Quantitative Risikobewertung als Instrument der Sicherheitsplanung und Risikoentscheidung

Wirksamkeit und Kosteneffizienz des Sicherheitsmanagements von
Luftverkehrsinfrastrukturen

Teilprojekt des Vorhabens FKZ 13N10026
„Sicherheit von Verkehrsinfrastrukturen (SiVe)"

Schlußbericht

Technische Universität München (TUM)
Institut für Betriebswirtschaftslehre / Finanzmanagement
Prof. Dr. Christoph Kaserer
Apl.-Prof. Dr. Gebhard Geiger
Dr. Philipp Schaller

München, 24. Februar 2012

Inhaltsverzeichnis

I. KURZDARSTELLUNG DES PROJEKTS

1. Projektaufgaben
2. Voraussetzungen des Vorhabens
3. Planung und Ablauf
4. Stand der Forschung zu Beginn des Teilprojekts
5. Zusammenarbeit mit anderen Stellen

II. EINGEHENDE DARSTELLUNG

1. Verwendung der Zuwendungen und erzielte Ergebnisse
2. Wichtige Positionen des zahlenmäßigen Nachweises
3. Notwendigkeit und Angemessenheit der durchgeführten Projektarbeiten
4. Nutzen und Verwertbarkeit der erzielten Resultate
5. Initiativen und Projekte anderer Forschungseinrichtungen
6. Internationale Initiativen und Projekte
7. Veröffentlichung der Projektergebnisse

Anlage 1: ERFOLGSKONTROLLBERICHT

Beitrag der Ergebnisse zu den förderpolitischen Zielen

Wissenschaftlich-technische Ergebnisse, Nebenergebnisse, wesentliche Erfahrungen

Fortschreibung des Verwertungsplans

Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Noch nicht abgeschlossene Arbeiten

Präsentationsmöglichkeiten für mögliche Nutzer

Einhaltung der Kosten- und Zeitplanung

Anlage 2: ZUSAMMENFASSUNGEN DER VERÖFFENTLICHUNGEN

I. KURZDARSTELLUNG DES PROJEKTS

1. Projektaufgaben

Der Schutz von Verkehrsinfrastrukturen vor Störfällen und gezielten Angriffen unterliegt in aller Regel den Bedingungen knapper Ressourcen und des risikobehafteten Planens und Entscheidens. Schutzmaßnahmen müssen daher nicht nur wirksam, sondern auch kosteneffizient sein. Die technologiegestützte Gefahrenabwehr macht entsprechende Planungsgrundlagen notwendig. Insbesondere verlangt sie eine genaue, möglichst quantitative Einschätzung potentieller Verluste sowie das Wissen um Ursachen und Begleitumstände von Schadensereignissen, gegen die Schutzmaßnahmen zu treffen sind. Neben Erkenntnissen über Art, Ausmaß, Wahrscheinlichkeit und Häufigkeit von Schadensereignissen muß sich die Gefahrenabwehr auch auf eine Systematik der Risikobewertung stützen. Hauptaufgaben des SiVe-Teilprojekts „Quantitative Risikobewertung als Instrument der Sicherheitsplanung und Risikoentscheidung“ waren

- neue, leistungsfähige, statistisch begründete Methoden der quantitativen Risikobewertung als Planungs- und Entscheidungsgrundlagen für Schutz- und Vorsorgemaßnahmen im Bereich der physischen Sicherheit von Verkehrsinfrastrukturen einzuführen,
- diese Methoden anhand szenariengestützter Simulationen von Sicherheitszwischenfällen (Flughafensicherheit) zu testen sowie
- ihren praktischen Nutzen für das Sicherheitsmanagement von Verkehrsinfrastrukturen anhand ausgewählter Pilotanwendungen aus dem Bereich der Flughafensicherheit nachzuweisen.

2. Voraussetzungen des Vorhabens

Für die Beteiligung am Projekt SiVe brachte die Technische Universität München besondere fachliche Voraussetzungen mit. Einerseits verfügt das TUM-Institut für Betriebswirtschaftslehre/Finanzmanagement über die erforderliche theoretische und methodische Spezialkenntnis sowie wissenschaftliche Erfahrung auf dem Gebiet moderner ökonometrischer Ansätze der quantitativen Risikoforschung und -bewertung. Andererseits besitzt einer der Projektmitarbeiter am Institut (G. G.) breite interdisziplinäre Erfahrung in der technologieorientierten Sicherheitsforschung und Sicherheitspolitik (als langjähriger Mitarbeiter der Stiftung Wissenschaft und Politik/SWP, Berlin). Weiterhin war bei der Konzeption der Projektaufgaben davon auszugehen, daß die Verwendung moderner ökonometrischer Ansätze wesentliche methodische Innovationen zur zivilen Sicherheit, Sicherheitsplanung und Risikoentscheidung beitragen kann. Denn sofern sich die

herkömmliche Sicherheitsforschung quanti-tativer Ansätze bedient, erstrecken sich diese auf statistische, ingenieur- und betriebswirtschaftliche Verfahren der Risikomessung, die viele Fragen der zivilen Sicherheit offen lassen müssen, da sie keine methodologisch ausreichend begründete Systematik der Risikobewertung einschließen (siehe den Abschnitt zum Stand der Forschung unten). Schließlich konnte sich die Projektbeteiligung des TUM-Instituts für Betriebswirtschaftslehre/Finanzmanagement auf Erfahrungen in zahlreichen nationalen und internationalen Forschungsprojekten, insbesondere auf die Forschungskooperation mit Industriebetrieben stützen. Insgesamt konnten die fachlichen und personellen Voraussetzungen für eine erfolgreiche Projektarbeit im Zusammenwirken mit den ingenieur- und sicherheitswissenschaftlich orientierten Partnern (vgl. hierzu auch Abschn. II.5) durch den methodischen Beitrag des TUM-Partners wirksam ergänzt und vervollständigt werden.

3. Planung und Ablauf

Die zeitliche Ablaufplanung des Teilprojekts entsprach im wesentlichen der Aufteilung in die 5 Arbeitspakete, die dem Projektantrag zugrunde lagen (Tab. 1). Gelegentliche Abweichungen hiervon hielten sich im Rahmen der festgelegten Projektaufgaben. Sie erstreckten sich hauptsächlich auf

- Erweiterungen des geplanten Themenspektrums im Bereich der Modellbildung, d. h. die Entwicklung theoretischer Grundlagen für ein mehrdimensionales Risikoentscheidungsmodell („multiple-attribute utility theory“, siehe [4])
- 1 vorgezogene Fallstudie hierzu, deren Ergebnisse bereits in einem frühen Projektstadium veröffentlicht wurden [2]
- die kostenneutrale Verlängerung des Teilprojekts von Juli bis Ende Oktober 2011.

