Verbundprojekt
Verbesserung der Sicherheit von Verkehrsinfrastrukturen

Teilvorhaben
Expertensystem für das Risikomanagement Kritischer Infrastrukturen

Szenariengestützte stochastische, ereignisorientierte Simulation zur quantitativen Risikoanalyse sowie Methoden- und Modellverbund zum effektiven und effizienten Management (Planung, Realisation und Kontrolle) Kritischer Infrastrukturen

Schlussbericht des BMBF Projekts FKZ 13N10031

Sönke Thoms, ckc AG
Roman Czaja, ckc AG
Prof. Dr. Erhard Petzel, IRPM GmbH

Mittwoch, 22. Februar 2012

Schlussbericht des BMBF Projekts FKZ 13N10031

Verbundprojekt
Verbesserung der Sicherheit von Verkehrsinfrastrukturen

Verbundkoordination
EADS Deutschland GmbH
Ansprechpartner: Dr. Dirk Dickmanns

Projektpartner
Bauhaus Luftfahrt e.V.
Ansprechpartner: Dr. Andreas Kuhlmann

ckc AG
Ansprechpartner: Sönke Thoms

EADS Deutschland GmbH
Ansprechpartner: Dr. Dirk Dickmanns

Flughafen München GmbH
Ansprechpartner: Thomas Ross

Fraunhofer Anwendungszentrum für Logistiksystemplanung
Ansprechpartner: Prof. Dr.-Ing. Uwe Meinberg

Technische Universität München - Lehrstuhl für Betriebswirtschaftslehre/ Finanzmanagement
Ansprechpartner: Prof. Dr. Gebhard Geiger

1. KURZDARSTELLUNG DES PROJEKTS

1.1. Gegenstand und Aufgabenstellung des Projektes

Das Teilvorhaben betraf alle Arbeitspakete des Gesamtvorhabens, wobei klare Schwerpunkte durch die gemeinsame Planung aller Projektpartner gesetzt waren. Daher wird im Folgenden auf die Aufgabenstellung des Gesamtvorhabens Bezug genommen. Demnach waren folgende Aufgaben zu erfüllen:

1. Förderung der Sicherheit der deutschen Verkehrsinfrastruktur durch eine umfassende Bedrohungsanalyse mit dem Ergebnis der Beschreibung und Analyse aktueller und künftiger Bedrohungsszenarien.
2. Beschreibung und Analyse aktueller und neuer Schutzmechanismen (Technik und Organisation) zur Früherkennung von Gefahren und Realisation einer geeigneten Gefahrenabwehr inklusive ethischer und ökonomischer Aspekte.
3. Risiko- und sicherheitsorientierte Systemanalyse durch die Anwendung neuer Modelle und Methoden im Rahmen einer umfassenden simulationsgestützten risikoorientierten Systemanalyse mit dem Ziel der Quantifizierung der erzielbaren Risikoreduktionen und des Restrisikos und der Beurteilung der Kosteneffizienz der Sicherheitslösungen
4. Entwicklung eines Methoden- und Modellverbundes auf der Basis einer zu konzipierenden Fach- und Informationsarchitektur für das Risikomanagement Kritischer Infrastrukturen, um optimale Systemlösungen für die Flughafensicherheit zu erreichen.
5. Konzeption und Implementation eines Demonstrators als computergestütztes Expertensystem zum Risikomanagement Kritischer Infrastrukturen.
6. Durchführung szenarienbasierter Simulationsstudien und quantitative Risikobewertungen zur Validierung des entwickelten Gesamtsystems.

Schwerpunkte des Projektes waren die Aufgabenstellungen entsprechend den oben aufgeführten Punkten 3 bis 6, während an den Aufgabenstellungen 1 und 2 mitgewirkt wurde. Die folgende Abbildung zeigt die Aufgabenstellungen des Teilvorhabens im Kontext des Gesamtprojektes zum Projektbeginn. Während des Vorhabens wurde jedoch entschieden, auch die Erstellung von Szenarien mittels einer Anwendungssoftware zu

unterstützen. Der von Partner Bauhaus Luftfahrt e.V. entwickelte Scenario Builder wurde dann ebenfalls in den Demonstrator integriert.

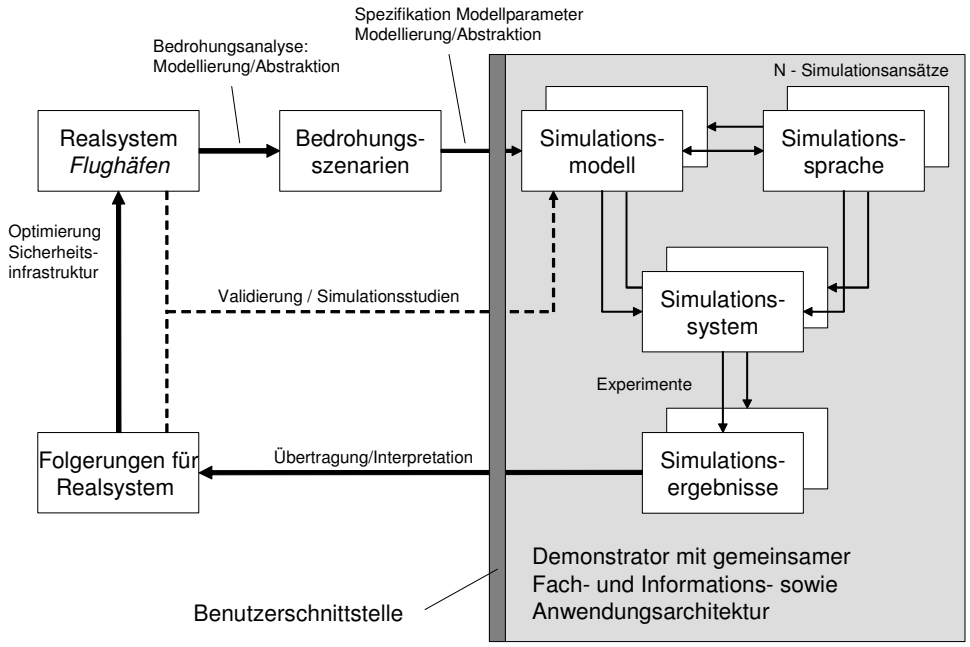

Abb. Aufgaben des Teilvorhabens im Kontext des Gesamtprojektes

Hinsichtlich des Punktes 3 war zunächst die Weiterentwicklung und Implementation eines neuen stochastischen, ereignisorientierten Simulationssystems vorzunehmen, welches auf der Methodik der Prozessanalyse zum Design und zur Optimierung von Systemen beruht und dafür geeignet ist, empirisch fundierte quantitative Risikoanalysen auf der Basis von Bedrohungsszenarien durchzuführen. Zentrale Aufgabenstellung war dabei die Umsetzung von Bedrohungsszenarien in Simulationsmodelle, die mittels des Simulatonssystems direkt ausführbar sein sollten. Als Simulationsergebnisse sollten spezifische Schadensverteilungen für das ausgewählte Szenario berechnet werden. Diese Schadensverteilungen stellten zugleich die Grundlage für die Quantifizierung der erzielbaren Risikoreduktionen und des Restrisikos sowie der Beurteilung der Kosteneffizienz der Sicherheitslösungen dar.

Das Simulationssystem bildete somit den Kern des angestrebten Methoden- und Modellverbundes (Pkt. 4 lt. obiger Liste), welcher mittels der Entwicklung einer entsprechenden Fach- und Informationsarchitektur (EADS-Teilprojekt) zu einem computergestützten Expertensystem zum Risikomanagement Kritischer Infrastrukturen auszubauen und in Form eines lauffähigen Demonstrators (Pkt. 5 lt. obiger Liste) zu realisieren war. Der zu erstellende Demonstrator sollte die Leistungsfähigkeit des

Verbundes mehrerer, teilweise neu zu entwickelnder Methoden für das Risikomanagement von Verkehrsinfrastrukturen unter Beweis stellen und so konzipiert sein, dass er auch auf andere Verkehrsinfrastrukturen angewendet werden kann. Dazu waren die teilweise erst im Projekt zu entwickelnden Softwaremodule funktionell und datentechnisch zu integrieren, ohne dass die selbstständige Nutzbarkeit der Einzelmodule verloren gehen sollte.

Die letzte Hauptaufgabe (Pkt. 6) war die Durchführung gemeinsamer Simulationsstudien mit dem Ziel, die Gesamtmethodik theoretisch und praktisch unter der Verwendung von Bedrohungsszenarien zu validieren und zugleich für die Anwender wertvolle Aussagen zur Optimierung der Sicherheitsinfrastruktur zu liefern. Die Simulationsstudien haben zum Ergebnis, welche Risiken mit welchem Schadensausmaß beim Eintreten von bestimmten Bedrohungsszenarien und dem Einsatz unterschiedlicher Sicherheitsmaßnahmen zu erwarten sind und wie diese von den Gegebenheiten des Flughafenbetriebes und der Verfügbarkeit von Einsatzkräften abhängen.

1.2. Voraussetzungen des Projekts

Für eine erfolgreiche Projektrealisierung brachte die ckc AG als erfahrener IT-Dienstleister die besonders wichtige Expertise hinsichtlich der Realisierung verteilter Systeme sowie das erforderliche Integrations-Know-How ein, denn ein verteilt verfügbares Expertesystem zum Risiko- und Sicherheitsmanagement Kritischer Infrastrukturen existierte in der geplanten Form bisher noch nicht. Außerdem konnte die ckc AG auf Informatiker zurückgreifen, welche tiefergehende Erfahrungen bei der Implementation von Sprach- und Modellkonstrukten hatten. Damit waren die besonderen IT-fachlichen Voraussetzungen gegeben, um die Projektziele zu erreichen.

Hinsichtlich der Entwicklung von Sprach- und Modellkonstrukten konnte mittels eines Unterauftrages auf das Know-How des Institutes für Risiko- und Prozessmanagement GmbH zurückgegriffen werden. Dieses Institut wird von Prof. Dr. Petzel geleitet, der sich seit dreizehn Jahren mit der Entwicklung von Konzepten zum Risiko- und Sicherheitsmanagement befasst und im Rahmen seiner Forschungsarbeit erste Grundlagen für eine spezielle Simulationssprache für die Risikoanalyse entwickelt hat. Damit waren vor allem die notwendigen theoretischen Kenntnisse für die Entwicklung des Simulationssystems als wichtige Voraussetzung für den Erfolg des Projektes vorhanden.

Schließlich konnten sich sowohl die ckc AG als auch das Institut für Risiko- und Prozessmanagement GmbH auf vielfältige Erfahrungen in Forschungs- und Entwicklungsprojekten stützen, so dass ein professionelles Projektmanagement das Erreichen der Projektziele von Beginn an sicherstellen konnte. Insgesamt waren somit die fachlichen und personellen Voraussetzungen für eine erfolgreiche Projektarbeit im Zusammenwirken mit den anderen Partnern vollumfänglich gegeben.

1.3. Planung und Ablauf des Projektes

Die zeitliche Ablaufplanung des Teilprojekts sah gemäß dem Projektantrag eine Aufteilung in fünf Arbeitspakete vor (vgl. folgende Tabelle). Dieser Ablaufplan konnte weitgehend erfüllt werden. Geringfügige Abweichungen waren durch die Erkenntnisse und Erfahrungen aller Partner im Laufe des Projektes notwendig, aber sie hielten sich im Rahmen der definierten Projektaufgaben.

AP 1: Bedrohungsszenarien	**7/2008 – 6/2009**
AP 1.1: Definition und Spezifikation von Bedrohungsszenarien (Systematik) und Festlegung von Messgrößen sowie Modell- u. Simulationsparametern. AP 1.2: Auswahl und Festlegung geeigneter Testszenarien. AP 1.3: Entwicklung konzeptueller Modellelemente zur Abbildung von Bedrohungsszenarien. AP 1.4: Implementation konzeptueller Modellelemente zur Abbildung von Bedrohungsszenarien in Simulationsmodellen	
AP 2: Schutzmechanismen	**10/2008 – 12/2009**
AP 2.1: Spezifikation bestehender und neuer Schutzmechanismen. AP 2.2: Entwicklung konzeptueller Modellelemente zur Abbildung von Schutzmechanismen. AP 2.3: Implementation konzeptueller Modellelemente zur Abbildung von Schutzmechanismen.	
AP 3: Risiko- und sicherheitsorientierte Systemanalyse	**1/2009 - 1/2010**
AP 3.1: Spezifikation und Abbildung von Strukturen und Prozessen AP: 3.2: Entwicklung konzeptueller Modellelemente zur Abbildung von Sicherheitsinfrastrukturen. AP 3.3: Implementation konzeptueller Modellelemente zur Abbildung von Sicherheitsinfrastrukturen. AP 3.4: Durchführung von Simulationsstudien und Validierung der Ergebnisse.	
AP 4: Modell- und Methodenintegration	**1/2010 – 1/2011**
AP 4.1: Entwurf der Systemarchitektur und Systemintegration AP 4.2: Entwicklung eines Konzeptes zum Risikomanagement Kritischer Infrastrukturen. AP 4.3: Implementation der Erweiterungen des Simulationssystems bzw. der einzelnen Modellansätze hinsichtlich eines integrierten	

Ansatzes. AP 4.4: Konzeption, Implementation und Test einer gemeinsamen Benutzerschnittstelle. AP 4.5: Realisierung und Test des Demonstrators. AP 4.6. Theoretische Validierung der Gesamtmethodik.	
AP 5: Szenarienorientierte Systemsimulation, quantitative Risikobewertungen	**7/2010 – 10/2011**
AP 5.1: Analyse und Bewertung von ausgewählten Bedrohungsszenarien. AP 5.2: Durchführung von Sensitivitätsanalysen.	

Hierzu gehörte zum Einen die Erkenntnis, dass die Definition, Spezifikation und Auswahl von Bedrohungsszenarien kaum vollständig ohne Rechnerunterstützung zu leisten ist. Daher wurde vom Partner Bauhaus Luftfahrt e.V. eine Applikation entwickelt, die zusätzlich in den Demonstrator zu integrieren war. Die Implementation der Modellelemente erfolgte im oben bereits genannten Scenario Builder. Dieser wurde zunächst als Prototyp in Excel erstellt, später jedoch durch eine Java-Applikation abgelöst. Aus diesem Grunde wurde zunächst eine Excel-Schnittstelle in das Simulationssystem implementiert, die dann später zum Zwecke der Systemintegration nicht mehr notwendig war.

Ferner war nicht vorn vorneherein klar, mit welcher Modellierungssprache die Spezifikation von Schutzmechanismen am besten zu realisieren war. Zunächst wurde daher von einem zweistufigen Modellierungsansatz ausgegangen. In der ersten Stufe sollten die Schutzmechanismen mittels der EPK-Notation modelliert werden und dann hinsichtlich der Simulationsfähigkeit in einer zweiten Stufe erweitert werden. Bei der Modellierung mit der EPK-Notation erwies sich jedoch die mögliche Parallelität und die gegenseitige Beeinflussbarkeit von Sicherheits- und Alarmprozessen als unzureichend darstellbar. Daher wurde auf die BPMN-Notation gewechselt, was ein Umarbeiten der Modelle sowie die Implementierung einer zusätzlichen Schnittstelle im Simulationssystem bedeutete.

Weiterhin wurde zusammen mit dem Projektpartner TU München im Frühstadium des Projektes die vorliegende theoretische Grundlagenarbeit von Prof. Dr. Geiger hinsichtlich der Risikomodellbildung und -bewertung als Software implementiert, um frühzeitig erste Ergebnisse für Kongresse und Publikationen präsentieren zu können und das Projektrisiko zu minimieren.

Die kostenneutrale Verlängerung der Projektlaufzeit um 4 Monate wurde insbesondere zur Optimierung der Performance des Simulators genutzt, da dies während der laufenden Entwicklung und Integration der anderen Komponenten nicht möglich war.

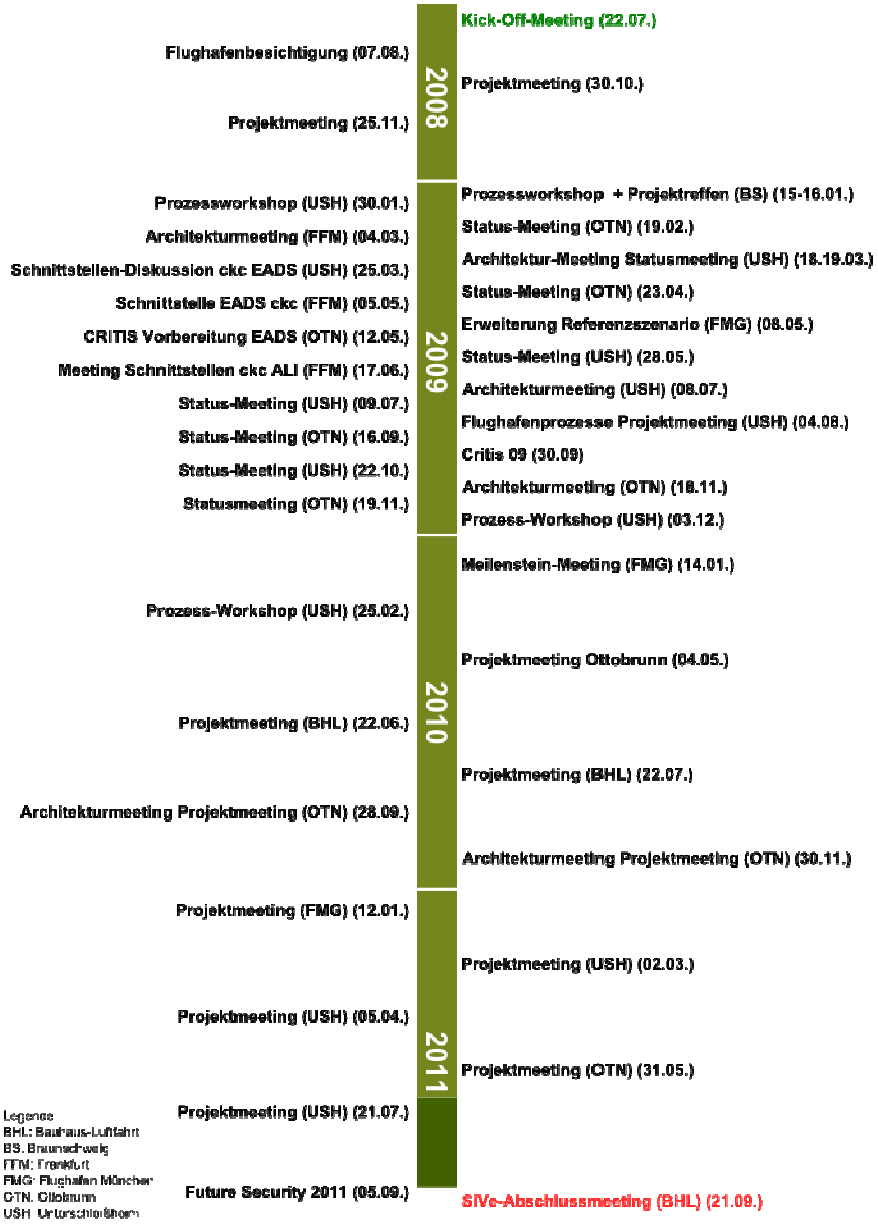

Abb. Ablaufplan des SiVe-Projektes

Die obige Abbildung zeigt auf, dass der Ablauf des Teilprojekts von den häufigen, regelmäßigen Arbeitssitzungen zur Planung und Koordination der Projektabschnitte geprägt war. Diese Sitzungen fanden vorwiegend an den Münchener Standorten des Koordinators EADS statt. Nur durch eine solche Koordination war ein zügiger, reibungsloser und immer zielorientierter Projektablauf möglich. Ergänzend dazu fanden fast wöchentlich Telefonkonferenzen der Partner statt.

