Verbundforschungsprojekt RiKoV

Risiken und **Ko**sten der terroristischen Bedrohungen des schienengebundenen ÖP**V**:

Entwicklung einer Planungslösung für die ökonomische und organisatorische Optimierung präventiver und abwehrender Maßnahmen

Schlussbericht

gem. § 9 Abs. 2 – BMBF-ZE 98

Auftragnehmer:	Technische Hochschule Köln
Kennzeichen:	FKZ 13N12305
Auftragsbezeichnung:	RiKoV Risiken und Kosten der terroristischen Bedrohungen des schienengebundenen ÖPV: Entwicklung einer Planungslösung für die ökonomische und organisatorische Optimierung präventiver und abwehrender Maßnahmen
Laufzeit:	01.11.2012 - 31.01.2016

Technische Hochschule Köln

Institut für Rettungsingenieurwesen und Gefahrenabwehr

Prof. Dr.-Ing. Ompe Aimé Mudimu

Prof. Dr. med. Dr. rer. nat. Alex. Lechleuthner

Dr.-Ing. Florian Brauner

Betzdorfer Str. 2

D-50679 Köln

Erschienen im Juni 2016 in Köln

ISBN **978-3-946573-02-9**

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Inhaltsverzeichnis

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

1 Rahmenbedingungen

Dieser Schlussbericht beinhaltet die geleisteten Arbeiten der Technischen Hochschule Köln im Verbundforschungsprojekt RiKoV (Risiken und Kosten der terroristischen Bedrohungen des schienengebundenen ÖPV: Entwicklung einer Planungslösung für die ökonomische und organisatorische Optimierung präventiver und abwehrender Maßnahmen) innerhalb der Laufzeit vom 01. November 2012 bis zum 31. Januar 2016. Dabei gliedert sich der Schlussbericht auf der einen Seite in die grundsätzlichen Aufgaben und Voraussetzungen sowie Planungen für den Auftrag sowie auf der anderen Seite die produzierten Ergebnisse der Technischen Hochschule Köln. Für eine inhaltlich logische Zusammenstellung der notwendigen Informationen werden auf Bestandteile der Gesamtvorhabenbeschreibung des Verbundforschungsprojekts “RiKoV” sowie auf die Teilvorhabenbeschreibung der Technischen Hochschule Köln (Fachhochschule Köln) zurückgegriffen. Aufgrund der Übersichtlichkeit wird auf eine detaillierte Zitierung entsprechend verzichtet.

Anmerkung
Die „Fachhochschule Köln“ trägt seit dem 01. September den Namen „Technische Hochschule Köln“ (TH Köln).

1.1 Aufgabenstellung

Basierend auf der Gesamtvorhabenbeschreibung sollte am Beispiel des schienengebundenen öffentlichen Personenverkehrs (ÖPV) im Rahmen des Verbundforschungsprojekts RiKoV gezeigt werden, wie kritische Infrastrukturen durch ein ganzheitliches Risikomanagement (RM) besser vor terroristischen Anschlägen geschützt werden können. Im Rahmen eines solchen Risikomanagements werden die terroristischen Bedrohungen und Verwundbarkeit der Infrastruktur erfasst, die dadurch verursachten Risiken hinsichtlich Konsequenzen und Kosten unter Berücksichtigung der praktischen Erfahrungen von Polizei und Betreibern bewertet, die abgeschätzten Infrastrukturrisiken mit den Erkenntnissen der Sicherheitsbehörden evaluiert, abgestimmt und gegebenenfalls abgeglichen, geeignete Maßnahmen identifiziert und bewertet, die inakzeptable Risiken beseitigen beziehungsweise deren Konsequenzen abmildern, ohne gegen gesellschaftliche Wertvorstellungen, Grundrechte und gesetzliche Regelungen zu verstoßen. Weiterhin werden Realisierungspläne für die Schutzmaßnahmen unter Berücksichtigung wirtschaftlicher Rahmenbedingungen aufgestellt und die Konsequenzen aufgezeigt. Hierbei finden insbesondere auch behördliche Entscheidungsparameter Eingang, nach denen Schutzmaßnahmen vorgeschlagen oder angeordnet werden. Damit zielt das ganzheitliche Risikomanagement darauf ab, in dem Spannungsfeld zwischen den technisch und organisatorisch maximal erreichbaren, der wirtschaftlich sinnvollen und den von den gesellschaftlichen Werten abgeleiteten Sicherheitsbegriffen die optimale Sicherheit zu erreichen, die Prävention als auch Gefahrenabwehr umfasst.

Der Lösungsansatz von RiKoV sieht vor, die Vorgehensweise des Projektes am Bedarf des RM-Prozesses auszurichten und für jeden der RM-Teilprozesse geeignete quantitative und qualitative Methoden bereit zu stellen, die aufeinander aufbauen und in ihrer Gesamtheit ein Planungssystem für betriebswirtschaftlich optimale Sicherheit darstellen. Dazu wird ein Konzept „terroristische Bedrohung“ erstellt,

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

das Angreifer hinsichtlich ihrer Motivation und ihres Verhaltens unter Berücksichtigung ihrer technischen und operationellen Möglichkeiten modelliert und potentielle Angriffsziele, eingebettet in eine generische ÖPV-Infrastruktur, beschreibt. Auf dieser Basis und auf der Basis des Antwortverhaltens der generischen Infrastruktur werden Angriffsszenarien erarbeitet, die die Grundlage für eine szenariobasierte Risikobewertung bilden. Die Szenarien werden einer operationsanalytischen Bewertung unterzogen und die Kosten der Schäden werden bewertet. Für alle nicht tolerierbaren Risiken werden technologische, organisatorische, personelle und betriebliche Sicherheitsmaßnahmen ermittelt, hinsichtlich ihrer Kosten sowie ihres Beitrages zur Risikoeindämmung und ihrer gesellschaftlichen Akzeptanz bewertet und unter Berücksichtigung von Mehrzielentscheidungen priorisiert. Die Realisierungsmöglichkeiten der Sicherheitsmaßnahmen werden mit Hilfe eines regelbasierten Optimierungsansatzes untersucht. Die Validierung der „realisierbaren“ Maßnahmen geschieht mit Hilfe der operationsanalytischen Bewertung unter Berücksichtigung der Bedrohungsszenarien.

Das Durchlaufen dieses Analyse- und Bewertungsprozesses, die Auswahl möglicher Lösungen sowie Analyse der Realisierungsmöglichkeiten der Sicherheitsmaßnahmen erfordert eine enge Zusammenarbeit mit den für den Schutz dieser Infrastrukturen zuständigen Behörden. Zur Verbreitung und Verwertung der Projektergebnisse wurde ein eigenes Arbeitspaket eingerichtet, das zunächst den Kreis der Interessenten identifiziert und im Laufe des Projektes die Projektergebnisse diesem Kreis bekannt macht. Dabei wurde auf bewährte Hilfsmittel der Verbreitung und Verwertung von Ergebnissen zurückgegriffen wie zum Beispiel:

- Bereitstellung von Kommunikationstools zur Verbreitung relevanten Projektergebnisse
- Präsenz und Präsentationen auf Konferenzen und Workshops
- Networking zum Ergebnistransfer und zur Verbesserung der Marktchancen
- Wissenschaftliche Ergebnisverwertung durch die Universitäten
- Wirtschaftliche Ergebnisverwertung: Jeder Verbundpartner stellt seine originären Ergebnisse in geeigneter Form dar und vertritt sie in den entsprechenden Gremien mit dem Ziel, neue Geschäftsentwicklungen zu ermöglichen.

Dazu hat jeder Verbundpartner die Projektergebnisse so weit wie möglich bei den verschiedenen Interessensgruppen seines Netzwerks verankert und Wege aufgezeigt, wie die Projektergebnisse nach Abschluss des Projektes zu markt- und konkurrenzfähigen Produkten weiterentwickelt und mit welchen Geschäftsmodellen für „Security made in Germany“ deutsche Unternehmen in Zukunft auf dem internationalen Markt bestehen könnten.

1.2 Voraussetzungen

Die Voraussetzungen für die Durchführung des Forschungsvorhaben der Technischen Hochschule Köln zur Erreichung der Aufgabenstellung ergaben sich auf der einen Seiten durch die genehmigten Vorhabenbeschreibungen für das Verbundforschungsprojekt durch den Projektträger und auf der anderen Seite durch den Zuwendungsbescheid durch das Bundesministerium für Bildung und Forschung (BMBF) vom 26. Oktober 2012 mit dem Förderkennzeichen 13N12305. Durch die Technische Hochschule Köln wurden während der gesamten Projektlaufzeit die dort definierten Voraussetzungen stets eingehalten, um ein erfolgreiches Forschungsvorhaben zu ermöglichen.

RiKoV strebte als Ziel an die Auswahl von Sicherheitsmaßnahmen auf Basis von Aufwand-, Nutzen- und Akzeptanzbewertungen zu erheben, um ÖPV-Systeme sicherer zu machen und leistet somit einen Beitrag zu den Forschungsthemen „Sicherheitsökonomie“ und „Sicherheitsarchitektur“, die in der Bekanntmachung des BMBF über die Förderung von Forschungsvorhaben zu Sicherheitsökonomie und Sicherheitsarchitektur vom 19.11.2010 aufgeführt sind. Zu diesen Themen leistete das Projekt wie folgt wertvolle Beiträge:

a) **Sicherheitsökonomie:** „Ökonomische Folgen sicherheitskultureller Wandlungsprozesse“ Terroristische Anschläge auf den ÖPV und kriminelle Ereignisse in Zügen und Bahnhöfen erzeugen ein wachsendes Verunsicherungspotential bei Kunden und verstärken die Forderung nach mehr Sicherheit im ÖPV. Diese Entwicklung wurde durch erheblichen Personalabbau durch die Betreiber sowie durch Fehlen von Alternativen zum ÖPV verstärkt. Mittlerweile ist dieses Problem den Betreibern bewusst und sie beginnen gegenzusteuern. Im Rahmen der Risikoanalyse muss hier zwischen Mitteleinsatz und Risikoreduzierung abgewogen werden. Wie aber schon im Flugverkehr[1] wird auch bei den Kunden des ÖPV ein sicherheitskultureller Wandlungsprozess einsetzen, der zu vermehrten Sicherheitsinvestitionen führen wird. Dabei sind Wertekonflikte[2] möglich und müssen behutsam ausbalanciert werden. Der Mix an Sicherheitsmaßnahmen wird im Projekt hinsichtlich seines Beitrages zur zivilen Sicherheit, aber auch seiner gesellschaftlichen und juristischen Akzeptanz überprüft.

b) **Sicherheitsökonomie:** „Ökonomische Bewertung von Sicherheitsanforderungen“: Das Projekt hat Maßnahmen zur Eindämmung von Sicherheitsrisiken identifiziert, sie hinsichtlich ihrer Kosten und Realisierungsmöglichkeiten innerhalb eines vorgegebenen Planungshorizontes bewertet und einen optimierten Investitionsplan unter Berücksichtigung vorgegebener Planungsrestriktionen empfohlen.

c) **Sicherheitsarchitektur**: „Gestaltung von Sicherheit unter zunehmender Beteiligung gesellschaftlicher Akteure im Bereich von kritischen Infrastrukturen“ Angebot und Nachfrage bestimmen nicht mehr alleine die Ausgestaltung des ÖPV. Neben Wirtschaftlichkeit werden auch ökologische Aspekte und Sicherheit als Wettbewerbsvorteil des ÖPV angeführt. Das heißt, neben Betreiber und Kunden bestimmen auch Staat und gesellschaftliche Gruppen (z.B. Umweltbewegung) die Agenda des ÖPV. RIKOV erfasst die Einflüsse solcher Akteure über die gesellschaftlichen Dimensionen des Vier-Säulenmodells.

d) **Sicherheitsarchitektur:** „Sicherheit des öffentlichen Raums im Kontext des Zusammenwirkens öffentlicher und privater Sicherheitsdienstleister“. Im Vergleich zu anderen Infrastrukturbetreibern hat der ÖPV viel Erfahrung in der Zusammenarbeit von privaten Sicherheitsdiensten und der Polizei. In diesem Projekt interessiert nicht nur die Frage, inwieweit durch neuartige Technologien (z.B. integrierte Leitstellen, Common Operational Picture (COP), Command and Control (C2)) die Zusammenarbeit effizienter gestal-

[1] Im Vergleich zum Flugverkehr mit seinem abgeschlossenen Sicherheitssystem wird es aber beim ÖPV kaum zu einem abgeschlossenen Sicherheitssystem kommen können (innerhalb des offenen Gesamtsystems sind allenfalls geschlossene Insellösungen denkbar wie z.B. beim EUROSTAR), da sonst der bestimmungsgemäße Betrieb zusammenbrechen würde.

2 Beispiele für solche Konflikte sind: Sicherheit versus Freiheit des Individuums, Sicherheit versus Schutz der Privatsphäre oder „privatisierte“ Sicherheit versus gesellschaftlicher Zusammenhalt.

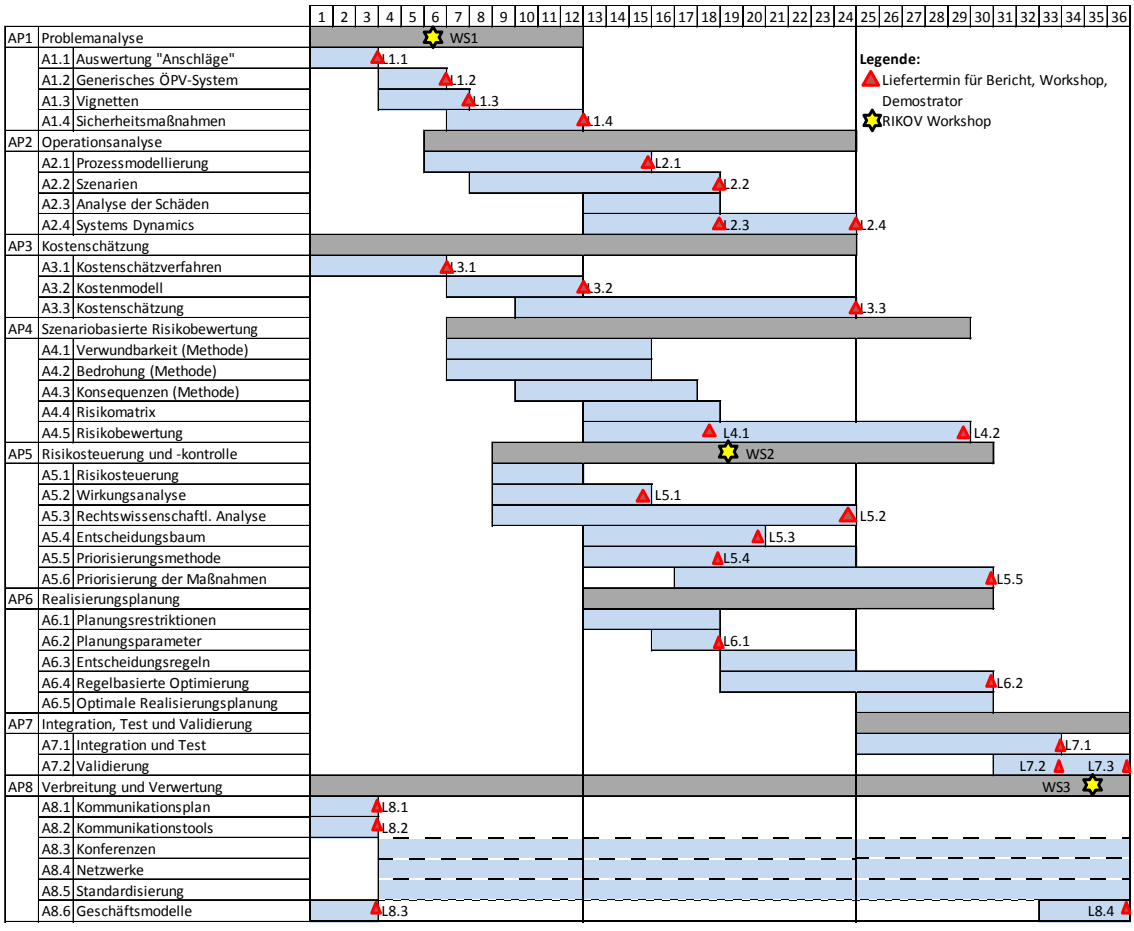
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

tet werden kann, sondern auch wie eine Sicherheitspartnerschaft von Behörden und Betreibern etwa im Rahmen einer Private Public Partnership (PPP) vor dem Hintergrund reduzierter Finanzmittel entworfen werden kann.

1.3 Planung und Ablauf des Vorhabens

Die Planungen und der Ablauf des Forschungsvorhabens zur Erreichung der Aufgabenstellung orientierten sich an der Gesamtvorhabenbeschreibung des Verbundforschungsprojekts RiKoV sowie an der eigenen Teilvorhabenbeschreibung der Technischen Hochschule Köln. Für eine einfache inhaltliche Verknüpfung sind diese Beschreibungen dem vorliegenden Schlussbericht als Anhang beigefügt (siehe Anhang A 5). Der ebenfalls auf diesen Beschreibungen basierende Projektplan ist in Tabelle 1 ersichtlich. Das Verbundforschungsprojekt „RiKoV“ unterteilte sich dabei aufbauend in acht verschiedene Arbeitspakte, welche inhaltlich aufbauend zusammenfließen. Auf eine detaillierte Beschreibung der einzelnen Arbeitspakete wird in diesem Schlussbericht verzichtet, da diese der Gesamtvorhabenschreibung entnommen werden können. Vielmehr sollen in Kapitel 3 die durch die Technische Hochschule Köln produzierten Ergebnisse in den einzelnen Teilarbeitspaketen aufgeführt werden.

Tabelle 1: Projektplan



Seitens der Technischen Hochschule Köln konnten die in der Teilvorhabenbeschreibung festgelegten Lieferungen innerhalb der Arbeitspakete fristgerecht dem Projektkonsortium zur Verfügung gestellt werden. Dabei handelt es sich spezifisch um die folgenden Lieferungen, welche als Dokumentationsnachweis diesem Schlussbericht als Anhang beigefügt werden (siehe Anhang A 4).

- L1.4 Bericht „Analyse potenzieller Sicherheitsmaßnahmen“
- WS1 Workshop „ÖPV-Vignetten“ mit externen Experten
- L2.1 Bericht „Prozessmodellierung der Operationspläne“
- L7.2 Bericht „Integration und Test“
- L7.3 Bericht „Validierung der Planungsergebnisse“

Darüber hinaus wurden im Rahmen der zur Verfügung stehenden Mann-Monate die entsprechenden Aufgaben nach Teilvorhabenbeschreibung übernommen. Diese konkreten produzierten Ergebnisse und Aktivitäten der Technischen Hochschule Köln innerhalb des Verbundforschungsprojekts „RiKoV“ können ebenfalls dem Kapitel 3 entnommen werden.

1.4 Wissenschaftlicher und technischer Stand

Bereits in der Gesamtvorhabenbeschreibung des Verbundforschungsprojekts „RiKoV“ sind diverse bereits vorhandene wissenschaftliche Forschungsvorhaben, Studien und Verfahren aufgeführt, auf denen das Forschungsvorhaben des Projektkonsortiums und damit auch der Technischen Hochschule Köln aufbaut. Dieser Stand von Wissenschaft und Technik wurde durch die Technische Hochschule Köln bei der Durchführung des Forschungsvorhabens durchgängig berücksichtigt. Darüber hinaus haben sich im Laufe des Verbundforschungsprojekts „RiKoV“ viele Schnittstellen zu anderen aktuellen Forschungsvorhaben der Sicherheitsforschung im deutschen und europäischen Raum ergeben. So konnten Kenntnisse des bereits abgeschlossen EU-Projekts COUNTERACT[3] in RiKoV integriert und entsprechend weiterentwickelt werden. Mit Hilfe des Projektträgers konnte Kontakt zum BMBF-Projekt TERAS-INDEX[4] hergestellt werden, welches thematisch eng mit RiKoV verknüpft ist. Des Weiteren konnten Projektergebnisse und –Erfahrungen mit den Projekten SECUR-ED[5] und InREAKT[6] ausgetauscht werden, was zur positiven Weiterentwicklung eigener Forschungsergebnisse verhalf. Darüber hinaus erfolgte die Verwendung eigener recherchierter Fachliteratur sowie die Benutzung von verschiedenen Informationsdiensten, um die das Forschungsvorhaben durchzuführen und die gewünschten Ergebnisse zu erzielen. Eine alphabetische Auflistung der verwendeten Fachliteratur und Informationsdienste kann dem Anhang A 3 entnommen werden.

[3] http://cordis.europa.eu/project/rcn/85653_en.html

[4] http://www.bmbf.de/pubRD/Projektumriss_TERAS-INDEX.pdf

[5] http://cordis.europa.eu/project/rcn/98621_en.html

[6] http://www.bmbf.de/pubRD/Projektumriss_InREAKT.pdf

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

1.5 Zusammenarbeit mit anderen Stellen

Im Rahmen des Verbundforschungsprojekts RiKoV erfolgte die Zusammenarbeit überwiegend mit den projektzugehörigen Verbundpartnern und assoziierten Partnern, welche nachfolgend in Kurzform dargestellt werden. Dabei erfolgt eine kurze Beschreibung der wissenschaftlichen Tätigkeiten im Projektkontext, um die vorhandene Expertise für das Verbundforschungsprojekt RiKoV aufzuzeigen. Es handelt sich um eine Beschreibung, welche durch die Verbundpartner und assoziierten Partner im Projektkontext eigenständig erstellt worden sind. Darüber hinaus erfolgte durch die Technische Hochschule Köln, zur Erreichung der Projektziele, die Einbindung von weiteren Behörden, Organisationen und Unternehmen.

1.5.1 Verbundpartner

Tabelle 2: Verbundpartner

der Bundeswehr Universität München	**Universität der Bundeswehr München** Professur für Operations Research Prof. Dr. Stefan Pickl (Projektleitung) Werner-Heisenberg-Weg 39 85577 Neubiberg Telefon: +49 89 6004 2400 Email: Stefan.Pickl@unibw.de
Der Schwerpunkt der Arbeiten der „Professur für Operations Research (OR)“ an der Universität der Bundeswehr München (UniBw) liegt auf dem Forschungsgebiet „Safety and Security“: Schlüsseldisziplinen in diesem Kontext sind Decision Analysis, Data Mining, Network Communication und Sicherheit kritischer Infrastrukturen. Die Professsur für OR ist auch verantwortlich für das Projekt „Modelling Operations Research Simulation and Experimentation“ (MORSE), leitet darüber hinaus das Forschungsprogramm „Critical Infrastructures and Systems Analysis“ und ist Kooperationspartner der Naval Postgraduate School Monterey/USA in dem internationalen Experiment „CENETIX“ (Centre for Network Innovation and Experimentation), in dessen Rahmen neue Techniken und Methoden entwickelt werden mit dem Ziel, mittels Training die Zusammenarbeit und Koordination aller Elemente des Risiko- und Krisenmanagements zu verbessern. Das der Professur angeschlossene Kompetenzzentrum COMTESSA beschäftigt sich mit Schwerpunkt mit der Anwendung von „Soft Computing“ für Krisen- und Notfallmanagement. Weitere Forschungsprojekte des Lehrstuhls waren “Intelligent Networks and Security Structures” (INESS), “Critical Infrastructures and System Analysis” (CRISYS) und „Experimentelle Prozess Optimierung“ (EXPO). Daneben bestehen Kompetenzen im Bereich Optimierungsverfahren, insbesondere Heuristiken. Im Rahmen des EU-Projekts „Network for the Economic Analysis of Terrorism“ (NEAT), wurde vom Lehrstuhl für OR gemeinsam mit den Herren Neubecker und Schmitz eine Kurzstudie zum Thema „An Economic Impact Analysis on Terrorist Attacks against Public Transport Networks“ (Oktober 2009) durchgeführt, die sich mit den wirtschaftlichen Auswirkungen terroristischer Angriffe auf den öffentlichen Personennahverkehr befasste. Diese Kurzstudie kann als Vor- und Machbarkeitsstudie für dieses Forschungsvorhaben angesehen werden.	

