisation 2002.

Haberfellner/Daenzer 1999
Haberfellner, R./Daenzer, W. F.: *Systems Engineering – Methodik und Praxis*, Zürich: Verlag Industrielle Organisation 1999.

Hanenkamp 2004
Hanenkamp, N.: *Entwicklung des Geschäftsprozesses. Komplexitätsmanagement in der kundenindividuellen Serienfertigung; ein Beitrag zum Informationsmanagement in mehrdimensional modellierten Produktionssystemen*, Aachen: Shaker 2004.

Heinrich 2015
Heinrich, H.: *Systemisches Projektmanagement. Grundlagen, Umsetzung, Erfolgskriterien*, München: Hanser Verlag 2015.

Hinrichsen/Pritchard 2005
Hinrichsen, D./Pritchard, A. J.: *Mathematical Systems Theory I; Modelling, State Space Analysis, Stability and Robustness*, Berlin, Heidelberg: Springer Verlag 2005.

Huber 2014
Huber, M.: „Ansatz zur Nutzung vernetzter virtueller Produktmodelle für die kundenintegrierte Produktentwicklung". In: *Schriftenreihe des Instituts Product and Service Engineering*, Ruhr-Universität Bochum, Bochum 2014.

IEC 61508:1998
IEC 61508:1998: International Electrotechnical Commission (Hrsg.): *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, 1998.

IEEE 1220-2005
IEEE Std 1220-2005: *IEEE Standard for Application and Management of the Systems Engineering Process*. IEEE Computer Society, IEEE: New York, 2005.

INCOSE 2006
INCOSE (2006): *What is Systems Engineering? A Consensus of the INCOSE Fellows. International Council on Systems Engineering*, Seattle 2006. URL: http://www.incose.org/practice/fellowsconsensus.aspx. [Stand: 21.09.2012].

INCOSE 2007
INCOSE: *Systems Engineering Vision 2020*, INCOSE-TP-2004-004-02 (Version/Revision: 2.03), 2007 und INCOSE 2015. URL: http://www.incose.org/Home/ [Stand: 13.12.2015].

ISO/IEC/IEEE 42010:2011
ISO/IEC/IEEE 42010:2011: *System- und Software-Engineering – Architekturbeschreibung*, Berlin: Beuth Verlag 2011.

Jackson 2000
Jackson, M. C.: *Systems Approaches to Management*, New York: Kluwer Academic/Plenum 2000.

Jamshidi 2009
Jamshidi, M.: „Introduction to Systems of Systems". In: Jamshidi, M. (Hrsg.): *Systems of Systems Engineering Innovations for the 21th Century*, New Jersey, Hoboken: John, Wiley & Sons Inc. 2009.

Jing et al. 2013
Jing, Z./Ming-Yang, W./Wie, L./Jan, H./Li-Qun, Y./Ze-Min, L./Qin-Zhang, Y.: „Enormal Approach auf SOS Modelling und Comprehensive Evaluation based Ontology". In: *Proceedings of the 8th International Conference on Systems of Systems Engineering*, Mauwi, Hawaii, USA 2013.

Keating et al. 2003
Keating, C./Roger, R./Ruault, R./Dreier, D./Sousa-Poza, A./Safford, R./Petersen, W./Rabadi, G.: „System of Systems Engineering". In: *Engineering Management Journal* (ENJ), 15: 3, 2003.

Labudde 2018
Labudde, D.: „Sicherheit ist die Abwesenheit von Kriminalität – eine Hypothese". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Lamm/Weilkiens 2014
Lamm, J. G./Weilkiens, T.: „Method for Deriving Functional Architectures from Use Cases". In: *Systems Engineering*, 17: 2, 2014, S. 225–236.

Lichte/Wolf 2018
Lichte, D./Wolf, K.-D.: „Quantitative Analyse der Vulnerabilität am Beispiel Verkehrsflughafen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Lim/Ncube 2013
Lim, S. L./Ncube, C.: „Social Networks and Outsourcing for Stakeholder Analysis for Systems of System Projects". In: *Proceedings of the 8th Conference of Systems of Systems Engineering*, Mauwi, Hawaii, USA, 2013.

Lindemann 2005
Lindemann, U.: *Methodische Entwicklung technischer Produkte; Methoden flexibel und situationsgerecht anwenden*, Berlin: Springer 2005.

Ludwig 2001
Ludwig, B.: *Management komplexer Systeme; der Umgang mit Komplexität bei unvollkommener Information: Methoden, Prinzipien, Potentiale*, Berlin: Ed. Sigma 2001.

Luhmann 1980
Luhmann, N.: *Komplexität. Enzyklopädie der Betriebswirtschaftslehre*, Stuttgart: Poeschel 1980.

Luzeaux/Ruault 2010
Luzeaux, D./Ruault, J. R. (Hrsg.): *Systems of Systems*, Hoboken, New Jersey, USA: John, Wiley & Sons Inc. 2010.

Maier 2005
Maier, M. W.: Research *Challenges for Systems of Systems in Systems, Man und Cybernetics* (IEEE International Conference), 4, 2005, S. 3149–3157.

Mamrot et al. 2014
Mamrot, M./Marchlewitz, S./Nicklas, J. P./Winzer, P.: *Using Systems Engineering for a Requirement-Based Design Support for Autonomous Robots* (IEEE International Conference on Systems, Man, and Cybernetics, October 5-8, 2014), San Diego, CA, USA 2014, S. 3146–3151.

Ncube et al. 2013
Ncube, C./Linn, S. L./Dogan, H.: „Identifying Top Challenges for international Research on Requirements Engineering for Systems of Systems Engineering". In: *Requirements Engineering Conferences*, 2013.

Nicklas 2016
Nicklas, J.-P.: *Ansatz für ein modellbasiertes Anforderungsmanagement für Unternehmensnetzwerke* (Berichte zum Generic-Management 2016, 2), 1. Auflage, Herzogenrath: Shaker 2016.

Nicklas et al. 2016
Nicklas, J. P./Marchlewitz, S./Winzer, P.: „Generic Systems Engineering zur Unterstützung des Requirements Engineering in Unternehmensnetzwerken". In: Maurer, M./Schulze, S. O. (Hrsg.): *Tag des Systems Engineering* (Proceedings Systems Engineering Konferenz, Bremen, 12. bis 14. November 2014), Carl Hanser Verlag 2016, S. 383–392.

Oppenheim 2011
Oppenheim, B. W.: *Lean for Systems Engineering with Lean Enablers for Systems Engineering*, Hoboken, New Jersey, USA: John Wiley & Sons 2011.

Ott 2009
Ott, S.: *Konzept zur methodischen Systemmodellierung in der anforderungsgerechten Produktentwicklung,* Aachen: Shaker 2009.

Padilla et al. 2008
Padilla, J. J./Logan, B./Sousa-Poza, A./Keating, C. B.: „A Systems of Systems Engineering Environment to Deal with Complex Situation". In: *Systems of Systems Engineering Conference* (SoSE), IEEE, 2008.

Pahl et al. 2005
Pahl, G./Beitz, W./Feldhusen, J./Grote, K.: *Konstruktionslehre; Grundlagen erfolgreicher Produktentwicklung – Methoden und Anwendung*, Berlin, Heidelberg: Springer 2005.

Raabe 2018
Raabe, O.: „Datenschutz- und IT-sicherheitsrechtliche Risikomodelle". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Rink 2002
Rink, A. W.: *Entwicklung einer Methode für die systemtechnische Auslegung verteilter und sicherheitskritischer Führungsfunktionen für Fahrzeugantriebe* (Dissertation), Bergische Universität Wuppertal, 2002.

Ropohl 2012
Ropohl, G.: *Allgemeine Systemtheorie – Einführung in transdisziplinäres Denken*, Berlin: Edition Sigma 2012.

Sahen et al. 2009
Sahen, F./Jamshidi, M./Sridhaer, P.: „Systems of Systems Simulation Frame Work and its applications". In: Jamshidi, M. (Hrsg.): *Systems of Systems Engineering, Principals und Applications*, Bocaarton, FL: CRC Press Taylor und Transis Group 2009.

Sage/Rouse 2009
Sage, A. P./Rouse, W. B. (Hrsg.): *Handbook of Systems Engineering and Management*, Hoboken, New Jersey, USA: John Wiley & Sons, 2009.

Schenk 2004
Schenk, M.: *Fabrikplanung und Fabrikbetrieb; Methoden für die wandlungsfähige und vernetzte Fabrik*, Berlin, Heidelberg: Springer-Verlag 2004.

Schnieder/Schnieder 2013
Schnieder, E./Schnieder, L.: *Verkehrssicherheit; Maße und Modelle, Methoden und Maßnahmen für den Straßen- und Schienenverkehr*, Wiesbaden: Springer Vieweg 2013.

Schnieder/Schnieder 2018
Schnieder, E./Schnieder, L.: „Formalisierung von Begriffen der Sicherheit und Sicherheitsmetriken". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schuh 2007
Schuh, G.: *Effizient, schnell und erfolgreich; Strategien im Maschinen- und Anlagenbau*, Frankfurt am Main: VDMA-Verlag 2007.

Schuldt 2003
Schuldt, C.: *Systemtheorie*, Hamburg: Europäische Verlagsanstalt 2003.

Schlüter/Sochacki 2012
Sochacki, S./Schlüter, N.: „Qualitative Netzwerkanalyse hinsichtlich der Anwendbarkeit von KuWiss-Netz". In: Winzer, P. (Hrsg.). *Generic Systems Engineering als Basis für die Weiterentwicklung des WGMK-Modells* (Berichte zum Generic-Management 02/2012), Aachen: Shaker Verlag, 2012, S. 79–107.

Schlüter/Winzer 2015
Schlüter N./Winzer, P.: „Systems Engineering für die Entwicklung der Theorie zu Verlässlichkeit von Systemen". In: Schulze, S.-O./Muggeo, C. (Hrsg.): *Tag des Systems Engineering – Verteiltes Arbeiten mit ganzheitlicher Kontrolle*, München: Hanser Verlag 2015.

Schlüter 2013
Schlüter, N.: „Entwicklung einer Vorgehensweise zur Implementierung einer forderungsgerechten Kundenzufriedenheitsmessung in Unternehmensnetzwerken". In: *Berichte zum Generic-Management*, 2013: 1, Aachen: Shaker 2013.

Schlüter 2017
Schlüter, N.: *Der Dynamic-Ansatz – Entwicklung eines Ansatzes zur verlässlichen Gestaltung von Unternehmensnetzwerken und ihren Produkt-Service-Systemen* (Habilitationsschrift), Fakultät für Maschinenbau und Sicherheitstechnik, Bergische Universität Wuppertal 2017.

Sell 1989
Sell, R.: *Angewandtes Problemlösungsverhalten. Denken und Handeln in komplexen Zusammenhängen*, 2. Auflage, Berlin: Springer 1989.

Sitte/Winzer 2011
Sitte, J./Winzer, P.: „Systemmodellierung im Fokus von Generic Systems Engineering". In: Gesellschaft für Systems Engineering e. V. (Hrsg.): *Tag des Systems Engineering 2011*.

Sommerville 2005
Sommerville, J.: *Integrated Requirements Engineering: A Tutorial*, IEEE 2005.

Sommerville 2007
Sommerville, J.: *Software Engineering*, München: Verlag Pearson Studium 2007.

VDI 2221
VDI-Richtlinie 2221 – *Methodik zum Entwickeln und Konstruieren technischer Systeme und Produkte*, Berlin: Beuth Verlag 1993.

VDI 2247
VDI-Richtlinie 2247: *VDI-Gesellschaft Produkt- und Prozessgestaltung – Qualitätsmanagement in der Produktentwicklung*, Berlin: Beuth Verlag 1994.

Vieweg 2018
Vieweg, K.: „Sicherheit – Begriffe, Szenarien, Verantwortlichkeiten und Entscheidungsprozesse aus juristischer Sicht". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Weilkiens 2007
Weilkiens, T.: *Systems Engineering with SysML; Modeling, Analysis, Design*, Amsterdam: Morgan Kaufmann OMG Press/Elsevier 2007.

Weiss 2013
Weiss, S. I.: *Product und Systems Development Evalu Approach*, Hoboken, New Jersey, USA: John Wiley & Sons 2013.

Weyer et al. 2018
Weyer, J./Adelt, F./Konrad, J./Hoffmann, S.: „Agentenbasierte Simulation des Risikomanagements soziotechnischer Systeme mit dem Simulator SimCo". In: Beyerer, J./Winzer, P. (Hrsg.): B*eiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Wiendahl et al. 2009
Wiendahl, H./Reichardt, J./Nyhuis, P.: *Handbuch Fabrikplanung; Konzept, Gestaltung und Umsetzung wandlungsfähiger Produktionsstätten*, München: Hanser Verlag 2009.

Winzer 1997
Winzer, P.: *Chancen zur umfassenden Unternehmensgestaltung; Methodischer Ansatz zur qualitäts-, human- und ökologieorientierten Gestaltung von Arbeits- und Fabriksystemen*, Frankfurt am Main: Lang 1997.

Winzer 2013
Winzer, P.: *Generic Systems Engineering – Ein methodischer Ansatz zur Komplexitätsbewältigung*, Wiesbaden: Springer Vieweg Verlag 2013.

Winzer 2016
Winzer, P.: *Generic Systems Engineering. Ein methodischer Ansatz zur Komplexitätsbewältigung*, 2. Auflage, Berlin: Springer 2016.

Wulf 2002
Wulf, J.: *Elementarmethoden zur Lösungssuche*, München: Verlag Dr. Hut 2002.

Züst 2004
Züst, R.: *Einstieg ins Systems Engineering: Optimale, nachhaltige Lösungen entwickeln und umsetzen*, Zürich: Verlag Industrielle Organisation 2004.

3 Formalisierung von Begriffen der Sicherheit und Sicherheitsmetriken

Prof. Dr.-Ing. Eckehard Schnieder
Institutsleiter im Ruhestand
Technische Universität Braunschweig

Dr.-Ing. Lars Schnieder
ESE Engineering und Software-Entwicklung GmbH

1 Einleitung und Motivation

Sicherheit ist nach unmittelbaren physiologischen Bedürfnissen das höchste menschliche Bedürfnis.[1] Trotz dieses allgemeinen Verständnisses ist jedoch die Interpretation des Sicherheitsbegriffs in den verschiedenen Sprachen und Fachdisziplinen zum Teil sehr unterschiedlich.[2] Daher erscheint es zweckmäßig, den Sicherheitsbegriff im jeweiligen Kontext bewusst zu definieren. Darüber hinaus ist es wissenschaftlich interessant, ob dem Verständnis ein übergeordneter einheitlicher begrifflicher Kern zugrunde liegt oder ob ein solcher entwickelt werden kann. Auf dieser Grundlage kann möglicherweise eine Quantifizierung zur Gestaltung und Beurteilung sicherer Systeme erfolgen.

Im allgemeinen Kontext der Sicherheit sind die folgenden Begriffe gebräuchlich (hier in alphabetischer Reihenfolge angegeben): Ausfall, Diagnose, Eintrittswahrscheinlichkeit, Ereignis, Gefahr, Gefährdung, Gefährder, Gefährlichkeit, Integrität, Kontaminierung, Kontrollierbarkeit, Korrektheit, Kriminalität, Resilienz, Risiko, Safety, Schaden, Schadensart, Schadensausmaß, Schadenshäufigkeit, Schadensminderung, Schädigung, Schutz, Security, Sicherheit, Sicherung, Verlässlichkeit, Versicherung, Widerstandsfähigkeit, Wiederherstellung.

Diese Begriffe stehen in vielfältigen begrifflichen Beziehungen zueinander, deren Komplexität man sich anfangs nicht immer bewusst ist. Weiterhin bestehen in einer gesprochenen Sprache sehr viele Ausdrucksmöglichkeiten für Beziehungen, die nicht alle mit mathematischen Relationen formalisiert werden können. Eine gezielte Erforschung von Begriffsbeziehungen bringt jedoch Klarheit in die Zusammenhänge und zielt auf ein konsistentes formalisiertes Begriffsgebilde als Grundlage einer Theorie. Hierbei werden wie in der Entwicklung jeder wissenschaftlichen Disziplin mehrere aufeinander aufbauende Phasen durchlaufen:

- In einer **ersten Phase** beginnt jede Entwicklung wissenschaftlicher Disziplinen, beispielsweise der Mechanik oder Elektrotechnik, zuerst mit der Präzisierung elementarer Begriffe.
- In einer **zweiten Phase** werden die elementaren Begriffe dann mehr oder weniger erfolgreich in Beziehung zueinander gesetzt.[3]
- In einer **dritten Phase** erfolgt eine formalisierte Darstellung der Begriffe und der zwischen ihnen bestehenden Relationen im Rahmen einer geschlossenen Theorie. Hierbei zeigt sich die Ausdrucksstärke von Begriffsgebilden dank effizienter Beschreibung und plausibler Erklärung.
- In einer **vierten Phase** tritt der interdisziplinäre Diskurs in den Vordergrund. Die Wissenschaften vernetzen sich zunehmend zur Lösung komplexer Problemstellungen. Dies erfordert eine domänenübergreifende Terminologiearbeit.

Eine Theorie der Verlässlichkeit kann dabei wesentlich auf die in den letzten Jahrzehnten entwickelte Theorie der Zuverlässigkeit aufbauen (dritte Phase). Um zunehmend interdisziplinären Bezügen zu entsprechen, müssen aber auch die in jüngerer Zeit entwickelten Begriffe und Konzepte der Resilienz, der Security und der Korrektheit aus anderen technischen Disziplinen, den Gesellschaftswissenschaften, der Jurisprudenz und weiteren Fachdisziplinen berücksichtigt und einbezogen werden (erste und zweite Phase). Insgesamt kristallisiert sich somit in der gegenwärtigen vierten Phase eine Integration der Zuverlässigkeit und Sicherheit unter Einschluss des betreffenden Kontextes anderer Disziplinen und somit eine Theorie der Verlässlichkeit (im Englischen: Dependability) heraus.

Allgemeines und entsprechend auch hier verfolgtes Ziel einer wissenschaftlichen Theorie ist es, eine genügend genaue Beschreibung und Erklärung der realen und angenommenen Phänomene und Beobachtungen zu geben. Basis sind ein axiomatisches Fundament und die Verwendung von passenden Modellkonzepten. Dies beinhaltet eine vollständige und konsistente (am besten mathematische) Beschreibung der Mengen an Entitäten und ihrer strukturellen Beziehungen. Mit diesem

1 | Vgl. Maslow 1943.
2 | Vgl. Schnieder/Yurdakul 2016.
3 | Vgl. Menne 1992.

Anspruch sind in letzter Konsequenz auch die Definition und Quantifizierung von Größen verbunden, die in Zusammenhang mit den Begriffen der Verlässlichkeit stehen. Dies wird zuerst durch eine sprachliche Formulierung und eine anschließende Formalisierung auf der Grundlage von mathematischen Theorien ermöglicht. Die mathematische Fundierung gestattet wiederum die Formulierung von Hypothesen, die dann validiert werden können und zu reproduzierbaren Gesetzmäßigkeiten führen. In Bezug auf ihre Methodik umfasst eine Theorie auch Verfahren der Analyse und Synthese der Domäne. Eine weitreichende Zielsetzung besteht darin, technische und soziotechnische Systeme mit definierter Sicherheit zu planen und zu gestalten.

2 Begriffsbildung und -modellierung

Im Mittelpunkt jeder theoretischen Beobachtung steht die Klärung ihrer Domäne, in diesem Fall der Betriebssicherheit (im Englischen: *safety*) und der Angriffssicherheit (im Englischen: *security*).[4] Für die präzise Definition dieser beiden Sichten auf Sicherheit – in den meisten Sprachen vertreten durch einen umfassenden Begriff – ist die Verwendung eines umfassenden Begriffskonzepts zweckmäßig, welches die aus einem einfacheren Begriffskonzept herrührenden Missverständnisse zu vermeiden hilft. Dieses neue Begriffskonzept – in der Fachsprache der Linguistik auch als Zeichenmodell bezeichnet – ist das trilaterale varietätsbezogene Zeichenmodell und darüber hinaus die vierschichtige Abstraktionshierarchie mit Merkmalen, Größen und Werten zusammen mit (physikalischen) Einheiten auf der strukturalistischen Grundlage von Carnap.[5] Auf dieser Grundlage können mithilfe von Modellkonzepten und formalen Beschreibungsmitteln dann konsistente und formale Modelle sowie quantitative Berechnungsverfahren entstehen.

2.1 Trilaterales Zeichenmodell

Begriffe werden nach DIN 2342 definiert als „Denkeinheit, die aus einer Menge von Gegenständen unter Ermittlung der diesen Gegenständen gemeinsamen Eigenschaften mittels Abstraktion gebildet wird". Begriffe dienen dem Erkennen von Gegenständen, der Verständigung über Gegenstände sowie dem gedanklichen Ordnen von Gegenständen. Abbildung 1 veranschaulicht das Verhältnis des Begriffs zu sprachlicher Bezeichnung und materiellem oder auch nicht materiellem Gegenstand. Der Begriff ist die mentale, abstrahierte Repräsentation einer bestimmten Gruppe von Gegenständen (Kognition) und wird selbst wiederum durch eine Bezeichnung repräsentiert, die auf einzelne oder mehrere dieser Gegenstände referiert (Expression). Das Verhältnis zwischen einzelnen Begriffen und Benennungen ist keineswegs immer eindeutig. So kann ein Begriff über mehrere verschiedene Bezeichnungen verfügen (Synonymie) oder eine einzelne Bezeichnung auf gleich mehrere Begriffe verweisen (Homonymie, Polysemie), was eine häufige Ursache von Missverständnissen darstellt.

Abbildung 1: Semiotisches Dreieck (Quelle: nach Ogden/Richards 1974)

Erschwert wird dieser Umstand auch durch die Ausdifferenzierung einer Vielzahl unterschiedlicher Fachsprachen, in denen Begriffe in aller Regel fachspezifische Bedeutungen oder Bezeichnungen aufweisen (Fachbegriffe), die sich oft nicht oder nur teilweise mit denen anderer Fachsprachen decken. Begriffe werden oftmals primär innerhalb einer fachlichen Domäne beschrieben und standardisiert. Um allerdings sprachliche Verständnisschwierigkeiten zwischen unterschiedlichen Fachsprachen zu lösen, wurde ein semiotisches (trilaterales varietätsbezogenes) Zeichenmodell mit frei typisierbaren Relationen (Relationstypen) entwickelt, das differenziertere Unterscheidungen und Zusammenhänge darstellt.[6] Bei diesem Modell (vergleiche Abbildung 2) wird zwischen Lexemen, die in lexikologisch-deskriptiver Hinsicht sowohl auf gemeinsprachliche als auch auf fachsprachliche Zeichen zutreffen, und Termini, die in terminologisch-präskriptiver Perspektive nur fachsprachliche Zeichen betreffen, differenziert.

4 | Vgl. Schnieder et al. 2009, Schnieder 2017.
5 | Vgl. Schnieder/Schnieder 2010a.
6 | Vgl. Schnieder et al. 2011a, Schnieder et al. 2011b.

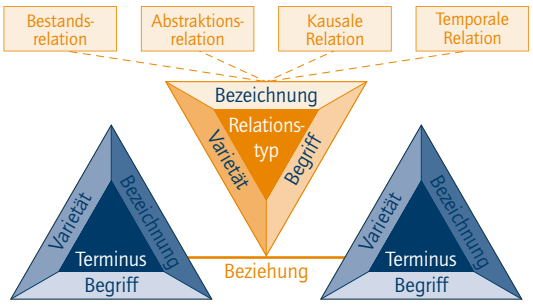


Abbildung 2: Trilaterales varietätsbezogenes Zeichenmodell (Quelle: eigene Darstellung)

Daher sind Termini auch eine besondere Art von Lexemen. Grundsätzlich besteht das Zeichenmodell aus den folgenden drei konstituierenden Seiten: **Lemma** (Bezeichnung des Lexems), **Definition** (Bestimmung der Lexem-Intension) und **Varietät** (fachsprachlicher Kontext des Lexems).

- **Lemma** (Bezeichnung des Lexems): Die Repräsentation des Begriffs erfolgt durch sprachliche (Benennung) oder andere Mittel (Symbol, Gleichung), vergleiche DIN 2342. Eine Bezeichnung ist zum Beispiel die Zeichenfolge, die Lautfolge oder aber eine Gleichung.
- **Definition** (Bestimmung der Lexem-Intension): Ein Begriff verstanden als mentale Einheit ist als solcher nicht darstellbar und muss indirekt über eine Definition oder eine alternative Repräsentation vertreten werden. So kann der zu der Bezeichnung „Ausfall" gehörige Begriff beispielsweise nach „IEV 191-0401" definiert werden als „Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen". Ein Begriff kann mit mehreren unterschiedlichen Definitionen beschrieben werden (Phrasenäquivalenz) und lässt sich weiterhin differenzieren durch die folgenden Komponenten. So werden Definitionen nach dem Begriffsumfang (extensionale Definitionen) und Definitionen nach dem Begriffsinhalt (intensionale Definitionen) unterschieden:
  - **Extension** (Umfang): Die Extension ist die Menge aller Unterbegriffe der nächsttieferen Hierarchiestufe, einschließlich ihres jeweils eigenen Begriffsumfangs (vergleiche DIN 2342, 4.4).
  - **Intension** (Inhalt): Die Intension stellt Eigenschaften eines Begriffs und die hierfür charakteristischen Merkmale mit ihren Größen und Werten dar, welche in der unten erläuterten Attributhierarchie spezifiziert werden können. Der durch die Benennung repräsentierte Eigenschaftsbegriff „Ausfall" weist beispielsweise das Merkmal „Verteilungsfunktion der Ausfallabstände" mit der Größe „Ausfallrate" auf.
- **Varietät** (fachsprachlicher Kontext des Lexems): Der Begriff Varietät bezeichnet in der Sprachwissenschaft eine bestimmte Ausprägung einer Einzelsprache, die diese Einzelsprache ergänzt, erweitert oder modifiziert, jedoch nicht unabhängig von dieser existieren kann. Von Varietät spricht man jedoch nur, wenn die Sprachformen einer untersuchten Gruppe eindeutige sprachliche Gemeinsamkeiten aufweisen. Beispiele für Varietäten sind verschiedene Fachsprachen. So ist beispielsweise der Begriff Ausfall in der Zuverlässigkeit ganz anders konnotiert als im Militärwesen.

2.2 Relationierung der sprachlichen Zeichen

Eine Zusammenfassung thematisch ähnlicher, durch Begriffsbeziehungen geordneter Begriffe bildet ein Begriffssystem. Dabei spielt zunächst eine Klassifikation des Begriffs eine ordnende Rolle, also zum Beispiel Objekt, Vorgang, Attribut, Beziehung. Beziehungen sind zentral, da die Bedeutungen erst über die logische Stellung in einem Begriffssystem entstehen. Die Beziehungen zwischen den einzelnen Attributen konstituieren die Begriffssysteme der Fachdisziplinen. Vertreter der wesentlichen Beziehungstypen sind

- **Bestandsbeziehung**: Begriffsbeziehung, bei der sich der übergeordnete Begriff auf einen Gegenstand als Ganzes bezieht und die untergeordneten Begriffe sich auf die Teile dieses Gegenstands beziehen.
- **Abstraktionsbeziehung**: Begriffsbeziehung, bei der die Intension des übergeordneten Begriffs die Intension des untergeordneten Begriffs einschließt. Der untergeordnete Begriff unterscheidet sich in mindestens einem zusätzlichen Merkmal vom übergeordneten Begriff.
- **Dynamische Begriffsbeziehungen** (Kausal- und Temporalbeziehungen): Hierbei handelt es sich um eine Begriffsbeziehung, die auf einer direkten Abhängigkeit zwischen Begriffen im Sinne einer Vor- und Nachordnung beruht. Diese dynamische Begriffsbeziehung (vergleiche „sequenzielle Begriffsbeziehung" in DIN 2342) kann zeitlich (als temporale Begriffsbeziehung) bestehen und mittels deterministischer oder stochastischer Merkmale beschrieben werden. Ebenso kann sie auf kausalen Zusammenhängen beruhen. Anders als in DIN 2342 können die kausalen Begriffsbeziehungen im technischen Kontext weiter untergliedert werden in nebenläufige Begriffsbeziehungen und sequenzielle Begriffsbeziehungen. Ein Beispiel ist die funktionale Sequenz in einem Regelkreis von „Messen", „Regeln" und „Stellen" und dem beeinflussten Prozess. Im Sinne der Kausalordnung wird zwischen Zuständen und Zustandsübergängen unterschieden. Der unmittelbare Zustandsübergang wird als Ereignis bezeichnet.

2.3 Abstraktionshierarchie der Attribute

Zur technischen Spezifikation des Begriffsinhalts werden hier die folgenden Attributklassen definiert, die sich in vier distinkte Konkretionsstufen gliedern. Ziel ist es, Quantifizier- und Messbarkeit durch hierarchische Dekomposition herzustellen.

- **Eigenschaften**: Eigenschaften beziehen sich auf allgemeine und abstrakt wahrnehmbare, mental verdichtete Zustandsformen der Wirklichkeit. Eigenschaften können über Benennungen sprachlich ausgedrückt werden und stellen somit wieder Begriffe im Sinne des zuvor beschriebenen metasprachlichen Modells dar. Für eine präzise terminologische Klärung sind die beobachteten Eigenschaften auf empirisch beobachtbare Merkmale zurückzuführen. Eigenschaften entstehen durch eine Abstraktion dieser Merkmale.
- **Merkmale**: Über abgrenzende Merkmale kann eine Menge von Elementen von einer anderen unterschieden werden. Dieses Verhältnis wird zwischen Begriffen in verschiedene Begriffsbeziehungen ausdifferenziert (vergleiche Abbildung 3). Merkmale sind Grundelemente für das Erkennen und Beschreiben von Gegenständen und mithin zentral für die Ordnung innerhalb eines Begriffssystems. Merkmale sind objektiv bestimmbar und somit in objektiver Weise präzisierte Eigenschaften. Durch sie werden Eigenschaften von Objekten der außersprachlichen Wirklichkeit qualifizierbar beziehungsweise messbar. Ein Objekt kann Merkmalswerte unterschiedlicher Merkmale aufweisen, aber von jedem Merkmal kommt ihm nur ein Merkmalswert zu. Diese Merkmalswerte müssen für den jeweiligen Zweck hinreichend präzise festgelegt sein. Es muss somit ein prinzipielles Verfahren (beispielsweise Beobachtung, Erprobung, Test, Zählung und Messung) geben, um die Merkmalswerte für einen gegebenen Merkmalsträger zu ermitteln. Dies ist in der Regel die Vorgabe einer Systematik von Merkmalswerten (Skalenniveau), aus der hervorgeht, wie sich der Merkmalswert einordnet. Merkmale sind damit nominal-, ordinal-, intervall- oder verhältnisskaliert und demnach einer Messung (kontinuierliche Merkmale) oder Zählung (diskrete Merkmale) zugänglich. Genau wie die Objekte, die sie qualifizieren, sind sie gegenständlich und können daher zu Merkmalsbegriffen abstrahiert werden. Sprachlich können sie durch Bezeichnung und Definition repräsentiert und terminologisch verwaltet werden.

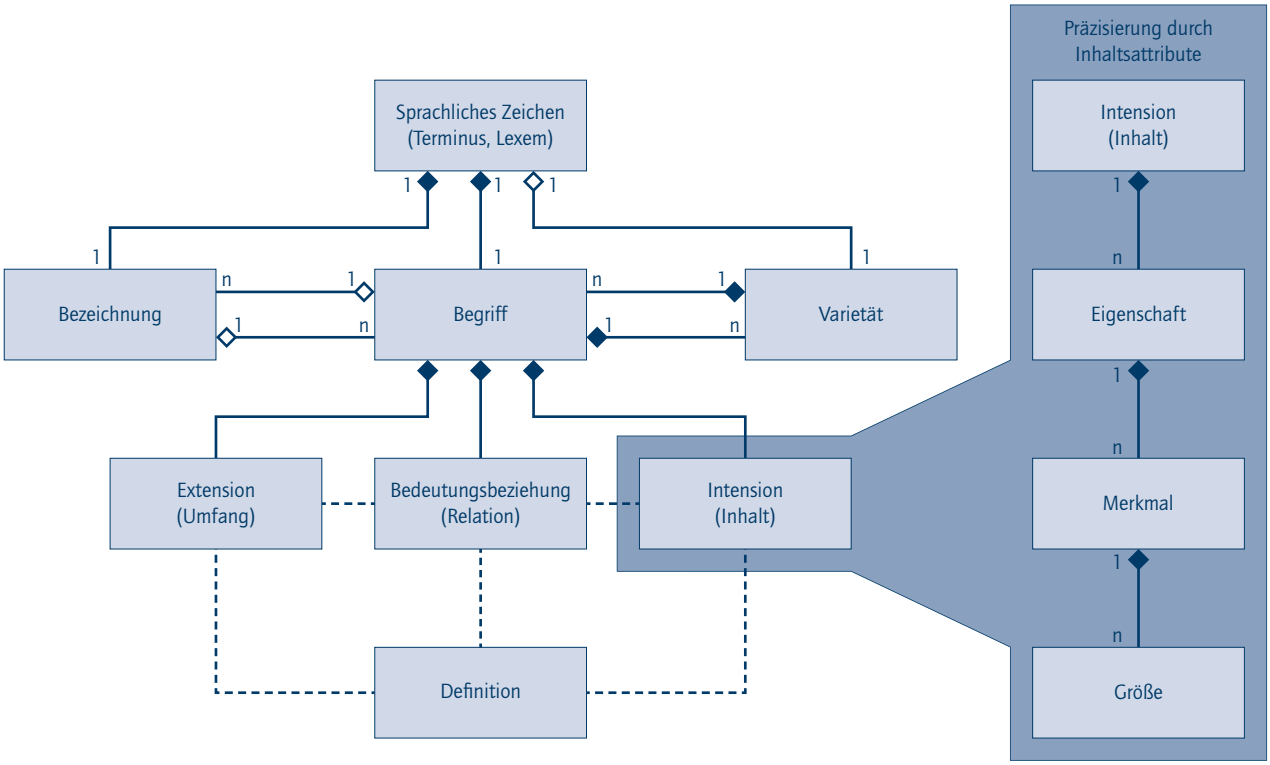


Abbildung 3: Begriffsmodellierung und Attributhierarchie (Quelle: nach Schnieder/Schnieder 2013)

- **Größen**: Größen beschreiben verhältnisskalierte Merkmale. In der Physik beziehen sich Größen auf eine Klasse physikalischer Eigenschaften, die eine Skala numerischer Messwerte ausmachen und die man konkreten Phänomenen zusprechen kann, die sich unter wohldefinierten experimentellen Bedingungen erzeugen lassen. Die Festlegung einer physikalischen Größe beinhaltet unter anderem die metrische Definition (Festlegungen zu Skalenform, Nullpunkt und Einheit). Es wird unterschieden zwischen Basisgrößen (Zeit, Masse und so weiter) und abgeleiteten Größen (Geschwindigkeit, Dichte und so weiter). Da die Merkmale eines Gegenstands nicht immer auf einer Verhältnisskala angeordnet werden können, ist bei der Beschreibung der Intension eines Begriffs nicht immer eine Größe ermittelbar.
- **Werte und Einheiten**: Werte einer Größe (Größenwert) können als Produkt aus Zahlenwert und Maßeinheit dargestellt werden. Die Maßeinheit ist hierbei ein durch internationale Übereinkunft definierter reeller skalarer Wert, mit dem jeder andere Wert der Größe verglichen oder als Verhältnis der beiden Größenwerte als Zahlenwert ausgedrückt werden kann. Analog zur Größe kann auch bei den Einheiten in Basiseinheiten (Sekunde als Basiseinheit der Größe Zeit) und abgeleitete Einheiten unterschieden werden, zum Beispiel Failure In Time (FIT) als abgeleitete Einheit der Größe Ausfallrate, die mit der Einheit 1/h, das heißt Anzahl von Ausfällen in Stunden, und einer äquivalenten Sicherheitsintegritätsstufe (SIL) angegeben wird.

3 Modellkonzepte

Modelle werden genutzt, um spezielle Teilaspekte zu erläutern. Um verschiedene Aspekte des interessierenden Problembereichs der Sicherheit zu verdeutlichen, werden mehrere einander ergänzende Modelle hinzugezogen. Grundlage ist das im vorigen Abschnitt dargelegte Modellkonzept des Begriffs zusammen mit der Attributhierarchie.

In diesem Abschnitt werden zwei weitere für Sicherheit und Verlässlichkeit grundlegende Modellkonzepte beschrieben. Dies sind vor allem

- Modelle des Systems als solches,
- kybernetische Modelle, das heißt geschlossene prozedurale Wirkketten wie Regelkreise und
- das modulare Verlässlichkeitsmodellkonzept Profund.

3.1 Systemmodell

Verlässlichkeit und damit auch Sicherheit wird hier als umfassende Eigenschaft eines Systems verstanden, was auch die Definition des Begriffs System verlangt. Eine gute Grundlage ist die axiomatische Definition eines Systems nach Schnieder/Schnieder 2010,[7] welches abstrakt durch die vier orthogonalen Eigenschaften Zustand, Funktion, Struktur und Verhalten beschrieben wird. Sicherheit kann damit als explizite Verhaltenseigenschaft betrachtet werden, die sich in emergenter Weise aus den elementaren Eigenschaften Zustand und Funktion durch eine geeignete Strukturierung ergibt.

3.2 Kybernetische Modelle

Versteht man Sicherheit als Fähigkeit eines Systems, Prozesse durchzuführen, ohne Schäden zu erleiden beziehungsweise zu verursachen, kann aus abstrakter Perspektive Sicherheit sowohl als Ziel- wie auch als Messgröße eines komplexen dynamischen Systems verstanden werden. In Analogie zur Regelung komplexer dynamischer Systeme könnte eine regelungstechnische Interpretation der Regel-, Mess- und Stellgrößen sowie der dem System und seiner Umgebung innewohnenden hybriden Systemdynamik mit ihren kontinuierlich-diskreten sowie probabilistisch-stochastischen Eigenschaften modelliert werden. Diese Modellierung dient als Grundlage, um entsprechende qualitative Einflussgrößen zu identifizieren und ihre quantitative Wirksamkeit zu beurteilen. Die Eigenschaft Stabilität, welche Sicherheit gewährleistet, zum Beispiel beim Fahrradfahren oder bei Hubschraubern, wird so durch die Funktionsstruktur eines Regelkreises mit den Teilfunktionen erreicht. Im Bereich der Eisenbahnsicherheit wurde dank umfassender Pakete sekundärer Rechtsakte der EU[8] mit den Common Safety Targets (CST), den Common Safety Methods (CSM) und den Common Safety Indicators (CSI) eine Regelkreisstruktur der „Sicherheits-Governance" etabliert (vergleiche Abbildung 4). Diese zielt auf ein gleiches Sicherheitsniveau der Eisenbahnen in der Gemeinschaft.

7 | Vgl. Schnieder/Schnieder 2010b.
8 | Vgl. EU 2004 und EU 2013.

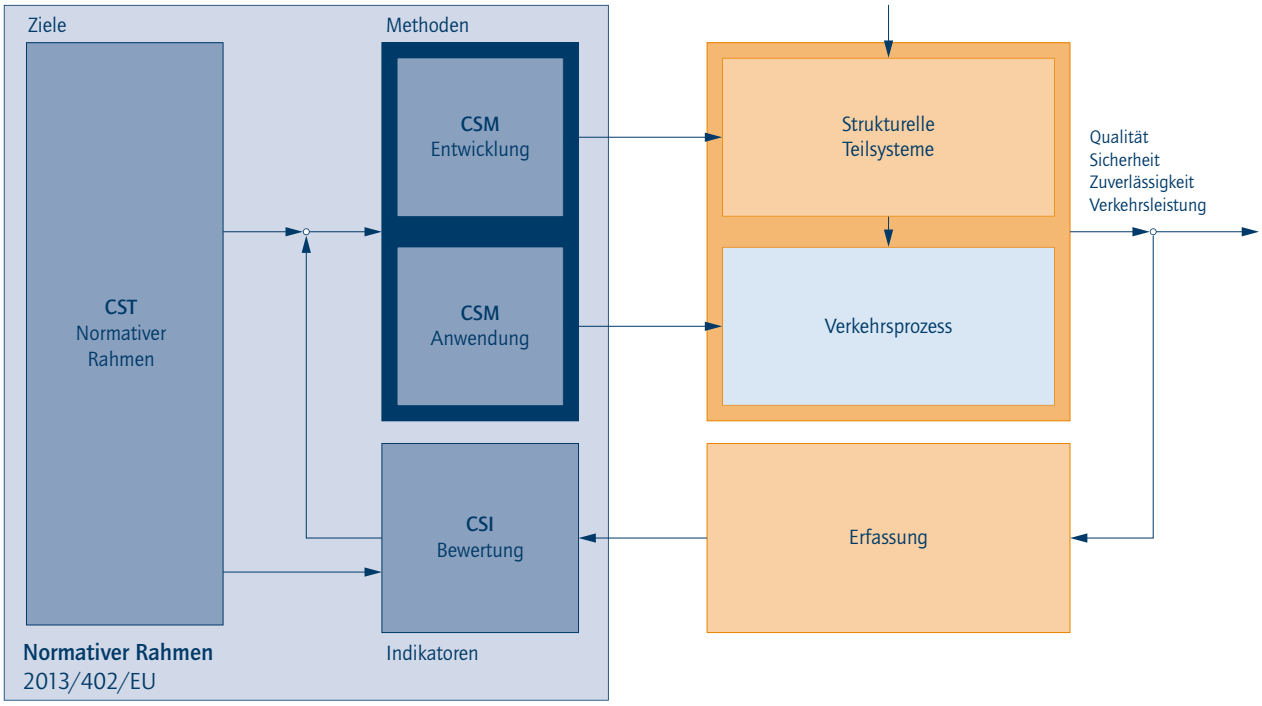


Abbildung 4: Regelkreis der Eisenbahnverkehrssicherheit im europäischen Rechtsrahmen (Quelle: nach Schnieder/Schnieder 2013)

3.3 Modulares Verlässlichkeitsmodell (ProFunD)

Ein neuartiger und geschlossener Ansatz ist das PROFUND-Modellkonzept, welches für Verkehrssysteme entwickelt wurde,[9] jedoch auf allgemeine Systeme übertragbar ist. Das Akronym PROFUND steht für die formale Modellierung von drei essenziellen Systemteilen:

1. Prozess des ungesteuerten idealen (Verkehrs-)Prozessverhaltens,
2. Funktion der idealen (Verkehrs-)Prozesssteuerung und
3. Verlässlichkeit (Dependability) der Ressourcen als Träger der als ideal angenommenen Verkehrsprozesse und Steuerungsfunktionen mit ihren Gefährdungs- und emergenten Schadensereignissen und -zuständen.

Damit ergibt sich ein modulares und ganzheitliches Systemmodell, in dem alle einzelnen Aspekte separat und sukzessiv sowie in fortschreitender Verfeinerung auch formal beschrieben werden können. Die breite internationale Akzeptanz für diesen Ansatz führte daher auch zu seiner Normung (DIN/IEC 62551 2011) und Aufnahme in einen Leitfaden der Europäischen Eisenbahnagentur.[10] Abbildung 5 zeigt das modulare Modellkonzept, mit dessen Ansatz das im nächsten Abschnitt vorgestellte Modellkonzept der Risikogenese noch weiter differenziert und formalisiert wird.

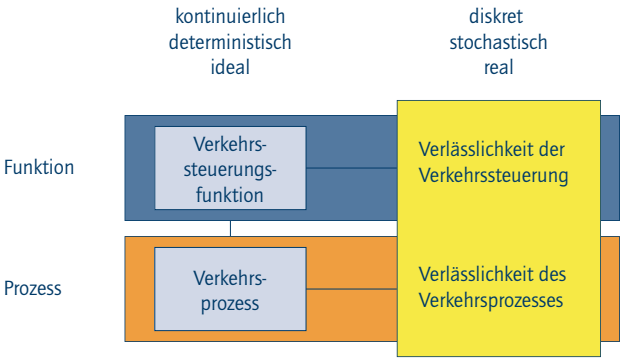


Abbildung 5: PROFUND-Modellkonzept (Quelle: nach Schnieder/Schnieder 2013)

9 | Vgl. Slovák 2006.
10 | Vgl. European Agency for Railways 2015.

4 Formalisierte Beschreibung

Zur Beschreibung komplexer Sachverhalte ist neben der textuellen auch eine grafisch-symbolische und formal(isiert)e Beschreibung zweckmäßig. Hierzu haben sich in den verschiedenen Wissenschaftsdisziplinen eigene Beschreibungsmittel etabliert, so auch in der Zuverlässigkeits-, Regelungs-, oder Automatisierungstechnik (zum Beispiel Petrinetze, Unified Modeling Language – UML).[11] Merkmale dieser Beschreibungsmittel sind ihre visuellen Elemente (Symbole), ihre Syntax und ihre Semantik unterschiedlicher Ausprägung. Je formaler diese sind, desto größer ist die Möglichkeit einer formalen Verifikation. Auf diese Weise lassen sich Begriffe, das heißt ihre Definitionen und insbesondere ihre Beziehungen untereinander, explizit formalisieren, maschinenlesbar modellieren und verifizieren. So können

- die **Konsistenz** der Gesamtterminologie inhaltlich, thematisch und logisch geprüft werden,
- die **Vollständigkeit** der Gesamtterminologie geprüft werden, indem fehlende Elemente identifiziert werden,
- **Ambiguitäten** (Doppeldeutigkeiten) eliminiert werden, da eine bewusste Eingrenzung der Bedeutung auf die Semantik des Beschreibungsmittels erfolgt, sowie
- **Inkonsistenzen** wie beispielsweise Widersprüche und Zirkelverweise aufgedeckt werden.

Eine formalisierte, vernetzte Terminologie ermöglicht eine formale Konsistenzprüfung und eine anschauliche Darstellung der Zusammenhänge im Begriffssystem. Falsche und unklare Verwendung von Terminologie und daraus entstehende Missverständnisse und Fehler können so häufig vermieden werden.

Aufgrund der Tatsache, dass zwischen der Zuverlässigkeit technischer Systeme und der Sicherheit viele strukturelle und begriffliche Gemeinsamkeiten bestehen,[12] und dem Ziel, diese Eigenschaften in einer gemeinsamen Theorie der Verlässlichkeit zu vereinen, erscheint es zweckmäßig, die bereits für die Zuverlässigkeit entwickelten, mittlerweile genormten sowie empfohlenen und bewährten Formalisierungsmittel für Begriffsmodellierungen, nämlich Klassendiagramme für statische und Petrinetze für dynamische Zusammenhänge, auch für die Formalisierung der Sicherheitsbegriffe und -beziehungen zu verwenden.[13] Abbildung 6 stellt dar, wie unterschiedliche Aspekte des Modellkonzepts des Systems (vergleiche Abschnitt 3.1) mit verschiedenen Beschreibungsmitteln dargestellt werden können.

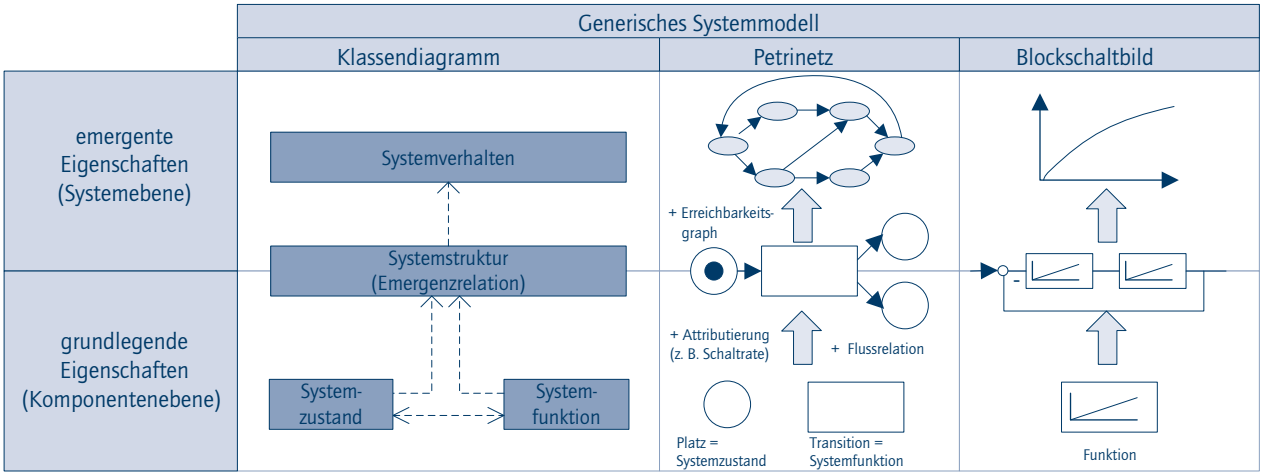


Abbildung 6: Beschreibung des Modellkonzepts des Systems mit verschiedenen Beschreibungsmitteln (Quelle: nach Schnieder 2010)

11 | Vgl. VDI 2015.
12 | Vgl. Schnieder 2013.
13 | Vgl. VDI 2017, Schnieder 2010, Müller 2015, European Agency for Railways 2015, DIN 2013.

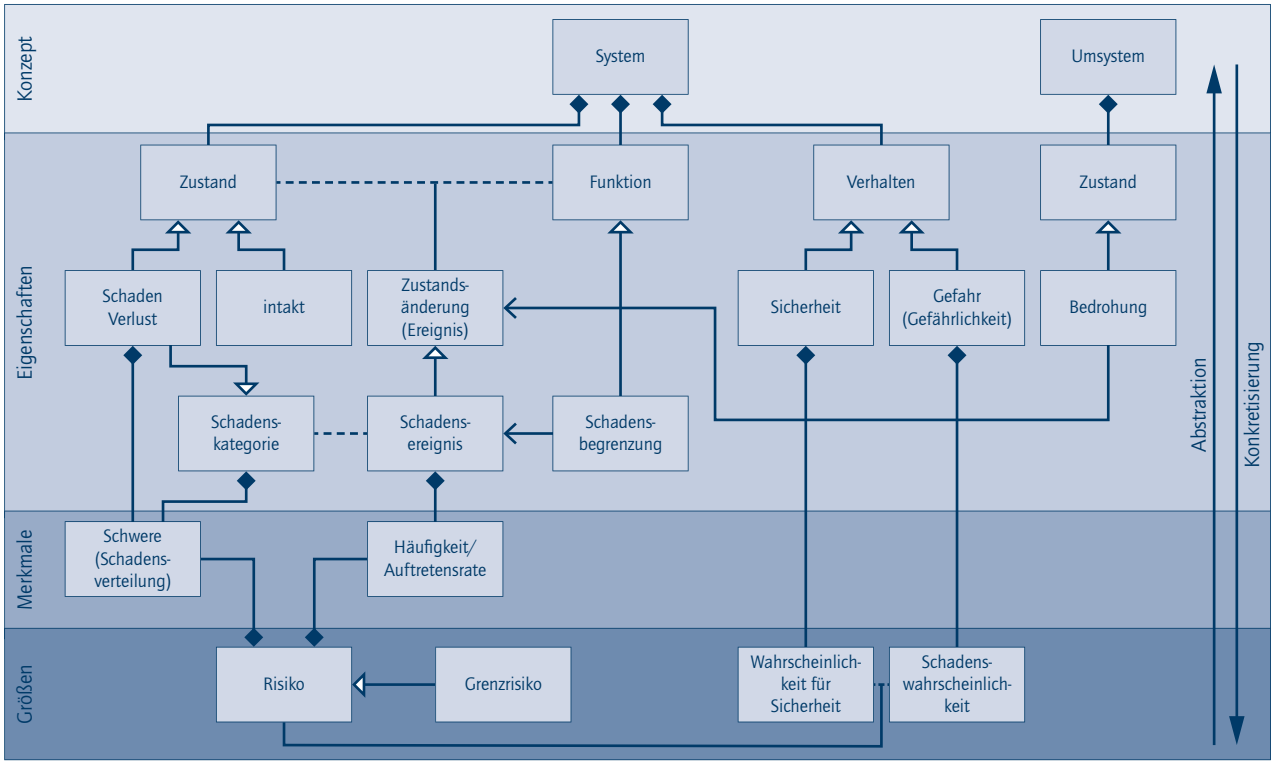


Abbildung 7: Kombinierte und formalisierte Darstellung von Begriffen der Sicherheit als UML-Klassendiagramm (Quelle: eigene Darstellung)

4.1 UML-Klassendiagramme

Klassendiagramme sind ein semiformales Beschreibungsmittel, das heißt, sie haben eine Menge definierter Symbole und Relationen, jedoch keine mathematisch definierte Semantik. Klassendiagramme dienen primär zur Darstellung struktureller Zusammenhänge. Wie die Ausdrucksmöglichkeiten von UML-Klassendiagrammen für die Darstellung von Begriffssystemen genutzt werden können, zeigt auch ISO 24156-1. In der UML-Notation werden dafür Begriffe durch Klassen und Begriffsbeziehungen durch Assoziationen repräsentiert. Abbildung 7 zeigt eine nach diesen Modellkonzepten kombinierte und formalisierte Darstellung von Begriffen der Sicherheit als UML-Klassendiagramm. Unabhängig von der speziellen fachsprachlichen Formulierung kann Sicherheit über die Abstraktionshierarchie präzise formuliert werden. Zu der begrifflichen Verhaltenseigenschaft Sicherheit gelangt man über Zustandsmerkmale in Form von Häufigkeitsverteilungen des Schadenseintrittsabstands sowie des Schadensausmaßes als Produkt der Mittelwerte der Verteilungsfunktionen auf die aggregierte Größe Risiko. Allerdings sind die einem Schaden zugehörigen Schadenseinheiten in der Regel nicht kommensurabel, zum Beispiel Getötete, Verletzte, Sach- oder Umweltschäden.

4.2 Petrinetze

Geht man von der Frage aus, wie die Aufbau- und Verhaltensstruktur sowie die Merkmale der Objektorientierung darstellbar sind, stellen netzartige Repräsentationskonzepte außerordentlich leistungsfähige Beschreibungen bereit. Hierzu zählen vor allem semantische Netze, Kanal-Instanzen-Netze und Petrinetze. Insbesondere sind farbige Petrinetze mit ihren Attribuierungsmöglichkeiten in der Lage, sämtliche Ausprägungen der Systemaxiomatik und Objektorientierung anschaulich graphisch sowie formal, das heißt mathematisch exakt und präzise, zu definieren. Darüber hinaus ermöglichen sie in der (statischen) Netzstruktur die implizierte Modellierung der Dynamik, woraus sich durch rein formale Handhabung die expliziten Zustandsmengen dynamischer Abläufe ermitteln und in Erreichbarkeitsgraphen darstellen lassen. Die damit zusammenhängende, in etwa logarithmische Reduktion der Komplexität dynamischer Vorgänge ist gerade bei hochgradig nebenläufigen beziehungsweise modularen Systemen von enormem Vorteil. Die Petrinetzbeschreibung bildet in Symbolik, Syntaktik und Pragmatik ein allgemein gültiges und umfassendes Fundament für die Beschreibung der Systemaxiomatik und Objektorientierung sowie vor allem inhaltlicher Aspekte von Automatisierungssystemen.

Die für die Verlässlichkeit bestimmenden aggregierten Wahrscheinlichkeiten werden besonders gut mit stochastischen Petrinetzen modelliert.[14] Diese Ansätze werden durch den neuartigen Ansatz probabilistisch-stochastischer Petrinetze erweitert, der in Abschnitt 5 erläutert wird.

4.3 Weitere Beschreibungsmittel

Für die Modellierung von Systemaufbau- und -funktionsstrukturen verlässlicher Systeme eignen sich auch weitere Beschreibungsmittel, wie zum Beispiel semiformale Fehlerbäume, Ereignisbäume, regelungstechnische oder Zuverlässigkeitsblockschaltbilder und formale Instrumente wie Boolesche Algebra, Markovketten oder wahrscheinlichkeitstheoretische Formalismen.[15]

5 Formalisierte Modellkonzepte der Sicherheit

Für die verallgemeinerte dynamische Modellierung der Schadensentstehung und damit des Sicherheitsverhaltens haben Schnieder und Schnieder das Modell der Risikogenese entwickelt, welches Abbildung 8 schematisch in Form eines Kanal-Instanzen-Netzes zeigt.[16] Die jeweiligen Benennungen der Kanäle und Instanzen wurden unmittelbar aus dem DIN-Fachbericht 144 übernommen.[17]

Sicherheit entsteht, wenn keine Schäden auftreten. Umgekehrt führt die Schadensentstehung zum Komplement der Sicherheit, in der Regel Gefahr genannt, welche durch die aggregierte Risikogröße quantifiziert wird. Wenn ein exponiertes Objekt, zum

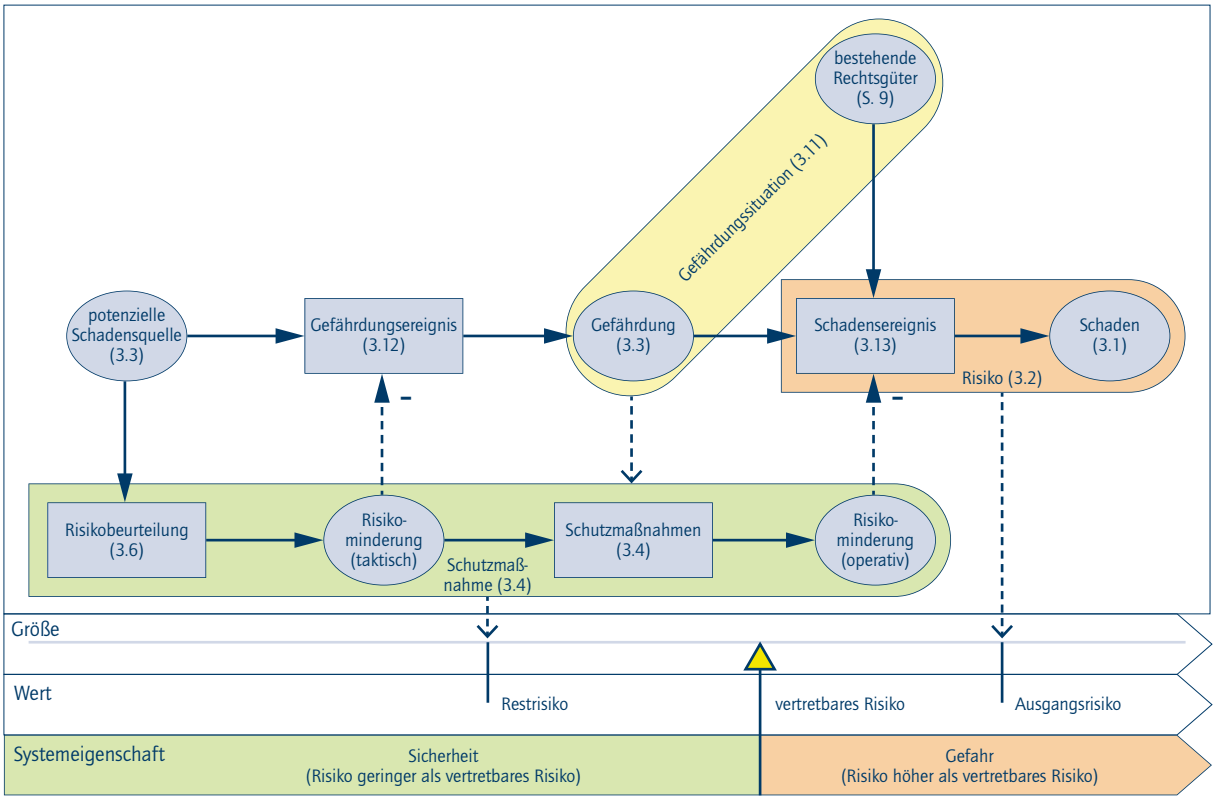


Abbildung 8: Formalisierung des Begriffssystems „Sicherheit" mittels des Modelles der Risikogenese gemäß Termini und Benummerung nach DIN 2005 (Quelle: nach Schnieder/Schnieder 2013)

14 | Vgl. Schnieder 1999.
15 | Vgl. Vose 2008.
16 | Vgl. Schnieder/Schnieder 2013.
17 | Vgl. DIN 2005.

Beispiel ein Verkehrsobjekt als bestehendes Rechtsgut, von einer Gefährdung bedroht wird, entsteht eine Gefährdungssituation, und das Schadensereignis kann eintreten, was den Schaden zur Folge hat.

Das *Risiko* R selbst wird einerseits als Summe aller einzelnen *Schäden* D in einem bestimmten *Bezugs(zeit)raum* B oder andererseits als Produkt der mittleren Schadenshäufigkeit im Sinne einer mittleren *Schadensfrequenz* $\overline{f}$ und der mittleren *Schadenshöhe* $\overline{D}$ im Verkehr bestimmt:

$$R = \sum_{i \in B} D_i = \overline{f_D} * \overline{D}. \qquad (1)$$

Damit liegt eine quantitative Beschreibung für die Sicherheit vor, die jeweils auf bestimmte Objekte, Regionen, Nutzergruppen etc. mehr oder weniger aggregiert bezogen werden kann. So wird in der Regel Sicherheit dann erreicht, wenn ein vorhandenes Risiko kleiner als ein vertretbares Risiko, das heißt akzeptables Grenzrisiko, ist. Damit wird Sicherheit als Relation zwischen dem tatsächlichen Risiko R und einem wünschenswerten Grenzrisiko R_L formuliert.

$$S <=> R < R_L. \qquad (2)$$

Als Grenzrisiko kann entweder das gesellschaftlich akzeptierte Risiko betrachtet werden, welches sich im Lauf der Jahre „stationär" einstellt, wie beispielsweise im Luft- und Schienenverkehr, oder das sich als Ziel relativer Verbesserung in einem gewissen Zeitraum ergibt, wie zum Beispiel die Halbierung der Zahl der Verkehrstoten im Straßenverkehr in einem Jahrzehnt, oder als Vorgabe eines bestimmten Risikowertes oder gar visionär als Nullrisiko, der sogenannten „Vision Zero".[18] In diesem Zusammenhang ist das Risiko jetzt sowohl eine Mess- als auch eine Regelgröße des Verkehrssystems, wobei es auch als Ziel- oder Begrenzungsgröße mit geeigneten Werten fungiert.

Die dem Schadenseintritt als Voraussetzung zugrundeliegende Bedingung lautet sprachlich, dass kein Grenzwert physikalisch überschritten werden darf, der zu einer Gefährdung und einem anschließenden Schadenseintritt führen kann. Beispiele für Grenzwerte verschiedener Domänen zeigt Tabelle 1. Konkret heißt das zum Beispiel im Bauwesen, dass die Belastung einer Gebäudedecke beispielsweise weit genug von deren Festigkeit entfernt sein muss. Aufgrund der in der Regel physikalisch bedingten und mathematisch in statistischen Verteilungsfunktionen ausgedrückten Unschärfe der jeweiligen Zahlenwerte muss der ursprünglich als **Sicherheitsindex** benannte Abstand so groß sein, dass es nur mit einer ganz geringen Wahrscheinlichkeit dazu kommen könnte, dass der Abstand zu klein wird. Beispiele für ein Versagen von Bauwerken in dieser Folge sind der Einsturz der Berliner Kongresshalle („Schwangere Auster") im Jahr 1980 oder der Einsturz der Eishalle in Bad Reichenhall im Jahr 2006.

Eigenschaft	Ausprägung	Merkmale und Größen für Grenzwerte
Physikalisch	Dynamik	Weg, Geschwindigkeit, Beschleunigung, Kraft
	Elektromechanik	Strom, Spannung, EMV, elektromagnetische Strahlung(senergie)
		Radioaktive Strahlung(senergie)
	Thermodynamik	Temperatur
		Luftfeuchtigkeit
Chemisch	Konzentration	Maximale Säure-, Gas- oder Schadstoffkonzentration, Arbeitsplatzkonzentrationen Partikelkonzentrationen
Leib und Leben	Biologisch, medizinisch	Erschütterungen Schall Physische Integrität (AIS, MAIS) Psychische Integrität
Informationen	Kriminologisch	Verfügbarkeit Vertraulichkeit Integrität Authentizität
	Sachwerte	Immaterielle Güter Materielle Güter

Tabelle 1: Beispiele für Gefährdungsgrenzwerte verschiedener Domänen

18 | Vgl. Schnieder/Schnieder 2013.

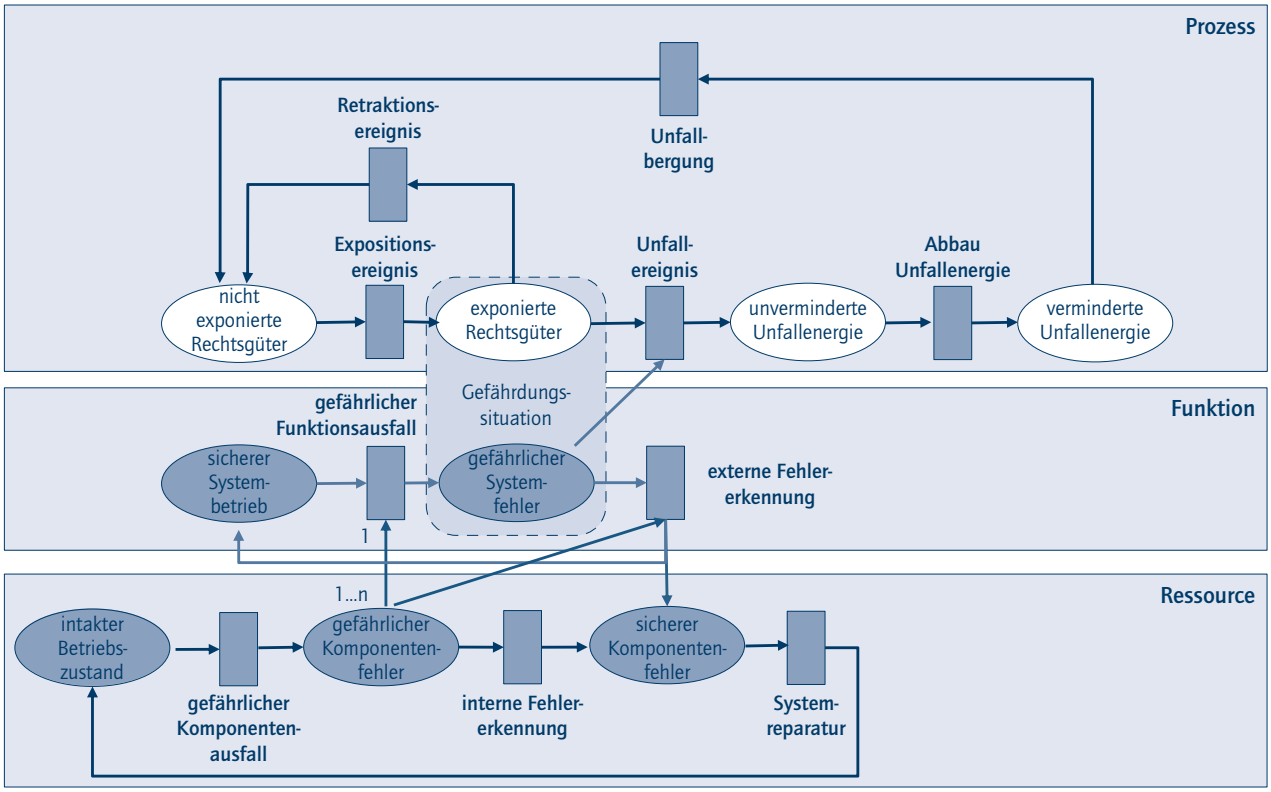


Abbildung 9: Detailliertes Modell der Risikogenese (Quelle: eigene Darstellung)

Die Gefährdungs- beziehungsweise Schadensbedingung kann mathematisch formalisiert werden. Wenn im Zustandsübergangsmodell der schadensfreie Zustand in den Schadenszustand übergeht, kann die Bedingung für den Übergang durch die Verletzung einer Grenze mathematisch formuliert werden, das heißt:

$$x_{LO} < x < x_{LU}\,. \qquad (3)$$

Damit existiert Sicherheit, solange sich das System in einem erlaubten Zustandsraum befindet. Gleiches gilt, wenn das System gefährdet wird. Diese absolute Sicherheitsbedingung kann auf eine probabilistische Beziehung übertragen werden, indem die Wahrscheinlichkeit von Schadens- oder Gefährdungsereignissen niedriger sei als ein bestimmter Wert:

$$P(x_{LO} < x) + P(x < x_{LU})) \leq P_L. \qquad (4)$$

Das Risikogenesemodell aus Abbildung 8 kann nun gemäß dem modularen Verlässlichkeitsmodell PROFUND entsprechend den funktionalen Teilsystemen Prozess und Funktion sowie dem Verlässlichkeitsmodell verfeinert werden, um so zu einer ganzheitlichen Modellierung aller Eigenschaften zu gelangen. Abbildung 9 zeigt ein entsprechendes Modell für Unfallentstehung und -verhinderung im Straßenverkehr. Mit diesem Ansatz wurde die Sicherheit von Bahnübergängen in der EU, der Schweiz und Australien sowie für Fußgängerquerungen in Kuala Lumpur analysiert.[19]

5.1 Merkmale der Schadenshäufigkeit

Für die Beurteilung der Verlässlichkeit ist nicht nur die unmittelbare Häufigkeit von Bedeutung, sondern insbesondere ihre zeitliche Ausprägung, das heißt, wie oft in einem Bezugszeitraum die Gefährdungsgrenze überschritten wird oder wie oft ein Schaden eintritt. Das Auftreten von Unfallereignissen kann als stochastischer Prozess aufgefasst werden. Hinsichtlich der Schadenshäufigkeit kann die stochastische Modellierung mit einer charakteristischen Verteilungsfunktion des statistisch verteilten zeitlichen Schadensereignisabstands T_D erfolgen. Unabhängig von der Schwere des Ereignisses konnte im Straßen- und Schienenverkehr hierfür eine negative Exponential- beziehungsweise Log-Normalverteilung

$$p(T_D) = e^{-t/\overline{T}_D} \qquad (5)$$

19 | Vgl. Slovák 2006 und Siti Zaharah/Yue 2008.

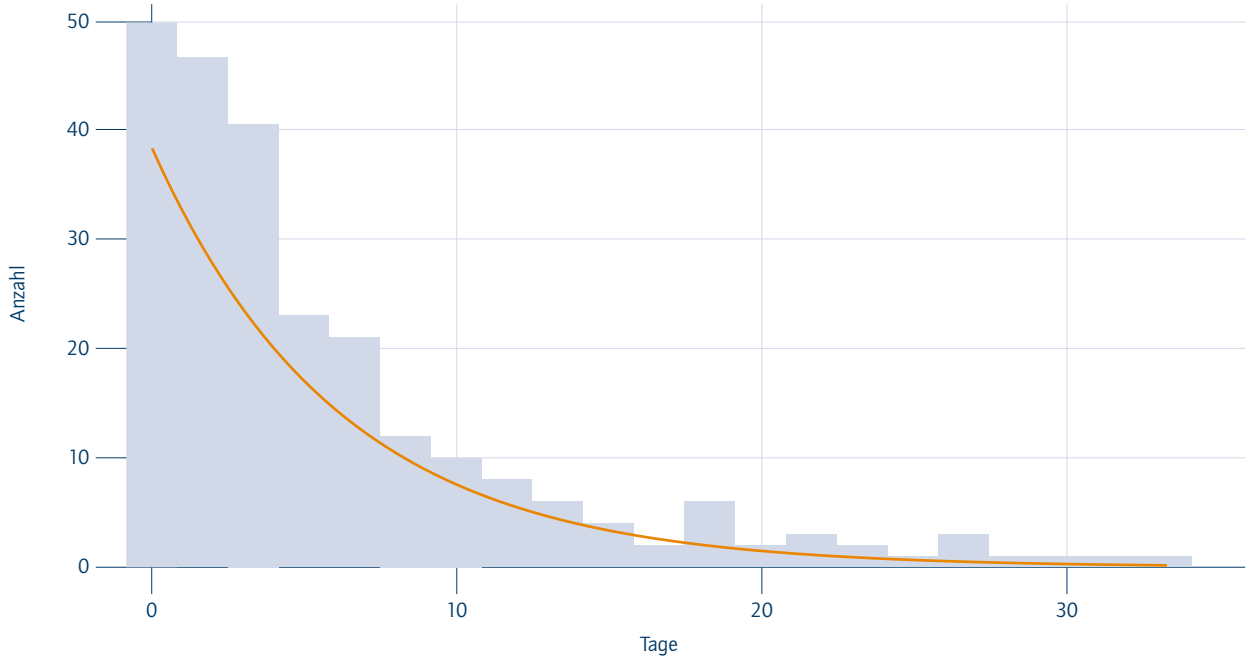


Abbildung 10: Annäherung der Schadenshäufigkeitsverteilung durch eine negative Exponentialverteilung (auf Basis von Eisenbahnzusammenstößen in der Schweiz von 2006 bis 2011) (Quelle: eigene Darstellung)

mit sehr hoher Korrelation ermittelt werden.[20] Abbildung 10 zeigt am Beispiel von Eisenbahnzusammenstößen, wie im Zeitraum von fünf Jahren der zeitliche Abstand bei achtzig Zusammenstößen innerhalb von zwei Tagen lag, längere Abstandsdauern waren dagegen seltener.

5.2 Merkmale und Größen des Schadensausmaßes

Das Schadensausmaß wird häufig in den nominalen Kategorien Getötete sowie Schwer- und Leichtverletzte mit der jeweiligen Fallzahl angegeben. Um diese inkommensurablen Kategorien auf einer einheitlichen Skala abzubilden, werden verschiedene Ansätze verfolgt, zum Beispiel durch die sogenannte Zehnerregel, bei der die Schadensstufen jeweils den zehnten Teil der schwereren Klasse betragen. Daraus ergibt sich als kombiniertes Risikomaß die gewichtete Fatality Weighted Injuries (FWI) aus den einzelnen Schadensfällen jeder Schadensklasse zu

$$FWI = 1 * \Sigma\, n_{\text{Tote}} + 0{,}1\, \Sigma\, n_{\text{Schwerverletzte}} + 0{,}0\,1\, \Sigma\, n_{\text{Leichtverletzte}} \quad (6)$$

Mit der Zehnerregel für die vereinheitlichte Skalierung der Unfallschwere D ergibt sich für den Verteilungsfunktionsverlauf bereits, dass eine logarithmische Normalverteilung oder in Teilen eine Exponentialverteilung zur Beschreibung geeignet ist. Eine weitergehende Justierung der Gewichtungsfaktoren könnte gegebenenfalls zu einer noch besseren Passung führen. So könnte eine Harmonisierung mit einer einheitlichen Skala durch die originäre Unfallschwere zum Beispiel nach der Abbreviated Injury Scale (AIS) oder der Maximal Abbreviated Injury Scale (MAIS) erfolgen. Hier sind jedoch spezifische Angaben bei der Unfallentstehung nötig, die nicht in jedem Fall vorliegen.

Darüber hinaus kann es sich um Sachschäden sowie Schäden an der Umwelt handeln. Andere Ansätze zur Bewertung der ökonomischen Kosten sind schwierig umzusetzen. Sie können zwar für ein einziges homogenes Land mit einer homogenen sozialen Struktur gelten, aber ein internationaler Vergleich zeigt, dass diese um mehr als eine Zehnerpotenz variieren. Ein alternativer Ansatz, um Größen für menschliche Schäden zu finden, wurde analog zum Verlust menschlicher Lebensdauer der Medizin (Years Life Lost, YLL) vorgeschlagen, indem die durch Schäden bedingte Verkürzung der menschlichen Lebensdauer T auf die regionale Lebenserwartung TM bezogen wird. Deren negative logarithmische Skalierung skaliert eine Kenngröße zwischen null und unendlich.[21]

$$\Psi = -\log\,(\Delta T / T_M). \quad (7)$$

20 | Vgl. Von Buxhoeveden/Schnieder 2013.
21 | Vgl. Schnieder/Drewes 2008.

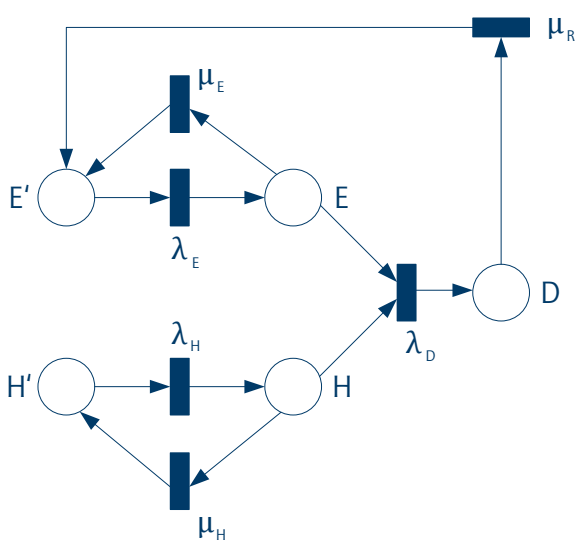


Abbildung 11: Vollständiges (formalisiertes) generisches Petrinetzmodell der Risikogenese (Quelle: eigene Darstellung)

Die erst im Kanal-Instanzen-Netz vorhandene Unterscheidung zwischen kurzfristigen Zustandsübergängen (Kästen) und länger dauernden Zuständen (Ellipsen) ermöglicht den Übergang zu einer formalisierten Beschreibung in Form eines stochastischen Petrinetzes (nach IEC 62551) mit Ereignissen (Transitionen) und Stellen, welches Abbildung 11 zeigt.

Das Zustandspaar H'/H bezeichnet die Nichtgefährdungs-/Gefährdungszustände, dazwischen liegen die stochastischen Übergänge mit den Raten λ_H und μ_H. Das Verhalten des potenziell gefährdeten Objekts wird dann analog mit dem Zustandspaar E'/E für Nichtexposition/Exposition und den Zustandsübergängen mit den Raten λ_E und μ_E modelliert. Bei Koinzidenz von Exposition E und Gefährdung H schaltet die Unfalltransition, und der Schadenszustand D tritt ein, aus dem über die Transition der Wiederherstellung (Rate μ_R) schließlich der nicht exponierte Objektzustand H' erreicht werden kann. Die Testkante vom Gefährdungszustand H zur Unfalltransition besagt, dass auch nach einem Unfall die verursachende Gefährdung nicht beseitigt wird. Alle einzelnen Zustände im Petrinetz können mit entsprechenden Zustandswahrscheinlichkeitsverteilungen attribuiert werden. In diesem Modell verkörpern die Übergangsraten aggregierte Zustandsänderungen, die ihrerseits noch weiter differenziert werden können. Mit dieser Modellierung gelingt die Symbiose individueller Schadensentstehung und statistischer Aggregation.

5.3 Probabilistisch-stochastische Modellkonzepte der Risikogenese

Die Modellierung mittels stochastischer Petrinetze ermöglicht die Darstellung der Gefährdungs- und Schadenshäufigkeiten, indem diese durch spezielle Verteilungsfunktionen zeitlich stochastischer Ereignisabstände parametriert werden. Die im exponierten Objektzustand oder im Gefährdungszustand enthaltene potenzielle Schadensenergie ist hier noch nicht modelliert. Diese Attribuierung und quantitative Ausprägung der einzelnen Zustände durch geeignete Zustandsverteilungsfunktionen (zum Beispiel des Schadensausmaßes) wird im Folgenden betrachtet.

Mit einem auf farbigen Petrinetzen fußenden Ansatz[22] wird dieser Risikofaktor ebenfalls in die Modellierung einbezogen. In den farbigen Petrinetzen werden Stellen beziehungsweise den darauf liegenden Marken individuelle Merkmale in Form sogenannter Colorsets als Informationsträger zugeordnet. Wenn nun ein Colorset als Verteilungsfunktion definiert wird, kann zum Beispiel dem exponierten Rechtsgut als möglichem Schadensobjekt eine Energieverteilungsfunktion zugeordnet werden, die im Fall des Schadensereignisses gegebenenfalls im Zusammenhang mit einer Gefährdungsintensitätsverteilungsfunktion zur resultierenden Schadensverteilung führt. Die zugehörige Transition des Schadenereignisses wird entsprechend mit einer CPN-Guardfunktion gemäß der Gefährdungswirkung auf ein Schadensobjekt definiert. Zum Beispiel ist bei einer Kollision eines Fahrzeugs mit einem anderen die Schadensintensität nach dem Impuls- und Energieerhaltungssatz berechenbar. Mathematisch müssen in diesem Fall beide Verteilungsfunktionen gefaltet werden, um die Schadenintensitätsverteilung zu bestimmen. Ähnlich geht man bei der Risikominderung durch Barrieren vor, um die resultierende Schadensverteilung zu erhalten. Alternativ ist auch eine Bestimmung durch Monte-Carlo-Simulationen dieser als probabilistisch-stochastische Petrinetze bezeichneten neuartigen Netzklasse möglich.

Ähnlich wie bei diesem vorgestellten Ansatz der Schadensausmaßentstehung mit probabilistisch attribuierten Stellen und Marken kann ein Widerstand gegen Attacken oder Bedrohungen oder auch die Wirksamkeit von Schadensbegrenzungen ebenfalls mit diesem Ansatz probabilistisch-stochastischer Petrinetze wahrscheinlichkeitstheoretisch modelliert werden. Die Wirksamkeit von Schutzmaßnahmen wie Firewalls und anderen Vorkehrungen gegen Bedrohungen wird genauso durch Faltung der Intensitätswahrscheinlichkeitsverteilungen von Gefährdungs- und Barriereintensität berechnet.

22 | Vgl. Jensen 1992.

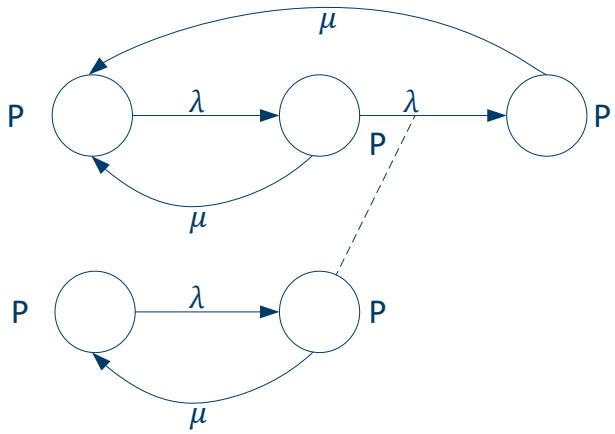


Abbildung 12: Markovkette des Sicherheitsverhaltens (Quelle: eigene Darstellung)

5.4 Sicherheitszyklus und Markovkette

Ein aus der Risikogenese abgeleitetes weiteres Modellierungskonzept ist der Sicherheitszyklus, der sich als stochastisch attribuierter Erreichbarkeitsgraph aus dem stochastischen Petrinetz ergibt und bei konstanten Raten als Markovkette aufgefasst werden kann (vergleiche Abbildung 12). Das dynamische Verhalten der Zustandsentwicklung im Sicherheitszyklus kann in Form einer linearen Matrizendifferenzialgleichung beschrieben werden, wenn alle Zustandsübergangsraten in einer Matrix Λ zusammengefasst werden:

$$P = \Lambda \cdot P. \qquad (8)$$

Für den Fall rückwirkungsfreier Gefährdung H ergibt sich aus dem Petrinetz (vergleiche Abbildung 11) mit der Anfangsmarkierung E′/H′ ein einfacher Erreichbarkeitsgraph, der infolge der Petrinetzstruktur vom Typ Zustandsmaschine dem oberen Teil des Petrinetzes isomorph ist (Abbildung 12).

Für die Schadensrate ergibt sich infolge der Testkante vom Gefährdungszustand auf die zum Schaden führende Transition.

$$\lambda_D = \lambda_D \cdot P_H. \qquad (9)$$

In ähnlicher Weise kann aus dem unteren Teil des Petrinetzes ein entsprechendes Differenzialgleichungssystem der Gefährdungszustandswahrscheinlichkeiten aufgestellt werden. Dabei wird vereinfachend angenommen, dass die Zustandsübergänge unabhängig von den obigen Expositionswahrscheinlichkeiten sind, was in der Wirklichkeit nicht immer der Fall ist. Die zugehörigen Zustandsdifferenzialgleichungen sind

$$\dot{P_H} = +\lambda_H P_{H'} - \mu_H P_H \qquad (10a)$$

$$\dot{P_{H'}} = -\lambda_H P_{H'} + \mu_H P_H \qquad (10b)$$

mit der Normalisierungsbedingung

$$1 = P_{H'} + P_H. \qquad (10c)$$

Im Fall konstanter Übergangsraten gestaltet sich der untere Gefährdungszyklus als Markovkette, wobei sich die zeitveränderlichen und stationären Werte der einzelnen Zustandswahrscheinlichkeiten durch Lösung des Gleichungssystems (9) analytisch bestimmen lassen. So ergibt sich die stationäre Wahrscheinlichkeit, dass keine Gefährdung auftritt, analog zur Unverfügbarkeit reparierbarer Systeme zu.

$$P_{H'} = \frac{\mu_H}{\mu_H + \lambda_H}. \qquad (11)$$

Damit kann dann die stationäre Schadenswahrscheinlichkeit $P_{D\infty}$ mit (7) und (10) bestimmt werden, die allein von den Übergangsraten abhängig ist. Die stationäre Schadenswahrscheinlichkeit ergibt sich aus (6) nach einer Zwischenrechnung.

$$P_{D\infty} = \frac{\lambda_E \mu_R}{\mu_R \mu_E + (\mu_R + \lambda_E)\lambda_H \frac{\mu_H}{\mu_H + \lambda_H}} \qquad (12)$$

Für den Fall nicht konstanter Übergangsraten ist eine numerische Simulation oder eine Monte-Carlo-Analyse zweckmäßig.

6 Regelung der Sicherheit (Safety und Security)

Die Verhaltensdynamik der Gefährdungs- und Schadenswahrscheinlichkeit beschreiben sowohl die Zustandsdifferenzialgleichungen als auch ein regelungstechnisches Blockschaltbild, das unmittelbar aus der Zustandsübergangsmatrix beziehungsweise den Differenzialgleichungen (6) und (8) hergeleitet werden kann. Im rechten Teil der Abbildung 13 stellt der obere Teil die Expositions- und die Schadensdynamik als dynamisches System zweiter Ordnung dar, das von dem unteren dynamischen Teilsystem über die Schadensrate als Einflussgröße und faktoriell beeinflusst wird. Die Schadensrate λ_D resultiert aus der unteren „Gefährdungsregelstrecke" mit einem Integrator sowie zwei proportionalen Rückführungen, der

Gefährdungsrate λ_H sowie der Behebungsrate μ_H für erkannte Gefährdungen. In dieser einfachen Darstellung übernimmt der Zahlenwert 1 die Soll-Zustandswahrscheinlichkeit absoluter Gefährdungsfreiheit, die wie bei jeder proportional geregelten Strecke nie erreicht werden kann. Werden die Schadensrate sowie die Behebungsrate nicht als konstant aufgefasst, ergibt sich ein nichtlineares Differenzialgleichungssystem.

Dieses Modell kann nun als nichtlineares Prozessmodell der Sicherheit und – wenn es um das Schadensausmaß erweitert wird – des Risikos aufgefasst werden. Dabei kann der Sicherheitsbegriff sowohl Safety als auch Security umfassen.