In der ersten Projektphase 2008 wurden vor allem die von den Partnern verfolgten Konzepte und vorgesehenen Softwarekomponenten vorgestellt. Ihre Ziele, Potenziale und Funktionsweise wurden gegenseitig erläutert und gemeinsam an der Systemanalyse des Flughafens gearbeitet. In dieser Phase wurde die Entscheidung getroffen, dass auch die Entwicklung von Szenarien rechnergestützt erfolgen soll.

Ab 2009 rückte die Prozessmodellierung und der Vergleich und die Auswahl der Modellierungssprache sowie die Entwicklung der Fach- und Informationsarchitektur in den Mittelpunkt der gemeinsamen Arbeit. In diese Phase war es notwendig, die von den Partnern verwendeten Konzepte aufeinander abzustimmen und die Schnittstellen der Softwarekomponenten sowohl funktionell als auch datentechnisch zu definieren. Da das Simulationssystem von der ckc AG selbst entwickelt wurde, konnten die notwendigen Schnittstellen ohne Einschränkungen realisiert werden.

Ab 2010 konnte mit der Integration der einzelnen Softwarebestandteile aufgrund der gemeinsam definierten Fach- und Informationsarchitektur begonnen werden. In den gemeinsamen Projektmeetings wurden die Fortschritte dargestellt und jeweils die nächsten Schritte festgelegt.

In der letzten Phase des Projektes wurde das Simulationssystem und der Demonstrator intensiv von allen Partnern zur Erfüllung der Aufgaben nach dem Arbeitspaket 5 genutzt und dabei erkannte Schwachstellen bereinigt. Der Demonstrator stand dabei über einen Webserver allen Partnern zur Verfügung und jeder Partner wurde auch in der Nutzung technisch unterstützt. Als wesentliches Ergebnis konnte eine umfangreiche Simulationsstudie erstellt werden, welche auch die geforderten Sensitivitätsanalysen beinhaltete. Untersucht wurde dabei, unter welchen Bedingungen ein kosteneffizienter Einsatz von Flüssigkeitsscannern zu erwarten ist. Die Ergebnisse wurden sowohl in einem umfassenden Konferenzbeitrag[1] als auch in einem Vortrag zum Kongress „Future Security 2011“ in Berlin der Öffentlichkeit vorgestellt.

[1] Vgl. Future Security 2011 Conference Proceedings. Fraunhofer Verlag, ISBN 978-3-8396-0295-9.

1.4. Anknüpfung an den wissenschaftlichen und technischen Stand

Es sind bezüglich der Anknüpfung an den Stand von Wissenschaft und Technik vier Bereiche zu unterscheiden, die für die simulationsgestützte Risikoanalyse und sicherheitsorientierte Gestaltung komplexer Systeme relevant sind:

1. Stand der Entwicklung von Simulationsmethoden.
2. Stand der Modellierungsverfahren.
3. Entwicklungsstand der Konzepte zum Risikomanagement.
4. Stand der Expertensysteme zum Risikomanagement Kritischer Infrastrukturen.

Für diese Bereiche wird im Folgenden der Stand von Wissenschaft und Technik skizziert, wie er sich zu Beginn des Projektes darstellte.

1.4.1. Stand der Entwicklung von Simulationsmethoden

Nach dem Stand der Wissenschaft und Technik gab es im Prinzip zwei Arten der Risikobetrachtung. Wollte man Aussagen über den Risikogehalt eines komplexen Realsystems gewinnen, so wählte man eine statistische Betrachtung von vielen Risikoereignissen, die innerhalb eines (zumeist willkürlich) abgegrenzten Teilssystems und Zeitbereiches aufgetreten sind. Dabei ging man von singulären Ereignissen aus, die keinen Zusammenhang hinsichtlich Ursachen und Konsequenzen haben. Bei einer ausreichend hohen Zahl von Ereignissen können dann empirische Schadensverteilungen aufgestellt und diese durch Verteilungsfunktionen angenähert werden. Auf dieser Basis kann man dann durch Integration annähernd einen zeitbezogenen Value at Risk bestimmen. Dieses Verfahren versagt aber bei seltenen Risiken oder wenn sich das System schnell ändert, da dann alte Risikoereignisse evtl. nicht mehr auftreten und/oder neue Risiken auftreten, die noch nicht bekannt sind. Verbessern kann man dieses Verfahren, wenn Korrelationen zwischen diesen Risiken analysiert und berücksichtigt werden. Allerdings bleiben auch dann die Ursachen und Konsequenzen der beobachteten Risikoereignisse im Dunkeln.

Die zweite Art der Risikobetrachtung erfordert eine eingehende Analyse der Ursachen und Konsequenzen der dem Risiko zugrunde liegenden Prozesse. In der Praxis blieben die Analysen jedoch in der Regel sehr grob oder beschränken sich oftmals auf einen klar umrissenen, einfachen Prozess. Eine dynamische Betrachtung war nicht möglich.

Ebenso war es nicht möglich, stochastische Beziehungen im Sinne bedingter Wahrscheinlichkeiten zu modellieren.

In Forschungsprojekten an den Universitäten Bruchsal und Regensburg (2003-2007) waren bereits vor der Projektbewilligung eine Reihe von Arbeiten durchgeführt worden, mit denen ein Simulationskonzept zur prozessbasierten Risikoanalyse entwickelt wurde. Dieses Konzept wurde auf der Grundlage einer Prozessanalyse in zwei Großbanken zur Analyse und Quantifizierung der operationellen Risiken mit Erfolg eingesetzt. Ebenso wurden die Folgen der Modifikation von Kontrollmaßnahmen untersucht und die Auswirkungen auf die Risiken quantifiziert. Dabei wurde das Simulationskonzept prototypisch als lauffähige Bibliothek von verschiedenen Modellelementen in einer höheren Programmiersprache (Java) implementiert.

1.4.2. Stand der Modellierungsverfahren

Betrachtet man den Stand der Modellierungsverfahren zu Beginn des Projektes, so waren zwei prinzipielle Alternativen mit spezifischen Vor- und Nachteilen verfügbar. Dazu gehörten zum Ersten allgemeine Simulationssprachen wie Simula, Simscript, ModSim (II und III) und Silk. Außerdem existierten Frameworks für eine objektorientierte Simulation in Java [z.B. Page/Lechler/Claasen 2000].

Zweitens gab es umfangreiche Arbeiten, welche auf der Basis von Bayesschen Netzen Risikoanalysen und -betrachtungen durchführten. Da diese Netze zeitlos sind und für zeitbezogene Prozesse und Entwicklungen keine verwendbaren Modellkonstrukte vorlagen, konnten sich Simulationssysteme, die auf Bayesianischen Netzen beruhten, in der Praxis bisher nicht durchsetzen. Diese Ansätze hatten daher erhebliche Defizite, die einen Einsatz zur Simulation von risikobehafteten Prozessen behindern. Die wesentlichen Punkte waren:

- Nicht vorhandene Funktionen, um stochastische Ursachen- und Wirkungsspektren abbilden zu können oder keine Möglichkeiten, Simulationen durchzuführen, die einen Zeitbezug aufweisen.
- Keine Anschlussfähigkeit an die Methoden der Prozessanalyse oder der Prozessmodellierung.
- Unvollständige Abbildung der typischen Eigenschaften von Prozessen, wie sie z.B. durch das π-Kalkül definiert werden. (Anm.: Der π-Kalkül ist eine Prozess-

algebra und formalisiert das Konzept der nachrichtenbasierten Kooperation mittels Kommunikation von Kanalnamen. Er erlaubt insbesondere die Beschreibung von Prozess-Systemen, in denen sich die Kommunikationstopologie dynamisch ändert. Dies war bei den hier betrachteten Kritischen Infrastrukturen von herausragender Bedeutung).

1.4.3. Entwicklungsstand der Konzepte zum Risikomanagement

Für verschiedene Anwendungsbereiche wurden bereits spezifische Konzepte zum Risiko- und Sicherheitsmanagement entwickelt. Ihre grundsätzliche Struktur bestand daraus, dass im Rahmen der Risikobewältigung Sicherheitskonzepte erstellt, ausgewählte Sicherheitsmechanismen implementiert und dann zu einer Sicherheitsarchitektur bzw. -infrastruktur integriert wurden.

Genereller Mangel der bestehenden Konzeptionen war die Annahme, dass es eine einzige Zuständigkeit und Entscheidungsinstanz für das Risikomanagement gibt. Dies ist jedoch bei Kritischen Infrastrukturen generell nicht der Fall. Zu einem dezentralen Management kommt hinzu, dass sehr unterschiedliche Sicherheitsstrategien und Sicherheitsarchitekturen gezielt zusammen wirken müssen, um Bedrohungen effizient bekämpfen zu können. Dabei ist die Frage zu untersuchen, ob und inwieweit diese einzelnen Architekturen in eine gemeinsame Sicherheitsinfrastruktur zu integrieren sind und wie diese gestaltet sein muss.

Bei der Entwicklung der Sicherheitsarchitekturen stand zudem immer die möglichst vollständige Abdeckung aller Risiken im Vordergrund. Eine Risikobewertung und -quantifizierung wurde mangels geeigneter Verfahren nicht durchgeführt. Die Verbindung von Risiko- und Sicherheitsmanagement konntet mit dem Entwicklungsstand der Konzepte nicht hergestellt werden.

1.4.4. Stand der Expertensysteme zum Risikomanagement Kritischer Infrastrukturen

Ein verteilt verfügbares Expertensystem zum Risiko- und Sicherheitsmanagement Kritischer Infrastrukturen existierte in der geplanten Form bisher nicht. Es waren zwar eine Vielzahl von Tools auf dem Markt, diese adressieren jedoch bestimmte Anwendungsfelder, wobei Tools zur IT-Sicherheit, zur qualitativen Risikoanalyse und zur

Notfallplanung überwogen. Keines der bekannten Tools unterstützt jedoch mehrere relevante Modelle und das Zusammenwirken verteilter Institutionen im Risikomanagement, sondern es wird eine einzige verantwortliche Institution vorausgesetzt.

Weiterhin basierten diese Werkzeuge auf relativ einfachen, subjektiven Bewertungsmethoden und stellen daher im Grunde Content-Management-Systeme dar, die nicht geeignet sind, neue Informationen mittels Simulationsexperimenten zu generieren. Eine integrierte Anwendung verschiedener, hochentwickelter oder neuer Methoden, welche unterschiedliche Aspekte des Risikomanagements betrachteten, fehlte zu Beginn des Projektes völlig.

1.5. Kooperationen im Rahmen des Projektes

1.5.1. Interne Kooperation

Das Konsortium im SiVe Projekt bestand aus fünf Konsortialpartnern: Bauhaus Luftfahrt, ckc AG, EADS Deutschland, Flughafen München, Frauenhofer ALI, und der Technischen Universität München. Jeder dieser Partner hatte ein eigenes Teilprojekt, das sich mit einem Teilaspekt der Aufgabenstellung befasste. Eine Herausforderung des Projekts war es, die unterschiedlichen Aktivitäten so zu koordinieren, dass schließlich ein vollständig integriertes Gesamtsystem entstehen konnte. Diese Koordinationsaufgabe wurde durch den Koordinator sehr gut erfüllt und von ihm dabei die geeigneten Maßnahmen ergriffen, um den Projekterfolg sicher zu stellen. In der zweiten Hälfte des Projektes unterstützte zusätzlich die Bereitstellung der ersten Version des Demonstrators die Zusammenarbeit in einem erheblichen Maße, da die Leistungen der Partner nun in ihrem Zusammenwirken getestet werden konnten.

1.5.2. Kooperation mit externen Partnern

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

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

- Fraport AG
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
- Hersteller von Sicherheitstechnologien (Scanner und Sonden)

Dabei wurde über Forschungsergebnisse, Strategien und Maßnahmen informiert und diskutiert. Weiterhin wurde hinsichtlich der Planung gemeinsamer nationaler und europäischer Forschungsaktivitäten (FhG ICT, IFF und ValueSec) kooperiert. Beim Querschnittprojekt INFRANORM wurde bei Interviews, Umfragen und statistischen Erhebungen mitgewirkt.

Da die Detektionswahrscheinlichkeit der eingesetzten Scanner als Parameter bei den Simulationsstudien von besonderem Interesse waren, wurde Kontakt mit verschiedenen Herstellern aufgenommen. Dies ermöglichte eine wirklichkeitsgetreue Abbildung der Prozesse, der Kosten und Sensitivitätsanalysen hinsichtlich der technologischen Parameter.

2. EINGEHENDE DARSTELLUNG DES PROJEKTS

2.1. Verwendung der Zuwendungen und der Ergebnisse

In dem ckc-Teilvorhaben wurden vier Mitarbeiter kontinuierlich über die dreijährige Laufzeit des Projekts (=144 Personenmonate) eingesetzt. Dieses umfasst auch die Zeiten gemeinsamer Arbeit mit den anderen Projektpartnern. Davon wurde ein Unterauftrag im Volumen von 36 Personenmonaten an das Institut für Risiko- und Prozessmanagement GmbH vergeben.

Das Projekt wurde durch einen Meilenstein nach 18 Monaten der Gesamtlaufzeit in zwei Phasen aufgespaltet. In der ersten Phase war eine risikoorientierte Strukturanalyse des Flughafens samt der möglichen Bedrohungsszenarien und der vorhandenen Schutzmechanismen durchzuführen und alle konzeptionellen Fragen hinsichtlich des Demonstrators zu klären. Zum Meilenstein wurde geprüft, ob eines oder mehrere der Abbruchkriterien erfüllt waren oder das Projekt mit einer hohen Erfolgswahrscheinlichkeit die geplanten Ergebnisse liefern kann.

Nach einem positiven Prüfungsergebnis wurde in der zweiten Phase von weiteren 18 Monaten Projektlaufzeit der Demonstrators entwickelt und sowohl hinsichtlich seiner Einzelkomponenten als auch des Zusammenwirkens aller Module getestet und

fehlerbereinigt. Ferner wurde eine umfangreiche Dokumentation mit Hilfe eines Wiki erstellt, die allen Projektpartnern über das Internet zur Verfügung gestellt wurde.

Bereits während der ersten Projektphase wurden Simulationsstudien vorgenommen, um die Anwendbarkeit des Demonstrators abzusichern. Allerdings waren umfangreichere Simulationsstudien erst nach Erreichen eines ausreichenden Reifegrades des Demonstrators möglich. Die Ergebnisse dieser Studien wurden auf internationalen Tagungen präsentiert und als Konferenzbeiträge veröffentlicht (CRITIS´09, Bonn; Future Security 2009, Karlsruhe; Future Security 2011, Bonn).

Die im Forschungsantrag durchgeführte detaillierte Ressourcenplanung konnte während der gesamten Projektlaufzeit weitestgehend eingehalten werden. Personelle Ausfälle wegen Krankheit oder aus anderen Gründen waren nicht zu verzeichnen. Aus den laufenden Projekterkenntnissen ergab sich zwar die Notwendigkeit, bereits eingeschlagene Lösungswege zu revidieren, was zu ungeplanten Zusatzarbeiten führte. Diese konnten jedoch durch eine entsprechende Neudisponierung der Ressourcen ohne eine wesentliche Erhöhung des Projektbudgets geleistet werden.

Die erzielten Ergebnisse sollen im Folgenden anhand der oben aufgeführten Arbeitspakete detailliert dargestellt werden. Dabei wird jeweils auf die Verwendung der Zuwendung und die erzielten Ergebnisse, auf wichtige Positionen des zahlenmäßigen Nachweises, der Notwendigkeit und Angemessenheit der durchgeführten Projektarbeiten, den Nutzen und die Verwertbarkeit der erzielten Resultate eingegangen.

2.1.1. Arbeitspaket 1

Dieses Arbeitspaket bestand aus vier Unterarbeitspaketen, die im Folgenden mit ihren Ergebnissen und geplanten Aufwendungen aufgeführt sind.

AP 1.1: Definition und Spezifikation von Bedrohungsszenarien (Systematik) und Festlegung von Messgrößen sowie Modell- u. Simulationsparametern.
Ergebnisse:

- Genaues Verständnis der Zuständigkeiten, Abläufe und Zusammenhänge im Realsystem.

- Allgemein anwendbares Systemmodell für Bedrohungsszenarien als erste gemeinsame Grundlage für den Methoden- und Modellverbund sowie als Grundlage zur Entwicklung konzeptueller Modellelemente für die stochastische, ereignisorientierte Simulation.
- Anleitung für Anwender, um für die Simulation geeignete Bedrohungsszenarien zu beschreiben.

Aufwand: 160 PT (inkl. Werksführungen, Interviews, Workshops, Validierung des Systemmodells und der Modellparameter bei den verschiedenen Anwendern)

AP 1.2: Auswahl und Festlegung geeigneter Testszenarien
Ergebnis: Liste potenzieller Szenarien für die weiteren Tests unter methodischen und experimentellen Gesichtspunkten und Auswahl der weiter zu verfolgenden Szenarien.
Aufwand: 20 PT

AP 1.3: Entwicklung konzeptueller Modellelemente zur Abbildung von Bedrohungsszenarien
Ergebnis: Spezifikationen als Grundlage für die Implementation von Modellelementen.
Aufwand: 140 PT

AP 1.4: Implementation konzeptueller Modellelemente zur Abbildung von Bedrohungsszenarien in Simulationsmodellen
Ergebnisse: Programm-Modul zur Eingabe/Formulierung von Bedrohungsszenarien und erstes Framework für die Anwendungsarchitektur des späteren Demonstrators.
Aufwand: 220 PT

2.1.2. Verwendung der Zuwendungen und erzielte Ergebnisse AP1

Aufgrund einer Komplexitätsanalyse wurde ein logisches Modell für Spezifikation von Bedrohungsszenarien erarbeitet (unter Führung von Bauhaus Luftfahrt e.V.). Dieses Modell spezifiziert die wesentlichen Systemelemente, die in einem Bedrohungsszenario zu berücksichtigen sind und ermöglicht eine erste grobe Festlegung von Messgrößen sowie Modell- u. Simulationsparametern. Damit wurde das Ziel des Arbeitspaketes 1.1 erreicht. Da durch die mögliche Kombinatorik der Systemelemente die Anzahl möglicher Bedrohungsszenarien explodiert, war dieses Modell nur mit Rechnerunterstützung

handhabbar. Implementiert wurde daher eine erste Version dieses Modell mit Hilfe des Tabellenkalkulationsprogrammes Excel. Die folgende Abbildung zeigt die wesentlichen Elemente dieses Modells und die Erfassung der Beziehungen dieser Elemente.