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Karlsruher Institut für Technologie (KIT)
Institut für Industriebetriebslehre und Industrielle Produktion (IIP)
Prof. Dr. Frank Schultmann
Hertzstraße 16
76187 Karlsruhe
Telefon: +49 721 608 44469 44569
Email: Frank.Schultmann@kit.edu

Das Institut für Industriebetriebslehre und Industrielle Produktion (IIP) am Karlsruher Institut für Technologie (KIT) verwendet interdisziplinäre Methoden zur Lösung technischer und ökonomischer Problemstellungen. Das Institut berät Auftraggeber (BMBF, EU, Unternehmen, etc.) auf regionaler, nationaler und internationaler Ebene durch Projekte zu Problemstellungen und Forschungsfragen aus den Bereichen Risiko- und Notfallmanagement. Dazu kommen verschiedene methodische Ansätze aus den Bereichen Szenarioanalyse, Indikatorensysteme und multikriterielle Entscheidungsanalyse (MCDA) zum Einsatz. Das IIP war (oder ist) unter anderem involviert in die EU-Forschungsprojekte: EVATECH („Information Requirements and Countermeasure Evaluation Techniques in Nuclear Emergency Management“), EURANOS („European approach to nuclear and radiological emergency management and rehabilitation strategies“), DIADEM („Distributed information acquisition and decision-making for environmental management”) und WEATHER („Weather Extremes: Assessment of impacts on Transport Systems and Hazards for European Regions”). Das IIP ist außerdem innerhalb des interdisziplinären Forschungszentrums „Center for Disaster Management and Risk Reduction Technology“ (CEDIM) in ein umfassendes nationales sowie internationales Netzwerk für Risiko- und Krisenmanagement eingebunden. CEDIM ist eine interdisziplinäre Forschungseinrichtung des Helmholtz-Zentrums Potsdam Deutsches Geoforschungszentrum (GFZ) und des KIT im Bereich des Katastrophenmanagements. Es wurde eingerichtet, um natürliche und anthropogene Risiken besser zu verstehen, früher zu erkennen und besser bewältigen zu können. Forschungsschwerpunkte des IIP im Bereich Risikomanagement sind, unter anderem, Entscheidungsunterstützung im Risiko- und Notfallmanagement, Risikoanalysen und Risikoabschätzungen für kritische Infrastrukturen, Management von komplexen und dynamischen Systemen, Umgang mit Komplexität und Sicherheit und Beurteilung und Bewertung von Risikomanagementstrategien.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Karlsruher Institut für Technologie (KIT)
Institut für Kern- und Energietechnik (IKET)
Wolfgang Raskob
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen
Telefon: +49 721 608 22480
Email: Wolfgang.Raskob@kit.edu

Schwerpunkt der Arbeiten des Institut für Kern-und Energietechnik (IKET) am Karlsruher Institut für Technologie (KIT) waren Forschungsaufträge hinsichtlich des Entscheidungshilfesystems RODOS (Real-time On-line DecisiOn Support system) zur Unterstützung des Katastrophenstabes bei einem radiologischen oder kerntechnischen Notfall. Das Entscheidungshilfesystem RODOS wurde im Rahmen des von der EU geförderten Projektes EURANOS von IKET federführend in Zusammenarbeit mit 17 Katastrophenschutzbehörden und 32 Forschungseinrichtungen entwickelt. Seit 2010 entwickelt und forscht das IKET auch an Methoden und Werkzeugen für die Entscheidungsunterstützung in der Notfallvorsorge. Während des BMBF-Projekts Security2People und im Rahmen von CEDIM (Centre of Disaster management and Risk Reduction) forscht das IKET an einem integrierten System zur strategischen Entscheidungsunterstützung bei Großschadenslagen. Hierzu werden verschiedenste Methoden und Tools wie z. B. Wissensdatenbanken, selbstlernende Systeme, Multikriterielle Entscheidungsanalyse (MCDA) und Kennzahlensimulation genutzt, die es ermöglichen sollen, schnell und transparent Entscheidungen vorzubereiten und zu bewerten.

AIRBUS Defence & Space
Institut für Kern- und Energietechnik (IKET)
Dr. Holger Bracker
Landshuter Straße 26
85716 Unterschleißheim
Telefon: +49 89 3179 3886
Email: Holger.Bracker@cassidian.com

Airbus Defence and Space ist die Sparte für zivile und militärische Sicherheit der Airbus Group. Airbus Defence and Space deckt dabei alle Bereiche der Sicherheit ab:

- Innere Sicherheit: Schutz von Menschen, Infrastruktur, kritischen Standorten und Großveranstaltungen.
- Nationale Sicherheit und Internationale Kooperation: Management von Krisen und Notfällen, nationales und regionales Sicherheitszentrum
- Grenzsicherung: Überwachung von Land- und Seegrenzen, Kontrolle von Personen und Waren an Grenzübergängen.

Die Produkte, Systeme und Lösungen von Airbus Defence and Space im Bereich Notfallschutz und Gefahrenabwehr reichen von vorbereitenden Maßnahmen wie Risikobewertung, Simulation, Design, Training von Spezialkräften, über Lagebildüberwachung bis hin zur Steuerung und Evaluierung von Krisenfällen. Airbus Defence and Space bietet dabei komplette C4I-Systeme, Softwarelösungen und Applikationen für alle Prozesse im Notfall- und Katastrophenschutzmanagement an. Diese ermöglichen es den Sicherheitsbehörden, schneller zu handeln, effektiver zu kommunizieren und besser miteinander zu kooperieren.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

1.5.2 Assoziierte Partner

Tabelle 3: Assoziierte Partner

DB Mobility Networks Logistics	**Deutsche Bahn AG** DB Lagezentrum Rüdiger Czech Köthener Str. 4 10963 Berlin Telefon: +49 30 297 69304 Email: Ruediger.Czech@deutschebahn.com
Die Deutsche Bahn AG gehört zu den weltweit führenden Mobilitäts- und Logistikunternehmen und betreibt in über 130 Ländern 2.000 Niederlassungen. Rund 300.000 Mitarbeiter, davon ca. 194.000 in Deutschland, setzen sich täglich dafür ein, Mobilität und Logistik für die Kunden sicherzustellen und die dazugehörigen Verkehrsnetze auf der Schiene, im Landverkehr sowie in der See- und Luftfracht effizient zu steuern und zu betreiben. Im Geschäftsjahr 2012 betrug der bereinigte Umsatz rund 39,3 Milliarden Euro. Kern des Unternehmens ist die Eisenbahn in Deutschland mit täglich rund 5,6 Millionen Kunden im Personenverkehr und rund 230 Millionen Tonnen auf der Schiene beförderter Güter jährlich. In dem mehr als 33.000 km langen Schienennetz in Deutschland werden 5.645 Personenbahnhöfe betrieben. Darüber hinaus sind in Deutschland täglich rund zwei Millionen Kunden mit den Bussen der DB unterwegs. Im Rahmen der Strategie „DB2020“ soll der Umsatz der DB bis 2020 auf 70 Milliarden Euro gesteigert werden. Um nachhaltig erfolgreich zu sein, setzt die DB auf zufriedene Kunden, eine exzellente Qualität, qualifizierte und hoch motivierte Mitarbeiter sowie umweltschonende Produkte. Mit der Strategie „DB2020“ möchte die DB profitabler Marktführer werden, in Deutschland zu den zehn Top-Arbeitgebern gehören und in Sachen Umwelt absoluter Vorreiter sein. Ferner sind die Maßnahmen der unternehmerischen Sicherheitsvorsorge des DB-Konzerns daher darauf ausgerichtet, Möglichkeiten zu suchen und Festlegungen zu treffen, den öffentlichen Personenverkehr bei gleichbleibenden Angebotsmöglichkeiten sowie die Lieferketten (Güterverkehr/Logistik) so sicher wie möglich zu machen.	
KVB Kölner Verkehrs-Betriebe AG	**Kölner Verkehrs-Betrieb AG** Detlef Frisenhahn Scheidtweilerstr. 38 50933 Köln Telefon: +49 221 547 1301 Email: Detlef.Friesenhahn@kvb-koeln.de
Die Kölner Verkehrs-Betriebe AG (KVB) ist der Mobilitätsdienstleister Nummer 1 in Köln und das fünftgrößte Unternehmen des Öffentlichen Personennahverkehrs in Deutschland. Mit elf Stadtbahn- und 50 Bus-Linien verbindet die KVB fast alle Ziele in Köln und seinen direkten Nachbargemeinden. Über 275 Millionen Fahrgäste nutzen jährlich die Angebote der KVB, durchschnittlich 208 Mal im Jahr steigen jede Kölnerinnen und jeder Kölner ein. Seit nunmehr sechs Jahren in Folge erreicht das Unternehmen jährlich einen neuen Fahrgastrekord. Dieses Fahrgastaufkommen bewältigt die KVB mit 382 Bahnen und über 300 Bussen. Auf den Betriebshöfen und in den Werkstätten in Braunsfeld, Merheim, Riehl und	

Wesseling sowie in der Hauptwerkstatt in Weidenpesch und im Fahrdienst sind rund 3.200 Mitarbeiterinnen und Mitarbeiter beschäftigt. Sie sorgen dafür, dass Busse und Bahnen den Fahrgästen tagtäglich zur Verfügung stehen, Kunden beraten werden und die Infrastruktur unterhalten wird.

Münchener Verkehrsgesellschaft mbH
Rainer Cohrs
Emmy-Noether-Str. 2
80287 München
Telefon: +49 89 2191 2539
Email: Cohrs.Rainer@swm.de

München ist eine der attraktivsten Städte Deutschlands. Für Touristen aus aller Welt, aber auch als Wirtschaftsstandort. Ein Grund für die Attraktivität der bayerischen Landeshauptstadt ist das gut ausgebaute und funktionierende Öffentliche Personennahverkehrssystem, in dem die Leistungen der Münchner Verkehrsgesellschaft (MVG), der privaten Busunternehmen, die als Kooperationspartner der MVG im Stadtgebiet fahren, der S-Bahn München und der Regionalbusunternehmen ineinander greifen. Die Münchner Verkehrsgesellschaft (MVG) als Betreiberin von U-Bahn, Bus und Tram in München spielte und spielt in dieser Erfolgsstory eine wichtige Rolle. Moderne, umweltfreundliche und behindertengerechte Fahrzeuge, gut ausgebildetes Personal sowie umfangreiche Info- und Serviceleistungen sind ihre Stärken. Insgesamt 572 U-Bahnwagen, 106 Straßenbahnzüge und 246 Busse aus dem Fuhrpark der MVG Muttergesellschaft Stadtwerke München GmbH (SWM), sind für das zweitgrößte kommunale Verkehrsunternehmen in Deutschland im Einsatz. Dazu kommen 189 Busse der privaten Partnerunternehmen. In München hat man nur wenige Minuten bis zur MVG, denn auf einem Streckennetz von über 600 Kilometern befindet sich beinahe jeder Haushalt innerhalb eines 400 Meter-Radius zu einer U-Bahn-, Bus- oder Trambahn-Haltestelle! Die MVG als starker Partner im Münchner Verkehrs- und Tarifverbund (MVV) ist mit München bis in den letzten Winkel verwachsen. Ohne sie und ihre täglich über 1,4 Millionen Fahrgäste wäre das berühmte Flair an der Isar nicht das, was es ist. Und das soll so bleiben.

Bundespolizeipräsidium
Rocco Stein
Heinrich-Mann-Allee 103
14473 Potsdam
Telefon: +49 33197997 2301
Email: bpolp.referat.23@polizei.bund.de

Die Bundespolizei untersteht dem Bundesministerium des Innern. Im Sicherheitssystem der Bundesrepublik Deutschland nimmt sie umfangreiche und vielfältige polizeiliche Aufgaben wahr. Hierzu gehört im Rahmen der bahnpolizeilichen Aufgabenwahrnehmung gemäß § 3 Bundespolizeigesetz auch die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes, die den Benutzern, den Anlagen oder dem Betrieb der Bahn drohen. Das Gebiet der Bahnanlagen der Eisenbahnen des Bundes mit mehr als 5.500 Personenbahnhöfen und

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

über 33.000 Streckenkilometern stellt für die Bundespolizei einen weitläufig dimensionierten Einsatzraum dar, der als Bestandteil der Kritischen Infrastruktur in Deutschland zu schützen ist. Das Verkehrsmittel "Eisenbahn" wird als Teil der Daseinsvorsorge täglich von über 6 Millionen Reisenden in Deutschland genutzt. Die Gewährleistung der Bahnsicherheit als eine der Schwerpunktaufgaben der Bundespolizei wird dabei 24 Stunden an 7 Tagen in der Woche durch rund 5.100 Polizeivollzugsbeamte der Bundespolizei sichergestellt. Das Zielspektrum bahnpolizeilicher Aufgabenwahrnehmung umfasst gleichermaßen den Schutz der kritischen Infrastruktur Bahn vor nachhaltigen Störungen, insbesondere Anschlagsgefahren, die Abwehr konkreter Gefahren bei unterschiedlichen Einsatzlagen, die Stärkung des Sicherheitsgefühls der Reisenden durch präventiv-polizeiliche, bürgerorientierte Aktivitäten sowie die Kriminalitätsbekämpfung. Des Weiteren ist die Bundespolizei u.a. auch für die Verfolgung von den Straftaten zuständig, die auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes begangen werden und gegen die Sicherheit eines Benutzers, der Anlagen oder des Betriebs der Bahn gerichtet sind.

RheinlandPfalz
HOCHSCHULE DER POLIZEI
RHEINLAND-PFALZ
LANDESPOLIZEISCHULE

Hochschule der Polizei Rheinland-Pfalz
Wolfgang Willems
Postfach 11 11
55482 Hahn-Flughafen
Telefon: +49 6543 985 264
Email: Wolfgang.Willems@polizei.rlp.de

Die Hochschule der Polizei obliegt die Organisation und Durchführung des Bachelorstudiengangs Polizeidienst für die rheinland-pfälzischen Polizeikommissar-Anwärterinnen und -Anwärter sowie einzelner Veranstaltungen des Masterstudiengangs Öffentliche Verwaltung - Polizeimanagement. Das interdisziplinäre Team in der Lehre aus erfahrenen Polizei- und Verwaltungsbeamtinnen und -beamten, Experten aus unterschiedlichen akademischen Disziplinen, wie z.B. Psychologen, Soziologen, Theologen, Juristen sowie Sportlehrern und Fremdsprachendozenten haben sich zum Ziel gesetzt, junge Berufsanfänger in einem akkreditierten Bachelorstudiengang und angehende Führungskräften in einem anerkannten Masterstudiengang auf die hohen Anforderungen innerhalb der rheinland-pfälzischen Polizei vorzubereiten. Zurzeit studieren an der Hochschule der Polizei in sechs Bachelorstudiengängen und einem Masterstudiengang über 1.200 begeisterungsfähige Studierende. Jährlich besuchen bis zu 12.000 interessierte Polizeibeamtinnen und -beamte sowie sonstige Teilnehmer Fortbildungsseminare und -trainings der Landespolizeischule.

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

1.5.3 Sonstige Partner

Die Technische Hochschule Köln hatte neben den Verbundpartnern und assoziierten Partnern regelmäßigen Austausch, besonders im Zusammenhang der durchgeführten Realübung “Terroristischer Anschlag im ÖPV”, mit den folgenden Institutionen:

Tabelle 4: Sonstige Partner

Stadt Köln	**Stadt Köln** Amt für Feuerschutz, Rettungsdienst und Bevölkerungsschutz Dr. Jörg Schmidt Scheibenstraße 13 50737 Köln Telefon: +49 0221 97 48 94 00 Email: Joerg.Schmidt@stadt-koeln.de **Stadt Köln** Ordnungs- und Verkehrsdienst Jörg Breetzmann Willy-Brandt-Platz 3 50679 Köln Telefon: +49 221 221 27657 Email: Joerg.Breetzmann@stadt-koeln.de
POLIZEI Nordrhein-Westfalen Köln	**Polizeipräsidium Köln** Direktion Besondere Aufgaben Stefan Werner Walter-Pauli-Ring 2-6 51103 Köln Telefon: +49 221 229 3107 Email: Stefan01.Werner@polizei.nrw.de
ceia GmbH	**CEIA GmbH** Simon Ernst Rohrbergstr. 23 65343 Eltville am Rhein Telefon: +49 6123 790860 Email: Simon.Ernst@ceia.net
FLIR	**FLIR Systems GmbH** Samir Al-Ghazal Berner Straße 81 60437 Frankfurt am Main Telefon: +49 212 2220 90 Email: Samir.Al-Ghazal@flir.com
VIDEMO Intelligente Videoanalyse	**Videmo Intelligente Videoanalyse GmbH & Co. KG** Dr. Keni Bernardin Haid-und-Neu-Str. 7 76131 Karlsruhe Telefon: +49 721 62710135 Email: Bernardin@videmo.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

2 Zuwendungsverwendung

Die bewilligten Mittel wurden gemäß dem Zuwendungsbescheid des Bundesministeriums für Bildung und Forschung vom 26.10.2012 für die Technische Hochschule Köln verwendet. Während der Projektlaufzeit gab es einige Mittelumwidmungen sowie eine dreimonatige zuwendungsneutrale Projektlaufzeitverlängerung (von 01.11.2015 bis 31.01.2016), die vorher mit dem Projektträger VDI abgestimmt wurden.

Eine detaillierte Aufstellung der Zuwendungsverwendung wurde durch die Drittmittelabteilung der Technischen Hochschule Köln im Rahmen des Schlussverwendungsnachweises aufbereitet und an den Projektträger VDI geschickt. Daher wird an dieser Stelle auf eine weitere Darstellung verzichtet.

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

3 Eingehende Darstellung des Projektverlaufes

In diesem Kapitel erfolgt eine eingehende Darstellung der gesamten Forschungsergebnisse und durchgeführten Aktivitäten der Technischen Hochschule Köln. Dabei wird zunächst auf eine detaillierte Ausführung der Teilergebnisse eingegangen, bevor das Gesamtergebnis der Technischen Hochschule Köln erläutert und ein Forschungsfazit gezogen wird.

3.1 Detaillierte Darstellung der Teilergebnisse

Im Rahmen der detaillierten Darstellung der Teilergebnisse werden zunächst die durchzuführenden Aufgaben der Technischen Hochschule Köln aus der Teilvorhabenbeschreibung aufgeführt, um anschließend in den grauen Kästen die tatsächlich durchgeführten Aktivitäten im Rahmen des Verbundforschungsprojekts RiKoV darzulegen. Aufgrund der Übernahme aus der Teilvorhabenbeschreibung erfolgt bei der Aufgabenbeschreibung die Verwendung des Originalwortlauts „Fachhochschule Köln“ oder „FHK“.

3.1.1 AP 1 – Problemanalyse

- A1.1 Auswertung historischer Anschläge auf den ÖPV
  Identifizierung von Terroranschlägen gegen ÖPV-Systeme und Auswertung nach folgenden Gesichtspunkten: Täterprofil, Angriffsziel und –mittel, verursachte Sach- und Personenschäden, so weit möglich auch Kosten der Primär- und Folgeschäden

  – FHK führt nach Maßgabe des PL von AP1 zusammen mit anderen AP1-Partnern eine Literaturrecherche zu historischen ÖPV-Terroranschläge durch, wertet seine Ergebnisse der Literaturrecherche nach einem fest vorgegebenen Schema aus, leitet daraus „Lessons learned“ ab und greift dabei auf Erfahrungen zurück, die im Rahmen des EU-Projektes NEAT gewonnen wurden.

Die TH Köln hat im AP1 zusammen mit den anderen AP1-Partnern unter der Koordination des PL eine Literaturrecherche zu historischen terroristischen Anschlägen durchgeführt. Bei der internationalen Literaturrecherche wurde der Fokus insbesondere auf den öffentlichen Personenverkehr gelegt. Auf Basis der ermittelten historischen Anschläge konnten “Lessons Learned” und Anforderungen an den RiKoV-Methodenverbund abgeleitet werden. Auf Basis der Ergebnisse konnten Vignetten und Szenarien zur Beschreibung der potentiellen ÖPV-Bedrohungssituation erstellt werden.

Die TH Köln hat den Bericht L 1.1 Auswertung historischer Anschläge, für den die UniBW verantwortlich war, begutachtet.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- A1.2 Generisches ÖPV-System

  Das Mengengerüst eines generischen ÖPV-Systems wird aus real existierenden Verkehrssystemen abgeleitet. Es enthält alle aus Sicht eines Terroristen lohnende Angriffsziele, ohne auf Schwachstellen einer bestimmten ÖPV-Infrastruktur einzugehen.

  – FHK hilft der UniBw bei der Durchführung einer Datenrecherche zum Aufbau eines generischen ÖPV-Mengengerüsts , analysiert und vergleicht dazu die Mengengerüste verschiedener ÖPV-Systeme in deutschen Großstädten, um daraus ein realistisches, aber generisches ÖPV-System abzuleiten. Aus den dazugehörigen statistischen Angaben des Mengengerüsts werden Anzahl, Lage und Ausstattung potentieller Angriffsziele des generischen ÖPV-Systems abgeleitet[7].

Die TH Köln hat die UniBw bei der Datenrecherche zum Aufbau eines generischen ÖPV-Systems in AP1.2 unterstützt. Weiterhin wurden durch die TH Köln kritische Teilprozesse in schienengebundenen ÖPV-Systemen definiert und beschrieben. Aus der Definition der kritischen Prozesse konnten im Anschluss Gefahrenbereiche entwickelt werden. Darüber hinaus wurden Bestandteile des generischen ÖPV-Systems durch die TH Köln in eine bereitgestellte Datenbank überführt.

- A1.3 Teilszenarien/Vignetten

  Erfassung und Beschreibung von Motivation und Absicht potentieller Terroristen sowie der heute und in absehbarer Zukunft zur Verfügung stehenden Angriffsmittel. Zu jeder Kombination „Angriffsmittel - Angriffsziel wird ein spezifisches Teilszenario – eine „Vignette“ – skizziert, das Motivation des Angreifers, seinen Angriffsplan sowie die angestrebten Konsequenzen (Primär- und Folgeschäden, Verletzte, Tote) des Angriffs unter Berücksichtigung der vom Angreifer angenommenen Abwehrmaßnahmen beschreibt.

  – Aus dem Ergebnis des Paketes A1.2 werden die lohnenden Angriffsziele für Terroristen erfasst. Dabei werden Ergebnisse von Untersuchungen anderer Partner zu Motivation und Erfolgskriterien sowie Angriffsmitteln von Terroristen als Grundlage einbezogen. Die Ergebnisse werden innerhalb eines Experten-Workshops zusammengetragen, besprochen und bewertet. Die FHK wird gemeinsam mit den anderen Verbundpartnern innerhalb des Workshops Teilszenarien (Vignetten) aus den möglichen Kombinationen von Angriffszielen und Angriffsmitteln definieren. Diese Vignetten werden in dem Prozess auf Plausibilität überprüft. Die Vignetten werden anschließend nach Gefahrenbereichen kategorisiert. Die FHK organisiert und moderiert den Experten-Workshop „ÖPV-Vignetten“.