Im Fall der Safety dienen als spezifische Einflussgrößen auf die Gefährdungswahrscheinlichkeit einerseits die Gefährdungsrate λ_H, die vom Systemdesign und der angestrebten Sicherheitsintegrität beziehungsweise der zulässigen Gefährdungsrate abhängig ist. Andererseits kann die Entdeckungsrate genutzt werden, die durch einen Regler vorgegeben werden kann, dessen Eingangsgröße die Differenz einer Schadenswahrscheinlichkeit und dem Zielwert „0" ist. In der Realität ist die Entdeckungsrate beispielsweise durch eine technische Diagnose oder menschliche Überwachung bis hin zur Alarmbereitschaft verwirklicht. So konnte zum Beispiel durch die Verringerung der Eintreffdauer von Rettungskräften am Unfallort die Überlebenswahrscheinlichkeit von Verletzten signifikant erhöht werden. Auch der

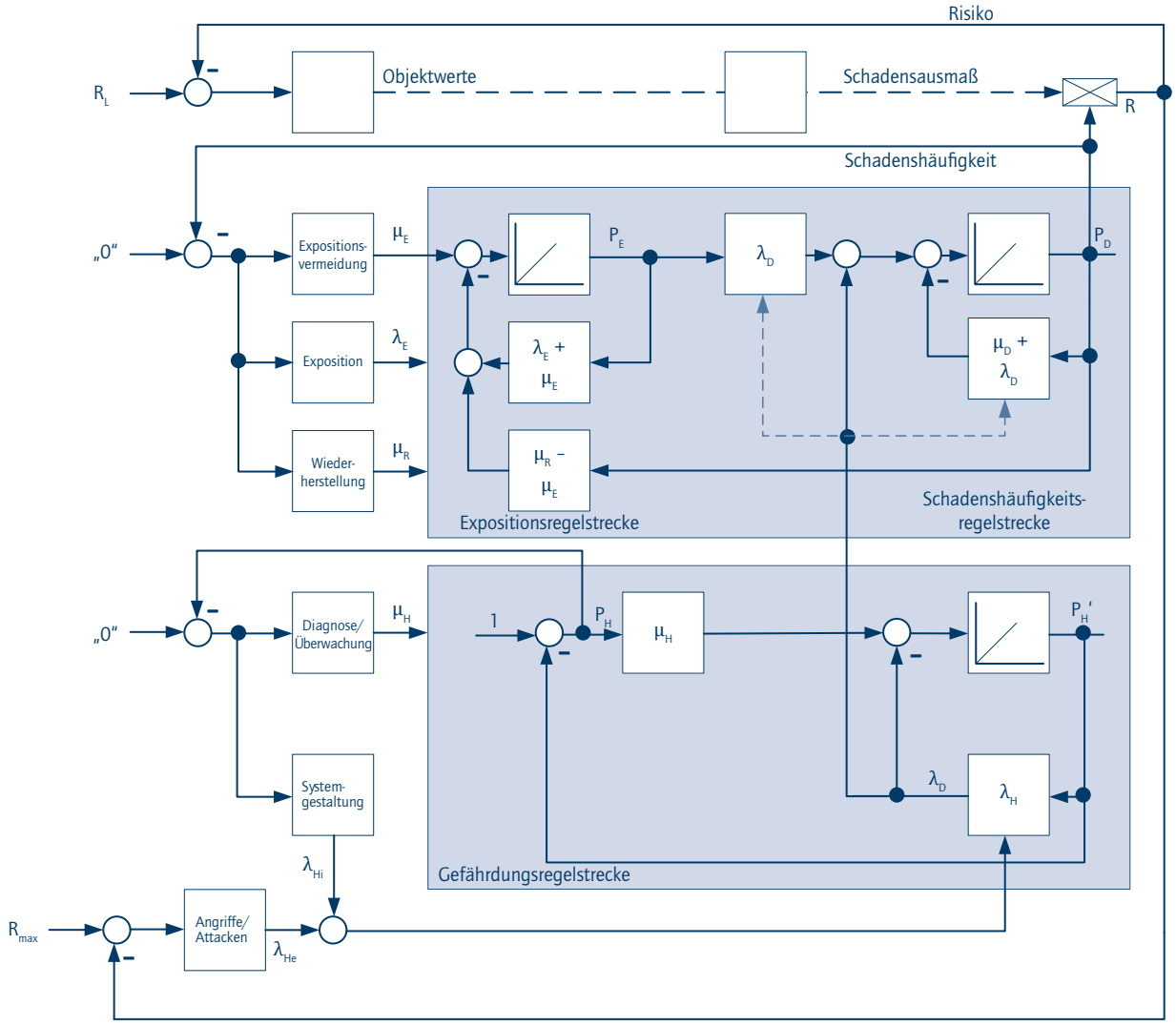


Abbildung 13: Regelungstechnisches Blockschaltbild des Expositions- und des Gefährdungsverhaltens (Quelle: eigene Darstellung)

Ausbau der technischen Überwachung von älteren Kraftfahrzeugen würde eine erhöhte Verkehrssicherheit ermöglichen. Gleiches gilt für die Assistenz und Automatisierung bei der Kraftfahrzeugführung (vergleiche [WS07]).[23]

Aus Sicht der Security ist – neben der bevorzugten Auswahl exponierter Objekte – regelungstechnisch die Gefährdungsrate als externe Störgröße aufzufassen. Beispiele dafür sind kriminalistische Delikte, Hackerattacken, aber auch terroristische Bedrohungen. Hier gilt es ebenfalls, die Gefährdungswahrscheinlichkeit durch kurzfristige Entdeckung, das heißt dynamisch durch hohe Entdeckungsfrequenz, zu minimieren. Ein Beispiel sind Hackerangriffe durch Denial of Service, welche durch schnelle Entdeckung rasch bekämpft werden können. Für kriminelle Bedrohungen wird zum Beispiel durch erhöhte Polizeipräsenz und kurzfristigen Zugriff beziehungsweise durch schnelle Rechtsprechung die Gefährdungs- und damit die Schadenswahrscheinlichkeit reduziert. Letztendlich führt nur eine extrem hohe Entdeckungsrate zu einer niedrigen Gefährdungswahrscheinlichkeit, erfordert allerdings einen hohen finanziellen, technischen oder personellen Aufwand, sodass hier eine entsprechende Kosten-Nutzen-Abwägung nach dem Prinzip *as low as reasonably practicable* (ALARP) vorgenommen wird.

Zusammenfassung und Empfehlungen

In diesem Beitrag werden methodische Ansätze für die transdisziplinäre Verlässlichkeitsforschung vorgestellt. Geeignete Termini, Beschreibungsmittel sowie Modellkonzepte symbolischer und formaler Natur sind dabei der Schlüssel zur eindeutigen Kommunikation, zu konsistenten Begriffsgebäuden und zu akzeptablen oder sogar universellen Metriken der Verlässlichkeit. Durch Abstraktion werden gemeinsame Konzepte identifiziert, konsistent formuliert, modelliert und schließlich formalisiert. Mit dieser Vorgehensweise könnte eine Theorie der Verlässlichkeit begründet werden.

Zur Verwirklichung dieses Ziels werden die folgenden fünf Thesen formuliert und mit konkreten (ingenieurmäßigen) Lösungsansätzen hinterlegt.

These 1: Kommunikation und Begriffsbildung (Terminologie)
Eine fachdisziplinübergreifende Sicherheitsforschung und -technologie erfordert eine gemeinsame Kommunikationsbasis mit harmonisierten Begriffen, Terminologien und Kommunikationsprozessen der menschlichen und organisatorischen Akteure.
Lösungsansatz: Harmonisierte Terminologie
Die Herausbildung einer harmonisierten Terminologie im Begriffsfeld der erweiterten Sicherheit beziehungsweise Verlässlichkeit im soziotechnischen Kontext ist die Basis für die zu entwickelnde gemeinsame Kommunikationsplattform. In diesem Zusammenhang müssen Modelle von Kommunikationsprozessen, die auch die Wahrnehmung von Verlässlichkeit betreffen, bei der Modellentwicklung untersucht werden, wie sie beispielsweise in der zentralen Modellierung sicherer Systeme funktioniert.

These 2: Überwindung der Vielfalt
Die Verlässlichkeit technischer und soziotechnischer Systeme kann nur nachhaltig gewährleistet werden, wenn die disziplin- und domänenspezifische Aufspaltung des Wissenschaftsgebiets „Sicherheit" überwunden wird.
Lösungsansatz: Abstraktion, Integration und Formalisierung
Voraussetzung für eine domänen- beziehungsweise disziplinübergreifende Sicht ist eine inter- und transdisziplinäre Erarbeitung von fachdisziplinübergreifender Terminologie und Modellierung. Das ist die Basis zur inter- beziehungsweise transdisziplinären Modell- und Theoriebildung. Besonderes Augenmerk ist dabei auf die Integration bestehender Methoden zu legen, wobei eine disziplinübergreifende Herangehensweise zu fokussieren ist. Zur Formalisierung der Modelle sollen in anderen Bereichen beziehungsweise Disziplinen bewährte Theorien und Beschreibungsmittel (zum Beispiel Wahrscheinlichkeitstheorie, statistische Entscheidungstheorie, linguistische Textanalyse, juristische Interpretationen) auf ihre Eignung untersucht werden, um die Untersuchungsproblematik nicht zu sehr durch ungeprüfte Ansätze zu belasten.

23 | Vgl. Wansart/Schnieder 2007.

These 3: Integration von Safety und Security

Safety- und Security-Aspekte sind bei der Entwicklung technischer wie auch soziotechnischer Systeme integriert zu betrachten, um die Gemeinsamkeiten der beiden zurzeit isolierten Sichten zu erschließen und zu nutzen und weil sich Security-Aspekte auf Safety auswirken. Daher ist eine Brücke zwischen Safety und Security zu schlagen.

Lösungsansatz: Abstraktion, Integration und Formalisierung

Es ist zwingend eine Brücke zwischen Safety- und Security-Aspekten für technische wie auch soziotechnische Systeme zu schlagen. Das erfordert eine integrierende Herangehensweise. Zahlreiche Zielkonflikte, die sich durch den erweiterten Sicherheitsbegriff frühzeitig detektieren lassen, können so rechtzeitig gelöst werden.

These 4: Sicherheit als emergente Systemeigenschaft

Sicherheit ist eine emergente Verhaltenseigenschaft komplexer Systeme. Die zunehmende Komplexität von technischen wie auch soziotechnischen Systemen erfordert eine systemische Betrachtung, auf deren Basis abstrahierte Modelle für die Sicherheit beziehungsweise Verlässlichkeit dieser Systeme gebildet werden können. Somit ist eine Systemtheorie der Verlässlichkeit beziehungsweise des erweiterten Sicherheitsverständnisses zu erarbeiten.

Lösungsansatz: Modellierung

Um dem Charakter der Systemtheorie der Sicherheit als wissenschaftliches Rückgrat der Forschung zur Verlässlichkeit technischer beziehungsweise soziotechnischer Systeme gerecht zu werden, muss die Entwicklung dieser Theorie fokussiert werden. Ziel ist es, Sicherheit als inhärente und emergente Eigenschaft von Systemen systemtheoretisch zu identifizieren, zu modellieren und qualitativ wie quantitativ zu beschreiben. Dies soll durch eine Verschränkung von sozialwissenschaftlichen und ingenieurwissenschaftlichen Ansätzen in einer transparenten Modellierung von technischen und soziotechnischen Systemen erreicht werden.

These 5: Metriken der Verlässlichkeit

Sicherheit ist eine emergente Verhaltenseigenschaft komplexer Multisysteme. Durch die Formalisierung und durch Metriken ist eine Basis für die Vergleichbarkeit zu schaffen. Grundlage dafür sind geeignete Modellkonzepte mit formalisierter Beschreibung, welche qualitative Analysen und quantitative Berechnungen zulassen.

Lösungsansatz: Kontinuierliche Verbesserung eines quantifizierten Sicherheitsniveaus

Die zielgerichtete Beeinflussung (Bewertung und Gestaltung) der Sicherheit beziehungsweise Verlässlichkeit technischer und soziotechnischer Systeme ist über die Entwicklung von standardisierten und auf Referenzgrößen beziehungsweise -werten bezogenen Sicherheitskenngrößen und deren Integration zu einer Sicherheitsmetrik möglich. Sie dient der quantitativen Bestimmung beziehungsweise Beschreibung von Verlässlichkeitseigenschaften komplexer technischer beziehungsweise soziotechnischer Systeme durch geeignete qualitative und quantitative Merkmale und Größen sowie Merkmalsausprägungen. Dies ermöglicht eine objektivierte Bestimmung der Verlässlichkeitseigenschaften.

Literatur

Von Buxhoeveden/Schnieder 2013
Von Buxhoeveden, G./Schnieder, E.: *Advanced Approaches for Traffic Safety Evaluation in Public Transport* (ITSC 2013 – 16th International IEEE Conference on Intelligent Transportation Systems), Den Haag, Niederlande, Oktober 2013.

DIN 2005
DIN-Fachbericht 144:2005-08: *Sicherheit, Vorsorge und Meidung in der Technik*, Berlin: Beuth Verlag 2005.

DIN2013
DIN EN 62551:2013-08: *Analysemethoden für Zuverlässigkeit – Petrinetze* (IEC 62551:2012); deutsche Fassung EN 62551:2012.

European Agency for Railways 2015
European Agency for Railways: *Guideline for the Application of Harmonised Design Targets (CSM-DT) for Technical Systems as Defined in (EU) Regulation 2015/1136 within the Risk Assessment Process of Regulation 402/2013*.

EU 2004
EU: *Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über Eisenbahnsicherheit in der Gemeinschaft und zur Änderung der Richtlinie 95/18/EG des Rates über die Erteilung von Genehmigungen an Eisenbahnunternehmen und der Richtlinie 2001/14/EG über die Zuweisung von Fahrwegkapazität der Eisenbahn, die Erhebung von Entgelten für die Nutzung von Eisenbahninfrastruktur und die Sicherheitsbescheinigung* (Richtlinie über die Eisenbahnsicherheit), 2004.

EU 2013
EU: *Durchführungsverordnung (EU) Nr. 402/2013 der Kommission vom 30. April 2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken und zur Aufhebung der Verordnung (EG) Nr. 352/2009, 2013*.

Jensen 1992
Jensen, K.: *Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use* (Volume 1: Basic Concepts. EATCS Monographs on Theoretical Computer Science), Springer Verlag 1992.

Maslow 1943
Maslow, A.: „A Theory of Human Motivation". In: *Psychological Review*, Vol. 50 (1943) 4, S. 377 ff.

Menne 1992
Menne, A.: *Einführung in die Methodologie*, Darmstadt: Wissenschaftliche Buchgesellschaft 1992.

Müller 2015
Müller, J. R.: *Die Formalisierte Terminologie der Verlässlichkeit Technischer Systeme*, Berlin: Springer 2015.

Ogden/Richards 1974
Ogden, Ch. K./Richards, I. A.: *Die Bedeutung der Bedeutung: eine Untersuchung über den Einfluss der Sprache und der Wissenschaft des Symbolismus*, Frankfurt: Suhrkamp 1974.

Schnieder 1999
Schnieder, E.: *Methoden der Automatisierung – Beschreibungsmittel, Modellkonzepte und Werkzeuge für Automatisierungssysteme*, Braunschweig: Vieweg 1999.

Schnieder 2010
Schnieder, L.: *Formalisierte Terminologien der Zuverlässigkeit technischer Systeme* (Dissertation, Fakultät für Maschinenbau der Technischen Universität Braunschweig, 2010), erschienen in der Schriftenreihe des Instituts für Verkehrssystemtechnik (Band 10).

Schnieder 2013
Schnieder, E.: *Ähnlichkeiten und Unterschiede zwischen Sicherheit und Zuverlässigkeit soziotechnischer Systeme* (Fachtagung Technische Zuverlässigkeit April 2013), Leonberg, 2013.

Schnieder 2017
Schnieder, L.: „Safety und Security in der Zulassung von Bahnanwendungen – Umfassende Schutzkonzepte zum Schutz kritischer Infrastrukturen im Eisenbahnsektor". In: *Der Eisenbahningenieur* 67: 7, 2017, S. 15–20.

Schnieder/Drewes 2008
Schnieder, E./Drewes, J.: „Merkmale und Kenngrößen zur Bemessung der Verkehrssicherheit". In: *Zeitschrift für Verkehrssicherheit* 54: 3, 2008, S. 117–123.

Schnieder/Schnieder 2010a
Schnieder, E./Schnieder, L.: „Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung". In: Winzer, P. et al. (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven*, Berlin: Springer Verlag 2010, S. 73–115.

Schnieder/Schnieder 2010b
Schnieder, E./Schnieder, L.: „Terminologische Präzisierung des Systembegriffs. Grundlage formaler Systembeschreibungen". In: atp edition. *Automatisierungstechnische Praxis*, 52: 9, 2010, S. 46–59.

Schnieder/Schnieder 2013
Schnieder, E./Schnieder, L.: *Verkehrssicherheit – Maße und Modelle, Methoden und Maßnahmen für den Straßen- und Schienenverkehr*, Berlin: Springer 2013.

Schnieder et al. 2009
Schnieder, L./Schnieder, E./Ständer, T.: *Railway Safety and Security – Two sides of the same coin ?!* (International Railway Safety Conference), Båstad, Sweden, 2009.

Schnieder et al. 2011a
Schnieder, L./Stein, Ch./Schielke A.G.: „Terminologiemanagementsysteme der nächsten Generation – Schlüssel für den Fachwortschatz". In: *eDITion – Fachzeitschrift für Terminologie*, 7: 1, 2011, S. 26–31.

Schnieder et al. 2011b
Schnieder, L./Stein, Ch./Schielke, A. G./Pfundmayr, M.: „Effektives Terminologiemanagement als Grundlage methodischer Entwicklung automatisierungstechnischer Systeme". In: *at – Automatisierungstechnik*, 59: 1, 2011, S. 62–70.

Schnieder/Yurdakul 2016
Schnieder, E./Yurdakul, A.: „Sind Sie sicher?" In: Hettinger, A./Neeff, M./Wermbter, K. (Hrsg.): *Babel Researched* (Braunschweiger Beiträge zu Mehrsprachigkeit und Interkulturalität), Marburg: Tectum Verlag 2016, S. 211–233.

Siti Zaharah/Yue 2008
Siti Zaharah, I./Yue, W. L.: *Methodological Framework for Developing Railway Level Crossing Safety Assessment Model Using PetriNets* (Proceedings of the 10th International Conference On The Application Of Advanced Technologies in Transportation AATT'08), Athens, Greece, May 2008.

Slovák 2006
Slovák, R.: *Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs* (Dissertation), Technische Universität Braunschweig 2006.

Slovák et al. 2008
Slovák, R./El Koursi, E. M./Tordai, L./Woods, M./Schnieder, E.: *SELCAT – A European Contribution to Level Crossing Safety*, EURAILmag 2008.

VDI 2015
Verein Deutscher Ingenieure: *VDI-Richtlinie: VDI/VDE 3682 Blatt 2 Formalisierte Prozessbeschreibungen – Informationsmodell* (VDI/VDE 3682), Düsseldorf 2015.

VDI 2017
Verein Deutscher Ingenieure: *VDI-Statusreport: Formalisierte Begriffsmodellierung*, Düsseldorf 2017.

Vose 2008
Vose, D.: *Risk Analysis – A quantitative Guide*, 3. Auflage, Hoboken, New Jersey: Wiley 2008.

Wansart/Schnieder 2007
Wansart, J./Schnieder, E.: „Qualifizierung des Nutzens von Fahrerassistenzsystemen". In: GZVB e. V. (Hrsg.): *Tagungsband des 8. Braunschweiger Symposiums „Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel – AAET"*, Braunschweig 2007, S. 103–120.

4 Integrative Theorie der Verlässlichkeit (iTV) für soziotechnische Systeme (STS)

Prof. Dr.-Ing. Bernd Bertsche
Institut für Maschinenelemente, Universität Stuttgart

Prof. Dr.-Ing. habil. Jürgen Beyerer
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
Lehrstuhl Interaktive Echtzeitsysteme, Institut für Anthropomatik und Robotik, Fakultät für Informatik am KIT Karlsruhe

Dr. phil. Claas Digmayer
Institut für Sprach- und Kommunikationswissenschaft, Textlinguistik und Technikkommunikation, RWTH Aachen

Dr. Rüdiger Goldschmidt
Zentrum für Interdisziplinäre Risiko- und Innovationsforschung, Universität Stuttgart

Prof. Dr. phil. Eva-Maria Jakobs
Institut für Sprach- und Kommunikationswissenschaft, Textlinguistik und Technikkommunikation, RWTH Aachen

Prof. Dr. Dr. h.c. Ortwin Renn
Institut für Sozialwissenschaften, Abteilung für Technik- und Umweltsoziologie, Universität Stuttgart

PD Dr.-Ing. habil. Nadine Schlüter
Fachgebiet Produktsicherheit und Qualitätswesen, Bergische Universität Wuppertal

Prof. Dr.-Ing. habil. Petra Winzer
Fachgebiet Produktsicherheit und Qualitätswesen, Bergische Universität Wuppertal

Prof. Dr. phil. habil. Johannes Weyer
Fachgebietsinhaber Techniksoziologie, Technische Universität Dortmund

Zusammenfassung

Ausfälle und steigende Rückrufe durch Fehlfunktionen von Systemen verursachen große wirtschaftliche Schäden und können Menschenleben gefährden. Die Ursachen für nicht verlässliche Systeme sind vielfältig. Sie umfassen unter anderem Kommunikationsfehler zwischen den Akteuren, mangelnde Beherrschung von Komplexität sowie fehlende oder unzureichend ausgestaltete Schnittstellen zwischen Methoden und Modellen.

Was bislang fehlt, ist eine integrative Theorie der Verlässlichkeit (iTV) als Basis für die Gestaltung verlässlicher soziotechnischer Systeme (STS). Der Ausdruck Verlässlichkeit bezeichnet die Gesamtheit der vier Eigenschaften Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit für Schutz der Umwelt vor negativen Auswirkungen des Betrachtungssystems sowie für Schutz des Systems vor Fremdeinwirkungen.[1] Die iTV wird von den Autorinnen und Autoren als erweitertes Sicherheitsverständnis gesehen. Um verlässliche STS systematisch entwickeln und nachhaltig nutzen zu können, ist es notwendig, Elemente wie Mensch, technisches System, Organisationsstruktur sowie gesellschaftliche, soziale und politische Rahmenbedingungen in ihren gegenseitigen Wechselbeziehungen und Interaktionen synergetisch zu analysieren und zielgerichtet in den konzeptionellen Rahmen von STS zu integrieren. Mittels geeigneter Beschreibungen, Modelle und Methoden sind verlässliche STS gestaltbar. Die Entwicklung eines derartigen ganzheitlichen Ansatzes erfordert die Zusammenarbeit der Ingenieurwissenschaften mit anderen Disziplinen, wie der Informatik und den Sozial- beziehungsweise Geisteswissenschaften, sowie eine integrative Theorie, die verschiedene relevante Aspekte von Verlässlichkeit systematisch aufeinander bezieht.

Eine im Sommer 2015 durchgeführte Recherche von 239 nationalen und europäischen Forschungsprojekten in verschiedenen Sicherheitsbereichen zeigt, dass es keine systemische integrative Sichtweise auf Wechselwirkungen zwischen Technik, Organisation und soziokulturellem Kontext zur Gewährleistung von Verlässlichkeit gibt. Eine integrative Theorie der Verlässlichkeit soziotechnischer Systeme fehlt. Diese zu entwickelnde Querschnittstheorie hat ein großes Potenzial zur Sicherung der Verlässlichkeit von STS und könnte einen Paradigmenwechsel einleiten, der künftigen technologischen und gesellschaftlichen Entwicklungen, wie dem Autonomen Fahren, gerecht wird.

1 | Vgl. Schnieder 2013, S. 57.

1 Ausgangssituation

Unternehmen und ihr Umfeld unterliegen einem gravierenden Wandel. Während die Digitalisierung kontinuierlich Veränderungen bei Unternehmen fordert, führen neueste, zum Beispiel adaptive Technologien zu revolutionären, für die Unternehmen nicht absehbaren Veränderungen. Gleichzeitig steigt die Anzahl der Rückrufe in allen Branchen – etwa in der Luft- und Raumfahrt, der Automobil- oder der Investitionsgüterindustrie[2] –, und infolgedessen verstärken sich die Forderungen nach verbesserter Sicherheit, Verfügbarkeit, Instandhaltbarkeit und Zuverlässigkeit. Die Autorinnen und Autoren fassen diese Forderungen unter dem Begriff Gewährleistung der Verlässlichkeit von soziotechnischen Systemen (STS) zusammen.

Verlässlichkeit umfasst die Aspekte Zuverlässigkeit (Reliability), Verfügbarkeit (Availability), Instandhaltbarkeit (Maintainability) und Sicherheit (Safety und Security), kurz RAMSS. Security beschreibt eine intendierte Gefährdung, wohingegen Safety-Fälle bei stochastisch eintretenden Schadensereignissen vorliegen.[3] Das RAMSS-Konstrukt gilt als Ausgangspunkt der Forschung. Davon ausgehend ist zu prüfen, ob weitere Randbedingungen wie Risiko, Resilienz oder Kultur im weiteren Verlauf integriert werden müssen. Nur wenn die zuvor genannten Aspekte umfassend und gemeinsam in ihren Wechselwirkungen betrachtet werden, anstatt beispielsweise „nur" Safety-Aspekte, ist eine anforderungsgerechte Gestaltung von soziotechnischen Systemen und ihren Outputs möglich.[4]

STS sind mentale Konstrukte, mit deren Hilfe die Interaktionen zwischen Menschen und technischen Artefakten verknüpft und ihre Wechselwirkungen (Organisieren von Regeln) sowie Rahmenbedingungen systemisch verstanden werden können. Ihre Maxima an funktionaler Leistung erzielen sie bei Systemelementen mit einer hohen sozialen und technischen Interaktion, wie es beispielsweise bei einem Bahnhof der Fall ist. Um Verlässlichkeit beobachten und analysieren zu können, bedarf es daher neben den Kompetenzen in Technik- und Geistes- beziehungsweise Sozialwissenschaften auch der Einsicht in deren Beziehungen und die Kontextbedingungen, wie gesellschaftliche Lebens- und Produktionsverhältnisse, die sich in wirtschaftlichen Organisationsformen, politisch-rechtlichen Rahmenbedingungen, ökonomischen Konstellationen, individuellen und sozialen Lebensstilen sowie ethischen Bewertungskriterien und Akzeptanzmustern niederschlagen. Wie dieser Forderung nach Verlässlichkeit entsprochen werden kann, ist unklar, und es muss Grundlagenforschung betrieben werden. So ist wissenschaftlich zu klären, wie

- verlässliche soziotechnische Systeme beschrieben, quantifiziert und modelliert werden können,
- verlässliche soziotechnische Systeme lebenslang garantiert werden können,
- Verlässlichkeit systemimmanenter Bestandteil von Organisationen werden kann,
- Verlässlichkeit für, mit und durch den Menschen zu gewährleisten ist.

Es gibt eine Vielzahl zum Teil stark unterschiedlicher Beschreibungen, Skalen, Modelle und Methoden diverser Fachdisziplinen (hauptsächlich Ingenieurwesen, Informatik und Sozial- beziehungsweise Geisteswissenschaften), die Teilaspekte von Verlässlichkeit wie Safety, Security, Reliability etc. prozess- oder produkt- und/oder organisationsbezogen für soziologische oder technische Systeme betrachten.[5] Aber was fehlt, ist eine Symbiose der Ansätze in abstrahierender Verdichtung.[6] Es existieren keine Untersuchungen zu organisationalen Beiträgen zur Sicherheitsgewährung[7] sowie zu systemtheoretischen Ansätzen, die Security-Systems Engineering[8] und Safety-Systems Engineering[9] vereinen. Es fehlt eine über die reine Numerik einzelner Branchen oder Domänen hinausgehende Quantifizierung, die sich an den Metriken der deskriptiven Statistik orientiert, anstatt fokussierter, nicht vereinbarer Spezialmethoden.[10] Auch der gemeinsame Aspekt menschlicher und technischer Verlässlichkeit sowie verlässliche Informations- und Kommunikationssysteme sind zu erforschen und in einem integrativen und ganzheitlichen Ansatz zu vereinen,[11] der durch eine einheitliche Begrifflichkeit auch der Divergenz und der Erosion in den Begriffsfeldern Sicherheit und Risiko entgegenwirkt.[12]

2 | Vgl. Baua 2015.
3 | Vgl. Beyerer/Geisler 2018.
4 | Vgl. Schlüter/Winzer 2016.
5 | Vgl. Schnieder/Schnieder 2018, Schlüter/Winzer 2018, Lichte/Wolf 2018.
6 | Vgl. Dhillon 2005.
7 | Vgl. Fahlruch 2000.
8 | Vgl. Beyerer 2008, Beyerer et al. 2009, Fischer et al. 2011, Kuwertz/Beyerer 2013a.
9 | Vgl. EN 954-1 1996.
10 | Vgl. Bertsche et al. 2009, Forschergruppe DFG 460, Lichte/Wolf 2018, Beyerer/Geisler 2018.
11 | Vgl. Thoma 2011, Winzer 2015, Beyerer/Geisler 2015, Fischer/Beyerer 2013, Ropohl 2012.
12 | Vgl. Schirmer 2008.

Eine im Sommer 2015 durchgeführte Recherche[13] belegt, dass es bislang an einer domänen- und techniktypübergreifenden Konzeptualisierung fehlt, die ein STS bezüglich der Verlässlichkeit betrachtet. Die Auswertung der Analyse erfolgte über ein Clustering der erfassten Forschungsprojekte nach ihrem Untersuchungsgegenstand, das heißt, inwieweit diese STS in der Makro- oder Mikroebene betrachten und ob sie Beschreibungen, Skalen, Modelle und Methoden für STS fachspezifisch oder integrativ mit dem Ziel entwickeln, Facetten der Verlässlichkeit von STS zu gewährleisten. Die analysierten ganzheitlichen Ansätze der Makroebene wie auch die interdisziplinären Konzepte der Mikroebene von STS lassen keine gemeinsamen Modelle, Methoden und Vorgehensweisen erkennen. Somit sind umfangreiche wissenschaftliche Teilergebnisse verfügbar, die noch nicht synergetisch verbunden und kohärent abgeglichen sind. Das könnte die Basis für die fehlende Systemtheorie der Verlässlichkeit sein. Ein integrativer Ansatz der Verlässlichkeit für STS auf der Makroebene ist nicht existent, wie Schlüter/Winzer 2016 nachgewiesen haben.[14]

Was insgesamt fehlt, ist eine die verschiedenen Perspektiven (Mensch, Technik, Kontext) verbindende, wissenschaftsdisziplinübergreifende Betrachtung der Verlässlichkeit von STS, das heißt eine integrative Beschreibung und Modellierung der Verlässlichkeit für STS, zum Beispiel in Form einer Unternehmung, die Beschreibungen, Skalen, Methoden und Modelle thematisch relevanter Fachdisziplinen (Ingenieurwissenschaften, Informatik, Sozial- beziehungsweise Geisteswissenschaften) zusammenführt. Der fachliche Diskursraum, der alle genannten Punkte strukturiert, ist in Abbildung 1 visualisiert.

Im Folgenden wird zunächst der Bedarf der Verlässlichkeitsforschung aus dem Blickwinkel der drei Kernelemente der STS, das heißt Maschine, Mensch und Kontext, konkretisiert. Anschließend wird aufgezeigt, dass eine wissenschaftsspezifische Forschung nicht zielführend ist, um eine grundlagenbasierte und integrative Beschreibung und Modellierung der Verlässlichkeit für soziotechnische Systeme (STS) zu entwickeln. Insbesondere mit Blick auf den gewählten Untersuchungsgegenstand „Bahnhof" müssen die drei STS-Kernelemente bezüglich des Forschungsstands analysiert und diese Erkenntnisse mit den genannten Wissenschaftsdisziplinen anschließend hinsichtlich des Handlungsbedarfes für die Entwicklung einer iTV für STS abgeglichen werden.

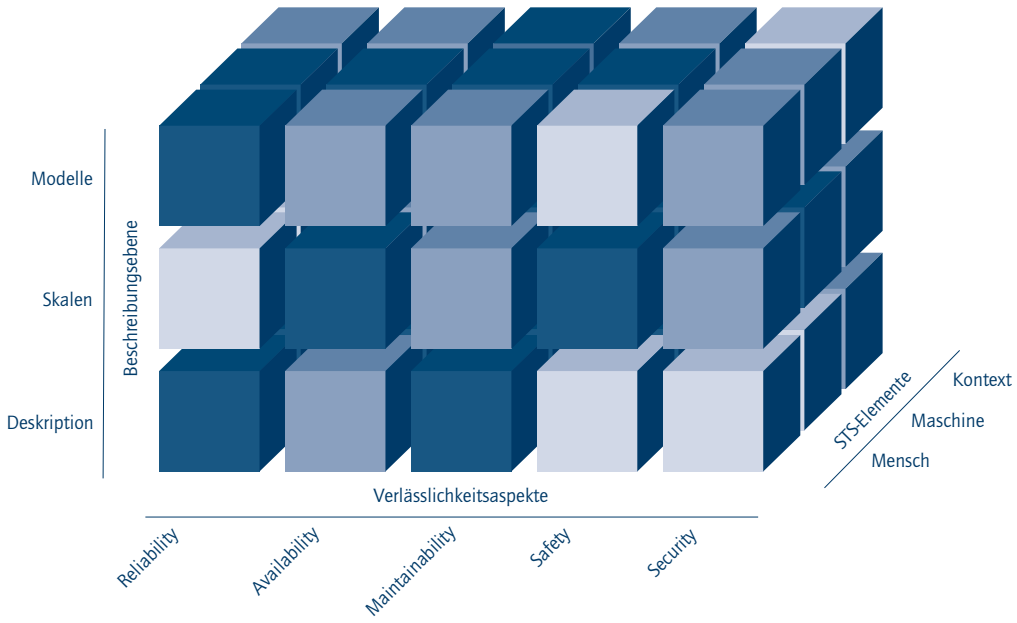


Abbildung 1: Visualisierung des fachlichen Diskursraums (Quelle: eigene Darstellung)

13 | Vgl. Schlüter/Winzer 2016.
14 | Vgl. Schlüter/Winzer 2016.

1.1 Verlässlichkeit aus der Perspektive der Maschine

Traditionsgemäß wird die technische Verlässlichkeit isoliert betrachtet. Dies bezieht sich aktuell unter anderem auf die technischen Domänen Mechanik, Elektronik und IT. Sicherheit wird ebenfalls separat als Eigenschaft der Verlässlichkeit sowohl im Bereich Safety als auch im Bereich Security untersucht.[15]

Schnieder/Schnieder 2013 beschreiben Sicherheit als emergente Eigenschaft komplexer technischer Systeme.[16] Sie leiten daraus eine Möglichkeit zur Modellierung von Verkehrssicherheit sowie Konzepte zur Risikobeherrschung ab. Bertsche/Lechner 2004 beschreiben grundlegende quantitative und qualitative Methoden zur Zuverlässigkeitsanalyse,[17] wie etwa FMEA und FTA; neben Test- und Erprobungsmethoden wird unter anderem die Modellierung reparierbarer Systeme beschrieben. Bertsche et al. 2009 zeigen Modelle und Methoden zur Zuverlässigkeitsanalyse mechatronischer Systeme, wobei auch die Zuverlässigkeitstestplanung in frühen Entwicklungsphasen betrachtet wird.

Einen Ansatz zur Anlagenmodellierung bietet Trost 2008;[18] sie nutzt Petrinetze zur Modellbildung und -analyse. Birolini 2014 beschreibt Instandhaltbarkeit und Zuverlässigkeitsplanung in Entwicklungsphasen.[19] Ergänzend werden Aspekte der Softwarezuverlässigkeit und entsprechende Modellierungsmethoden betrachtet.[20] Zuverlässigkeits- und Testplanungsmethoden werden in Meyna/Pauli 2010 vorgestellt.[21]

Kemmler/Bertsche 2014 beschreiben eine Methode zur Entwicklung zuverlässiger und gleichzeitig robuster Produkte. Der Zusammenhang zwischen Zuverlässigkeit und Robustheit wird für intralogistische Systeme betrachtet.[22] Gillepsie 2015 beschreibt eine Möglichkeit, wie Logistik- und Instandhaltungsplanung die Verfügbarkeit verbessern kann.[23]

Im Bereich der adaptiven Zuverlässigkeitsplanung werden von Stohrer 2013 Methoden beschrieben, die durch Eingriff in die Betriebsstrategie eine Verlängerung der Lebensdauer ermöglichen.[24] Sondermann-Wölke 2014 erforscht selbstoptimierende Systeme, die durch Betriebsstrategieanpassung resilient gegenüber Komponentenausfällen sind.[25] Botzler et al. 2014 beschreiben ein Entscheidungstool zur Instandhaltungsplanung und Methoden, mit denen Zuverlässigkeitsprognosen durch Nutzungsdaten verbessert werden.[26]

Die bisherigen Arbeiten bieten nur Lösungsansätze für isolierte Problemstellungen. Es fehlen domänenübergreifende (Mechanik, Elektrotechnik, IT)[27] sowie einzelaspektübergreifende (R, A, M, Sa, Se) Beschreibungen und Modelle.[28] Derzeit ist zum Beispiel eine durchgängige Analyse und Gestaltung von verlässlichen technischen Systemen über alle Lebenszyklusphasen hinweg nicht möglich. Dass dieser Missstand zur Gefährdung von Menschenleben (und ebenso zur Gefährdung von Unternehmen) führen kann, zeigte beispielsweise die Explosion der Bohrplattform „Deepwater Horizon" im Jahr 2010.

1.2 Verlässlichkeit aus der Perspektive des Menschen

Ein wesentliches Element von STS und ihrer Verlässlichkeit sind die darin agierenden Menschen. Ihr Handeln wird durch viele verschiedene Faktoren beeinflusst, zum Beispiel bildungsbiografisch, soziokulturell und professionell geprägte Wertesysteme, Grundannahmen, Motive sowie Persönlichkeitseigenschaften.

Die Arbeitswissenschaft befasst sich unter anderem mit der Arbeit des Menschen im Fertigungssystem und damit, wie die Kompetenzen der Beschäftigten durch eine geeignete Zuordnung zu Arbeitsvorgängen gefördert werden können.[29] Die Berufspädagogik betrachtet Kompetenzentwicklung bezogen auf die Weiterentwicklung

15 | Vgl. Schlüter/Winzer 2016.
16 | Vgl. Schnieder/Schnieder 2013.
17 | Vgl. Bertsche/Lechner 2004.
18 | Vgl. Trost 2008.
19 | Vgl. Birolini 2014.
20 | Vgl. Krasich 2015.
21 | Vgl. Meyna/Pauli 2010.
22 | Vgl. Wildner 2013.
23 | Vgl. Gillepsie 2015.
24 | Vgl. Stohrer et al. 2013.
25 | Vgl. Sondermann-Wölke 2014.
26 | Vgl. Botzler et al. 2014.
27 | Vgl. Schlüter/Winzer 2018, Weyer et al. 2018.
28 | Vgl. Lichte/Wolf 2018, Beyerer/Geisler 2018.
29 | Vgl. Schlick et al. 2010.

der Angestellten wie auch den Unternehmenserfolg und konzentriert sich auf die Aneignung einer umfassenden beruflichen Handlungskompetenz.[30] Es wird nicht untersucht, inwieweit die Arbeitskräfte im Prozess der Arbeit verlässlich ihre Aufgaben erledigen und einen verlässlichen Prozessablauf garantieren. Vielfach wird die Notwendigkeit konstatiert, eigene Instrumente zur Erfassung von Kompetenzen in Unternehmen zu entwickeln.[31] Dafür wurden aktuelle Verfahren konzipiert. Fragen der Verlässlichkeit des Menschen im Arbeitsprozess werden in den genannten Disziplinen jedoch nicht betrachtet.

Für Sicherheit und Zuverlässigkeit ist es in den genannten Disziplinen essenziell, dass in Entscheidungssituationen die Option gewählt wird, bei der das Risiko eines Schadens minimiert und die Funktionsfähigkeit des Systems sichergestellt wird. Je komplexer Entscheidungssituationen ausfallen, desto schwieriger wird es für die Entscheidungsverantwortlichen, die vielfältigen Optionen zu überschauen und eine rational begründbare Auswahl zu treffen. Dabei wenden Individuen intuitive Heurismen (Faustregeln) der Entscheidungsfindung an, die nur zum Teil der Komplexität der Materie angemessen sind.[32] Dies sind Heurismen der Verfügbarkeit, Verankerung, Repräsentativität und affektiven Aufladung.[33] Die Heurismen führen aber häufig auch in die Irre, weil sie komplexe Sachverhalte unsachgemäß vereinfachen und den Entscheidungsverantwortlichen eine Sicherheit des eigenen Urteils vorgaukeln, die nach bestem Wissen aller Expertinnen und Experten nicht gerechtfertigt ist.

Sensible Punkte der Verlässlichkeit betreffen insbesondere die Kooperations-, Schnittstellen- und Sicherheitskommunikation[34] sowie das Verhältnis formaler Kommunikation (die Kommunikationsflüsse offiziell regelt) zu informeller Kommunikation (in der berufliches Erfahrungswissen „unter der Hand" weitergegeben wird[35]). Es gibt wenige Studien, die den Einfluss kommunikativer Praktiken auf Verlässlichkeit an sich und ihre Komponenten systematisch betrachten und modellieren. Vielversprechende Ansätze bietet unter anderem die Akteur-Netzwerk-Theorie.[36] Zu Krisen-, Risiko-, Präventions- und Sicherheitskommunikation gibt es einige Forschungsprojekte, die den Begriff der Kommunikation jedoch oft sehr weit fassen und eher selten die Ebene konkreter sprachlich-diskursiver Praktiken erreichen.

Die systematische Verankerung und Erfassung „menschbezogener" Größen in einer Theorie der Verlässlichkeit soziotechnischer Systeme bedarf somit entsprechender Grundlagenforschung, um Fehlentscheidungen zu reduzieren beziehungsweise zu vermeiden.[37]

1.3 Verlässlichkeit aus der Perspektive des Kontextes

Der Kontext von STS ist in den weiteren und den engeren Kontext gegliedert. Während sich der engere Kontext mit der Organisation und dem physischen Umfeld befasst, betrachtet der weitere Kontext das soziale Umfeld und die Regulierung.

Bezüglich des engeren Kontextes ist als Beispiel der VW-Abgasskandal zu nennen.[38] Dieser zeigt, dass die Regeln in Unternehmen (das heißt das Organisieren der Elemente und die Wechselbeziehungen eines STS) deren Verlässlichkeit bestimmen. Angeregt durch Perrow[39] sind Sozialforscherinnen und -forscher der empirischen Frage nachgegangen, welche Eigenschaften das Organisieren des STS als Instrument der Unternehmensführung[40] besitzen muss, um hochkomplexe und eng gekoppelte technische Systeme verlässlich steuern zu können.[41] In diesem Kontext wird Zuverlässigkeit als Leistung des Managements verstanden, um zu einem effektiven System der Intervention, Antizipation und Überwachung zu gelangen. Organisationen, die eine hohe Zuverlässigkeit anstreben, müssen folgende Probleme in ihren Managementplänen berücksichtigen:[42]

- Fehler und Irrtümer sind allgegenwärtig, heimtückisch und können überall auftauchen; der Preis des Erfolgs ist somit die immerwährende Wachsamkeit.

30 | Vgl. Denbostel 2007.
31 | Vgl. BiP 2008, Becker/Spöttel 2015, Denkena et al. 2013.
32 | Vgl. Kahneman 2011, S. 102, Silver 2012, S. 142 ff.
33 | Vgl. Jungermann et al. 2010, S. 169 ff., Renn 2014, S. 186 ff.
34 | Vgl. Jakobs 2008, Jakobs et al. 2011.
35 | Vgl. Brünner 2000.
36 | Vgl. Latour 2005, Rauer 2012, Villiger 2014.
37 | Vgl. Raabe 2018, Beyerer/Geisler 2018.
38 | Vgl. Spiegel 2015.
39 | Vgl. Perrow 1984, Perrow 1990, Perrow 1992.
40 | Vgl. Schulte-Zurhausen 2014.
41 | Vgl. Roberts 1989, Roberts/Gargano 1990, Schulman 1993, Rochlin 1993.
42 | Vgl. Rochlin 1993, Renn et al. 2007, S. 86 ff.

- Quellen von Fehlern und Irrtümern sind dynamisch und nicht statisch, sodass die Überwachungsmechanismen selbst stetig erneuert und wiederbelebt werden müssen.
- Permanente Gefahrenquelle ist die Betriebsumwelt, die eine ständige Wachsamkeit erfordert, gerade auch (und besonders) zu jenen Zeiten, in denen die Dinge gut zu laufen scheinen.
- Redundante Methoden zur Problemlösung müssen auf der operationalen Ebene aufrechterhalten werden. Dem Druck, Prozesse durch die Einführung einer einzigen, „besten" Lösung festzuschreiben oder zu „rationalisieren", sollte widerstanden werden.
- Vielfache gleichzeitige informelle Organisationsstrukturen müssen geschaffen, aufrechterhalten und angewendet werden, um sich Eventualitäten anpassen zu können (strukturelle Variationen gemäß der Natur der Probleme).
- Organisatorische Verpflichtungen zur Antizipation sowie reaktive Methoden, die sich mit realen und potenziellen Problemen beschäftigen, müssen vorhanden sein.
- Selbstverbesserung und Selbstregulierung sollten nicht beschränkt werden, solange organisatorische Ressourcen und Zeit zur Verfügung stehen, sodass zusätzliche Informationen als Mittel der Kontrolle und der Begrenzung von Ungewissheiten immer grenzkosteneffektiv sind.

Ein Höchstmaß an Sicherheit und Resilienz gegenüber Überraschungen zählt zu den Grundbedürfnissen des Menschen und somit zum organisationalen Bestandteil eines STS. Um hohe Verlässlichkeit zu erreichen, sind technische Systeme so auszurichten, dass die Komplexität der Steuerung der Steuerungskapazität der Managementorganisation entspricht und eng gekoppelte Systeme durch Puffer und Redundanzen abgefedert werden.[43] Zudem sind innerhalb des STS klare Zuständigkeiten, ein offener Kommunikationsfluss, eine Kultur der Achtsamkeit und Wachsamkeit sowie ständige Mitarbeiterschulung und -betreuung essenziell.[44]

Bezüglich des weiteren Kontextes von STS ist dem Umstand Rechnung zu tragen, dass STS unter bekannten wie noch nicht bekannten Rahmenbedingungen operieren. Diese sind vielfältig; sie umfassen sozioökonomische, legale und kulturelle Umweltbedingungen (lokal, national, international), Regeln und Standards, die verfügbaren materiellen wie immateriellen Ressourcen, Klima- und Umweltbedingungen sowie weitere Punkte. Es gibt Studien und Projekte, die in unterschiedlicher Qualität und Quantität den Einfluss von Randbedingungen auf Aspekte von Verlässlichkeit wie Zuverlässigkeit, Verfügbarkeit, Instandsetzung und Sicherheit (Safety und Security) untersuchen; es existiert allerdings kein Ansatz, der diese Aspekte systematisch in ihrem Zusammenspiel und Einfluss auf STS erfasst, modelliert und bewertet. Es gibt jedoch vielversprechende Ansätze, die sich dafür eignen, Closed-World-Einschränkungen aufgrund des Systementwurfs unter der Annahme bestimmter Randbedingungen mittels Adaptions- und Lernmechanismen zur Systemlaufzeit zu überwinden. Das reicht von der Nachführung von Systemparametern bis hin zum Lernen neuer Objekt- und Relationskonzepte, die zur Entwurfszeit als Randbedingung noch nicht bekannt waren.[45]

Forschungsbedarf besteht in der Frage, wie die Rahmenbedingungen, unter denen sich Verlässlichkeit herausbildet, erfasst, modelliert und aufeinander bezogen werden können und welche Rahmenbedingungen gegeben sein müssen, damit die Verlässlichkeit eines STS auf dem gewünschten Niveau gewährleistet und aufrechterhalten werden kann.

2 Handlungsbedarfe für eine iTV aus Sicht der Fachdisziplinen

Im Folgenden werden Handlungsbedarfe aus Sicht der von den Autorinnen und Autoren repräsentierten Wissenschaftsdisziplinen dargestellt.

2.1 Ingenieurperspektive

Die Ingenieurwissenschaften, die für die Entwicklung einer Theorie der Verlässlichkeit die Basis bilden, setzen sich unter anderem mit technischen Systemen, deren Produktion, Fabrikorganisation und dem Zusammenspiel von Mensch und Technik auseinander, wobei kontinuierlich neue Erkenntnisse anderer Forschungsdisziplinen aufgegriffen und in Kooperation mit diesen weiterentwickelt werden.

Bezüglich der Verlässlichkeitsforschung bestehen unter anderem Handlungsbedarfe, die sich aus der Erweiterung klassischer Fragestellungen des Ingenieurwesens um soziotechnische Aspekte ergeben. Relevante Forschungsbereiche betreffen die Verbindung bestehender quantitativer und qualitativer RAMSS-Modelle mit sozialwissenschaftlichen Aspekten, die Erforschung von

43 | Vgl. Winzer et al. 2010.
44 | Vgl. Thoma 2011.
45 | Vgl. Kuwertz et al. 2015, Kuwertz/Beyerer 2013b, Kuwertz/Schneider 2013, Kuwertz 2012a, Kuwertz 2012b, Pfrommer et al. 2013.

Schnittstellen zwischen bewährten Modellen der Zuverlässigkeitstechnik zu neuen, technikfremden Modellen, die domänenübergreifende Modellverknüpfung sowie die Anwendbarkeit und Übertragbarkeit bestehender Modelle in weitere Domänen.

Dementsprechend ergeben sich folgende Handlungsbedarfe:

- Schaffung einer adäquaten integrativen Beschreibung (Deskription) relevanter Sachverhalte, Zusammenhänge und Wirkungsmechanismen inklusive qualitativer Merkmale und quantitativer Größen,
- Zusammenführung, Weiterentwicklung und Nutzung etablierter Beschreibungsmittel, Skalen, Modelle und Methoden für die Analyse von Systemen, die Ableitung von darauf basierenden Schlussfolgerungen (Inferenz) sowie die Optimierung bestehender und der Entwurf (Synthese) neuer Systeme im Hinblick auf deren Verlässlichkeit,
- Quantifizierung RAMSS-bezogener Aspekte.

2.2 Informatikperspektive

Im Zuge von Industrie 4.0 hat die Informatik ganz entscheidende Bedeutung für die Zukunftsfähigkeit von Unternehmen gewonnen. Diese Erkenntnisse sollen in die aktuelle Forschung einfließen und für die zu entwickelnde iTV abstrahiert und integriert werden.

Eine iTV für STS soll nicht nur eine Deskription, sondern auch Analyse, Inferenz, Synthese und Optimierung erlauben. Es muss ein Kalkül entworfen werden, der entscheidbar ist und mit dem gerechnet werden kann. Beschreibungssprache und Kalkül müssen geeignet sein, die Komplexität realer STS abzubilden und zu beherrschen.[46] Selbst einfache STS sind sehr komplex, sodass Risikoberechnung und -optimierung nicht mehr exakt durchgeführt werden können.[47] Dies erfordert geeignete Metriken sowie effiziente approximative Algorithmen, die eine ausreichend genaue und schnelle Risikoberechnung erlauben.

Unter anderem ergeben sich folgende Handlungsbedarfe:

- Formalismen für die verlässlichkeitsbezogene dynamische Interaktion der Akteure von STS sowie Modellierung von zufälligen, strategischen, rationalen und irrationalen Verhaltenskomponenten,
- Entwicklung von Algorithmen zur effizienten Risikoberechnung und verlässlichkeitsbezogenen Simulation von STS,
- Entwicklung verlässlichkeitsförderlicher Verfahren für die Mensch-Maschine-Interaktion,
- Verstehen der Verantwortlichkeit von Operateur und Computersteuerung, etwa bei autonomen Prozessen oder in der Zuordnung von Überwachungsfunktionen im Zusammenspiel von IT und Operateur.

2.3 Perspektive der Geistes- und Sozialwissenschaften

Es ergeben sich zahlreiche Forschungsbedarfe, wie zum Beispiel die folgenden:

- Konzepte zur produktiven Verarbeitung unbekannter Ereignisse, Sachverhalte und sich verändernder Rahmenbedingungen durch den Menschen,
- Bestimmung der Beschaffenheit individueller Handlungsweisen, die Risiken verstärken oder abschwächen (zum Beispiel für die Mensch-Maschine-Interaktion),
- frühzeitige Erkennung und Überwindung individueller Fehlurteile und Heurismen in komplexen Entscheidungssituationen,
- Bestimmung der Auswirkung von Kommunikation, Interaktion und Kultur auf die Verlässlichkeit von STS sowie Ableitung von Konzepten und Maßnahmen verlässlichkeitsfördernder Kommunikation und Interaktion.

3 Stand von Wissenschaft und Technik

Eine europaweite Recherche zu relevanten Forschungsprojekten ergab 239 themenbezogene Projekte diverser Forschungsprogramme und Institutionen (Horizon 2020, 7. EU-Rahmenprogramm, DFG, BMWI, BMBF, BA Sicherheit und Informationstechnik, AiF, VDI, VDE, acatech).[48] Sie behandeln aber jeweils nur Einzelaspekte der Verlässlichkeit.

Die umfangreichen Rechercheergebnisse bezogen auf EU-, DFG-, Ministeriums- und AiF-Forschungsprojekte wurden unter anderem dahingehend geprüft, inwieweit Anforderungen wie „integrativer Ansatz", „ganzheitlicher Ansatz" oder „fachdisziplinärer Ansatz bezüglich Modellen, Methoden oder Vorgehenskonzepten" erfüllt werden (siehe Abbildung 2).

46 | Vgl. Schnieder 2012.
47 | Vgl. Schnieder/Schnieder 2013.
48 | Vgl. Schlüter/Winzer 2016.

Projekt	Typ	Titel des Forschungsprojekts	Quelle (Internetlink)	Integrativer Ansatz	Ganzheitlicher Ansatz	Fachdisziplinärer Ansatz			Transdisziplinäre Theorie der Verlässlichkeit
						Modelle	Methoden	Vorgehenskonzepte	
...	...	...	...	...	...	...	...	...	...
7EU Programm	Collaborative project (generic)	Security Impact Assessment Measure - A decision support system for security technology investments	http://cordis.europa.eu/project/rcn/97990_en.html	1	0	1	1	1	0
...	...	...	...	...	...	...	...	...	...
DFG	Forscher-gruppen	Entwicklung von Konzepten und Methoden zur Ermittlung der Zuverlässigkeit mechatronischer Systeme in frühen Entwicklungsphasen	http://gepris.dfg.de/gepris/projekt/5354095	1	1	1	1	1	0
...	...	...	...	...	...	...	...	...	...

Abbildung 2: Ausschnitt aus den Rechercheergebnissen (Quelle: eigene Darstellung)

Dies wurde mit dem Ziel realisiert, den Grad der Anforderungserfüllung (1 = erfüllt, 0 = nicht erfüllt) als Maß für die Nutzbarkeit von Forschungsprojektergebnissen und für das Abstraktionspotenzial zu verwenden. Für Forscherinnen und Forscher dient dieses Rechercheergebnis somit auch als Kompass und Datenbasis bezüglich der Weiternutzung aktueller nationaler und internationaler Forschungsergebnisse für die Entwicklung einer iTV.

4 Ziele

Die Autorinnen und Autoren verstehen die integrative Verlässlichkeit von STS als ein Themenfeld, das sich von Reliability über Availability, Maintainability bis hin zu Security und Safety erstreckt sowie eine Vielzahl maschinen-, mensch- und kontextbezogener Aspekte umfasst. Bislang fehlt eine Theorie, die die genannten Aspekte ganzheitlich betrachtet.

Ziel zukünftiger Arbeiten ist die Überwindung des nachgewiesenen Forschungs- und Praxisdefizits durch die Entwicklung einer integrativen Theorie der Verlässlichkeit für soziotechnische Systeme (iTV für STS), die entlang der Beschreibungsebene von der Deskription über Skalen bis hin zu Modellen die ganzheitliche Abbildung eines STS bezüglich der Verlässlichkeit ermöglicht.

Die Autorinnen und Autoren sehen folgende Anforderungen an die Entwicklung einer iTV für STS: Es ist ein (I) ganzheitlicher und (II) integrativer Ansatz der Verlässlichkeit für STS zu entwickeln, der eine (III) einheitliche Deskription aufweist und auf Basis von untereinander abgestimmten (IV) Skalen miteinander vernetzbare (V) Modelle und Methoden zusammenführt, die eine verlässliche Auslegung von STS ermöglichen. Die im Sommer 2015 durchgeführte Recherche zu deutschen und europäischen Forschungsprojekten im Bereich Verlässlichkeit zeigt, dass die Anforderungen I) bis V) für eine iTV für STS nur ansatzweise erfüllt sind, sie jedoch ein reiches Repertoire an Einzelerkenntnissen für die Herleitung einer neuen Wissenschaftstheorie bieten. Hieraus kann ein integrativer Ansatz entwickelt werden. Die Geschichte der Wissenschaften zeigt, dass fachspezifische Betrachtungsweisen oft erst durch die additive Verbindung von Einzelaspekten oder durch Abstraktion und Verallgemeinerung zu einer übergeordneten theoretischen Integration führten. Dabei sind die folgenden grundlegenden Forschungsfragen zu klären:

- Können durch das integrative Betrachten verschiedener verlässlichkeitsrelevanter Forschungsfelder Zusammenhänge erkannt, Dopplungen vermieden und Synergien gestiftet werden?
- Gibt es Möglichkeiten, zukünftige Herausforderungen durch erstmalig fachdisziplinübergreifende Modellkonzepte und ihre einheitliche Formalisierung zu analysieren?
- Ist eine Änderung der Blickrichtung von einer reaktiven zu einer präventiven Sichtweise zur Gewährleistung der Verlässlichkeit von STS möglich?

Ein Screening der Fachbereiche zeigt für die iTV eine Vielzahl an Forschungsthemen, Zielen und Lösungsansätzen. Bezüglich der **Verlässlichkeit von Maschinen** ist zu erforschen, wie technische Systeme verlässlich über ihren Lebenszyklus hinweg funktionieren. Dies schließt folgende Schwerpunkte mit ein:

- Quantifizierung der Verlässlichkeit eines STS anhand einer formalen, probabilistischen Systembeschreibung,
- quantitative Bewertung der Vulnerabilität technischer Systeme und Infrastrukturen,

- Kopplung verschiedenartiger Verlässlichkeitsmethoden,
- Verlässlichkeit von digitalen Modellen (oder eingeschränkt: Simulationsmodellen) als STS in der Planung,
- verlässliche Instandhaltung von technischen Systemen,
- Predictive Maintenance oder im weiteren Sinne Prognostics and Health Management (PHM).

Die **Verlässlichkeit von Menschen** ist hinsichtlich der Verlässlichkeitsmechanismen im menschlichen Arbeitskontext zu untersuchen, was folgende Aspekte beinhaltet:

- Modelle und Methoden zur Schätzung menschlicher Zuverlässigkeit und ihre Integration in die Methoden zur Gestaltung verlässlicher STS,
- subjektive Faktoren,
- Erweiterung von Zuverlässigkeitsmethoden um soziotechnische Aspekte.

Zudem ist der **Kontext** zu erforschen. Im engeren Kontext ist zu untersuchen, wie Organisationen verlässlich zu gestalten sind. Hierbei ist unter anderem die Gewährleistung von Verlässlichkeit bezüglich multikultureller Organisationen zu betrachten. Sozialpsychologische Mechanismen in STS mit mehr als einem Operateur sind zu verstehen und integrative Methoden zur Analyse und Beurteilung der Verlässlichkeit von Mensch-Maschinen-Interaktionen zu entwickeln. Ein weiteres Themenfeld ist IT-Sicherheit sowie die Sicherheit durch Organisationen im Sinne von Nachhaltigkeit. Die Bestimmung von Verlässlichkeitsanforderungen an Organisationen und relevanter, verlässlichkeitssensibler Organisationsmerkmale sowie deren Auswirkungen sind entlang der Organisationsprozesse zu bestimmen und mit den Kompetenzen der Menschen in diesen Organisationen zu koppeln.

Bezüglich des weiteren Kontextes der Verlässlichkeit ist das Erfassen, Verstehen und Systematisieren von Systemen im Kontext der Verlässlichkeit zu fokussieren. Hier sind folgende Themenschwerpunkte zu nennen:

- domänenübergreifende Quantifizierung der Verlässlichkeit,
- Reduzierung der Komplexität umfassender soziotechnischer Aspekte,
- Entwicklung eines übergreifenden/allgemeinen Verlässlichkeitsmodells unter Einbeziehung unterschiedlicher Umweltfaktoren und Detailbetrachtung der Mensch-Maschinen-Interaktion,
- Compliance von STS,
- Interaktion Mensch-Maschine-soziale Umgebung,
- Automatisierbarkeit von Sicherungsfunktionen,
- dynamische Konvergenz individueller Informationsstände durch adäquate Kommunikation sowie Gewährleistung von Verlässlichkeit durch ein ausreichend kohärentes Verständnis des Systemzustands.

Ziel des Forschungsvorhabens ist die Überwindung des nachgewiesenen Forschungs- und Praxisdefizits durch die Entwicklung einer integrativen Theorie der Verlässlichkeit für soziotechnische Systeme (iTV für STS) einschließlich entsprechender Deskriptionen, Skalen und Modelle.

5 Fazit und Ausblick

Es ist festzustellen, dass Verlässlichkeit im allgemeinen und fachspezifischen Sprachgebrauch zahlreiche Aspekte aus allen Lebenslagen in Gesellschaft, Wirtschaft und Technik umfasst. Die Fülle an Aspekten zeigt, dass zur zielgerichteten Bearbeitung ein gemeinsamer Startpunkt festgelegt werden muss. Zur Beschreibung der Verlässlichkeit verständigen sich die Autorinnen und Autoren aus diesem Grund auf die Aspekte Reliability, Availability, Maintainability, Safety und Security als integrativem Startpunkt. Inwieweit diese Definition im Rahmen weiterer Forschungsarbeiten anzupassen beziehungsweise zu ergänzen ist, ist bislang offen.

Eine ganzheitliche Betrachtung zur Gewährleistung der Verlässlichkeit von STS ist nicht existent. In der Fachliteratur gibt es eine Reihe von Forschungsansätzen, die sich mit Zuverlässigkeit von technischen Systemen aus Ingenieurperspektive, mit Resilienz aus sozial- und geisteswissenschaftlicher Sicht, mit Sicherheit aus Informatik- und Ingenieurperspektive, mit Bedrohung von Organisationen von innen und außen jeweils aus Ingenieur- und Informatik- oder geisteswissenschaftlicher Sichtweise auseinandersetzen. Gleiches trifft auf die Risiken innerhalb von STS zu. Es fehlt aber eine fachdisziplinübergreifende Betrachtung der Verlässlichkeit von STS. Im Rahmen einer Vielzahl von EU-, BMBF- und DFG-geförderten Projekten werden entweder fachspezifische Aspekte der Verlässlichkeit oder Teilaspekte der Verlässlichkeit modelliert beziehungsweise Methoden hierfür entwickelt. Diese zahlreichen Einzelerkenntnisse betrachten jeweils nur einzelne Facetten der Verlässlichkeit; eine synergetische Integration besteht nicht. Die Recherche verdeutlicht auch den Bedarf der Entwicklung einer integrativen Theorie für die Verlässlichkeit von STS.

Aus der Wissenschaftsgeschichte ist erkennbar, dass eine solche Situation nur durch einen Paradigmenwechsel beherrschbar ist. Beispiele hierfür sind die Maxwell'sche Theorie in der

Elektrodynamik oder die Wiener'sche Kybernetik. Folglich stellen die Autorinnen und Autoren die These auf, dass aufgrund der vielfältigen gegenwärtigen Forschungserkenntnisse der Zeitpunkt für die Entwicklung einer iTV für STS günstig ist. Diverse Einzelerkenntnisse aus Fachdisziplinen liegen bereits vor. Allerdings fehlt eine Verdichtung und Abstimmung zu einer disziplinübergreifenden Theorie.

Ziel ist die Entwicklung einer integrativen Beschreibung und Modellierung der Verlässlichkeit soziotechnischer Systeme, die Teilaspekte wie Safety, Security, Instandhaltbarkeit, Zuverlässigkeit und Verfügbarkeit subsummiert und diese auf praktische Anwendungen wie zum Beispiel in Produktion und Dienstleistung überträgt. Insgesamt lassen die geplanten Forschungsaktivitäten wichtige Beiträge für ein erweitertes Sicherheitsverständnis erwarten.

Literatur

Baua 2015
Baua (2015): Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. URL: http://www.baua.de/de/Produktsicherheit/Produktinformationen/Rueckrufe-2015/07-BICO.html [Stand: 14.09.2015].

Becker/Spöttel 2015
Becker, M./Spöttel, G.: „Berufliche (Handlungs-)Kompetenzen auf der Grundlage arbeitsprozessbasierter Standards messen". In: *bwp@ Berufs- und Wirtschaftspädagogik – online*, Ausgabe 28, 1-19. URL: http://www.bwpat.de/ausgabe28/becker_spoettl_bwpat28.pdf [Stand: 15.09.2015].

Bertsche/Lechner 2004
Bertsche, B./Lechner, G.: *Zuverlässigkeit im Fahrzeug- und Maschinenbau: Ermittlung von Bauteil- und System-Zuverlässigkeiten*, Berlin: Springer-Verlag 2004.

Bertsche et al. 2009
Bertsche, B./Göhner, P./Jensen, U./Schinköthe, W./Wunderlich, H.-J.: *Zuverlässigkeit mechatronischer Systeme: Grundlagen und Bewertung in frühen Entwicklungsphasen*, Berlin: Springer-Verlag 2009.

Beyerer 2008
Beyerer, J.: „Sicherheitsforschung als umfassende Aufgabe". In: *Jubiläumsausgabe Strategie und Technik,* 51. Jahrgang, Report Verlag Sulzbach/Ts, Februar/März 2008, S. 102–105.

Beyerer et al. 2009
Beyerer, J./Geisler, J./Dahlem, A./Winzer, P.: „Sicherheit: Systemanalyse und -design". In: Winzer, P./Schnieder, E./Bach, F. (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven*, Berlin: Springer 2010, S. 39–72.

Beyerer/Geisler 2015
Beyerer, J./Geisler, J.: „A Quantitative Risk Model for a Uniform Description of Safety and Security". In: Beyerer, J./Meissner, A./Geisler, J. (Hrsg.): *Proceedings of the Security Research Conference: 10th Future Security* (Berlin, 15th–17th September 2015), S. 317–324.

Beyerer/Geisler 2018
Geisler, J./Beyerer, J.: „Formaler Rahmen für eine einheitliche quantitative Beschreibung des Risikos bezüglich Safety und Security". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

BiP 2008
Bundesinstitut für Berufsbildung (Hrsg.): „Internationale Vergleichsstudie in der Berufsbildung („Large-Scale-Assessment")". In: *Berufsbildung in Wissenschaft und Praxis – BWP*, 2008, Beilage zu 1/2008.

Birolini 2014
Birolini, A.: *Reliability Engineering: Theory and Practice*, Heidelberg: Springer 2014.

Botzler et al. 2014
Botzler, M./Zeiler, P./Bertsche, B.: „Failure Prediction by Means of Advanced Usage Data Analysis". In: Institute of Electrical and Electronics Engineers (IEEE) (Hrsg.): *Annual Reliability and Maintainability Symposium: Proceedings*, Colorado Springs 2014.

Brünner 2000
Brünner, G.: *Wirtschaftskommunikation*, Tübingen: Niemeyer 2000.

Denbostel 2007
Denbostel, P.: *Lernen im Prozess der Arbeit*, Münster: Waxmann Verlag 2007.

Denkena et al. 2013
Denkena, B./Scharin, F./Merwart, M.: *Concept Base Process Planning for the Workshop Production in Production Engineering Research and Development*, Vol. 7, Berlin: Springer 2013, S. 299–308.

Dhillon 2005
Dhillon, J. S.: *Reliability, Quality, and Safety for Engineers*, CRC Press 2005.

EN 954-1 1996
DIN EN 954-1:1996: *Sicherheit von Maschinen. Sicherheitsbezogene Teile von Steuerungen*, Beuth Verlag 1996.

Fahlruch 2000
Fahlruch, B.: *Vom Unfall zu den Ursachen – Empirische Bewertung von Analyseverfahren* (Dissertation), Ruhr-Universität Bochum 2000.

Fischer et al. 2011
Fischer, Y./Bauer, A./Beyerer, J.: „A Conceptual Framework for Automatic Situation Assessment". In: *Proceedings of the Conference on Cognitive Methods in Situation Awareness and Decision Support*, 2011, S. 234–239.

Fischer/Beyerer 2013
Fischer, Y./Beyerer, J.: „Ontologies for Probabilistic Situation Assessment in the Maritime Domain". In: *Proceedings of the IEEE Conference on Cognitive Methods in Situation Awareness and Decision Support*, San Diego 2013, S. 105–108.

Forschergruppe DFG 460
DFG Forschergruppe 460: *Systemzuverlässigkeit – Entwicklung von Konzepten und Methoden zur Ermittlung der Zuverlässigkeit mechatronischer Systeme in frühen Entwicklungsphasen*. URL: http://www.ima.uni-stuttgart.de/forschung/bereich_zuv/abgeschlossene/forschergruppe_460/ [Stand: 10.09.2015].

Gillepsie 2015
Gillepsie, A. M.: „Reliability & Maintainability Applications in Logistics & Supply Chain". In: *Institute of Electrical and Electronics Engineers (IEEE): Annual Reliability and Maintainability Symposium: Proceedings*, Palm Harbor 2015.

Jakobs 2008
Jakobs, E.-M.: „Unternehmenskommunikation. Arbeitsfelder, Trends und Defizite". In: Niemeyer, S./Dieckmannshenke, H. (Hrsg.): *Profession und Kommunikation*, Frankfurt/M.: Lang 2008, S. 13–31.

Jakobs et al. 2011
Jakobs, E.-M./Fiehler, R./Eraßme, D./Kursten, A.: „Industrielle Prozessmodellierung als kommunikativer Prozess. Eine Typologie zentraler Probleme". In: *Gesprächsforschung 12*, 2011, S. 223–264.

Jungermann et al. 2010
Jungermann, H./Pfister, H.-R./Fischer, K.: *Die Psychologie der Entscheidung – Eine Einführung*, Berlin, Heidelberg: Spektrum Akademischer Verlag 2010.

Kahneman 2011
Kahneman, D.: *Thinking Fast and Slow*, London, New York: Penguin 2011.

Kemmler/Bertsche 2014
Kemmler, S./Bertsche, B.: *Systematic Method for Axiomatic Robustness-Testing (SMART). 1st International Symposium on Robust Design*, Kopenhagen 2014.

Krasich 2015
Krasich, M.: „Modeling of SW Reliability in Early Design with Planning and Measurement of Its Reliability Growth". In: Institute of Electrical and Electronics Engineers (IEEE) (Hrsg.): *Annual Reliability and Maintainability Symposium: Proceedings*, Palm Harbor 2015.

Kuwertz 2012a
Kuwertz, A.: „Extending Object-Oriented World Modeling for Adaptive Open-World Modeling" (Technischer Bericht IES-2012-06). In: Beyerer, J./Pak, A.: *Proceedings of the 2012 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory*, Karlsruhe: KIT Scientific Publishing 2012.

Kuwertz 2012b
Kuwertz, A.: „Towards Adaptive Open-World Modeling" (Technischer Bericht IES-2011-10). In: Beyerer, J./Pak, A.: *Proceedings of the 2011 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory*, Karlsruhe: KIT Scientific Publishing 2012.

Kuwertz et al. 2015
Kuwertz, A./Goldbeck, C./Hug, R./Beyerer, J.: „Towards Web-based Semantic Knowledge Completion for Adaptive World Modeling in Cognitive Systems". In: *Proceedings of the UKSIM-AMSS 17th International Conference on Modelling and Simulation (UKSim2015),* 2015, S. 165–170.

Kuwertz/Beyerer 2013a
Kuwertz, A./Beyerer, J.: „Quantitative Measures for Adaptive Object-Oriented World Modeling". In: *Proceedings of 4th Workshop on Dynamics of Knowledge and Belief* (36th German Conference on Artificial Intelligence), Fernuniversität Hagen 2013, S. 89–104.

Kuwertz/Beyerer 2013b
Kuwertz, A./Beyerer, J.: *Knowledge Model Quantitative Evaluation for Adaptive World Modeling.* IEEE Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA 2013), San Diego 2013.

Kuwertz/Schneider 2013
Kuwertz, A./Schneider, G.: *Ontology-Based Meta Model in Object-Oriented World Modeling for Interoperable Information Access* (International Conference on Systems ICONS), Sevilla 2013.

Latour 2005
Latour, B.: *Reassembling the Social. An Introduction to Actor-Network-Theory*, New York 2005.

Lichte/Wolf 2018
Lichte, D./Wolf, K.-D.: „Quantitative Analyse der Vulnerabilität am Beispiel Verkehrsflughafen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Meyna/Pauli 2010
Meyna, A./Pauli, B.: *Zuverlässigkeitstechnik: Quantitative Bewertungsverfahren*, München: Hanser 2010.

Perrow 1984
Perrow, C.: *Normal Accidents – Living with High-Risk Technologies*, New York: Basic Books 1984.

Perrow 1990
Perrow, C.: *Normale Katastrophen: Die unvermeidbaren Risiken der Großtechnik*, Frankfurt am Main: Campus 1990.

Perrow 1992
Perrow, C.: „Unfälle und Katastrophen – ihre Systembedingungen". In: *Journal für Sozialforschung 1*, 1992, S. 61–75.

Pfrommer et al. 2013
Pfrommer, J./Schleipen, M./Beyerer, J.: *Fähigkeiten adaptiver Produktionsanlagen*, Atp edition 55: 11, München: Deutscher Industrieverlag 2013, S. 42-49..

Raabe 2018
Raabe, O.: „Datenschutz- und IT-sicherheitsrechtliche Risikomodelle". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Rauer 2012
Rauer, V.: „Interobjektivität: Sicherheitskultur aus Sicht der Akteur-Netzwerk-Theorie". In: Daase, Chr./Offermann, Ph./Rauer, V. (Hrsg.): *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*, Frankfurt am Main/New York 2012, S. 69–91.

Renn 2014
Renn, O.: D*as Risikoparadox. Warum wir uns vor dem Falschen fürchten*, Frankfurt am Main: Fischer Taschenbuch 2014.

Renn et al. 2007
Renn, O./Schweizer, P.-J./Dreyer, M./Klinke, A.: *Risiko aus sozialökologischer Perspektive*, München: OEKOM Verlag 2007.

Roberts 1989
Roberts, K. H.: *New Challenges in Organizational Research: High Reliability Organizations. Industrial Crisis Quarterly*, 3, 1989, S. 111–125.

Roberts/Gargano 1990
Roberts, K. H./Gargano, G.: „Managing a High-Reliability Organization: A Case for Interdependence". In: Glinow, M. A./Mohrmann, S. A.: *Managing Complexity in High Technology Organizations*, New York, Oxford: Oxford University Press 1990, S. 146–159.

Rochlin 1993
Rochlin, G. I.: „Defining ‚High Reliability' Organizations in Practice: A Taxonomic Prologue". In: Roberts, K. H.: N*ew Challenges to Understanding Organizations*, New York: Macmillan 1993, S. 11–32.

Ropohl 2012
Ropohl, G.: *Allgemeine Systemtheorie – Einführung in transdisziplinäres Denken*, Berlin: Edition Sigma 2012.

Schirmer 2008
Schirmer, W.: *Bedrohungskommunikation: Eine gesellschaftstheoretische Studie zu Sicherheit und Unsicherheit*, Vs Verlag 2008.

Schlick et al. 2010
Schlick, C. M./Buder, R./Luscher, H.: *Arbeitswissenschaft*, Heidelberg: Springer Verlag 2010.

Schlüter/Winzer 2016
Schlüter, N./Winzer, P.: „Qualitätswissenschaft als Bestandteil der geforderten Verlässlichkeitsforschung zu soziotechnischen Systemen". In: Refflinghaus, R./Kern, C./Klute-Wenig, S. (Hrsg.): *Qualitätsmanagement 4.0 – Status Quo! Quo vadis?*, Bericht zur GQW-Jahrestagung 2016 in Kassel, Kasseler Schriftenreihe Qualitätsmanagement Band 6, Kassel University Press, Kassel, 2016, S. 207–226.

Schlüter/Winzer 2018
Schlüter, N./Winzer, P.: „Bedeutung des Systems Engineering für die Entwicklung einer Systemtheorie der Sicherheit". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schnieder 2012
Schnieder, E.: *Towards A Theory Of Safety*. 17th International Conference of the Society for Design and Process Science (SDPS), Berlin 2012.

Schnieder 2013
Schnieder, E.: *Ähnlichkeiten und Unterschiede zwischen Sicherheit und Zuverlässigkeit soziotechnischer Systeme*, 26. Fachtagung Technische Zuverlässigkeit 2013 (TTZ 2013), Leonberg.

Schnieder/Schnieder 2013
Schnieder, E./Schnieder, L.: *Verkehrssicherheit: Maße und Modelle, Methoden und Maßnahmen für den Straßen- und Schienenverkehr*, Berlin: Springer Vieweg 2013.

Schnieder/Schnieder 2018
Schnieder, E./Schnieder, L.: „Formalisierung von Begriffen der Sicherheit und Sicherheitsmetriken". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schulman 1993
Schulman, P. R.: „The Analysis of High Reliability Organizations, A Comparative Framework". In: Roberts, K. H.: *New Challenges to Understand Organizations*, London, New York: Macmillan 1993, S. 33–54.

Schulte-Zurhausen 2014
Schulte-Zurhausen, M.: *Organisation*, München: Franz Vahlen 2014.

Silver 2012
Silver, N.: *The Signal and The Noise*, New York: Penguin 2012.

Sondermann-Wölke 2014
Sondermann-Wölke, C.: *Entwurf und Anwendung einer erweiterten Zustandsüberwachung zur Verlässlichkeitssteigerung selbstoptimierender Systeme*, Aachen: Shaker Verlag 2014.

Spiegel 2015
Spiegel (2015): *Abgasaffäre*. URL: http://www.spiegel.de/auto/aktuell/volkswagen-fuenf-millionen-autos-der-marke-vw-muessen-in-die-werkstatt-a-1055329.html [Stand: 05.10.2015].

Stohrer et al. 2013
Stohrer, M./Kemmler, S./Koller, O./Bertsche, B.: *Zuverlässigkeitsorientierte Online-Optimierung von Betriebsstrategien mechatronischer Produkte*, Stuttgarter Symposium für Produktentwicklung (SSP), Stuttgart 2013.

Thoma 2011
Thoma, K. (Hrsg.): *European Perspectives on Security Research*, Berlin: Springer 2011.

Trost 2008
Trost, M.: *Gesamtheitliche Anlagenmodellierung und -analyse auf Basis stochastischer Netzverfahren* (Dissertation), Stuttgart: Berichte aus dem Institut für Maschinenelemente, 128, 2008.

Villiger 2014
Villiger, C.: „Unsichtbare Gefahren. Risikokommunikation im Spannungsfeld von Technikvermittlung, Sicherheitskultur, Akzeptanz und Partizipation". In: Banse, G./Rothkegel, A. (Hrsg.): *Neue Medien. Interdependenzen von Technik, Kultur und Kommunikation*, trafo 2014, S. 103–120.

Weyer et al. 2018
Weyer, J./Adelt, F./Konrad, J./Hoffmann, S.: „Agentenbasierte Simulation des Risikomanagements soziotechnischer Systeme mit dem Simulator SimCo". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Wildner 2013
Wildner, C.: „Robustheit: Eine Anforderung an intralogistische Systeme". In: *Logistics Journal,* 10, 2013, S. 1–11. URL: http://www.logistics-journal.de/proceedings/2013/3770/wildner_2013wgtl.pdf {Stand: 15.09.2015}.

Winzer et al. 2010
Winzer, P./Schnieder, E./Bach, F.-W. (Hrsg.): *Sicherheitsforschung: Chancen und Perspektiven* (acatech DISKUTIERT), Berlin: Springer 2010.

Winzer 2015
Winzer, P.: „Generic System Description and Problem Solving in Systems Engineering". In: *IEEE Systems Journal*, Volume: PP, Issue: 99, 2015, S. 1–10.

5 Formaler Rahmen für eine einheitliche quantitative Beschreibung des Risikos bezüglich Safety und Security

Prof. Dr.-Ing. habil. Jürgen Beyerer
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
Institut für Anthropomatik und Robotik am Karlsruher Institut für Technologie KIT

Dr. Jürgen Geisler
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB

Zusammenfassung

Der vorliegende Aufsatz stellt einen formalen mathematischen Rahmen vor, der „Risiko" im Kontext von Sicherheitsproblemen soziotechnischer Systeme (STS)[1] quantitativ und in einer alle Aspekte des Problemkontexts umfassenden Weise beschreibt. Eine scharf definierte Notation und wohlbegründete Begrifflichkeiten sind dafür notwendige Grundlagen.

Dieser grundlegende Beitrag ist eine überarbeitete und erweiterte Fassung unserer Aufsätze „A Framework for a Uniform Quantitative Description of Risk with Respect to Safety and Security" im European Journal for Security Research 2016.[2]

Eine quantitative Formulierung des Risikos ist das Schlüsselkonzept dieses Aufsatzes. Unsicherheiten werden mit dem Wahrscheinlichkeitskalkül modelliert, Risiko durch rein stochastische Gefahrenquellen wird durch objektive Wahrscheinlichkeiten und Kosten beschrieben. Dagegen wird das Risiko von Individuen (sogenannten intelligenten Agenten) aus deren jeweils eigener Sicht, das heißt vollständig gestützt auf deren subjektive Bewertung möglicher Kosten und deren subjektive Einschätzung der Häufigkeit des Auftretens kostenträchtiger Vorfälle, bemessen. Somit wird Wahrscheinlichkeit im Bayes'schen Sinne als „Grad des Dafürhaltens" (Degree of Belief – DoB) gedeutet.

Das Risiko wird mit den Mitteln der statistischen Entscheidungstheorie und der Spieltheorie quantitativ auf Basis eines Modells dreier streng voneinander unterschiedener Rollen beschrieben: „Gefahrenquelle", „Schutzbedürftiger" und „Schützer".

Die Menge D der Gefahrenquellen ist ausgestattet mit einer DoB-Verteilung, welche die Wahrscheinlichkeit des Auftretens von Gefahrenereignissen beschreibt. D ist in drei Untermengen eingeteilt, die drei mögliche Gefahrengründe umfassen: zufällige Gefährdung, Gefährdung aufgrund von Fahrlässigkeit und willentliche Gefährdung.

Jedem Schutzbedürftigen ist eine Menge von sogenannten „Flanken der Verwundbarkeit" F zugeordnet. Sie charakterisieren verschiedene Aspekte der Verwundbarkeit: mechanische, physiologische, informationelle, wirtschaftliche, reputatorische, psychologische und so weiter. Diese Flanken der Verwundbarkeit sind mit bedingten DoB-Verteilungen ausgestattet, die beschreiben, in welchem Maße ein Vorfall oder ein Angriff mit Wirkung auf die jeweilige Flanke schädlich ist. Zusätzlich ist jede Flanke mit einer Kostenfunktion belegt, welche die Kosten beziffert, die dem Schutzbedürftigen durch einen Vorfall mit Schadenswirkung oder einen Angriff über diese Flanke entstehen würden.

Mit diesen Ingredienzen kann das Risiko für einen Schutzbedürftigen auf Grundlage eines auf alle Gefahrenquellen und alle Flanken der Verwundbarkeit bezogenen Ensemble-Funktionals beziffert werden. Abhängig von der jeweiligen Teilmenge betrachteter Gefährdungen ist dieses Funktional im Falle zufälliger oder aus Fahrlässigkeit herbeigeführter Gefährdungen ein Erwartungswert. Im Falle absichtlich herbeigeführter Gefährdung ist es ein Auswahloperator, da der Angriff voraussichtlich auf die schwächste Flanke der Verwundbarkeit zielt.

Das so berechnete Risiko kann dann den Kosten für Schutzmaßnahmen gegenübergestellt werden, die der Rollenträger Schützer anbietet. Damit wird eine wesentliche Voraussetzung für wirtschaftlich rationale Entscheidungen bezüglich Investitionen in Schutzmaßnahmen geschaffen.

Aus Sicht eines Angreifers wird eine Nutzenfunktion aufgestellt, die ein im Sinne seines eigenen Vorteils rational handelnder Angreifer voraussichtlich verwenden würde, um sein

1 | Unter einem soziotechnischen System (STS) sind eine organisierte Menge von Menschen und mit diesen verknüpfte Technologien zu verstehen, welche in einer bestimmten Weise strukturiert sind, um ein spezifisches Ergebnis zu produzieren. Quelle: Wikipedia 2018.

2 | Vgl. Beyerer/Geisler 2016 sowie Beyerer/Geisler 2015.

Kosten-Nutzen-Verhältnis als Grundlage der Entscheidung über einen Angriff beziehungsweise dessen Optionen zu bestimmen.

Die Herausforderung des vorgestellten Risikomodells besteht in der Bestimmung der Kostenfunktionen und insbesondere der Wahrscheinlichkeiten (DoBs). Zwei Ansätze zur Bestimmung von DoBs werden hier vorgestellt und diskutiert: das „Maximum-Entropie-Prinzip" (MEP) und das „Conditioning On Rare Events" (CORE).

Zur Dynamisierung des Modells wird eine diskretisierte Zeit eingeführt, die alle veränderlichen Größen parametrisiert. Übergänge von einem Zeitschritt zum nächsten werden durch einen Transitionsoperator beschrieben, der alle Wechselwirkungen zwischen Akteuren und Objekten vermittelt.

Die räumlichen Dimensionen von Liegenschaften, die von STS eingenommen werden und auf denen sich das STS zeitlich abspielt, werden durch einen attribuierten Graphen modelliert. Auf den Knoten und Kanten dieses Graphen tummeln sich die modellierten Akteure und Objekte und wechselwirken miteinander. Der Graph stellt eine sparsame Datenstruktur dar, um die räumlich-zeitliche Entwicklung eines STS effizient simulieren zu können.

Das Modell kann verwendet werden, um die Gefährdung des Schutzbedürftigen quantitativ zu simulieren und zu evaluieren, zum Beispiel mit einer Implementierung mittels Softwareagenten, bei der die Agenten in ihren Rollen als Schutzbedürftige, Gefährder und Schützer jeweils mit Kostenfunktionen und DoBs des hier vorgestellten formalen Rahmens ausgestattet sind.

1 Einführung

Der Begriff Sicherheit kann, ohne dass es dafür wörtliche Entsprechungen in der deutschen Sprache gibt, in die beiden Aspekte Safety und Security unterteilt werden. Kurz gefasst – und unten detaillierter ausgeführt – beschreibt Safety die Sicherheit vor zufälligen oder unbeabsichtigten, Security die Sicherheit vor beabsichtigten Gefährdungen. Die beiden Aspekte haben trotz ihrer begrifflichen Unterscheidung viele Gemeinsamkeiten. Dennoch werden Maßnahmen und Systeme zur Gewährleistung von Safety und Security oft unabhängig voneinander und von unterschiedlichen Fachleuten geplant und umgesetzt. Würden die beiden Aspekte integriert und im Zusammenhang betrachtet, könnten Synergien genutzt und Kosten gesenkt werden.

Wenn wir Safety und Security von komplexen Systemen wie kritischen Infrastrukturen und soziotechnischen Systemen sicherstellen wollen, müssen die Perspektiven zahlreicher Disziplinen einbezogen werden: Technik, Recht, Wirtschaft, Sozial- und Geisteswissenschaften und viele andere mehr.

Bis heute hat sich keine gemeinsame formale Sprache zur Bewältigung von Safety- und Security-Problemen etabliert, schon gar nicht über alle beteiligten Disziplinen hinweg.[3] Ziel dieses Aufsatzes ist es, einen mathematischen Ansatz vorzustellen, der dazu dienen soll, Safety- und Security-Probleme einheitlich zu beschreiben und zu analysieren, um damit die Grundlage für eine gezielte Planung und Optimierung von Sicherheitsmaßnahmen bereitzustellen.

1.1 Verwandte Arbeiten

Statistische Entscheidungstheorie und Spieltheorie bieten reife und bewährte Methodengerüste, die in vielen unterschiedlichen Domänen Verwendung finden, vor allem in den Wirtschaftswissenschaften.[4] In Verbindung mit Bedrohungsbäumen (Attack Trees) wurde die Spieltheorie bereits angewandt, um einen „rationalen" Angreifer zu modellieren.[5] Einige Aspekte der mit diesem Aufsatz vorgeschlagenen Herangehensweise wurden bereits in einer vorausgehenden qualitativen Formulierung vorgestellt.[6]

5.2 Safety und Security

Die Begriffe Safety und Security ergeben nur dann Sinn, wenn eine Gefährdung, das heißt ein Potenzial für schädliche Ereignisse, vorliegt. Die Gefährdung geht von einer Gefahrenquelle d aus (d für das englische „danger"), breitet sich auf einem Übertragungsweg aus und wirkt auf einen Schutzbedürftigen s (Abbildung 1). Der Übertragungsweg ist alles zwischen d und s, was erforderlich ist, um die Gefährdungswirkung zu übertragen; er gehört weder zu d noch zu s.

Im Fall beispielsweise eines funkferngezündeten Sprengsatzes umfasst dieser Pfad sowohl die Funkstrecke vom Auslöser zum Sprengsatz als auch die Luftstrecke zwischen Sprengsatz und Ziel, welche die Bombensplitter überwinden müssen. Im Fall

3 | Vgl. Müller-Quade 2018.
4 | Vgl. Berger 1993.
5 | Vgl. Buldas et al. 2006.
6 | Vgl. Beyerer et al. 2010, Beyerer 2009.

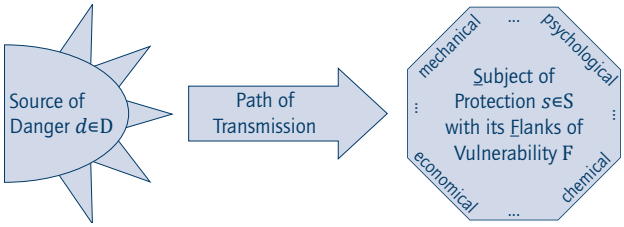


Abbildung 1: Relation zwischen der Gefahrenquelle d und dem Schutzbedürftigen s. D und S benennen die jeweiligen Mengen (Quelle: eigene Darstellung).

eines Tsunami ist es die Wassermasse zwischen dem Epizentrum eines Erdbebens und dem Küstenstreifen, dem das Schutzinteresse gilt.

Die Gefährdung d trifft den Schutzbedürftigen s an einer oder mehreren „Flanken der Verwundbarkeit" f, die in der Menge F zusammengefasst sind und von ganz unterschiedlicher Art sein können: mechanisch, chemisch, psychologisch, finanziell, informationell und so weiter. Die Flanken der Verwundbarkeit gehören zu dem Schutzbedürftigen s und unterliegen dessen Kontrolle.

Die beiden oben genannten Beispiele – Sprengsatz und Tsunami – illustrieren zwei fundamentale Kategorien von Gefährdungen: gewollte und ungewollte oder zufällige. Gewollte Gefährdungen gehören in die Domäne der Security, ungewollte oder zufällige hingegen in den Bereich der Safety. Gewollte Gefährdungen können auf der einen Seite angedroht oder ausgeübt werden, um ein bestimmtes (zum Beispiel materielles) Ziel zu erreichen, beispielsweise im Fall eines Raubs. Oder sie können als Selbstzweck ausgeführt werden, beispielsweise bei einem Amoklauf oder Vandalismus. Die Quelle ungewollter Gefährdung hingegen kann zum einen menschliche Fahrlässigkeit sein, wobei die Schadenswirkung unterschätzt oder ignoriert wird, zum anderen kann es ein zufälliger Vorfall wie ein unvorhersehbarer technischer Fehler oder ein überraschendes Naturereignis wie ein Erdbeben sein. Abbildung 2 zeigt die entsprechende Kategorisierung.