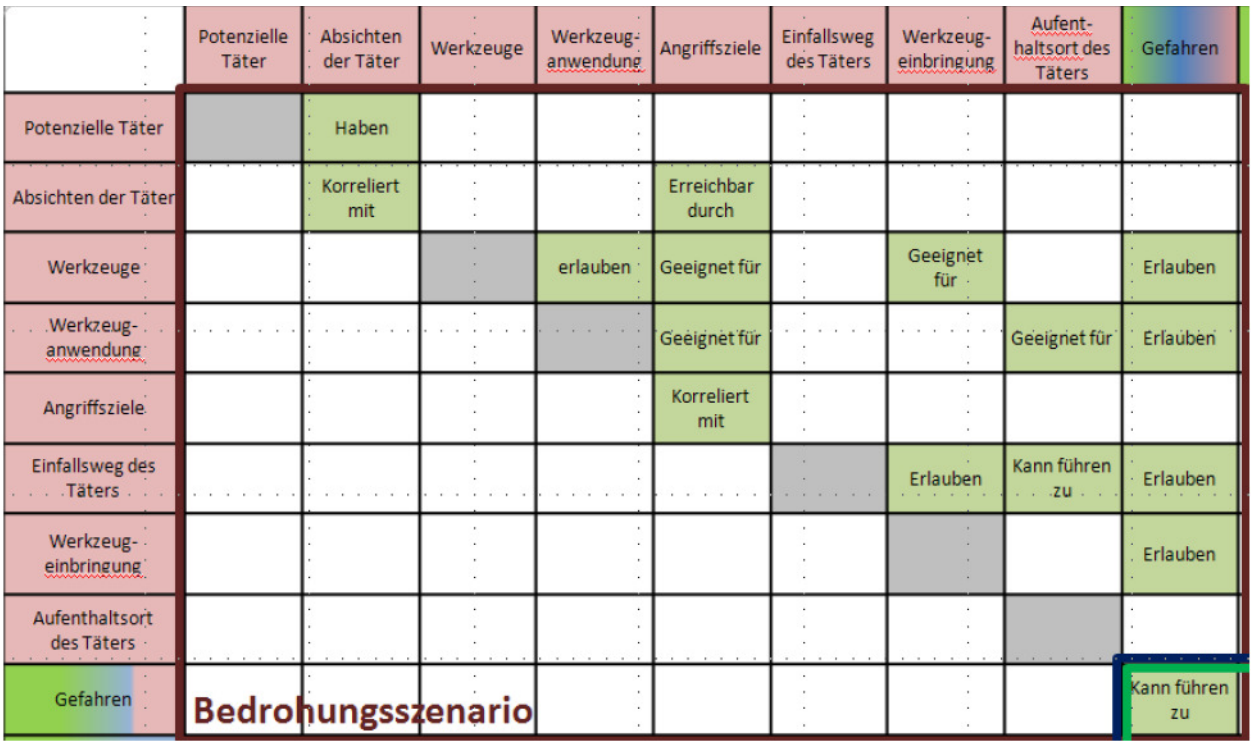

Abb. Spezifikationsmodell für Bedrohungsszenarien

Auf der Grundlage des Spezifikationsmodells wurden Bedrohungsszenarien konstruiert und hinsichtlich ihrer aktuellen Relevanz analysiert. Aus dieser Liste potenzieller Szenarien wurde ein Testszenario von allen Partnern gemeinsam ausgewählt und als Grundlage zur Entwicklung konzeptueller Modellelemente für die stochastische, ereignisorientierte Simulation verwendet. Damit war das Ziel des Arbeitspaketes 1.2 erreicht.

Das Testszenario war mit folgenden Parametern belegt:

- Potentieller Täter: Politisch motiviert (Terrorist)
- Absichten der Täter: Aufmerksamkeit, Angst/Demoralisieren, Erpressung
- Werkzeug: selbstgebauter/unklassifizierter Sprengstoff
- Werkzeuganwendung: Unkontrolliert, Tod einkalkulierend
- Angriffsziele: Menschenansammlung im Sicherheitsbereich
- Einfallsweg des Täters: Sicherheitsbereich
- Werkzeugeinbringung: Gewaltloses Umgehen/ im Handgepäck

- Aufenthaltsort des Täters: Im Sicherheitsbereich
- Gefahr: Entführung

Da Bedrohungsszenarien typischerweise dadurch gekennzeichnet sind, dass unabhängig agierende Aktoren mit eigenen Handlungsplänen (Prozessabläufen) aufeinander einwirken, wurden zur Abbildung dieser Eigenschaft folgende konzeptuelle Modellelemente entwickelt und implementiert:

- Simulatorkern, der in der Lage ist, parallel ablaufende Prozessmodelle zu steuern, die miteinander in Interaktion stehen: Dadurch wird die Abbildung komplexer, mitein-ander in Wechselwirkung Handlungsabläufe sowie die Verwendung von grafischen Modellen zur Abbildung der Prozesslogik möglich.
- Modularisierungskonzept, mit dessen Hilfe Teilprozesse abgegrenzt und gekapselt werden können: Dadurch wurde der wachsenden Modellkomplexität im weiteren Projektverlauf Rechnung getragen.

Die Steuerung parallel ablaufender Prozesse und das Modularisierungskonzept wird in der folgenden Abbildung verdeutlicht. Dabei repräsentiert die Prozessgruppe die drei an dem Testszenario beteiligte Systeme/Akteure: Passagier, Torbogensonde und Sicherheitspersonal.
Diese interagieren mittels Kommunikation und/oder Aktion. Somit repräsentieren die Prozessmodelle die Menschen mit ihren individuellen Handlungsplänen oder Arbeitsvorschriften sowie die durch die Sicherheitstechnik bestimmten Prozessabläufe.

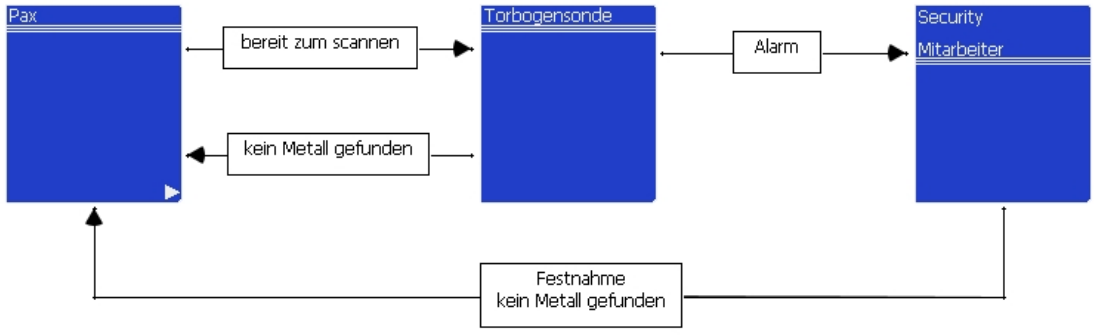

Abb. Prozessgruppe mit drei interagierenden Prozessen

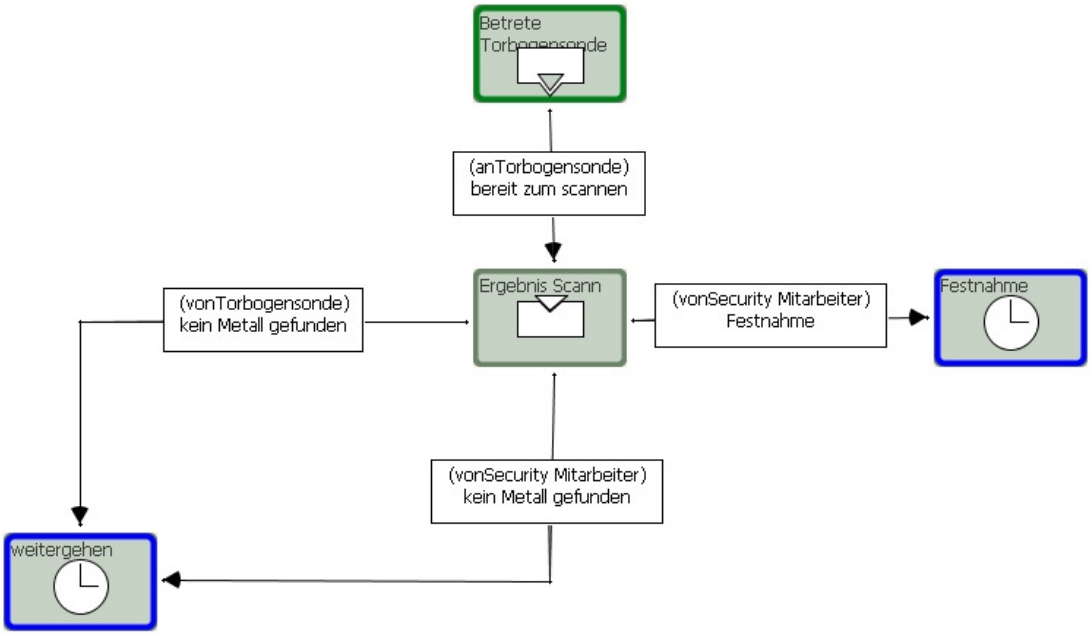

Abb. Interner Prozessablauf für den Passagier (PAX)

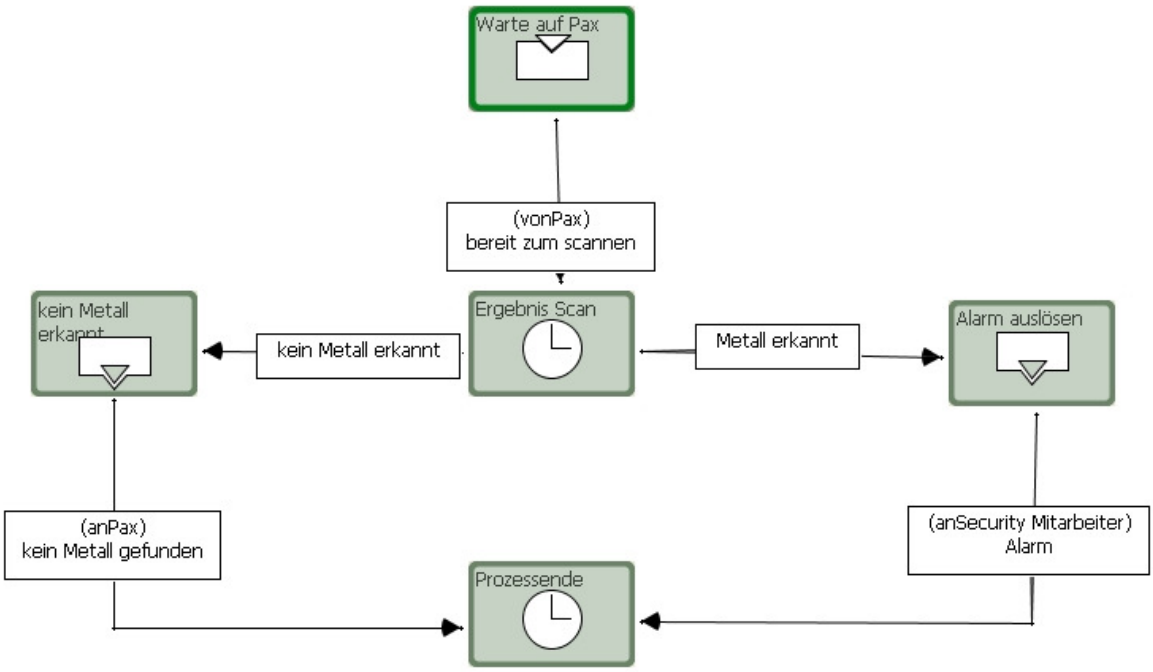

Abb. Interner Prozessablauf für die Torbogensonde

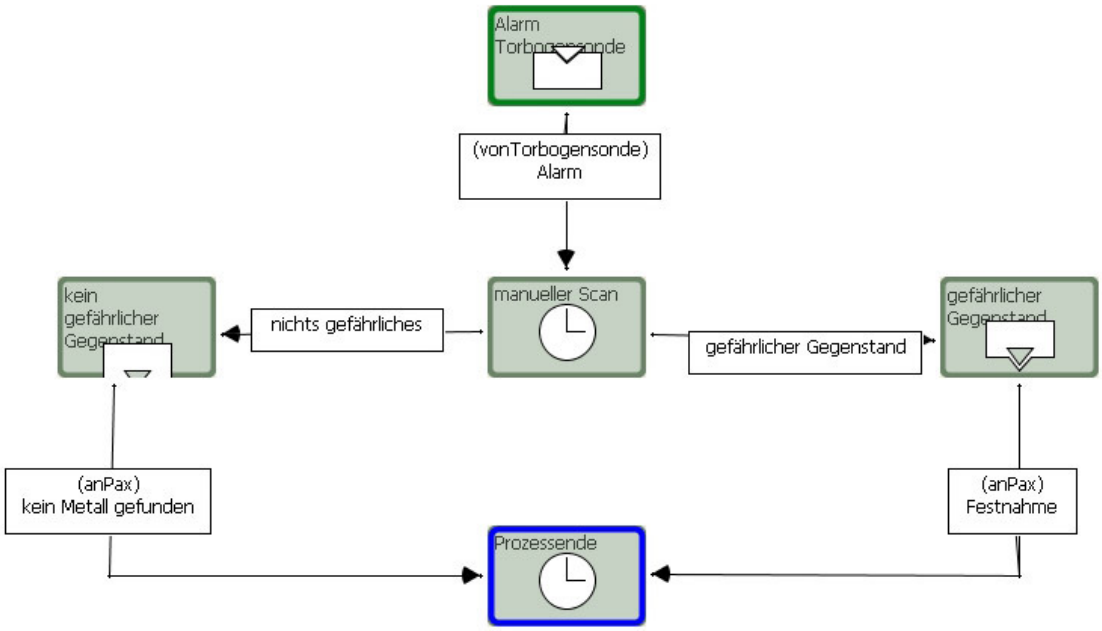

Abb. Interner Prozessablauf für die manuelle Kontrolle des Sicherheitspersonals.

Mit der Entwicklung dieser konzeptuellen Modellelemente war das Ziel des Arbeitspakets 1.3 erreicht. Aufgrund dieser Spezifikationen konnte eine erste Version eines Simulationskerns implementiert werden, der in der Lage ist, entsprechend spezifizierte Prozessabläufe zu simulieren und damit Bedrohungsszenarien in Simulationsmodelle umzusetzen. Mit dem selbst entwickelten grafischen Editor konnten damit Bedrohungsszenarien mit Hilfe von Prozessabläufen konkretisiert und zum Zwecke der Simulation eingegeben werden.

Es wurde gemeinsam ein erstes Framework für die Anwendungsarchitektur des späteren Demonstrators entwickelt, das in der folgenden Abbildung dargestellt ist. Damit sind zugleich die Zieles des Arbeitspaketes 1.4 vollständig erreicht worden.

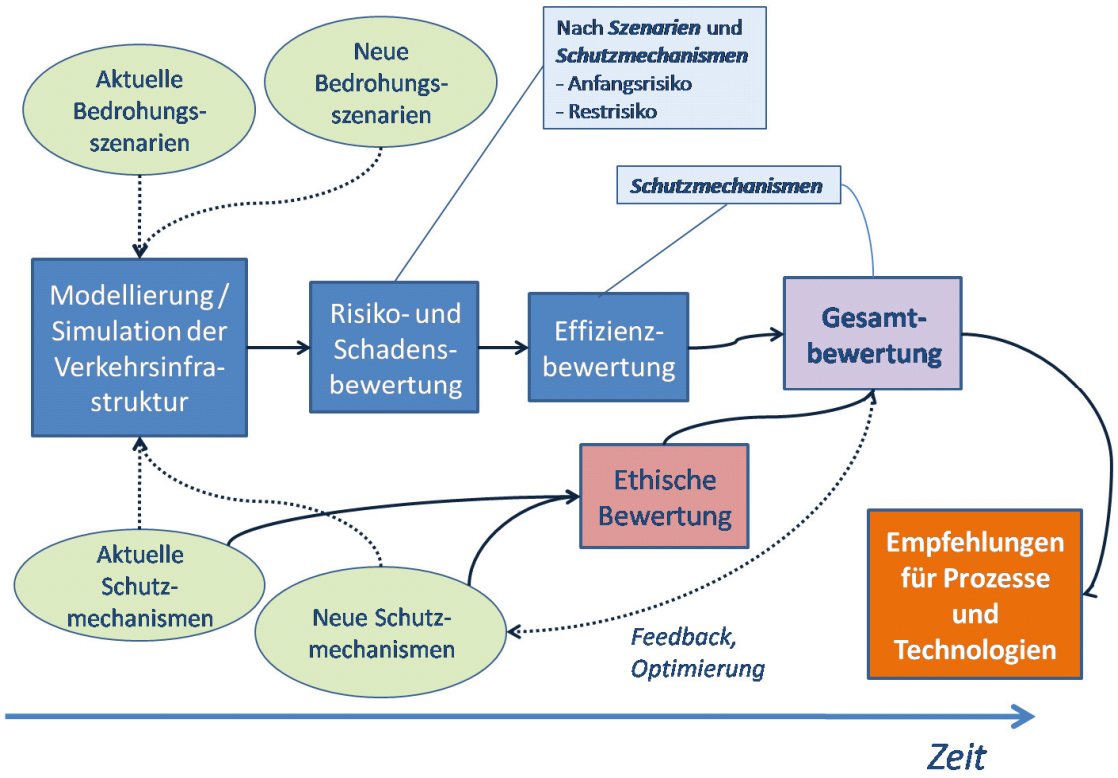

Abb. Framework für die Anwendungsarchitektur

Als wichtige Positionen des zahlemmäßigen Nachweises konnten alle Ziele des Arbeitspaketes mit den kalkulierten Personentagen erreicht werden. Die Notwendigkeit und Angemessenheit der durchgeführten Projektarbeiten zeigt sich anhand der erzielten Resultate, mit denen erstmals logisch konsistent üblicherweise schwach definierte Bedrohungsszenarien in simulationsfähige, mathematisch vollständig definierte Modelle überführt werden konnten. Weiterhin erwies sich die erarbeitete Anwendungsarchitektur für die weiteren Projektphasen als zielführend. Damit war der Nutzen und die Verwertbarkeit der erzielten Resultate für die weitere Projektarbeit nachgewiesen.