Die Analyse charakteristischer Bedrohungsszenarien und geeigneter Sicherheitstechnologien/Schutzmaßnahmen (AP 1, 2) wurde bereits in einer frühen Projektphase durch die ökonometrischen Arbeiten der Risikomodellbildung und –bewertung und durch die Softwareentwicklung in diesen Bereichen ergänzt (AP 3, in Zusammenarbeit mit dem Projektpartner ckc). Erste Beiträge zu AP 4 und 5 wurden dann mit allen weiteren Projektpartnern bereits ab 2009 erstellt, z. T. ohne bereits über den vollen Softwareapparat (automatisierte Szenariobildung, Simulationssoftware) zu verfügen, dessen Entwicklung und Test für spätere Projektabschnitte geplant war. Zweck dieser vorgezogenen Maßnahmen war es, SiVe 2009 bei mehreren internationalen Tagungen, aber auch bei workshops der deutschen zivilen Sicherheitsforschung, möglichst schon mit Ergebnissen zu präsentieren. [1], [2] Diese Entwicklungen und ersten Anwendungen konnten dann bis zur Erreichung des geplanten „Meilensteins“ im Januar 2010 nochmals deutlich erweitert werden. Möglich wurde die Erweiterung durch die

Tab. 1: Arbeitspakete (AP) und zeitliche Ablaufplanung

AP 1 Bedrohungsszenarien	**2008**
Auswahl, Analyse, Festlegung geeigneter Testszenarien	
AP 2 Schutzmechanismen	**2008 - 2009**
Technologien, sichere Betriebsabläufe, physischer Schutz, modell- und simulationsgestützte Planung und Entscheidung unter Risiko	
AP 3 Risiko- und sicherheitsorientierte Systemanalyse	**2008-2010**
Ökonometrische Modellbildung, Software-Entwicklung und –test	
AP 4 Modell- und Methodenintegration	**2010 - 2011**
Software-gestützte Integration des Risko-Entscheidungsmodells	
AP 5 Szenarienorientierte Systemsimulation, quantitative Risikobewertung	**2010 - 2011**
Anwendungen, Auswertung der Ergebnisse, erste Verwertungen der Projekterträge	

schrittweise Einbettung des quantitativen Risikobewertungs- und Entscheidungsmodells in die System- und Simulationssoftware der anderen Projektpartner (Konzeption und Simulation von Angriffsszenarien/Flughafensicherheit). AP 4 und 5 standen in der 2. Hälfte der Projektlaufzeit (nach dem „Meilenstein“) im Vordergrund auch des TUM-Teilprojekts. Ergebnisse dieser Arbeiten, ihre Anwendung auf Maßnahmen der Flughafensicherheit sowie Darstellungen allgemeiner Nutzenaspekte für die Sicherheit von Verkehrsinfrastrukturen und das Risikomanagement finden sich in den Publikationen bzw. in Manuskripten, die zur Veröffentlichung vorbereitet werden (Tab. 2 sowie Anlage 2).

Die kostenneutrale Verlängerung der Projektlaufzeit um 4 Monate wurde einerseits zum Sammeln und zur Auswertung empirischer Befunde verwandt, die zum experimentellen Test des Risikoentscheidungsmodells erhoben wurden. Andererseits wurde die Verlängerung zum theoretischen Ausbau des Risikoentscheidungsmodells genutzt. Beide Beiträge erfolgten hauptsächlich unter den Perspektiven der wissenschaftlichen Anschlußfähigkeit und Weiterverwertung der Projektergebnisse zugunsten der methodischen Fundierung der zivilen Sicherheitsforschung. Sie sind in Tabelle 2 unter [4], [5] und [7] dokumentiert.

Die Ressourcenplanung des Teilprojekts ging von der vollen Arbeitszeit eines wissenschaftlichen Mitarbeiters aus (36 Personenmonate). Hauptsächlich mit Blick auf die Weiterverwertung der Ergebnisse durch die Hochschule wurde in der Schlußphase ein weiterer wissenschaftlicher Mitarbeiter kostenneutral hinzugezogen (1/2 wissenschaftliche Mitarbeiterstelle).

Der Ablauf des Teilprojekts war u. a. von den häufigen, regelmäßigen Arbeitssitzungen zur Planung und Koordination der Projektabschnitte bestimmt. Die Sitzungen fanden vorwiegend

an den Münchener Standorten des Koordinators EADS statt. Den dort getroffenen Absprachen und Entschlüssen war ein zügiger, reibungsloser und immer zielorientierter Ablauf zu verdanken.

Die wesentlichen Ergebnisse des Teilprojekts sind unter „II. Eingehende Darstellung“ zusammengefaßt und bilanziert.

4. Stand der Forschung zu Beginn des Teilprojekts

Statistik, Ökonometrie und Operations Research boten dem Stand der methodischen Forschung zufolge im wesentlichen 3 verschiedene Typen der quantitativen Risikobewertung an: Klassische statistische Ansätze, die „lineare“ ökonometrische Theorie der Risikonutzenerwartung sowie moderne „nichtlineare“ Risikonutzentheorien.[1] Aus der Sicht der anwendungsorientierten Forschung sind diese Ansätze jedoch bis auf wenige Ausnahmen, die erst in jüngster Zeit entwickelt worden sind, mit methodischen Mängeln behaftet, die ihre Anwendung fragwürdig, strittig oder gar unmöglich machen oder doch zumindest sehr behindern. Als Beispiele seien die bekannten methodischen und theoretischen Ansätze der klassischen statistischen Risikobewertung genannt. Sie beurteilen Risiken ausschließlich anhand der statistischen Parameter ihrer Wahrscheinlichkeitsverteilung (Mittelwert, Varianz, Value at Risk u. a.). An der Technischen Universität München waren bereits vor der Bewilligung des Projekts eine Reihe von Arbeiten zur Axiomatik und Methodik der quantitativen Risikobewertung entstanden (Hinweise in [4]), die sich aufgrund ihrer theoretischen und empirischen Fundierung und rechnerischen Einfachheit für Managementanwendungen auch im Bereich der zivilen Sicherheit eignen.

5. Zusammenarbeit mit anderen Stellen

Über die Zusammenarbeit mit den SiVe-Projektpartnern hinaus ist der sicherheitswissenschaftliche Kontakt und Austausch mit folgenden Partnern hervorzuheben:

- Arbeitsgruppe Luftfahrt der BMBF-geförderten Innovationsplattform „Schutz von Verkehrsinfrastrukturen“ mit den Projekten „FluSs“ und „Critical Parts“
- EU-Projektgruppen der Sicherheitsforschung (FP7), insbesondere Projekt DECOTESSC1 und „ValueSec“

[1] „Linear“ und „nichtlinear“ beziehen sich darauf, ob der mathematische Ausdruck für das „Nutzenfunktional“ linear oder nichtlinear von der Wahrscheinlichkeit der Schadensfolgen eines Ereignisses abhängt.