Aus spieltheoretischer Sicht gibt es eine weitere interessante Interpretation von Safety und Security.[7] Mit Bezug zu Safety spielt der Schutzbedürftige s ein Spiel gegen die Natur (siehe Abbildung 3). Sein „Gegner" verhält sich gemäß einem Zufallsprozess. Mit statistischer Analyse kann die Verteilung, die den „Gegner" kennzeichnet, gelernt und es können auf dieser Basis

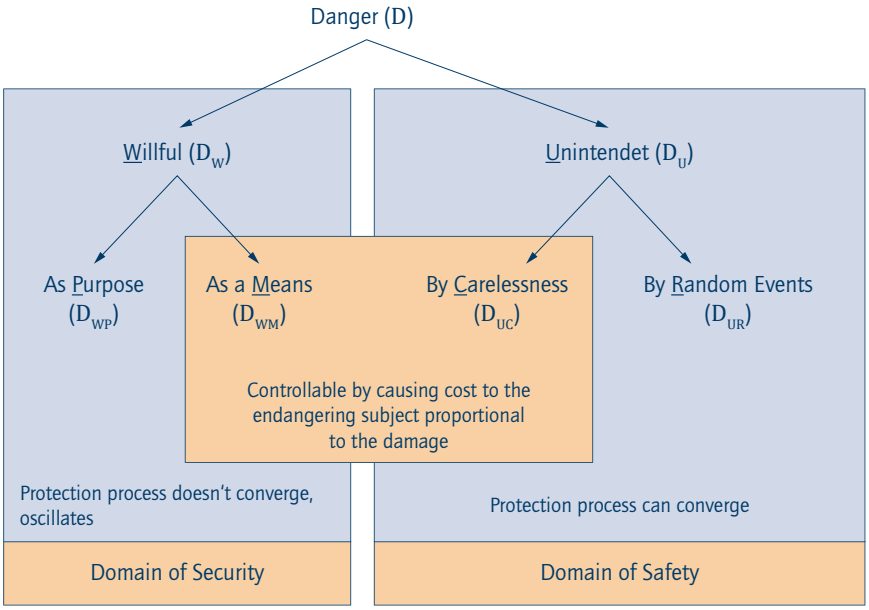


Abbildung 2: Kategorisierung von Gefährdungen in Safety und Security. Die Elemente d der Menge D_W werden Angreifer, die der Menge D_U Verursacher genannt. Im Fall eines Angreifers $d \in D_{WM}$ (Gefährdung als Mittel) oder eines Verursachers $d \in D_{UC}$ (Gefährdung durch Fahrlässigkeit) kann das betreffende Risiko durch Beaufschlagung von d mit Kosten beeinflusst werden, sodass d von einem Angriff abgeschreckt oder zu vorsichtigerem Verhalten veranlasst werden kann (Quelle: eigene Darstellung).

7 | Vgl. Beyerer et al. 2010.

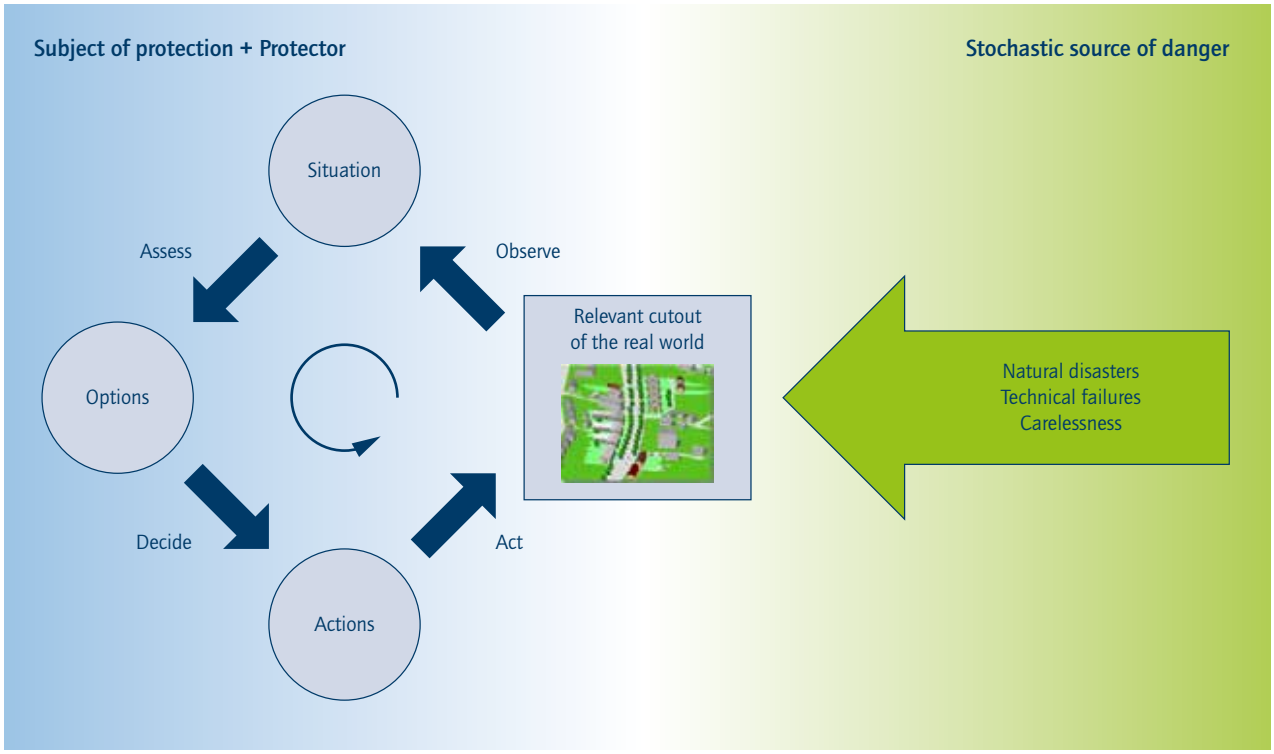


Abbildung 3: Spieltheoretische Sicht auf Safety (Quelle: eigene Darstellung)

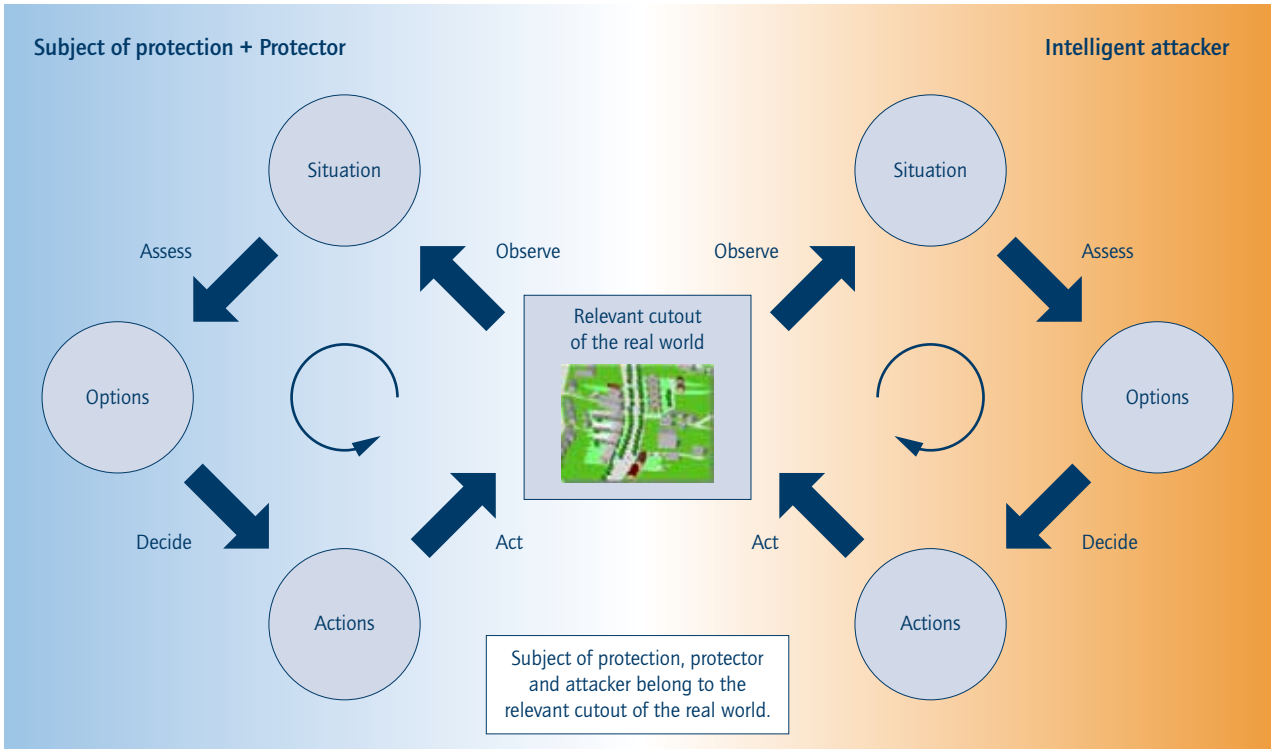


Abbildung 4: Spieltheoretische Sicht auf Security (Quelle: eigene Darstellung)

Gegenmaßnahmen zur Risikominderung geplant und angewandt werden. Insbesondere dann, wenn sich die Verteilung nicht ändert, kann allein mit passiven, statischen Maßnahmen ein gewünschtes stationäres Sicherheitsniveau erreicht und gehalten werden. Der Schutzprozess kann konvergieren (siehe Abbildung 2, rechte Seite).

Betrachtet man dagegen die Domäne der Security, verhält sich der Gegner intelligent (siehe Abbildung 4). In diesem Fall „spielt" s gegen einen Gegner, der sich strategisch verhält und sich dem Verstandenwerden zu entziehen versucht, der die Schwachpunkte von s analysiert und seinen eigenen Nutzen zu maximieren trachtet. So wird jede Maßnahme mit einer Gegenmaßnahme beantwortet und kein stationärer Zustand erreicht. Der Schutzprozess oszilliert also (siehe Abbildung 2, linke Seite).

Aus dem bisher Diskutierten erschließt sich auch ein weiterer Aspekt: Ein rationaler Angreifer zielt nicht auf zufällig ausgewählte Flanken der Verwundbarkeit. Vielmehr wird er seinen Angriff auf die Flanken richten, die für ihn am erfolgversprechendsten sind.

Für die Domäne der Security lässt sich damit folgendes **Minimumprinzip** postulieren: Die schwächste Flanke bestimmt den Grad der Verwundbarkeit.

Darüber hinaus hängt es ausschließlich von der Gefahrenquelle d ab, ob wir uns in der Domäne der Security oder derjenigen der Safety befinden. Weder der Übertragungsweg noch der Schutzbedürftige s bestimmen dies (siehe Abbildung 1). Wenn beispielsweise Feuer von einem Brandstifter gelegt wurde, handelt es sich um einen Security-Fall. Wird das Feuer hingegen von einem elektrischen Kurzschluss ausgelöst, liegt ein Safety-Fall vor. Was den Übertragungsweg und den Schutzbedürftigen betrifft, so brauchen die beiden Fälle nicht unterschieden zu werden, da sie die gleichen Folgen nach sich ziehen.

3 Rollen und Risikomodell

3.1 Rollen

Das Ziel jeder Maßnahme zur Erhöhung von Sicherheit ist es, den Schutzbedürftigen vor Schädigungen durch eine Gefährdung zu bewahren. Dafür führen wir eine weitere Rolle neben s und d ein: den Schützer (Protektor) p. Der Schützer spielt zuallererst eine Rolle, deren tragende Entität nicht notwendigerweise von der für s getrennt ist. Wenn sich ein s selbst schützt, dann sind s und p zwei Rollenausprägungen derselben Entität. Mit der Einführung von p können wir sämtliche Schutzmaßnahmen auf diese Rolle konzentrieren. Diese sind (siehe Abbildung 5): eine Gefahrenquelle entdecken und sie möglicherweise neutralisieren sowie den Übertragungsweg verlängern, um gegebenenfalls. die Gefährdungswirkung abzuschwächen, den Schutzbedürftigen zu decken und dessen Flanken der Verwundbarkeit zu härten. Eine notwendige Voraussetzung für die Beziehung zwischen dem Schutzbedürftigen und seinem Schützer, also für den Fall, dass s und p verschiedene Entitäten sind, ist Vertrauen, oft bestätigt durch einen Vertrag.

Um die Beziehung zwischen den drei Rollen mit Abbildung 5 zu vervollständigen, muss klargemacht werden, dass es außer für unbeabsichtigte Gefährdung durch zufällige Vorfälle (siehe Abbildung 2 und Abbildung 3) immer einen Wertfluss von s nach d gibt. Dies wird ausgedrückt durch die Relation „s bereichert d"

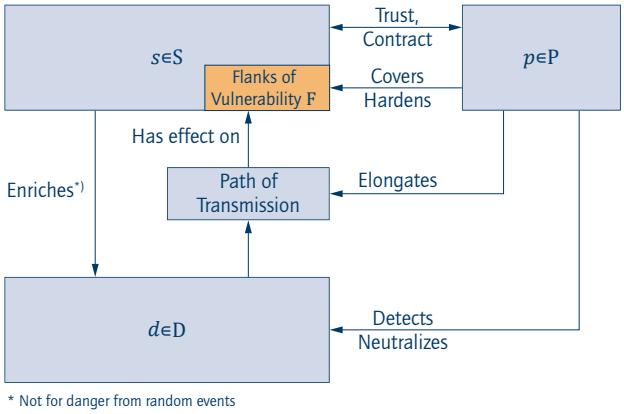


Abbildung 5: Rollen und deren Beziehungen untereinander. Verschiedene Rollen können von unterschiedlichen Entitäten eingenommen werden, können aber auch in einer Entität zusammenfallen. So kann sich jemand selbst schützen, sich aber auch selbst gefährden (Quelle: eigene Darstellung).

3.2 Formalisierung der Bestandteile

In diesem Kapitel werden Entitäten, Attribute und Relationen entsprechend den oben erläuterten Überlegungen formalisiert und quantifiziert. Die Formulierung stützt sich auf die statistische Entscheidungstheorie nach Bayes.[8]

8 | Vgl. Berger 1993.

3.2.1 „Degree of Belief" – Interpretation von Wahrscheinlichkeit

Der zwingenden Argumentation von Lindley folgend[9] werden sämtliche Unsicherheiten auf Basis von Wahrscheinlichkeiten modelliert. In vorliegendem Aufsatz wird Wahrscheinlichkeit im erweiterten Sinne als „Grad des Dafürhaltens" (*Degree of Belief*, kurz DoB) verstanden.[10] Diese Interpretation ist eine Verallgemeinerung der klassischen frequentistischen Bedeutung von Wahrscheinlichkeit, die dennoch kompatibel mit den zugrunde liegenden Kolmogorov'schen Axiomen ist.[11] Abbildung 6 illustriert dieses Konzept.

Die Axiome Kolmogorovs definieren Wahrscheinlichkeit als maßtheoretisches Konzept. Doch sie legen nur die Syntax fest, also die Art und Weise, wie mit Wahrscheinlichkeiten gerechnet werden muss, sagen aber nichts über die Bedeutung von Wahrscheinlichkeiten aus. In der Tat können auf Grundlage der Kolmogorov'schen Axiome viele Interpretationen (das heißt verschiedene Semantiken) koexistieren, solange sie konsistent mit den Axiomen sind.[12]

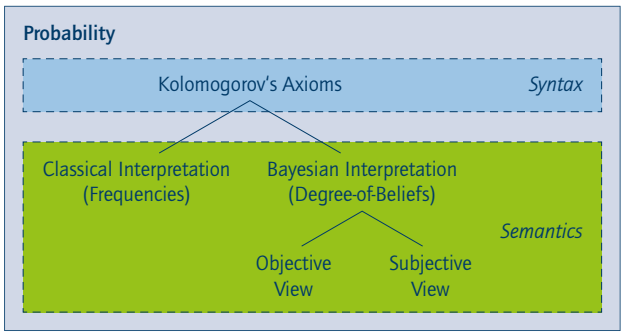


Abbildung 6: Verschiedene Bedeutungen von Wahrscheinlichkeiten (Quelle: eigene Darstellung)

Auf der einen Seite gibt es die frequentistische Interpretation von Wahrscheinlichkeit. Wahrscheinlichkeit wird hier ähnlich einer physikalischen Größe betrachtet, welche experimentell beobachtet und gemessen werden kann; wenigstens Gedankenexperimente sollten möglich sein.

Wenn zum Beispiel ermittelt werden soll, wie hoch bei einem Würfel die Wahrscheinlichkeit ist, dass eine der sechs Zahlen nach dem Wurf nach oben zeigt, kann man den Würfel N mal werfen und die relativen Häufigkeiten der eintretenden Ereignisse als Schätzung für die entsprechenden Wahrscheinlichkeiten betrachten. Strebt N gegen unendlich, garantiert das Gesetz der großen Zahlen, dass die relativen Häufigkeiten gegen die tatsächlichen Wahrscheinlichkeiten konvergieren.

Wenn man andererseits jemanden fragt, wie wahrscheinlich es ist, dass Leben auf dem Mars existiert, wäre dessen Antwort nach einigem Nachdenken vielleicht 0,0001 oder auch 0,5. Offensichtlich haben diese Antworten also keine frequentistische Bedeutung.[13] Entweder es gibt Leben auf dem Mars, oder es gibt keines. Tatsächlich wissen wir es einfach nicht, und kein wiederholbares Experiment, nicht einmal ein Gedankenexperiment, mit dem Versuche durchgeführt werden könnten, um die Fälle abzuzählen, in denen Leben auf dem Mars existiert oder nicht, ist sinnvoll vorstellbar.

Die erste Antwort, 0,0001, könnte das Ergebnis gründlicher Überlegungen über die physikalischen und biochemischen Voraussetzungen auf dem Mars und deren Folgen für Leben in uns bekanntem biologischem Sinne sein; sie beziffert ein individuelles Dafürhalten („Belief"). Die zweite Antwort, 0,5, könnte ausdrücken, dass man keine Ahnung von der Möglichkeit von Leben auf dem Mars hat und dieser Wert schlichtweg komplettes Nicht-Wissen ausdrückt.[14] Wiederum beziffert es ein Dafürhalten – oder genauer einen Grad des Dafürhaltens („Degree of Belief" – DoB). DoBs sind kompatibel mit den Axiomen von Kolmogorov und verallgemeinern die frequentistische Interpretation. Wenn man ein frequentistisches Experiment durchführen kann und die relativen Häufigkeiten berechnet, kann das Ergebnis ohne Weiteres als DoB übernommen werden, welches in diesem Sonderfall empirisch bestimmt wird.

Es kann zwischen objektiven und subjektiven DoBs unterschieden werden. Im ersten Fall werden Fakten so in DoBs transformiert, dass zwei Individuen, die den gleichen Wissensstand haben und die mit denselben Fakten konfrontiert werden, den gleichen DoB ableiten werden. Im zweiten Fall kann jedes Individuum seinen persönlichen DoB aus den vorliegenden Fakten ableiten.

Objektive DoBs sind von besonderem Interesse, weil es gut verstandene Ansätze gibt, DoBs individuell auf unvoreingenommene Weise festzulegen, wie zum Beispiel durch Anwendung des

9 | Vgl. Lindley 1982.
10 | Vgl. Huber/Schmidt-Petri 2009.
11 | Vgl. Bernardo 1994, Beyerer 1999.
12 | Vgl. Hofstadter 1979.
13 | Vgl. Lehner et al. 1996.
14 | Vgl. ebd.

Maximum-Entropie-Prinzips (MEP)[15] – siehe dazu auch Abschnitt 2.4 für eine tiefergehende Erläuterung. Das MEP nimmt alle gegebenen Fakten und alles verfügbare relevante Wissen als Randbedingung und berechnet den DoB, der die maximale Entropie hat und gleichzeitig alle Randbedingungen erfüllt. MEP-DoBs sind also minimal voreingenommen und führen keine zusätzlichen impliziten Annahmen, das heißt keinen zusätzlichen Bias, ein. Wenn das Risiko von einem objektiven Standpunkt aus beziffert wird, ist das MEP ein gut geeigneter Ansatz, um Fakten und Wissen formal in DoBs zu transformieren und damit einer probabilistischen Behandlung zugänglich zu machen.

Auf der anderen Seite erlauben es die subjektiv ermittelten DoBs, dass jeder Handelnde in einem Szenario seinen eigenen Blickwinkel und seine eigene Einschätzung über die Wahrscheinlichkeit von Vorfällen und die Ausprägung von Variablen haben kann. Individuelle Einschätzungen können vom einen zum anderen Individuum stark schwanken und auch von objektiven DoBs deutlich abweichen. Aber die Entscheidungen eines jeden Handelnden hängen von dessen eigenen Einschätzungen ab. Wenn beispielsweise ein Einbrecher den Einbruch in ein Haus plant, bewertet er sein persönliches Risiko auf Grundlage seiner subjektiven DoBs über die Verwundbarkeit und die Wahrscheinlichkeit, erfolgreich zu sein oder ertappt und bestraft zu werden. Er entscheidet also nicht auf Basis der ihm in der Regel unbekannten objektiven Werte dieser Größen.

3.2.2 Schutzbedürftige, Gefahrenquellen und Schützer

Alle Größen sind auf einen bestimmten Zeitabschnitt der Länge T bezogen, innerhalb dessen sie als konstant angenommen werden.

$$\mathrm{S} = \mathrm{S}_{\text{Persons}} \cup \mathrm{S}_{\text{Objects}} \cup \mathrm{S}_{\text{Systems}} \cup \mathrm{S}_{\text{Legal Interests}} \qquad (1)$$

bezeichnet die Menge der Schutzbedürftigen. Bei der Formalisierung wird hier gleichzeitig eine Verallgemeinerung des Schutzbedürftigen über Personen hinaus vorgenommen. Das mag sprachlich nicht ganz stimmig wirken, jedoch leuchtet ein, dass auch Objekte, Systeme und so weiter schützenswert sein können, sodass im Folgenden unter „schutzbedürftig" auch Schutzbedürftiges, zu schützende Gegenstände, aber auch Immaterielles wie zum Beispiel Rechtsgüter zu verstehen sind.[16]

Schutzbedürftige $s \in \mathrm{S}$ haben ein Budget $b(s)$ (beziehungsweise für sie steht ein Budget zur Verfügung) für Schutzmaßnahmen, und sie haben Flanken der Verwundbarkeit $f \in \mathrm{F}_S$.

Gefährdungen d (durch Angreifer, Verursacher oder Ursachen) sind Elemente der Menge von Gefahrenquellen

$$\mathrm{D} = \mathrm{D}_{\mathrm{WP}} \cup \mathrm{D}_{\mathrm{WM}} \cup \mathrm{D}_{\mathrm{UC}} \cup \mathrm{D}_{\mathrm{UR}}\,, \qquad (2)$$

wobei die Indizes Folgendes bedeuten:

WP: Willentliche Gefährdung als Zweck (**W**illful Danger as a **P**urpose: Vandalismus, Amok, Terror ...)

WM: Willentliche Gefährdung als Mittel (**W**illful Danger as a **M**eans: Einbruch, Raub ...)

UC: Unbeabsichtigte Gefährdung durch Fahrlässigkeit oder Nachlässigkeit (**U**nintended Danger due to **C**arelessness: Unaufmerksamkeit, Pflichtverletzung)

UR: Unbeabsichtigte Gefährdung durch Zufallsereignisse (**U**nintended Danger with **R**andom Characteristic: technische Fehler, Naturkatastrophen)

Wir definieren zwei weitere Teilmengen $\mathrm{D}_{\mathrm{U}} := \mathrm{D}_{\mathrm{UC}} \cup \mathrm{D}_{\mathrm{UR}}$ und $\mathrm{D}_{\mathrm{W}} := \mathrm{D}_{\mathrm{WP}} \cup \mathrm{D}_{\mathrm{WM}}$, welche die Gefährdungen $\mathrm{D} := \mathrm{D}_{\mathrm{W}} \cup \mathrm{D}_{\mathrm{U}}$ in die Unterklassen willentlich und unbeabsichtigt gliedern.

Im Folgenden werden $d \in \mathrm{D}_{\mathrm{W}}$ „Angreifer" genannt. Angreifer führen Angriffe a durch, die Elemente einer Menge A sind: $a \in \mathrm{A}$. Ein Angreifer verfügt über ein Budget $b(d)$, mit dem er seinen Angriffsaufwand finanziert. Die Angriffe a, die ein Angreifer d durchführen kann, sind in der Teilmenge $\mathrm{A}_{\mathrm{d}} \subseteq \mathrm{A}$ zusammengefasst.

Gefahrenquellen $d \in \mathrm{D}_{\mathrm{U}}$, die auf Nachlässigkeit zurückzuführen sind, rufen Vorfälle i hervor, die in einer Menge I von Vorfällen zusammengefasst sind, das heißt $i \in \mathrm{I}$. Im Folgenden werden $d \in \mathrm{D}_{\mathrm{U}}$ „Verursacher" beziehungsweise „Ursachen" genannt, weil diese Vorfälle verursachen. Die Menge von Vorfällen $d \in \mathrm{D}_{\mathrm{U}}$, die ein Verursacher beziehungsweise eine Ursache auslösen kann, wird in der Teilmenge $\mathrm{I}_{\mathrm{d}} \subseteq \mathrm{I}$ zusammengefasst.

Wenn ein Angriff oder ein Vorfall eintritt, wird der Erfolg (Schaden) mit dem Erfolgsgrad β eines solchen Vorfalls bemessen mit $\beta \in [0,1]$. $\beta = 1$ bedeutet vollständigen Erfolg, und $\beta = 0$ steht für kompletten Misserfolg.

15 | Vgl. Jaynes 1968.
16 | Vgl. Raabe 2018.

Ein Angriff oder ein Vorfall mit Wirkung auf s über dessen Flanken der Verwundbarkeit f mit Erfolgsgrad β kostet s: $c(s,f,\beta) \in [0,\infty)$.

Die Verwundbarkeit (Vulnerabilität) gegenüber Angriffen oder Vorfällen wird modelliert als DoB-Dichte. $p_v(\beta|i,s,f)$ und $p_v(\beta|a,s,f)$ beschreiben die DoB-Dichten für die Erfolgsgrade β, falls a beziehungsweise i den Schutzbedürftigen s an f treffen (siehe Abbildung 7).

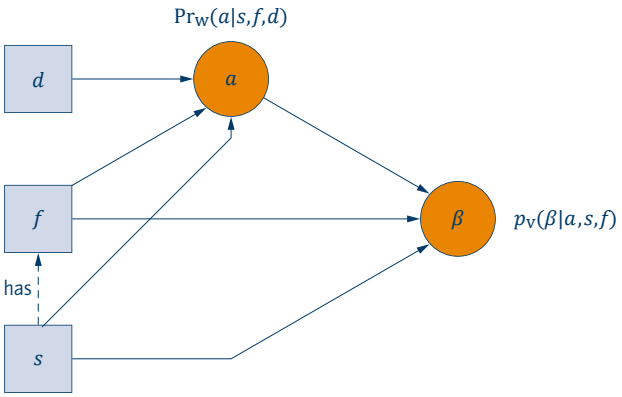


Abbildung 7: Verwundbarkeit (Vulnerabilität) wird modelliert als DoB-Dichte des Erfolgsgrads β eines Angriffs a auf den Schutzbedürftigen s über dessen verwundbare Flanken der Verwundbarkeit f (hier im Beispiel mit Wahrscheinlichkeiten $\mathrm{Pr_w}$ für eine willentliche Gefährdung; siehe Gleichung (11)). So hängt die Verwundbarkeit nicht von der Gefahrenquelle ab, sondern von dem Angriff a, den ein Angreifer d ausführt. Das Gleiche gilt, wenn ein Angreifer durch einen Verursacher $d \in \mathrm{D_U}$ und Angriffe durch Vorfälle i ersetzt werden (Quelle: eigene Darstellung).

Anmerkung: Für den Fall, dass die Kosten $c(s,f,\beta)$ proportional zum Erfolg β sind, das heißt

$$c(s,f,\beta) = \beta \cdot c(s,f), \tag{3}$$

können Kosten und Verwundbarkeit faktorisiert werden:

$$\int_0^1 c(s,f,\beta) \cdot p_V(\beta \mid i,s,f)\,\mathrm{d}\beta = c(s,f) \cdot v(s,f,i) \ , \tag{4}$$

wobei

$$v(i,s,f) := \mathrm{E}_{\beta|i,s,f}\{\beta\} = \int_0^1 \beta \cdot p_V(\beta \mid i,s,f)\,\mathrm{d}\beta \tag{5}$$

die mittlere Erfolgs-DoB eines Vorfalls i ist.

Verursacher von Gefährdungen aus Fahrlässigkeit $d \in \mathrm{D_{UC}}$ werden mit Kosten $k(s,f,b) \in [0,k_{\mathrm{d\_Ruin}}]$ belastet. Diese Kosten entsprechen einer Strafe dafür, dass d einen Vorfall $i \in \mathrm{I_d}$ verursacht hat, welcher s an f mit Erfolgsgrad β trifft. Je höher die Kosten für d sind, desto geringer sollte die Wahrscheinlichkeit sein, dass d einen solchen schädigenden Vorfall verursacht (Abschreckungswirkung).

Ein Schützer $p \in \mathrm{P}$ stellt Schutzmaßnahmen $m(s,f) \in \mathrm{M}$ für die Flanke f von s bereit. M bezeichnet die Menge der verfügbaren und $\mathrm{M^*} \subseteq \mathrm{M}$ die Menge der implementierten Maßnahmen. Für eine Maßnahme m muss s den Betrag $c(m(s,f))$ aufwenden. Da sich s nur Maßnahmen im Rahmen seines Budgets leisten kann, begründet dies die Randbedingung $\sum_{m \in \mathrm{M^*}} c(m(s,f)) \le b(s)$.

Die Maßnahmen $m(s,f)$ sollen die Verwundbarkeit, das heißt den Erfolg von Angriffen und/oder Vorfällen und/oder die Wahrscheinlichkeit von Angriffen und/oder Vorfällen, mindern. Dennoch ist $m(s,f)$ so modelliert, dass die Schutzmaßnahmen die Kosten $c(s,f,\beta)$ nicht mindern. Wenn zum Beispiel ein Wertgegenstand durch ein besseres Türschloss abgesichert wird, ändern sich nicht die Kosten, die durch den Verlust des Wertgegenstands entstehen würden.

Die folgenden Größen quantifizieren die Sicht des Angreifers. $g(s,f,\beta)$ bezeichnet den Gewinn durch einen Angriff auf s via f bei einem Erfolgsgrad β. $p_{\mathrm{Success}}(\beta|a,s,f)$ ist die Wahrscheinlichkeitsdichte für einen Erfolgsgrad β, wenn a s via f trifft. $c_{\mathrm{Effort}}(a,s,f)$ beschreibt die Kosten, die a für einen Angriff auf s via f aufwenden muss. $c_{\mathrm{Penalty}}(s,f,\beta)$ bezeichnet das monetäre Äquivalent einer etwaigen Strafe für einen Angriff auf s via f mit Erfolgsgrad β.

Und schließlich bezeichnet $\mathrm{Pr(Penalty}|s,f,b) = 1\text{-}\mathrm{Pr}(\neg\mathrm{Penalty}|s,f,\beta)$ den DoB für die Bestrafung eines Angriffs auf s via f mit Erfolgsgrad β.

3.3 Quantifizierung des Risikos

Das Gesamtrisiko $R_{\mathrm{s\_total}}$ eines Schutzbedürftigen s kann aus dem Blickwinkel von s ausgedrückt werden als:

$$R_{\mathrm{s\_total}} := \underbrace{R_s}_{\text{Modell}} + \underbrace{R_0}_{\text{Außerhalb der Modellierung}} , \tag{6}$$

wobei R_s den modellierten und R_0 den nicht modellierten Anteil bezeichnen. Es wird hier angenommen, dass Schutzmaßnahmen m, die den modellierten Risikoanteil R_S mindern, den nicht

modellierten Anteil R_0 nicht um mehr als diesen Minderungsbetrag erhöhen, das heißt:

$$\Delta R_{s\_\text{total}}(m) := R_{s\_\text{total}}(\text{ohne } m) - R_{s\_\text{total}}(\text{mit } m) \geq 0 \tag{7}$$

mit

$$\Delta R_s(m) := R_s(\text{ohne } m) - R_s(\text{mit } m) > 0\,. \tag{8}$$

Das Risiko R_s für s aus dessen eigenem Blickwinkel kann ausgedrückt werden als:

$$R_s = \sum_{d\in \mathrm{D_U}} \sum_{i\in \mathrm{I}_d} \sum_{f\in \mathrm{F}_s} \int_0^1 c(s,f,\beta)\cdot p_\mathrm{V}(\beta\,|\,i,s,f)\,\mathrm{d}\beta \cdot \mathrm{Pr_U}(i\,|\,s,f) + \sum_{d\in \mathrm{D_W}} \sum_{a\in \mathrm{A}_d} \int_0^1 c(s,\tilde{f},\beta)\cdot p_\mathrm{V}(\beta\,|\,a,s,\tilde{f})\,\mathrm{d}\beta \cdot \mathrm{Pr_W}(a\,|\,s,\tilde{f}) + \sum_{m\in \mathrm{M}^*} c(m(s,f)) \tag{9}$$

$\mathrm{Pr_U}(i|s,f)$ bezeichnet die Eintrittswahrscheinlichkeit (DoB) eines durch d gegen s via f verursachten Vorfalls. $\mathrm{Pr_W}(a|s,f)$ ist die Eintrittswahrscheinlichkeit (DoB) eines Angriffs von d auf s via f.

Hier werden die Risikobeiträge unter den Summen und Integralen gegenüber der klassischen Beschreibung „Risikobeitrag = Kosten × Eintrittswahrscheinlichkeit" erweitert zu einer Summe aus den drei Faktoren „Risikobeitrag = Kosten × Vulnerabilität × Eintrittswahrscheinlichkeit".[17] Dieser in Anlehnung an Lichte und Wolf verwendete Ansatz erlaubt es, reale Fragestellungen sachgerechter zu modellieren und gleichzeitig durch Verwendung des Wahrscheinlichkeitskalküls formal sauber zu beschreiben[18] (siehe Abbildung 7).

Der erste Summand von R_s entspricht dem mit einem *Safety*- und der zweite Summand dem mit einem *Security*-Problem verbundenen Risiko. Der dritte Summand quantifiziert die mit den Schutzmaßnahmen m verbundenen Kosten. Damit vereinigt R_s die Bewertung von Safety und Security und betrachtet ebenso die Aufwendungen zur Minderung des Risikos.

Im Vergleich zur statistischen Entscheidungstheorie[19] kommt mit p_v ergänzend zu den klassischen Risikofaktoren Wahrscheinlichkeit und Kosten ein weiterer Faktor hinzu, welcher die Verwundbarkeit modelliert. Dies geschieht in Übereinstimmung mit den Ansätzen in Baker und Broder/Trucker,[20] wobei wir diesen dritten Faktor als bedingte DoB-Dichte formulieren, sodass die Verträglichkeit mit der Wahrscheinlichkeitstheorie gewahrt bleibt. So ist zum Beispiel

$$p_\mathrm{V}(\beta\,|\,i,s,f)\cdot \mathrm{Pr_U}(i\,|\,s,f) \tag{10}$$

gleich der verbundenen DoB-Dichte $p(i, \beta|s, f)$ für den Eintritt eines Vorfalls i mit Erfolgsfaktor β, gegeben s und f.

Nur wenn ein Angreifer sowohl die Motivation und die Fähigkeit als auch die Gelegenheit hat, wird er einen Angriff unternehmen. Daher wird $\mathrm{Pr_W}(a|s,f)$ modelliert als Produkt dreier DoB-Faktoren:

$$\mathrm{Pr_W} = \mathrm{Pr_{Motivation}}\cdot \mathrm{Pr_{Power}}\cdot \mathrm{Pr_{Occasion}}\,. \tag{11}$$

$$\tilde{f} := \arg\max_{f\in \mathrm{F}_s} \{\max_{a\in \mathrm{A}_d} \{U_d(a,s,f)\}\} \tag{12}$$

bezeichnet die aus Sicht des Angreifers d aussichtsreichste Flanke der Verwundbarkeit von s.

Um den erwarteten Gewinn von d aus einem Angriff a auf s via f zu quantifizieren, wird der Nutzen $U_d(a, s, f) \in [U_{\min,\,d}, U_{\max,\,d}]$ modelliert als:

$$\begin{aligned} U_d(a,s,f) &:= \int_0^1 g(s,f,\beta)\cdot p_{\text{Success}}(\beta\,|\,a,s,f)\,\mathrm{d}\beta - c_{\text{Effort}}(a,s,f) \\ &\quad - \int_0^1 c_{\text{Penalty}}(s,f,\beta)\cdot \Pr(\text{Penalty}\,|\,s,f,\beta)\cdot p_{\text{Success}}(\beta\,|\,a,s,f)\,\mathrm{d}\beta \\ U_d(a,s,f) &= \int_0^1 \left[g(s,f,\beta) - c_{\text{Penalty}}(s,f,\beta)\Pr(\text{Penalty}\,|\,s,f,\beta)\right] p_{\text{Success}}(\beta\,|\,a,s,f)\,\mathrm{d}\beta \\ &\quad - c_{\text{Effort}}(a,s,f) \end{aligned} \tag{13}$$

wobei $c_{\text{Effort}}(a, s, f) \leq b(d)$ gilt. Es erscheint offensichtlich, dass dieser Ansatz zur Risikomodellierung auch auf Mengen S von Schutzbedürftigen s angewendet werden kann, die durch D gefährdet werden. In diesem Fall kann das Risiko einfach durch Summation über die Elemente der Menge S definiert werden: $R_\mathrm{S} = \sum_{s\in \mathrm{S}} R_s$.

3.4 Bestimmung der Wahrscheinlichkeiten

Die wesentliche Herausforderung in dem hier vorgestellten formalen Rahmen ist die Bestimmung der Wahrscheinlichkeiten oder genauer der DoBs als Bestandteile der Risikoterme. Dies ist besonders dann schwierig, wenn die Wahrscheinlichkeiten sehr gering sind, sodass es nicht genügend Daten für die Schätzung von DoBs mit statistischen Methoden gibt. Von einem methodischen Standpunkt aus gibt es verschiedene Optionen, diese Aufgabe zu lösen.

17 | Vgl. Berger 1993.
18 | Vgl. Lichte/Wolf 2018.
19 | Vgl. Berger 1993.
20 | Vgl. Baker 2005 und Broder/Trucker 2012.

3.4.1 Das Maximum-Entropie-Prinzip (MEP)

Um die DoBs objektiv zu bestimmen, kann das *Maximum-Entropie-Prinzip* (MEP) angewandt werden.[21] Shannons Entropie

$$H := \sum_{\omega \in \Omega} -\Pr(\omega) \log(\Pr(\omega)) \tag{14}$$

für den diskreten Fall und die differenzielle Entropie

$$h := \int_{\omega \in \Omega} -p(\omega) \log(p(\omega)) \, \mathrm{d}\omega \tag{15}$$

für die kontinuierliche Variable ω quantifizieren die DoB-Konzentration auf der Definitionsmenge Ω. Je geringer die Konzentration, desto höher ist die entsprechende Entropie. Ohne jede Randbedingung erreicht diese DoB-Verteilung mit konstanten DoB-Werten für jedes $\omega \in \Omega$ (Gleichverteilung) die maximale Entropie. Kennen wir irgendwelche Fakten über $\omega \in \Omega$, werden diese als Randbedingung herangezogen, auf die bezogen die DoB mit der maximalen Entropie berechnet wird. So verkörpert die daraus resultierende DoB die gegebenen Fakten in einer Weise innerhalb des probabilistischen Kalküls, die keine zusätzlichen Annahmen implizit einführt. In diesem Sinne ist die MEP-DoB unvoreingenommen bezüglich allem, was über die betrachteten Fakten hinausgeht.

Die Übernahme des MEP wird durch einen Satz von Axiomen gerechtfertigt, aus denen das MEP eindeutig abgeleitet werden kann.[22] Gemäß Beierle et al. sind diese sieben Axiome allgemein verständlich formuliert:[23]

(a) Prinzip der irrelevanten Information (Irrelevant Information Principle): Alles für das vorliegende Problem vollständig irrelevante Wissen kann ignoriert werden.

(b) Prinzip der Umbenennung (Renaming Principle): Die Umbenennung aller Variablen, die für die Modellbeschreibung verwendet werden, beeinflusst nicht die Wahl des besten Modells.

(c) Prinzip der Redundanzvermeidung (Obstinacy Principle): Erhält man Informationen über bereits Bekanntes, sind diese redundant und ändern nichts am besten Modell.

(d) Prinzip der Äquivalenz (Equivalence Principle): Wenn zwei Wissensbasen entsprechend den Axiomen der Wahrscheinlichkeitstheorie semantisch äquivalent sind, sollten sie dasselbe beste Modell haben.

(e) Prinzip der Relativierung (Relativization Principle): Probabilistisches Wissen über einen Vorfall bleibt unbeeinflusst von Wissen, welches annimmt, dass der Vorfall nicht eingetreten ist.

(f) Prinzip der schwachen Unabhängigkeit (Weak Independence Principle): Wenn zwei Vorfälle A und B nicht gleichzeitig auftreten können, dann beeinflusst probabilistisches Wissen über B nicht die gewählte Wahrscheinlichkeit für Vorfälle, die gleichzeitig mit A auftreten.

(g) Stetigkeit (Continuity Principle): Sehr kleine Änderungen in dem faktischen probabilistischen Wissen in der gegebenen probabilistischen Wissensbasis können sich nur in sehr kleinen Änderungen der resultierenden Wahrscheinlichkeiten im besten Modell niederschlagen.

Das „Beste Modell" ist die Wahrscheinlichkeitsverteilung, die mit allen gegebenen Fakten (das heißt zu der oben genannten probabilistischen Datenbasis) und allen oben genannten Axiomen (a) bis (g) verträglich ist. Ein rationaler Agent (Individuum, Schlussfolgerungsautomat), der Wahrscheinlichkeiten nutzt und mit diesen Prinzipien übereinstimmt, sollte das MEP verwenden, um seine Wahrscheinlichkeitsverteilungen zu bestimmen.[24]

3.4.2 Konditionierung durch seltene Ereignisse (CORE: Conditioning on Rare Events)

Um mit dem Problem der Wahrscheinlichkeitsbestimmung extrem seltener Ereignisse umgehen zu können (Vorfälle oder Angriffe), kann deren Schätzung oder Festlegung vollständig vermieden werden, wenn das Risiko als bedingt formuliert wird, wie dies zum Beispiel in Arens/Kühne geschieht.[25] Das heißt, für ein seltenes Ereignis i beziehungsweise a wird das Risiko ausgedrückt unter der Bedingung, dass das Ereignis i beziehungsweise a eingetreten ist. Liegt beispielsweise ein Vorfall i vor, so ändert sich der erste Summand von Gleichung (9) zu

$$\sum_{f \in \mathrm{F}_s} \int_0^1 c(s,f,\beta) \cdot p_{\mathrm{V}}(\beta \mid i,s,f) \, \mathrm{d}\beta \tag{16}$$

und bildet damit eine Komponente für das bedingte Risiko $R_s|i$.

21 | Vgl. Jaynes 1968.
22 | Vgl. Paris 1999.
23 | Vgl. Beierle et al. 2015.
24 | Vgl. Beierle et al. 2015.
25 | Vgl. Arens/Kühne 2018.

3.5 Subjektive Sicht von Agenten

Objektive Kostenfunktionen und Eintrittswahrscheinlichkeiten müssen klar von subjektiven Beurteilungen dieser Größen unterschieden werden. Ein rationaler Agent entscheidet aufgrund seiner subjektiven Sicht, das heißt aufgrund seiner Einschätzung über Kosten bei einem Vorfall oder Angriff und der DoBs über Eintrittswahrscheinlichkeiten. Nach Mainzer und Tversky/Kahnemann bewerten Individuen Kosten und Eintrittswahrscheinlichkeit mit einer kognitiven Voreingenommenheit.[26] Zum einen wird die Wahrscheinlichkeit sehr seltener Ereignisse üblicherweise überschätzt und die Wahrscheinlichkeit sehr häufiger Ereignisse unterschätzt. Zum anderen ist die Einschätzung über die Kosten nicht linear verzerrt, weil ein Kostenanstieg gewöhnlich im Verhältnis zum absoluten Kostenniveau bewertet wird, was näherungsweise zu einer logarithmischen Kennlinie führt – und damit zu einer starken Abflachung der subjektiven Kostenfunktion mit höheren Werten. Weiterhin erzeugt Risikobereitschaft beziehungsweise Risikoaversion eines Individuums eine Asymmetrie zugunsten positiver beziehungsweise negativer Kosten (Gewinn). Wenn $c_{\text{objective}}$ beziehungsweise $p_{\text{objective}}$ die objektiven Kosten beziehungsweise die objektiven Wahrscheinlichkeiten sind, kann der Übergang zu subjektiven Kosten, subjektiven Wahrscheinlichkeiten (DoBs) und somit zu subjektivem Risiko mathematisch mit den Bewertungsfunktionen $\upsilon(.)$ und $\pi(.)$ beschrieben werden:

$$c_{\text{subjective}} = \upsilon(c_{\text{objective}}) \tag{17}$$

$$p_{\text{subjective}} = \pi(p_{\text{objective}}) \tag{18}$$

$$R_{\text{subjective}} = \Psi\left\{\upsilon(c_{\text{objective}})\pi(p_{\text{objective}})\right\} \tag{19}$$

Wobei $\Psi\{.\}$ ein Ensemble-Funktional bezeichnet, wie zum Beispiel ein Integral oder einen Auswahl-Operator. Innerhalb des hier vorgestellten formalen Rahmens werden alle Größen, die vom Standpunkt eines Individuums aus gesehen werden, als subjektive Größen verstanden. Im Fall von Wahrscheinlichkeiten umfasst der Begriff DoB sowohl die individuelle Einschätzung der Häufigkeit von Ereignissen als auch die individuelle Voreingenommenheit.

3.6 Einführung zeitlicher Dynamik

Bis zu dieser Stelle wurden alle Größen so behandelt, als wären sie zeitlich konstant. Um reale Probleme angehen zu können, ist es erforderlich, den Ansatz mit einer Zeitabhängigkeit zu versehen. Alle relevanten Größen werden als Zeitreihen modelliert. Ein hochgestellter Index $k \in \mathbf{N}_0$ bezeichnet einen diskreten Zeitschritt. Zusätzlich wird ein Transitionsoperator Φ^k eingeführt, der die relevanten Größen des Zeitschritts k auf den Zeitschritt $k+1$ abbildet.

$$\left(b^k(s), m^k, \ldots, p_V^k, \Pr_{\text{U}}^k, \Pr_{\text{W}}^k, R_s^k, U_d^k\right) \xrightarrow{\Phi^k}$$

$$\left(b^{k+1}(s), m^{k+1}, \ldots, p_V^{k+1}, \Pr_{\text{U}}^{k+1}, \Pr_{\text{W}}^{k+1}, R_s^{k+1}, U_d^{k+1}\right) \tag{20}$$

Um mit der Dynamik des modellierten Systems Schritt halten zu können, muss die Zeit-Diskretisierung fein genug gewählt werden, sodass alle Größen innerhalb eines Zeitschritts k der Dauer T als konstant angenommen werden können. Damit kann zum Beispiel der Einfluss einer Maßnahme m, die getroffen wird, um die Sicherheit von s zu erhöhen, auf das Verhalten eines intelligenten Angreifers d in den Übergang zum nächsten Zeitschritt hineinmodelliert werden, sodass innerhalb eines Zeitschritts T die Modellgrößen nicht unnötig verkoppelt werden.

Der Einfluss zum Beispiel auf die Größen $b(s)$, p_{V}, $\Pr_{\text{W}}$, R_s und U_d einer im Zeitschritt k ergriffenen Schutzmaßnahme m^k wird mithin modelliert durch die Änderung von $b^k(s)$, p_V^k, $\Pr_{\text{W}}^k$, R_s^k und U_d^k nach $b^{k+1}(s)$, p_V^{k+1}, $\Pr_{\text{W}}^{k+1}$, R_s^{k+1} und U_d^{k+1}, die durch den Transitionsoperator Φ^k vermittelt wird.

3.7 Einführung eines Ortsbezugs

Nichttriviale STS haben eine örtliche Ausdehnung und müssen entsprechend auch räumlich modelliert werden. Ein möglicher Ansatz besteht darin, den Ort durch eine geeignete Partitionierung in endlich viele Regionen zu zerlegen und damit zu diskretisieren. Zur weiteren Abstraktion wird jeder dieser örtlichen Bereiche als ein Knoten und die Nachbarschaft zwischen den Bereichen als Kanten eines Graphen beschrieben.[27] Eine Liegenschaft, die das räumliche Gebiet darstellt, das von einem STS eingenommen wird, kann somit abstrakt durch einen Graphen sparsam dargestellt werden (siehe Abbildung 8).

Die örtliche Auflösung der Diskretisierung hängt von der zu modellierenden Umgebung ab. Einerseits sollte die Diskretisierung fein genug sein, um das Geschehen zwischen Akteuren des STS räumlich ausreichend auflösen zu können, andererseits führt eine zu feine Diskretisierung zu mehr Speicher- und Rechenaufwand bei Berechnungen und Simulationen.

26 | Vgl. Mainzer 2016, Tversky/Kahnemann 2000.
27 | Vgl. Labudde 2018, Weyer et al. 2018.

Würde es sich bei der Liegenschaft zum Beispiel um einen Bahnhof handeln, bei dem man die Sicherheit der Bahnreisenden modellieren möchte, könnten Knoten etwa Parzellen von einigen Quadratmetern beschreiben, innerhalb derer Aufenthaltsorte, Stationen wie Infostände und Kioske, technische Systeme wie Rolltreppen und Fahrstühle kompakt beinhaltet sind und innerhalb derer Aktionen wie Fortbewegung, Interaktion mit anderen Reisenden, Bahnbediensteten und Sicherheitskräften, aber auch zum Beispiel mit Taschendieben auf hohem Abstraktionsniveau als zeitlich diskrete Ereignisse stattfinden können. An jedem dieser Knoten könnten sich mehrere Akteure (Agenten) und Objekte befinden, die in einem Zeitschritt miteinander wechselwirken könnten.

In Anlehnung an Weyer et al. wäre der Graph also ausgestattet mit attribuierten Knoten und Kanten und bildet sozusagen das digitale „Spielbrett", auf dem eine räumlich-zeitliche Simulation der Agenten und Objekte, die das STS konstituieren, durchgeführt werden kann.[28]

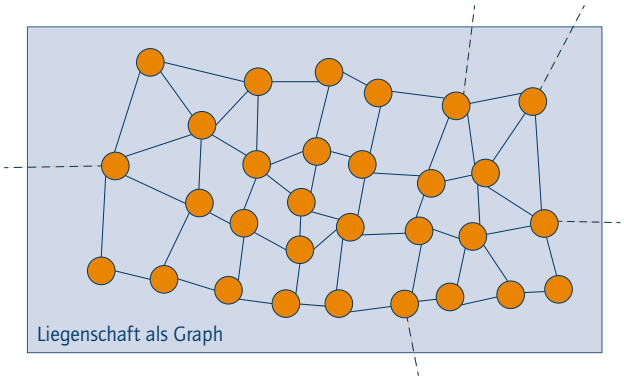


Abbildung 8: Liegenschaft als attribuierter Graph $G = (V, \Theta_V, E, \Theta_E)$ zur Repräsentation der räumlichen und sachlichen Gegebenheiten. Knoten V: diskretisierte, attribuierte Orte. Kanten E: diskretisierte, attribuierte Nachbarschaften und Wege. Die Mengen Θ beschreiben die jeweiligen Attribute (Quelle: eigene Darstellung).

In Lichte/Wolf werden im Kontext der Sicherheit (Security) an Flughäfen räumliche Angriffspfade untersucht,[29] entlang derer sich Barrieren befinden, deren Überwindung einen potenziellen Angreifer Zeit kosten und mit der die Wahrscheinlichkeit der Angriffsdetektion monoton steigt, was wiederum Voraussetzung dafür ist, erfolgreich Gegenmaßnahmen einleiten zu können. Räumlich verteilte Barrieren und Detektionssysteme lassen sich zwanglos als Attribute eines attribuierten Graphen $G = (V, \Theta_V, E, \Theta_E)$ modellieren.

4 Schlussfolgerung, Herausforderungen und Zusammenfassung

Soziotechnische Systeme (STS) bestehen aus menschlichen Akteuren und technischer Infrastruktur. Ihre Komplexität und Vielschichtigkeit machen es sehr schwierig, Risiken bezüglich der Sicherheit quantitativ zu beschreiben und zu analysieren. In diesem Aufsatz wird ein mathematischer Rahmen vorgestellt, mit dem sich die Risiken der Akteure eines STS modellieren lassen. Auf Grundlage eines Rollenkonzepts wurde ein formaler Rahmen vorgestellt, der das Risiko eines Schutzbedürftigen sowohl bezüglich Safety als auch bezüglich Security einheitlich modelliert. Rollen und Größen haben eine eindeutige Semantik – eine hilfreiche Voraussetzung, um die Modellparameter quantitativ zu bestimmen, sobald das Modell auf Realweltprobleme übertragen wird. Nichtsdestotrotz ist es in der Praxis ziemlich herausfordernd, die betreffenden Größen ausreichend präzise zu bestimmen. Insbesondere die Schätzung der verschiedenen Wahrscheinlichkeiten ist alles andere als trivial. Wenn sich Angriffe oder Vorfälle sehr selten ereignen, liegen in der Regel auch nicht genügend Daten für eine statistische Analyse vor. Ein möglicher Ausweg ist die erweiterte Interpretation von Wahrscheinlichkeit als „Grad des Dafürhaltens" (DoB: Degree of Belief). In der Bayes'schen Statistik ist dies die übliche Semantik für Wahrscheinlichkeit.

Im äußersten Fall erlaubt dies die Nutzung von Wahrscheinlichkeiten, um subjektives Dafürhalten eines Agierenden auszudrücken,[30] solange die Syntaxregeln für das Rechnen mit Wahrscheinlichkeiten, das heißt die Axiome von Kolmogorov, eingehalten werden.

Auf der Basis einer zeitlichen Diskretisierung werden alle relevanten Größen zu Zeitreihen. Durch eine Diskretisierung und Abstraktion des Raums können Liegenschaften, welche die STS beherbergen, durch attribuierte Graphen verkörpert werden, auf denen dann die räumlich-zeitliche Entwicklung des sicherheitsrelevanten Geschehens simuliert und quantitativ bewertet werden kann.

Die quantitative Formulierung des Risikos eines Schutzbedürftigen und des Nutzens für einen Angreifer sollte es erlauben, Simulationen durchzuführen, zum Beispiel Monte-Carlo- oder agentenbasierte Simulationen, um das Risiko numerisch

28 | Vgl. Weyer et al. 2018.
29 | Vgl. Lichte/Wolf 2018.
30 | Vgl. Bernardo 1994.

berechnen zu können und aus einem simulierten Zusammenspiel der Instanzen der eingeführten Rollen plausible Ereignisfolgen zu erzeugen.

Weiterführende Arbeiten werden sich unter anderem auf Methoden konzentrieren, um die Parameter des Modells zu schätzen und den Ansatz auf realweltliche Sicherheitsaufgaben anzuwenden.

Zur Bestimmung der zahlreichen Parameter der Risikomodelle bedürfte es eigentlich sehr vieler Daten, wenn die Parameterschätzung klassisch statistisch durchgeführt werden soll. Eine große empirische Basis wird aber in der Praxis kaum vorliegen, sodass es essenziell ist, Experteneinschätzungen und Vorwissen ebenfalls in die Inferenz einzubeziehen, was mit der Interpretation von Wahrscheinlichkeiten als DoBs im Bayes'schen Sinne harmoniert. Interessant wären hier auch die Heuristiken, die in Deutschmann/Milbredt genutzt werden.[31] Obwohl der dort verwendete Fuzzy-Ansatz syntaktisch nicht kompatibel mit der probabilistischen Herangehensweise dieses Beitrags ist, ist es jedoch gerade eine Stärke des Fuzzy-Ansatzes, dass er es erlaubt, Experteneinschätzungen in numerische Repräsentationen zu überführen. Das verbindet ihn auf semantischer Ebene mit der subjektiven Auffassung von Wahrscheinlichkeiten als DoBs.

Für eine stärkere Formalisierung der Begriffe dieses Aufsatzes sowie für eine eindeutige relationale Verknüpfung zwischen diesen Begriffen wird eine UML-basierte Konzeptualisierung aller Terme des Modells entsprechend den in Schnieder/Schnieder vorgeschlagenen Ideen angestrebt.[32]

Für die zeitliche Modellierung von STS soll bezüglich Kausalstrukturen, wie sie in Gleirscher eingeführt werden,[33] untersucht werden, inwieweit sie bei der Formulierung des Transitionsoperators Φ^k vorteilhaft genutzt werden können.

In einem größeren Kontext sollen die vorgestellten Ideen Bestandteile einer integrativen Theorie der Verlässlichkeit für soziotechnische Systeme werden, wie sie in Bertsche et al. angeregt wird.[34] Insbesondere spielen dabei auch die Methoden des Systems Engineering zur Beschreibung, Abgrenzung und auch zur Optimierung von STS hinsichtlich ihrer Verlässlichkeit eine wichtige Rolle und sollen intensiv genutzt und eingebunden werden.[35]

Die künftige Entwicklung der vorgestellten Ansätze wird insbesondere im „Themennetzwerk Sicherheit" der Deutschen Akademie der Technikwissenschaften acatech weiterverfolgt werden.

31 | Vgl. Deutschmann/Milbredt 2018.
32 | Vgl. Schnieder/Schnieder 2010, Schnieder/Schnieder 2013, Schnieder/Schnieder 2018.
33 | Vgl. Gleirscher 2018.
34 | Vgl. Bertsche et al. 2018.
35 | Vgl. Schlüter/Winzer 2018.

Literatur

Arens/Kühne 2018
Arens, U./Kühne, U.: „Schutz und Sicherheit in Offshore-Windparks". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Baker 2005
Baker, G.: *A Vulnerability Assessment Methodology for Critical Infrastructure Sites* (DHS Symposium: R&D Partnerships in Homeland Security), Boston 2005.

Beierle et al. 2015
Beierle, C./Kern-Isberner, G./Finthammer, M./Potyka, N.: „Extending and Completing Knowledge and Beliefs Without Bias". In: *Künstliche Intelligenz*, 29: 3, Berlin, Heidelberg: Springer 2015, S. 255–262.

Berger 1993
Berger, J. O.: *Statistical Decision Theory and Bayesian Analysis*, Berlin: Springer 1993.

Bernardo 1994
Bernardo, J. M./Smith, A. F. M.: *Bayesian Theory*, New York: John Wiley & Sons 1994.

Bertsche et al. 2018
Bertsche, B./Beyerer, J./Goldschmidt, R./Jakobs, E. M./Renn, O./Schlüter, N./Winzer, P./Weyer, J.: „Integrative Theorie der Verlässlichkeit (iTV) für soziotechnische Systeme (STS)". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Beyerer 2009
Beyerer, J.: „Sicherheitstechnik, Sicherheitssysteme und Sicherheitsforschung – Aktuelle Herausforderungen". In: Stober, R.: *Sicherheitsgewerbe und Sicherheitstechnik – Von der Personalisierung zur Technisierung – 9. Hamburger Sicherheitsgewerberechtstag*, Köln: Carl Heymanns Verlag 2009, S. 1–10.

Beyerer 1999
Beyerer, J.: *Verfahren zur quantitativen statistischen Bewertung von Zusatzwissen in der Meßtechnik* (VDI Fortschritt-Berichte), 8: 783, Düsseldorf: VDI Verlag 1999.

Beyerer et al. 2010
Beyerer, J./Geisler, J./Dahlem, A./Winzer, P.: „Sicherheit: Systemanalyse und -design". In: Winzer, P./Schnieder, E./Bach, F. (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven* (acatech DISKUTIERT), Berlin: Springer 2010, S. 39–72.

Beyerer/Geisler 2016
Beyerer, J./Geisler, J.: „A Framework for a Uniform Quantitative Description of Risk with Respect to Safety and Security". In: *European Journal for Security Research*, 1: 2, Berlin: Springer 2016, S. 135–150.

Beyerer/Geisler 2015
Beyerer, J./Geisler, J.: „A Quantitative Risk Model for a Uniform Description of Safety and Security". In: Beyerer, J./Meissner, A./Geisler, J. (Hrsg.): *Proceedings of the 10th Future Security – Security Research Conference* (Berlin, 15th–17th September 2015), Stuttgart: Fraunhofer Verlag 2015, S. 317–324.

Broder/Tucker 2012
Broder, J. F./Tucker, E.: *Risk Analysis and the Security Survey*, 4. Auflage, Waltham, MA, USA: Butterworth-Heinemann 2012.

Buldas et al. 2006
Buldas, A./Laud, P./Priisalu, J./Saarepera, M./Willemson, J.: „Rational Choice of Security Measures via Multi-Parameter Attack Trees". In: *Critical Infrastructures Security*, Lecture Notes in Computer Science, 4347, Berlin: Springer 2006, S. 235–248.

Deutschmann/Milbredt 2018
Deutschmann, A./Milbredt, O.: „Globale Bewertung des Sicherheitsniveaus von kritischen Infrastrukturen am Beispiel von Verkehrsflughäfen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Gleirscher 2018
Gleirscher, M.: „Strukturen für die Gefahrenerkennung und -behandlung in autonomen Maschinen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Hofstadter 1979
Hofstadter, D. R.: Gödel, Escher, Bach: *An Eternal Golden Braid*, New York: Basic Books Inc., 1979.

Huber/Schmidt-Petri 2009
Huber, F./Schmidt-Petri, C. (Hrsg.): *Degrees of Belief*, Springer Science + Business Media B. V. 2009.

Jaynes 1968
Jaynes, E. T.: *Prior Probabilities. IEEE Transactions on Systems, Science, and Cybernetics,* 4: 3, 1968, S. 227–241.

Labudde 2018
Labudde, D.: „Sicherheit ist die Abwesenheit von Kriminalität – eine Hypothese". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Lehner et al. 1996
Lehner, P. E./Laskey, K. B./Dubois, D.: *An Introduction to Issues in Higher Order Uncertainties. IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, 26: 3, 1996, S. 289–293.

Lichte/Wolf 2018
Lichte, D./Wolf, K.-D.: „Quantitative Analyse der Vulnerabilität am Beispiel Verkehrsflughafen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Lindley 1982
Lindley, D. V.: S*coring Rules and the Inevitability of Probability. International Statistical Review*, 50, 1982, S. 1–26.

Mainzer 2016
Mainzer, K.: *Künstliche Intelligenz – Wann übernehmen die Maschinen?,* Heidelberg, Berlin: Springer-Verlag 2016.

Müller-Quade 2018
Müller-Quade, J.: „Das Verhältnis der Kryptographie zu einer Systemtheorie Sicherheit". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Paris 1999
Paris, J.: *Common Sense and the Maximum Entropy. Synthese 117*, 1999, S. 75–99.

Raabe 2018
Raabe, O.: „Datenschutz- und IT-sicherheitsrechtliche Risikomodelle". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schlüter/Winzer 2018
Schlüter, N./Winzer, P.: „Bedeutung des Systems Engineering für die Entwicklung einer Systemtheorie der Sicherheit". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schnieder/Schnieder 2018
Schnieder, E./Schnieder, L.: „Formalisierung von Begriffen der Sicherheit und Sicherheitsmetriken". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schnieder/Schnieder 2013
Schnieder, E./Schnieder, L.: *Verkehrssicherheit – Maße und Modelle, Methoden und Maßnahmen für den Straßen- und Schienenverkehr*, Heidelberg, Berlin: Springer 2013.

Schnieder/Schnieder 2010
Schnieder, E./ Schnieder, L.: „Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung". In: Winzer, P./ Schnieder, E./Bach, F. (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven* (acatech DISKUTIERT), Berlin: Springer 2010, S. 73–115.

Tversky/Kahnemann 2000
Tversky, A./Kahnemann, D.: „Advances in Prospect Theory: Cumulative Representation of Uncertainty". In: Kahnemann, D./ Tversky, A. (Hrsg.): *Choices, Values and Frames*, Cambridge: Cambridge University Press, 2000, S. 44–66.

Weyer et al. 2018
Weyer, J./Adelt, F./Konrad, J./Hoffmann, S.: „Agentenbasierte Simulation des Risikomanagements soziotechnischer Systeme mit dem Simulator SimCo". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

6 Das Verhältnis der Kryptographie zu einer Systemtheorie Sicherheit

Prof. Dr. rer. nat. Jörn Müller-Quade
Lehrstuhl für Kryptographie und Sicherheit
Karlsruher Institut für Technologie (KIT)
Direktor am Forschungszentrum Informatik (FZI)

Einleitung

In diesem Band „acatech DISKUSSION" werden vielfältige Annäherungen an eine umfassende Systemtheorie Sicherheit präsentiert. Verschlüsselungstechniken und andere kryptographische Verfahren werden aber in ihrer Scientific Community anders behandelt und beurteilt, als es die hier gesammelten Ansätze nahelegen. Warum das so ist und warum es sogar sinnvoll ist, beschreibt dieser Beitrag.

Eine Systemtheorie Sicherheit macht idealerweise quantitative Vorhersagen. Die Kenngrößen einer Systemtheorie Sicherheit sollten eine Risikoabschätzung ermöglichen und auf diese Weise verschiedene Risiken vergleichbar machen, damit ein Investor eine fundierte, rationale Entscheidung treffen kann, wie er in Schutzmaßnahmen investiert. Quantitative Vorhersagen ermöglichen auch eine empirische Überprüfung und damit einen naturwissenschaftlichen Zugang zur Sicherheit.

Die Kryptographie unterscheidet sich auffällig von diesem Ideal einer Systemtheorie Sicherheit und betrachtet einen intelligenten Angreifer, dessen Verhalten nicht über Wahrscheinlichkeiten beschrieben werden kann; insbesondere kann man nicht aus dem Verhalten des Angreifers in der Vergangenheit auf sein Verhalten in der Zukunft schließen. Die Kryptographie betrachtet keine Risikokenngrößen, sondern versucht innerhalb eines mathematischen Modells und unter klaren Sicherheitsannahmen, alle innerhalb des Modells formulierbaren Angriffe abzuwehren. Dieser Beitrag ist ein Plädoyer für diese Sichtweise, denn sie vereinfacht eine übergeordnete Systemtheorie Sicherheit: Sichere kryptographische Protokolle verhalten sich ununterscheidbar zu bestimmten idealisierten Bausteinen, die der Angreifer nicht manipulieren kann.[1] Dadurch ist es möglich, alle kryptographischen Protokolle in einem komplexen System durch passende, idealisierte Bausteine zu ersetzen und eine Risikoanalyse danach viel einfacher durchzuführen. Das Gesamtrisiko kann nun abgeschätzt werden durch das Risiko, das für das idealisierte System besteht, und das Risiko, dass die Sicherheitsannahmen falsch sind.

1 Systemtheorie Sicherheit und Verschlüsselungsverfahren

Inwieweit sich die Sicherheitsmodellierung der Kryptographie von der einer Systemtheorie Sicherheit unterscheidet und wie die Ergebnisse der Kryptographie dennoch zu einer quantitativen Theorie der Sicherheit beitragen können, wird zunächst konkret am Beispiel der Verschlüsselung erörtert. Das wiederkehrende Motiv ist dabei, dass die Kryptographie von Einflussgrößen abstrahiert, die man nur kennen kann, wenn man den konkreten Anwendungsbezug hat und die konkrete Bedrohungslage kennt. Natürlich hat diese Abstraktion nur Sinn, wenn auch klar wird, wie man die wegabstrahierten Einflussgrößen, etwa die Schadenshöhe oder den Zeitraum, in dem ein System überhaupt angegriffen werden kann, hinterher wieder einbeziehen kann. Dass und wie dies möglich ist, wird bei der Darstellung der Kryptographie leider meist unterschlagen. Um die Kryptographie für eine Vereinfachung einer Systemtheorie Sicherheit verwenden zu können, muss sie also eine klare Schnittstelle bereitstellen. Wegen der Abstraktion vom Anwendungskontext unterscheidet sich die Kryptographie von einer Systemtheorie Sicherheit und liefert andere Ergebnisse als beispielsweise ein konkretes Risiko. Dafür erlaubt die Kryptographie aber die Identifikation einer Klasse von Sicherheitsproblemen sowie die Erforschung und Beurteilung von Lösungen, ohne den konkreten Anwendungsbezug kennen zu müssen. Die Kryptographie bietet somit eine Komplexitätsreduktion, denn eine Systemtheorie Sicherheit kann nun von konkreten Details der verwendeten Verschlüsselung abstrahieren und dadurch das Risiko einfacher abschätzen.

Ein sehr einfaches Beispiel soll dies zeigen. In der Kryptographie ist die Wahrscheinlichkeit, dass ein Angriff überhaupt versucht wird, immer gleich eins. Die daraus errechnete Erfolgswahrscheinlichkeit eines Angreifers entspricht damit nicht dem realen Risiko. Für eine Einschätzung des Risikos in einem konkreten Umfeld ist diese Erfolgswahrscheinlichkeit ein Teilergebnis, eine bedingte Wahrscheinlichkeit, die noch mit der Wahrscheinlichkeit multipliziert werden muss, dass ein Angreifer überhaupt einen

1 | Vgl. Goldreich 2004b.

Angriff durchführt. Genauer gesagt sollte diese Wahrscheinlichkeit nach oben abgeschätzt werden, damit die Abschätzung unabhängig von dem konkret eingesetzten Verschlüsselungsverfahren wird und man die Wahrscheinlichkeiten einfach multiplizieren darf. Eine Systemtheorie Sicherheit, die die bedingte Wahrscheinlichkeit als Teilergebnis nutzt, muss nur noch die Wahrscheinlichkeit eines Angriffs abschätzen.

1.1 Asymptotik

Die Kryptographie abstrahiert stark von der aktuell verwendeten Rechnertechnologie des Angreifers. Man interessiert sich nicht für konkrete Schranken der Fähigkeit des Angreifers, etwa dass kein Angreifer 2^{80} Rechenschritte durchführen kann. Insbesondere wird gar nicht versucht, eine konkrete obere Schranke an die Fähigkeit des Angreifers zu bestimmen, um anschließend beispielsweise ein Verschlüsselungsverfahren gegen Angreifer abzusichern, die solch eine konkrete Schranke nicht überwinden können. Die Aussagen der Kryptographie sind vor allem asymptotische Aussagen. Kryptographische Sicherheitsgarantien betrachten den Aufwand des Angreifers als eine Funktion in einem Sicherheitsparameter k, etwa der Schlüssellänge eines Verschlüsselungsverfahrens.[2] Ein Verfahren wird nun als sicher beurteilt, wenn der Aufwand für den Angreifer im Sicherheitsparameter schneller wächst als jedes Polynom in k. Besonders wünschenswert ist beispielsweise ein exponentielles Wachstum des Aufwands, also ein Wachstum wie 2^k, denn dies entspricht dem Aufwand für ein vollständiges Durchsuchen aller Schlüssel der Länge k. Die Idee hinter dieser Betrachtungsweise ist, dass man so für jede konkrete Technologie, also für jeden (in k polynomial beschränkten) Angreifer den Sicherheitsparameter geeignet skalieren kann, um den Aufwand für den Angreifer unschaffbar zu machen.

Diese asymptotische Betrachtung der Sicherheit erlaubt insbesondere eine Arbeitsteilung in der Community der Kryptographen: Die asymptotische Sicherheit kann technologieunabhängig nachgewiesen und die konkrete Wahl des Sicherheitsparameters aus dem Stand der Informatikforschung geschätzt werden.[3] Dies entspricht etwa der Arbeitsteilung, die früher zwischen Kryptographie und Kryptoanalyse bestand, also zwischen „Code Makers" und „Code Breakers".

Für eine Systemtheorie Sicherheit, die das Schutzniveau gegen konkrete Angriffe beurteilen soll, ist die asymptotische Sicherheit also eine Art Zwischenergebnis, das es erleichtert, den konkret notwendigen Sicherheitsparameter zu schätzen. Es genügt, die Informatikforschung zur Lösung von anerkannten Standardproblemen zu betrachten, ohne die Feinheiten eines neu vorgeschlagenen Verschlüsselungs-verfahrens berücksichtigen zu müssen. Typische Standardprobleme, auf denen kryptographische Sicherheit basieren kann, sind beispielsweise das Zerlegen großer Zahlen in Primfaktoren[4], die Fehlerkorrektur für zufällige lineare Codes[5] oder das Finden von kürzesten Vektoren in hochdimensionalen Gittern[6]. Algorithmen zur Lösung dieser Probleme werden auch unabhängig von ihrer kryptographischen Bedeutung in der Informatik erforscht.

1.2 Beweisbare Sicherheit

In der Geschichte der Kryptographie gab es lange einen Wettlauf zwischen denen, die sich immer raffiniertere Verfahren ausdachten, etwa komplizierte elektromechanische Verschlüsselungsmaschinen wie die Enigma, und denen, die doch Struktur in der scheinbar perfekten Unordnung fanden und dann die Verfahren brechen konnten. Die Beurteilung der Sicherheit war früher häufig unvollständig und fehlerhaft, weil von den eigenen Kenntnissen auf die Möglichkeiten eines Angreifers geschlossen wurde. Die Sicherheit gegenüber sehr intelligenten Angreifern oder noch unbekannten Angriffen konnte so überhaupt nicht beurteilt werden.

Die moderne Kryptographie fußt dagegen auf drei Prinzipien.[7] Erstens wird in einem mathematischen Modell definiert, was Sicherheit, etwa für Verschlüsselungsverfahren, überhaupt bedeutet. Diese Sicherheitsdefinition kann beispielsweise eine Art Spiel sein, bei dem der Angreifer nur gemäß gewissen Spielregeln agieren darf. Gewinnt ein Angreifer das Spiel, etwa indem er den Inhalt einer verschlüsselten Nachricht bestimmen kann, so entspricht dies einer Sicherheitslücke gemäß der Sicherheitsdefinition. Zweitens werden explizite Sicherheitsannahmen getroffen, etwa über die rechnerische Schwierigkeit mathematischer Probleme, wie das Zerlegen großer Zahlen in Primfaktoren. Das dritte Grundprinzip ist der Sicherheitsbeweis. Hier wird bewiesen, dass unter den gegebenen Sicherheitsannahmen der Angreifer die Sicherheitsdefinition nicht verletzen kann, also etwa

2 | Vgl. Katz/Lindell 2015.
3 | Vgl. BSI TR-02102-1.
4 | Vgl. Rivest et al. 1978.
5 | Vgl. McEliece 1978.
6 | Vgl. Hoffstein et al. 1998
7 | Vgl. Katz/Lindell 2015.

das Spiel nur mit vernachlässigbarer Wahrscheinlichkeit gewinnen kann. Dies gibt eine sehr starke Sicherheitsgarantie: Selbst noch unbekannte Angriffe eines intelligenten Angreifers können ausgeschlossen werden.

1.3 Sicherheitsdefinitionen

Zur Zeit des Zweiten Weltkriegs hatte man keine Sicherheitsdefinition für die Verschlüsselung; es war eher die Vorstellung, dass ein Angreifer aus einer verschlüsselten Nachricht nichts erfahren dürfe.

Eine Sicherheitsdefinition, die von der konkreten Anwendung abstrahiert, birgt die Gefahr, mögliches Vorwissen, das der Angreifer hat, zu unterschlagen und damit die Sicherheit eines Verfahrens zu optimistisch zu beurteilen. Eine abstrakte Sicherheitsdefinition muss daher die pessimistische Annahme treffen, dass der Angreifer den Klartext vielleicht bis auf ein einziges Bit bereits kennt.[8] Eine moderne Definition verlangt daher, dass man aus dem Chiffrat nichts zusätzlich erfahren kann, egal wie viel man schon weiß. Solch eine Sicherheitsdefinition wird formal mathematisch beschrieben über ein Spiel, bei dem der Angreifer selbst zwei (gleich lange) Nachrichten vorschlägt und hinterher trotzdem nicht unterscheiden kann, welche der beiden Nachrichten in einem gegebenen Chiffrat enthalten ist.[9]

Die Enigma erfüllt eine solche moderne Sicherheitsdefinition nicht, denn sie kann konstruktionsbedingt keinen Buchstaben bei der Verschlüsselung gleich lassen: Ein „e" wird also niemals in ein „e" verschlüsselt. Ein Angreifer kann nun leicht zwei Nachrichten unterscheiden, indem er überprüft, ob irgendein Buchstabe beim vermuteten Klartext und beim Chiffrat an derselben Position steht. Diesen vermuteten Klartext kann er dann ausschließen.

Um von der konkreten Anwendung zu abstrahieren, muss man auch verschiedene Angreiferfähigkeiten betrachten, etwa Angreifer, die nur passiv lauschen, oder solche, die Chiffrate für den Angriff verändern dürfen.[10] Da es viel weniger Typen von Angreiferfähigkeiten in der Kryptographie gibt als potenzielle Anwendungen, ist diese Abstraktion eine Komplexitätsreduktion. Um kryptographische Verfahren im Rahmen einer Systemtheorie Sicherheit zu nutzen, muss lediglich gewährleistet sein, dass der Angriffstyp richtig gewählt ist. Häufig neigt man dazu, die Verschlüsselung gegen sehr starke, eventuell sogar zu starke Angreiferfähigkeiten zu sichern. Dadurch ist man auf der sicheren Seite, und häufig sind selbst sehr starke kryptographische Verfahren noch effizient genug, sodass man sich sogar ein Zuviel an kryptographischer Sicherheit leisten kann.

1.4 Sicherheitsmaßnahmen

Von wenigen Ausnahmen abgesehen, etwa der sogenannten One-Time-Pad-Verschlüsselung, bei der der Schlüssel so lang ist wie die Nachricht selbst, oder dem Quantenschlüsselaustausch, kann kryptographische Sicherheit bisher nur auf der Basis von Sicherheitsannahmen nachgewiesen werden. Man muss dabei zwei Arten der Annahmen unterscheiden: zum einen Annahmen, die durch die Wahl des Bedrohungsmodells implizit getroffen werden, zum anderen Annahmen, die sehr explizit getroffen werden. Bei der Verschlüsselung wird beispielsweise implizit angenommen, dass die Endgeräte der Kommunikationspartner nicht vom Angreifer korrumpiert sind und dass die Maschinen die Schlüssel für die Verschlüsselung echt zufällig ziehen können. Diese impliziten Annahmen werden sogar beim One-Time-Pad oder beim Quantenschlüsselaustausch getroffen. Eine explizite Annahme ist etwa, dass das Faktorisieren langer Zahlen asymptotisch nicht in Polynomialzeit möglich ist[11] oder dass das Faktorisieren von 4.000 bit-Zahlen mit der Technologie der nächsten sechs Jahre nicht möglich sein wird[12]. Solche Annahmen über die Schwierigkeit von Problemen sind unter anderem nötig, weil immer noch unbewiesen ist, ob es schwierige Probleme gibt, deren Lösung leicht überprüfbar ist. Die Frage, ob es solche Probleme gibt, ist bekannt als das P-versus-NP-Problem.[13] Gäbe es solche Probleme nicht, so wäre beispielsweise das Lösen eines Sudoku-Rätsels ähnlich einfach wie das Überprüfen der Korrektheit eines gelösten Sudoku, selbst wenn man Sudokus beliebiger Größe betrachtet. Insbesondere wären dann nahezu alle Verschlüsselungsverfahren unsicher, weil das Errechnen des verwendeten Schlüssels ähnlich einfach wäre wie das Überprüfen, ob ein gegebener Schlüssel zu einem konkreten Chiffrat der passende Schlüssel ist.

In der Kryptographie wird von Sicherheitsannahmen ausgegangen. Eine Systemtheorie Sicherheit, die ein reales Risiko errechnen will, muss auch berücksichtigen, wie plausibel eine solche Annahme ist, das heißt, wie hoch die Wahrscheinlichkeit ist, dass die Annahme nicht gilt. Mit der letzten Formulierung wird

8 | Vgl. Goldwasser/Micali 1984.
9 | Vgl. Bellare et al. 1997.
10 | Vgl. Bellare et al. 1998.
11 | Vgl. Goldreich 2004a.
12 | Vgl. BSI TR-02102-01.
13 | Vgl. Cook 1971.

auch klar, dass solche Wahrscheinlichkeiten in einer Systemtheorie Sicherheit eher einem „Degree of Belief" entsprechen, denn natürlich ist eine konkrete Annahme wahr oder falsch.

Wieder ergibt sich eine Arbeitsteilung. Einige Sicherheitsforscher können ausgehend von Sicherheitsannahmen Verfahren entwickeln, während andere die Plausibilität der Annahmen untersuchen. Da mit Sicherheitsannahmen immer ein Risiko verbunden ist, plädieren Kryptographen für eine hohe Diversität bei den Annahmen, also für eine Risikostreuung, damit eine fehlerhafte Annahme keine katastrophalen Folgen hat. Leider wird in der Praxis häufig nach der Effizienz der Verfahren ausgewählt und die Gefahr einer Monokultur nicht beachtet.

1.5 Sicherheitsbeweise

Hat man eine präzise Sicherheitsdefinition und explizite Sicherheitsannahmen, ist es möglich, die Sicherheit von einem Verschlüsselungsverfahren mathematisch zu beweisen. Dazu zeigt man, dass jeder effiziente Algorithmus, der für das Verschlüsselungsverfahren die Sicherheitsdefinition bricht, zu einem Algorithmus umgebaut werden kann, der die Sicherheitsannahme verletzt. Da ein Verschlüsselungsverfahren verhältnismäßig kompliziert sein kann, die zugrunde liegende Sicherheitsannahme aber einfach formuliert werden kann, ist ein solcher Sicherheitsbeweis eine Komplexitätsreduktion, und das Risiko, dass ein Verschlüsselungsverfahren gebrochen wird, kann mit dem Risiko gleichgesetzt werden, dass die zugrunde liegende Annahme nicht stimmt.

Die beweisbare Sicherheit trägt also zu einer Systemtheorie Sicherheit bei, indem sie das Abschätzen des Risikos erleichtert. Der Beweis reduziert das Abschätzen des Risikos auf die Wahrscheinlichkeit, dass die zugrunde liegenden Sicherheitsannahmen nicht gelten. Dennoch muss man mit dem Begriff der beweisbaren Sicherheit vorsichtig sein, da die Aussagen und Beweise nur innerhalb der Grenzen der Modellwelt und nur insoweit gültig sind, als die Modellwelt die Wirklichkeit genau genug beschreibt. Angriffe, die sich in diesem Modell nicht abbilden lassen, werden Seitenkanalangriffe genannt. Ein bekanntes Beispiel dafür ist der Stromverbrauch von Chipkarten.[14] So kann ein beweisbar sicheres kryptographisches Verfahren über den Stromverbrauch Geheimnisse preisgeben, wenn im Modell der Stromverbrauch gar nicht berücksichtigt wird. Erfolgreiche Seitenkanalangriffe führen natürlich dazu, dass neue mathematische Modelle entwickelt werden, die diese Angriffe mit betrachten.

Eine umfassende Systemtheorie Sicherheit muss also auch das Risiko berücksichtigen, dass das einem Sicherheitsbeweis zugrunde liegende Modell falsch ist und Angriffe außerhalb des Modells möglich sind. Es ist aber völlig unklar, inwieweit dieses Risiko sinnvoll berechnet oder abgeschätzt werden kann. Vielleicht muss jede Systemtheorie Sicherheitsannahmen treffen, und das Risiko, dass diese Annahmen falsch sind, könnte ein nicht präzise quantifizierbares Restrisiko sein. Eine Vergleichbarkeit von Schutzniveaus bleibt jedoch trotz Restrisiko erhalten, da Modelle miteinander verglichen werden können. Kann ein Modell beispielsweise alle Angriffe eines anderen Modells darstellen, so sind die Sicherheitsgarantien in dem umfassenderen Modell weitreichender.

Abgesehen von dem Restrisiko, dass Angriffe außerhalb des Modells möglich sind, ist die Garantie, die die beweisbare Sicherheit gibt, sehr stark. Relativ zu den Sicherheitsannahmen werden alle Angriffe, die innerhalb des Modells überhaupt formulierbar sind, ausgeschlossen; dies beinhaltet auch bisher unbekannte Angriffe von beliebig intelligenten Angreifern.

Aber auch in der Kryptographie gibt es Verfahren, etwa sogenannte kryptographische Hashfunktionen oder symmetrische Verschlüsselungsverfahren, bei denen das Prinzip der beweisbaren Sicherheit nicht angewandt wird, sondern der Fortschritt viel stärker auf der Erfahrung mit bekannten Angriffen beruht. Dies liegt daran, dass beweisbar sichere Alternativen hier bisher deutlich weniger effizient sind und symmetrische Verfahren sowie Hashfunktionen selten erfolgreich angegriffen wurden, man also bisher wenig schlechte Erfahrung mit dieser Herangehensweise gemacht hat.

Die Snowden-Enthüllungen haben gezeigt, dass die NSA kryptographische Verfahren nicht direkt angreifen konnte. Stattdessen wurden Hintertüren in der Software installiert, die Nachrichten ausleiten, bevor sie verschlüsselt werden, oder Zufallszahlengeneratoren so modifiziert, dass keine Schlüssel mit hoher Sicherheit gewählt werden konnten.[15] Dies macht deutlich, dass das Restrisiko, dass die Modellannahmen der Kryptographie falsch sein könnten, nicht unterschätzt werden darf. Trotzdem spricht gerade dieses Beispiel für die Herangehensweise der Kryptographie. Es genügt, das Risiko zu betrachten, dass die Annahmen falsch sind (oder ein Fehler im Beweis sein könnte).

14 | Vgl. Kocher et al. 1999.
15 | Vgl. Perlroth et al. 2013.

2 Kryptographische Protokolle

Kryptographische Verfahren werden anders erforscht und anders beurteilt als über einen Risikobegriff. Dennoch liefert die Forschung präzise Ergebnisse, die eine Systemtheorie Sicherheit unterstützen. Die Überlegungen zur Verschlüsselung sollen nun auf allgemeinere und komplexere kryptographische Protokolle erweitert werden.

Kryptographie ermöglicht weitaus mehr als sichere Kommunikation. Digitale Signaturen erlauben es, Verträge online abzuschließen, und die Blockchain-Technologie ermöglicht es sich gegenseitig misstrauenden Parteien, eine gemeinsame, konsistente Sicht, etwa auf Kontostände und Überweisungen, zu erhalten. Elektronische Bezahlverfahren[16], Online-Banking[17] und Online-Voting[18] sind weitere Beispiele komplexerer kryptographischer Protokolle. Immer geht es darum, verteilt eine Berechnung gemeinsam durchzuführen, obwohl die unterschiedlichen Parteien nicht notwendigerweise vertrauenswürdig sind.

Ein erstaunliches Ergebnis der theoretischen Kryptographie ist, dass prinzipiell jede beliebige Berechnung verteilt so durchgeführt werden kann, dass korrumpierte Teilnehmer weder die Geheimnisse anderer Teilnehmer erfahren noch die Ergebnisse verfälschen können.[19] Man spricht hier von sicheren Mehrparteienberechnungen. Beispiele hierfür sind Online-Auktionen, bei denen außer dem gewinnenden Gebot keine anderen Gebote bekannt werden, oder ein Abgleich von Fahndungslisten, ohne dass eine Fahndungsliste offengelegt werden muss. Dass die Kryptographie jenseits der Verschlüsselung viele andere Probleme, die durch Misstrauen entstehen, lösen kann, ist einem breiteren Publikum erst durch kryptographische Währungen wie Bitcoins und die dahinterliegende Blockchain-Technologie bekannt geworden.

Wieder versucht die Kryptographie, gegen große Klassen von Angreifern sicher zu sein und nicht nur schon bekannte Angriffe abzuwehren. So wie bei der Verschlüsselung müssen – innerhalb eines mathematischen Modells – die Sicherheit präzise definiert und klare Annahmen über die Mächtigkeit des Angreifers getroffen werden. Danach ist es möglich, alle Angriffe, die innerhalb des Modells zulässig sind, beweisbar abzuwehren. Interessanterweise zielt die Sicherheitsdefinition aber nicht auf eine Risikokenngröße. Häufig ist selbst ein komplexes kryptographisches Protokoll nur Teil eines größeren Systems, und ein Risiko oder die genaue Absicht eines Angreifers sind auf der Ebene des Protokolls noch nicht definiert. Wieder muss die Kryptographie von dem Anwendungskontext abstrahieren, und es muss dennoch klar sein, wie man die Ergebnisse der Kryptographie im Rahmen einer Systemtheorie Sicherheit nutzen kann, um das Gesamtrisiko besser bestimmen zu können.