  – FHK führt den Workshop „ÖPV-Vignetten“ mit externen Experten durch.

[7] z. B. Länge der Gleiskörper über und unter der Erde, Anzahl Bahnhöfe über und unter der Erde, Anzahl der Strecken über und unter der Erde, Anzahl Waggons, Busse, Straßenbahnen, Anzahl Beschäftigte und Passagiere pro Jahr etc.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

In AP1.3 wurden von den RiKoV-Partner Angriffsziele für Terroristen im ÖPV erfasst und in Form von Vignetten beschrieben. Die TH Köln hat in diesem AP den ersten RiKoV-Workshop "ÖPV-Vignetten" konzipiert, vorbereitet und durchgeführt. Ebenfalls wurde der Workshop durch die TH Köln ausgewertet und im Bericht "Dokumentation Workshop: ÖPV-Vignetten" verschriftlicht. Der Workshop fand vom 23.04 bis zum 25.04.2013 in den Räumlichkeiten der TH Köln statt. Unter der Einbindung von Experten der VDV AG Security und den assoziierten Partnern des Projekts RiKoV wurden die entwickelten Vignetten auf ihre Plausibilität geprüft und die Anwendbarkeit für den weitere Verlauf des Projektes festgelegt. Neben initiativen Vorträgen zur aktuellen Bedrohungslage in Deutschland und den geplanten Methoden des Projekts RiKoV stand insbesondere die Erarbeitung von plausiblen Vignetten in kleinen Expertengruppen im Vordergrund. Die Gestaltung des Workshops ermöglichte einen intensiven Austausch mit den Experten und eine Anpassung des Zieles des Forschungsprojektes RiKoV an die aktuellen Bedürfnisse der Sicherheitsexperten der Betreiber eines ÖPV-Systems.

Die TH Köln hat den Bericht L1.3 "Vignetten" des KIT-IKET gelesen und begutachtet.

- A1.4 Schutzmaßnahmen (FHK verantwortlich)
  Die Vignetten von A 1.3 dienen als Entscheidungsgrundlage für die Identifikation von möglichen Gegenmaßnahmen. Dazu werden Schwachstellen der Angriffsziele (siehe A 1.2) nach potenziellen Gefahrenbereichen (z.B. Prozesse, IT, Technik, Ressourcen, Gebäude) erfasst. Da innovative Sicherheitslösungen nur dann erfolgreich sein können, wenn ihr Nutzen und Mehrwert von Anwendern und Öffentlichkeit anerkannt werden, werden das Für und Wider der Sicherheitsmaßnahmen in den gesellschaftlichen Dimensionen der zivilen Sicherheitsforschung erfasst und analysiert.

  - Bezogen auf die Gefahrenbereiche (aus A 1.3) werden Schutzziele entwickelt, welche die Grundlage für alle Sicherheitsmaßnahmen bilden. Aufgrund der Schutzziele kann jede Maßnahme auf ihre Effektivität und Effizienz überprüft werden.

    Für jede Vignette werden spezifische Sicherheitsmaßnahmen entwickelt und definiert, um die aufgestellten Schutzziele zu erreichen. Dabei wird systematisch zwischen technischen und organisatorischen sowie präventiven und reaktiven Maßnahmen unterschieden. Die Auswirkungen der dargestellten Sicherheitsmaßnahmen werden analysiert und gemeinsam mit dem Unterauftragnehmer KVB auf die Akzeptanz von Kunden, Mitarbeitern und indirekt Beteiligten geprüft. Hierzu wird eine repräsentative Befragung der Beteiligten entwickelt und durchgeführt.

  - FHK Abschlusslieferung: Bericht „Analyse potentieller Sicherheitsmaßnahmen" 31.10.2013

Im AP1.4 hat die TH Köln zunächst aus den in AP1.2 definierten Gefahrenbereichen Schutzziele entwickelt. Auf Basis dieser Grundlagen wurden potentielle Sicherheitsmaßnahmen zur Verwendung im ÖPV identifiziert. Die Ermittlung der potentiellen Sicherheitsmaßnahmen fand auf Basis einer internationalen Literaturrecherche statt. Die Recherche orientierte sich dabei regelmäßig an derzeit vorhandenen und neuartigen Sicherheitsmaßnahmen für den internationalen Luftverkehr. Erfasst wurden technische, bauliche, organisatorische und personelle Sicherheitsmaßnahmen, welche überwiegend eine präventive Wirkung haben. Jedoch wurden auch Sicherheitsmaßnahmen mit einer reaktiven Wirkung ausgeführt. Die identifizierten Sicherheitsmaßnahmen wurden analysiert und mit spezifischen Details beschrieben. Die Dokumentation erfolgte in der Datenbank Sicherheitsmaßnahmen und dem Bericht L1.4 “Analyse potentieller Sicherheitsmaßnahmen”. Dieser Bericht wurde durch die Projektpartner begutachtet und intern zur Verfügung gestellt.

Darüber hinaus hat die TH Köln in Zusammenarbeit mit einem Unterauftragnehmer und der KVB eine Befragung von fast 1.000 KVB-Kunden durchgeführt. Ziel der Befragung war es, die Akzeptanz von Sicherheitsmaßnahmen und deren indirekte Wirkung zu erfassen. Dazu wurde zunächst eine Onlinebefragung von KVB-Stammkunden durchgeführt. Anschließend erfolgte eine Feldbefragung in unterschiedlichen Haltestellen und zu unterschiedlichen Tageszeit von zufälligen KVB-Fahrgästen. Im letzten Schritt wurden die Ergebnisse der beiden Befragungen ausgewertet, verglichen und wiederrum mit KVB-Stammkunden diskutiert und besprochen.

3.1.2 AP 2 – Operationsanalyse

- A2.1 Prozessmodellierung

  Unter Berücksichtigung der in den Vignetten von A1.3 erarbeiteten Angriffspläne werden Operationspläne zur Abwehr der geplanten Anschläge entworfen und die Prozesse zur Durchführung der Operationspläne von Angreifer und Verteidiger analysiert und modelliert. Hierbei werden bestehende Modellierungsstandards[8] *als Vorgehensmodell verwendet. Das Verhalten der Akteure zur Durchführung ihrer Operationspläne wird mit Hilfe von Regeln beschrieben.*

  - Die in A1.4 entwickelten Sicherheitsmaßnahmen zur Abwehr geplanter Anschläge werden zu Strategien erweitert und in Operationspläne umgesetzt. Die zugrunde liegenden Prozesse werden mit Hilfe von bestehenden Standards modelliert. Aus den entstehenden Modellen zur Abwehr werden allgemeine Regeln entwickelt und in ein Regelwerk umgesetzt. Die erfasste Prozessmodellierung wird mit dem UA KVB auf Plausibilität und anschließend auf Umsetzbarkeit überprüft.
  - FHK Abschlusslieferung: Bericht „Prozessmodellierung der Operationspläne“

[8] z.B. das NATO Architecture Framework

Die TH Köln hat auf Basis der in AP1.3 beschriebenen Vignetten und den in AP1.4 erfassten Sicherheitsmaßnahmen ein generisches Prozessmodell für einen terroristischen Angriff im ÖPV erarbeitet. Dieses Modell bildete sowohl die Bewegung des Täters durch das ÖPV-System als auch die Reaktion der Sicherheitsmaßnahmen ab. Somit konnten einzelne Operationspläne erfasst und dargestellt werden. Das Prozessmodell diente der generischen Beschreibung des terroristischen Angriffs (Täterweg durch das ÖPV-System) und der Beschreibung der Auswirkungen beim Wirken einer Sicherheitsmaßnahme (Reaktion der Sicherheitsmaßnahme). Beide Teile wurden in der Methode zur Bestimmung der Wirkung von Sicherheitsmaßnahmen verwendet, um die Prozessstellen zu identifizieren, an denen eine Sicherheitsmaßnahme wirken kann. In enger Absprache mit den beteiligten Experten der KVB wurde das entwickelte Prozessmodell auf Plausibilität geprüft. Das Prozessmodell und eine ausführliche Beschreibung dazu sind im Bericht L2.1 „Prozessmodellierung der Operationspläne“ dokumentiert, durch die Projektpartner begutachte und diesen zur Verfügung gestellt.

- A2.2 Szenarien

  Die in AP1 erarbeiteten Vignetten werden unter Berücksichtigung der Abwehrpläne zu Szenarien für operationsanalytische Untersuchungen ausgebaut und in standardisierter Form in einer Szenario-Datenbank abgelegt. Jedes Szenario wird als XML-File bereitgestellt.

  – Unter Berücksichtigung der in A2.1 erarbeiteten Operationspläne für Angreifer und Verteidiger werden die in AP1 erarbeiteten Vignetten zu Szenarien für operationsanalytische Untersuchungen ausgebaut. Dabei ist zu beachten, dass ein Szenario mehr ist als nur ein Drehbuch. Nach Hermann Kahn ist unter Szenario eine hypothetische Sequenz von Ereignissen zu verstehen mit dem Zweck, die Aufmerksamkeit auf Kausalzusammenhänge und Entscheidungspunkte zu richten. Für RIKOV heißt das:
    - Das Szenario beschreibt sowohl die Testumgebung zur Bewertung von Sicherheitsmaßnahmen als auch den Einfluss der Ereignisse auf die Zielobjekte des ÖPV-Systems, die durch die Sicherheitsmaßnahmen zu schützen sind.
  - Die Entwicklung eines problemadäquaten Demonstrationsszenarios setzt voraus, dass Zweck der Demonstration sowie die Ziele der anschließenden Auswertung bekannt sind.
  - Zweck der Demonstration ist, die Wirksamkeit der ausgewählten Sicherheitsmaßnahmen aufzuzeigen.
  – Die in AP1 entwickelten Vignetten werden unter Berücksichtigung der Abwehrpläne zu Szenarien für operationsanalytische Untersuchungen ausgebaut und in standardisierter Form in einer Szenario-Datenbank[9] abgelegt. Jedes Szenario wird als XML-File bereitgestellt.
  – Die FHK unterstützte die Verbundpartner beim Aufbau der beschriebenen Szenario-Datenbank, in dem der Umwandlungsprozess der Abwehrpläne zu standardisierten Datensätzen.

[9] Ein Scenario Support Tool mit einer standardisierten Scenario-Datenbank wurde im EU-Projekt INSPIRE entwickelt.

Die im AP1.3 entwickelten und im 1. RiKoV-Workshop auf Plausibilität geprüften Vignetten wurden in diesem AP zu komplexe Szenarien ergänzt. Das generische Prozessmodell aus AP2.1 diente dazu als Vorlage. Die Szenarien wurden mit ihrer Umgebung beschrieben. Die TH Köln unterstützte die anderen AP-Partner bei der Beschreibung der Szenarien und der Anwendung des Prozessmodells.

- A2.3 Analyse der Schäden

  Für jede Vignette werden die Auswirkungen der Anschläge hinsichtlich Primär- und Folgeschäden analysiert. Zur Schadensanalyse gehören: die Analyse der direkten Wirkung auf Personen, Einrichtungen und Betrieb; die Analyse der Folgeeffekte; die Analyse der Auswirkungen auf weiche Faktoren wie Medien, Geschäftsbeziehungen, öffentliche Meinung, Nachfrageverhalten der Kunden und insbesondere der psychologischen Wirkung von Terroranschlägen.

  – Zur Vorbereitung einer strukturierten Risikobetrachtung werden die Primär- und Folgeschäden eines Angriffs analysiert. Hierfür stellt die FHK gemeinsam mit der KVB eine Liste mit möglichen Schäden für ÖPV-Systeme auf. Hierfür dient das generische ÖPV-System als Grundlage. Davon ausgehend werden Konsequenzen von Schäden und der daraus resultierenden Folgen für Personen, Rettungskräfte, Ressourcen und Infrastruktur erfasst. Anschließend werden die einzelnen Punkte der Liste mit den Vignetten aus AP1 verknüpft.
  – Im Rahmen des AP2 wird die FHK eine Planspiel-Übung durchführen. Hierbei werden die theoretischen Ergebnisse und erfassten Szenarien mit potentiellen Beteiligten durchgespielt. Mithilfe eines Planspiels lassen sich kostengünstig und in kurzer Zeit Optionen und Abläufe auf Plausibilität und Wirkungen durchspielen. Die Konzeption hierzu wird durch die FHK in Abstimmung mit den anderen Partnern erarbeitet. Aufgrund der hohen Belastung in der Umsetzung und der technischen Gestaltung der Übungsumgebung soll diese Aufgabe an einen Unterauftragnehmer vergeben werden.

Basierend auf dem generischen ÖPV-System hat die TH Köln zusammen mit der KVB bei der Analyse möglicher Schäden auf ein ÖPV-System unterstützt und somit die Ermittlung von Primär-, Sekundärschäden und Schäden auf weiche Faktoren ermöglicht.

Weiterhin wurde im Rahmen des AP2.3 durch die TH Köln ein Planspiel am 25.11.2014 durchgeführt. Zu diesem Planspiel waren verschiedene Experten aus den Reihen der ÖPV-Betreiber in die Räumlichkeiten der KVB eingeladen. An einer realistischen Nachbildung einer neuen Haltestelle der KVB (Planspielplatte) wurde das entwickelte Prozessmodell, die Methode zur Bestimmung der Vulnerabilität inklusive der Methode zur Bestimmung der Wirkung von Sicherheitsmaßnahmen diskutiert. Ziel des Planspiels war die Validierung der Methoden zur Bestimmung der Vulnerabilität und der Wirkung von Sicherheitsmaßnahmen. Dazu wurde durch die TH Köln in einem Unterauftrag eine realistische Test-Umgebung entwickelt und gebaut. Weiterhin hat die TH Köln die Methode zur Validierung der Methoden in einem Planspiel entwickelt. Die Ergebnisse dieser Planspielübung sind in der „Dokumentation der Planspielübung“ festgehalten und Teil des Berichts L7.2 „Integration und Test“.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

3.1.3 AP 4 – Szenariobasierte Risikobewertung

- A4.1 Methode zur Bestimmung der Vulnerabilität
  - Input: N x M Vignetten von A1.3 (N Angriffsvarianten und M Angriffsziele)
  - Ausgangspunkt der Überlegungen sind die Vignetten von AP1, die den Rahmen für eine Vulnerabilitätsmatrix aufspannen, deren Werte zu bestimmen sind. Zu diesem Zweck werden Vorgehensregeln zur Werteermittlung erarbeitet, die den Nutzer in die Lage versetzen, die Werte der Vulnerabilitätsmatrix zu bestimmen.
  - Output: ausgefüllte N x M Vulnerabilitätsmatrix
  - Die Vulnerabilität einzelner ÖPV-Teile entspricht der relativen Möglichkeit, dass ein Angriff auf ein bestimmtes Ziel erfolgreich ist. Zur Wertebestimmung wird die FHK Regeln zur Bemessung und zum Vorgehen ermitteln, um die Möglichkeit eines Angriffes für definierte Systemteile bestimmen zu können. Hierbei werden detaillierte Angriffswege und technische sowie organisatorische Abwehrmaßnahmen in ein zu bestimmendes Verhältnis gesetzt.
  - Für die vorhandenen Vignetten wird das Regelwerk exemplarisch angewendet und eine Vulnerabilitätsmatrix erstellt.
  - Die Ergebnisse werden während des ganzen Prozesses mit der KVB abgestimmt und auf Plausibilität überprüft.

Die TH Köln hat im AP4.1 eine Methode zur Bestimmung der Vulnerabilität verschiedener Elemente eines ÖPV-Systems entwickelt. Diese Methode basierte aus zwei Schritten. Zunächst wurden szenariounabhängige Eigenschaften des Elementes in Gefährdungskategorien ermittelt. Dazu erfolgte eine systematische Erfassung von beeinflussenden Parametern zur Ermittlung der Bedrohung. Die Beschreibung dieses Schrittes erfolgte in dem internen Projektbetrag zum AP4.1 „Methode zur Bestimmung der Vulnerabilität eines schienengebundenen ÖPV-Systems“. Anschließend erfolgte die Verrechnung mit der szenarioabhängigen Wirkung von Sicherheitsmaßnahmen. Diese wurde in AP5.2 näher erläutert. Mit dieser Möglichkeit konnte die Vulnerabilität der Szenarien eines terroristischen Angriffs auf ein ÖPV-System bestimmt und diese untereinander verglichen werden.

Die in AP2.2 beschriebenen komplexen Szenarien wurden auf Basis des vorhandenen, generischen ÖPV-Systems auf ihrer Vulnerabilität untersucht, qualitativ bewertet und in einer Matrix zusammengefasst (Vulnerabilitätsmatrix). Die Ergebnisse wurden in Zusammenarbeit mit der KVB auf Plausibilität geprüft und dem Planungsverbund zur Verfügung gestellt.

- A4.2 Methode zur Bestimmung der Bedrohung
  - Input: N x M Vignetten von A1.3
  - Analog zur Bestimmung der Vulnerabilitätsmatrix bilden die Vignetten von AP1 sowie die daraus abgeleiteten Szenarien von AP2 den Rahmen für eine Bedrohungsmatrix, deren Werte zu bestimmen sind. Dazu werden ebenfalls Vorgehensregeln zur Werteermittlung erarbeitet, die es erlauben, die Werte der Bedrohungsmatrix zu ermitteln.
  - Output: ausgefüllte N x M Bedrohungsmatrix
  - Die Bedrohung des ÖPV entspricht der Wahrscheinlichkeit für einen terroristischen Angriff. Rein statistisch ist die Bestimmung der Wahrscheinlichkeit in diesem Feld nicht möglich. Die geringe Anzahl an Ereignissen in der Vergangenheit lässt mathematisch keine eindeutige Aussage zu. Die FHK wird Regeln entwickeln, welche die beeinflussenden Parameter zur Ermittlung von Bedrohungswerten in eine Beziehung zu einander setzt und eine Abschätzung der Wahrscheinlichkeit zulässt. Hierfür werden die Parame-

ter systematisch erfasst und definiert. Aus dieser Vorarbeit wird ein Regelwerk aufgestellt, anhand dessen auch zukünftig Bedrohungen abgeschätzt und eingeordnet werden können.
- Für die vorhandenen Vignetten wird das Regelwerk exemplarisch angewendet und eine Bedrohungsmatrix erstellt.
- Die Ergebnisse werden während des ganzen Prozesses mit dem Unterauftragnehmer KVB abgestimmt und auf Plausibilität überprüft.

Die TH Köln unterstützte die anderen AP-Partner bei der Bestimmung der Bedrohung. Die ausgefüllte Bedrohungsmatrix wurde in den weiteren Schritten mit der Vulnerabilitätsmatrix verrechnet.

- A4.3 Methode zur Bestimmung der Konsequenzen eines Anschlags
  - Input: N x M Vignetten von A1.3
  - Anhand historischer Ereignisse und operationsanalytischer Untersuchungen (siehe AP2) werden die Sach- und Personenschäden sowie die Kosten ausgewertet und analog zu den Vignetten klassifiziert. Potentielle Datenlücken werden durch Expertenschätzungen gefüllt. Anhand einheitlicher Regeln werden die Werte (Sach-/Personenschaden, Kosten) in qualitative Werte für den Einheitswert „Konsequenz“ übersetzt.
  - Output: N x M Konsequenzmatrix
  - Die Konsequenzen eines Anschlags entsprechen seinen Folgen. Die in AP 1, AP 2 und AP 3 gewonnenen Erkenntnisse, in Bezug auf Sach-, Personenschäden sowie deren Kosten, werden zusammengeführt und den Vignetten zugeordnet. Datenlücken werden dabei durch qualifizierte Schätzungen geschlossen. Hierbei wird die FHK durch die KVB unterstützt. Die FHK erstellt ein Regelwerk, mit dessen Hilfe die Ergebnisse in einen qualitativen Einheitswert für die Konsequenz übertragen werden können.
  - Für die vorhandenen Vignetten wird das Regelwerk angewendet und eine Konsequenzen Matrix erstellt.
  - Die Ergebnisse werden während des ganzen Prozesses mit der KVB und den anderen UA abgestimmt und auf Plausibilität überprüft.

Die TH Köln unterstützte die anderen AP-Partner bei der Bestimmung der Konsequenzen eines Anschlages. Dabei konnte auf die Ergebnisse des AP2.3 zurückgegriffen werden. Die ausgefüllte Matrix der Schäden wurde in den weiteren Schritten mit der Vulnerabilitätsmatrix und der Bedrohungsmatrix verrechnet.

- A4.4 Risikomatrix
  - Input: N x M Vulnerabilitätsmatrix; N x M Bedrohungsmatrix; N x M Konsequenzmatrix
  - Es werden Aggregationsregeln identifiziert, die das Verhalten eines intelligenten Täters reflektieren und die drei Inputmatrizen zu einer Risikomatrix zusammenführen, die angibt, wie ernsthaft die potentiellen Ziele eines Anschlages innerhalb des ÖPV-Systems gefährdet sind.
  - Output: ausgefüllte Risikomatrix
  - Das Risiko ist eine Funktion aus Vulnerabilität, Bedrohung und Konsequenz. Die drei Regelwerke der vorangegangenen Arbeitspakete werden in diesem Sinne zusammengeführt. Hierfür wird ein eigenes Aggregationsregelwerk entwickelt, mit dem sich das Risiko für eine Vignette abschätzen lässt.
  - Für die vorhandenen Vignetten wird das Regelwerk exemplarisch angewendet und eine Bedrohungsmatrix erstellt.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- Die Ergebnisse werden während des ganzen Prozesses mit der KVB abgestimmt und auf Plausibilität überprüft.

Die TH Köln prüfte die zusammengeführten Matrizen in Zusammenarbeit mit der KVB auf Plausibilität.

- A4.5 Modell „Risikobewertung“
  - Das Risikobewertungsverfahren wird in ein IT-Modell übersetzt.
  - Step 1:
    - Aus den Vignetten werden die Bedrohungsmatrix und die Verwundbarkeitsmatrix mit Hilfe der in A4.1 und A4.2 erarbeiteten Regeln abgeleitet.
    - Unter Berücksichtigung historischer Anschläge werden aus den Vignetten die Personen- und Sachschäden sowie der ökonomische Schaden in Form einer Verlust- und einer Schadensmatrix abgeleitet.
  - Step 2:
    - Die Bedrohungsmatrix und die Verwundbarkeitsmatrix werden unter Berücksichtigung von Verhaltensregeln intelligenter Täter zu einer Wahrscheinlichkeitsmatrix verknüpft.
    - Die Verlustmatrix und die Schadensmatrix werden unter Berücksichtigung der in A4.3 erarbeiteten Verknüpfungsregeln zu einer Konsequenzmatrix zusammengeführt. Die Verknüpfungsregeln sollen die Wirkung der Anschläge auf die öffentliche Meinung widerspiegeln wie z.B. je mehr menschliche Opfer zu beklagen sind, umso schlimmer wird die Wirkung des Anschlages eingeschätzt.
  - Step 3:
    - Die Wahrscheinlichkeitsmatrix und die Konsequenzmatrix werden unter Berücksichtigung der in A4.4 erarbeiteten Verknüpfungsregeln zu einer qualitativen Risikomatrix zusammengeführt. Sie gibt unter Berücksichtigung einer ausgewählten Angriffstaktik das Risiko eines jeden Angriffsziels des ÖPV-Systems an.
    - Verknüpfungsregeln können z.B. sein: hohe Wahrscheinlichkeit und hohe Konsequenz führen zu einem hohen Risiko. Bei sehr unterschiedlichen Werten der Eintrittswahrscheinlichkeit und der Konsequenz entscheiden die Verhaltensregeln eines intelligenten Täters, mit welchem Wert das Risiko zu bewerten ist.