- Querschnittprojekt INFRANORM im Themenfeld „Schutz von Verkehrsinfrastrukturen“ der „Forschung für die zivile Sicherheit“ der Bundesregierung
- Institute der Fraunhofer-Gesellschaft / zivile Sicherheit (INT Euskirchen, ICT Pfinztal, IFF Magdeburg).

Die Zusammenarbeit umfaßte den Austausch von Forschungsergebnissen, Planung und Durchführung gemeinsamer nationaler und europäischer Forschungsaktivitäten (FhG ICT, IFF), Konferenzteilnahme und -beiträge (EU-Sicherheitsforschung, DECOTESSC1 workshops), Projektbeteiligung („ValueSec“) sowie die Mitwirkung bei Interviews, Umfragen und statistischen Erhebungen (INFRANORM).

II. EINGEHENDE DARSTELLUNG DES TEILPROJEKTS

1. Verwendung der Zuwendungen und erzielte Ergebnisse

Die Aufgabe des Teilprojekts bestand zunächst darin, den Grad an Risikoreduktion, der mit einer bestimmten Schutz- oder Vorsorgemaßnahme unter gegebenen Anwendungsbedingungen erzielt werden kann, systematisch abzuschätzen (Wirksamkeit des Risikomanagements) und ihn mit den Kosten für den erforderlichen technischen und organisatorischen Aufwand in Bezug zu setzen (Kosteneffizienz des Risikomanagements). Weiterhin sollte gezeigt werden, wie mit dem methodischen Apparat des Teilprojekts Grenzen der öffentlichen Zumutbarkeit verbleibender Restrisiken (soziale Risikotoleranz/-akzeptanz) des Sicherheitsmanagements (Verkehrsinfrastrukturen, Beispiel Flughafensicherheit) numerisch abzuschätzen und nach einer systematischen Güterabwägung durch Gesetzgeber, Behörden und Anlagebetreiber sinnvoll festzulegen sind.

In Kooperation mit den Anwendern im Konsortium (Flughafen München) sowie mit den Projektpartnern in den Bereichen Systemanalyse, Modellbildung und Prozeßsimulation wurden unterschiedliche Bedrohungsszenarien entwickelt. Ihre möglichen Schadensfolgen in zentralen Problembereichen der Sicherheit von Großflughäfen

- Kontrollsysteme (Passagiere, Betriebspersonal, geschützte Sicherheitsbereiche, Stoffe/Materialien/Transportgüter/Gepäck)
- Flughafen-Inspektionssysteme und –verfahren, Sicherheitsüberwachung
- sicherheitskonformer Betrieb

wurden mittels rechnergestützter probabilistischer Geschäftsprozeßmodelle simuliert. Die szenariogestützten Modellsimulationen lieferten statistische bzw. wahrscheinlichkeitstheoretische Darstellung des Risikos als Häufigkeits- bzw. Wahrscheinlichkeitsverteilung der möglichen Schadensfolgen eines Sicherheitszwischenfalls. Dieses Verfahren eignet sich auch zur Risikobewertung von Angriffsszenarien, für die Eintrittswahrscheinlichkeiten nicht sinnvoll definiert werden können und Häufigkeitsaussagen wenig informativ sind (z. B. im Hinblick auf Angriffe, die nur ein einziges Mal erfolgen und von planmäßig agierender Tätern ausgehen – im Gegensatz zu mehr oder weniger häufigen bzw. wahrscheinlichen Störfällen aufgrund technischen oder menschlichen Versagens oder aufgrund von Naturereignissen). Das risikobehaftete Systemverhalten wurde für den Angriffsfall mit Hilfe sogenannter What-if-Szenarien angemessen beschrieben. Die Wahrscheinlichkeit eines Sicherheitszwischenfalls (Angriffs usw.) wurde dabei zu Analysezwecken willkürlich gleich 1 gesetzt, das Systemverhalten im Angriffsfall aber weiterhin als zufallsbedingt (risikobehaftet) vorausgesetzt und unter verschiedenen Annahmen über vorhandene Schutzvorkehrungen simuliert. Die Systematik der quantitativen Risikobewertung bestand nun darin, mittels der zugrundegelegten ökonometrischen Risikonutzentheorie einer jeden im Simulationsexperiment ermittelten statistischen Schadensverteilung ein eindeutig definiertes „Sicherheitsäquivalent“, d. h. einen festen, nicht länger mit Unsicherheit behafteten Schadensbetrag („intrinsischer Preis“ eines Sicherheitsrisikos[2]) zuzuweisen. Unterschiedliche Risikomanagementmaßnahmen führten in der Simulation von Schadensszenarien somit zu unterschiedlichen, aber wohldefinierten Risikopreisen. Durch ihren Vergleich konnten Sicherheitsrisiken und die Effizienz alternativer Risikoreduktionsmaßnahmen („Sicherheitsmanagement“) quantitativ erfaßt, bewertet und damit systematisch überprüft werden.

In regelmäßigen (monatlichen) workshops des gesamten Konsortiums sowie in speziellen Arbeitsgruppensitzungen mußten geeignete aktuelle/künftige Bedrohungsszenarien entworfen sowie bei gegebenen Anforderungen der Anwender (Flughafenbetreiber, Sicherheitsmanagement) auf ihre Eignung hin beurteilt werden. Hierzu lieferte der TUM-Partner regelmäßig Beiträge und Ausarbeitungen, die zu ersten rechnergestützte Testrechnungen (Risikomessung, Risikobewertung) eingesetzt wurden. Solche ersten Modell- und Testrechnungen konnten ab Januar 2009 in Zusammenarbeit mit der ckc AG erfolgen. Die Ergebnisse der ersten Schritte der Szenarienentwicklung wurden darin bereits umgesetzt. Sie wurden beim Frühjahrstreffen der BMBF-Innovationsplattform „Schutz von Verkehrsinfrastrukturen“ am 26. 02. 2009 in Bonn präsentiert (poster session). Weitere TUM-

[2] Finanzieller Verlust, Anzahl von Verletzten und/oder Toten usw. „Intrinsische“ Preise sind keine Preise auf Märkten für risikobehaftete Güter oder Dienstleistungen, sondern Buchhaltungsgrößen, d. h. Zahlenwerte innerhalb des jeweils zugrundeliegenden Systems der Bilanzierung von Gewinnen und Verlusten.

Beiträge zu SiVe-Ergebnispräsentationen dieser Art erfolgten bei internationalen Tagungen im Herbst 2009 (CRITIS ’09, Bonn, und Future Security 2009, Karlsruhe).