2.1.3. Arbeitspaket 2

Dieses Arbeitspaket bestand aus drei Unterarbeitspaketen, die im Folgenden mit ihren Ergebnissen und geplanten Aufwendungen aufgeführt sind.

AP 2.1: Spezifikation bestehender und neuer Schutzmechanismen
Ergebnis: Systemmodell von Schutzmechanismen als gemeinsame Grundlage für den Methoden- und Modellverbund sowie als Grundlage der Konstruktion konzeptueller Modellelemente, die als Basis für die Implementierung dienen können.

Aufwand: 120 PT

AP 2.2: Entwicklung konzeptueller Modellelemente zur Abbildung von Schutzmechanismen
Ergebnis: Spezifikationen als Grundlage der Implementation der Konzepte und Elemente.
Aufwand: 100 PT

AP 2.3: Implementation konzeptueller Modellelemente zur Abbildung von Schutzmechanismen
Ergebnis: Programm-Modul zur Eingabe/Formulierung und Simulation der Wirkung von Schutzmechanismen.
Aufwand: 180 PT

2.1.4. Verwendung der Zuwendungen und erzielte Ergebnisse AP2

Anhand des gemeinsam ausgewählten Testszenarios wurde die Personenkontrolle am Flughafen als Forschungsobjekt für die Erstellung eines Systemmodells von Schutzmechanismen ausgewählt. Das konzipierte Systemmodell basiert auf einem Prozessmodell, welches die Sicherheitskette aus den einzelnen Schutzmechanismen der Personen- und Handgepäckabfertigung abbildet. Im nachfolgend dargestellten Modell ist die Torbogensonde (metal detector gate) ein solcher Schutzmechanismus.

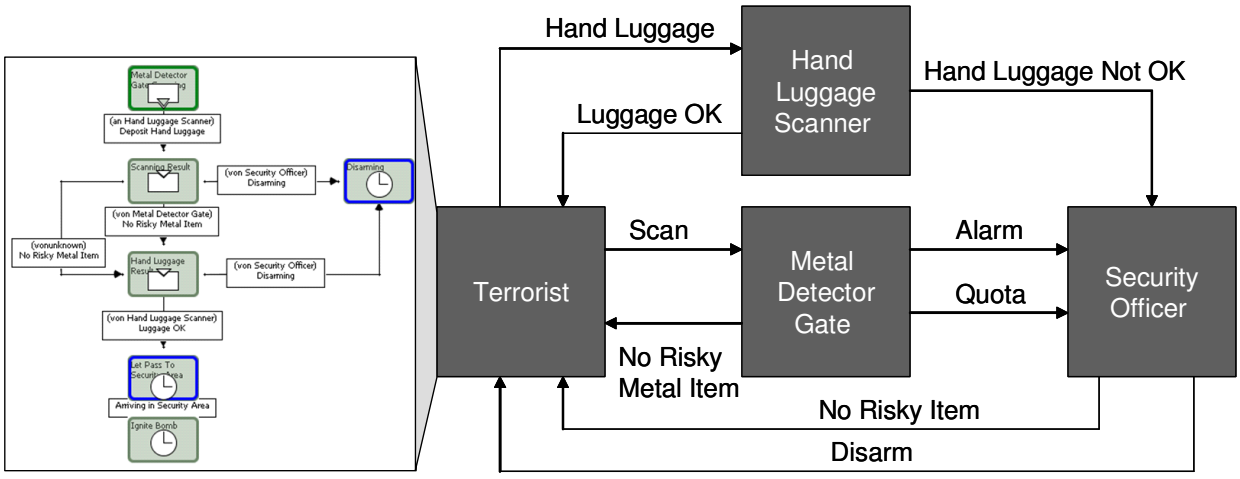

Abb. Systemmodell für Schutzmechanismen

Die bei jeder Instanz (hier Passagier) generierten Zustände des Schutzmechanismus sind in einem Verbund von Sicherheitsmechanismen als Nachrichten an andere Prozesse zu interpretieren. Bei „Alarm“ bei der Gepäckkontrolle wird diese z.B. als Nachricht an den Prozess „Sicherheitspersonal“ gesendet, wobei dort die Aktion „Festsetzen bis Klärung“ ausgelöst wird. Das Sicherheitspersonal kann somit weitere Untersuchungsschritte einleiten, hier z.B. ein verdächtiges Gepäckstück mittels eines Sprengstoffkontrollsystems.

Die Sicherheitskette muss nicht unbedingt streng sequentiell ablaufen, sondern sie kann auch parallele Prozessteile enthalten, wie dies z.B. bei der Durchleuchtung des Gepäcks einerseits und der Erfassung metallischer Gegenstände bei Personen mittels der Torbogensonde andererseits geschieht. Die einzelnen Schutzmechanismen werden dabei im komplexen Fall selbst durch (beliebig komplexe) Prozesssysteme dargestellt, welche mittels Nachrichten zunächst initialisiert und während der Simulation neu parametrisiert werden können.

Für die im Projekt verfolgte Effizienzbetrachtung von Schutzmechanismen sind aber nicht nur die Prozessabläufe wichtig, sondern auch die Abbildung der risikoreduzierenden technologischen Faktoren und der operativen Kosten sowie der Investitionskosten. Als zentraler technologischer Parameter wurde die Entdeckungswahrscheinlichkeit risikohaften Verhaltens (z.B. durch Videoüberwachung) oder gefährlicher Gegenstände (z.B. Waffen, Explosivstoffe) erkannt. Allerdings ist dies nicht ausreichend, da mit der Empfindlichkeit oder Sensitivität der eingesetzten Sicherheitstechnologie auch die Wahrscheinlichkeit eines Fehlalarms steigt.
Als finalen Output bzw. finale Zustände liefert das Systemmodell daher alternativ die Nachrichten (1.) „Alarm“, (2.) „kein Alarm“. Der Fall eines (3.) falschen Alarmes oder eines (4.) falschen „kein Alarm“ kann im System intern nicht festgestellt werden, sondern muss durch weitere (externe) Prozesse nachgeprüft werden. Das bedeutet, dass bei Schutzmechanismen immer auch die Fehlinterpretation bzw. der Fehlalarm zu beachten ist, da die damit ausgelösten falschen Alarm- und unnötigen Reaktionsprozesse in der Regel ein Vielfaches an Kosten der regulären Abfertigungsprozesse betragen.

Der Output ist bei einem Mensch-Maschine-System, wie es z.B. die Personenkontrolle darstellt, in der Regel von einer ganzen Reihe von Parametern abhängig. Zu nennen sind der Wartungszustand der Maschine, die Empfindlichkeit der Sensorik, der Trainingszustand bzw. die Erfahrung und die Tagesform (Ermüdung) des Menschen. Diese Parameter sind einstellbare bzw. beeinflussbare Größen des Systems, welche in der Simulation entsprechend der Tageszeit (z.B. Leistungstief nach der Mittagspause beim Menschen) sowie technische Parameter (z.B. Erkennungswahrscheinlichkeiten in Abhängigkeit von der Metallmasse) durch Parameterkurven oder durch diskrete Werte für Einzelparameter (Tabelle) dargestellt werden können. Durch systematische Parametervariationen können dann mittels Simulation die Einflüsse der spezifischen Parameter auf den Output (siehe oben) analysiert werden und ein kosteneffizientes Optimum bestimmt werden.

Allgemein kann daher festgestellt werden, dass aus der Sicht des verwendeten Prozessmodells ein Schutzmechanismus selbst als ein eigenständiger Prozess zu modellieren ist, dessen Ablauf aufgrund einer Menge von Eingangsnachrichten (externe Parameter) und interne Parameter zu den finalen oben genannten Ausgangszuständen führt. Dabei können die Parameter im einfachsten Fall fest eingestellt werden oder in komplizierteren Fällen mittels Funktionen von weiteren Systemparametern abhängig gemacht werden (Möglichkeit der Eingabe von zeitabhängigen Kurven) oder mittels Wahrscheinlichkeitsverteilungen als stochastische Größe eingeführt werden.

Da in Flughäfen, aber auch in anderen Infrastrukturen an Schutzmechanismen in der Regel Warteschlangen entstehen, die für eine ökonomische Bewertung von maßgeblicher Bedeutung sind, bestand ein wesentliches Problem darin, dass die bekannten Prozessmodelle keine Konstrukte zur Abbildung und zur Analyse von Warteschlangen beinhalten, die typischerweise an Schutzmechanismen entstehen. Es wurde daher in das Systemmodell das Konzept beliebig setzbarer Zähler für Instanzen eingeführt, die bestimmte Aktivitäten durchlaufen. Somit können Warteschlangen durch das Setzen von Zählern an bestimmten Punkten nunmehr im Systemmodell frei definiert werden und damit auch das Schadenspotenzial an bestimmten Systemorten erfasst werden (z. B. steigt das Schadenspotenzial bei einem Sprengstoffanschlag, je länger die betroffenen Wartenschlangen von Passagieren sind).

Für Effizienzbetrachtungen sind zudem die Kostenwirkungen der Schutzmechanismen zu berücksichtigen. Daher wurde für die Simulation ein Kostenmodell entwickelt, das es ermöglicht, die entstehenden Prozesskosten von Schutzmechanismen realitätsgerecht zu simulieren.

Für die (vereinfachte) Modellierung der Wirkung von Scannertechnologien, bei denen Erkennungswahrscheinlichkeiten als wesentlicher technologischer Parameter interessieren, wurden Entscheidungsknoten als Modellierungselement spezifiziert. Diese ermöglichen es, empirisch beobachtete Daten (z.B. Anzahl von Fehlalarmen) zur Abbildung des Schutzmechanismus zu verwenden, ohne dass der komplexe Kausalzusammenhang interner Parameter bekannt sein muss. Damit wurde es möglich, Fehlalarme und Verhaltensfehler (z.B. Stressreaktionen) als Wahrscheinlichkeitsgröße in Bezug zu einem „richtigen“ oder erwarteten Verhalten zu setzen, indem man den Entscheidungsmöglichkeiten bestimmte Gewichte zuordnet.

Als Vorteile des entwickelten Systemmodells sind zu nennen die Möglichkeit der integrativen Abbildung sowohl ökonomischer, technischer, organisatorischer als auch menschlicher Parameter des Schutzmechanismus, sowie die mögliche Einbettung dieses Mechanismus in die Prozessumgebung mit ggf. weiteren Schutzmechanismen. Denn sowohl die internen Leistungsparameter als auch die organisatorische Einbettung bestimmen gemeinsam die Effektivität und Effizienz von Schutzmechanismen. Ein zweiter Vorteil dieses Systemmodells ist seine Skalierbarkeit, um beliebig komplexe Schutzmechanismen realitätsgetreu abbilden zu können.

Mit der Spezifikation des Systemmodells für Schutzmechanismen und der Entwicklung und Implementation der oben beschriebenen zusätzlichen konzeptuellen Modell-elemente war das Systemmodell von Schutzmechanismen als gemeinsame Grundlage für den Methoden- und Modellverbund verfügbar und damit die Ziele der Unterarbeitspaketes 2.1, 2.2 und 2.3 erreicht worden.

Als wichtige Positionen des zahlenmäßigen Nachweises konnten alle Ziele des Arbeitspaketes mit den kalkulierten Personentagen erreicht werden. Die Notwendigkeit und Angemessenheit der durchgeführten Projektarbeiten zeigt sich anhand der erzielten Resultate, mit denen erstmals Schutzmechanismen im Sinne der Kosteneffizienz und

als integrierter Bestandteil der Einsatzumgebung vollständig beschrieben und in Simulationsmodelle überführt werden konnten. Mit Hilfe des Systemmodells für Schutzmechanismen und des Kostenmodells konnten nun spezifische Bedrohungsszenarien sehr schnell in Simulationsmodelle umgesetzt werden, um realitätsgerechte Schadensverteilungen zu erzeugen, die dann unmittelbar einer ökonomischen Bewertung unterzogen werden können. Damit war die Grundlage für erste Simulationsstudien (siehe Arbeitspaket 3.4) geschaffen worden.

2.1.5. Arbeitspaket 3

Dieses Arbeitspaket bestand aus vier Unterarbeitspaketen, die im Folgenden mit ihren Ergebnissen und geplanten Aufwendungen aufgeführt sind.

AP 3.1: Spezifikation und Abbildung von Strukturen und Prozessen
Ergebnis: Formale Beschreibung von geeigneten Mechanismen zur Modellierung von Systemarchitekturen.
Aufwand: 140 PT

AP: 3.2: Entwicklung konzeptueller Modellelemente zur Abbildung von Sicherheitsinfrastrukturen
Ergebnis: Spezifikationen als Grundlage der Implementation der Modellelemente.
Aufwand: 120 PT

AP 3.3: Implementation konzeptueller Modellelemente zur Abbildung von Sicherheitsinfrastrukturen
Ergebnisse: Programmsystem und weiterentwickelte Simulationssprache zur stochastischen, ereignisorientierten Simulation von Bedrohungsszenarien in Sicherheitsinfrastrukturen.
Aufwand: 160 PT

AP 3.4: Durchführung von Simulationsstudien und Validierung der Ergebnisse
Ergebnis: Erste Aussagen zum Stellenwert des Verfahrens im Rahmen des Risikomanagements Kritischer Infrastrukturen.
Aufwand: 80 PT

2.1.6. Verwendung der Zuwendungen und erzielte Ergebnisse AP3

Sowohl das erweiterte Prozessmodell als auch das Systemmodell der Schutzmechanismen (Programmiersprache Java) wurden formal vollständig beschrieben und konnten nun mittels der Mechanismen der Objektorientierten Softwareentwicklung als Module zu komplexen Teilsystemen zusammengefügt werden, die wiederum miteinander interagieren können (mehrstufige Modellierung). Damit konnten beliebig viele Abstraktionsebenen realisiert werden und damit auch komplexe Systemarchitekturen übersichtlich modelliert werden. Als Erweiterung wurde die Möglichkeit der Einführung von Black-Box-Betrachtungen eingeführt. Während es bisher erforderlich war, die Modellgrenzen mittels vollständiger, ablauffähiger Prozessmodelle zu ziehen, konnten nun Nachrichten-Schnittstellen dafür eingesetzt werden. An dieser Schnittstelle muss jetzt nur noch das Dialog-Verhalten (im Sinne eines Nachrichtenaustausches) spezifiziert werden. Die interne Prozessstruktur kann verborgen bleiben. Damit war die Aufgabe des Unterarbeitspaketes 3.1 erfüllt.

Um alle sicherheitsrelevanten Objekte eines Flughafens abbilden zu können, war ein flexibles Ressourcenmodell zu spezifizieren, das auch auf andere Flughäfen leicht anpassbar ist. Es wurde ein Ressourcenmodell spezifiziert, welches eine übersichtliche Verwaltung dieser Ressourcen ermöglicht. Das Ressourcenmodell beinhaltet auch die Kapazitäten und die Einsatzmöglichkeiten (Rollen) der Ressourcen. Alle Objekte sind frei anlegbar und können hinsichtlich ihrer ökonomischen Eigenschaften genau parametrisiert werden.

Ein wichtiger Bestandteil einer Simulationssprache ist die Spezifikation der Ressourcensteuerung während der Simulation. Dabei wurde sich für das Verfahren entscheiden, dass der Simulator für jede Aktivität genau spezifizierte Ressourcen anfordert. Sind eine oder mehrere Ressourcen durch einen anderen Auftrag belegt, und ist keine bestimmte Ressource oder eine äquivalente Ressource aus einem Pool verfügbar, dann geht der Prozess in Wartestellung und die Wartezeiten werden erfasst. Sobald die Ressource wieder verfügbar ist, wird der Prozess fortgesetzt. Damit kann verhindert werden, dass Ressourcen fälschlicherweise mehrfach verwendet werden oder ggf. zu lange belegt werden. Für jede Ressource ist zudem ein Betriebskalender definierbar, der die möglichen Einsatzzeiten festlegt.

Um eine vollständige Simulationssprache zur stochastischen, ereignisorientierten Simulation von Bedrohungsszenarien in Sicherheitsinfrastrukturen verfügbar zu haben, fehlte als konzeptionelles Modellelement noch die Spezifikation von Risikoereignissen. Da es nicht möglich ist, das Auftreten und die Art von Risikoereignissen generell in einem Prozessmodell festzulegen, sondern dies eine Vorgabe aus dem Bedrohungsszenario ist, musste die Möglichkeit geschaffen werden, jeder Aktivität eines oder mehrere Risikoereignisse zuzuordnen. Jedes Risikoereignis wird durch eine stochastische Schadensvariable spezifiziert, welche entsprechend ihrer Parametrisierung einen Zufallswert für den Schadenwert beim Auftreten dieses Ereignisses liefert. Ob und wie häufig dieses Ereignis auftritt, bestimmt sich aus den Entscheidungsknoten im Prozessmodell, die das Verhalten von Angreifern modellieren. Sind mehrere Risikoereignisse in einem Bedrohungsszenario möglich, dann ermöglicht das Programm die Aggregation der einzelnen Schadensverteilungen zu einer Gesamtschadensverteilung.

Die untenstehende Abbildung zeigt typische Verteilungen dieser Art. Dabei wurde simuliert, welchen Einfluss es hat, an welchem Ort der Angreifer einen Sprengstoff zur Explosion bringt (während der Personenkontrolle oder im Sicherheitsbereich). Für die realitätsgerechte Parametrisierung solcher Simulationsmodelle müssen jedoch die Verteilungen wesentlicher stochastischer Variablen z. B. aus der logistischen Simulation gewonnen werden, da der hier verfolgte Simulationsansatz räumliche Aspekte und damit auch die Schadenswirkung von z.B. Explosionen nicht abzubilden vermag. Die Stärke des hier verfolgten Ansatzes liegt in seiner integrativen Potenz und der Möglichkeit, fast beliebig komplexe Systemmodelle mit grafischer Unterstützung erstellen zu können.