Das Risikobewertungsverfahren wird von den Verbundpartnern in ein IT-Modell übersetzt. Die FHK unterstützt die Partner dabei.

Die TH Köln unterstützte die AP-Partner bei der Erstellung eines Modells zur Risikobewertung und prüfte das erstellte IT-Modell aus Plausibilität unter Berücksichtigung der Endanwenderbedürfnisse

3.1.4 AP 5 – Risikosteuerung und -Kontrolle

- A5.1 Risikosteuerung

  Die in AP1 identifizierten Sicherheitsmaßnahmen werden hinsichtlich ihrer Steuerungswirkung qualifiziert. Steuerungsmaßnahmen sind: Risiken vermeiden, Risiken mindern, Risiken auf andere überwälzen (z.B. Versicherungen) oder Risiken selbst tragen. Anhand dieser Klassifizierung kann entschieden werden, bis zu welchem Risikograd welche Vorgehensweise zu wählen ist. Dies bedingt Kontrollen, die bei erfolgreicher Anwendung die Bedrohung oder Vulnerabilität und damit auch den Schaden

senken können. Bei diesen Kontrollen handelt es sich sowohl um organisatorische als auch technische Kontrollen. Die Etablierung von Kontrollen muss auf Wirksamkeit geprüft werden.

- Mit Hilfe von Kontrollen kann die Wirksamkeit von Sicherheitsmaßnahmen in Bezug auf die Vulnerabilität und Bedrohung überprüft werden. Hierfür werden definierte Kenngrößen aufgestellt, um mögliche Abweichungen bewerten zu können. In die Kontrollen werden technische Einrichtungen sowie organisatorische Abläufe einbezogen. In enger Abstimmung mit dem Unterauftragnehmer KVB werden Kontrollsysteme entwickelt, welche die Schwachstellen der Operationspläne hinsichtlich der Wirksamkeit von Sicherheitsmaßnahmen entdeckt. Die theoretischen Überlegungen zu den Kontrollen werden in praktischen Übungen auf ihre Zielerreichung hin überprüft.
- Zur Prüfung werden Übungen durchgeführt, für welche die KVB eine realistische Umgebung zur Verfügung stellt. Die Kontrollsysteme werden dabei im Feldversuch offen und verdeckt angewendet und ausgewertet.
- Der Personalaufwand für die Gestaltung der Umgebung, die Vorbereitung und Durchführung einer realistischen Übung ist punktuell sehr hoch. Aus diesem Grund wird die Ausführung an einen Unterauftragnehmer vergeben. Hierbei ist eine effiziente, effektive und damit ökonomisch sinnvolle Aufgabenbewältigung möglich.

Die TH Köln hat Regeln für die Wirksamkeit von Sicherheitsmaßnahmen aufgestellt. Dabei wurde unterschieden in indirekte Wirkungen, welche auf die Absicht des Täters (Teil der Bedrohung) wirken und direkte Wirkungen. Direkte Wirkungen von Sicherheitsmaßnahmen verringerten die Vulnerabilität und das Schadensausmaß. Die Wirkungen der Sicherheitsmaßnahmen beeinflusst somit über diese Faktoren das Risiko des jeweiligen Szenarios.

Zur Überprüfung der aufgestellten Regeln führte die TH Köln ein Planspiel mit Experten durch (vgl. AP2.3). Dazu wurde eine Methode entwickelt, um die Aussagen der Experten, welche in interaktiven Diskussionen an der realistischen Testumgebung erarbeitet wurden, mit den Ergebnissen der Methode zur Bestimmung der Vulnerabilität eines schienengebundenen ÖPV-Systems zu vergleichen. Zur einfacheren Anwendung hat die TH Köln ein automatisiertes Worksheet entwickelt. In diesem Worksheet wurden nacheinander alle wichtigen Schritte zur Bestimmung der präventiven Wirkung von Sicherheitsmaßnahmen und der Vulnerabilität durchlaufen und miteinander verrechnet, sodass dieses Worksheet ebenfalls Grundlage für den Planungsverbund ist und mit diesem verknüpft werden kann.

- A5.2 Analyse der Wirkung der Sicherheitsmaßnahmen

  Folgende Analysen werden angestellt: (a) in welchem Umfang verringern die Sicherheitsmaßnahmen die Zahl der Opfer sowie das Ausmaß des Schadens pro Vignette (direkter Einfluss), (b) in welchem Umfang verringern die Sicherheitsmaßnahmen die Folgeschäden pro Vignette (indirekter Einfluss), (c) in welchem Umfang beeinflussen die Sicherheitsmaßnahmen weiche Faktoren (wie z.B. Medien, öffentliche Meinung, Nachfrage).

  - Die Wirkung von Sicherheitsmaßnahmen ist eine wichtige Information, um Realisierungspläne aufstellen zu können. Hierzu wird die FHK alle möglichen Wirkungen auflisten und nach direkter und indirekter Wirkung unterscheiden. Hierbei kommen zusätzlich

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Erfahrungen mit Sicherheitsmaßnahmen aus historischen Anschlägen, anderen Großschadenslagen sowie durchgeführten Übungen zum Tragen.
- Gerade die indirekten Wirkungen sind schwer zu erfassen. Hierzu werden mögliche Betroffene gezielt befragt, um deren Reaktionen und der damit verbundenen indirekten Wirkungen von Sicherheitsmaßnahmen abschätzen zu können. Die einzelnen Wirkungen werden klassifiziert und mit den Sicherheitsmaßnahmen der Operationspläne verknüpft.
- Aus der Analyse werden Regeln für die Wirkung von Sicherheitsmaßnahmen abgeleitet und aufgestellt.
- Die Ergebnisse werden gemeinsam mit der KVB auf Plausibilität geprüft.

▪

Im AP5.2 wurden durch die TH Köln zunächst direkte und indirekte Wirkungen von Sicherheitsmaßnahmen erfasst und aufgelistet. Anschließend entwickelte die TH Köln eine Methode zur Bewertung der präventiven Wirkung von Sicherheitsmaßnahmen. Diese Methode beruhte auf dem erstellten Prozessmodell aus AP2.1. Insbesondere die Stellen, an denen die Sicherheitsmaßnahme im Prozessmodell den Täter oder das Angriffsmittel als solche erkennen kann (Wirkstellen), sind relevant für die Wirkung der Sicherheitsmaßnahmen. Dabei galt, an je mehr Stellen eine Sicherheitsmaßnahme wirkt, des hoher ist die Gesamtwirkung. Zusätzlich ergaben sich weitere Faktoren zur Wirkungen der Sicherheitsmaßnahmen, welche durch die Experten in verschiedenen Fragen beantwortet wurden. Beide Ergebnisse zusammen ergaben eine semi-quantitative Bewertung der einzelnen Sicherheitsmaßnahmen, welche zu der Wirkung eines Maßnahmenbündels verrechnet wurde.

Die Methode ist im internen Projektbeitrag zum AP5.2 der TH Köln dokumentiert.

A5.6 Priorisierung der Sicherheitsmaßnahmen

Der analytische Hierarchieprozess (AHP) nach Saaty oder andere geeignete Multi Criteria Methoden werden auf ihre Eignung hin überprüft und die am besten geeignete Methode wird ausgewählt und an die Problemstellung angepasst. Hierbei werden auch Wissensdatenbanken und damit verknüpfte selbstlernende Systeme untersucht

- Der UA KVB unterstützte die Verbundpartner bei der Priorisierung der Sicherheitsmaßnahmen nach der entwickelten Priorisierungsmethode.

Entsprechend der erarbeiteten Methode zur Bestimmung der Wirkung von Sicherheitsmaßnahmen hat die TH Köln die erfassten Sicherheitsmaßnahmen aus AP1.4 priorisiert. Die Ergebnisse wurden in die Vulnerabilitätsmatrix aus AP4.1 integriert.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

3.1.5 AP 7 – Integration, Test, Validierung

- A 7.1 Integration und Test

  Die zentrale Schnittstelle aller in den verschiedenen Arbeitspaketen bereitzustellenden Methoden ist die Szenario Datenbank von AP2 (Aktivität A 2.3), in der auch alle relevanten Input- und Output-Daten der anderen Arbeitspakete abgelegt bzw. bereitgestellt werden. Die Methoden zur Unterstützung des Risikomanagements werden in den Arbeitspaketen AP2, AP5 und AP6 bereitgestellt, so dass im AP7 das Portal mit den Interfaces zu den verschiedenen Modellen entworfen und im Gesamtverbund getestet werden muss.

  – Alle im Projekt entwickelten Methoden und relevanten Input- und Output-Daten werden in der zentralen Szenario-Datenbank aus AP 2 erfasst und integriert. Die FHK integriert alle Daten, die in den beteiligten Arbeitspaketen aufgestellt wurden. Der Gesamtverbund aller Daten wird getestet. Hierfür werden die integrierten Daten im ersten Schritt auf Richtigkeit überprüft. Im zweiten Schritt werden gemeinsam mit dem UA KVB aus den Vignetten eine Reihe von exemplarischen Testfällen entwickelt, anhand derer die Datenbank im Gesamtverbund auf Plausibilität überprüft werden kann.
  – Aus den Testfällen wird ein Planspiel für die Validierung in A7.2 vorbereitet.

Die TH Köln hat die In-/Output-Daten der Projektpartner erfasst und ein Szenario als exemplarische Testreihe bestimmt. Dieses Szenario wurde sowohl im Planspiel AP2.1 als auch in der Realübung AP7.2 zur Validierung der Ergebnisse angewendet.

- A 7.2 Validierung

  AP6 stellt eine Liste von Sicherheitsmaßnahmen zur Verfügung, die innerhalb eines vorgegebenen Planungshorizontes finanziert und eingeführt werden können (realisierbare Sicherheitsmaßnahmen). In diesem Arbeitsschritt soll mit Hilfe der Operationsanalyse (siehe AP2) nachgewiesen werden, dass die realisierbaren Sicherheitsmaßnahmen die Anforderungen der in A 2.2 bereitgestellten Szenarien erfüllen (= Praxistest in einer virtuellen Umwelt). Dazu wird jedes Szenario in 2 Varianten untersucht: Variante 1 simuliert den Ablauf des im jeweiligen Szenario beschriebenen Terroranschlages, aber ohne Berücksichtigung der von AP6 gelieferten realisierbaren Sicherheitsmaßnahmen. Variante 2 simuliert den Ablauf des im jeweiligen Szenario beschriebenen Terroranschlages, aber diesmal unter Berücksichtigung der realisierbaren Sicherheitsmaßnahmen. Die Ergebnisse der beiden Varianten werden verglichen und hinsichtlich der Konsequenzen bewertet.

  - Die FHK schafft eine realistische Test-Umgebung in Form eines Planspiels, um die Ergebnisse der vorangegangenen Arbeitspakete zu validieren. Die Szenarien aus den Vignetten werden in ihren Abläufen und Folgen innerhalb des Planspiels von der FHK und Akteuren des UA KVB durchgespielt. Exemplarisch werden ausgesuchte Szenarien (Testfälle) in einer realen Test-Umgebung des UA KVB durchgespielt, um die Ergebnisse mit denen des Planspiels zu vergleichen und zu bewerten. Die Überprüfung wird nach vorgegebenen Regeln durch die FHK durchgeführt und dokumentiert.
  - Abschließend werden alle Ergebnisse in einem internen Arbeitskreis miteinander verglichen und die Wirksamkeit der Sicherheitsmaßnahmen sowie der Test-Umgebung bewertet.
  – FHK Abschlusslieferung: Bericht „Validierung der Planungsergebnisse“

Zur Validierung der Ergebnisse aus den vorherigen AP wurde durch die TH Köln, neben dem Planspiel aus AP2.1, eine Realübung in Zusammenarbeit mit der KVB durchgeführt. Die Testumgebung für diese Realübung war eine neue Haltestelle der KVB, die zum Übungszeitpunkt (30. und 31.05.2015) vollständig ausgebaut, jedoch noch nicht in den aktuellen Linienbetrieb integriert war. Die Realübung fand in zwei Teilen statt. So wurde am ersten Tag, in Zusammenarbeit mit verschiedenen Herstellern von Sicherheitsmaßnahmen, die Implementierung neuer Sicherheitsmaßnahmen geübt und die Auswirkungen auf die Fahrgäste und den Betrieb erforscht. Insbesondere die Wirkung der Sicherheitsmaßnahmen stand im Vordergrund der Übung, um diese Ergebnisse mit den Simulationen der Projektpartner und dem Planspiel zu vergleichen. Zur Durchführung der Übung wurde von der TH Köln ein eigenes Übungskonzept erarbeitet.

Im zweiten Teil der Realübung wurde besonderen Wert auf die Verknüpfung des Risikomanagements des Betreibers mit dem behördlichen Krisenmanagement gelegt. Dazu wurden 100 verletzte Personen durch Studierende der TH Köln simuliert, welche durch Einsatzkräfte der Stadt Köln (Berufsfeuerwehr und Ordnungsamt), der Polizei Köln und der KVB versorgt und betreut werden mussten. Die TH Köln hat diese Übung wissenschaftlich begleitet, um den Einfluss der Sicherheitsmaßnahmen, den Zusammenhang von Risiko- und Krisenmanagement und die Zusammenarbeit der einzelnen Behörden und Organisationen zu erfassen und auszuwerten. Dazu wurde ebenfalls lange im Vorfeld ein Konzept in Absprache mit den beteiligten Partnern erarbeitet.

Weiterhin wurde die gesamte Realübung durch die TH Köln organisatorisch vorbereitet, geplant, durchgeführt und nachbereitet. Neben den laufenden Absprachen mit allen beteiligten Partnern, wurde durch die TH Köln die Medienarbeit organisiert. Diese beinhaltete die Information der Anwohner der Übungsumgebung, das Ausformulieren der Pressemitteilungen, sowie die Organisation der Pressekonferenz am Tag der Übung. Außerdem wurde die gesamte messtechnische Einrichtung für die Übung von dem Labor für Großschadensereignisse der TH Köln aufgebaut und betrieben.

Die Ergebnisse der Realübung sowie des Planspiels sind im Bericht L7.2 „Integration und Test“ dokumentiert.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

3.1.6 AP 8 – Verbreitung und Verwertung

- A 8.3 Konferenzen

  Die Projektpartner werden vorzugsweise solche Workshops und Konferenzen besuchen, an denen für das Projekt relevante Interessensgruppen teilnehmen. Darüber hinaus wird das Konsortium eigene Workshops organisieren.

  – FHK unterstützt aktiv die Durchführung der drei RIKOV-Workshops und beabsichtigte, an folgenden Konferenzen teilzunehmen:
    - UITP, World Congress, Geneva, Switzerland, 26.-30. Mai 2013
    - WCRR, World Congress, Sydney, Australia, 25.-27. Nov 2013 (gestrichen durch VDI)

Die TH Köln hat im Rahmen des Forschungsprojekts RiKoV an folgenden Konferenzen teilgenommen:

- 8th Conference Future Security, Session 6: Supply Chain Security and Logistics // Urban and Land Transportation Security, Sep 17-19, 2013, Berlin, Germany

- Safety & Security Innovations Alliance der Hochschulen NRW, Jun 18, 2014, Innovations Allianz, Representation of the State of North Rhine-Westfalia to the EU, 1000 Brussels, Belgium (nicht aus RiKoV finanziert)

- 10th World Congress on Railway Research 2013, Nov. 25-28, 2013, Organizer: Association of American Railroads / Transportation Technology Center Inc. (AAR / TTCI), Deutsche Bahn AG, Rail Safety and Standards Board (RSSB), Railway Technical Research Institute (RTRI), Trenitalia SpA, International Union of Railways (UIC), Australasian Railway Association, The CRC for Rail Innovation, SNCF; Sydney, Australia (nicht aus RiKoV finanziert)

- Verband der deutschen Verkehrsunternehmen (VDV), AG Security Tagung, RiKoV Workshop, KIT Karlsruher Institute of Technology, Apr 27, Karlsruhe, Germany

- 5th International Disaster and Risk Conference - IDRC Davos 2014; "Integrative Risk Management - The role of science, technology & practice" Global Risk Forum Davos, Aug 24-28, 2014; Davos, Switzerland

- 9th Conference Future Security, Session 6: RiKoV, Sep. 16-18, 2014, Berlin, Germany

- ISCRAM 2015 - Information Systems for Crisis Response and Management, May 24-27, 2015 in Kristiansand, Norway.

- 4th World Congress on Risk 2015, Society for Risk Analysis, July 19-23, 2015 in Singapore (nicht aus RiKoV finanziert).

- OR 2015 International Conference in Operations Research, Sep. 1-4, 2015 in Vienna, Austria (nicht aus RiKoV finanziert).

Dabei wurden im Rahmen der Workshops und Konferenzen die wissenschaftlichen Ergebnisse von RiKoV den Experten (Endanwendern und Wissenschaftlern) vorgestellt und validiert.

- A 8.4 Experteneinbindung

  Um eine möglichst große Verbreitung der Projektergebnisse zu erreichen, werden die Projektpartner ihre Kontakte zu anderen Forschungseinrichtungen, Behörden und Infrastrukturbetreiber erweitern, um diese für die erzielten Ergebnisse zu sensibilisieren. Andrerseits werden diese Kontakte auch für Interviews genutzt, um so weit wie möglich die aktuellen methodischen Erkenntnisse dieser Experten in RIKOV einzubinden

  – Die FHK und die Unterauftragnehmer werden themenspezifische Kontakte aufbauen und diese für das Projekt-Thema sensibilisieren.

Die TH Köln hat über seinen Unterauftragnehmer Kölner Verkehrs-Betriebe AG Kontakt zu dem Verband der Deutschen Verkehrsunternehmen aufgebaut. Im Rahmen des Unterausschusses Security wurden die TH Köln RiKoV Ergebnisse vorgestellt und validiert. Die Teilnahme der Experten an mehreren Projekt-Workshops sowie der RiKoV Übung (Mai 2015) zeigten ein hohes Interesse an der Thematik.

In Bezug auf die Entwicklung des Demonstrators Vulnerabilität wurden die Anforderungen der Experten erhoben und bei der Entwicklung berücksichtigt.

Publikationsliste

Folgende Publikationen wurden im Rahmen des Forschungsprojekts RiKoV von der TH Köln erstellt, publiziert bzw. auf Konferenzen bzw. Journals veröffentlicht:

- Brauner, F.; Mudimu, O.A.; Lechleuthner, A. (2013) ***RiKoV – Risk and Costs of terrorist Threats To Public Transit.*** In Hollricher, K.; Garwood, J.; Schwarz K.; Koch, H. (Ed.) ***SAFETY & SECURITY*****. Safety & Security InnovationsAllianz;** InnovationsAllianz der NRW-Hochschulen e.V. & VDI Technologiezentrum GmbH, 2013, Düsseldorf, Germany, pg. 14, ISBN: 978-3-00-041075-8
- Lin, L.; Brauner, F.; Muenzberg, T.; Meng, S.; Moehrle, S. (2013) ***Prioritization of security measures against terrorist threats to public rail transport systems using a scenario-based multi-criteria method and a knowledge database.*** In: Lauster, M. (Ed.): 8th Future Security, Security Research Conference; Sept. 17-19, 2013 in Berlin/Germany; Fraunhofer Verlag Stuttgart; ISBN 978-3-8396-0604-9; pg. 195-204.
- Brauner, F.; Fiedrich, F.; Lechleuthner, A. (2013) ***Integration of customers' perception of security and uncertainties into risk management concepts for public transportation providers***. Poster und Beitrag In: Lauster, M. (Ed.): 8th Future Security, Security Research Conference; Sept. 17-19, 2013 in Berlin/Germany; Fraunhofer Verlag Stuttgart; ISBN 978-3-8396-0604-9; pg. 465-467.
- Brauner, F.; Baumgarten, C.; Schmitz, W.; Neubecker, K.A.; Mudimu, O.A.; Lechleuthner, A. (2013) ***RiKoV Risk analysis of terrorist threats to rail-bound public transportation: Development of an integrated planning solution for efficient economic and organisational measures.*** In: 10th World Congress on Railway Research 2013; Nov. 25-28, 2013 in Sydney/Australia; paper ID 112 Conference Proceedings

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- Brauner, F.; Fiedrich, F.; Lechleuthner, A.; Mudimu, O.A. (2013) ***Terror threats in public transportation - A study about customers perception of security measures.*** In: 10th World Congress on Railway Research 2013; Nov. 25-28, 2013 in Sydney/Australia; paper ID 132 Conference Proceedings

- Baumgarten, C.; Brauner, F.; Bentler, C.; Mudimu, O.A.; Lechleuthner, A. (2014) ***A methodology to compare risk management (RM) systems for the application and validation of specific threats in public transportation.*** In: Brebbia, C.A. (Ed.): RISK ANALYSIS IX, WIT Transactions on Information and Communication Technologies, DOI: 10.2495/RISK140191, Vol 47, ISSN 1743-3517 (online), pg. 219-228.

  http://www.witpress.com/elibrary/wit-transactions-on-ecology-and-the-environment/47/26347

- Brauner, F.; Baumgarten, C.; Bentler, C.; Kornmayer, T.; Mudimu, O.A.; Lechleuthner, A. (2014) ***Vulnerability analysis for terrorist attacks on public transportation systems based on process modelling.*** Poster PB 054 / Short abstract published in: Ammann, W. J. (Ed.) Global Risk Forum GRF Davos, 5th International Disaster and Risk Conference - IDRC Davos 2014; "Integrative Risk Management - The role of science, technology & practice" – Programme & Short Abstracts, Aug. 24.-28., 2014; Davos, Switzerland, ISBN 978-3-033-04701-3, pg. 206-207.

  Extended abstract published in Ammann, W. J. (Ed.) Global Risk Forum GRF Davos, 5th International Disaster and Risk Conference - IDRC Davos 2014; "Integrative Risk Management - The role of science, technology & practice" – Poster Collection, Aug. 24.-28., 2014; Davos, Switzerland, pg. 48-52; http://idrc.info/programme/conference-proceedings/

- Bentler, C.; Baumgarten, C.; Brauner, F.; Kornmayer, T.; Mudimu, O.A.; Lechleuthner, A. (2014) ***An integrated risk and crisis management approach for terrorist attacks in public transport networks***. Short abstract published in: Ammann, W. J. (Ed.) Global Risk Forum GRF Davos, 5th International Disaster and Risk Conference - IDRC Davos 2014; "Integrative Risk Management - The role of science, technology & practice" – Programme & Short Abstracts, Aug. 24.-28., 2014; Davos, Switzerland, ISBN 978-3-033-04701-3, pg. 113.

  Extended abstract published in Ammann, W. J. (Ed.) Global Risk Forum GRF Davos, 5th International Disaster and Risk Conference - IDRC Davos 2014; "Integrative Risk Management - The role of science, technology & practice" – Extended Abstracts, Aug. 24-28, 2014; Davos, Switzerland, pg. 89-92 http://idrc.info/programme/conference-proceedings/

- Brauner, F.; Baumgarten, C.; Kornmayer, T.; Bentler, C.; Mudimu, O.A.; Lechleuthner, A. (2014) ***A Methodology for a vulnerability analysis of public transportation systems in context of terrorist attacks.*** In: Thoma, K.; Häring, I.; Leismann, T. (Eds.): 9th Future Security, Security Research Conference; Sept. 16-18, 2014 in Berlin, Germany; Fraunhofer Verlag, Stuttgart; ISBN 978-3-8396-0778-7; pg. 271-277.