Analog entwickelten sich die Untersuchungen zu ausgewählten vorhandenen/künftigen Schutzmechanismen der Flughafensicherheit (Technologien der Passagier- und Gepäckkontrolle, Zugangskontrollen, Alarm- und Überwachungssysteme, softwaregestützte Modelle solcher Mechanismen, Sicherheitsorganisation, Sicherheitsvorschriften) in Zusammenarbeit bzw. Kontakt mit dem Flughafen München, Anbietern am Markt für Sicherheitssysteme sowie Sicherheitsbehörden. Die Zusammenarbeit mit den Sicherheitsbehörden, aber auch die mit den Herstellern sicherheitstechnischer Systeme, erwies sich dabei allerdings als weniger ergiebig, da diese Ansprechpartner aus Geheimhaltungsgründen keine technischen Leistungskennzahlen über sicherheitskritische Systeme weitergeben konnten/durften (typisches Beispiel: Experimentell ermittelte Entdeckungsquoten von mitgeführten Waffen mittels sog. Torbogen-Sonden der Passagierkontrolle, Terahertz-Scannern u. a.). In den Testrechnungen mußten solche Leistungskennzahlen daher im Sinne von Modellannahmen simuliert werden. Dabei konnten z. T. die Angaben grober Vergleichszahlen durch die amerikanische Transportation Security Administration (TSA) in der Fachliteratur genutzt werden. Für die Demonstration der Funktionsweise und Leistungsfähigkeit der eingesetzten Risikoschätz- und –bewertungsverfahren waren diese Zahlen jedoch ausreichend.

Testrechnungen zur Optimierung des technologiegestützten Sicherheitsmanagements unter Kosteneffizienzgesichtspunkten erfolgten seit März 2009 am Beispiel ausgewählter einfacher Gefährdungsszenarien und Betriebsabläufen der Personenkontrolle (Torbogen-Sonden). Erste Präsentationen dieser und erweiterter Modelle, Simulationen, Rechnungen und Ergebnisse erfolgten bei internationalen Tagungen im Herbst 2009, wie bereits erwähnt. Die TUM-Beiträge hierzu erstreckten sich auf mathematisch-analytische und softwaregestützte numerische Modellrechnungen zur Risikostatistik und quantitativen Risikobewertung, die Optimierung von Sicherheitslösungen unter den jeweils modellierten und simulierten (technischen, organisatorischen) Betriebsabläufen sowie auf die quantitative Bewertung der Wirksamkeit und Kosteneffizienz der simulierten Sicherheitsmaßnahmen.

Parallel zu diesen Projektschritten, in denen schwerpunktmäßig die Ergebnisse der AP 1 und 2 (Tab. 1) umgesetzt wurden, verlief seit Juli 2008 die Weiterentwicklung des Formalismus zur quantitativen Risikobewertung im Rahmen des zugrundeliegenden ökonometrischen Risikomodells. Als Hauptergebnisse sind festzuhalten:

- Entwicklung eines rein analytischen Formalismus zur Berechnung der Sicherheitsäquivalente probabilistischer/statistischer Schadensverteilungen. Hiermit entfiel die (Notwendigkeit der) Bestimmung solcher „Risikopreise“ mittels numerischer Näherungsverfahren, wie dies im Projektantrag ursprünglich vorgesehen war.

- Beträchtliche Vereinfachung und Verkürzung der Programmierarbeit/Software-entwicklung hierdurch
- Erleichterung und Verbesserung aller formalen/mathematischen Verfahren hierdurch: Risikoanalyse und -bewertung, System- und Prozeßoptimierung unter Nebenbedingungen, Sensitivitätsanalyse der Ergebnisse u. a.

Softwareentwicklung und –test zur Programmierung des TUM-Formalismus zur quantitativen Risikobewertung erfolgten seit Herbst 2008 gemeinsam mit dem ckc-Projektpartner. Damit konnte schließlich ein Rechnerprogramm für diesen Teil der Projektarbeit vorgelegt werden – vollständig einsatzfähig, wenngleich noch in der einfachsten Version (April 2009).

Mit den skizzierten Projektschritten und vorläufigen Ergebnissen zeichnete sich im Herbst 2009 bereits ab, daß die angestrebten Meilenstein-Ziele (Projekt-Halbzeit, Januar 2010) im wesentlichen erreicht werden konnten. Entsprechend richtete sich die Arbeit im Teilprojekt ab Ende 2009 zunehmend auf Probleme aus AP 4 und 5. Die früher bereits erzielten Resultate wurden dann schrittweise mit den Ergebnisse aus den neuen Projektabschnitten verbunden beziehungsweise um die neuen methodischen Ansätze, Softwareentwicklungen, Szenarien und Simulationen erweitert. Hervorzuheben sind:

- Ausbau des Formalismus zur Bewertung von Sicherheitsrisiken mit mehrdimensionalen Schadensattributen (finanzielle/wirtschaftliche Verluste, Todesfallrisiken, Betriebsstörungen/-unterbrechungen usw.)
- Entwicklung eines Kostenmodells für den finanziellen, technischen und organisatorischen Sicherheitsaufwand von Flughäfen
- szenario- und rechnergestützte Pilotanwendungen zum Funktions- und Leistungsnachweis dieser erweiterten Ansätze.

In seiner Zielsetzung war das Teilprojekt davon ausgegangen, daß Sicherheitsbedrohungen gesellschaftlicher Infrastrukturen praktisch immer mehr- (hoch-)dimensional sind. Andererseits ist die methodisch fundierte, quantitative Bewertung von Risiken mit mehrdimensionalen Schadensattributen in Wissenschaft und Anwendung eine schwierige und bisher bestenfalls nur näherungsweise zu lösende Aufgabe. Problematisch ist vor allem das systematische, konsistente Abwägen von Gütern, von denen jedes einzelne zulasten der anderen geht („trade-offs“) und die im Sicherheitsmanagement zudem in aller Regel mit Risiken und Unsicherheit behaftet sind.

Zu diesem Problemkreis wurde in der zweiten Hälfte der Projektlaufzeit ein umfangreiches Manuskript [4] zu den ökonometrischen Grundlagen von „trade-offs“ zwischen risikobehafteten Gütern, Maßnahmen oder Dienstleistungen (in Teilen) erarbeitet, aber nicht ganz fertiggestellt. Der Formalismus dieser Arbeit erwies sich als zu umfangreich, um im

Rahmen des Teilprojekts bereits als Software programmiert und getestet zu werden. Einfache Anwendungsbeispiele wurden jedoch bereits von Hand durchgerechnet (Quantifizierung und gemeinsame Bewertung finanzieller Schadensrisiken und Todesfallrisiken bei einem Bombenattentat in der Abfertigungshalle eines Flughafens). Das Beispiel ist in [2] dokumentiert. Das Manuskript [4] wird derzeit zur Publikation vorbereitet. Weitergehende Anwendungen fallen unter die längerfristigen Verwertungsperspektiven des Teilprojekts und seiner Ergebnisse (s. Abschn. II.4 unten).