Die Sicherheitsdefinition für ein komplexeres kryptographisches Protokoll erfolgt über eine Spezifikation in einer idealisierten Modellwelt, in der eine vertrauenswürdige Instanz die Aufgabe des Protokolls ausführt.[20] In dieser idealen Welt sind die Fähigkeiten eines Angreifers auf das beschränkt, was prinzipiell nicht zu verhindern ist. Ein Angreifer kann seine eigenen Eingaben an die vertrauenswürdige Instanz oder die für ihn bestimmte Ausgabe der vertrauenswürdigen Instanz verändern. Ansonsten wird jede Abweichung eines realen Protokolls von der idealen Spezifikation als erfolgreicher Angriff gewertet. Genauer wird gefordert, dass es für jeden realen Angreifer auf das reale Protokoll einen (wie beschrieben stark beschränkten) Angreifer im idealen Protokoll gibt, sodass das Systemverhalten des realen Protokolls mit realem Angreifer und das Systemverhalten der vertrauenswürdigen Instanz mit eingeschränktem Angreifer ununterscheidbar sind. Diese sehr strenge Sicherheitsdefinition bietet Sicherheit für jeden Anwendungskontext, da jede Unsicherheit in irgendeinem Kontext zu einer Unterscheidbarkeit des Realen und des Idealen führen würde. Den eingeschränkten Angreifer im Idealen, der in der Lage sein muss, einen vom realen Angriff ununterscheidbaren Angriff durchzuführen, nennt man auch „Simulator", und man spricht vom Simulationsparadigma, wenn eine Sicherheitsdefinition fordert, dass es für jeden realen Angreifer einen Simulator gibt, sodass das reale Protokoll und das ideale Protokoll, das von der vertrauenswürdigen Partei durchgeführt wird, ununterscheidbar sind.

Der Begriff Simulator ist etwas missverständlich, denn es geht nicht darum, reale Angriffe zu simulieren und ein System als sicher zu erachten, wenn keiner der simulierten Angriffe erfolgreich ist. Ein solches Vorgehen würde lediglich schon bekannte Angriffe untersuchen und ausschließen können. Aussagen über einen sehr intelligenten Angreifer sind so nicht möglich. Der Simulator in der Sicherheitsdefinition ist vielmehr eine Art Gedankenexperiment, das plausibel macht, dass die Sicherheit nicht durch einen realen Angreifer verletzt werden kann, da ein

16 | Vgl. EMVCo 2011.
17 | Vgl. Die Deutsche Kreditwirtschaft 2018.
18 | Vgl. Adida 2008.
19 | Vgl. Goldreich et al. 1987.
20 | Vgl. Goldreich 2004b.

Angreifer in der idealen, per definitionem sicheren Modellwelt dasselbe tun kann – oder zumindest etwas, das ununterscheidbar vom realen Angriff ist.

Eine sehr starke Variante des Simulationsparadigmas garantiert sogar, dass reale Protokolle und ideale Protokolle ununterscheidbar bleiben, selbst wenn beliebig viele davon nebenläufig durchgeführt werden.[21] Dies ist nicht selbstverständlich, da Protokollnachrichten aus einem Protokoll in ein anderes Protokoll eingeschleust werden könnten. Protokolle können für sich genommen sicher sein und dennoch in einem größeren Kontext unsicher werden, wenn der Sicherheitsbegriff nicht streng genug ist. Die starke Variante des Simulationsparadigmas, die garantiert, dass Protokolle sogar in beliebigem Anwendungskontext sicher bleiben, ist besonders nützlich für eine Systemtheorie Sicherheit, denn man kann nun in komplexen Anwendungen alle kryptographischen Protokolle durch ideale Protokolle ersetzen, und jede Risikokenngröße bleibt gleich. Die komplexe Anwendung ist mit idealisierter Kryptographie aber viel einfacher zu analysieren, und eine Risikoabschätzung wird unter Umständen dadurch erst möglich. Das Simulationsparadigma bedeutet für eine Systemtheorie Sicherheit eine Reduktion der Komplexität, obwohl die Aussagen der simulationsbasierten Sicherheit keine Risikokenngröße sind. Es ist vielmehr so, als ob man die Kryptographie „vor die Klammer gezogen hat". Das Gesamtrisiko lässt sich abschätzen durch das Risiko, dass die Sicherheitsannahmen für eine konkrete Anwendung nicht gelten, und das Risiko der Anwendung selbst, in der die Kryptographie aber idealisiert und unangreifbar ist.

3 Fazit

Die Beurteilung von Verschlüsselungsverfahren und auch von komplexeren kryptographischen Protokollen erfolgt nicht über einen Risikobegriff, sondern über eine Ununterscheidbarkeit des realen Protokolls von einem idealisierten Baustein. Obwohl in der Kryptographie also keine Risikokenngröße bestimmt wird, unterstützt sie das Berechnen eines Gesamtrisikos, denn man kann in einer Risikoanalyse eines komplexen Gesamtsystems alle realen kryptographischen Protokolle durch ideale Bausteine ersetzen und die Risikoanalyse damit substanziell vereinfachen, weil von der verwendeten Kryptographie völlig abstrahiert wird.

Es stellt sich nun die Frage, ob eine Systemtheorie Sicherheit vielleicht gar keine alles in sich vereinende komplexe Theorie sein muss, sondern vielmehr eine Menge von Theorien, die es erlauben, ein Gesamtsystem immer einfacher zu machen. Auf oberster Ebene ginge es dann nur noch darum, wie man die Ergebnisse und Beiträge der einzelnen Theorien verbindet. So wäre die Systemtheorie Sicherheit ein – vielleicht niemals ganz vollständiger – Werkzeugkasten, mit dem ein komplexes Gesamtsystem modularisiert, also in einfachere Teilsysteme zerlegt, oder durch Abstraktion vereinfacht werden kann. Eine Systemtheorie Sicherheit könnte über Fallunterscheidungen, etwa ob bestimmte Sicherheitsannahmen gelten oder nicht, die Risikoanalyse in mehrere einfachere Analysen zerlegen. Idealerweise nutzt eine Systemtheorie Sicherheit viele Teildisziplinen und bietet Schnittstellen, die es erlauben, die durch Abstraktion oder Vereinfachung gewonnenen Teilergebnisse der einzelnen Disziplinen wieder auf das Gesamtsystem zu übertragen.

Vielleicht wird die Suche nach einem Gesamtmodell aber auch zeigen – hier könnte man eine Idee aus dem Software-Engineering aufgreifen –, dass ein solches Gesamtmodell zu komplex und nicht handhabbar wäre. Dann müsste man aus verschiedenen Teildisziplinen heraus unterschiedliche Sichten auf das Gesamtsystem entwickeln und versuchen, diese Sichten konsistent zu halten. Als Konsequenz gäbe es nicht mehr eine Zahl, die das Risiko am besten abschätzt, sondern viele Risikokenngrößen aus unterschiedlichen Disziplinen, die nicht weiter integriert werden können, etwa weil die Plausibilität von Sicherheitsannahmen oder Restrisiken verschieden eingeschätzt werden können.

Wir kennen die Systemtheorie Sicherheit noch nicht vollständig; vielleicht ist sie auch eine Theorie des Prozesses, wie man Systeme immer sicherer macht, aber selbst wenn wir nur eine unvollständige Theorie haben, können wir schon jetzt kryptographische Ergebnisse zur Vereinfachung der Risikoanalyse nutzen. Interessanterweise scheint dieser Nutzen der Kryptographie unabhängig von der konkreten Ausgestaltung der Systemtheorie zu sein.

21 | Vgl. Canetti 2001.

Literatur

Adida 2008
Adida, B.: *Helios: Web-based Open-Audit Voting*, 2008.

Bellare et al. 1997
Bellare, M./Desai, A./Jokipii, E./Rogaway, P: *A Concrete Security Treatment for Symmetric Encryption*, 1997.

Bellare et al. 1998
Bellare, M./Desai, A./Pointcheval, D./Rogaway, F.: „Relations Among Notions of Security for Public-Key Encryption Schemes". In: *Cryptology – Crypto 98 Proceedings, Lecture Notes in Computer Science*, 1462, Springer-Verlag 1998.

BSI TR-02102-1
BSI – TR-02102-1: *Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen*, 2018-02. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf;jsessionid=AF2398D8B90DB2602E950F897EC20F03.2_cid351?__blob=publicationFile&v=8 [Stand: 11.06.2018].

Canetti 2001
Canetti, R.: *Universally Composable Security: A New Paradigm for Cryptographic Protocols*, 2001.

Cook 1971
Cook, S.: *The Complexity of Theorem Proving Procedures*, 1971.

Die Deutsche Kreditwirtschaft 2018
Die Deutsche Kreditwirtschaft: *FinTS Financial Transaction Services*, 2018

EMVCo 2011
EMVCo: *Book 2: Security and Key Management*, 2011.

Goldwasser/Micali 1984
Goldwasser, S./Micali, S.: *Probabilistic Encryption*, 1984.

Goldreich et al. 1987
Goldreich, O./Micali, S./Widgerson, A.: *How to Play any Mental Game*, 1987.

Goldreich 2004a
Goldreich, O.: *Foundations of Cryptography. I Basic Techniques*, Cambridge: Cambridge University Press 2004.

Goldreich 2004b
Goldreich, O.: *Foundations of Cryptography. II Basic Applications*, Cambridge: Cambridge University Press 2004.

Hoffstein et al. 1998
Hoffstein, J./Pipher, J./Silverman, J. H.: „NTRU: A Ring-Based Public Key Cryptosystem". In: Buhler, J. P. (Hrsg.): *Algorithmic Number Theory* (ANTS 1998. Lecture Notes in Computer Science), 1423, Berlin, Heidelberg: Springer 1998.

Kocher et al. 1999
Kocher, P./Jaffe, J./Jun, B.: „Differential Power Analysis". In: Wiener M. (Hrsg.): *Advances in Cryptology – CRYPTO' 99*. (CRYPTO 1999. Lecture Notes in Computer Science), 1666, Berlin, Heidelberg: Springer 1999.

Katz/Lindell 2015
Katz, J./Lindell, Y.: *Introduction to Modern Cryptography, Chapman & Hall/Crc Cryptography and Network Security Series*, Zweite Auflage, 2015.

McEliece 1978
McEliece, R.: *A Public-Key Cryptosystem Based On Algebraic Coding Theory*, 1978.

Perlroth et al. 2013
Perlroth, N./Larson, J./Shane, S.: *N.S.A: Able to Foil Basic Safeguards of Privacy on Web*, 2013.

Rivest et al. 1978
Rivest, R./Shamir, A./Adleman, L.: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 1978.

7 Rechtliche Rahmenbedingungen

7.1 Sicherheit – Begriffe, Szenarien, Verantwortlichkeiten und Entscheidungsprozesse aus juristischer Sicht[1]

Prof. Dr. Klaus Vieweg
Direktor des Instituts für Recht und Technik (1991 – 2016)
Friedrich-Alexander-Universität Erlangen-Nürnberg

1 Einleitung

Technik ist häufig ambivalent. Sie schafft Nutzen, ist aber auch mit Risiken verbunden. Aus juristischer Perspektive sind insbesondere die Risiken in den Blick zu nehmen. Mit dem in vielfältiger Weise steuernden Recht soll die Grundlage für eine hinreichende Sicherheit geschaffen werden. Vereinfacht lassen sich die Zusammenhänge von technischen Risikoszenarien, den Rechtsetzern als generellen Entscheidungsträgern, den zuständigen Behörden und Gerichten als Entscheider in konkreten Einzelfällen sowie den Reaktionen der Adressaten der Rechtsetzung und Rechtsanwendung in einem Regelkreismodell darstellen.

Im Folgenden werden nach begrifflichen Klärungen (dazu 2) exemplarisch einige Risikoszenarien dargestellt (dazu 3), bevor die Verantwortlichkeiten (dazu 4) und Entscheidungsprozesse erörtert werden (dazu 5).

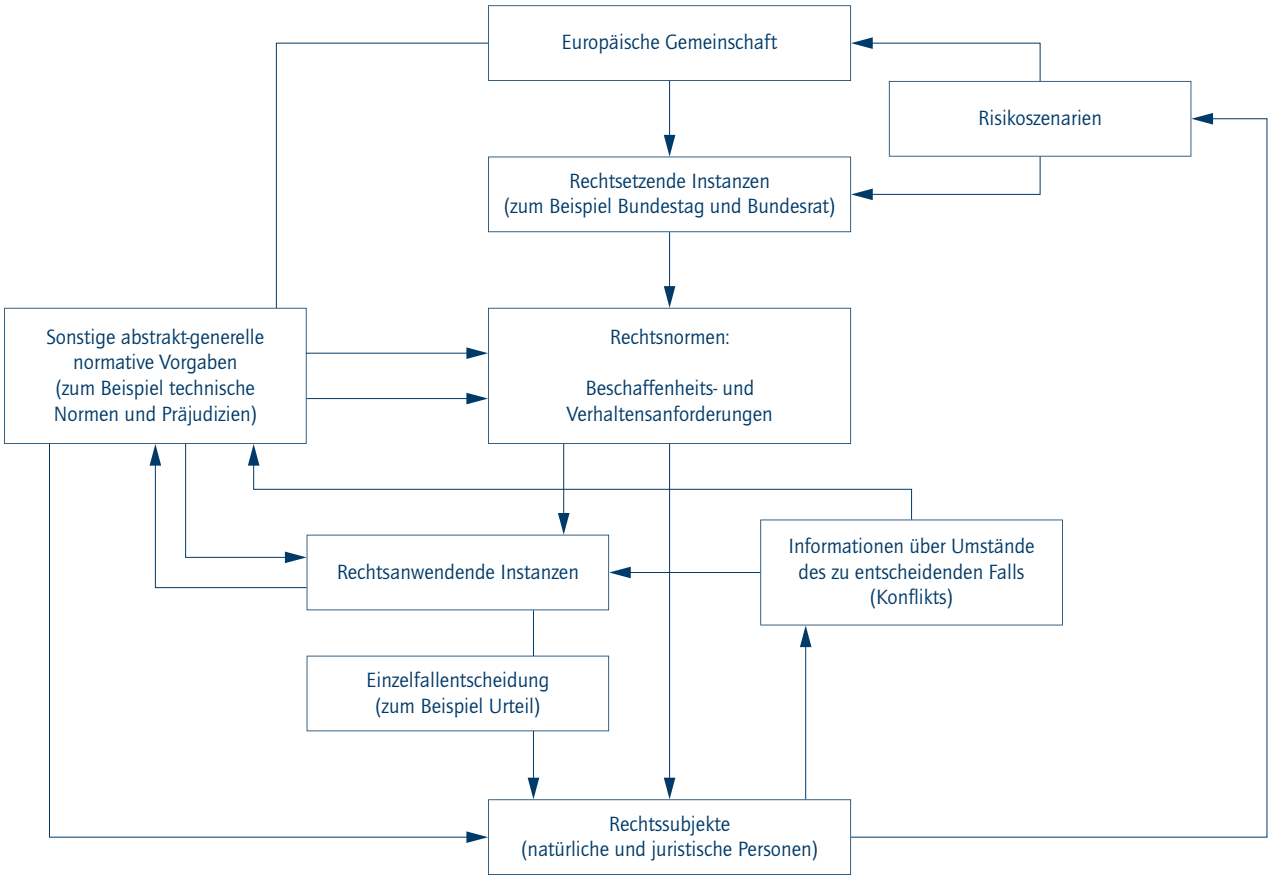


Abbildung 1: Rechtsetzung und Rechtsanwendung bezüglich technischer Risiken (Quelle: eigene Darstellung)

1 | Der Beitrag verbindet und aktualisiert die für diesen Band relevanten Teile der Beiträge Regenfus/Vieweg 2010 und Vieweg 2010.

2 Begriffe

Sicherheit und die Gegenbegriffe Risiko und Gefahr finden in der Alltagssprache und in den Fachsprachen der Technik und des Rechts Verwendung. Sie stehen dort mit weiteren Begriffen wie Gefährdung, Safety, Security, Restrisiko, Risikomanagement und Schaden in inhaltlichem Zusammenhang. Diese begriffliche Vielfalt kann zu Verständigungsproblemen führen.

Geht man davon aus, dass Entwicklung und Anwendung von Technik zwangsläufig mit Risiken verbunden ist – eine absolute Sicherheit gibt es nicht – und dass wesentliche Entscheidungen auf rechtlichen Vorgaben beruhen, so folgt daraus, dass den Verständigungsbrücken zwischen den Disziplinen „Technik" und „Recht" eine ganz besondere Bedeutung zukommt. Mit anderen Worten: Soll Fehlinvestitionen aufgrund negativer Zulassungsentscheidungen und/oder fehlender Marktfähigkeit sowie Schadensersatzpflichten bei fehlerhaften Produkten und im äußersten Fall strafrechtlichen Verurteilungen aus dem Weg gegangen werden, so sind bei der Entwicklung und Anwendung von Technik die rechtlichen Vorgaben im Blick zu behalten.

Im Bereich der Technik, insbesondere der technischen Sicherheit, hat die technische Normung eine Bedeutung erreicht, die kaum zu überschätzen ist. Sie bildet quasi synaptische Verbindungen an den Nahtstellen von Technik und Recht. Ihre praktische Relevanz zeigt sich im Umfang der Normenwerke, in der Anerkennung im Rahmen des Normenvertrags der Bundesregierung mit dem DIN und seit nunmehr über drei Jahrzehnten auf europäischer Ebene zunächst im „New Approach", seit 2008 im „New Legislative Framework" und seit 2012 in der EU-Verordnung 1025/2012 zur europäischen Normung. Angesichts dieser praktischen Relevanz ist der im Jahr 2005 vom DIN mit Blick auf europäische Rechtsakte herausgegebene Fachbericht 144 „Sicherheit, Vorsorge und Meidung in der Technik" ein exzellenter Prüfstein, um herauszufinden, ob und inwieweit die Sicherheits- und Risikoterminologie in einem ganz wesentlichen Bereich der Technik mit der des Rechts in Einklang zu bringen ist und welche Bedeutung wirtschaftliche Überlegungen dabei haben können.

Der Fachbericht 144 unterscheidet drei Bereiche des Umgangs mit Risiken, nämlich „Sicherheit", „Vorsorge" und „Meidung". Wichtig ist ferner die Gegenüberstellung von „Risikobearbeitung" und „Risikomanagement".

Unter „Sicherheit" eines Produkts versteht der Fachbericht 144 – entsprechend einem verbreiteten Begriffsverständnis – die „Freiheit von unvertretbaren Risiken". Da nur sichere Produkte auf den Markt gebracht werden dürfen, muss das naturwissenschaftlich nachweisbare Risiko ohne Rücksicht auf mit dem Einsatz verbundene Chancen (verstanden als Oberbegriff für Vorteile, Nutzen und andere positive Effekte sowie Erwartungen) so lange gemindert werden, bis es vertretbar ist.

„Risiko" ist nach den Definitionen der DIN 820-120 und des ISO/IEC-Guide 51 die Kombination aus Wahrscheinlichkeit des Schadenseintritts und Schadensausmaß. Die Berücksichtigung von Chancen sowie eine Verrechnung mit den Nachteilserwartungen finden nicht statt.

Die Begriffe „Gefahr" und „Sicherheit" korrespondieren insofern, als sie einmal die Anwesenheit, das andere Mal die Abwesenheit eines unvertretbaren Risikos bezeichnen. Für die Vertretbarkeit des Risikos ist entscheidend, ob es „in einem bestimmten Zusammenhang nach den gültigen Wertvorstellungen der Gesellschaft akzeptiert wird". Das „Restrisiko" ist das Risiko, das nach der Anwendung der jeweiligen Schutzmaßnahmen bestehen bleibt.

Neben diesen Termini verwendet der Fachbericht 144 den Begriff der „Gefährdung" als Übersetzung des englischen Begriffs „Hazard" und bezeichnet damit eine potenzielle Schadensquelle. Aus dem Begriff der Gefährdung werden drei weitere Begriffe abgeleitet: Die „Gefährdungssituation" ist ein Zustand, in dem Menschen, Güter oder die Umwelt einer oder mehreren Gefährdungen ausgesetzt sind; aus der Gefährdungssituation kann ein „Gefährdungsereignis", das heißt ein Ereignis, das einen Schaden verursachen kann, hervorgehen. Resultiert aus einer Gefährdungssituation tatsächlich ein Schaden, wird von einem „Schadensereignis" gesprochen.

Die „Vorsorgesituationen" zeichnen sich dadurch aus, dass der kausale Schadensablauf hinsichtlich der im Raum stehenden Risiken nicht bewiesen, jedoch ein begründeter Verdacht eines Zusammenhangs mit gewissen Schadensabläufen gegeben ist. Die Beantwortung der Frage, welche Vorkehrungen zu treffen sind, unterliegt daher – vor allem politischen – Nützlichkeitserwägungen. Chancen und Risiken werden an dieser Stelle abgewogen und zu einer von Verhältnismäßigkeitsüberlegungen geprägten Lösung verarbeitet.

In den als „Meidungssituationen" bezeichneten Fällen ist weder eine Wirkursächlichkeit wissenschaftlich nachweisbar noch ein Wirkmodell für denkbare Schadensszenarien bekannt; die Annahme eines Risikos beruht vielmehr ausschließlich auf statistischen Auffälligkeiten (sogenannten Pseudorisiken). Dementsprechend basiert die Entscheidung, vom Einsatz einer Technologie Abstand zu nehmen, nicht auf einer wissenschaftlichen Beurteilung, sondern allein auf politischen Erwägungen.

Die „Risikobearbeitung" ist ein Vorgang, bei dem es ausschließlich um die Minderung von Risiken geht, ohne die Chancen des jeweiligen Produkts zu berücksichtigen. Beim „Risikomanagement" – damit befasst sich der Fachbericht 144 nicht näher – findet dagegen eine Abwägung zwischen Chancen einerseits sowie Risiken andererseits statt, die in ein mit subjektiven Maßstäben gewonnenes Ergebnis mündet.

Ein von Dietz und Regenfus unternommener Vergleich der Terminologie des Fachberichts 144 mit dem Begriffsverständnis wesentlicher gesetzlicher Regelungen (Bundes-Immissionsschutzgesetz, Störfallverordnung, Geräte- und Produktsicherheitsgesetz, Produkthaftungsgesetz) hat bereits 2006 ergeben, dass der Fachbericht 144 im Ergebnis dem juristischen Verständnis sehr nahekommt und damit eine wertvolle Verständigungsbrücke zwischen Recht und Technik bildet.

3 Szenarien

Die Verständigung zwischen den verschiedenen Disziplinen und speziell das Verständnis von Gesetzgebung, Verwaltungsentscheidungen und Rechtsprechung erfordern neben den begrifflichen Klärungen Transparenz bezüglich des methodischen Vorgehens.

Deutlich werden sollten die Schritte, die in den verschiedenen Fachdisziplinen zwischen der Problemidentifikation (Risiken) und der Problemlösung (Reduzierung der Risiken) liegen. Angesichts der Vielfalt der Risiken und der Maßnahmen zu ihrer Reduzierung sind Vereinfachungen unumgänglich, um eine Verständigungsbasis zu schaffen. Als hilfreiche Orientierung erweist sich die systematische Erfassung von Szenarien in einem Risiko-Raster, das aus den Risikoquellen – menschliches Versagen (einschließlich organisatorisches Versagen), technisches Versagen, Naturereignis, Eingriff Unbefugter – und drei idealtypischen Steuerungsmodellen der Gesetzgebung – Selbstregulierung,

Risikoquelle / Steuerung (betroffene Interessen)	Menschliches Versagen (einschließlich organisatorisches Versagen)	Technisches Versagen	Naturereignis	Eingriff Unbefugter, insbes. externer Angriff
Selbstregulierung **(Eigeninteresse des Gefährdeten und etwaiger Vertragspartner)**	Hausunfall, z. B. Sturz von Stuhl bei Fehlgebrauch als Leiterersatz	Kabelbrand, Verschleiß (nach Inverkehrbringen und Ablauf der Gewährleistungsfrist)	Überschwemmung des Kellers durch Starkregen; Blitzschlag in Einfamilienhaus (Blitzableiter nicht obligatorisch)	Einbruch in Einfamilienhaus (nur staatliche Aktion ex post)
Kooperative Steuerung EG/Staat – Unternehmen/ Privatperson **(Allgemeininteresse und Eigeninteresse)**	Bedienungsfehler, der den Verhaltensanforderungen aufgrund des „New Approach" und des „New Legislative Framework" widerspricht	Konstruktions- oder Fabrikationsfehler, der den Beschaffenheitsanforderungen aufgrund des „New Approach" und des „New Legislative Framework" widerspricht	Blitzschlag/Hochwasser in genehmigungsbedürftiger Anlage § 3 Abs. 2 Nr. 2 i.V.m. § 9 Abs. 1 Nr. 2 Störfall-VO (Bezugnahme in Vollzugshilfe [9.2.6.1.2 i.V.m. Anhang 1 1.2.1.1 und 1.2.2])	Zielgerichtete Verursachung eines Störfalls in einer genehmigungsbedürftigen Anlage § 3 Abs. 2 Nr. 3 i.V.m. § 9 Abs. 1 Nr. 2 Störfall-VO Leitfaden SFK-GS-38 (Bezugnahme in Vollzugshilfe [9.2.6.1.3 i.V.m. Anhang 1 1.5])
Europäische/staatliche imperative Regulierung **(erhebliches Allgemeininteresse)**	Verstoß z. B. gegen: ■ Alkoholverbot für Fahranfänger (§ 24c StVG) ■ 0,5 Promille-Grenze Kfz-Führer (§ 24a StVG) ■ Fachkundenachweise ■ Pflicht, Schutzausrüstung zu tragen (§ 21a StVO: Sicherheitsgurte, Schutzhelme)	Risikoquellen werden erfasst vom (anlagenbezogenen) Sicherheitsbericht gemäß § 9 Störfall-VO; betroffen sind ca. 7.800 Anlagen i.S.v. § 3 Abs. 5 BImSchG in Deutschland	■ Erdbeben: Auslegung genehmigungsbedürftiger Anlagen (§ 5 Abs. 1 Nr. 1 Störfall-VO) ■ Blitzschlag: Blitzableiter für Versammlungsstätten (Art. 38 Abs. 3 Nr. 4 LStVG; Art. 44 BayBO) ■ Brandschutz für alle Gebäude ■ Hochwasserschutz (Bauverbot; Dammhöhe)	Zielgerichtete Verursachung eines Störfalls in einer genehmigungsbedürftigen Anlage § 3 Abs. 2 Nr. 3 i.V.m. § 9 Abs. 1 Nr. 2 Störfall-VO (Bezugnahme in Vollzugshilfe [13.3])

Abbildung 2: Risiko-Raster (Quelle: eigene Darstellung)

kooperative Steuerung und imperative Regulierung – gebildet wird. Diese Steuerungsmodelle spiegeln die berührten (Individual- und Allgemein-)Interessen wider und entsprechen im Idealfall dem Prinzip der Verhältnismäßigkeit. Auch die exemplarisch in die Matrix aufgenommenen Maßnahmen der Risikoreduzierung sind Ausdruck von Zweckmäßigkeits- und Verhältnismäßigkeitserwägungen (siehe Abbildung 2: „Risiko-Raster"). Selbstverständlich sind Kombinationen der Risikoquellen und Abstufungen der drei Steuerungsmodelle in der Praxis verbreitet.

Weitere Differenzierungen und Varianten des – recht groben – Risiko-Rasters sind möglich. Im Einzelfall ist zu prüfen, ob die Berücksichtigung zusätzlicher Aspekte hilfreich ist. So kann die Differenzierung nach den Steuerungsinstrumenten zwischen strafrechtlicher Verantwortlichkeit, zivilrechtlicher Haftung und öffentlich-rechtlichen Pflichten zweckmäßig im Hinblick auf die Verhaltenssteuerung sein. Sie geht ins Leere bei gezielten Eingriffen Unbefugter (insbesondere bei terroristischen Angriffen). Die Differenzierung nach dem Willen des Schädigers – gewollt oder ungewollt – führt hingegen kaum weiter, da sich die wichtigsten Fälle gewollter Schadenszufügung bereits als Eingriff Unbefugter im Risiko-Raster wiederfinden.

Das Risiko-Raster kann sowohl als Informationsbasis als auch als Prüfstein für die Vollständigkeit einer querschnittlichen Systemtheorie dienen. Es macht mit der Erwähnung des New Approach und des New Legislative Framework auch die Funktion der technischen Normung deutlich, die in der Praxis in weiten Bereichen eine nicht zu unterschätzende Bedeutung dadurch erlangt hat, dass der europäische Gesetzgeber die Konkretisierung seiner allgemein gehaltenen Sicherheitsanforderungen den europäischen Normungsorganisationen CEN, CENELEC und ETSI übertragen hat.

4 Verantwortlichkeiten

Das gemeinsame Ziel Sicherheit wird zweckmäßigerweise durch eine Verteilung der Aufgaben und Verantwortlichkeiten nach Fachqualifikation und Interesse verfolgt. Diese Verteilung findet auf unterschiedliche Weise statt. Wesentlich ist insofern, ob die gesetzlichen Regelungen eine Selbstregulierung erlauben oder konkrete Vorgaben enthalten. Zu beachten ist zudem die Einflussnahme von Lobbygruppen.

- Die Fälle der „Selbstregulierung" sind dadurch gekennzeichnet, dass das Eigeninteresse des Gefährdeten im Vergleich zum Allgemeininteresse derart im Vordergrund steht, dass der Gesetzgeber nicht aktiv wird, sondern den allgemeinen rechtlichen Rahmen (Vertragsrecht, deliktische Haftung, strafrechtliche Verantwortlichkeit) als ausreichend erachtet. Die Verteilung der Aufgaben und Verantwortlichkeiten erfolgt bilateral auf vertraglicher Grundlage zwischen demjenigen, der sich einem von ihm nicht gewünschten Risiko ausgesetzt sieht, und demjenigen, von dem er annimmt, dass er in der Lage ist, dieses Risiko auszuschließen oder zumindest auf ein für ihn akzeptables Maß zu senken (zum Beispiel Überprüfung elektrischer Endgeräte durch einen Fachmann, Installation eines Blitzableiters gegen Blitzschlag oder einer Alarmanlage als Einbruchsicherung für ein Einfamilienhaus). Beruht das Risiko allein auf einem menschlichen Versagen des Gefährdeten selbst, so kommt als wirtschaftliche Absicherung des Risikos auch eine Versicherungslösung in Betracht. Ebenso lässt sich das Haftpflichtrisiko eines potenziellen Schädigers durch eine entsprechende Versicherung abdecken.
- Die Verteilung der Aufgaben und Verantwortlichkeiten erfolgt tri- oder multilateral, wenn das Risiko über den individuellen Bereich hinausgeht und insbesondere (schutzbedürftige) Dritte und deren (Sach-)Güter sowie Allgemeingüter und -interessen betroffen sein können (zum Beispiel beim Brandschutz). In aller Regel gibt es in diesen Fällen gesetzliche Regelungen, die das konkrete Risiko betreffen. Insbesondere sind konkrete Vorgaben hinsichtlich der Zuständigkeit von Behörden und Gerichten, der zivilrechtlichen Haftung und der strafrechtlichen Verantwortlichkeit zu berücksichtigen.

Soweit die Verteilung der Aufgaben und Verantwortlichkeiten durch gesetzliche Vorgaben (tri- oder multilateral) erfolgt, sind im Idealfall zwei legislatorische Steuerungsansätze voneinander zu unterscheiden. Zum einen spielt die „klassische" imperative Regelung durch konkrete Gebote und Verbote nach wie vor sowohl auf nationaler als auch auf europäischer Ebene eine wichtige Rolle. Sie kommt insbesondere dann zum Tragen, wenn erhebliche Allgemeininteressen oder individuelle Rechtsgüter von besonderem Gewicht berührt sind. Zum anderen nimmt die Bedeutung der kooperativen Steuerung zwischen EU beziehungsweise Staat einerseits und den betroffenen Unternehmen und Privatpersonen andererseits zu. Besonders praxisrelevant sind der „New Approach" (1985) und das „New Legislative Framework" (2008). Typischerweise liegen der kooperativen Steuerung sowohl Allgemein- als auch Eigeninteressen der Regelungsadressaten zugrunde. Die in Teilen der Wissenschaft und Praxis vorgenommene Differenzierung zwischen sogenannten Safety- und Security-Problemen hat sich in den gesetzlichen Regelungen bislang nicht in Gänze niedergeschlagen (zum Beispiel fehlt noch eine Spezialregelung im Hinblick auf terroristische Angriffe auf

Kernkraftwerke). Hierfür dürften zwei Gründe maßgeblich sein: zum einen ein Nachhinken der Rechtsordnung, das man als „Legal Lag" bezeichnen kann (spätestens seit dem 11. September 2001 steht fest, dass durch Strafandrohung terroristische Angriffe nicht verhindert werden können), und zum anderen ein übergreifendes legislatorisches Schutzkonzept, das nicht – nach der Risikoquelle – zwischen „Safety" und „Security" unterscheidet, sondern den Rechtsgüterschutz als Ganzes im Blick hat.

5 Entscheidungsprozesse

Die wesentlichen (Sicherheits-)Entscheidungen werden in den Feldern Politik, Technik, Wirtschaft und Recht getroffen. Wesentliche Vorinformationen liefern die Naturwissenschaften, die Psychologie, Soziologie, Philosophie, Ethik und Geschichte. Die (Sicherheits-)Entscheidungen haben als Ausgangspunkt in der Regel unerwünschte Zustände und Ereignisse, die mit Begriffen wie „Risiko", „Gefährdung", „Gefahr" und „Schaden" beschrieben werden. Getroffen werden die (Sicherheits-)Entscheidungen nicht nach einheitlichen Methoden und Ansätzen; sie divergieren vielmehr insbesondere nach Funktion und fachlicher Ausrichtung des Entscheidenden einerseits sowie nach Art und Ausmaß des unerwünschten Zustands beziehungsweise Ereignisses andererseits. Auch die Safety-Security-Diskussion ist hier zu verorten. Fokussierungen auf die eigene Fachdisziplin und vor allem die Ausblendung der in den Bereichen Politik und Recht getroffenen Entscheidungen können den Aussagewert wissenschaftlicher Ergebnisse erheblich relativieren. Dahingegen dient die Schaffung von Verständigungsbrücken zwischen den verschiedenen Disziplinen der Qualität der Entscheidungsfindung und vermeidet Zeitverlust und Zusatzkosten.

Ausgangspunkt ist dabei die Überzeugung, dass es eine absolute, vollständige Sicherheit nicht gibt. Möglich ist nur eine relative, von den Umständen des Einzelfalls und dem Zeitablauf abhängige Sicherheit. Die Fragen lauten insbesondere: „Wie sicher ist sicher genug?" und „Wer entscheidet nach welchen Prinzipien und Kriterien?" Konkret stellen sich für die Entscheidungsträger die folgenden weiteren Fragen:

- Wer und/oder was sind die Schutzobjekte? Sind es der Mensch und seine (Sach-)Güter, oder ist es auch die ihm nicht zugeordnete, das heißt ungebundene Natur (Problem des sogenannten ökologischen Risikos beziehungsweise Schadens)?
- Wogegen soll geschützt werden? Gegen zielgerichtete Angriffe und Eingriffe (Security) und/oder gegen sonstige negative Wirkungen durch unerwünschte Zustände und Ereignisse (Safety – technisches Versagen, menschliches und organisatorisches Versagen, Naturereignisse)?
- Sollen noch unbekannte, aber bei der Entwicklung neuer Technologien nicht ausschließbare unerwünschte Zustände und Ereignisse (sogenannte Entwicklungsrisiken) in den Schutz miteinbezogen werden?
- Handelt es sich bei den unerwünschten Zuständen und Ereignissen um statistisch erfassbare oder zumindest schätzbare Größen oder um ein taktisch angepasstes Verhalten, einen dynamischen Prozess (zum Beispiel einen terroristischen Angriff, aber auch – als Naturereignis – die Mutationen von Viren bei Resistenzen)?
- Soll bereits der Begriff Ausgangspunkt für die Ergreifung von Maßnahmen sein? Mit anderen Worten: Sollen bei Vorliegen von Tatsachen, die sich unter den Begriff des unerwünschten Zustands beziehungsweise Ereignisses subsumieren lassen, Maßnahmen ergriffen, das heißt Konsequenzen gezogen werden (zum Beispiel Realisierung technisch-organisatorischer Maßnahmen, Einschreiten einer Behörde, Verweigerung der Genehmigung des Betriebs einer Anlage, Haftung, Strafbarkeit)?
- Sollen außer dem Ausmaß des unerwünschten Zustands beziehungsweise Ereignisses (dem potenziellen Schadensausmaß) und der Wahrscheinlichkeit des Eintritts dieses unerwünschten Zustands beziehungsweise Ereignisses – diese beiden Aspekte bilden den klassischen Risikobegriff (im Englischen: Risk) – auch Vorteile und Chancen in die Definition einbezogen werden? Falls ja: wie? Sollen zum Beispiel Quantifizierungen ausschlaggebend sein? Soll beispielsweise bei der Abwägung zwischen dem Risiko und den Vorteilen und Chancen das Verhältnismäßigkeitsprinzip gelten?
- Sollen auch Kostenaspekte einbezogen werden? Falls ja: wie (Quantifizierungsproblem, Abwägungsproblem)?

Im Rasterfeld, das durch das Steuerungsmodell der Selbstregulierung (betroffen sind vor allem Eigeninteressen) und die Risikoquelle des Eingriffs Unbefugter gebildet wird, lässt sich der Entscheidungsprozess (Eigenentscheidung des Gefährdeten) wie folgt kennzeichnen (siehe auch Abbildung 3: „Bilaterale Sicherheitslösung bei individueller Gefährdung"):

Kenntnisse, Erfahrungen, Gefühle und Interessen des Gefährdeten prägen dessen individuelle Risikobeurteilung, für die Schadensausmaß, Eintrittswahrscheinlichkeit, eigene Maßnahmen (wie Versicherung) und der Grad der Furcht vor dem Schadenseintritt maßgeblich sind. Hinzu kommen die diesbezüglichen Informationen durch den zur Beratung herangezogenen technischen Experten. Die vom technischen Experten unterbreiteten

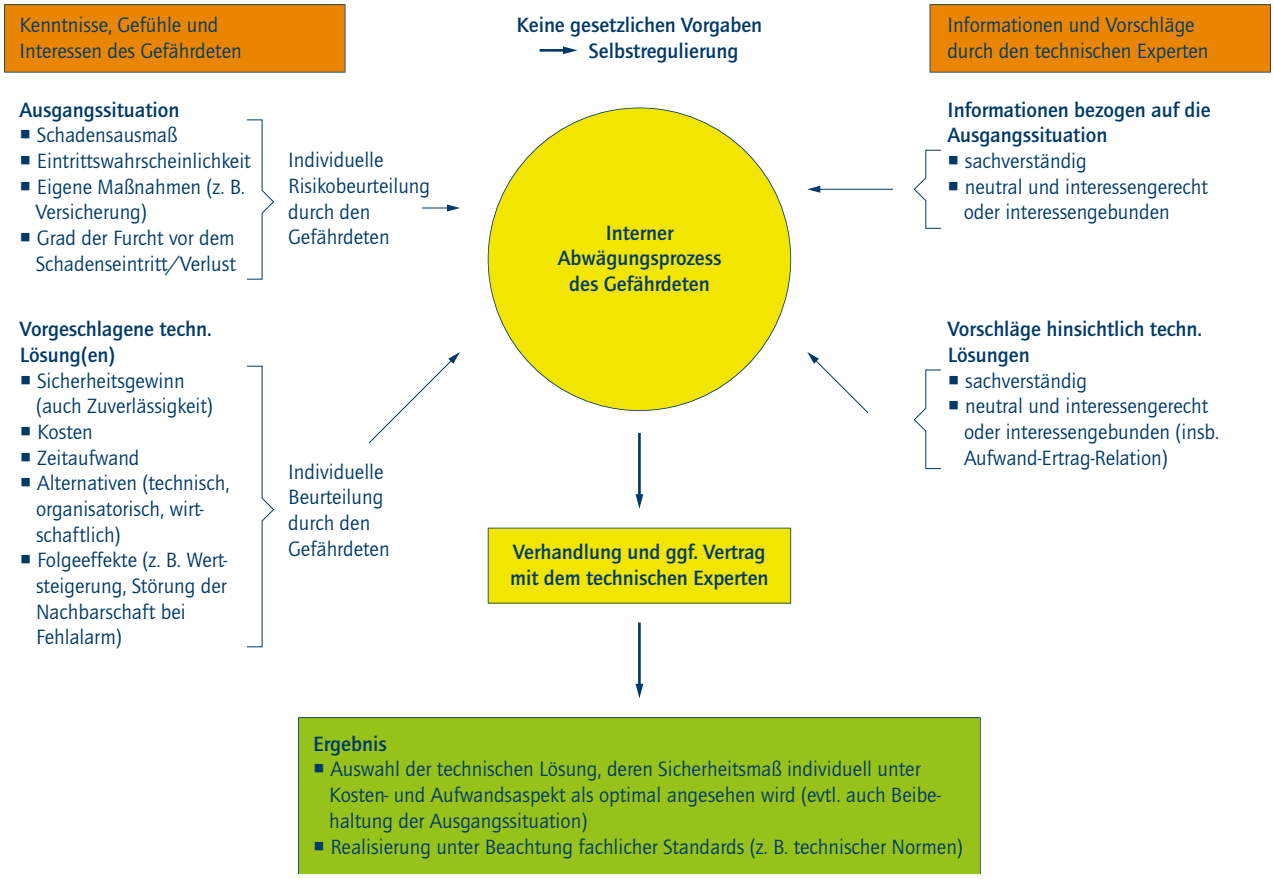


Abbildung 3: Bilaterale Sicherheitslösung bei individueller Gefährdung (Beispiel: Alarmanlage für Einfamilienhaus) (Quelle: eigene Darstellung)

technischen Lösungsvorschläge werden durch den Gefährdeten ebenfalls individuell unter den Aspekten Sicherheitsgewinn, Kosten, Zeitaufwand, Alternativen und Folgeeffekte beurteilt. Zentral ist ein interner Abwägungsprozess des Gefährdeten. Seine Verhandlungen mit dem technischen Sachverständigen können als Ergebnis – in Vertragsform – die Auswahl der technischen Lösung beinhalten, deren Sicherheitsmaß er individuell unter dem Kosten- und Aufwandsaspekt als optimal ansieht. Bei negativer Entscheidung bleibt es bei der risikoreicheren Ausgangssituation.

In den Rasterfeldern, die durch die Steuerungsmodelle der kooperativen Steuerung und der europäischen beziehungsweise nationalen imperativen Regulierung einerseits und den Risikoquellen des technischen Versagens, des Naturereignisses und des Eingriffs Unbefugter andererseits gebildet werden, lässt sich der Entscheidungsprozess hinsichtlich der Sicherheitslösung (vereinfacht) wie folgt kennzeichnen (siehe Abbildung 4: „Tri-/multilaterale Sicherheitslösung bei überindividueller Gefährdung"):

Der Entscheidungsprozess wird zum einen wesentlich beeinflusst durch die gesetzlichen Vorgaben zum Ausschluss beziehungsweise zur Verminderung der Risiken. Hierzu gehören die Vorgaben hinsichtlich der Zuständigkeiten, der Verantwortlichkeiten, des Verfahrens der Entscheidungsfindung, der in Betracht kommenden technisch-organisatorischen sowie administrativen Maßnahmen, der Versicherungslösungen sowie – vor allem – des Sicherheitsstandards. Zum anderen spielen auch bei dieser Entscheidung die Informationen über das Risiko – konkret: über die Ausgangssituation sowie die technischen Lösungsmöglichkeiten – eine wesentliche Rolle. Sowohl die gesetzlichen Vorgaben als auch die Informationen über das Risiko beeinflussen die Kommunikation und Kooperation zwischen dem Verantwortlichen für die Risikoquelle, dem technischen Experten und dem Staat, insbesondere dessen zuständigen Behörden. Die Entscheidung über die Sicherheitslösung ist dabei abhängig vom konkreten risikospezifischen gesetzlichen Steuerungsansatz.

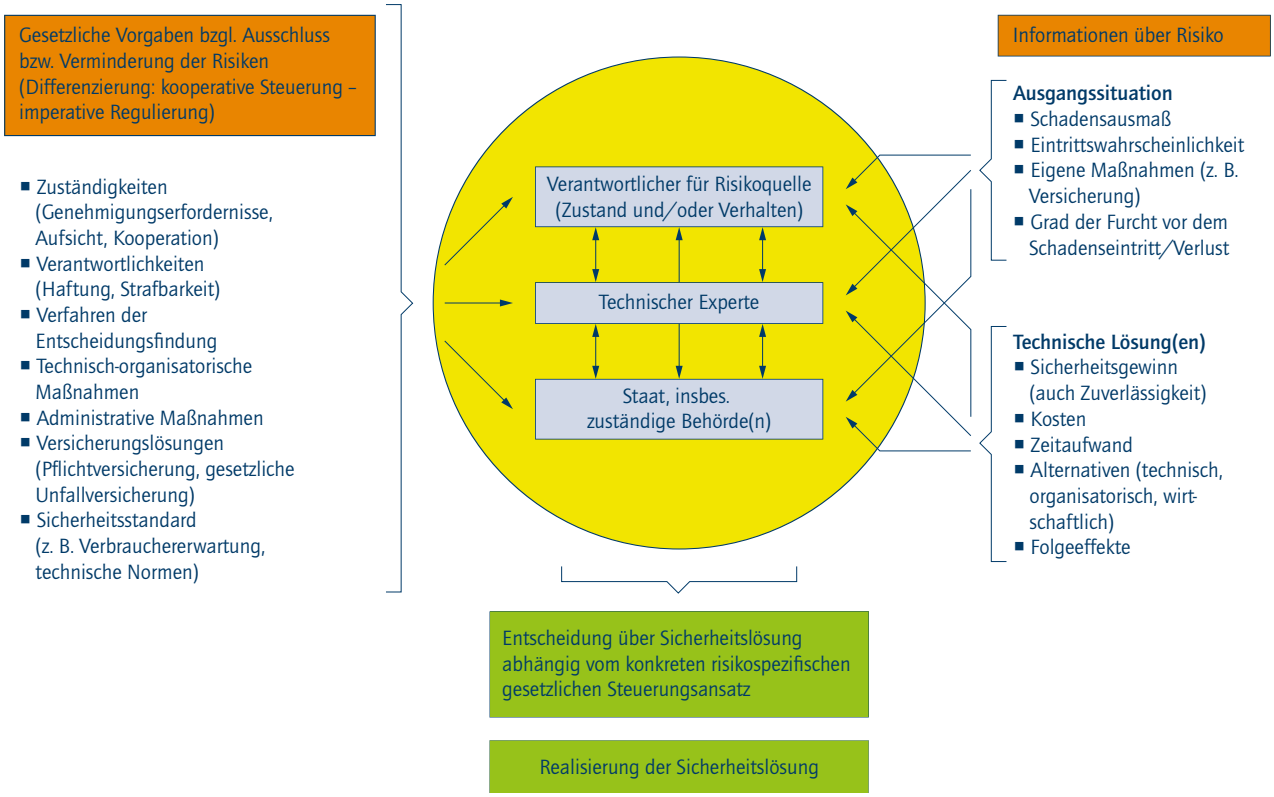


Abbildung 4: Tri-/multilaterale Sicherheitslösung bei überindividueller Gefährdung (insbesondere Dritter und deren Sachgüter sowie von Allgemeingütern und Allgemeininteressen) (Quelle: eigene Darstellung)

Aus der Warte eines – insbesondere europäischen oder nationalen – Regelungsgebers stellt sich ein systematisches Vorgehen hinsichtlich eines konkreten Risikos (zum Beispiel eines terroristischen Angriffs auf ein Kernkraftwerk oder eine genehmigungsbedürftige Anlage) wie folgt dar:

- Identifizierung des Risikos beziehungsweise der Risiken und Entscheidung über den Regelungsbedarf;
- Formulierung des Sicherheitsziels für das konkrete Szenario im Rahmen des Gesetzeszwecks;
- Festlegung des Steuerungsansatzes anhand der berührten Interessen und des Grundsatzes der Verhältnismäßigkeit;
- Ermittlung der in Betracht kommenden präventiven, kompensatorischen und repressiven Maßnahmen zur Beseitigung beziehungsweise Reduzierung der Risiken (zum Beispiel technische oder administrative Maßnahmen, Benutzerinformation);
- Festlegung der Aufgaben und Verantwortlichkeiten der Entscheidungsträger (Behörden, Industrie allgemein, konkrete Hersteller und Zulieferer, Normungsorganisationen, technische Sachverständige, Betreiber/Nutzer/Verbraucher);
- Steuerung des Verhaltens der Entscheidungsträger (zivilrechtliche Haftung, Kosten aufgrund administrativer Maßnahmen wie zum Beispiel Rückruf, Strafbarkeit, Ansehensverlust);
- Festlegung der Maßnahmen zur Beseitigung beziehungsweise Reduzierung der Risiken (zum Beispiel technischer oder administrativer Maßnahmen, Benutzerinformation) aufgrund der Risikobewertung.

Klärungsbedarf besteht hinsichtlich der Frage, ob den bisherigen Regelungen ein solches systematisches Vorgehen zugrunde liegt und ob insbesondere dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit Rechnung getragen wird. Unabhängig davon fördert die Transparenz des Vorgehens das wechselseitige Verständnis aller Beteiligten. Die Schwierigkeiten des Regelungsgebers werden deutlich, wenn man die Zusammenhänge in einem Regelkreismodell (siehe Abbildung 1: „Rechtsetzung und Rechtsanwendung“) betrachtet.

Zusammenfassung

1. Die Sicherheitsthematik ist interdisziplinär und damit auf Verständigung über Begriffe und über das methodische Vorgehen angewiesen. Verständigungsprobleme führen zu Zeitverlust, verursachen Zusatzkosten und mindern häufig die Qualität der Entscheidungsfindung.

2. Die technische Normung bildet die Brücke zwischen Technik und Recht. Daher ist es zweckmäßig, an die Terminologie des DIN-Fachberichts 144 anzuknüpfen. Sicherheit ist danach die Freiheit von unvertretbaren Risiken. Risiko wird definiert als Kombination aus Wahrscheinlichkeit des Schadenseintritts und Schadensausmaß. Für die Vertretbarkeit des Risikos ist entscheidend, ob es in einem bestimmten Zusammenhang nach den gültigen Wertvorstellungen der Gesellschaft akzeptiert wird. Unter Restrisiko wird das Risiko verstanden, das nach Anwendung der jeweiligen Schutzmaßnahmen verbleibt. Der Begriff der Gefährdung als Übersetzung des englischen Begriffs „Hazard" bezeichnet eine potenzielle Gefahrenquelle.

3. Hinsichtlich des methodischen Vorgehens, das die (Sicherheits-)Entscheidungen kennzeichnet, können – als Verständigungshilfe – Szenarien modelliert werden. Ausgangspunkt ist ein Risiko-Raster, das durch die vier Risikoquellen – menschliches Versagen (einschließlich organisatorisches Versagen), technisches Versagen, Naturereignis, Eingriff Unbefugter – sowie durch die drei idealtypischen rechtlichen Steuerungsmodelle – Selbstregulierung, kooperative Steuerung und imperative Regelung – gebildet wird.

4. Für die auf diese Weise gebildeten zwölf Rasterfelder werden die Aufgaben und Verantwortlichkeiten zweckmäßigerweise nach Fachqualifikation und Interesse verteilt. In den Fallgestaltungen, in denen das Eigeninteresse des Gefährdeten im Vordergrund steht, kommt die Selbstregulierung zum Tragen. Die Verantwortlichkeiten werden hingegen tri- oder multilateral vom Gesetzgeber verteilt, wenn es um den Schutz Dritter sowie um vorrangige Allgemeininteressen geht.

5. Die Entscheidungsprozesse divergieren insbesondere nach Funktion und fachlicher Ausrichtung der Entscheider sowie nach Art und Ausmaß des unerwünschten Zustands oder Ereignisses. Die Grundfragen lauten: Wie sicher ist sicher genug? Und: Wer entscheidet nach welchen Prinzipien und Kriterien? Hinzu kommen eine Reihe von Detailfragen, die bei den Entscheidungen gesehen und beantwortet werden müssen. In den Fällen der Selbstregulierung ist – gegebenenfalls nach Einholung externen technischen Sachverstands – ein interner Abwägungsprozess des Gefährdeten zentral. Handelt es sich um Fälle der kooperativen Steuerung oder der europäischen beziehungsweise staatlichen imperativen Regulierung, sind zum einen die gesetzlichen Vorgaben und zum anderen die verfügbaren Informationen über das Risiko sowie über die technischen Lösungsmöglichkeiten wesentlich.

Literatur

BMBU 2004
Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: *Vollzugshilfe zur Störfall-Verordnung vom März 2004*. URL: http://www.bmu.de/fileadmin/Daten_BMU/Download_PDF/Wirtschaft_und_Umwelt/vollzugshilfe_stoerfall_vo.pdf [Stand: 22.05.2018].

DIN 2005
Deutsches Institut für Normung e. V. (Hrsg.): *Sicherheit, Vorsorge und Meidung in der Technik*, DIN-Fachbericht 144, Berlin: Beuth Verlag 2005.

DIN 2008
Deutsches Institut für Normung e. V. (Hrsg.): *Sicherheitsgerechtes Gestalten technischer Erzeugnisse*, DIN 31000 (VDE 1000), Berlin: Beuth Verlag 2008.

DKE 2008
Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE) im DIN und VDE (Hrsg.): *Sicherheitsgerechtes Gestalten technischer Erzeugnisse*, Sonderdruck (Auszüge aus DIN 31000 (VDE 1000) und andere), Berlin: VDE Verlag/Beuth Verlag 2008.

Dietz/Regenfus 2006
Dietz, F./Regenfus, T.: „Risiko und technische Normung im Spannungsfeld von Recht und Technik". In: Vieweg, K. (Hrsg.): *Risiko – Recht – Verantwortung*, Köln, Berlin, Bonn, München: Carl Heymanns Verlag 2006, S. 403–429.

Di Fabio 1996
Di Fabio, U.: *Produktharmonisierung durch Normung und Selbstüberwachung*, Köln, Berlin, Bonn, München: Carl Heymanns Verlag 1996.

Hosemann 2007
Hosemann, G.: „Risikobeurteilung zur Konkretisierung staatlicher Vorschriften". In: *etz*, 12, 2007, S. 76–81.

Intertek Research and Testing Centre et al. 2005
Intertek Research and Testing Centre et al.: „Produktsicherheit in Europa – Ein Leitfaden für Korrekturmaßnahmen einschließlich Rückrufe". In: Geiß, J./Doll, W. (Hrsg.): *Geräte- und Produktsicherheitsgesetz (GPSG) – Kommentar und Vorschriftensammlung*, Stuttgart: Kohlhammer 2005, S. 366 ff.

Marburger 1976
Marburger, P.: *Regeln der Technik im Recht*, Köln, Berlin, Bonn, München: Carl Heymanns Verlag 1976.

Regenfus/Vieweg 2010
Regenfus, T./Vieweg, K.: „Sicherheits- und Risikoterminologie im Spannungsfeld von Recht und Technik". In: Winzer, P./Schnieder, E./Bach, F.-W. (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven* (acatech DISKUTIERT), Berlin, Heidelberg: Springer-Verlag 2010, S. 131–144.

Schneider 2018
Schneider, C.: „Durchsetzung technischer Anforderungen im Spannungsfeld zwischen sekundärrechtlicher Harmonisierung und privater Normung". In: Vieweg, K. (Hrsg.): *Festgabe Institut für Recht und Technik*, Köln, Berlin, Bonn, München: Carl Heymanns Verlag 2018.

Vieweg 1980
Vieweg, K.: „Gesamtdiskussion". In: Lukes, R. (Hrsg.): *Gefahren und Gefahrenbeurteilungen im Recht*, Teil I, Köln, Berlin, Bonn, München: Carl Heymanns Verlag 1980, S. 177–201.

Vieweg 1993
Vieweg, K.: „Recht und Risiko". In: GSF-Forschungszentrum für Umwelt und Gesundheit (Hrsg.): *mensch + umwelt*, 8. Auflage, Neuherberg 1993, S. 47–52.

Vieweg 1997
Vieweg, K.: „Reaktionen des Rechts auf Entwicklungen in der Technik". In: Schulte, M. (Hrsg.): *Technische Innovation und Recht – Antrieb oder Hemmnis?*, Heidelberg: C. F. Müller 1997, S. 35–54.

Vieweg 1999
Vieweg, K.: „Technik und Recht". In: Berlin-Brandenburgische Akademie der Wissenschaften/Nordrhein-Westfälische Akademie der Wissenschaft (Hrsg.): *Technik und Technikwissenschaften – Selbstverständnis, Gesellschaft, Arbeit, Beiträge zum Arbeitssymposium des Konvents für Technikwissenschaften (KTW)* (Tagungsband), Berlin, Düsseldorf 1999. Auch abgedruckt in Vieweg, K./Haarmann, W. (Hrsg.): *Beiträge zum Wirtschafts-, Europa- und Technikrecht – Festgabe für Rudolf Lukes zum 75. Geburtstag*, Köln, Berlin, Bonn, München, Carl Heymanns Verlag 2000, S. 199–213.

Vieweg 2000
Vieweg, K. (Hrsg.): *Techniksteuerung und Recht – Referate und Diskussionen eines Symposiums an der Universität Erlangen-Nürnberg*, Köln, Berlin, Bonn, München: Carl Heymanns Verlag 2000.

Vieweg 2001
Vieweg, K.: „Sicherheitsgesetzbuch als Instrument zur Straffung des Technikrechts?" In: TÜV Saarland-Stiftung (Hrsg.): *Congress Documentation of the World Congress Safety of Modern Technical Systems*, Köln: TÜV-Verlag 2001, S. 473–478.

Vieweg 2006
Vieweg, K. (Hrsg.): *Risiko – Recht – Verantwortung*, Köln, Berlin, Bonn, München: Carl Heymanns Verlag 2006.

Vieweg 2010
Vieweg, K.: „Thesen zum Problemfeld technische Sicherheit aus juristischer Sicht". In: Winzer, P./Schnieder, E./Bach, F.-W. (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven* (acatech DISKUTIERT), Berlin, Heidelberg: Springer-Verlag 2010, S. 117–129.

7.2 Datenschutz- und IT-sicherheitsrechtliche Risikomodelle

PD Dr. iur. Oliver Raabe
Forschungszentrum Informatik und Institut für Informations- und Wirtschaftsrecht
Karlsruher Institut für Technologie

1 Hintergrund

Das Datenschutz- und das IT-Sicherheitsrecht in komplexen IKT-Infrastrukturen sehen sich schon seit geraumer Zeit einer Reihe von Herausforderungen ausgesetzt, deren rationale und widerspruchsfreie Lösung von der abstrahierenden Sicht einer „Systemtheorie Sicherheit" profitieren könnte. Dies gilt beim Einsatz konvergenter Technologie insbesondere auch im Hinblick auf die notwendige europäische Harmonisierung von Begriffen und Methoden von IT-Sicherheit und Datenschutz.[1] Das technisch-organisatorische Schutzregime für komplexe IKT-Infrastrukturen ist historisch durch ordnungsrechtliche Detailregelungen von angemessenen Schutzmaßnahmen zur Erreichung der jeweiligen Schutzziele angelegt. Dieser Ansatz gerät aber wegen der systemimmanenten Prognosedefizite des Gesetzgebers zu den Sachgrundlagen dieser Systeme an seine Grenzen. Infolge dieser Defizite werden in bereichsspezifischen Gesetzen zunehmend Bewertungs- und Schutzprogramme zur Identifikation von Risiken und zur Auswahl von konkreten Schutzmaßnahmen implementiert, welche die Risikoprognose und -bewältigung weitgehend an die Rechtsunterworfenen delegieren. Vor diesem Hintergrund sollen im Folgenden das rechtliche Rollenmodell sowie der Risikobegriff der europäischen Datenschutzgrundverordnung (DSGVO) untersucht werden. Als Maßstab dient die abstrahierende Sicht der in diesem Band eingeführten entscheidungstheoretischen Modellierung des Risikobegriffs.

2 Risiko in der DSGVO

Mit der ab Mai 2018 unmittelbar in den Mitgliedstaaten der EU geltenden Datenschutzgrundverordnung (DSGVO) werden in einem gestuften Schutzkonzept organisations- und technikrechtliche Datenschutzmaßnahmen auf Basis einer vorgängigen Risikobewertung in den Mittelpunkt des technischen Datenschutzrechts gestellt. Dies wird in der Literatur schon als Verlagerung vom strengen Verbotsprinzip des klassischen Datenschutzrechts zu einem risikobasierten Ansatz verstanden.[2] Zudem findet sich in der Datenschutzgrundverordnung zum Beispiel in den Artikeln 24, 25, 32, 34 und 35 DSGVO nunmehr ein Risikobegriff, der aus oberflächlicher Sicht mit der hier eingeführten Modellierung eines quantitativen Bewertungsmaßstabes korrelieren könnte.

2.1 Normativer Rahmen und konkrete Fragen

Normativer Rahmen

Normativ soll die folgende Untersuchung auf die Regelung des Artikels 25 Absatz 1 DSGVO zum Datenschutz durch Technikgestaltung beschränkt werden.[3]

Frage 1 – das Rollenmodell der DSGVO

Die erste Frage betrifft zunächst das Rollenmodell der DSGVO. Grundrechtlich und regulierungstheoretisch motiviert stellt sich hier die Frage nach der Legitimität einer Zuständigkeitszuweisung für die Risikobewertung vom grundsätzlich zur Sicherung der informationellen Selbstbestimmung berufenen staatlichen Souverän auf private Akteure. Daneben kumuliert im Modell der DSGVO aus der Perspektive und in der Begrifflichkeit des quantitativen Risikomodells in der Rolle des „Schützers" als des gesetzlich „Verantwortlichen" auch gleichzeitig die Rolle des „Gefährders", was zu einem Wertungswiderspruch hinsichtlich der Rationalität der Risikobewertung durch den „Verantwortlichen" führen könnte.

Frage 2 – die Methode der Risikobewertung

Die zweite Frage betrifft die normative Stellung der DSGVO zur Methode der Risikobewertung. Im Hinblick auf das theoretische Risikomodell ist dies insbesondere die Stellung der DSGVO zu einem quantitativen Risikobegriff auf Kostenbasis. Dieser für das spieltheoretische Fundament der Theorie maßgebliche Faktor ist

1 | Vgl. Schallbruch 2016.
2 | Vgl. Veil 2015, S. 347.
3 | Der hier relevante Normwortlaut bestimmt: „(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche [...] geeignete technische und organisatorische Maßnahmen [...], die dafür ausgelegt sind, [...] die Rechte der betroffenen Personen zu schützen."

der gegenwärtigen Praxis von Modellen der Informationssicherheit und des technischen Datenschutzes fremd. Der Umstand, dass als Schutzgut konkretisierend „Rechte und Freiheiten natürlicher Personen" benannt sind, streitet zudem intuitiv nicht für die Verwendung von Metriken als Basis für die Risikobewertung der DSGVO.

Beide Fragenkomplexe sind insoweit miteinander verknüpft, als durch die grundrechtliche und regulierungstheoretische Begründung des Rollenmodells gleichzeitig auch die Legitimität eines eigenständigen Risikobegriffs der DSGVO, in Abgrenzung zum Begriffsgehalt in der klassischen staatlichen Risikoverwaltung, vorgezeichnet wird.

3 Das Rollenmodell der DSGVO

3.1 Legitimität der Zuständigkeitsverlagerung auf Private

Die Intuition des hier mit der spieltheoretisch motivierten Theorie eines quantitativen Risikobegriffs auf Basis der Bayes-Wahrscheinlichkeit eingeführten Rollenmodells von „Schutzbedürftigen" und „Schützern" einerseits und dem „Gefährder" andererseits kollidiert vermeintlich mit dem gesetzlichen Modell, als der „Verantwortliche" hier in einem Agenten sowohl die Rolle des „Gefährders" wie auch des „Schützers" einnehmen soll. Daneben stellt sich grundrechtlich und regulierungstheoretisch motiviert die Frage nach der grundsätzlichen Legitimität einer Risikobewertung durch Private. Insofern soll zunächst die grundrechtsdogmatische und regulierungstheoretische Legitimität des gesetzlichen Rollenmodells, die sich aus den durch Aufgabenverlagerung ergebenden Maßstäben von verwaltungsverfahrensrechtlichen Regelungen zur Risikobewertung durch Private ergibt, und schließlich die Frage nach dem vermeintlichen Wertungswiderspruch im Rahmen der Beurteilung nach dem quantitativen Risikomodell geklärt werden.

3.2 Input-Legitimation (Legalität) des gesetzlichen Rollenmodells

Das Rollenmodell in Subordinationsverhältnissen

Im klassischen, ordnungsrechtlich ausgestalteten Ansatz des Datenschutzrechts waren im Sinne der Legalität als Wahrung rechtsstaatlicher Grundsätze[4] die Bewertung und Prognose von Risiken für die informationelle Selbstbestimmung der Betroffenen und die Bestimmung verhältnismäßiger technisch-organisatorischer Schutzmaßnahmen weitgehend dem Gesetzgeber selbst oder delegierter behördlicher Zuständigkeit vorbehalten. Dieser Maßstab zeigt sich auch heute im sicherheitskritischen IKT-Recht, zuletzt bei den gesetzlichen Aktivitäten zur Einführung von SmartMetern. Auf Basis eines im Messstellenbetriebsgesetz (MsbG) von der Legislative vorstrukturierten materiellen Schutzkonzepts ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der konkretisierenden Bewertung und Entwicklung von Schutzprofilen und technischen Richtlinien für SmartMeter sowie im Rahmen kooperativer Verfahren mit der Bestimmung konkreter technisch-organisatorischer Maßnahmen für den Sachbereich betraut. Aus der Perspektive der rechtsstaatlichen Grundsätze entspricht das dem klassischen Konzept staatlicher Aufgabenzuweisung an Behörden bei grundrechtsrelevanten Sachgestaltungen.

Vor dem Hintergrund der Möglichkeit rein privater BigData-Analysen durch „*Verantwortliche*" oder Dritte und einer zunehmenden Durchdringung von Alltagsgegenständen mit datenschutzrelevanter Sensorik besteht aber im Hinblick auf die grundrechtlich geschützte informationelle Selbstbestimmung der Betroffenen kaum ein geringerer grundrechtlicher Schutzbedarf in rein privat ausgestalteten Konstellationen. Gleichwohl delegiert die für diese Sachverhalte anwendbare DSGVO die Ermittlung und Bewertung des Risikos und die Konkretisierung der angemessenen Schutzmaßnahmen grundsätzlich auf die Rolle des privaten „Gefährders" als „Verantwortlicher". Diese Sicht wirft nachvollziehbar die Frage nach der Legitimität der unterschiedlichen Aufgabenzuweisungen in Subordinationsverhältnissen und bei privater Gleichordnung auf. Die unterschiedliche Wertung ließe sich allerdings grundsätzlich dadurch grundrechtsdogmatisch begründen, dass zwischen einer gefahrerhöhenden staatlich gesetzten Pflicht zur Duldung von IKT-Artefakten in den betroffenen Haushalten des SmartMetering und den durch private Akteure gesetzten Risiken von Verarbeitungsaktivitäten aus Legitimitätserwägungen der jeweiligen Steuerungsprogramme unterschiedlich zu gewichten sein könnte.

Das Rollenmodell bei privater Gleichordnung

Für Fallgruppen der privaten Gleichordnung kann grundsätzlich aus der Perspektive der Legalitätserfordernisse der Input-Legitimation[5] ein angemessener Einfluss staatlicher, demokratisch vermittelter Legalität verbleiben, wenn das Schutzprogramm aus grundlegend materiellen Schutzprinzipien und verfahrensrechtlichen Begleitumständen nach wie vor durch den Gesetzgeber

4 | Siehe zu den Grundsätzen: Klafki 2017, S. 69.
5 | Vgl. zum Begriff Wiesner et al. 2006, S. 172 ff.

selbst ausgestaltet ist. Jedoch dürfen aus grundrechtlicher Sicht diese Verfahrensnormen nicht zur Disposition durch den „Verantwortlichen" stehen. Unter der Geltung der DSGVO muss der These einer Abkehr vom Verbotsprinzip zu einem risikobasierten Ansatz[6] insofern grundsätzlich widersprochen werden, als das materielle Schutzprogramm der DSGVO und grundsätzliche Verfahrensnormen nach wie vor vom staatlichen Souverän selbst gestaltet werden. Von einem risikobasierten Ansatz im obigen Sinne wäre nur zu sprechen, wenn die Anwendbarkeit der DSGVO selbst und in der Folge das auch weiterhin geltende materielle Verbotsprinzip von einer Schwelle risikobedingter Eingriffsintensität abhinge. Zu diesem sicher diskussionswürdigen Ansatz ist aber nichts ersichtlich, da die Anwendbarkeit allein vom Personenbezug – ohne Berücksichtigung des relevanten Informationsgehaltes von Daten – abhängt. Vielmehr geht es mit der Inkorporation eines Risikobegriffs lediglich um einen Wandel der gesetzlich und behördlich vorstrukturierten Methoden und Maßstäbe für den technisch-organisatorischen Datenschutz, wie er zum Beispiel auch in Paragraf 3a und der Anlage zu Paragraf 9 Absatz 1 BDSG schon grundsätzlich im bislang geltenden Datenschutzrecht angelegt war. Insofern ist der Maßstab der Beurteilung der Legitimität des Rollenmodells der DSGVO in Fallgruppen des Gleichordnungsverhältnisses der Bürgerinnen und Bürger zueinander grundrechtlich und regulierungstheoretisch im Wesentlichen nicht durch die Input-Legitimation (Legalität) des gesetzlichen Modells, sondern als Verfahrenselement primär durch Aspekte der Output-Legitimation (Effizienz und Wirksamkeit) der Verantwortlichkeitszuweisung bestimmt – auch wenn beide Prinzipien von Legitimität staatlichen Handelns in einem wechselseitigen Abhängigkeitsverhältnis stehen.

3.3 Output-Legitimation (Effizienz und Wirksamkeit)

Bei der Bewertung der Output-Legitimität des Rollenmodells zur Risikobewertung in Artikel 25 DSGVO stellen sowohl die Effizienz wie auch die Wirksamkeit des Steuerungsprogramms den Maßstab der Bewertung dar.[7] In Fällen der Entscheidung technisch-organisatorischer Schutzmechanismen steht in Bezug auf diese Faktoren, aufgrund des Wandels der Komplexität von relevanten Sachgestaltungen, die weitgehende Formulierung von technischen Detailvorgaben unmittelbar durch den Staat aber infrage. Insofern gilt, dass staatliche Normen „im Großen und Ganzen auch eine Chance der Anwendung und Durchsetzung haben müssen"[8], um wirksam zu sein. Wirksames Recht verwirklicht sich insofern nur als Ausdruck staatlicher Macht, wenn die Rechtsnormen auch effektiv mit Anwendungs- und Durchsetzungschancen verbunden sind.[9] Dies könnte für technikrechtliche Detailvorgaben im Datenschutzrecht fraglich sein.

Fehlende Effizienz und Wirksamkeit des klassischen Rollenmodells

Im Hinblick auf die mangelnde Anwendung und Durchsetzung des Datenschutzrechts bei privaten Normadressaten ist ein Versagen und mithin ein Mangel an Output-legitimierender Wirksamkeit eines rein ordnungsrechtlich ausgestalteten Datenschutzrechts grundsätzlich zu konstatieren.[10] So wurde in der Literaturdiskussion um den Nachweis eines ordnungsrechtlichen Versagens des Datenschutzrechts[11] angemerkt, dass dem Ordnungsrecht insbesondere die zur Steuerung in komplexen Systemen erforderlichen entscheidungsrelevanten Informationen regelmäßig fehlten, diese vielmehr gerade im zu steuernden Subsystem vorhanden seien.[12] Deshalb sollte sich nach Teilen der Literatur in Konzepten regulierter Selbstregulierung der Staat darauf beschränken, ein Regelungsumfeld zu schaffen, das eine Selbstregulierung ermöglicht, und nur im Falle eines Versagens der Marktsteuerung im Rahmen einer Auffangverantwortung eingreifen.[13] Damit müsste sich nach diesem Regulierungskonzept, wie nun auch in der Konzeption der Risikoregulierung der DSGVO teilweise angelegt, der Staat von einer eigenen Erfüllungsverantwortung lösen und lediglich eine rahmensetzende Gewährleistungsverantwortung übernehmen, indem der traditionelle Datenschutz die Funktion eines Sicherheitsnetzes einnimmt.[14]

Wissensdefizite in staatlichen Steuerungsprogrammen

Damit stünde – im Ansehen dieser modernen Konzeption – das beim jeweils handelnden Akteur vorhandene für eine Risikoentscheidung notwendige Wissen im Mittelpunkt der Effektivitätsüberlegung zu einem optimalen Steuerungsprogramm. Im Hinblick auf die hier thematisierten neuartigen Entwicklungen in der Informationsgesellschaft wird in der Literatur zunächst abstrakt konstatiert, dass die Verwaltung hinsichtlich der

6 | Vgl. Veil 2015, S. 347.
7 | Vgl. zum Begriff Wiesner et al. 2006, S. 172 ff.
8 | Vgl. Zippelius 2006, S. 20.
9 | Vgl. Zippelius 2006, S. 21.
10 | Vgl. zum Meinungsstand: Friedewald et al. 2010, S. 113 ff.
11 | Vgl. Vesting 2001, S. 21 ff., Ladeur 2000, S. 16 ff.
12 | Vgl. Grimm 2001, S. 17.
13 | Vgl. Hoffmann-Riem et al. 2000, S. 50.
14 | Vgl. Hoffmann-Riem 2005, S. 537.

verschiedenen entscheidungsrelevanten Wissensaspekte schon zunehmend qualitativ und quantitativ an ihre Grenzen stoße.[15] Allein dieser Umstand würde auf eine Verminderung der Effizienz wissensbasierter staatlicher Einzelentscheidungen in diesem Bereich hindeuten. Der Effektivitätsgedanke der Aufgabenerfüllung könnte deshalb, abstrakt betrachtet, grundsätzlich für eine Zuweisung der Risikobewertung an Private sprechen. Ob dies auch im konkreten Fall des Bewertungs- und Entscheidungsprogramms nach Artikel 25 DSGVO zutrifft und sich deshalb das Rollenmodell der DSGVO als effektiver als eine klassische Risikobewertung durch Aufsichtsbehörden erweisen würde, muss deshalb im nächsten Schritt im Hinblick auf die verschiedenen relevanten Wissenstatbestände zur Risikobewertung und zur Auswahlentscheidung von Schutzmaßnahmen untersucht werden. Eine pauschale Beurteilung ist allerdings nicht möglich, da sich die für eine Risikoentscheidung notwendigen Informationen in vielgestaltigen Kategorien zeigen.

Grundsätzlich ist in einem wissensbasierten Entscheidungsprogramm zwischen Sach-, Erfahrungs- und Regelwissen des Entscheiders zu differenzieren. In der klassischen Verwaltung wird das zunächst notwendige Sachwissen auch schon in klassischen ordnungsrechtlichen Verfahren naturgemäß für die Behörden als instabil angesehen.[16] Dies verhält sich im Fall der datenschutzrechtlichen Risikoentscheidung erwartungsgemäß ebenso. Gerade im Bereich der Regulierung komplexer Technologien und der Dynamisierung von Rechtsgebieten wird nun aber auch ein Mangel bezüglich der stabilen Verfügbarkeit der zweiten notwendigen Wissenskategorie, dem Erfahrungswissen bei Prognoseentscheidungen unter Unsicherheit, zunehmend auch beim staatlichen Entscheider angenommen.[17] Und schließlich steht auch die dritte für Entscheidungen im prognostischen Bereich relevante Wissenskategorie, das klassischerweise stabile Regelwissen staatlicher Akteure, zunehmend zur Disposition. Dies zeigte sich nicht zuletzt am Beispiel der durch Mängel im notwendigen Regelwissen aus verschiedenen rechtlichen Fachdomänen induzierten technischen Inkompatibilität bei der erforderlichen konvergenten Regulierung von Kommunikationsprotokollen des SmartGrid.[18] Denn häufig sind in solchen neuartigen Anwendungsfeldern überlagernde Regelungskomplexe zu berücksichtigen, die die notwendige Breite des entscheidungsrelevanten Regelwissens wegen der in der klassischen Ausgestaltung der Verwaltung regelmäßig nicht mehrdimensional ausgerichteten domänenspezifisch behördlichen Kompetenzen übersteigen. Insofern kann die theoretische Grundannahme zur geringeren Effizienz staatlicher Entscheidung wegen allfälliger Wissensdefizite in diesem Bereich jedenfalls grundsätzlich als begründet angesehen werden. Ebenso sind auch die Leistungsgrenzen staatlicher Aufsicht bei den großen Fallzahlen von Risikoentscheidungen nach Artikel 25 DSGVO offensichtlich.

Anforderungen an Alternativprogramme

Die insofern behauptete grundsätzliche Instabilität des für Entscheidungen relevanten Wissens staatlicher Entscheidungsträger sagt allerdings über bessere Effektivität von konkreten Alternativprogrammen noch nichts aus. Einigen Stimmen in der Literatur zufolge soll der Staat in der Folge eines Fehlens von überlegenem Wissen in IKT-Sachverhalten die Rolle des souveränen Entscheiders verlieren, da die notwendigen Entscheidungen zukünftig problembezogen und netzwerkabhängig seien.[19] Vielmehr soll aus dem Netzwerkcharakter eine Ordnung von verteilten Entscheidungsrechten folgen, die sowohl auf Flexibilität als auch auf Lernfähigkeit ausgelegt sein müsse. Denn auch weiterhin seien normative Erwartungen zu sichern und gleichzeitig auch Veränderungen zu ermöglichen.[20] Dieser Perspektive könnte für die Erfüllung ehemals staatlicher Schutzaufgaben dann abstrakt zu folgen sein, wenn eine hinreichende Kompensation für die Machtverluste des Staates beziehungsweise die Schwächung der Input-Legitimität bei einer derartigen Aufgabenverlagerung gewährleistet würde. Denn es ist zu berücksichtigen, dass die rechtliche Regelung von gesellschaftlichen Zuständen zugleich einen Machttatbestand schafft, der durch ebendiese Regeln wiederum stabilisiert wird.[21] Soll diese grundsätzliche Ordnung durch eine Verlagerung im Gleichgewicht von In- und Output-Legitimation nicht infrage gestellt werden, bedarf es der Kompensation eines sonst destabilisierend wirkenden staatlichen Machtverlustes der bei der Verhaltenssteuerung Rechtsunterworfenen. Im Hinblick auf die damit gebotene Kompensation muss die Begründung einer Verlagerung insofern in einer auch im konkreten Fall gesteigerten Effektivität liegen. Bei der Frage nach der Zuständigkeit für Risikobeurteilungen muss also die konkret vorhandene bessere Lernfähigkeit der „Verantwortlichen" für den relevanten Weltausschnitt der DSGVO nachgewiesen werden.

15 | Vgl. Herzmann 2010, S. 35.
16 | Vgl. Röhl 2012, S. 748 ff.
17 | Vgl. Wollenschläger 2009, S. 31.
18 | Vgl. Raabe et al. 2011, S. 16 ff.
19 | Vgl. Ladeur 2000, S. 64.
20 | Vgl. Vesting 2001, S. 23.
21 | Vgl. Zippelius 2006, S. 21.

Zudem muss hernach aus grundrechtlicher Sicht untersucht werden, ob das Entscheidungsverfahren selbst durch den Staat verfahrensrechtlich hinreichend bestimmt und normklar ausgestaltet ist. In diesem Rahmen ist der Maßstab, ob durch die staatliche Verfahrensregelung sichergestellt wird, dass sowohl der praktische Prozess wie auch die Methode der Wissensgenerierung für die Risikobewertung dem Schutzgut angemessen ist.

Wissen im Konditionalprogramm der DSGVO

Ordnet man zunächst im Entscheidungsprogramm von staatlichen beziehungsweise privat generierbaren Wissensbeständen die einzelnen für eine konkrete Entscheidung über Risiken und Kosten-Nutzen-Erwägungen notwendigen Wissenskategorien im Rahmen des Artikels 25 DSGVO den jeweils relevanten Akteuren zu, ergibt sich das folgende Bild:

Auf der Ebene des Sachwissens besteht beim staatlichen Akteur kein originäres Wissen zur „Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung". Dieses Wissen liegt innerhalb der beherrschbaren Systemgrenzen unmittelbar und überlegen beim privaten „verantwortlichen" Systemgestalter vor – nicht jedoch zwangsläufig hinsichtlich der kontextübergreifenden Drittverwendung von Daten.

Auf der Ebene des „Erfahrungswissens" um Eintrittswahrscheinlichkeiten und Folgenschwere von möglichen Schäden bei den Betroffenen ist für die konkrete Sachgestaltung bei privaten Akteuren eine bessere Kenntnis domänenspezifischer Risiken zu erwarten. Die Ungewissheitsaspekte bezüglich möglicher Schäden der Schutzbedürftigen können sie daher im Vergleich zu staatlichen Akteuren sachgerechter selbst oder auch in typischen Verbandskonstellationen beurteilen. Für die Beurteilung allgemeiner Risiken bei der Datenverarbeitung dürfte hingegen die staatliche Aufsicht über besseres Erfahrungswissen verfügen.

Auf der Ebene des notwendigen „Regelwissens" könnte hingegen im Hinblick auf eine effektive Rollenzuweisung eine deutliche Überlegenheit aufsichtsbehördlicher Kompetenzen angelegt sein. Sowohl bei der notwendigen Interpretation der unbestimmten Rechtsbegriffe als auch hinsichtlich der Methoden der Risikobewertung wäre die Delegation auf staatliche Aufsichtsbehörden wegen deren spezifischer Regelexpertise grundsätzlich sachgerechter. Auf der anderen Seite ist im Hinblick auf Kapazitätsüberlegungen ja gerade zweifelhaft, ob die Vielzahl von Bewertungen nach Artikel 25 DSGVO von den Aufsichtsbehörden selbst geleistet werden könnten. Aus grundrechtlicher Perspektive könnte aber nach den oben erarbeiteten Kompensationskriterien die mangelnde Normklarheit/Bestimmtheit des Artikels 25 DSGVO derzeit gegen eine legitime Verlagerung der Aufgabe der Norminterpretation auf die Verantwortlichen sprechen. So liegen im derzeit bestehenden rechtlichen Rahmen keine hinreichenden Interpretationen zum Verständnis des Schutzgutes und von potenziellen Schadereignissen, den „Rechten und Freiheiten natürlicher Personen" in Artikel 25 DSGVO, vor. Zudem werden gegenwärtig weder die grundlegende Methodik der Bewertung des Risikos noch die Maßstäbe der Ermittlung der Wahrscheinlichkeit eines Schadeintritts, mithin der Risikobegriff der DSGVO, im Gesetz selbst oder abgeleitet durch behördliche Interpretationshilfen hinreichend normklar und bestimmt dargelegt; Gleiches trifft derzeit auch auf die Methodik der Wahl von „geeigneten" Schutzmaßnahmen zu. Insofern bleibt abzuwarten, ob sich beispielsweise im Rahmen von zukünftigen Zertifizierungsverfahren nach Artikel 40 DSGVO, die nach Artikel 25 Absatz 3 DSGVO grundsätzlich zum Nachweis der Erfüllung der Verpflichtungen herangezogen werden können, maßstabsbildende normklare und hinreichend bestimmte Konkretisierungen ergeben. Unter der Bedingung einer zukünftig hinreichenden Verfahrenssicherung ist aus der Perspektive der Output-Legitimation, in der Gesamtschau des bei den Akteuren notwendigen Entscheidungswissens, gleichwohl ein hinreichend effektives Steuerungsprogramm auch bei privater Ausführung durch „Verantwortliche" motiviert, welches geeignet ist, die Nachteile begrenzter staatlicher Kapazität zur Risikobeurteilung und Maßnahmenauswahl im Rahmen des Artikels 25 DSGVO zu kompensieren.

Wertungswiderspruch im Risikomodell

Es verbleibt mithin aus der Perspektive des theoretischen Risikomodells und des grundsätzlichen Schutzkonzepts staatlicher Auffangverantwortung bei einer Anomalie: Selbst in Konstellationen der Selbstgefährdung, in der ein „Schutzbedürftiger" gleichzeitig auch sein eigener „Gefährder" ist, tritt der Staat grundsätzlich als „Schützer" auf. Es ist also jedenfalls im grundrechtsrelevanten Bereich keine Situation gegeben, in der alle Rollen allein in einer Person (Agent) kumulieren. Insofern erscheint es als Wertungswiderspruch, dass ein Agent in der Rolle des „Schützers" als „Verantwortlicher", der im Rahmen der Risikobewertung auch die Rollensicht des schutzbedürftigen „Betroffenen" einzunehmen hat, gleichzeitig noch die Rolle des „Gefährders" innehat. Diesem Widerspruch kann aber im Rahmen von Erwägungen aus der regulierungstheoretischen Diskussion Abhilfe geschaffen werden. Denn im Hinblick auf die Wirksamkeitsaspekte der Output-Legitimation ist grundlegend anerkannt, dass die Normumsetzung, zu der der „verantwortliche" Agent in seiner Rolle als „Schützer" berufen ist, regelmäßig nicht um ihrer selbst willen

erfolgt. Vielmehr werden Normen zumeist zur Vermeidung der Kosten bei ihrer Missachtung befolgt.[22] Eben hier trifft die Kostenfunktion des „Gefährders" auf die abstrakte Modellierung mit der normativen Wirklichkeit der DSGVO.

Im quantitativen Risikomodell auf Basis der Bayes-Wahrscheinlichkeit können den „Gefährdern" durch die jeweiligen Vorfälle Kosten entstehen, die einer Strafe für die Verursachung des Vorfalls entsprechen.[23] In Verbindung mit der Risikobeurteilung durch den „Schützer" ist die Höhe dieser Kosten wiederum mit einer geringeren Eintrittswahrscheinlichkeit eines Vorfalls/Angriffs korreliert. Beim Zusammenfallen von „Schützer" und „Gefährder" in einem Agenten können nunmehr neben den Strafen für dessen Schadverursachung in der Rolle des „Gefährders" auch die Kosten für die Nichtbefolgung des normativen Appels in der kumulativ im Agenten verwirklichten Rolle des „s" eingestellt werden. Damit wird das Budget des die Rollen vereinigenden Agenten aus einem direkten Saldo beider Kostenpositionen generiert. Insofern hinge die Effektivität des verfahrensrechtlichen und materiellen Begleitprogramms zur Sicherung einer künstlichen Rollentrennung in einem budgetbezogenen, rational handelnden „*Verantwortlichen*" von der Aufdeckungswahrscheinlichkeit eines Regelverstoßes bei der Risikobeurteilung beziehungsweise Maßnahmenauswahl und den insofern einzustellenden Strafmaßen ab. Mit der Rechenschaftspflicht des Artikels 5 Absatz 2 DSGVO, den Meldepflichten nach Artikel 33 Absatz 2 DSGVO, der Pflicht zur Dokumentation nach Artikel 30 DSGVO, der Pflicht zur Konsultation nach Artikel 36 DSGVO, den Überwachungspflichten der Aufsichtsbehörden nach Artikel 57 Absatz 1 a DSGVO und den unbedingten Beschwerderechten von Betroffenen bei einer Aufsichtsbehörde nach Artikel 77 DSGVO ist im Vergleich zum deutschen BDSG zunächst ein deutlich höheres Entdeckungsrisiko für Verstöße gegen zwingende Vorschriften der DSGVO zu erwarten. Entscheidend ist aber, dass die Geldbußen nach Artikel 83 Absatz 4 DSGVO bei Verstößen gegen die Pflichten der Verantwortlichen gemäß Artikel 25 DSGVO bis zu 10.000.000 Euro oder im Fall eines Unternehmens bis zu 2 Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen. Dies sollte im Hinblick auf das Entdeckungsrisiko und die Strafhöhe im Vergleich zum BDSG durchaus auch zur praktischen Berücksichtigung beider Aspekte bei einem in Bezug auf sein Gesamtbudget rational handelnden „Verantwortlichen" führen und sich der Wertungswiderspruch insoweit auflösen lassen.

4 Die Risikobewertung des Artikels 25 DSGVO

4.1 Einleitung

Der zweite Fragenkomplex bezieht sich auf die von Artikel 25 DSGVO intendierte Methode der Risikobewertung, da die Norm selbst keine ausdrückliche Aussage hierzu trifft.

Grundsätzlich wird im Folgenden das Risiko als Produkt aus Eintrittswahrscheinlichkeit eines Schadereignisses und Folgenschwere verstanden. Herausforderungen bestehen insoweit im Rahmen der DSGVO bei der Wahl der Methode zur Ermittlung der schutzgutabhängigen Eintrittshäufigkeit möglicher Schäden und der Bestimmung des Ausmaßes dieser Schäden. Im Optionenraum der Methodenwahl könnten grundsätzlich quantitative, semi-quantitative und qualitative Bewertungsmuster in Betracht kommen. Darüber hinaus ist zudem auch im Rahmen eines nach dem hier vertretenen Verständnis gestuft entkoppelten Verfahrens von Risikobewertung und Risikomanagement die gleichwohl notwendige Methodik zur Beschreibung und Prüfung von koppelnden Effekten zwischen der Risikobeurteilung des „Schutzbedürftigen"/„Schützers" und der Angriffsmotivation des „Gefährders" bei der Wahl und dem Einsatz von Schutzmaßnahmen relevant. Nach dem gestuften Programm von „geeigneten" Schutzmaßnahmen des Artikels 25 DSGVO im Rahmen der Auswahl von Schutzmaßnahmen stellt das Risiko einer Schutzgutverletzung nur einen zu berücksichtigenden Belang neben den Verarbeitungszwecken und den Investitionskosten dar.