- Roth K.; Barth K.; Mudimu O.A.; Lechleuthner A.; Brauner F.; Stiehl M. (2014) ***Technische Möglichkeiten zur Datenermittlung zur Evaluierung von MANV-Übungen.*** INFORMATIK 2014: Big Data – Komplexität meistern, 44. Jahrestagung der Gesellschaft für Informatik; Workshop IT-Unterstützung in Emergency Management & Response, Sept. 22-26, 2014 in Stuttgart, Germany.

- Brauner, F.; Muenzberg, T.; Wiens, M.; Fiedrich, F.; Lechleuthner, A.; Schultmann, F. (2015) ***Critical Infrastructure Resilience: A Framework to Consider Multiple Observation Levels.*** The 12th International Conference on Information Systems for Crisis Response and Management. In: L. Palen, M. Buscher, T. Comes, and A. Hughes (Eds.), ISSN: 2411-3387, ISBN: 978-82-7117-788-1.

- Brauner, F.; Maertens, J.; Bracker, H.; Mudimu, O.A.; Lechleuthner, A. (2015) ***Determination of the effectiveness of security measures for low probability but high consequence events: A comparison of multi-agent-simulation & process modelling by experts.*** The 12th Interna-

tional Conference on Information Systems for Crisis Response and Management. In: L. Palen, M. Buscher, T. Comes, and A. Hughes (Eds.), ISSN: 2411-3387, ISBN: 978-82-7117-788-1.

- Brauner, F.; Pickl, S.; Schmitz, W.; Mudimu, O.A.; Lechleuthner, A. (2015) ***Decision support in dynamic systems – Risk Assessment of effective countermeasures against terrorist attacks in rail-bound public transportation systems.*** Presentation T3-A.1 on July 21, 2015, Session Modeling Risks to Infrastructure Systems, 4th World Congress on Risk 2015, Society for Risk Analysis, July 19-23, 2015 in Singapore.
- Brauner, F.; Fiedrich, F.; Lechleuthner, A. (2015) ***Analysis of the social effects of security measures on the customers' security perception - Integration of social-scientific aspects into risk management.*** Presentation W4-A.4 on July 22, 2015, Session Transportation Risks, 4th World Congress on Risk 2015, Society for Risk Analysis, July 19-23, 2015 in Singapore.
- Brauner, F.; Mudimu, O.A.; Lechleuthner, A.; Lotter, A. (2015) ***Cologne Mass Casualty Incident Exercise 2015 - Evaluation by Use of Linked Databases to Improve Risk and Crisis Management in Critical Infrastructure Protection***. OR 2015 International Conference in Operations Research, Sep. 1-4, 2015 in Vienna, Austria.
- Meyer-Nieberg, S.; Zsifkovits, M.; Brauner, F. (2015) ***Assessing the Effects of Security Measures: From Real-Life Exercises to Simulation-Based Analyses.*** 10th Future Security, Security Research Conference; Sept. 15-17, 2015 in Berlin, Germany.
- Brauner, F.; Bracker, H.; Kornmayer, T.; Maertens, J. (2015) ***Conceptual Framework for Evaluation of Intelligent Security Measures in Multi-Agent-Simulations - A Proof of Concept for Decision-Makers.*** 10th Future Security, Security Research Conference; Sept. 15-17, 2015 in Berlin, Germany.

3.2 Zusammenfassung des Gesamtergebnis

Zusammenfassend ist das Projekt RiKoV aus Sicht der TH Köln als erfolgreich zu bewerten. Das angestrebte Ziel der Entwicklung einer neuartigen Methode zur Ingenieurmässigen Risikobeurteilung wurde erfüllt. Die Methode zur Bestimmung der Vulnerabilität, welche ebenfalls eine Methode zur Bestimmung der Wirkung von Sicherheitsmaßnahmen im ÖPNV beinhaltet, ist ein innovativer Fortschritt in der Beurteilung von systemischen Risiken wie Terrorismus.

Der Entwicklungsprozess, welche seitens der TH Köln von Beginn des Projekts mit den Endanwendern durchgeführt worden ist, zeigt ein hohes Maß an Anwendbarkeit der Methode und Praxisbezug. Die Integration der gesellschaftlichen bzw. kundenspezifischen Akzeptanz von Sicherheitsmaßnahmen stellt ein Mehrgewinn in der Gesamtbeurteilung von Risiken dar. Bei der wissenschaftlichen Disputation der Ergebnisse auf nationalen und internationalen Konferenzen wurde insbesondere die Validierung der Ergebnisse in mehreren Schritten (Planspiel, Multi-Agenten Simulation und Realübung) besonders gelobt.

Die Sensibilisierung für diese Thematik und Verbreitung erfolgte in enger Kooperation mit dem Verband der Deutschen Verkehrsunternehmen, sowie der Deutschen Bahn und Kölner Verkehrs-Betriebe AG.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

3.3 Ausblick

In Bezug auf die aktuellen Ereignisse Anfang August 2015 als im Hochgeschwindigkeitszug Thalys ein versuchter, terroristischer Anschlag von zwei Passagieren vereitelt werden konnte, rücken die Ergebnisse von RiKoV immer weiter ins Licht der Öffentlichkeit. Die Balance der öffentlichen Sicherheit in diesem Spannungsfeld ist eine Herausforderung für Betreiber von kritischen Infrastrukturen, wie dem Bahnverkehr, sowie für Behörden.

Im Rahmen dieses Spannungsfelder wird es ein zukünftiges Forschungsprojekt mit dem Titel RE(H)STRAIN „Resilience of the Franco-German High-Speed Train Network“ geben. In dieses Projekt werden die Ergebnisse von RiKoV durch die teilnehmenden Projektpartner einfließen und auf das Hochgeschwindigkeitsnetz zwischen Frankreich und Deutschland übertragen.

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Anhang

A 1. Erfolgskontrollbericht

Siehe Anlage

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

A 2. Kurzfassung

Am Beispiel des schienengebundenen öffentlichen Personenverkehrs (ÖPV) im Rahmen des Verbundforschungsprojekt RiKoV gezeigt werden, wie kritische Infrastrukturen durch ein ganzheitliches Risikomanagement (RM) besser vor terroristischen Anschlägen geschützt werden können. Im Rahmen eines solchen Risikomanagements werden die terroristischen Bedrohungen und Verwundbarkeit der Infrastruktur erfasst, die dadurch verursachten Risiken hinsichtlich Konsequenzen und Kosten unter Berücksichtigung der praktischen Erfahrungen von Polizei und Betreibern bewertet, die abgeschätzten Infrastrukturrisiken mit den Erkenntnissen der Sicherheitsbehörden evaluiert, abgestimmt und gegebenenfalls abgeglichen geeignete Maßnahmen identifiziert und bewertet, die inakzeptable Risiken beseitigen beziehungsweise deren Konsequenzen abmildern, ohne gegen gesellschaftliche Wertvorstellungen, Grundrechte und gesetzliche Regelungen zu verstoßen. Weiterhin werden Realisierungspläne für die Schutzmaßnahmen unter Berücksichtigung wirtschaftlicher Rahmenbedingungen aufgestellt und die Konsequenzen aufgezeigt. Hierbei finden insbesondere auch behördliche Entscheidungsparameter Eingang, nach denen Schutzmaßnahmen vorgeschlagen oder angeordnet werden. Damit zielt das ganzheitliche Risikomanagement darauf ab, in dem Spannungsfeld zwischen den technisch und organisatorisch maximal erreichbaren, der wirtschaftlich sinnvollen und den von den gesellschaftlichen Werten abgeleiteten Sicherheitsbegriffen die optimale Sicherheit zu erreichen, die Prävention als auch Gefahrenabwehr umfasst.

Die Technische Hochschule Köln befasste sich dabei gemäß ihrer Teilvorhabenbeschreibung und dem Zuwendungsbescheid durch das Bundesministerium für Bildung und Forschung (BMBF) schwerpunktmäßig mit den folgenden Tätigkeiten:

- Ingenieurmäßige Risikobeurteilung von schienengebundenen ÖPV-Systemen
- Erfassung, Entwicklung und Validierung von Sicherheitsmaßnahmen im ÖPV
- Bewertung von gesellschaftlicher und kundenspezifischer Akzeptanz von Risiken und konkreten Sicherheitsmaßnahmen im ÖPV
- Entwicklung einer Methode zur Bestimmung von Verletzlichkeiten (Vulnerabilität) in ÖPV-Systemen für terroristische Szenarien
- Validierung von Projektergebnissen in Zusammenarbeit mit der Kölner Verkehrs-Betriebe AG und anderen Endanwendern durch die Organisation und Durchführung von Planübungen und einer Realübung

Kontaktdaten

Technische Hochschule Köln
Institut für Rettungsingenieurwesen und Gefahrenabwehr
Prof. Dr.-Ing. Ompe Aimé Mudimu
Prof. Dr. med. Dr. rer. nat. Alex Lechleuthner
Betzdorfer Str. 2
50679 Köln
E: ompe_aime.mudimu@th-koeln.de
T: 0221 / 8275 - 2206

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

A 3. Literaturliste / Informationsdienste

Abdellaoui, Mohammed (2008): Advances in Decision Making Under Risk and Uncertainty: Springer. Online verfügbar unter http://katalog.ub.uni-heidelberg.de/cgi-bin/titel.cgi?katkey=66610292.

ABUS (Hg.) (2014): ABUS IR Mini HD-SDI 1080p Außenkamera. Online verfügbar unter http://www.abus.com/Objektsicherheit/Videoueberwachung/Ueberwachungskameras/Aussenkameras/Aussen-HD-SDI-Kameras/IR-Mini-HD-SDI-1080p-Aussenkamera, zuletzt geprüft am 10.02.2014.

acal (Hg.) (2013): Security & Detection. Produktkatalog. Online verfügbar unter www.acalbfi.de, zuletzt geprüft am 23.10.2013.

Albrecht, Hans-Jörg (2009): Sicherheitswahrnehmung im 21. Jahrhundert. Präsentation Workshoph Man-Planck-Institut, 30.10.2009, zuletzt geprüft am 09.05.2012.

American Petroleum Institute (Hg.) (2003): Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries. Washington.

American Public Transportation Association (2010): Survey of United States Transit System Security Needs, zuletzt geprüft am 03.08.2012.

American Science and Engineering, Inc. (2014): Smartcheck HT. Internetauftritt. Billerica. Online verfügbar unter http://www.as-e.com/products-solutions/personnel-screening/checkpoint-lobby/product/smartcheck-ht#, zuletzt geprüft am 12.02.2014.

Andritsos, Fivos; Rafaeli, Gilad; Abbot, Paul (2011): Public Transport Security Terminology & Definitions. Hg. v. SECUR-ED. Joint Research Centre (D21.1).

Arbeitskreis Technische Systeme, Risiko und Verständigungsprozesse (2004): Bericht: Risikomanagement im Rahmen der Störfall-Verordnung. SFK-GS-41. Störfall-Kommission beim Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit. Berlin, zuletzt geprüft am 05.01.2013.

Arrow, Kenneth J.: Risk Perception in Psychology and Economics. In: *Economic Inquiry* 1982 (20:1), S. 1.

AS/NZS 4360:2004, 2004: Risk Management.

ASIS International (Hg.) (2003): The General Security Risk Assessment Guideline. Virginia (ASIS GLCO 01 012003).

ASME-Innovative Technologies Institute (Hg.) (2006): The RAMCAP Framework. Risk Analysis and Management for Critical Asset Protection. Version 2.0. Washington DC.

Aven, Terje (2010): Misconceptions of Risk. Chichester: Wiley.

Bailer, A. John (1999): Uncertainty in the Risk Assessment of Environmental and Occupational Hazards. An international workshop. New York: New York Academy of Sciences (Annals of the New York Academy of Sciences, 895).

Bajon, Arno; Lülsdorf, Dominic; Schröter, Reinhold (2012): Wenn es "brennt" - Krisen im ÖPNV. Die Arbeit von Krisenstäben im ÖPNV. In: *DER NAHVERKEHR* (11), S. 7–12.

Baker, George H. (2005): A Vulnerability Assessment Methodology for Critical Infrastructure Sites. Harrisonburg.

Balog, John N.; Boyd, Annabelle; Caton, James E. (2003): The Public Transportation. System Security and Emergency Preparedness. Planning Guide. Hg. v. U.S. Department of Transportation. Cambridge, Massachusetts.

Bammer, Gabriele; Smithson, Michael (2009): Uncertainty and Risk. Multidisciplinary perspectives. Pbk. ed. London, Sterling, VA: Earthscan (Earthscan risk in society series).

Barr, Lindsey; Luyten, Denis (2010): Conducting Risk Assessment in PT Networks. Guidelines for Operators. In: *Public Transport International magazine* 59 (1), S. 22–25.

Beate Kucher; Guntram Schäfer, Thilo Puhle: Sicherheit mit Methode. Security-Risk-Assessments als Teil des Qualitätsmanagments der Stuttgarter Straßenbahnen AG. In: *DER NAHVERKEHR*, S. 16–21, zuletzt geprüft am 27.05.2013.

Becker, Ulrike (1993): Risiko ist ein Konstrukt. Wahrnehmungen zur Risikowahrnehmung. Hg. v. Bayerische Rückversicherung. München: Knesebeck (Reihe Gesellschaft und Unsicherheit, 2).

Bellido Zúniga, Eduardo; Blobner, Christian (2013): VALUESEC. Mastering the Value Function of Security Measures, zuletzt geprüft am 21.11.2013.

Belyová, L.; Schulze-Bramey, U. (2009): Der Mensch, das Maß aller Dinge? Sicherheitskulturelle Aspekte auf dem Prüfstand. In: Petra Winzer (Hg.): Weiterentwicklung des Wuppertaler Generic-Management-Konzeptes. Aachen: Shaker (2009,1), S. 107–114.

Bennet, Brian T. (2007): Understanding, Assessing and Responding to Terrorism. Protecting Critical Infrastructure and Personnel. Hg. v. John Wiley & Sons. New Yersey.

Berche, B.; Ferber, C. von; Holovatch, T.; Holovatch, Yu. (2009): Resilience of public transport networks against attacks. In: *Eur. Phys. J. B* 71 (1), S. 125–137. DOI: 10.1140/epjb/e2009-00291-3.

Bettelini, M.; Rigert, S.; Seifert, N. (2013): Optimum Emergency Management Through Physical Simulation. Findings from the Emili Research Project. Hg. v. G. Anagnostou und H. Ehrbar. Genf.

Birkmann, J.; Bach, C.; Guhl, S.; Witting, M.; Welle, T.; Schmude M.: State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Stromausfall. In: *Schriftenreihe Forschungsforum Öffentliche Sicherheit,* zuletzt geprüft am 19.11.2012.

Birkmann, Jörn (2011): Indikatoren zur Abschätzung von Vulnerabilität und Bewältigungspotenzialen. Am Beispiel von wasserbezogenen Naturgefahren in urbanen Räumen. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Forschung im Bevölkerungsschutz, 13).

Bjorn Schuller, Matthias Wimmer, Dejan Arsic, Tobias Moosmayr, Gerhard Rigoll (2008): Detection of Security Related Affect and Behaviour in Passenger Transport. ISCA. Brisbane, zuletzt geprüft am 28.10.2013.

Blalock, Garrick; Kadiyali, Vrinda; Simon, Daniel H. (2005): The Impact of Post 9/11 Airport Security Measures on the Demand for AirTravel. Cornell University, Ithaca,. Online verfügbar unter http://dyson.cornell.edu/faculty_sites/gb78/wp/airport_security_022305.pdf, zuletzt geprüft am 21.11.2013.

Blanchard, Wayne (2007): Guide to Emergency Management and Related Terms, Definitions, Concepts, Acronyms, Organizations, Programs, Guidance, Executive Orders & Legislation. A Tutorial on Emergency Management, Broadly Defined, Past and Present.

Blennemann, Friedhelm (2005): Brandschutz in Fahrzeugen und Tunneln des ÖPNV. Düsseldorf: Alba-Fachverl.

BMBF (2013): Internetauftritt des Bundesministeriums für Bildung und Forschung. Bewilligte Projekte aus dem Themenfeld "Gesellschaftliche Aspekte der zivilen Sicherheitsforschung". Hg. v. Bundesministerium für Bildung und Forschung. Online verfügbar unter http://www.bmbf.de/de/13979.php, zuletzt aktualisiert am 27.11.2013, zuletzt geprüft am 29.11.2013.

Bockslaff, Klaus (1999): Die eventuelle Verpflichtung zur Errichtung eines sicherungstechnischen Risikomanagements durch das KonTraG. In: *Neue Zeitschrift für Versicherung und Recht (NVersZ)* (3), S. 104–110.

Bodur, Kaabet (2010): Inflationsentwicklung - Schweiz. Online verfügbar unter http://aysenurum.com/staat.php?iso=CHE&k=inflation, zuletzt geprüft am 22.01.2013.

Böhm, Gisela (Hg.) (2001): Environmental Risks. Perception Evaluation and Management. 1. Aufl. Amsterdam: JAI (Research in social problems and public policy).

Bonß, Wolfgang: (Un-)Sicherheit in der Moderne. Professur für Allgemeine Soziologie, Universität der Bundeswehr München, Neubiberg.

Bowyer, Kevin W. (2004): Face Recognition Technology. Security versus Privacy. In: *IEEE Technology and Society Magazine*, S. 9–20.

Boyd, Annabelle; Sullivan, John P.: Emergency Preparedness for Transit Terrorism. In: *TR News 208* 2000 (May-June), S. 12–17.

Boyd, Annabelle; Sullivan, John P. (1997): Emergency Preparedness for Transit Terrorism. A Synthesis of Transit Practice. Washington, D.C.

Brugnoli, Alberto (2010): Dangerous Materials: Control, Risk Prevention and Crisis management. From New Global Threats to New Global Responses: A Picture of Transition. Dordrecht: Springer.

Bundesamt für Bevölkerungschutz und Katastrophenhilfe Deutschland (2010): Schutz kritischer Infrastrukturen. In: *Bevölkerungsschutz* (3). Online verfügbar unter http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Publ_magazin/bsmag_3_10.pdf;jsessionid=E90B99907FFD0D830E3FC170A4559CDD.1_cid330?__blob=publicationFile, zuletzt geprüft am 30.07.2014.

Bundesamt für Bevölkerungsschutz der Schweiz (Hg.) (2003): KATARISK. Katastrophen und Notlagen in der Schweiz, eine Risikobeurteilung aus Sicht des Bevölkerungsschutzes. Erläuterung der Methode. Bern. Online verfügbar unter http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/gefaehrdungen-risiken/studien/katarisk.parsys.0005.downloadList.00051.DownloadFile.tmp/methodemonitor.pdf, zuletzt geprüft am 17.01.2013.

Bundesamt für Bevölkerungsschutz Schweiz (Hg.) (2008): Leitfaden KATAPLAN - Gefährdungsanalyse und Vorbeugung. Teil: Grundlagen zur Erarbeitung einer kantonalen Gefährdungsanalyse. Bern.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hg.) (2008): Schutz Kritischer Infrastrukturen: Risikomanagement im Krankenhaus. Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens. Bonn. Online verfügbar unter http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_2_Leitfaden_Risikomanagm_Krankenh_Kritis_Langfassung.pdf, zuletzt geprüft am 04.01.2013.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hg.) (2011): Leitfaden für strategische Krisenmanagement-Übungen. Bonn.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Deutschland (2010): Methode für die Risikoanalyse im Bevölkerungsschutz. Bonn (Wissenschaftsforum, 8).

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Deutschland (2011): BBK-Glossar. Ausgewählte zentrale Begriffe des Bevölkerungsschutzes. Bonn (Praxis im Bevölkerungsschutz, 8).

Bundesamt für Statistik (03.04.2012): Noch nie so viele Fahrgäste bei Bussen und Bahnen wie 2011. Pressemitteilung Nr. 122 vom 03.04.2012.

Bundeskriminalamt (2006): Terrorismus und Extremismus, zuletzt aktualisiert am 22.05.2006, zuletzt geprüft am 28.06.2012.

Bundesministerium des Innern (Hg.): Nationale Strategie zum Schutz Kritischer Infrastrukturen. KRITIS-Strategie. Berlin. Online verfügbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/SicherheitAllgemein/kritis.html, zuletzt geprüft am 02.12.2012.

Bundesministerium des Innern (Hg.) (2006): Zweiter periodischer Sicherheitsbericht. Langfassung.

Bundesministerium des Innern (Hg.) (2008): Krisenkommunikation. Leitfaden für Behörden und Unternehmen.

Bundesministerium des Innern (Hg.) (2010): Empfehlungen zur Sicherstellung des Zusammenwirkens zwsichen staatlichen Ebenen des Krisenmanagements und den Betreiber Kritischer Infrastrukturen.

Bundesministerium des Innern (2011): Das Gemeinsame Terrorismusabwehrzentrum · Zusammenarbeit der Sicherheitsbehörden zur Bekämpfung des islamistischen Terrorismus. Berlin.

Bundesministerium des Innern (Hg.) (2011): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden. 2. Auflage. Berlin.

Bundesministerium des Innern (31.08.2011): Körperscanner im Test: Leistungsfähig, aber noch nicht flächendeckend einsetzbar. Pressemitteilung vom 31.08.2011. Berlin. Online verfügbar unter

http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/08/koerperscanner.html, zuletzt geprüft am 11.02.2013.

Bundesministerium des Innern (2012): System des Krisenmanagements in Deutschland.

Bundesministerium für Bildung und Forschung: Risikomanagement bei terroristischen Bedrohungen des schienengebundenen Personenverkehrs (RIKOV).

Bundesministerium für Bildung und Forschung (Hg.) (2011): BMBF › Hightech-Strategie › Sicherheitswahrnehmungen zu Beginn des 21. Jahrhunderts: Perspektiven, Thesen, Themen. Online verfügbar unter http://www.bmbf.de/de/14031.php, zuletzt aktualisiert am 30.06.2011, zuletzt geprüft am 09.05.2012.

Bundesministerium für Verkehr, Bau und Stadtentwicklung (Hg.): Leitfaden für die Durchführung von Kundenzufriedenheitsbefragungen im ÖPNV. Online verfügbar unter http://www.mobilitaet21.de/wp-content/uploads/fops/leitfaden_kundenzufriedenheitserhebungen.pdf, zuletzt geprüft am 23.10.2013.

Bundesministerium für Verkehr, Bau und Stadtentwicklung: Sicherheit im Eisenbahnbetrieb. Rechtliche Grundlagen.

Burns, W. J.; Slovic, P.: Risk Perception and Behaviors: Anticipating and Responding to Crises. In: *RISK ANALYSIS* 32: 2012 (4), S. 579–582.

Canada (1986): A Report on the Public Perception of Risk. Ottawa: Advisory Committee on Nuclear Safety = Comitâe consultatif de la sãuretâe nuclâeaire.

Carnegie, J.; Deak, D. (2010): Customer Perceptions of Transit Security. Final Report.

Cats, O.; Jenelius, E.: Vulnerability Analysis of Public Transport Networks. A Dynamic Approach and Case Study for Stockholm.

CEIA GmbH (Hg.) (2012): Produktborschüre PMD2 Plus. Metal Detecion & Security Screening Solutions. Eltville. Online verfügbar unter http://www.ceia.net/security/product.aspx?a=PMD2%20Plus, zuletzt geprüft am 21.05.2015.

CEIA GmbH (Hg.) (2012): Produktkatalog LAGs Analysegerät. Metal Detecion & Security Screening Solutions. Eltville. Online verfügbar unter http://www.ceia.net/security/product.aspx?a=EMA%20series, zuletzt geprüft am 21.05.2015.