In Manuskript [4] sind auch die wesentlichen begrifflichen und methodischen Ansätze entwickelt und dargestellt, die auf der Basis des zugrundegelegten Risikobewertungs- und Entscheidungsmodells für die systematische Bestimmung von „trade-offs“ zwischen finanziellen/wirtschaftlichen und nichtwirtschaftlichen Gütern erforderlich sind. Auf die im Projekt angestrebten Anwendungen auf Probleme der öffentlichen/sozialen Risikotoleranz und ihrer Grenzen geht Abschnitt III. 4 ein.

Zu Planungs- und Entscheidungszwecken wird die herkömmliche lineare Risikonutzentheorie in der anwendungsorientierten Forschung gegenüber neuen, auch im Projekt verwendeten nichtlinearen Ansätzen oftmals immer noch bevorzugt (vgl. die sog. „normative Interpretation“ der linearen Risikonutzentheorie in der ökonometrischen Literatur). Daß diese „normative“ Auffassung der herkömmlichen Risikonutzentheorie auf falschen Voraussetzungen beruht, wird in einer Arbeit [5] nachgewiesen, die ebenfalls 2011 in ihren Grundzügen fertiggestellt wurde. Insbesondere im Hinblick auf die Anschlußfähigkeit der im Teilprojekt erzielten Ergebnisse trägt die Arbeit dazu bei, die methodischen Grundlagen der Risiko- und Sicherheitsforschung auf eine praxisorientierte Weise auszubauen.

Beim Schutz von Verkehrsinfrastrukturen sind, wie auch in anderen Anwendungsbereichen, die Risiken finanzieller Schadensfolgen von Fragen des Kostenaufwandes für Sicherheitsmaßnahmen zu unterscheiden. Aber auch hier stellt sich das Problem der „trade-offs“, d. h. der angemessenen Kosten (Kostenobergrenzen) für ein zu erwartendes oder erforderliches (etwa vom Gesetzgeber vorgeschriebenes) Maß an Störfall- oder Bedrohungssicherheit
von Infrastruktureinrichtungen. Für diese Fragen wurde 2011 ein Kostenmodell der Flughafensicherheitsbetriebs ausgearbeitet (Rohfassung [6]). Hervorzuheben ist hier die Kooperation mit dem Projektpartner Bauhaus Luftfahrt e. V., München. Zudem konnte hier auf die rasch wachsende Fachliteratur zu diesem Problemkreis zurückgegriffen werden. Bereits vor seiner schriftlichen Ausarbeitung wurden Elemente des Kostenmodells in den Schadensfallsimulationen und den Veröffentlichungen im SiVe-Rahmen genutzt. Aber auch dabei mußten Zahlen über Kostenumfang und Kostenstruktur des Flughafen-Sicherheitsbetriebs analog zu den verfügbaren Literaturangaben weitgehend modellhaft

konstruiert werden. Empirische Daten hierzu waren aus den Arbeitskontakten zu fachlichen, industriellen und behördlichen/administrativen Stellen kaum zu erhalten. Die Schwierigkeiten und der erhebliche Zeitaufwand bei der Beschaffung nicht nur sicherheitstechnischer, sondern auch betrieblicher und betriebswirtschaftlicher Daten ergaben sich u. a. daraus, daß die indirekten, nicht budgetierbaren Kosten des Sicherheitsmanagements von Flughafenbetreibern oft nicht erfaßt oder anderweitig beziffert werden. Umgekehrt ist das Kostenmodell für künftige Anwendungen unter günstigeren Voraussetzungen bei Bedarf praktisch beliebig erweiterungs-, ausbau-, übertragungs- und anpassungsfähig.

Schließlich fallen in den Zeitraum seit Februar 2011 Arbeiten zur Dokumentation der Simulationssoftware („SiVe-Demonstrator“): Aufbau, Funktionsweise, Format der Eingabedaten, und korrekte Interpretation der Ausgabedaten. Diese Arbeiten erfolgten hauptsächlich zusammen mit EADS München/Unterschleißheim (Cassidian) sowie der ckc AG.

Das Teilprojekt wurde um 4 Monate über die reguläre Laufzeit hinaus verlängert (Juli – Oktober 2011). In diesen Zeitraum fallen weitere Simulationsexperimente, die Ausarbeitung des mehrdimensionalen Risikoentscheidungsmodells [4] sowie eine empirische Studie zum Test des verwendeten Risikonutzenmodells in seiner ursprünglichen (eindimensionalen) Fassung [7].[3] Diese Arbeiten dienten hauptsächlich den weiterführende wissenschaftlichen Interessen an den SiVe-Ergebnissen und an deren Verwendung in künftigen Projekten (Forschung, Kooperationen mit Industrie und Dienstleistern) und der akademischen Ausbildung.

Eine zusammenfassende Ergebnis- und Nutzenbilanz des Teilprojekts findet sich unten in Abschnitt II.4.

2. Die Positionen des zahlenmäßigen Nachweises

Die finanziellen Zuwendungen für das Teilprojekt erstreckten sich gemäß des BMBF-Bewilligungsbescheides auf insgesamt 5 Positionen:

- Personalausgaben
- die Vergabe von Aufträgen
- allgemeine Verwaltungsausgaben
- die Beschaffung von Gegenstände im Wert von mehr als € 400,– im Einzelfall
- Reisekosten.

[3] Die Frage war, inwieweit das verwendete Risikonutzenmodell das individuelle Risikoverhalten beschreibt – ein Problem der Verhaltensökonomik, das für Risikomanagementanwendungen des Modells von erheblicher praktischer Bedeutung ist.

Hinzu kam die Bewilligung einer Projektpauschale zum Jahresbeginn 2011, die von der Hochschule „zentral zugeordnet und verausgabt“ wurde.

Aufträge an Dritte wurden im Teilprojekt keine vergeben, die Mittel für die Beschaffung von Gegenständen wurden lediglich in 2 Fällen in Anspruch genommen. Bei allen 3 übrigen Positionen blieben die Ausgaben hinter den bewilligten Beträgen zurück, z. T. sogar deutlich wie bei den Reisekosten, die den bewilligten Betrag um etwa 50% unterschritten. Trotz der gewährten Laufzeitverlängerung des Teilprojekts um 4 Monate wurden rund € 11.000,– von den insgesamt gewährten Bundesmitteln in Höhe von € 329.560,– nicht ausgegeben.

3. Notwendigkeit und Angemessenheit der durchgeführten Projektarbeiten

Die im Teilprojekt durchgeführten Arbeiten hielten sich nach Zielsetzung, Ablauf und erwartetem Ergebnis fast ausnahmslos im Rahmen des Projektantrags. Gelegentlich gingen sie – wie etwa bei der Erweiterung des zugrundegelegten Risikobewertungs- und Entscheidungsmodells auf den mehrdimensionalen Fall – über die ursprüngliche Zielsetzung hinaus. Einige andere, allerdings weniger zentrale Aufgaben konnten nicht vollständig im geplanten Umfang gelöst werden (vgl. Abschn. III.4 unten). Die Kriterien der Notwendigkeit und Angemessenheit blieben dabei jedoch in vollem Umfang gewahrt.