Im Rahmen eines eingeschränkten Optionenraums[24] zwischen derzeit praxisrelevanten semi-quantitativen Methoden der Risikobewertung und den in diesem Band eingeführten Methoden qualitativer Risikobewertung auf Basis von Bayes-Wahrscheinlichkeiten soll die Bewertung einerseits anhand der vorhergehenden regulierungstheoretischen Erwägungen mit Blick auf die Output-Legitimation der gewählten Methode erfolgen. Dies bedeutet, dass die maßgeblich effektivitätsbestimmenden Faktoren eines optimalen Lernprozesses und die Praktikabilität der Methode beurteilt werden. Andererseits wird, wegen der Frage nach der Fähigkeit zur allgemeinen Maßstabsbildung, auch für den Risikobegriff der DSGVO als Nebenziel die Falsifikation des in diesem Band eingeführten quantitativen Risikomodells verfolgt.

22 | Vgl. Grimm 2001, S. 17.
23 | Vgl. Beyerer/Geisler 2018.
24 | Wegen des rein risikoidentifizierenden Charakters von quantitativen Methoden sollen diese hier für die Betrachtung schon ausgeschlossen werden.

Zunächst ist gleichwohl aus grundsätzlicher Perspektive zu klären, ob ein quantitatives Risikomodell auf Kostenbasis nicht grundsätzlich eine unzulässige Bepreisung der unabdingbaren Menschenwürde aus Artikel 1 Absatz 1 GG enthält. Diese Grundrechtsdimension von kostenbasierten Risikomodellen drängt sich wegen der grundrechtlich geschützten informationellen Selbstbestimmung der Betroffenen, die aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG gebildet wird, hier auf. Sodann soll ebenfalls anhand von grundsätzlichen Erwägungen der juristischen Literatur zu quantitativen Risikomodellen untersucht werden, ob es schon eine einheitliche Risikodefinition im Recht gibt, die auch als Maßstab für die Bewertungsmethode im Rahmen des Artikels 25 DSGVO herangezogen werden könnte. Schließlich sollen in einem konkretisierenden Schritt, mit besonderem Blick auf die Falsifikation der theoretischen Modellierung des quantitativen Risikobegriffs und die regulierungstheoretisch motivierten Faktoren, quantitative und semi-quantitative Methoden der Risikobewertung im Rahmen des Artikels 25 DSGVO vergleichend bewertet werden. Diese Bewertung beruht im Hinblick auf die optimale Output-Legitimation des Bewertungsverfahrens und aus Gründen der Effektivität im Wesentlichen auf der Beurteilung der Integrationsfähigkeit der konkreten Methodik in das Risikomanagement des Artikels 25 DSGVO. Die Gewähr von schutzgutangemessener Lernfähigkeit des Verfahrens und die Praktikabilität der Methode sind dabei ebenfalls zu berücksichtigen.

4.2 Grundrechtsrelevanz eines quantitativen Risikomodells

Gegen die Verwendung von ökonomischen Zahlenwerten, mithin die Beschreibung von Risiken in Kostenfunktionen, könnte im Rahmen des Datenschutzrechts schon ganz grundsätzlich sprechen, dass im bisherigen Konzept der informationellen Selbstbestimmung aus Artikel 2. Absatz 1 in Verbindung mit der Menschenwürde aus Artikel 1 Absatz 1 GG ein Element enthalten ist, das nicht bepreisbar und mithin auch nicht auf Basis von Kostenerwägungen einschränkbar sein könnte. Jedoch können auch grundsätzlich nicht einschränkbare Grundrechte – jedenfalls bei Kollisionslagen mit anderen Grundrechten – im Wege der „praktischen Konkordanz" in verhältnismäßigen Ausgleich gebracht werden. Daneben gilt, dass regelmäßig bei strafenden Unwerturteilen von Schutzgutverletzungen gestufte Strafmaße in geldwerten Faktoren dargestellt werden, ohne dass damit das Schutzgut als solches mit einem Preis versehen würde. Es stellt sich insofern vielmehr die Frage, ob es aus grundrechtlicher Sicht einen Unterschied macht, wenn die durch den Staat in einem materiellen Rahmen delegierte Verhältnismäßigkeitsabwägung und der Ausdruck in geldwerten Sanktionsmechanismen zum Ausgleich widerstreitender Interessenlagen auch in einer metrischen Kostensymbolik der Risikotheorie formuliert sein könnten – ob also auch hier nicht dem Element der Menschenwürde ein absoluter Preis zugewiesen wird, sondern lediglich eine Verhältnismäßigkeitserwägung und die Eingriffsintensität in Bezug auf das Schutzgut in metrischer Symbolik ausgedrückt werden. Die gesetzliche Wahl der Indikatoren für die Vulnerabilität als „Rechte und Freiheiten natürlicher Personen" und die in Erwägungsgrund 75 enthaltene Konkretisierung in physische, materielle oder immaterielle Schadmaße zeigen, dass hier eben gerade nicht die Menschenwürde der Betroffenen an und für sich in Kosten bewertet werden soll. Es setzt lediglich die Kostenfunktion bei der regelmäßig judikativ ermittelten Eingriffsschwere einer Schutzgutverletzung in Schadmaßen und ihren vertretenden geldwerten Symboliken an. Damit wird also nicht die Menschenwürde an und für sich absolut bepreist, sondern es erfolgt eine Transformation der in möglichen Strafurteilen zu Schutzgutverletzungen ausgedrückten schutzgutbezogenen Verhältnismäßigkeitserwägungen und auf die Eingriffsintensität bezogenen Unwerturteilen durch die Umrechnung in ein korrespondierendes geldwertes Preismaß. Insofern spricht nichts dagegen, die Bewertung der Folgenschwere eines Schadereignisses im Rahmen des Artikels 25 DSGVO quantitativ in der symbolischen Form einer Kostenfunktion auszudrücken.

4.3 Der rechtliche Risikobegriff

Ob es einen allgemeinen rechtlichen Risikobegriff geben kann, der auch in der DSGVO Geltung verlangt, ist zweifelhaft. Aus der oben regulierungstheoretisch und grundrechtlich begründeten Darlegung zur Legitimität einer Aufgabenverlagerung der Risikobeurteilung in Artikel 25 DSGVO vom ursprünglich zur Bewertung berufenen Staat auf private „Verantwortliche" folgt, dass auch der Risikobegriff der DSGVO nicht zwangsläufig den theoretischen Rahmenbedingungen des klassischen Risikoverwaltungsrechts, insbesondere hinsichtlich der Abgrenzung von Gefahr, Risiko und Restrisiko,[25] folgen muss. Vielmehr kann er sich grundsätzlich auch als Aliud mit eigenen Maßstäben gerieren. Dies ist insofern bedeutend, als in der rechtswissenschaftlichen Literatur regelmäßig zunächst das Risiko gegenüber der Gefahr abgegrenzt wird. In diesem Sinne sollen zukünftig mögliche Schadereignisse mit einer zwischen Risiko und Gefahr eingestuften Eintrittswahrscheinlichkeit und unterschiedlichen Schadmaßen abgewehrt werden. Mithin ist im Risikoverwaltungsrecht Risiko als Minus zur Gefahr zu sehen, wobei sich in beiden Fällen das Ergebnis als Produkt von Eintrittswahrscheinlichkeit und

25 | Vgl. Vieweg 2018.

Folgenschwere zeigt. Im Risikoverwaltungsrecht soll das Risiko gleichzeitig eine spezifische Eingriffsschwelle für staatliches Handeln markieren.[26]

4.4 Literaturkritik eines quantitativen Risikobegriffs

In der juristischen Literatur wird eine rechtliche Risikodefinition auf Basis des naturwissenschaftlichen Risikobegriffs, definiert als Produkt von Eintrittswahrscheinlichkeit und Folgenschwere einer nachteiligen Auswirkung, teilweise pauschal in Abrede gestellt. Dies wird im Hinblick auf das klassische Risikoverwaltungsrecht einerseits damit begründet, dass es bei rechtlichen Entscheidungssituationen auf die Eingriffsschwelle ankomme und die naturwissenschaftliche Definition hierfür keine Anhaltspunkte liefere, weshalb eine rechtliche Entscheidung über die Begrenzung eines Gefahrenpotenzials gerade ohne wissenschaftlich abgesicherte Prognosen zu treffen sei.[27] Fundamentaler setzt eine andere Stimme in der Literatur an, wenn die mathematische Berechenbarkeit des rechtlich relevanten Risikobegriffs in den hier relevanten Situationen von Unsicherheit grundsätzlich infrage gestellt wird. Da Eintrittswahrscheinlichkeit und Schadenshöhe in der Naturwissenschaft auf Grundlage empirischer Erfahrungen für die Zukunft prognostisch berechnet würden, es aber gerade bei neuartigen technischen Entwicklungen an diesen empirischen Erfahrungswerten mangle, seien insofern keine tragfähigen Prognosen über Eintrittswahrscheinlichkeit und Folgenschwere möglich.[28] In die Bewertung ist zunächst einzustellen, dass sich die vorgenannten Positionen offensichtlich auf eine spezifische Fallgestaltung des staatlichen Umgangs mit Risiko beziehen. Bei diesen Fallgestaltungen werden, unter der Bedingung geringer Empirie zu den Sachgrundlagen der Bewertung, von Menschen erstellte technische Artefakte oder Naturkatastrophen als Zufallsprodukte (Safety), die zu einem Schadereignis führen können, angesehen. Die Diskussion bewegt sich dann entlang der Frage, ob von einer Gefahr, einem Risiko oder einem Restrisiko gesprochen werden müsse und welche Schutzmaßnahmen jeweils angemessen seien. Diese Fallgestaltung liegt aber dem Risikobegriff der DSGVO gerade nicht zugrunde, als es sich hier um den Fall eines stochastischen intelligenten Angreifers handelt (Security), bei dem die schutzgutabhängige Eingriffswahrscheinlichkeit im Sinne einer Häufigkeitsverteilung von Schadvorfällen und die schutzgutabhängige Folgenschwere für Personen ermittelt werden müssen. Anders als bei Zufallsereignissen der Safety ist hier auch die geldwertnutzenorientierte Eingriffsmotivation des Angreifers zu berücksichtigen. Der Risikobegriff ist insofern umfassender, als er auch diese Wechselwirkung in gekoppelten Wahrscheinlichkeiten berücksichtigen muss.

Gemeinsamkeiten ergeben sich insofern, als beide Sachgestaltungen als Maßstäbe des Risikobegriffs die Bewertung der Eintrittswahrscheinlichkeit und die mögliche Folgenschwere beinhalten. Nicht geht es im Rahmen der DSGVO jedoch um die Ermittlung von relevanten Eingriffsschwellen im Vorfeld von Gefahren. Wegen dieser Unterschiede soll im Folgenden für den Risikobegriff der DSGVO einer Auffassung gefolgt werden, die das Risiko als Aliud zur ordnungsrechtlichen Gefahr begreift. Zentrales Wesensmerkmal dieses Risikobegriffs sei hiernach das „Wissen um die Ungewissheit der Wahrscheinlichkeit des Eintritts und der Folgenschwere".[29] Gleichwohl kann aus den vorgenannten Erwägungen zum Risiko bei staatlichen Entscheidungen unter Unsicherheit und geringer empirischer Basis zu Eintrittshäufigkeit und Folgenschwere eines Risikos etwas gewonnen werden: In beiden Fällen geht es darum, bei unvollständiger Information über eine zu untersuchende Einheit Aussagen über diese treffen zu können.[30] Betrachtet man zunächst die Frage nach der Ermittlung der Wahrscheinlichkeit einer Schutzgutverletzung, so ergeben sich bei der Anwendung der DSGVO durch Dritte gleichartige Probleme wie bei staatlichen Risikoentscheidungen. Das Bundesverfassungsgericht konkretisiert in Übereinstimmung mit einem technisch-naturwissenschaftlichen Verständnis, dass der Beurteilende „weitgehend auf Schlüsse aus Beobachtungen vergangener tatsächlicher Geschehnisse auf die relative Häufigkeit des Eintritts und den gleichartigen Verlauf gleichartiger Geschehnisse in der Zukunft angewiesen" sei.[31] Dies entspricht der klassischen frequentistischen Definition von Wahrscheinlichkeit, die schon grundsätzlich für die meisten Sicherheitsprobleme nicht anwendbar sein soll.[32] Gleiches dürfte auch für die begrenzte Prognosemöglichkeit konkreter Folgeschweren gelten.

Zwei Aspekte aus der vorgenannten Risikodebatte könnten nun aber für die grundsätzliche Untersuchung von Bayes-Wahrscheinlichkeiten im Rahmen der DSGVO streiten: Einerseits wird bei begrenzter empirischer Basis dem Bundesverfassungsgericht

26 | Vgl. Klafki 2017, S. 13.
27 | Vgl. Arndt 2012, S. 43.
28 | Vgl. Klafki 2017, S. 14.
29 | Vgl. Klafki 2017, S. 15.
30 | Vgl. Ziegler 2017, S. 5.
31 | Vgl. BVerfGE 49, 89, S. 142.
32 | Vgl. Merz 2006, S. 9.

(BVerfG) in der Literatur zugeschrieben, dass es sich immer nur um gegenwärtige, subjektive Wahrscheinlichkeitsannahmen handele und stets ein Rest an Ungewissheit verbleibe.[33] Auf der anderen Seite sieht das BVerfG, dass bei Fehlen einer hinreichenden Erfahrungsgrundlage sich der Beurteilende „auf Schlüsse aus simulierten Verläufen beschränken" müsse.[34] Die erste Annahme des BVerfG legt entgegen der pauschalen Beurteilung der vorgenannten Literaturstimme[35] nahe, dass Methoden, welche die Berücksichtigung von subjektiven Faktoren ermöglichen, grundsätzlich bei der Methodenwahl in einem rechtlichen Risikoverständnis erfasst sein sollen. Insofern fehlt der Literaturstimme in ihrer Pauschalität die Auseinandersetzung mit den Optionen von subjektiven oder Bayes-Wahrscheinlichkeiten. Denn die Alternative wäre nach dem klaren Beurteilungsauftrag der DSGVO eine vollkommen intransparente, rein subjektive Schätzung der das Risiko bestimmenden Faktoren durch den Verantwortlichen.

4.5 Konkretisierende Bewertung der Effektivität

Es ist mit der Literaturmeinung auch im Rahmen der DSGVO eine qualitative Bewertung allein auf Basis frequentistischer qualitativer Risikomodelle nicht möglich, da wegen mangelnder empirischer Grundlage diese Methoden ausscheiden.

Bei der Anwendung von semi-quantitativen Verfahren der Wahrscheinlichkeitsbewertung wäre vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts zur Subjektivität von Risikoentscheidungen kritisch anzumerken, dass die Identifikation und Bewertung weitgehend als Ausdruck des wenig rationalen subjektiven Glaubens der zur Beurteilung berufenen Stelle anzusehen ist. Zudem würde sich im Hinblick auf die Lernfähigkeit der Methode das Problem ergeben, wie die Berücksichtigung eines möglichen Zuwachses von Empirie bei den „Verantwortlichen" zu Eintrittswahrscheinlichkeiten von Schadereignissen verfahrensrechtlich und methodisch gesichert werden kann. Diese Frage stellte sich jedenfalls jenseits der Datenschutzfolgenabschätzungen des Artikels 35 DSGVO, welche mit Listen von Verarbeitungstätigkeiten „hoher Risiken" eine rudimentäre Lernfähigkeit im staatlichen Entscheidungsprogramm implementiert. Insofern ist zu hinterfragen, ob ein quantitatives Risikomodell auf Basis der Bayes-Wahrscheinlichkeit – jedenfalls in theoretischer Perspektive – nicht grundsätzlich vorzugswürdig erscheinen muss. In diesem Sinne wird in der Literatur die Bayes-Wahrscheinlichkeit als Vermittler zwischen frequentistischer und subjektiver Wahrscheinlichkeit eingeordnet,[36] welche die vorgenannten Nachteile der Integration von wachsender Empirie und unerkannter subjektiver Verzerrung des semi-quantitativen Modells gerade meidet. Im Hinblick auf die erstrebte Optimierung der Output-Legitimation der Methode kann es aber bei der theoretischen Vorzugswürdigkeit nicht bleiben, vielmehr muss sich das gewählte Modell im Rahmen von Artikel 25 DSGVO auch als mehrdimensional effektiv und passfähig erweisen.

Gewähr von Schutzgutangemessenheit und Lernfähigkeit

Die nächste Forderung an das gewählte Modell, die Schutzgutangemessenheit und Lernfähigkeit des Verfahrens im Rahmen von Artikel 25 DSGVO, speist sich aus der vorgenannten Überlegung, dass trotz und gerade wegen der Delegation von grundrechtsrelevanten Entscheidungsrechten an Private eine Kompensation des staatlichen Entscheidungsverzichts durch die Präferenz angemessener Lernverfahren und die Schutzgutangemessenheit sichergestellt werden muss.

Gerade für semi-quantitative Methoden wird nun explizit ins Feld geführt, dass es schwierig, aufwendig und zudem fehleranfällig sei, für Schäden und Eintrittswahrscheinlichkeiten individuelle Werte zu ermitteln. Eine Kategorisierung mit der Eintrittswahrscheinlichkeit selten, häufig und sehr häufig sowie der potenziellen Schadenshöhe mittel, hoch und sehr hoch sei hinreichend praxistauglich.[37] Dieser Maßstab zur angemessenen Granularität der Risikobeurteilung von Privaten im Rahmen der Unternehmens-IT-Sicherheit kann für die datenschutzrechtliche Fallgestaltung aber nicht zwangsläufig auch gelten. Denn es fehlt dieser Konstellation an einer schutzpflichtauslösenden Drittbetroffenheit von Grundrechten, die vielmehr einen höheren Aufwand bei der Beurteilung aus Gründen der Schutzgutangemessenheit der Methode gebieten könnte.

Die schutzgutangemessene Rationalität und Willkürfreiheit sowie die inhärente Lernfähigkeit eines quantitativen Risikomodells auf Basis der Bayes-Wahrscheinlichkeit könnten insofern schon allein mit Blick auf die Empfindlichkeit des grundrechtlichen Schutzgutes angemessener sein. Gleiches fordert daneben aber auch die Angemessenheit und rationale Begründung von Investitionsentscheidungen, die aus der staatlich gesetzten Pflicht zum technisch-organisatorischen Grundrechtsschutz erwachsen und die „Verantwortlichen" wiederum in ihrer kollidierenden Grundrechtssphäre von Eigentumsrechten aus Artikel 14

33 | Vgl. Delhey 2014.
34 | Vgl. BVerfGE 49, 89, S. 142 ff.
35 | Vgl. Klafki 2017, S. 15.
36 | Vgl. Seiler 1997, S. 47.
37 | Vgl. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), S. 28.

GG schützen. Wegen der Kumulation dieser rechtlich relevanten Kriterien ist insofern auch bei kleinen Fallzahlen das rationale methodische Fundament eines Wahrscheinlichkeitsbegriffs, der das subjektive Element des Degree of Belief (DoB) als Wahrscheinlichkeit formuliert sowie Vorwissen und einen empirischen Zuwachs in der Datenbasis konsistent integrieren kann, vorzugswürdig. Denn es ist auch bei höheren Aufwänden in der Ermittlung der notwendigen Datenbasis besser geeignet, das Telos datenschutzrechtlicher Normen zu erfüllen. Gerade bei einer Delegation von Risikobewertungen auf private „Verantwortliche", die gleichzeitig „Schützer" und „Gefährder" des „Schutzbedürftigen" sind, ist zudem zur schutzgutangemessenen Transparenzsicherung die verfahrensrechtliche Vorgabe einer expliziten Modellierung subjektiv verzerrender Faktoren geboten, wie sie die qualitative Risikomodellierung auf Basis der Bayes-Wahrscheinlichkeit vorsieht. Dies wäre bei der Wahl von semi-quantitativen Methoden nicht inhärent gegeben.[38]

Gegen die bis hierhin theoretisch fundierte Vorzugswürdigkeit des quantitativen Risikomodells könnten aus der Perspektive der zur Grundrechtsangemessenheit und Effektivität als notwendig dargestellten Lernfähigkeit des Verfahrens die Gesamtsystematik der verschiedenen risikobasierten Regelungen der DSGVO und insbesondere die Wertung des Artikels 35 DSGVO bei „hohen Risiken" streiten. Denn der Verordnungsgeber der DSGVO hat in Artikel 35 Absatz 4, 5, 6 DSGVO explizit statuiert, dass die Aufsichtsbehörden auf Basis eines Kohärenzverfahrens nach Artikel 63 DSGVO Listen mit Tätigkeiten veröffentlichen sollen, bei denen eine Datenschutzfolgenabschätzung (nicht) durchzuführen ist. Da diese Listen inhärent auch die Ergebnisse von aufsichtsbehördlichen Risikobewertungen enthalten, könnte dieser gesetzlich angeordnete Lernprozess bei unsicheren Wissensbeständen eher auf die Intention einer pauschalen Klassifikation von Fallgruppen zu Risikoklassen deuten. Dessen ungeachtet ist aber gleichwohl auch nach Artikel 35 Abs. 7c DSGVO im Rahmen einer mit der Methodik des Artikels 25 DSGVO korrespondierenden Datenschutzfolgenabschätzung durch den „Verantwortlichen" eine konkrete Bewertung der „Risiken für die Rechte und Freiheiten der betroffenen Personen" erforderlich. Dies spricht in systematischer Gesamtbetrachtung für ein gestuftes Lernverfahren zwischen staatlicher Auffangverantwortung und Effektivitätssicherung. Eine praktikable Festlegung von Fallgruppen „hohen Risikos" durch die Aufsichtsbehörden, als Vorstufe einer konkreten Risikoermittlung, muss im Rahmen von Artikel 25 DSGVO nicht zwangsläufig präjudizierend gegen die Schutzgutangemessenheit von Lernverfahren privater Dritter auf Basis quantitativer Risikobewertungen sprechen.

Integrationsfähigkeit der Methodik der Risikobewertungen

Wie ausgeführt ist die Risikobewertung kein Selbstzweck, sondern im Rahmen von Artikel 25 DSGVO ein zu berücksichtigender Belang im Risikomanagement der DSGVO und mithin relevant bei der Auswahlentscheidung von technisch-organisatorischen Schutzmaßnahmen entlang der einzelnen Flanken der Verwundbarkeit des Schutzbedürftigen. Auch hier gilt es aus grundrechtlicher Perspektive, eine möglichst rational fundierte[39], willkürfreie Abwägungsentscheidung zur Angemessenheit und somit auch von Kosten und Nutzen zu treffen. Auch wenn in semi-quantitativen Verfahren grundsätzlich mittels Indikatoren, Abstufungen oder Klassifizierungen rechnerisch ein Risiko und korrespondierende Maßnahmen auf beschreibende/numerische Art dargelegt werden können, ist im Resultat keine Bewertung der Folgenschwere einer Schutzgutverletzung der Maßnahmenauswahl auf Basis einer rationalitätssichernden einheitlichen Bewertungsmetrik möglich. Dies spricht bei Zugrundelegung der oben entwickelten Anforderungen zum Ausgleich von Output-Legitimität und Schutzgutangemessenheit der Methode grundsätzlich gegen die Verwendung semi-quantitativer Risikomodelle für den Gesamtprozess der Maßnahmenauswahl im Rahmen des Artikels 25 DSGVO.

Ein Vorteil für ein quantitatives Risikomodell, welches eine einheitliche Bewertungsmetrik der Folgenschwere und Maßnahmenauswahl auf einheitlichen Kostenmaßen inhärent erlaubt, würde sich aber erst dann zeigen, wenn grundsätzlich für die verschiedenen Flanken der Vulnerabilität auch Schadmaße zu finden wären, die eine Beschreibung in Kosten erlaubten. Im Hinblick auf das Schutzgut des Artikels 25 DSGVO, die unbestimmten „Rechte und Freiheiten natürlicher Personen", könnten insofern Zweifel bestehen, als beispielsweise immaterielle

38 | Zudem kann bei der entscheidungserheblichen Risikobeurteilung im Rahmen des Artikels 25 DSGVO auch die Perspektive des subjektiven DoB des eigentlich grundzuständigen staatlichen Entscheidungsträgers neben dem DoB des „*Schützers*" als verantwortlicher Stelle angemessen berücksichtigt werden. Dies ist im Entscheidungsprogramm des Artikels 25 DSGVO materiell jedenfalls grundsätzlich im Rahmen der konkreten Maßnahmenwahl gesichert. Die aus staatlicher Sicht markierten, auch risikorelevanten Eingriffsschwellen werden im Rahmen der Entscheidung zur Maßnahmenwahl nach Artikel 25 im Konditionalprogramm der materiellen Schutzprinzipien wie zum Beispiel den materiellen Bewertungen zur Datenminimierung oder zur grundlegenden Datensicherheit durch die Verpflichtung der verantwortlichen Stelle, „den Anforderungen dieser Verordnung zu genügen", dem privaten „*Schützer*" unmittelbar als berücksichtigungsrelevante, unabdingbare Zielfunktion zugewiesen. Mithin werden auch die subjektiven Elemente der gestuften staatlichen Vorabentscheidung zu unterschiedlichen Eingriffsintensitäten und Risikoanlagen für die informationelle Selbstbestimmung der Betroffenen damit grundsätzlich an den Bewertenden vermittelt.

39 | Vgl. zum Rationalitätsaspekt Merz 2006, S. 17.

Schäden nicht zwangsläufig zivilrechtliche Haftungsfolgen nach sich ziehen müssen. Allerdings führt Erwägungsgrund 75 konkretisierend aus, dass die Risiken, welche aus einer Verarbeitung personenbezogener Daten hervorgehen können, neben materiellen auch zu physischen oder immateriellen Schäden führen könnten. Es sind also alle Schadfolgen grundsätzlich in den unbestimmten Begriff aufgenommen. Insofern kann eine Schadbemessung in Kostenfunktionen in diesem Rahmen nicht daran scheitern, dass keine einfachrechtliche Haftung für die Schutzgutverletzung vorgesehen ist. Insofern gewinnt jedoch an Gewicht, dass hinsichtlich der Kostenbasis grundsätzlich auch keine Lücke entstehen kann, wo das Zivilrecht keinen Schadenersatz in Geld vorsieht. Denn die DSGVO gewährt in Artikel 82 selbst Haftung und ein Recht auf Schadenersatz sowohl bei materiellen wie aber auch bei immateriellen Schäden durch die Verletzung von Schutzmechanismen der DSGVO. Unter der Bedingung einer zu erwartenden Kasuistik zu den verschiedenen Fallgruppen von Verstößen gegen einzelne Schutzprinzipien ist also die „Bepreisung" der Folgenschwere auch bei immateriellen Schutzgutverletzungen grundsätzlich gewährleistet. Insofern streitet auch die bessere Integration in das kostenbasierte Konditionalprogramm zur Wahl von geeigneten, auch risikoangemessenen Schutzmaßnahmen hier für die Wahl eines quantitativen Risikomodells auf einheitlicher Bewertungsbasis in Kostenfunktionen. Neben einer Betrachtung des Eingriffs in die Grundrechte ist eine Risikoanalyse notwendig, in deren Ergebnis beurteilt werden soll, wie groß die Wahrscheinlichkeit ist, dass die betreffende Organisation trotz aller getroffenen Maßnahmen zum Schutz der Grundrechte Datenschutzvorgaben nicht einhalten wird.

Praktikabilität der Risikomodelle

Um die notwendige Effektivität des Schutzprogramms zu gewährleisten, müssen die Risikomodelle nicht nur im Theoretischen vergleichend bewertet werden, sondern auch für die verantwortlichen Stellen im Rahmen des Risikomanagements praktikabel umsetzbar sein. Maßstabsbildend ist, dass gemäß der Literatur die ideale Strategie für ein rationales Risikomanagement jene ist, die Gefahren und Risiken identifiziert, quantifiziert und bewertet und durch Festlegung konsistenter Schutzziele beherrschbar sein lässt.[40] Dieses Ziel wird von den vorhandenen Modellen semi-quantitativer Bewertung im Datenschutz unter der Bedingung eines Höchstmaßes an Praktikabilität – mit einem klaren Schwerpunkt auf konsistenten technischen Schutzzielen – in den Fokus genommen. Es ist allerdings fraglich, inwiefern bei aller Praktikabilität diese Modelle auch die Systematik des Risikokonzepts der DSGVO noch reflektieren. Grundsätzlich wird sowohl im möglicherweise referenzbildenden Standard-Datenschutzmodell (SDM)[41] wie auch in weiteren Konkretisierungen wie der Privacy Impact Assessment Guideline des BSI[42] eine Methodik vorgeschlagen, die den Verantwortlichen zunächst in drei Stufen „Schutzbedarfe" für spezifische „Schutzziele" feststellen lässt. Sodann soll der Verantwortliche Maßnahmen identifizieren, die den Gefährdungen adäquat entgegenwirken. Diese Maßnahmen sind wiederum in die drei Ausprägungen gering (1), mittel (2) und groß (3) differenziert und sollten so gewählt werden, dass ihre Ausprägung dem zuvor festgestellten Schutzbedarf entspricht.[43] Dem entspricht in der Methodik auch die Privacy Impact Assessment Guideline des BSI.[44] Auch wenn im letztgenannten Modell darauf verwiesen wird, dass ein vollständiges Privacy Impact Assessment auch die Wahrscheinlichkeit von Schutzgutverletzungen in die Risikobewertung aufnehmen würde,[45] findet sich dort keine Methodik dieser Bewertung.

Im SDM wird für die hier relevante Maßnahmenauswahl zunächst nur die Folgenschwere von Schutzgutverletzungen als Eingriffsintensität semi-quantitativ bewertet, und generische Referenz-Schutzmaßnahmen werden abgeleitet. Aus einer Risikoanalyse sollen sich in diesem Modell allenfalls zusätzliche Schutzmaßnahmen ergeben, welche die aus der Eingriffsintensität resultierenden Maßnahmen ergänzen.[46] Diese Methodik entspricht – bei aller Praktikabilität – nicht der Struktur des Risikomanagements in Artikel 25 DSGVO. Die Methodenkritik ist insofern wegen des potenziell maßstabbildenden Charakters des SDM hier noch weiter zu fundieren. Ebenso fehlt dem SDM die im Rahmen der Risikoermittlung erforderliche unmittelbare Auseinandersetzung mit den Schutzgütern der informationellen Selbstbestimmung. Während die DSGVO die eigentlichen Schutzgüter der informationellen Selbstbestimmung in den Mittelpunkt der Bewertung von Risiken und Maßnahmenauswahl stellt, setzt das SDM zentral beim Schutz der sekundären, flankierenden Sicherungsmechanismen des Grundrechtsschutzes und den dort genannten Gewährleistungszielen an,[47] die sich

40 | Vgl. Merz 2006, S. 17.
41 | Vgl. Das Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung, 2016.
42 | Vgl. Privacy Impact Assessment Guideline, Bundesamt für Sicherheit in der Informationstechnik 2011.
43 | Vgl. Das Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung 2016, S. 37.
44 | Vgl. Privacy Impact Assessment Guideline, Bundesamt für Sicherheit in der Informationstechnik 2011.
45 | Vgl. Privacy Impact Assessment Guideline, Bundesamt für Sicherheit in der Informationstechnik 2011, S. 24.
46 | Vgl. Das Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung 2016, S. 39.
47 | Vgl. Das Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung 2016, S. 11 ff.

wiederum lediglich aus einfachrechtlichen Schutzprinzipien des Datenschutzrechts speisen. Erst im Rahmen der Verortung von semi-quantitativ beschriebenen Schutzbedarfskategorien wird die Schwere von Schadereignissen an den konkreten Schutzgütern, mithin den „Rechten und Freiheiten" der DSGVO, reflektiert. Diese grundsätzlichen perspektivischen Mängel des Modells sind insofern nur mit der privaten IT-Sicherheit erklärbar. Die dort eingeführte Risikobewertung stellt die möglichen Schäden durch Verlust von „Vertraulichkeit", „Integrität" und „Verfügbarkeit" von Daten als Schutzgut und Selbstzweck der Bewertung ein.[48] Es sollte offensichtlich sein, dass diese „Schutzgüter" nicht im Ansatz mit den Kategorien von Schutzgütern in den konkretisierenden Regelbeispielen aus Erwägungsgrund 75 der DSGVO korrespondieren. Nunmehr wird explizit angemerkt, dass die Skalen zur „Risikobewertung" im SDM ihren Ursprung in der Datensicherheit nach BSI-Grundschutz haben.[49] Eine praktische Herausforderung bei der Verwendung von quantitativen Risikomodellen auf Basis der Bayes-Wahrscheinlichkeit könnte jedoch abschließend die Gewinnung der notwendigen Datenbasis für eine Bewertung darstellen. Diese Frage kann derzeit nicht abschließend geklärt werden, und es sind insofern Instanziierungen des abstrakten Modells im Hinblick auf Artikel 25 DSGVO in weiteren Untersuchungen notwendig.

Zusammenfassung und Ausblick

Es wurde gezeigt, dass das *Rollenmodell* des Artikels 25 DSGVO aus grundrechtlicher Perspektive nicht zu beanstanden ist. Aus einer Gesamtschau der Wechselwirkungen zwischen Schutzgutangemessenheit und der besseren Effektivität von Lernprozessen in privater Aufgabenerfüllung ist diese Aufgabenzuweisung beim Vorliegen eines hinreichend bestimmten und normklaren Verfahrensrahmens zur Methodik und Auslegung unbestimmter Begriffe auch legitim. Der vermeintliche Wertungswiderspruch des Rollenmodells der DSGVO mit der spieltheoretischen Modellierung kann auf grundrechtsdogmatischer und regulierungstheoretischer Basis über angemessene Kostenfunktionen aufgelöst werden.

Der *Risikobegriff* der DSGVO ist nach der grundrechtsdogmatischen Bewertung mit eigenständigen Maßstäben im Verhältnis zur Bedeutung des Risikoverwaltungsrechts versehen. Grundsätzlich erweisen sich in der Gesamtschau die vorhandenen, aus der Methodik der klassischen IT-Sicherheit motivierten Verfahren auf Basis einer Methodik semi-quantitativer Risikobewertung als unvollständig und in ihrer Schutz- und Bewertungsperspektive für Risikoentscheidungen der DSGVO auch als ungeeignet. Wie ein praktisch anwendbares Modell unter Zugrundelegung einer spieltheoretisch motivierten quantitativen Risikobewertung auf Basis der Bayes-Wahrscheinlichkeit zu gestalten ist, ist weiter zu erforschen. Das Modell ist in Bezug auf die Risikosystematik der DSGVO und die hier entwickelten Wertungsmaßstäbe nicht widerlegt worden. Es ist zukünftig eine schutzgutangemessene, normklare und bestimmte verfahrensrechtliche Sicherung der Effektivität der Risikobewertung und der Wahl von Schutzmaßnahmen notwendig. Hierfür kann das theoretische Modell grundsätzlich sogar als methodischer Maßstab gelten.

Da das Bundesverfassungsgericht schon bei staatlichen Risikoentscheidungen die Option der Verbesserung von Entscheidungswissen unter Unsicherheit durch Simulationen angesprochen hat, ist in der weiteren Forschung eine technische Werkzeugunterstützung für Risikoentscheidungen der DSGVO auf Basis quantitativer Risikobewertungs- und Risikomanagementverfahren zu betrachten. Der Aspekt der Lernfähigkeit in der entscheidungserheblichen Datenbasis und der im theoretischen Modell angelegte Vorteil einer Optimierung der risikoangemessenen Maßnahmenauswahl in einem dynamischen Prüfverfahren sprechen hierfür. Denn in einem simulativen, werkzeugunterstützten Prüfverfahren können – anders als bei der bisherigen statischen Beurteilung – die Wechselwirkungen zwischen der Risikobewertung und der möglichen Wahl von Schutzalternativen sowie die über Zeitabschnitte gekoppelten Veränderungen der Kosten-Nutzen-Betrachtung eines Angreifers erfasst werden. Ein technikunterstützendes Werkzeug sollte zudem auf einer technisch-formalen Beschreibung der relevanten Begriffe basieren, wie sie in diesem Band eingeführt wird. Da es sich bei der Bewertung um einen Akt domänenübergreifender Kommunikation handelt, ist ein Allgemeinverständnis auf Basis eindeutiger Bedeutungsgehalte der Symboliken unabdingbar, um unerkannte Maßstabsverzerrungen bei der Bewertung zu minimieren.[50]

48 | Vgl. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), S. 28.
49 | Vgl. Rost 2012, S. 436.
50 | Vgl. Schnieder/Schnieder 2018.

Literatur

Arndt 2012
Arndt, B.: „Das Risikoverständnis der Europäischen Union". In: Jaeckel, L./Janssen, G.: *Risikodogmatik im Umwelt- und Technikrecht*, Tübingen: Mohr Siebeck 2012, S. 35 ff.

Beyerer/Geisler 2018
Beyerer, J./Geisler, J.: „Formaler Rahmen für eine einheitliche quantitative Beschreibung des Risikos bezüglich Safety und Security". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Delhey 2014
Delhey, M.: *Staatliche Risikoentscheidungen – Organisation, Verfahren und Kontrolle*, Baden-Baden: Nomos Universitätsschriften 2014.

Friedewald et al. 2010
Friedewald, M./Raabe, O./Georgieff, P./Koch, D. J./Neuhäusler, P.: *Ubiquitäres Computing – Zukunftsreport für das Büro für Technikfolgenabschätzung beim Deutschen Bundestag*, BTDrs. 17/405, 2010.

Grimm 2001
Grimm, D.: „Selbstregulierung in der Tradition des Verfassungsstaates". In: Berg, W. (Hrsg.): *Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlass des 60. Geburtstages von Wolfgang Hoffmann-Riem*, DV, Beiheft 4, 2001, S. 9 ff.

Herzmann 2010
Herzmann, K.: *Konsultationen – Eine Untersuchung von Prozessen kooperativer Maßstabskonkretisierung in der Energieregulierung*, Tübingen: Mohr Siebeck 2010.

Hoffmann-Riem et al. 2000
Hoffmann-Riem, W./Schulz, W./Held, T.: *Konvergenz und Regulierung – Optionen für rechtliche Regelungen und Aufsichtsstrukturen im Bereich Information, Kommunikation und Medien*, Baden-Baden 2000.

Hoffmann-Riem 2005
Hoffmann-Riem, W.: *Gesetz und Gesetzesvorbehalt im Umbruch. Zur Qualitäts-Gewährleistung durch Normen*, AöR, 2005, S. 5 ff.

Klafki 2017
Klafki, A.: *Risiko und Recht – Risiken und Katastrophen im Spannungsfeld von Effektivität, demokratischer Legitimation und rechtsstaatlichen Grundsätzen am Beispiel von Pandemien*, Tübingen: Mohr Siebeck 2017.

Ladeur 2000
Ladeur, K.-H.: „Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken". In: *Datenschutz und Datensicherheit*, Springer 2000, S. 16 ff.

Merz 2006
Merz, B.: *Hochwasserrisiken. Grenzen und Möglichkeiten der Risikoabschätzung*, Stuttgart: Schweizerbart'sche Verlagsbuchhandlung 2006.

Raabe et al. 2011
Raabe, O./Lorenz, M./Pallas, F./Weis, E.: *Harmonisierung konträrer Kommunikationsmodelle im Datenschutzkonzept des EnWG – „Stern" trifft „Kette", Ansätze zur datenschutzrechtlichen Konfliktlösung im Smart Metering*, CR 2011, S. 831 ff.

Röhl 2012
Röhl, H. C.: „Ausgewählte Verwaltungsverfahren". In: Hoffmann-Riem, W./Schmidt-Aßmann, E./Voßkuhle, A. (Hrsg.): *Grundlagen des Verwaltungsrechts*, Bd. II, Informationsordnung, Verwaltungsverfahren, Handlungsformen, München: C.H. Beck Verlag, 2. Auflage, 2012, S. 748 ff.

Rost 2012
Rost, M.: „Standardisierte Datenschutzmodellierung". In: *Datenschutz und Datensicherheit*, Springer 6/2012, S. 433 ff.

Schallbruch 2016
Schallbruch, M.: *Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste. Wie groß ist der Umsetzungsbedarf der NIS-Richtlinie in deutsches Recht im Bereich digitaler Dienste?,* CR 2016, S. 663–670.

Schnieder/Schnieder 2018
Schnieder, E./Schnieder, L.: „Formalisierung von Begriffen der Sicherheit und Sicherheitsmetriken". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Seiler 1997
Seiler, H.: *Recht und technische Risiken: Grundzüge des technischen Sicherheitsrechts* (Polyprojekt Risiko und Sicherheit), 18, Zürich 1997.

Veil 2015
Veil, W.: DS-GVO: *Risikobasierter Ansatz statt rigides Verbotsprinzip. Eine erste Bestandsaufnahm*e, Zeitschrift für Datenschutz (ZD), 8, 2015, S. 347.

Vesting 2001
Vesting, T.: „Subjektive Freiheitsrechte als Elemente von Selbstorganisations- und Selbstregulierungsprozessen in der liberalen Gesellschaft". In: Berg, W. (Hrsg.): *Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlass des 60. Geburtstages von Wolfgang Hoffmann-Riem*, DV, Beiheft 4, 2001, S. 21 ff.

Vieweg 2018
Vieweg, K.: „Sicherheit – Begriffe, Szenarien, Verantwortlichkeiten und Entscheidungsprozesse aus juristischer Sicht". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Wiesner et al. 2006
Wiesner, A./Schneider, S./Nullmeier, F./Krell-Laluhova, Z./Hurrelmann, A.: *Legalität und Legitimität – erneut betrachtet*, Politische Vierteljahresschrift, 36, 2006, S. 164–183.

Wollenschläger 2009
Wollenschläger, B.: *Wissensgenerierung im Verfahren*, Tübingen: Mohr Siebeck 2009.

Ziegler 2017
Ziegler, M.: *Induktive Statistik und soziologische Theorie. Eine Analyse des theoretischen Potenzials der Bayes-Statistik*, 1. Auflage, Weinheim: Beltz Verlag, 2017.

Zippelius 2006
Zippelius, R.: *Das Wesen des Rechts. Eine Einführung in die Rechtstheorie*, 6. Auflage, Stuttgart: Kohlhammer Verlag, 2012.

8 Anwendungen systemtheoretischer Ansätze am Beispiel konkreter Problemstellungen

8.1 Quantitative Analyse der Vulnerabilität am Beispiel Verkehrsflughafen

Dr.-Ing. Daniel Lichte
Institut für Sicherungssysteme, Bergische Universität Wuppertal

Prof. Dr.-Ing. Kai-Dietrich Wolf
Institut für Sicherungssysteme, Bergische Universität Wuppertal

Zusammenfassung

Das Bedrohungspotenzial möglicher Angriffsszenarien an wichtigen Infrastrukturen rückt mehr und mehr sowohl in den gesellschaftlichen als auch in den wissenschaftlichen Fokus. Diese Entwicklung wird durch eine steigende Anzahl Security-relevanter Ereignisse an Flughäfen bestätigt. Die internationale Organisation der zivilen Luftfahrt ICAO (International Aviation Organization), die eine Sonderorganisation der UN ist, legt in ihren Empfehlungen fest, dass eine Bewertung der physischen Sicherheit von Flughafeninfrastrukturen vorgenommen werden sollte. Bis heute gibt es unterschiedliche Ansätze zur Sicherheits- und Risikobewertung von kritischen Infrastrukturen, die sich auch auf Flughäfen anwenden lassen. Bei genauer Betrachtung wird jedoch deutlich, dass diese Ansätze Unzulänglichkeiten bei der Modellierung von Vulnerabilität als einem zentralen Aspekt der Bewertung der physischen Sicherheit aufweisen. In diesem Artikel wird ein analytischer Modellierungsansatz vorgeschlagen, der eine quantitative und szenarioübergreifende Vulnerabilitätsanalyse innerhalb der Risikoanalyse von physischen Bedrohungen erlaubt. Dieser Ansatz wird beispielhaft auf einen fiktiven Bereich eines Flughafens angewendet und basiert auf den Parametern Protektion, Observation und Intervention, welche die Eigenschaften des Sicherungssystems charakterisieren.

Die Bewertung von Sicherungsmaßnahmen zur Verbesserung der Security orientiert sich oft an der klassischen Risikodefinition

Risiko = Eintrittswahrscheinlichkeit × Auswirkung

die auch in anderen Beiträgen dieses Bandes[1] verwendet, aber zum Beispiel von Rechtswissenschaftlerinnen und -wissenschaftlern[2] durchaus kritisch gesehen wird. Während die Auswirkung eines Angriffs in der Regel ohne größere formale Schwierigkeiten monetär zu quantifizieren ist (ethische Herausforderungen bestehen selbstverständlich, wenn zum Beispiel Menschen zu Schaden kommen), wird die Eintrittswahrscheinlichkeit eines erfolgreichen Angriffs oft aufgeteilt in Bedrohungswahrscheinlichkeit und die sogenannte Vulnerabilität oder Verwundbarkeit.[3] Alle Faktoren, die zum Eintreten eines konkreten Bedrohungsszenarios beitragen, also zum Beispiel Motivation und Fähigkeit des Angreifers, Attraktivität des Ziels (Asset) etc., werden in der Bedrohungswahrscheinlichkeit zusammengefasst. Die Vulnerabilität erfasst die Wahrscheinlichkeit, dass ein Angriff erfolgreich durchgeführt wird, also nicht etwa durch technische oder organisatorische Sicherungs- und Interventionsmaßnahmen abgewehrt werden kann, und stellt somit ein Maß für die (Nicht-)Wirksamkeit dieser Maßnahmen dar. Das Risiko im Sinne einer Bewertung der Security ließe sich also wie folgt beschreiben:

Risiko = Bedrohungswahrscheinlichkeit × Vulnerabilität × Auswirkung

Dieser nun dreigeteilte Risikobegriff ist oft die Basis praxisrelevanter, meist semi-quantitativer[4] Risikobewertungen der Security. Wird die obige Formulierung des Risikos im Sinne einer Multiplikation quantifizierter Größen interpretiert, so ist die Gültigkeit ganz offensichtlich auf diskrete Wahrscheinlichkeiten

1 | Vgl. Beyerer/Geisler 2018, Schnieder/Schnieder 2018, Vieweg 2018, Deutschmann/Milbredt 2018, Arens/Kühne 2018.
2 | Vgl. Raabe 2018.
3 | Vgl. Arens/Kühne 2018.
4 | Vgl. ebd.

stochastisch unabhängiger Ereignisse beschränkt. Diese Voraussetzungen werden in aller Regel nicht gegeben sein. Eine Bedrohungswahrscheinlichkeit[5] ist mit Unschärfe behaftet und die konkrete Bedrohung das Ergebnis willkürlicher Handlungen.[6] Man kann hinterfragen, ob der Begriff „Wahrscheinlichkeit" hier überhaupt angebracht ist. In jedem Fall ist die Wahrscheinlichkeitstheorie ein fundiertes Konzept, das den Umgang mit unscharfen Größen in elaborierter Weise ermöglicht und für die Bewertung von Sicherheitsrisiken in geeigneter Form widerspruchsfrei erweitert werden kann.[7]

Auch die Vulnerabilität eines Objekts und damit die Wahrscheinlichkeit des Erfolgs bei gegebener Bedrohung unterliegt wesentlichen Unschärfen und hängt neben willkürlichen Entscheidungen des Angreifers ganz wesentlich von der Ausprägung von Sicherungsmaßnahmen ab. Wie sich die Wirksamkeit dieser Maßnahmen auf der Basis einer Metrik quantifizieren lässt, wird in diesem Beitrag am Beispiel eines Verkehrsflughafens dargestellt. Die grundlegenden Wirkmechanismen Protektion, Observation und Intervention beschreiben dabei die Abwehrmöglichkeiten und sind über Zeitverteilungen abgebildet. Bestehen unterschiedliche Angriffspfade, so wird die Entscheidung eines intelligenten und informierten Angreifers wohl zugunsten des am wenigsten gesicherten, also schwächsten Angriffspfades fallen. Damit legt der schwächste Pfad[8] die Vulnerabilität des Objekts bezüglich eines oder mehrerer definierter Angriffsziele fest. Die Quantifizierung der Vulnerabilität technischer Systeme und kritischer Infrastrukturen wird als Baustein einer integrativen Theorie der Verlässlichkeit gesehen.[9,10]

Die Entwicklung einer objektiven Basis zur quantitativen Beschreibung von Vulnerabilität, zu der wir hier einen Beitrag leisten möchten, kann in Zusammenfassung der obigen Erläuterungen ohne einen formalen Rahmen für die quantitative Beschreibung des Sicherheitsrisikos[11] nicht gelingen. Dabei verstehen wir unsere Bottom-up-Vorgehensweise, die bei etablierten Methoden ansetzt und diese schrittweise verallgemeinert, somit die Anschauung befördert und erste quantitative Ergebnisse bei moderatem Modellierungs- und Berechnungsaufwand liefert, als komplementär zur Entwicklung einer fundierten und notwendigerweise abstrakten Theorie.

1 Einführung

Durch die zunehmende Bedrohung, die von potenziellen terroristischen Anschlägen ausgeht, gelangt die Sicherheit von zivilen Flughäfen, die als kritische Infrastrukturen betrachtet werden können, mehr und mehr in den Fokus von Gesellschaft und Wissenschaft. Tatsächlich gab es in den letzten Jahren eine beträchtliche Anzahl von Vorfällen, die für die Sicherheit von Flughäfen relevant sind.

Eine Befragung an US-amerikanischen Flughäfen durch den Pressedienst Associated Press (AP) im Jahr 2016 ergab, dass allein im Bereich des Perimeterschutzes zahlreiche Vorfälle verzeichnet wurden.[12] Die physische Sicherheit von zivilen Flughäfen wird durch die ICAO, die internationale Organisation für zivile Luftfahrt, reguliert und kontrolliert. Annex 17 des Abkommens über die internationale zivile Luftfahrt, der sich mit der Abwehr von äußeren Gefahren wie Sabotageakten und anderen, beispielsweise terroristisch motivierten Angriffen oder Eingriffen beschäftigt, sieht vor, dass eine Analyse der physischen Sicherheit von Flughafeninfrastrukturen erfolgen soll. Das Aviation Security Manual,[13] welches öffentlich nicht verfügbar ist, beschreibt weitere Einzelheiten zu diesen geforderten Analysen und zeigt relativ unspezifisch mögliche Methoden auf, die auf qualitativen Modellen und Expertenwissen basieren.

Darüber hinaus sind zahlreiche institutionelle Forschungsprogramme aufgelegt worden, die sich mit dem physischen Schutz und der Cyber-Security von kritischen Infrastrukturen befassen. In diesem Kontext entwickelten sich verschiedene Ansätze zur Risikobewertung kritischer Infrastrukturen,[14] die sich auch im Kontext von Flughäfen anwenden lassen. Eine detaillierte Analyse dieser Ansätze zeigt jedoch, dass sie Defizite in der Modellierung der Vulnerabilität als einer wesentlichen Komponente der physischen Risiko- und Sicherheitsbewertung aufweisen.

5 | Mit der Ermittlung der Bedrohungswahrscheinlichkeit aus kriminellen Aktivitäten befasst sich Labudde 2018.
6 | Die Abbildung willkürlicher Handlungen wird von Weyer et al. 2018 beschrieben (in diesem Band).
7 | Vgl. Beyerer/Geisler 2016.
8 | Vgl. Beyerer/Geisler 2018.
9 | Vgl. Bertsche et al. 2018.
10 | Vgl. Deutschmann/Milbredt 2018: Über einen Fuzzy-Ansatz kann das globale Sicherheitsniveau eines Verkehrsflughafens auch ohne konkrete Quantifizierung der Wirkmechanismen von Sicherungsmaßnahmen bewertet werden.
11 | Vgl. Beyerer/Geisler 2018.
12 | Vgl. Associated Press 2016.
13 | Vgl. ICAO 2015.
14 | Vgl. Giannopoulus et al. 2012.

Bestehende Ansätze beschränken sich gleichermaßen auf die Analyse und Bewertung spezifischer Szenarien, wobei die Art des Angriffs, die Assets als definierte Angriffsziele und die resultierenden Folgen als Auswirkungen festgelegt sind.[15] Aus diesem Grund beziehen sich die erzielten Ergebnisse der Risikobewertung nur auf das betrachtete Szenario; eine szenarioübergreifende Analyse kann auf dieser Grundlage nicht geleistet werden. Hinzu kommt, dass die meisten Ansätze auf qualitativen oder semi-quantitativen Methoden basieren, die oft die subjektive Einschätzung von Fachleuten erfordern, sodass eine objektive Quantifizierung der Vulnerabilität der betrachteten Infrastruktur nicht möglich ist. Die Verwendung diskreter Wahrscheinlichkeiten, die üblicher Bestandteil quantitativer Risikobewertungen sind, kann dabei irreführende Ergebnisse liefern. Gleichzeitig werden Unsicherheiten, die der Charakterisierung von Komponenten und Systemen von Sicherheitseinrichtungen inhärent sind, in der Regel nicht weiter berücksichtigt.[16]

In diesem Artikel sollen die beschriebenen Probleme dezidiert betrachtet werden. Gleichzeitig wird ein übergreifender analytischer Modellierungsansatz präsentiert, der eine quantitative und szenarioübergreifende Vulnerabilitätsanalyse innerhalb der Bewertung der physischen Sicherheit erlaubt. Der Ansatz, der in der Beschreibung der Fähigkeiten von Sicherungssystemen in einer Infrastruktur auf den Parametern Protektion, Detektion und Intervention basiert, wird auf einen fiktiven Bereich einer Flughafeninfrastruktur angewendet. Zunächst werden die grundlegenden Annahmen hierzu dargestellt und die Berechnung der systemischen Angriffspfade näher erläutert. Wahrscheinlichkeitsdichtefunktionen, die die Wirksamkeit von Sicherheitsbarrieren beschreiben können, werden vorgestellt. Im Weiteren folgt eine Herleitung der analytischen mathematischen Beziehungen, die aus den grundlegenden Annahmen resultieren. Die Analyse der Detektion ergibt den sogenannten kritischen Detektionspunkt, der von Garcia eingeführt wurde[17] und in eine Barrieren-orientierte Berechnung der Vulnerabilität der möglichen Angriffspfade des Flughafenbereichs überführt wird. So wird gezeigt, dass eine szenarioübergreifende Bewertung und Analyse sowie auch die Betrachtung möglicher Unsicherheiten bei der Beschreibung des Systems möglich sind. Die Vulnerabilitätsanalyse der gesamten Flughafensektion basiert auf der Anwendung des Prinzips des schwächsten Angriffspfades. Abschließend erfolgt eine kritische Diskussion des analytischen Ansatzes, und es werden weitere Forschungsbedarfe skizziert. Insbesondere wird die Möglichkeit erwogen, die Konfiguration von Sicherungsmaßnahmen für definierte Infrastrukturen zu optimieren, um deren Vulnerabilität mithilfe des dargestellten Modells zu minimieren.

2 Stand der Forschung

Im ersten Teil des Kapitels werden aktuelle Maßnahmen, Regulierungen und Bestimmungen sowie neue Ansätze zur Luftsicherheit eingeführt. Hierbei ist festzustellen, dass aus der Verschärfung der Bestimmungen in der Luftsicherheit verstärkt die Notwendigkeit resultiert, eine Risikobewertung im Bereich der Security zu entwickeln, die insbesondere auf einer Vulnerabilitätsanalyse der Infrastrukturen ziviler Flughäfen basiert. Während der aktuelle Stand der Forschung in der Risikobewertung im zweiten Kapitel des Artikels behandelt wird, wird im letzten Teil ein kurzer Überblick über bestehende Methoden im Kontext der Vulnerabilitätsanalyse gegeben.

2.1 Luftverkehr und Flughafensicherheit

Insbesondere seit den Terroranschlägen am 11. September 2001 wurden diverse Maßnahmen zur Flugsicherung und Flughafensicherheit ergriffen; Annex 17 des Chicago-Abkommens über die internationale Zivilluftfahrt[18] führt diese detailliert auf. Es werden hier nicht nur die Maßnahmen im Einzelnen aufgelistet – der Maßnahmenkatalog nennt darüber hinaus auch konkrete Beispiele, wie diese Maßnahmen umgesetzt und Bestimmungen eingehalten werden können. Er enthält 66 Sicherheitsmaßnahmen sowie zusätzlich 16 empfohlene Methoden zu deren Anwendung und ein sogenanntes Programm für Sicherheitsaudits (USAP – Universal Security Audit Program), mit welchem ein entsprechender Umsetzungs- und Implementierungsstand ermittelt werden kann.

Sowohl Annex 17 als auch daraus resultierende weiterführende Entwicklungen in Wissenschaft und Anwendung beinhalten neue Modelle und Methoden sowie Maßnahmen zur Sicherung und zum Schutz von Flugzeugen und zivilen Flughäfen vor unterschiedlichsten terroristischen Bedrohungen. Konkrete Maßnahmen zur Bekämpfung potenzieller terroristischer Angriffe sind zum Beispiel detaillierte Reisegepäckkontrollen, die biometrische Identifizierung von Fluggästen sowie eine risikobasierte Bedrohungsbeurteilung.[19]

15 | Vgl. French/Gootzit 2011.
16 | Vgl. Cox 2009.
17 | Vgl. Garcia 2008.
18 | Vgl. ICAO 2014.
19 | Vgl. Tamasi/Demichela 2011.

Die wissenschaftlich fundierte Methodik fokussiert hier auf die Bedeutung des Risikomanagements sowie eine Bewertung der Vulnerabilität und potenzieller Bedrohungen. Das nicht öffentlich zugängliche ICAO-Dokument 8973[20] umreißt verschiedene Ansätze zur analytischen und semi-quantitativen Risikoanalyse. Es bieten sich jedoch zusätzlich noch weitere Maßnahmen an – diese sollten sowohl die Bedrohungs- als auch eine Vulnerabilitätsanalyse umfassen und auf potenzielle Folgen und deren Kritikalität eingehen.[21]

Im Allgemeinen basiert eine Vulnerabilitätsbewertung auf der Analyse der bestehenden Infrastrukturen und identifiziert deren Schwachstellen wie bestehende Protektions- und Observationssysteme oder auch Prozesse, die anfällig für potenzielle Anschläge durch Terroristen oder unbefugte Angreifer sind.[22] Dies können im Falle eines geplanten Angriffs kritische Angriffspunkte sein, die zum Erfolg des Angreifers führen.[23]

Eine Identifizierung der kritischen Assets der betrachteten Infrastruktur als potenziell bevorzugter Angriffsziele stellt einen ersten essenziellen Schritt in der sicherheitsbezogenen Risikoanalyse dar, da hier wichtige Grundstrukturen sowie Standorte identifiziert werden, die einen besonderen Schutz erfordern.[24]

2.2 Security-Risikoanalyse

Sicherheit im Sinne von Security, also Schutz vor gewollten Gefährdungen,[25] umfasst eine Reihe von Aspekten, die verschiedene Kompetenzbereiche abdecken. Daher ist eine ganzheitliche Betrachtung wesentliche Grundlage für eine umfassende Sicherheitsbewertung.[26] Physische Sicherheit als ein Teil davon behandelt den Schutz von Infrastrukturen vor geplanten physischen Angriffen.[27] Das Ziel von physischen Sicherheitsmaßnahmen ist es, einen Angreifer durch unterschiedlichste Maßnahmen wie Protektion, Detektion und Intervention davon abzuhalten, sein Ziel zu erreichen, sowie gleichermaßen resiliente Strukturen zu schaffen, welche die Konsequenzen erfolgreicher Angriffe mindern können.[28]

Der Risikobegriff in der (physischen) Sicherheit ist definiert als:

$$Risiko = Bedrohung \times Vulnerabilität \times Auswirkung. \quad (1)$$

Diese Definition stellt eine quantitative Beziehung her, die die Auswirkungen eines Angriffs sowie die Eintrittswahrscheinlichkeiten von Bedrohungsszenarien mit der Vulnerabilität, also der Wahrscheinlichkeit, dass ein aus dem Bedrohungsszenario resultierender Angriff Erfolg haben könnte, kombiniert. Über die Vulnerabilität lässt sich somit die Wirkung von Sicherheitsmaßnahmen abbilden, die die Wahrscheinlichkeit erfolgreicher Angriffe vermindern. Die dargestellte Definition des Risikobegriffs erleichtert die Herleitung und Definition akzeptabler Risiken und notwendiger Maßnahmen zur Risikominimierung.[29] Unsicherheiten mit Bezug zu den drei Risikofaktoren sollten sorgfältig betrachtet werden.[30]

Es wurden bereits einige Ansätze zur Risikobewertung entwickelt; diese lassen sich unterscheiden in qualitative, quantitative und hybride Methoden.[31] Qualitative Methoden basieren in der Regel auf Expertenwissen, während quantitative Methoden diskrete Wahrscheinlichkeiten zur Beschreibung der Parameter verwenden. Erstere sind aufgrund ihrer einfachen Nutzung weit verbreitet, wobei der Rückgriff auf Expertenwissen gleichermaßen auch zu ungenauen oder sogar falschen Ergebnissen führen kann.[32] Darüber hinaus wurden quantitative Methoden zur Kosten-Nutzen-Analyse entwickelt. In der Regel berücksichtigen Kosten-Nutzen-Analysen von Sicherheitsmaßnahmen potenzielle finanzielle Verluste als Folge eines erfolgreichen Angriffs, die Eintrittswahrscheinlichkeit verschiedener Angriffsszenarien sowie die Vulnerabilität der Infrastruktur.[33] Hierbei können exakte Ergebnisse berechnet werden, die jedoch zum einen Unsicherheiten nicht berücksichtigen und zum anderen gleichzeitig die Komplexität der Berechnung erhöhen.[34]

20 | Vgl. ICAO 2015.
21 | Vgl. Morgeson et al. 2011, Solano 2010.
22 | Vgl. Tamasi/Demichela 2011.
23 | Vgl. Garcia 2008.
24 | Vgl. White et al. 2014.
25 | Vgl. Beyerer/Geisler 2018.
26 | Vgl. Harnser Group 2010.
27 | Vgl. Beyerer et al. 2010.
28 | Vgl. Garcia 2008.
29 | Vgl. Broder/Tucker 2012.
30 | Vgl. Campbell/Stamp 2004.
31 | Vgl. Meritt 2008.
32 | Vgl. Landoll 2011.
33 | Vgl. Flammini et al. 2009.
34 | Vgl. Landoll 2011.

3 Vulnerabilitätsanalyse

Die quantitative Vulnerabilitätsanalyse als Teil der quantitativen Risikoanalyse basiert im Wesentlichen auf Methoden der Zuverlässigkeits- und allgemeinen Risikoanalyse. Bisher entwickelte Ansätze zur Vulnerabilitätsanalyse sind abhängig von definierten Angriffsszenarien.[35] Diese Abhängigkeit wirkt sich nachteilig auf eine umfassende Analyse aus, da das Wissen über das mögliche Verhalten eines potenziellen Angreifers als unzureichend angesehen werden muss.[36] Die bestehenden Modellansätze lassen sich differenzieren in vorwiegend analytische, aber auch formale Methoden. Eine Übersicht über bestehende Modelle findet sich bei Nicol et al.[37] Analytische Methoden basieren häufig auf sogenannten Angriffsbäumen, die eine Weiterentwicklung der aus der Zuverlässigkeitsanalyse bekannten Fehlerbäume darstellen. Eingeführt wurden Angriffsbäume ursprünglich durch Schneier,[38] um Analysen im Bereich der IT-Sicherheit durchführen zu können. Seitdem erfuhren sie eine rasche Fortentwicklung durch diverse Autorinnen und Autoren, zusammenfassend zu finden zum Beispiel bei Vintr et al.[39]

Eine weitere Entwicklung besteht in der Überführung von Angriffsbäumen in Bayes'sche Netzwerke, um die Zeitabhängigkeit erfolgreicher Angriffe berücksichtigen zu können.[40] Über bedingte Wahrscheinlichkeiten kann dann in Bayes'schen Netzwerken die Vulnerabilität von Infrastrukturen ermittelt werden.

Contini et al. entwickelten Modelle inkohärenter Angriffspfade, um das dynamische Verhalten des betrachteten Systems darzustellen.[41] Zusätzlich werden in diesem Ansatz einfache Wahrscheinlichkeitsverteilungen für die Protektionseigenschaften in die Angriffspfade integriert, um die chronologische Reihenfolge der Angriffe zu untersuchen. Dies ermöglicht die Analyse der Interventionsfähigkeit innerhalb der betrachteten Infrastruktur, indem die Wahrscheinlichkeiten für Restprotektion und Systemreaktion (Intervention) verglichen werden können.[42]

Garcia beschreibt diese Relation, indem mögliche potenzielle Angriffspfade als Teil der verschiedenen Angriffsszenarien und entsprechenden Barrieren genutzt werden.[43] Das Modell ist zeitbasiert und führt den kritischen Detektionszeitpunkt ein, der eine Voraussetzung für die erfolgreiche Intervention darstellt. Ein weiterer hybrider Ansatz, der insbesondere auf der Beschreibung von Garcia basiert, wird von Landucci et al.[44] vorgeschlagen. Dort werden zusätzlich zur quantitativen Betrachtung qualitative Bewertungen miteinbezogen und mit diskreten Wahrscheinlichkeitsintervallen quantifiziert.

Zusammenfassend zeigt sich, dass die Berücksichtigung von Unsicherheiten in den systemischen Parametern sowie im Systemverhalten insgesamt mithilfe bisher existierender Ansätze zur analytischen Modellierung kaum möglich ist. Hinzu kommt, dass eine szenarioübergreifende Analyse gesamter Infrastrukturen bisher kaum möglich ist, da die Analyse jeweils von spezifischen Szenarien abhängt.

4 Ansatz

Nachfolgend wird der neue analytische Modellierungsansatz eingeführt. Er basiert auf den von Contini et al. und Garcia getroffenen Annahmen und wendet Wahrscheinlichkeitsdichtefunktionen (pdf) an, um die spezifischen Eigenschaften der Komponenten eines Sicherungssystems für Protektion, Detektion und Intervention zu beschreiben. Der Parameter Observation wird hier neu eingeführt, um die Systembeschreibung auf die technischen Fähigkeiten der Einzelelemente zu beziehen: Detektion wird dann betrachtet als Ergebnis der Wirkung von Protektions- und Observationselementen. Somit wird die Entdeckung (Detektion) eines Angriffs durch Observation ein zeitabhängiger Prozess. Durch die Beschreibung der Schutzwirkung des Sicherungssystems auf Basis der technischen Eigenschaften seiner Elemente wird es möglich, zu einer szenarioübergreifenden Sicht auf das gesamte Sicherungssystem einer Infrastruktur zu gelangen respektive Vulnerabilität szenarioübergreifend zu bestimmen.

In einem ersten Schritt werden vier Grundannahmen über das Systemverhalten und die wechselseitigen Beziehungen der jeweiligen Systemkomponenten zueinander getroffen. Diesen Annahmen folgend wird ein Modell abgeleitet, welches – basierend auf pdf – eine Analyse möglicher Angriffspfade und ihrer Vulnerabilität erlaubt.

35 | Vgl. French/Gootzit 2011.
36 | Vgl. Cox Jr. 2009.
37 | Vgl. Nicol et al. 2004.
38 | Vgl. Schneier 1999.
39 | Vgl. Vintr et al. 2012.
40 | Vgl. Fakhravar et al. 2017.
41 | Vgl. Contini et al. 2008.
42 | Vgl. Contini et al. 2012.
43 | Vgl. Garcia 2008.
44 | Vgl. Landucci et al. 2017.

4.1 Grundannahmen

Das im Fokus stehende Verhalten des Sicherungssystems einer betrachteten Infrastruktur lässt sich durch vier grundlegende Annahmen zu Abhängigkeiten und Beziehung der Systemkomponenten zueinander charakterisieren:

1. Der schwächste Angriffspfad der Infrastruktur definiert deren Vulnerabilität, da der vom Angreifer ausgewählte Pfad unbekannt ist.
2. Die Kombination aus Protektion und Observation an einer Barriere ist unerlässlich, da ein potenzieller Angreifer ohne eine Möglichkeit zur Erkennung (Detektion) des Angriffs beliebig viel Zeit hat, eine Barriere zu überwinden.
3. Die Detektion eines Angriffs ist nur möglich, wenn Protektionselemente einen Angriff so lange verzögern können, dass die Observation zu einer Detektion führt.
4. Nach erfolgter Detektion kann ein Angriff nur gestoppt werden, wenn die verbleibende Verzögerung durch Protektionselemente entlang der verbleibenden Angriffspfade den Angreifer hinreichend lange aufhält, sodass eine Intervention vollständig erfolgt ist, bevor der Angreifer das Asset erreicht.

4.2 Modellierung der Angriffspfade

Mithilfe dieser Überlegungen, ergänzt durch die topologischen Beziehungen einer definierten Infrastruktur, lässt sich die Schutzwirkung eines Sicherungssystems modellieren. Der ersten Annahme folgend, müssen alle Angriffspfade eines Objekts berücksichtigt werden, da der zunächst unbekannte schwächste Pfad die Vulnerabilität des betrachteten Objekts definiert. So werden alle möglichen Angriffspfade einer Infrastruktur in ein pfadbasiertes Modell extrahiert.

Abbildung 1 zeigt das Ergebnis einer generischen Modellierung. In einem zweiten Schritt wird das Modell der einzelnen Angriffspfade, die sich aus dem topologischen Modell extrahieren lassen, detaillierter ausgeführt (Abbildung 1). In Übereinstimmung mit der zweiten Annahme umfasst das detaillierte Modell der Angriffspfade sowohl Elemente der Protektion als auch der Observation, die die Barrieren des Modells bilden.

Zusätzlich wird eine Option zur Intervention an jeder Barriere im Modell berücksichtigt, da diese in direkter Abhängigkeit zur Interaktion zwischen Elementen der Protektion und Observation steht. Alle Angriffspfade lassen sich dann, wie beispielhaft in Abbildung 2 gezeigt, weiter detaillieren. Das detaillierte Modell repräsentiert die verschiedenen Systemkomponenten an den betrachteten Barrieren.

4.3 Probabilistische Analyse

Die dritte Annahme impliziert, dass eine Detektion des Angreifers an einer Barriere nur bei hinreichend langem Aufenthalt des Angreifers im Observationsbereich möglich ist, sodass mit zunehmender Überwindungszeit (Protektionszeit t_p) das Erreichen der Observationszeit t_o und damit die Detektion an der Barriere

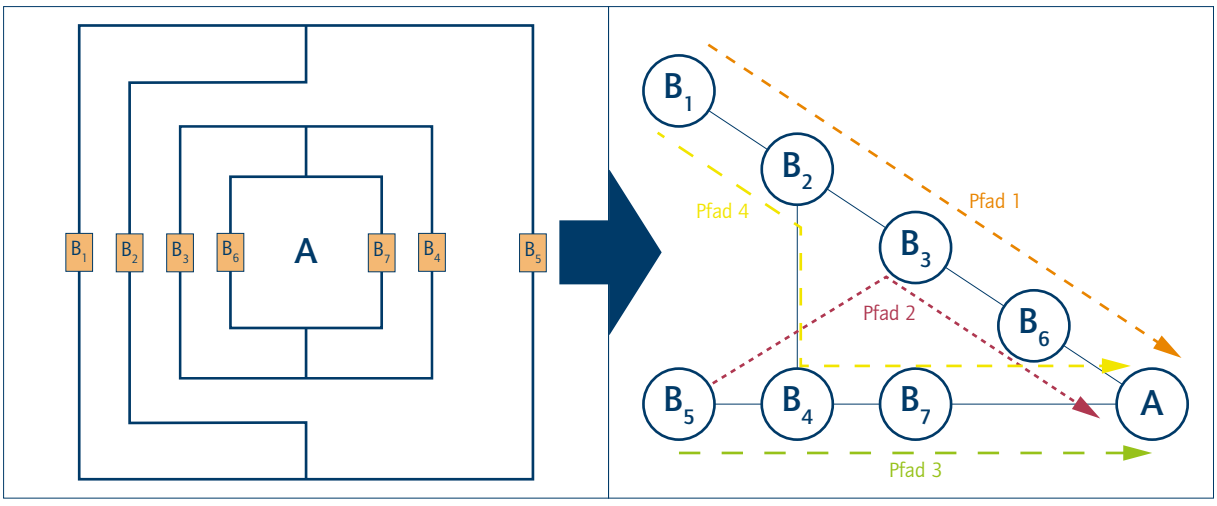


Abbildung 1: Topologisches Modell eines Beispielsystems (Quelle: eigene Darstellung)

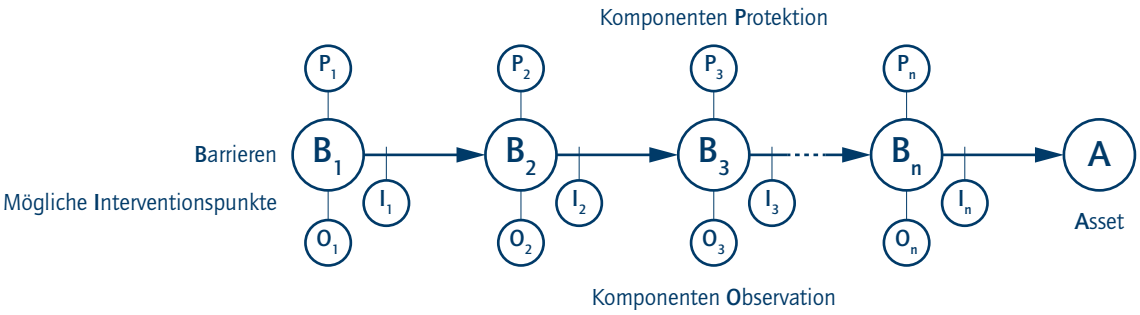


Abbildung 2: Detaillierter Angriffspfad 1 des Beispielsystems (Quelle: eigene Darstellung)

eintritt. Die bedingte Wahrscheinlichkeit für Detektion D ist bestimmt durch:

$$D = P\,(t_p > t_o). \tag{2}$$

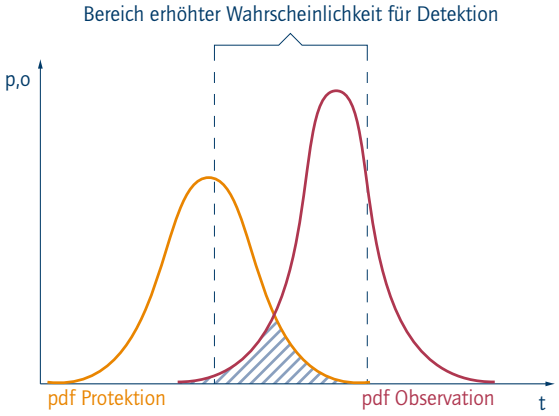


Abbildung 3: Detektion (Quelle: eigene Darstellung)

Abbildung 3 beschreibt schematisch die Relation zwischen Observation und Protektion für die Zeit eines Angriffs *t*. Die pdf für Detektion resultiert aus dem Bereich, in dem sich die Detektion potenziell ereignen kann. Die daraus resultierende kumulierte Verteilungsfunktion (cpdf) D(t) lässt sich als die technische Möglichkeit zur Detektion eines Angriffs interpretieren, die sich aus dem Zusammenspiel zwischen Protektions- und Observationseinrichtungen ergibt. Hinsichtlich der Eintrittswahrscheinlichkeit bedeutet dies:

$$D(t) = \int_0^t o(t_o) \cdot [\int_{t_o}^{\infty} p(\tau) d\tau] dt_o. \tag{3}$$

4.4 Rechtzeitige Intervention bei Angriffspfaden

Die vierte grundsätzliche Annahme wird durch die Einführung der rechtzeitigen Intervention auf einem Angriffspfad berücksichtigt. Die Intervention kann durch eine pdf beschrieben werden, die die Verteilung der Interventionszeiten wiedergibt.

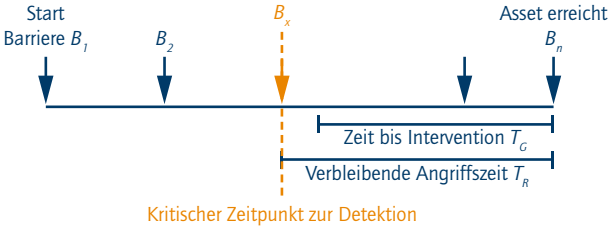


Abbildung 4: Kritischer Detektionszeitpunkt (Quelle: eigene Darstellung)

Wie von Garcia vorgeschlagen, muss für eine rechtzeitige Intervention die hierfür benötigte Interventionszeit t_I kürzer sein als die Zeit, die der Angreifer für die Überwindung des Restschutzes auf dem betrachteten Angriffspfad benötigt (siehe Abbildung 4).[45] Die daraus resultierende vereinfachte Relation an einer Barriere B_x auf dem Angriffspfad mit n Barrieren kann wie folgt beschrieben werden:

$$t_I < \sum_{x+1}^{n} t_{p,i}. \tag{4}$$

Entsprechend Contini et al. folgt aus der Beschreibung der Parameter durch pdf, dass die rechtzeitige Intervention die bedingte Wahrscheinlichkeit von benötigter Interventionszeit t_i und verbleibender Protektion auf dem Pfad t_x ist.[46]

$$T = P(t_x > t_I). \tag{5}$$

45 | Vgl. Garcia 2008.
46 | Vgl. Contini et al. 2012.

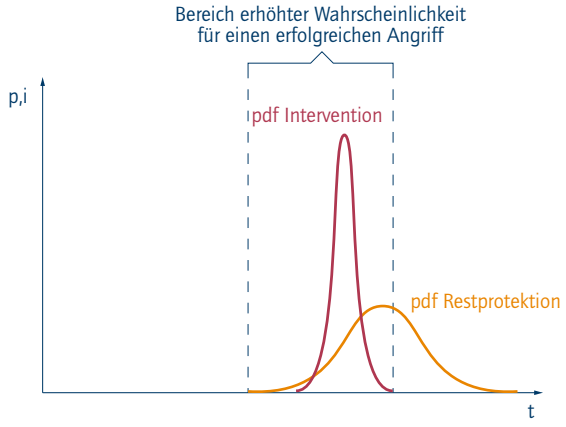


Abbildung 5: Rechtzeitige Intervention (Quelle: eigene Darstellung)

In Abbildung 5 wird der von Contini et al. beschriebene Zusammenhang illustriert. Die dort dargestellte pdf der Restprotektion kann durch eine Faltung der Protektionsdichten der verbleibenden Barrieren auf dem Angriffspfad berechnet werden. Für Barriere B_x auf dem Angriffspfad lässt sich definieren:

$$p_{Pfad,x}(t) = p_{x+1}(t) * \ldots * p_n(t). \quad (6)$$

Die kumulierte bedingte Wahrscheinlichkeit für eine rechtzeitige Intervention T(t) lässt sich also ableiten, indem man die pdf für Intervention und Restprotektion verknüpft:

$$T(t) = \int_0^t i(t_I) \cdot [\int_t^\infty p_{Pfad,x}(\tau) d\tau] dt_I. \quad (7)$$

Die Detektionswahrscheinlichkeit D_i und die Gesamtwahrscheinlichkeit einer rechtzeitigen Intervention T_i können dann zur Berechnung der Vulnerabilität jeder Barriere V_i kombiniert und die beiden Faktoren als kumulierte Wahrscheinlichkeiten für $t \to \infty$ betrachtet werden. Auf diese Weise werden alle Möglichkeiten einer detektierten Überwindung einer Barriere sowie einer nachfolgenden rechtzeitigen Intervention berücksichtigt. Die Stärke einer Barriere S_i wird beschrieben als die Wahrscheinlichkeit, den Angreifer durch Detektion und rechtzeitige Intervention davon abzuhalten, das angestrebte Asset zu erreichen. Die Vulnerabilität ist dann das Komplement der Stärke:

$$V_i = 1 - S_i = 1 - D_i \cdot T_i. \quad (8)$$

Da sich die verbliebene Protektionszeit an den Barrieren entlang des Angriffspfades verringert, reduziert sich gleichzeitig die absolute Detektionsrate eines Angriffspfades. Dies spiegelt sich in der seriellen Verbindung der Barrieren entlang eines Angriffspfades wider und führt zur Berechnung der Vulnerabilität.

$$V_{Pfad,j} = \prod_{i=1}^{n} V_i. \quad (9)$$

Die daraus resultierende Pfadvulnerabilität lässt sich auf alle Angriffspfade innerhalb eines Objekts anwenden.

5 Beispiel

Der vorgestellte analytische Ansatz zur Vulnerabilitätsanalyse wird auf den Teilbereich einer zivilen Flughafeninfrastruktur angewandt. Zum Verständnis der Topologie und der Barrierenelemente werden zunächst die generelle Struktur sowie Schlüsselbereiche näher erläutert. Zusätzlich wird ein Überblick über vorhandene Sicherungseinrichtungen und deren Charakteristika im Sinne des präsentierten Modellierungsansatzes gegeben.

Nachfolgend wird der eingeführte Ansatz zur Vulnerabilitätsanalyse auf einen möglichen Angriffspfad innerhalb der Flughafeninfrastruktur angewandt. Die Ergebnisse für alle Angriffspfade werden dann detailliert präsentiert, um mögliche Implikationen und die generelle Konsistenz der Ergebnisse zu diskutieren.

5.1 Flughafenstruktur und Szenario

Üblicherweise besteht ein Flughafen aus einer Land- und einer Luftseite, wobei verschiedenste Bereiche geschützt werden müssen.

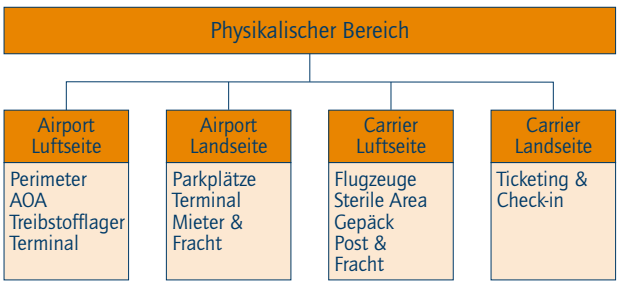


Abbildung 6: Allgemein übliche physische Bereiche von Zivilflughäfen (Quelle: Tamasi/Demichela 2011)

In Abbildung 6 sind die wichtigsten physischen Bereiche eines zivilen Flughafens zusammengefasst. Die Landseite ist zugänglich für die Öffentlichkeit, während nur Passagiere und autorisiertes Personal auf der Luftseite zugelassen sind. Die Luftseite beginnt nach dem Sicherheitscheck und wird als „priorisierter Sicherheitsbereich" (Priority Security Area)[47] bezeichnet.

Der Terminalbereich, der in diesem Artikel betrachtet wird, besteht sowohl aus einer Land- als auch aus einer Luftseite. Ein kleiner Teil ist zusätzlich als besondere Sicherheitszone (Security Restricted Area) deklariert, für die sich autorisiertes Personal einem zusätzlichen Hintergrundcheck und einer speziellen Zugangskontrolle unterziehen muss. Die Prüfung des Handgepäcks ist obligatorisch für alle Passagiere.

Abbildung 7 gibt einen Überblick über die analysierten Bereiche der Flughafeninfrastruktur. Sie umfasst das Terminal, Fracht- und Personalbereiche sowie das Flugfeld und den Perimeterschutz des Flughafens. Die besondere Sicherheitszone der Luftseite sowie das Gate sind hellgrau gekennzeichnet. Die unterschiedlichen Barrieren beziehungsweise Sicherheitsmaßnahmen an den Ein- und Ausgängen der spezifizierten Bereiche sind in Tabelle 1 ausgewiesen und aufgelistet:

Barriere	Beschreibung
1	Öffentlicher Eingang/Check-in
2a	Personal-/Mitarbeitereingang
2b	Durchgang Mitarbeiter
2c	Durchgang Mitarbeiter
3	Security Check/Kontrolle Handgepäck
4	Grenzkontrolle
5a	Boarding-Kontrolle
5b	Boarding-Kontrolle
6	Freight-/Cargo-Eingang
7	Zugang Fracht zum Flugfeld
8	Perimeterzaun
9	Patrouille Flugfeld

Tabelle 1: Sicherheitsmaßnahmen der spezifizierten Bereiche (Quelle: eigene Darstellung)

Die technischen Merkmale werden durch die pdf der Parameter Protektions-, Observations- und Interventionszeit beschrieben. Es werden normalverteilte Wahrscheinlichkeitsdichtefunktionen (npdf) ausgewählt, um das Beispiel zu erläutern. Die fiktiven, aber nach unserer Ansicht möglichen charakteristischen Werte für mittlere Abweichungen μ und Standardabweichungen σ sind in Tabelle 2 dargestellt.

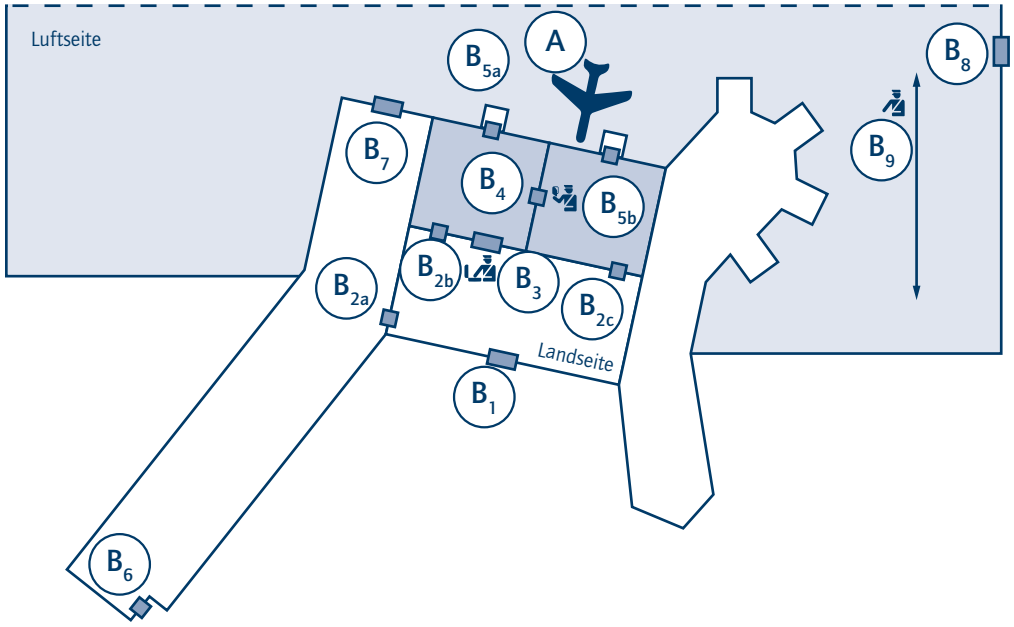


Abbildung 7: Schema der analysierten Flughafeninfrastruktur (Quelle: eigene Darstellung)

47 | Vgl. ICAO 2014.

Barriere	Protektion [s]		Observation [s]		Intervention [s]	
	μ	σ	μ	σ	μ	σ
1	-	-	-	-	-	-
2	120	40	240	60	360	60
3	120	20	90	10	30	5
4	60	20	30	10	30	5
5	60	20	120	30	180	30
6	150	30	240	60	600	120
7	360	60	180	60	360	60
8	600	120	180	60	300	60
9	240	30	300	20	30	5

Tabelle 2: Charakteristische Werte für Sicherheitsmaßnahmen in Sekunden (Quelle: eigene Darstellung)

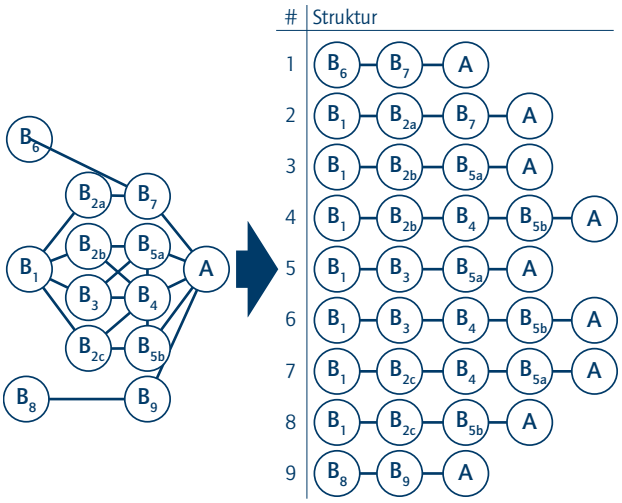


Abbildung 8: System der möglichen Angriffspfade und extrahierte Pfade (Quelle: eigene Darstellung)

5.2 Vulnerabilitätsanalyse für Flughafeninfrastrukturen

Die Analyse beginnt mit der Modellierung der topologischen und physischen Relationen der Flughafenstrukturen. Aus diesem Grund werden alle möglichen Angriffspfade der Infrastruktur in ein pfadbasiertes Modell extrahiert.

Das aus der Extraktion hervorgehende Modell und alle Einzelpfade sind in Abbildung 8 dargestellt. Die betrachtete Struktur enthält insgesamt neun Angriffspfade, wobei deren Länge variiert (zwei bis vier sicherheitsrelevante Barrieren). Die extrahierten Angriffspfade werden weiter detailliert, indem die verschiedenen Elemente der Protektion und Observation sowie die möglichen Zeitpunkte der Intervention der betrachteten Barrieren abgebildet werden.