CEIA GmbH (Hg.) (2012): Produktkatalog PD240. Metal Detecion & Security Screening Solutions. Eltville. Online verfügbar unter http://www.ceia.net/security/product.aspx?a=PD240, zuletzt geprüft am 21.05.2015.

CEIA GmbH (Hg.) (2015): Internetauftritt - EMA serie. Typ B & Typ A LAGs Analysegerät. Online verfügbar unter http://www.ceia.net/security/product.aspx?a=EMA%20series, zuletzt geprüft am 25.03.2015.

CEIA GmbH (Hg.) (2015): Internetauftritt - SAMD. Schuh- und Beinscanner. Online verfügbar unter http://www.ceia.net/security/product.aspx?a=EMA%20series, zuletzt geprüft am 25.03.2015.

Center for Disaster Management and Risk Reduction Technology (Hg.) (2005): Begriffe und Definitionen aus den Risikowissenschaften. Karlsruhe.

Cillis, Francesca de; De Maggio, Maria Carla; Pragliola, Concetta; Setola, Roberto (2013): Analysis of Criminal and Terrorist Related Episodes in Railway Infrastructure Scenarios. In: *Journal of Homeland Security and Emergency Management* 10 (2). DOI: 10.1515/jhsem-2013-0003.

College of Policing (Hg.): The effects of CCTV on Crime. What Works Briefing.

COUNTERACT Consortium (Hg.) (2009): COUNTERACT. Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities.

COUNTERACT Consortium (2009): Crisis Communication Strategy and Guidlines Final Report. In: COUNTERACT Consortium (Hg.): COUNTERACT. Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities, Deliverable 5.

COUNTERACT Consortium (2009): PT4: Generic Guidelines for Conducting Risk Assessment in Public Transport Network. Final Report 4. In: COUNTERACT Consortium (Hg.): COUNTERACT. Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities, Deliverable 3.

Cox, Louis Anthony, Jr. (2008): Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. In: *RISK ANALYSIS* 28 (6), S. 1749–1761. DOI: 10.1111/j.1539-6924.2008.01142.x.

Cox, Louis Anthony, Jr. (2009): Improving Risk-Based Decision Making for Terrorism Applications. In: *RISK ANALYSIS* 29 (3), S. 336–341. DOI: 10.1111/j.1539-6924.2009.01206.x.

Cox, Louis Anthony, Jr. (2009): Risk Analysis of Complex and Uncertain Systems. Boston, MA: Springer US (129).

Cramer, Jürgen (1993): Financial Engineering durch Finanzinnovationen. Univ, Wiesbaden, Münster (Westfalen).

Crime and Social Policy Section (2002): To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime.

CRS Report for Congress: Guarding America: Security Guards and U.S. Critical Infrastructure Protection. Order Code RL32670, Bd. 2004, zuletzt geprüft am 04.02.2014.

D.R. Greenlee (1991): A framework for the objective test and evaluation of explosive detection technology. Proceedings of the First International Symposium on Explosive Detection Technology.

Danish Emergency Management Agency (Hg.): DEMA's Approach to Risk and Vulnerability Analysis for Civil Contingency Planning. Backround paper. Online verfügbar unter http://brs.dk/eng/inspection/contingency_planning/rva_model/Documents/Background_paper_on_DEMAs_approach_to_risk_and_vulnerability_analysis.pdf, zuletzt geprüft am 05.12.2012.

Danish Emergency Management Agency (Hg.) (2006): RVAmodel. DEMA's Model for Risk and Vulnerability Analysis. Introduction and User Guide. Online verfügbar unter http://brs.dk/eng/inspection/contingency_planning/rva_model/Pages/rva_model.aspx, zuletzt geprüft am 04.12.2012.

Danish Emergency Management Agency (Hg.) (2009): Comprehensive Preparedness Planning. 1. Aufl. Birkeroed. Online verfügbar unter http://brs.dk/eng/inspection/contingency_planning/comprehensivepreparednessplanning/Pages/ComprehensivePreparednessPlanning.aspx, zuletzt geprüft am 04.12.2012.

Davis, Paul K.; Henninger, Amy (2007): Analysis, Analysis Practices, and Implications for Modeling and Simulation. Hg. v. National Defense Research Institute. RAND Corporation. Pittsburgh.

Department of Homeland Security (2010): Challenges to Risk Analysis for Homeland Security, S. 44–51.

Der Rat der Europäischen Union (29.04.2004): Richtlinie über die Eisenbahnsicherheit. 2004/49/EG. In: *Amtsblatt der Europäischen Union* (220), S. 16–39.

Der Rat der Europäischen Union (08.12.2008): Richtlinie 2008/114/EG des Rates vom 08. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. In: *Amtsblatt der Europäischen Union* (L 345), S. 75–82.

Deutsche Bahn (2003): Unsere Schienenfahrzeuge im Reginal- und Stadtverkehr. Frankfurt am Main.

Deutsche Bahn (2012): DB Sicherheit - Werte sichern, Kunden schützen. Online verfügbar unter http://www.deutschebahn.com/de/konzern/geschaeftsfelder/dbdienstleistungen_/2228610/sicherheit.html, zuletzt aktualisiert am 08.03.2012, zuletzt geprüft am 18.09.2012.

Deutsche Bahn (2012): Sicherheit im ÖPNV. Ein Produkversprechen an Ihre Kunden. Online verfügbar unter http://www.deutschebahn.com/de/geschaefte/weitereserviceleistungen/, zuletzt aktualisiert am 31.01.2012, zuletzt geprüft am 18.09.2012.

Deutscher Bundestag (27.12.1993): Allgemeines Eisenbahngesetz. AEG, vom 12.09.2012.

Deutscher Bundestag (27.04.1998): Gesetz zur Kontrolle und Transparenz im Unternehmensbereich. KonTraG. In: *Bundesgesetzblatt 745* 1998 (24), S. 786–794.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Deutscher Bundestag (29.07.2009): Luftsicherheitsgesetz. LuftSiG.

DIN 33450: Graphisches Symbol zum Hinweis auf Beobachtung mit optischelektronischen Einrichtungen (Video-Infozeichen.

DIN EN ISO 22301: Sicherheit und Schutz des Gemeinwesens – Aufrechterhaltung der Betriebsfähigkeit.

DIN EN 50126 (VDE 0115), 1999: Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS).

EN 1816, 2002: Definition, Festlegung von Leistungszielen und Messung der Servicequalität.

DIN EN 13816, 2002-07-00: Transport - Logistik und Dienstleistungen Öffentlicher Personenverkehr Definition, Festlegung von Leistungszielen und Messung der Servicequalität.

DIN EN 31010 (VDE 0050-1), 2010: Risikomanagment - Verfahren zur Risikobeurteilung.

DIN ISO 31000:2009, 2011: Risikomanagement – Grundsätze und Leitlinien.

Dillon, Robin L.; Liebe, Robert M.; Bestafka, Thomas (2009): Risk-Based Decision Making for Terrorism Applications. In: *RISK ANALYSIS* 29 (3), S. 321–335. DOI: 10.1111/j.1539-6924.2008.01196.x.

Dittmann, Jörg (2005): Entwicklung der Kriminalitätseinstellungen in Deutschland. Eine Zeitreihenanalyse anhand allgemeiner Bevölkerungsumfragen. Working Paper Nr. 468. Deutsches Institut für Wirtschaftsforschung e.V. Berlin.

Dittmann, Jörg (2005): Kriminalitätsfurcht sinkt in Deutschland entgegen dem EU-Trend. In: GESIS - Leibniz-Institut für Sozialwissenschaften, Zentrum für Sozialindikatorenforschung (Hg.): Informationsdienst Soziale Indikatoren. Sozialberichterstattung, gesellschaftliche Trends, aktuelle Informationen, 34 (1). Mannheim: GESIS, S. 6–9.

Döring, Holger (2010): Sicherheit im öffentlichen Personenverkehr. 1. Aufl. Stuttgart: Steinbeis-Ed.

Dräger Safety AG & Co. KGaA: Funktionale Sicherheit und Gaswarnsysteme. Safety Integrity Level - SIL. Lübeck, zuletzt geprüft am 12.02.2014.

Duden (2013): Online Wörterbuch. Stichwort: Sicherheit. Online verfügbar unter http://www.duden.de/rechtschreibung/Sicherheit, zuletzt geprüft am 04.10.2013.

Duden (2013): Online Wörterbuch. Stichwort: Drohne. Online verfügbar unter http://www.duden.de/rechtschreibung/Drohne, zuletzt geprüft am 29.07.2013.

Einarsson, Stefán; Rausand, Marvin (1998): An Approach to Vulnerability Analysis of Complex Industrial Systems. In: *RISK ANALYSIS* 18 (5).

Elias, Bartholomew (2010): Airport and aviation security. U.S. policy and strategy in the age of global terrorism. Boca Raton, FL: CRC Press.

Engelmann, Peter A. (1979): On the Methodology of Cost Benefit Analysis and Risk Perception. Unter Mitarbeit von Ortwin Renn. Stuttgart: Universitätsbibliothek der Universität Stuttgart. Online verfügbar unter http://nbn-resolving.de/urn:nbn:de:bsz:93-opus-54488.

ENISA (Hg.) (2007): Methodology for evaluating usage and comparison of risk assessment and risk management items. 1. Aufl. ENISA ad hoc working group on risk assessment and risk management.

Ezell, Barry Charles; Bennett, Steven P.; Winterfeldt, Detlof von; Sokolowski, John; Collins, Andrew J. (2010): Probabilistic Risk Analysis and Terrorism Risk. In: *RISK ANALYSIS* 30 (4), S. 575–589. DOI: 10.1111/j.1539-6924.2010.01401.x.

Fachhochschule Köln (FH) (Hg.) (2012): Bilder ÖPNV. Unter Mitarbeit von Florian Brauner, Christian Bentler und Christian Baumgarten. Köln.

Federal Ministry of the Interior (2008): Protecting Critical Infrastructures – Risk and Crisis Management. A guide for companies and government authorities. Berlin. Online verfügbar unter http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile, zuletzt geprüft am 13.06.2014.

FEMA (Hg.) (2005): Risk Assessment. A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings (452).

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

FH KÖLN - IRG, 27. Mai. 2013. Dokumentation Workshop. ÖPV Vignetten. RIKOV Projektintern. Köln.

FH KÖLN - IRG, 17. Okt. 2013. Analyse potenzieller Sicherheitsmaßnahmen. Bericht L1.4. RIKOV Projekt. Köln.

FH KÖLN - IRG, 31. Jan. 2014. Methode zur Bestimmung der Vulnerabilität eines schienengebundenen ÖPV-Systems. Interner Projektbeitrag zum AP 4.1. RIKOV Projekt. Köln.

FH KÖLN - IRG, 31. Jan. 2014. Methode zur Bestimmung der Wirkung von Sicherheitsmaßnahmen. Interner Projektbeitrag zum AP5.2. RIKOV Projekt. Köln.

FH KÖLN - IRG, 31. Jan. 2014. Prozessmodellierung der Operationspläne. Bericht L2.1. RIKOV Projekt. Köln.

FH KÖLN - IRG, 31. Jan. 2015. Konzeption Realübung - Planspiel - (Übungsphase2). Interner Projektbeitrag zum AP 7.2. RIKOV Projekt. Köln.

FH KÖLN - IRG, 31. Aug. 2015. Integration und Test. Bericht L7.2. RIKOV Projekt. Köln.

Fiedler, Joachim (2005): Bahnwesen. Planung, Bau und Betrieb von Eisenbahnen, S-, U-, Stadt- und Strassenbahnen. 5., neubearb. und erw. Aufl. [Düsseldorf]: Werner (Werner-Ingenieur-Texte, WIT).

finanzen.net GmbH (2013): EURO - SCHWEIZER FRANKEN. historische Kurse. Karsruhe. Online verfügbar unter http://www.finanzen.net/devisen/euro-schweizer_franken-kurs/historisch, zuletzt geprüft am 17.01.2013.

Flammini, Francesco (2012): Critical Infrastructure Security. Assessment, Prevention, Detection, Response. Southampton: WIT Press (Information & communication technologies).

Fleischhack, Hans (2013): Museum of Drones. Search and Rescue vs. Search and Destroy. Department für Informatik - Theoretische Informatik der Carl von Ossietzky Universität Oldenburg. Oldenburg. Online verfügbar unter http://www.informatik.uni-oldenburg.de/~iug08/snd/definition.html, zuletzt geprüft am 29.07.2013.

Fletcher, KC. (2011): Aviation Security. Case for Risk-Based Passenger Screening. Hg. v. Naval Postgraduate School. Monterey.

FLIR Systems (Hg.) (2013): FLIR Detection. Fido X3 Capabilities. Wilsonville.

Floeting, Holger (2006): Sicherheitstechnologien und neue urbane Sicherheitsregimes. Wien.

Focus online (Hg.) (2011): Ständig Fehlalarm beim Körperscanner. Flugverkehr. dpa. Online verfügbar unter http://www.focus.de/politik/deutschland/flugverkehr-zeitung-staendiger-fehlalarm-beim-koerperscanner_aid_650842.html, zuletzt geprüft am 13.01.2013.

Frank, Thomas (2008): 10 airports install body scanners. USA Today. Baltimore. Online verfügbar unter http://usatoday30.usatoday.com/travel/flights/2008-06-05-bodyscan_N.htm, zuletzt aktualisiert am 06.06.2008, zuletzt geprüft am 10.09.2013.

Franz, Robert (2013): Teil 2: Drohnen zur Überwachung: Im Bann des fliegenden Auges. WDR.de. Köln. Online verfügbar unter http://www1.wdr.de/themen/politik/drohnen144.html, zuletzt aktualisiert am 18.06.2013, zuletzt geprüft am 16.09.2013.

Frevel, Bernhard; Schulze, Verena: Public Safety and Security Governance. Pluralisierung und Vernetzung in der Sicherheitspolitik. KoSiPol-Kooperative Sicherheitspolitik in der Stadt, zuletzt geprüft am 19.07.2012.

Frey, Peter (2008): FBI will künftig sogar Hirnströme scannen. Kampf gegen den Terrorismus. Hg. v. Springer AG. Die Welt. Online verfügbar unter http://www.welt.de/wissenschaft/article1541476/FBI-will-kuenftig-sogar-Hirnstroeme-scannen.html, zuletzt aktualisiert am 11.01.2008, zuletzt geprüft am 12.09.2013.

Furedi, Frank (2005): Culture of fear. Risk-taking and the morality of low expectation. London: Continuum.

Fyhri, Aslak; Backer-Grøndahl, Agathe (2012): Personality and risk perception in transport, zuletzt geprüft am 28.06.2012.

Ganz, Christian (unbekannt): Risikoanalysen im internationalen Vergleich. Promotion. Bergische Universität Wuppertal, Wuppertal. Abteilung D - Maschinenbau / Werkstofftechnik.

Gerhold, Lars (2009): Umgang mit makrosozialer Unsicherheit. Zur individuellen Wahrnehmung und Bewältigung gesellschaftlich-politischer Phänomene. Lengerich: Pabst Science Publishers. Online verfügbar unter http://www.wiso-net.de/webcgi?START=A60&DOKV_DB=PBST,APBS&DOKV_NO=9783899675573290&DOKV_HS=0&PP=1.

GESIS - Leibniz-Institut für Sozialwissenschaften, Zentrum für Sozialindikatorenforschung (Hg.) (2005): Informationsdienst Soziale Indikatoren. Sozialberichterstattung, gesellschaftliche Trends, aktuelle Informationen. GESIS - Leibniz-Institut für Sozialwissenschaften. Mannheim: GESIS.

Giannopoulos, Georgios; Filippini, Roberto; Schimmer, Muriel (2012): Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art. EUR 25286 EN. Hg. v. JRC European Commission. Institute for the Protection and Security of the Citizen. Italy.

Golz, Hans-Georg (2004): Bürgerrechte und Innere Sicherheit. In: *Aus Politik und Zeitgeschichte* 2004 (B44). Online verfügbar unter http://www.bpb.de/apuz/28012/editorial, zuletzt geprüft am 09.12.2012.

Government of Canada (o.J.): Building Resilience Against Terrorism. Canda´s Counter-Terrorism Strategy.

Grethe, Christian (Hg.) (2010): Restrukturierung von Krisenunternehmen durch Private-Equity-Gesellschaften. Wiesbaden: Gabler.

Grethe, Christian (2010): Unternehmenskrisen. In: Christian Grethe (Hg.): Restrukturierung von Krisenunternehmen durch Private-Equity-Gesellschaften. Wiesbaden: Gabler, S. 13–44.

Guerrero, Peter (2002): Mass Transit: Challenges in Securing Transit Systems. GAO - United States General Accounting Office, zuletzt geprüft am 02.08.2012.

Haimes, Y. Y.; Lambert, J. H.; Kaplan, S.; Pikus, I.; Leung, F. (2002): A Risk Assessment Methodology for Critical Transportation Infrastructure. Final Contract Report. Hg. v. Virginia Transportation Research Council. Charlottesville.

Haller, Ludger (2003): Risikowahrnehmung und Risikoeinschätzung. Hamburg: Kovac (Schriftenreihe Schriften zur Arbeits-, Betriebs- und Organisationspsychologie, 3).

Harms, J. Menno Harms: Sicherheitsgewinn mit technologischen Innovationen.

Harpes, Carlo (2010): Risk prediction and information sharing with linked but competing operators. MICIE Workshop. Luxemburg Workshop. Luxembourg-Kirchberg, 20.05.2010.

Hausken, Kjell (2010): Defense and Attack of Complex and Dependent Systems (1), zuletzt geprüft am 02.07.2012.

Heads of the European Radiological protection Competent Authorities (2010): Facts and d figures concerning the use Full body scanners using X-Rays for security reason. presented by HERCA Working Group 2. Oslo, zuletzt geprüft am 12.02.2014.

Heesen, Jessica (2011): Herrschaft durch Sicherheit. XXII. Deutscher Kongress für Philosophie. München, 11.09.2011.

Hempel, Leon (2003): Verdrängen statt Vorbeugen. Telepolis. Online verfügbar unter http://www.heise.de/tp/artikel/13/13928/1.html, zuletzt geprüft am 09.12.2012.

Hempel, Leon; Meier, Jana; Rau, Heike; Steltner, Claudia; Vedder, Dagny (2011): Gemeinsamer Abschlussbericht 2011. Test und Evaluation ausgewählter Maßnahmen. Subjektive Sicherheit im Öffentlichen Personennahverkehr. Hg. v. SuSiteam. Bundesministerium für Wirtschaft und Technologie. Berlin.

Hempel, Leon; Töpfer, Eric (2004 (Übersetzung 2007)): URBANEYE Abschlussbericht. Videoüberwachung in Europa. Arbeitspapier Nr. 15. Hg. v. Zentrum für Technik und Gesellschaft. Technische Universität Berlin, zuletzt geprüft am 02.12.2013.

Herbst, Sandra (2011): Untersuchungen zum Viktimisierungs-Furcht-Paradoxon. Ein empirischer Beitrag zur Aufklärung des "Paradoxons" anhand von Vorsicht und Vulnerabilität im Alter. 1. Aufl. Baden-Baden: Nomos (Interdisziplinäre Beiträge zur kriminologischen Forschung, 38).

Hess, Bettina (2012): Neue Lebensretter in der U-Bahn. MVG-Information für die Medien. Stadtwerke München GmbH MVG. München. Online verfügbar unter http://www.mvg-mobil.de/presse/2012-12-14_mvg-pressemeldung.pdf, zuletzt aktualisiert am 14.12.2012, zuletzt geprüft am 12.09.2013.

Hess, Josef Th. (2008): Schutzziele im Umgang mit Naturrisiken in der Schweiz. Dissertation ETH, Nr. 17956. Eidgenössische Technische Hochschule Zürich, Zürich. Online verfügbar unter http://e-collection.library.ethz.ch/eserv/eth:31113/eth-31113-02.pdf, zuletzt geprüft am 11.12.2012.

Hill, Michael (2010): NEPA at the Limits of Risk Assessment: Whether to Discuss a Potential Terrorist Attack on a Nuclear Power Plant Under the National Environment Policy Act. In: *Fordham Law Review* 78 (6), 10.

Hofmann, Thorsten; Röhrich, Raimund (2006): Krisenmanagement als Vorstandsaufgabe. Zur Bedeutung der Krisenkommunikation im Rahmen der Prävention und Bewältigung von Krisen. In: *KSI* 2006 (05), S. 167–190. Online verfügbar unter http://www.ksidigital.de/ce/krisenmanagement-als-vorstandsaufgabe/detail.html.

Hokstad, Per; Utne, Ingrid B.; Vatn, Jørn (2012): Risk and Interdependencies in Critical Infrastructures. A Guideline for Analysis. New York: Springer.

Horbach, Matthias (Hg.) (2013): Informatik 2013 - Informatik angepasst an Mensch, Organisation und Umwelt; Tagung vom 16.-20. September 2013 in Koblenz. Bonn: Ges. für Informatik (GI-Edition : Proceedings, 220).

Howitt, Arnold M.; Makler, Jonathan (2005): Protecting America´s Road Transit Against Terrorism. In: *The Brookings Institution Series on Transportation Reform* April 2005.

Huber, Florian (2000): Wahrnehmung von Aufgaben im Bereich der Gefahrenabwehr durch das Sicherheits- und Bewachungsgewerbe: Duncker & Humblot. Online verfügbar unter http://katalog.ub.uni-heidelberg.de/cgi-bin/titel.cgi?katkey=65159538.

Hummelmeier, Andreas (2012): Diskussion über effizientere Videoüberwachung (tagesschau). ARD, 17.12.2012. Online verfügbar unter http://www.tagesschau.de/multimedia/video/video1232248.html, zuletzt geprüft am 17.12.2012.

Hummelsheim, Dina (2009): Schützt soziale Sicherheit vor Kriminalitätsfurcht? Eine ländervergleichende Untersuchung zum Einfluss nationaler Wohlfahrtspolitiken auf kriminalitätsbezogene Unsicherheitsgefühle. Max-Planck-Institut Freiburg, 30.10.2009.

Hutter, Reinhard; Blobner, Christian (2013): MEASURING THE VALUES OF SECURITY. In: Michael Lauster (Hg.): 8th Future Security Security Research Conference. Proceedings. Future Security 2013. Berlin, 17-19.09.2013. Fraunhofer-Verbund Verteidigungs- und Sicherheitsforschung; Future Security Research Conference. Stuttgart: Fraunhofer Verl, S. 424–432.

I.G.T. Informationsgesellschaft Technik mbH (Hg.) (2009): Präventiver Einsatz von Videotechnik. sicherheit.info. Online verfügbar unter http://www.sicherheit.info/SI/cms.nsf/si.ArticlesByDocID/2103520?Open, zuletzt geprüft am 16.11.2012.

InnovationsAllianz der NRW-Hochschulen e.V. (2013): Saftey & Security. Düsseldorf.

Institut Wohnen und Umwelt GmbH (2004): Subjektives Sicherheitsempfinden im Personennahverkehr mit Linienbussen, U-Bahnen und Stadtbahnen. Auszug aus dem Abschlussbericht: Zusammenfassung und wichtigste Ergebnisse. In: SuSiteam (Hg.): Subjektives Sicherheitsempfinden im Personenverkehr mit Linienbussen, U-Bahnen und Stadtbahnen (SuSi-PLUS). Forschungsverbundvorhaben SuSi-Plus. Unter Mitarbeit von Institut Wohnen und Umwelt GmbH. Darmstadt.