4. Nutzen und Verwertbarkeit der erzielten Resultate

Insgesamt gesehen zeigt sich der Nutzen des Teilprojekts vor allem in der nachgewiesenen Praxistauglichkeit des methodischen Instrumentariums für das wirksame und kosteneffiziente Sicherheitsmanagement. Anhand von Fallstudien konnte gezeigt werden, daß mit diesem Instrumentarium Erkenntnisse und Sicherheitslösungen unmittelbar möglich sind, die nach dem oben skizzierten Stand der Wissenschaft nicht oder nur näherungsweise zu erzielen gewesen wären. Aus wissenschaftlicher Sicht kann somit für das Teilprojekt die angestrebte methodische Innovationsleistung insofern festgestellt werden, als neuartige, leistungsfähige Methoden und Ergebnisse der Grundlagenforschung für die sicherheitsorientierten Organisations- und Planungswissenschaften zugänglich gemacht wurden. Unter praktischen Gesichtspunkten konnte anhand von ausgewählten, aussagekräftigen Fallbeispielen der Nachweis eines erheblichen Anwendungsnutzens geführt werden.

Der sicherheitswissenschaftliche Ertrag des Teilprojekts ist auf vielfältige Weise in den Aufgabenbereichen der Hochschule verwertbar. Die TUM unterhält zahlreiche Kooperationsbeziehungen u. a. zu Industrieunternehmen und Wirtschaftsverbänden, die ihrerseits an den Pilotstudien und Ergebnissen des Projekts ein weitergehendes Interesse haben. Die TUM kann ihr Wissens- und Technologietransferangebot durch die

Projektergebnisse um wesentliche, innovative Komponenten der Risiko- und Sicherheitsforschung erweitern, für die der öffentliche und privatwirtschaftliche Bedarf auf der Hand liegt. Insbesondere gilt dies für die Unternehmen des Bayerischen Verbandes für Sicherheit in der Wirtschaft (BVSW) und – damit – für den deutschen Dachverband, die Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW). Weiterhin profitiert die wissenschaftliche und wirtschaftliche Anschlußfähigkeit des Projekts von der allgemeinen Anwendbarkeit der Simulationstools und des Risikomodells, die nicht auf Probleme der (Verkehrs-) Infrastruktursicherheit eingeschränkt ist. An erster Stelle stehen hier die Sicherheitsbelange der Finanzwirtschaft (operationelle und finanz–/versicherungswirtschaftliche Risiken), die sich im wesentlichen mit den gleichen Methoden der rechnergestützten Prozeßsimulation und ökonometrischen Bewertung behandeln lassen.

Schließlich liegen aus der Sicht der Hochschule wichtige Anschluß- und Verwertungsmöglichkeiten für die Projekterträge in der Weitergabe und Fortentwicklung im Rahmen der akademischen Lehre und Ausbildung.

5. Initiativen, Projekte und Forschungsergebnisse anderer Forschungseinrichtungen

Thematisch gab es Berührungspunkte zwischen SiVe und den anderen BMBF-geförderten Vorhaben zur Sicherheit von Verkehrsinfrastrukturen, insbesondere den erwähnten Projekten „FluSs“ und „Critical Parts“ zur Flughafensicherheit. Nennenswerte Überschneidungen mit den Aufgaben und Zielen des TUM-Teilprojekts waren dabei jedoch nicht zu erkennen. Dies gilt insbesondere im Hinblick auf die quantitativen Modelle der Risikobewertung und erst recht für die der Kosteneffizienzrechnung der Sicherheitsplanung und -organisation, die im Teilprojekt zum Einsatz kamen. In diesen Fragen verhalten sich die Forschungsfelder der verschiedenen Projekte eher komplementär denn sich wechselseitig überschneidend.

Ähnliche Feststellungen gelten für die EU-geförderte Sicherheitsforschung im FP7. Dieses Forschungsprogramm umfaßt zwar neben dem Aufgabengebiet „Infrastruktursicherheit“ auch ein eigenes Schwerpunktthema „Sicherheitsökonomik“, das jedoch nicht die ausgeprägte ökonometrische Methodenorientierung des TUM-Teilprojekts aufweist. Eine Ausnahme bildet das oben erwähnte EU-Projekt „ValueSec“ (seit Februar 2011), in dem jedoch SiVe-Partner – darunter ein Mitarbeiter (G. G.) des TUM-Teilprojekts – die ökonometrischen Arbeiten weiterführen. Hier ist das SiVe-Teilprojekt die eindeutig frühere Forschungsaktivität, und statt Konkurrenz steht die Kontinuität der Forschungsarbeit im Vordergrund.

6. Veröffentlichung der Projektergebnisse

Tabelle 2 enthält eine Liste der bereits veröffentlichten und zur Veröffentlichung vorgesehenen SiVe-Arbeiten, zu denen das Teilprojekt beigetragen hat. Weiterhin sind Manuskripte und Materialien aufgelistet, die in künftigen Arbeiten zum Thema des Teilprojekts weitergeführt, ergänzt oder sonst in geeigneter Form weiterverwendet werden sollen. Sofern sie in Publikationen Eingang finden, wird auf ihre Entstehung im Teilprojekt und auf die BMBF-Förderung hingewiesen. Dies gilt insbesondere für [6]. Inhaltsangaben der einzelnen Veröffentlichungen und Manuskripte finden sich in Anlage 2.

Tab. 2: Liste der Veröffentlichungen sowie zur Veröffentlichung vorgesehener/ vorbereiteter Manuskripte

[1] G. Geiger, E. Petzel und M. Breiing, “Process-Based Identification and Pricing of Risks: Methodological Foundation and Applications to Risk and Security Management”. In P. Elsner (Hg.): Future Security – 4th Security Research Conference. Fraunhofer Verlag, Stuttgart 2009, S. 208-220.

[2] M. Breiing, M. Cole, J. D’Avanzo, G. Geiger, S. Goldner, A. Kuhlmann, C. Lorenz, A. Papproth, E. Petzel und O. Schwetje, “Optimisation of Critical Infrastructure Protection: The SiVe Project on Airport Security”. In E. Rome und R. Bloomfield (Eds.): CRITIS 2009. Lecture Notes in Computer Science 6027. Springer-Verlag, Berlin-Heidelberg 2010, S. 73–84.

[3] S. Goldner, A. Papproth, E. Petzel und G. Geiger, “Improving the Security of Critical Transport Infrastructures - New Methods and Results”. In J. Ender und J. Fiege (Hg.): 6th Future Security Research Conference – Proceedings. Fraunhofer Verlag, Stuttgart 2011, S. 545-554.