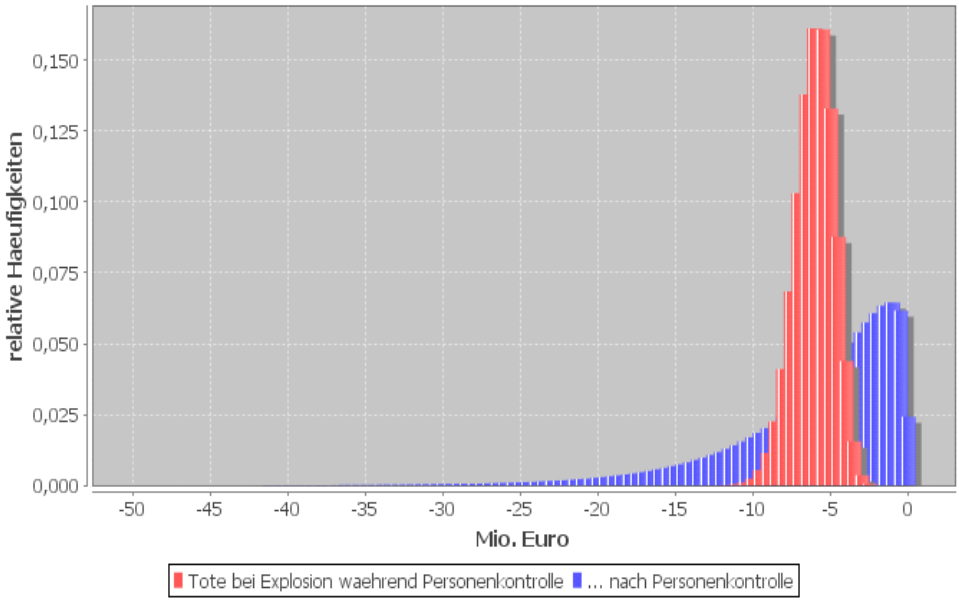

Abb. Simulativ erzeugte Schadensverteilungen aufgrund unterschiedlicher Risikoereignisse.

Als weiteres Element fehlte nun die Möglichkeit, die erzeugten Schadensverteilungen rechnerisch in ein Sicherheitsäquivalent überführen zu können, um damit verschiedene Schadensverteilungen zu bewerten bzw. zu vergleichen. In enger Zusammenarbeit mit dem Partner TU München wurde somit das von dort gelieferte Risikobewertungs- und Entscheidungsmodell in einer ersten Version als webbasierte Software zur ökonometrischen Bewertung implementiert und getestet. Die Webfähigkeit war wichtig, um einen komfortablen, gemeinsamen Zugriff auf die Software zu ermöglichen. Da sich der hierfür benötigte Aufwand in Grenzen hielt (ca. 50 PT), konnte dies durch die geplanten Kapazitäten zusätzlich abgedeckt werden. Die folgende Abb. zeigt die Oberfläche dieser Software.

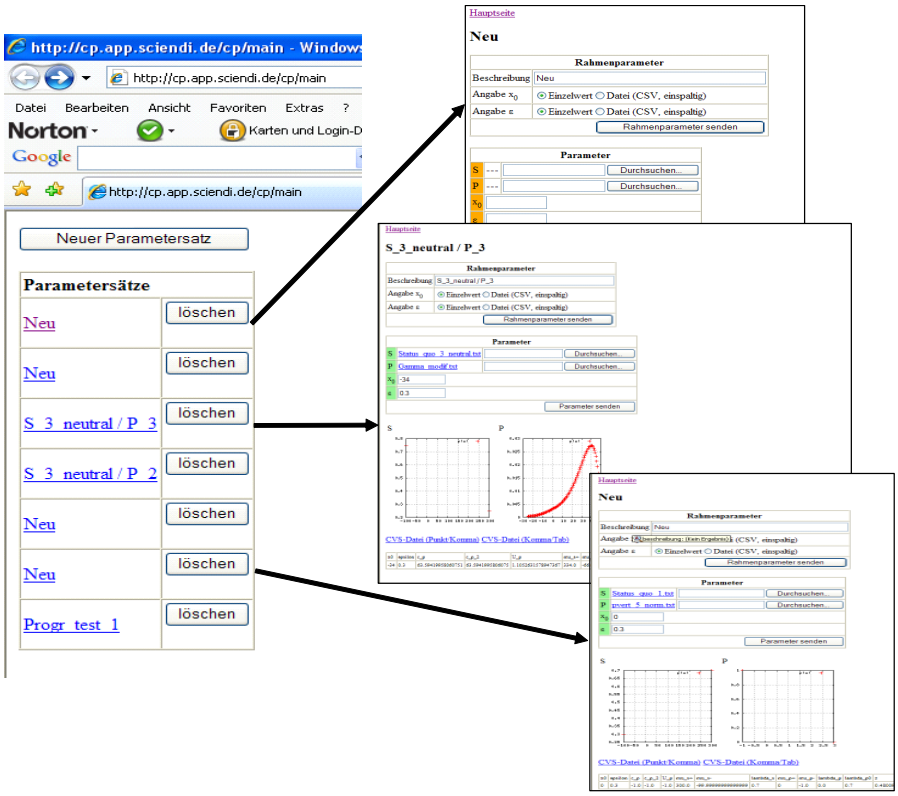

Abb. Weboberfläche des Programms zur ökonomischen Bewertung.

Mit der Spezifikation und Implementation des Ressourcenmodells, der Ressourcensteuerung, der Risikoereignisse und der ökonometrischen Bewertung stand ein erstes Programmsystem mit einer weiterentwickelten Simulationssprache zur stochastischen, ereignisorientierten Simulation von Bedrohungsszenarien in Sicherheitsinfrastrukturen zur Verfügung. Damit waren die Ziele der Unterarbeitspakete 3.2 und 3.3 fristgerecht erreicht worden. Mit Hilfe des Programmsystems konnten nun spezifische Bedrohungsszenarien sehr schnell in Simulationsmodelle umgesetzt werden, um realitätsgerechte Schadensverteilungen zu erzeugen, die dann unmittelbar einer ökonomischen Bewertung unterzogen werden können. Dies war Gegenstand des Unterarbeitspaketes 3.4, mit dem erste Aussagen zum Stellenwert des Verfahrens im Rahmen des Risikomanagements Kritischer Infrastrukturen gewonnen werden sollten.

Aufgrund der in Arbeitspaket 1 definierten Testszenarien wurden erste Simulationsstudien zum Test des Simulationssystems durchgeführt und die Ergebnisse allen Partnern zur Verfügung gestellt. Die Ergebnisse wurden auf Plausibilität mit den Partnern und Anwendern geprüft. Als besonderes Testszenario wurde die Optimierung der Quoteneinstellung bei einer Torbogensonde ausgewählt und die Ergebnisse auf den

Kongressen CRITIS´09 und Future Security 2009 präsentiert und als Konferenzbeiträge veröffentlicht.

Es zeigte sich, dass sich mit der Methodik sehr praxisrelevante Erkenntnisse gewinnen lassen, die sonst kaum anders erhältlich sind. Weiterhin konnte aufgrund der durchgeführten Simulationsstudien Gewissheit darüber gewonnen werden, dass das als zweiter Meilenstein formulierte Ziel einer Modell- und Methodenintegration erreicht werden konnte.

Mit dem Abschluss des Arbeitpaketes 3 wurde der erste Meilenstein im Gesamtprojekt erreicht. Im Rahmen dieses Teilvorhaben lagen nun folgende Ergebnisse und Erkenntnisse vor:

- Abgestimmte Definitionen von Bedrohungsszenarien, Schutzmechanismen und der Systemarchitektur von Sicherheitsinfrastrukturen (gemeinsames Ergebnis)
- Methoden- und modellneutrale Systemmodelle für Bedrohungsszenarien, Schutzmechanismen und Sicherheitsinfrastrukturen (Ergebnis des Teilvorhabens)
- Ein getestetes und validiertes Programmsystem zur stochastischen, ereignisorientierten Simulation zum Zweck einer risikoorientierten Systemanalyse (Ergebnis des Teilvorhabens).
- Aufgrund der durchgeführten Simulationsstudien Erkenntnisse darüber, ob das als zweiter Meilenstein formulierte Ziel einer Modell- und Methodenintegration erreicht werden konnte und welche Nutzeneffekte dadurch zu erzielen sind (gemeinsames Ergebnis).

2.1.7. Arbeitspaket 4: Modell- und Methodenintegration

Dieses Arbeitspaket bestand aus sechs Unterarbeitspaketen, die im Folgenden mit ihren geplanten Ergebnissen und Aufwendungen aufgeführt sind.

AP 4.1: Entwurf der Systemarchitektur und Systemintegration
Ergebnisse:

- Festlegung der anzuwendenden Integrationstools.

- Entwurf der Anwendungsarchitektur als Vorgabe zum Realisierung des Demonstrators.

Aufwand: 120 PT

AP 4.2: Entwicklung eines Konzeptes zum Risikomanagement Kritischer Infrastrukturen
Ergebnis: Konzept zum Risikomanagement Kritischer Infrastrukturen am Beispiel der Verkehrsinfrastruktur.
Aufwand: 180 PT

AP 4.3: Implementation der Erweiterungen des Simulationssystems bzw. der einzelnen Modellansätze hinsichtlich eines integrierten Ansatzes
Ergebnis: Methoden und Modelle als integrationsfähige Module.
Aufwand: 120 PT

AP 4.4: Konzeption, Implementation und Test einer gemeinsamen Benutzerschnittstelle
Ergebnis: Evaluierte und implementierte grafische Oberfläche (inkl. praxisgerechtem Rollenkonzept).
Aufwand: 100 PT

AP 4.5: Realisierung und Test des Demonstrators
Ergebnis: Getestetes, lauffähiges System zum Risikomanagement Kritischer Infrastrukturen.
Aufwand: 340 PT

AP 4.6. Theoretische Validierung der Gesamtmethodik
Ergebnisse:

- Validierung der Simulationsergebnisse und Bewertung des Nutzens der Gesamtmethodik anhand der Optimierung der Sicherheitsinfrastruktur.
- Nachweis der Eignung des Demonstrators für ein effektives und effizientes Risikomanagement Kritischer Infrastrukturen.

Aufwand: 40 PT

2.1.8. Verwendung der Zuwendungen und erzielte Ergebnisse AP4

Der Entwurf der Systemarchitektur musste die Art der verwendeten Anwendungssysteme aller Projektpartner und die fachlich gewünschten Schnittstellen berücksichtigen. In der folgenden Tabelle werden die Systeme aller Projektpartner und ihre Schnittstellen gemäß der Facharchitektur dargestellt. Es zeigt sich, dass Mehrfachschnittstellen existieren, die eine Systemintegration kompliziert werden ließ.

Projektpartner	**Anwendungssystem**	**Schnittstellen gemäß Facharchitektur**
EADS	Oryx	ALI, ckc, BHL
ckc	jSIM	ALI, EADS, TUM
Bauhaus Luftfahrt	Scenario Builder	EADS
ALI	Anylogic	EADS, ckc
TUM	Ökonomische Bewertung	ckc

Als zweite Rahmenbedingung für den Entwurf der Systemarchitektur und die Systemintegration waren die technischen Merkmale der Anwendungssysteme zu berücksichtigen. Diese Merkmale sind vor allem die verwendete Programmiersprache, die Plattform und die Datenverwaltung bzw. das verwendete Datenbanksystem. Die folgende Tabelle fasst die technischen Aspekte der eingesetzten Anwendungssysteme zusammen.

Projektpartner	**Programmier-sprache**	**Plattform**	**Datenverwaltung**
EADS	Java, Java Script, HTML	Apache Tomcat Webserver	PostgreSQL Datenbank
ckc	Java	Eclipse Rich Client Plattform	PostgreSQL Datenbank, (MySQL, H2)
Bauhaus Luftfahrt	Java (Excel-Makros)	Java Swing	HSQL Datenbank
ALI	Java	Java Applet	Datendateien, Konfigurationsdateien
TUM	Java	Eclipse Rich Client Plattform	PostgreSQL Datenbank, (MySQL, H2)

Da alle Softwarekomponenten auf Java als Programmiersprache basieren, bot es sich an, diese Sprache direkt für die Systemintegration einsetzen und die Integrationstools einer entsprechenden Java-Entwicklungsumgebung einzusetzen. Da sich Umfang und Qualität der Integrationstools je nach Entwicklungsumgebung unterscheiden, wurden

verschiedene Entwicklungsumgebungen hinsichtlich unserer Anforderungen untersucht (Eclipse, NetBeans, IntelliJ IDEA, JBuilder, JCreator). Die Entscheidung ist hierbei auf die Open Source Entwicklungsumgebung Eclipse gefallen, da diese eine umfangreiche und vielfältige Unterstützung bei der Systemintegration bot.

Als gemeinsame Plattform für die Integration wurde die Eclipse Rich Client Plattform gewählt, da diese als einzige Plattform die Möglichkeit bot, alle vorhandenen anderen Plattformen zu integrieren. Ein wesentlicher Vorteil war dabei die leichte Realisation einer gemeinsamen Benutzeroberfläche und die Möglichkeit, einen komfortablen Workspace für die Datenverwaltung einzurichten. Da es mittlerweile mit einfachen Mitteln möglich geworden war, die Anwendungsarchitektur webfähig zu machen (die Eclipse Rich Application Plattform ermöglicht die einfache Transformation der Quelldateien in eine Webanwendung, die den komplexen Anforderungen an die Benutzeroberfläche direkt gerecht wird), bot die ursprünglich vorgesehene Netweaver-Plattform als Integrationsplattform keine wesentlichen Vorteile, so dass wegen der relativ hohen Lizenzkosten auf den geplanten Einsatz der Netweaver-Plattform verzichtet wurde.

Neben der Programmiersprache und der zu verwendenden Plattform war für den Entwurf einer integrierten Anwendungsarchitektur ein geeignetes Konzept zur integrierten Datenverwaltung zu erstellen. Aufgrund der unterschiedlichen Anwendungssysteme existierten unterschiedliche Datenbestände, die auch in unterschiedlichen Datenbanksystemen und Datentabellen abgelegt wurden. Es stellte sich heraus, dass bis auf den Scenario Builder alle Systeme die PostgreSQL-Datenbank nutzen konnten. Der Szenario Builder verwendete exklusiv die eigene HSQL-Datenbank, die aber durch den geringen Ressourcenverbrauch parallel zu den anderen Datenbanken betrieben werden konnte. Im PostgreSQL-Datenbankserver existierten zwei separate Datenbanken. Eine Datenbank wurde von Oryx genutzt während die andere Datenbank von jSim und der Ökonomischen Bewertung genutzt wurde. Für den Demonstrator wurde daher vorgesehen, dass gleichzeitig drei Datenbankverbindungen aufgebaut werden, die auch parallel genutzt werden können. Hierfür wurden entsprechende Abstraktionsschichten entworfen und implementiert, um auf die jeweiligen Daten zuzugreifen.

Es erwies sich im Projektablauf weiterhin als sinnvoll, die ursprünglich für Prozessmodelle genutzte ARIS-Notation (eEPK-Modelle) aufzugeben und auf den Standard BPMN 2.0. zu wechseln. Grund dafür war die angestrebte Durchgängigkeit der Modelle,

d.h. es sollten die wesentlichen Modellteile und Modellparameter von allen Simulationsansätzen möglichst weitgehend benutzt werden können. Das von EADS ausgewählte Anwendungssystem Oryx bot jedoch keine Unterstützung für andere Prozessmodellierungssprachen. Ebenso erwiesen sich marktgängige Produkte wie z.B. BPM-Xchange der Firma BPM-X GmbH für den Einsatz als Modellkonverter untauglich. Daher wurde ein Modellierungsstandard für AnyLogic und jSim erstellt, der die Nutzung der BPMN-Modelle sicherstellt und es ermöglicht, die Modelle automatisch umzuwandeln. Für den Datenaustausch zwischen den anderen Komponenten wurden spezifische Datenformate konzipiert und implementiert, um die Durchgängigkeit der Datennutzung zu ermöglichen (zum Datenfluß vgl. AP 4.3 unten).

Den erarbeiteten Entwurf der Anwendungsarchitektur als Vorgabe zum Realisierung des Demonstrators zeigt die folgende Abbildung. Die Architektur wurde zweidimensional gemäß moderner Konzepte strukturiert.

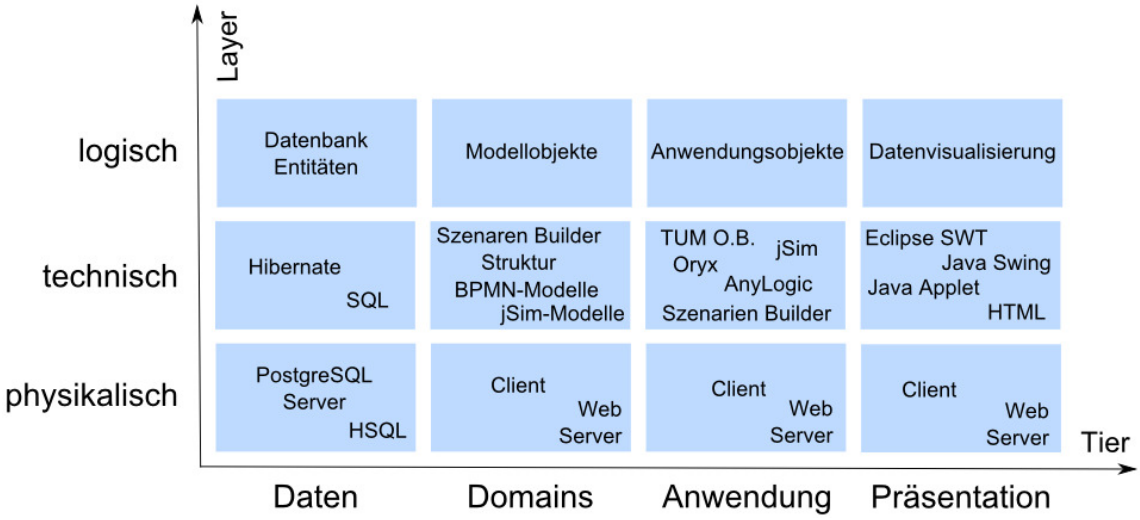

Abb. SiVe-Anwendungsarchitektur

Mit der Festlegung der anzuwendenden Integrationstools und dem Entwurf der Anwendungsarchitektur als Vorgabe zum Realisierung des Demonstrators wurden die Ziele des Unterarbeitspaketes 4.1 zeitgerecht erreicht. Ungeplante größere Aufwendungen entstanden durch den Wechsel von der ARIS-Notation auf den mittlerweile etablierten Standard BPMN. Dieser Aufwand konnte allerdings durch geringere Aufwände in den anderen Unterarbeitspaketen des AP 4 kompensiert werden.

Ziel des Unterarbeitspaketes 4.2 war die Entwicklung eines Konzeptes zum Risikomanagement Kritischer Infrastrukturen. Das Risikomanagement Kritischer Infrastruk-

turen weist einige Besonderheiten auf, die in den klassischen Ansätzen des Risikomanagements vernachlässigt werden:

- Es sind immer mehrere Organisationen am Risikomanagement beteiligt. Dabei können die Aufgabenschwerpunkte nach präventiven (z.B. Sicherheitskontrollen, Scanner), permanenten (Bestreifung, Videoüberwachung) und reaktiven Maßnahmen (Entwaffnung, Rettung, Schadensbegrenzung, Wiederherstellung) differenziert werden.
- Es sind komplexe Angriffsszenarien von geplant agierenden Tätern zu berücksichtigen, die ein Höchstmaß an Schäden verursachen wollen.

Das Konzept zum Risikomanagement Kritischer Infrastrukturen sollte insbesondere auch eine Grundlage für die zielgerechte Nutzung des Demonstrators zur Verfügung stellen. Beim Risikomanagement Kritischer Infrastrukturen sind unterschiedliche Ist-Situationen mit spezifischen Aufgabenstellungen zu unterscheiden. Es wird daher empfohlen, das strategische Risikomanagement Kritischer Infrastrukturen und das operative Risikomanagement Kritischer Infrastrukturen zu unterscheiden.

Kern einer Strategie ist immer die Positionierung der Kritischen Infrastruktur in ihrer Umwelt, die durch neue Bedrohungen und neue Sicherheitstechnologien gekennzeichnet ist. Dies führt zu den folgenden zwei Kernfragestellungen:

1. Welcher Maßnahmenbedarf ergibt sich aufgrund einer geänderten oder neuen Bedrohungslage?
2. Wie können die Flughafenprozesse aufgrund neuer Sicherheitstechnologien kosteneffizient optimiert werden?

Die nachfolgenden zwei Abbildungen zeigen auf, in welcher Reihenfolge die einzelnen Modelle und Methoden dabei zu durchlaufen sind.

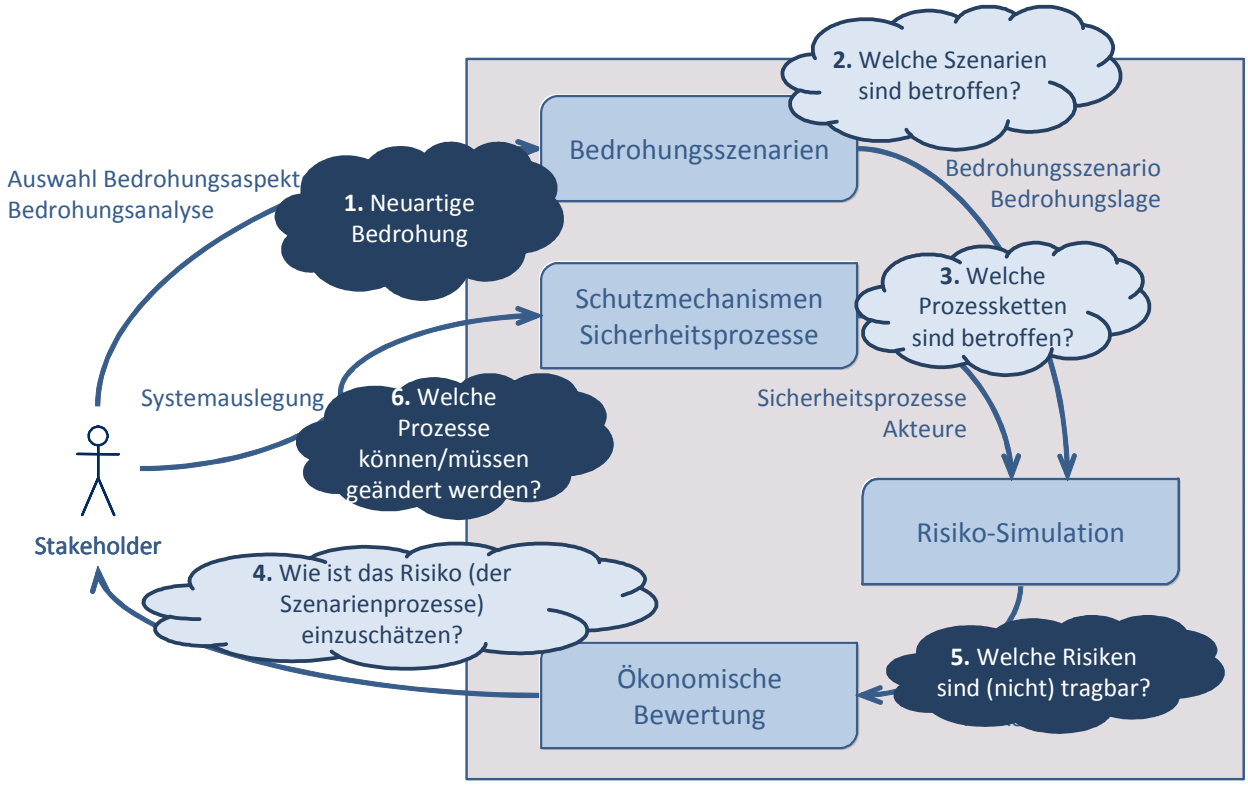

Abb. Fragestellungen zum Maßnahmenbedarf aufgrund einer geänderten oder neuen Bedrohungslage

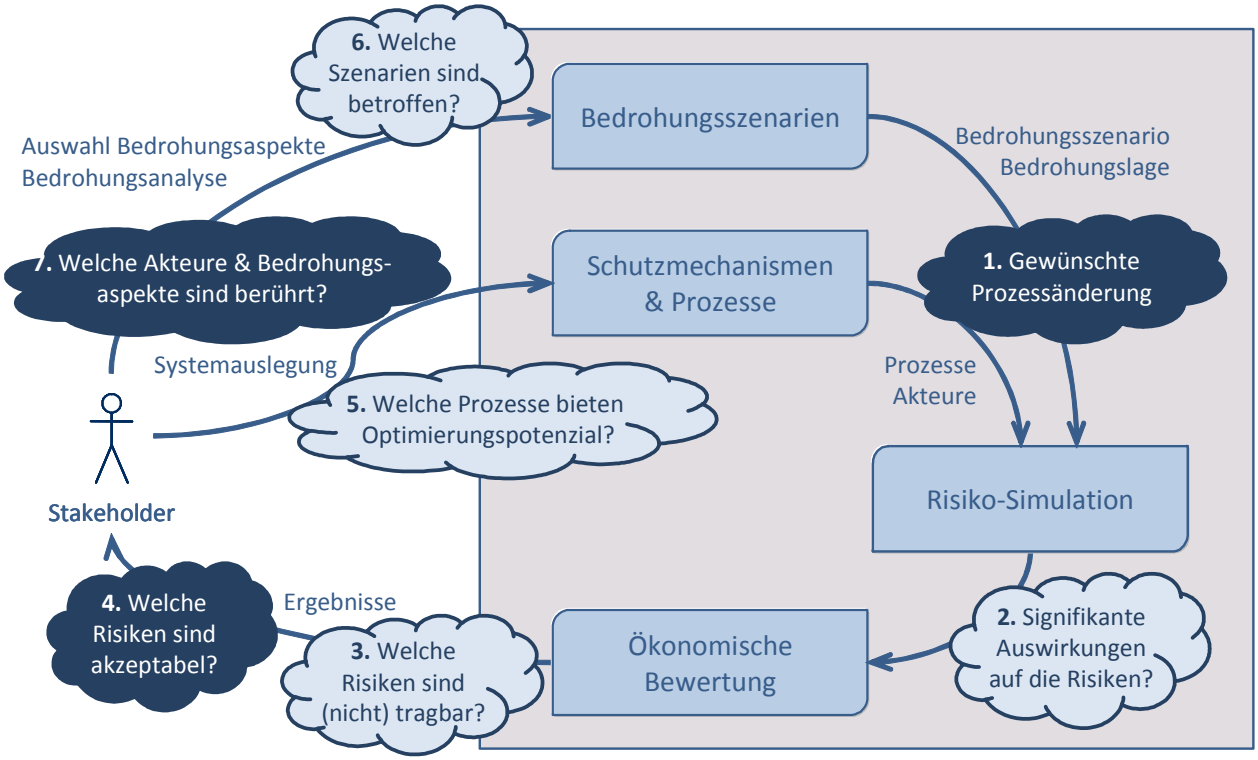

Abb. Fragestellungen zur Prozessoptimierung aufgrund neuer Sicherheitstechnologien

Im ersten Fall wird davon ausgegangen, dass eine neuartige Bedrohung bekannt geworden ist. Dann ist zu prüfen, welche Bedrohungsszenarien davon betroffen sind bzw. zu welcher Klasse von Szenarien diese Bedrohung zuzuordnen ist. Eventuell wird dadurch auch eine neue Klasse von Bedrohungsszenarien gebildet. Im dritten Schritt wird abgeleitet, welche Flughafenprozesse inkl. ihrer vorhandenen Schutzmechanismen davon betroffen sind. Durch die Simulation der Flughafenprozesse mit der Möglichkeit des Auftretens dieser neuen Risikoereignisse kann eine Abschätzung der zu erwartenden Schadensverteilungen bei der Risikorealisation vorgenommen werden. Damit kann beurteilt werden, ob das Risiko tragbar ist oder nicht. Die Ökonomische Bewertung errechnet für diese Schadensverteilungen ein Sicherheitsäquivalent, so dass unterschiedliche Systemauslegungen mit geänderten Prozessen vergleichbar werden und die Kosteneffizienz der Maßnahmen bewertet werden kann.

Im zweiten Fall ist aufgrund neuer oder verbesserter Sicherheitstechnologien eine Änderung der Prozesse möglich oder erforderlich. Mit Hilfe der Risiko-Simulation kann untersucht werden, welche Auswirkungen solche Änderungen auf die Risikosituation haben. Somit können nicht akzeptable Risiken erkannt werden, die durch solche Änderungen bewirkt werden. Zugleich wird aber auch erkennbar, welche Prozesse ein Optimierungspotenzial bieten. Ferner ist der Gegencheck durchzuführen, ob nicht die mögliche Prozessänderung auch andere Bedrohungsaspekte berührt und gegebenenfalls die Sicherheit der Infrastruktur dadurch beeinträchtigt werden kann.

In beiden Fällen des strategischen Risikomanagements wird jeweils eine ganzheitliche Betrachtung der Sicherheit der Infrastruktur gefordert, die ihren Ausgang entweder in neuen Bedrohungen oder in neuen Sicherheitsmaßnahmen hat und damit wird die in der Praxis nicht operable Forderung eines ständigen ungerichteten Sicherheitsmanagements durch ein Risikomanagement ersetzt, dass auf konkrete Anlässe aufbaut.

Weiterhin ist ein Infrastruktur-Risikomanagement als ein organisationsübergreifender Prozess zur gemeinsamen Identifikation, Bewertung, Steuerung, Kontrolle und Kommunikation von Risikoereignissen bezogen auf die Prozesse der gesamten Infrastruktur zu konzipieren. Derzeit fehlt insbesondere die Etablierung eines organisationsübergreifenden Zusammenwirkens der am Risikomanagement beteiligten Institutionen. Außerdem sind präventive und permanente Sicherheitsmaßnahmen gut dokumentiert und leicht in Prozessmodellen abbildbar, während reaktive Maßnahmen (Kriseninter-

vention, Notfallmanagement) wegen ihres Einmaligkeitscharakters nur exemplarisch dokumentiert sind. Die adäquate Erfassung und Darstellung solcher Maßnahmen ist daher in der Praxis noch eine zukünftig zu lösende Aufgabe.

Die im Demonstrator abgebildeten Prozesse sowie präventiven und permanenten Sicherheitsmaßnahmen bieten derzeit eine geeignete Grundlage für eine gemeinsame, organisationsübergreifende Optimierung der Sicherheitsinfrastruktur. Dies gilt insbesondere für die Abwehr von komplexen Angriffsszenarien, da diese systematisch konstruiert werden können und die Verantwortlichen damit in die Lage versetzt werden, den Möglichkeitsraum an Gegenmaßnahmen systematisch zu analysieren.

Ein geeignetes Konzept zum Risikomanagement muss zudem den Weg eröffnen, schrittweise von der derzeitigen Form eines vorschriftenorientierten (policy-driven) Risikomanagements zu einem kosteneffizienten (economic-driven) Risikomanagement zu migrieren. Daher muss ein geeignetes Risikomanagementkonzept beide Formen unterstützen.

Der Demonstrator unterstützt derzeit das policy-driven Risikomanagement dadurch, dass die Prozessmodelle um Informationen wie Gesetze, Erlasse und Richtlinien erweitert wurden. Damit ist ableitbar, welche Sicherheitsmaßnahmen den einzelnen Vorschriften konkret zuzuordnen sind. Erkennbar wird damit auch, welche Vorschriften noch keine Maßnahmen zur Folge gehabt haben und damit Handlungsbedarf besteht.

Ein economic-driven Risikomanagement erfordert notwendigerweise die Betrachtung der Kostenseite von Maßnahmen und eine Bewertung der damit erzielbaren Risikoreduktion. Diese Funktionen werden ebenfalls vom Demonstrator bereitgestellt. Damit ist der Demonstrator grundsätzlich geeignet, den schrittweisen Übergang zu einem (economic-driven) Risikomanagement zu vollziehen.

Ergänzend zum strategischen Risikomanagement orientiert sich das operative Risikomanagement Kritischer Infrastrukturen an bestimmten Bedrohungsszenarien, die sich angesichts der gegebenen Infrastruktur als besonders gefährlich oder kostenintensiv darstellen. Dies sind aktuelle Schwachstellen der Infrastruktur. Je nach erkannter Schwachstelle erfolgt zunächst die Selektion relevanter Szenarien. Dies sind Cluster ähnlicher Szenarien, die mit gleichen Maßnahmen verhindert bzw. deren negative Konsequenzen gemindert werden können. Im nächsten Schritt wird der Status Quo des Systems analysiert. Dies ist notwendig, um die Kosten und Nutzen von Alternativen zu untersuchen. Durch eine Bewertung und einem Vergleich der Alternativen kann dann

die Lösung selektiert werden, welche die kosteneffizienteste ist. Die folgende Abbildung verdeutlicht die grundlegenden Schritte.

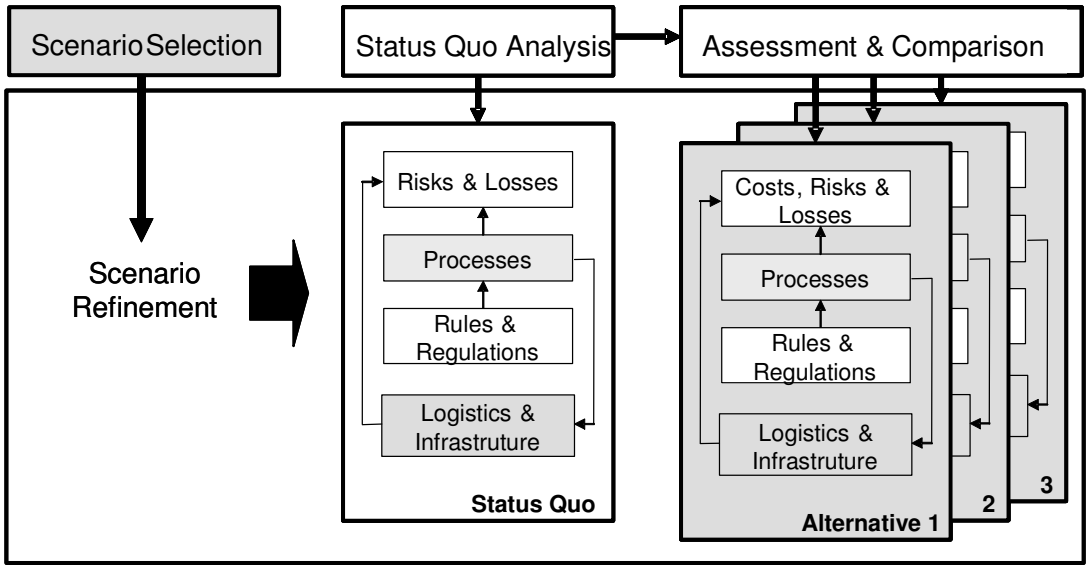

Abb. Konzept zum operativen Risikomanagement Kritischer Infrastrukturen

Mit den Ergebnissen des SiVe-Projektes ist das Konzept inhaltlich ausreichend konkretisiert worden und wird auch toolmäßig weitestgehend unterstützt. Hinsichtlich der Organisationsfragen eines solchen Risikomanagements kann auf die Erfahrungen verwiesen werden, die mit task forces oder interdisziplinären Arbeitsgruppen gemacht wurden. Vieles spricht dafür, für Kritische Infrastrukturen ein zentrales Risikomanagement zu etablieren, welches mit ausreichenden Kompetenzen und Informationsmöglichkeiten ausgestattet sein muss. Mit diesem Konzept eines Risikomanagements Kritischer Infrastrukturen wurde das Ziel des Unterarbeitspaketes 4.2 zeitgerecht erreicht.

Da sich die unterschiedlichen Anwendungssysteme sowohl hinsichtlich der Inhalte als auch hinsichtlich deren technischer Realisierung relativ stark voneinander unterschieden, war im Unterarbeitspaket 4.3 geplant, notwendige Erweiterungen für die unterschiedlichen Systeme zu erstellen, um eine nahtlosen Übergang zwischen den Simulationssystemen herzustellen.

Da ein direkter Austausch über gemeinsame Datenobjekte nicht möglich war, wurden Austauschformate erstellt bzw. entsprechende Erweiterungen entwickelt, um entsprechende andere Daten einzulesen. Für die Entwicklung eines integrierten Ansatzes waren dazu aufwendige Diskussionen notwendig, welche Daten für wen relevant sind und wie

diese in der benötigten Form übergeben werden können. Das nachfolgende Diagramm stellt den im Projekt festgelegten Nachrichtenaustausch zwischen den einzelnen Komponenten dar, die im Folgenden näher erläutert werden:

- Die Schutzaktivitäten bzw. Schutzsysteme des ausgewählten Szenarios werden mittels einer Textdatei aus dem Scenario Builder exportiert. Diese Datei wird in Oryx eingelesen und die Schutzaktivitäten ausgewertet, um die dazu gehörigen Prozessmodelle in Oryx aufzurufen. Diese können in Oryx ergänzt und modifiziert werden.
- Die Modelle in Oryx werden in Form von JSON-Dateien in der Datenbank abgespeichert und können auch als JSON-Datei ausgegeben werden. In AnyLogic können diese Dateien (= Prozessmodelle) eingelesen werden. Sie sind ein Teil des möglichen Agentenverhaltens. Dieses kann mit Anylogic weiter spezifiziert werden und es können Simulationen auf der Basis des modellierten Agentenverhaltens durchgeführt werden. Die Ergebnisse aus AnyLogic werden in Form von XML-Dateien ausgegeben. Dabei werden die Wahrscheinlichkeiten für die Verzweigungen im Modell (Entscheidungswerte) und die simulierten Schadenswerte (3D-Simulation) an die stochastische Simulation übergeben.
- Die stochastische Simulation (jSim) greift auf die Datenbank zu und liest darüber die JSON-Modelle (= Prozessmodelle) ein und transformiert sie in das von jSim genutzte Format. Auch das direkte Einlesen von JSON-Dateien ist möglich. Diese Daten fließen als Parameter in die Simulation ein.
- Die Ökonomische Bewertung (TUM) greift direkt auf die gleichen Datenbanktabellen wie jSim zu, so dass die Daten direkt von der Datenbank eingelesen werden können. Hierbei handelt es sich um die Schadenswerte, die während der Simulation generiert wurden. In der Ökonomischen Bewertung werden insbesondere Sicherheitsäquivalente zu den in jSim erzeugten Schadensverteilungen berechnet und damit verschiedene Sicherheitslösungen direkt vergleichbar gemacht.

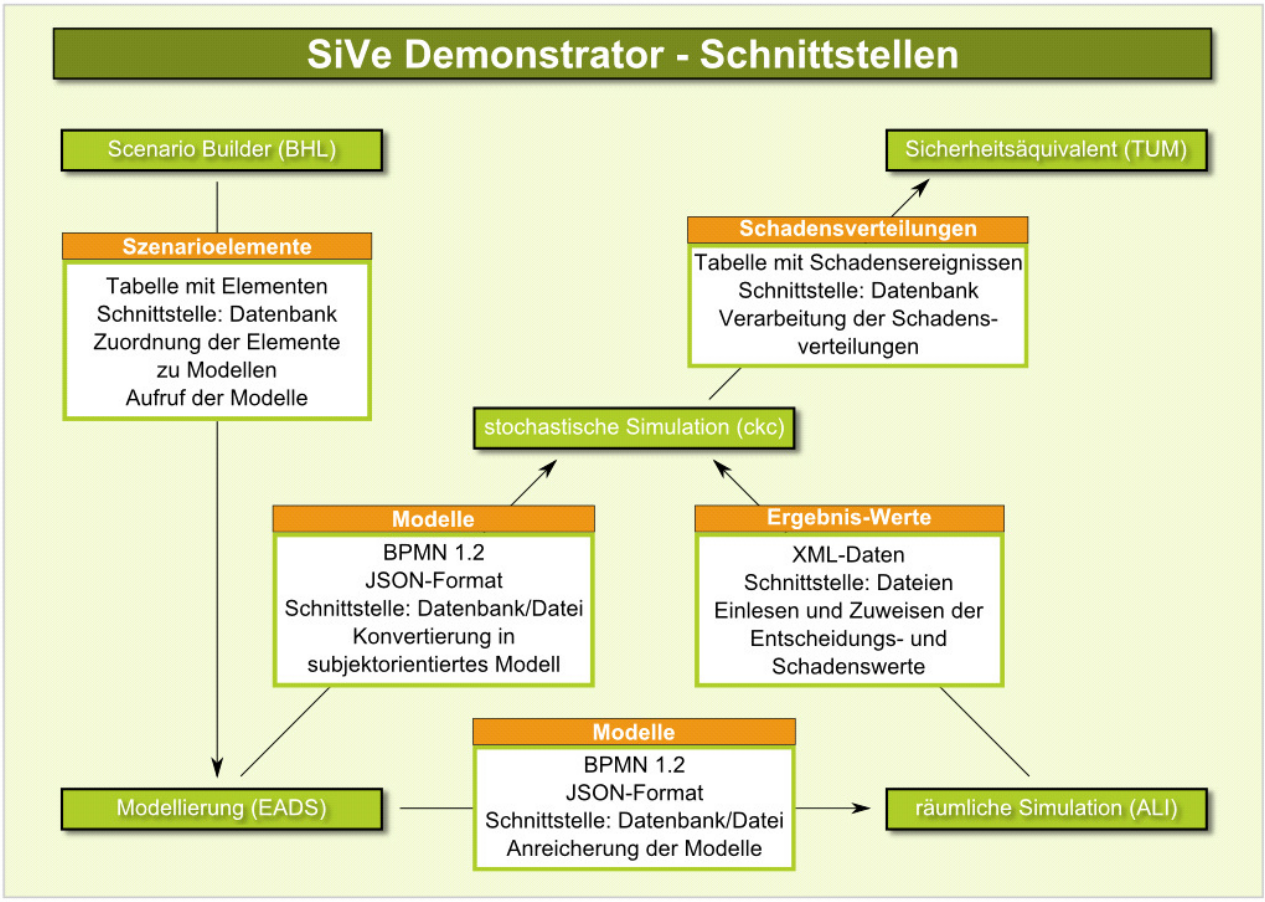

Abb. Methoden und Modelle mit Austauschformaten und Datenschnittstellen als integrationsfähige Module.

Mit der Erweiterung der Methoden und Modelle zu integrationsfähigen Modulen wurden die Ziele des Unterarbeitspakets 4.3 planmäßig erreicht.

Im Unterarbeitspaket 4.4 sollte die Konzeption, die Implementation und der Test einer gemeinsamen Benutzerschnittstelle erfolgen und als Ergebnis eine evaluierte und implementierte grafische Oberfläche (inkl. praxisgerechtem Rollenkonzept) allen Projektpartnern zur Verfügung gestellt werden. Die Konzeption und Implementation einer gemeinsamen und einheitlichen Benutzerschnittstelle stellte sich aufgrund der unterschiedlichen technischen Plattformen als eine besondere Herausforderung dar, die jedoch mit der in der Anwendungsarchitektur gewählten Eclipse Rich Client Plattform erfüllt werden konnte.

Diese Plattform stellte die wesentlichen Komponenten für den Aufbau einer gemeinsamen Oberfläche zur Verfügung und ermöglichte es auch, verschiedenartige Komponenten im dynamischen Wechsel zu nutzen. Die Plattform bietet dazu einen

Rahmen (Programmfenster), der es erlaubt diesen in unterschiedliche Bereiche (Ansichten) aufzuteilen. Diese Ansichten werden zu Perspektiven zusammengefasst, die für einen bestimmen Anwendungszweck erstellt werden. Mit diesem Konzept ist es möglich, komplexe Aufgaben strukturiert darzustellen, da der Aufbau nicht starr vorgegeben ist, sondern die Perspektiven und Ansichten je nach Anforderungen miteinander vermischt werden können.

Die Oberfläche wurde so gegliedert, dass für jedes System der Projektpartner eine eigene Perspektive vorhanden ist, die für diesen Bereich spezifisch angepasst wurde. Inwieweit die Perspektive noch in unterschiedliche Ansichten unterteilt ist, hängt vom jeweiligen Anwendungsbereich ab. Jede Perspektive enthält einen Hauptbereich (Editor), der die wesentliche Darstellung dieses Bereiches darstellt. Außerdem enthält jede Perspektive eine Ansicht für den gemeinsamen Workspace. Die Perspektiven können beliebig aufgerufen werden und die Hauptansichten in unterschiedlichen Perspektiven genutzt werden. Die folgende Abbildung verdeutlicht dieses Konzept.

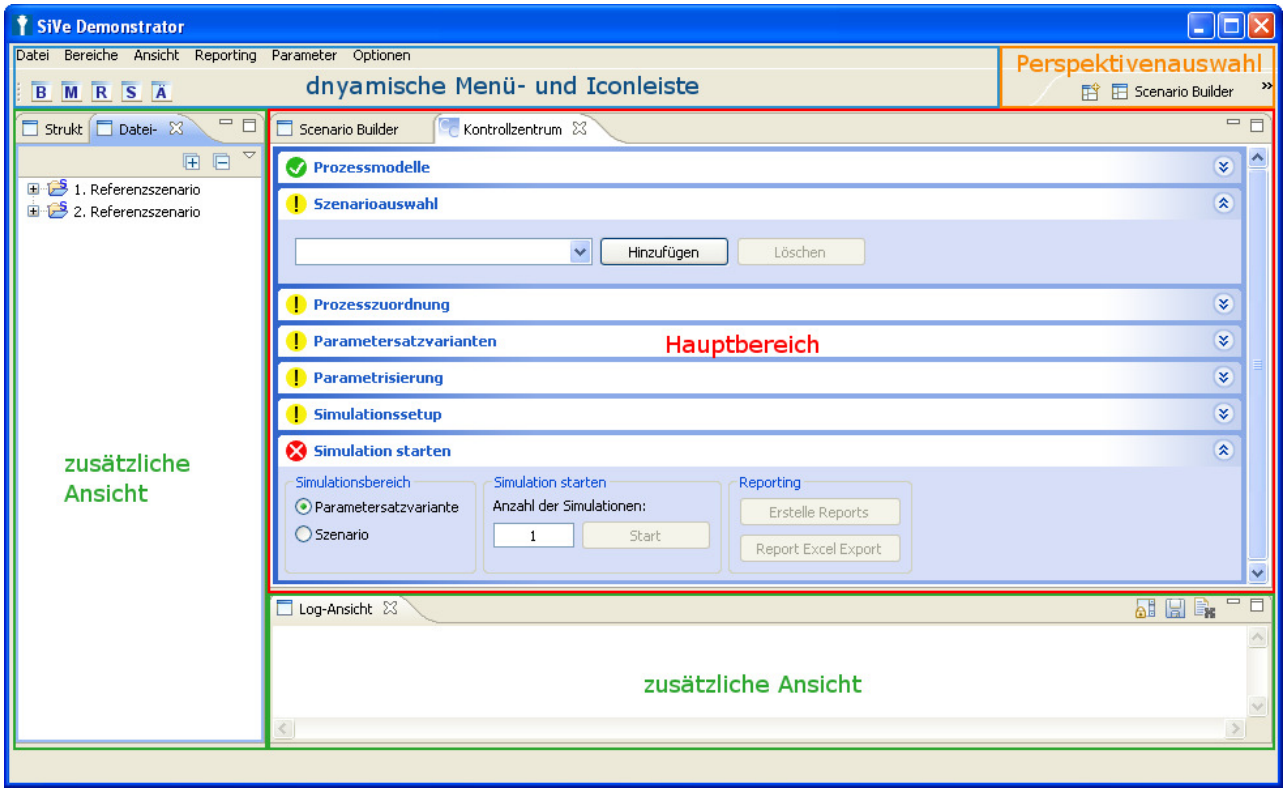

Abb. Oberflächengliederung des Demonstrators in Perspektiven und Ansichten

Für das Projekt wurde eine entsprechende Oberfläche implementiert. Hauptaufgabe war dabei nicht die Gestaltung der Oberfläche, sondern die Integration der anderen

technischen Grundplattformen. Hierbei mussten spezifische Abhängigkeiten und Anforderungen berücksichtigt werden, um die jeweilige Systemkomponente integrieren zu können. Als Beispiel kann die Integration von Oryx in die Oberfläche dienen, welches einen spezifischen Webbrowser für die Darstellung erfordert (Mozilla). Daher war es notwendig, diesen spezifischen Webbrowser mit seinen besonderen Funktionen und Merkmalen zu integrieren.

Aufgrund der Möglichkeit, die Ansichten dynamisch erstellen zu können, ist es auch möglich, die entsprechende Funktionalität aus dem Demonstrator verfügbar zu machen oder zu sperren. Dadurch sind die grundlegenden Voraussetzungen gegeben, um ein Rollenkonzept zu realisieren. Für jede Rolle wird ein besonderes Login bereitgestellt und die entsprechende Funktionalität kann aktiviert bzw. deaktiviert werden. Folgende Rollen wurden konzipiert und realisiert:

Rolle	**Rollenumfang**
Modellexperte	Erstellen, Verändern und Entfernen von Modellen. Umfasst die Bereiche Scenario Builder und Oryx.
Simulations-studienleiter	Erstellen, Verändern und Entfernen von Simulationen. Umfasst die Bereiche AnyLogic und jSim.
Analyst (Standardnutzer)	Kann bestehende Simulationen wählen und diese anhand der verfügbaren Parameter optimieren. Umfasst die Bereiche AnyLogic, jSim und Ökonomische Bewertung.
Finanzanalyst	Kann bestehende Simulationsdaten innerhalb der Ökonomischen Bewertung verwenden und zur Berechung nutzen. Umfasst den Bereich der Ökonomischen Bewertung.
Administrator	Wahrnehmung aller Aufgaben der Benutzer- und Systemverwaltung.

Die folgende Abbildung verdeutlicht das Rollenkonzept. In der untersten Ebene befindet sich der Administrator mit vollen Rechten in jedem Bereich. Je höher die Stufe, desto weniger Rechte haben die jeweiligen Nutzer.

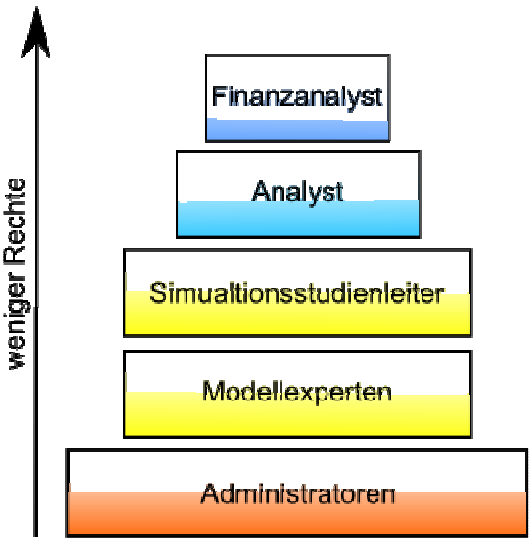

Abb. Rollenkonzept des Demonstrators

Mit der Implementation und den Test der oben dargestellten Oberfläche wurde das Ziel des Unterarbeitspaketes 4.4 plangerecht erreicht.

Das Unterarbeitspaket 4.5 betraf die Realisierung und den Test des Demonstrators und sollte den Projektpartnern ein getestetes, lauffähiges System zum Risikomanagement Kritischer Infrastrukturen zur Verfügung stellen. Der Prototyp für die gemeinsame grafische Oberfläche (AP 4.4) diente als Ausgangspunkt für die Realisierung des Demonstrators. Die wesentliche Herausforderung bei der Realisierung war die einheitliche Steuerung der unterschiedlichen, komplexen Anwendungssysteme. Für den Betrieb aller Komponenten des Demonstrators waren drei Datenbankverbindungen aufzubauen und ein Webserver zu starten. Das folgende Diagramm veranschaulicht den Aufbau des Demonstrators auf technischer Ebene.

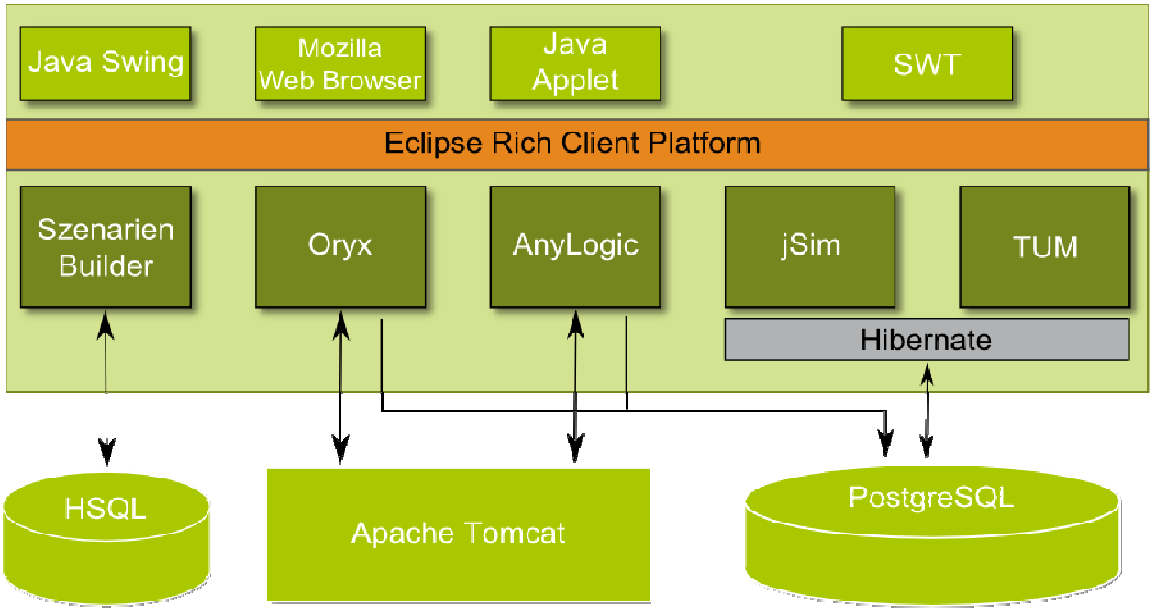

Abb. Technische Architektur des Demonstrators

Auf der untersten Ebene befinden sich die Datenbanken und der Apache Tomcat Web Server. Diese sind keine direkten Bestandteile des Systems, aber dennoch für die korrekte Funktionsweise des Demonstrators notwendig. Mit diesen Komponenten findet eine direkte bidirektionale Kommunikation statt. In den Systemen jSim und der Ökonomischen Bewertung gibt es eine Datenbankabstraktionsschicht, die von beiden Anwendungen gemeinsam genutzt werden und die Anwendungen unabhängig von der Datenbank macht. Auf der nächsten Ebene befinden sich Anwendungen der einzelnen Projektpartner, die in die Eclipse Rich Client Plattform eingebunden wurden. Diese Plattform stellt alle wesentlichen Elemente zur Verfügung, um die jeweiligen Komponenten steuern und bedienen zu können.

Im Falle von jSim und der Ökonomischen Bewertung wurden die Oberflächen allein mit der Eclipse Rich Client Plattform erstellt. Die anderen Anwendungssysteme nutzen andere Oberflächen, die jedoch über zusätzliche Softwarekomponenten in der Plattform verfügbar gemacht werden konnten. Im Folgenden wird kurz auf das jeweilige Anwendungssystem eingegangen und die Besonderheiten bei der Implementierung dargestellt.

- **Scenario Builder:** Die Integration erfordert die Lösung zweier Probleme. Diese waren die zusätzliche Datenbank und die Verwendung einer anderen Sprache für die Oberfläche (Java Swing). Die im Scenario Builder verwendeten

Datenbanktabellen hätten eigentlich problemlos in der gemeinsam genutzten PostgreSQL-Datenbank integriert werden können, allerdings werden einige spezielle Funktionen der HSQL-Datenbank genutzt, die eine größere Anpassung erfordert hätten. Da die HSQL-Datenbank wenige Ressourcen beansprucht, ist ein Parallelbetrieb zur PostgreSQL-Datenbank ohne Nachteile für die Benutzer. Die Verwendung einer eigenen Sprache für die Oberfläche konnte mit dem Einsatz einer speziellen Abstraktionsschicht gelöst werden, so dass nicht der komplette Quellcode umgeschrieben werden musste.

- **jSim:** Die Integration konnte mit einfachen Mitteln vorgenommen werden, da die gleiche Plattform genutzt wird. Es waren aus diesem Grunde nur Anpassungen an den Menüs und Iconleisten notwendig. Da jSim mehrere Abhängigkeiten zu lokalen Daten besitzt, musste der Zugriff auf die notwendigen Dateien anpasst bzw. je nach Kontext dynamisch vorgenommen werden.
- **Ökonomische Bewertung:** Da auch hier die Rich Client Plattform genutzt wird, waren nur geringe Anpassungen an Menü- und Iconleisten notwendig. Da ausschließlich die Datenbank für Datenoperationen genutzt wird waren hier keine weiteren Anpassungen notwendig.
- **AnyLogic**: Obwohl dieses Anwendungssystem ebenfalls die Rich Client Plattform verwendet, war aus lizenzrechtlichen Gründen der erforderliche Zugriff auf den Quellcode nicht möglich, so dass die Integration über ein Applet vorgenommen wurde. Ein Applet enthält bereits die notwendigen Interaktionsmöglichkeiten, so dass ein entsprechendes Web Browser Fenster zur Darstellung ausreicht. Da Applets einem strikten Sicherheitssystem folgen, muss sich das Applet in einem Web Server befinden, in dem es auch auf Dateien und Web Service zugreifen kann.
- **Oryx:** Da dies eine Open Source Software ist, stand der notwendige Quellcode zur Verfügung. Allerdings ist für den Betrieb von Oryx ein komplexes System an Software notwendig, die als Umgebung auf dem Zielrechner vorhanden sein muss. Zwingend für den Betrieb von Oryx ist der Einsatz einer PostgreSQL-Datenbank, da viele spezifische Funktionen dieser Datenbank genutzt werden. Für die spezifischen Funktionen der Datenbank muss auf dem System eine passende Version der Programmiersprache Python vorhanden sein. Auch müssen vor der Nutzung die entsprechenden Datenbanktabellen erstellt werden, da die Software diese nicht selbstständig erzeugen kann. Ein weiter wichtiger Aspekt ist, dass Oryx eine

Webanwendung ist und somit einen Web Browser benötigt. Zusätzlich muss dies als Voraussetzung der Mozilla Web Browser sein, da die Anwendung nur auf diesem Browser angepasst ist und auch dementsprechend korrekt funktioniert. Zum Betrieb muss Mozilla XUL auf dem System registriert sein, damit dieser in der Rich Client Plattform genutzt werden kann. Ein anderer Aspekt ist, dass für den Zugriff auf Oryx ein Web Server (Servlet Container) laufen muss, damit dieser die Dateien von Oryx an den Browser ausliefert. Da ein permanent laufender Webserver auf einem Client keine erstrebenswerte Lösung war, wurde eine Realisierung gewählt, dass der Server nur nach Bedarf des Demonstrators gestartet und beendet wird.

Für die Nutzung der gewünschten Komponenten im Demonstrator ist ein umfangreiches Set an Softwarekomponenten notwendig, die auch noch entsprechend konfiguriert sein müssen, um gemeinsam zu funktionieren. Da diese Installation und Konfiguration ein komplexer und fehlerträchtiger Prozess ist, war die Entwicklung einer automatischen Installation unumgänglich. Die entwickelte Routine installiert zunächst alle notwendigen Softwarekomponenten. Danach werden die vielfältigen Konfigurationen der einzelnen Softwarekomponenten vorgenommen. Zum Schluss werden entsprechende Verknüpfungen zur Software auf dem Desktop erstellt, um schnell und gezielt den Demonstrator starten zu können. Die Installationsroutine ermöglicht es jedem Projektpartner ohne eine aufwändige Installationsarbeit in wenigen Minuten eine lauffähige Version des Demonstrators nutzen zu können.

Die erste Version des getesteten Demonstrators wurde im Oktober 2010 den Projektpartnern zum Download auf einer Webplattform zur Verfügung gestellt. Diese dient auch für das Bereitstellen von Fehlerkorrekturen und aktualisierten Versionen des Demonstrators. Die Updates sind wiederum in einer Routine enthalten, die durch wenige Interaktionen eine sichere Aktualisierung des Demonstrators bereitstellt. Die Webplattform enthält zudem ein Wiki, das eine Benutzerdokumentation bereitstellt. Bis zum Projektende wurden sechs umfangreichere Updates bereitgestellt.

Für die Bereitstellung und Pflege des Demonstrators bis zum Projektende waren keine besonderen Mittel eingeplant worden. Diese Mittel wurden daher als zusätzliche Eigenleistung für die Projektpartner erbracht. Mit der Bereitstellung und Pflege des Demonstrators wurden die Ziele des Unterarbeitspaketes 4.5 planmäßig erreicht.

Im Unterarbeitspaket 4.6 sollte die Theoretische Validierung der Gesamtmethodik erfolgen. Erwartete Ergebnisse waren die Validierung der Simulationsergebnisse und

eine Bewertung des Nutzens der Gesamtmethodik anhand der Optimierung der Sicherheitsinfrastruktur sowie der Nachweis der Eignung des Demonstrators für ein effektives und effizientes Risikomanagement Kritischer Infrastrukturen.

Mit Hilfe des Demonstrators wurde auf zwei Projekttreffen Anfang 2011 beim Anwender und beim Projektkoordinator die Gesamtmethodik anhand eines Fallbeispiels zur Optimierung der Sicherheitsinfrastruktur (Einsatz von Flüssigkeitsscannern) validiert und damit der Nachweis für die Eignung des Demonstrators für ein effektives und effizientes Risikomanagement Kritischer Infrastrukturen erbracht. Das Fallbeispiel wurde in Arbeitspaket 5 systematisch weiterentwickelt und wurde in [3] ausführlich dargestellt.

Das Fallbeispiel dient zugleich als Grundlage für die Anwenderdokumentation des SiVe-Demonstrators worin der Aufbau, die Funktionsweise, das Format der Eingabedaten und die korrekte Interpretation der Ausgabedaten beschrieben werden. Diese Arbeiten erfolgten hauptsächlich zusammen mit EADS München/Unterschleißheim (Cassidian) sowie der Technischen Universität München.

2.1.9. Arbeitspaket 5: Szenarienbasierte Simulation und quantitative Risikobewertungen

Dieses Arbeitspaket bestand aus zwei Unterarbeitspaketen, die im Folgenden mit ihren geplanten Ergebnissen und Aufwendungen aufgeführt sind.

AP 5.1: Analyse und Bewertung
Ergebnis: Praktische Validierung der Gesamtmethodik.
Aufwand: 500 PT

AP 5.2: Sensitivitätsanalysen
Ergebnis: Erkenntnisse über die Sensitivität der Sicherheitsinfrastrukturen hinsichtlich der Simulationsparameter als Grundlage für das Treffen von Investitionsentscheidungen zur Entwicklung neuer Sicherheitstechnologien.
Aufwand: 40 PT

2.1.10. Verwendung der Zuwendungen und erzielte Ergebnisse AP 5

Im Unterarbeitspaket 5.1 waren mittels der Durchführung von Simulationsstudien die theoretische Validierung der Gesamtmethodik zusammen mit den Anwendern dem Praxistest zu unterwerfen. Dazu wurden zusammen mit dem Anwender (Flughafen München) ein Bedrohungsszenario ausgewählt und in umfangreichen Simulationsstudien untersucht. Da verlässliche Daten insbesondere hinsichtlich der Erkennungsraten der untersuchten Sicherheitstechnologie (Flüssigkeitsscanner) nicht zur Verfügung standen, wurde der relevante Parameterraum systematisch variiert, um praxisrelevante Aussagen zu erhalten. Damit erwies es sich nicht nur als sinnvoll, sondern auch als notwendig, die geplanten Sensitivitätsanalysen innerhalb der Simulationsstudien durchzuführen. Dabei bestätigte sich die Annahme bei der Projektplanung, dass aussagekräftige Simulationsstudien sehr zeitaufwändig sind.

Es wurden vier Simulationsstudien mit unterschiedlichen Zielstellungen und Prozessen durchgeführt. Dabei wurden zwei unterschiedliche Ausgestaltungen einer Personenkontrolle am Flughafen zugrunde gelegt. Die erste Ausgestaltung stellte eine Personenkontrolle dar, wie sie derzeit an den meisten Flughäfen vorzufinden war. Die zweite Ausgestaltung beinhaltete als moderne Sicherheitstechnologie verschiedene Varianten der neu am Markt verfügbaren Flüssigkeitsscanner. Jede der beiden Ausgestaltungen wurde durch Simulationsstudien hinsichtlich ihrer Nutzen (im Sinne einer Risikoreduktion) und ihrer Kosten hin analysiert.

Neben der Simulation und Bewertung der Schäden wurde auch die Durchkommenswahrscheinlichkeit eines Täters in Abhängigkeit von der Erkennungsrate des Scanners ermittelt. Ferner wurden die Auswirkungen des Einsatzes von Flüssigkeitsscannern auf die Abfertigungszeit und die Kosten pro Passagier ermittelt. Die Ergebnisse sind in der folgenden Abbildung zusammengefasst dargestellt. Eine ausführliche Beschreibung der Modellannahmen und Darstellung der Simulationsergebnisse erfolgte in [3].

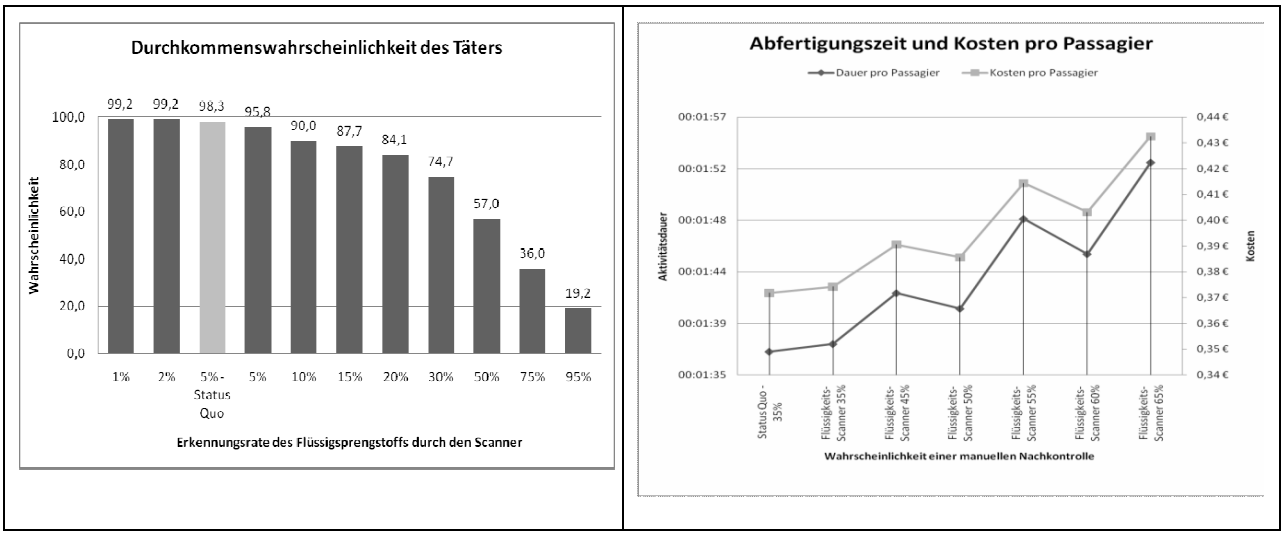

Abb. Erkennungsraten von Flüssigkeitsscannern und Durchkommenswahrscheinlichkeit von Tätern sowie Abfertigungszeit und Kosten pro Passagier bei unterschiedlichen Ausgestaltungen der Personenkontrolle und Einsatz unterschiedlicher Scanner.

Aufgrund von Kosten-Nutzen-Betrachtungen lässt sich aufgrund der Simulationsstudien zeigen, dass eine kosteneffiziente Scannertechnologie eine Detektionsrate von ca. 58% haben sollte.

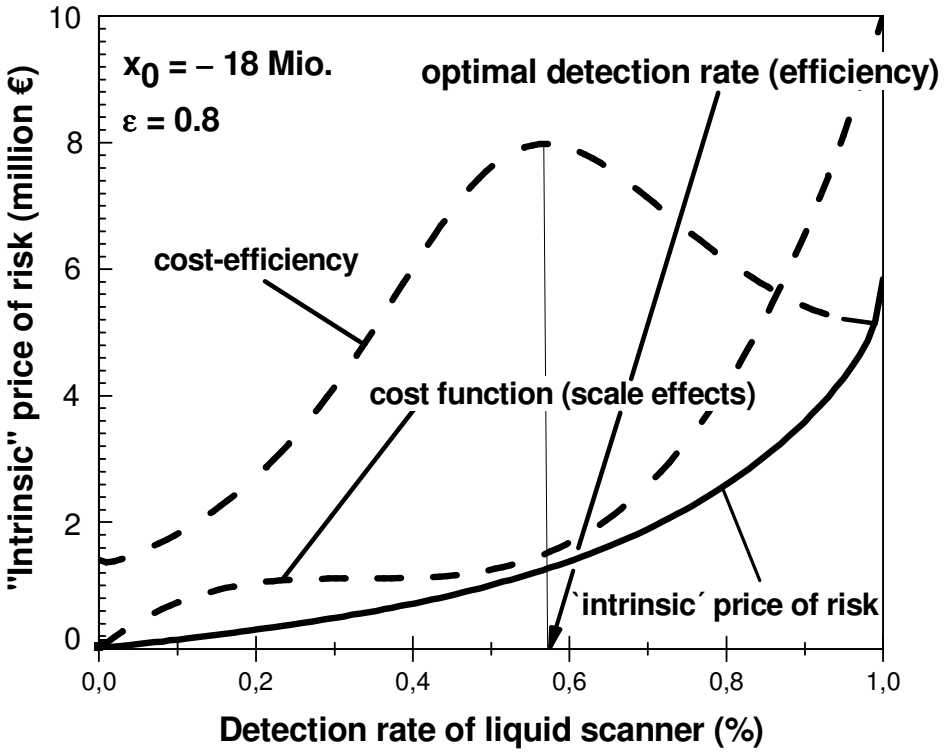

Abb. Optimale Erkennungsrate von Flüssigkeitsscannern bei der Personenkontrolle in Flughäfen

Mit diesen Ergebnissen konnte die Signifikanz sowie die Eignung des eingesetzten Modell- und Methodenverbundes zur Optimierung von Sicherheitsinfrastrukturen nachgewiesen werden. Die Erkenntnisse über die Sensitivität der Kosteneffizienz hinsichtlich des simulierten Technologieparameters (Erkennungswahrscheinlichkeit) kann als geeignete Grundlage für das Treffen von Investitionsentscheidungen zum Einsatz neuer Sicherheitstechnologien dienen.

2.2. Die wichtigsten Positionen des zahlenmäßigen Nachweises

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

- Personalausgaben: 1.127.050,00 €
- FE-Fremdleistungen: 415.850,00 €[2]
- Abschreibungen auf vorhabenspezifische Anlagen: 4.700,00 €
- Reisekosten: 24.000,00 €

2.3. Notwendigkeit und Angemessenheit der geleisteten Arbeit

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 Integration und des Betriebs des Demonstrators – über die ursprüngliche Planung hinaus. Die Kriterien der Notwendigkeit und Angemessenheit blieben dabei jedoch in vollem Umfang gewahrt.

Insgesamt gesehen zeigt sich der Nutzen des Teilprojekts vor allem in der nachgewiesenen Praxistauglichkeit des methodischen Instrumentariums für das wirksame und kosteneffiziente Risikomanagement von Kritischern Infrastrukturen. Anhand von Fallstudien konnte gezeigt werden, dass mit diesem Instrumentarium Erkenntnisse gewonnen werden können, die nach dem oben skizzierten Stand der Wissenschaft nicht oder nur näherungsweise zu erzielen gewesen wären.

2.4. Voraussichtlicher Nutzen (fortgeschriebener Verwertungsplan)

Für den voraussichtlichen wissenschaftlichen und wirtschaftlichen Nutzen des Teilprojektes ist vor allem die allgemeine Anwendbarkeit der Methodik von Bedeutung,

[2] Es wurde ein Unterauftrag an das Institut für Risiko- und Prozessmanagement (IRPM GmbH) in der Höhe von 407.027,03 € vergeben.

wie sie im Demonstrator realisiert wurde. Die bisherigen Erfahrungen mit dem Demonstrator sprechen dafür, dass der gesamte Modell- und Methodenverbund auch für andere kritische Infrastrukturen anwendbar sein wird und insbesondere für eine kosteneffiziente Gestaltung dieser Infrastrukturen unabdingbar ist. Allerdings werden die Spezifika dieser Infrastrukturen besonders berücksichtigt werden müssen. Eine solche Übertragung wird aber erheblich weniger aufwändig sein, als die Erstellung des Demonstrators in dem vorliegenden Projekt.

Ein Einsatz der Simulationssoftware jSIM für die Prozessoptimierung im Allgemeinen und die Anwendung der Ökonomischen Bewertung im Bereich der operationellen Risiken bei Banken im Speziellen erfolgte bereits erfolgreich in separaten Pilotprojekten. Allerdings zeigt sich auch ein Weiterentwicklungsbedarf der Software, insbesondere die Notwendigkeit der Integration von Kennzahlensystemen. Insgesamt wurden mit den Pilotprojekten die wirtschaftlichen Erfolgsaussichten abgesichert und verbessert. Außerdem ist es erforderlich die vorhandenen Softwarekomponenten weiterzuentwickeln, um eine gute Softwarequalität zu erzielen.

2.5. Fortschritt auf den Forschungsgebiet während des Projekts

Thematisch gab es während des Projektes Berührungspunkte zwischen SiVe und den anderen BMBF-geförderten Vorhaben zur Sicherheit von Verkehrsinfrastrukturen, insbesondere den Projekten „FluSs“ und „Critical Parts“ zur Flughafensicherheit. Nennenswerte Überschneidungen mit den Aufgaben und Zielen dieses Teilprojekts waren dabei jedoch nicht zu erkennen. Dies gilt insbesondere im Hinblick auf den entwickelten Demonstrator. 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 auf Simulationsstudien basiert.

Insofern kann festgestellt werden, dass die Ergebnisse des Projektes im wesentlichen den Fortschritt auf dem Forschungsgebiet während des Projektes geprägt haben und zukünftig bei weiteren Vorhaben zu berücksichtigen sein werden.

2.6. Veröffentlichungen der Projektergebnisse

Die folgende Liste enthält die veröffentlichten SiVe-Arbeiten, zu denen das Teilprojekt beigetragen hat.

[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.