International Association of Public Transport (2007): Public Transport Security in Stations: Prevention, Responding and Recovering in the Face Terrorism: UITP. Online verfügbar unter http://books.google.de/books?id=5vQvSQAACAAJ.

ISO 31000, 01.09.2008: Risk management— Principles and guidelines on implementation.

International Strategy for Disaster Reduction (Hg.) (2005): Hyogo Framework for Action 2005-201. Building the Resilience of Nations and Communities to Disasters. World Conference on Disaster Reduction, 18-22 January 2005,. Kobe, Japan. Online verfügbar unter www.unisdr.org/wcdr, zuletzt geprüft am 04.12.2013.

Jahn, Harald A. (2010): Die Zukunft der Städte. Die französische Strassenbahn und die Wiedergeburt des urbanen Raumes. Wien: Phoibos-Verl.

Jenkins, Brian M.; Gersten, Larry N. (2001): Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices. An Executive Overview. San Jose.

Jenkins, Brian M.; Gersten, Larry N. (2001): Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices. San Jose.

John-Koch, Monika (2010): Strategische Meilensteine. Kritische Infrasturkturen im Blick. In: *Bevölkerungsschutz* 2010 (3), S. 2–6.

Johnson, Branden B. (Hg.) (1987): The Social and Cultural Construction of Risk. Essays on Risk Selection and Perception. Dordrecht: Reidel (Technology, risk, and society).

Jungbluth, F. (Hg.) (2005): Recht und Haftung für technische Manager (NOCH NICHT GEFUNDEN!). Grundlagen, Aufbau und Methoden eines effektiven Notfallmanagements. Euroforum Verlag. Düsseldorf.

Kalscheuer, Britta: Grenzen der Technik. Kameras alleine verhindern keine Straftaten im ÖPNV. In: *W&S* 2009 (6), S. 14–15.

Kaschner, Holger (2008): Neues Risiko Terrorismus. Entgrenzung, Umgangsmöglichkeiten, Alternativen. 1. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften / GWV Fachverlage, Wiesbaden.

Killias, Martin; Clerici, Christian (200): Different Measures of Vulnerability in their Relation to Different Dimensions of Fear of Crime. Hg. v. ISTD. The Centre for Crime and Justice Studies.

Kleinschmidt, Helmut; Kuhlmey, Marcel (2009): Verbesserung der subjektiven Sicherheit im öffentlichen Personennahverkehr. Beiträge aus dem Fachbereich Polizei und Sicherheitsmanagement Nr. 03/2009. Hg. v. Dirk Fleischer. Dekan Fachbereich Polizei und Sicherheitsmanagement. Berlin, zuletzt geprüft am 28.10.2013.

Klibi, Walid; Martel, Alain (2012): Scenario-Based Supply Chain Network Risk Modeling. In: *European Journal of Operational Research. DOI:* 10.1016/j.ejor.2012.06.027.

Klitou, Demetrius (2008): Backscatter body scanners – A strip search by other means. In: *Computer Law & Security Review* 24 (4), S. 316–325. DOI: 10.1016/j.clsr.2008.05.005.

Ko, Teddy (o.J.): A Survey on Behavior Analysis in Video Surveillance for Homeland Security Applications. Raytheon Company.

Koch, Susanne (2010): Einführung in das Prozessmanagement von Geschäftsprozessen. Six Sigma, Kaizen und TQM. 1. Aufl. Berlin: Springer.

Koch, Wolfgang (2011): Hannover-Messe: Fraunhofer-Institut kann Terroristen erschnüffeln. Pressemitteilung 03.04.2011. Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE. Online verfügbar unter http://www.fkie.fraunhofer.de/de/presse/pressemitteilungen-2011/11-04-03-terroristen-erschnueffeln.html, zuletzt aktualisiert am 03.04.2011, zuletzt geprüft am 11.09.2013.

Köhn, Anne; Bornewasser, Manfred (2012): Kooperative Sicherheitspolitik in der Stadt. Subjektives Sicherheitsempfinden. Working Paper Nr.9. Hg. v. Bernhard Frevel. Münster (Westfalen), zuletzt geprüft am 28.10.2013.

Kölner Verkehrs Betriebe AG (Hg.) (2012): Die Zentrale Leitstelle. Das Herz der KVB. Köln.

Kölner Verkehrs Betriebe AG (2012): Sicherheitseinrichtungen in den Fahrzeugen und an den U-Bahn-Haltestellen. Köln. Online verfügbar unter http://www.kvb-koeln.de/german/fahrplan/helfen.html, zuletzt geprüft am 16.10.2012.

KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN (12.12.2006): Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen. Fundstelle: Brüssel.

Kompetenzzentrum kritische Infrastrukturen e.V. (Hg.): Imagebroschüre. Berlin.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Kravets, David (2011): Airport 'Nude' Body Scanners: Are They Effective? Condé Nast. New York. Online verfügbar unter http://www.wired.com/threatlevel/2011/03/scanners-part3/, zuletzt aktualisiert am 03.08.2011, zuletzt geprüft am 11.02.2014.

Krystek, Ulrich (2002): Unternehmenskrisen: Vermeidung und Bewältigung. In: Peter M. Pastors (Hg.): Risiken des Unternehmens - vorbeugen und meistern. München und Mering: Rainer Hampp Verlag, S. 87–134.

L-3 Communications Security and Detection Systems (2014): Advanced Personnel Screening. Internetauftritt inklusive Datenblätter. Online verfügbar unter http://www.sds.l-3com.com/products/advancedimagingtech.htm, zuletzt geprüft am 12.02.2014.

Landoll, Douglas J. (2006): The Security Risk Assessment Handbook. A Complete Guide for Performing Security Risk Assessments. Boca Raton, FL: Auerbach Publications.

Lauster, Michael (Hg.) (2013): 8th Future Security Security Research Conference. Proceedings. Future Security 2013. Berlin, 17-19.09.2013. Fraunhofer-Verbund Verteidigungs- und Sicherheitsforschung; Future Security Research Conference. Stuttgart: Fraunhofer Verl, zuletzt geprüft am 21.11.2013.

Lauwe, Peter (2012): Schutzkonzepte Kritischer Infrastrukturen im Bevölkerungsschutz. Ziele, Zielgruppen, Bestandteile und Umsetzung im BBK. Bonn (Wissenschaftsforum, 11).

Lenz, Susanne (2009): Vulnerabilität Kritischer Infrastrukturen. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Leson, Joel (2005): Assessing and Managing the Terrorism Threat. Hg. v. Bureau of Justice Assistance. Washington (NCJ 210680). Online verfügbar unter www.ncjrs.gov/pdffiles1/bja/210680.pdf, zuletzt geprüft am 04.01.2013.

Leucker, Roland (2012): Mobilität - ein unkalkulierbares Risiko? STUVA e.V. BmBF Innovationsforum Zivile Sicherheit, 17.04.2012, zuletzt geprüft am 22.05.2012.

Leven, J.; Langescheid, T.; Gerlach, J.: Sicherheitskonzepte im ÖPNV. In: *DER NAHVERKEHR* 2010 (4), S. 14–19.

Linkov, Igor; Wenning, R. J.; Kiker, Gregory Alan (2007): Managing Critical Infrastructure Risks. Decision tools and applications for port security. Dordrecht, the Netherlands: Springer Verlag (NATO science for peace and security series. Series C, Environmental security).

Lipinski, Klaus (2013): SCADA (Supervisory Control and Data Acquisition). DATACOM Buchverlag GmbH. Online verfügbar unter http://www.itwissen.info/definition/lexikon/supervisory-control-and-data-aquisition-SCADA.html, zuletzt geprüft am 29.07.2013.

Liu, Chunlin; Tan, Chong-Kuan; Fang, Yea-Saen; Lok, Tat-Seng (2012): The Security Risk Assessment Methodology. In: *Procedia Engineering* 43, S. 600–609. DOI: 10.1016/j.proeng.2012.08.106.

Lohmann, Günter; Rölle, Daniel (2004): Subjektive Sicherheit der Fahrgäste im ÖPNV. Eine Fahrgastbefragung in Mannheim zur Bestimmung des subjektiven Sicherheitsgefühls an der Haltestelle Hauptbahnhof. Band 6. In: SuSiteam (Hg.): Subjektives Sicherheitsempfinden im Personenverkehr mit Linienbussen, U-Bahnen und Stadtbahnen (SuSi-PLUS). Forschungsverbundvorhaben SuSi-Plus. Unter Mitarbeit von Institut Wohnen und Umwelt GmbH. Darmstadt.

Lohmann, Günter; Rölle, Daniel (2004): Videoüberwachung in Fahrzeugen und an Haltestellen des ÖPNV. - Akzeptanz und Sicherheitsgewinn -. In: SuSiteam (Hg.): Subjektives Sicherheitsempfinden im Personenverkehr mit Linienbussen, U-Bahnen und Stadtbahnen (SuSi-PLUS). Forschungsverbundvorhaben SuSi-Plus. Unter Mitarbeit von Institut Wohnen und Umwelt GmbH. Darmstadt.

Lorei, Clemens (o.J.): Ergebnisse einer Bürgerbefragung zur Akzeptanz von polizeilichen Kontroll- und Eigensicherungsmaßnahmen. Redaktion Polizei und Wissenschaft. Frankfurt.

Lösel, Friedrich (2005): Wirksamkeit der Videoüberwachung. Hg. v. Stiftung Deutsches Forum für Kriminalprävention. Bonn.

Lutz, M.; Exner, U. (2011): Der Pannenscanner – viel Kleidung, viel Alarm. Die Welt. Berlin. Online verfügbar unter http://www.welt.de/politik/deutschland/article13516870/Der-Pannenscanner-viel-Kleidung-viel-Alarm.html, zuletzt aktualisiert am 31.07.2011, zuletzt geprüft am 11.02.2014.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Macaulay, Tyson (2009): Critical Infrastructure. Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies. Boca Raton, FL: CRC Press.

MacKinnon, Lachlan; Bacon, Liz; Gan, Diane; Loukas, Georgios; Chadwick, David; Frangiskatos, Dimitrios (o.J.): Cyber Security Countermeasures to Combat Cyber Terrorism, zuletzt geprüft am 26.09.2013.

Maertens, Julia (2013): Wirkmodell eines terroristischen Anschlags. Airbus Space and Defence. Friedrichshafen.

Malyska, Arndt (2010): Das integrierte Sicherheitskonzept der Hamburger Hochbahn AG. Hamburger Hochbahn-Wache GmbH. Hamburg, 20.10.2010.

Martonosi, S. E.; Barnett, A. (2006): How effective is security screening of airline passengers? In: *Interfaces* 36, S. 545–552.

Martz, Harry F.; Johnson, Mark E. (1987): Risk Analysis of Terrorist Attacks. In: *RISK ANALYSIS* 7 (1).

Masse, Todd; O'Neil, Siobhan; Rollins, John (2007): The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress.

Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. (Hg.) (2011): Barometer Sicherheit Deutschland. Module. Online verfügbar unter http://basid.mpicc.de/basid/de/pub/projekt/module.htm, zuletzt aktualisiert am 30.11.2011, zuletzt geprüft am 24.09.2013.

May, Thorsten (2009): Mit der THz-Technologie zu neuer Sicherheit. Forschung & Entwicklung. In: *Photonik* (2/2009). Online verfügbar unter http://www.photonik.de/index.php?id=5&artid=3221&np=2, zuletzt geprüft am 10.09.2013.

Menski, Ute; Gardemann, Joachim (2008): Auswirkungen des Ausfalls kritischer Infrastrukturen auf den Ernährungssektor am Beispiel des Stromausfalls im Münsterland im Herbst 2005. Empirische Untersuchung im Auftrag der Bundesanstelt für Landwirtschaft und Ernährung. Unter Mitarbeit von Gustm Sarah, Eva Holtmann, Linda Quartey und Claudia Wilken. Fachhochschule Münster, Kompetenzzentrum Humanitäre Hilfe; Fachhochschule Münster, Fachbereich Oecotrophologie. Münster.

Merz, Mirjam (2011): Entwicklung einer indikatorenbasierten Methodik zur Vulnerabilitätsanalyse für die Bewertung von Risiken in der industriellen Produktion. Dissertation. KIT.

Mineta Transportation Institute (2012): Annual Report 2011-2012.

Mironenko, Olga (2011): Body scanners versus privacy and data protection. In: *Computer Law & Security Review* 27 (3), S. 232–244. DOI: 10.1016/j.clsr.2011.03.006.

Moechel, Erich (2010): Die neue Generation der Nacktscanner. ORF. Online verfügbar unter http://www.fuzo-archiv.at/artikel/1635643v2, zuletzt aktualisiert am 04.01.2011, zuletzt geprüft am 10.09.2013.

Moore, David A. (2006): Application of the API/NPRA SVA methodology to transportation security issues☆ (1-2), zuletzt geprüft am 28.06.2012.

Morral, Andrew R.; Price, Carter C.; Ortiz, David S.; Wilson, Bradley; LaTourrette, Tom; Mobley, Blake W. et al. (2012): Modeling Terrorism Risk to the Air Transportation System. An Independent Assessment of TSA's Risk Management Analysis Tool and Associated Methods. Hg. v. National Defense Research Institute. RAND Corporation. Pittsburgh.

Münchner Verkehr- und Tarifverbund GmbH (2000): MVV-Kundenbarometer-Untersuchungen im Jahres-Vergleich. Der MVV aus der Sicht seiner Fahrgäste 1999/2000 und 1997/1998. In: *Daten, Analysen, Perspektiven* (6).

Münchner Verkehrsgesellschaft mbH (MVG) (2010): U-Bahnbetriebszentrale. Operativer Kern der Münchner U-Bahn. München.

Nagenborg, Michael (2011): Zum Verhälthis von "sicherheit" und "(negativer) Freiheit" am Beispiel von Isaiah Berlin's Two Concepts of Liberty (1969). XXII. Deutscher Kongress für Philosophie. München, 11.09.2011.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

National Center for Transit Research: Florida Public Transportation Anti-Terrorism Resource Guide.

NATO (2007): NATO Architecture Framework. Version 3.

NATO (2007): NATO Architecture Framework. Version 3. Chapter 3 NNEC Architecture Concepts and Elements.

Neubecker, Karl Adolf (2013): Szenarien für RIKOV. RiKoV Zwischenbericht. Ein Katalog möglicher Szenarien.

Neumayr, Martina (Hg.) (2010): Risikoprophylaxe im Unternehmensalltag. Köln: Bank-Verlag.

Nicholas G. Paulter, Jr. (2003): Walk-Through Metal Detectors for Use in Concealed Weapon and Contraband Detection. NIJ Standard–0601.02. Hg. v. National Institute of Justice. National Institute of Standards and Technology. Washington DC, zuletzt geprüft am 12.02.2014.

Niggl, Peter (2009): Sicherheit bahn-t sich ihren Weg. In: *Security inside* 2009 (4), S. 8–11, zuletzt geprüft am 09.12.2012.

Niklas, Cornelia (2002): Mehr Entscheidungssicherheit mit der Nutzwertanalyse. In: *ProjektMagazin* (23), zuletzt geprüft am 16.12.2012.

Nordfjærn, Trond; Rundmo, Torbjørn (2010): Differences in risk perception, priorities, worry and demand for risk mitigation in transport among Norwegians in 2004 and 2008 (3), zuletzt geprüft am 28.06.2012.

OECD / OCDE (2002): ECMT Round Tables : Vandalism, Terrorism and Security in Urban Public Passenger Transport, zuletzt geprüft am 11.07.2012.

O'Hare, M.: The Social and Cultural Construction of Risk: Essays on Risk Perception.

Oswald, Michelle; Treat, Christian (3): Assessing Public Transportation Vulnerability to Sea Level Rise. A Case Study Application. In: *Journal of Public Transportation* 16 (2013).

Panzieri, S. (Hg.) (2010): MICIE. Tool für systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures. MICIE delivrable 3.2.1.

Pastors, Peter M. (Hg.) (2002): Risiken des Unternehmens - vorbeugen und meistern. München und Mering: Rainer Hampp Verlag.

Paul, Matthias; Hans-Jörg, von Mettenheim; Breitner, Michael H. (2008): Akzeptanz von Sicherheitsmaßnahmen: Modellierung, Numerische Simulation und Optimierung. IWI Diskussionsbeiträge # 28 (16. Oktober 2008). Hannover, zuletzt geprüft am 28.10.2013.

Pechlaner; Glaeßer (Hg.) (2005): Risiko und Gefahr im Tourismus. Berlin: Schmidt.

Peter, Bettina; Grolms, Wolfgang; Wellige, Wolfgang (2012): Sicherheit auf der ganzen Linie - Einrichtungen für den Notfal. Münchner Verkehrsgesellschaft mbH (MVG). München. Online verfügbar unter http://www.mvg-mobil.de/service/sicherheit.html, zuletzt geprüft am 27.09.2013.

Pickl, Stefan (2012): Gesamtvorhabenbeschreibung zum Verbundprojekt Risiken und Kosten der terroristischen Bedrohungen des schienengebundenen ÖPV: Eine Planungslösung für die ökonomische und organisatorische Optimierung präventiver und abwehrender Maßnahmen. RiKoV. Vorhabensbeschreibung. Universität der Bundeswehr, München. Professur für Operations Resaerch, zuletzt geprüft am 02.09.2013.

Pickl, Stefan; Loechel, Alexander; Neubecker, Karl; Schmitz, Walter (2009): An Economic Impact Analysis on Terrorist Attacks against Public Transport Networks. In: *NEAT "Network for the Economic Analysis of Terrorism"*.

Pidgeon, Nick (2003): The Social Amplification of Risk. Cambridge: Cambridge University Press.

Policastro, Anthony J.; Gordon, Susanna P. (1999): The Use Of Technology In Preparing Subway Systems For Chemical/Biological Terrorism, zuletzt geprüft am 09.12.2012.

Potoglou, Dimitris; Robinson, Neil; Kim, Chong W.; Burge, Peter; Warnes, Richard (2010): Quantifying individuals' trade-offs between privacy, liberty and security: The case of rail travel in UK 44 (3), S. 169–181. DOI: 10.1016/j.tra.2009.12.006.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Public Safety Canada (Hg.) (2009): National Strategy for Critical Infrastructure. Ottawa, zuletzt geprüft am 11.12.2012.

Public Safety Canada (Hg.) (2010): Risk Management Guide for Critical Infrastructure Sectors. 1.0. Aufl. Online verfügbar unter http://www.publicsafety.gc.ca/prg/ns/ci/_fl/rmgcis-ggrsie-eng.pdf, zuletzt geprüft am 04.01.2013.

Public Safety Canada (Hg.) (2012): All Hazards Risk Assessment. Methodology Guidelines. Ottawa. Online verfügbar unter http://www.publicsafety.gc.ca/prg/em/emp/2012-ahra/_fl/2012-ahra-eng.pdf, zuletzt geprüft am 04.01.2013.

R+V Versicherung: Die Ängste der Deutschen 2011. Studie.

Ragnitz, Joachim (2012): Regionale Lohnunterschiede in Deutschland. In: *ifo Dresden berichtet* (2), S. 26–32. Online verfügbar unter http://www.cesifo-group.de/portal/pls/portal/docs/1/1214460.PDF, zuletzt geprüft am 17.01.2013.

Rapiscansystems (2014): Rapiscan Secure 1000 DP. Comprehensive people screening for high security applications. Online verfügbar unter http://www.rapiscansystems.com/en/products/ps/productsrapiscan_secure_1000_dual_pose, zuletzt geprüft am 12.02.2014.

Reichenbach, Gerold; Wolff, Hartfrid; Göbel, Ralf; Stokar von Neuforn, Silke (Hg.) (2008): Risikien und Herausforderungen für die öffentliche Sicherheit in Deutschland. Szenarien und Leitfragen. 1. Aufl. Berlin. Online verfügbar unter http://www.zukunftsforum-oeffentliche-sicherheit.de/downloads/Gruenbuch_Zukunftsforum.pdf, zuletzt geprüft am 04.01.2013.

Reinkober, Norbert (2011): VeRSiert - Sicherheit im ÖPNV bei Großveranstaltungen. Vernetzung von Verkehrsunternehmen, Einsatzkräften, Veranstaltern und Fahrgästen des ÖPNV. Kiel: Buchwerft-Verl.

Renn, Ortwin (1984): Psychological and sociological approaches to study risk perception. Unter Mitarbeit von Elisabeth Swaton. Stuttgart: Universitätsbibliothek der Universität Stuttgart. Online verfügbar unter http://nbn-resolving.de/urn:nbn:de:bsz:93-opus-53824.

Renn, Ortwin (Hg.) (2000): Cross cultural risk perception. A survey of empirical studies. Dordrecht: Kluwer Academic Publ (Technology, risk, and society).

Reuter, Christian; Ludwig, Thomas (2013): Anforderungen und technische Konzepte der Krisenkommunikation bei Stromausfall. In: Matthias Horbach (Hg.): Informatik 2013 - Informatik angepasst an Mensch, Organisation und Umwelt; Tagung vom 16.-20. September 2013 in Koblenz. Bonn: Ges. für Informatik (GI-Edition : Proceedings, 220), S. 1604–1618.

Rölle, Daniel (2004): Sicherheitsgefühle Im ÖPNV - die Perspektive der Verkehrsunternehmen. Dokument aus der Internetdokumentation Deutscher Präventionstag. Hg. v. Hans-Jürgen Kerner und Erich Marks. Deutsche Stiftung für Verbrechensverhütung und Straffälligenhilfe. Hannover, zuletzt geprüft am 28.10.2013.

Rölle, Daniel; Flade, Antje (2004): Theorien und Modelle zur Erklärung von Unsicherheitsgefühlen im öffentlichen Raum. Band 2. In: SuSiteam (Hg.): Subjektives Sicherheitsempfinden im Personenverkehr mit Linienbussen, U-Bahnen und Stadtbahnen (SuSi-PLUS). Forschungsverbundvorhaben SuSi-Plus. Unter Mitarbeit von Institut Wohnen und Umwelt GmbH. Darmstadt.

Rölle, Daniel; Flade, Antje; Lohmann, Günter (2004): Subjektives Sicherheitslagebild im ÖPNV – Methodisches Vorgehen und Handlungsempfehlungen. Band 3. In: SuSiteam (Hg.): Subjektives Sicherheitsempfinden im Personenverkehr mit Linienbussen, U-Bahnen und Stadtbahnen (SuSi-PLUS). Forschungsverbundvorhaben SuSi-Plus. Unter Mitarbeit von Institut Wohnen und Umwelt GmbH. Darmstadt.

Rölle, Daniel; Lohmann, Günter; Flade, Antje (2004): Subjektive Sicherheit im öffentlichen Verkehr aus Sicht der Verkehrsunternehmen. Eine Bestandsaufnahme in kleineren und mittleren Großstädten mit oberirdischen Verkehrsträgern. Band 1. In: SuSiteam (Hg.): Subjektives Sicherheitsempfinden im Personenverkehr mit Linienbussen, U-Bahnen und Stadtbahnen (SuSi-PLUS). Forschungsverbundvorhaben SuSi-Plus. Unter Mitarbeit von Institut Wohnen und Umwelt GmbH. Darmstadt.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Romberg, Benjamin; Tanriverdi, Hakan (2013): Warum die Bahn Drohnen gegen Graffiti-Sprayer einsetzt. süddeutsche.de (27. Mai 2013). Online verfügbar unter http://www.sueddeutsche.de/digital/ueberwachungstechnik-warum-die-bahn-drohnen-gegen-graffiti-sprayer-einsetzt-1.1682317, zuletzt geprüft am 29.07.2013.