[4] G. Geiger, “Multi-Attribute Non-Expected Utility”, Manuskript 2011, 45 S. Zur Publikation vorbereitet.

[5] G. Geiger, “The Independence Axiom of Expected Utility Theory Generally Invalid as a Principle of Rational Choice under Risk”. Manuskript 2011, 17 S. Zur Veröffentlichung vorgesehen.

[6] G. Geiger, „Kostenmodell Flughafensicherheit“. Arbeitspapier/Manuskript 2011, 14 S. Materialien für Modellbildung, Simulation und weitere Veröffentlichungen.

[7] P. Schaller, „Variability of individual risk preferences – Empirical tests“. Arbeitspapier/ Manuskript 2011, 14 S.

Anlage 2: Kurzfassungen der veröffentlichten Projektergebnisse sowie zur Veröffentlichung vorbereiteter / vorgesehener Manuskripte / Materialien

Process-Based Identification and Pricing of Risks: Methodological Foundations and Applications to Risk and Security

Authors

G. Geiger[1], E. Petzel and M. Breiing[2]

Affiliations

[1] Technische Universität München, Fakultät für Wirtschaftswissenschaften, Institut für Finanzmanagement und Kapitalmärkte, Arcisstrasse 21, 80333 München, Germany

[2] Institut für Risiko- und Prozessmanagement GmbH, Bubenreuther Strasse 18, 91083 Baiersdorf, Germany

Journal / Conference Volume

P. Elsner (Ed.): Future Security – 4th Security Research Conference

Abstract

Risk and security management requires planning and decision-making under risk and uncertainty. It has long been suffering from the fact that risk is an elusive concept and from methodological inadequacies for the identification and evaluation of all relevant risks. Correspondingly, conventional methods of assessing risks and risk reduction measures tend to be unreliable and controversial, if not manifestly inconsistent, and the quality of the assessments is questionable. In view of this situation, an innovative risk assessment methodology is presented as a security incident prevention and management device. It draws on recently developed approaches to process-based risk identification and quantitative risk assessment. To optimise security planning and decision-making, we simulate risk events and occurrences of security incidents using computer-based probabilistic models (process models with integrated dynamic random variables). The simulation techniques are

specifically devised to analyse the likely consequences of risk events and attack scenarios, and risk planning measures to prevent them, in application settings typically arising in the risk and security management of large-scale systems and public infrastructures. In a first step, the likely losses and gains from risky decisions in security management are conceptualised as random variables with probability density functions. Computations are done by means of Monte Carlo simulation of risk process models based on information about the systems, processes and variables of interest such as profit, loss or any other kind of utility. The method is not limited to the use of any specific type of variable such as a monetary one. It also allows the computation of the joint distribution of two or more random variables. In a second step, these distributions are assessed by a probability-dependent utility function. The core concept of quantitative risk assessment is the pricing of risk, where the fair, or “intrinsic” price of a risk is the so-called certainty equivalent of that risk. Accordingly, alternative arrangements for risk provision and mitigation can be “priced”, that is, assigned to a certainty equivalent for each one, whereby such intrinsic risk prices can be systematically and consistently calculated and compared. Comparison with the risk inherent in the status quo (i.e. current state of affairs prevailing if nothing is done), gives the effectiveness of the measures planned. Taking the cost of a specific security measure into account, one can calculate the cost-efficiency of risk management, that is, the amount of risk reduction achieved per euro invested. This approach is profoundly scaleable with respect to system or process complexity, and diverse individual needs and preferences.

Publisher

Fraunhofer Verlag, Stuttgart 2009

Optimisation of Critical Infrastructure Protection: the SiVe Project on Airport Security

Authors

M. Breiing[1], M. Cole[2], J. D'Avanzo[3], G. Geiger[4], S. Goldner[5], A. Kuhlmann[2], C. Lorenz[6], A. Papproth[6], E. Petzel[1], O. Schwetje[2]

Affiliations

[1] ckc AG, Am Alten Bahnhof 13, 38122 Braunschweig, Germany

[2] Bauhaus Luftfahrt, Boltzmannstrasse 15, 85748 Garching b. München, Germany

[3] EADS Deutschland GmbH, EADS Innovation Works, 81663 München, Germany

[4] Technische Universität München, Fakultät für Wirtschaftswissenschaften, Institut für Finanzmanagement und Kapitalmärkte, Arcisstrasse 21, 80333 München, Germany

[5] EADS Deutschland GmbH, Defence & Security, System Design Centre Germany, 85716 Unterschleißheim, Germany

[6] Fraunhofer-Anwendungszentrum für Logistiksystemplanung und Informationssysteme, Konrad-Wachsmann-Allee 1, 03046 Cottbus, Germany

Journal / Conference Volume

E. Rome and R. Bloomfield (Eds.): CRITIS 2009. Lecture Notes in Computer Science 6027

Abstract:

This paper outlines the scientific goals, ongoing work and first results of the SiVe research project on critical infrastructure security. The methodology is generic while pilot studies are chosen from airport security. The outline proceeds in three major steps, (1) building a threat scenario, (2) development of simulation models as scenario refinements, and (3) assessment of alternatives. Advanced techniques of systems analysis and simulation are employed to model relevant airport structures and processes as well as offences. Computer experiments are carried out to compare and optimise alternative solutions. The optimality analyses draw on approaches to quantitative risk assessment recently developed in the operational

sciences. To exploit the advantages of the various techniques, an integrated simulation workbench is build up in the project.

Publisher

Springer-Verlag, Berlin-Heidelberg 2010

Improving the Security of Critical Transport Infrastructures: New Methods and Results

Authors

S. Goldner[1], A. Papproth[2], E. Petzel[3], G. Geiger[4]

Affiliations

[1] CASSIDIAN Germany, 85716 Unterschleißheim, Germany

[2] Fraunhofer-Anwendungszentrum für Logistiksystemplanung und Informationssysteme, Konrad-Wachsmann-Allee 1, 03046 Cottbus, Germany

[3] Institut für Risiko- und Prozessmanagement GmbH, Bubenreuther Strasse 18, 91083 Baiersdorf, Germany

[4] Technische Universität München, Fakultät für Wirtschaftswissenschaften, Institut für Finanzmanagement und Kapitalmärkte, Arcisstrasse 21, 80333 München, Germany

Journal / Conference Volume

J. Ender and J. Fiege (Eds.): 6th Future Security Research Conference – Proceedings

Abstract

As one of the critical infrastructures of modern society, air transport has become a prevalent target of terrorist attacks. Exposure to terrorist threat is particularly high for international airports since they provide the operational bases of large-scale air traffic. SiVe (Verbesserung der Sicherheit von Verkehrsinfrastrukturen) is a research project co-funded by the German Federal Ministry of Education and Research which aims to develop an innovative methodology of risk management suitable to optimise critical infrastructure protection. It starts from the fact that, on the one hand, airport security management is increasingly being forced to combine advanced security standards with cost efficiency in a more closely-knit and systematic way, while, on the other hand, measurements of the effectiveness and efficiency of risk reduction provisions continue to pose considerable methodological problems. This paper describes the scientific goals and the essential

research findings of the SiVe project on the

basis of a concrete case study. The newly developed methodology is generic while pilot application examples are chosen from airport security.

Publisher

Fraunhofer Verlag, Stuttgart 2011

Multi-Attribute Non-Expected Utility

Author

G. Geiger

Affiliation

Technical University of Munich, Faculty of Economics, Institute of Financial Management and Capital Markets, Arcisstrasse 21, 80333 München, Germany

Journal / Conference Volume

Manuscript, 2011, prepared for submission

Abstract

In management applications of risk theory, planning and decision making are typically concerned with complex multi-dimensional attributes of risk and utility trade-offs between them. This paper presents a novel approach to multi-attribute non-expected utility which is especially designed to serve application and risk management purposes. It is based on a recently developed non-expected utility model that accommodates systematic violations of expected utility of various kinds observed in risky choice experiments. In the model, the possible outcomes of risky decisions are assumed to be multi-dimensional, that is, classified, measured, compared and assessed from different economic and non-economic perspectives simultaneously. Of the risk attributes to be jointly evaluated in a decision problem, each is supposed to be utility independent of the complementary set of all the other attributes also considered. Mutual utility independence and additive independence are characterised as special, more pronounced forms of utility independence. An order-preserving preference functional exists if the agent's risk preferences satisfy familiar rationality requirements. The functional provides a consistently scaled, multi-linear representation in terms of single-attribute probability-dependent utility functions. Finally, the formalism is applied to explain observed trade-offs between monetary benefits obtained, and fatalities incurred, in the operation of large-scale industrial systems.

The Independence Axiom of Expected Utility Theory Generally Invalid as a Principle of Rational Choice under Risk

Author

G. Geiger

Affiliation

Technical University of Munich, Faculty of Economics, Institute of Financial Management and Capital Markets, Arcisstrasse 21, 80333 München, Germany

Journal / Conference Volume

Manuscript, 2011, prepared for submission

Abstract

The normative interpretation of expected utility theory is rejected as a guideline for rational planning and decision making under risk. To serve as a general guiding principle, expected utility maximisation would have to take constraints of the application context on dynamic choice into account that are incompatible with the independence axiom. The incompatibilities arise from the presence of background risks in combination with uncertain risk duration in sequential choice problems. Expected utility maximisation constitutes a kind of “pure” theoretical rationality abstracting from basic practical dimensions of choice under risk.

Kostenmodell Flughafensicherheit: Materialien, allgemeine Prinzipien, Festlegungen für Szenarien in der Beschreibung der SiVe-Simulationssoftware

Autor

G. Geiger

Technische Universität München, Fakultät für Wirtschaftswissenschaften, Institut für Betriebswirtschaftslehre / Finanzmanagement und Kapitalmärkte, Arcisstrasse 21, 80333 München

Arbeitspapier

Materialien für Modellbildung, Simulation und bereits erfolgte / künftige Veröffentlichungen

Kurzfassung

Das im folgenden dargestellte Kostenmodell mit den unterlegten Parameterwerten bezieht sich auf das Szenario „Personen-/ Sprengstoffscanner“ und die Simulationsexperimente auf der Grundlage dieses Szenarios. Für andere Szenarien müssen die zugehörigen Kostenmodelle für Sicherheitsmaßnahmen ähnlich, wenngleich separat entwickelt werden. Das folgende Kostenmodell kann hierfür als Ausgangsbasis dienen. Die Kosten für die Personen- und Gepäckkontrolle, die ein Flughafen aufwenden muß, werden durch den Beschaffungspreis des einzelnen Scanner-Gerätes und durch die Stundenlöhne des Betriebspersonals eines Scanners allein nicht ausreichend erfaßt. Die Flughafensicherheit hängt vielmehr wesentlich davon ab, daß alle abfliegenden Passagiere überprüft werden, d. h. sie hängt von der Gesamtzahl der hierfür erforderlichen Geräte ab. Den zutreffenden Kostenindikator liefern somit die Gesamtkosten (Anschaffung, Betrieb, Infrastruktur usw.) aller für einen Flughafen und dessen Abfertigungskapazität erforderlichen sicherheitstechnischen Geräte. Deren Anzahl hängt wiederum vom Passagieraufkommen, der Dauer der Betriebszeiten (pro Tag, pro Jahr), der Abfertigungskapazität aller eingesetzten Scanner usw. ab. Entsprechend treten weitere, ganz wesentliche Kostenfaktoren hinzu: Störungen / Verzögerungen des gesamten Abfertigungs- und Flugbetriebs (Starts) durch falsche Scanneralarmsignale, der gesamte Verwaltungs- und technische Aufwand für das screening, die Kosten für die technische und räumliche Infrastruktur (Verkabelung, Datenverarbeitung, Räumlichkeiten für Personen- und Gepäckkontrollen), für den Stromverbrauch usw. Was für ein solches Modell benötigt wird,

sind explizite Darstellungen dessen, wie die Kosten aus den Sicherheitsprozessen entstehen bzw. diesen Prozessen zugeordnet sind. Die Orientierung an vorhandenen Kostenmodellen in der Literatur führt in der folgenden Darstellung zunächst zu einem recht komplizierten Formalismus, der hier jedoch insofern uneingeschränkt wiedergegeben wird, als er für künftige Modelle und Anwendungen ohne „voreilige“ Näherungen als möglichst breite Ausgangsbasis zur Verfügung stehen sollte. Näherungen und Kürzungen können dann später – passend zum jeweiligen Anwendungsfall – vorgenommen werden.

Variability of individual risk preferences: empirical tests

Author

Philipp Schaller

Affilitation

Technische Universität München, Fakultät für Wirtschaftswissenschaften, Institut für Finanzmanagement und Kapitalmärkte, Arcisstrasse 21, 80333 München, Germany

Working paper, 2011

Abstract

The present work has been carried out to exploit the SiVe results for the specific purposes of risk management in the field of business administration. An empirical survey has been devised and carried out to establish whether the risk assessment theory employed in SiVe can also be successfully applied to explain basic patterns of risk-taking in financial decision making. Furthermore, the theory has been applied to the observed behavioural variability in risk-taking constrained by basic individual dispositions such as age and current wealth and income of the decision maker. Although this research needs to be carried on further, the findings obtained thus far are encouraging. They indicate that, besides perceptions of potential loss and probability of loss as the classical impact factors of risky choice, other constraints on economic ("rational") planning and decision making are important. They help to make these constraints explicit and accessible to systematic, empirical (statistical) research,