Beispielhaft zeigt Abbildung 9 das Resultat für Angriffspfad 4. Der im Detail modellierte Angriffspfad ermöglicht es nun, die in Kapitel 3.3 vorgestellte probabilistische Bewertung durchzuführen. Für den ausgewählten Pfad 4 der Flughafeninfrastruktur erhält man folgende Pfadvulnerabilität:

$$V_{pfad,4} = V_1 \cdot V_{2b} \cdot V_4 \cdot V_{5b} = 0{,}101. \tag{10}$$

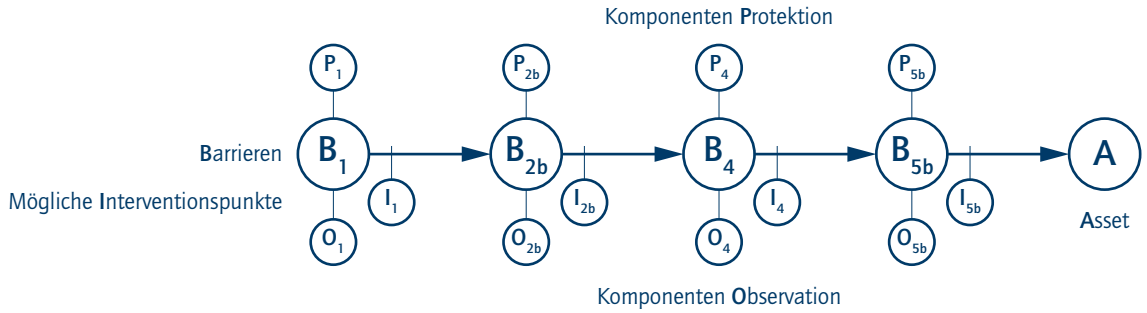


Abbildung 9: Detailliertes Angriffspfadmodell für Pfad 4 (Quelle: eigene Darstellung)

Pfad	1	2	3	4	5	6	7	8	9
V_{pfad}	0,496	0,488	0,999	0,101	0,09	0,009	0,101	0,999	0,001

Tabelle 3: Detaillierte Vulnerabilitäten der bewerteten Angriffspfade (Quelle: eigene Darstellung)

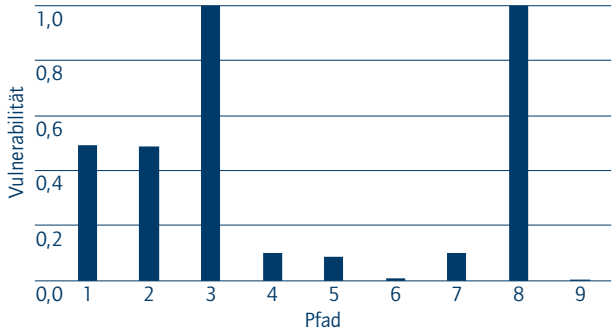


Abbildung 10: Darstellung der Vulnerabilität aller Pfade (Quelle: eigene Darstellung)

Die Ergebnisse für alle Pfade sind in Tabelle 3 zusammengefasst; Abbildung 10 stellt den unterschiedlichen Grad der Vulnerabilität dar. Es zeigt sich, dass die Angriffspfade 3 und 8 die schwächsten Pfade der betrachteten Infrastruktur darstellen, da sie nahezu keinen Schutz gegen mögliche Angriffe aufweisen. Im Gegensatz dazu ist Pfad 9, der am Perimeter beginnt und durch das Flugfeld direkt zum potenziellen Angriffsziel führt, der am wenigsten vulnerable Pfad der Infrastruktur bei der ausgewählten Konfiguration des Sicherungssystems. Offensichtlich sind die Ergebnisse der Vulnerabilität von Angriffspfaden hier insbesondere von zwei Eigenschaften der modellierten Infrastruktur mit dem betrachteten Sicherungssystem abhängig.

Einerseits hängt die Vulnerabilität von der Güte der eingesetzten Sicherungsmaßnahmen ab – dies zeigt Pfad 9, der nur aus zwei Barrieren besteht, aber der stärkste Pfad des Systems ist. Das hohe Schutzniveau des Perimeters und eine zusätzliche Patrouille sichern eine schnelle Intervention, um einen Angreifer zu stoppen. Der Vergleich der nahezu identischen Pfade 3, 5 und 8 (siehe Abschnitt 4.1) zeigt ein ähnliches Ergebnis: In diesem Fall ist die nur in Pfad 5 enthaltene Hochsicherheitsbarriere der Untersuchung des Handgepäcks (B_3) der einzig relevante Unterschied, der jedoch zu einer signifikant niedrigeren Vulnerabilität führt.

Andererseits hängt die Vulnerabilität auch von der Länge des Angriffspfades ab. Angriffspfade, die Barrieren mit einem vergleichbaren Niveau von Sicherheitsmaßnahmen aufweisen, sind verwundbarer, wenn das Asset mit der Überwindung einer geringeren Anzahl von Barrieren erreicht werden kann. Diese Eigenschaft wird bei einem Vergleich der Vulnerabilität der Pfade 4, 6 und 7, die vier Barrieren enthalten, mit den „kürzeren" Pfaden 2, 3 und 8 deutlich. Die kürzeren Pfade mit einer kleineren Anzahl Barrieren zeigen eine höhere Vulnerabilität, da eine rechtzeitige Intervention für diese Pfade weniger wahrscheinlich ist.

Die beschriebenen Modelleigenschaften zeigen, dass die Grundannahmen zur Wirkung eines Sicherungssystems im hier präsentierten Modellansatz berücksichtigt werden. Wichtigste Faktoren sind die Wahrscheinlichkeit, einen Angriff mithilfe entsprechend ausreichenden Sicherheitsmaßnahmen zu detektieren, sowie die nach erfolgter Detektion verbleibende Protektion auf dem betrachteten Pfad, die eine rechtzeitige Intervention ermöglicht.

6 Fazit

Der Artikel beschreibt Entwicklungen im Bereich der Richtlinien für die Flughafensicherheit und zeigt die damit einhergehende Notwendigkeit für Risikoanalysen im Bereich der Security für zivile Flughafeninfrastrukturen auf. Durch Beschreibung des aktuellen Stands der Technik werden Unzulänglichkeiten in der gegenwärtigen Analyse der physischen Sicherheit und Vulnerabilität von Flughäfen aufgedeckt. Es wird deutlich, dass insbesondere die Berücksichtigung bestehender Unsicherheiten in der Analyse bisher schwierig ist. Hiervon ausgehend beschreibt der Beitrag einen analytischen Modellansatz, der auf der probabilistischen Beschreibung der charakteristischen Parameter Protektion, Observation und Intervention sowie dem Prinzip des schwächsten Pfades basiert.

Der Ansatz wird auf Basis von vier Grundannahmen weiter detailliert. Die Herleitung des Modells beginnt mit einer Beschreibung der topologischen Beziehungen von Sicherungssystemen innerhalb einer Infrastruktur. Im Anschluss daran werden individuelle Angriffspfade im Detail entwickelt und beschrieben, wobei die grundlegenden Parameter an jeder einzelnen Barriere kombiniert werden. Darauf folgen eine Beschreibung der möglichen Detektion sowie in einem letzten Schritt die Herleitung der probabilistischen Relation für eine rechtzeitige Intervention.

Der vorgelegte Ansatz wird auf eine zivile Flughafeninfrastruktur angewendet; aus diesem Grund werden der hier betrachtete Teil eines fiktiven zivilen Flughafens präsentiert sowie die Objektstruktur und das vorhandene Sicherungssystem skizziert. Anschließend erfolgt die Vulnerabilitätsbewertung der Infrastruktur.

Der vorgeschlagene analytische Ansatz zeigt, dass die Modellierung von Vulnerabilität anhand von probabilistischen Methoden eine Betrachtung der Unsicherheiten in der Bewertung erlaubt. Des Weiteren ermöglicht der Ansatz eine szenarioübergreifende Systemanalyse im Sinne der Reduktion der Beschreibung des Sicherungssystems auf systemimmanente Parameter der Barrieren, sodass – zum Beispiel unter Anwendung des Prinzips des

schwächsten Pfades – eine Evaluation der gesamten Infrastruktur möglich wird. Darüber hinaus bietet dieses Modell die Möglichkeit einer Optimierung der Vulnerabilität, worauf sich zukünftige Forschungsarbeiten fokussieren werden.

Gleichwohl sollte der dargestellte Ansatz für eine weitere Anwendung noch ausgebaut werden. An dieser Stelle kann eine Überführung des Modellansatzes in eine formale Beschreibung, beispielsweise hybride oder zeitbasierte Bayes'sche Netzwerke, zielführend sein. Diese ermöglichen eine übersichtliche Darstellung der Systemstrukturen und vereinfachen die Berechnung. Zudem kann diese Darstellung Ausgangspunkt für Kosten-Nutzen-Betrachtungen und Optimierungen sein.

Da die Bestimmung der in das Modell einfließenden Parameter Protektion, Observation und Intervention bisher noch nicht Gegenstand weiterer Forschungsarbeit war, muss diese noch detaillierter betrachtet werden. Aus diesem Grund sollte eine Analyse der beeinflussenden Faktoren und ihrer Zusammensetzung erfolgen. Die Abhängigkeit zwischen Vulnerabilität und Angreifertypus beziehungsweise Bedrohungswahrscheinlichkeit sollte näher analysiert werden, wobei die prinzipiell uneingeschränkte Form der Dichtefunktionen, welche oben genannte Parameter beschreiben, eine Modellierung von Wechselwirkungen grundsätzlich zulässt. Darüber hinaus bedarf es weiterer Evaluierung zur Überprüfung der Modellkonsistenz und des Einflusses von Unsicherheiten; hier bietet sich möglicherweise die varianzbasierte Sensitivitätsanalyse an, um zu einem tieferen Verständnis des Modellverhaltens zu gelangen. Nach erfolgreicher Evaluierung könnte der präsentierte Ansatz die Basis für eine Optimierung der Vulnerabilität unter Sachzwängen wie zum Beispiel Kostenrestriktionen darstellen.

Literatur

Arens/Kühne 2018
Arens, U./Kühne, U.: „Schutz und Sicherheit in Offshore-Windparks". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Associated Press 2016
Associated Press: *Airport Security,* 2016. URL: http://data.ap.org/projects/2015/airport-security/ [Stand: 21.08.2017].

Bertsche et al. 2018
Bertsche, B./Beyerer, J./Goldschmidt, R./Jakobs, E. M./Renn, O./Schlüter, N./Winzer, P./Weyer, J.: „Integrative Theorie der Verlässlichkeit (iTV) für soziotechnische Systeme (STS)". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Beyerer et al. 2010
Beyerer, J./Geisler, J./Dahlem, A./Winzer, P.: „Sicherheit: Systemanalyse und Design". In: *Sicherheitsforschung – Chancen und Perspektiven*, Berlin: Springer Verlag 2010.

Beyerer/Geisler 2016
Beyerer, J./Geisler, J.: „A Framework for a Uniform Quantitative Description of Risk with Respect to Safety and Security". In: *European Journal for Security Research*, October 2016, 1: 2, S. 135–150, Springer 2016.

Beyerer/Geisler 2018
Geisler, J./Beyerer, J.: „Formaler Rahmen für eine einheitliche quantitative Beschreibung des Risikos bezüglich Safety und Security". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Broder/Tucker 2012
Broder, J. F./Tucker, E.: *Risk Analysis and the Security Survey*, 4. Auflage, Waltham: Butterworth-Heinemann 2012.

Campbell/Stamp 2004
Campbell, P. L./Stamp J. E.: *A Classification Scheme for Risk Assessment Methods*, Albuquerque: Sandia National Laboratories 2004.

Contini et al. 2008
Contini, S./Cojazzi, G. G. M./Renda, G.: „On the Use of Non-Coherent Fault Trees in Safety and Security Studies". In: *Reliability Engineering and System Safety,* 93: 12, 2008, S. 1886–1895.

Contini et al. 2012
Contini, S./Fabbri, L./Matuzas, V./Cojazzi, G.: „Protection of Multiple Assets to Intentional Attacks. A Methodological Framework". In: *11th Probalistic Safety Assessment 2012, Proc. Intern. Conf.*, Helsinki 2012.

Cox Jr. 2009
Cox Jr., L. A.: *Risk Analysis of Complex and Uncertain Systems*, New York: Springer 2009.

Deutschmann/Milbredt 2018
Deutschmann, A./Milbredt, O.: „Globale Bewertung des Sicherheitsniveaus von kritischen Infrastrukturen am Beispiel von Verkehrsflughäfen". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Fakhravar et al. 2017
Fakhravar, D./Cozzani, V./Kahkzad, N./Reniers, G.: „Security Vulnerability Assessment of Gas Pipeline Using Bayesian Network". In: Cepin/Bris (Hrsg.): *ESREL 2017: Safety and Reliability – Theory and Applications*, London: Taylor & Francis Group 2017, S. 1171–1180.

Flammini et al. 2009
Flammini, F./Gaglione, A./Mazzocca, N./Pragliola, C.: „Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures". In: *Critical Information Infrastructure Security*, Berlin: Springer 2009.

French/Gootzit 2011
French, G. S./Gootzit, D.: „Defining and Assessing Vulnerability of Infrastructure to Terrorist Attack". In: *Vulnerability, Uncertainty and Risk: Analysis, Modeling and Management, Proc. Conf.*, Hyattsville 2011.

Garcia 2008
Garcia, M. L.: *The Design and Evaluation of Physical Protection Systems*, 2. Auflage, Burlington: Butterworth-Heinemann 2008.

Giannopoulus et al. 2012
Giannopoulos, G./Filippini, R./Schimmer, M.: „Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A state of the art". In: *JRC Technical Notes*, Luxembourg: Publications Office of the European Union 2012.

Harnser Group 2010
Harnser Group (Hrsg.): *A Reference Security Management Plan for Energy Infrastructure*, Brussels: European Commission 2010.

ICAO 2014
ICAO (Hrsg.): *Annex 17, Security – Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Montréal: International Civil Aviation Organization 2014.

ICAO 2015
ICAO (Hrsg.): *DOC 8973 – Aviation Security Manual*, 9. Auflage, Montréal: International Civil Aviation Organization 2015.

Labudde 2018
Labudde, D.: „Sicherheit ist die Abwesenheit von Kriminalität – eine Hypothese". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Landoll 2011
Landoll, D. J.: *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, 2. Auflage, Boca Raton: CRC Press 2011.

Landucci et al. 2017
Landucci, G./Argenti, F./Cozzani, V./Reniers, G.: „Quantitative Performance Assessment of Physical Security Barriers for Chemical Facilities". In: Cepin/Bris (Hrsg.): *ESREL 2017: Safety and Reliability – Theory and Applications*, London: Taylor & Francis Group 2017, S. 1279–1287.

McGill et al. 2007
McGill, W. L./Ayyub, B. M./Kaminskiy, M.: „Risk Analysis for Critical Asset Protection". In: *Risk Analysis*, 27: 5, 2007, S. 1265–1281.

Meritt 2008
Meritt, J. W.: „A Method for Quantitative Risk Analysis". In: *22nd National Information Systems Security Conference, Proc. Nat. Conf.*, Arlington 2008.

Morgeson et al. 2011
Morgeson, J. D./Brooks, P. S./Disraelly, D. S./Erb, J. L./Neiman, M. L./Picard, W. C.: „Doctrinal Guidelines for Quantitative Vulnerability Assessments of Infrastructure-Related Risks". In: *Volume I. Alexandria: Institute for Defense Analyses*, Alexandria 2011.

Nicol et al. 2004
Nicol, D. M./Sanders, W. H./Trivedi, K. S.: „Model-Based Evaluation: From Dependability to Security". In: *IEEE Transactions on Dependable and Secure Computing*, 1: 1, 2004, S. 48–65.

Raabe 2018
Raabe, O.: „Datenschutz- und IT-sicherheitsrechtliche Risikomodelle". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Schneier 1999
Schneier, B.: „Attack Trees". In: *Dr. Dobbs Journal*, 24: 12, 1999, S. 21–29.

Schnieder/Schnieder 2018
Schnieder, E./Schnieder, L.: „Formalisierung von Begriffen der Sicherheit und Sicherheitsmetriken". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Solano 2010
Solano, E.: *Methods for Assessing Vulnerability of Critical Infrastructure*, Institute for Homeland Security Solutions 2010.

Tamasi/Demichela 2011
Tamasi G./Demichela M.: „Risk Assessment Techniques for Civil Aviation Security". In: *RELIABILITY ENGINEERING & SYSTEM SAFETY*, 96, 2011, S. 593–599.

Vieweg 2018
Vieweg, K.: „Sicherheit – Begriffe, Szenarien, Verantwortlichkeiten und Entscheidungsprozesse aus juristischer Sicht." In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Vintr et al. 2012
Vintr, Z./Valis, D./Malach, J.: „Attack Tree-Based Evaluation of Physical Protection Systems Vulnerability". In: *2012 IEEE International Carnahan Conference on Security Technology (ICCST), Proc. Intern. Conf.*, Carnahan 2012.

Weyer et al. 2018
Weyer, J./Adelt, F./Konrad, J./Hoffmann, S.: „Agentenbasierte Simulation des Risikomanagements soziotechnischer Systeme mit dem Simulator SimCo". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

White et al. 2014
White, R./Boult, T./Chow, E.: „A Computational Asset Vulnerability Model for the Strategic Protection of the Critical Infrastructure". In: *International Journal of Critical Infrastructure Protection*, 7: 3, 2014, S. 167–177.

8.2 Globale Bewertung des Sicherheitsniveaus von kritischen Infrastrukturen am Beispiel von Verkehrsflughäfen

Dr. rer. nat. Andreas Deutschmann
Dr. Olaf Milbredt
Institut für Flughafenwesen und Luftverkehr
Deutsches Zentrum für Luft- und Raumfahrt

1 Einleitung

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit großer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.[1] Diese kritischen Infrastrukturen werden aufgrund ihrer technischen, strukturellen und funktionellen Spezifika in unverzichtbare technische Basisinfrastrukturen und unverzichtbare sozioökonomische Dienstleistungsinfrastrukturen eingeteilt.[2] Zu den technischen Basisinfrastrukturen gehören neben der Energieversorgung und den Informations- und Kommunikationstechnologien der Bereich Transport und Verkehr sowie die (Trink-)Wasserversorgung und Abwasserentsorgung. Das Gesundheitswesen und der Bereich Ernährung sowie das Notfall- und Rettungswesen inklusive Katastrophenschutz zählen neben Parlament, Regierung, öffentlicher Verwaltung und Justizeinrichtungen ebenso zu den sozioökonomischen Dienstleistungsinfrastrukturen wie das Finanz- und Versicherungswesen oder die Bereiche Medien und Kulturgüter. Im vorliegenden Beitrag wird eine der unverzichtbaren technischen Basisinfrastrukturen, ein Flughafen, herangezogen, um mit einem Verfahren das globale Sicherheitsniveau bezüglich spezifizierter Leistungskennzahlen (ähnlich den Key Performance Indicators/KPI) zu quantifizieren. Flughäfen sind das verbindende Element zwischen land- und luftseitigem Verkehr und insbesondere für moderne und industriell geprägte Gesellschaften von herausragender Bedeutung. Zum einen sind sie aufgrund ihrer verkehrlichen Brückenfunktion zwischen unterschiedlichen Verkehrsmodi der Garant für Mobilität über große – insbesondere interkontinentale – Distanzen. Zum anderen ermöglichen sie den Transport von hochwertigen Industrie- und produktionsrelevanten Gütern. Dabei ist der zivile Luftverkehr seit seinen Anfängen Ziel von kriminellen und terroristischen Anschlägen.

2 Sicherheit an Flughäfen

2.1 Definition des Begriffs Sicherheit im Luftverkehr

Der Begriff Sicherheit lässt sich grundsätzlich in zwei Kategorien einteilen:

- betriebliche Sicherheit, insbesondere in der Luftfahrt auch als Safety bezeichnet, sowie
- Angriffs- und Manipulationssicherheit, oft auch Security genannt.

Dabei beschreibt der Begriff Sicherheit einen nicht genau quantifizierbaren Zustand eines Systems. Die technische Sicherheit eines Systems, die oft auch als objektive Sicherheit verstanden wird, setzt sich aus der Sicherheit der einzelnen Systemkomponenten zusammen, die in den Ingenieurwissenschaften durch Ausfallwahrscheinlichkeiten determiniert werden. Die Ausfallwahrscheinlichkeit wird dabei in der Einheit „Ausfälle" oder „Störungen" pro Jahr (zum Beispiel 10^{-6} pro Jahr) angegeben. Werte für technische Systeme lassen sich zum Beispiel aus gezielten Materialprüfungen ableiten. Eine weitere Steigerung der technischen Sicherheit wird durch Zertifizierungsprozesse, die von spezialisierten Organisationen ausgeführt werden (zum Beispiel TÜV), erreicht.

Demgegenüber ist der Bereich Security technisch sehr schwer zu erfassen, da Angriffe beziehungsweise Manipulationen an Systemen in der Regel gezielt und mit Vorsatz von Menschen durchgeführt werden und sich so zunächst einer dezidierten mathematischen Beschreibung entziehen. In diesem Zusammenhang wird auch von subjektiver Sicherheit gesprochen, die das ebenfalls nicht quantifizierbare Sicherheitsgefühl von Personen widerspiegelt.

1 | Vgl. BMI 2009, S. 3.
2 | Vgl. ebd.

Grundsätzlich wird in beiden Kategorien ein hohes Maß an Sicherheit geschaffen, wenn sowohl die Eintrittswahrscheinlichkeit P_{Event} für ein Ereignis als auch das Schadensausmaß K_M im Falle einer Störung klein sind.[3] Mathematisch lässt sich dies als Produkt wie folgt darstellen:

$$Sicherheit \sim \frac{1}{P_{Event} K_M} \qquad (1).$$

Dementsprechend sorgen Sicherheitsmaßnahmen technischer, prozessualer und personeller Art dafür, Eintrittswahrscheinlichkeiten und Schadensausmaße zu minimieren. Diese sind, insbesondere für den Bereich der Security, sowohl technisch als auch mathematisch schwer zu beschreiben. Ziel jeder Beschreibung ist es, für beide Terme geeignete Formulierungen zu finden, die es gestatten, beide Größen zu quantifizieren. Ein Ansatz, dies unter Berücksichtigung von insbesondere humanen Einflussfaktoren zu erreichen, wird in der vorliegenden Arbeit vorgestellt.

Darüber hinaus existieren weitere, auf konkrete Bedrohungsszenarien bezogene Sicherheitskategorien, zum Beispiel die kollektive Sicherheit, auf die hier nicht näher eingegangen wird. Die Herausforderung, mit Bedrohungen umzugehen, diese zu verstehen und darauf zu reagieren, betrifft jede einzelne Person, die zunächst für sich selbst einschätzen muss, ob sie das Risiko eingeht, eine technische Einrichtung (zum Beispiel das Auto für die Fahrt zur Arbeit) zu nutzen, oder ob sie die Nähe zu anderen Menschen sucht, hier mit dem Risiko, dass diese Anschläge planen und durchführen. Darüber hinaus hat der Staat beziehungsweise der Gesetzgeber die Aufgabe, die Bevölkerung bestmöglich – wie im folgenden Abschnitt beschrieben – vor Bedrohungen zu schützen.

2.2 Rahmenbedingungen und Vorgehensweisen für die Sicherheit am Flughafen

Sowohl erfolgte Anschläge als auch erfolgreich verhinderte Angriffe auf das System Flughafen führten dazu, dass auf Basis der oben beschriebenen Definition der Sicherheit an Flughäfen schrittweise Sicherheitskontrolltechnologien und offene sowie verdeckte Sicherheitsprozesse etabliert wurden, um einerseits die Wahrscheinlichkeit für das Eintreten eines potenziell gefährlichen Ereignisses zu minimieren, andererseits die Folgen eines nicht verhinderten Anschlags zu reduzieren. Parallel wird aufgrund von Anschlägen auf Terminalgebäude in der jüngeren Vergangenheit damit begonnen, Materialien im Flughafen zu verbauen, die in erster Linie großen Druckwellen, die bei Explosionen entstehen, standhalten und damit verhindern, dass Menschen durch zerborstene Trümmerteile erschlagen werden.

Die Rechtsgrundlage[4], auf der die Einführung von Technologien und Prozessen beruht, wurde sukzessive den sich wandelnden Bedrohungslagen angepasst. Darüber hinaus wurden auf der globalen Ebene durch die ICAO, als übergeordnetes Luftfahrtgremium der Vereinten Nationen, weltweit einheitliche Sicherheitsstandards und Prozesse in Flughäfen, die sowohl den Bereich der Betriebssicherheit (Safety) als auch den der Luftsicherheit (Security) abdecken,[5] definiert, die in jedem Land mit ziviler Luftfahrt einzuhalten sind. Zuwiderhandlungen führen unweigerlich zum Entzug von sogenannten Freiheiten der Luftfahrt. Das bedeutet, dass unsichere Flüge (im Sinne von Safety und/oder Security) nicht im internationalen Rahmen durchgeführt werden dürfen. Diese internationalen Vereinbarungen dienen darüber hinaus als Grundlage für weiterreichende europäische Luftsicherheitsregelungen, die als Basis für das beispielsweise in Deutschland geltende Luftsicherheitsgesetz[6] dienen.

Im Luftsicherheitsgesetz wird geregelt, wie Sicherheit, im Sinne von Security, herzustellen ist. Darüber hinaus wird festgelegt, welche Instanzen für unterschiedliche Sicherheitsprozesse verantwortlich sind und wer für die Umsetzung der Prozesse am Flughafen sorgt. So wird zum Beispiel in § 5 LuftSiG die Passagierkontrolle geregelt. Analog dazu ist in § 8 LuftSiG die Mitarbeiter- und Warenkontrolle beschrieben. Ergänzend werden auf europäischer und nationaler Ebene Durchführungsbestimmungen erlassen, die regeln, welche Gegenstände und Substanzen von welchen Personengruppen an Bord eines Flugzeugs beziehungsweise in den Sicherheitsbereich eines Flughafens eingeführt werden dürfen.

Zur praktischen Umsetzung dieser Bestimmungen werden technische Hilfsmittel benötigt. Auch diese unterliegen einer Zertifizierungskurse- und Zulassungsverordnung, die allerdings aus Sicherheitsgründen nicht öffentlich ist und nur den staatlichen Behörden vorliegt. Parallel wurden zur Durchführung einer Kontrolle Prozesse entwickelt, die aus Sicherheitsperspektive eine bestmögliche Überprüfung ermöglichen. Verkehrliche Aspekte, wie Warteschlangen oder Personensichten, waren dabei zunächst von untergeordneter Bedeutung. Hier findet gegenwärtig bei allen Beteiligten ein substanzielles, prozessuales Umdenken statt. Zu den großflächig eingesetzten Technologien gehören Metalldetektoren in Form von

3 | Vgl. McCarthy 2013, Gopalakrishnan et al. 2013.
4 | Vgl. Bundesanzeiger 2017.
5 | Vgl. ICAO 2017.
6 | Vgl. Bundesanzeiger 2017.

Torsonden, Handscannern und Bodyscannern zur Überprüfung des mitgeführten Handgepäcks sowie Röntgenscanner (CT) für das beim Check-in beziehungsweise Baggage-Drop-Off abgegebene Reise- und Sondergepäck. Die Unterscheidung, ob Reisende unerlaubte Gegenstände beziehungsweise Substanzen mitführen, wird bei Bodyscannern, die gegenwärtig sukzessive die Metalldetektoren ersetzen, von der mitgelieferten Software getroffen. Wird ein Alarm ausgelöst, führt das Sicherheitspersonal in Form einer Nachkontrolle eine manuelle Überprüfung der Reisenden, in der Regel durch Abtasten und mittels Handscanner, durch. Dabei wird der potenziell gefährdende Bereich dem Personal bildlich in abstrahierter Form dargestellt. Metalldetektoren geben aufgrund ihres physikalischen Wirkungsprinzips, das auf den Maxwell'schen Gleichungen beruht, im Fall einer positiven Detektion ein akustisches Signal beziehungsweise zeigen bei Torsonden optisch unterstützt einen groben Höhenbereich an, in dem ein metallischer Gegenstand zu erwarten ist. In diesem Fall wird, wie bei den Bodyscannern beschrieben, ebenfalls eine manuelle Nachkontrolle durchgeführt. Bodyscanner können über metallische Gegenstände hinaus zahlreiche weitere Materialien wie beispielsweise Keramik erkennen und stellen damit einen weiteren Baustein zur Erhöhung der Sicherheit an Flughäfen dar. Röntgenscanner zur Kontrolle des mitgeführten Handgepäcks können je nach Gerätetyp ebenfalls automatische Alarme generieren. In der Regel ist aber bei diesen Geräten Personal, welches sich das Röntgenbild auf einem Bildschirm ansieht, für die Auswertung verantwortlich. Ein hoher Ausbildungsstandard und Erfahrungen des Sicherheitspersonals sind hier die Hauptgaranten für eine erfolgreiche Detektion von Schusswaffen, Sprengstoffen, Messern und weiteren gefährlichen Gegenständen. Bei abgegebenem Reisegepäck erfolgt eine mehrstufige Kontrolle, beginnend mit einem automatischen Röntgenscan (CT) bis hin zu einer manuellen Kontrolle – das heißt Öffnung des Gepäcks durch Sicherheitspersonal, gegebenenfalls auch im Beisein des Gepäckstückbesitzers.

3 Methode zur Ermittlung des Level of Security mittels Fuzzy-Ansatz

3.1 Grundlagen des Level-of-Security-Ansatzes

Die einleitende Beschreibung verdeutlicht, dass Sicherheit im Luftverkehr maßgeblich durch den Einsatz von Technik, aber auch durch den Menschen, der die Technik bedient beziehungsweise deren Daten auswertet, determiniert wird. Das bedeutet, dass sich ein Sicherheitsniveau einerseits durch physikalisch messbare Größen, andererseits aber auch durch weiche Einflussfaktoren wie Erfahrung und Ausbildungsstand von Personal ergibt. Daraus wird ersichtlich, dass Sicherheit keine Konstante ist.

An dieser Stelle ist zu erwähnen, dass dieselben Technologien und ähnliche Kontrollprozesse wie im Luftverkehr auch beim Schutz von anderen Infrastrukturen, zum Beispiel bei der Sicherung von Behörden, Konzerten oder Fernsehtürmen, aber auch von U-Bahnen, zum Beispiel in Russland und China, oder des Fernverkehrs in Spanien (Gepäckkontrolle) zur Anwendung kommen.

Mit dem durch Milbredt/Deutschmann[7] erarbeiteten „Level of Security" wurde ein mathematischer Formalismus entwickelt, der es gestattet, die Verknüpfung von Messdaten mit weichen Informationen in einer Kennzahl zusammenzufassen, die ein Sicherheitsniveau zu einem Zeitpunkt in einem definierten Bereich widerspiegelt. Insbesondere zur Bewertung von menschlichen Einflussfaktoren bietet der im Jahr 1964 durch den Mathematiker Lotfi A. Zadeh[8] entwickelte Fuzzy-Ansatz Möglichkeiten, unterschiedliche Meinungen, Erfahrungen und Ansichten zu berücksichtigen beziehungsweise zu verarbeiten. Im Gegensatz zu klassischen Ansätzen, die eine klare Trennung zwischen Informationskategorien vornehmen, ist dies auf Basis der menschlichen Erfahrungswelt oft sehr schwierig. Die folgenden Abbildungen zeigen diese Unterschiede am Beispiel der Wahrnehmung von Temperaturen. Mithilfe des Fuzzy-Ansatzes wird zugelassen, dass Überlappungen zwischen mehreren Kategorien grundsätzlich möglich sind (siehe Abbildung 1). Im dargestellten Beispiel wird durch Überlappung zugelassen, dass eine Temperatur von unterschiedlichen Personen unterschiedlich wahrgenommen wird (siehe Abbildung 2).

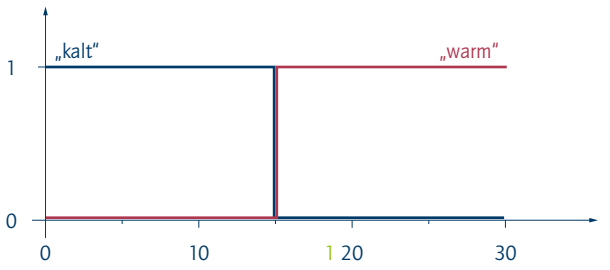


Abbildung 1: Klassische technische Parameterseparation (Quelle: eigene Darstellung)

7 | Vgl. Milbredt/Deutschmann 2016.
8 | Vgl. Zadeh 1965, Zadeh 1975.

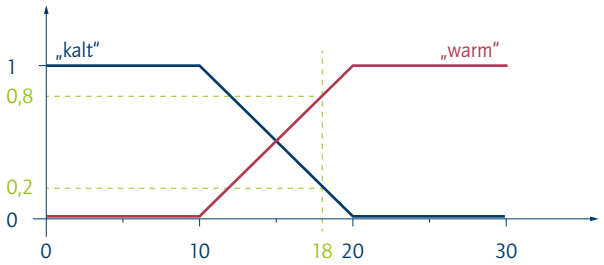


Abbildung 2: Tatsächliches Temperaturempfinden von Menschen (Quelle: eigene Darstellung)

Um eine Datenmenge, bestehend aus weichen Informationen, aus- und bewerten zu können, wird wie folgt vorgegangen:

1. Fuzzyfikation: Da eine zu betrachtende Größe von unterschiedlichen Personen unterschiedlich empfunden wird, ist die Zugehörigkeit zu einer Gruppe zu beschreiben. Beispielsweise nimmt jeder Mensch Temperaturen subjektiv unterschiedlich wahr. So werden 22 Grad Celsius von einigen Menschen als kalt empfunden, für andere sind 22 Grad Celsius bereits zu warm, während eine dritte Gruppe die Temperatur von 22 Grad Celsius als sehr angenehm empfindet. Die Zugehörigkeit zu einer dieser drei Gruppen kann durch unterschiedliche Funktionen beschrieben werden. Diese lassen sich durch gezielte Befragung von Personen oder Messungen in Abhängigkeit von der Fragestellung spezifizieren. Das bedeutet, dass in jedem Anwendungsfall ein Satz Auswahlregeln zu erstellen ist, der eine spätere Zuordnung ermöglicht. Dieses kann sich bei zusätzlichen, im Rahmen der Problembearbeitung gewonnenen Erkenntnissen ändern. Dabei sind Auswirkungen auf die im Weiteren betrachteten Schritte zu erwarten. Grundsätzlich ist sicherzustellen, dass kleine Änderungen in den Randbedingungen nur kleine Änderungen im Gesamtprozess nach sich ziehen. Treten große Änderungen auf, ist es wahrscheinlich, dass sich das betrachtete System in einem nicht-linearen und daher sehr defizilen Zustand, der eine besondere Problembehandlung erfordert, befindet und damit klassische Methoden der Systembeschreibung nicht anwendbar sind.

2. Implikation: Plausibilitätsprüfung der in der Fuzzyfikation ermittelten Werte.

3. Akkumulation: Kamen mehrere Fuzzy-Regeln zum Einsatz, sind die durch die einzelnen angewandten Regeln erhaltenen Werte zu kombinieren.

4. Defuzzyfikation: Die durch Akkumulation erhaltene Punktmenge wird auf einen einzigen Repräsentanten dieser Menge reduziert.

Die großen Herausforderungen dieser Methode bestehen darin, die relevanten Parameter zu identifizieren und ein geeignetes Regelwerk zu definieren. Ein solches Regelwerk wurde durch Milbredt/Deutschmann[9] erarbeitet und verifiziert. Die Frage, welche Parameter beziehungsweise Parameterklassen einen signifikanten Einfluss auf die Sicherheit haben, wurde von Milbredt[10] sowie Assmer[11] detailliert untersucht. Dabei zeigte sich, dass die Auswahl der Parameter, die ausschließlich durch Expertenwissen getroffen werden kann, sehr stark mit der jeweiligen politischen Interessenlage des für Sicherheit Verantwortlichen variiert. Aus diesen Studien, die auf Umfragen von Sicherheitsbehörden, Sicherheitsverantwortlichen der Bahn, des Schiffsverkehrs sowie von wissenschaftlichen Verkehrs- und Sicherheitsexperten beruhen, folgt, dass

- Infrastrukturmerkmale (zum Beispiel Art der Infrastruktur, deren Lage und gesellschaftliche Bedeutung),
- Charakteristika der in der Infrastruktur agierenden Personen (zum Beispiel Reiseerfahrung von Passagieren),
- die Personenanzahl in der interessierenden Infrastruktur,
- Charakteristika des Sicherheitspersonals (zum Beispiel Erfahrung und Ausbildungsstand in Relation zur Zahl der Sicherheitskräfte) sowie
- Sicherheitslage

die Kerneinflussgrößen auf das Sicherheitsniveau – insbesondere für Flughäfen und Bahnhöfe – darstellen.

Darüber hinaus konnte Assmer[12] zeigen, dass die genannten Parameterklassen neben dem Flughafen auch auf die Verkehrsträger beziehungsweise Verkehrsmittel Bahn und Häfen übertragbar sind. Da der Level of Security sowohl von messbaren als auch von weichen Einflussfaktoren determiniert wird und eine Online-Erfassung der von Kontrolltechnologien erzeugten Daten bisher nicht existiert beziehungsweise dem Datenschutz unterliegt, ist der Wirkungsnachweis der Methode in einem realen Umfeld gegenwärtig nicht möglich. Aus diesem Grund wurde versucht,

9 | Vgl. Milbredt/Deutschmann 2016.
10 | Vgl. Milbredt 2016.
11 | Vgl. Assmer 2017.
12 | Vgl. Assmer 2017.

diesen mittels einer Simulation zu erbringen. Dazu wurden, basierend auf der Simulationssoftware AnyLogic,[13] zwei Simulationsmodelle entwickelt (vgl. Abbildungen 3 und 4).

Das erste Simulationsmodell entspricht einem mittelgroßen Flughafen, dessen terminalseitige Abfertigungsprozesse, Passagierzahlen sowie typische Infrastrukturmerkmale entsprechend den Ergebnissen des EU-Projekts ASSET[14] vollständig abgebildet wurden.

Das zweite Modell repräsentiert einen Kategorie-2-Bahnhof, der in Anlehnung an die Verkehrsinfrastrukturen des Bahnhofs Braunschweig simuliert wurde.[15]

Für beide Modelle wurden Verkehrsszenarien erstellt, in denen im Basisszenario Personen-, Luftverkehrs- und Bahnverkehrsszenarien eines jeweils typischen Tages Berücksichtigung fanden. Darüber hinaus wurde zur Messung von technischen Parametern auf Module zurückgegriffen, deren Entwicklung im vom BMBF geförderten Projekt „Critical Parts" erfolgte.[16]

Nach Abschluss der Simulation wurden die Simulationsdaten in die Fuzzy-Auswertungsroutinen übertragen, ausgewertet und der Level of Security als Funktion von Zeit und Ort berechnet. Die bereits erwähnten weichen Parameter, die in die Bewertung eingingen, wurden durch Befragung von Prozessbeteiligten des Luft- und Bahnverkehrs ermittelt und mit diesen abgestimmt. Analog erfolgte die Definition des Fuzzy-Regelwerks. Auf dem Basisszenario aufbauend wurden weitere Verkehrsszenarien[17] entwickelt, in denen insbesondere die Personenanzahl respektive die Personendichte im Flughafen beziehungsweise im Bahnhof erhöht wurden (vergleiche Parameterklassen). Jedes Szenario wurde fünffach simuliert.[18] Das mehrfache Simulieren beruht auf dem Umstand, dass in der Simulation Zufallszahlen generiert werden, um auszuschließen, dass bezogen auf die genutzten Verteilungsfunktionen sehr unwahrscheinliche Randwerte die Ergebnisse der Simulation beziehungsweise die Interpretation der Ergebnisse verfälschen.

Nach Abschluss der Simulation wurden die dort ermittelten Daten gespeichert und für die Level-of-Security-Analysen aufbereitet, welche post-simulativ durchgeführt wurden.

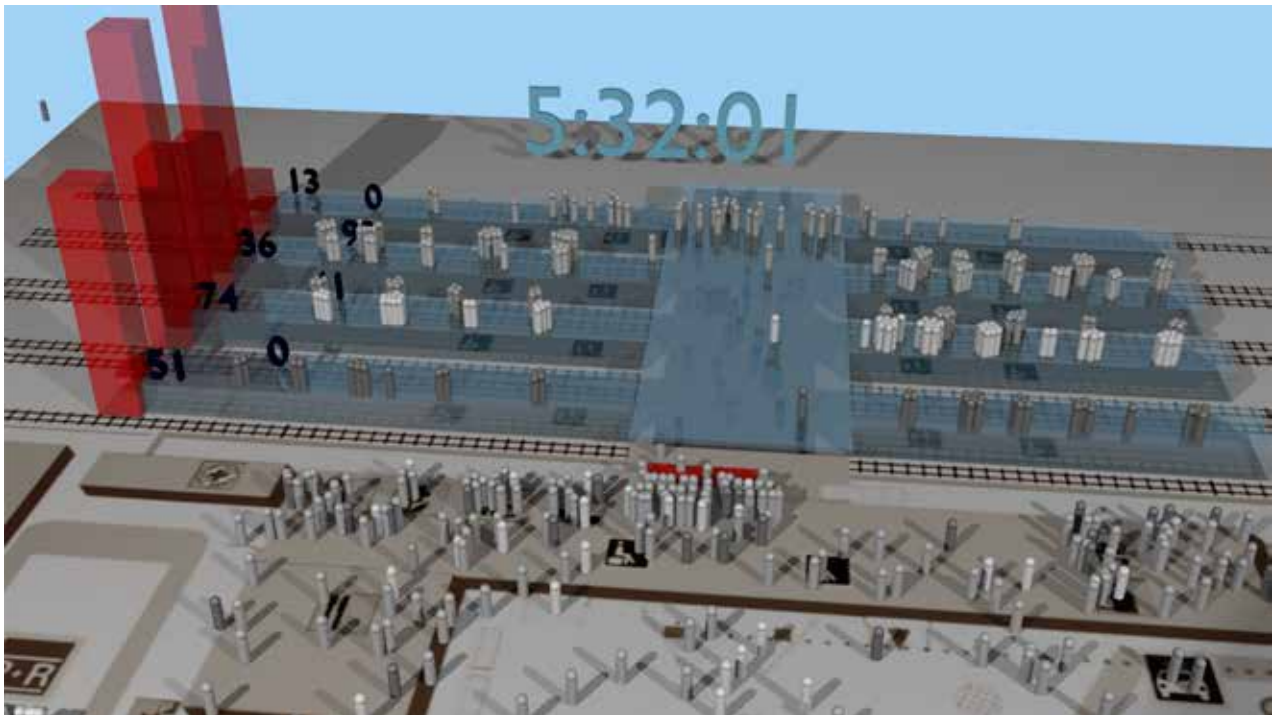


Abbildung 3: Verwendetes Simulationsmodell des betrachteten Flughafens (Quelle: AnyLogic 2017)

13 | Vgl. AnyLogic 2017.
14 | Vgl. ASSET 2012; im Projekt ASSET wurden europaweit standardisiert Eigenschaften für unterschiedliche Flughafenkategorien definiert.
15 | Vgl. Assmer 2017.
16 | Vgl. Deutschmann 2011.
17 | Vgl. Milbredt/Deutschmann 2016, Assmer 2017.
18 | Vgl. Otte 2010.

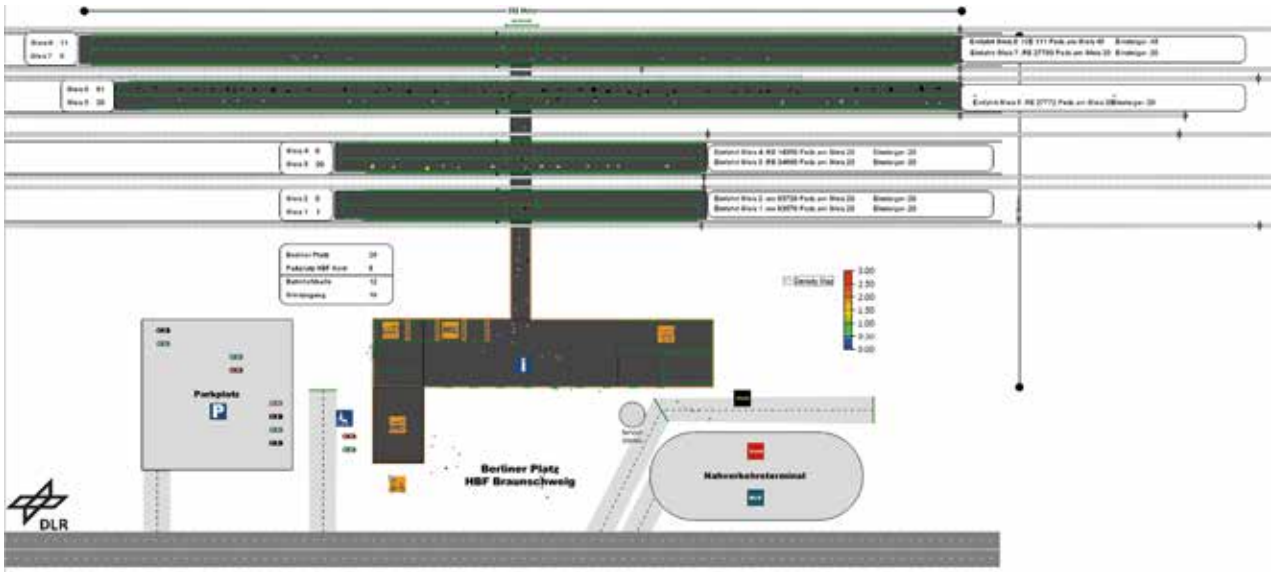


Abbildung 4: Verwendetes Simulationsmodell des betrachteten Bahnhofs (Quelle: AnyLogic 2017)

3.2 Erweiterung des Fuzzy-Ansatzes um die What-if-Funktionalität

Die zuvor dargestellte Methode wurde im nächsten Schritt um eine in Abbildung 5 dargestellte „What-if-Funktionalität" erweitert, um sie im operativen Geschehen an Flughäfen von Sicherheitsbehörden und Sicherheitsdienstleistern einsetzen zu können.

Der Indikator Level of Security besteht aus zwei Teilen. Im ersten Teil, der unter 3.1 beschrieben wurde, wird ein Evaluationsprozess auf der Basis von Fuzzy Logic mithilfe von Expertenwissen sowie Auswahl und Gewichtung von Parametern entwickelt. Dieser Evaluationsprozess verarbeitet Parameter wie zum Beispiel Warteschlangenlänge und Gefährdungslage zu einer Zahl, die die Gesamtsicherheitslage widerspiegelt. Eine Zahl ohne Möglichkeit eines Eingreifens ist nutzlos. Der zweite Teil begegnet diesem Umstand mit einer What-if-Funktionalität. Das System schlägt verschiedene Reaktionen auf die geänderte Sicherheitslage vor und evaluiert die Änderung im Level of Security. Das Einbeziehen von Expertenwissen am Beispiel der Gewichtung von Parametern wurde näher untersucht. Zur Repräsentation der Gewichtung wurde eine Methode des Analytic Hierarchy Process (AHP)[19] benutzt. Im Kontext des AHP werden Handlungsalternativen untereinander gewichtet. Zur Repräsentation der Gewichtungen untereinander wird eine Gewichtungsmatrix verwendet. Unter Einsatz einer solchen Matrix wurde von Milbredt/Deutschmann[20] und Milbredt[21] ein Formalismus zur automatischen Generierung von Regeln eines Fuzzy-Inference-Systems entwickelt.

Abbildung 6 zeigt das Verhalten von Fuzzy-Inference-Systemen mit den Parametern Personendichte und Erkennen von Gefahren, wobei die Skala exemplarisch in elf Stufen[22] aufgeteilt ist. Der Indikator Level of Security nimmt Werte zwischen 0 und 1 an. Die Parameter beeinflussen den Level of Security in entgegengesetzter Weise: Während eine höhere Stufe beim Erkennen von Gefahren zu einem höheren Level of Security führt, sinkt der Level of Security bei einer höheren Stufe der Personendichte. Die Identifizierung von relevanten Größen sowie deren Wertebereich müssen durch Sicherheitsexperten erfolgen. In Abbildung 6a ist ein Fuzzy-Inference-System mit zwei Parametern gleicher Gewichtung dargestellt. Die Summe der Gewichte ergibt 1. Während in Abbildung 6a die Steigung des Level of Security für das Erkennen von Gefahren = 0 oder Personendichte = 10 gleich ist, ist in Abbildung 6b eine vergrößerte Steigung zugunsten des Parameters Personendichte zu sehen. In Abbildung 6c wurde die Gewichtung des Parameters Personendichte als so gering

19 | Vgl. Saaty 1980, Zadeh 1975.
20 | Vgl. Milbredt/Deutschmann 2016.
21 | Vgl. Milbredt 2016.
22 | Im Rahmen der Arbeit zeigte sich, dass geringe Auflösungen (< 11) zu ungenau interpretierbare Ergebnisse lieferten, während eine höhere Anzahl den Rechenaufwand signifikant steigerte, ohne eine deutliche Steigerung des Informationsgehalts zu erreichen.

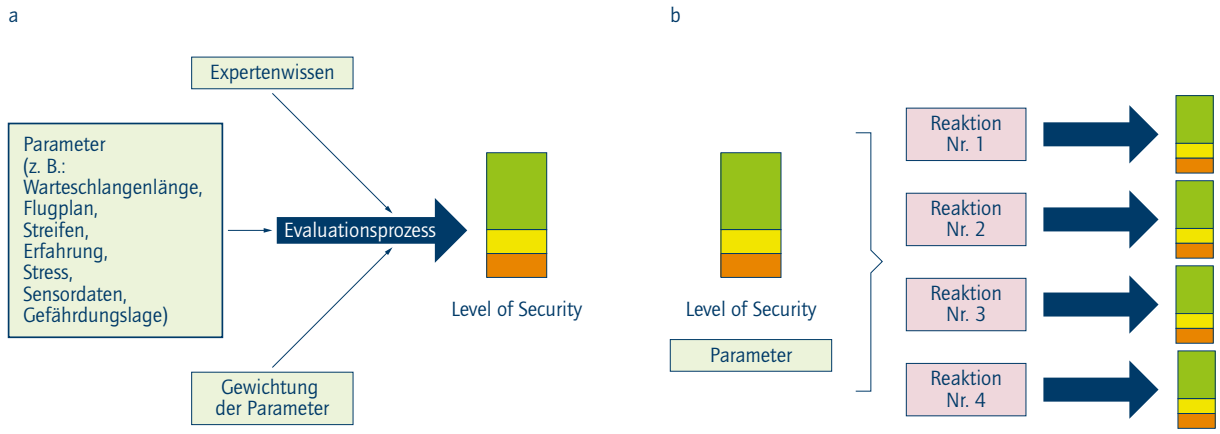


Abbildung 5: Phasen des Indikators Level of Security; (a) Eingabewerte und beeinflussende Größen des Evaluationsprozesses; (b) What-if-Eigenschaft der Managementstruktur (Quelle: eigene Darstellung)

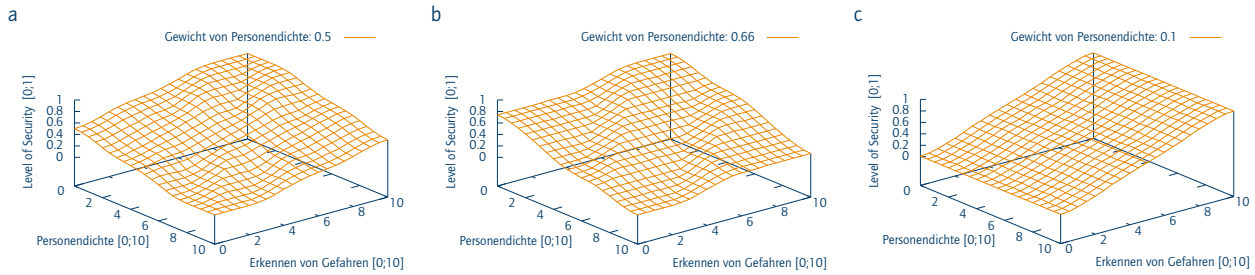


Abbildung 6: : Fuzzy-Inference-Systeme mit zwei Parametern unterschiedlicher Gewichtung (Quelle: eigene Darstellung)

angenommen, dass der Wert dieses Parameters keinen Einfluss auf den Level of Security hat. Obwohl mithilfe der Methode von Milbredt[23] Fuzzy-Inference-Systeme automatisch unter Berücksichtigung der Gewichtung der Parameter generiert werden können, bleibt die Eigenschaft der Anpassung auf Regel-Ebene erhalten. Das Sicherheitspersonal kann also direkt in die Berechnung eingreifen, um das Verhalten anzupassen. Im operativen Betrieb bietet ein solches System keine Anpassung der Berechnung. Neuronale Netze, die es erlauben, aus Ereignissen und Verläufen der Vergangenheit zu lernen, beinhalten die Möglichkeit einer kontinuierlichen Anpassung, allerdings zum Preis der Nachvollziehbarkeit, da kausale Zusammenhänge nicht berücksichtigt werden. Während bei Fuzzy-Inference-Systemen bei jeder Eingabe die zur Anwendung kommenden Regeln identifiziert werden können, gibt es bei neuronalen Netzen keine Möglichkeit, das Zustandekommen eines Ergebnisses nachzuvollziehen. Die Implementierung des Level of Security mithilfe der Verbindung beider Welten eliminiert die Nachteile.

4 Level of Security – Fallbeispiele

Im Folgenden werden zwei Szenarien vorgestellt, die zeigen, welche Änderungen sich im Sicherheitsniveau im Falle der Variation der Personalqualifikation (Szenario 1) und der Personalquantität (Szenario 2) ergeben (siehe Abbildung 7).

23 | Vgl. Milbredt 2016.

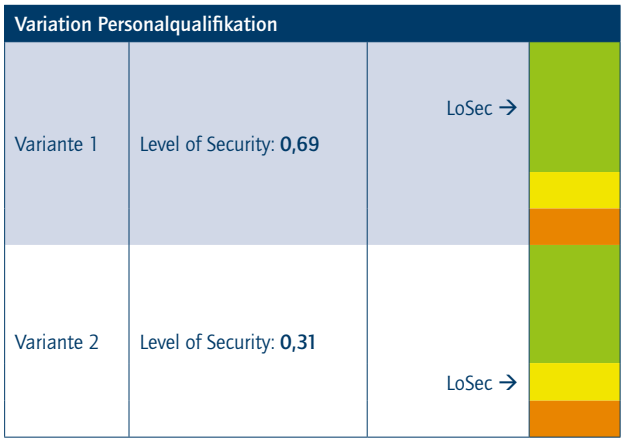


Abbildung 7: Vergleich unterschiedlicher Personalqualifikationsvarianten und deren Auswirkung auf das Sicherheitsniveau (Quelle: eigene Darstellung)

4.1 Einfluss der Personalqualifikation auf das Sicherheitsniveau

Im ersten hier dargestellten Szenario wird die Personalqualifikation variiert. Dabei repräsentiert die Variante 2 die Basisausbildung von Sicherheitspersonal. Variante 2 unterscheidet sich von Variante 1 durch die Annahmen, dass das Personal in den folgenden Bereichen gezielt über das in der Grundausbildung hinausgehende Maß geschult beziehungsweise trainiert wurde:

- Erkennung von gefährlichen Gegenständen und Substanzen,
- Erkennung von auffälligem Verhalten von Reisenden sowie
- Profiling.

In der Simulation wurde auf verkehrliche Unregelmäßigkeiten und sicherheitskritische Störungen verzichtet, um den reinen Effekt der unterschiedlichen Ausbildungsstände zu erfassen.

Ausgehend von den von Assmer[24] formulierten Regelwerken und Verteilungsfunktionen konnte für Personal mit zusätzlichen Qualifikationen beziehungsweise Fähigkeiten ein Sicherheitslevel von 0,69 berechnet werden. Im Szenario, das die Basisausbildung widerspiegelt, konnte ein Level of Security von 0,31 ermittelt werden. Auf Basis der von Experten festgelegten Grenzen zwischen sicheren und weniger sicheren Bereichen zeigt sich an diesem Beispiel, dass ein höheres Ausbildungsniveau ein hohes Sicherheitsniveau ergibt, allerdings bereits die Grundausbildung für hinreichend Sicherheit sorgt. Der Vergleich der Szenarien zeigt weiterhin, dass durch gezielte Ausbildungsmaßnahmen das Sicherheitsniveau deutlich verbessert werden kann.

4.2 Einfluss der Personalquantität auf das Sicherheitsniveau

Das zweite Szenario beschreibt eine Situation, in der durch gezielte Maßnahmen zwar das Sicherheitsniveau beeinflusst, aber nicht signifikant gesteigert werden kann. Dazu wurde die Zahl des Personals, das im Flughafen beziehungsweise im Bahnhof für Sicherheit sorgt (Kontrollpersonal, Streifenpersonal etc.), variiert. Dabei enthält Variante 1 das erhöhte Personalvolumen. Mithilfe der Simulation konnte unter denselben Annahmen wie in Szenario 1 gezeigt werden, dass die Erhöhung des Personalvolumens kaum Einfluss auf das Sicherheitsniveau hat. Bei der Interpretation dieses Ergebnisses sind zwei Komponenten zu berücksichtigen: Auf der einen Seite sorgen zusätzliche Streifen für eine Erhöhung des subjektiven Sicherheitsgefühls und auch der objektiven Sicherheit durch Abschreckung. Demgegenüber stehen allerdings die Steigerung der Attraktivität des Anschlagsziels (auch in Form von uniformiertem Personal) und – im Falle eines Anschlags – die Erhöhung des Schadensausmaßes, da sich mehr Menschen (zusätzliches Sicherheitspersonal) im potenziell gefährdeten Bereich befinden. Daher ergibt sich für die Variante mit erhöhtem Personaleinsatz ein Level of Security von 0,53, während sich in der Variante mit herkömmlichem Personaleinsatz ein Sicherheitsniveau von 0,47 einstellt (siehe Abbildung 8).

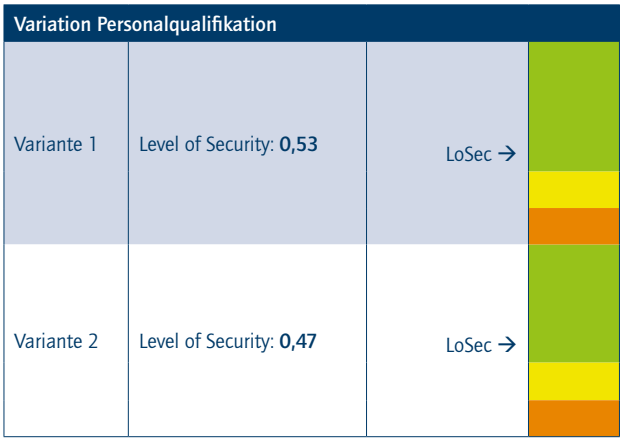


Abbildung 8: Vergleich unterschiedlicher Personalquantitäten und deren Wirkung auf das Sicherheitsniveau (Quelle: eigene Darstellung)

24 | Vgl. Assmer 2017.

Der Vergleich beider Szenarien lässt darauf schließen, dass es zur „Herstellung" von Sicherheit generell sinnvoller ist, hochqualifiziertes statt durchschnittlich ausgebildetes Personal in hoher Zahl einzusetzen. Damit wird auf Basis der Simulation deutlich, dass die eingangs beschriebenen Parameterklassen einen nachweisbaren Einfluss auf den Level of Security besitzen.

Zusammenfassung und Ausblick

Nachdem die grundsätzliche Tragfähigkeit des Level-of-Security-Ansatzes und der What-if-Funktionalität gezeigt werden konnte, eröffnen sich eine Reihe interessanter und herausfordernder Fragestellungen. Die erste Herausforderung ist die Übertragung der Methode in Echtzeit, um operative Szenarien abdecken zu können. Der Level of Security ist eine Größe, die alle am Sicherheitsprozess Beteiligten im operativen Geschehen betrifft und deren Arbeit beeinflusst. Das bedeutet, dass die in die Bewertung einfließenden Daten in Echtzeit zur Verfügung gestellt werden müssen. Hier ist zu berücksichtigen, dass rechtliche Grundlagen zur Weitergabe und Verarbeitung technisch erhobener Daten juristisch und gesellschaftspolitisch zu diskutieren und gegebenenfalls zu schaffen sind. Zudem muss gewährleistet werden, dass der Datentransfer umfassend sicher, das heißt nicht manipulierbar von und nicht lesbar für Dritte, erfolgt. Darüber hinaus sind Schnittstellen zur Level-of-Security-Software zu etablieren und die Algorithmen so anzupassen, dass eine permanente Neuberechnung des LoSec erfolgen kann. Eine weitere Kernfrage ist, wie Grenzübergänge zwischen den einzelnen Sicherheitsniveaus festgelegt werden. Diese Grenzen können sich, je nach Schwerpunkt und Änderung von Sicherheitsproblemstellungen, auf operativen bis hin zu strategischen Zeithorizonten verändern. Diese Herausforderung ist ebenfalls mit den an den Sicherheitsprozessen Beteiligten zu diskutieren. Eine deutliche Erweiterung des Konzepts muss im Kontext der Digitalisierung stattfinden. Insbesondere die Frage „Wie sicher sind IT-Systeme?" steht im Fokus von künftigen Forschungsbemühungen. Es ist zu untersuchen, welche Leistungsparameter die Sicherheit eines IT-Systems repräsentieren und wodurch diese beeinflusst werden. Ferner ist zu beachten, dass auch das Speichern und Übertragen von Daten abzusichern ist.

Zwischen Safety und Security besteht generell ein enger Zusammenhang. Damit ist die Frage, welche Auswirkungen Störungen beziehungsweise Manipulationen von IT-Systemen auf ganze Infrastrukturen beziehungsweise Teile davon und die darin ablaufenden Prozesse haben, ebenfalls ein Schwerpunkt künftiger Forschungsarbeiten. Im Zuge der Digitalisierung ist die Frage, wie Infrastrukturen künftig miteinander vernetzt sind und miteinander kommunizieren, ebenfalls von immenser Bedeutung. Welche Wege für Störungsausbreitungen werden damit eröffnet, und wie können diese im Kontext von Safety und Resilienz behandelt werden?

Der Level of Security bietet in Kombination mit einer erweiterten Simulationsumgebung die Möglichkeit einer weiteren Evolutionsstufe. Mit einem erweiterten Konzept lassen sich direkt Auswirkungen strategischer Entscheidungen und Maßnahmen simulativ untersuchen und bewerten. Ein weiterer Entwicklungsschritt besteht darin, den Fuzzy-Ansatz mit neuronalen Netzen zu kombinieren. Diese eröffnen die Möglichkeit, aufgetretene Situationen zu erfassen, zu bewerten und daraus zu lernen. Auf diesem Wege kann aus Erfahrungen der Vergangenheit gelernt und diese auf künftige beziehungsweise aktuelle Situationen angewandt werden. Der Nachteil von neuronalen Netzen besteht allerdings darin, dass kausale Zusammenhänge nicht explizit erkannt, sondern nur Wirkungen betrachtet werden. Grundsätzlich lassen sich die dargestellten Methoden aber auch auf weitere technische Entwicklungen anwenden, um zu bewerten, ob eine Maßnahme zu erhöhter Sicherheit führt.

Literatur

AnyLogic 2017
AnyLogic: o. T. 2017. URL: http://www.anylogic.com/ [Stand: Oktober 2017].

ASSET 2012
ASSET: o. T. 2012. URL: http://www.asset-project.eu/ [Stand: Mai 2012].

Assmer 2017
Assmer: „Level of Security – Dynamische Lagebilddarstellung an Verkehrsknoten Bahnhof", gemeinsamer Bericht DLR-Ostfalia (FH Braunschweig Wolfenbüttel) 2017.

BMI 2009
Bundesministerium des Innern: „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)", Berlin 2009.

Bundesanzeiger 2017
Bundesanzeiger: „Luftsicherheitsgesetz", BAnz AT 18.07.2017 B1.

Deutschmann 2011
Deutschmann, A.: „Abschlussbericht Critical Parts", im Auftrag des BMBF 2011.

Gopalakrishnan et al. 2013
Gopalakrishnan et al.: „Cyber Security for Airports". In: *International Journal for Traffic and Transport Engineering*, 2013, 3(4): S. 365–376.

ICAO 2017
ICAO Annex17: o. T. 2017. URL: https://www.icao.int/Security/SFP/Pages/Annex17.aspx [Stand: Oktober 2017].

McCarthy 2013
McCarthy, M.: „SCADA Threats in the Modern Airport". In: *32nd International Journal of Cyber Warfare and terrorism*, 2013, 3(4) S. 32–39.

Milbredt/Deutschmann 2016
Milbredt/Deutschmann: „Key Performance Indicator for Security Measurement at Airports". In: *AIAA Modeling and Simulation Technologies Conference*. AIAA AVIATION 2016, 13. bis 17. Juni 2016, Washington D. C., USA. DOI: 10.2514/6.2016-4300.

Milbredt 2016
Milbredt, O.: „Parameter Weighting for Multi-Dimensional Fuzzy Inference Systems". In: *2016 IEEE International Conference on Control, Automation and Information Sciences (ICCAIS)*, 27. bis 29. Oktober, Ansan, Korea. doi:10.1109/ICCAIS. 2016.7822465.

Otte 2010
Otte, B.: „Verification and Validation of Simulations", 2010.

Saaty 1980
Saaty, R. W.: „The Analytic Hierarchy Process", McGraw-Hill, 1980.

Zadeh 1965
Zadeh, L. A.: „Fuzzy Sets". In: *Inf. Control*, 1965, 8, S. 338–353.

Zadeh 1975
Zadeh, L. A.: „The Concept of a Linguistic Variable and Its Application to Approximate Reasoning I, II, III". In: I*nformation Sciences*, 1975, 8, S. 199–249.

8.3 Sicherheit ist die Abwesenheit von Kriminalität – eine Hypothese

P(Sicherheit) = 1 – P(Kriminalität)

Prof. Dr. Dirk Labudde
Fachgruppe Forensik, Hochschule Mittweida (FoSIL) und
Institut für Sichere Informationstechnologie SIT in Darmstadt

Zusammenfassung

Der Wunsch nach größtmöglicher Sicherheit einerseits und möglichst weitgehender individueller Freiheit andererseits steht in einem starken Spannungsverhältnis. In dieser Arbeit soll ein Zusammenhang zwischen dem Konzept Sicherheit (im Sinne der Security) und Kriminalität hergestellt werden. Die Bearbeitung der Hypothese „Ist Sicherheit die Abwesenheit von Kriminalität?" erfolgt auf der Grundlage von Modellansätzen aus den Bereichen des Predictive Policing und der Aufstellung eines Wechselwirkungsmodells zwischen Akteuren und einer wohldefinierten urbanen Struktur. Somit können Maßnahmen, die mit der Maximierung beziehungsweise Optimierung von Sicherheit in diesem Kontext einhergehen, auf Basis der Analyse von Kriminalität in urbanen Systemen direkt abgeleitet und umgesetzt werden.

1 Sicherheit und Beschreibungsebenen

Der Begriff beziehungsweise das Verständnis von Sicherheit in einer Gesellschaft ist sehr vielschichtig. Im Gegensatz zum angloamerikanischen Sprachraum wird im deutschen Sprachraum normalerweise nicht zwischen den beiden Begriffen beziehungsweise Themenfeldern Security und Safety unterschieden. Dieser Sachverhalt wird eher unter dem Begriff Sicherheit zusammengefasst. Während Safety den Schutz der Umgebung vor einem Objekt, also eine Art Isolation, beschreibt, handelt es sich bei Security um den Schutz des Objekts vor der Umgebung. Im Zusammenhang mit dem Terminus Kriminalität werden hier die Inhalte des Begriffs Security näher beleuchtet.

Verallgemeinert kann Sicherheit als ein relativer Zustand betrachtet werden. Dieser Zustand hat eine zeitlich abhängige Lebensdauer, und er wird auf der einen Seite durch technische Entwicklungen und auf der anderen Seite durch gesellschaftliche Vorschriften, Auffassungen und Verhaltensregeln stark beeinflusst. Sicherheit gilt in einer wohldefinierten Umgebung oder unter bestimmten Bedingungen. In Grenzfällen – im Sinne von unvorhersehbaren Ereignissen – können wohldefinierte und erprobte Sicherheitsvorkehrungen versagen.

Sicherheit in diesem Kontext bedeutet den Schutz des Menschen vor Dingen beziehungsweise vor anderen Menschen. An dieser Stelle kann der direkte Bezug zum Verhalten der Individuen (Mitglieder) einer Gesellschaft hergestellt werden. Die Konzepte und Begriffe der Sicherheit und der Kriminalität sind durch das Regelwerk Justiz und Moralauffassung (Recht und Unrecht) verbunden. Unter einem Verbrechen wird gemeinhin ein schwerwiegender Verstoß gegen die Rechtsordnung einer Gesellschaft oder die Grundregeln menschlichen Zusammenlebens verstanden. Allgemein gesprochen handelt es sich um eine von der Gemeinschaft als Unrecht angesehene und von ihrem Gesetzgeber als kriminell qualifizierte und mit Strafe bedrohte Verletzung eines Rechtsguts durch den von einem oder mehreren Tätern schuldhaft gesetzten verbrecherischen Akt.

Welche Handlungen unter Strafandrohung verboten werden, bestimmt der jeweilige Gesetzgeber mit verbindlicher Wirkung für seinen Zuständigkeitsbereich – und insofern bestimmt er auch, was Kriminalität ist und was nicht. Denn aus seiner Sicht ist Kriminalität nichts anderes als die Summe der Straftaten. Als Kriminalität wird in der gesellschaftlichen Wirklichkeit zunächst einmal das bezeichnet, was im Gesetz als strafbare Handlung definiert ist – Kriminalität als Summe der strafbedrohten Handlungen. Das ist sozusagen die strafrechtlich definierte beziehungsweise theoretische Kriminalität.[1] Eine weitere Definition von Kriminalität nach Härter ist die Bezeichnung der Kriminalität als Summe der von einer Gesellschaft beziehungsweise einem Rechtssystem als besonders schädlich und strafbar erachteten devianten Verhaltensweisen beziehungsweise rechtlich definierten Normverstößen: die Verbrechen, lateinisch crimina, heute im engeren Sinne die Straftaten.[2] Schäfer und Zapf definieren Kriminalität wie folgt: Kriminalität ist die Gesamtzahl aller Handlungen, die gegen kodifizierte Strafrechtsnormen (Verbrechen im weiteren Sinne) verstoßen und sich innerhalb eines bestimmten Zeitraums sowie innerhalb eines geografisch abgegrenzten Raums ereignen und erfasst werden.[3]

1 | Vgl. Schmidt-Semisch/Hess 2014.
2 | Vgl. Härter 2013.
3 | Vgl. Schäfers/Zapf 2013.

Der Begriff Sicherheit im Sinne der Security ist mit Interessen und verschiedenen Aspekten eng verknüpft. Die Interessen können in verschiedene Ebenen eingeteilt werden:

- Internationale Interessen (Terror, Bürgerkrieg oder Flugzeugentführung)
- Nationale Interessen (Extremismus, Amoklauf, organisierte Kriminalität)
- Regionale Interessen (Einbruchsserien)
- Persönliche Interessen (Einbruch oder Diebstahl)

Aspekte der Sicherheit können wie folgt aufgeteilt werden:

- Gesetzliche Sicherheit
- Technische Sicherheit
- Gefühlte Sicherheit

In Gesellschaften und den zugrunde liegenden urbanen Systemen lassen sich Akteure definieren, die mit den Konzepten Sicherheit und Kriminalität verbunden sind. Akteure in diesem Sinne sind Mitglieder einer Gesellschaft, mit einer wohldefinierten Rollenverteilung. Alle Akteure handeln in einem vorgegebenen urbanen System. In solchen komplexen Systemen wie einer Gesellschaft (im Sinne einer Staatsform) ist es unmöglich, Risiken vollständig auszuschließen.

Die Hypothese „Ist Sicherheit die Abwesenheit von Kriminalität?" soll durch einen Wahrscheinlichkeitsansatz näher beleuchtet werden. Dazu werden wir uns des aus der Systemtechnik bekannten Top-down-Ansatzes bedienen, den Begriff Sicherheitszustand in den Mittelpunkt rücken und Kriminalität modellieren. Top-down geht vom Abstrakten, Allgemeinen, Übergeordneten schrittweise hin zum Konkreten, Speziellen, Untergeordneten, während das Konzept Bottom-up den umgekehrten Ansatz bezeichnet. Hierbei handelt es sich um zwei grundsätzlich verschiedene Denkrichtungen, um komplexe Sachverhalte zu verstehen, zu beschreiben und darzustellen. Ziel ist die Identifikation und Charakterisierung neuer Mechanismen, um ein besseres Verständnis über die komplexen Zusammenhänge einer „besiedelten urbanen Struktur" zu schaffen. Die zur Modellierung und Simulation verwendeten Daten stammen aus statistischen Erhebungen, zum Beispiel der Kriminalstatistik. Anhand der Messung des Sicherheitszustands beziehungsweise der Kriminalitätsrate in einem wohldefinierten Gebiet sollen ein prädiktives Modell erstellt sowie die Ausbreitung von Kriminalität unter Beachtung von Sicherheit genauer analysiert werden.

Abbildung 1 zeigt schematisch den Top-down-Ansatz. Mithilfe von Netzwerkanalysen kann das kollektive Verhalten der Akteure im urbanen System analysiert und visualisiert werden.

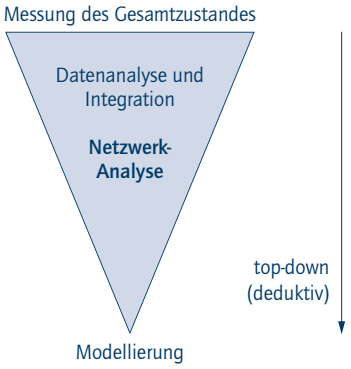


Abbildung 1: Systemtheoretischer Ansatz – top-down. Anhand der Beschreibung des Gesamtzustands können konkrete Modelle erstellt und simuliert werden (Quelle: eigene Darstellung).

Die Simulation ist eine Vorgehensweise zur Analyse von Systemen, die für die theoretische oder formelmäßige Behandlung zu komplex sind. Dies ist überwiegend bei dynamischem Systemverhalten der Fall. Bei der Simulation werden Experimente an einem Modell durchgeführt, um Erkenntnisse über das reale System zu gewinnen. Methoden der Informationsgewinnung dienen der Aufklärung von Netzwerkstrukturen auf verschiedenen Ebenen. Während der Simulation erfolgt die Erfassung zeitlicher und räumlicher Dynamiken von „zellulären/System-"Komponenten unter verschiedenen Bedingungen. Durch die Visualisierung von Netzwerken und den darin befindlichen Prozessen sollen Erkenntnisse der Prozesse als Ganzes gewonnen werden.

Die theoretischen Ansätze sollen nun am Beispiel von Hauseinbrüchen durch zelluläre Automaten beziehungsweise Graph-Automaten umgesetzt werden.

2 Das Konzept „Predictive Policing"

Ist es möglich, durch die Simulation von Kriminalität Sicherheit zu modellieren? Diese Fragestellung ist eng mit dem Begriff Predictive Policing verbunden. Erste Ansätze gehen in das 18. Jahrhundert zurück (Abbildung 2).

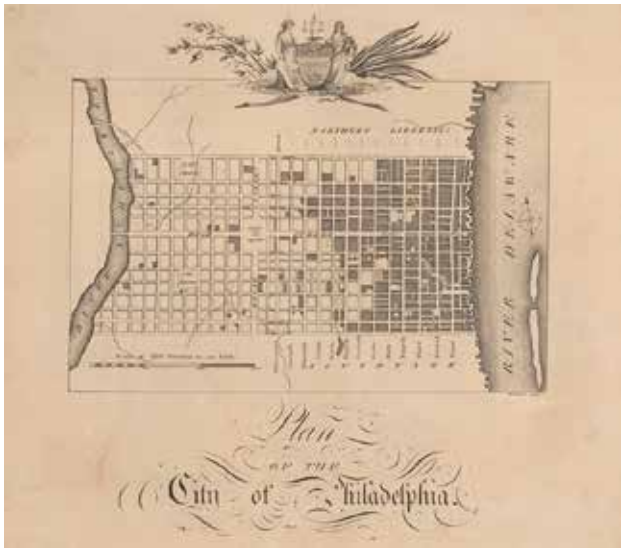


Abbildung 2: Erste Ansätze der Kriminalstatistik. Städte wurden in Quadranten eingeteilt und die Anzahl der Verbrechen visualisiert (Quelle: Foster 2004, S. 147).

In Gitternetzen, welche sich über eine Region erstrecken, wurde die Anzahl der Verbrechen eingezeichnet. In der heutigen Zeit werden computergestützte Ansätze verwendet. Ziel dieser Werkzeuge ist die Definition von sogenannten Hotspots, Gebieten mit einer erhöhten Kriminalitätsrate. Erst in der letzten Dekade entwickelten sich Wahrscheinlichkeitsmodelle beziehungsweise Ausbreitungsmodelle, analog zu Ansätzen aus der Epidemiologie. Die Epidemiologie (von griechisch epi: „auf, über", demos: „Volk", lógos: „Lehre") ist eine wissenschaftliche Disziplin, die sich mit der Verbreitung sowie den Ursachen und Folgen von gesundheitsbezogenen Zuständen und Ereignissen in Bevölkerungen oder Populationen beschäftigt. Die meisten Infektionskrankheiten können mathematisch modelliert werden, um ihr epidemiologisches Verhalten zu untersuchen oder zu prognostizieren. Solche mathematischen Ansätze und Modelle wurden auf das Gebiet des Predictive Policing in urbanen Räumen übertragen.

„Predictive Policing" bedeutet „vorausschauende Polizeiarbeit" und bezeichnet die Verwendung mathematischer Modelle, um Tatwahrscheinlichkeiten vorherzusagen und mithilfe operativer Maßnahmen, beispielsweise erhöhter polizeilicher Präsenz, auf diese reagieren zu können.

In der Verbrechenssoziologie wird seit den 1970er Jahren von der Repeat Victimisation[4] gesprochen, die sich Vorhersagesoftware zunutze macht. Gemeint ist die Annahme, dass Orte oder Personen mehrfach aufgesucht („viktimisiert") werden. „Re-Viktimisierungen" finden demnach sehr bald (meist bis zu 48 Stunden) nach den vorherigen Ereignissen statt. Dies lässt sich leicht in einen Algorithmus umwandeln. Vielleicht erklärt dies die momentane Beschränkung der in Deutschland getesteten Software auf Wohnungseinbruch, denn dort wurde die Repeat Victimisation häufig getestet. Allerdings wurde die Hypothese laut der Studie in den USA auch auf Feuergefechte, KFZ-Diebstahl oder Raub ausgeweitet und später um die „Broken-Windows-Theorie" ergänzt.

Eine weitere theoretische Grundlage ist die „Routine-Activity-Theorie"[5], die regelmäßige Tätigkeiten untersucht und einbezieht. Zu diesen Routineaktivitäten gehören das Ausgehen am Wochenende, der Besuch von Großveranstaltungen oder das Pendeln zur Arbeit. Computergestützte Ansätze machen sich dies zunutze, indem Daten von Großveranstaltungen oder Verkehrsdaten eingebunden werden. In einer ähnlichen Herangehensweise wird ein Lifestyle Approach angenommen, der bestimmte Tätigkeiten nach Alter, Geschlecht, Einkommen, Familienstand oder Bildung zuschreibt. So kann etwa berücksichtigt werden, in welchen Gegenden Menschen mit hohem Einkommen oder wenig Bildung leben, woraus Rückschlüsse auf bevorstehende Straftaten gezogen werden können.

Insbesondere im urbanen Raum kann durch Predictive Policing eine ökonomische Effizienzsteigerung der Polizeiarbeit erfolgen. Durch die stetig wachsende Datengrundlage infolge moderner Technologien wird diese Technik seit einigen Jahren immer bedeutsamer. Dabei werden die Methoden zur Vorhersage bereits in anderen Branchen eingesetzt, so zum Beispiel bei der Vorhersage des Konsumverhaltens in Supermärkten. Beispielsweise können Zusammenhänge zwischen dem Kauf gewisser Artikel und bevorstehenden Wetterereignissen gezogen werden. Die amerikanische Supermarktkette Wal-Mart stellte dabei fest, dass Kunden vor derartigen Ereignissen gehäuft Wasserflaschen, Klebeband und Erdbeerkuchen kaufen. Die Verbindung der ersten beiden Artikel zu schlechten Wetterereignissen ist offensichtlich, die der Erdbeerkuchen jedoch nicht. Dennoch kann mithilfe von

4 | Vgl. Grove/Farrell 2011.
5 | Vgl. Pesch/Neubacher 2011.

statistischen Analysen eine derartige Verbindung aufgedeckt werden.[6] In gleicher Art und Weise können Zusammenhänge zwischen kriminalistisch relevanten Ereignissen durch die Techniken des Predictive Policing abgeleitet werden. Durch Untersuchung und Auswertung vergangener Ereignisse in lokaler Umgebung können zukünftige Verbrechen mit einer gewissen Konfidenz vorhergesagt werden.

Vor allem durch das Aufkommen der Massendaten und neuartiger Auswertungsmethoden hat Predictive Policing in den letzten Jahren stark an Popularität gewonnen.

Eine im Jahr 2008 veröffentlichte Studie bedient sich der Analyse wiederkehrender lokaler Muster, um das Auftreten von Schießereien im US-amerikanischen Philadelphia vorherzusagen.[7] Durch die Anwendung räumlich-zeitlicher Clusteringmethoden konnte gezeigt werden, dass das Auftreten einer erneuten Schießerei innerhalb von zwei Wochen und maximal einen Bezirk entfernt um 33 Prozent erhöht ist (siehe Abbildung 3).

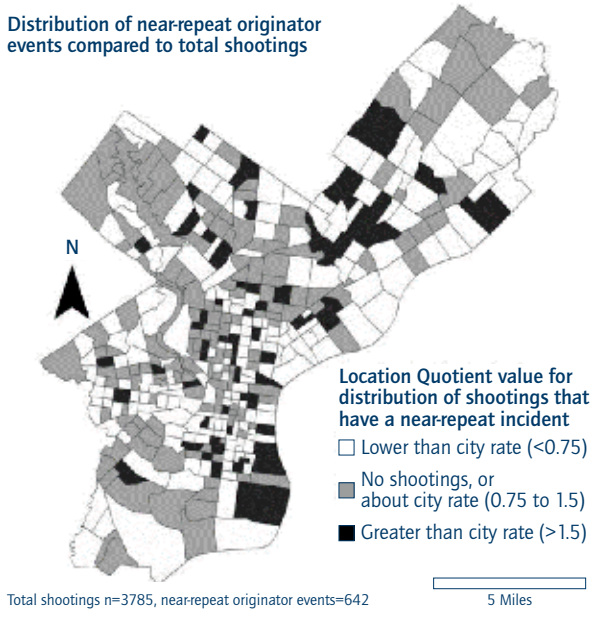


Abbildung 3: Vorhersage des Auftretens von Schießereien im räumlich-zeitlichen Umfeld von Philadelphia, USA (Quelle: Ratcliffe/Rengert 2008)

Vor allem in Bezug auf die Wiederholung von Straftaten kann Predictive Policing einen wertvollen Beitrag leisten. Eine Untersuchung aus dem Jahr 2012 analysierte das Auftreten von Einbruchsserien. Hierbei wurde gezeigt, dass zwischen Beginn und Ende der Serie selten mehr als sieben Tage liegen.[8] Auch der organisatorische Umfang der präventiven Bekämpfung derartiger Verbrechen kann durch den Einsatz von Predictive Policing besser abgeschätzt werden. Dies erweist sich jedoch als besonders anspruchsvoll, wenn – wie im Beispiel kurz andauernder Einbruchsserien – schnelles Eingreifen und Flexibilität in der Organisationsstruktur notwendig sind.

Generell sind die Aussichten des Vorhersagens sogenannter Kriminalitätshotspots vielversprechend. Insbesondere das Verwenden von aufgezeichneten Daten zur Bildung einer Hotspotkarte führt zu erfolgreichen Vorhersagen von Kriminalitätsschwerpunkten.[9]

Insbesondere die Anwendung auf urbane Systeme ist Gegenstand aktueller Forschung.[10] Dies beruht häufig auf der Annahme, dass sich Straftaten sowohl räumlich als auch zeitlich zuordnen lassen.[11] Dabei existieren zwei Grundannahmen: Die sogenannte Boost-Theorie besagt, dass durch einen Einbruch betroffene Häuser zukünftig noch weitere Straftäter anziehen, die die gute Gelegenheit weiter ausnutzen wollen (zum Beispiel nach dem ersten Einbruch ersetzte oder zurückgelassene Gegenstände). Konträr dazu geht die Flagged-Theorie davon aus, dass mehrere Einbrüche das Risiko für die Straftäter erhöhen: Die attraktiven Ziele sind bereits polizeibekannt oder markiert (flagged).

Auch die Vorhersage des wahrscheinlich nächsten räumlichen Ballungszentrums (Clusters) einer Verbrechensserie ist ein wichtiger Indikator, der für die Analyse herangezogen werden sollte. Wenngleich die konkrete Lokalisierung zukünftiger Cluster schwierig erscheint, zeigen sich gewisse Muster, die ein „Gleiten" in nahe Stadtgebiete widerspiegeln.[12]

Die Integration taggenauer Informationen in die Vorhersage von Kriminalitätshotspots erhöht die Chance, engere Zeitfenster angeben zu können, in denen ein Verbrechen wahrscheinlich stattfinden wird. Damit können vorhandene Ressourcen und Polizeikräfte effizienter und intelligenter verteilt werden.[13]

6 | Vgl. Katrandjian 2011.
7 | Vgl. Ratcliffe/Rengert 2008.
8 | Vgl. Haberman/Ratcliffe 2012.
9 | Vgl. Bowers 2004.
10 | Vgl. Groff 2007.
11 | Vgl. Johnson 2008.
12 | Vgl. Johnson 2004.
13 | Vgl. Tompson/Townsley 2010.

Studien haben gezeigt, dass die Vorhersage von Verbrechensschauplätzen an Genauigkeit gewinnt, sobald größere Datengrundlagen betrachtet werden. Am Beispiel von Seattle, USA, wurden Daten von 14 Jahren einbezogen, um den generellen Trend und die Verschiebung von Kriminalitätshotspots zu untersuchen.[14]

3 Simulation von Kriminalitätsausbreitung in urbanen Systemen

Für die Simulation der Dynamik räumlicher Prozesse können zelluläre Automaten (ZA) und Multi-Agenten-Systeme (MAS) verwendet werden. Zelluläre Automaten wurden erstmals in den 1940er Jahren von Stanislaw Ulam und John von Neuman entwickelt, um das Verhalten von Teilchen beim atomaren Zerfall zu beobachten. Dabei bestimmt ein einfaches Set von Regeln das Verhalten des ZA im Laufe der Zeit. Der zugrunde liegende zu simulierende Raum wird in Kompartimente (die namensgebenden Zellen) eingeteilt, die in Nachbarschaftsbeziehungen zueinander stehen. ZA stellen eine Möglichkeit dar, komplexe Interaktionen wie Schwarmverhalten und Selbstorganisation zu verstehen. Formal handelt es sich bei zellulären Automaten um eine Sonderform der deterministischen endlichen Automaten. Der grundlegende ZA lässt sich wie folgt definieren:

Sei Z eine Sequenz von Zellen, und in jeder Zelle $z \in Z$ wird ein Automat $A = (Q, q_0, \delta, q_+)$ platziert. Dabei ist Q die Menge an Zuständen, q_0 der neutrale Zustand, q_+ der akzeptierte Zustand und δ die Übergangsfunktion. Die Übergangsfunktion bildet von Q^3 auf Q ab. Die Definitionsmenge Q^3 besteht aus den Zuständen der Nachbarschaft des Automaten (linker und rechter Nachbar in einem eindimensionalen System) sowie dem Zustand des Automaten selbst. Die Zielmenge ist wiederum ein Zustand, der durch einen Regelsatz vorgeschrieben ist.[15]

Bei dieser Definition für ZA sind die Zellen streng geometrisch definiert und können durch regelmäßige sogenannte Parkettierungen abgebildet werden. In den 1970er Jahren wurde diese strenge Definition von ZA um eine flexiblere erweitert.[16]

Dabei sind die Nachbarschaftsbeziehungen nicht mehr durch angrenzende Geometrien bestimmt, sondern ergeben sich aus einem Graphen (siehe Abbildung 4).

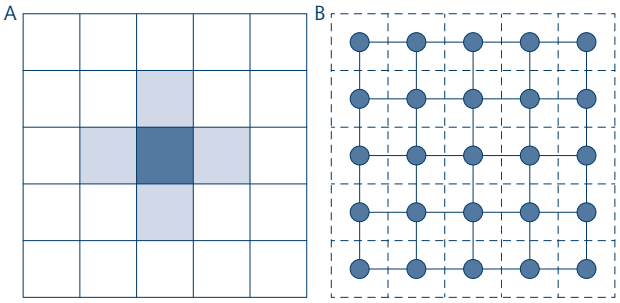


Abbildung 4: A zeigt die Parkettierung eines klassischen zweidimensionalen zellulären Automaten. B zeigt den gleichen Automaten mit einer dynamischen, auf Graphen basierenden Nachbarschaftsbeziehung (Quelle: eigene Darstellung).

Multi-Agenten-Systeme sind eine weitere Möglichkeit, das Verhalten komplexer Systeme zu modellieren und zu simulieren. Hierbei handelt es sich um ein Simulationssystem, angelehnt an das Forschungsfeld der verteilten künstlichen Intelligenz. Jeder sogenannte Agent ist eine Entität, die in Abhängigkeit ihrer Umgebung Handlungen vollführt. Dabei interagiert jeder Agent mit anderen Agenten in der unmittelbaren Umgebung und tauscht Informationen mit diesen aus.

Durch Kombination und Interaktion der beiden Konzepte MSA und ZA können sowohl unabhängig agierende Gruppen von Agenten als auch die eher statischen Rahmenbedingungen abgebildet werden. Dieses System aus MSA und ZA konnte bereits in der Planung von urbanen Systemen Anwendung finden.[17]

ZA bilden räumliche Elemente wie Straßen, Parzellen und Gebäude ab. Diese werden als örtlich fixierte Objekte behandelt, deren Zustände sich zu bestimmten Zeitpunkten verändern können. In einem ersten Abstraktionsschritt werden diese Elemente in die Zellen eines regelmäßigen Rasters übertragen und als Status einer solchen Zelle gespeichert (Abbildung 5: Ebene für fixierte Objekte). Eine zweite Ebene beinhaltet die individuellen und kollektiven urbanen Akteure, die im Folgenden als Agenten bezeichnet werden. Im Gegensatz zu den Zellen sind Agenten mobil und können sich frei über das Zellenraster, den zellulären Raum, bewegen. Es lassen sich verschiedene Arten der Kommunikation der Agenten untereinander sowie der Agenten mit den Zellen definieren (Abbildung 5: Ebene für mobile Agenten).

14 | Vgl. Weisburd et al. 2004.
15 | Vgl. Wolfram 1994.
16 | Vgl. Wu/Rosenfeld 1979.
17 | Vgl. König 2010.

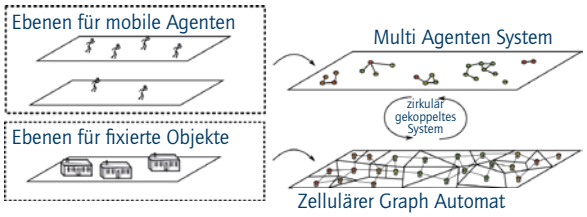


Abbildung 5: Für die Simulation der Dynamik räumlicher Prozesse können zelluläre Automaten (ZA) und Multi-Agenten-Systeme (MAS) verwendet werden (Quelle: eigene Darstellung).

Der Übergang von zellulären Automaten zu Graphen-Automaten stellt eine deutliche Verbesserung des Modells dar. Die Definition der Nachbarn durch einen Graphen führt zur flexiblen Modifizierung der Nachbarschaftsgeometrie, und die Nachbarschaftsbeziehungen können sich so jederzeit ändern. Im Umkehrschluss können nun auch Topologien (Nachbarschaftsgeometrien) gebildet werden, die eine Ausbreitung von Kriminalität hemmen beziehungsweise unterbinden. Die Ausbreitung eines Ereignisses (zum Beispiel Einbruch) wird im Wesentlichen von der Topologie beeinflusst; in der Zeitreihendarstellung (Abbildung 6) wird dies noch im Detail deutlich. In der Arbeit von Porta et al. werden verschiedene Szenarien der Topologieveränderung und deren Einfluss auf die Ausbreitung von Ereignissen detailliert dargestellt und diskutiert.

4 Anwendungsfälle von Predictive Policing

Im Sinne der oben dargestellten Definition von Predictive Policing lassen sich in erster Näherung zwei Fragestellungen ableiten:

- Wie verhält sich das Risiko in der Umgebung bei einem kriminellen Ereignis?
- Gibt es bestimmte Tage im Jahr, Wochentage, Tageszeiten, an denen kriminelle Ereignisse tendenziell öfter zu erwarten sind?

Beide Fragen können mit der Near-Repeat-Pattern-Analyse und einer zugrunde liegenden Kriminalstatistik beantwortet werden. Wiederholte Überfälle auf gleiche oder in der Nähe liegende Orte können als bedingte Wahrscheinlichkeit abgebildet werden: $P(A|x,t) \rightarrow P(B \mid x+\Delta x, t+\Delta t)$ und geben Aufschluss über

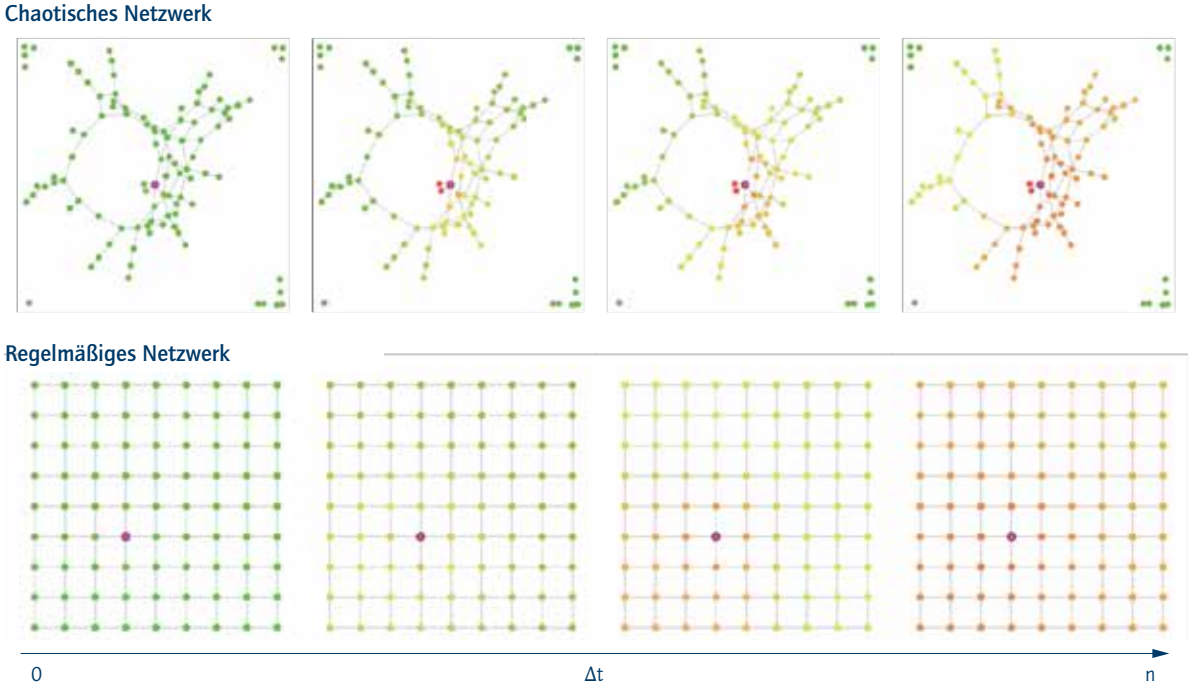


Abbildung 6: Darstellung des Einflusses der Topologie auf die zeitliche Ausbreitung von Ereignissen. Im oberen Panel ist die zugrunde liegende Topologie durch eine reale Nachbarschaftsbeziehung (chaotisches Netzwerk) dargestellt und im unteren Panel aus zellulärem Automat (regelmäßiges Netzwerk) (Quelle: eigene Darstellung).

den Einfluss eines Überfalls A an einem Ort x zur Zeit t zu einem späteren Zeitpunkt $t+\Delta t$ und an einem nahe gelegenen Ort $x+\Delta x$. Die Relationen für Zeit und Ort können aus Statistiken abgeleitet werden. Die Beantwortung der Frage nach dem Auftreten von kriminellen Ereignissen zu bestimmten Zeiten kann durch das Konzept des Cyclic-Load Forecasting abgebildet werden. Die Gleichung

P(Ereignis|Zeitpunkt)=P(**Ereignis**|Monat)+
P(**Ereignis**|Tag)+ P(**Ereignis**|Wochentag)+
P(**Ereignis**|Tageszeit)+ ...

kann zur Berechnung der Wahrscheinlichkeiten genutzt werden.

Diese Modelle können nun in den verschiedensten Szenarien verwendet und die Ausbreitung möglicher krimineller Ereignisse analysiert werden.

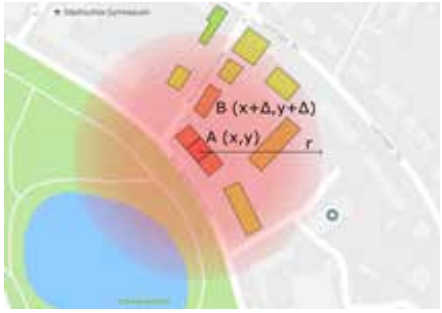
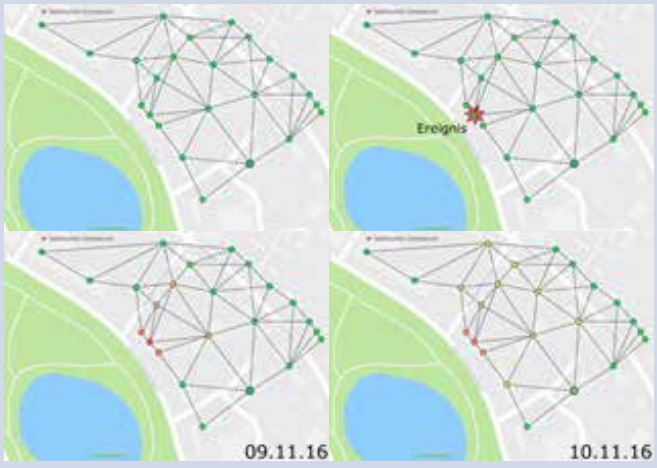
Szenario	Exemplarische Darstellung möglicher Ergebnisse
Die Werte aus der Near-Repeat-Pattern-Analyse, der Korrelation zwischen Ort und Zeit, können als sphärische Ausbreitung über einer urbanen Struktur abgebildet werden.	
Mithilfe von Graph-Automaten und einer Definition der benötigten Übergangswahrscheinlichkeiten kann die Ausbreitung von Ereignissen auf einer realen Topologie analysiert werden.	

Abbildung 7: Darstellung verschiedener Szenarien und der Ausbreitung eines möglichen kriminellen Ereignisses (Quelle: eigene Darstellung)

5 Verhältnis Sicherheit und Kriminalität

Im obigen Abschnitt wurden die Ausbreitungsprozesse von kriminellen Ereignissen beleuchtet. Um die eingangs aufgestellte Hypothese „Ist Sicherheit die Abwesenheit von Kriminalität?" zu beantworten, sollte ein Makro-Mikro-Modell herangezogen werden. Als Makroebene kann der Staat und dessen Systemverhalten eingeführt werden, als Mikroebene sind die Haushalte und deren Einzelentscheidungen definierbar. Beide Ebenen sind über einen Rahmen (Regeln, Vorgaben, Interessen und Verhaltensweisen) eng miteinander verbunden und haben Einfluss auf Strukturen und Phänomene. Die Phänomene und Strukturen wiederum haben Einfluss auf die ablaufenden Prozesse. So kann zum Beispiel eine Erhöhung der Kriminalitätsrate in einem abgeschlossenen urbanen System (zum Beispiel Land, Gemeinde, Stadt oder Stadtteil) zu spürbaren Veränderungen führen. Die Akteure können das System verlassen (Abwanderung durch Umzug) oder erhöhte technische Sicherheitsmaßnahmen (Sicherung von Hab und Gut, Bürgerwehren) vornehmen. Die Akteure stehen auf verschiedenen Ebenen in Wechselwirkung. Dies hat zur Folge, dass alle Handlungsträger gegenseitig aufeinander einwirken, indem sie gleichzeitig die Umgebung der anderen Handlungsträger darstellen und das gemeinsam erzeugte Handeln mitbestimmen. Die Verhaltensweisen sind nicht direkt, sondern nur über die Änderung gewisser Rahmenbedingungen beeinflussbar. Die Variation eines Parameters (zum Beispiel Erhöhung der Kriminalitätsrate) kann einen systemweiten Phasenübergang hervorrufen oder das makroskopische Verhalten eines Systems bestimmen. Kontrollparameter können eine den Intentionen entsprechende Wirkung nur dann entfalten, wenn die zirkulärkausale Verbindung zwischen den Ebenen (urbane Struktur und mobile Aktuare) Berücksichtigung findet, die auf einen Wirkungszusammenhang zwischen Prozessen, Strukturen und Phänomenen zurückgeführt werden kann.

Sowohl auf der Makro- als auch auf der Mikroebene werden die Verhaltensweisen der Handlungsträger dadurch bestimmt, dass sie stets versuchen, die negativen Faktoren zu minimieren und die positiven zu maximieren. Somit wirkt sich das Vorhandensein von Kriminalität direkt auf das Konzept Sicherheit aus. Die eingeführten Interessen, welche mit dem Begriff Sicherheit (im Sinne der Security-Definition) verbunden sind, stellen intrinsische Parameter dar. So sollen Terroranschläge oder Einbruchsserien verhindert und die Sicherheit auf den verschiedenen Ebenen (gesetzliche, technische und gefühlte) maximiert werden.

Somit können Maßnahmen, die mit der Maximierung beziehungsweise Optimierung von Sicherheit in diesem Kontext einhergehen, auf der Grundlage der Analyse von Kriminalität in urbanen Systemen direkt abgeleitet und umgesetzt werden.

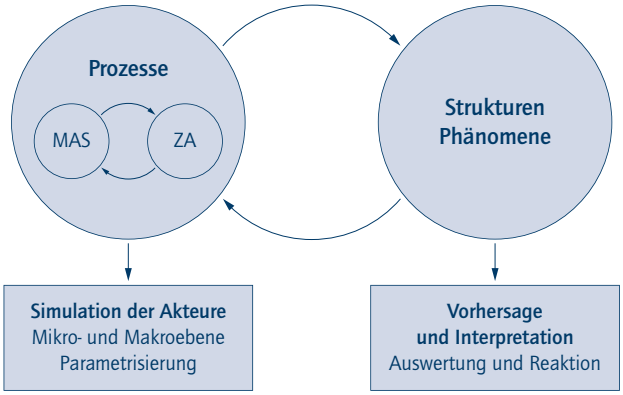


Abbildung 8: Innerer Zusammenhang von Prozessen, die durch zelluläre Automaten und ein Multi-Agenten-System beschreibbar sind, und den Strukturen und Phänomenen der Gesellschaft und/oder der urbanen Struktur (Quelle: eigene Darstellung)

Danksagung

Der Autor möchte sich an dieser Stelle bei den Mitarbeitern und Mitarbeiterinnen der Arbeitsgruppe FoSIL (Forensic Science Investigation Lab) bedanken. Nur durch deren Unterstützung konnte dieses Manuskript erstellt werden.

Literatur

Bowers 2004
Bowers, K. J.: „Prospective Hot-Spotting: The Future of Crime Mapping?". In: *The British Journal of Criminology 44(5)* 2004, S. 641–658.

Foster 2004
Foster, A. K. (Hrsg.): Moral Visions and Material Ambitions: Philadelphia Struggles to Define the Republic, 1776-1836, Lexington: Lexington Books 2004, S. 147.

Groff 2007
Groff, E. R.: „Simulation for Theory Testing and Experimentation: An Example Using Routine Activity Theory and Street Robbery". In: *Journal of Quantitative Criminology 23(2)* 2007, S. 75–103.

Grove/Farrell 2011
Grove, L./Farrell, G.: *Repeat Victimization, in Criminology,* 2011. URL: http://dx.doi.org/10.1093/obo/9780195396607-0119 [Stand: 31.07.2017].

Haberman/Ratcliffe 2012
Haberman, C. P./Ratcliffe, J. H.: „The Predictive Policing Challenges of Near Repeat Armed Street Robberies". In: *Policing 6(2)* 2012, S. 151–166.

Härter 2013
Härter, K.: „Kriminalität". In: Cordes, A. et al. (Hrsg.): *Handwörterbuch zur deutschen Rechtsgeschichte*, 2. Auflage, Berlin: Erich Schmidt Verlag GmbH & Co. 2013, S. 271–275.

Johnson 2008
Johnson, S. D.: „Repeat Burglary Victimisation: A Tale of Two Theories". In: *Journal of Experimental Criminology 4(3)* 2008, S. 215–240.

Johnson 2004
Johnson, S. D.: „The Stability of Space-Time Clusters of Burglary". In: *The British Journal of Criminology 44(1)* 2004, S. 55–65.

Johnson 2007
Johnson, S. D. et al.: *Prospective Crime Mapping in Operational Context. Final Report*, 2007. URL: http://library.college.police.uk/docs/hordsolr/rdsolr1907.pdf [Stand: 31.07.2017].

Katrandjian 2011
Katrandjian, O., ABC News: „Hurricane Irene: Pop-Tarts Top List of Hurricane Purchases", 2011. URL: https://abcnews.go.com/US/hurricanes/hurricane-irene-pop-tarts-top-list-hurricane-purchases/story?id=14393602 [Stand: 31.07.2017].

König 2010
König, R: *Simulation und Visualisierung der Dynamik räumlicher Prozesse: Wechselwirkungen zwischen baulichen Strukturen und sozialräumlicher Organisation städtischer Gesellschaften*, Berlin: Springer Verlag 2010.

Pesch/Neubacher 2011
Pesch, B./Neubacher, F.: „Der Routine Activity Approach – Ein vielseitiges Instrument der Kriminologie". In: *Jura Heft 3/2011*, S. 205–209.

Ratcliffe/Rengert 2008
Ratcliffe, J. H./Rengert, G. F.: „Near-Repeat Patterns in Philadelphia Shootings". In: *Security Journal 21(1-2)* 2008, S. 58–76.

Schäfers/Zapf 2013
Schäfers, B./Zapf, W. (Hrsg.): *Handwörterbuch zur Gesellschaft Deutschlands*, Berlin: Springer Verlag 2013.

Schmidt-Semisch/Hess 2014
Schmidt-Semisch, H./Hess, H. (Hrsg.): *Die Sinnprovinz der Kriminalität – Zur Dynamik eines sozialen Feldes*, Berlin: Springer Verlag, 2014. S. 17–46.

Tompson/Townsley 2010
Tompson, L./Townsley, M. K.: „(Looking) Back to the Future: Using Space – Time Patterns to Better Predict the Location of Street Crime". In: *International Journal of Police Science & Management 12(1)* 2010, S. 23–40.

Weisburd 2004
Weisburd, D. et al.: „Trajectories of Crime at Places: A Longitudinal Study of Street Segments in the City of Seattle*". In: *Criminology. An Interdisciplinary Journal 42(2)* 2004, S. 283–322.

Wolfram 1994
Wolfram, S.: *Cellular Automata and Complexity: Collected Papers*, Boston: Addison-Wesley Longman 1994.

Wu/Rosenfeld 1979
Wu, A./Rosenfeld, A.: „Cellular Graph Automata. I. Basic Concepts, Graph Property Measurement, Closure Properties". In: *Information and Control 42(3)* 1979, S. 305–329.

8.4 Strukturen für die Gefahrenerkennung und -behandlung in autonomen Maschinen

Dr. Mario Gleirscher
Department of Computer Science, University of York und
Fakultät für Informatik, Technische Universität München

In diesem Abschnitt werden hochautomatisierte – insbesondere autonom handelnde – Maschinen (AM) wie zum Beispiel autonome mobile Roboter betrachtet. Man erwartet von solchen Systemen, dass deren Regelungen in Gefahrensituationen ebenso nützliche Handlungsalternativen bieten wie im Normalbetrieb. Ausgehend von dieser Problemstellung wird nun eine werkzeuggestützte Herangehensweise

i. für die Modellierung von Gefahrensituationen sowie

ii. für die Bewertung der Plausibilität und Vollständigkeit solcher Modelle

anhand eines Beispiels aus dem Bereich des automatisierten Fahrens (AF) diskutiert.

1 Motivation

Im Rahmen der gefahrenreduzierenden Absicherung von Systemen ist es eine Herausforderung, möglichst starke Sicherheitseigenschaften für autonome, hochautomatisierte Maschinen schon zum Entwurfszeitpunkt festzulegen und Regler solcher Maschinen für die Einhaltung dieser Eigenschaften zur Laufzeit zu entwerfen. Im Folgenden werden formale Strukturen, welche für die Modellbildung und später für die detaillierte Entwicklung von Reglern hilfreich sind, besprochen. Die Motivation, solche Strukturen zu nutzen, resultiert aus

- Bestrebungen, die Risikobewertung und den Verlässlichkeitsnachweis für allgemeine Systemklassen durch spezialisierte Modellbildung zu unterstützen (siehe Kapitel 4/ Bertsche et al.),
- Erfahrungen in der Architekturabsicherung komplexer eingebetteter Systeme[1] und
- der Beobachtung, dass einige Empfehlungen für die Gewährleistung von AM-Sicherheit nicht eindeutig und vollständig sind.[2]

2 Hintergrund

In diesem Abschnitt werden einige Begriffe aus der Literatur und Vorarbeiten des Autors dargestellt, auf denen die spätere Diskussion aufbaut.

2.1 Allgemeine Grundlagen

In der Risikoanalyse wird bewertet, inwiefern eine Gefahrenquelle (Aggressor) ein Risiko für ein Schutzziel (zum Beispiel Safety, Security, körperliche Unversehrtheit) eines Schutzobjekts (im Englischen: asset) darstellt und inwieweit ein Schutzmechanismus (auch Beschützer, Sicherheitsfunktion) dieses Risiko wenigstens auf ein akzeptables Restrisiko[3] reduzieren kann. Häufig wird dazu eine Menge wahrscheinlicher Szenarien in Form von potenziell unendlichen Ursache-Wirkungs-Ereignisketten betrachtet, wobei die ultimativen und unerwünschten Auswirkungen als Unglücks-, Unfalls- oder Schadensereignis und alle Ereignisse auf diesem Wege als Zusammensetzung von potenziell verursachenden Faktoren beschrieben werden. Hierzu wird weiter unten von Kausalfaktoren und -strukturen gesprochen. Ein kompatibler Begriffsrahmen wird in den Kapiteln 3/Schnieder und Schnieder, 5/Beyerer und Geisler sowie 7.1/Vieweg ausführlicher behandelt.

Dieser vielfach diskutierte Begriffsrahmen lässt sich auf ganz unterschiedliche Bereiche anwenden, zum Beispiel technische Anlagen, IT-Systeme, in der Patientenbehandlung im Krankenhaus, im unternehmerischen Projektmanagement, in Arbeitsprozessen im Hochbau oder an Flughäfen (siehe Kapitel 8.1/Wolf und Lichte sowie 8.2/Deutschmann et al.). Je nach Art des Schutzziels und -objekts gibt es spezifische Herangehensweisen zur RA sowie verschiedene Bezeichnungen, wie zum Beispiel funktionale Sicherheit in der Mechatronik und Automatisierungstechnik[4] oder Cyber Security für stark vernetzte IT-Systeme.[5] Regelmäßig wird versucht, Erkenntnisse aus verschiedenen Arbeitsfeldern

1 | Vgl. Kugele et al. 2017.
2 | Vgl. Alexander et al. 2009.
3 | Vgl. McDermid 2001 und Kumamoto 2007 diskutieren „As Low As Reasonably Practicable" (ALARP).
4 | Vgl. Schnieder/Schnieder 2009, Schnieder/Schnieder 2008, Schnieder/Drewes 2008.
5 | Vgl. Lund et al. 2011.

wieder zusammenzuführen.[6] Hierfür ist es wichtig, eine gemeinsame[7] Begriffswelt zu finden, wie dies zum Beispiel auch im Kapitel 7.2/Raabe für RA im Datenschutz erfolgt.

Schon vor oder im Rahmen der RA beginnt man üblicherweise mit

i. der Identifikation von Gefahrenquellen und Schadensereignissen gemeinsam mit dem Verstehen der zugrunde liegenden Kausalstrukturen,

ii. der Bewertung von Eintrittswahrscheinlichkeiten und Folgenschweregraden sowie

iii. der Entwicklung von Maßnahmen zur Risikoreduktion.

Zur systematischen Durchführung, Vervollständigung und Plausibilisierung der RA werden oft auch spezielle Modelle des Regelkreises, insbesondere des zu regelnden Prozesses, genutzt.[8]

Im Folgenden wird davon ausgegangen, dass solche Modelle für die RA von und in autonomen Maschinen entwickelt und genutzt werden können. Die Aufgabe besteht in der Entwicklung hochwertiger Schutzmechanismen in solchen Maschinen bei Betrieb.

2.2 Eigene Vorarbeiten

RA-Methodik

Diesem Beitrag gingen Arbeiten[9] in folgenden Bereichen voraus:

- Kernkonzepte und -schritte einer RA wurden in den Formalismus von Transitionssystemen übertragen,
- ein iteratives Vorgehen zur Absicherung von Systementwürfen wurde entwickelt,
- wesentliche Abstraktionsschritte in der RA – Regelkreismodell, Prozessmodell, Kausalstruktur – wurden identifiziert,
- Schlüsselwörter oder Eigenschaftsmuster für die Gefahrenquellenidentifikation (vgl. HazOp) wurden festgelegt und
- Entwurfsmuster für Schutzmechanismen (zum Beispiel Fail-Operational, Fail-Silent) wurden entsprechend formalisiert.

Kausalstrukturen

Im Folgenden werden der Aufbau und der Umgang mit Kausalstrukturen, einer Anwendung von Transitionssystemen, thematisiert.[10] Dazu werden nun einige Grundlagen eingeführt:

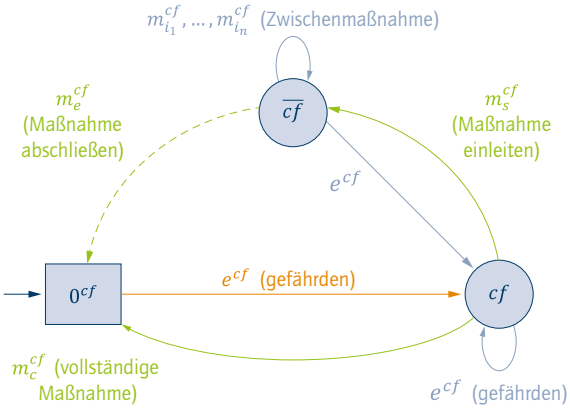


Abbildung 1: Phasenmodell für einen Kausalfaktor cf. Kausalfaktoren cf für die Schadensmodellierung nutzen nur die Phasen 0cf und cf. Graue Transitionen werden nicht besprochen; sie weisen auf erweiterte Varianten dieses Phasenmodells (Quelle: eigene Darstellung).

Zentraler Bestandteil einer Kausalstruktur ist der Kausalfaktor, für dessen Modellierung das in Abbildung 1 gezeigte Phasenmodell[11] genutzt wird. Es gibt im Prozess je Kausalfaktor cf die Phasen „inaktiv" (0^{cf}), „aktiv" (cf) und „entschärft" ($\overline{cf}$) sowie die Basisaktionen „gefährden" (e^{cf}), „Reduktionsmaßnahme einleiten" (m_s^{cf}) und „Reduktionsmaßnahmen abschließen" (m_e^{cf}). Eine Kausalstruktur kann dann durch Komposition mehrerer Phasenmodelle zusammengesetzt werden. Die endlichen Mengen aller

6 | Vgl. Schneider et al. 2017.
7 | Vgl. zum Beispiel Freiling et al. 2013 zur Klärung von Safety versus Security.
8 | Leveson 2012 schlägt eine vereinfachte Variante dessen vor.
9 | Vgl. Gleirscher 2014, S. 33.
10 | Vgl. Baier/Katoen 2008.
11 | Gleirscher/Kugele 2017 besprechen eine Variante mit zusätzlicher Schadensphase.

- Kausalfaktoren werden mit H,
- Gefährdungsaktionen mit E und
- Reduktionsaktionen mit M

bezeichnet, wobei $E \cap M = \emptyset$ und $A = E \cup M$. Aus der in Vorarbeiten[12] beschriebenen Komposition geht damit stets eine endliche Kausalstruktur $R = (\Sigma, A, \Delta)$ als gerichteter Graph hervor: Dabei ist der Raum von Basiszuständen (Basisereignissen), welcher in

- sichere Zustände, in denen kein $cf \in H$ aktiv ist, und
- Risikozustände (auch Gefahrensituationen), in denen mindestens ein cf aktiv ist,

partitioniert wird. Dazu wird die Abbildung $phase: \Sigma \times H \to \{0^{cf}, cf, \overline{cf}\}$, welche für einen Zustand $\sigma \in \Sigma$ die Phase eines Kausalfaktors $cf \in H$ liefert, genutzt. Basiszustände sind durch Basisaktionen entsprechend der Komposition der über H instantiierten Phasenmodelle verbunden. Man erhält eine Transitionsrelation $\Delta \subseteq \Sigma \times A \times \Sigma$. Δ^* bezeichnet die Menge aller zyklenfreien (also endlich langen) Pfade in Δ. Für die folgende Diskussion werden Projektionen von R benötigt: Für $H' \subseteq H$ bezeichnet $R|_{H'} = (\Sigma|_{H'}, A|_{H'}, \Delta|_{H'})$ die Abbildung von R auf die Komposition der Phasenmodelle für H'.

Von Bedeutung in R ist die Risikopriorität eines Zustands $\sigma \in \Sigma$, welche sich aus der Eintrittswahrscheinlichkeit und dem Schweregrad eines von σ aus erreichbaren Schadensereignisses σ_m ergibt. Bildet man eine Kausalstruktur auf ein Markov-Modell ab, so kann man fragen, zu welchen Zeitpunkten sich die Eintrittswahrscheinlichkeiten von σ und σ_m in kritischen Bereichen aufhalten. Die Schätzung des Schweregrads kann unabhängig davon auf einer qualitativen Skala erfolgen.[13]

Der Kausalstruktur zugrunde liegend werden hier ein qualitativ-diskretes Modell des Prozesses P[14] sowie der eigentlich kontinuierliche Regelkreis betrachtet. Im Folgenden heißt die Menge aller durch das Prozessmodell beschriebenen Abläufe $[[P]]$. Durch den Einsatz von Kausalstruktur und Prozessmodell erhält man ein regelkreisbasiertes, vorerst abstraktes Entwurfsverfahren für Laufzeitschutzmechanismen für autonome Maschinen.

2.3 Beitrag, Überblick und Querbezüge

In diesem Beitrag

- erfolgen eine Vereinfachung des Phasenmodells aus Vorarbeiten[15] und dessen Erweiterung um Risiko- und Schadenszustände sowie die damit erleichterte Behandlung von Kombinationen mehrerer Schadensereignisse,
- gelten Schadensereignisse nicht mehr als Phasen je Kausalfaktor, sondern als finale Kausalfaktoren mit den Phasen *nicht eingetreten* (0^m) und *eingetreten* (m),[16]
- gelten Schadensereignisse somit auch als finale Zustände $\subset \Sigma$ mit mindestens einem aktiven finalen Kausalfaktor, womit Σ weiter partitioniert wird.

Darüber hinaus werden ein für autonome Maschinen charakteristisches Schutzziel (Abschnitt 3.1), Zustandsraumvereinfachungen auf Basis der Zusammenfassung von (a) Zustandsmengen und (b) auf gleiche Reduktionsaktionen abgebildeten Basisaktionen (Abschnitt 3.2) sowie ein entsprechendes Beispiel beschrieben (Abschnitt 4). Zur Anfertigung des Beispiels dient das Analysewerkzeug Yap.[17]

Querbezüge zu den Beiträgen dieses Bandes

Da Kausalstrukturen schrittweise aufgebaut und weiterentwickelt werden können, lassen sie sich in die meist iterativ und inkrementell durchzuführenden Kernaktivitäten des Systems Engineering – insbesondere der RAMSS-Aspekte nach Kapitel 2/Schlüter und Winzer) – von autonomen Systemen eingliedern.

In Kapitel 3/Schnieder und Schnieder (Unterabschnitte 4 bis 6) ist eine Abbildung der besprochenen Begrifflichkeiten auf stochastische Petri-Netze und Markov-Ketten zu finden. Das Modell der Risikogenese lässt sich durch Verfeinerung des in Abbildung 1 gezeigten Phasenmodells sowie durch die Abbildung in eine Kausalstruktur darstellen. Kausalstrukturen eignen sich damit einhergehend auch zur Untersuchung der im Kapitel 8.6/Arens vorgestellten Anwendung einer Ereignisbaumanalyse (ETA).

12 | Vgl. Gleirscher/Kugele 2017.
13 | Vgl. Lund et al. 2011, Kapitel 8.2.3.
14 | Gleirscher 2017a zeigt zum Beispiel die Zerteilung der Mobilitätsaufgabe unter Anwendung verschiedener Dekompositionskriterien.
15 | Vgl. Gleirscher 2017a; Gleirscher/Kugele 2017.
16 | Damit wird die Aktion zu einer Gefährdungsaktion in einem finalen Zustand.
17 | Vgl. Gleirscher 2017b.

Beyerer und Geisler schlagen im Kapitel 5/Beyerer und Geisler eine Klassifikation von Kausalfaktoren vor, um Safety- und Security-Fragestellungen innerhalb eines formalen Rahmens zu behandeln. Ferner unterstützt das dort besprochene Modell die Entwicklung einer wahrscheinlichkeits- und spieltheoretischen Semantik für Transitionen in Kausalstrukturen. Somit können Kausalstrukturen zur Charakterisierung des in Kapitel 5 beschriebenen Transitionsoperators Φ^k zwischen zwei logischen Zeitschritten $(k,k+1)$ herangezogen werden.

Kapitel 7.1/Vieweg (Unterabschnitt 3) diskutiert die Reduktion und organisatorische Handhabung der Vielfalt von Risiken und Maßnahmen anhand eines Risikorasters. Kausalstrukturen eignen sich für den systematischen Umgang mit mehreren zueinander in Beziehung stehenden Risikorastern aus der Betrachtung komplexerer Systeme.

Den Kausalstrukturen liegt ebenso wie Kapitel 8.5/Weyer die Arbeitsannahme[18] zugrunde, dass Schadensereignisse viele und insbesondere mehrschichtige Ursachen haben können und dies besonders gut durch frühzeitige, disziplinübergreifende RA sowie durch regelkreisbasierte Modellbildung ergründet werden kann. Die dort beschriebene agentenbasierte Modellierung kann zur Beschreibung des zu regelnden Prozesses für AM-Kollektive herangezogen werden.

2.4 Verwandte Arbeiten

Die Elemente der Kausalstruktur sind angelehnt an die Denkmodelle in klassischen Methoden wie der Fehlerauswirkungs (FMEA)- und Fehlerbaumanalyse (FTA), insbesondere an einschlägigen Taxonomien.[19]

Eine besonders anschauliche Art der Risikoanalyse und -modellierung zeigt der CORAS-Ansatz, welcher eine grafische Darstellung für Kausalstrukturen sowie Berechnungsvorschriften für zusammengesetzte Ereigniswahrscheinlichkeiten und -frequenzen unter der Berücksichtigung von Unsicherheiten bietet.[20]

Die kürzesten Gefährdungspfade in R von Zustand 0 zu einem Risikozustand oder Schadensereignis können als minimale Schnittsequenzen (im Englischen: minimal cut sequences) einer dynamischen FTA aufgefasst werden.[21] Im weiter unten eingesetzten Analysewerkzeug Yap können ODER-Gatter derzeit noch nicht direkt dargestellt werden, was die Modellierung aufwendiger gestaltet. Auch die in Yap angebotenen Direktiven für die Zustandsraumeinschränkung (Abschnitt 4) erreichen aus Gründen der Einfachheit noch nicht die Ausdrucksstärke klassischer Aussagenlogik. Kausalstrukturen (Abschnitt 3.2) haben diesbezüglich jedoch keine Einschränkungen.

Darüber hinaus bespricht Kumamoto (2007)[22] eine Modellierungsweise eng verwandt mit der hier diskutierten Anwendung von Kausalstrukturen zuzüglich der Abbildung auf ein Markov-Modell am Beispiel einer degradierungsfähigen elektronischen Lenkung.

3 Strukturen für Laufzeitrisikoreduktionsplanung

Dieser Abschnitt beschreibt zuerst ein Schutzziel (Abschnitt 3.1) und darauf aufbauend die Herleitung der in Abschnitt 2 eingeführten Kausalstrukturen für die Laufzeitrisikoreduktionsplanung (Abschnitt 3.2).

3.1 Festlegung von Planungszielen aus Sicherheitseigenschaften

Das Schutzziel beziehungsweise die gröbste Sicherheitseigenschaft, die hier betrachtet wird, ist die Vermeidung von Schadensereignissen sowie die Beibehaltung einer möglichst geringen Distanz zu sicheren Zuständen. Zur Laufzeitrisikoreduktionsplanung[23] dient nun folgendes Ziel:

Eigenschaft 1: Ein optimaler AM-Regler (AMR) versucht so oft wie möglich, einen b-sicheren[24] Zustand in Bezug auf (i) die erfasste Situation beziehungsweise Aktivität im Prozess, (ii) den vorhersagbaren Zustandsraum und (iii) die verfügbaren Reduktionsaktionen zu erreichen und zu erhalten.

18 | Vgl. Leveson 2012.
19 | Vgl. Schnieder/Schnieder 2009.
20 | Vgl. Lund et al. 2011, Kapitel 13.
21 | Vgl. Dugan et al. 2007.
22 | Vgl. Kumamoto 2007, Kapitel 8.3.
23 | Vgl. Gleirscher 2017a, Abschnitt 6.2.
24 | bezeichnet ein maximales „Risikobudget" zur Darstellung des akzeptablen Restrisikos, siehe Abschnitt 2.1.

Auf Basis von Kausalstrukturen (Abschnitt 2.2) kann nun folgende vereinfachte[25] Variante von Eigenschaft 1 betrachtet werden:

Eigenschaft 2: Der AMR führt zu jedem Zeitpunkt und vom jeweils aktuellen Risikozustand σ jene Sequenz π an verfügbaren Reduktionsaktionen durch, (i) welche unter allen s-erreichbaren[26] Zuständen zu einem Zustand σ' mit der kleinsten Anzahl an aktiven Kausalfaktoren und zu keinen Zuständen σ'' gefährlicher als σ führt und (ii) welche sowohl die kürzeste unter allen derzeit möglichen Sequenzen ist als auch die maximale Anzahl an Betriebsfunktionen aufrechterhält.

Gebe $\mathrm{time}\colon \Delta^* \dashrightarrow \mathrm{N}_0$ die Laufzeit eines Pfades in Δ^* zurück. Der Risikoreduktionspfad $\sigma \xrightarrow{\pi} \sigma'$ im Zeitintervall $[t,t+\mathrm{time}(\pi)]$ erlaubt nun die Betrachtung zweier Ergebnisaspekte:

- Man kann das System zum Zeitpunkt t als (l, p, e)-sicher bewerten, wenn σ' eine Risikopriorität $< l$ hat und mit einer Erfolgswahrscheinlichkeit $> p$ sowie einem Aufwand beziehungsweise Verlust $< e$ erreichbar ist.
- Darüber hinaus kann die sichere Region $\subset\Sigma$ zum Zeitpunkt $t+\mathrm{time}(\pi)$ als die Menge aller Zustände festgelegt werden, deren Risikopriorität $< l$ ist.[27]

Damit kann auch für einen Ablauf $\rho\in[[P]]$ konstatiert werden, zu welchen Zeitpunkten p akzeptabel (l, p, e)-sicher ist – im Speziellen, zu welchen Zeitpunkten p in der sicheren Region ist.

3.2 Konstruktion von Kausalstrukturen zur Risikoreduktionsplanung

Seien nun das Schutzziel in Eigenschaft 2 sowie ein Zustandsraum Σ (Abschnitt 2.2) aus der RA gegeben. Für die Konstruktion eines Planungsmodells R werden nun

- die Vereinfachung von Σ und
- die schrittweise Planung von einem spezifischen Risikozustand σ aus besprochen.

Vereinfachung von Kausalstrukturen

Diese sind besonders bei komplexem R maßgeblich, um die Laufzeitplanung effizienter oder überhaupt erst möglich zu machen.

Neben den Erreichbarkeitseinschränkungen,[28] mit denen die Komposition von Phasenmodellen (Abbildung 1) und damit die Erreichung von Zuständen gesteuert werden kann, können weitere Vereinfachungen angewandt werden:

Gegeben sei eine Kausalstruktur $R=(\Sigma,A,\Delta)$. Aufbauend auf bereits angedeuteten Äquivalenzen[29] über Σ seien im Folgenden die drei Relationen $\approx_{h'}, \approx_{h_m}$ und $\approx_m$ über $\Sigma\times\Sigma$ gegeben. Es handelt sich hierbei um Äquivalenzrelationen:

Gefährdungsäquivalenz:
Es gilt $\sigma_1 \approx_h \sigma_2$ genau dann, wenn

$$\forall h\in H:\mathrm{phase}(\sigma_1,h)\in\{cf,\overline{cf}\}\Leftrightarrow\mathrm{phase}(\sigma_2,h)\in\{cf,\overline{cf}\}$$

Reflexivität und Symmetrie werden durch die Bi-Implikation in dieser Definition induziert, Transitivität erfolgt durch den per $\forall$-Quantor geforderten paarweisen Vergleich der Phasen.

Schadensäquivalenz:
Zwei Zustände $\sigma\_1,\sigma\_2\in\Sigma$ sind äquivalent bezüglich $\approx_{h_m}$, wenn sie dieselben aktiven finalen Kausalfaktoren – also Schadensereignisse – aufweisen.[30] Es gilt dann $\sigma_1 \approx_{h_m} \sigma_2$. Für $\approx_{h_m}$ sind Reflexivität, Symmetrie und Transitivität leicht zu erkennen. Aufgrund des verallgemeinerten Phasenmodells und der in Abschnitt 2.3 beschriebenen Partitionierung in Risiko- und Schadenszustände gilt zudem $\approx_{h_m} \subset \approx_h$.

Reduktionsäquivalenz:
Es gilt $\sigma_1 \approx_m \sigma_2$ genau dann, wenn

$$\sigma_1 \underset{h}{\approx} \sigma_2 \wedge \forall h \in \mathcal{H}: phase(\sigma_1, h) \underset{h}{\succ} cf \Leftrightarrow phase(\sigma_2, h) \underset{h}{\succ} cf \ .$$

Für $\approx_m$ ergeben sich die Äquivalenzeigenschaften zusätzlich zu jenen von $\approx_h$ noch aus der logischen Konjunktion.

Diese drei Äquivalenzen können in den folgenden beiden Vereinfachungsregeln für R genutzt werden:

Regel *mis*:
Es erfolgt die Bildung von Äquivalenzklassen $[\Sigma]_{\underset{hm}{\approx}}$ und die Umwandlung von Σ durch beliebige Wahl eines Repräsentanten pro

25 | Man müsste Risikozustände und Basisaktionen mehrfach parametrisieren, was den Rahmen dieses Beitrags sprengen würde.
26 | s bezeichnet die betrachtete Höchstzahl an Reduktionsaktionen in π.
27 | Zur Konsistenz besteht die Forderung, dass sich alle sicheren Zustände in der sicheren Region befinden (vgl. Abschnitt 2.2).
28 | Vgl. Gleirscher 2017a.
29 | Vgl. Gleirscher/Kugele 2017.
30 | Hier wird der Einfachheit halber nicht zwischen Unfall- oder Unglücksereignissen und dem damit einhergehenden Schaden unterschieden. Diese Unterscheidung lässt sich jedoch als Parameter in das Modell einführen.

Klasse und Zusammenfassung der jeweiligen Transitionen in eine abstraktere Kausalstruktur $R'=(\Sigma',A,\Delta')$.

Regel *mit*:
Gegeben sei eine Menge M' „leistungsfähiger" Reduktionsaktionen sowie eine partielle Abbildung $\alpha_m:\Delta^*\dashrightarrow M'$ wobei $M\cap M'=\emptyset$. Für $a,b\in H$ und $R|_{\{ab\}}$ mit $\Sigma|_{\{ab\}}=\{a,b,ab,\bar{a},\bar{b},\bar{a}b,a\bar{b},\overline{ab}\}$ kann man die Zustände $\{\bar{a},\bar{b},\bar{a}\bar{b},a\bar{b},\overline{ab}\}$ als äquivalent bezüglich $\approx_h\cup\approx_m$ behandeln. $\overline{ab}$ sei nun der bezüglich der Reduktionsordnung $\preccurlyeq_m$ Größte beziehungsweise „Beste". α_m ist für jeden Pfad in $\Delta^*|_{\{ab\}}$ definiert, welcher mit a oder b startet und in $\overline{ab}$ endet. Bezüglich R gibt es nun Äquivalenzklassen $[\Sigma]_{\approx_h\cup\approx_m}$, Transitionen in Δ auf allen Pfaden $\pi\in\Delta^*$, für welche $\alpha_m(\pi)$ definiert ist, werden eliminiert und unerreichbare Zustände entfernt. Man erhält somit eine abstraktere Kausalstruktur $R'=(\Sigma',A\cup M',\Delta')$ mit $\Sigma'\subseteq\Sigma$ und $\Delta'\subset\Delta$.

Die Regel *mis* nutzt den einfachen Umstand, dass es bei Schadensereignissen nur mehr auf die finalen Kausalfaktoren und deren Phasen ankommt, und kann somit als universell anwendbar definiert werden.

Die Regel *mit* fasst auf dieselben Reduktionsaktionen abbildbare Sequenzen von Basisaktionen zusammen. Damit wird die Leist- oder Abdeckungsfähigkeit zur Verfügung stehender Reduktionsaktionen ausgereizt, was durch $\mathrm{dom}(\alpha_m)$ dargestellt wird. Die Anwendung der Regel *mit* erfordert, dass a und b „kompatibel" im Sinne der anzuwendenden Reduktionsaktion m^{ab} sind.

Es kann eine ganze Reihe weiterer Vereinfachungsregeln definiert werden, was den Rahmen dieses Beitrags allerdings ebenso sprengen würde.

Planung auf Kausalstrukturen

Nach Anwendung der Vereinfachungsregeln *mis* und *mit* auf R kann nun die Planung im Kontext des Schutzziels (Eigenschaft 2) beschrieben werden.

Wie sieht die Planung aus?

Das betrachtete System ist zu jedem Zeitpunkt durch eine Situation $S\in[[P]]$, eine Kausalstruktur $R_S=(\Sigma_S,A_S,\Delta_S)$ und einen Zustand $\sigma\in\Sigma_S$ bestimmt:[31]

1. Erst wird eine Breitensuche auf R_S ausgehend von σ unter Berücksichtigung der Pfadkriterien von Eigenschaft 2 durchgeführt.
2. Dann wird aus der (in der Regel einelementigen) Menge der lokal optimalen Sequenzen zufällig eine Sequenz π ausgewählt und deren Durchführung durch den AMR gestartet.
3. Gleichzeitig werden das Tupel (S,R_S,σ) sowie die Informationen für R_S aktualisiert und π so lange durchgeführt, bis das verbleibende Suffix von durch eine bezüglich Eigenschaft 2 bessere Sequenz π' ersetzbar ist.
4. Die Reduktionsbemühungen des AMR enden spätestens, wenn π abgearbeitet ist.

In diesem noch qualitativen Modell ist der Suchraum sehr übersichtlich, sodass der hier gezeigte Planungsansatz noch sehr naiv ist.

Welchen Handlungsspielraum gibt es in jedem Zustand?

Die Anzahl $DS(\sigma,s)$ der qualitativ unterscheidbaren Handlungssequenzen der Länge s aus denen in einem Zustand $\sigma\in\Sigma_S$ gewählt werden kann, lässt sich durch folgende Vorschrift einschränken:

$$DS(\sigma,s)=\Sigma_{\{(\sigma,m_i^h,\sigma')\in\Delta_S|h\in\mathcal{H}\wedge phase(\sigma,h)=cf\}}DS(\sigma',s-1)$$

wobei $DS(\sigma,0)=1$, wenn für jeden aktiven Kausalfaktor h beliebig viele Reduktionsaktionen m_i^h zur Verfügung stehen.

Wann und wie oft wird geplant?

Die Frequenz der Planaktualisierung richtet sich im Wesentlichen nach der Systemantwortzeit t_r, also der Zeit, die der AMR verstreichen lassen muss, um ausreichende Wirkungen seiner Handlungen messen, bewerten und die Informationen in R aktualisieren zu können. Es ist zu prüfen, ob noch ein Zeitlimit unabhängig von t_r zur Anwendung kommen kann, um eventuell zusätzliche Handlungen vorzunehmen.

4 Beispiel: Risikoreduktion bei der Übernahme der Fahraufgabe

Motiviert durch einen Pressebeitrag[32] aus dem AF-Bereich soll hier der Prozess „AF mit Übernahme der Fahraufgabe durch den menschlichen Fahrer" (AFÜM) genauer behandelt werden: zuerst das Modell und danach mögliche Vereinfachungen als Vorbereitung für die Laufzeitplanung.

31 | Zur Vereinfachung kann hier angenommen werden, dass sowohl S als auch σ eindeutig bestimmbar sind.
32 | Vgl. http://www.autoservicepraxis.de/continental-entwickelt-cruising-chauffeur-1970091.html.

4.1 Risikoidentifikation und Modellbildung

Zur RA wird hier eine vereinfachte Kombination aus „Layer Of Protection"-Analyse (LoPA) und ETA durchgeführt.[33]

Zuerst wird angenommen, dass die Straßeninfrastruktur in disjunkte Bereiche aufgeteilt ist: solche, für die AF zugelassen ist, und solche, in denen AF nicht zugelassen ist. Nun wird der Fahrprozess als betrachteter Prozess in drei Fahrsituationen aufgeteilt (siehe Abbildung 2):

- **ADArea:** automatisiertes Fahren im AF-zugelassenen Straßenbereich,
- **soonLeavingADArea:** Phasen der Übernahme der Fahraufgabe bei Navigation in nicht AF-zugelassene Straßenbereiche und
- **nonADArea:** manuelles Fahren in nicht AF-zugelassenen Straßenbereichen.

Für diese Fahrsituationen werden wesentliche Schadensereignisse in Tabelle 1 identifiziert. Der Kasten takeOverGeneric verkörpert für alle drei Fahrsituationen geltende Charakteristiken. Man beachte, dass hier **kein** abstraktes geometrisches Kollisionsmodell entwickelt wird, welches gegebenenfalls per Parametrisierung und Einschränkung wieder auf die genannten qualitativen Fälle spezialisiert werden kann. Die noch hypothetische Bewertung ergibt, dass alle betrachteten Schadensereignisse für alle betrachteten Fahrsituationen gleichermaßen relevant sind, die *Verantwortung* für die Einhaltung von Eigenschaft 2 jedoch vom AMR auf den menschlichen Fahrer übertragen wird.

Der Regler mit dem Teilsystem AMR ist technisch durch die folgenden Einheiten (Struktur, Funktionen, Reduktionsaktionen) realisiert:

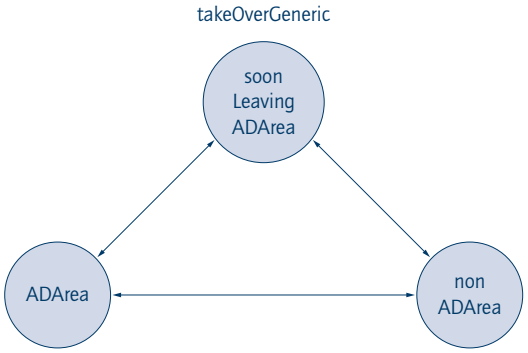


Abbildung 2: Drei Fahrsituationen (Quelle: eigene Darstellung)

- Struktur: Sensoren (zum Beispiel Kamera, Radar, LiDAR), Regelungsrecheneinheit, Aktuatoren (zum Beispiel Blinklichter, Innenraumlautsprecher, Anzeigenpanel, Sitzvibrationseinheit),
- Funktionen: Fahrerassistenzhauptfunktion, automatische Lenk- und Geschwindigkeitsregelung,
- Reduktionsaktionen: sicheres Ansteuern eines sicheren Standplatzes, sichere Abschaltung des Fahrzeugs, Steuerungsaufgabe übergeben, optische, akustische und vibrationsbasierte Fahrerinformation.

Für Tabelle 2 und Tabelle 3 werden nun folgende Kausalfaktoren hergeleitet, ausgehend von der Aufgabe AFÜM unter Anwendung von Schlüsselwörtern[34] und Expertenwissen aus der Straßenverkehrsdomäne (siehe Fußnote 69). Nun können diese Gefährdungen nach deren Relevanz für die Schadensereignisse aus Tabelle 1 bewertet werden. Genauere Bewertungen fordern weitere Parameter sowie statistische Schätzungen, auf die hier nicht zurückgegriffen wird – nicht zuletzt deshalb, weil Aussagen zu den selteneren Ereignissen in Σ inhärent schwierig sind.[35]

Schadensereignis	Fahrsituation		
	ADArea	soonLeavingADArea	nonADArea
Kollision mit vorderem Fahrzeug (Cf)	R/[4,5]	RF/[4,5]	F/[4,5]
Kollision mit hinterem Fahrzeug (Cr)	R/[3,5]	RF/[3,5]	F/[3,5]
Kollision mit Straßenrand (Cb)	R/[2,5]	RF/[2,5]	F/[2,5]
Kollision mit Nebenfahrzeug (Cs)	R/[2,4]	RF/[2,4]	F/[2,4]

Tabelle 1: Verantwortlichkeits- und Schweregradmatrix: Wer ist für die Vermeidung spezifischer Schadensereignisse in spezifischen Fahrsituationen (Abbildung 2) verantwortlich?/Wie schwer können Auswirkungen eines Schadensereignisses abhängig von der Fahrsituation sein? Legende: AM(R), (F)ahrer, sehr gering (1) ... sehr schwer (5), [min,max] ... Intervall (Quelle: eigene Darstellung)

33 | Die Fahrsituation *requestTakeOverByDr* verfeinert hier ein anderes Beispiel; vgl. Gleirscher 2017a.
34 | Vgl. Gleirscher 2014.
35 | Vgl. Rychlik/Rydén 2006, Kapitel 6.7.

4.2 Übertragung des Modells nach Yap

Die Ergebnisse aus dieser *qualitativen* Analyse werden nun in das Analysewerkzeug Yap übertragen, welches mittels der Konzepte der Abschnitte 2.2 und 3

- relevante Kombinationen aus Kausalfaktoren auflistet und
- miteinander über Transitionen verbindet.

Yap bietet so auch eine Basis für die automatische Analyse von Kausalstrukturen, zum Beispiel die in Abschnitt 3.2 beschriebenen Schritte, sowie deren Nutzung für die Wahl und Durchführung von Reduktionsaktionen laut Eigenschaft 2. Die qualitativen Informationen aus Abbildung 2, Tabelle 1, Tabelle 2 und Tabelle 3 sind in Form eines Yap-Modells in Abbildung 6 im Anhang abgebildet.

Planungsmodellkonstruktion mit Yap

Abbildung 3a zeigt $\Sigma/_{\{nAD,V1\}}$ für $soonLeavingADArea$. Auf eine Gesamtdarstellung von Σ wird verzichtet, nicht nur aus Platzgründen, sondern auch deshalb, weil eine grafische Darstellung ohnehin den Zweck verfehlen würde. Im nächsten Schritt wird Σ vereinfacht, weil in der Regel[36] davon ausgegangen wird, dass nur wenige Kausalfaktoren aus Tabelle 2 in beliebiger Kombination und Reihenfolge auftreten können.

Abbildung 3b zeigt die vereinfachte Kausalstruktur, welche Einschränkungen unterliegt, die nur mehr sinnvolle Kombinationen und Abfolgen der Kausalfaktoren zulassen. Eine ausführlichere Diskussion dieser Einschränkungen findet in Vorarbeiten[37] statt.

Für dieses Beispiel werden der übersichtlicheren Darstellung halber die Schadensereignisse Cr, Cb und Cs zum finalen Kausalfaktor C zusammengefasst. Basierend auf Tabelle 3 werden zuerst alle Risikozustände mit diesem Schadensereignis verknüpft. Abbildung 4 zeigt dann die Anwendung der Regel *mis*.

Kausalfaktor (Kürzel)	Fahrsituation		
	ADArea	Soon-Leaving-ADArea	nonAD-Area
Fahrtrajektorie führt demnächst nach nonADArea (nAD)	1	2	1
Lenkung noch nicht von Fahrer übernommen (V1)	1	2	5
Nach zweitem Versuch noch immer V1 (V2)	1	3	5
Nach drittem Versuch noch immer V1 (V3)	1	4	5
Keine Fahrerabsicht zur Übernahme erkannt (D)	1	4	5
Keine sichere Trajektorie zu sicherem Standplatz ermittelt (O)	2	5	5

Tabelle 2: Relevanzmatrix, Teil 1: Wie stark erhöht ein Kausalfaktor isoliert betrachtet im Mittel das Schadensrisiko in einer Fahrsituation? Legende: Erhöhung vernachlässigbar (1) ... stark (5) (Quelle: eigene Darstellung).

Kausalfaktor (Kürzel)	Schadensereignis: Kollision mit ...		
	Vorderem Fahrzeug	Hinterem Fahrzeug	Straßenrand
Fahrtrajektorie führt demnächst nach nonADArea (nAD)	1	1	1
Lenkung noch nicht von Fahrer übernommen (V1)	2	4	4
Nach zweitem Versuch noch immer V1 (V2)	2	4	4
Nach drittem Versuch noch immer V1 (V3)	3	5	5
Keine Fahrerabsicht zur Übernahme erkannt (D)	4	5	5
Keine sichere Trajektorie zu sicherem Standplatz ermittelt (O)	3	5	3

Tabelle 3: Relevanzmatrix, Teil 2: Wie stark trägt ein Kausalfaktor isoliert betrachtet im Mittel zum Eintritt eines Schadensereignisses bei? Legende: Beitrag vernachlässigbar (1) ... stark (5) (Quelle: eigene Darstellung).

36 | Vgl. die Modellierungsannahmen bei der dynamischen Fehlerbaumanalyse.
37 | Vgl. Gleirscher 2017a; Gleirscher 2017b.

Zum Abschluss des Beispiels werden die Kausalfaktoren V1 und V2 als *mit*-kompatibel bewertet. Man erhält damit eine Aktion m^{V1V2}, welche auf die Zustände V1, V2, V1V2 angewandt werden kann und stets Zustand $\overline{V1V2}$ garantiert. Für die bereits beschränkte Kausalstruktur in Abbildung 3b erhält man keine nennenswerte Vereinfachung durch die Anwendung der Regel *mit*. Zur Veranschaulichung zeigt Abbildung 5a die Struktur $R|_{\{V1,V2\}}$ welche durch einmalige Anwendung von $mit_{\{V1,V2\}}$ und weiteren Regeln zur Struktur in Abbildung 5d vereinfacht werden kann.

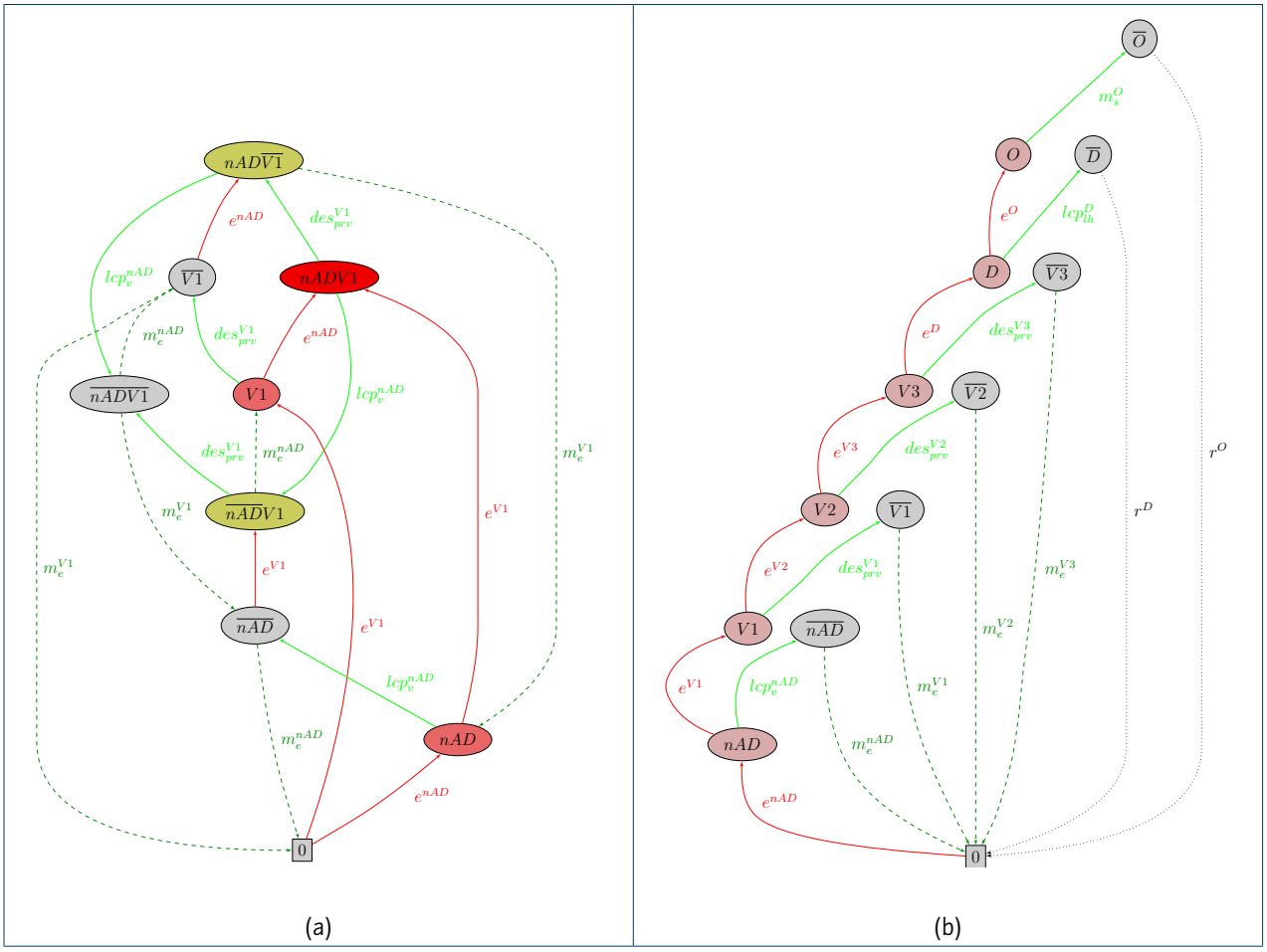


Abbildung 3: Konstruktion realistischer Kausalstrukturen als Vorhersagemodelle für Laufzeitrisikoreduktionsplanung (Quelle: eigene Darstellung)

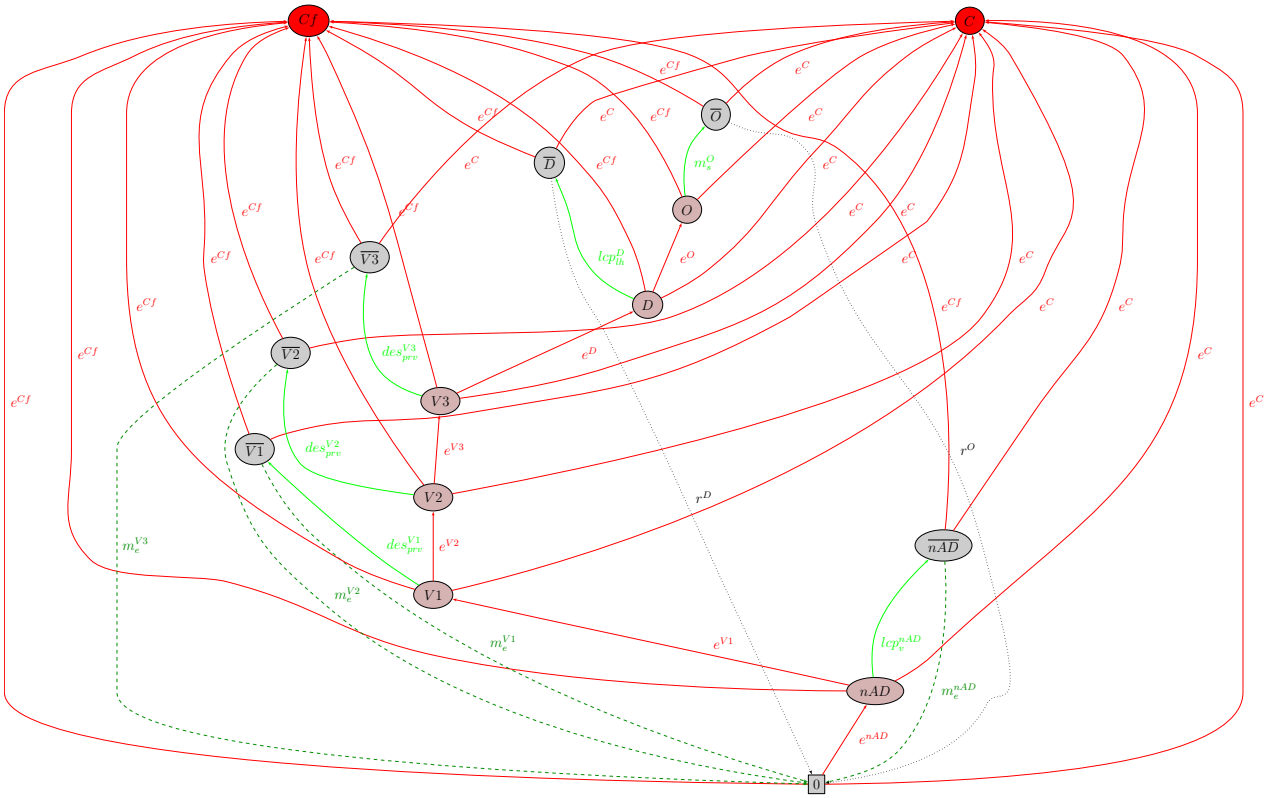


Abbildung 4: Kausalstruktur R für die beiden Schadensereignisse C und Cf nach Anwendung der Regel mis (Quelle: eigene Darstellung)

5 Diskussion, Zusammenfassung und Ausblick

Kausalstrukturen und entsprechende Yap-Modelle sind, wie für RA typisch, relativ vollständig in Bezug auf *bekannte* Unbekannte und messbare Parameter. Über unbekannte Unbekannte (im Englischen: black swans) kann zuerst nichts gesagt, also auch nicht gehandelt werden. Die in Abschnitt 8.4.2.2 erwähnten Schlüsselwörter zur Risikoidentifikation in Kombination mit Expertenwissen und der oft unvermeidbaren Unfallerfahrung sollen einen möglichst großen Anteil von unbekannten in bekannte Unbekannte und, idealerweise, messbare Parameter überführen. So kann die Nutzung von Schüsselwörtern[1] zur Verfeinerung des Schutzziels und somit zur Bewertung der Effektivität und Vollständigkeit automatisch konstruierter Kausalstrukturen als Planungsmodelle zur Laufzeitrisikoreduktion beitragen.

Zu den nächsten Herausforderungen gehören die

i. Anreicherung der Phasenmodelle und somit der Kausalstruktur mit probabilistischen Informationen für eine Markov-Analyse – wie zum Beispiel in Kapitel 3/Schnieder und Schnieder (Unterabschnitte 4 bis 6) vorgeschlagen, in Kapitel 5/Beyerer und Geisler für einen Schritt spieltheoretisch formalisiert oder im Abschnitt 8.1/Wolf und Lichte angewandt –,

ii. die Übertragung der Kausalstruktur in eine Kripke-Struktur zur Durchführung qualitativer temporaler Eigenschaftsprüfungen sowie

iii. die Realisierung stärkerer Vereinfachungsregeln im Analysewerkzeug Yap.

1 | Vgl. Gleirscher 2014, Dobi, et al. 2013.

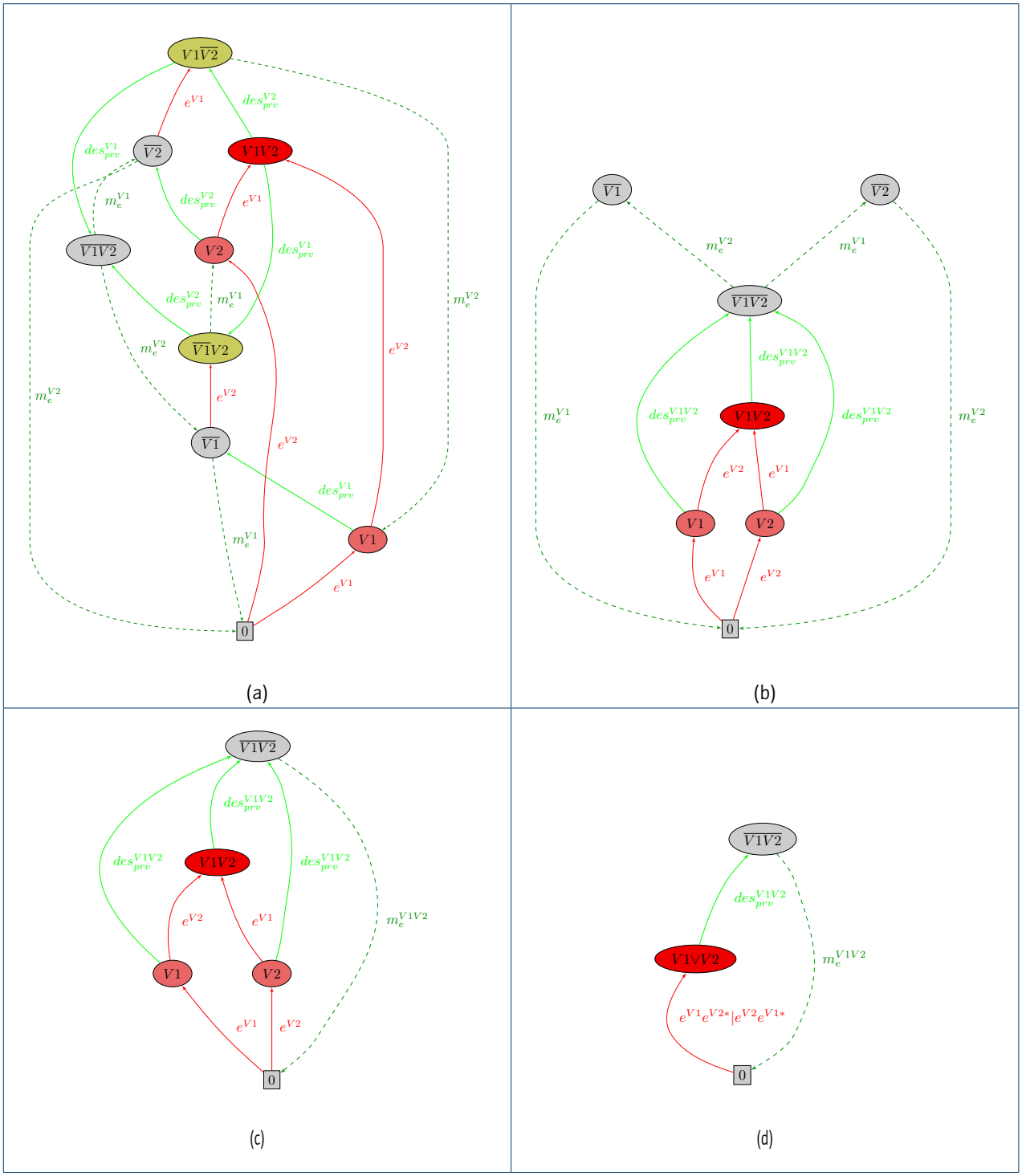


Abbildung 5: Kausalstruktur $R|_{\{V1,V2\}}$ vor (a) und nach (b) Anwendung der Regel mit$_{\{V1,V2\}}$ sowie nach Vereinfachung der Rückkehr zum sicheren Zustand 0 (c) und nach der Zusammenlegung von Risikozuständen (d) (Quelle: eigene Darstellung)

```
Settings { suppressMishaps = true; }

OperationalSituation "soonLeavingADArea" {
        include "takeOverGeneric";
        successor "nonADArea";
}

ControlLoop "L4Car" for "soonLeavingADArea" {
        optNotif partOf Actuators;
        accusNotif partOf Actuators;
        seatVibr partOf Actuators;
        finalizeHO partOf ADCU;
}

HazardModel for "soonLeavingADArea" {
        nAD alias "trajectory approaching non-AD area"
          mitigatedBy (CHECK_VIGILANCE)
          endMitigatedBy (H2M_HANDOVER.finalizeHO);
        V1 alias "steering wheel not yet manually operated by driver"
          requires (nAD)
          excludes (nAD)
          deniesMit (nAD)
          mitigatedBy (NOTIFY.optNotif,H2M_HANDOVER.initializeHO)
          endMitigatedBy (H2M_HANDOVER.finalizeHO);
        V2 alias "see V1: 2nd trial"
          requires (V1)
          excludes (nAD,V1)
          deniesMit (nAD,V1)
          mitigatedBy (NOTIFY.accusNotif,H2M_HANDOVER.initializeHO)
          endMitigatedBy (H2M_HANDOVER.finalizeHO);
        V3 alias "see V1: 3rd trial"
          requires (V2)
          excludes (nAD,V2)
          deniesMit (nAD,V1,V2)
          mitigatedBy (NOTIFY.seatVibr,H2M_HANDOVER.initializeHO)
          endMitigatedBy (H2M_HANDOVER.finalizeHO);
        D alias "driver suppresses intent of immediate take over"
          # on activation of D:
          requires (V3)
          excludes (nAD,V3) # = resets
          deniesMit (nAD,V1,V2,V3)
          # on mitigation of D:
          mitigatedBy (LIMP_HOME.initiateLH)
          endMitigatedBy (SHUTDOWN)
          offRepair (_);
        O requires (D)
          excludes (nAD,D)
          deniesMit (V1,V2,V3,D)
          offRepair (_);
        Cf alias "collision with front vehicle"
          mishap;
}
```

Abbildung 6: Yap Skript für die Situation „*soonLeavingADArea*" (Quelle: eigene Darstellung)

Danksagung

Dieser Beitrag wird von der DFG gefördert (Nr. GL 915/1-1). Zunächst richte ich meinen herzlichen Dank an Prof. Beyerer für die Möglichkeit der Teilnahme am acatech Themennetzwerk Sicherheit sowie an alle Mitglieder für den sehr hilfreichen interdisziplinären Austausch. Ferner danke ich meinen Projektpartnern aus der deutschen Automobilindustrie, insbesondere den Praktikern der funktionalen Sicherheit, für dort gewonnene Einblicke sowie hilfreiche Diskussionen.

Literatur

Alexander et al. 2009
Alexander, R. D./Kelly, T. P./Herbert, N. J.: *A Critique of the „Unmanned Systems Safety Guide for DoD Acquisition"*, 27th Int. System Safety Conference (ISSC), 2009.

Baier/Katoen 2008
Baier, Ch./Katoen, J.-P.: *Principles of Model Checking*, Cambridge (Massachusetts): MIT Press 2008.

Dobi et al. 2013
Dobi, S./Gleirscher, M./Spichkova, M./Struss, P.: *Model-based Hazard Analysis and Risk Assessment*, Tech. rep., Technische Universität München 2013.

Dugan et al. 2007
Dugan, J. B./Pai, G. J./Xu, H.: „Combining Software Quality Analysis with Dynamic Event/Fault Trees for High Assurance Systems Engineering." In: *High Assurance Systems Engineering Symposium*, 2007. HASE ,07. 10th IEEE, 2007, S. 245–255.

Freiling et al. 2013
Freiling, F./Grimm, R./Großpietsch, K.-E./Keller, B. H./Mottok, J./Münch, I./Rannenberg, K./Saglietti, F.: „Technische Sicherheit und Informationssicherheit." In: *Informatik-Spektrum* 37 (2013), S. 14–24.

Gleirscher 2014
Gleirscher, M.: *Behavioral Safety of Technical Systems*, Dissertation, Technische Universität München 2014.

Gleirscher 2017a
Gleirscher, M.: „Run-Time Risk Mitigation in Automated Vehicles: A Model for Studying Preparatory Steps." In: Bulwahn, L./Kamali, M./Linker, S. (Hrsg.): *First iFM Workshop on Formal Verification of Autonomous Vehicles 2017 (FVAV 2017)* 2017.

Gleirscher 2017b
Gleirscher, M.: *Yap – Yet Another Planner: User's Manual*, Technical University of Munich 2017.

Gleirscher/Kugele 2017
Gleirscher, M./Kugele, S.: „From Hazard Analysis to Hazard Mitigation Planning: The Automated Driving Case." In: Barrett, C. et al. (Hrsg.): *{NASA} Formal Methods ({NFM}) – 9th Int. Symp., Proceedings*. Springer, Berlin/New York 2017.

Kugele et al. 2017
Kugele, S./Cebotari, V./Gleirscher, M./Farzaneh, M. H./Segler, C./Shafaei, S./Vögel, H.-J./Bauer, F./Knoll, A./Marmsoler, D./Michel, H.-U.: „Research Challenges for a Future E/E Architecture – A Project Statement." In: *15th GI Workshop on Automotive Software Engineering (ASE)* 2017.

Kumamoto 2007
Kumamoto, H.: *Satisfying safety goals by probabilistic risk assessment*, London: Springer 2007.

Leveson 2012
Leveson, N. G.: *Engineering a Safer World: Systems Thinking Applied to Safety*, Cambridge (Massachusetts): MIT Press 2012.

Lund et al. 2011
Lund, M. S./Solhaug, B./Stølen, K.: *Model-Driven Risk Analysis: The CORAS Approach*, 1st, Berlin, Heidelberg: Springer 2011.

McDermid 2001
McDermid, J. A.: „Software Safety: Where's the Evidence?" In: *6th Australian Workshop of Industrial Experience with Safety Critical Systems and Software*, Brisbane, Australia 2001, S. 1–6.

Rychlik/Rydén 2006
Rychlik, I./Rydén, J.: *Probability and Risk Analysis*, Berlin: Springer 2006.

Schneider et al. 2017
Schneider, D./Trapp, M./Dörr, J./Dukanovic, S./Henkel, Th./Khondoker, R./Krauß, Ch./Mauthofer, S./Scheuermann, D./Zelle, D.: *Informatik-Spektrum*, 2017, 40, S. 419–429.

Schnieder et al 2005
Schnieder, E. et al. *Integrierte Modellierung der Funktion und Zuverlässigkeit komplexer Mensch-Maschine-Systeme zur Bestimmung der Verfügbarkeit und Sicherheit. Tagungsband 22. Tagung Technische Zuverlässigkeit*, S. 67–85, Düsseldorf, Stuttgart: VDI Verlag 2005.

Schnieder/Drewes 2008
Schnieder, E./Drewes. J.: „Bemessung und Kenngrößen der Verkehrssicherheit." In: *Zeitschrift für Verkehrssicherheit* 54 (2008), S. 117–123.

Schnieder/Schnieder 2008
Schnieder, E./Schnieder, L.: „Axiomatik der Begriffe für die Automatisierungstechnik." In: *atp – Automatisierungstechnische Praxis*, 10 2008.

Schnieder/Schnieder 2009
Schnieder, L./Schnieder. E.: „Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung." In: acatech (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven*, Berlin, Heidelberg: Springer 2009.

8.5 Agentenbasierte Simulation des Risikomanagements soziotechnischer Systeme mit dem Simulator SimCo

Prof. Dr. Johannes Weyer, Fabian Adelt,
Julius Konrad, Sebastian Hoffmann
Fachgebiet Techniksoziologie
Technische Universität Dortmund

1 Einleitung

Sicherheit und Verlässlichkeit komplexer soziotechnischer Systeme sind insofern von hoher gesellschaftlicher Relevanz, als Ausfälle kritischer Infrastruktursysteme oder Katastrophen in Chemieanlagen, Atomkraftwerken und ähnlichen sicherheitskritischen Bereichen erhebliche Auswirkungen auf die Umwelt oder die Gesundheit der Betroffenen haben (vgl. auch den Beitrag von Bertsche et al. in diesem Band). Nicht erst seit Charles Perrows provozierendem Buch „Normale Katastrophen"[1] diskutieren auch Soziologinnen und Soziologen über die Risiken komplexer Systeme sowie über Konzepte zur Verbesserung von deren Sicherheit. Perrow hatte die aus seiner Sicht zu enge These des menschlichen oder technischen Versagens abgelehnt und stattdessen postuliert, dass man das Design des Gesamtsystems, also das Zusammenspiel sämtlicher – technischer wie sozialer – Komponenten in den Fokus der Aufmerksamkeit rücken müsse.

Zudem hatte er die These aufgestellt, dass bestimmte Typen von Hochrisikosystemen, deren Prozesse eng gekoppelt und durch komplexe Interaktionen gekennzeichnet sind, nahezu zwangsläufig scheitern müssen. Auf derartige Systeme müsse man daher verzichten, weil sie nicht beherrschbar seien. Kritische Stimmen haben immer wieder darauf verwiesen, dass vor allem die pauschale Zuordnung ganzer Branchen zu einem bestimmten Risiko-Typus auf methodisch fragwürdigen Annahmen basiere.[2]

Zudem trat eine andere Gruppe von Organisationssoziologinnen und -soziologen mit der Behauptung auf, dass es einen Typus von High-Reliability-Organizations (HRO) gebe, die komplexe, eng gekoppelte Systeme managen und – selbst in hochdynamischen und komplexen Umwelten – Spitzenlasten unter Zeitdruck bewältigen könnten, ohne dass es zu Katastrophen käme.[3] Derartige „perfekte" Organisationen seien zwar theoretisch unmöglich, funktionierten aber in der Praxis recht gut.

Nach gut zwanzig Jahren Kontroverse zwischen diesen beiden „Schulen" der organisationssoziologischen Risikoforschung schien die Debatte in einer Sackgasse angelangt zu sein. Beide Konzepte hatten offenkundige Schwächen und Mängel, die sich nicht beheben ließen; zudem waren beide nicht im strengen Sinne falsifizierbar, sodass man gegenteilige Evidenzen immer leicht „wegargumentieren" konnte.

Frischen Schwung in die Debatte hat in jüngster Zeit ein Ansatz gebracht, der unter dem Label „Systems-Theoretic Accident Modelling and Processes" (STAMP) bekannt geworden ist und der sowohl die Normal-Accidents-Theory wie auch das Konzept der High-Reliability-Organizations scharf kritisiert.[4] Er fokussiert – zunächst ähnlich wie Perrow – „auf das integrierte sozio-technische System als Ganzes und die Beziehungen zwischen den technischen, organisationalen und sozialen Aspekten", begreift aber „Sicherheit als eine emergente Systemeigenschaft", die man nur verstehe, wenn es gelinge, „spezifische organisationale Sicherheitsstrukturen zu modellieren, zu analysieren und zu designen"[5]. Statt „allgemeine Prinzipien zu spezifizieren, die für alle Organisationen Gültigkeit"[6] beanspruchten, gehe es darum, das konkrete Sicherheits- und Risikomanagement zu erfassen und die Strukturen und Prozesse – unter anderem mithilfe der Methode der Computersimulation – abzubilden. Damit ließen sich Schwachstellen identifizieren, aber auch die langfristigen Wirkungen kleiner Veränderungen sowie der mit diesen einhergehenden Risiken aufdecken.

Sicherheit wird zudem als ein „Kontrollproblem" und nicht als ein „Problem des Komponentenversagens" aufgefasst. Fehlerhafte Komponenten (technische wie soziale) gebe es immer, aber Unfälle geschähen erst, „wenn Ausfälle von Komponenten, externe Störungen und/oder dysfunktionale Interaktionen zwischen Systemkomponenten nicht angemessen verarbeitet (handled) bzw. beherrscht (controlled) werden."[7]

1 | Vgl. Perrow 1987.
2 | Vgl. Shrivastava et al. 2009.
3 | Vgl. LaPorte/Consolini 1991, Roberts 1993, Weick/Sutcliffe 2007.
4 | Vgl. Leveson et al. 2009.
5 | Leveson et al. 2009, S. 241.
6 | Ebd.
7 | Leveson et al. 2009, S. 242.

Mit dem Simulator SimCo (Simulation of the Governance of Complex Systems) greifen wir die Idee des STAMP-Ansatzes auf, dem zufolge die Risiken komplexer soziotechnischer Systeme sowie das Risikomanagement nur dann sinnvoll erfasst werden können, wenn man ein Modell des betreffenden Systems entwickelt, das dessen Strukturen abbildet und zudem dessen Dynamiken analysierbar macht.[8]

2 ABMS

Dabei verwenden wir die Methode der agentenbasierten Modellierung und Simulation (ABMS), die es erlaubt, soziotechnische Systeme wie etwa das Verkehrs- oder das Energiesystem im Computer nachzubauen, deren Dynamik sich auf der Systemebene (Makro) durch die Aktionen und Interaktionen einer Vielzahl autonomer Agenten auf der Mikroebene ergibt.[9] Da die Agenten zudem mit individuellen Eigenschaften ausgestattet werden können, ergibt sich ein realistisches Bild, das die soziale Wirklichkeit in ihrer gesamten Vielfalt widerspiegelt. Vor allem bekommt man so die Tatsache in den Griff, dass Menschen nicht perfekt rational handeln, sondern subjektiv rational, das heißt entsprechend ihren spezifischen Interessen und Präferenzen:[10] Der eine entscheidet sich in einer bestimmten Situation für das Fahrrad, während sich der andere in dieser Situation für das Auto entschieden hätte. Diese Heterogenität des Sozialen lässt sich mit soziologisch fundierten ABMS-Modellen gut abbilden. Die Handlungslogik der Agenten auf der Mikroebene basiert dabei im Kern darauf, dass bei der Entscheidung zwischen unterschiedlichen Alternativen die subjektiv am höchsten bewertete Option gewählt wird.[11]

ABMS-Modelle erlauben es, Experimente mit unterschiedlichen „What if"-Szenarien durchzuführen, also beispielsweise zu untersuchen, wie sich ein Verkehrssystem mit beziehungsweise ohne Förderung der Elektromobilität entwickelt.[12] AMBS ist damit wie kaum eine andere sozialwissenschaftliche Methode in der Lage, zukünftige Entwicklungen zu antizipieren und zu bewerten. Zudem lässt sich beurteilen, welche Auswirkungen steuernde Interventionen haben. Dazu zählen zum einen staatliche Eingriffe, etwa in Form des Setzens von Emissionsgrenzwerten, zum anderen aber auch das Risikomanagement von Organisationen, etwa in Form einer verbesserten Sicherheitskultur. ABMS ermöglicht es also, Zukunftsszenarien experimentell zu erproben und am Computer durchzuspielen.

3 Konzeption von SimCo

Der Simulator SimCo wurde an der Technischen Universität Dortmund entwickelt, um die Steuerung komplexer soziotechnischer Systeme zu untersuchen, beispielsweise des Verkehrssystems oder des Energiesystems. Es wurde aber bewusst darauf verzichtet, ein konkretes System abzubilden. Stattdessen besteht das Simulationsframework aus abstrakten Knoten und Kanten, die Szenario-spezifisch ausgestaltet werden können. Dafür verfügen sie über frei parametrisierbare Dimensionen.[13]

Ein Knoten kann beispielsweise eine Kreuzung, ein Parkhaus, ein Bahnhof oder eine Ladestation, aber auch ein Supermarkt, ein Kino oder ein Kindergarten sein. Eine Kante ist eine gerichtete Verbindung zwischen zwei Knoten, beispielsweise in Form einer Straße, die von unterschiedlichen Verkehrsmitteln genutzt werden kann, aber auch in Form einer Busspur, eines Fahrradwegs oder einer Autobahn, die nur einem spezifischen Verkehrsmittel zur Verfügung steht.

SimCo ist eine agentenbasierte Modellierung und Simulation, was bedeutet, dass die Dynamik und die Komplexität auf Systemebene durch die Interaktion einer Vielzahl heterogener Agenten erzeugt werden, die individuelle und durchaus sehr unterschiedliche Entscheidungen treffen. Die Logik dieser Entscheidungen lässt sich mithilfe soziologischer Handlungstheorien abbilden, die besagen, dass jeder Agent auf Basis seiner individuellen Präferenzen und Zielvorstellungen und unter Berücksichtigung der Situation, in der er sich befindet, die Handlungsalternativen wählt, mit denen er sich subjektiv am besten stellt.

Eine Besonderheit von SimCo besteht darin, dass die Agenten in ihren Entscheidungen von den infrastrukturellen Rahmenbedingungen beeinflusst werden, also zum Beispiel von der Verfügbarkeit von Radwegen (Kanten) beziehungsweise Ladestationen für Elektroautos (Knoten).[14] Die Komponenten der Infrastruktur bilden zugleich die Ansatzpunkte für steuernde Eingriffe, wenn bei-

8 | Vgl. Beyerer/Geisler 2018.
9 | Vgl. Esser 1993.
10 | Vgl. Kroneberg 2014.
11 | Vgl. Velasquez/Hester 2013.
12 | Vgl. Gilbert et al. 2010, van Dam et al. 2013.
13 | Eine ausführliche Beschreibung der Modellkomponenten findet sich in (Adelt et al. 2018) sowie auf www.simco.wiwi.tu-dortmund.de.
14 | Vgl. Beyerer/Geisler 2018.

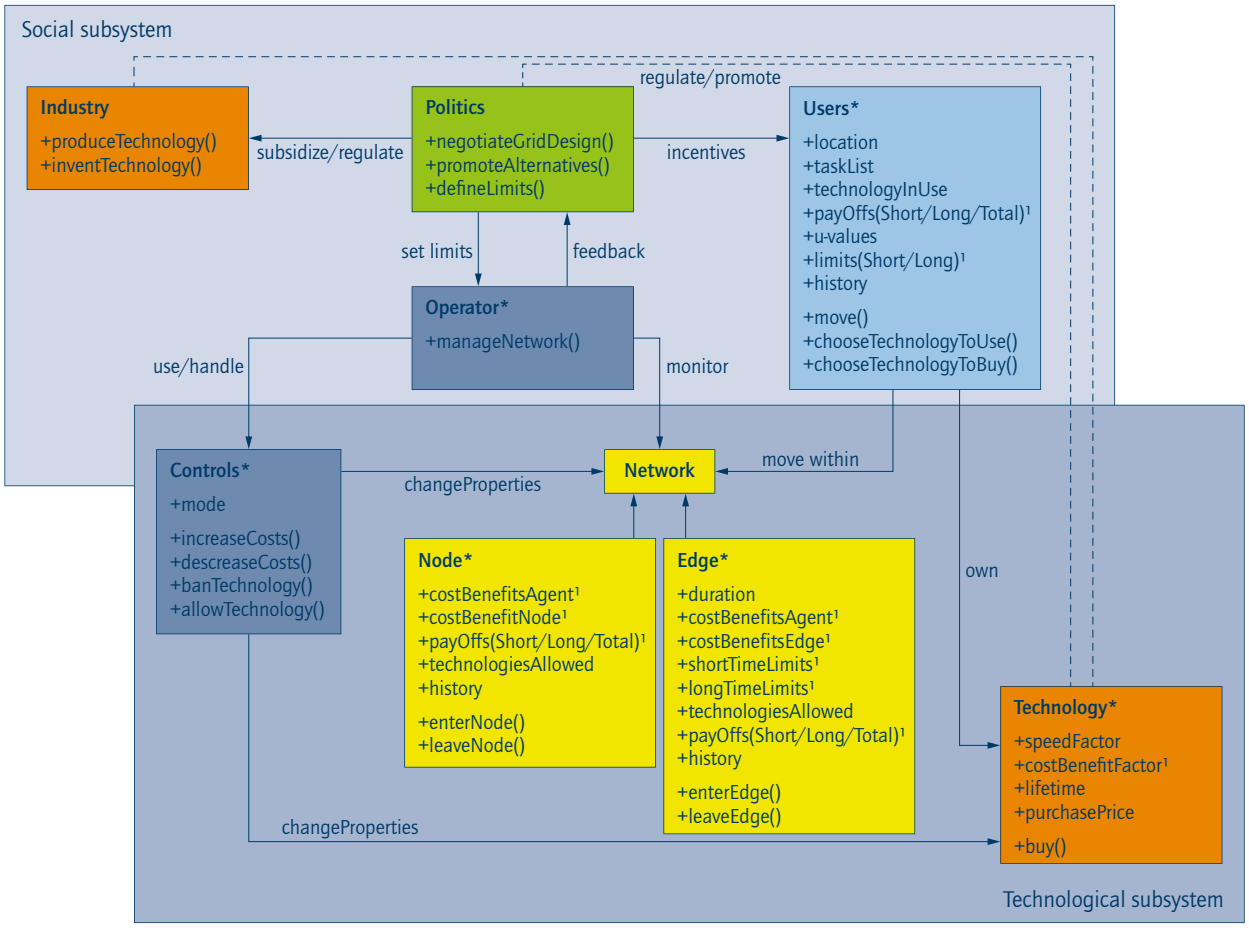


Abbildung 1: Subsysteme von SimCo und ihre Verknüpfungen (Quelle: Adelt et al. 2018)

spielsweise das Fahren mit dem Auto verteuert und die Benutzung öffentlicher Verkehrsmittel verbilligt wird oder neue Ladestationen errichtet werden.

4 Das Inventar

In der Endausbaustufe wird der Simulator SimCo aus einer Vielzahl von Modulen bestehen, die soziale Akteure abbilden. Bislang haben wir bereits die mit einem Stern (*) markierten Module technisch implementiert (vgl. Abbildung 1):

- Die Nutzer und Nutzerinnen, die sich durch das Netzwerk bewegen, um ihre Aufgaben zu erledigen, die wir mit einer einfachen Task-Liste, bestehend aus drei Aufgaben (zum Beispiel Kinder zum Kindergarten bringen, zur Arbeit fahren, im Supermarkt einkaufen), abgebildet haben;
- das Netzwerkmanagement, das für einen reibungslosen Betrieb sorgen soll und im Zweifelsfall mit einem Repertoire abgestufter Maßnahmen eingreift;
- Unternehmen, die bestimmte Dienstleistungen anbieten (zum Beispiel Transport mit Bus und Bahn);
- Unternehmen, die die benötigten Technologien herstellen und vertreiben, darunter etablierte Technologien, aber auch innovative Alternativen (zum Beispiel Elektroautos);
- die Politik, die Entscheidungen über die Struktur des Netzwerks trifft (zum Beispiel Ausbau der Radwege), Grenzwerte setzt (zum Beispiel in Bezug auf Emissionen) und schließlich auch Alternativen fördert (zum Beispiel Elektro-Ladestationen).[15]

Hinzu kommen noch die bereits erwähnten technischen Module, Knoten, Kanten und Technologien sowie schließlich die Steuerungsinstrumente.

15 | Diese Entscheidungen werden zurzeit über Szenarien eingespielt, aber nicht agentenbasiert modelliert.

5 Interaktionen

Mit jeder Aktion verändern die Agenten den Zustand der Knoten und Kanten des Netzwerks, und zwar in unterschiedlichen Dimensionen. Bei der Fahrt mit dem Auto zur Arbeit belegt ein Agent beispielsweise ein Stück Straße und stößt zudem Emissionen aus – beides größer als im Fall der Nutzung eines Fahrrads. In beiden Fällen können Grenzen erreicht werden, beispielsweise die maximale Kapazität einer Straße, nach deren Erreichen es einen Stau gibt, oder – politisch gesetzte – Grenzwerte für Emissionen, bei deren Erreichen Fahrverbote verhängt werden können.

Der Agent verändert zudem seinen eigenen Zustand, weil die Nutzung von Knoten und Kanten Kosten verursacht (Spritkosten, Parkgebühren etc., gegebenenfalls Maut), der Besuch von Knoten (Arbeitsstätte) hingegen Einkommen generiert. Und schließlich nutzt er die ihm zur Verfügung stehende Technologie ab – irgendwann muss das Fahrrad ersetzt beziehungsweise eine neue Monatskarte für den öffentlichen Nahverkehr gekauft werden.

Durch die Aktionen und Interaktionen einer Vielzahl von Agenten verändert sich der Zustand des Gesamtsystems permanent. Der nächste Agent, der die betreffende Straße nutzen will, trifft bereits auf eine andere Situation als sein Vorgänger und entscheidet sich möglicherweise anders, nämlich für die Nutzung des Fahrrads, was wiederum Auswirkungen auf die folgenden Entscheidungen anderer Agenten hat.

Agentenbasierte Modelle sind also in der Lage, die Entscheidungen einer Vielzahl von Agenten abzubilden und die aus ihnen resultierenden komplexen Systemdynamiken zu beschreiben sowie zu analysieren.

6 Interventionen/Steuerung

SimCo enthält eine Vielzahl von „Hebeln" und „Stellschrauben", über die in das Geschehen eingegriffen werden kann; dies kann aus unterschiedlichen Gründen geschehen.

6.1 Risikomanagement

Wenn es das Ziel ist, Risiken zu bewältigen, die zu Fehlfunktionen, zum Stillstand oder gar zum Zusammenbruch des Systems führen können (Verkehrsstau, Blackout im Stromnetz etc.), wird das Netzmanagement versuchen, Abweichungen vom Sollzustand durch Gegensteuern (negatives Feedback) zu verhindern, um so die Stabilität des Systems zu gewährleisten (beziehungsweise wiederherzustellen).

6.2 Systemtransformation

Wenn aber das Ziel darin besteht, das System zu verändern, zum Beispiel in Richtung Nachhaltigkeit, werden steuernde Eingriffe darauf abzielen, Abweichungen zu verstärken (zum Beispiel durch Subventionen für Photovoltaikanlagen), um auf diese Weise einen Trend in Gang zu setzen, der letztendlich zum Regimewechsel führen soll (positives Feedback).

Rein instrumentell unterscheiden sich beide Konzepte überraschenderweise wenig voneinander, geht es doch im Wesentlichen darum, durch entsprechende Anreize und Eingriffe ein erwünschtes Verhalten auf Agentenebene wahrscheinlicher zu machen und ein unerwünschtes zu verhindern.

6.3 Governance-Modi

Steuernde Eingriffe setzen an den Dimensionen von Knoten, Kanten, Technologien oder Agenten an, indem sie beispielsweise die Nutzung einer Technologie auf einer Kante verteuern (Pkw-Maut) oder einen Knoten für eine bestimmte Technologie sperren (Fußgängerzone). Dabei kommen drei unterschiedliche Modi zum Einsatz:

- die Selbstkoordination, in der die Agenten sich untereinander koordinieren und das Netzwerkmanagement das Geschehen lediglich beobachtet (dies ist zugleich unser Basisszenario);
- die weiche Steuerung, die mit (negativen oder positiven) Anreizen operiert, die ein bestimmtes Verhalten attraktiv beziehungsweise unattraktiv machen sollen;
- und schließlich die harte Steuerung, die Verbote beinhaltet, beispielsweise ein Verbot der Nutzung bestimmter Technologien auf bestimmten Kanten.

7 Software-Implementation

SimCo ist in NetLogo programmiert, einer Programmiersprache, die häufig für sozialwissenschaftliche Experimente genutzt wird. Es hat ein grafisches Nutzer-Interface (vergleiche Abbildung 2), in dem die Struktur des Netzwerks angezeigt und verschiedene Messwerte ausgegeben werden.

Das abstrakte Simulationsmodell erlaubt es, unterschiedliche Szenarien zu konfigurieren und zu laden. Wir haben uns für das Szenario eines Verkehrssystems in einer mittleren deutschen Großstadt entschieden, das wir mit Daten der Stadt Dortmund kalibriert haben. Zudem haben wir auf Basis einer Befragung von 506 Personen und deren Präferenzen unterschiedliche Agententypen identifiziert (vgl. Tabelle 1), und zwar:

- Pragmatikerinnen und Pragmatiker, die in erster Linie schnell ans Ziel kommen wollen,
- Umweltbewusste, denen die Umweltauswirkungen des Transports am wichtigsten sind,
- Indifferente, die keine klaren Präferenzen haben,
- „Sparfüchse", die fast ausschließlich auf den Preis schauen,
- und schließlich den Komfortorientierte, denen neben der Geschwindigkeit vor allem der Komfort wichtig ist.

	Präferenzen			
Akteurtypen	Preiswert	Schnell	Umwelt-freundlich	Komfor-tabel
Pragmatiker/innen	3.7	6.8	2.4	1.2
Umweltbewusste	4.4	2.0	7.6	1.9
Indifferente	4.0	4.6	2.8	4.2
Sparfüchse	9.0	4.7	3.7	0.7
Komfortorientierte	0.6	6.4	0.2	6.8

Tabelle 1: Akteurtypen (N = 506, Quelle: Teigelkamp 2015)

Bei der Befragung wurde auch erhoben, wie die Befragten die Wahrscheinlichkeit einschätzen, mit bestimmten Technologien die angestrebten Ziele zu erreichen, also zum Beispiel mithilfe des Fahrrads schnell oder günstig ans Ziel zu kommen. Diese Daten sind allesamt in ein Szenario eingeflossen, mit dem wir unterschiedliche Experimente durchgeführt haben.

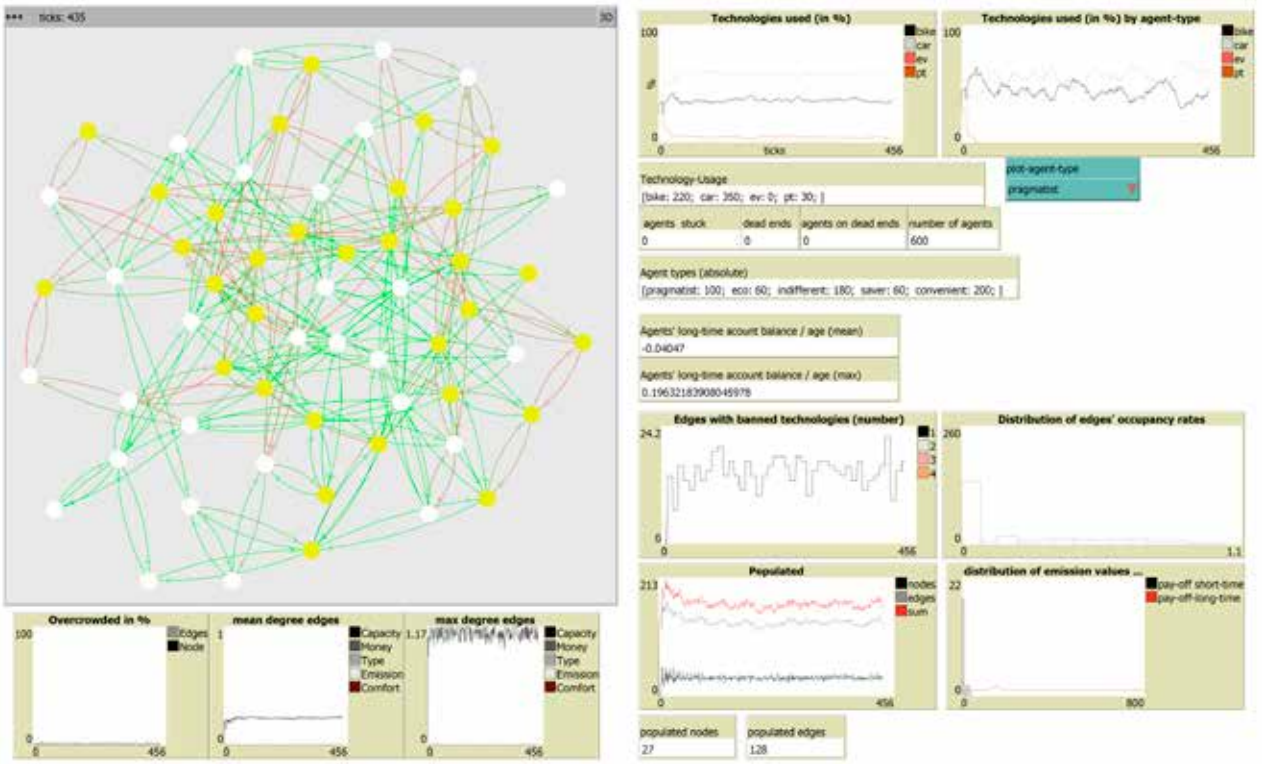


Abbildung 2: Grafische Benutzeroberfläche von SimCo (Quelle: Adelt et al. 2018)

8 Szenarien

Mit SimCo lassen sich Experimente zu Fragen der Systemtransformation (zum Beispiel Energiewende) wie auch zu Fragen des Risikomanagements durchführen. Im Folgenden konzentrieren wir uns auf Letzteres und nehmen als Basisszenario das oben beschriebene Verkehrssystem im Modus der Selbstkoordination, bei dem nicht von außen interveniert wird.

Die Implementation unterschiedlicher Szenarien des Risikomanagements orientiert sich an den beiden anderen Governance-Modi der weichen und der harten Steuerung, wobei die Interventionen auf zweierlei Weise implementiert werden:

- als einmalige, statische Interventionen zu Beginn eines Experiments, mit denen bestimmte Parameter dauerhaft festgelegt werden;
- als situativ wirkende Interventionen, die dynamisch-adaptiv und in Echtzeit auf Veränderungen bestimmter Systemparameter reagieren und bei unerwünschten Entwicklungen „gegensteuern", etwa wenn bestimmte Grenzwerte überschritten werden, und wieder zurückgenommen werden können, wenn die Grenzwerte unterschritten werden.[16]

Neben der weichen Steuerung, die mit Anreizen operiert (zum Beispiel Pkw-Maut), und der harten Steuerung, die über Verbote umgesetzt wird (zum Beispiel zeitlich und räumlich begrenzte Fahrverbote), untersuchen wir zudem ein Szenario, in dem beide Maßnahmen kombiniert werden.[17]

8.1 Risikoindikatoren

Das Risiko, das mit dem Betrieb eines komplexen soziotechnischen Systems einhergeht, lässt sich auf der Mikroebene der einzelnen Agenten wie auch auf der Systemebene (Makro) bemessen.[18] Ein Agent trägt beispielsweise ein Risiko, wenn er zu spät zu seinem Task-Knoten (Arbeitsplatz) gelangt, weil er das falsche Verkehrsmittel gewählt hat oder in einen Stau geraten ist.

Wir konzentrieren uns hier jedoch auf die Risiken auf der Makroebene des Systems, die wir mit drei ausgewählten Indikatoren vermessen, nämlich der Kapazitätsauslastung der Kanten sowie den Emissionen, welche die von den Agenten genutzten Technologien verursachen. Die damit einhergehenden Systemrisiken sind der Stillstand von Teilen des Netzwerks (Stau), was dessen Funktionsfähigkeit – bis zum lokalen Systemzusammenbruch – beeinträchtigen kann, sowie die Umweltverschmutzung (CO_2-Emissionen), welche die Legitimität des Handelns der Agenten infrage stellen kann. Bei den Emissionen unterscheiden wir zudem zwischen Kurzzeitlimits, die zeitlich befristete Überschreitungen von Grenzwerten signalisieren (zum Beispiel im Laufe eines Tages), und Langzeitlimits, die eine Aufsummierung aller Emissionen über einen Monat beziehungsweise ein Jahr enthalten und vor allem für statistische Zwecke (sowie darauf basierende politische Maßnahmen) relevant sind.

Die im Folgenden verwendeten Prozentangaben für die Kapazitätsauslastung sowie die Kurzzeit- und die Langzeitemissionen orientieren sich an den Limits dieser drei Indikatoren: Ab einem Wert von 100 Prozent ist das Limit überschritten und das System überlastet.[19] Dabei messen wir globale Durchschnitts- und Maximalwerte über den gesamten Simulationslauf, welche die Gesamteffizienz des Verkehrssystems anzeigen. Punktuelle lokale Überlastungen ermitteln wir hingegen über den Maximalwert der höchstbelasteten Kante, der Hinweise auf kritische Situationen gibt.

8.2 Ergebnisse der Experimente mit statischer Intervention

Im folgenden Experiment wurden zu Beginn jedes Versuchslaufs einzelne Parameter fixiert und über die gesamten Versuchsläufe unverändert belassen, die allesamt eine weiche Anreizsteuerung beinhalten, nämlich

- eine Erhöhung des Komforts des Radfahrens (zum Beispiel durch den Ausbau von Radwegen, die Optimierung von Ampelschaltungen, bewachte Fahrradparkhäuser etc.),
- eine Erhöhung des Komforts des ÖPNV (zum Beispiel durch bessere Taktzeiten und Anschlussverbindungen, komfortablere Züge, günstigere Preise etc.)
- sowie eine Erhöhung der Kosten des Autos (zum Beispiel durch Anhebung der Mineralölsteuer, Erhebung einer City-Maut etc.).

16 | Wir unterscheiden zudem in beiden Governance-Modi drei Level der Steuerung, beispielsweise eine geringe, eine mittlere und eine hohe Maut für den Pkw, verzichten hier aber aus Platzgründen auf diese Differenzierung.

17 | Die steuernden Interventionen greifen in unserem Modell bei 60 Prozent (hier setzt die weiche Steuerung ein) beziehungsweise 80 Prozent des Limits (ab hier wird hart gesteuert).

18 | Vgl. Adelt et al. 2014.

19 | Die Limits werden durch die Experimentatoren gesetzt und orientieren sich beispielsweise an technischen Werten (Kapazität eines Parkhauses) oder an normativen Vorgaben (Emissionsgrenzwerte).

Wie Tabelle 2 zeigt, führen alle drei Maßnahmen, deren Effekte wir separat (und nicht kombiniert) gemessen haben, im Vergleich zum Basisszenario zu einer Verbesserung der Werte der drei Indikatoren: Die Kapazitätsauslastung sinkt, während die Emissionen – sowohl die Kurzzeit- als auch die Langzeitemissionen – zurückgehen. Den deutlichsten Effekt hat dabei die Steigerung des Komforts des Radfahrens, dicht gefolgt von der Erhöhung der Kosten für das Autofahren. Beim ÖPNV sind die Wirkungen statischer Interventionen deutlich geringer.

Intervention	Kapazitäts-auslastung	Kurzzeit-emission	Langzeit-emission
Basisszenario	21,6 %	18,0 %	33,4 %
Komfort Fahrrad	17,3 %	**13,2 %**	**24,6 %**
Komfort ÖPNV	19,1 %	16,5 %	30,5 %
Kosten Auto	**16,7 %**	13,3 %	25,4 %

Tabelle 2: Durchschnittswerte für das gesamte Netzwerk bei statischer Intervention (in Prozent der Limits) (Quelle: eigene Darstellung)

8.3 Ergebnisse der Experimente mit situativer Intervention

Im nächsten Experiment werden die Parameter während des gesamten Simulationslaufs in Abhängigkeit von der aktuellen Situation dynamisch verändert, um beispielsweise punktuellen Überlastungen entgegenzuwirken. Anders als im vorigen Experiment steht hier einzig die Technologie „Auto" im Fokus, deren Kosten verändert werden (weiche Steuerung) beziehungsweise die mit Fahrverboten belegt wird, falls Probleme auf einer Kante auftreten (harte Steuerung). Der kombinierte Modus umfasst beide Instrumente.

Governance-Modus	Kapazitäts-auslastung	Kurzzeit-emission	Langzeit-emission
Selbst-koordination (Basisszenario)	21,6 %	18,0 %	33,4 %
weich	18,2 %	14,5 %	27,7 %
hart	19,5 %	15,7 %	29,2 %
kombiniert	**18,0 %**	**14,1 %**	**26,9 %**

Tabelle 3: Durchschnittswerte für das gesamte Netzwerk bei situativer Intervention (in Prozent der Limits) (Quelle: eigene Darstellung)

Tabelle 3 zeigt die globalen Durchschnittswerte für das gesamte Netzwerk, gemessen jeweils über den gesamten Simulationslauf. Alle Governance-Modi führen demzufolge zu einer Verbesserung der Werte im Vergleich zum Basisszenario der ungesteuerten Selbstkoordination. Am besten schneidet dabei die kombinierte Steuerung ab, dicht gefolgt von der weichen Steuerung, während die harte Steuerung etwas schlechtere Ergebnisse erzielt. Es spricht also viel für eine „intelligente" Steuerung, die unterschiedliche Governance-Modi – je nach situativem Anlass – miteinander kombiniert.

Governance-Modus	Kapazitäts-auslastung	Kurzzeit-emission	Langzeit-emission
Selbst-koordination (Basisszenario)	25,7 %	36,1 %	71,7 %
weich	25,7 %	34,8 %	60,4 %
hart	**22,0 %**	31,8 %	63,1 %
kombiniert	**22,0 %**	**31,5 %**	**58,6 %**

Tabelle 4: Maximalwerte für das gesamte Netzwerk bei situativer Intervention (in Prozent der Limits) (Quelle: eigene Darstellung)

Tabelle 4 zeigt hingegen die globalen Maximalwerte für das gesamte Netzwerk, also den jeweils schlechtesten Zustand im jeweiligen Experiment. Das Basisszenario weist kritische Werte vor allem bei den Emissionen auf, die – gemittelt über das gesamte Netzwerk – deutlich über den Durchschnittswerten liegen (vgl. Tabelle 3). Bei den Governance-Modi zeigt sich ein ähnliches Bild wie in Tabelle 3, dass nämlich alle drei Modi zu einer spürbaren Reduktion der Werte beitragen, wobei die kombinierte Steuerung wiederum die besten Resultate liefert.

Die globalen Maximalwerte sagen jedoch nichts über mögliche lokale Belastungen (zum Beispiel Staus oder Überschreiten der Emissionsgrenzwerte) auf einzelnen Kanten aus. Tabelle 5 zeigt daher die Maximalwerte, die bei der jeweils höchstbelasteten Kante beobachtet wurden. Gemessen an den relativ unspektakulären globalen Mittelwerten, die im Basisszenario lediglich bei 20 bis 30 Prozent lagen (vgl. Tabelle 3), zeigen sich hier deutliche, lokal begrenzte Überlastungen vom bis zu Fünffachen des jeweiligen Limits (471 Prozent), die steuernde Interventionen erforderlich machen.

Governance-Modus	Kapazitäts-auslastung	Kurzzeit-emission	Langzeit-emission
Selbst-koordination (Basisszenario)	120,5 %	251,8 %	471,9 %
weich	133,8 %	244,8 %	444,6 %
hart	**128,4 %**	**108,0 %**	**202,1 %**
kombiniert	132,6 %	111,5 %	204,9 %

Tabelle 5: Maximalwerte für einzelne Kanten bei situativer Intervention (in Prozent der Limits) (Quelle: eigene Darstellung)

Wie in Tabelle 5 zu sehen, zeigen alle drei Governance-Modi Wirkung, insbesondere bei der Senkung der Emissionen. Bei der Kapazitätsauslastung ergibt sich hingegen der kontraproduktive Effekt, dass Fahrverbote und damit einhergehende Verlagerungen des Pkw-Verkehrs die Kapazitätsauslastungen einzelner Kanten sogar leicht erhöhen.[20]

Erkennbar sind allerdings auch die deutlichen Unterschiede zwischen den Governance-Modi: Die weiche Anreizsteuerung zeigt kaum Effekte, sondern führt lediglich zu einer Verlagerung des Pkw-Verkehrs auf andere Routen, messbar an den kaum spürbaren Reduktionen der Emissionen. Die harte und die kombinierte Steuerung bewirken hingegen deutliche Reduktionen der Maximalwerte auf weniger als die Hälfte der Werte des Basisszenarios. Bei den Langzeitemissionen sinkt der Wert zum Beispiel von 471,9 auf 202,1 Prozent. Offenbar steigt in diesem Fall eine größere Zahl von Autofahrern auf umweltfreundliche Verkehrsmittel um.

9 Fazit

Mithilfe der Simulationsexperimente, die wir mit dem Simulator SimCo durchgeführt haben, kann man Ansatzpunkte für ein Risikomanagement in einem komplexen soziotechnischen System identifizieren, das mit dem Ziel betrieben wird, die Systemstabilität zu gewährleisten, lokal begrenzte Systemzusammenbrüche (Stau) zu vermeiden und zugleich deren Legitimität zu sichern (Einhaltung von Emissionsgrenzwerten). SimCo erlaubt es, unterschiedliche Szenarien (mit politisch definierten Zielvorstellungen) durchzuspielen und auf ihre Wirksamkeit sowie mögliche, nicht intendierte Nebenfolgen hin zu testen.

Mit SimCo wollen wir auch einen Beitrag zu organisationssoziologischen Risikodebatten leisten, indem wir zeigen, dass die Modellierung und Simulation soziotechnischer Systeme ein Verfahren ist, mit dem man insbesondere die Effekte nichtlinearer Interaktionen systematisch erforschen kann. Ob Nichtlinearität zwangsläufig in die Katastrophe führt (Perrow) oder ob derartige Systeme beherrschbar sind (Leveson), kann mithilfe von SimCo systematisch erforscht werden.

Zudem liefert SimCo einen Beitrag zum RAMSS-Modell,[21] indem es insbesondere die Aspekte „Safety" und „Availability", darüber hinaus jedoch auch „Legitimacy" und „Governability" komplexer soziotechnischer Systeme akzentuiert.

20 | Die Autofahrer haben die Wahl, wie sie auf steuernde Impulse reagieren: Sie können das Verkehrsmittel wechseln oder an ihrer Wahl des Pkws festhalten und lediglich die Route ändern.

21 | Vgl. Bertsche et al. 2018.

Literatur

Adelt et al. 2014
Adelt, F./Weyer, J./Fink, R. D.: „Governance of Complex Systems. Results of a Sociological Simulation Experiment". In: *Ergonomics* (Special Issue „Beyond human-centered automation"), 57, 2014, S. 434–448.

Adelt et al. 2018
Adelt, F./Weyer, J./Hoffmann, S./Ihrig, A.: „Simulation of the Governance of Complex Systems (SimCo). Basic Concepts and Initial Experiments". In: *Journal of Artificial Societies and Social Simulation,* 21: 2, URL: http://jasss.soc.surrey.ac.uk 21/2/2.html.

Bertsche et al. 2018
Bertsche, B./Beyerer, J./Goldschmidt, R./Jakobs, E. M./Renn, O./Schlüter, N./Winzer, P./Weyer, J.: „Integrative Theorie der Verlässlichkeit (iTV) für soziotechnische Systeme (STS)". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Beyerer/Geisler 2018
Geisler, J./Beyerer, J.: „Formaler Rahmen für eine einheitliche quantitative Beschreibung des Risikos bezüglich Safety und Security". In: Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

Esser 1993
Esser, H.: *Soziologie. Allgemeine Grundlagen*, Frankfurt/M.: Campus 1993.

Gilbert et al. 2010
Gilbert, N./Ahrweiler, P./Pyka, A.: „Learning in Innovation Networks. Some Simulation Experiments". In: Petra Ahrweiler (Hrsg.): *Innovation in Complex Social Systems*, London: Routledge 2010, S. 235–249.

Kroneberg 2014
Kroneberg, C.: „Frames, Scripts, and Variable Rationality: An Integrative Theory of Action". In: Gianluca Manzo (Hrsg.): *Analytical Sociology: Norms, Actions, and Networks*, Hoboken, NJ: Wiley 2014, S. 97–123.

LaPorte/Consolini 1991
LaPorte, T. R./Consolini, P. M.: „Working in Practice But Not in Theory: Theoretical Challenges of ‚High Reliability Organizations'". In: *Journal of Public Administration Research and Theory* 1: 1991, S. 19–47.

Leveson et al. 2009
Leveson, N./Dulac, N./Marais, K./Carroll, J.: „Moving Beyond Normal Accidents and High Reliability Organizations: a Systems Approach to Safety in Complex Systems". In: *Organization Studies*, 30: 2-3,2009, S. 227–249.

Perrow 1987
Perrow, Ch.: *Normale Katastrophen. Die unvermeidbaren Risiken der Großtechnik*, Frankfurt/M.: Campus 1987.

Roberts 1993
Roberts, K. A. (Hrsg.): *New Challenges to Understanding Organisations*, New York: Macmillan 1993.

Shrivastava et al. 2009
Shrivastava, S./Sonpar, K./Pazzaglia, F.: „Normal Accident Theory Versus High Reliability Theory: a Resolution and Call for an Open Systems View of Accidents". In: *Human Relations*, 62: 9, 2009, S. 1357–1390.

Van Dam et al. 2013
Van Dam, K. H./Nikolic, I./Lukszo, Z. (Hrsg.): *Agent-Based Modelling of Socio-technical Systems*, Dordrecht: Springer 2013.

Velasquez/Hester 2013
Velasquez, M./Hester, P. T.: „An Analysis of Multi-Criteria Decision Making Methods". In: *International Journal of Operations Research*, 10: 2, 2013, S. 56–66.

Weick/Sutcliffe 2007
Weick, K. E./Sutcliffe, K. M.: *Managing the Unexpected: Assuring High Performance in an Age of Complexity, 2. Auflage,* New York: John Wiley & Sons 2007.

8.6 Schutz und Sicherheit in Offshore-Windparks

Prof. Dr.-Ing. Uwe Arens
Institute for Safety and Security Studie (ISaSS)
Hochschule Bremerhaven

Uta Kühne
fk-wind: Institut für Windenergie, Hochschule Bremerhaven

1 Einleitung

Der Anteil der Windenergie an der bundesdeutschen Stromversorgung hat in den zurückliegenden Jahren stetig zugenommen.[1] Einen wesentlichen Beitrag leistet die Windenergie auf See („offshore"). Höhere Windgeschwindigkeiten als an Land sorgen für eine bessere Auslastung und tragen damit zur wirtschaftlichen Effizienz bei. Aus diesem Grund ist geplant, den Ausbau der Offshore-Windenergie weiter voranzutreiben. Erklärtes Ziel der Bundesregierung ist es, die Stromerzeugung auf See bis zum Jahr 2020 auf 6,5 Gigawatt zu erhöhen.[2] Um dieses Ziel realisieren zu können, ist die Nutzung der ausschließlichen Wirtschaftszone (AWZ) für die Errichtung weiterer Windenergieanlagen vorgesehen.[3]

Die Offshore-Windenergie ist als Teil der nationalen Energieversorgung den kritischen Infrastrukturen zuzurechnen. Die Erzeuger sind somit aufgefordert, besondere Anstrengungen zur Gewährleistung einer ausreichenden Versorgungssicherheit der Bevölkerung zu unternehmen.[4] Für die Offshore-Windenergie stellt diese Verpflichtung eine besondere Herausforderung dar. Schlechte Erreichbarkeit der technischen Anlagen, raue Umgebungsbedingungen auf See und die bislang unzureichenden praktischen Erfahrungen erfordern erhebliche Anstrengungen.

Zur Unterstützung der Offshore-Windenergie fördert das Bundesministerium für Bildung und Forschung im Rahmenprogramm „Forschung für die zivile Sicherheit II" in der Bekanntmachung „Maritime Sicherheit" unter anderem das Forschungsvorhaben „OWiSS – Offshore-Windenergie – Schutz und Sicherheit". Ziel dieses Verbundvorhabens ist es, einen Beitrag zur Versorgungssicherheit der Bevölkerung zu leisten, indem Ursachen möglicher Störungen und Unterbrechungen in Offshore-Windenergieparks und deren Subsystemen systematisch ermittelt und Vorschläge zur Verbesserung der Sicherheit erarbeitet werden.[5]

Dieser Artikel beschäftigt sich mit den theoretischen Ansätzen zur systematisierten Ermittlung und Bewertung der Sicherheit der Offshore-Windenergie und berichtet über die praktischen Erfahrungen bei der Umsetzung. Vorangestellt ist ein kurzer Überblick über Aufgaben und Ziele des Forschungsvorhabens.

2 Das Forschungsprojekt OWiSS

Bei dem Forschungsprojekt OWiSS handelt es sich um ein Verbundprojekt mit fünf Verbundpartnern. Das übergeordnete Ziel aller Beteiligten ist es, einen Beitrag zur Gewährleistung der Versorgungssicherheit der Bevölkerung zu leisten. Mögliche Beeinträchtigungen der Stromerzeugung aus Offshore-Windenergie sollen ausgeschlossen oder auf ein Minimum reduziert werden.[6]

Am Anfang der Untersuchungen steht eine proaktive Analyse aller Risiken, denen die Offshore-Windenergie ausgesetzt sein kann. Es schließt sich eine Bewertung an mit dem Ziel, diejenigen Risiken zu benennen, die für die Versorgungssicherheit von Bedeutung sind.[7]

Die proaktive Analyse wird durch eine retrospektive Analyse ergänzt. Vorfälle aus der Vergangenheit werden systematisch untersucht und ausgewertet. Zusammen mit den Ergebnissen aus der proaktiven Analyse werden anschließend in enger Abstimmung mit den Verbundpartnern und den betroffenen Unternehmen Maßnahmenkonzepte erarbeitet. Zur Validierung einzelner Maßnahmenvorschläge werden Fallstudien entworfen, in denen besondere Szenarien simuliert werden; diese werden gemeinsam mit betrieblichen Vertretern bearbeitet. Parallel zu den Untersuchungen werden rechtliche und gesellschaftliche Fragestellungen beantwortet, die sich während des Projektverlaufs ergeben. Am Ende steht ein Konzept, welches dazu beiträgt, die Offshore-Windenergie zukunftssicher zu gestalten.[8]

1 | Vgl. BWE 2017.
2 | Vgl. BMWi 2015 S. 7.
3 | Vgl. BMWi 2015, S. 10–11.
4 | Vgl. BMI 2009.
5 | Vgl. OWiSS 2017.
6 | Vgl. ebd.
7 | Vgl. ebd.
8 | Vgl. OWiSS 2017.

3 Theoretische Ansätze

Der folgende Abschnitt beschreibt die theoretischen Grundlagen, auf denen die proaktive Risikoanalyse im Rahmen des OWiSS-Forschungsvorhabens basiert. Hierzu wird ein Wirkmodell vorgestellt, aus dem sich die Vorgehensweise und die Methoden ableiten lassen.

3.1 Wirkmodell

Die interdisziplinäre Zusammensetzung der Verbundpartnerschaft führt zu unterschiedlichen Sichtweisen auf die Sicherheit. Der grundlegende Ansatz des OWiSS-Forschungsvorhabens macht es daher erforderlich, vor Beginn der Untersuchung ein einheitliches Verständnis für Sicherheit zu schaffen. Hierzu soll ein Wirkmodell dienen, das folgende Rahmenbedingungen erfüllt:

- Mögliche Beeinträchtigungen der Versorgungssicherheit können auf „gewollte" oder „ungewollte" Ereignisse zurückzuführen sein. Diese im allgemeinen Sprachgebrauch mit „Safety" oder „Security" umschriebenen Ausrichtungen der Sicherheit sollen durch das Wirkmodell in gleichem Maße berücksichtigt werden.
- Das übergeordnete Ziel des OWiSS-Forschungsvorhabens ist es, einen Beitrag zur Versorgungssicherheit der Bevölkerung zu leisten. Das Wirkmodell muss in der Lage sein, diese Zielsetzung abzubilden.
- Es kommt vor, dass einzelne sicherheitswissenschaftliche Begriffe in den jeweiligen Fachdisziplinen eine unterschiedliche Bedeutung aufweisen. Das Wirkmodell soll daher auf Begriffe zurückgreifen, die dem aktuellen Stand der Wissenschaft und Technik entsprechen beziehungsweise Eingang in die allgemein anerkannten Regeln der Technik gefunden haben.

Grundlage für die Erarbeitung eines gemeinsamen Wirkmodells bilden die Arbeiten von Schnieder und Schnieder.[9] Die Autoren schlagen zwei Wirkmodelle für den Schadensablauf vor, die zwischen „Safety" und „Security" unterscheiden. Während sich „Safety" mit dem Schutz der Umgebung vor den Gefahren des Systems beschäftigt, wird in Abgrenzung dazu „Security" als der Schutz des Systems vor Gefahren aus der Umgebung definiert.[10] Beide Ausrichtungen werden durch zentrale Begriffe unterschieden. Im „Safety"-Wirkmodell stellen die Autoren den Begriff der „Gefährdung" in den Mittelpunkt; im „Security"-Wirkmodell dagegen ist die „Bedrohung" der zentrale Terminus. Trotz dieser begrifflichen Unterschiede gelingt es den Autoren, eine gemeinsame Grundstruktur für beide Wirkmodelle herzustellen.[11]

Innerhalb der Verbundpartnerschaft erfährt die Grundstruktur des Wirkmodells breite Zustimmung, sodass entschieden wird, dieses als Grundlage für ein gemeinsames Verständnis innerhalb des OWiSS-Forschungsvorhabens zu nutzen. Allerdings sind Anpassungen notwendig, um die postulierten Rahmenbedingungen zu erfüllen. Folgende Überlegungen führen zu den Anpassungen:

1. **Aktualisierung der Begriffsdefinitionen**

   Der Begriff der „Gefährdung" hat inzwischen als „potenzielle Schadensquelle" Eingang in nationale und internationale Normen gefunden.[12,13] Auch Schnieder und Schnieder verwenden diese Definition. Anders verhält es sich mit dem Begriff „Bedrohung": Während Schnieder und Schnieder analog zur Definition der Gefährdung die Bedrohung ebenfalls als „potenzielle Schadensquelle"[14] ansehen, werden auch andere Definitionen diskutiert.

   Da ist zunächst das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es folgt im Wesentlichen der Auffassung, dass die Bedrohung der Ausgangspunkt eines Schadens ist, wenn die Bedrohung als „Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann"[15], definiert wird. Eine abweichende Sichtweise vertritt Roper, indem er die Bedrohung in Zusammenhang mit Akteuren stellt. Bedrohung (im Englischen: threat) ist demnach aufzufassen als „[...] the intention and capability of an adversary to undertake actions that would be detrimental to the interests of the asset owner"[16]. Die Bedrohung unter Einbezug eines „Akteurs" zu definieren, entspricht auch den Vorschlägen von Beyerer et al., indem sie eine Unterteilung der Gefährdung in „gewollt" und „ungewollt" vornehmen.[17] Gewollte Gefährdungen

9 | Vgl. Schnieder und Schnieder 2010, S. 73–115.
10 | Vgl. Schnieder und Schnieder 2010, S. 105.
11 | Vgl. Schnieder und Schnieder 2010, S. 107–109.
12 | Vgl. DIN 820-12 2014, S. 11.
13 | Vgl. ISO Guide 73 2009, S. 6.
14 | Schnieder und Schnieder 2010, S. 108.
15 | BSI 2017.
16 | Roper 1999, S. 13.
17 | Vgl. Beyerer et al. 2010, S. 50.

beziehen sich dabei ausschließlich auf menschliche Handlungen, die einem Motiv folgen.[18]

Auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) stellt eine Verbindung zwischen Menschen und Gefährdungen her. Das BBK definiert die „Bedrohungslage" als „Gesamtheit aller von Menschen verursachten (...) Gefährdungen".[19] Im Unterschied zu den vorgenannten Sichtweisen fehlt hier jedoch der Bezug zum aktiven Wollen.

Aus den genannten Überlegungen lässt sich der Schluss ziehen, dass die Bedrohung einen besonderen Aspekt der Gefährdung beleuchtet, indem sie auf den Menschen als bewusst Handelnden abzielt. Es ist daher naheliegend, die „Bedrohung" ausschließlich mit „Security" in Verbindung zu bringen. Dieser Sichtweise ist auch die Verbundpartnerschaft gefolgt, indem sie die Bedrohung für das OWiSS-Forschungsvorhaben definiert als „(...) eine auf einen Schaden abzielende vorsätzliche Handlung, die zu Zuständen und/oder Vorgängen führt, die die Möglichkeit eines Schadens an einem Schutzgut in sich bergen".

2. Definition der Begriffe Notfall und Notfallereignis

Schnieder und Schnieder unterscheiden die Begriffe „Schadensereignis" und „Notfall" als mögliche Folgen einer Gefährdungs- beziehungsweise Bedrohungssituation.[20] Beide Begriffe stehen für die jeweilige Ausrichtung der Sicherheit. Der Schaden kann als „Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt"[21] definiert werden. Die Zielrichtung des OWiSS-Forschungsvorhabens wird durch diese Definition jedoch nicht abgebildet. Anders verhält es sich mit der Definition des Notfalls im Sinne des BSI, wonach dieser als „(...) Schadensereignis, bei dem wesentliche Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren"[22], beschrieben wird. Für die Betrachtungen im Rahmen des OWiSS-Forschungsvorhabens ist diese Definition grundsätzlich geeignet, da die Stromerzeugung insgesamt als Prozess betrachtet werden kann, der sich wiederum in Teilprozesse gliedert.

Eine geeignetere Definition liefert der Technische Hinweis des Forums Netztechnik/Netzbetrieb im VDE. Ein Notfall ist demnach „ein schwerwiegendes, außergewöhnliches Ereignis, das Personenschäden, erhebliche Sachschäden oder gravierende Beeinträchtigungen der Stromversorgung zur Folge hat (...)".[23] Diese Definition führt den Schadensbegriff und die Zielrichtung des OWiSS-Forschungsvorhabens in adäquater Weise zusammen, sodass diese Definition von der Verbundpartnerschaft als gemeinsame Grundlage herangezogen wird. Allerdings suggerieren die verwendeten Adjektive „erheblich" und „gravierend" eine Art der Bewertung. Diese erfolgt jedoch erst nach einer Festlegung auf ein bestimmtes Ergebnis. In Übereinstimmung mit dem Wirkmodell von Schnieder und Schnieder wird daher der Begriff „Notfallereignis" eingeführt, womit ein Zustand bezeichnet wird, in dem Menschen, Güter und die Stromversorgung einen oder mehreren Gefährdungen beziehungsweise Bedrohungen ausgesetzt sind.

3. Einführung des Begriffs „Verwundbarkeit"

Das Risiko, definiert als Kombination aus Schadensausmaß und Wahrscheinlichkeit des Schadenseintritts, ist ein Bewertungsmaßstab für die Sicherheit.[24] Die Bestimmung des Risikos setzt die Kenntnis der jeweiligen Verteilungen voraus. In der Praxis stehen diese Datensätze allerdings nicht immer zur Verfügung. Dies gilt besonders für „Security"-Betrachtungen. Auch eine Abschätzung ist schwierig. Deutlich einfacher ist es jedoch, die Wirkung möglicher Barrieren abzuschätzen, die das zu betrachtende System dem Bedrohungsereignis möglicherweise entgegensetzt. Diese Überlegungen führen im Rahmen des OWiSS-Forschungsvorhabens zu dem Begriff der Verwundbarkeit. Das BBK definiert diese als „Maß für die anzunehmende Schadensanfälligkeit eines (...) Schutzgutes in Bezug auf ein bestimmtes (...) Ereignis"[25]. Ähnlich definiert Roper die Verwundbarkeit (im Englischen: vulnerability): „Any weakness that can be exploited by an adversary to gain access to an asset."[26] Im internationalen Regelwerk findet sich die Definition „intrinsic properties of something resulting to a risk source (...) that can lead to an event with a consequence (...)"[27].

18 | Vgl. Beyerer et al. 2010, S. 45–49.
19 | BBK 2013, S. 6.
20 | Vgl. Schnieder und Schnieder 2010, S. 107–109.
21 | DIN 820-12 2014, S. 11.
22 | BSI 2017.
23 | FNN 2011, S. 7.
24 | Vgl. Schnieder und Schnieder 2010, S. 102.
25 | BBK 2013, S. 28.
26 | Roper 1999, S. 14.
27 | ISO Guide 73 2009, S. 8.

Aus diesen Überlegungen ist zu folgern, dass die Verwundbarkeit als Maß für die Sicherheit herangezogen werden kann. Folgt man der Auffassung von Roper, dann ist die Verwundbarkeit in direkter Beziehung zur Bedrohung zu sehen. Insofern ist festzuhalten, dass die Verwundbarkeit als Bewertungsmaßstab für „Security"-Betrachtungen herangezogen werden kann. Für das OWiSS-Forschungsvorhaben wird daher festgelegt, die Bewertung der Gefährdungen auf Grundlage des Risikobegriffs und die Bewertung der Bedrohungen unter dem Aspekt der Verwundbarkeit zu betrachten.

Unter Berücksichtigung dieser Anpassungen lässt sich ein Wirkmodell entwerfen, das Abbildung 1 illustriert.

Ausgangspunkt des Wirkmodells ist eine Gefährdungs- beziehungsweise Bedrohungssituation. Diese ist dadurch gekennzeichnet, dass eine Gefährdung beziehungsweise Bedrohung in einem zeitlichen und räumlichen Zusammenhang mit dem Schutzgut steht. Diese Situation hat ihren Ursprung in einem konkreten Ereignis, das als Gefährdungs- beziehungsweise Bedrohungsereignis bezeichnet wird. Aus dieser Situation kann ein Notfallereignis entstehen. Ob es sich dabei um einen Notfall handelt, ist Gegenstand einer Bewertung auf Grundlage des Risikos beziehungsweise der Verwundbarkeit.

Dieses Wirkmodell dient als Grundlage für die weiteren Untersuchungen im Rahmen des OWiSS-Forschungsvorhabens.

3.2 Methodik

Die Vorgehensweise für die proaktive Analyse lässt sich aus dem Wirkmodell ableiten. Folgende Einzelschritte sind notwendig:

1. Identifizierung möglicher Notfallereignisse auf Grundlage der Gefährdungen und Bedrohungen,

2. Analyse der Notfallereignisse durch Risiko und Verwundbarkeit sowie

3. Bewertung der Notfallereignisse anhand der analysierten Risiken beziehungsweise Verwundbarkeiten.

Das beschriebene Vorgehen entspricht damit den Prozessschritten zur Risikobeurteilung nach ISO 31000.[28]

In der Praxis haben sich in der Vergangenheit zahlreiche Methoden und Techniken entwickelt, die eine proaktive Analyse unterstützen.[29] Für das OWiSS-Forschungsvorhaben wird entschieden, auf diese Methoden zurückzugreifen. Mögliche Notfallereignisse sollen daher durch eine Ereignisablaufanalyse bestimmt und analysiert werden. Die Bewertung erfolgt mithilfe der Risikomatrix.

Bei der Ereignisablaufanalyse handelt es sich um eine induktive Methode, bei der ausgehend von einem Anfangsereignis, dem auslösenden Ereignis oder Startereignis, mögliche Folgeereignisse bis hin zum Endzustand, Ergebnis genannt, betrachtet werden. Bei der Modellierung ist die Kenntnis derjenigen Einflüsse erforderlich, die der prognostizierten Wirkung des Folgeereignisses entgegenstehen; es wird von schadensmindernden Faktoren gesprochen. Die Abläufe lassen sich in einer baumartigen Struktur zusammenfassen, die Ereignisbaum genannt wird.[30,31]

Die Stärke der Ereignisablaufanalyse liegt in der Visualisierung der zeitlichen und logischen Darstellung der Folgeereignisse. Außerdem lassen sich bei bekannten Datensätzen die Wahrscheinlichkeiten der Ergebnisse nach dem Theorem der beding-

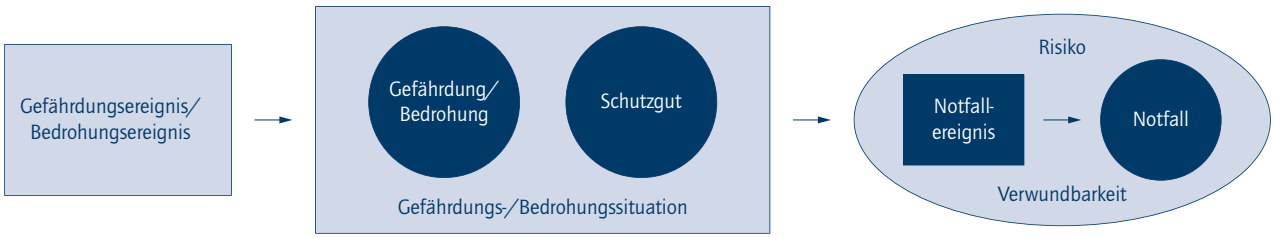


Abbildung 1: Wirkmodell für das Notfallereignis im Rahmen des OWiSS-Forschungsvorhabens (Quelle: eigene Darstellung)

28 | Vgl. ISO 31000:2009(E), S. 14.
29 | Vgl. ISO/IEC 31010, S. 22.
30 | Vgl. Preiss 2009, S. 94–100.
31 | Vgl. DIN EN 62502(VDE 0050-3) 2011, S. 8–9.

ten Wahrscheinlichkeit berechnen. Eine weitere Stärke ist das breite Anwendungsspektrum. Zu den Schwächen zählt dagegen die eingeschränkte Möglichkeit, zeitliche Abhängigkeiten zu modellieren sowie auslösende Ereignisse zu bestimmen. Auch die erforderlichen vertieften System- und Prozesskenntnisse können sich insbesondere bei der Anwendung auf komplexe Systeme als Schwäche bemerkbar machen.[32,33]

Eine Übertragung der Begrifflichkeiten des Wirkmodells auf die Ereignisablaufanalyse führt zu folgenden Analogien:

Das Gefährdungs- beziehungsweise Bedrohungsereignis des Wirkmodells kann als auslösendes Ereignis und damit als Startereignis für die qualitative Modellierung des Ereignisbaums angesehen werden. Das Notfallereignis stellt das Ergebnis und damit den Endpunkt der Ereignisablaufanalyse dar. Die Auswirkungen des Notfallereignisses manifestieren sich in dem Notfall, der sich durch Personenschaden, erhebliche Sachschäden und bedeutende Beeinträchtigungen der Stromversorgung beschreiben lässt. Eine quantitative Modellierung ist möglich. Angaben über die Häufigkeit des Startereignisses und die Abschätzung der Verzweigungswahrscheinlichkeiten sind hierzu zwingende Voraussetzung.

Für die Bewertung der Notfallereignisse und damit der Ergebnisse der Ereignisablaufanalysen wird die Risikomatrix gewählt.[34,35]

Ausgangspunkt der Risikomatrix ist ein Koordinatensystem, das durch die Variablen Häufigkeit und Folgen charakterisiert wird. Jede Achse wird durch Angabe von Grenzen in Kategorien eingeteilt, sodass eine Matrix entsteht, die üblicherweise aus neun beziehungsweise 25 Elementen besteht. Jedes Element symbolisiert einen Risikowert, der sich aus der Kombination der beiden Variablen ergibt.[36]

Eine Bewertung analysierter Risiken erfordert die Festlegung eines Grenzrisikos, das als Trennung zwischen einem akzeptablen und einem nicht akzeptablen Risiko aufgefasst werden kann. Da das Grenzrisiko nicht in allen Fällen eindeutig zu bestimmen ist, wird häufig ein dritter Bereich definiert; dieser symbolisiert den tolerablen Risikobereich. In der Risikomatrix wird die Dreiteilung der Matrixelemente üblicherweise farblich unterschieden.[37]

Die Stärke der Risikomatrix liegt in der Einfachheit des Aufbaus und der Nachvollziehbarkeit. Eine Schwäche ist die fehlende Möglichkeit zur Schadensaggregation.[38]

Während die Risikomatrix in der beschriebenen Art für die Bewertung aller Notfallereignisse, die auf einer Gefährdungssituation beruhen, unverändert angewandt werden kann, sind bei Notfallereignissen aus Bedrohungssituationen Anpassungen erforderlich.

Aufgrund der Überlegungen, dass eine Abschätzung der Häufigkeit eines Notfallereignisses ausgehend von einer Bedrohung nur schwer möglich ist (siehe Abschnitt 3.1), wird anstelle der Häufigkeit die Erfolgswahrscheinlichkeit gesetzt. Sie lässt Aussagen über die Wahrscheinlichkeit eines erfolgreichen Bedrohungsereignisses zu.

4 Praktische Umsetzung

Der folgende Abschnitt beschäftigt sich mit der Umsetzung der Risikobeurteilung im Rahmen des OWiSS-Forschungsvorhabens. Nach einer Beschreibung des Systems erfolgt eine Darstellung der Ergebnisse zur Risikoanalyse und zur Risikobewertung.

4.1 Systembeschreibung

Voraussetzung für eine wirksame Risikobeurteilung ist eine eindeutige räumliche und zeitliche Festlegung des Systems. Die räumliche Festlegung orientiert sich an der Gesamtheit des Systems und den darin befindlichen technischen Komponenten. In der ausschließlichen Wirtschaftszone der Nordsee findet sich die höchste Komplexität und größte Anzahl an Systemen und Systemvarianten; somit stehen diese im Fokus des Forschungsvorhabens OWiSS. Die zeitlichen Systemgrenzen werden durch das Offshore-Ausbauszenario bis 2020 festgelegt und durch die Lebensphasen beschrieben. Da das OWiSS-Gesamtvorhaben auf die Sicherung der Stromversorgung ausgerichtet ist, soll das System auf die Lebensphase des Betriebs beschränkt sein. In dieser Lebensphase besteht das System der Offshore-Stromerzeugung aus technischen Komponenten für die materielle Erzeugung des Stroms, den Personen, die für den Betrieb der Anlagen sorgen, und dem Umfeld, in dem die Erzeugung des Stroms erfolgt. Die Betriebsphase der Offshore-Stromerzeugung

32 | Vgl. ISO/IEC 31010, S. 53.
33 | Vgl. DIN EN 62502(VDE 0050-3) 2011, S. 9–10.
34 | Vgl. ISO/IEC 31010, S. 22.
35 | Vgl. Preiss 2009, S. 72–75.
36 | Vgl. ebd.
37 | Vgl. Preiss 2009, S. 72.
38 | Vgl. ISO/IEC 31010, S. 85–86.

ist damit ein soziotechnisches System, das von einer Vielzahl an Prozessen und Abläufen gekennzeichnet ist.

Abbildung 2 zeigt eine schematische Darstellung des betrachteten Systems Offshore-Windenergiepark und seiner Subsysteme. Zu den technischen Komponenten gehört der Windenergiepark (1) mit der Innerparkverkabelung und der Anbindung an eine parkeigene Umspannplattform (2) zur Transformation des Wechselstroms auf ein höheres Spannungsniveau. Bei großen Entfernungen von der Küste und hohen zu übertragenden Nennleistungen erfolgt die Weiterleitung des Stroms aus technischen und wirtschaftlichen Gründen durch die Hochspannungs-Gleichstrom-Übertragungstechnologie (HGÜ). Hierbei werden zwei bis drei Windenergieparks zu Clustern zusammengefasst, die den in den einzelnen Umspannplattformen gesammelten Strom an eine Konverterplattform (3) weiterleiten. Diese wandelt den Drehstrom der Windenergieparks in Gleichstrom um, wobei Leistungen von bis zu 900 MW übertragen werden. Die sogenannten Mutter-Tochter-Systeme (4) bilden zwei nah beieinanderliegende, über einen Steg miteinander verbundene Konverterplattformen mit einer hohen Gesamtübertragungsleistung. Eine dieser Konverterplattformen wird auch als Wohnplattform zur Unterbringung von Personal genutzt, sodass eine effiziente und wirtschaftliche Instandhaltung beider Plattformen erfolgen kann. Hinsichtlich des übergeordneten Ziels von OWiSS, der Sicherung der Energieversorgung, stellen sie daher ein besonders risikobehaftetes Systemelement dar. Die an das Land führenden Exportkabel (5) werden in wenigen Trassen verlegt, um den Eingriff in die Natur so gering wie möglich zu halten. Hierdurch kommt es in einigen Gebieten zu einer starken Bündelung. Dies gilt insbesondere für die Querung der Nordseeinsel Norderney (6), über die bis zu 3.000 MW Übertragungsleistung geführt wird und die somit eine hohe Risikoeinstufung erreicht. In einem ähnlichen Bereich liegen die Konverterstationen (7) an Land, die den Strom aus den Exportkabeln von bis zu drei Offshore-Konverterplattformen aufnehmen.[39,40]

Die Lebensphase des Betriebs der Offshore-Windenergieparks und ihrer Subsysteme unterteilt sich in verschiedene Prozesse, die sich von den Zuständen der Anlage ableiten.[41]

Innerhalb des OWiSS-Vorhabens werden im Wesentlichen die Kernprozesse Betrieb und Betriebsführung mit der Anlagen- und Netzüberwachung sowie die Instandhaltung mit den logistischen Unterstützungsprozessen Luftverkehr und Seeverkehr betrachtet. Die aufgeführten Prozesse werden in einzelne Teilprozesse und daraus abgeleitete Einzelschritte der Teilprozesse unterteilt und bilden damit eine Grundlage für die weiterführende Risikobetrachtung und Maßnahmenableitung.

Das für die Betriebs- und Überwachungsprozesse eingebundene Personal arbeitet im Schichtbetrieb in den Leitstellen und auf zum Teil mit Personal besetzten Umspann- und Konverterplattformen – diese Menschen zählen bei einem Notfallereignis zu den direkt Betroffenen.

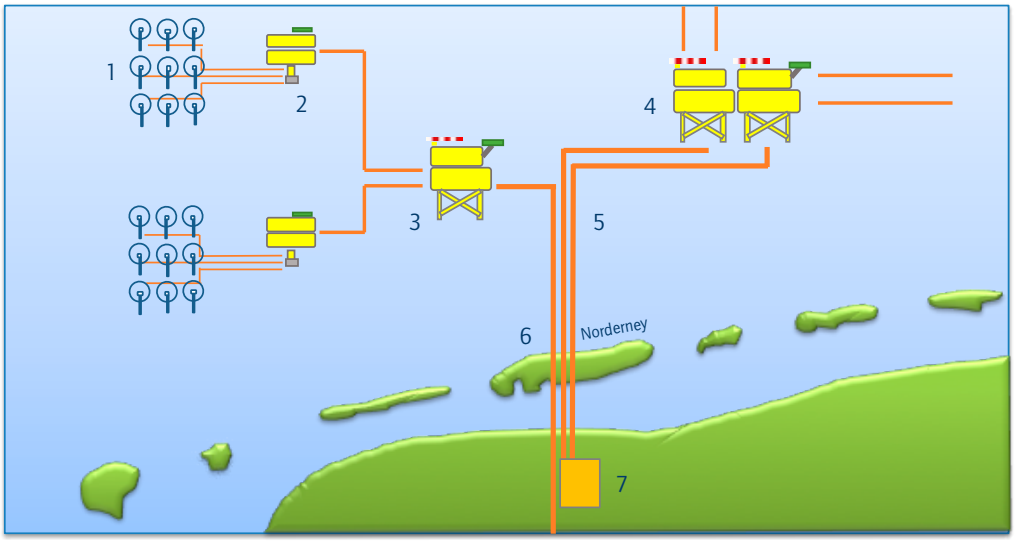


Abbildung 2: Schematische Darstellung des Systems Offshore-Windenergie (Quelle: eigene Darstellung)

39 | Vgl. Siemens 2017.
40 | Vgl. WAB e.V.
41 | Vgl. SystOP Offshore Wind 2015.

Es ist daher wichtig, die Systemgrenzen im Sinne der Safety- und Security-Definition festzulegen. Die Grenzen des Systems Offshore-Windenergiepark und seiner Subsysteme umfassen alle in Abbildung 2 aufgeführten technischen Komponenten, wobei für die Sicherung der Energieversorgung den Komponenten 3 bis 7 eine besondere Bedeutung beigemessen wird.

4.2 Identifizierung und Analyse

Die Identifizierung möglicher Notfallereignisse mithilfe der Ereignisablaufanalyse setzt die Kenntnis möglicher Gefährdungs- und Bedrohungsereignisse als Startereignisse voraus. Da die Ereignisablaufanalyse die Auswahl der Startereignisse nicht ausreichend unterstützt, wird im OWiSS-Forschungsvorhaben ein gestuftes Verfahren angewandt, das aus folgenden Schritten besteht:

1. Erstellung einer Liste möglicher Startereignisse durch „Brainstorming" unter den Verbundpartnern, Ergänzung durch Expertenbefragung und Sichtung einschlägiger Literatur,

2. Reduktion der erarbeiteten Liste durch Streichung von Doppelungen sowie

3. Erweiterung der Liste durch Bildung möglicher Kombinationen.

Das Vorgehen führt zu einer Liste von 25 Startereignissen (14 Bedrohungsereignisse, elf Gefährdungsereignisse), die den Ausgangspunkt für die Modellierung der Ereignisbäume bilden.

Um die Ereignisablaufanalyse durchführen zu können, sind grundsätzlich detaillierte System- und Prozesskenntnisse notwendig. Je ausgeprägter diese sind, desto detaillierter können die Folgeereignisse und damit die Ergebnisse ermittelt werden. Die technischen Komponenten unterliegen jedoch ebenso wie die zugehörigen Prozesse einem stetigen Wandel, der zu unterschiedlichen Realisierungen führen kann. Eine hohe Detaillierung lässt sich daher letztlich nur bei individuellen Betrachtungen jedes einzelnen Windparks erreichen. Für die Fragestellungen im OWiSS-Forschungsvorhaben wäre eine solche Vorgehensweise nicht zielführend. Daher wird entschieden, orientierende Ereignisbäume zu modellieren, die mehrere Folgeereignisse schildern und sich auf die System- und Prozessbeschreibung beziehen (siehe Abschnitt 3.3.1).

Eine weitere Reduktion der Komplexität lässt sich durch Standardisierung der Ergebnisse erzielen. Die Ergebnisse der Ereignisablaufanalysen dienen lediglich dazu, eine Entscheidung über die Notwendigkeit einer detaillierteren Folgebetrachtung zu treffen. Aus diesem Grund ist es ausreichend, wenn die erzeugten Ergebnisvarianten zu Gruppen zusammengefasst werden, die sich an der Definition des Notfalls orientieren. Unterschieden werden demnach der Personenschaden, die Beeinträchtigung des Betriebs und die Unterbrechung der Netzeinspeisung. Anhand dieser Überlegungen lässt sich ein Ereignisbaum modellieren, der lediglich aus drei Ebenen besteht. Abbildung 3 zeigt ein Beispiel für den Aufbau und die Gestaltung des Ereignisbaums für das Startereignis „Absturz Luftfahrzeug", das im Rahmen des OWiSS-Forschungsvorhabens erstellt worden ist.

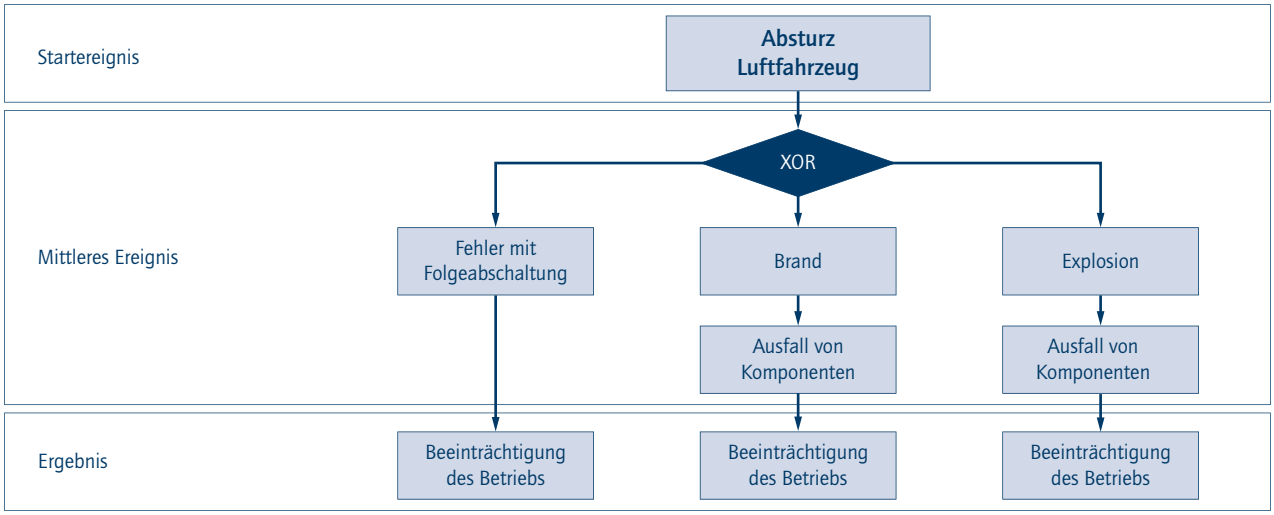


Abbildung 3: Gestaltung des Ereignisbaums im Rahmen des OWiSS-Forschungsvorhabens (Quelle: eigene Darstellung)

Trotz der vorgenommenen Reduktionen führen die Ereignisablaufanalysen zu einer Gesamtzahl von 207 Ergebnissen.

4.3 Bewertung

Die Bewertung der Ergebnisse ist darauf ausgerichtet, diejenigen Notfallereignisse zu bestimmen, die eine Relevanz für die Zielstellung des OWiSS-Forschungsvorhabens haben. Für die Bewertung mithilfe der Risikomatrix sind folgende vorbereitende Schritte notwendig:

- Festlegung der Notfallkategorien sowie
- Kategorisierung der Häufigkeiten beziehungsweise der Erfolgswahrscheinlichkeiten.

Die Notfallkategorien werden in Diskussionen mit betrieblichen Fachleuten der Windenergie festgelegt. Für die Erstellung der Risikomatrix werden die Notfälle in zwei Gruppen unterteilt und mit „immateriell" und „materiell" beschrieben. Die immateriellen Notfälle bezeichnen alle Notfallereignisse, die mit einem Personenschaden einhergehen. Alle anderen Notfälle werden der Gruppe der materiellen Notfälle zugewiesen. Durch diese Gruppeneinteilung wird die benannte Schwäche der Schadensaggregation abgemildert (siehe Abschnitt 3.2).

Nach dieser Gruppeneinteilung lassen sich nun die Notfälle kategorisieren. Die materiellen Notfallfolgen werden in Geldeinheiten gemessen, die immateriellen Folgen bemessen sich an der Zahl der irreversibel verletzten beziehungsweise getöteten Personen. Tabelle 1 zeigt beispielhaft die Kategorisierungen für Notfälle mit immateriellen Folgen, die im Rahmen des OWiSS-Forschungsvorhabens für die Bewertung herangezogen werden.

Verbale Beschreibung der Kategorie	Kategoriegrenze
Gering	Keine irreversibel Verletzten oder Toten
Mittel	Ein bis maximal vier irreversibel Verletzte oder Tote
Hoch	Fünf und mehr irreversibel Verletzte oder Tote

Tabelle 1: Kategorisierung der Notfälle mit immateriellen Folgen im OWiSS-Forschungsvorhaben (Quelle: eigene Darstellung)

Die zweite Bewertungsgröße betrifft die Häufigkeit beziehungsweise die Erfolgswahrscheinlichkeit.

Grundlage für Kategorisierungen der Notfallereignisse, die ihren Ursprung in einer Gefährdungssituation haben, sind die Häufigkeiten. Sie werden abgeschätzt und auf ein Jahr bezogen. Analog zu den Notfallfolgen wird eine Unterteilung in drei Kategorien vorgenommen, die mit hoch, mittel und gering beschrieben werden. Als gering wird dabei ein Notfallereignis betrachtet, das nur einmal in fünfzig Jahren auftritt; hoch ist die Häufigkeit dagegen bei einem Auftreten von einmal pro Jahr.

Für die Notfallereignisse, die auf ein Bedrohungsereignis zurückzuführen sind, wird ausgehend vom Ereignisbaum das Startereignis als sicheres Ereignis angesehen. Unter dieser Annahme lassen sich bei Kenntnis der jeweiligen Verzweigungswahrscheinlichkeiten die bedingten Wahrscheinlichkeiten des Notfallereignisses bestimmen. In Übereinstimmung mit den Überlegungen zum Wirkmodell lassen sich diese als Erfolgswahrscheinlichkeit interpretieren und werden in Absprache mit den Verbundpartnern in Prozent angegeben. Die Unterteilung erfolgt ebenfalls in drei Kategorien, die mit gering, mittel und hoch beschrieben sind. Eine geringe Erfolgswahrscheinlichkeit hat dabei einen Wert von unter einem Prozent, eine hohe Erfolgswahrscheinlichkeit ist bei neunzig Prozent und mehr anzunehmen.

Unter Berücksichtigung der Kategorisierungen kann nunmehr die Risikomatrix gestaltet werden. Eine Bewertung macht die Festlegung des Grenzrisikos notwendig und erfolgt gemeinsam mit den Verbundpartnern in Workshops. Die Beschränkung der Risikomatrix auf neun Elemente wirkt sich förderlich aus.

Die Ergebnisse der Festlegungen für die Grenzbereiche zeigt Abbildung 4 am Beispiel der Notfallfolgen mit Ursprung in einem Bedrohungsereignis. Die roten Elemente stellen den nicht akzeptablen Bereich, die grünen Elemente den akzeptablen Bereich und die gelben Elemente den tolerablen Bereich dar.

	Immaterielle Notfallfolgen			
Erfolgswahrscheinlichkeit		gering	mittel	hoch
	hoch			
	mittel			
	gering			

Abbildung 4: Risikomatrix für die Bewertung der „immateriellen Notfallfolgen" ausgehend von „Security"-Betrachtungen (Quelle: eigene Darstellung)

Nach Abschluss der Bewertung werden von 207 Ergebnissen insgesamt 105 als nicht akzeptabel angesehen.

5 Fazit

Die Bedeutung der Windenergie für die Stromversorgung nimmt stetig zu. Der Ausbau auf See („offshore") trägt zur Befriedigung dieser steigenden Nachfrage bei. Die Bedingungen, unter denen „offshore" Strom erzeugt wird, unterscheiden sich dabei von denen an Land. Unzureichende Erfahrungen sowie besondere Gefährdungen und Bedrohungen können zu Beeinträchtigungen der Stromversorgung führen. Das Forschungsvorhaben „OWiSS Offshore-Windenergie – Schutz und Sicherheit" setzt hier an, indem es die Gefährdungen und Bedrohungen systematisch analysiert und Maßnahmenvorschläge zur Sicherung der Energieversorgung erarbeitet.

Grundlage für die Untersuchungen im Rahmen des OWiSS-Forschungsvorhabens ist ein angepasstes Wirkmodell, das sowohl „Safety"- als auch „Security"-Betrachtungen vereint. Auf der Grundlage veröffentlichter Wirkmodelle wird unter Berücksichtigung aktueller Entwicklungen in Bezug auf die Begriffsdefinitionen ein angepasstes Wirkmodell vorgestellt, aus dem sich die Vorgehensweise für das OWiSS-Forschungsvorhaben ableiten lässt.

Für die praktische Umsetzung greift das OWiSS-Forschungsvorhaben auf etablierte Methoden und Techniken zurück. Allerdings sind auch hier Anpassungen bei den Ereignisablaufanalysen und der Risikomatrix erforderlich. Nach Abschluss der proaktiven Analyse werden insgesamt 207 Notfallereignisse identifiziert, von denen 107 als nicht akzeptabel anzusehen sind.

Die Zielstellung des OWiSS-Forschungsvorhabens erfordert an vielen Stellen eine Reduktion der Komplexität. Diese ist vor allem im Bereich der Ereignisablaufanalysen notwendig. Aber auch die Kategorisierungen im Zuge der Bewertung führen zu Vereinfachungen. Es ist davon auszugehen, dass diese grundsätzlich Informationsverluste in der Analyse zur Folge haben. Auf der anderen Seite lassen die Vereinfachungen aufgrund der Komplexität und des Umfangs erst einen Erkenntnisgewinn zu. In einer weiteren Betrachtung ist es so möglich, detailliertere Ergebnisse zu erarbeiten.

Das dem OWiSS-Forschungsvorhaben zugrunde liegende Wirkmodell hat sich als konsensfähig erwiesen und bietet sich als Grundlage für eine Übertragung auf andere interdisziplinäre Untersuchungen an. Die Vorzüge dieses Wirkmodells liegen in der Zusammenführung der nach „Safety" und „Security" getrennten Modelle und der Bezugnahme auf aktuelle Begriffsdefinitionen. Die dem Wirkmodell vorausgehenden umfangreichen Diskussionen in der Verbundpartnerschaft zeigen jedoch auch, dass ein einheitliches, interdisziplinäres Wirkmodell zur Gewährleistung der Sicherheit dringend erforderlich ist.

Literatur

BBK 2013
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): *BBK-Glossar Ausgewählte zentrale Begriffe des Bevölkerungsschutzes*, Bonn: s. n. 2013.

Beyerer et al. 2010
Beyerer, J. et al.: „Sicherheit: Systemanalyse und -design". In: Winzer, P./Schnieder, E./Bach, F.-W. (Hrsg.): *acatech DISKUTIERT Sicherheitsforschung – Chancen und Perspektiven*, Berlin: Springer-Verlag 2010.

BMI 2009
Bundesministerium des Innern: *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)* [Broschüre], Berlin: MEDIA CONSULTA Deutschland GmbH 2009.

BMWi 2015
Bundesministerium für Wirtschaft und Energie: *Die Energiewende – ein gutes Stück Arbeit Offshore-Windenergie Ein Überblick über die Aktivitäten in Deutschland* [Broschüre], Berlin: s. n. 2015.

BSI 2017
Bundesamt für Sicherheit in der Informationstechnik [online] 2017 [Zitat vom: 11.08.2017]. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/glossar/04.html.

BWE 2017
Bundesverband für Windenergie e. V. [online] 2017 [Zitat vom: 17.08.17]. URL: https://www.wind-energie.de/infocenter/statistiken/deutschland/entwicklung-der-windstromeinspeisung.

DIN 820-12. 2014
Norm DIN 820-12:2014-06 Normungsarbeit – Teil 12: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC Guide 51:2014) 2014.

DIN EN 62502(VDE 0050-3). 2011
NORM DIN EN 62502 (VDE 0050-03) Verfahren zur Analyse der Zuverlässigkeit-Ereignisbaumanalyse (ETA) (IEC 62502:2010; deutsche Fassung EN 62502:2010) 2011.

FNN. 2011
S 1002 Sicherheit in der Stromversorgung Hinweise für das Krisenmanagement des Netzbetreibers, Berlin: Forum Netztechnik/Netzbetrieb im VDE 2011.

ISO 31000:2009(E)
Norm ISO 31000:2009(E): *Risk Management – Principles and Guidelines.*

ISO Guide 73: 2009
ISO Guide 73: 2009: *Risk Management – Vocabulary.*

ISO/IEC 31010
Norm ISO/IEC 31010:2009-11: *Risk Management – Risk Assessment Techniques*.

OWiSS 2017
Offshore Windenergie – Schutz und Sicherheit [online] 2017 [Zitat vom: 17.08.2017]. URL: https://www.owiss.de/projektinformationen.

Preiss 2009
Preiss, R.: *Methoden der Risikoanalyse in der Technik Systematische Analyse komplexer Systeme*, Wien: TÜV Austria Akademie GmbH 2009. 10-3-901942-09-2.

Roper 1999
Roper, C. A.: *Risk Managemnt for Security Professionals*, Boston: Butterworth Heinemann 1999.

Schnieder und Schnieder 2010
Schnieder, E./Schnieder, L.: „Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung". In: Winzer, P./Schnieder, E./Bach, F.-W. (Hrsg.): *acatech DISKUTIERT Sicherheitsforschung – Chancen und Perspektiven*, Berlin: Springer-Verlag 2010.

Siemens 2017
www.siemens.com [online] 2017 [Zitat vom: 28.08.2017]. URL: http://www.siemens.com/press/pool/de/feature/2013/energy/2013-08-x-win/praesentation-tennet-d.pdf

SystOP Offshore Wind 2015
www.systop-wind.de [online] 2017 [Zitat vom: 27.08.2017]. URL: http://www.systop-wind.de/fileadmin/pdf/systop_gowog_20150630_webseite.pdf

WAB e. V. 2017
www.wab.net [online] 2017 [Zitat vom: 27.08.2017]. URL: https://www.wab.net/images/stories/2017-WAB-Offshorekarte.pdf

Zusammenfassung

Prof. Dr.-Ing. habil. Petra Winzer
Fachgebiet Produktsicherheit und Qualitätswesen
Bergische Universität Wuppertal

Prof. Dr. rer. nat. Jörn Müller-Quade
Lehrstuhl für Kryptographie und Sicherheit
Karlsruher Institut für Technologie

Prof. Dr.-Ing. Bernd Bertsche
Institut für Maschinenelemente, Universität Stuttgart

Sicherheit umfasst, so zeigen alle Beiträge in diesem Band, im Allgemeinen und im fachsprachlichen Gebrauch viele Aspekte aus allen Lebenslagen in Gesellschaft, Wirtschaft und Technik. Der Sicherheitsbegriff erstreckt sich von Gewissheit und Vertrauenswürdigkeit über Zuverlässigkeit bis hin zum Schutz vor Gefährdungen und Bedrohungen von innen und außen. Diese Facetten des Sicherheitsbegriffs sind Ausdruck eines erweiterten Sicherheitsverständnisses, welches den aktuellen und zukünftigen Bedürfnissen der Gesellschaft entspricht und über die sozialwissenschaftlich orientierte Risikoforschung hinausgeht. Dieses erweiterte Sicherheitsverständnis wird von den Autorinnen und Autoren auch unter dem Begriff Verlässlichkeit zusammengefasst. Die Fachleute, die im acatech Themennetzwerk „Sicherheit" zusammenarbeiten, zeigen, dass es vielfältige Initiativen, Forschungsnetzwerke sowie nationale und internationale Forschungsprojekte gibt, die sich diesem Themenfeld intensiv widmen. Trotz dieser vorwiegend zweckbestimmten Ansätze bedarf es eines methodengestützten, disziplinübergreifenden und integrierenden Theoriekonzepts, welches es gestattet, die vielfältigen Aktivitäten auch theoretisch zu bündeln. Die Systemtheorie kann dazu einen entscheidenden Beitrag leisten und die Aktivitäten in einer transdisziplinären Sicherheitsforschung zusammenführen. Schwerpunkt dessen ist zum einen, durch Abstraktion gemeinsame Konzepte zu identifizieren und diese dann zu modellieren, wobei geeignete Termini und Beschreibungsmittel symbolischer und formaler Natur zu finden sind. Dies kann dann zu konsistenten Begriffsgebäuden und akzeptablen oder sogar universellen Metriken der Sicherheit beziehungsweise Verlässlichkeit führen. Durch diese methodisch-systematische Vorgehensweise werden zum anderen die verschiedenen Perspektiven, Begrifflichkeiten und so weiter transparent, was zu deren Integration – allerdings auf einem höheren Abstraktionsniveau – führen wird. Mit dieser Vorgehensweise könnte eine Theorie der Sicherheit/Verlässlichkeit begründet werden.

Die Herausforderungen der Zukunft werden in folgenden vier Thesen zusammengefasst:

1. These: Überwindung der begrifflichen Vielfalt ist Voraussetzung für ein zu entwickelndes transdisziplinäres Theoriekonzept der Sicherheit.

2. These: Kommunikation und Begriffsbildung sind die Basis für das gemeinsame Handeln.

3. These: Sicherheit ist eine emergente Verhaltenseigenschaft und erfordert eine systemische Betrachtung.

4. These: Verlässlichkeit von technischen und soziotechnischen Systemen ist konstruierbar.

1. These: Überwindung der begrifflichen Vielfalt ist Voraussetzung für ein zu entwickelndes transdisziplinäres Theoriekonzept der Sicherheit

Die Sicherheit/Verlässlichkeit technischer und soziotechnischer Systeme kann nur nachhaltig gewährleistet werden, wenn die disziplin- und domänenspezifische Aufspaltung des Wissenschaftsgebiets Sicherheit überwunden wird.

Lösungsansatz:
Voraussetzung für eine domänen- beziehungsweise disziplinübergreifende Sicht ist eine inter- und transdisziplinäre Erarbeitung von fachdisziplinübergreifender Modellierung und Terminologie. Das ist die Basis zur inter- beziehungsweise transdisziplinären Modell- und Theoriebildung. Besonderes Augenmerk ist dabei auf die Integration bestehender Methoden zu legen, wobei eine disziplinübergreifende transdisziplinäre Herangehensweise zu fokussieren ist.

2. These: Kommunikation und Begriffsbildung sind die Basis für das gemeinsame Handeln

Eine fachdisziplinübergreifende Sicherheitsforschung und -technologie erfordert eine gemeinsame Kommunikationsbasis mit harmonisierten Begriffen, Terminologien und Kommunikationsprozessen der menschlichen und organisatorischen Akteure.

Lösungsansatz:
Die Herausbildung einer harmonisierten Terminologie im Begriffsfeld der erweiterten Sicherheit beziehungsweise Verlässlichkeit im soziotechnischen Kontext ist Basis für eine zu entwickelnde gemeinsame Kommunikationsplattform. In diesem Zusammenhang müssen Modelle von Kommunikationsprozessen, die auch die Wahrnehmung von Verlässlichkeit betreffen, bei den Modellentwicklungen untersucht werden, wie sie beispielsweise in der zentralen Modellierung sicherer Systeme funktionieren.

3. These: Sicherheit ist eine emergente Verhaltenseigenschaft und erfordert eine systemische Betrachtung

Sicherheit ist als emergente Verhaltenseigenschaft komplexer Systeme modellierbar. Die zunehmende Komplexität von technischen wie auch soziotechnischen Systemen erfordert eine systemische Betrachtung, auf deren Basis abstrahierte Modelle für Sicherheit beziehungsweise Verlässlichkeit dieser Systeme gebildet werden können. Somit ist eine Systemtheorie der Verlässlichkeit beziehungsweise ein erweitertes Sicherheitsverständnis zu erarbeiten.

Lösungsansatz:
Um dem Charakter der Systemtheorie der Sicherheit als wissenschaftliches Rückgrat der Forschung zur Verlässlichkeit technischer und soziotechnischer Systeme gerecht zu werden, muss die Entwicklung dieser Theorie vorangetrieben werden. Ziel ist es, Sicherheit als inhärente und emergente Eigenschaft von Systemen systemtheoretisch zu identifizieren, zu modellieren und qualitativ wie quantitativ zu beschreiben. Dies soll durch eine Verschränkung von sozialwissenschaftlichen und ingenieurwissenschaftlichen Ansätzen in einer transparenten Modellierung von technischen und soziotechnischen Systemen erreicht werden.

4. These: Verlässlichkeit von technischen und soziotechnischen Systemen ist konstruierbar

Die präventive Gestaltung komplexer technischer und soziotechnischer Systeme gemäß dem erweiterten Sicherheitsverständnis erfordert eine methodische Vorgehensweise zum Entwurf integrierter Verlässlichkeitskonzepte.

Lösungsansatz:
Modellkonzepte und Terminologien sind Voraussetzungen und Instrumente eines methodischen Vorgehens, um Sicherheit in komplexen technischen beziehungsweise soziotechnischen Systemen erzeugen und aufrechterhalten zu können. Dazu dienen konkrete Vorgehensweisen auf normativer, strategischer und operativer Ebene unter zweckdienlicher Einbeziehung der einzelnen Beteiligten und Betroffenen in ihrer jeweiligen Rolle sowie geeignete Methoden der Kommunikation und der Darstellung von Bedürfnissen, um neben der erforderlichen Transparenz auch die Balance zwischen rechtlichen Ressourcen, Nutzen oder anderen Zielkonflikten herzustellen.

Zusammenfassend kommt die Expertengruppe des acatech Themennetzwerks „Sicherheit" zu dem Schluss, dass die Überwindung der Diversität im Sinne des erweiterten Sicherheitsverständnisses, auch als Verlässlichkeit bezeichnet, durch eine systemische Betrachtung möglich wird. Diese kann allgemeine und spezielle Konzepte und Methoden der Systemtheorie aus der Technik sowie den Sozialwissenschaften mittels formalisierter Modelle transdisziplinär integrieren. So kann auf Basis der Systemtheorie eine Theorie für das erweiterte Sicherheitsverständnis beziehungsweise der Verlässlichkeit entwickelt werden. Ihre hervorstechenden Merkmale sind die Änderung des Blickwinkels von einer reaktiven zu einer formalisierten, analysefähigen und konstruktiven Sichtweise und die ganzheitliche effiziente sowie effektive Gestaltung der Sicherheit komplexer technischer und soziotechnischer Systeme.

acatech – Deutsche Akademie der Technikwissenschaften

acatech vertritt die deutschen Technikwissenschaften im In- und Ausland in selbstbestimmter, unabhängiger und gemeinwohlorientierter Weise. Als Arbeitsakademie berät acatech Politik und Gesellschaft in technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Darüber hinaus hat es sich acatech zum Ziel gesetzt, den Wissenstransfer zwischen Wissenschaft und Wirtschaft zu unterstützen und den technikwissenschaftlichen Nachwuchs zu fördern. Zu den Mitgliedern der Akademie zählen herausragende Wissenschaftlerinnen und Wissenschaftler aus Hochschulen, Forschungseinrichtungen und Unternehmen. acatech finanziert sich durch eine institutionelle Förderung von Bund und Ländern sowie durch Spenden und projektbezogene Drittmittel. Um den Diskurs über technischen Fortschritt in Deutschland zu fördern und das Potenzial zukunftsweisender Technologien für Wirtschaft und Gesellschaft darzustellen, veranstaltet acatech Symposien, Foren, Podiumsdiskussionen und Workshops. Mit Studien, Empfehlungen und Stellungnahmen wendet sich acatech an die Öffentlichkeit. acatech besteht aus drei Organen: Die Mitglieder der Akademie sind in der Mitgliederversammlung organisiert; das Präsidium, das von den Mitgliedern und Senatoren der Akademie bestimmt wird, lenkt die Arbeit; ein Senat mit namhaften Persönlichkeiten vor allem aus der Industrie, aus der Wissenschaft und aus der Politik berät acatech in Fragen der strategischen Ausrichtung und sorgt für den Austausch mit der Wirtschaft und anderen Wissenschaftsorganisationen in Deutschland. Die Geschäftsstelle von acatech befindet sich in München; zudem ist acatech mit einem Hauptstadtbüro in Berlin und einem Büro in Brüssel vertreten.

Weitere Informationen unter www.acatech.de

Herausgeber:

Prof. Dr.-Ing. Jürgen Beyerer
Fraunhofer-Institut für Optronik, Systemtechnik
und Bildauswertung IOSB
Fraunhoferstraße 1
76131 Karlsruhe

Prof. Dr.-Ing. Petra Winzer
Bergische Universität Wuppertal
Fachgebiet Produktsicherheit/Qualitätswesen
Gaußstraße 20
42119 Wuppertal

Reihenherausgeber:
acatech – Deutsche Akademie der Technikwissenschaften, 2018

Geschäftsstelle
Karolinenplatz 4
80333 München
T +49 (0)89/52 03 09-0
F +49 (0)89/52 03 09-900

Hauptstadtbüro
Pariser Platz 4a
10117 Berlin
T +49 (0)30/2 06 30 96-0
F +49 (0)30/2 06 30 96-11

Brüssel-Büro
Rue d'Egmont/Egmontstraat 13
1000 Brüssel (Belgien)
T +32 (0)2/2 13 81-80
F +32 (0)2/2 13 81-89

info@acatech.de
www.acatech.de

Empfohlene Zitierweise:
Beyerer, J./Winzer, P. (Hrsg.): *Beiträge zu einer Systemtheorie Sicherheit* (acatech DISKUSSION), München: Herbert Utz Verlag 2018.

ISSN 2192-6182

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Koordination: Dr. Anna Frey
Redaktion: Evi Draxl
Layout-Konzeption: Groothuis, Hamburg
Konvertierung und Satz: Fraunhofer IAIS, Sankt Augustin

Die Originalfassung der Publikation ist verfügbar auf www.utzverlag.de

Die Sicherheit soziotechnischer Systeme ist von großem gesellschaftlichem Interesse. Jedoch sind soziotechnische Systeme komplex, und ihre Sicherheit involviert viele Disziplinen: Technik- und Naturwissenschaften sowie Rechts-, Geistes- und Sozialwissenschaften. Bislang gibt es keine durchgängige Theorie, mit der sich die Sicherheit derart komplexer Systeme beschreiben und berechnen lässt und die ein einheitliches Theoriekonstrukt zur Verfügung stellt. In der Geschichte der Wissenschaft und Technik sind jedoch viele Gebiete bekannt, die erst nach Erscheinen einer grundlegenden Theorie eine erfolgreiche Entwicklung genommen haben.

Im Rahmen des acatech Themennetzwerks Sicherheit wurde in den letzten drei Jahren intensiv mit der Fragestellung einer Systemtheorie für die Sicherheit gerungen. Eine interdisziplinäre Gruppe von Wissenschaftlerinnen und Wissenschaftlern stellt in dem vorliegenden Band erste Beiträge zu einer generalisierenden Systemtheorie Sicherheit der Fachgemeinde und der interessierten Öffentlichkeit zur Diskussion.