Rössler, Bernd (2011): Situation analysis and adaptive risk assessment for advanced intersection safety systems. Univ., FB Inf, Berlin, Hamburg.

Rowshan, Shahed; Simonetta, Richard (2003): TCRP Report 86. Intrusion Detection for Public Transportation Facilities Handbook. Transit cooperative research program. Federal Transit Administration. Washington, D.C.

Ryu, Dae Hyun; Kim, HyungJun; Um, Keehong (2009): Reducing security vulnerabilities for critical infrastructure. In: *Journal of Loss Prevention in the Process Industries* 22 (6), S. 1020–1024. DOI: 10.1016/j.jlp.2009.07.015.

Sanchez, M. M. (2011): Security Risk Assessments in Public Transport Networks. In: *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit* 225 (4), S. 417–424. DOI: 10.1243/09544097JRRT409.

Sanquist, Thomas; Thurman, David; Mahy, Heidi: The Human Element Homeland Security Systems: Application Issues and Research Approaches, zuletzt geprüft am 03.08.2012.

Saurugg, Herbert (2012): Blackout. Eine nationale Herausforderung bereits vor der Krise. Hochschule für Management Budapest. Wien.

Schlüter, N.; Schulze-Bramey, U.; Winzer, P.: Sicherheitsbefragungen Die sozialwissenschaftlichen Dimensionen beim Schutz von Verkehrsinfrastrukturen. Bonn: Köllen Druck + Verlag GmbH (INFORMATIK 2010).

Schmid, Werner (2005): Risk Management Down Under. Die australisch-neuseeländische Risikomanagement-Norm AS/NZS 4360. In: *Risk News*.

Schmidt-Bentum (2013): Forschungsprojekt RIKOV: Schutz kritischer Infrastrukturen vor Terrorismus. In: *GIT Sicherheit* 2013, März 2013 (22), S. 6.

Schmitz, Martin Johannes (2008): Mikrowellen gegen den Terror. Personen- und Objektschutz mit High Power Mikrowave-Systemen. In: *S&I-Kompendium* 2008, S. 42–44, zuletzt geprüft am 26.09.2013.

Schmitz, Walter (2014): SCENEX System. Crealab GmbH. Feldkirchen-Westerham. Online verfügbar unter http://scenex.crealab-gmbh.de/login.php, zuletzt geprüft am 29.01.2014.

Schneider, Thomas; Weber, Karl; Locher, Reto (1994): Risikoakzeptanz aus technischer und soziologischer Sicht. Ein Einstieg in den Risikodialog. Hg. v. Schweizerische Unfallversicherungsanstalt und Schweizerische Akademie der Technischen Wissenschaften. Zürich: [Schweizerische Akademie der Technischen Wissenschaften] (Schrift / SUVA-Fonds, 1).

Schulze, Tillmann (2006): Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA. 1. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften/GWV Fachverlage, Wiesbaden.

Schulze-Bramey, U. (2009): Customer satisfaction in local passenger transport considering safety sensation. In: Juraj Sinay (Hg.): From integrated management systems towards generic management systems. Approaches from Slovakia and Germany. Herzogenrath: Shaker (3/2009), S. 97–108.

Schulze-Bramey, U. (2009): Sicherheitsempfinden von Fahrgästen in Wertschöpfungsketten, dargestellt am Beispiel des ÖPNV. In: Ludwig Theuvsen (Hg.): Qualitätsmanagement in Wertschöpfungsnetzwerken. [Bericht zur GQW-Jahrestagung 2009], Bd. 11. Aachen: Shaker-Verl (11), S. 201–2016.

Schwarte, Georg (2012): Videoüberwachung ist kein Allheilmittel. Debatte nach Anschlagsversuch. NDR. Online verfügbar unter http://www.tagesschau.de/inland/bombenfund-bonn104.html, zuletzt aktualisiert am 17.12.2013, zuletzt geprüft am 02.01.2013.

Schweickart, Nikolaus; Töpfer, Armin (Hg.) (2006): Wertorientiertes Management. Werterhaltung - Wertsteuerung - Wertsteigerung ganzheitlich gestalten. 1. Aufl. Berlin: Springer.

Senk, Christian (2011): Akzeptanzvon Security-as-a-Service-Lösung. Unter Mitarbeit von Lutz Neugebauer. BITKOM, zuletzt geprüft am 28.10.2013.

Sinay, Juraj (Hg.) (2009): From integrated management systems towards generic management systems. Approaches from Slovakia and Germany. Herzogenrath: Shaker (3/2009).

Singh, Sameer; Singh, Maneesha (2002): Explosives detection systems (EDS) for aviation security. Hg. v. Elsevier Science B.V. University of Exeter. Devon.

Skiera, Bernd; Gensler, Sonja: Berechnung von Nutzenfunktionen und Marktsimulationen mit Hilfe der Conjoint-Analyse. Teil I, zuletzt geprüft am 23.10.2013.

Slovic, Paul (2010): The feeling of risk. New Perspectives on Risk Perception. 1. Aufl. London: Earthscan.

Slovic, Paul (2011): The Perception of Risk. Reprinted. London: Earthscan (Risk, society and policy series).

Smit, Barry; Wandel, Johanna (2006): Adaptation, Adaptive Capacity and Vulnerability. In: *Global Environmental Change* 16 (3), S. 282–292. DOI: 10.1016/j.gloenvcha.2006.03.008.

Spriggs, Martin; Spriggs, Angela (2005): Assessing the impact of CCTV. Home Office Research Study 292. Hg. v. Home Office Research, Development and Statistics Directorate.

Stewart, Mark G.; Mueller, John (2013): Terrorism Risks and Cost-Benefit Analysis of Aviation Security. In: *RISK ANALYSIS* 33 (5), S. 893–908. DOI: 10.1111/j.1539-6924.2012.01905.x.

STEWART, C. H. M.: Risk Perception and Likelihood of Action in Criminal Offenders. In: *THE BRITISH JOURNAL OF CRIMONOLOGY* 1979 (Vol. 19 No. 2), S. 105–119.

Störfallkommission (Hg.) (2004): Risikomanagement im Rahmen der Störfall-Verordnung des Arbeitskreises Technische Systeme, Risiko und Verständigungsprozesse. am 21.04.2004 von der SFK zustimmend zur Kenntnis genommen. Deutschland. Bonn (SFK-GS-41). Online verfügbar unter http://www.kas-bmu.de/publikationen/sfk/sfk_gs_41.pdf, zuletzt geprüft am 04.01.2013.

Strandberg, Veronica (2013): Rail bound traffic - a prime target for contemporary terrorist attacks? In: *J Transp Secur* 6 (3), S. 271–286. DOI: 10.1007/s12198-013-0116-0.

Straube, Martina (2011): Volkswirtschaftliche Kosten durch Straßenverkehrsunfälle 2009. Bundesanstalt füt Straßenwesen. Bergisch Gladbach (Forschung Kompakt, 04/11). Online verfügbar unter www.bast.de/cln_030/nn_42254/SharedDocs/Publikationen/Forschung-kompakt/2011-04,templateId=raw,property=publicationFile.pdf/2011-04.pdf, zuletzt geprüft am 17.01.2013.

SuSiteam (Hg.) (2004): Subjektives Sicherheitsempfinden im Personenverkehr mit Linienbussen, U-Bahnen und Stadtbahnen (SuSi-PLUS). Forschungsverbundvorhaben SuSi-Plus. Unter Mitarbeit von Institut Wohnen und Umwelt GmbH. Bundesministerium für Wirtschaft und Technologie. Darmstadt.

Taylor, Brian D. (o.J.): Terrorism and Transit Security. 12 Recommendations for Progress. Center for American Progress.

TELOPS (2012): Hyper-Cam GDI. The remote gas detection and identification system. Quebec.

Theuvsen, Ludwig (Hg.) (2009): Qualitätsmanagement in Wertschöpfungsnetzwerken. [Bericht zur GQW-Jahrestagung 2009]. Universität Göttingen; Gesellschaft für Qualitätswissenschaft; GQW-Jahrestagung. Aachen: Shaker-Verl (11).

Thießen, Ansgar (2011): Organisationskommunikation in Krisen. Reputationsmanagement durch situative, integrierte und strategische Krisenkommunikation. In: *Organisationskommunikation in Krisen*.

Thießen, Ansgar (2013): Handbuch Krisenmanagement. In: *Handbuch Krisenmanagement*.

Thießen, Ansgar (Hg.) (2014): Handbuch Krisenmanagement. 2. Aufl. 2014. Wiesbaden: Springer Fachmedien Wiesbaden GmbH.

Thywissen, Katharina (2006): Components of Risk. A Comparative Glossary. Hg. v. UNU Institute for Environment and Human Security. Bonn.

Tinnes, Judith (2013): The Art of Searching. How to Find Terrorism Literature in the Digital. In: *Perspectives on Terrorism* 7 (4), S. 79–111.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

TNS Infratest (Hg.): DAS ÖPNV-Kundenbarometer 2012. Verkehrsverbünde und Verkehrsunternehmen im Vergleich. Die Spitzenreiter.

Todd Litman (2012): Terrorism, Transit and Public Safety Evaluating the Risks. In: *Journal of Public Transit* 2005 (Vol. 8,No. 4), S. 33–46.

Töpfer, Armin (2006): Werterhaltung und -steigerung durch Risiko- und Krisenmanagement. In: Nikolaus Schweickart und Armin Töpfer (Hg.): Wertorientiertes Management. Werterhaltung - Wertsteuerung - Wertsteigerung ganzheitlich gestalten. 1. Aufl. Berlin: Springer, S. 377–403.

Transit Cooperative Research Program (2009): TCRP Synthesis 80. Transit Security Update. A Synthesis of Transit Practice. Unter Mitarbeit von Yuko Nakanishi. Federal Transit Administration. Washington, D.C., zuletzt geprüft am 04.01.2013.

Transportation Research Board (2003): Using Simulation to Evaluate Impacts of Airport Security. 2003 Simulation Workshop. Washington, D.C.

TRB (2000): TCRP Report 47: A Handbook for Measuring Customer Satisfaction and Service Quality (Part D), zuletzt aktualisiert am 04.10.2000, zuletzt geprüft am 13.05.2013.

TSA (2011): CSIS: Evolution of Aviation Security since 9/11. Hg. v. Transportation Security Administration. Washington, DC. Online verfügbar unter http://www.tsa.gov/press/speeches/tsa-administrator-john-s-pistole-csis-evolution-aviation-security-911-washington-dc, zuletzt geprüft am 12.02.2014.

Turley, C.; Stone, V. (2006): Public Attitudes towards Transport Security Measures. Report.

U.S. Department of Energy (Hg.) (2012): Climate Change and Infrastructure, Urban Systems and Vulnerabilities. Technical Report for the US. Department of Energy in Support of the National Climate Assessment.

U.S. Department of Homeland Security (Hg.) (2008): A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal and Territorial Level. Washington DC.

U.S. Department of Justice (Hg.) (2002): A Method to Assess the Vulnerability of U.S. Chemical Facilities. Office of Justice Programs. Washington.

UITP (2010): Secure Public Transport in a Changeable World. A UITP position paper.

UITP (2010): Sicherer ÖPNV in einer sich verändernden Welt. Positionspapier der UITP. Brüssel. UITP-Ausschuss für Sicherheit, info@uitp.org, zuletzt geprüft am 02.09.2013.

UITP (Hg.) (2012): UTIP Training Programme. Security Risk Assessment and Emergency Preparedness & Response. Online verfügbar unter http://trainingsecurity.uitp-events-expo.org/, zuletzt geprüft am 11.12.2012.

Uni BW München (2014): vorläufiger Bericht Methode zur Bestimmung der Konsequenz eines terroristischen Anschlages. Arbeitspaket 4.3. Neubiberg, zuletzt geprüft am 29.01.2014.

United Nations Development Programme (Hg.) (2004): Reducing Disaster Risk. A Challenge for Development. A Global Report. New York.

VBG (2009): Sicherheitsmaßnahmen gegen Übergriffe Dritter in Verkehrsunternehmen. VBG-Fachinformation BGI 5039. Hamburg.

VBG (Hg.) (2012): Zwischenfall, Notfall, Katastrophe. Leitfaden für die Sicherheits- und Notfallorganisation. VBG-Fachwissen BGI 5097. Gesetzliche Unfallversicherung. Hamburg.

VDI/VDE (Hg.) (2009): Marktpotenzial von Sicherheitstechnologien und Sicherheitsdienstleistungen. Der Markt für Sicherheitstechnologien in Deutschland und Europa - Wachstumsperspektiven und Marktchancen für deutsche Unternehmen. Schlussbericht, zuletzt geprüft am 02.09.2013.

VDV AG Security (2008): VDV-Sicherheitsleitfaden für ÖPNV-Unternehmen - Safety und Security. Hg. v. Verband Deutscher Verkehrsunternehmen. Köln.

Venna, Haritha; Fricker, Jon (2009): Synthesis of Best Practices in Transportation Security, Volume I: Vulnerability Assessment. West Lafayette, IN: Purdue University.

Verband Deutscher Verkehrsunternehmer (Hg.) (2012): VDV-Statistik 2011. Köln. Online verfügbar unter http://www.vdv.de/module/layout_upload/st2011_online.pdf, zuletzt geprüft am 16.11.2012.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Verbundprojekt PiraT (Hg.): Indikatoren zur Risikobewertung von Piraterie und maritimem Terrorismus: Problematisierung und Ergebnisse – Gemeinsamer Bericht der wissenschaftlichen Partner des Projekts PiraT.

Videmo (Hg.) (2015): Produktwebsite XSControl. Karlsruhe. Online verfügbar unter http://www.xscontrol.de/, zuletzt geprüft am 21.05.2015.

Vowe. Gerhard: Sicherheit als mediales Konstrukt. Sicherheitswahrnehmung aus Sicht der Kommunikationswissenschaft. Universität Düsseldorf.

Wagner, Dieter; Lehnigk, Nadine (2010): Sicherheit im Öffentlichen Personennahverkehr des Landes Brandenburg. Hg. v. Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH, zuletzt geprüft am 11.07.2012.

Wagner, Katrin; Bonß, Wolfgang; Fischer, Susanne (2011): Vor Prothesenträgern wird gewarnt. Sicherheitsmaßnahmen im zivilen Luftverkehr. In: *Security inside* (6/2011), S. 31–33, zuletzt geprüft am 28.10.2013.

Warnke, Philine; Zoche, Peter (2009): Sicherheitswahrnehmungen zu Beginn des 21. Jahrhunderts, 12.11.2009, zuletzt geprüft am 10.05.2012.

Webb, Dave; Wills Herrera, Eduardo (2012): Subjective Well-Being and Security. Dordrecht, New York: Springer (Social indicators research series, v.46).

Weber, Ines (2013): Generisches ÖPV-System. Präsentation zum RIKOV Workshop. Uni BW München. Köln, 13.05.2013.

Wehrheim, Jan: Städte im Blickpunkt Innerer Sicherheit. In: *Aus Politik und Zeitgeschichte* 2004 (B44), S. 21–27, zuletzt geprüft am 02.01.2013.

Welsh, Brandon C.; Farrington, David P.; O'Dell, Sean J. (2010): Effectiveness of Public Area Surveillance for Crime Prevention. Security Guards, Place Managers and Defensible Space. Stockholm, zuletzt geprüft am 04.02.2014.

Welsh, C. Brandon (2007): EVIDENCE-BASED CRIME PREVENTION: SCIENTIFIC BASIS, TRENDS, RESULTS AND IMPLICATIONS FOR CANADA. Research Report. Ottawa.

Welsh, C. Brandon; Farrington, David P. (2008): Effects of closed circuit television surveillance on crime: The Campbell Collaboration.

Werdich, Martin (2011): FMEA - Einführung und Moderation. Durch systematische Entwicklung zur übersichtlichen Risikominimierung (inkl. Methoden im Umfeld). 1. Aufl. Wiesbaden: Vieweg+Teubner Verlag / Springer Fachmedien Wiesbaden GmbH Wiesbaden. Online verfügbar unter http://ebooks.ciando.com/book/index.cfm/bok_id/284826.

Werner, Jan; Berschin, Felix (1996): Begriffsdefinitionen im Verkehrsbereich. Online verfügbar unter http://www.nahverkehrsberatung.de/downloads/zur1.97.begriffe.pdf, zuletzt geprüft am 16.11.2012.

White, Jonathan Randall (2013): Terrorism and Homeland Security. 8. Aufl. Belmont, Calif, Andover: Wadsworth.

Wiedenhoefer, Torben; Reuter, Christian; Ley, Benedikt; Pipek, Volkmar (2013): Entwicklung IT-basierter internationaler Krisenmanagement-Infratrukturen für Stromausfälle. In: Matthias Horbach (Hg.): Informatik 2013 - Informatik angepasst an Mensch, Organisation und Umwelt; Tagung vom 16.-20. September 2013 in Koblenz. Bonn: Ges. für Informatik (GI-Edition : Proceedings, 220), S. 1649–1658.

Wilis, Henry H.; Morral, Andrew R.; Kelly, Terrence K.; Medby, Jamison Jo (2005): Estimating Terrorism Risk. Hg. v. Center for Terrorism Risk Management Policy. RAND Corporation. Pittsburgh.

Willis, Henry H.; LaTourrete, Tom; Kelly, Terrence K.; Hickey, Scot; Neill, Samuel (2007): Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection. Hg. v. Center for Terrorism Risk Management Policy. RAND Corporation. Pittsburgh.

Willkommen, Dominik (2005): Videoüberwachung und Sicherheit(sgefühl). Vordiplomarbeit. Universität Oldenburg, München. Online verfügbar unter http://www.hausarbeiten.de/faecher/vorschau/109874.html, zuletzt geprüft am 12.01.2013.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Wilson, Jeremy M.; Jackson, Brian A.; Eisman, Mel; Steinberg, Paul; Riley, K. Jack (2007): Securing America's Passenger-Rail Systems. Hg. v. Homeland Security. RAND Corporation. Pittsburgh.

Winter, Stefanie (2000): Quantitative vs. Qualitative Methoden. Online verfügbar unter http://imihome.imi.uni-karlsruhe.de/nquantitative_vs_qualitative_methoden_b.html, zuletzt geprüft am 22.01.2013.

Winzer, P.; Schlüter, N.; Schulze-Bramey, U. (2009): Indicators for security and safety in public transportation platforms: a case study. 12th International QMOD and Toulon-Verona Conference on Quality and Service Sciences (ICQSS), 08.2009.

Winzer, Petra (Hg.) (2009): Weiterentwicklung des Wuppertaler Generic-Management-Konzeptes. Aachen: Shaker (2009,1).

Winzer, Petra (Hg.) (2012): Methodik zur permanenten Erfassung und Auswertung des individuellen subjektiven Sicherheitsempfindens, dargestellt am Beispiel von Fahrgästen des ÖPNV bei Großveranstaltungen. Unter Mitarbeit von Ulf Schulze-Bramey. 1. Aufl. Aachen: Shaker Verlag (Berichte zum Generic-Management, 3).

Wirtschaftskammer Österreich (2012): INFLATIONSRATEN. Veränderung der Verbraucherpreise. Online verfügbar unter http://wko.at/statistik/eu/europa-inflationsraten.pdf, zuletzt geprüft am 17.01.2013.

Wolke, Thomas (2009): Risikomanagement. 2. Aufl. München: Oldenbourg. Online verfügbar unter http://www.oldenbourg-link.de/isbn/9783486587142.

Woo, Gordon Dr.: Quantitative Terrorism Risk Assessment.

Wortley, R.; Mazerolle, L. (2013): Environmental Criminology and Crime Analysis: Taylor & Francis. Online verfügbar unter http://books.google.de/books?id=bjKo1sjd4mIC.

Zakaria, Tabassum; Hosenball, Mark (2012): UPDATE 1-US airport security could detect Qaeda device-officials. Thomson Reuters. New York. Online verfügbar unter http://www.reuters.com/article/2012/05/08/usa-security-plot-idUSL1E8G88JH20120508, zuletzt aktualisiert am 08.05.2012, zuletzt geprüft am 11.02.2013.

Zehnder, Michael; Stutzter, Alois (2009): Ökonomische Überlegungen zur Kameraüberwachung als Maßnahme gegen den Terrorismus. In: *Vierteljahrshefte zur Wirtschaftsforschung* (78), S. 119–135.

Zelewski, S. (1994): Unternehmenskrisen und Konzepte zu ihrer Bewältigung. Universität Leipzig, Institut für Produktionswirtschaft und industrielle Informationswirtschaft. Leipzig.

Ziegleder, Diana; Kudlacek, Dominic; Fischer, Thomas (2011): Zur Wahrnehmung und Definition von Sicherheit durch die Bevölkerung. Erkenntnisse und Konsequenzen aus der kriminologisch-sozialwissenschaftlichen Forschung. Berlin: Forschungsforum Öffentliche Sicherheit (Schriftenreihe Sicherheit, 5), zuletzt geprüft am 29.11.2013.

Zimmermann, Jürgen; Rieck, Julia; Stark, Christoph (2006): Projektplanung. Modelle, Methoden, Management. Berlin: Springer.

Zoll (2010): Zollhunde am Flughafen Frankfurt. Frei Schnauze kontrolliert. In: *ZOLL aktuell* 2010 (3/10), S. 4–6. Online verfügbar unter http://www.zoll.de/SharedDocs/Downloads/DE/Publikation/Broschuere_Bestandteile/Zoll-aktuell/2010/2010_3_2.pdf?__blob=publicationFile, zuletzt geprüft am 11.09.2013.

Zumpe, Hagen (2009): Weiche steht auf Videoüberwachung. Sicherheit bei der Deutschen Bahn. In: *PROTECTOR* (5), S. 14–15, zuletzt geprüft am 11.10.2012.

Zwick, Michael M.; Renn, Ortwin (Hg.) (2002): Perception and evaluation of risks. Findings of the "Baden-Württemberg risk survey 2001". [S.l.]: Universität Stuttgart / Akademie für Technikfolgenabschätzung in Baden-Württemberg (Arbeitsbericht / Akademie für Technikfolgenabschätzung in Baden-Württemberg). Online verfügbar unter http://www.bsz-bw.de/cgi-bin/xvms.cgi?SWB11244213.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

A 4. Lieferungen

Die gemäß Teilvorhabenbeschreibung der Technischen Hochschule Köln definierten Lieferungen werden diesem Schlussbericht in einem separaten Anhang als Dokumentationsnachweis beigefügt.

- L1.4 Bericht „Analyse potenzieller Sicherheitsmaßnahmen“
- WS1 Workshop „ÖPV-Vignetten“ mit externen Experten
- L2.1 Bericht „Prozessmodellierung der Operationspläne“
- L7.2 - L7.3 Bericht „Integration und Test“ - „Validierung der Planungsergebnisse“

Anmerkung
Dieser Anhang ist nicht für die Öffentlichkeit bestimmt, sondern wird ausschließlich dem Projektkonsortium sowie dem Projektträger des Verbundforschungsprojekts RiKoV zur Verfügung gestellt.

A 5. Vorhabenbeschreibung

Für eine inhaltliche Verknüpfung dieses Schlussberichts sind die Gesamtvorhabenbeschreibung des Verbundforschungsprojekts „RiKoV“ sowie die Teilvorhabenbeschreibung der Technischen Hochschule Köln in einem separaten Anhang beigefügt.

Anmerkung
Dieser Anhang ist nicht für die Öffentlichkeit bestimmt, sondern wird ausschließlich dem Projektkonsortium sowie dem Projektträger des Verbundforschungsprojekts RiKoV zur Verfügung gestellt.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung