Schlussbericht nach Nr. 8.2 NKBF 98

BMBF-Verbundforschungsvorhaben

ZE: EADS Deutschland GmbH
Förderkennzeichen: 13N10027

Vorhabenbezeichnung:
„Verbesserung der Sicherheit von Verkehrsinfrastrukturen (SiVe)“

Teilvorhaben: Entscheidungsbasierte Simulation von Sicherheitsprozessen und Gesamtintegration

Laufzeit des Vorhabens: 01.07.2008 - 31.06.2011

kostenneutral verlängert bis 30.09.2011

Projektleiter: Olaf Heinzinger

Autoren: Dr. D’Avanzo, John; Dr. Dickmanns, Dirk ; Goldner, Sascha; Diehl, Hermann

EADS Deutschland GmbH,

handelnd für den Bereich EADS Innovation Works Germany

Willy-Messerschmitt-Str., 85521 Ottobrunn

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung, und Forschung unter dem Förderkennzeichen 13N10027 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den einzelnen Autoren.

Berichtsblatt

1. ISBN oder ISSN geplant	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht
3. Titel Verbesserung der Sicherheit von Verkehrsinfrastrukturen: Entscheidungsbasierte Simulation von Sicherheitsprozessen und Gesamtintegration	
4. Autor(en) [Name(n), Vorname(n)] Dr. D'Avanzo, John; Dr. Dickmanns, Dirk ; Goldner, Sascha; Diehl, Hermann	5. Abschlussdatum des Vorhabens 30.09.2011
	6. Veröffentlichungsdatum geplant
	7. Form der Publikation geplant
8. Durchführende Institution(en) (Name, Adresse) EADS Deutschland GmbH, EADS Innovation Works Germany Willy-Messerschmitt-Str., 85521 Ottobrunn	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 13N10027
	11. Seitenzahl 122
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 17
	14. Tabellen 32
	15. Abbildungen 70
016. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Themenschwerpunkt von SiVe („Verbesserung der Sicherheit von Verkehrsinfrastrukturen") ist die systematische Analyse, Modellierung, Simulation, Berechnung und Evaluierung von Bedrohungs- und Lastszenarien sowie von Sicherheitssystemen. Neuartige Risiken und Bedrohungssituationen, die zunehmende Komplexität der Sicherheitssysteme und das bislang praktizierte reaktive Risiko- und Sicherheitsmanagement motivieren eine objektive Bewertung von Restrisiken und die daran orientierte werkzeugunterstützte Optimierung von Sicherheitssystemen. Die Systeme zur Gewährleistung der Sicherheit bei Verkehrsinfrastrukturen – insbesondere in sensiblen Bereichen wie Flughäfen – sind äußerst komplex und vielschichtig. In der vorliegenden Arbeit des Teilvorhabens „Entscheidungsbasierte Simulation von Sicherheitsprozessen und Gesamtintegration" wird gezeigt, dass eine Gesamtsimulation dieses Themenkomplexes unter Berücksichtigung von Sicherheits- und Wirtschaftlichkeitsaspekten dennoch möglich ist; es werden verschiedene Ansätze verglichen und anhand von Simulationsstudien auf realitätsnahen Daten evaluiert.	
19. Schlagwörter Verkehrsinfrastruktur, Sicherheit, Gesamtsimulation	
20. Verlag	21. Preis

Document Control Sheet

<table>
<tr><td>1. ISBN or ISSN tbd</td><td colspan="2">2. type of document (e.g. report, publication) final report</td></tr>
<tr><td colspan="3">3. Title

Improving the Security of Traffic Infrastructures: decision-based simulation of security processes and their integration</td></tr>
<tr><td rowspan="3">4. author(s) (family name, first name(s))

Dr. D'Avanzo, John; Dr. Dickmanns, Dirk ; Goldner, Sascha; Diehl, Hermann</td><td colspan="2">5. end of project

30.09.2011</td></tr>
<tr><td colspan="2">6. publication date tbd</td></tr>
<tr><td colspan="2">7. form of publication tbd</td></tr>
<tr><td rowspan="3">8. Durchführende Institution(en) (Name, Adresse)

EADS Deutschland GmbH,

EADS Innovation Works Germany

Willy-Messerschmitt-Str., 85521 Ottobrunn</td><td colspan="2">9. originator's report no.</td></tr>
<tr><td colspan="2">10. reference no. 13N10027</td></tr>
<tr><td colspan="2">11. no. of pages 122</td></tr>
<tr><td rowspan="3">12. sponsoring agency (name, address)

Bundesministerium für
Bildung und Forschung (BMBF)

53170 Bonn</td><td colspan="2">13. no. of references 17</td></tr>
<tr><td colspan="2">14. no. of tables 32</td></tr>
<tr><td colspan="2">15. no. of figures 70</td></tr>
<tr><td colspan="3">16. supplementary notes</td></tr>
<tr><td colspan="3">17. presented at (title, place, date)</td></tr>
<tr><td colspan="3">18. abstract

Focus of SiVe (Improving the security of traffic infrastructures) is the systematic analysis, modeling, simulation, computation and evaluation of threat and load scenarios as well as security systems. New risks and threat situations, the increasing complexity of security systems and the commonly employed reactive risk and security management justify an objective assessment of remaining risks and a task-oriented, tool-assisted optimization of these security systems.

Approaches to guaranteeing the security of traffic infrastructures – in particular in sensitive areas such as airports – are extremely complex and involve multiple technology and security layers. The present work as part of the research project "decision-based simulation of security processes and their integration" shows that an integrative simulation of these topics based on security and economic aspects is feasible; several variations of alternative approaches are compared and quantitatively evaluated using simulation studies on realistic data.</td></tr>
<tr><td colspan="3">19. keywords

Traffic infrastructure, security, integrative simulation</td></tr>
<tr><td colspan="2">20. publisher</td><td>21. price</td></tr>
</table>

Inhalt

Abbildungen

Tabellenverzeichnis

I. KURZE DARSTELLUNG

I.1. AUFGABENSTELLUNG

Themenschwerpunkt von SiVe („Verbesserung der Sicherheit von Verkehrsinfrastrukturen“) ist die systematische Analyse, Modellierung, Simulation, Berechnung und Evaluierung von Bedrohungs- und Lastszenarien sowie von Sicherheitssystemen. Neuartige Risiken und Bedrohungssituationen, die zunehmende Komplexität der Sicherheitssysteme und das bislang praktizierte reaktive Risiko- und Sicherheitsmanagement motivieren eine objektive Bewertung von Restrisiken und die daran orientierte werkzeugunterstützte Optimierung von Sicherheitssystemen.

Der übergeordnete Ansatz zur Beantwortung der Fragestellungen ist „Modellbildung und Simulation“ (M&S), d.h. im Sinne einer Kosten-Nutzen-Betrachtung und Risikobewertung von Sicherheitssystemen werden die zu betrachtenden Realsysteme durch virtuelle Rechnermodelle abgebildet und im Rechner simuliert. Somit können unterschiedliche Parametrisierungen und Layouts von Sicherheitssystemen und den gewählten Bewertungsaspekten analysiert und optimiert werden.

Um eine möglichst umfassende Abbildung der Realsysteme zu gewährleisten, werden mehrere Modellbildungsansätze verwendet. Eine Agenten-basierte Modellierung (AP 3.2) wird zur Abbildung von Personenströmen und –verhaltensweisen verwendet. Eine Geschäftsprozessmodellierung (AP 3.5) dient zur Repräsentation der operativen Abläufe des betrachteten (Sicherheits-) Systems. Ökonomische Parameter werden durch ein gesondertes Kostenmodell (AP 3.4) abgebildet und die, für die Simulation notwendigen stochastischen Parameter, werden in einem separaten stochastischen Modell (AP 3.3) zusammengefasst. Schlussendlich erfolgt eine Integration der verschiedenen Modellierungsansätze zu einem Gesamtsystem (AP 4), das dann durch Simulationsstudien (AP5) analysiert werden kann.

Grundlage für sämtliche Simulationsstudien ist ein Bedrohungs-Szenario (AP 1) vor dessen Hintergrund die Analyse des Sicherheitssystems erfolgt.

I.2. VORAUSSETZUNGEN, UNTER DENEN DAS VORHABEN DURCHGEFÜHRT WURDE

Das Vorhaben hatte eine Laufzeit von drei Jahren und drei Monaten und wurde durch den Fördergeber mit einer Zuwendung in Höhe von 1.476.500 EUR ausgestattet. Für das Teilvorhaben „Entscheidungsbasierte Simulation von Sicherheitsprozessen und Gesamtintegration“ konnte als Projektpartner aus Anwendersicht die Flughafen München GmbH gewonnen werden. Entsprechend des Projektantrags sollte die detaillierte Ausgestaltung der Arbeitsanteile in enger Abstimmung mit dem Anwender erst nach Projektbeginn erfolgen. Dabei wurde für jedes der im Projektantrag beschrieben Forschungsthemen ein Szenario erarbeitet, das einerseits als Anwendungsszenario für die Forschungsarbeiten geeignet ist und andererseits einem realen Bedarf im Rahmen des Sicherheitskonzeptes des Flughafens München entspricht.

I.3. Planung und Ablauf des Vorhabens

Durch Integration der genannten multidisziplinären Ansätze zu einer gemeinsamen Methodik soll eine Demonstrator-Software entstehen, ein Expertensystem für Risikomanagement, das eine Simulationsumgebung umfasst. Dazu werden Bedrohungsszenarien definiert und verschiedenen Sicherheitssystemen gegenübergestellt. Dazu gehören unter anderem die Auswahl von Sicherheitstechnologien und von Sicherheitsprozessen und Handlungsvorschriften durch die jeweils zuständigen Stellen.

Zu Projektbeginn waren die Anforderungen an die Ereignisbasierte Modellierung nur ungenau beschrieben. Die erste Aufgabe bestand somit darin, die Rolle der Prozessmodellierung im Projektkontext zu identifizieren und darauf aufbauend die Anforderungen zu konkretisieren. Im Laufe dieses iterativen Verfahrens wurden mehrere Prozessnotationen und –tools in Betracht gezogen.

I.4. Wissenschaftlicher und Technischer Stand bei Vorhabensbeginn

Die Modellierung und Simulation von in Sicherheitsszenarien eingesetzten Verfahren ist nur teilweise methodisch entwickelt. Die Wirksamkeit dieser Verfahren und insbesondere spezieller Technologieausprägungen konnte vor Projektbeginn nicht ausreichend quantifiziert werden.

Die vielfältigen Sicherheitsprozesse in Flughäfen sind verschiedenen zuständigen Behörden und Institutionen zugeordnet. Es existiert kein definierter Prozess zur Integration; dementsprechend ist die Vernetzung der Sicherheitsprozesse nicht vollständig.

I.5. Zusammenarbeit mit anderen Stellen

Als Projektpartner war die Flughafen München GmbH, Bauhaus Luftfahrt (BHL), die ckc AG, Das Frauenhofer-Anwendungszentrum für Logistiksystemplanung und Informationssysteme (ALI) und die TU München (TUM) einbezogen.

Während und nach der Modellierungsphase für den SiVe Demonstrator erfolgte im Rahmen von Interviews eine enge Abstimmung mit dem Flughafen München und dem Fraunhofer-Institut für Materialfluss und Logistik am Flughafen Frankfurt zur Sicherstellung der Korrektheit der Prozessmodelle.

Am Flughafen München erfolgte ein Abgleich der Prozessmodelle mit den Abteilungen:

- Operativer Sicherheitsdienst (Hr. Bauer)
- Prozessmanagement (Fr. Reiser)
- Qualitätsmanagement (Fr. Sitter, Hr. Haufe)
- Flughafenfeuerwehr (Hr. Leiwering, Hr. Hecker)

- Sicherheitsmanagement (Fr. Drohm)
- Gepäckabfertigung (Hr. Marx)

Die Prozessmodelle wurden abschließend von den Abteilungen des Flughafens München akzeptiert und können somit als valide betrachtet werden.

II. EINGEHENDE DARSTELLUNG

II.1. VERWENDUNG DER ZUWENDUNG UND ERZIELTE ERGEBNISSE

II.1.1. *ÜBERBLICK*

Eines der Ergebnisse des Projektes ist der SiVe-Demonstrator. Der Demonstrator vereint sämtliche methodischen Erkenntnisse und Ergebnisse des Projektes in einer Software-Lösung. Er besteht aus mehreren verschiedenen Software-Werkzeugen (Module), die jedoch über eine gemeinsame grafische Benutzeroberfläche durchgängig miteinander verbunden sind und bedient werden können. Diese sind:

- Szenario-Builder
- Prozess-Modellierung
- Agenten-basierte Simulation
- Stochastische Simulation
- Risikobewertung.

Mit Hilfe des SiVe-Demonstrators können somit Kosten-Nutzen-Analysen von Sicherheitssystemen bezüglich einer gegebenen Bedrohung durchgeführt werden.

Ein weiteres Ergebnis des Projektes sind Business Cases, die mit Hilfe des Demonstrators behandelt werden können und die dessen Mehrwert veranschaulichen (vgl. II.1.2.4).

Als Ergänzung und Erweiterung des SiVe Demonstrators wurde ein weiteres System mit einem etwas anderen mathematisch-logischen Ansatz implementiert, das PoC (Proof of Concept). Während der SiVe Demonstrator auf beispielbasierter Regelbildung beruht, verwendet der PoC eine direkte wahrscheinlichkeitsbasierte Modellierung.

II.1.2. *DER SIVE DEMONSTRATOR*

Systemarchitektur des SiVe Demonstrators

Referenz-Szenarien
Als Grundlage für die Entwicklung der Facharchitektur des SiVe-Demonstrators sind sog. Referenz-Szenarien definiert worden. Zweck dieser Szenarien war es, die Entwicklung der Facharchitektur und damit deren Funktionsumfang an konkreten Beispielen zu orientieren, um einen möglichst großen Praxisbezug der Lösung zu erhalten.

Die Referenz-Szenarien enthalten die wichtigsten beteiligten Akteure, operative Abläufe und grobe Zeitangaben. Details wie beispielsweise Detektionsraten von Scannern sind nicht enthalten. Die Beschreibung der Referenz-Szenarien ist im Projektordner zu finden.

Facharchitektur

Die SiVe-Facharchitektur samt Integration der verschiedenen Modellierungsaspekte auf oberster Ebene ist in Abbildung 1 darstellt. Jedes Modul stellt einen Modellierungsansatz bzw. eine Methodik dar. Eine Ausnahme hiervon ist der Prozessbuilder, der anstatt einer (fachlichen) Modellierung den fachlichen Integrationskern des Systems umsetzt. Der Prozessbuilder stellt einerseits die Ergebnisse der Szenario- und Prozessmodellierung fallbezogen dar, andererseits dient er als Grundlage der nachfolgenden Simulationen und Bewertungen. Die Pfeile in Abbildung 1 stellen den Informationsfluss im Gesamtsystem dar, d. h. die Abhängigkeiten zwischen den einzelnen Modulen.

Im Folgenden werden die Module und deren Rolle in SiVe im Gesamtbild des Systems beschrieben. Hieraus ist auch die Rolle der einzelnen Projektpartner ersichtlich. Lediglich die Flughafen München GmbH (FMG) nimmt keine aktive Rolle bei der Umsetzung der Systemarchitektur ein, sondern steht dem Projekt als Informationslieferant und Berater zur Verfügung. Ergänzend ist in der SiVe-Systemdokumentation **Fehler! Verweisquelle konnte nicht efunden werden.** die Facharchitektur inkl. der Systemintegration detailliert beschrieben.

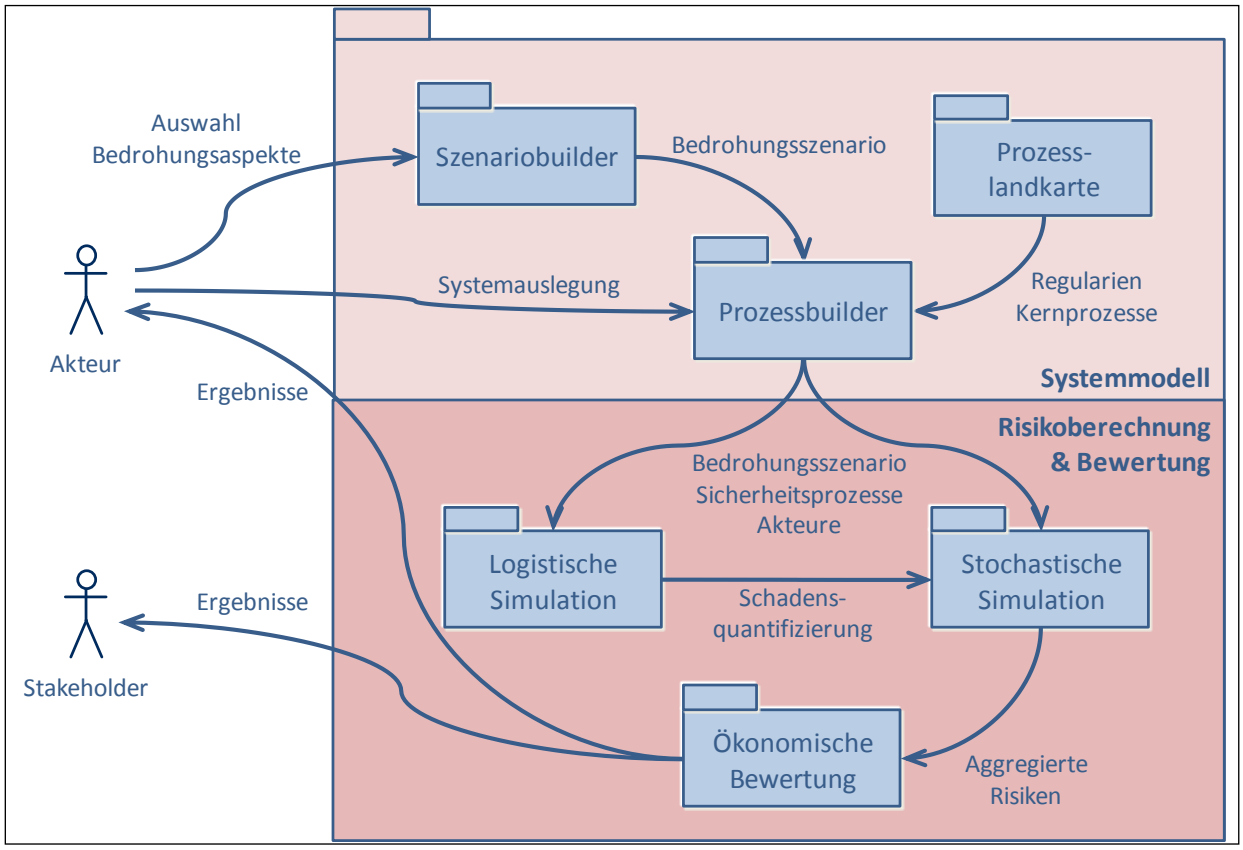


Abbildung 1: SiVe-Facharchitektur

SiVe besteht aus zwei fachlichen Sichten, dem Systemmodell sowie der Risikoberechnung und Bewertung. Szenariobuilder, Prozesslandkarte und Prozessbuilder dienen der Abbildung des

Systemmodells – in der hier vorliegenden Betrachtung des Flughafens. Der Prozessbuilder verdichtet hierbei die Erkenntnisse des Systemmodells, so dass diese in der Risikoberechnungssicht (Simulation) verwendbar sind. Mittels der logistischen und stochastischen Simulation sowie der nachgelagerten ökonomischen Bewertung wird die Risikoberechnung auf Basis des vorgeschalteten Systemmodells durchgeführt. Die Integration der unterschiedlichen Modellierungsansätze erfolgt durch die abgebildeten Informationsflüsse. Letztlich ausgegebene Risiko- und Kostenwerte ergeben sich auf Basis des SiVe-Prozessmodells. In Abbildung 1 sind Akteur und Stakeholder die externen Nutzer von SiVe. Akteure interagieren hierbei direkt mit dem betrachteten System Flughafen; sie konfigurieren und bedaten das System. Stakeholder unterscheiden sich von Akteuren insofern, dass sie nur Informationen bzw. Ergebnisse aus SiVe beziehen. Akteure sind beispielweise Anbieter von Sicherheitssystemen und Betreiber des Systems Flughafen. Der Gesetzgeber stellt einen exemplarischen Stakeholder dar.

Im Folgenden sind die Module und deren Rolle in SiVe kurz beschrieben.

Der Szenariobuilder (BHL)

Der Szenariobuilder basiert auf der Struktur- und Systemanalyse (mittels der Methode des „Structural Complexity Management“) und stellt ein Analysewerkzeug dar. Er beinhaltet die strukturellen, logischen Abhängigkeiten zwischen den grundlegenden Systemelementen. Diese Systemelemente sind zum einen (in Klassen eingeteilte) Bedrohungsaspekte, die in Kombination die möglichen Bedrohungsszenarios ergeben. Zum anderen sind Systemelemente auch präventive Sicherheitsmechanismen, die im System Flughafen (ebenfalls in Kombination) zum Einsatz kommen. Der Szenariobuilder erlaubt auf Basis der hinterlegten Zusammenhänge zwischen Systemelementen die Bildung konsistenter Bedrohungsszenarien sowie die Identifikation der hierfür relevanten Schutzmechanismen (präventiv und reaktiv). Daraus abgeleitet können zudem die Akteure identifiziert werden, die in die Schutzmechanismen eingebunden sind. Der Szenariobuilder stellt damit das Grund-Systemmodell für SiVe.

Detaillierte Informationen zu Aufbau und Funktionsweise des Szenariobuilders sind im Beitrag zu den Arbeitspaketen „Bedrohungsszenarien“ und „Schutzmechanismen“ von Bauhaus Luftfahrt und in Zwischenbericht von Bauhaus enthalten.

Die Prozesslandkarte (CASSIDIAN)

Die Prozesslandkarte liefert eine Übersicht der sicherheitsrelevanten Kernprozesse am Flughafen auf verschiedenen Abstraktionsebenen. Die Prozessabläufe werden als BPMN-Modelle, die durch Regularien definiert bzw. spezifiziert sind, abgebildet. Die Prozessschritte/-ketten der Prozesslandkarte sind mit den Systemelementen aus dem Szenariobuilder (Bedrohungsaspekte bzw. Schutzmechanismen) im Prozessbuilder (s. nächster Absatz) vernetzt und daher auch Bestandteil des Systemmodells. Aufgrund dieser Vernetzung erlaubt SiVe die Identifikation der relevanten (Sicherheits-)Prozessketten basierend auf der Bildung spezifischer Bedrohungsszenarien, d.h. für jedes mit dem Szenariobuilder zusammengestellte, gültige Bedrohungsszenario beinhaltet die Prozesslandkarte die vorhandenen, wirkenden Prozessketten. In anderer Richtung können durch die Auswahl von Prozessketten die hiervon betroffenen Bedrohungsszenarien automatisch ermittelt werden. Somit kann bei Fokussierung eines bestimmten Prozessablaufs identifiziert werden, welche Szenarios bei einer Änderung dieses Prozessablaufs betroffen wären.

Die Prozesslandkarte oder Prozessmodellierung entspricht der Ereignis-basierten Modellierung (AP 3.5) und liegt somit in der Verantwortung von CASSIDIAN, SDGE1. Weitere Informationen zu Aufbau und Anwendung der Prozesslandkarte sind Kapitel II.1.2.3 Integration zu finden.

Der Prozessbuilder (CASSIDIAN, BHL, ALI, ckc)

Der Prozessbuilder verbindet Szenariobuilder und Prozesslandkarte und stellt mit seinen Ergebnissen den Kern von SiVe dar. Ein Prozess wird in der Facharchitektur auf Basis des SiVe-Prozesselementmodells definiert. Ein Prozesselement ist für ein Szenario die kleinste Einheit, aus der sich ein Prozess aufbaut und die durch Metriken und Ressourcen beschrieben wird. Metriken ermöglichen die Bewertung von Prozessen, d. h. die Performance/Wirksamkeit eines Prozesses wird durch sie quantifizierbar. Die Ressourcen definieren die Größen, die mit Kosten verbunden sind (z. B. Betriebs- und Personalkosten, Durchsatz, Prozessdauer usw.). Sowohl die Prozessressourcen als auch die Prozessmetriken sind vom zugehörigen Bedrohungsszenario abhängig.

Der Prozessbuilder stellt die Ergebnisse aus dem Systemmodell, und damit die Informationen aus dem Szenariobuilder und der Prozesslandkarte, für die Risikoberechnung und Bewertung integriert zur Verfügung (SiVe-Berechnungsgrundlage). Da alle Simulationsmodelle auf diesen Daten aufsetzen gewährleistet diese Methodik die Konsistenz des Gesamtansatzes.

Detaillierte Informationen zum Aufbau, der Funktionsweise und zu den Schnittstellen des Prozessbuilders sind in Kapitel 0 enthalten.

Stochastische Simulation (ckc)

Die stochastische Modellierung und Simulation stellt den Simulationskern von SiVe dar. Hier wird durch Prozessmodelle das System Flughafen mit Bedrohungslage und Sicherheitssystemen modelliert. Die Modelle dafür werden aus der SiVe-Berechnungsgrundlage über eine funktionale Schnittstelle bereitgestellt. Der Einfluss der Logistik auf die Risikobetrachtung wird als Schadensquantifizierung durch eine agentenbasierte Simulation ermittelt.

In die stochastische Simulation fließen Prozess-, Risiko- und Schadensmodelle ein. Details über die angewendete Methodik sind in der Systemdokumentation der ckc AG zu finden.

Logistische Simulation (ALI)

Logistische Aspekte in der Risikobetrachtung werden über die Agenten-basierte/logistische Modellierung abgebildet und simuliert. Die Grundlage dieser Modelle wird durch den Prozessbuilder bereitgestellt. Die Simulationsergebnisse dienen der Schadensquantifizierung durch die stochastische Simulation. Die Verantwortung für diesen Arbeitsanteil liegt beim Fraunhofer-Anwendungszentrum für Logistiksystemplanung und Informationssysteme (ALI).

Ökonomische Bewertung (TUM)

Nachdem mögliche Schadensverteilungen für ein Szenario bzw. mehrere Szenario-Cluster ermittelt wurden, können die Risiken unter Kosten/Nutzen-Aspekten in diesen nachgelagerten Modul ermittelt werden. Der Technischen Universität München obliegt die Verantwortung für die ökonomische Bewertung.

Die SiVe-Methodik erlaubt somit ein integriertes Vorgehen für die Risikobewertung und -quantifizierung von Bedrohungsszenarien und Schutzmechanismen über Prozessmodelle: Bedrohungsaspekte, die daraus resultierenden konsistenten Bedrohungsszenarien und die angewandten sicherheitsrelevanten Prozessketten fließen nach Attributierung in das Risiko-

modell ein. Durch die Aggregation der Risiken kann die Sicherheitsperformance des betrachteten Systems übergreifend ermittelt werden.

Demonstrator-Aufbau

Bei der Erstellung der Demonstrator-Software wurde die Facharchitektur nahezu unverändert übernommen, so dass der modulare Charakter der Architektur erhalten blieb. Die nachfolgende Abbildung zeigt die einzelnen Module der Software und deren Zusammenspiel.

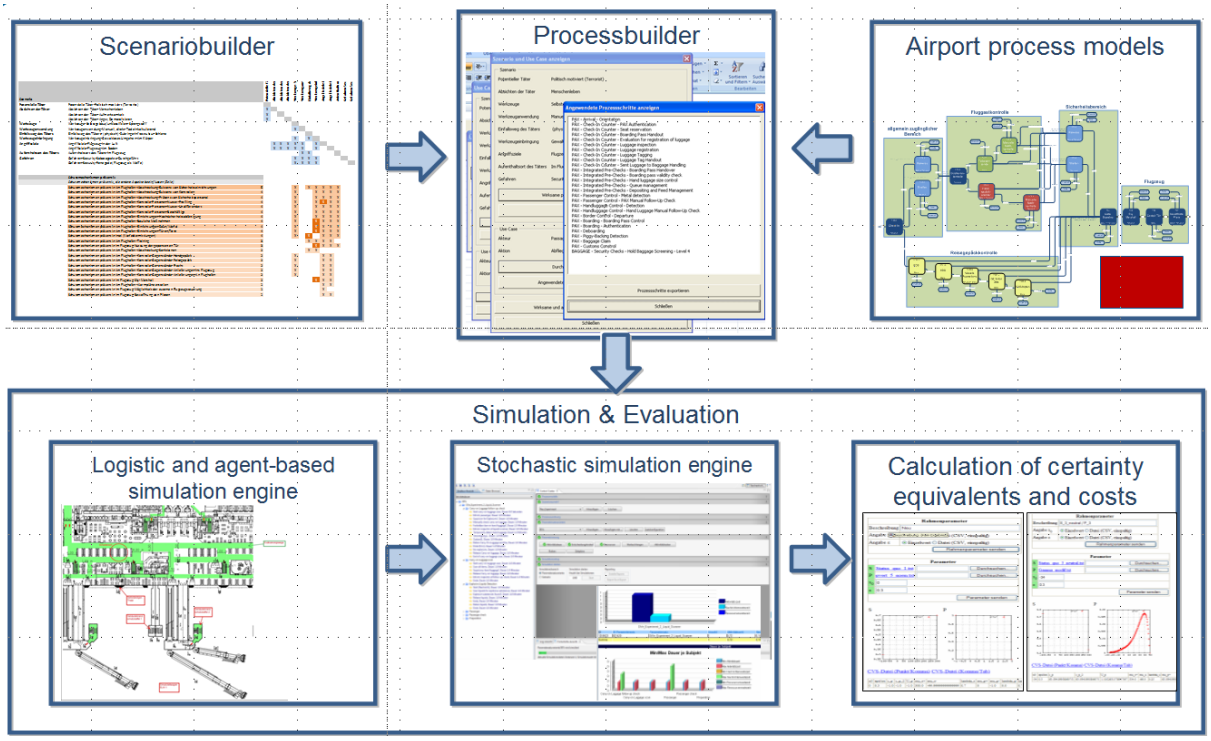


Abbildung 2: Module der Demonstrator-Software

Detaillierte Erläuterungen zur Verwendung des SiVe-Demonstrators sind im Projekt-Wiki zu finden (siehe Anhang).

Prozessmodellierung

Den Hauptarbeitsanteil von CASSIDIAN im Projekt bildet die Ereignis-basierte Modellierung, d.h. die Prozessmodellierung. Ziel hierbei ist es sämtliche operative Geschäftsprozesse, die im Projektkontext relevant sind, abzubilden. Wie bereits erläutert, wurden im Projekt ausschließlich präventive Sicherheitsmechanismen analysiert, d.h. im Rahmen der Prozessmodellierung werden ebenfalls ausschließlich präventive Sicherheitsprozesse behandelt.

Grundlagen

Bei der Geschäftsprozessmodellierung gilt es verschiedene Arten von Prozessen zu unterscheiden: Kernprozesse, Unterstützungsprozesse und Management-Prozesse. Die Kernprozesse tragen direkt zur Erzeugung eines Produktes oder einer Dienstleisung bei. Die Unterstützungsprozesse stellen sicher, dass die Rahmenbedingungen für die Kernprozesse erfüllt

sind, wie z.B. eine funktionierende IT-Infrastruktur, auf welche die Kernprozesse aufsetzen. Management-Prozesse sind selbsterklärend.

Fokus im Projekt sind ausschließlich die Kernprozesse eines Flughafens.

Chronologie

Zu Projektbeginn wurde zur Darstellung von operativen Abläufen das Softwarewerkzeug Erudine verwendet, so wie im Projektantrag beschrieben. Anschließend erfolgte die Darstellung der Prozesse als EPKs (Ereignis-basierte Prozessketten) mittels Microsoft Visio. Schlussendlich wurde BPMN (Business Process Modelling Notation) als Beschreibungssprache beschlossen und als Modellierungs-Werkzeug Oryx festgelegt. Nachfolgende Abschnitte geben diesbezüglich eine kurze Übersicht.

Notationen

Bei der Betrachtung von möglichen Notationen zur Geschäftsprozessmodellierung wurden im Wesentlichen zwei Notationen detailliert betrachtet – EPKs und BPMN.

Ereignis-gesteuerte Prozessketten (EPK)

EPKs ist eine grafische Modellierungssprache zur Darstellung von Geschäftsprozessen einer Organisation. Sie wurde 1992 von einer Arbeitsgruppe unter Leitung von August-Wilhelm Scheer an der Universität des Saarlandes in Saarbrücken im Rahmen eines Forschungsprojektes mit der SAP AG zur semiformalen Beschreibung von Geschäftsprozessen entwickelt. Die Methode wurde im Rahmen der Architektur Integrierter Informationssysteme (ARIS) zur Sichten-orientierten Modellierung von Geschäftsprozessen entwickelt und ist wesentliches Element des ARIS-Konzepts. Eine erweiterte Form der Modellierungsmethode EPK stellt die erweiterte Ereignisgesteuerte Prozesskette (eEPK) dar. Die in der EPK dargestellten logischen Abläufe eines Geschäftsprozesses werden anhand der eEPK um die Elemente der Organisations-, Daten- und Leistungsmodellierung erweitert.

Entscheidungen innerhalb von Prozessen werden bei EPKs mit den Verknüpfungsoperatoren „und“, „oder“, „exklusivoder“ beschrieben. Das Grundmodell der Ereignisgesteuerten Prozesskette umfasst neben diesen Operatoren auch Ereignisse und Funktionen. Dazu werden die Objekte mit gerichteten Sequenzpfeilen in einer 1:1-Zuordnung verbunden. Hierbei muss jedoch eine alternierende Reihenfolge von Ereignis und Funktion eingehalten werden. Insgesamt bietet die EPK ca. 10 Modellierungselemente.

Business Process Modelling Notation (BPMN)

BPMN ist ebenfalls eine grafische Notation zur Darstellung von Geschäftsprozessen. Nach Entwicklung durch einen IBM-Mitarbeiter wurde die BPMN im Juni 2005 durch die Object Management Group (OMG) zur weiteren Pflege übernommen und gilt seit 2005 als OMG-Standard. Seit Januar 2011 liegt die Version BPMN 2.0 vor.

BPMN unterstützt eine Vielzahl an unterschiedlichen grafischen Elementen, welche in folgende Kategorien eingeteilt werden:

- Flow Objects: die Knoten (Activity, Gateway und Event) in den Geschäftsprozessdiagrammen
- Connecting Objects: die verbindenden Kanten in den Geschäftsprozessdiagrammen
- Pools und Swimlanes: die Bereiche, mit denen Akteure und Systeme dargestellt werden

- Artifacts: weitere Elemente wie Data Objects, Groups und Annotations zur weiteren Dokumentation

Die BPMN bietet mehr als 50 Modellierungselemente.

Bewertungskriterien

Folgende Bewertungskriterien wurden definiert, um einen Vergleich von verschiedenen Prozessmodellierungsnotationen durchzuführen:

- Intuitivität: intuitive Benutzung und Verständnis der Notationselemente
- Erweiterbarkeit: Möglichkeit benutzerspezifische Notationselemente zu definieren
- Ausdrucksstärke: Umfang der Notationselemente und damit die Möglichkeit der Ausdrucksstärke
- Integrationsfähigkeit: dieses Kriterium bezieht sich ausschließlich auf das Projekt SiVe. Es wird die Verträglichkeit bzw. Ähnlichkeit der Notation mit den anderen in SiVe gewählten Modellierungsansätzen bewertet, d.h. wie gut sich Prozessmodelle mit den anderen Ansätzen integrieren lassen.
- Ausführbarkeit: standardmäßige Ausführbarkeit der erstellten Prozessmodelle in einer Simulationsumgebung
- Kausale Abhängigkeit: Darstellung von kausalen Abhängigkeiten zwischen verschiedenen Prozessen bzw. Akteuren
- Hierarchisierung: Möglichkeit die Prozessmodelle zu gliedern bzw. zu verschachteln, so dass verschiedene Detailierungsebenen definiert werden können.
- Verifizierbarkeit: formeller Nachweis, dass ein Prozessmodell (syntaktisch) korrekt ist.

Vergleich

Basierend auf den definierten Bewertungskriterien wurden mehrere Notationen miteinander verglichen. Untenstehende Tabelle zeigt das Ergebnis, wobei die erste Zeile das am höchsten gewichtete Kriterium und die unterste Zeile das am geringsten gewichtete Kriterium darstellt.

	Standard Petri Netze	Prozess-Algebra	BPMN 2.0	eEPK	Workflow-Netze	Protocol Interfaces
Intuitivität	–	–	+	+	–	–
Ausdrucksstärke	–	–	+	+	+	+
Erweiterbarkeit	+	+	+	+	+	+

	Standard Petri Netze	Prozess-Algebra	BPMN 2.0	eEPK	Workflow-Netze	Protocol Interfaces
Hierarchisierung	–	–	+	+	+	+
Integrationsfähigkeit	+	+	+	–	+	+
Kausale Abhängigkeit	+	+	+	–	–	+
Ausführbarkeit	+	–	+	–	+	+
Verifizierbarkeit	+	+	+	–	+	+

Tabelle 1: Vergleich der Prozess-Notationen

Weitere Informationen zu den Anforderungen an die Notationen, sowie deren Vergleich sind in Goldner 2011 und Babau 2011 zu finden.

Modellierungs-Werkzeuge

Nach der Festlegung von BPMN als Modellierungsnotation erfolgte ein Vergleich verschiedener Modellierungswerkzeuge. Eine umfassende Beschreibung ist in BA2011 zu finden, Tabelle 2 zeigt das Ergebnis.

	Business process modeling tools						
	Innovator 11 Personal Edition	Innovator 11 Enterprise Edition	Signavio SaaS	Jadex Processes	Intalio|BPMS Designer Open source	Intalio |BPMS Enterprise Edition	Oryx
Intuitive	++	++	++	++	++	++	++
BPMN 1.2	– –	– –	++	++	++	– –	++
BPMN 2.0	++	++	++	– –	– –	++	++
Syntax checker for BPMN	++	++	++	++	+	++	++
Semantic validation for BPMN	++	++	++	++	+	++	++
Step through execution for BPMN	– –	– –	++	– –	– –	– –	++
Extensible	++	++	-	++	+	++	++
Import different formats	– –	– –	+	+	+	++	++
Export different formats	– –	– –	+	+	+	++	++
BPMN 1.2 translation to BPEL	– –	– –	– –	– –	++	++	– –
BPMN 1.2 Translation to XPDL	– –	– –	++	– –	– –	– –	– –
Modeling with pools (BPMN specs)	++	++	++	++	++	++	++
Modeling with collapsed-pools (BPMN specs)	– –	– –	– –	– –	++	++	– –
BPMN 1.2 translation to BPMN 2.0	– –	– –	++	– –	– –	– –	– –
User-friendly local installation	++	++	++	-	+	+	– –
Documentation generation in HTML/Word	++	++	– –	– –	-	+ +	– –

Tabelle 2: Vergleich von BPMN-Modellierungs-Werkzeugen

Erudine

Bei Projektbeginn wurde das Expertensystem Erudine als Modellierungs-Werkzeug festgelegt. In Erudine lassen sich Abläufe grafisch darstellen, sowie Beispieldatensätze verwenden, um das modellierte System zu durchlaufen. An den Verzweigungspunkten können Regeln hinterlegt werden, die definieren welcher nachfolgende Pfad bei einem gegebenen Datensatz weiter durchlaufen wird. Die Regeln können interaktiv durch einen Domänenexperten festgelegt werden. Der Experte wird mit konkreten Situationen konfrontiert und definiert für diese konkrete Situation die Entscheidungsregeln. Der Vorteil dieser interaktiven Regelerstellung ist, dass innerhalb kürzester Zeit ein Gesamtverhalten des modellierten Systems über Regeln spezifiziert werden kann, das den Vorstellungen des Experten entspricht. Dadurch wird die Lücke zwischen technischer Modellierung und fachlicher Verhaltensspezifikation verringert, d.h. der Domänenexperte muss kein ausgeprägtes technisches Wissen zur Erstellung von Systemmodellen haben und der technische Modellierer benötigt kein ausgeprägtes fachliches Wissen in Bezug auf Verhaltenszusammenhänge des Systemmodells.

Im Laufe des Projektes wurde gemeinsam entschieden Erudine nicht im Rahmen der Ereignis-basierten Modellierung zu verwenden. Hauptgründe hierfür waren zum einen die Fokussierung im Projekt auf die reine Geschäftsprozessmodellierung und zum anderen die ungenügende Unterstützung seitens Erudine zur Anbindung an das Gesamtsystem des SiVe-Demonstrators. Der direkte, programmtechnische Zugriff auf das Regelsystem von Erudine wäre notwendig gewesen. Erudine hat zum derzeitigen Zeitpunkt keine Möglichkeiten hierzu angeboten. Zur Evaluation der Eignung von Erudine wurde in Zusammenarbeit mit EADS Innovation Works

unter anderem ein Fragebogen angefertigt auf dessen Basis die Entscheidung gegen die Verwendung von Erudine gefällt wurde. Auch die fachliche Einschätzung von EADS Innovation Works, die für die Erstellung der fachlichen Architektur des SiVe-Demonstrators verantwortlich sind, empfiehlt keine Verwendung von Erudine auf Grund der mangelnden Integrationsfähigkeit in das Gesamtsystem.

Oryx

Oryx ist ein Open-Source Modellierungs-Werkzeug zur Visualisierung von Geschäftsprozessen und unterstützt hierzu unterschiedliche Notationen. Der Editor wird durch das Hasso-Plattner-Institut für Software-Systeme (HPI) entwickelt und besitzt vor allem eine herausragende Unterstützung zur Prozessmodellierung mit BPMN 1.2 und BPMN 2.0. Mit Hilfe eines Erweiterung-Mechanismus, der auf ein Plug-In-Prinzip basiert, kann das Werkzeug benutzerspezifischen Anforderungen angepasst und erweitert werden. Darüber hinaus besteht eine große Google-Groups-Gemeinschaft, die schnelle Unterstützung bei Problemen bietet.

Oryx ist ein web-basiertes Werkzeug, das keine lokale Installation erfordert und über einen Web-Browser bedient wird. Die erstellten Modelle werden entweder in einem lokalen oder in dem zentralen Repository des HPI gespeichert. Durch die zentrale Speicherung kann der Benutzer (über eine gesicherte Verbindung) global auf die Prozessmodelle zugreifen. Weitere herausragende Merkmale von Oryx sind ein Syntax-Check, der das erstellte Modell auf die syntaktische Korrektheit hin überprüft, sowie ein Mechanismus, zum schrittweisen Durchlauf durch das Prozessmodell. Der Benutzer kann bei Letzterem festlegen, welcher Prozesspfad eingeschlagen werden soll und so überprüfen, ob das Prozessmodell das gewünschte Verhalten abbildet. Prozess-Simulation oder Prozess-Automatisierung wird nicht unterstützt.

Neben BPMN unterstützt Oryx die Modellierung mit Petri-Netzen, Workflow-Netzen, UML, EPK und Block Diagrammen. Eine kommerzielle Version von Oryx samt entsprechenden Erweiterungen wird von Signavio in Form des Signavio Process Editors angeboten. Durch eine Schnittstelle zu dem Ausführungs-Framework Activiti können die Oryx-Prozessmodelle automatisiert werden. Hierbei übernimmt Activiti die Rolle einer Koordinierungs-Instanz, welche zum einen die auszuführenden Aufgaben an die entsprechenden Rollen / Akteure verteilt und zum anderen die Ausführung des Prozesses überwacht.

Eine Einführung in das Werkzeug ist auf der Oryx-Website[1] zu finden.

Rechtliche Rahmenbedingungen

Rechtliche Rahmenbedingungen, wie Gesetze und Richtlinien, sind besonders im Bereich der Sicherheit bestimmende Einflussfaktoren und geben oftmals sehr genaue und enge Grenzen vor innerhalb dieser sich operative Geschäftsprozesse bewegen müssen. Somit ist eine Kenntnis der zutreffenden rechtlichen Rahmenbedingungen im Projektkontext zwingend erforderlich. Hierzu wurde die internationale, europäische und nationale Legislative in Bezug auf Luftverkehrssicherheit analysiert und die zutreffenden gesetzlichen Rahmenbedingungen zusammengetragen.

[1] http://www.oryx-project.org/

Internationale Rahmenbedingungen

Internationale Rahmenbedingungen zur Sicherheit im Luftverkehr werden im Anhang 17 zum Chicagoer Abkommen definiert und sind für die 190 Mitgliedsstaaten der ICAO (International Civil Aviation Organisation) verbindlich. Deren konkrete Ausgestaltung muss entweder in nationalem Recht oder bei europäischen Mitgliedsstaaten in europäischem Recht nachgewiesen werden.

Der ICAO Annex 17 ist im Rahmen des Projektes maßgebend. Darin sind die rechtlichen Grundlagen und Rahmenbedingungen für die Sicherheitsmaßnahmen an sämtlichen europäischen Flughäfen definiert. Insbesondere in Kapitel 4 des Annexes sind konkrete Vorgaben zu präventiven Sicherheitsmechanismen beschrieben, denen alle operativen Sicherheitsabläufe und Sicherheitsprozesse an den Flughäfen der europäischen Mitgliedsstaaten genügen müssen.

Es existieren weitere internationale Abkommen zum Schutz der Zivilluftfahrt (wie z.B. das Tokioter Abkommen), die jedoch alle im Chicagoer Abkommen und dessen Annexe aufgegangen sind.

Europäische Rahmenbedingungen

Europäische Rahmenbedingungen sind in SiVe die wesentliche Informationsquelle, da diese konkrete Anforderungen an die Sicherheitsmechanismen im Luftverkehr beschreiben. Verbindliche Vorgaben können auf europäischer Ebene grundsätzlich nur in Form von EU-Verordnungen realisiert werden. Hierbei gilt es zwei unterschiedliche Arten von Verordnungen zu unterscheiden: Rahmenverordnungen und Durchführungsbestimmungen. Die Rahmenverordnungen spannen den gesetzlichen Rahmen auf und sind vorwiegend allgemein gehalten. Durchführungsbestimmungen konkretisieren die Rahmenbedingungen durch ausführliche Beschreibungen, wie die Rahmenverordnungen umzusetzen sind.

Im Vergleich zu internationalen und nationalen Gesetzen, haben sich europäische Verordnungen für das Projekt als ergiebige Quelle erwiesen. Internationale Gesetze sind zu allgemein formuliert, nationale Gesetze verweisen oftmals auf die europäische Gesetzgebung.

Die Domäne der Luftverkehrssicherheit ist einem stetigen Wandel unterworfen. Neuen Sicherheitstechnologien und neuartige Bedrohungen verlangen nach einer beständigen Anpassung der Gesetzeslage. Dies ist auch der Grund für die Vielzahl an EU-Verordnungen und die häufige Anzahl an Ersetzungen und Harmonisierungen von Verordnungen. Abbildung 3 zeigt die Verordnungen, welche im Rahmen des Projektes betrachtet wurden. Die äußersten, grünen Elemente repräsentieren die Projekt-relevanten und aktuell gültigen EU-Rahmengverordnungen zur Sicherheit in der zivilen Luftfahrt. In der Vertikalen sind die jeweiligen Ergänzungen zu sehen, d.h. das unterste Element entspricht der aktuellen Ergänzung zur Rahmenverordnung.

Im Projekt-Kontext sind vornehmlich die Anhänge der Verordnungen relevant, da diese die konkreten Umsetzungsinformationen enthalten. Im Anhang der Verordnung (EU) 185/2010 sind beispielsweise Gegenstände aufgelistet, welche als verbotene Gegenstände gelten und deren Einbringung in den Flughafen zu verhindern ist. Auch werden konkrete Angaben gemacht, welche Sicherheitsmechanismen (Röntgengeräte, Sprengstoffdetektoren, etc.) angewendet werden dürfen, um Passagiere, Handgepäck und Reisegepäck zu kontrollieren.

Auszug Verordnung (EU) 185/2010, Anhang, 4.1.1 Kontrolle von Fluggästen:

4.1.1. Kontrolle von Fluggästen

4.1.1.1. Mäntel und Jacken der Fluggäste sind vor der Kontrolle abzulegen und als Handgepäck zu kontrollieren.

4.1.1.2. Die Kontrolle der Fluggäste erfolgt mittels

a) einer Durchsuchung von Hand oder

b) Metalldetektorschleusen.

Kann die Kontrollperson nicht ermitteln, ob der Fluggast verbotene Gegenstände mit sich führt oder nicht, so ist dem Fluggast der Zugang zu Sicherheitsbereichen zu verwehren oder er ist bis zu einem für die Kontrollperson zufrieden stellenden Ergebnis erneut zu kontrollieren.

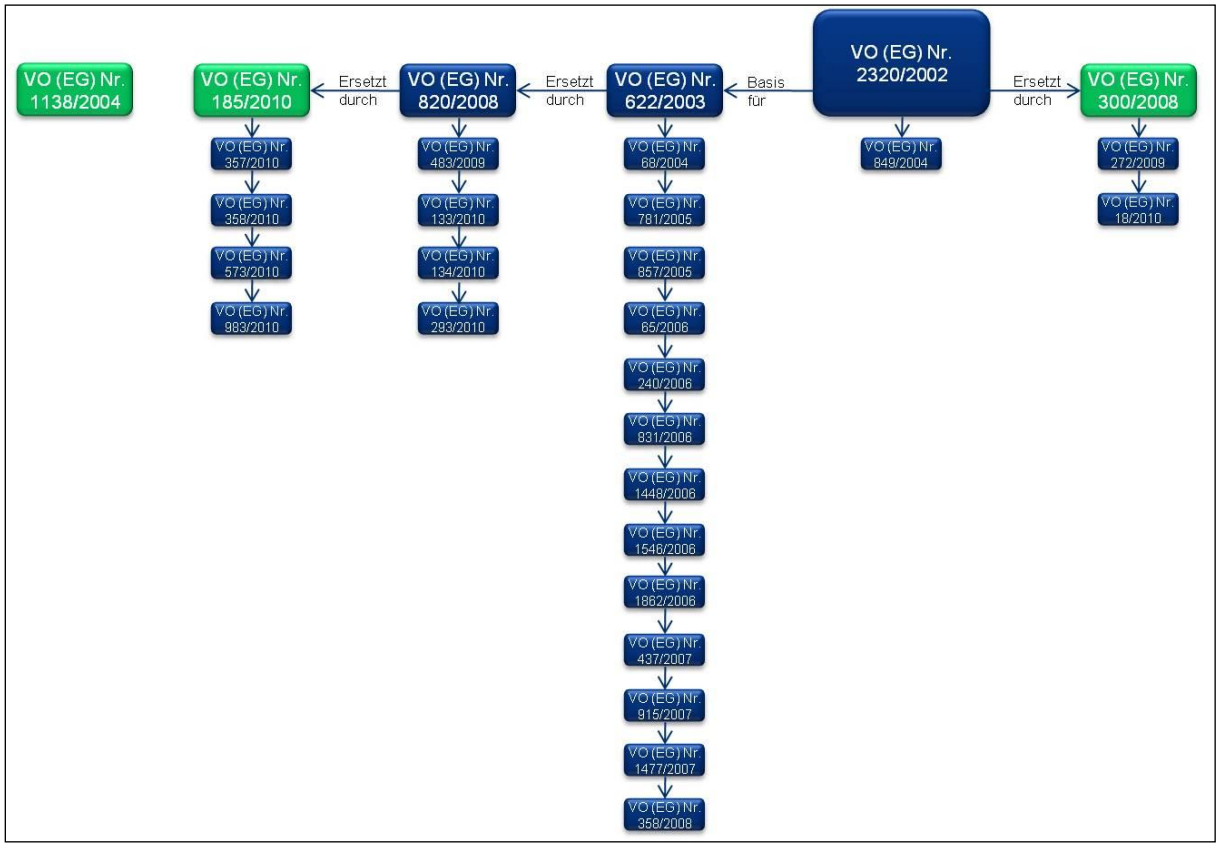


Abbildung 3: Übersicht der betrachteten EU-Verordnungen

Nationale Rahmenbedingungen

Grundelement der nationalen Gesetzgebung zur Sicherheit in der Zivilluftfahrt ist das Luftsicherheitsgesetzt (LuftSiG) und berücksichtigt die Vorschriften der europäischen Gesetzgebung (insbesondere die Verordnung (EU) 2320/2002 respektive deren Ergänzungen). Das Luftsicherheitsgesetz regelt die Kontrolle von Personen und Sachen im Flughafen bzw. auf dem Flugplatz (§ 5 LuftSiG), gibt vor, welche Personen auf ihre Zuverlässigkeit hin zu überprüfen sind (§ 7 LuftSiG) und schreibt vor, welche Sicherungsmaßnahmen die Flughafen- und Flugplatzbetreiber und die Fluggesellschaften zu ergreifen haben (§ 8 und § 9 LuftSiG). Konkrete Angaben, wie beispielsweise in den EU-Verordnungen sind im LuftSiG nicht zu finden.

Luftsicherheitsbehörden

Die gesetzgebenden Behörden zur Ausgestaltung der Sicherheit im zivilen Luftverkehr gliedern sich wie folgt:

Ebene	Behörde
International	ICAO (International Civil Aviation Organisation)
Europäisch	Europäische Union (EU)
National	Bundesministerium des Innern (BMI)
Länder	Bayerisches Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie (BayStMWIVT)

Tabelle 3: Übersicht Luftsicherheitsbehörden

In Deutschland übernimmt im Normalfall die Bundespolizei im Auftrag des BMI die §5-Aufgaben des LuftSiG (Passagier- und Gepäckkontrolle) war. Bayern und insbesondere der Flughafen München stelle hierbei eine Ausnahme dar. Die Verantwortlichkeit wird hierbei vom BMI an das BayStMWIVT weitergereicht, das wiederum die Regierung von Oberbayern (ROB) mit der Aufgabe betraut, welche die Aufgabe schlussendlich über das Luftamt Süd von der Firma SGM durchführen lässt.

Ein wesentlicher Fokus im Projekt SiVe liegt auf der Passagier- und Gepäckkontrolle, die durch den §5, LuftSiG geregelt ist. Um eine Analyse dieser Kontrolle durchzuführen, sind fundierte Kenntnisse darüber erforderlich. Da es sich hierbei meist um sicherheitsrelevante und sensible Daten handelt, ist die Freigabe dieser Informationen durch die verantwortlichen Behörde, d.h. BMI, notwendig. Das BMI ist kein Projektpartner und konnte auch nicht anderweitig zur Freigabe der Informationen bewegt werden, wodurch sich die Datenbeschaffung für die Analysen als sehr schwierig herausgestellt hat und schlussendlich die Datenlage als dünn zu bezeichnen ist.

Modellierung rechtlicher Rahmenbedingungen

Gesetze und Regularien spielen besonders in sicherheitskritischen Anwendungsdomänen eine wichtige Rolle, da sie den Handlungsrahmen, in dem sich die Akteure und die operativen Abläufe bewegen dürfen, vorgeben. Aus diesem Grund ist es notwendig bereits während der Entwicklung von Prozessen und operativen Abläufen die Regularien zu berücksichtigen und auch explizit zu dokumentieren. In Bezug auf die Prozessmodellierung war die Schlussfolgerung, dass die Regularien bereits in den Prozessmodellen explizit hinterlegt werden müssen. Dies hat den Vorteil, dass sofort ersichtlich ist, welche Gesetzmäßigkeiten gelten und erfüllt werden müssen. Auch ist es für den Betrachter der Prozessmodelle hilfreich, die entsprechenden Gesetzestexte direkt vorliegen zu haben und darin nachschlagen zu können.

Im Projekt wurden keine internationalen und nationalen Gesetze angewendet, da die europäischen Vorschriften wesentlich konkretere Angaben enthalten und somit einen wesentlich exakteren Handlungs- und Modellierungsrahmen vorgeben.

Da keine der betrachteten Prozessmodellierungswerkzeuge eine Darstellungsmöglichkeit für Regularien standardmäßig unterstützt, wurde die Erweiterbarkeit des Oryx Editors genutzt und eine entsprechende Funktionalität implementiert. Darüber hinaus wurde eine Schnittstelle zu

Erudine implementiert, die es erlaubt die in Oryx modellierten Regularien als Requirements in den Requirements Manager von Erudine zu importieren, um so nachverfolgen zu können, welche Regularien in den Prozessmodellen abgebildet wurden.

Oryx
Der Oryx Editor unterstützt zwei Arten von Erweiterungen, die über einen Plug-In-Mechanismus angebunden werden. Mit der ersten Art der Erweiterung können ausschließlich die verfügbaren Symbole der Prozessmodellierungsnotation ergänzt werden (*stencil set plug-in*), die zweite Erweiterung erlaubt die Ergänzung der Funktionalität des Editors (*functional plug-in*). Zur expliziten Darstellung von Regularien wurde die BPMN-Notation über das *stencil set-plug-in* um entsprechende Elemente erweitert. Hierzu werden drei verschiedene Elemente benötigt:

- Eine JSON-Datei (Java Script Object Notation), welche die Spezifikation des neuen Elements beinhaltet. Hierzu zählen insbesondere dessen Attribute und die Regeln, die angeben, an welche bestehenden Elemente das neue Symbol angeknüpft werden kann.
- Eine SVG-Datei (Scalable Vector Graphic), die eine Beschreibung der grafischen Darstellung des neuen Elements beinhaltet
- Eine PNG-Datei (Portable Network Graphics) als grafische Repräsentation in Form eines Icons.

Im Projekt wurden zwei neue BPMN-Elemente vom Typ *Artifact* eingeführt: *Regulation* und *Regulation Group* (siehe Abbildung 4). Das Element *Regulation* wird verwendet, wenn für einen Prozess oder einen Bestandteil eines Prozesses ein einziges Gesetz gilt und dieses bzw. Passagen daraus verknüpft werden sollen. Das Regulation *Element* besitzt fünf Attribute:

- LawName: Name des Gesetzes
- LawText: Gesetzestext
- Article: Nummer des relevanten Artikels
- Paragraph: Nummer des relevanten Paragraphen
- Organisation: Name der Organisation, welche die Einhaltung des Gesetzes sicherstellen muss.

Das Element *Regulation Group* wird angewendet, wenn mehr als ein Gesetz mit einem Prozess oder Prozessbestandteil verknüpft werden soll, wie z.B. europäische und nationale Gesetzesstellen. Das Element weist demnach nur die drei Attribute *LawNames*, *LawTexts* und *Organisations* auf.

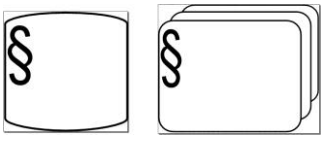


Abbildung 4: BPMN-Erweiterung Regulation und Regulation Group

In Abbildung 5 ist zu sehen, wie das Element *Regulation Group* zur expliziten Dokumentation von Prozess-Schritten in Oryx verwendet wird. Auf der linken Seite des Editors im *Shape Repository* sind die neuen BPMN-Elemente zur Platzierung in der Zeichenfläche verfügbar. Im mittleren Bildbereich, der Zeichenfläche, ist ein Prozessausschnitt zu sehen. Die *Regulation*

Group ist mit den vier sichtbaren Prozess-Schritten verknüpft, d.h. für alle Prozess-Schritte gelten die Gesetze, die in der *Regulation Group* hinterlegt sind. Im rechten Bildbereich sind die Attribute der *Regulation Group* zu sehen.

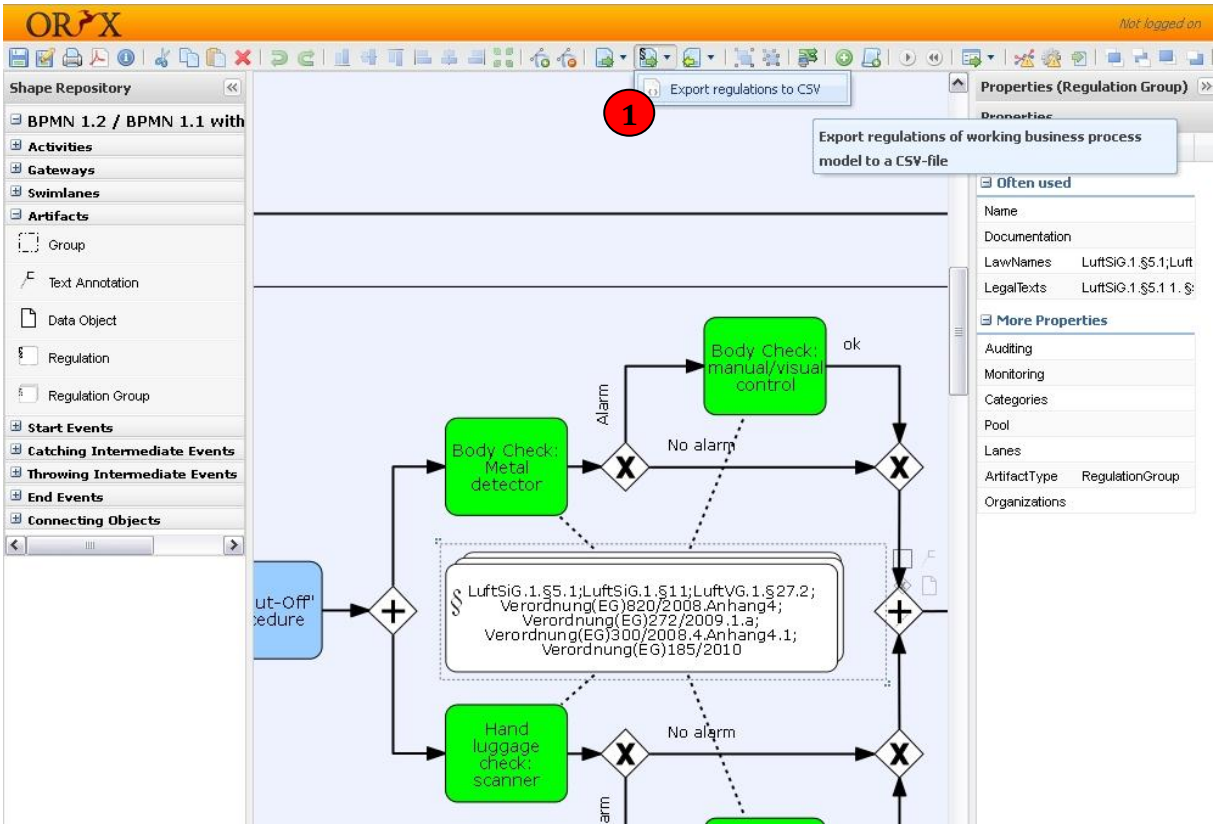


Abbildung 5: Verwendung des Elements Regulation Group in Oryx

Das zweite Plug-In-In, das für Oryx implementiert wurde ist vom Typ *functional plug-in*. Es dient dazu, die Gesetze bzw. *Regulation*- und *Regulation Group-Elemente* eines Prozessmodells in eine CSV-Datei (Comma separated values) zu exportieren. Die CSV-Dateien können dann in den Requirements Manager von Erudine importiert werden, so dass damit nachvollzogen werden kann, welche Gesetze bereits im Prozessmodell abgedeckt wurden und welche nicht. Diese Art der Erweiterung verlangt nach zwei Schritten: zunächst erfolgt die Erstellung einer JavaScript-Datei, welche die eigentliche Funktionalität der Erweiterung abbildet. Anschließend wird in der Oryx-Konfigurationsdatei das neu entwickelte Plug-in eingetragen und somit registriert. Über die Menüleiste kann dann auf die neue Export-Funktion zugegriffen werden und die Gesetze des Prozessmodells exportiert werden (siehe Abbildung 5, Punkt 1).

Erudine

Trotz der Entscheidung, Erudine nicht als Modellierungswerkzeug für Prozesse im Projekt zu verwenden, kann der in Erudine integrierte Requirements Manager zur Verwaltung und zur Nachverfolgung von Requirements verwendet werden. Als Requirements gelten Gesetze, die von einem zu modellierenden Prozess eingehalten werden müssen. Nach dem Export via Oryx können die Gesetze importiert werden und stehen dann im Requirements Manager mitsamt der ausgefüllten Attribute zur Verfügung (siehe Abbildung 6).

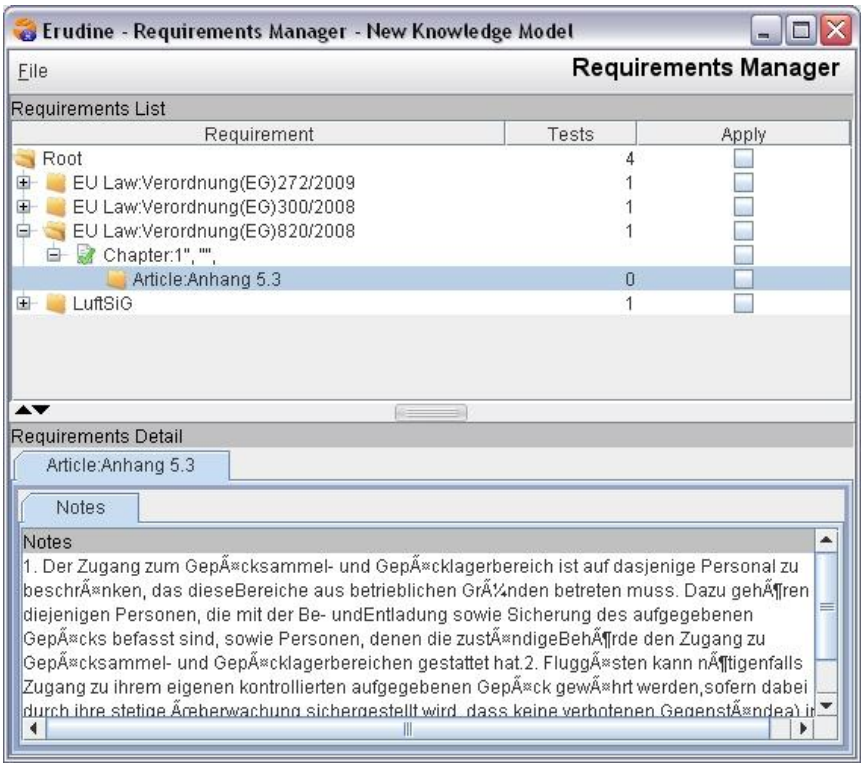


Abbildung 6: Erudine Requirements Manager mit importierten Gesetzen

Details zur Implementierung der Erweiterungen sind in Babau 2011 zu finden.

Prozessmodellierung in SiVe

Vorgehen

Zur Modellierung der operativen und sicherheitsrelevanten Kernprozesse am Flughafen München wurde folgendes Vorgehen gewählt:

(1) Erfassung
- Recherche der operativen Abläufe an Flughäfen
- Erfassung der relevanten internationalen, europäischen und nationalen Gesetze
- Durchführung von Interviews am Flughafen München und Frankfurt

(2) Modellierung der erfassten Abläufe mit BPMN

(3) Abgleich der Prozessmodelle mit dem Flughafen München und Frankfurt und ggf. Anpassung mit erneutem Abgleich (iteratives Vorgehen)

Interviews

Interviews wurden im Projekt mit dem Ziel der Informationsbeschaffung und zur Validierung durchgeführt. Insbesondere in der Anfangsphase des Projektes erfolgten viele Workshops am Flughafen München, um eine breite Wissensgrundlage über das System Flughafen und die damit verbundenen Prozesse aufzubauen.

Während und nach der Modellierungsphase erfolgte im Rahmen von Interviews eine enge Abstimmung mit dem Flughafen München und dem Fraunhofer-Institut für Materialfluss und Logistik am Flughafen Frankfurt zur Sicherstellung der Korrektheit der Prozessmodelle.

Am Flughafen München erfolgte ein Abgleich der Prozessmodelle mit den Abteilungen:

- Operativer Sicherheitsdienst (Hr. Bauer)
- Prozessmanagement (Fr. Reiser)
- Qualitätsmanagement (Fr. Sitter, Hr. Haufe)
- Flughafenfeuerwehr (Hr. Leiwering, Hr. Hecker)
- Sicherheitsmanagement (Fr. Drohm)
- Gepäckabfertigung (Hr. Marx)

Die Prozessmodelle wurden abschließend von den Abteilungen des Flughafens München akzeptiert und können somit als valide betrachtet werden.

Im Rahmen der Abstimmung mit dem Flughafen München wurden die von CASSIDIAN angefertigten Prozessmodelle in das Qualitätsmanagement-System des Flughafen eingepflegt, da bis zu diesem Zeitpunkt keine Prozessmodelle in grafischer Form am Flughafen vorlagen.

Modellierungskonventionen

Durch die zentrale Rolle der Prozessmodellierung im Projekt SiVe ist es notwendig die Schnittstellen zu den Projektpartnern detailliert zu definieren und zu beschreiben. Die Prozessmodellierung bildet die Basis für die logistische und stochastische Simulation (vgl. Abbildung 1). Um eine Weiterverarbeitung der Prozessmodelle in der logistischen und stochastischen Simulation zu garantieren, wurden Modellierungskonventionen festgelegt. In Abstimmung mit den betroffenen Projektpartnern sind Vorgaben und Regeln festgehalten, welche erlaubte und verbotene Modellierungspraktiken beschreiben. Hierzu zählt beispielsweise die Vorgabe einer Modellierungshierarchie, dessen unterschiedliche Ebenen jeweils einen spezifischen Detaillierungsgrad der Prozessmodelle definieren. Dadurch wird eine Verringerung der Komplexität erreicht. Modelle auf der obersten Hierarchieebene sind abstrakt und geben einen schnellen Überblick, wohingegen die Prozessmodelle auf der untersten Ebene einen detaillierten Einblick in die auszuführenden Prozess-Schritte der beteiligten Akteure geben. Die Konventionen sind im Anhang zu finden.

Die SiVe Prozesslandkarte

Die Gesamtheit der Prozessmodelle wird im Projekt als Prozesslandkarte bezeichnet. Alle erstellten Prozessmodelle sind im Anhang, im Projektordner und in der Oryx-Datenbank zu finden.

Wie in den Modellierungskonventionen festgelegt, werden die Prozessmodelle nach unterschiedlichen Detailierungsebenen gegliedert. Folgende hierarchische Struktur gilt:

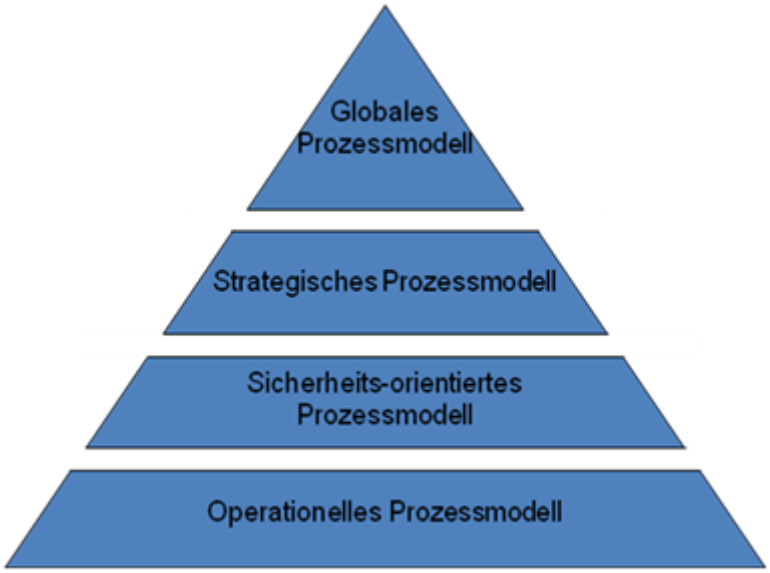


Abbildung 7: Prozesshierarchie

Das globale Prozessmodell zeigt die betrachteten operativen Kernprozesse. Diese sind die Gepäck-, Passagier- und Frachtabfertigung.

Im strategischen Prozessmodell ist jeder einzelne Kernprozess übersichtlich in seinen elementaren Prozess-Schritten abgebildet.

Das sicherheits-orientierte Prozessmodell erweitert das strategische Prozessmodell um sicherheits-relevante Prozess-Schritte. Ziel hierbei ist es eine Übersicht über die sicherheits-kritischen Prozess-Elemente im Kernprozess zu geben.

Im operativen Sicherheitsmodell sind die Prozesse in der höchsten Detailierungsstufe beschrieben. Durch die Prozessbeschreibung sollen die ausführenden Akteure eine Orientierungshilfe für ihre tägliche Arbeit erhalten und ein klares Verständnis entwickeln können, wie sie zu arbeiten haben.

Die entsprechenden Modellierungsebene wird im Dateinamen eines Prozessmodells angegeben: L01 entspricht dem globalen, L02 dem strategischen, L03 dem sicherheits-orientierten und L04 dem operationellen Prozessmodell.

Integration

Das Ziel der Integration ist die Vereinigung der unterschiedlichen Modellierungsansätze unter einer grafischen Benutzeroberfläche mit dem SiVe-Demonstrator als Endergebnis. Die Leitung bei der technischen Umsetzung liegt bei der ckc AG. Als Grundgerüst für die Benutzeroberfläche dient das Eclipse-Framework, in das die unterschiedlichen Anwendungen der Modellierungsparteien integriert werden, um eine durchgängige Tool-Kette zu erhalten. Die unterschiedlichen Module bzw. Werkzeuge des SiVe-Demonstrators sind:

- Der Szenario-Builder zur Generierung von Bedrohungsszenarien
- Oryx als Editor zur Prozessmodellierung
- AnyLogic zur Agenten-basierten Modellierung und Simulation
- jPass! von jCOM1 zur stochastischen Modellierung und Simulation
- eine Java-basierte benutzerspezifische grafische Oberfläche zur ökonomischen Bewertung

Da es sich bei den unterschiedlichen Software-Werkzeugen meist um COTS2-Produkte handelt oder die Import/Export-Funktionalität eine direkte Anknüpfung der verschiedenen Werkzeuge nicht erlaubt, ist eine Eigenimplementierung der Schnittstellen notwendig. CASSDIDIAN hat die Verantwortung für die Schnittstelle zum Szenario-Builder und unterstützte bei der Umsetzung der Schnittstellen zur Agenten-basierten und stochastischen Modellierung.

Schnittstelle zwischen Szenario-Beschreibung und Prozessmodellierung
Mit Hilfe des Szenario-Builders wird eine konkrete Bedrohung für den Flughafen beschrieben. Aufgabe der Schnittstelle zwischen Szenario-Builder und Oryx ist es, basierend auf der definierten Bedrohung, automatisch den betroffenen Teil des Flughafens, also die betroffenen Flughafenprozesse, zu bestimmen. Die Implementierung Schnittstelle liegt bei CASSIDIAN und wird über eine Konfigurations-Datei realisiert, in der den Schutzmechanismen des Szenario-Builders entsprechende Prozessmodelle in Oryx zugewiesen sind. Änderungen der Schutzmechanismen im Szenario-Builder oder der Prozessmodelle in Oryx bedingen eine manuelle Anpassung der Konfigurations-Datei.

Untenstehende Grafik zeigt auf der linken Bildhälfte die Szenario-Datei des Szenario-Builders, in der Mitte die Konfigurations-Datei und am rechten Bildrand symbolisch die Prozessmodelle in Oryx.

Beispiel:

In der Szenario-Datei sind die zu durchlaufenden Schutzaktivitäten aufgelistet („zu durchlaufen“ → „Schutzaktivitäten“), wie beispielsweise die „Personen-Körper-Kontrolle“. Die Personen-Körper-Kontrolle ist Bestandteil eines Prozesses am Flughafen, der in einem oder mehreren Prozessmodellen in Oryx abgebildet ist. Über die Konfigurations-Datei werden nun die Oryx-Modelle den zu durchlaufenden Schutzaktivitäten zugewiesen. Konkret werden der „Personen-Körper-Kontrolle“ die Prozessmodelle „Passenger Handling (L02)“, „Passenger Handling (L03)“ und „Security Check Point – Body Check (Passenger Handling – L04)“ zugeordnet.

[22] Commercial Of The Shelf

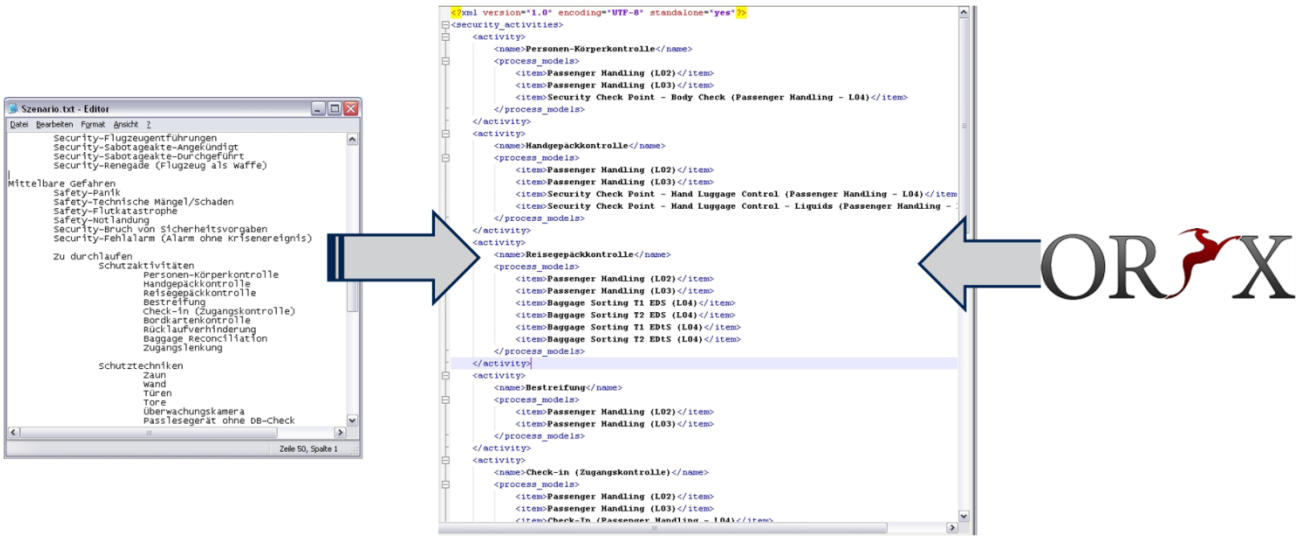


Abbildung 8: Schnittstelle Szenario-Builder - Oryx

Schnittstelle zur Agenten-basierte Modellierung

Die Schnittstelle zwischen der Prozessmodellierung mittels Oryx und der Agenten-basierten Modellierung mittels AnyLogic wird vom Fraunhofer ALI implementiert. Einzige Anforderung an die Prozessmodelle von CASSIDIAN ist, dass diese den Modellierungskonventionen genügen, um über den vom Fraunhofer ALI entwickelten BPMN-Parser direkt in AnyLogic eingelesen werden zu können.

Schnittstelle zur stochastische Modellierung

Die Schnittstelle zwischen Prozessmodellierung und stochastischer Modellierung wird identisch zur Schnittstelle zur Agenten-basierten Modellierung über die Modellierungskonventionen implementiert. Die Verantwortlichkeit der Implementierung liegt bei der ckc AG.

Business Cases

Die Business Cases stellen dar, wer SiVe für welche Zielsetzung wie einsetzen kann. Im Sinne des Verwertungsplans explizieren die Business Cases damit die praktische Anwendung. Aufgrund der oben beschriebenen Facharchitektur werden zwei Business Cases detailliert dargestellt, die die im Projekt-Gesamtantrag beschriebenen Anwendungsfälle konkretisieren (siehe SiVe-Gesamtvorhabenbeschreibung vom 09.05.2008, Abschnitt 1.1, Seiten 3-4). Die Business Cases sind in verschiedene Schritte untergliedert.

Business Case 1: geänderter Bedrohungslage

Schritt 1 repräsentiert den relevanten Input für die Anwendung des Business Cases. Die Schritte 5 und 6 beziehen sich auf die Ergebnisse und beinhalten den Nutzen für den Anwender des Business Cases. Die Eingangsinformation für die Anwendung dieses Business Cases ist die erstmalige Anwendung (oder Befürchtung der Anwendung) eines Bedrohungsaspekts. Ein Beispiel hierfür wäre das im Jahr 2009 erstmals zur Anwendung gekommene Einschleusen eines Sprengsatzes im Körper eines Attentäters („In-body-Sprengsatz"). Neue Bedrohungsaspekte haben in der Vergangenheit oft zu „rule-based" Entscheidungen geführt (oft durch regulatorische Bestimmungen direkt implementiert), ohne dass die Folgen an Restrisiken, Kosten und Systemwirksamkeit für Flughafenbetreiber, Fluggäste, Systemhersteller usw. bewertet wurden. SiVe bietet hier eine deutliche Verbesserung basierend auf dem im Folgenden beschriebenen Vorgehen: Mittels des Szenariobuilders kann eine Aussage darüber getroffen werden, welche Szenarien durch den neuartigen Bedrohungsaspekt betroffen sind (Schritt 2). Aus diesen Szenarien kann direkt ermittelt werden, welche Prozessketten der Flughafensicherheit betroffen sind (Schritt 3). Diese Prozessketten können unter Berücksichtigung des neuen Bedrohungsaspekts bewertet werden, d. h. dass das von dem Aspekt ausgehende Risiko quantifiziert werden kann (Schritt 4). Erst basierend auf dieser Risikoquantifizierung können valide Aussagen zu tragbaren Risiken erfolgen (Schritt 5). Sind bestimmte Risiken (unter der Berücksichtigung des neuen Bedrohungsaspekts) nicht tragbar, so kann durch SiVe ermittelt werden, an welchen Prozessketten der Flughafensicherheit Verbesserungen vorzunehmen sind (Schritt 6). Da sämtliche betroffenen Prozessketten vorliegen, können mögliche zusätzliche Sicherheitsmaßnahmen folglich dahingehend bewertet werden, ob sie mit den existierenden Prozessen kompatibel sind.

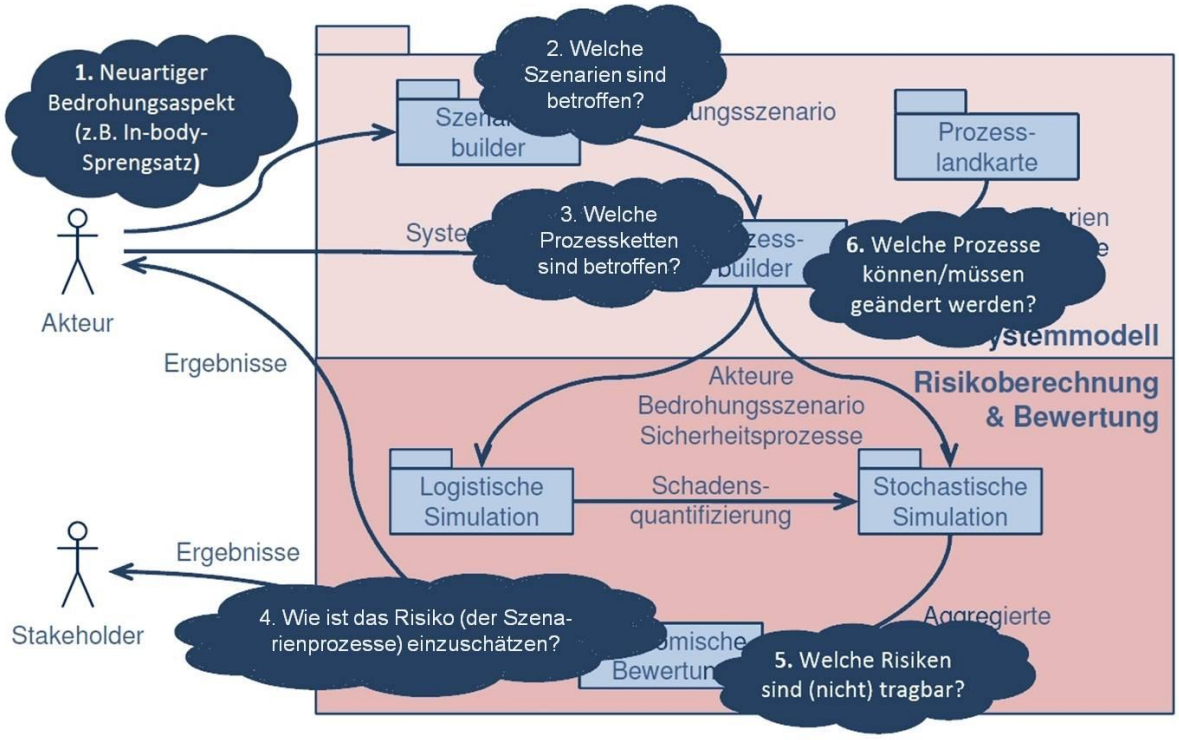


Abbildung 9: Business-Case 1: geänderte Bedrohungslage

Für diesen Business Case werden im Folgenden die Anwendungsfelder kurz beschrieben.

Bedrohungsszenarien

Strukturell konsistente und damit plausible Bedrohungsszenarien werden mit dem Szenariobuilder erstellt, indem alle relevanten Bestandteile (die Systemelemente der Bedrohung) systematisch berücksichtigt werden. Das Szenario bestimmt dabei auch, welche Sicherheitsprozesse am Flughafen im relevanten Szenario durchgeführt werden und damit eine mögliche Gefahr verhindern könnten. Diese jeweils relevanten präventiven Sicherheitsprozesse werden automatisch bei der Szenario-Erstellung ermittelt. Strukturelle Schwachstellen im Sicherheitssystem lassen sich so in Bezug auf relevante Szenarien erkennen. Durch die Quantifizierung von Kosten und Risiken können die Bedrohungsszenarien bewertet werden.

Analyse und Objektivierung

Die Modellierung ausgewählter Bedrohungsszenarien dient als Ausgangsbasis für die Analyse und Bewertung bestehender Sicherheitssysteme hinsichtlich ihrer Kosten und der erreichten Risikoreduktion für bestimmte Bedrohungen. Die Leistungsfähigkeit vorgegebener Sicherheitsstandards (z. B. EU-Normen für das Sicherheitsmanagement von Flughäfen und Verkehrsinfrastrukturen) kann auf diese Weise quantitativ überprüft werden: Welche Bedrohungspotentiale werden von diesen Standards erfasst und im angestrebten Maße reduziert, welche sind unwirksam?

Neue Bedrohungsaspekte

Durch Modellierung und Simulation neuer oder zu erwartender Bedrohungen mit neuen, dagegen wirkenden Sicherheitstechnologien und -prozessen können verschiedene Reaktionen auf diese neuen Bedrohungen bewertet und effiziente Lösungen ausgewählt werden. Dies würde zu einer „leistungsorientierten“ (und nicht „ruled-based“) Anpassung der regulatorischen Bestimmungen führen.

Business-Case 2: Prozessoptimierung & Lobbyarbeit

Einen weiteren Business Case für SiVe stellt die Optimierung von (Sicherheits-)Prozessen dar. Ein Prozess beschreibt nicht nur die Abläufe, sondern auch den Informationsaustausch zwischen den Prozessbeteiligten, die eingesetzten Technologien und Regularien usw. Prozessänderungen oder -optimierungen sind kritische Vorgänge, da sie Auswirkung auf Risiken und Kosten zu verhindernder Bedrohungsszenarien haben können. Bestehende Prozesse werden typischerweise geändert oder optimiert, wenn Kosten reduziert werden müssen, wenn Dienstleistungen verbessert werden sollen, wenn neue Technologien eingesetzt werden oder aufgrund neuer regulatorischen Bestimmungen.

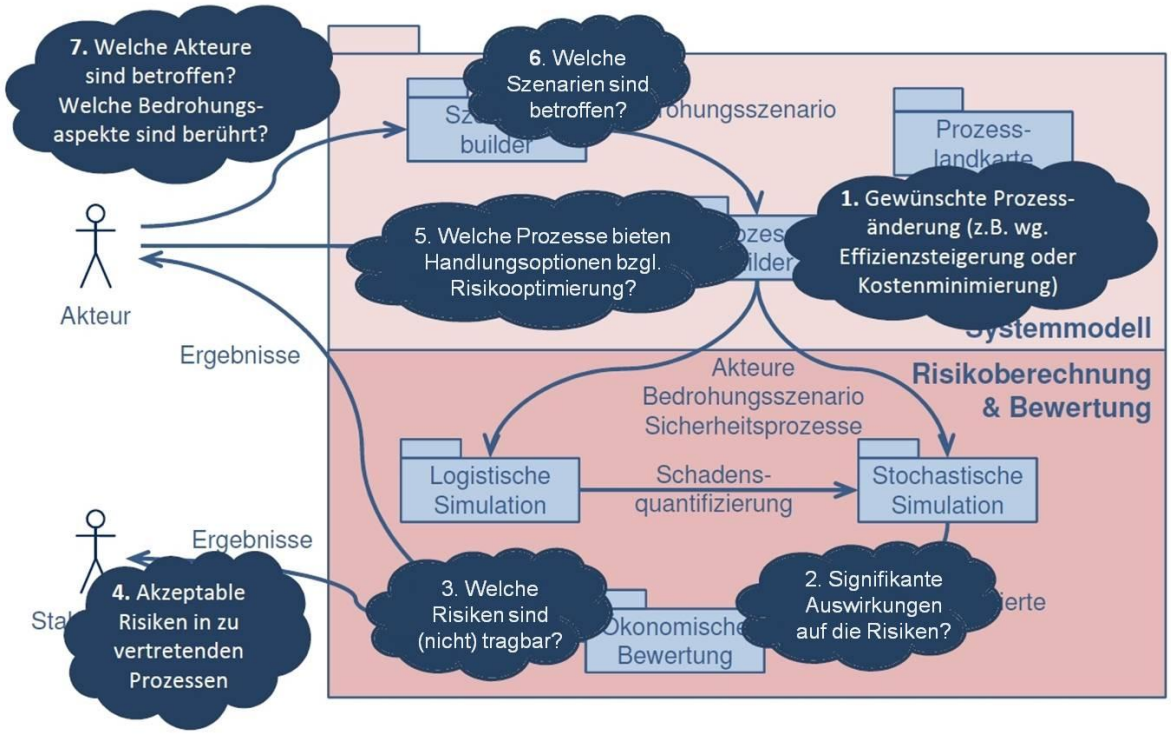


Abbildung 10: Business-Case 2: Prozessoptimierung und Lobbyarbeit

Eingangsgröße des Business Cases ist eine gewünschte Prozessänderung (z. B. aufgrund erwarteter Effizienzsteigerungen oder Kostenminimierung) (Schritt 1). Auf Basis dieser Prozessänderung kann mit SiVe eine ökonomische (Neu-)Bewertung des entsprechenden Prozesses erfolgen und damit die signifikanten Auswirkungen bzgl. der Risiken erfolgen (Schritt 2). In Schritt 3 kann nun eine begründete Aussage über tragbare bzw. nicht tragbare Risiken erfolgen. Stakeholder wissen damit um die quantifizierten, akzeptierten Risiken in den von ihnen zu vertretenden Prozessen (Schritt 4). Für den Fall, dass die (durch die Prozessänderung hervorgerufenen) Risiken für Stakeholder inakzeptabel sind, kann mittels der SiVe-Verknüpfungen identifiziert werden, welche Sicherheitsprozesse mögliche Handlungsoptionen zur Risikooptimierung darstellen (Schritt 5). Für diese Prozesse kann dann ermittelt werden, bei welchen Bedrohungsszenarien sie Anwendung finden (Schritt 6) und schließlich welche Akteure in die Vermeidung dieser Bedrohungsszenarien eingebunden sind (Schritt 7).

Für diesen Business Case werden im Folgenden die Anwendungsfelder kurz beschrieben.

Auslegung von Sicherheitssystemen

SiVe soll den Entwurf und die Konfiguration kostengünstigerer und leistungsfähigerer Sicherheitssysteme unterstützen. Die angestrebte Optimierung der Effizienz von Sicherheitssystemen soll zu verbesserten Bedingungen für Passagiere, Personal (Betrieb der Infrastrukturen, z. B. Flughafenpersonal, und Behörden) und Logistik führen. Damit können unnötige Belastungen für Flughafenbetreiber, Passagiere und andere Beteiligte vermieden oder zumindest hinterfragt werden (Prozessoptimierung, Unterstützung von Deregulierungsaktivitäten, Lobbyarbeit, leistungsorientierte Umsetzung von regulatorischen Bestimmungen).

Schwachstellenanalyse

Schwachstellenanalysen sollen strukturelle Lücken im Sicherheitssystem aufdecken. Dies dient wiederum als Basis für den Vorschlag neuer Schutzmechanismen, die das größte Potenzial aufweisen, diese Lücken zu einem akzeptablen Mehraufwand (Kosten für Flughafen und Belastung für die Passagiere) zu schließen. Beispielsweise können durch Simulation von Verhaltensfehlern der am Prozess beteiligten Akteure die Auswirkungen von Schulungen (mit der Folge einer geringeren Fehlerwahrscheinlichkeit) oder umgekehrt des Einsatzes von Hilfskräften hinsichtlich Kosten und Restrisikoänderung bewertet und so der Personaleinsatz optimiert werden.

Typische Fragestellungen der Schwachstellenanalyse zur Identifikation von Lücken im Sicherheitssystem sind:

- Gegen welche Bedrohungsszenarien wirken nur wenige präventive Schutzmechanismen?
- Welche Bestandteile von Bedrohungsszenarien werden (über alle Bedrohungsszenarien hinweg) wie häufig durch präventive Schutzmechanismen adressiert?
- Gegen wie viele Bedrohungsszenarien wirkt jeder Schutzmechanismus?
- Welche präventiven Schutzmechanismen wirken besonders häufig in Kombination gegen Bedrohungsszenarien?

Durch eine Schwachstellenanalyse der zu betrachtenden kritischen Infrastruktur können – aus rein struktureller Sicht – gefährliche Bedrohungsszenarien identifiziert werden. Solche Szenarien beinhalten Konstellationen von Bedrohungsaspekten, gegen die keine bzw. nur wenige Schutzmechanismen wirken. Es ist explizit zu beachten, dass die Strukturanalyse – wie schon oben angemerkt – nur die strukturellen Zusammenhängen zwischen den Bedrohungsaspekten und den betroffenen Schutzmechanismen liefert. Erst eine Risikoquantifizierung kann Aussagen über die Performance der betroffenen Schutzmechanismen und Prozesse liefern.

Außerdem kann mittels der Schwachstellenanalyse identifiziert werden, welche Bedrohungsaspekte Bedeutung für eine Vielzahl von Szenarien haben. Mittels geeigneter Sicherheitsmaßnahmen gegen genau diese Bedrohungsaspekte kann damit eine Vielzahl an Szenarien vermieden werden. Schließlich kann die Schwachstellenanalyse auch noch Aussagen darüber treffen, welche Schutzmechanismen wie häufig gegen Bedrohungsszenarien wirken. Einerseits können damit besonders wirksame bzw. wirkungsarme Schutzmechanismen herausgefiltert werden. Andererseits liefert der Vergleich verschiedener Schutzmechanismen eine Aussage darüber, ob diese redundant oder komplementär bei Bedrohungsszenarien zum Einsatz kommen.

Entwicklungssteuerung

Durch die Simulation neuer (bildverarbeitungsbasierter) Technologien oder veränderter Ausprägungen von Sicherheitssystemen soll eine gezielte Steuerung von Forschung und Entwicklung ermöglicht werden und so marktfähige Produkte wahrscheinlicher machen. So kann der Nutzen von bestimmten angenommenen Verbesserungen der Erfassungsleistung, zum Beispiel eine reduzierte Falschalarmrate, mit den geschätzten Entwicklungskosten verglichen werden. Eine strukturell detaillierte Schwachstellenanalyse wird im SiVe-Projekt von BHL durchgeführt.

Akteure und Stakeholder

Nachfolgende Liste zeigt die oben beschriebenen Business Cases zusammen mit den relevanten Akteuren und Stakeholdern.

Nr.	SiVe Business-Case	Akteure	Stakeholder
0	Systematische Konstruktion und Auswertung von Bedrohungsszenarien	• BKA • BPol • FMG (Sicherheitsdienste)	• BKA • BPol • FMG • Gesetzgeber • BMI
0	Analyse und Objektivierung von Bedrohungen, Sicherheitssystemen und Restrisiken	• FMG • Behörden	• Behörden
0	Reaktion auf neue Bedrohungsszenarien	• BKA • BPol	• BKA • BPol • FMG (Sicherheitsdienste)
0	Werkzeug zur optimierten Auslegung von Sicherheitssystemen	• FMG • Sicherheitsdienste • Hersteller von Sicherheitssystemen	• FMG • Hersteller von Sicherheitssystemen
0	Schwachstellenanalyse	• BKA • BPol	• BKA • BPol • FMG • Behörden
0	Entwicklungssteuerung von (bildverarbeitungsbasierten) Sicherheitssystemen	• Hersteller von Sicherheitssystemen • FMG	• Hersteller von Sicherheitssystemen • FMG

Tabelle 4: SiVe-Akteure und Stakeholder

Aus den Business-Cases können sich folgende Fragestellungen ergeben, die mit Hilfe der SiVe-Ergebnisse beantwortet werden sollen.

Akteur	Mögliche Fragestellungen bzw. Ziele
Flughäfen / Betreiber (FMG)	- Welche Prozesse waren bei Risikoereignissen bereits unwirksam und welche regulatorischen Randbedingungen sind davon betroffen? - Kostenoptimierung bei unveränderten Restrisiken - Ermittlung von Restrisiken und Sicherheitsperformance beim Einsatz (neuer) Technologien

Akteur	Mögliche Fragestellungen bzw. Ziele
	- Bewertung (Kosten, Nutzen, Akzeptanz, usw.) eigesetzter oder geplanter Technologien - Prozessoptimierung durch systematische Schwachstellenanalyse - Auswirkung regulatorischer Bestimmungen auf Sicherheitsperformance, Kosten und Restrisiken
Hersteller von Sicherheitstechnologien	- Ermittlung von Restrisiken und Sicherheitsperformance beim Einsatz von (etablierten/neuen) Technologien - Definition neuer bzw. optimierter Prozessabläufe basierend auf dem Einsatz neuer Technologien
Behörden	- Wie wirken die bestehenden/vorhanden Schutzmechanismen bei neu aufkommenden Bedrohungen und wo sind die Schwachstellen hierbei? - Auswirkung von regulatorischen Bestimmungen auf Sicherheitsperformance, Kosten und Restrisiken
Sicherheitsgesellschaften an Flughäfen	- Prozessoptimierung (Kostenreduktion, Prozesseffizienz, Risikoreduktion) - Folgen bei Austausch/Einführung neuer Technologien im Sinne von Sicherheitsperformance, Kosten und Restrisiken - Folgen auf Prozessabläufen bei Änderung / Einführung von (neuen) regulatorischen Bestimmungen
Flughafenfeuerwehr, Feuerwehren Umkreis, Technisches Hilfswerk THW(ggf. Bundeswehr)	- Optimierung von Prozessen und Informationsaustausch im Krisenfall
Sicherheitsbehörden	- Prozessoptimierung im Sinne einer Risikoreduktion - Folgen bei Austausch/Einführung neuer Technologien im Sinne von Sicherheitsperformance, Kosten und Restrisiken
Bundespolizei, Landespolizei	- Prozessoptimierung im Sinne einer Risikoreduktion - Folgen neuer Bedrohungsszenarien im Sinne von Sicherheitsperformance, Kosten und Restrisiken
BKA, LKA	- Folgen neuer Bedrohungsszenarien im Sinne von Sicherheitsperformance, Kosten und Restrisiken und Schadenausmaß
BBK	- Optimierung von Prozessen und Informationsaustauschen im Krisenfall

Tabelle 5: Akteure und Stakeholder, sowie deren mögliche Fragestellungen

Krisen- und Notfallmanagement

Im SiVe-Projektantrag wurde festgelegt, dass neben den präventiven Schutzmaßnahmen auch reaktive Mechanismen des Krisen- und Notfallmanagements betrachtet werden. CASSIDIAN widmete sich diesem Thema mit partieller Unterstützung von Bauhaus Luftfahrt. Ziel der Betrachtung ist die Erfassung und detaillierte Beschreibung von operativen Abläufen und Prozessen in Notfall- und Krisensituationen an Flughäfen, um diese in Simulationsmodelle zur eingehenden Analyse überführen.

Vorgehen

Zur Annäherung an das Thema hat CASSIDIAN ein Vorgehenskonzept erstellt, um das Thema strukturiert aufzuarbeiten. Im Anschluss wurde ähnlich wie im präventiven Fall eine Strukturanalyse durchgeführt, dessen Ziel die Identifikation der wichtigsten Elemente und Stakeholder im Krisenfall war. Hierzu wurde zunächst eine Mindmap erstellt, die dann in eine Meta-Matrix überführt wurde, um die einzelnen Elemente miteinander in Beziehung zu setzen und die Abhängigkeiten zu veranschaulichen. Anschließend erfolgte eine Verfeinerung der Meta-Matrix, indem die einzelnen Elemente weiter beschrieben und untergliedert wurden.

						Rahmenbedingungen			Schutzmechanismen				
	Akteure	Kommunikationsmittel	Alarmkategorien	Technische Einsatzmittel	Nicht-Technische Fähigkeiten	Notfallplan	Rechtliche Grundlagen	Infrastruktur	Schadensbegrenzung	Schadensbewältigung	Gefahren	Interessen der Akteure	Faktor Mensch
Akteure		verwenden		verwenden	haben		halten ein / definieren		führen durch	führen durch		haben	bestimmt
Kommunikationsmittel									Wirken auf	Wirken auf			
Alarmkategorien						definieren / bestimmen			definieren / bestimmen	definieren / bestimmen		wirken auf	
Technische Einsatzmittel					bedingen				wirken auf	wirken auf	wirken gegen		
Nicht-Technische Fähigkeiten		erfordern		erfordern					wirken auf	wirken auf	wirken gegen		
Rahmenbedingungen Notfallplan				definieren / erfordern	definieren / erfordern				bestimmen	bestimmen		wirken auf	
Rahmenbedingungen Rechtliche Grundlagen	Beeinlußt / betrifft						Beeinlußt / betrifft	Beeinflußt / definiert				Beeinlußt / betrifft	
Rahmenbedingungen Infrastruktur						beeinflußt			wirkt auf	wirkt auf			
Schutzmechanismen Schadensbegrenzung	Betrifft			bedingen / definieren	bedingen / definieren			Erfordert	Erfordert			Wirken auf	
Schutzmechanismen Schadensbewältigung	Betrifft			bedingen / definieren	bedingen / definieren			Erfordert		Erfordert		Wirken auf	
Gefahren							beeinflußen		Erfordert	Erfordert	Kann führen zu	beeinflußen	
Interessen der Akteure							Beeinflußt					Beeinflußt	
Faktor Mensch					Gestaltet				Gestaltet	Gestaltet			beeinflußt

Abbildung 11: Meta-Matrix der Krisen- & Notfallanalyse

Eine wesentliche Informationsquelle stellt der Notfallplan des Flughafens München dar, der in Bezug auf die operativen Prozesse konkrete Informationen enthält. Eine Auswertung des Notfallplans ist in den Zwischenberichten zu finden. Um das Gesamtbild hinsichtlich der operativen Abläufe der Maßnahmenträger zu vervollständigen, wurden mehrere Interviews mit den Verantwortlichen durchgeführt. Die Entwicklung der Fragebögen und Interviewvorbereitungen erfolgte teilweise mit Unterstützung von Bauhaus Luftfahrt.

Interviews

Mit folgenden Maßnahmenträgern wurden Interviews durchgeführt:

- Flughafenfeuerwehr München (30.06.2010)
- Krisen-/ Notfallmanagement Fraport (16.11.2010, 02.12.2010)
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (18.11.2010)

Ergebnisse

Eine wesentliche Erkenntnis der Interviews ist, dass eine detaillierte Erfassung operativer Abläufe zur weiteren Abbildung in Simulationsmodellen nicht zielführend ist. Die operativen Abläufe sind zu einem solch hohen Grad situationsabhängig und vielfältig, dass entweder eine enorm große Menge an Simulationsmodellen erstellt werden müsste, um zumindest einen Bruchteil möglicher Krisen- und Notfallsituationen abzubilden, oder die Modelle müssten dermaßen abstrahiert und generalisiert werden, dass schlussendlich nur allgemeine Aussagen ohne nennenswerten Mehrwert erzeugt werden.

Die Betrachtung strategischer Abläufe hingegen ist aus Endanwender- bzw. Maßnahmenträgersicht durchaus sinnvoll. Im Fokus dieser Betrachtung stehen vielmehr Kommunikationsflüsse und Verantwortlichkeiten der Maßnahmenträger mit detaillierter Analyse der jeweiligen Schnittstellen.

Bei der Analyse des Notfallplans des Flughafens München wird deutlich, dass besonders die Verantwortlichkeiten der Maßnahmenträger nicht immer eindeutig geregelt sind und es Überschneidungen gibt.

II.1.3. *PROOF OF CONCEPT*

Einordnung des Projektes „SiVe“ und Abgrenzung des Arbeitspakets „Systemarchitektur und –Integration“

Themenschwerpunkt von SiVe („Verbesserung der **Si**cherheit von **Ve**rkehrsinfrastrukturen“) ist die systematische Analyse, Modellierung, Simulation, Berechnung und Evaluierung von Bedrohungs- und Lastszenarien sowie von Sicherheitssystemen.

Neuartige Risiken und Bedrohungssituationen, die zunehmende Komplexität der Sicherheitssysteme und das bislang praktizierte reaktive Risiko- und Sicherheitsmanagement motivieren eine objektive Bewertung von Restrisiken und die daran orientierte werkzeugunterstützte Optimierung von Sicherheitssystemen. Ziel ist ein Werkzeug (Demonstrator) für die antizipative, Kosten-Nutzen-optimierte (statt derzeitig reaktiv durch Regularien vorgegebene) Auslegung von Sicherheitssystemen.

Verkehrsinfrastrukturen, Bedrohungsrisiken, Lastsituationen und Sicherheitssysteme werden in SiVe szenariobasiert mit mathematisch-systemtheoretischen Mitteln multidisziplinär modelliert und simuliert. Folgende Modellierungsarten kommen zum Einsatz und werden als Bestandteil in den SiVe-Demonstrator integriert:

- logistisch-agentenbasierte Modellierung;
- stochastisch-ereignisorientierte Modellierung;
- ökonomisch-nutzenorientierte Modellierung;
- entscheidungsbasiert-fallorientierte Modellierung.

Den einzelnen Modellierungen ist eine Strukturanalyse des Systems vorgeschaltet.

Diese Modellierungsansätze erfassen jeweils spezifische Aspekte einer komplexen Realität. Ziel und Schwerpunkt der SiVe-Facharchitektur ist die (fachliche) Integration der Ansätze und unterschiedlichen Methoden mit Hilfe einer gemeinsamen Methodik und einer durchgängigen Softwarearchitektur. Abbildung 12 fasst die zum Projektmeilenstein erreichten Ergebnisse zusammen. Eine ausführliche Beschreibung der SiVe-Facharchitektur wurde zum Projektmeilenstein präsentiert (D'Avanzo, et al., 2010) und ist in der Systemdokumentation (D'Avanzo, et al., 2010) und im Zwischenbericht für das Projektjahr 2009 ausführlich beschrieben.

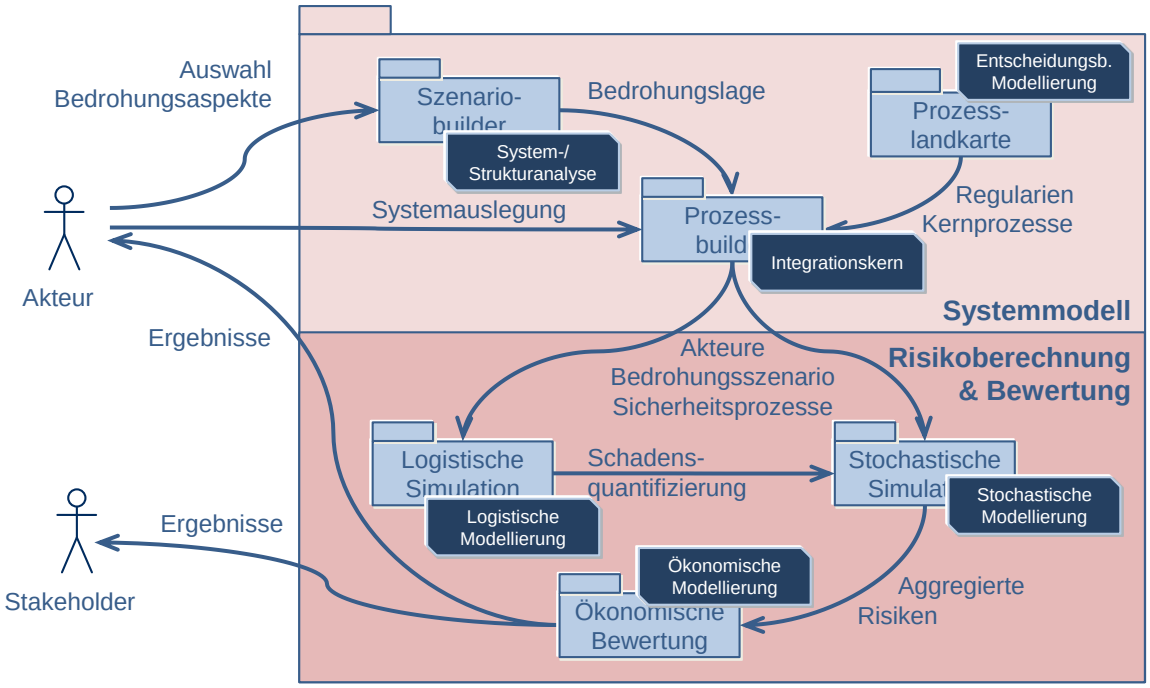


Abbildung 12: Die SiVe Facharchitektur zum Projektmeilenstein: Integration getrennter, unabhängiger Modellierungsansätze und Informationsflüsse zwischen den Modellen.

Die IT-Integration und –Architektur, die Zusammenführung und das „Zusammenspielen“ der unterschiedlichen Modellierungen sowie die genauen Schnittstellenbeschreibungen, Modellierungsinhalte und -Konventionen sind in den Dokumenten der jeweiligen Teilprojekte gemäß Vorhabenbeschreibung zu finden und sind nicht Bestandteil dieses Dokumentes.

Gesamtsystemintegration und Proof-of-Concept

Erzielte Ergebnisse

Die umfassende Systemanalyse eines Flughafens, insbesondere von Bedrohungssituationen[3] und Sicherheitssystemen, führte zur Erstellung eines Szenariobuilders, der

- als Konsistenzprüfung für potentielle Bedrohungssituationen,
- als Checklistengenerator bei untersuchten Änderungen an Sicherheitssystemen und
- für strukturelle Schwachstellenanalysen eingesetzt werden kann.

Dabei wurden in einer umfassenden Prozesslandkarte die bestehenden Sicherheitsprozesse als Grundlage für die weitere Modellierung abgebildet.

Eine aus relevanten und gewichteten Bedrohungssituationen definierte Bedrohungslage für die Risikobewertung und eine aus ebenfalls modellierten Lastsituationen kombinierte (normale) Last für die Betrachtung der Kostenseite ergeben zusammen die **Systemlast** als zentrale Auslegungsgröße für Sicherheitssysteme (**Quantifizierung der Lastgrößen**).

Die von der Bedrohungslage zu erwartenden Schadensgrößen werden in verschiedenen Schadenskategorien wie Menschenleben, Personenschäden, Sachschäden etc. aus der Literatur

[3] Eine Situation bezeichnet ein Fall, der in ein System wie das Flughafen passiert. Sie wird mit eindeutigen Eigenschaften definiert wie ein Subjekt, der ein Ziel und eine Motivation hat, die mit einem Werkzeug erreicht werden usw. Eine Situation kann sowohl eine Bedrohung als auch eine normale Last (z.B. normale Pax bzw. Beschäftigte) beschreiben. In der Systemanalyse wird dafür den Begriff Szenario verwendet.

abgeschätzt bzw. auf Basis der logistischen Simulation ermittelt (**Bedatung der ökonomischen Schadensgrößen**). Die logistische Simulation wird unter Verwendung der normalen Last auch zur Validierung der Umsetzbarkeit von alternativen Systemauslegungen genutzt.

Der Flughafen wird durch Infrastruktur, sicherheitsrelevante Prozesse, eingesetzte Technologien usw. modelliert **(Schutzmechanismen als Systemlayout)**.

Ausgehend von dieser gesamthaften Risikobetrachtung erlaubt die probabilistische Charakterisierung von Schutzmechanismen die Berechnung der durch das Sicherheitssystem erreichten Risikoreduktion. Diese ergibt sich aus den nun nicht mehr zum Schadensereignis führenden Bedrohungen und den damit vermiedenen Schäden. Die probabilistischen Kenngrößen müssen dabei spezifisch für jede Bedrohungs- und Lastsituation angepasst werden, da z.B. ausgebildete Täter die Detektionswahrscheinlichkeiten negativ beeinflussen können (**Quantifizierung der probabilistischen Kenngrößen als Verknüpfung von Systemlast und Schutzmechanismen**).

Die Kosten für das Sicherheitssystem werden für die einzelnen Schutzmechanismen erfasst (Bedatung der ökonomischen Kostengrößen) und auf Basis der normalen Last in verschiedenen Kostenkategorien wie Zeit, Geld, Platzbedarf usw. berechnet.

Damit kann die durch das System erreichte Risikoreduktion den durch das System verursachten Kosten gegenübergestellt und umfassende Kosten-Nutzen-Analysen durchgeführt werden.

Die verbliebenen Restrisiken stehen im Zuge der Berechnungen zur Verfügung und können insbesondere für Katastrophenereignisse gesondert bewertet werden. Generell sind absolute Risiko-/Schadensgrößen mit größerer Unsicherheit behaftet als Änderungen bei der Betrachtung alternativer Systemvarianten, wobei die relativen Größen aber für die Optimierung ausreichend sind.

Insgesamt steht ein Konzept zur Bewertung der Effektivität von Sicherheitssystemen in Form einer System- und Software-Architektur zur Verfügung, das in einer ablauffähigen SiVe-Facharchitektur (auch Proof-of-Concept benannt) validiert ist. Das Instrumentarium wird als Demonstrator integriert.

Abbildung 13 stellt die Facharchitektur des SiVe-Demonstrators nach dem Kontextdiagramm der Abbildung 12 detaillierter dar. Blau hinterlegt sind die Aspekte, die Bestandteil der ablauffähigen Facharchitektur sind.

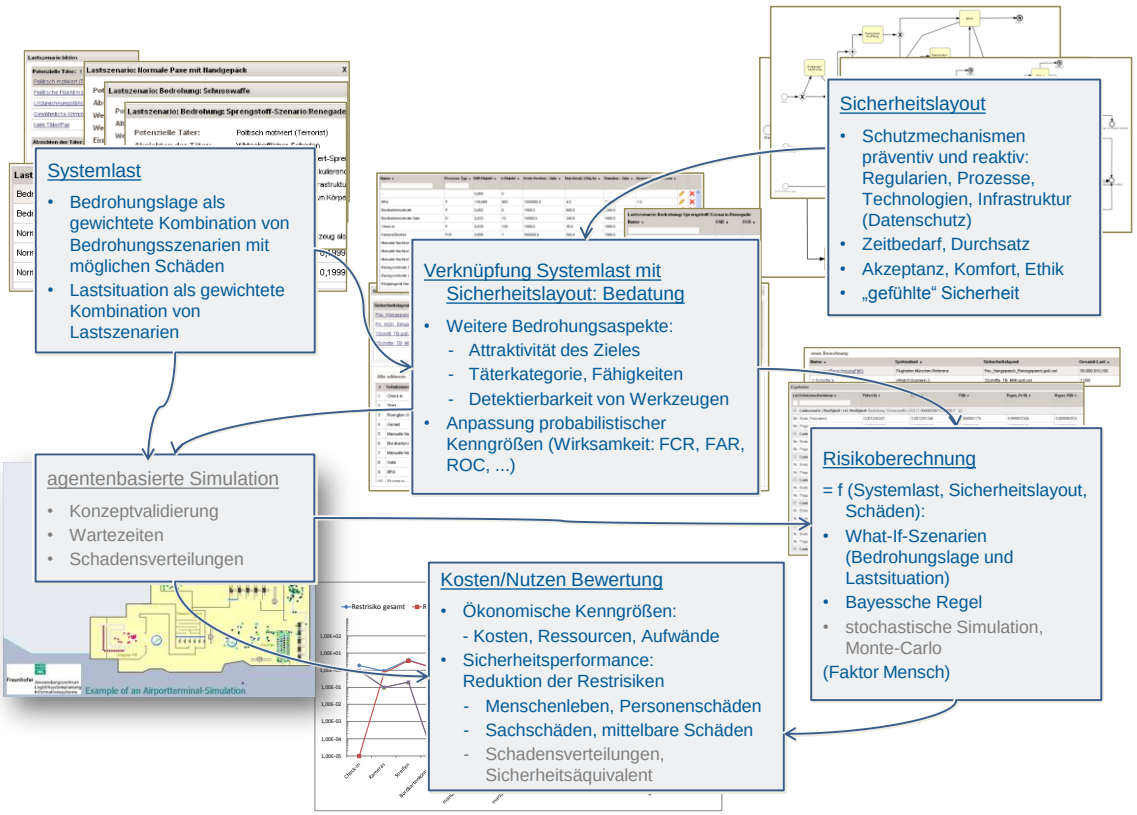


Abbildung 13: PoC nach der verabschiedeten Facharchitektur zum Projektmeilenstein. Die ausgegrauten Inhalte sind nicht im PoC, sondern nur im Demonstrator enthalten.

Anwendungsmöglichkeiten

Folgende technologischen oder prozessualen Innovationen resultieren aus dem Projekt:

- Gesamthafte Optimierung von Sicherheitssystemen statt lokaler ad-hoc Maßnahmen;
- Parametertuning für Schutzmechanismen im Gesamtsystemkontext;
- Berücksichtigung einer sich ändernden Bedrohungslage;
- Argumentationsbasis für die Sicherheitsdiskussion in Politik und Industrie.

Die Quantifizierung der Systemlast und der Schutzmechanismen kann aus Gründen der Geheimhaltung nicht im Projekt erfolgen. Daher wurde beim Demonstrator mit plausiblen Annahmen und Daten aus der Literatur gearbeitet, die nicht notwendigerweise auf die lokale bzw. aktuelle Situation übertragbar sind.

Anwendungsmöglichkeiten bestehen bei Behörden und gesetzgebenden Stellen zur Prüfung der Auswirkungen neuer Regularien sowie bei Anbietern von Sicherheitssystemen zur Optimierung der Sicherheitssysteme (Wettbewerbsvorteil) und als Argumentationshilfe im Vertrieb (Marketing-Hilfsmittel).

Weiterentwicklung der SiVe-Facharchitektur als Proof-of-Concept (PoC)
Zusätzlich zu den zum Projektbeginn spezifizierten Anforderungen haben sich Aufgaben und Fragestellungen im Rahmen der SiVe-Facharchitektur auf Grund der jüngsten Ereignisse[4] und nach Austausch mit Interessenten (Industrie und Behörden) weiterentwickelt.

Parallel zu den Bedrohungsaspekten, die für mögliche Risiken und Schadenereignisse verantwortlich sind, haben auch Lastsituationen eine tragende Rolle für eine objektive gesamthafte Bewertung von Risiken und Kosten von Verkehrsinfrastrukturen. Diese Aspekte wurden in die SiVe-Facharchitektur aufgenommen und weiterentwickelt.

Um die oben genannten Aspekte in der SiVe-Methodik zu demonstrieren, wurde nach dem Projektmeilenstein (Jan. 2010) eine Implementierung des Gesamtsystems und der Teilmodelle (logistische Modellierung ausgenommen) in einer ablauffähiger Facharchitektur erstellt. Diese (Fach-)Implementierung wurde Proof-of-Concept (PoC) benannt und ist Bestandteil des EADS-Arbeitspakets „Systemarchitektur und -integration".

Der PoC stellt eine Implementierungsstufe zwischen der Facharchitektur (die Spezifikation) und dem Demonstrator (die gesamte Umsetzung) dar und beschreibt die Methodik zur Integration der Ansätze in einer durchgängigen Softwarearchitektur. Abbildung 14 stellt dieser Ansatz grafisch dar. Hauptziel ist eine gesamthafte und abstrakte Analyse und Modellierung von kritischen Verkehrsinfrastrukturen gegenüber dem SiVe-Demonstrator. Der PoC ist ein voll integriertes System, das aus verschiedenen abstrakten und unabhängigen Komponenten besteht, die durch eine situationsbezogene Quantifizierung der Schutzmechanismen für einen (Risiko/Kosten) Berechnungsvorgang vernetzt werden.

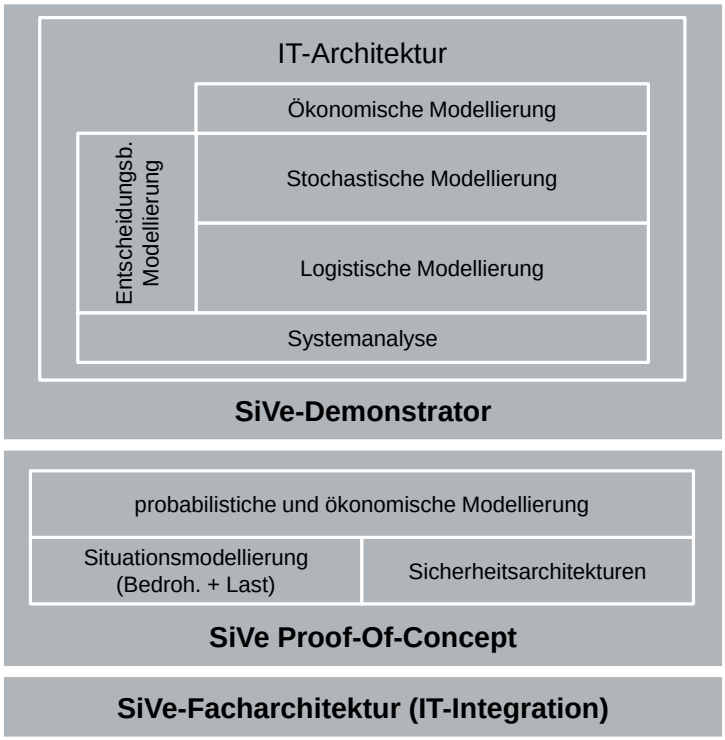


Abbildung 14: SiVe-PoC zwischen Facharchitektur und Demonstrator

4 Siehe z.B. 1.) Zwischenfall im Münchener Flughafen von 20.01.2010, der „einen Millionenschaden" verursacht hat, und 2.) „Unterhosenbomber" (NW Flug 253, Dezember 2009), der den „Körperscanner" in Europa und in den USA eingeführt hat, 3.) Bombe in DHL-Flugzeug/Jemen, Oktober 2010.

Das beiliegende Dokument beschreibt ausführlich die im PoC entwickelte Gesamtmethodik und die damit erreichten Ergebnisse.

Die allgemeine Anforderungen und Ziele von SiVe sind in den im Projekt erstellten Dokumenten (Vorhandenbeschreibung, Teilvorhandenbeschreibungen und die Dokumente der Teilprojekte) zu finden. Für den PoC beziehen wir uns auf die Gesamtvorhaben-beschreibung des Projektes und den Teilantrag EADS zur Facharchitektur, die SiVe-Facharchitektur-Dokumentation vom 2010-02-23 (D'Avanzo, et al., 2010), die Powerpoint-Präsentationen zum Meilensteinmeeting vom 2010-01-14 (D'Avanzo, et al., 2010) und vom 2011-01-12 vor VDI (D'Avanzo, et al., 2011) und die Zwischenberichte zum Teilprojekt von EADS 2009, 2010, 2011.

Motivation des "Proof-of-Concept"
Folgende neue Aspekte, die im SiVe-Demonstrator in der aktuellen Projektlaufzeit aus Zeitgründen nicht vollständig betrachtet wurden, wurden in die Facharchitektur aufgenommen und im PoC weiterentwickelt:

- **Gesamthafte Modellierung und Bewertung** von Verkehrsinfrastrukturen anstatt „What-If-Szenario"-Ansatz: Alle wesentlichen Situationen, sowohl Bedrohungs- als auch Lastsituationen, die sich am Flughafen ereignen können, werden als Systemlast modelliert und in die Systembewertung eingebunden (Kaplan, et al., 1981; Lampert, et al., 2003; Willis, et al., 2005). Im „What-If-Szenario"-Ansatz modellieren einzelne Bedrohungssituationen nur die Risiko- und Kosten-Aspekte von (Groß-)Schadenereignissen.
- **Modellierung von Lastsituationen:** Passagiere, Gepäck und Fracht, jeweils auch mit Sonderlasten, nicht erlaubten oder verbotenen Gegenständen. Dadurch werden die Kosten des Betriebes der Sicherheitssysteme bestimmt.
- **Systemlast-Modellierung** als Zusammenlegung von Bedrohungslage und Last.
- **Risiko- und Kostenorientierte Szenariobildung**. Die im SiVe-Demonstrator angewendete Methode für die Situationsbildung (Muliple Domain Matrix aus der Systems Engineering (Lindemann, et al., 2009)) ermöglicht eine statische, strukturelle Analyse eines Systems. Für eine Risiko- und Kosten-orientierte Analyse und Bewertung ist die Methodik nicht ausreichend, zumindest wie sie in der Strukturanalyse angewendet wurde. Diese Methodik wurde in der Facharchitektur quantitativ weiterentwickelt und in die gesamthafte Modellierung eingebunden. Beispielweise werden Bedrohungen mit weiteren Aspekten ergänzt, da beispielweise die Qualifikation der Täter mögliche Risiken (z.B. Detektionswahrscheinlichkeiten) und Schäden bei Großereignissen beeinflussen.
- Fokus auf das gesamte **Systemlayout**, d.h. eine Verkehrsinfrastruktur wird nicht nur aus Prozessen (als Aktivitäten zu verstehen), sondern auch aus weiteren Infrastrukturaspekten und Technologien modelliert.
- **Abstraktere Modellierung** gegenüber der umfassenden und detaillierten Modellierung im Demonstrator. Diese Entscheidung ist auf der schwierigen, aufwändigen und oft nicht möglichen Datenerhebung (Geheimhaltung sensibler Daten usw.) und der Anforderung von Interessenten („Rapid-Prototyping") zurückzuführen. Dieses Vorgehen wird auch in der Fachliteratur bestätigt (Kaplan, et al., 1981; Willis, et al., 2005).
- **Vereinfachung** der Modellerstellung und der Vorbereitung von Berechnungsstudien. Der Demonstrator ist eine heterogene Software, die aus unterschiedlichen komplexen Modellierungsansätzen, Werkzeugen und Software-Technologien und -Architekturen besteht. Die Modellerstellung im Demonstrator ist aufwändig und benötigt spezielles Know-

how in den verschiedenen Bereichen: von der Systemerstellung für den Szenariobuilder und Prozessmodellierung über die agentenbasierte Modellerstellung und Quantifizierung der stochastischen Modellen bis hin zur Interpretation der Ergebnisse. Durch Komplexität und Detaillierungsgrad ist die Fehlerwahrscheinlichkeit in den Modellen relativ hoch. Die Richtigkeit der Modelle und Annahmen ist auch nicht gewährleistet.
Der PoC vereinfacht die gesamte Modellierung durch eine höhere Modellabstraktion und die Einführung der Konzepte von Systemlast und Systemlayout, die durch die Quantifizierung vernetzt werden.

- **Validierung** der Ergebnisse des Demonstrators durch die Mittelwertbetrachtung. Die Modellvalidierung ist mit sehr geringem Aufwand möglich.
- **Ethische Aspekte** wie Akzeptanz, gefühlte Sicherheit und subjektive Wahrnehmung von Sicherheitsmechanismen fehlen in der Demonstrator-Software. Die Erfahrung aus den Medien im letzten Jahr bzgl. Flüssigkeitsregelung und Einführung von Körperscannern zeigt dagegen, dass diese Aspekte eine wichtige Rolle für Entscheidungsträger spielen. Diese können im PoC eingebaut werden.

Tabelle 6 stellt eine detaillierte Gegenüberstellung der Merkmale zwischen Demonstrator und PoC zusammen.

Tabelle 6: Gegenüberstellung der Merkmale zwischen SiVe-Demonstrator und Proof-of-Concept.

SiVe-Demonstrator	SiVe Proof-of-Concept
Fokus auf **Bedrohungsszenarien** mit dem „**What-If-Szenario-**“Ansatz, um potentielle Schaden bei Großschadenereignissen im System zu ermitteln. Der SiVe-Demonstrator kann nur einzelne What-If-Szenarien und eine Kosten-Bewertung bei Schadensereignissen betrachten. Die normale „Systemlast“, die die Höhe der Sicherheitskosten wesentlich mitbestimmt, wird im SiVe-Demonstrator noch nicht adäquat dargestellt.	**Gesamthafte** Betrachtung des Flughafens durch die Einführung der gesamten **Systemlast** als Zusammenstellung aller möglichen systembetroffenen **Lastsituationen** (Kostenträger) und **Bedrohungen** (Risikoträger). D.h. von seltsamen Großschadenereignissen bis hin zu den häufigen kleineren Zwischenfällen und Normalfällen.
Umfassende statische System- und Strukturanalyse mit der Aufnahme von System- und Bedrohungsaspekten und deren logischen Vernetzung miteinander.	Kosten- und risiko-orientierte Last-Eigenschaften für die Bildung von Last- und Bedrohungs-Situationen.
Umfassende detaillierte **Prozessmodellierung** mit viel Logik in den Prozessmodellen selbst.	Abstrakte, grobe Layoutmodellierung, mit der Prozesslogik in den Prozessschritten und der Berechnungsmethodik gekapselt.
Hoher Aufwand bei Datenerhebung (Systemanalyse, Prozessaufnahme, Interviews, Workshops) und Modellentwicklung. Die Time-To-Market ist zu lang.	Fokus auf „Rapid-Protyping“ für Interessenten auch während Workshops mit Interessenten (als langfristiges Projektziel).
Komplexe Modellerstellung und detaillierte Betrachtung (siehe logistische Modellierung/ Simulation und Prozessmodellierung) zur Ermittlung fehlender Daten. Hohe Fehlerwahrscheinlichkeit auf Grund der Komplexität der Modelle und der heterogenen Modellierungsansätze und –sprachen (ein übergreifendes Metamodell fehlt, dadurch sind Modellierungskonstrukte einer Methode nicht immer in den weiteren Modellen übertragbar).	Höhere Modellabstraktion, Vereinfachung der Modellierung, Definition eines Metamodells, Mittelwertberechnung.

SiVe-Demonstrator	SiVe Proof-of-Concept
Notwendigkeit von sensiblen und „klassifizierten“ Daten als Quantifizierung der Modelle für die Simulationsläufe.	Aufgrund der abstrakteren Modellierung und Mittelwertbetrachtung ist Quantifizierung im PoC weniger kritisch.
Integration von multidisziplinären Modellierungsansätze und Methoden mit loser Kopplung von unterschiedlichen Modellierungswerkzeugen (heterogene Software-Landschaft) und teilweise Redundanz der Modellierungen.	Durchgängiges Berechnungsmodell und homogene Software-Applikation mit voller Integration von Bedrohungen und Lastsituationen in der Sicherheitsarchitektur durch die direkte Vernetzung der jeweiligen Eigenschaften (Mapping Situationen-Layout) und die situationsbezogene Quantifizierung der Schutzmechanismen. Die Anbindung an externe Modellierungswerkzeuge für Datenerfassung (Systemanalyse), Prozessmodellierung und Datenanalyse erfolgt über Standard-Schnittstellen.
Ökonomische Bewertung von Schadensereignissen mit Verteilungen.	Mittelwertbetrachtung (Restrisiko = Schadenshöhe x Eintrittswahrscheinlichkeit).
Vom Entscheidungsträger abhängige ökonomische Bewertung bei Risikoereignissen (Großereignisse) – Sicherheitsäquivalent.	Restrisiken und Kosten (auch subjektive Wahrnehmung von Schutzmechanismen theoretisch möglich).
Ethische Bewertung außerhalb des Demonstrators.	Ethische Bewertung und subjektive Wahrnehmung von Sicherheitsmechanismen als Bestandteil des PoC möglich.
Die Vorbereitung einer Simulationsstudie mit dem Demonstrator ist sehr umfangreich und aufwändig aufgrund der erforderlichen Kenntnisse in den integrierten Modellierungsmethoden.	Als Ziel hat der PoC die Vereinfachung der Anwendung, sodass Kosten-Nutzen Analysen und Bewertungen mit relativ geringem Aufwand in der Einarbeitung durchgeführt werden können.
—	Abstrahierung der Methodik und Anwendbarkeit mit geringem Aufwand für weitere Sicherheits-architekturen, Verkehrsinfrastrukturen und Flug-/Missionssicherheit von UAV.
Die Integration der Modellierungsansätze ist derzeit eine Herausforderung für die Softwareentwicklung, die nicht Gegenstand der Forschung ist.	—

Die Systemkomponente des PoC und deren Vernetzung

Der Ablauf

Abbildung 15 stellt den Anwendungsablauf im PoC dar. Die Ausgangssituation für die Risiko- und Kostenberechnung sind das Sicherheitslayout und die Systemlast. Diese Kernkomponenten werden modelliert und miteinander vernetzt. Die Vernetzung erfolgt durch die situationsbezogene Quantifizierung der Schutzmechanismen.

Das Sicherheitslayout wird durch Prozessmodelle beschrieben. Die Prozessmodellierung erfolgt außerhalb des PoC. Die daraus resultierenden Prozessmodelle werden durch standardisierte Schnittstellen dem PoC zur Verfügung gestellt (derzeit wird BPMN 2.0 unterstützt, s. Kapitel 0). Die einzelnen Prozess- bzw. Layoutelemente werden mit einer Prozessdatenbank vernetzt, die alle möglichen Schutzmechanismen enthält. Jeder Schutzmechanismus wird mit Kostengrößen wie Anschaffungskosten, Anwendungskosten, (durchschnittlichen) Prozessdauer sowie die Quote (stichprobenartiger Alarmrate für eine Kontrolle) quantifiziert. Diese Informationen sind aus Gesprächen bzw. aus der Literatur zu erhalten oder werden angenommen. Die Prozessdatenbank dient als Input für die Kostenberechnung.

Die Systemlast besteht aus Bedrohungs- und Lastsituationen. Eine Last-Datenbank beinhaltet alle möglichen Situationen, sowohl historische Fälle als auch künftige und erfundene Fälle. Aus dieser Datenbank wird eine spezifische Systemlast zusammengestellt. Die Situationen der Systemlast werden mit Häufigkeit (Anzahl der Fälle / Jahr) und möglichen Schaden quantifiziert.

Um eine Berechnungsstudie durchzuführen, ist ein Szenario bestehend aus eine Systemlast und ein Layout zu erstellen. Die Situationen der ausgewählten Systemlast werden mit den Prozesselementen des Layouts miteinander vernetzt. Die Vernetzung erfolgt für jeden Prozessschritt des Layouts durch die situationsbezogene Eingabe von probabilistischen Kenngrößen wie Falsch-Alarm-Raten und Detektionswahrscheinlichkeiten.

Sicherheitslayout und Systemlast sowie die Vernetzung zwischen einander werden in den nachstehenden Unterkapiteln ausführlich beschrieben.

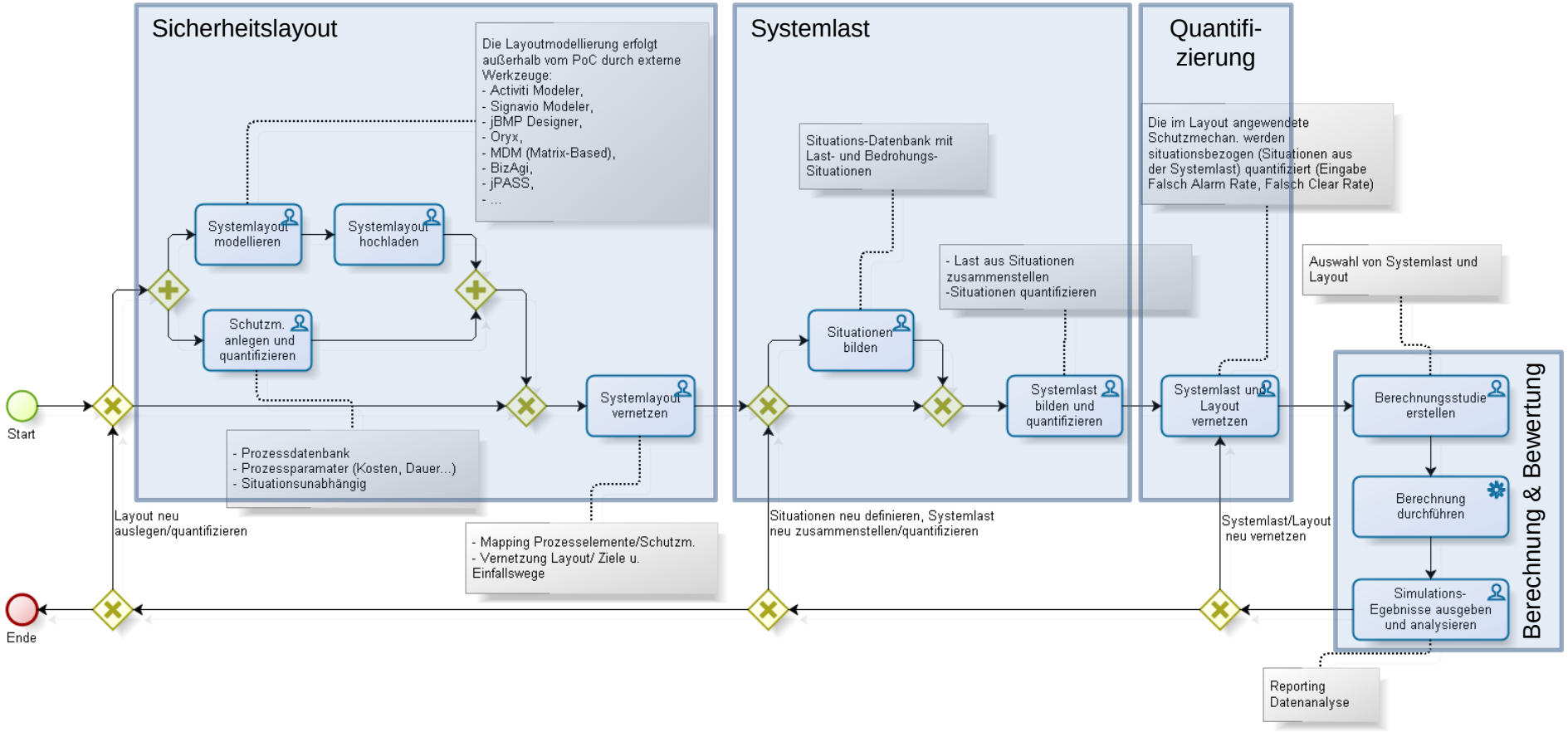


Abbildung 15: Anwendungsablauf im Proof-of-Concept. Die Abbildung zeigt die Kernkomponenten und deren Vernetzung.

Systemlayout

Das Layout eines Systems stellt die (Sicherheits-)Infrastruktur mit allen möglichen Abläufen und Sicherheitsschränke dar. Es wird auch Systemlayout bzw. Sicherheitslayout benannt. Im Projekt SiVe ist das System ein Flughafen. Das im PoC entwickelte Konzept ist an andere Infrastrukturen übertragbar. Ein Layout ist von der Systemlast unabhängig.

Im PoC wird ein Layout als Prozessmodell beschrieben. Die Modellierung erfolgt außerhalb des PoC. Das Modell wird durch eine Standard-Schnittstelle in den PoC hochgeladen.

Ein Prozessmodell besteht aus Prozesselementen (auch Layoutelement benannt) und Sequenzflüssen (Ablauf im System). Das Prozesselement modelliert eine Transformation von Inputgroßen nach Outputgroßen, nämlich Wahrscheinlichkeiten, und wird anhand von Eigenschaften beschrieben. Die Prozesseigenschaften sind nicht Bestandteil des Layoutmodells. Sie werden im PoC definiert und fließen direkt in das Berechnungsmodell ein.

Die Sequenzflüsse definieren die möglichen Prozesspfade zwischen Start- und End-Knoten als Wahrscheinlichkeit des Durchgehens im gesamten Layout (Wahrscheinlichkeits-Fortpflanzung). Die Zusammenstellung aller möglichen Prozesspfade eines Layouts definiert sich Sicherheits- bzw. Layoutarchitektur.

Ein Prozesspfad wird auch Prozessinstanz benannt. Eine Prozessinstanz im Layout kann zu einem Alarm (Systemalarm) bzw. einem Clear (Systemclear) führen.

Weitere Elemente im Prozessmodell sind außer den bereits erwähnten Start- und End-Ereignissen, Pools und Lanes.

Abbildung 16 zeigt ein Beispiellayout für die Personenabfertigung am einen beliebigen Flughafen in der EU. Der Ablauf wurde aus (SPT, 2006) abgebildet. Das Layout wurde mit der im PoC entwickelten Modellierungskonvention auf Basis der BPMN 2.0 (Business Process Modeling Notation Version 2.0) erstellt.

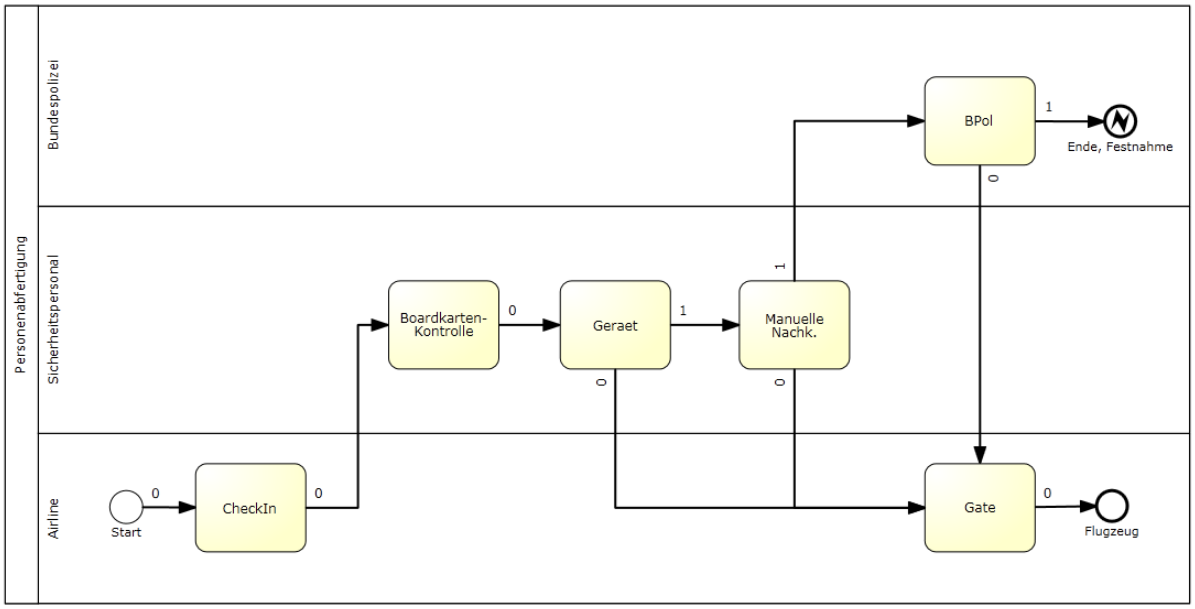


Abbildung 16: Typischer Ablauf für die Personenabfertigung im Flughafen ohne Handgepäckkontrolle.

Modellierungskonventionen

Im PoC wurde eine eigene Modellierungskonvention aus der Spezifikation der Prozessmodellierungssprache BPMN 2.0 entwickelt. Das Ziel ist, die Modellierung eines Layouts so einfach wie möglich zu halten und gleichzeitig die Möglichkeit auch komplexere Prozessabläufe zu modellieren. Der Nachteil ist, dass einfache Konstrukte durch komplexere Modelle abgebildet werden. Ein Beispiel ist die Unterscheidung aus einem Prozesselements zwischen mehreren Alarmarten, wie in Abbildung 17 und Abbildung 18 zu sehen ist. Da das PoC-Modell nur zwischen den zwei Stati „Alarm“ und „kein Alarm“ unterscheiden kann, ist das Verhalten durch mehrere Schritte zu modellieren. Dabei ist dann die Quantifizierung zu beachten.

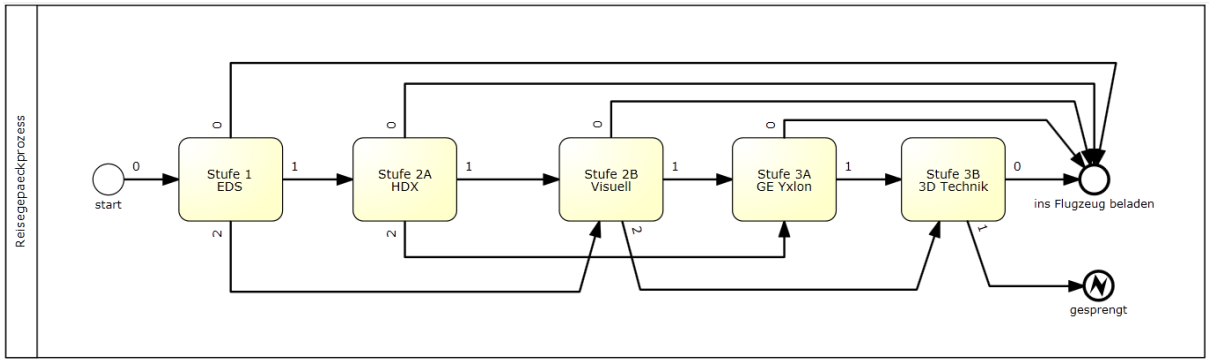


Abbildung 17: Layoutmodell für die Reisegepäckkontrolle mit drei Alarmstati aus den Prozesselementen.

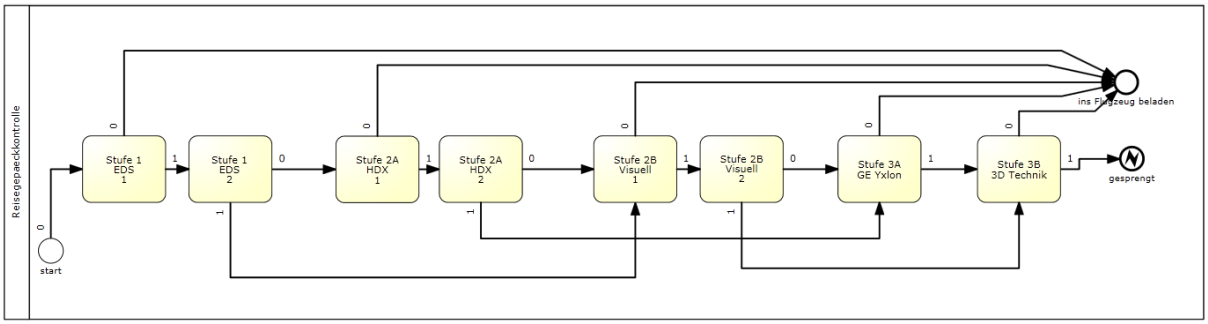


Abbildung 18: PoC-Modell der Reisegepäckkontrolle aus Abbildung 17.

Ein Prozesselement wird durch einen Task dargestellt und kann einen Alarm oder einen Clear auslösen. Ein Start-Knoten repräsentiert den Einfallsweg einer Situation. End-Knoten bzw. -Ereignisse sind Ziele der Situationen (mit Unterscheidung zwischen von Alarm und von Clear ausgelösten End-Ereignissen). Zur Vereinfachung werden die Gateways der BPMN-Notation nicht angewendet. Start- und End-Konten und Tasks werden durch Sequenzflüsse verbunden, um die möglichen Abläufe abzubilden. Die Prozesse werden durch Pools dargestellt und die Prozessverantwortlichen durch Lanes.

Tabelle 7 beschreibt die Modellierungskonventionen für den PoC. Es ist wichtig zu achten, dass diese Konvention als Grundlage für das Berechnungsmodell dient. Abweichungen in der Modellierung können beim Hochladen der Modelle in den PoC bzw. bei der Berechnung zu Fehlern führen.

Symbol	BPMN-Tag	Beschreibung	PoC-Tag
	startEvent	• Startereignis im Layoutmodell. • Es repräsentiert den Startpunkt für einen/mehreren Prozessabläufe bzw. -instanzen. • Ein Layout kann mehrere Startereignisse haben. Im aktuellen Entwicklungsstand wird nur ein Startereignis erkannt. • Es wird mit dem Situations-Aspekt „Einfallsweg“ nach dem Hochladen des Layouts manuell vernetzt.	start
	endEvent	• Zielereignis: Endknoten bei einem Clear im Layoutmodell (die Situation hat erfolgreich das Ziel erreicht). • Es repräsentiert das zu erreichendes Ziel (Angriffsziel für Bedrohungssituationen und Nutzungsziel bei normalen Lastsituationen) bei einem Clear. • Ein Layout darf mehrere Zielereignisse enthalten. • Es ist als Zielereignis für die Prozessinstanzen, die einen Clear auslösen sollen (z.B. Flugzeug erreichen), anzuwenden. • Im Berechnungsmodell ergibt das Endknoten die Wahrscheinlichkeit des Durchkommens und des Erreichens des Zieles. Bei Bedrohungssituationen wird dies mit Restrisiken assoziiert. • Es wird mit dem Situations-Aspekt „Ziel/Ende“ “ nach dem Hochladen des Layouts manuell vernetzt.	target
	endEvent + errorEventDefinition	• Endereignis: Endknoten bei einem Alarm im Layoutmodell (die Situation hat das Ziel nicht erfolgreich erreicht). • Es repräsentiert das erreichtes Ende im Alarmfall. • Ein Layout darf mehrere Endereignisse enthalten. • Es ist als Endereignis für die Prozessinstanzen, die einen Alarm auslösen sollen (z.B. Ende, Festnahme), anzuwenden. • Im Berechnungsmodell ergibt das Endknoten die Wahrscheinlichkeit der Festnahme (z.B. der Entdeckung bei Bedrohungssituationen), d.h. es wird mit den vermiedenen Risiken assoziiert. • Es wird mit dem Aspekt „Ziel/Ende“ nach dem Hochladen des Layouts manuell vernetzt.	end
	task	• Das Prozesselement. • Nach dem Hochladen des Layouts wird es mit einem Schutzmechanismus aus der Prozessdatenbank vernetzt. Dadurch werden die Situationen einer Systemlast indirekt (über die Quantifizierung) vernetzt. • Prozesselemente werden mit Eigenschaften beschrieben, die aber nicht Bestandteil des Layouts ist.	task

Symbol	BPMN-Tag	Beschreibung	PoC-Tag
	sequenceFlow	• Es definiert den Sequenzfluss bzw. die möglichen Prozessabläufe im Layoutmodell durch die Verbindung von Prozesselementen, Start- und Ziel-/End-Ereignissen miteinander. • Es wird mit „0“ für Alarm und „1“ für Clear bezeichnet (Prozessparameter „conditionExpression“) • Ein Sequenzfluss stellt die Flussrichtung für die Wahrscheinlichkeits-Fortpflanzung im Layoutmodell dar. (Input/Output eines Prozesselementes). • Ein Prozesselement muss mindestens einen, kann aber beliebige (Anzahl > 1) Sequenzflüsse als Input haben. • Ein Prozesselement muss mindestens einen und maximal zwei Sequenzflüsse als Output („0“ und „1“) haben. Diese Vorgabe hängt vom jetzigen Berechnungsmodell ab. Abweichungen führen zu Fehlermeldungen beim Hochladen des Layouts und in der Berechnung. • Ein Sequenzfluss stellt den Wahrscheinlichkeitsfluss grafisch dar.	-
	process	• Dies definiert den Prozess selbst. • Ein Layout muss mindestens ein Pool haben.	-
	lane	• Ein Lane definiert einen Prozessverantwortlichen. Damit können Prozessschritte zu Akteuren zugeordnet werden. • Ein Pool muss mindestens ein Lane haben. • Gekapselte Lanes werden im aktuellen Entwicklungsstadium im PoC nicht berücksichtigt.	-

Tabelle 7: Die Konventionen der Layoutmodellierung im PoC.

Das in Abbildung 16 modellierte Layout wurde mit der oben beschriebenen Konvention und mit allen benannten Elementen modelliert: Tasks, End- und Start-Ereignisse, Sequenzflüsse, Pools und Lanes. Abbildung 16 zeigt wie diese Modellierungskonvention zu verwenden ist.

Wie bereits erwähnt werden die Gateways der BPMN-Notation nicht modelliert. Die Sequenzflüsse werden direkt an den Tasks angeheftet (dies ist auch in der BPMN 2.0 Spezifikation erlaubt). Es ist auch zu achten, dass im aktuellen Entwicklungsstand nur XOR-Gateways in der Konvention angewendet werden. Dies ist auf das implementiertes Berechnungsmodell zurückzuführen.

Prozesselement

Ein Prozesselement ist das Grundelement des Layouts für die Kosten und Risiko-Berechnung. Es ist als Transformation eines bzw. mehreren Eingabe-Wahrscheinlichkeiten nach Ausgabe-Wahrscheinlichkeiten definiert. Die Prozesseigenschaften bestimmen aufgrund der internen Logik und der Quantifizierung die Aufteilung der Eingabewahrscheinlichkeit nach Alarm (Ausgabe „1“ im Layoutmodell) und Clear (Ausgabe „0“). Der Alarm kann aufgrund der Detektion eines Gegenstandes (**True Alarm**) oder aufgrund keiner Detektion (**False Alarm**) wie z.B. falsche Detektion bzw. gewünschten Alarm (Quote) ausgelöst werden. Der Clear-Fall kann durch einen richtigen Clear (**True Clear**) oder eine nicht-Detektion (**False Clear**) eintreten. Diese Ergebnisse bestimmen den nächsten Prozessschrift, der durchzulaufen ist. Abbildung 19 stellt diese Fälle für ein Prozesselement dar.

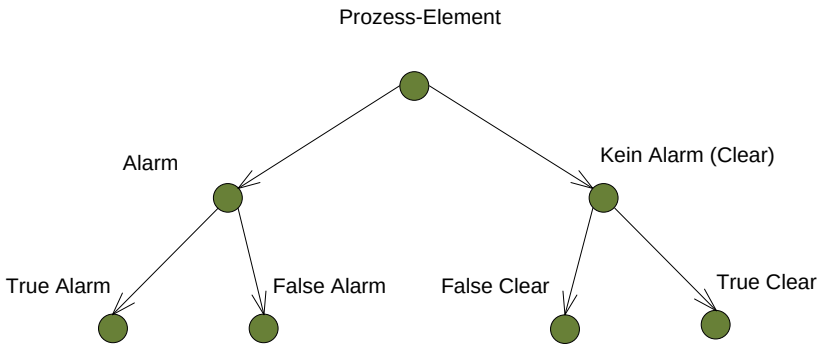


Abbildung 19: Ausgaben eines Prozesselements als Alarm und Clear.

In der SiVe-Facharchitektur-Dokumentation wurden Alarm und Clear als Prozessmetriken definiert, die die Grundlage des Berechnungsmodells bilden. Tabelle 8 beschreibt die Alarm- und Clear-Metriken.

Tabelle 8: Prozess-Alarm und –Clear.

Prozessmetriken	Beschreibung
True Alarm	• Prozesswirksamkeit: Wirksamkeit des Prozesselements durch Entdeckungswahrscheinlichkeit und Detektionsrate des Schrittes. • Eine Bedrohung wird korrekterweise entdeckt. Dafür ist der Prozessschritt da. • Von der Bedrohungssituation abhängig (z.B. Werkzeug). • Einflussfaktoren bei menschlichen Aktivitäten: Faktor Mensch, Trainingszustand, Stress, usw. • Einflussfaktoren bei Geräten: Geräteinstellungen, -eigenschaften • Einfluss auf Kosten. • Betrifft Bedrohungssituationen.
False Alarm	• Falschalarmrate (Fehler 1. Art) • Eine normale Last (keine Bedrohung) löst falscherweise einen Alarm aus. Beispiele sind: Alarm eines Metaldetektors bei nicht abgelegten metallischen Gegenständen; in der manuellen Nachkontrolle bei schlechter Trainingszustand des Sicherheitspersonals, usw. Die Quote (stich-probeartige gewünschter Alarm) ist ein provozierter/gewünschter Alarm. • Einfluss auf Kosten. • Betrifft Lastsituationen.
True Clear	• Zuverlässigkeit negativ: die richtige Nicht-Detektion bei keiner Bedrohung / normaler Last. • Einflussfaktoren bei Geräten: Einstellung • Einflussfaktoren bei Personal: Trainingszustand, Müdigkeit, … • Betrifft Lastsituationen.
False Clear	• Fehler 2. Art: Unwirksamkeit des Prozesselements durch die nicht-Detektion einer Bedrohung. • Diese Große bestimmt die Risiken und ist mit dem Schadenausmaß verbunden. • Es bestimmt, ob die Situation erfolgreich durchgeführt wird/wurde. • Betrifft Bedrohungssituationen.

Typischerweise löst eine Bedrohungssituation einen Alarm aus, wenn der Bedrohungsgegenstand vom Prozessschritt detektiert wird (True Alarm). Für einen normalen Passagier, der durch einen Prozessschritt durchläuft und nichts verbotenes mit sich hat, würde ein Alarm nur bei einer Quote bzw. bei einem nicht erwünschten Alarm ausgelöst (False Alarm). Beispiele von Falschalarm sind: 1. metallische Gegenstände wie Schlüssel oder Kleingeld am

Körper (die Torbogensonde löst einen Alarm aus, weil der Passagier (normale Last) vergessen hat, sie abzulegen); 2. Parfüm durch einen Sniffergerät.

Im Prozessmodell wird nicht zwischen True und False Alarm/Clear unterscheiden. Ein Alarm ist ein Alarm und das Layout bestimmt, was in diesem Fall passieren soll. Genauso ist es im Clear-Fall. Die Unterscheidung zwischen den Alarm-/Clear-Stati wird durch die Situationsart erreicht: True Alarm / False Clear bei Bedrohungssituationen und True Clear / False Clear bei Lastsituationen.

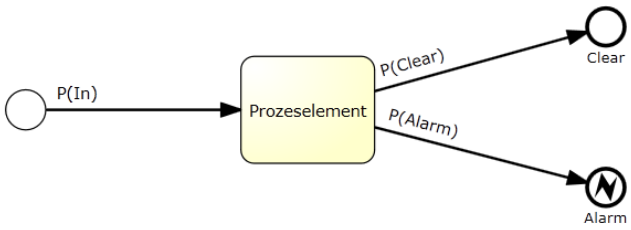


Abbildung 20: Darstellung von Alarm und Clear (keinem Alarm) im Layoutmodell. Die Unterscheidung zwischen True und False Alarm/Clear erfolgt im Prozesselement als Bestandteil des Berechnungsmodells.

Abbildung 20 stellt das Prozesselement dar. *P(In)* ist die Wahrscheinlichkeit, dass das Prozesselement aktiviert wird (Input), und ist der Output des / eines vorherigen Prozessschritts bzw. des Start-Ereignis. *P(Clear)* ist die Wahrscheinlichkeit, dass das Element keinen Alarm (Clear) ausgelöst hat, und *P(Alarm)* ist die Wahrscheinlichkeit, dass es einen Alarm ausgelöst hat (Alarm). *P(Clear)* und *P(Alarm)* sind die Inputs der nachgeschalteten Prozessschritte im Clear- bwz. Alarm-Fall. Die Unterscheidung zwischen True und False Alarm/Clear erfolgt im Prozesselement als Bestandteil des Berechnungsmodells.

Layoutarchitektur und Konfiguration

Die Ausgabe eines Prozesselements bestimmt den nächsten Schritt, der durchzulaufen ist. Eine Prozessinstanz ist ein exakter Pfad zwischen einen Start- und einen End-Knoten. Sie wird durch die Alarm/Clear-Ausgaben der dazwischen liegenden Prozessschritte definiert.

Alle Prozessinstanzen eines Layouts definieren zusammen die Systemkonfiguration (welches Prozesselement wird als nächstes durch Alarm / Clear aktiviert), auch Layout- bzw. Sicherheitsarchitektur benannt. Die Systemkonfiguration dient als Eingabe für die PoC-Berechnungsengine.

Sei Ω_l die Prozessinstanz l eines Layouts (genauer Pfad l zwischen einem Start- und einem End-Knoten). Die PoC Berechnungs-Engine ermittelt im Vorfeld alle möglichen Instanzen Ω_l von allen Start- bis zu allen End-Ereignissen. Die Prozesseigenschaften bestimmen dann, wie und wann jede Instanz „aktiviert“ wird. D.h., die Layoutarchitektur bestimmt, welche Endknoten aus welchem Grund (Alarm bzw. Clear) von einem Start-Knoten erreicht werden.

Die Layoutarchitektur der Personenabfertigung aus Abbildung 16 wird tabellarisch in Tabelle 9 dargestellt. Eine Spalte Ω_l stellt eine Prozessinstanz dar. Tabelle 9 ist wie folgt zu verstehen:

- „0“: Prozesselement wird durch einen Clear aktiviert;
- „1“: Prozesselement wird durch einen Alarm aktiviert;
- „-„: Prozesselement wird nicht aktiviert, d.h. nimmt zum Ablauf nicht teil;
- „Ziel“: erreichtes Ziel im Ablauf.

Der Ablauf ist nicht sequenziell zu verstehen. Die notwendige Information für das Berechnungsmodell ist nur: 1. Welches Element wird wie aktiviert (durch Alarm oder Clear) und 2. Welches Ziel/Ende wird erreicht.

Tabelle 9: Die Layoutarchitektur des Modells „Personenabfertigung“ aus Abbildung 16.

Prozesselement	Ω_1	Ω_2	Ω_3	Ω_4
CheckIn	0	0	0	0
Geraet	0	1	1	1
Start	0	0	0	0
Boardkarten-Kontrolle	0	0	0	0
Ende, Festnahme	-	-	-	Ziel/Ende
BPol	-	-	0	1
Manuelle Nachk.	-	0	1	1
Flugzeug	Ziel	Ziel	Ziel	-
Gate	0	0	0	-

Prozesseigenschaften

Die Prozesselemente eines Layouts sind im PoC abstrakte Konzepte, die unabhängig vom spezifischen Parameter sind. Dadurch ist ein Layout wiederverwendbar. Für eine Berechnungsstudie werden sie mit spezifischen Parametern bestückt, wie ein spezifisches Gerät bzw. spezielles Personal usw. Die Bestückung erfolgt anhand der Prozesseigenschaften **Objekttyp** und **Parametersatz**.

Der Objekttyp spezifiziert, welches Objekt durch das Prozesselemente untersucht / kontrolliert wird, wie z.B. die Person, das Handgepäck, das Reisegepäck usw. Im PoC werden derzeit die in Tabelle 10 beschriebene Objekttypen berücksichtigt (die Tabelle ist beliebig ergänzbar). Der Objekttyp wird mit dem Situationsaspekt Einbringungsart gemappt (s.

Tabelle *25*).

Tabelle 10: Prozesseobjetktypen.

Objekttyp	Schlüssel
Luftpost	A
Reisegepäck	B
Luftfracht	C
Handgepäck	H
Flughafenlogistik	L
Person	P
Person + Reisegepäck	P+B
Person + Handgepäck	P+H

Der **Parametersatz** dient zur Quantifizierung des Prozesselements. Jedes Prozesselements wird mit einem Schutzmechanismus aus der Prozessdatenbank gemappt. Ein Schutzmechanismus wird durch zwei Datensatzarten beschrieben. Der eine Datensatz beinhaltet situationsunabhängige Daten, die beispielweise die Nominalkosten und Nominaldauer (Kosten und Dauer pro untersuchtes Objekt) und die Quote (provozierter Alarm für eine Kontrolle nach dem Zufallsprinzip). Der zweite Datensatz beinhaltet die situationsbezogene Quantifizierung mit Falsch Alarm Rate (falsche Detektion) und Falsch Clear Rate (nicht Detektion). Diese Größen dienen zur probabilistischen Berechnung der Wahrscheinlichkeiten des Durchgehens durch die Prozessinstanzen.

Systemlast

Die Systemlast ist die Belastung eines Systems und setzt sich aus gewichteten Last- und Bedrohungssituationen zusammen, die in einem System vorkommen (können). Eine Situation wird durch sämtliche Eigenschaften eindeutig definiert (sogenannte Aspekte) und kann Kosten (Lastsituation) bzw. Risiken (Bedrohungssituation) verursachen.

Situationen und Systemlast werden in den nächsten Unterpunkten genauer beschrieben.

Situationen

Eine Situation (sei sie eine Last bzw. eine Bedrohung) beschreibt eine genaue Art von Belastung bzw. Störung eines Systems. Beispielweise sind normale Passagiere, die abfliegen möchten und die mit im Handgepäck Flüssigkeit in einem Behälter größer als 100ml haben, eine Situation. Sie ist ein abstraktes Konzept und wird erst in der Bildung einer Systemlast quantifiziert.

Um eine Situation im PoC eindeutig und verhaltensmäßig zu definieren, charakterisieren und mit dem Systemlayout zu vernetzten, wird sie mit statischen Eigenschaften beschreiben. Diese Eigenschaften nennen sich **Aspekte**: Sie definieren eindeutige Aspekte / Verhalten einer Situation, wie die Kategorie der Personen (Täter bzw. keinen Täter), deren Ziele und Motivation, die Interaktionspunkte/Vernetzung mit dem System wie Ziele und Einfallswege, die Reaktion des Systems auf dieser Last (welche Objekte haben sie mit, wie bringen sie sie ein und wie reagieren die Systemelemente darauf). **Aspektelemente** sind die Elemente eines Aspektes. Die Zusammenstellung dieser Eigenschaften definiert das PoC-**Situationsmetamodell**.

Das Situationsmetamodell des PoC ist in der Tabelle 11 beschrieben. Sie wurde aus der Literatur und teilweise aus den Ergebnissen des Teilprojektes von Bauhaus Luftfahrt (siehe entsprechende Dokumentation des Teilprojektes), wobei EADS IW mitgewirkt hat, erstellt.

Tabelle 11: Das PoC-Situationsmetamodell: die Situationsaspekte.

Aspekte	Beschreibung	Quantifizierung / Mapping
Kategorie	• Sie bestimmt, ob die Situation eine normale Last bzw. eine Bedrohung ist. • Beispielweise Täter oder Passagier.	• Beeinflusst die Hohe der Schaden.
Nutzung / Angriffsziel	• Das Ziel der Situation, z.B. ein Angriffsziel für einen Täter bzw. ein Aktions-/Nutzungsziel für den normalen Passagier – keinen Täter (Flugzeug für abfliegende Passagiere). • Das Ziel bestimmt, welche Prozessinstanzen durchlaufen werden sollen, um genau das Ziel zu erreichen.	• Mappingaspekt: Es wird zum End-Knoten im Layoutmodell gemappt (Ziel im Layout). • Beeinflusst die Hohe der Schaden.
Motivation / Absichten	• Sie kann die Quantifizierung der Prozesselemente beeinflussen.	• Beeinflusst die Hohe der Schaden und die Quantifizierung der Wahrscheinlichkeiten (False-Alarm-Rate, False-Clear-Rate).
Objekt	• Mitgenommene Objekte wie Werkzeuge. • Es beeinflusst die Quantifizierung der Prozesselemente.	• Beeinflusst die Hohe der Schaden und die Quantifizierung der Wahrscheinlichkeiten (False-Alarm-Rate, False-Clear-Rate).
Einbringungsart	• Beschreibt wie das Objekt / Werkzeug zum Ziel eingebracht wird/werden soll. • Sie bestimmt, welche Prozesselemente und -Instanzen des Layouts aktiviert werden.	• Bestimmt welches Prozesselement aktiviert wird. • Beeinflusst die Hohe der Schaden.
Einfallsweg	• Der Einfallsweg einer Situation stößt ein Startereignis eines Layouts an.	• Mappingaspekt: Es wird zum Start-Knoten im Layoutmodell gemappt (Startpunkt im Layout).
Attraktivität des Ziels	• Ein Ziel kann (qualitativ) äußerst attraktiv, sehr attraktiv, attraktiv, wenig attraktiv und nicht attraktiv sein (Veatch, et al., 1999). • Evtl. im Layout definieren. • Noch nicht im PoC integriert.	• Beeinflusst die Hohe der Schaden.
Fähigkeit des Täters	• Die Fähigkeit, ein Angriff auszuführen. • Noch nicht im PoC integriert.	• Beeinflusst die Hohe der Schaden und die Quantifizierung der Wahrscheinlichkeiten (False-Alarm-Rate, False-Clear-Rate).
Entdeckbarkeit eines Objektes	• Wie einfach/schwer ein Objekt entdeckt werden kann. • Noch nicht im PoC integriert.	• Beeinflusst die Hohe der Schaden und die Quantifizierung der Wahrscheinlichkeiten (False-Alarm-Rate, False-Clear-Rate).
Wo ist das Objekt	• Z.B. Stelle am Körper • Noch nicht im PoC integriert.	•

Eine Situation und das Metamodell sind per Definitionem systemunabhängig. Die Aspekt-Elemente sind dagegen systemabhängig. Für das PoC werden sie mit flughafenspezifischen Daten gefüllt. Das Unterkapitel „Aspektelemente der Situationen“ stellt die Aspektelemente für SiVe dar.

Eine Situation ist ein abstraktes Konzept (Metadaten) und unabhängig vom Systemlayout. Sie wird nicht als solche quantifiziert. Eine Situation ist generisch (abstrakt) und fasst viele Arten von Situationen zusammen. Das oben genannte Beispiel (der normale Passagier, der abfliegen möchte) fast beispielweise alle möglichen Situationen für Passagiere mit Handgepäck und Flüssigkeit, die abfliegen möchten. Die Anzahl von Handgepäcken, wie viel Flüssigkeit und welche Art davon (verboten, nicht erlaubt usw.) sowie die Entdeckbarkeit der Flüssigkeit usw. werden dabei nicht definiert. Nur bei der Bildung einer Systemlast wird sie erst quantifiziert.

Im PoC wird es zwischen Bedrohungs- und Lastsituationen unterscheiden. Bedrohungen sind die Zwischenfälle, die theoretisch nicht so oft geschehen und die Personen- und wirtschaftliche Schaden verursachen können. Diese sind Risikoträger und keine Kostenträger.

Lastsituationen sind dagegen die normale Belastung des Systems und verursachen Kosten. Die Kosten werden hier durch das Gehen durch die Prozesselemente des Layouts verursacht.

Das Zusammenspielen zwischen Last- und Bedrohungssituationen ist eine wichtige Komponente, die Entscheidungsträger nicht vernachlässigen dürfen und die genau im Demonstrator fehlt. Sicherheitsmaßnahmen, die Kosten für die normale Systemlast verursachen, werden beispielweise aufgrund von potentiellen Bedrohungen eingeführt, um die Sicherheit durch Minderung der Risiken zu erhöhen. Umgekehrt kann das Abschaffen von Sicherheitssystemen die Kosten des Systems mindern mit dem Preis aber, dass die Risiken steigen (können). Eine Gegenüberstellung der Kosten und (Rest-)Risiken verschiedener parametrisierten Layouts hilft Entscheidungsträger sachlich bei der Suche nach der optimalen Lösung. Dies ist das Hauptziel des PoC.

Das im PoC definierte Situationsmetamodell wurde für die Anforderungen aus SiVe konzipiert und spezifiziert. Erfahrung, Ergebnisse und Schwachstellen aus dem Teilprojekt „Struktur- und Systemanalyse“ von Bauhaus Luftfahrt und aus der Fachliteratur fließen ein. Trotz dem flughafenspezifischen Input ist das Metamodell flughafenunabhängig (soweit wie möglich im Rahmen des laufenden Projektes), so dass die Weiteranwendung in anderen Bereichen möglich ist. Das Metamodell ist auch erweiterbar (derzeit nur durch programmtechnische Änderungen).

Unterscheide zwischen der SiVe-Systemanalyse und das PoC-Situationsmetamodell

Das PoC-Situationsmetamodell mit den definierten Aspektelementen ähnelt sich auf dem ersten Blick dem MDM-Ansatz (Multiple Domain Matrix (Lindemann, et al., 2009)) der Systemanalyse im SiVe-Teilprojekt von Bauhaus Luftfahrt (Maurer, et al., 2010). Die Unterscheide zwischen den zwei Ansätzen sind in Tabelle 13 detailliert beschrieben. Da die Begrifflichkeit sich auch wesentlich unterscheiden, stellt Tabelle 12 diese Unterschiede dar. Die Erklärung der Begriffe aus der Systemanalyse ist in der Dokumentation von Bauhaus Luftfahrt, in der SiVe-Systemdokumentation (D'Avanzo, et al., 2010) und im Anhang A: Glossar zu finden.

Tabelle 12: Begriffsunterschiede zwischen der SiVe-Systemanalyse und PoC.

Systemanalyse	Beschreibung in der Systemanalyse	PoC
Szenario	Eine plausible Kombination von Bedrohungsaspekten, die eine konkrete Bedrohung der Flughafensicherheit zur Folge hat.	Situation Der Begriff ist übergreifend und beschreibt sowohl Bedrohungen als auch Lastsituationen.
Bedrohungsszenario	Kombinationen von Bedrohungsaspekten.	Bedrohungssituation

Systemanalyse	Beschreibung in der Systemanalyse	PoC
Domäne	In der Strukturanalyse beschreibt eine Domäne eine Gruppe gleichartiger Systemelemente in der Methodik der MDM.	Aspekt
Systemelement	Ein Element, das gemeinsam mit weiteren Systemelementen ein Bedrohungsszenario beschreiben kann. Wenn Systemelemente ein Bedrohungsszenario beschreiben bestehen Abhängigkeiten zwischen ihnen. Durch die Vernetzung mit weiteren nicht bedrohungsspezifischen Systemelementen ergibt sich die „strukturelle“ Wirksamkeit des Systems gegen das Szenario.	Aspektelement
Relation / Vernetzung zwischen Systemelementen	Abhängigkeit zwischen zwei Systemelementen.	Die Vernetzung zwischen Systemlast und Layout erfolgt durch eine situationsbezogene Quantifizierung von Schutzmechanismen, die wiederum mit den Prozesselementen des Layouts vernetzt werden.
Szenariobuilder	Methodik und Software-Werkzeug zur Bestimmung konsistenter, plausibler Bedrohungsszenarien aus Kombinationen von Bedrohungsaspekten.	Systemlast, bestehend aus Bedrohungs- und Lastsituationen.

Grundsätzlich ist der MDM-Ansatz für den PoC nicht geeignet, da sie statisch ist und nur strukturelle Abhängigkeiten zwischen den Aspekten und den Aspektelementen verfasst. Eine risiko- und kostenorientierte Analyse der Sicherheitsarchitekturen ist nach dem MDM-Ansatz nicht möglich. Beispielweise wäre die Vernetzung der Elemente aus der Systemanalyse (im SiVe-Szenariobuilder enthalten) mit den restlichen Modellierungsaspekten im Demonstrator ein Ansatz in dieser Richtung gewesen (gemäß der SiVe-Facharchitektur – s. Abbildung 12 auf Seite 41). Dieser wurde aber nicht weitgehend verfolgt.

Im PoC sind die Aspekte im Gegensatz zur SiVe-Systemanalyse unabhängig voneinander, da die Vernetzung erst mit dem Layout erfolgt. Dies ermöglicht die direkte Anbindung der Situationsmodellierung in der Bewertung einer Sicherheitsarchitektur gegen eine Systemlast.

Tabelle 13: Unterschiede zwischen dem MDM-Ansatz der Systemanalyse von BHL und dem PoC-Situationsmetamodell.

SiVe-Systemanalyse / MDM-Ansatz	PoC-Situationsmodellierung
Fokus auf Bedrohungssituationen (Bedrohungsszenarien benannt), daher passt es zum „**What-if-Szenario**“-Ansatz des SiVe-Demonstrator. Die Lastsituationen, die Kosten verursachen, werden nicht berücksichtigt.	Es werden sowohl Bedrohungs- als auch Lastsituationen für die Bildung von Systemlasten modelliert.

SiVe-Systemanalyse / MDM-Ansatz	PoC-Situationsmodellierung
Aspekte und Elemente (Domäne und Systemelemente) werden „logisch“ miteinander vernetzt (d.h. nach dem Prinzip ist vernetzt / ist nicht vernetzt). Die Abhängigkeit zwischen den Elementen ist daher statischer Natur und der Informationsgewinn über das System ist nur struktureller Art. Informationen über die „Stärke“ (Quantifizierung) einer Vernetzung fehlen. Beispielweise liefert die Schwachstellenanalyse nur Informationen über die **strukturelle Wirksamkeit** (nicht quantitativ) von Schutzmechanismen (d.h. welche und wie viele Schutzmechanismen gegen welche Bedrohungsszenarien wirken). Informationen über die Sicherheitsperformance des Systems fehlen. Die logische Vernetzung im MDM schließt mögliche Situationen aus, die rein theoretisch nicht vorkommen dürfen, die aber Kosten verursachen können, wenn sie wirkliche vorkommen.	Systemelemente sind voneinander unabhängig. Im PoC erfolgt eine Vernetzung zwischen Systemlast und Layout erst wenn das Layout modelliert und in die Anwendung hochgeladen ist. Diese erfolgt über die situationsbezogene Quantifizierung der Prozesselemente.
Die Vernetzung zwischen Elementen erfolgt bereits in der Systemanalyse.	Die Vernetzung erfolgt erst wenn ein Layout modelliert und hochgeladen ist (situationsbezogene Quantifizierung der Prozesselemente).
Die Systemanalyse ist layoutabhängig und daher nicht portabel. Layoutinformationen sind bereits in der Systemanalyse enthalten. Eine Änderung im Layoutmodell (z.B. Prozess- bzw. Infrastrukturänderung) erfordert / kann erfordern eine Änderung bzw. Neuerstellung der Systemanalyse.	Situationsmetamodell und Aspektelemente sind unabhängig vom Layout und sind portabel (anwendbar für andere Verkehrsinfrastrukturen). Eine Änderung des Layouts erfordert keine Änderung der Systemanalyse. Wenn durch die Layoutänderung neue Schutzmechanismen angewendet werden sollen, dann sind nur diese situationsbezogen zu quantifizieren.
Umfangreiche Datenerfassung mit Aufnahme der Domäne und Elemente und deren Vernetzung.	Geringer Aufwand bei der Datenerfassung, da nur Elemente für die Beschreibung der Aspekte erfasst werden müssen. Die Vernetzung erfolgt erst später bei der Quantifizierung.
Eine Erweiterung der Domäne und Elemente ist möglich. Dabei müssen die neue Domäne und Elemente logisch vernetzt werden.	Eine Erweiterung der Aspekte und Aspektelemente ist möglich bereits im PoC. Die neuen Elemente werden automatisch über die Situationen mit dem Layout vernetzt.
Für andere Verkehrsinfrastrukturen ist die Systemanalyse neu zu erstellen (sowohl Domäne als auch Systemelemente).	Für andere Verkehrsinfrastrukturen sind nur die Aspektelemente (Dateninhalte) anzupassen.
Die Integration des Szenariobuilders im SiVe-Demonstrator erfolgt über eine lose Datenschnittstelle (lose Kopplung). Dabei werden die vernetzten Prozesse (aus der Prozesslandkarte) nach der Szenariobildung gesamthaft ermittelt. Die Prozessmodelle sind aber unabhängig von der Systemanalyse. Das Verhalten der einzelnen Prozesselemente eines Prozessmodells gegen das Szenario wird nicht berücksichtigt.	Das PoC-Situationsmodell ist im PoC vollintegriert.

SiVe-Systemanalyse / MDM-Ansatz	PoC-Situationsmodellierung
Die Integration erfolgt nur auf Datenebenen zwischen Szenariobuilder und Prozessmodellierung (Mapping zwischen Systemelemente und Prozessmodelle). Ein übergreifendes Metamodell sowie eine Schnittstelle zu den anderen Modellierungsansätzen (z.B. logistische Simulation) fehlen.	Vollintegration im PoC.
Die Datenanalyse und –erfassung erfolgt erst in Excel. Die Daten werden dann in den Szenariobuilder importiert.	Vollintegriert im PoC. Die Elemente können auch erst im Excel erfasst werden und in den PoC importiert werden.
Die Strukturanalyse ist statisch und kann nur als Checkliste bei der Szenariobildung verwendet werden. Für szenariobasierte Prozesssimulationen (Ziel von SiVe) kann die aktuelle Strukturanalyse mittels MDM nur die Ausgangssituation einer Simulationsstudie ermitteln und definieren (Anfangswerte des Systems).	—
Die Systemelemente sind für die Bedatung kaum nutzbar. Im SiVe-Demonstrator erfolgt die Quantifizierung von Prozesselementen erst in der stochastischen / probabilistischen Modellierung und ist unabhängig von der Systemanalyse.	Die Quantifizierung der Schutzmechanismen erfolgt situationsbezogen und dient zur Vernetzung zwischen Last und Layout (durch das Mapping der Schutzmechanismen mit den Prozesselemente).
Die Vernetzung der Systemelemente (innerhalb des Szenariobuilders) erfolgte subjektiv (das Problem ist, dass die „Subjektivität“ bereits in der Modellierung versteckt wird und nicht nur in der Bedatung)	Die Vernetzung zwischen Systemlast und Layout erfolgt subjektiv während der situationsbezogene Quantifizierung der Schutzmechanismen.
Hoher Aufwand bei der Datenerhebung. Die ist auf der Datenerfassung und logischen Vernetzung aller Systemelemente zurückzuführen.	Geringer Aufwand bei der Datenerfassung, da nur die Aspektelemente erfasst werden. Die Vernetzung erfolgt erst später.
Die Szenarien sind zu abstrakt gegenüber der Detaillierung der Prozess-/logistischen/stochastischen Modelle. Diese Abstraktion findet sich wieder in den Details der Modellierungen; eine Hierarchisierung ist aber nicht gegeben und nicht möglich.	—
Problem der Durchgängigkeit Die Systemanalyse beinhaltet als Systemelemente Schutzmechanismen, die sich nur teilweise in den weiteren Modellierungen wieder finden (die Modellierung auf Metaebene passen nicht wirklich zusammen). Außerdem sind die Modelldetaills der verschiedenen Modellierungen im Demonstrator nicht immer passend zwischen einander auf Grund der fehlenden Metamodellierung.	Vollintegration und Integration im PoC.

Die Situationsaspekte werden mit Inhalt gefüllt (Aspektelemente). Interviews und Workshops mit Interessenten sind dafür erforderlich. Sie können direkt im PoC eingegebenen und verwaltet werden oder erst im Excel gesammelt und über eine standardisierte Schnittstelle in den PoC übernommen werden.

Aspektelemente der Situationen

Für SiVe wurden die Situationsaspekte mit folgenden Inhalten aus Literatur und aus dem Teilvorhanden von Bauhaus Luftfahrt gefüllt.

Tabelle 14: Kategorie.

Kategorie	**Bemerkung**
Kein Täter (Pax, Beschäftigte, usw.)	Last
Passagier	Last
Beschäftigte	Last
Besucher	Last
Terrorist	Bedrohung
Gewöhnliche Kriminelle	Bedrohung

Tabelle 15: Ziele.

Ziele / Ende	**Bemerkung**
Keine	
Menschen / Menschenleben	
Flugzeug In der Luft	
Flugzeug Am Boden	
Allgemein zugänglicher Bereich	Menschen und Sachschaden
Nicht allgemein zugänglicher Bereich	Menschen und Sachschaden
Sicherheitsempfindlicher Bereich	Menschen und Sachschaden
Flughafen-Frachtterminal	
Flughafen-Tower	
Flughafen-Treibstofflager	
Vorfeld	
Flughafen-Wartungsanlagen	
Kommunikationssystem-Boden-Luft	
IT (Buchungssystem, usw.)	
Flughafen Infrastruktur	
Ende, Festnahme	Dafür sollte eine eigene Tabelle definiert werden.

Tabelle 16: Motivation / Absichten.

Motivation / Absichten	**Bemerkung**
Keine	
Wirtschaftlicher Schaden	
Menschenleben	
Aufmerksamkeit	
Angst, Demoralisieren	

Tabelle 17: Objekt.

Objekt	**Bemerkung**
Keines	
Nicht erlaubter Gegenstand	

Objekt	Bemerkung
Verbotener Gegenstand	
Kleidung, Schmuck	
Sprengstoff klassifizierbar	
Stichwaffen klassifizierbar	
Schusswaffen klassifizierbar	
Abstandswaffe klassifizierbar	
Sportgeräte	
Alltagsgegenstände klassifizierbar	
Schlagwaffen klassifizierbar	
Sprengstoff unklassifiziert	
Stichwaffen unklassifiziert	
Schusswaffen unklassifiziert	
Abstandswaffe unklassifiziert	
Radiologisch unklassifiziert	
Biologisch unklassifiziert	
Chemisch unklassifiziert	
Schallwaffe unklassifiziert	

Tabelle 18: Einbringungsart.

Einbringungsart	Bemerkung
Keine	
Am Körper	
Im Körper	
Im Handgepäck	
Im Reisegepäck	
Über Luftfracht	
Über Luftpost	
Über Catering	
Über nicht kontrollierbare Lieferungen	
Im Flugzeug	

Tabelle 19: Einfallsweg.

Einfallsweg	Bemerkung
Kein	
Straße	Derzeit unterscheidet sich von Schiene nicht.
Schiene	Derzeit unterscheidet sich von Straße nicht.
Luft-Unterschiedliches Sicherheitsniveau	
Luft-Mit gleichem Sicherheitsniveau	
Umland	
Landside	

Nachstehend sind Beispiele für eine Bedrohungssituation (Tabelle 20) und eine normale Lastsituation (Tabelle 21). Beispielweise fasst die Bedrohungssituation in Tabelle 20 alle

möglichen Szenarien zusammen, die mit den ausgewählten Aspekt-Elementen definierbar sind, wie jeder Art vom flüssigen Sprengstoff und jede Hohe und Art von wirtschaftlichen Schäden.

Tabelle 20: Sprengstoff-Bedrohungssituation.

Lastszenario: BS: Renegade mit Sprengstoff am Körper	
Kategorie:	Terrorist
Absichten/Motivation:	Wirtschaftlicher Schaden
Objekt:	Sprengstoff unklassifiziert
Einfallsweg:	Straße
Einbringungsart:	Am Körper
Nutzung/Angriffsziele:	Flugzeug-In der Luft

Tabelle 21: Normale Passagiere, der über die Straße kommt und abfliegen möchte.

Lastszenario: LS: Normale Paxe	
Kategorie:	Passagier
Absichten/Motivation:	Keine
Objekt:	Keines
Einfallsweg:	Straße
Einbringungsart:	Keine
Nutzung/Angriffsziele:	Flugzeug-In der Luft

Im PoC ist es vorgesehen, alle möglichen Situationen zu erfassen und in eine Datenbank abzuspeichern (Situationsdatenbank). Die Tabelle 22 stellt sämtliche Beispiel-Situationen dar. Die Situationsdatenbank ist eine Sammlung aller möglichen Last- und Bedrohungssituationen, die vorgekommen sind (Historische Fälle) bzw. vorkommen könnten, und steht für die Bildung der Systemlasten zur Verfügung (Wiederverwendbarkeit).

Tabelle 22: Sämtliche Last und Bedrohungssituationen im PoC erfasst.

Situationen	B/L	Beschreibung	Kategorie	Ziel	Absichten / Motivation	Objekt	Einbringungs-art	Einfalls-weg
Gewöhnliche Kriminelle mit EMP-Waffe	B		Gewöhnliche Kriminelle	Flughafen-Sicherheits-empfindlicher Bereich	Menschenleben	EMP-Waffen klassifizierbar	Am Körper	Straße
Innentäter mit flüssigem Sprengstoff am Körper	B		Beschäftigte	Flugzeug-In der Luft	Menschenleben	Sprengstoff unklassifiziert	Am Körper	Straße
Innentäter mit flüssigem Sprengstoff im Hangepäck	B		Terrorist	Flugzeug-In der Luft	Menschenleben	Sprengstoff unklassifiziert	Im Handgepäck	Straße
Innentäter mit Schusswaffe am Körper	B		Beschäftigte	Flugzeug-In der Luft	Wirtschaftlicher Schaden	Schusswaffen klassifizierbar	Am Körper	Straße
Innentäter mit Schusswaffe im Handgepäck	B		Terrorist	Flugzeug-In der Luft	Menschenleben	Schusswaffen unklassifiziert	Im Handgepäck	Straße
Reisegepäck: flüssiger Sprengstoff, Flugzeug am Boden 2	B		Terrorist	Flugzeug-Am Boden	Wirtschaftlicher Schaden	Sprengstoff unklassifiziert	Im Reisegepäck	Straße
Reisegepäck: Sprengstoff, Flugzeug am Boden	B		Terrorist	Flugzeug-Am Boden	Wirtschaftlicher Schaden	Sprengstoff unklassifiziert	Im Reisegepäck	Schiene
Renegade mit Sprengstoff am Körper	B		Terrorist	Flugzeug-In der Luft	Wirtschaftlicher Schaden	Sprengstoff unklassifiziert	Am Körper	Straße

Situationen	B/L	Beschreibung	Kategorie	Ziel	Absichten / Motivation	Objekt	Einbringungs-art	Einfalls-weg
Renegade Terrorist (mit Kampftechniken ausgebildet)	B		Terrorist	Flugzeug-In der Luft	Aufmerksamkeit	Werkzeuglos unklassifiziert	Im Körper	Straße
Sabotage mit flüssigem Sprengstoff im Hangepäck	B		Terrorist	Flugzeug-In der Luft	Menschenleben	Sprengstoff unklassifiziert	Im Handgepäck	Straße
Sabotage mit Waffe am Körper	B		Terrorist	Flugzeug-In der Luft	Menschenleben	Schusswaffen unklassifiziert	Am Körper	Straße
Sprengstoff am Körper	B		Terrorist	Flugzeug-In der Luft	Wirtschaftlicher Schaden	Sprengstoff unklassifiziert	Am Körper	Straße
Sprengstoff am Körper, Einfallsweg Straße	B		Terrorist	Flugzeug-In der Luft	Wirtschaftlicher Schaden	Sprengstoff unklassifiziert	Am Körper	Straße
Sprengstoff im Handgepäck	B		Terrorist	Flugzeug-In der Luft	Menschenleben	Sprengstoff unklassifiziert	Im Handgepäck	Straße
Sprengstoff über Schiene eingebracht	B		Terrorist	Flugzeug-In der Luft	Wirtschaftlicher Schaden	Sprengstoff unklassifiziert	Am Körper	Schiene
nicht erlaubte Gegenstände im Handgepäck	L		Passagier	Flugzeug-In der Luft	Keine	Nicht erlaubter Gegenstand	Im Handgepäck	Straße
Normale Pax mit Alltagsgegenständen im Handgepäck	L		Passagier	Flugzeug-In der Luft	Keine	Alltagsgegenstände klassifizierbar	Im Handgepäck	Straße

Situationen	B/L	Beschreibung	Kategorie	Ziel	Absichten / Motivation	Objekt	Einbringungs-art	Einfalls-weg
Normale Pax mit Flüssigkeit am Körper	L		Passagier	Flugzeug-In der Luft	Keine	Nicht erlaubter Gegenstand	Keine	Straße
Normale Pax mit Flüssigkeit im Handgepäck	L		Passagier	Flugzeug-In der Luft	Keine	Nicht erlaubter Gegenstand	Im Handgepäck	Schiene
Normale Pax mit nicht erlaubten Gegenständen am Körper	L		Passagier	Flugzeug-In der Luft	Keine	Nicht erlaubter Gegenstand	Am Körper	Schiene
Normale Pax mit nicht erlaubten Gegenständen im Handgepäck	L		Passagier	Flugzeug-In der Luft	Keine	Nicht erlaubter Gegenstand	Im Handgepäck	Straße
Normale Pax mit verbotenen Gegenständen am Körper	L		Passagier	Flugzeug-In der Luft	Keine	Verbotener Gegenstand	Am Körper	Straße
Normale Paxe	L		Passagier	Flugzeug-In der Luft	Keine	Keines	Keine	Straße
Normale Paxe mit verbotenen Gegenständen im Handgepäck (Schiene)	L		Passagier	Flugzeug-In der Luft	Keine	Verbotener Gegenstand	Im Handgepäck	Schiene
Normale Paxe mit verbotenen Gegenständen im Handgepäck (Straße)	L		Passagier	Flugzeug-In der Luft	Keine	Verbotener Gegenstand	Im Handgepäck	Straße
Reisegepäck: Kleidung, Schmuck	L		Passagier	Flugzeug-Am Boden	Keine	Kleidung, Schmuck unklassifiziert	Im Reisegepäck	Straße

Situationen	B/L	Beschreibung	Kategorie	Ziel	Absichten / Motivation	Objekt	Einbringungs-art	Einfalls-weg
Reisegepäck: nicht erlaubte Gegenstände	L		Passagier	Flugzeug-Am Boden	Keine	Nicht erlaubter Gegenstand	Im Reisegepäck	Straße
Reisegepäck: Verbotener Gegenstand	L		Passagier	Flugzeug-Am Boden	Keine	Verbotener Gegenstand	Im Reisegepäck	Straße

Systemlast

Eine Systemlast definiert sich als **gewichtete und quantifizierte Zusammenstellung relevanter Situationen eines Systems**. Dieser wird gezielt für eine Berechnung verwendet. Die Last ist unabhängig vom Layout: Die gleiche Systemlast kann mit unterschiedlichen parametrisierten Layoutmodellen vernetzt werden, um beispielweise deren Sicherheitsperformance zu vergleichen. Auf der anderen Seite kann für ein definiertes/spezifisches Layout die Belastung variiert werden (unterschiedliche Systemlasten), um das Verhalten des Layouts zu analysieren und bewerten.

Die Situationen einer Systemlast werden gemäß Tabelle 23 quantifiziert. Aus der Häufigkeit / Jahr ergibt sich das gesamte Volume / Jahr der Systemlast. Für Bedrohungssituationen sind zusätzlich die Schadenarten Personenschaden, Sachschaden und Folgeschaden (als Mittelwert, falls die Situation eintritt) einzugeben. Die Schadenarten können erweitert werden (derzeit nur durch programmtechnischen Änderungen).

Tabelle 23: Quantifizierung der Situationen eine Systemlast.

Variable	Beschreibung
Häufigkeit / Jahr	• Anzahl der Fälle / Jahr
Menschenleben / Jahr	• Schadensart Personenschaden: Anzahl der Tote / Fall (Mittelwert) • Nur bei Bedrohungssituationen
Sachschaden (€ / Jahr)	• Schadensart Sachschaden: Wertverlust durch Beschädigung, Zerstörung oder Verlust der Sache. Folgeschäden fließen in den wirtschaftlichen Schaden ein: € / Fall (Mittelwert). • Nur bei Bedrohungssituationen
Wirtschaftliche Schaden (€ / Jahr)	• Schadensart wirtschaftliche Schaden: Folgeschaden durch das Eintreten eines Schadenereignisses als indirekte finanzielle Folgen in der Luftfahrtindustrie und Wirtschaft: € / Fall (Mittelwert). • Nur bei Bedrohungssituationen

Im PoC sind Systemlast und Layout im jetzigen Entwicklungsstadium unabhängig voneinander. Eine Layoutänderung kann aber Einfluss auf die Last haben (Rückkopplung). Um beispielweise die Sicherheit zu erhöhen, werden zusätzliche und strengere Maßnahmen eingeführt (höhere Kosten). Durch diese Änderung werden auch sämtlichen Bedrohungssituationen möglicherweise nicht mehr geschehen (geringere Restrisiken). Es stellt sich die Frage: Werden diese Änderungen von den Passagieren akzeptiert (aus ethischen oder Kostengründen)? Die Layoutänderung beeinflusst die Häufigkeit / Jahr jeder Situation (Einfluss auf Kosten und Umsatz).

Tabelle 24 zeigt ein Beispiel einer Systemlast mit einem Gesamtvolumen von ca. 40.200.000 Objekten (Personen ohne Gepäck), die durch die Kontrollen im Systemlayout durchgehen.

Tabelle 24: Beispiel einer Systemlast.

Lastsituation	B/L	Häufigkeit / Jahr	Menschen-Leben /Jahr	Sachschaden (€/Jahr)	Wirtschaftl. Schaden (€/Jahr)
Innentäter mit Schusswaffe am Körper	B	1,00	10.0	10.000.000 €	100.000 €
Renegade mit Sprengstoff am Körper	B	0,10	300.0	100.000.000 €	100.000.000 €

Lastsituation	B/L	Häufigkeit / Jahr	Menschen-Leben /Jahr	Sachschaden (€/Jahr)	Wirtschaftl. Schaden (€/Jahr)
Renegade Terrorist (mit Kampf-techniken ausgebildet)	B	0,10	150.0	100.000.000 €	100.000.000 €
Sabotage mit Waffe am Körper	B	0,05	500.0	200.000.000 €	200.000.000 €
Sprengstoff am Körper	B	0,50	150.0	100.000.000 €	100.000.000 €
Sprengstoff am Körper, Einfallsweg Straße	B	0,10	250.0	100.000.000 €	100.000.000 €
Normale Pax mit Flüssigkeit am Körper	L	34.200.000,00	–	–	–
Normale Pax mit verbotenen Gegenständen am Körper	L	5.000.000,00	–	–	–
Normale Pax	L	1.000.000,00	–	–	–

Vernetzung zwischen Systemlast und Layout

Um eine Berechnungsstudie durchzuführen, sind Systemlast und Layout zu vernetzen. Die Grundidee ist die folgende.

Zum einen werden die Prozesselemente des Layoutmodells (Tasks) mit situationsbezogenen quantifizierten Schutzmechanismen gemappt (**indirekte Vernetzung**) und zum anderen werden die Start- und End-Ereignisse mit den Mappingaspekten Ziel und Einfallsweg direkt vernetzt (**direkte Vernetzung**).

Die direkte Vernetzung dient zur Aktivierung der Situationen im Layout. Beinhaltet beispielweise die Last eine Situation mit einem Angriffsziel, das im Layout nicht definiert ist, so wird die Situation für die Berechnung nicht „aktiviert“ und nicht berücksichtigt.

Die indirekte Vernetzung dient zur Risiko- und Kostenberechnung aufgrund der situationsbezogenen Quantifizierung der Prozesselemente, die mit Schutzmechanismen gemappt werden.

Das folgende Beispiel erläutert besser das Konzept. Nehmen wir eine Last mit nur einer Situation, beispielweise die Bedrohungssituation aus der Tabelle 20 auf (Sprengstoff-Situation) und das Personenabfertigung-Layoutmodell in der Abbildung 16. Das Layout besteht aus Prozesselemente und alle möglichen Prozessabläufe zwischen den Start- und End-Ereignissen (Sicherheitsarchitektur der Tabelle 9). Die ausgewählte Situation kann erst vom Layout aktiviert werden, wenn sie durch das Layout durchlaufen kann und wenn sie sämtliche Prozesselemente aktiviert:

1. **Aktivierung von Prozessinstanzen**:
   Um Prozessabläufe eines Layouts aktivieren zu können, müssen die Mappingaspekte **Einfallsweg** (Startereignis) und **Ziel** (Endereignis) einer Situation im Layout definiert sein: Der Start-Knoten im Layout wird mit dem Einfallsweg „Straße“ und das Endereignis im Layout mit dem Ziel „Flugzeug in der Luft“ gemappt. Das Layout wird von der Situation durch eine **direkte Vernetzung** aktiviert.
2. **Aktivierung von Prozesselementen**:
   Um ein Prozesselement einer Prozessinstanz aktivieren zu können, müssen der

Situationsaspekt **Einbringungsart** und die Prozesseigenschaft **Objekttyp** miteinander gemappt werden. Wenn das Objekt beispielweise am Körper eingebracht wird, dann sind nur Prozesselemente relevant, die die Personen/Körper kontrollieren. Das Prozesselement wird von der Situation durch eine **direkte Vernetzung** aktiviert.

3. **Situationsbezogene Quantifizierung der Schutzmechanismen**:
   Durch das Mapping zwischen Prozesselementen des Layouts mit Schutzmechanismen, die situationsbezogen quantifiziert werden (Eingabe der Falsch Alarm Rate und Falsch Clear Rate) fließen die vom Layout aktivierten Situationen in die Wahrscheinlichkeitsberechnung ein (Risiko- und Kostenrechnung - **Indirekte Vernetzung**).

Tabelle 25: Mapping zwischen dem Situationsaspekt Einbringungsart und die Prozesseigenschaft Objekttyp.

Eibringungsart	Objekttyp
Luftfracht	Luftfracht
Keine	Person (die Person wird immer „kontrolliert“)
Am Körper	Person Person+Handgepäck Person+Reisegepäck
Im Körper	Person Person+Handgepäck Person+Reisegepäck
Im Handgepäck	Handgepäck Person+Handgepäck
Im Reisegepäck	Reisegepäck Person+Reisegepäck
Luftpost	Luftpost
Catering	Flughafenlogistik

Die direkten Vernetzungen erfolgen automatisiert auf Basis der erfassten Situationen und Layoutmodells im Hintergrund in der PoC-Berechnugsengine. Abbildung 21 zeigt für das Layoutmodell der Abbildung 16 die Erfassung der direkten Vernetzungen mit Objekttyp, Einfallsweg und Ziele. Aus diesem Beispiel ist klar, welche Situationen aktiviert werden.

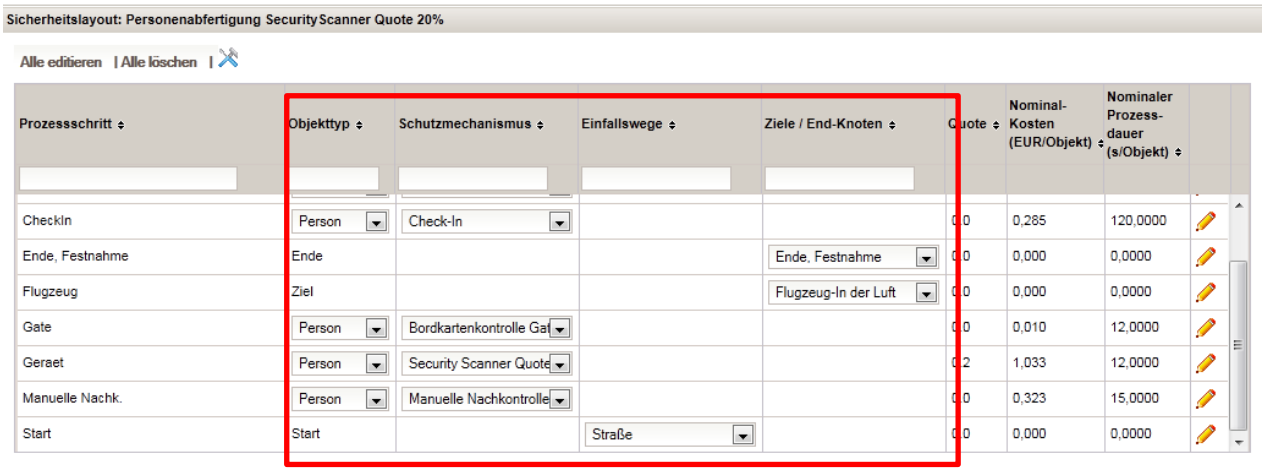


Abbildung 21: Erfassung der Vernetzung.

Die indirekte Vernetzung über die Schutzmechanismen verantwortet die Wirksamkeit der einzelnen Prozesselemente für jede Situation.

Tabelle 26 fasst die Vernetzung zwischen Systemlast und Layout tabellarisch zusammen.

Spalte	Beschreibung
Objekttyp	• Direkte Vernetzung zwischen Prozesselement/Objekttyp und Situation/Einbringungsart. • Ein Prozesselement ist für die Untersuchung/Kontrolle gezielter Objekten gedacht (Personen, Handgepäck, Reisegepäck, usw.). Der Objekttyp kennzeichnet damit das Prozesselement. Nur die Situationen der Systemlast mit passender Einbringungsart aktivieren das Prozesselement.
Schutzmechanismus	• Indirekte Vernetzung zwischen Prozesselementen und Situationen. • Ein Prozesselement wird mit einem Schutzmechanismus zugeordnet. Diese Zuordnung stellt die indirekte Vernetzung dar: Das zugeordnete Schutzmechanismus ist situationsbezogen mit Alarm- und Clear-Raten quantifiziert.
Start-Knoten	• Direkte Vernetzung zwischen Layout/Start-Ereignis und Situation/Einfallsweg. • Ein Start-Ereignis im Layout wird mit dem Situationsaspekt Einfallsweg zugeordnet.
Ziele / End-Knoten	• Direkte Vernetzung zwischen Layout/End-Ereignis und Situation/Ziel. • Ein End-Ereignis im Layout wird mit dem Situationsaspekt Ziel zugeordnet.

Tabelle 26: Vernetzung zwischen Systemlayout und Layout.

Berechnungsmodell

In diesem Kapitel werden die die Wahrscheinlichkeitstheorie und probabilistische Modellierung für die Risiko- und Kostenberechnungen beschrieben, die in die PoC-Berechnungsengine umgesetzt wurden. Die Grundlagen der Berechnung bilden die klassische und die bayesche Wahrscheinlichkeitstheorie und sind im (Singpurwalla, 2006) zu finden.

Wahrscheinlichkeitsberechnung

Sei Z_j eine Situation j, wobei $Z_j = 0$ eine Lastsituation und $Z_j = 1$ eine Bedrohungssituation definiert.

Sei X_j der Alarmstatus der Situation Z_j, wobei $X_j = 0$ den Clear-Status (System Clear) und $X_j = 1$ den Alarm-Status (System Alarm) für ein Layout (gesamthaft) definieren.

Dann ist $P_j(X_j|Z_j)$ die gesamthafte Wahrscheinlichkeit der Situation *j*, dass das Systemlayout einen Alarmstatus X_j unter der Bedingung der Situation Z_j (Bedrohung/Last) auslöst:

$$P_j(X_j|Z_j) = P_j^{Z_j}(1-P_j)^{1-Z_j}\sum\nolimits_{\Omega_{lj}}\left[\prod\nolimits_i\left(a_{ji}^{1-Z_j}\, b_{ji}^{Z_j}\right)\right] \qquad (1)$$

wobei

- j: *eine Situation;*
- i: *ein Prozesselement;*
- l: *eine Prozessinstanz;*
- P_j: *die Wahrscheinlichkeit, dass die Situation j eine Bedrohung ($P_j = 1$) bzw. eine normale Last ($P_j = 0$) ist;*
- Ω_{lj}: *die Menge $\{i\}_{lj}$ aller „aktivierten" Prozesselemente i der Instanz l für die Situation j. Die „Aktivierung" des Prozesselements i erfolgt aufgrund der Vernetzung zwischen Situation j und Layout.*

Formel (1) ergibt sich aus *Abbildung 19*. Die Summenbildung $\sum_{\Omega_{lj}}[\bullet]$ bedeutet, dass jede Situation *j* über alle aktivierten Prozessinstanzen Ω_{lj} berechnet und aufaddiert wird.

Für jede Situation *j* und Prozesselement *i* definieren sich in Formel (1):

$$\begin{aligned} a_{ji} &= a_{ji}(x_i) = \left[\alpha_{ji} + q_i(1-\alpha_{ji})\right]^{x_i}\left[(1-\alpha_{ji})(1-q_i)\right]^{1-x_i} \\ b_{ji} &= b_{ji}(x_i) = \left[\beta_{ji}(1-q_i)\right]^{1-x_i}\left[(1-\beta_{ji}) + q_i\beta_{ji}\right]^{x_i} \end{aligned} \qquad (2)$$

wobei

- α_{ji}: *„False-Alarm-Rate" für die Situation j und das Prozesselement i;*
- β_{ji}: *„False-Clear-Rate" für die Situation j und das Prozesselement i;*
- q_i: *Quote des Prozesselements i (situationsunabhängig);*
- x_i: *Alarmstatus des Prozesselements i (situationsunabhängig);*

In Formel (1) ist der Faktor a_{ji} der „Alarm"-Anteil der Wahrscheinlichkeit den Durchkommens durch das Prozesselement *i* für die Situation *j*. Analog ist der Faktor b_{ji} den „Clear"-Anteil der Wahrscheinlichkeit den Durchkommens durch das Prozesselement *i* für die Situation *j*.

Ohne Quote ($q_i = 0$) reduziert sich Formel (2) in:

$$a_{ji} = a_{ji}(x_i) = \alpha_{ji}^{x_i}\left(1-\alpha_{ji}\right)^{1-x_i}$$
$$b_{ji} = b_{ji}(x_i) = \beta_{ji}^{1-x_i}\left(1-\beta_{ji}\right)^{x_i} \quad (3)$$

Formel (1) zeigt, wie der Alarm-/Clearstatus vom Layout abhängt, und beinhaltet folgende Fälle:

- False Clear: $P_j\left(X_j = 0 \middle| Z_j = 1\right)$ ist die Wahrscheinlichkeit, dass die Bedrohungssituation ($Z_j = 1$) erfolgreich ($X_j = 0$) das Ziel erreicht.
- True-Alarm: $P_j\left(X_j = 1 \middle| Z_j = 1\right)$ ist die Wahrscheinlichkeit, dass die Bedrohungssituation ($Z_j = 1$) entdeckt wird ($X_j = 1$).
- True-Clear: $P_j\left(X_j = 0 \middle| Z_j = 0\right)$ ist die Wahrscheinlichkeit, dass die Lastsituation ($Z_j = 0$) erfolgreich ($X_j = 0$) das Ziel erreicht.
- False Alarm: $P_j\left(X_j = 1 \middle| Z_j = 0\right)$ ist die Wahrscheinlichkeit, dass die Lastsituation ($Z_j = 0$) nicht zum Ziel kommt ($X_j = 1$).

Risikoberechnung

Anhand der Formel (1) können die Restrisiken eines Layouts für eine Systemlast berechnen als:

$$R_s = \sum\nolimits_j P_j\left(Z_j \middle| X_j\right) S_{js} \quad (4)$$

wobei ist S_{js} das Schadenausmaß (Mittelwert) von Schadensart *s* der Situation *j*. Formel (4) gilt unter der Annahme, dass alle Situationen der Last unabhängig voneinander sind (realistisch).

Kostenrechnung

Die Kosten eines Layouts für eine definierte Systemlast errechnet sich als Summe über alle Prozesselemente *i* des Layouts und alle Situationen *j* der Systemlast als:

$$K = \sum\nolimits_{ji} N_{ji,input} k_i = \sum\nolimits_j \left\{ \sum\nolimits_i \left[N_{ji,input} k_i \right] \right\}$$
$$= \sum\nolimits_j \left\{ N_j \sum\nolimits_i \left[k_i \sum\nolimits_{\left\{ \begin{smallmatrix} \text{unmittelbare vorherige} \\ \text{Prozessschritte des} \\ \text{Prozesselements } i \end{smallmatrix} \right\}} p_{jl} \right] \right\} \quad (5)$$

wobei

j: *die Situation j;*
i: *das Prozesselement i in der Summe;*
N_j: *die Häufigkeit der Situation j;*
$N_{ji,input}$: *die Input-Häufigkeit in das Prozesselement i aus allen unmittelbaren vorherigen Prozessschritten:* $N_{ji,input} = N_j \sum_{l,i} p_{jl}$

p_{jl}: *die Input-Wahrscheinlichkeit der Situation j in das Prozesselement i aus dem unmittelbaren vorherigen Prozessschritt l:*

$$p_{jl}(x_l) = p_j\left[\beta_{jl}(1-q_l)\right]^{1-x_l}\left[\left(1-\beta_{jl}\right)+q_l\beta_{jl}\right]^{x_l} + \left(1-p_j\right)\left[\alpha_{jl}+q_l(1-\alpha_{jl})\right]^{x_l}\left[(1-\alpha_{jl})(1-q_l)\right]^{1-x_l}$$

wobei p_j, x_l, α_{jl}, β_{jl} bereits oben definiert worden sind.

k_i: *die Nominalkosten des Prozesselements i pro kontrolliertes Objekt:*

$$k_i = \frac{k_{i,fix}}{d_i h_i} + k_{i,op}$$

wobei für jedes Prozesselements i ist:

$k_{i,fix}$*: fixe Kosten / Jahr, wie Anschaffung, Wartung usw.;*

d_i: *Durchsatz als Anzahl zur kontrollierende Objekte / Std.;*

h_i: *Anwendungszeit, Std. / Jahr;*

$k_{i,op}$: *Anwendungskosten / Objekt.*

II.1.4. *SIMULATIONS-STUDIEN*

Das Ziel der Simulationsstudien ist der Nachweis der Erreichung der Projektziele, d.h. Durchführung einer Kosten-Nutzen-Analyse von Sicherheitssystemen vor dem Hintergrund einer definierten Bedrohungslage. Ziel der nachfolgenden Experimente ist es, diesen Nachweis zu erbringen. Bei der Durchführung der Experimente gilt generell, dass bei der Untersuchung bzw. Berechnung von Schäden und Durchkommenswahrscheinlichkeiten ausschließlich der Täter und keine Passagiere betrachtet werden. Bei der Kostenberechnung (im Sinne von Abfertigungskosten) hingegen werden ausschließlich Passagieren und kein Täter betrachtet. Für jede Betrachtungsgröße im Experiment, also z.B. Schaden, Durchkommenswahrscheinlichkeit des Täters oder Abfertigungskosten, werden jeweils eigenen Vignetten definiert. Vignetten strukturieren also das Experiment nach den Berechnungsgrößen. Eine Vignette kann wiederum in Subvignetten untergliedert werden, wobei in jeder Subvignette ein spezifischer Simulationsparameter variiert wird.

Die Experimente wurden von CASSIDIAN und EADS-IW definiert, simuliert und analysiert. Eine Mitarbeit der anderen Projektpartner erfolgte nur in sehr geringem Umfang. Die Ergebnisse von Experiment 1 und 2 wurden auf wissenschaftlichen Konferenzen publiziert.

Der erste Schritt bei der Durchführung der Experimente bestand in der Entwicklung einer generischen Vorlage zur umfassenden Beschreibung von Experimenten. Diese liegt den nachfolgenden Experimentbeschreibungen zu Grunde.

Experiment 1

Hauptziel des ersten Experiments ist der Nachweise der Durchgängigkeit und vollständigen Integration der unterschiedlichen Software-Werkzeuge im SiVe-Demonstrator. Im Rahmen des Experiments soll untersucht werden, wie sich eine Stichprobenkontrolle bei der Passagierkontrollstelle am Flughafen auf den Nutzen und die Kostenstruktur auswirkt. Als Berechnungsgrößen werden der Schaden durch einen Täter, die Durchkommenswahrscheinlichkeit des Täters und die Abfertigungskosten der Passagiere bei unterschiedlicher Ausprägung der Stichprobenwahrscheinlichkeit betrachtet.

Experiment-Beschreibung

Nachfolgend eine kurze Zusammenfassung der Experimentbeschreibung.

Kurzbeschreibung

Angriff durch einen Selbstmordattentäter mit einem selbstgebauten Sprengsatz. In der Simulation des Szenarios soll untersucht werden, wie sich eine Variation der Rate von stichprobenartigen Personenkontrollen (Quote) bei der Passagierkontrolle im Hinblick auf die Sicherheit und die Kostenstruktur auswirkt.

Fragestellungen

- Welche Veränderungen auf die Messgrößen ergeben sich durch eine Variation der Quote in Bezug auf den Status-Quo von derzeit 15%?
- Kann eine Variation der Quote zu einer Verbesserung der Sicherheit, d.h. Reduktion des potentiellen Gesamtschadens, beitragen?

- Kann eine Variation der Quote zu einer Verbesserung der Kostenstruktur, d.h. Reduktion der Betriebs- und Personalkosten, beitragen?
- Kann eine Variation der Quote zu einer Verbesserung der Sicherheit und gleichzeitig zu einer Verbesserung des Kosten-Nutzen-Verhältnisses beitragen, d.h. Reduktion des potentiellen Gesamtschadens bei gleichzeitiger Reduktion der Betriebs- und Personalkosten? Wenn ja, was ist die „optimale" Quote?

Bewertungskriterien (MOEs - Measures of Effectiveness)

- Schadensausmaß (Vignette A)
- Durchkommenswahrscheinlichkeit (Vignette B)
- Abfertigungskosten (Vignette C)

Operationelle Vorgabe

Der Täter betritt den öffentlichen Bereich des Terminalgebäudes. Den Sprengsatz trägt er zündbereit am Körper, verdeckt durch einen übergroßen Pullover. Handgepäck führt er nicht mit, trägt jedoch eine Jacke, die bei der Handgepäckkontrolle überprüft wird. Nachdem er bereits eine Online-Bordkarte besitzt, begibt er sich direkt zur Passagierkontrollstelle, reiht sich in die Warteschlange an der Kontrollspur ein und durchschreitet nach Aufforderung durch das Sicherheitspersonal die Torbogensonde. Wird hierbei kein Alarmsignal ausgelöst, setzt der Täter seinen Weg in den Wartebereich fort und zündet dort die Bombe. Ertönt ein Alarmsignal erfolgt eine manuelle Nachkontrolle. Wird hierbei der Sprengsatz entdeckt, zündet der Täter diesen an der Passagierkontrollstelle.

Vignette A – Schadensberechnung

Ziel ist die ausschließliche Berechnung des potentiellen Schadens, der durch den Täter verursacht werden kann. Somit wird in der Simulation alleinig der Täter abgebildet. Reguläre Passagiere finden keine Berücksichtigung, da diese keinen Schaden verursachen. Die Quote (Wahrscheinlichkeit einer Stichprobenkontrolle) wird im Bereich 0% – 100% (0, 10, 12, 15, 18, 20, 30, …, 100) variiert. Die möglichen finanziellen Schäden werden den zwei möglichen Schadensorten mit unterschiedlichen Werten angenommen, d.h. das Schadensausmaß bei einer Detonation im Wartebereich wird höher sein als in der Personenkontrollstelle.

Durch die Variation der Quote werden insgesamt 14 Subvignetten A.1 bis A.14 erzeugt.

Vignette B – Durchkommenswahrscheinlichkeit

Ziel ist die ausschließliche Berechnung der Wahrscheinlichkeit, dass der Täter die Personenkontrollstelle unerkannt mit dem Sprengstoff überwindet. Somit wird in der Simulation alleinig der Täter abgebildet. Reguläre Passagiere finden keine Berücksichtigung, da diese keinen Schaden verursachen. Die Quote wird im Bereich 0% – 100% (0, 10, 12, 15, 18, 20, 30, …, 100) variiert. Mit Hilfe einer Zählvariablen wird dokumentiert, wie oft der Täter bei definierter Quote das Zielgebiet (den Wartebereich) unerkannt erreicht.

Durch die Variation der Quote werden insgesamt 14 Subvignetten B.1 bis B.14 erzeugt.

Vignette C – Abfertigungskosten

Ziel ist die ausschließliche Berechnung der Kosten, welche sich durch eine Variation der Quote ergeben. Somit werden in der Simulation alleinig Passagiere abgebildet ohne Berücksichtigung des Täters und von möglichen Schäden. Die Quote wird im Bereich 0% – 100% (0, 10, 12, 15, 18, 20, 30, …, 100) variiert.

Durch die Variation der Quote werden insgesamt 14 Subvignetten C.1 bis C.14 erzeugt.

Simulationsergebnisse
Vignette A – Schadensberechnung

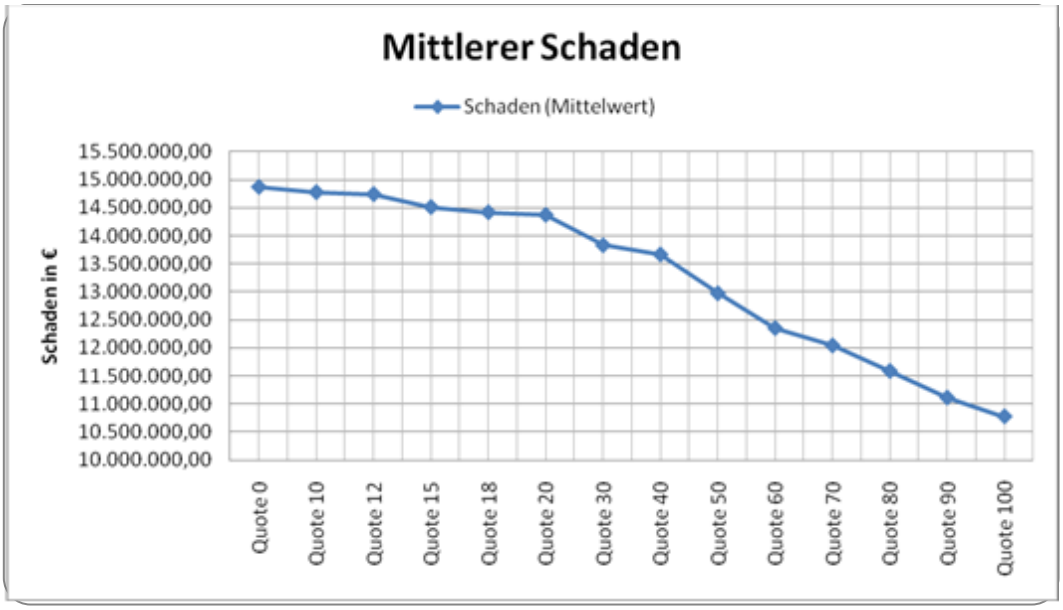


Abbildung 22: Mittlerer Gesamtschaden bei unterschiedlicher Quote

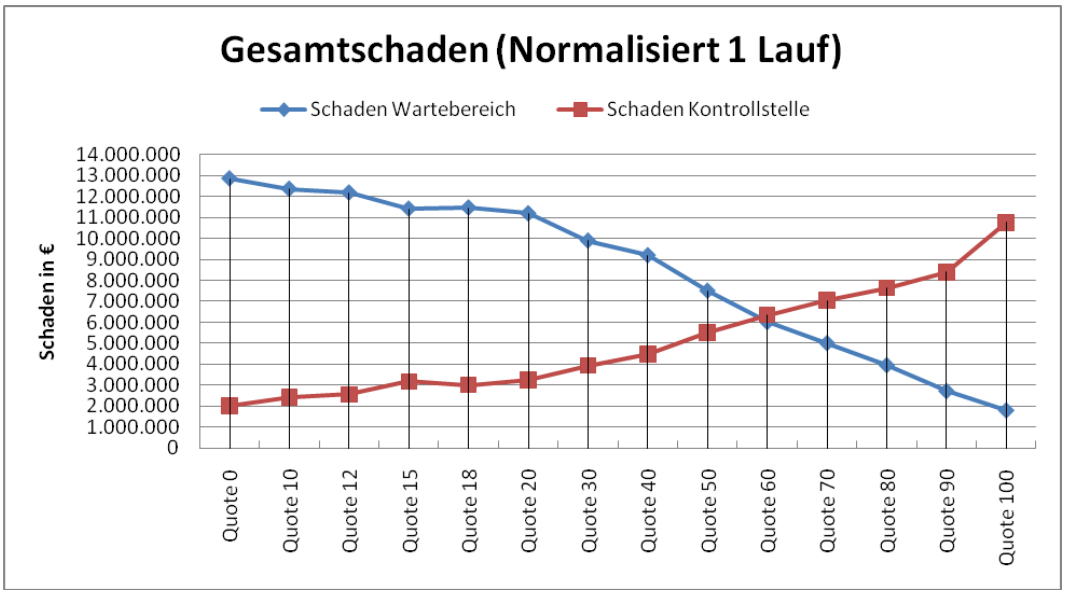


Abbildung 23: Durchschnittlicher Schaden eines Terroristen nach Schadensort

Vignette B – Durchkommenswahrscheinlichkeit

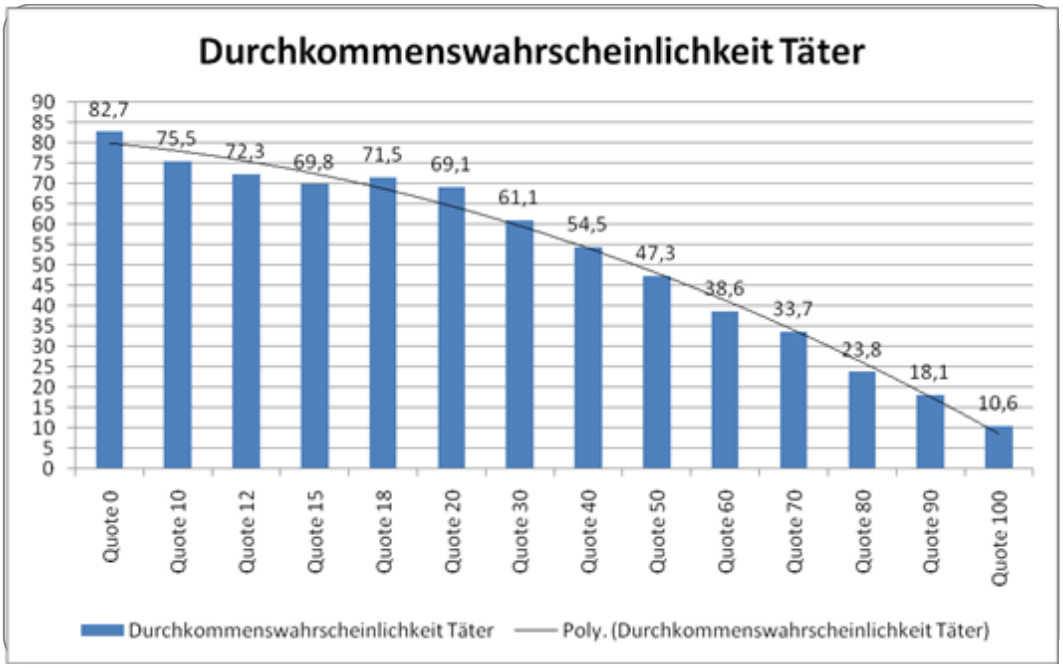


Abbildung 24: Durchkommenswahrscheinlichkeit des Täters

Vignette C – Abfertigungskosten

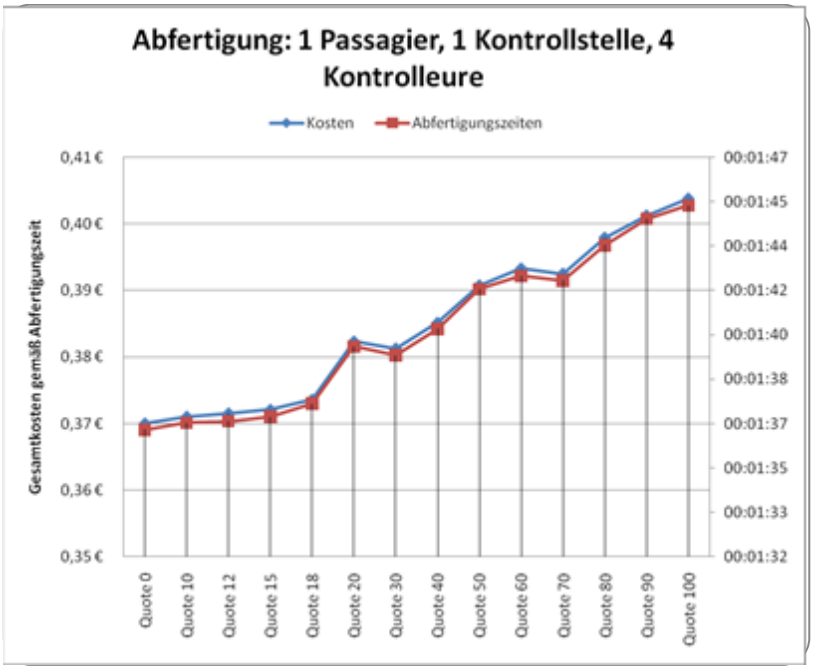


Abbildung 25: Kosten und Abfertigungszeiten pro Passagier

Auswertung

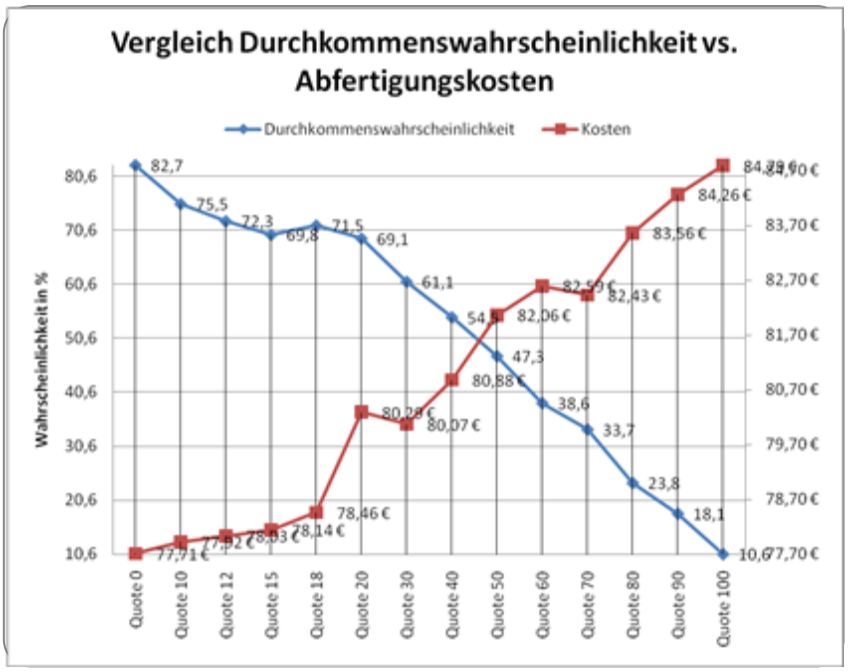


Abbildung 26: Durchkommenswahrscheinlichkeit vs. Kosten

Abbildung 26 zeigt ein optimales Kosten-Nutzen-Verhältnis bei einer Quote von ca. 45%.

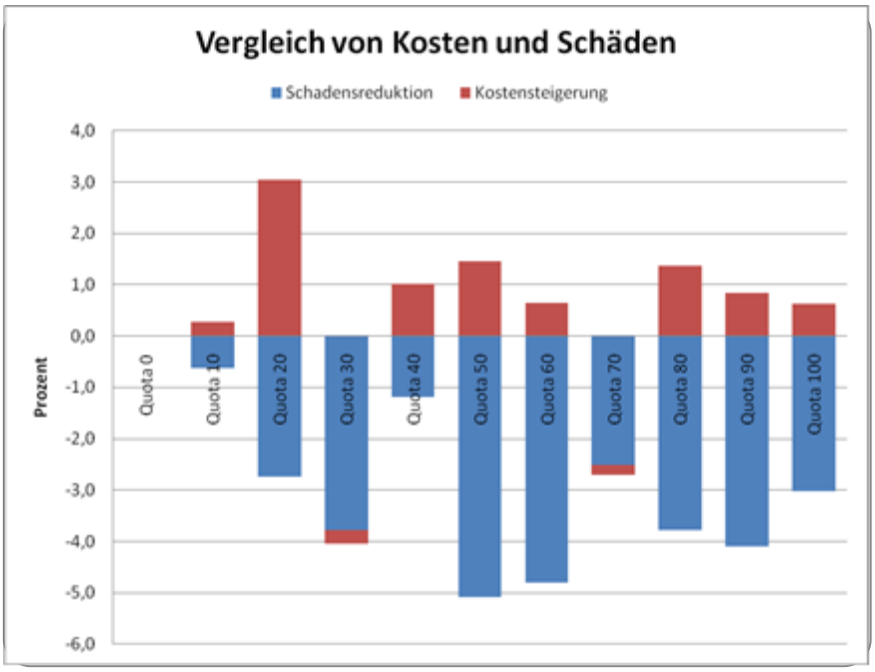


Abbildung 27: Prozentuales Verhalten von Kosten und Schaden

Abbildung 27 zeigt jeweils die Veränderung an Kosten und Schaden im Vergleich zur vorherig betrachteten Quote. So liegt die Kostensteigerung bei einer Quote von 10% im Vergleich zur vorherigen Quote von 0% bei ca. 0,3% und die Schadensreduktion bei ca. 0,5%.

Die Simulationsergebnisse wurden auf der ATRS2011-Konferenz veröffentlicht (vgl. Goldner 2011).

Experiment 2

Hauptziel des zweiten Experiments ist die Bewertung unterschiedlicher Scanner-Technologien bei der Passagierkontrollstelle am Flughafen. Im Rahmen des Experiments soll untersucht werden, wie sich der Einsatz eines Handgepäckscanners mit zusätzlicher Fähigkeit zur Flüssigsprengstoffdetektion im Vergleich zum Status-Quo mit herkömmlichen Handgepäckscannern auf den Nutzen und die Kostenstruktur auswirkt. Als Berechnungsgrößen werden der Schaden durch einen Täter, die Durchkommenswahrscheinlichkeit des Täters und die Abfertigungskosten der Passagiere bei unterschiedlicher Scanner-Technologie betrachtet. Im Vergleich zum ersten Experiment werden nicht nur die Parameter des Prozessmodelles, sondern auch das Modell an sich variiert.

Experiment-Beschreibung

Die Vorgehensweise in diesem Experiment ist nahezu identisch zu der in Experiment 1. Deshalb erfolgt an dieser Stelle nur eine sehr kurze Darstellung.

Kurz-Beschreibung

Verwendung eines Sprengsatzes basierend auf Flüssigsprengstoff. In der Simulation des Szenarios soll untersucht werden, wie sich der Einsatz eines neuartigen Scanners, der die Detektion von Flüssigsprengstoff im Handgepäck erlaubt, im Vergleich zum Status-Quo hinsichtlich der Sicherheit und der Kostenstruktur verhält.

Bewertungskriterien (MOEs - Measures of Effectiveness)

- Schadensberechnung bei Verwendung unterschiedlicher Scanner-Technologie (Vignette A)
- Durchkommenswahrscheinlichkeit (Vignette B)
- Vergleich der Abfertigungskosten (Vignette C)

Operationelle Vorgabe

Der Täter betritt den öffentlichen Bereich des Terminalgebäudes. Den Sprengsatz, bestehend aus DEGDN (Ethylenglykoldinitrat) ca. 1l aufgeteilt auf 10x100ml realistisch verpackte Behältnisse, trägt er zündbereit in einem Rucksack, der bei der Handgepäckkontrolle überprüft wird. Nachdem er bereits eine Online-Bordkarte besitzt, begibt er sich direkt zur Passagierkontrollstelle und reiht sich in die Warteschlange an der Kontrollspur ein. Nach dem Ablegen der Handgepäckgegenstände durchschreitet er nach Aufforderung durch das Sicherheitspersonal die Torbogensonde. Ertönt ein Alarmsignal erfolgt eine manuelle Nachkontrolle. Wird kein Alarmsignal ausgelöst, begibt sich der Täter zur Handgepäckkontrolle und wartet dort auf sein Handgepäck. Wird bei der Durchsuchung des Handgepäcks bereits Sprengstoff vermutet oder kommt es auf Grund eines unspezifischen Verdachts zur manuellen Durchsuchung des Handgepäcks, zündet dieser die Bombe an der Kontrollstelle. Wird kein Verdacht geschöpft, kann der Täter den Kontrollbereich verlassen und löst die Detonation im Wartebereich aus.

Simulationsergebnisse

Vignette A – Schadensberechnung

Die Schadensberechnung ist mittels der Agenten-basierten Simulation erstellt.

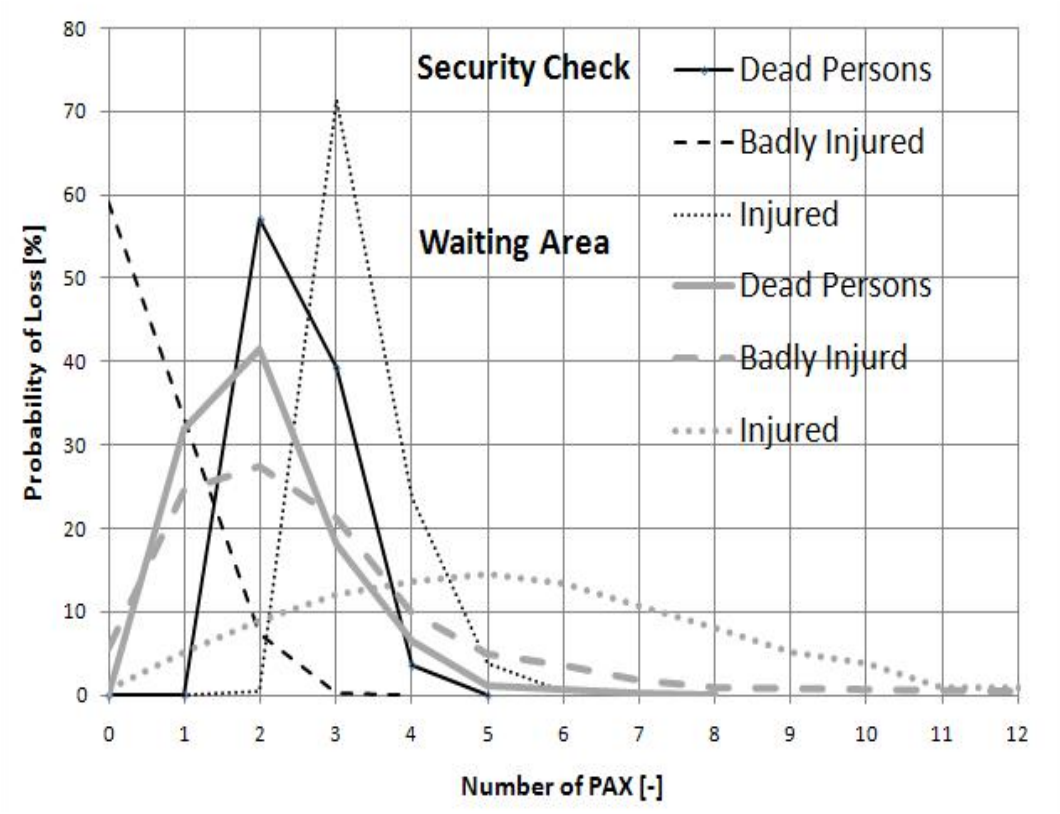


Abbildung 28: Schadensverteilung

Vignette B – Durchkommenswahrscheinlichkeit

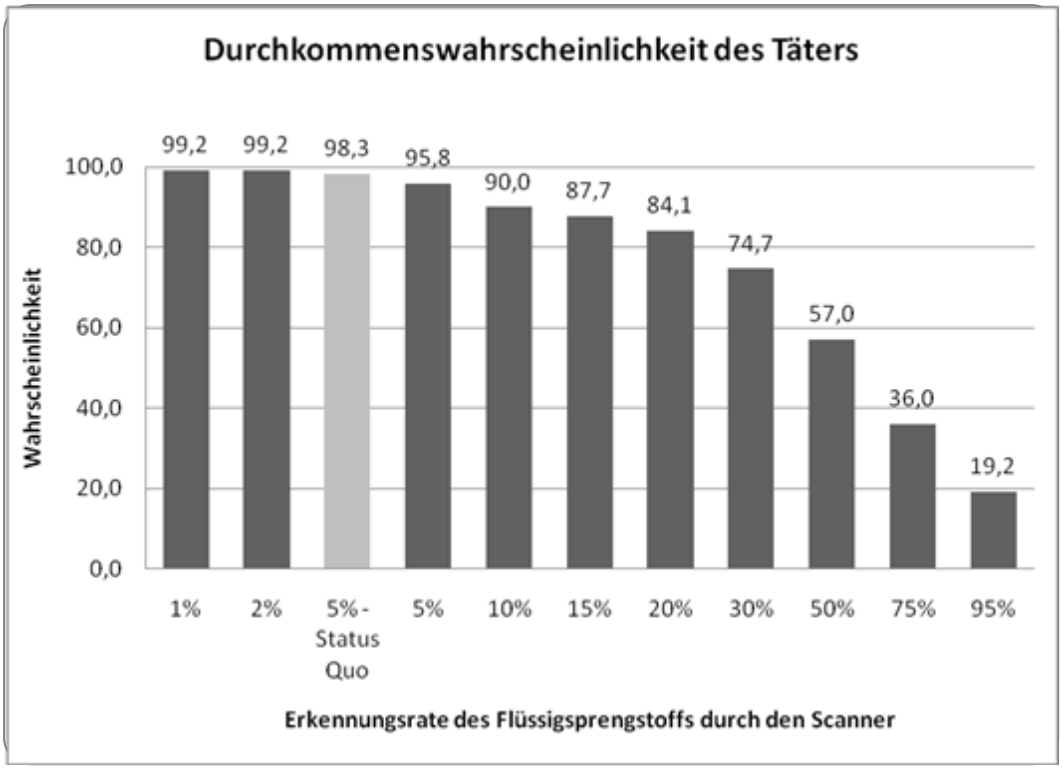


Abbildung 29: Durchkommenswahrscheinlichkeit des Täters

Vignette C – Abfertigungskosten

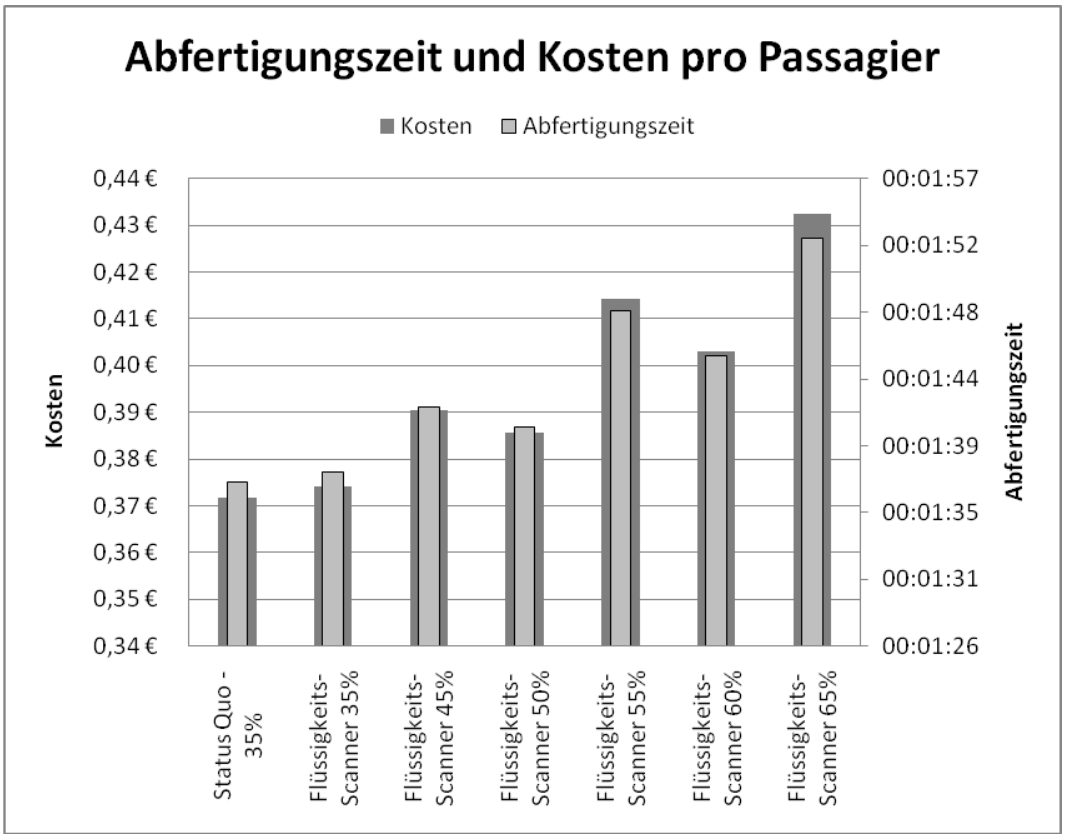


Abbildung 30: Abfertigungszeiten pro Passagier

Die Simulationsergebnisse werden auf der Future Security 2011-Konferenz veröffentlicht (vgl. Geiger 2011).

Ein Szenario bzw. Berechnungsszenario setzt sich aus einem Layout und eine Systemlast zusammen. Restrisiken und Kosten eines Szenarios können durchberechnet werden, wenn die modellierte Systemlast und Systemlayout zusammen vernetzt worden sind. Die PoC-Berechnungsengine sorgt dafür, dass für jede Situation der Systemlast alle möglichen passenden (durch die Vernetzung) Prozessinstanzen des Systemlayouts ermittelt werden. Dadurch werden die Wahrscheinlichkeiten des Erreichens (Systemclear) bzw. des nicht Erreichens (Systemalarm) eines Zieles im Layout (Risikoberechnung) sowie die Belastung (als Kosten und Dauer) aller Prozesselemente der passenden Instanzen (Kostenrechnung) berechnet.

Eine Studie bzw. Berechnungsstudie setzt sich aus mehreren Szenarien bzw. Berechnungen zusammen. Damit können Vergleiche zwischen Berechnungen durchgeführt werden. Dieses Vorgehen wird von uns empfohlen, da auf Grund der Kritikalität der Eingabedaten (Geheimhaltung) sind absolute Ergebnisse nicht aussagekräftig.

Abbildung 15 auf Seite 49 zeigt der Ablauf zur Erstellung einer Studie im PoC.

In den folgenden Unterkapiteln werden Ergebnisse aus berechneten Studien dargestellt. Als Beispiel wurden auch Studien, die mit dem SiVe-Demonstrator durchsimuliert wurden, um die Ergebnisse der zwei Anwendungen (PoC und Demonstrator) miteinander zu vergleichen.

Experiment 3

In diesem Simulations-Experiment wird das Potential des PoC demonstriert und auch die Vorteile von PoC gegenüber dem SiVe Demonstrator aufgezeigt.

Beschreibung

Angriff durch einen Selbstmordattentäter mit einem selbstgebauten Sprengsatz am Körper. In der Studie soll untersucht werden, wie sich eine Variation der Rate von stichprobenartigen Personenkontrollen (Quote) bei der Passagierkontrolle im Hinblick auf die Sicherheit und die Kostenstruktur auswirkt.

Fragestellungen

Welche Veränderungen auf die Messgrößen ergeben sich durch eine Variation der Quote in Bezug auf den Status-Quo von derzeit 15%?

- Kann eine Variation der Quote zu einer Verbesserung der Sicherheit, d.h. Reduktion des potentiellen Gesamtschadens, beitragen?
- Kann eine Variation der Quote zu einer Verbesserung der Kostenstruktur, d.h. Reduktion der Betriebs- und Personalkosten, beitragen?
- Kann eine Variation der Quote zu einer Verbesserung der Sicherheit und gleichzeitig zu einer Verbesserung des Kosten-Nutzen-Verhältnisses beitragen, d.h. Reduktion des potentiellen Gesamtschadens bei gleichzeitiger Reduktion der Betriebs- und Personalkosten? Wenn ja, was ist die „optimale“ Quote?

Situationsbeschreibung

Der Täter betritt den öffentlichen Bereich des Terminalgebäudes. Den Sprengsatz trägt er zündbereit am Körper, verdeckt durch einen übergroßen Pullover. Handgepäck führt er nicht mit, trägt jedoch eine Jacke, die bei der Handgepäckkontrolle überprüft wird. Nachdem er bereits eine Online-Bordkarte besitzt, begibt er sich direkt zur Passagierkontrollstelle, reiht sich in die Warteschlange an der Kontrollspur ein und durchschreitet nach Aufforderung durch das Sicherheitspersonal die Torbogensonde. Wird hierbei kein Alarmsignal ausgelöst, setzt der Täter seinen Weg in den Wartebereich fort und zündet dort die Bombe. Ertönt ein Alarmsignal erfolgt eine manuelle Nachkontrolle. Wird hierbei der Sprengsatz entdeckt, zündet der Täter diesen an der Passagierkontrollstelle.

Variationsgröße

Quote 0%-100%, Variation in 5-10%-Schritten

Layoutmodell

Hierbei handelt es sich um ein vereinfachtes Modell, bei dem die Handgepäckkontrolle nicht berücksichtigt wird, da diese keine Auswirkung auf die Schadensberechnung hat und somit nur unnötig die Komplexität erhöhen würde.

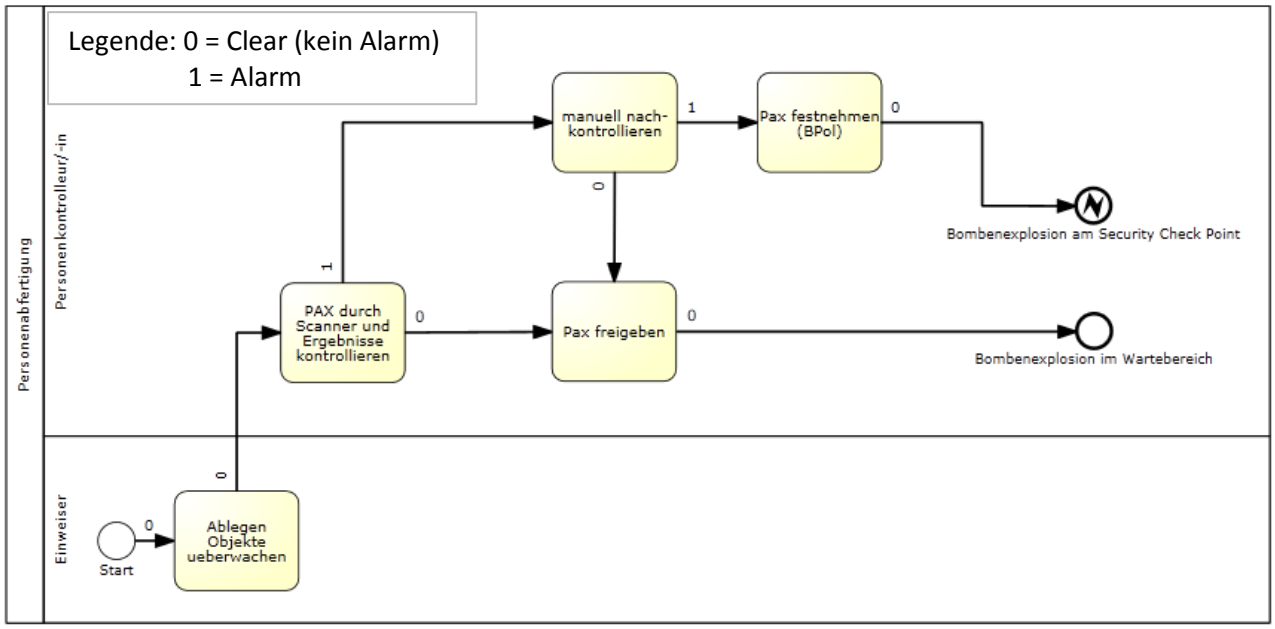


Abbildung 31: Layout für die beschriebene Berechnung.

Inputdaten

Tabelle 27:.Parametrisierung der Schutzmechanismen für die Kosten.

Parameter	Nominal-kosten (€/Obj.)	Nominal. Prozess-dauer (s/Obj.)	feste Kosten (€/Jahr)	Std./Jahr	Durchsatz (Obj./Std.)	Anwendungs-Kosten (€/Obj.)	Bemerkung
Ablegen Objekte überwachen	0,115	30	24.840 €	1800	120	0,00	• Feste Kosten berechnet als 13,80 € / Std. Personalkosten für 1800 Std. / Jahr
Metall-detektor	0,020	5	25.840 €	1800	720	0,00	• Variation der Quote von 0% bis 100% • Die feste Kosten beinhalten Personalkosten + Anschaffungskosten = 10.000 € → 1.000 €/Jahr für 10 Jahre
Manuelle Nachkontrolle	0,050	13	24.840 €	1800	277	0,00	• –
Pax Freigeben	0,000	0	24.840 €	1800	–	0,00	• Nicht Sicherheitsrelevant, nur Aktivität
Festnahme durch BPol	1,150	300	24.840 €	1800	12	0,00	• Aktion der Festnahme, nicht die Kontrolle durch die Bundespolizei • Nicht Sicherheitsrelevant, nur Aktivität

Systemlast

Gesamtlast: 36.000.000 Passagiere / Jahr, davon 1 Selbstmordattentäter mit Sprengstoff am Körper.

Tabelle 28: Systemlast

Situation	Art	Häufigkeit	Menschenleben	Wirtschaftliche Schaden
Normale Passagiere	L	35.999.999	–	–
Selbstmordattentäter	B	1	8	16.240.000 €

Annahme bei Schaden: 1 Menschenleben = 2.030.000 €.

Tabelle 29: Lastsituation „Normale Passagiere“

Situationslast "normale Passagiere"	
Kategorie:	Passagier
Absichten/Motivation:	Keine
Objekt:	Keines
Einfallsweg:	Straße
Einbringungsart:	Keine
Nutzung/Angriffsziele:	Flughafen-Nicht allgemein zugänglicher Bereich

Tabelle 30: Bedrohungssituation

Bedrohungssituation "Selbstmordattentäter"	
Kategorie:	Terrorist
Absichten/Motivation:	Menschenleben
Objekt:	Sprengstoff klassifizierbar
Einfallsweg:	Straße
Einbringungsart:	Am Körper
Nutzung/Angriffsziele:	Flughafen-Nicht allgemein zugänglicher Bereich

Tabelle 31: Detektions- und Alarmraten der Lastsituationen und der Bedrohung.

Schutzmechanismus	Lastsituationen		Bedrohungssituation		Quote	Dauer (s)
	Falsch Alarm Rate	Falsch Clear Rate	Falsch Alarm Rate	Falsch Clear Rate		
Ablegen Objekte überwachen	0,0	1,0	0,0	1,0	–	30,0
Pax festnehmen (BPol) (nur Aktivität)	0,0	1,0	0,0	1,0	–	300,0
Manuelle Nachkontrolle	0,05	1,0	0,0	0,1	–	13,0
Pax freigeben (nur Aktivität)	0,0	1,0	0,0	1,0	–	0,0
Metalldetektor	0,05	1,0	0,0	0,8	0,0 bis 1,00	5,0

Tabelle 32: Ergebnisse der Studie und Vergleich mit dem Demonstrator. Die Simulation mit dem Demonstrator wurde mit 1.000 Simulationsläufen durchgeführt.

Quote (Metall-Detektor)	P(durch)	Menschen-Leben	Wirtsch. Schaden	Gesamt-Kosten (Last)	P(durch) Demonstr.	Wirtsch. Schaden Demonstr.	Gesamt-Kosten Demonstr.
0%	0,820	6,560	13.316.800 €	5.053.500 €	0,830	13.482.229 €	4.961.099 €
10%	0,748	5,984	12.147.520 €	5.421.150 €	0,753	12.231.990 €	5.446.584 €
20%	0,676	5,408	10.978.240 €	5.788.800 €	0,644	10.465.409 €	5.346.947 €
30%	0,604	4,832	9.808.960 €	6.156.450 €	0,618	10.041.147 €	6.284.106 €
40%	0,532	4,256	8.639.680 €	6.524.101 €	0,524	8.508.196 €	6.508.631 €
50%	0,460	3,680	7.470.400 €	6.891.751 €	0,439	7.121.986 €	6.742.127 €
60%	0,388	3,104	6.301.120 €	7.259.401 €	0,401	6.515.322 €	7.382.312 €
70%	0,316	2,528	5.131.840 €	7.627.051 €	0,317	5.153.973 €	7.846.129 €
80%	0,244	1,952	3.962.560 €	7.994.701 €	0,240	3.892.647 €	8.108.328 €
90%	0,172	1,376	2.793.280 €	8.362.351 €	0,162	2.632.295 €	8.122.267 €
100%	0,100	0,800	1.624.000 €	8.730.001 €	0,105	1.710.868 €	8.983.801 €

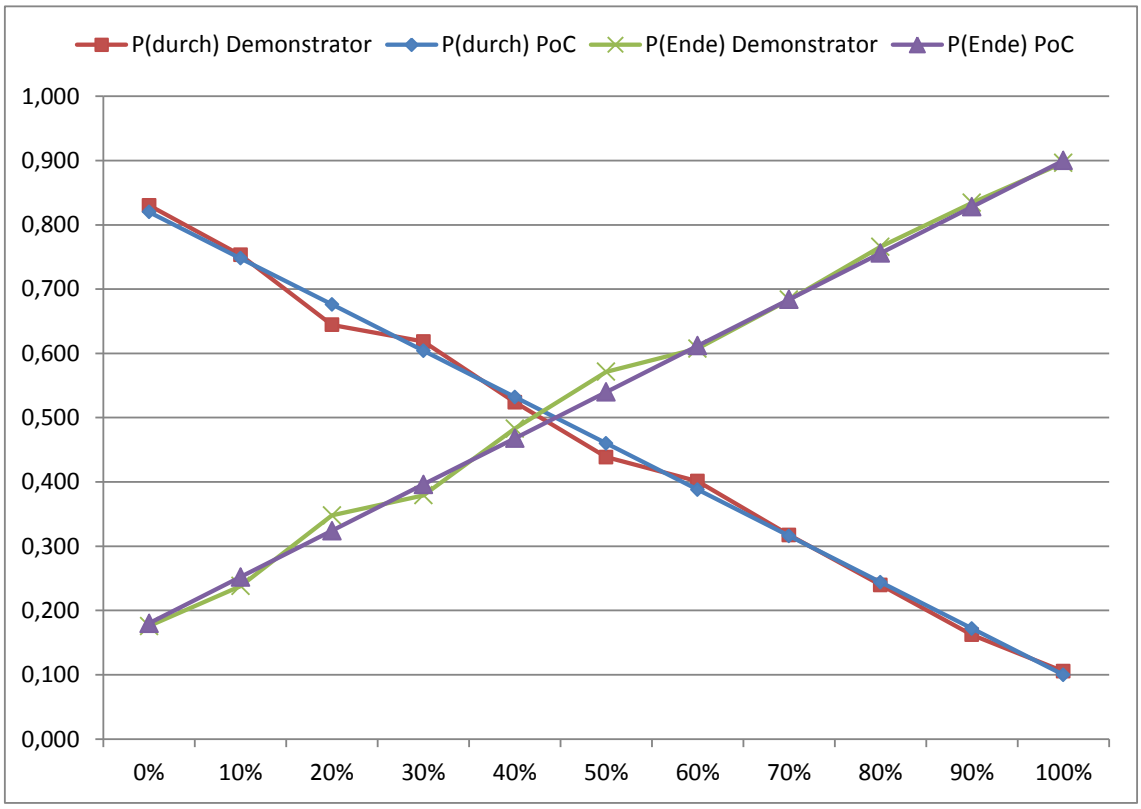


Abbildung 32: Vergleich P(durch) (Täter/Passagier erreicht das Ziel) und P(Ende) (Täter/Passagier werden „entdeckt“) zwischen PoC und Demonstrator.

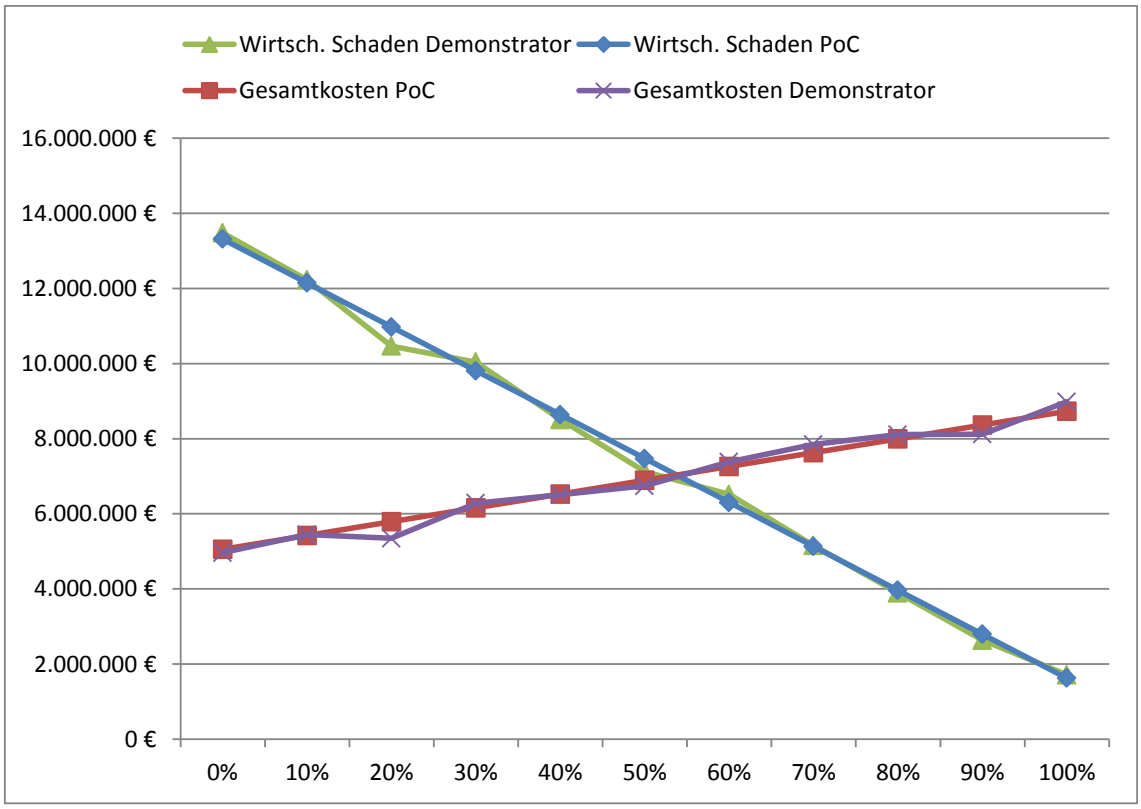


Abbildung 33: Vergleich von Ergebnissen aus dem PoC mit dem Demonstrator.

II.2. *Wichtigste Positionen des zahlenmäßigen Nachweises*

Siehe auch „Zahlenmässiger Verwendungsnachweis“ vom 11.4.2012; die Gesamtkosten erfüllen den beantragten Gesamtförderungsrahmen.

Über die gesamte Laufzeit aller Teilvorhaben der EADS fielen 13.490 EUR Reisekosten an, die primär für die Beteiligung an den regelmäßigen Projektmeetings und –Workshops und die Feldtests und Begehungen am Flughafen, sowie für Reisen der Erstautoren zum Vortrag der veröffentlichten Konferenzbeiträge (ca. 2.000EUR) verwendet wurden.

Wesentliche Material- und Fremdleistungskosten beinhalten Fachliteratur und Software zur Erstellung der Simulatoren.

II.3. *Notwendigkeit und Angemessenheit der geleisteten Arbeit*

Ein wesentliches technisches Projektrisiko ergab sich durch stark vernetzte Arbeitspakete und Modellzusammenhänge einerseits und dem Wunsch einer Integration sehr verschiedenartiger Ansätze zur Modellierung und Simulation von Bedrohungsszenarien und Schutzmechanismen andererseits. Die Aussagekraft der Quantifizierungen und der anderen Ergebnisse kann deshalb nicht vollumfänglich garantiert werden. Unklar ist auch, ob der zwar sehr systematische, aber auch sehr komplexe Ansatz zum Thema Sicherheit beim Kunden Akzeptanz findet. Damit hat das Projekt einen gewissen Pilotcharakter, der allerdings im Projektantrag ausdrücklich erwähnt wurde.

Der Projektantrag sah im Rahmen der identifizierten Forschungsthemen eine Festlegung der Detailzielsetzung jedes Arbeitspakets auch nach Projektbeginn vor, um die Abstimmung der Arbeiten mit den Anforderungen der potentiellen Anwender zu ermöglichen. Diese Anpassungen sind in diesem Bericht sowie den Zwischenberichten ausführlich dargelegt.

II.4. Verwertbarkeit des Ergebnisses

II.4.1. *Schutzrechtsanmeldungen*

Es wurden keine Schutzrechte in diesem Projektteil angemeldet, da diese auf dem Gebiet der Simulationssysteme sowie generell bei Softwareprodukten nur schwer zu erreichen sind. Stattdessen greifen Urheberrechte.

II.4.2. *Weitergehende Nutzung der Ergebnisse*

EADS Deutschland GmbH möchte sich in der Zukunft strategisch verstärkt auf dem zivilen Sicherheitsmarkt engagieren. Die Themen Transportsicherheit sowie Sicherheit von kritischen Infrastrukturen wurden als interessante Marksegmente erkannt. Um in Zukunft den Kunden bessere Produkte, eine kompetente Beratung und auf den Kunden zugeschnittene Dienstleistungen anbieten zu können, ist eine stetige Weiterentwicklung der Kernkompetenzen unverzichtbar. Hierfür sind detaillierte Kenntnisse der Prozesse der zukünftigen Kunden notwendig. Als Systemanbieter ist EADS auf ein Netzwerk kompetenter Partner angewiesen.

EADS Deutschland GmbH konnte als Ergebnis der Forschung im Vorhaben detaillierte Kenntnisse der Prozesse der einzelnen Hoheitsträger am Flughafen sowie der Leistungsfähigkeit der verwendeten Technologien gewinnen.

EADS-CASSIDIAN hat sich in diesem Rahmen am Projekt INFRANORM beteiligt und einen Normungsvorschlag zur „Gesamtheitlichen Beschreibung von Sicherheitsprozessen“ eingereicht. Der Vorschlag wurde seitens des DIN akzeptiert, so dass derzeit die DIN-Spezifikation DIN SPEC 91285 „Gesamtheitliche Beschreibung von Sicherheitsprozessen“ in Zusammenarbeit mit dem Fraunhofer Anwendungszentrum für Logistikplanung und Informationssysteme (ALI) erstellt wird. Folgende Personen sind an der Erstellung beteiligt: Sascha Goldner (Initiator, CASSIDIAN), Detlef von Busch (CASSIDIAN Systems), Alf Papproth (Fraunhofer ALI), Norbert Siegel (DIN).

II.5. FORTSCHRITT AUF DEM GEBIET DES VORHABENS BEI ANDEREN STELLEN

Es sind keine Ergebnisse von anderen Stellen bekannt, die derart umfassend die Problematik der Sicherheit von Verkehrsinfrastrukturen behandeln.

II.6. VERÖFFENTLICHUNGEN DES ERGEBNISSES

Arbeitsanteile des Vorhabens wurden auf internationalen Konferenzen veröffentlicht, die im Folgenden zusammen mit entsprechenden Links aufgelistet sind. Weitere Veröffentlichungen auf Grundlage der direkten Vorhabensergebnisse sind nicht geplant.

Autoren	Goldner, S.	Cassidian
Titel	Rapid Behavior Modelling for an Agent-Based Simulation	
Konferenz	ICAART 2011 – International Conference on Agents and Artificial Intelligence	
Jahr	2011	
Abstract	-	
URL	http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/g/Goldner:Sascha_A=.html	

Autoren	Goldner, S. et al.	Cassidian
Titel	Using Agent-Based Simulation and Business Process Modeling to Evaluate the Performance of Airport Security Systems	
Konferenz	The 2011 World Conference of Air Transport Research Society", Sydney, June 29 - July 2 2011	
Jahr	2011	
Abstract	-	
URL	http://www.tu-cottbus.de/fakultaet3/de/informationssysteme/forschung/veroeffentlichungen.html	

III. ERFOLGSKONTROLLBERICHT

III.1. BEITRAG DES ERGEBNISSES ZU DEN FÖRDERPOLITISCHEN ZIELEN

Das vorliegende Vorhaben wurde im Rahmen des Programms „Forschung für die zivile Sicherheit“ gefördert, das die Bundesregierung am 24. Januar 2007 als Bestandteil der Hightech-Strategie für Deutschland beschlossen hat. Im Mittelpunkt des Sicherheitsforschungsprogramms steht die Verbesserung des Schutzes der Bürgerinnen und Bürger. Das Ziel ist, gesellschaftlichen Bedrohungen durch Terrorismus, organisierte Kriminalität, Naturkatastrophen oder technische Großunfälle entgegenzuwirken. Charakteristischer Anspruch an die Vorhaben des Programms ist das anwendungsorientierte Arbeiten innerhalb der Projekte durch Einbeziehung der gesamten Innovationskette von der Forschung über die Industrie bis hin zu den Endnutzern.

Eine ausführliche Beschreibung des vorwiegend fachlichen Mehrwerts der Vorhabensergebnisse findet sich in II.1, Aussagen zur Verwertungsfähigkeit im Rahmen der förderpolitischen Ziele finden sich in II.4. Die im vorliegenden Vorhaben beschriebenen Ansätze und implementierten Methoden zur Kosten / Nutzen Analyse des gesamten Sicherheitssystems erlauben eine Bewertung von verschiedenen Sicherheitstechnologien und –vorrichtungen im Kontext des Gesamtsystems. Die erarbeiteten Methoden konnten auf teilweise synthetischem und teilweise realistischem Datenmaterial angewandt und evaluiert werden; auf Grundlage dieser Ergebnisse sollen nach Vorhabensende in enger Abstimmung mit den Anwendern zu einer kostenoptimierten Verbesserung der Gesamt-Sicherheit von Verkehrsinfrastrukturen, insbesondere Flughäfen, genutzt werden.

III.2. WISSENSCHAFTLICH-TECHNISCHES ERGEBNIS DES VORHABENS

Mit dem SiVe Demonstrator konnte erstmalig ein System vorgestellt werden, das in der Lage ist, Abläufe, Verfahren, Akteure, Prozesse und Techniken bzgl. Verkehrssicherheitssystemen unter der Berücksichtigung von juristischen, ethischen und sonstigen Randbedingungen ganzheitlich zu simulieren. Im PoC können darüberhinaus auch alternative Techniken, Prozesse oder Verfahren etc. bewertet werden.

Bisher waren solche Systeme nicht bekannt, auch wenn nicht ausgeschlossen werden kann, dass evtl. vorhandene Systeme von bestimmten Stellen verwendet werden, dies aber aus Sicherheitsgründen nicht publik gemacht wird.

III.3. FORTSCHREIBUNG DES VERWERTUNGSPLANS

III.3.1. SCHUTZRECHTSANMELDUNGEN

Keine Schutzrechtsanmeldungen, da die die Art der Aufgabenstellung / Lösung (Software bzw. Simulationssystem) eine Schutzrechtsanmeldung nur in Ausnahmefällen zulässt.

III.3.2. *WIRTSCHAFTLICHE ERFOLGSAUSSICHTEN NACH PROJEKTENDE*

Siehe II.1.2, „Business Cases“.

III.3.3. *WISSENSCHAFTLICHE ERFOLGSAUSSICHTEN NACH PROJEKTENDE*

Siehe II.1.

III.3.4. *WISSENSCHAFTLICHE UND WIRTSCHAFTLICHE ANSCHLUSSFÄHIGKEIT*

Siehe II.4.2.

III.4. ARBEITEN, DIE ZU KEINER LÖSUNG GEFÜHRT HABEN

Der Frachtverkehr wurde nicht implementiert, weil die Schaffung der entsprechenden Instrumente derart komplex war, dass man sich auf den Personenverkehr beschränken musste.

Etliche der benötigten Daten (Sicherheitsdaten) unterliegen hohen Sicherheitsklassifikationen, so dass sie nicht an die SiVe Partner überstellt werden konnten. Auch unter Einbeziehung der verantwortlichen Stellen (Bundespolizei, BMI, Smith Heimann etc) ließ sich dieses Ergebnis nicht ändern. Allerdings können sich obige Stellen vorstellen, die Bedatung selbst vorzunehmen. Zum Nachweis der Lauffähigkeit der Systeme wurden (evtl. unrealistische) Schätzdaten verwendet.

Bezüglich Krisen- und Notfallmanagement wurde eine detaillierte Erfassung operativer Abläufe zur weiteren Abbildung in den Simulationsmodellen nicht weiter verfolgt. Die operativen Abläufe sind zu einem solch hohen Grad situationsabhängig und vielfältig, dass entweder eine enorm große Menge an Simulationsmodellen erstellt werden müsste, um zumindest einen Bruchteil möglicher Krisen- und Notfallsituationen abzubilden, oder die Modelle müssten dermaßen abstrahiert und generalisiert werden, dass schlussendlich nur allgemeine Aussagen ohne nennenswerten Mehrwert erzeugt werden.

III.5. PRÄSENTATIONSMÖGLICHKEITEN FÜR MÖGLICHE NUTZER

Es kann nicht nur das Konzept gegenüber potentiellen Anwendern präsentiert werden, es sind auch die erstellten Simulatorsysteme ablauffähig und insbesondere in den Aspekten Datenerfassung und Systemvariation demonstrierbar.

Mögliche Nutzer sind

- Flughafenbetreiber bzw. für die Sicherheit am Flughafen verantwortliche Stellen,
- Behörden die Normen für die Sicherheit erstellen und Geräte / Systeme / Verfahren etc. zulassen,
- Gesetzgeber (Europa, Bund, Land) zur Abschätzung der Wirkung von gesetzlichen Vorgaben.

Im Anhang C werden Ablauf und insbesondere die Eingabeschnittstellen des PoC demonstriert.

III.6. EINHALTUNG DER AUSGABEN- UND ZEITPLANUNG

Am 12.4.2011 wurde ein Antrag auf kostenneutrale Verlängerung des Vorhabens um 3 Monate bis zum 30.9.2011 gestellt, der am 16.5.2011 genehmigt wurde.

Die antragsgemäße Gesamtkostenplanung für das Teilvorhaben wurde eingehalten, siehe Dokument „Zahlenmässiger Verwendungsnachweis“ vom 11.4.2012.

IV. LITERATURANGABEN

Babau, A., 2011. Modelling and Verification of Airport Security Proccesses using BPMN and Protocol Interfaces. Diploma Thesis. University of Passau and CASSIDIAN

Chawdhry, P.K. 2009. Risk Modeling and Simulation of Airport Passenger Departures Process. *Proceedings of the 2009 Winter Simulation Conference.* 2009, pp. 2820-2831.

D'Avanzo, J. und Dickmanns, D. 2011. SiVe: Verbesserung der Sicherheit von Verkehrsinfrastrukturen. *Präsentation zum Projektmeeting am 2011-01-12.* 2011.

D'Avanzo, J., Dickmanns, D. und Maurer, M. 2010. SiVe: Verbesserung der Sicherheit von Verkehrsinfrastrukturen – SiVe-Facharchitektur. Systembeschreibung und Fachkonzept für ein Simulationssystem zur Analyse und Bewertung von Bedrohungsszenarien und Sicherheitssystemen (SiVe-Demonstrator). *EADS Technischer Bericht Nr. CTO/IW-SI-2010-30.* 2010.

—. 2010. Systemarchitektur und -integration. *Präsentation zum Projektmeilenstein am 2010-01-14.* 2010.

Feng, Q., Sahin, H. and Karson, M. 2009. Bayesian Analysis Models for Aviation Baggage Screening. *IIE Transactions.* 2009, pp. 41(1), 1-12.

Geiger, G., Goldner, S., Petzel, E., Papproth, A., 2011. Improving the Security of Critical Transport Infrastructures. In Proceedings of Future Security 2011, to be published

Goldner, S., 2011. Rapid Behaviour Modelling for an Agent-Based Simulation. In Proceedings of ICAART 2011 – Third International Conference on Agents and Artificial Intelligence, SciTePress

Goldner, S. et al., 2011. Using Agent-Based Simulation and Business Process Modeling to Evaluate the Performance of Airport Security Systems. In Proceedings of ATRS2011 world conference, to be published

Kaplan, S. and Garrick, B.J. 1981. On The Quantitative Definition of Risk. *Risk Analysis.* 1981, pp. 1(1) 11-27. DOI:.

Lampert, R.J., Popper, S.W. und Bankes, S.C. 2003. Shaping the next one hundred years: new methods for quantitative, long term policy analysis. *Santa Monica, Calif.: RAND Corporation, MR-1626-CR.* 2003.

Lindemann, U., Maurer, M. und Braun, T. 2009. Structural Complexity Management – An Approach for the Field of Product Design. *Springer.* 2009.

Maurer, M., et al. 2010. Airport security: From single threat aspects to valid scenarios and risk assessment. *American Journal of Engineering and Applied Sciences.* 2010.

Singpurwalla, N.D. 2006. Reliability and Risk: A Bayesian Perspective. *John Wiley & Sons, Ltd.* 2006.

SPT. 2006. SPT: Ideal process flow V 2.0. *http://www.iata.org/NR/rdonlyres/31BD66A2-4446-4514-A911-3EA9DDAC7CAA/0/IPF_V20_FINAL.pdf.* 2006. zugegriffen am 26. August 2009.

Veatch, J.D., et al. 1999. An airport vulnerability assessment methodology. *Proceedings IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology.* 1999, pp. 134-151. DOI:10.1109/CCST.1999.797905.

Willis, H.H., et al. 2005. Estimating Terrorism Risk. *Santa Monica, Calif.: RAND Corporation, MG-388.* 2005.

ANHANG A: GLOSSAR

Situation	Eine Situation bezeichnet einen Fall, der in einem System wie dem Flughafen passiert. Sie wird mit eindeutigen Eigenschaften definiert wie dem Subjekt, dessen Ziel und Motivation, mit welchem Werkzeug usw. Eine Situation kann sowohl eine Bedrohung als auch eine normale Last beschreiben.
Personenschaden	Menschenleben
Sachschaden	Wertverlust durch Beschädigung, Zerstörung oder Verlust der Sache. Folgeschäden fließen in den wirtschaftlichen Schaden ein.
Wirtschaftliche Schaden	Folgeschäden durch das Eintreten eines Schadensereignisses als indirekte finanzielle Folgen in der Luftfahrtindustrie und Wirtschaft.
Alarm	Ein Alarm kann als Frühwarnung oder bei Eintritt eines Schadensereignisses ausgelöst werden. Ruf zur Bereitschaft. Warnung vor Gefahr.
Allgemein zugänglicher Bereich	Bereich des Flughafengeländes, der für die Öffentlichkeit ohne Sicherheitsmaßnahmen zu betreten ist.
Bedrohung	Resultat eines Bedrohungsszenarios (Zusammengesetzt aus 8 Domänen der Systemanalyse).
Bedrohungsaspekt	Systemelement, das gemeinsam mit weiteren Systemelementen ein Bedrohungsszenario beschreiben kann. Wenn Systemelemente ein Bedrohungsszenario beschreiben bestehen Abhängigkeiten zwischen ihnen. Beispiele sind Werkzeug, Absichten und Angriffsziel.
Bedrohungsszenario	Nach SiVe ist ein Bedrohungsszenario eine plausible Kombination von Bedrohungsaspekten, die eine konkrete Bedrohung der Flughafensicherheit zur Folge hat.
Bedrohungslage	Sammlung aller relevanten Bedrohungsszenarien eines Systems (z.B. Flughafen).
Business Case	Ein Business Case stellt dar, wer eine Anwendung für welche Zielsetzung wie einsetzen kann. Im Sinne des Verwertungsplans explizieren die Business Cases damit die praktische Anwendung. Business Cases spezifizieren die Fach- und IT-Architektur und werden umgekehrt durch die detaillierte Fach- und IT-Architektur detailliert.
Domäne	In der Strukturanalyse beschreibt eine Domäne eine Gruppe gleichartiger Systemelemente in der Methodik der Multiple-Domain Matrix. Domänen dienen der Abstrahierung der Zusammenhänge eines Systems und ermöglichen damit den effizienten Umgang mit ihnen.
Eintritts-wahrscheinlichkeit	Wahrscheinlichkeit, mit der ein bestimmtes Bedrohungsszenario realisiert wird.
Entscheidungsknoten	Logischer Baustein in einem Prozess zur Verzweigung von Prozesssträngen. Basierend auf dem Wert der zu treffenden Entscheidung wird der Prozessablauf fortgesetzt.
Erwartungswert	Der statistische Erwartungswert einer (statistisch verteilten) Größe gibt an, welchen Wert diese Größe bei Durchführung sehr vieler Versuche bzw. über einen sehr

	langen Zeitraum im Mittel annimmt.
Falschalarm	Ein Falschalarm oder Fehlalarm ist eine irrtümliche oder missbräuchliche Alarmierung.
Fehlalarm	s. Falschalarm.
Flughafensicherheit	Unter Flughafensicherheit versteht man alle Maßnahmen, die der Vorbeugung gegen Verbrechen und Terroranschläge auf einem Flughafen, also am Boden, dienen. Da sich eine große Zahl von Personen auf relativ engem Raum aufhalten, sind Flughäfen ein potenzielles Ziel für den Terrorismus. Die meisten großen Flughäfen haben eigene Sicherheitskräfte, die von Polizeibeamten unterstützt werden. In einigen Ländern schützen paramilitärische Kräfte oder Soldaten die Flughäfen vor Bedrohungen. Die Flughafensicherheit ist ein Teilbereich der Luftsicherheit, bei der es allgemein um die Verhinderung terroristischer oder anderer krimineller Einwirkungen auf die Sicherheit des zivilen Luftverkehrs geht (engl. security). Hiervon abzugrenzen sind die Begriffe Flugsicherheit (engl. flight safety), also im weitesten Sinne die Verhinderung von Flugunfällen, und Flugsicherung (engl. flight security), das ist die Regelung der Verkehrsabläufe im Luftraum.
Gefahr	Gefahr ist ein Zustand, aus dem ein Schaden entstehen kann. In der SiVe-Methodik ist eine Gefahr die Bezeichnung einer Domäne der Systemanalyse, die Bedrohungsaspekte mit Gefahrenpotential beinhaltet.
Intrinsischer Preis (auch „fairer" Preis)	Wert eines Gutes innerhalb eines gegebenen Verrechnungssystems, i. a. vom Marktpreis dieses Gutes verschieden.
Kontextdiagramm	Visualisierte Darstellung von Objektumfeldern, z. B. Geschäftsprozessen. Dies können Eingaben, Ausgaben, Steuerungen, Ressourcen usw. sein.
Kostenart	Die Kostenart kategorisiert in der Kostenrechnung angefallene Kosten nach ihrer eigenen Natur. Kostenarten sind also Personalkosten, Wartungs- und Betriebsmittelkosten, usw. Man kann Kostenarten auch in Einzelkosten und Gemeinkosten, oder auch fixe Kosten, variable Kosten und Mischkosten, unterteilen.
MDM (Multiple-Domain Matrix)	Matrixbasierte Methode zur systematischen Erfassung, Darstellung, Analyse und Optimierung komplexer Systeme [Lindemann et al. 2009]. Es werden direkte Abhängigkeiten zwischen Systemelementen meist rein binär erfasst. Systemelemente werden in Domänen eingeordnet, deren Zusammenhänge beschrieben werden. Algorithmen sowie spezielle Software unterstützen die Analyse und Optimierung der Systeme.
Metamodell	Ein Metamodell ist ein Modell, das beschreibt, wie Modelle gebaut werden.
Preis eines Risikos	Sicherheitsäquivalent oder Marktpreis eines Risikos (z. B. eines Lotterieloses, Wertpapiers usw.)
Prozess	Folge logischer zusammengehöriger Aktivitäten bzw. Vorgänge, wobei diese aber inhaltlich abgeschlossen sind, für sich betrachtet werden und sich im Kontext einer organisatorischen Struktur befinden, welche die funktionalen Rollen und Abhängigkeiten definiert. Ein Prozess ist normalerweise ergebnisorientiert, d. h., das Ziel, und nicht der Weg zum Erreichen dieses Zieles, steht im Vordergrund.

	Im Projekt SiVe werden insbesondere Prozesse mit Relevanz für die Flughafensicherheit betrachtet.
Prozessbuilder	Methodik und Software-Werkzeug zur Ableitung einer gültigen Prozesssequenz für einen Use Case aus der Gesamtheit aller betrachteten Prozesse (abgebildet in der Prozesslandkarte).
Prozesselement	Ein Prozesselement ist in SiVe die kleinste Einheit, aus der sich ein Prozess aufbaut und die durch Metriken und Ressourcen beschrieben wird. Das Prozesselement legt das SiVe-Prozessmodell zu Grunde. Die Informationsflüsse in einer Prozesskette werden durch logische Abhängigkeiten zwischen den Prozesselementen definiert. Durch das Mapping zu den präventiven Schutzmechanismen wirkt jedes Prozesselement gezielt gegen Bedrohungsaspekte eines Bedrohungsszenarios bzw. eines Szenario-Clusters (Sammlung ähnlicher Szenarien). Auch Prozessschritt genannt.
Prozesslandkarte	Gesamtheit aller betrachteten Prozesse. Im Projekt SiVe sind dies die für die Flughafensicherheit relevanten Prozesse.
Prozessmetrik	Eigenschaft eines Prozesselementes, die die Messung von Prozessen bzw. Prozesselementen ermöglicht, d. h. die Performance/Wirksamkeit eines Prozesses wird quantifizierbar. Beispiele sind Detektionsrate und Falschalarmrate. Prozessmetriken sind vom Bedrohungsszenario und Schutzmechanismus abhängig. Prozessmetriken sind indirekt mit Kosten verbunden.
Prozessmodell	Art der Modellierung von Prozessen. Das Prozessmodell besteht aus der Prozesskette (Prozesssequenz) und einem Prozesselement-Modell, das durch Ressourcen und Metriken beschrieben wird.
Prozessschritt	Ein Prozess besteht aus einzelnen Arbeitsschritten, die in ihrer Summe den Prozess ergeben. Ein solcher Schritt wird als Prozessschritt bezeichnet. S. auch Prozesselement.
Prozessstruktur	Ein Prozess wird beschrieben durch die Reihenfolge und die Regeln, gemäß denen die Prozessschritte durchlaufen bzw. abgearbeitet werden. Dies bezeichnet man auch als Prozessstruktur.
Regularien	Handlungsanweisungen, die von legislativer Instanz zur Anwendung auf die Flughafeninfrastruktur vorgegeben werden. Beispiel sind Gesetze, Arbeitsanweisungen, Richtlinien, Vorschriften und Alarmpläne.
Relation	Abhängigkeit zwischen zwei Systemelementen.
Relationsarten	Bedeutung von Relationen zwischen Systemelementen.
Ressourcenmodell	In einem Prozessmodell spezifizieren die Ressourcen die Größen, die mit Kosten verbunden sind. Beispiele sind Betriebs- und Personalkosten, Prozessdurchsatz und –dauer. Prozessressourcen sind vom Bedrohungsszenario und von Schutzmechanismen abhängig. Ein Ressourcenmodell legt ein Kostenmodell zu Grunde.
Restrisiko	Als Restrisiko wird die Gefährdung bezeichnet, die einer Tätigkeit, einer Methode, einem Verfahren oder einem (technischen) Prozess nach dem Stand der Wissenschaft selbst bei Anwendung aller theoretisch möglichen Sicherheitsvorkehrungen (wissenschaftlich denkbaren Vorkehrungen) noch

	anhaftet.
Risiko	Möglichkeit, dass ein Schaden lediglich mit einer Gewissheit eintritt, die nicht ausreicht, um das Vorhandensein einer Gefahr zu begründen. Ein Risiko wird mit einer zweidimensionalen Größe beschreiben, welche die Eintrittswahrscheinlichkeit eines gewissen unerwünschten Ereignisses mit dessen Schadensausmaß verknüpft.
Risikoanalyse	Im Rahmen einer Risikoanalyse wird mittels geeigneter Methoden das vorhandene oder zukünftig erwartete Risiko infolge einer bestimmten Risikoquelle ermittelt.
Risikobewertung	Auswertung der Ergebnisse einer Risikoanalyse. Ziel ist es dabei, eine Einschätzung darüber zu geben, ob die Risiken als eher hoch oder eher niedrig anzusehen sind. Letztendlich schließt sich daran auch die Frage an, ob die ermittelten Risiken als tragbar angesehen werden können.
Risikoereignis	Risikoereignisse sind eingetretene Risiken, die im weiteren Verlauf Folgerisiken mit negativen Auswirkungen auf die Wertschöpfungskette nach sich ziehen können.
Risikokategorie	Zusammenfassung ähnlicher oder ursächlich verwandter Risiken.
Risikomanagement	Ein Risikomanagement hat die Aufgabe, die vorhandenen Risiken zu quantifizieren, bezüglich ihrer Akzeptabilität zu bewerten und auch aktiv (mindernd) auf deren Größe Einfluss zu nehmen. Da es hierfür erforderlich ist, die bestehenden Ursachen und Zusammenhänge zu verstehen, eignen sich als Ausgangspunkt für ein Risikomanagement vor allem Risikoanalysen, die auf kausalen Modellen beruhen.
Risikoreduktion	Die relative Risikoreduktion beschreibt, um wie viel Prozent das Risiko durch eine Intervention verringert wird. Die absolute Risikoreduktion bezeichnet das absolute Ändern eines Ereignisses durch eine Intervention bzw. Behandlung oder auch durch ein Verhalten bezogen auf alle untersuchte Risiken.
Risk Assessment	Der englische Begriff sowohl für Risikoanalyse als auch Risikobewertung.
Schaden	Ein Schaden ist ein Nachteil durch Minderung oder Verlust an materiellen oder immateriellen Gütern. Prinzipiell können im Rahmen von Risikoanalysen und –bewertungen verschiedene Arten von Schäden infolge eines unerwünschten Ereignisses betrachtet werden. Denkbar wären z.B. Todesfälle oder (physische) Verletzungen von Menschen, Umweltschäden, materielle Schäden als auch psychische Folgen.
Schadensausmaß	Größe des Schadens (infolge eines eingetretenen Risikos).
Schadensbewertung	Klassifizierung und Beurteilung von Schadensfällen. Die Schadensursache soll festgestellt werden und Maßnahmen zur Reparatur und zur Vermeidung von Wiederholungsschäden definiert werden.
Schadenskategorie	Schäden können in verschiedenen Formen und aus verschiedenen Gründen auftreten und werden u. a. nach der Art der Schädigung, nach der Schadensursache oder nach dem geschädigten Objekt aufgeschlüsselt.
Schutzmechanismus	Technologie oder personengebundene Aktivität, die am Flughafen angewendet werden kann, um Gefahren für die Flughafensicherheit zu vermeiden oder zu verringern. Schutzmechanismen werden unterteilt präventive und reaktive (im Krisenfall anzuwendende). Auch Sicherheitsmaßnahme genannt.
Architektur-Schicht	Eine Schichtenarchitektur oder Schichtenmodell ist ein angewandtes

	Strukturierungsprinzip für die Architektur von Softwaresystemen. Dabei werden einzelne Aspekte des Softwaresystems konzeptionell einer Schicht zugeordnet. Die erlaubten Abhängigkeitsbeziehungen zwischen den Aspekten werden bei einer Schichtenarchitektur dahingehend eingeschränkt, dass Aspekte einer „höheren" Schicht nur solche „tieferer" Schichten verwenden dürfen. Die den Schichten zugeordneten Aspekte können dabei je nach Art des Systems oder dem Detaillierungsgrad der Betrachtung z. B. Funktionalitäten, Komponenten oder Klassen sein.
Sicherheit	Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird. Mit dieser Definition ist Sicherheit sowohl auf ein einzelnes Individuum als auch auf andere Lebewesen, auf unbelebte reale Objekte oder Systeme wie auch auf abstrakte Gegenstände bezogen.
Sicherheitsäquivalent	Schadens- oder Gewinnbetrag, der nicht mit Unsicherheit behaftet ist und für den Risikoträger genau so viel wert ist wie das Risiko selbst.
Sicherheitsbereich	Bereich des Flughafengeländes, der nur von Passagieren und Personal mit besonderen Aufgaben nach Durchlaufen von Sicherheitsmaßnahmen zu betreten ist.
Sicherheits-maßnahmen	S. Schutzmechanismen
Sicherheitssystem	Funktionell abgeschlossene Einheit von Sicherheitsmaßnahmen.
Simulation	Die Simulation oder Simulierung ist eine Vorgehensweise zur Analyse von Systemen, die für die theoretische oder formelmäßige Behandlung zu kompliziert sind. Bei der Simulation werden Experimente an einem Modell durchgeführt, um Erkenntnisse über das reale System zu gewinnen.
Stakeholder	Als Stakeholder wird eine Person oder eine Institution bezeichnet, die ein Interesse am Verlauf oder Ergebnis eines Prozesses hat.
Systemanalyse	Betrachtung der strukturellen, logischen Zusammenhänge zwischen den Systemelementen.
Systemelemente	Kleinste betrachtete Einheit in der Systemanalyse. Jedes Systemelement gehört zu genau einer Domäne und kann Abhängigkeiten zu anderen Systemelementen aufweisen.
Szenariobuilder	Methodik und Software-Werkzeug zur Bestimmung konsistenter, plausibler Bedrohungsszenarios aus Kombinationen von Bedrohungsaspekten.
Szenario-Cluster	Sammlung ähnlicher Szenarien.
Täter	Person, die durch ihr Handeln oder ihre Absicht eine Bedrohung der Flughafensicherheit bewirkt.
Use Case	Allgemein sichtbare Nutzung des betrachteten Infrastruktursystems (Flughafen). Ein Use Case setzt sich aus einem Akteur und einer Aktion zusammen.
Wahrscheinlichkeit	Die Wahrscheinlichkeit eines Ereignisses gibt den Quotienten der Anzahl der tatsächlichen oder erwarteten Realisierungen des Ereignisses und der Anzahl der theoretisch möglichenRealisierungen an.

ANHANG B: ANWENDUNGSBEISPIEL DES POC

STARTSEITE

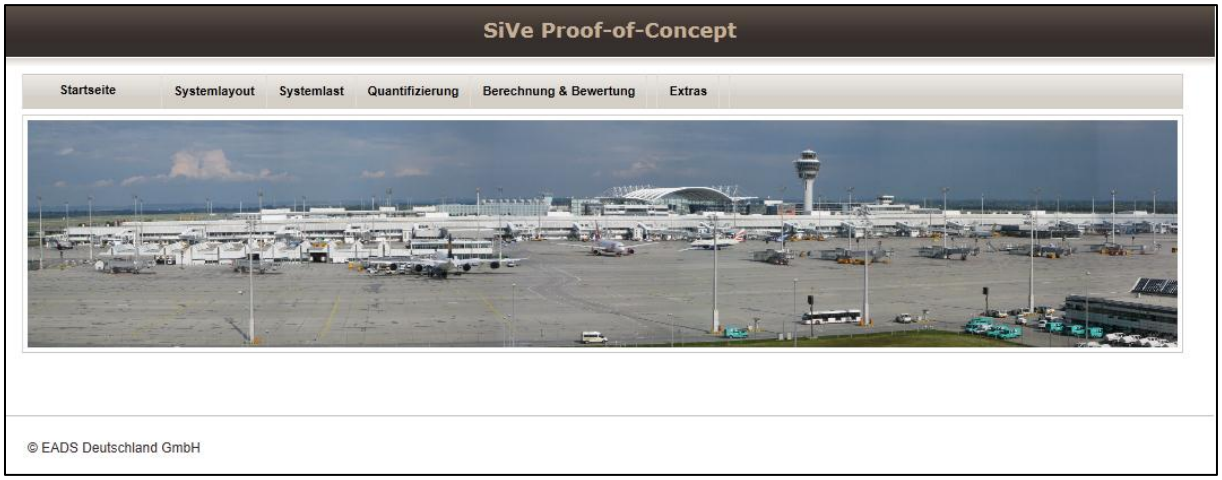


Abbildung 34: Startseite.

SYSTEMLAYOUT

Quantifizierung der Schutzmechanismen

Abbildung 35: Auswahl Schutzmechanismen anlegen und quantifizieren.

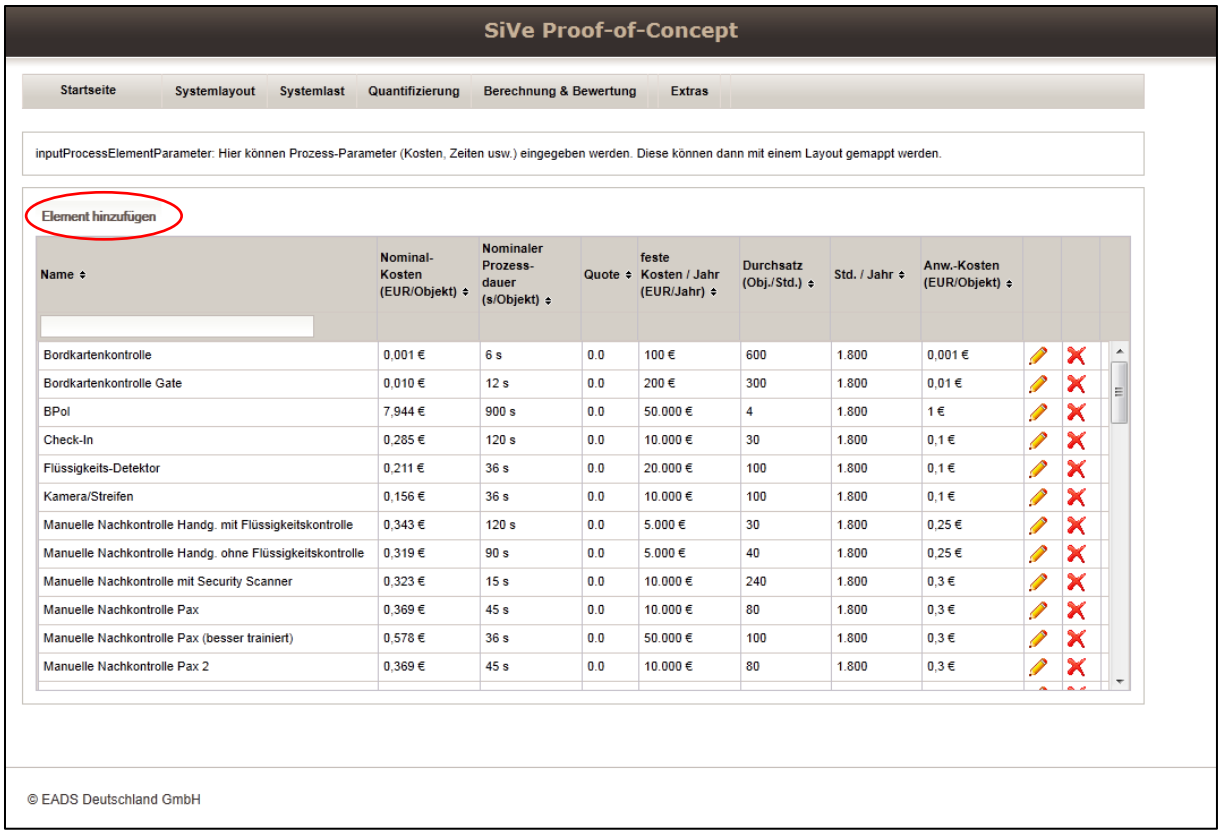


Abbildung 36: Anlegen (rot markiert) und Quantifizierung von Schutzmechanismen.

Layoutmodellierung

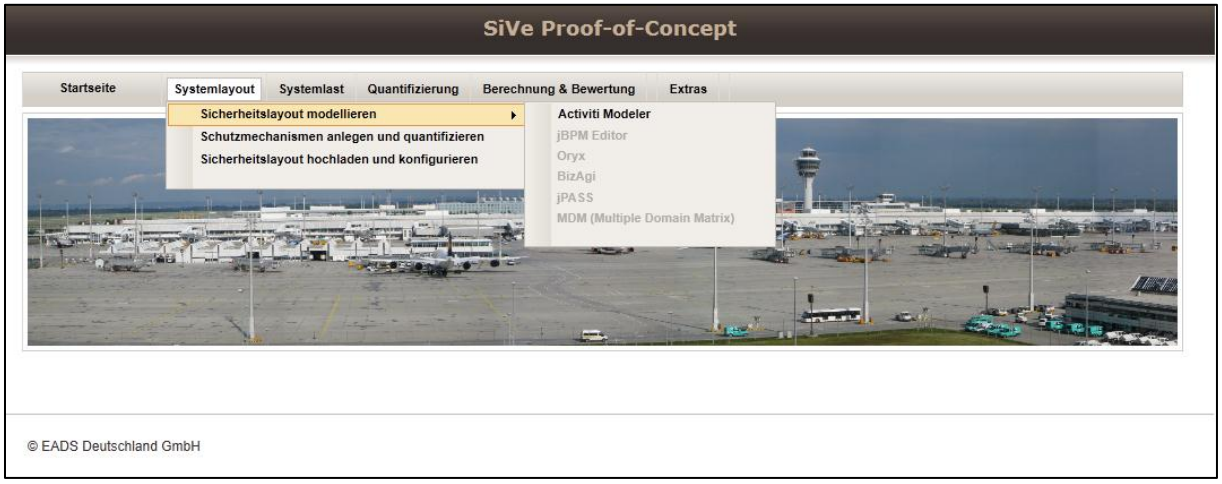


Abbildung 37: Auswahl Sicherheitslayout modellieren.

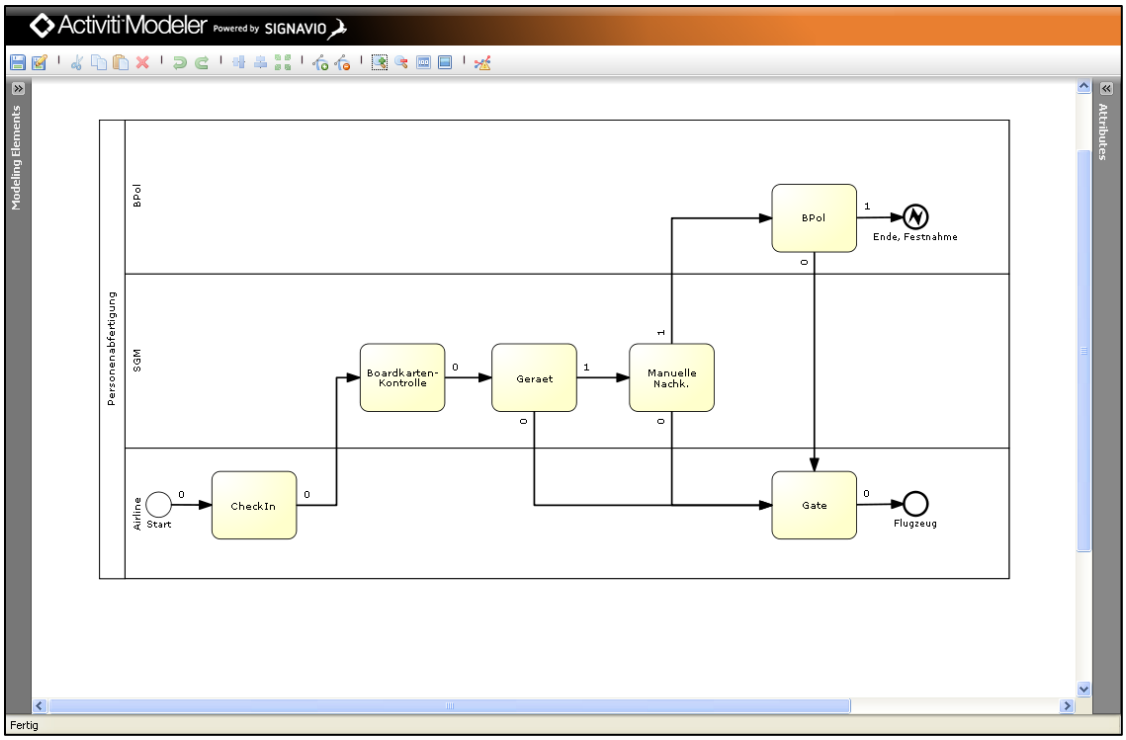


Abbildung 38: Layoutmodell im Activiti-Modeler nach den Modellierungskonventionen im PoC.

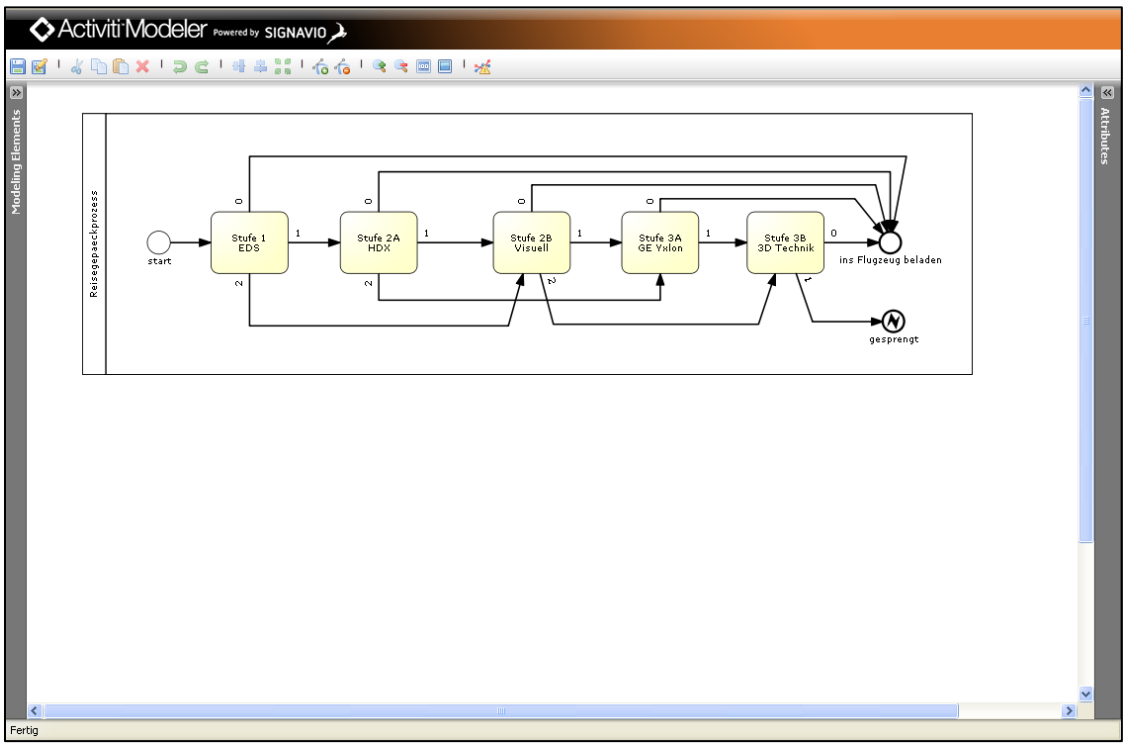


Abbildung 39: Beispiel der Reisegepäckkontrolle.

Prozess-/Layoutmodelle hochladen und konfigurieren

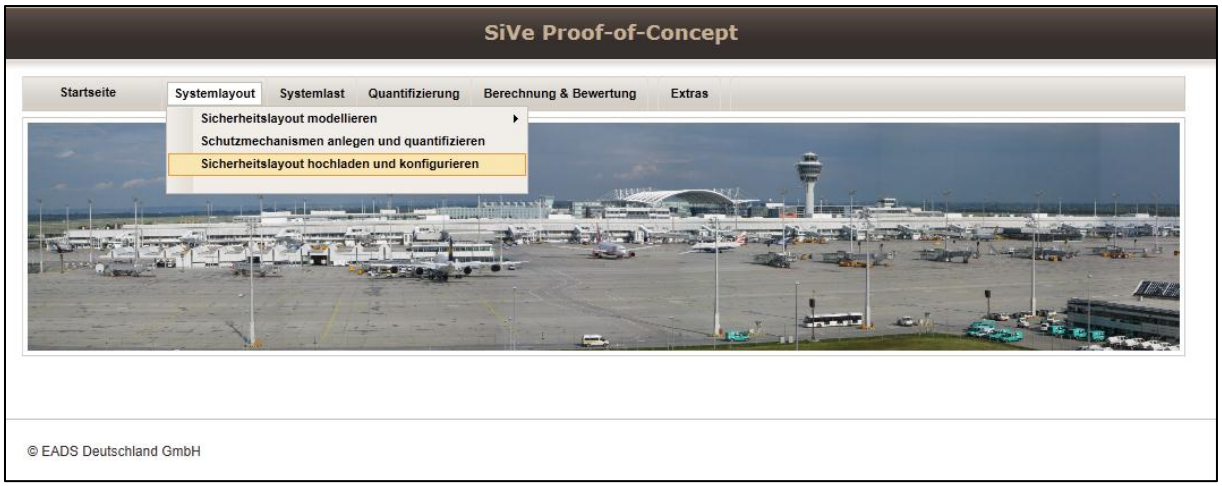


Abbildung 40: Auswahl Sicherheitslayout hochladen und konfigurieren.

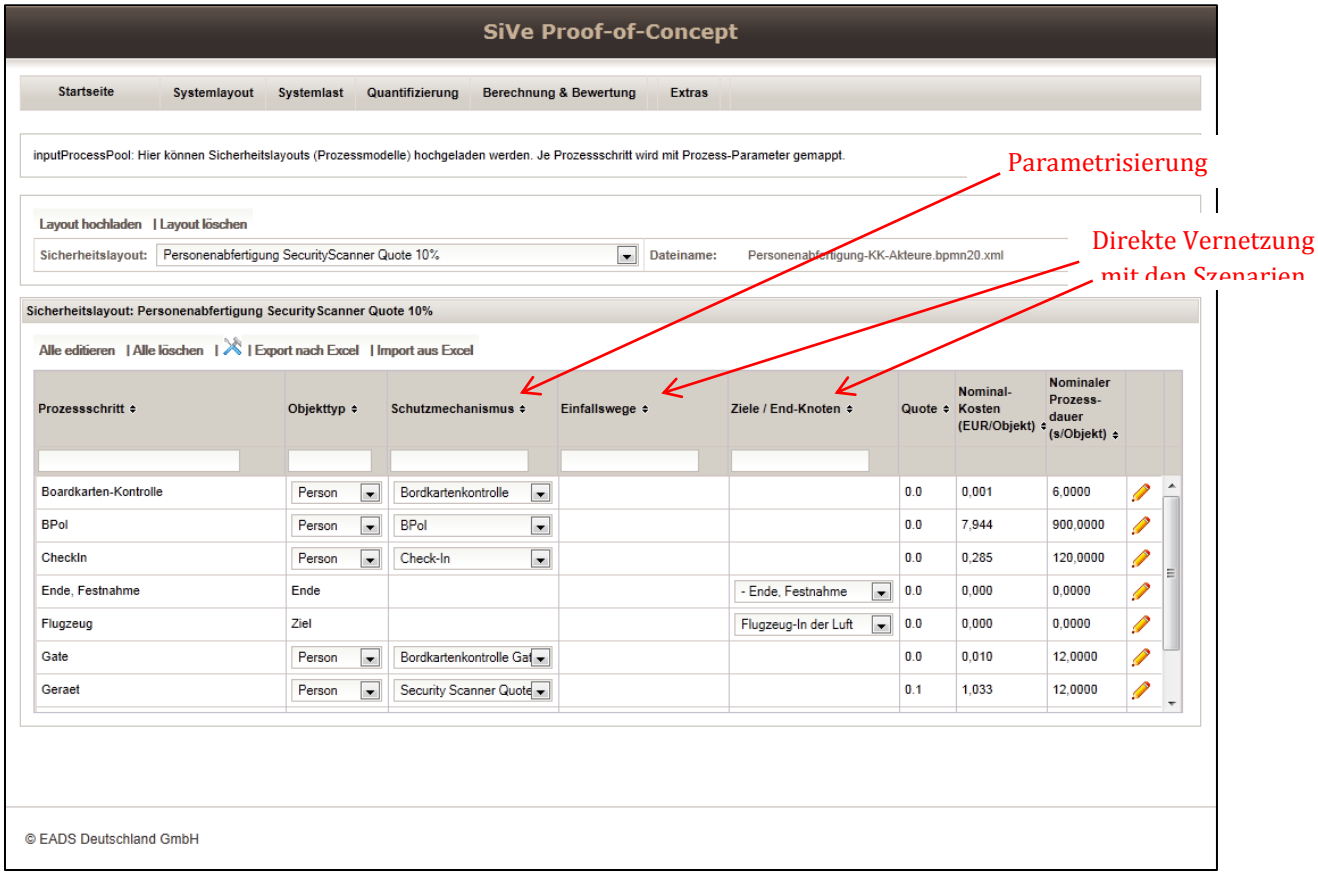


Abbildung 41: Beispiel der Personenabfertigung mit dem Security-Scanner (Konfiguration durch Parametrisierung und Vernetzung mit Situationsaspekten).

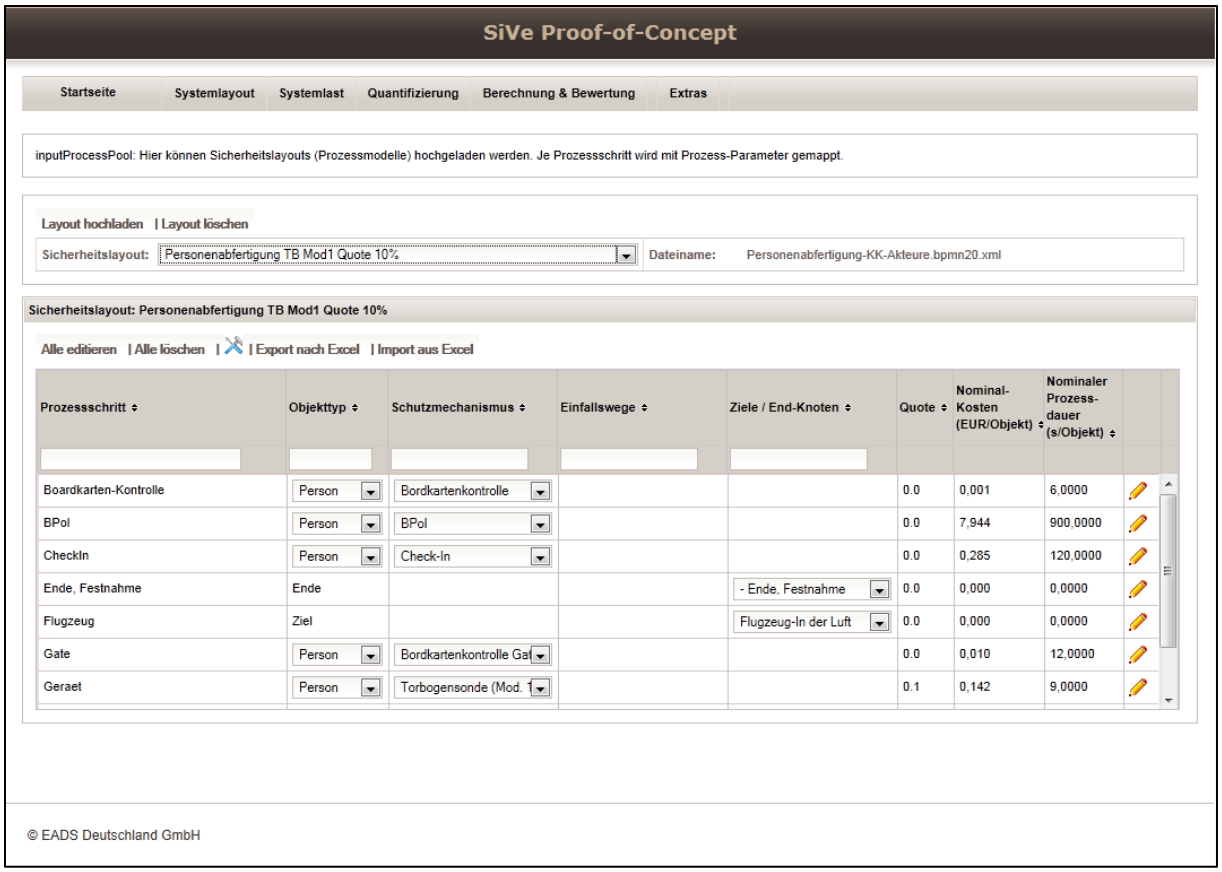


Abbildung 42: Beispiel der Personenabfertigung mit dem klassischen Metaldetektor (Torbogensonde).

Layoutmodell hochladen

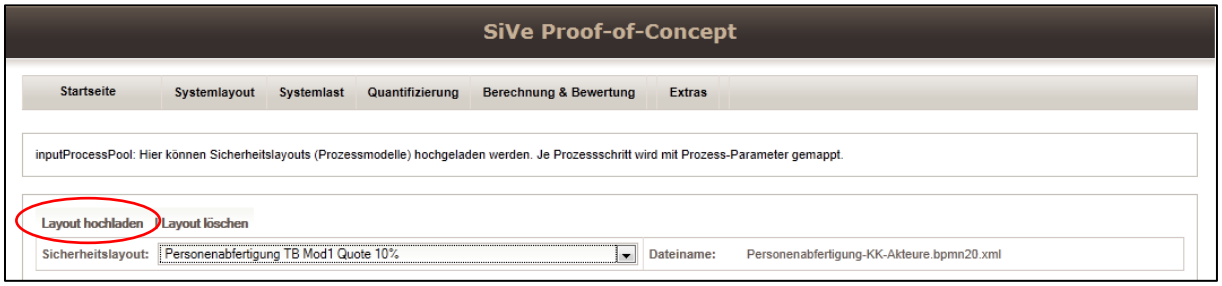


Abbildung 43: Auswahl Sicherheitslayout hochladen.

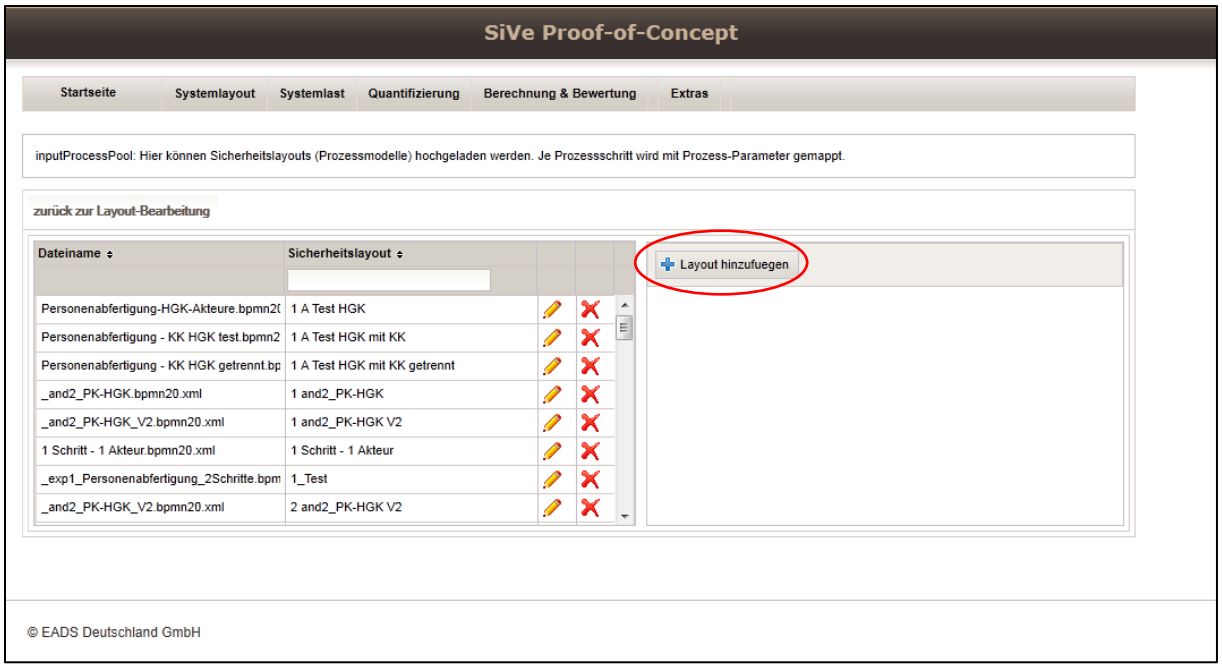


Abbildung 44: Sicherheitslayout hochladen (Upload von XML-Dateien – XML-Schnittstelle).

SITUATIONSBEZOGENE QUANTIFIZIERUNG DER SCHUTZMECHANISMEN

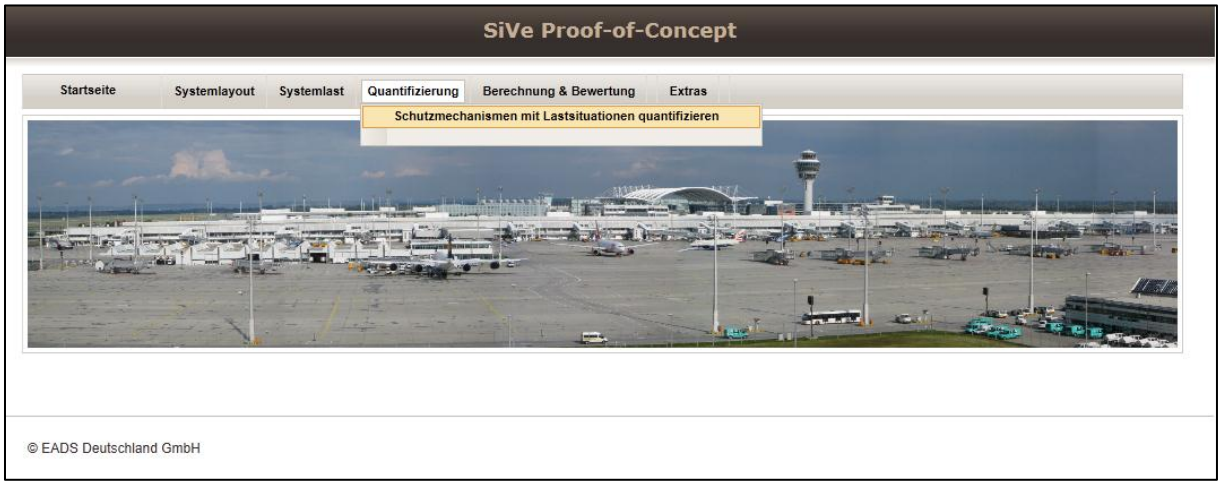
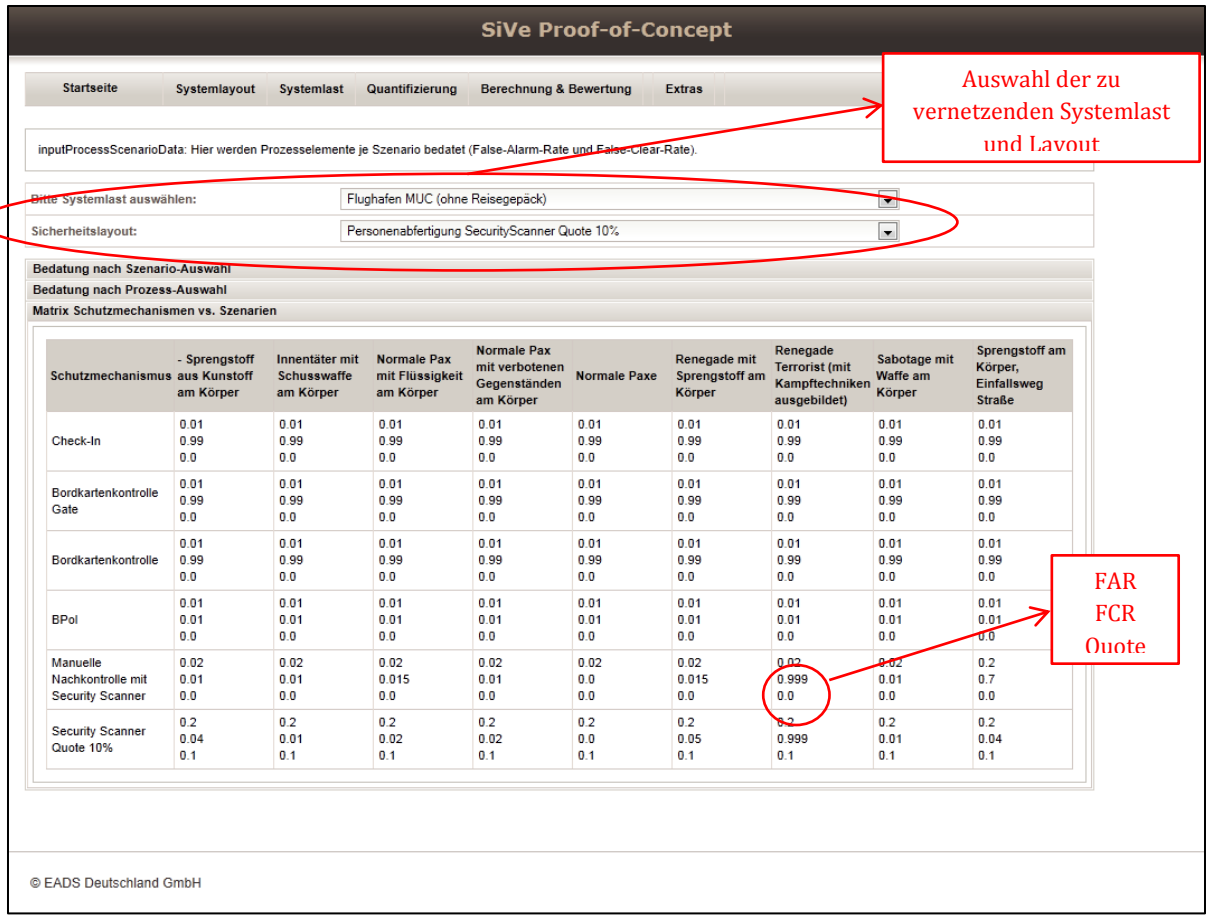


Abbildung 45: Auswahl situationsbezogene Quantifizierung der Schutzmechanismen (Vernetzung).



Schutzmechanismus	- Sprengstoff aus Kunstoff am Körper	Innentäter mit Schusswaffe am Körper	Normale Pax mit Flüssigkeit am Körper	Normale Pax mit verbotenen Gegenständen am Körper	Normale Paxe	Renegade mit Sprengstoff am Körper	Renegade Terrorist (mit Kampftechniken ausgebildet)	Sabotage mit Waffe am Körper	Sprengstoff am Körper, Einfallsweg Straße
Check-In	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0
Bordkartenkontrolle Gate	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0
Bordkartenkontrolle	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0	0.01 0.99 0.0
BPol	0.01 0.01 0.0	0.01 0.01 0.0	0.01 0.01 0.0	0.01 0.01 0.0	0.01 0.01 0.0	0.01 0.01 0.0	0.01 0.01 0.0	0.01 0.01 0.0	0.01 0.01 0.0
Manuelle Nachkontrolle mit Security Scanner	0.02 0.01 0.0	0.02 0.01 0.0	0.02 0.015 0.0	0.02 0.01 0.0	0.02 0.0 0.0	0.02 0.015 0.0	0.02 0.999 0.0	0.02 0.01 0.0	0.2 0.7 0.0
Security Scanner Quote 10%	0.2 0.04 0.1	0.2 0.01 0.1	0.2 0.02 0.1	0.2 0.02 0.1	0.2 0.0 0.1	0.2 0.05 0.1	0.2 0.999 0.1	0.2 0.01 0.1	0.2 0.04 0.1

Abbildung 46: Auszug der Quantifizierung der Schutzmechanismen (Zeilen) nach Szenarien (Spalten).

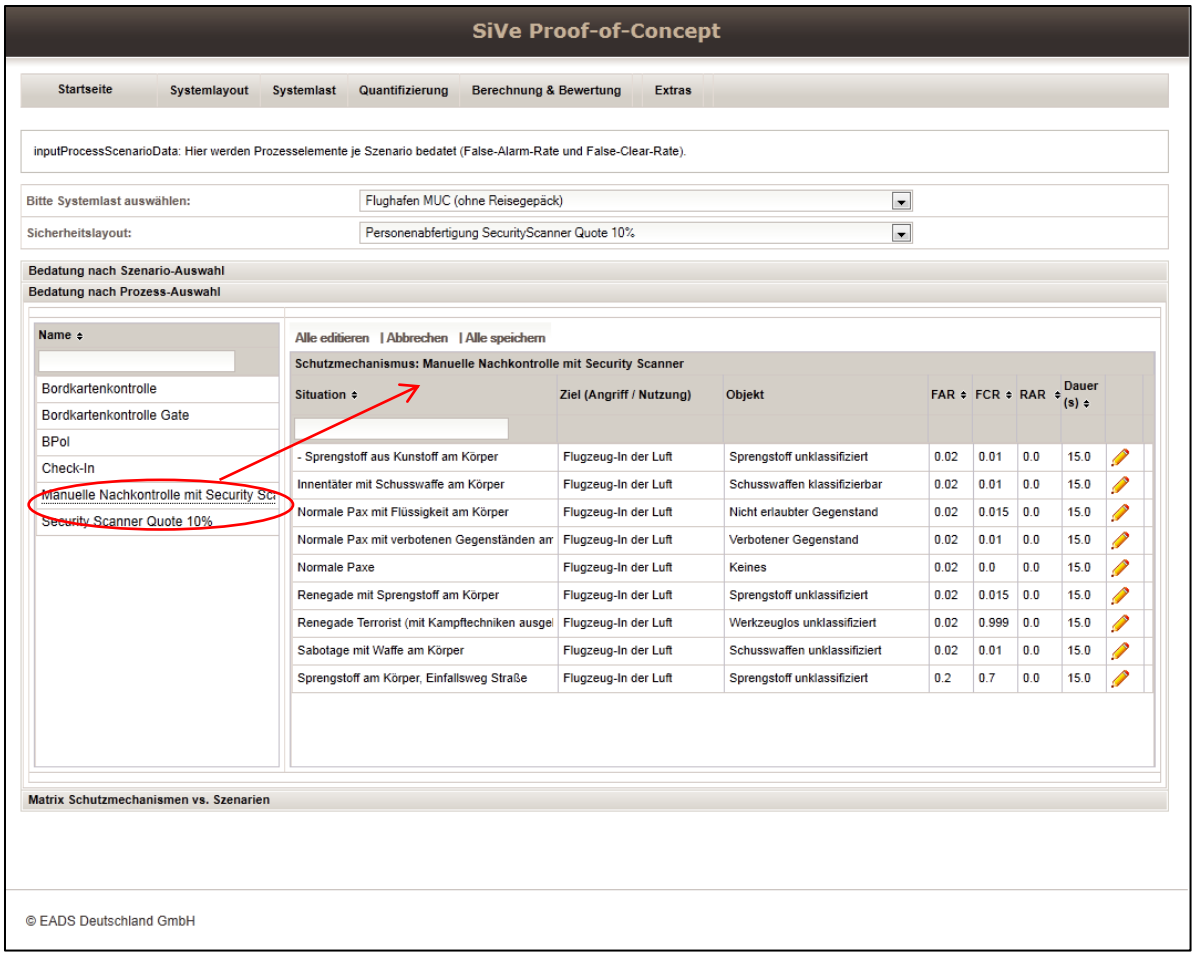


Abbildung 47: Eingabe der FAR und FCR nach Situationen nach Auswahl eines Schutzmechanismus.

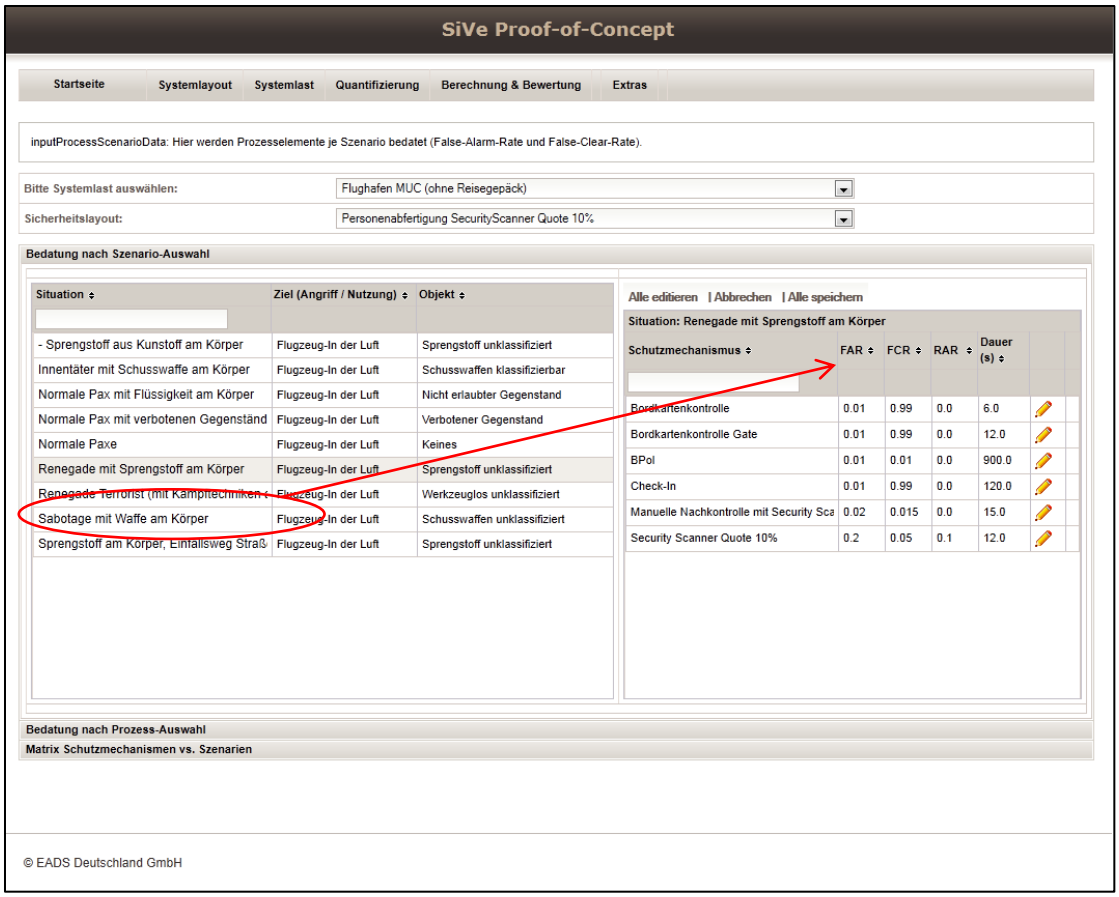


Abbildung 48: Eingabe der FAR und FCR nach Schutzmechanismen nach Auswahl einer Situation.

SYSTEMLAST

Modellierung der Bedrohungs- und Lastsituationen

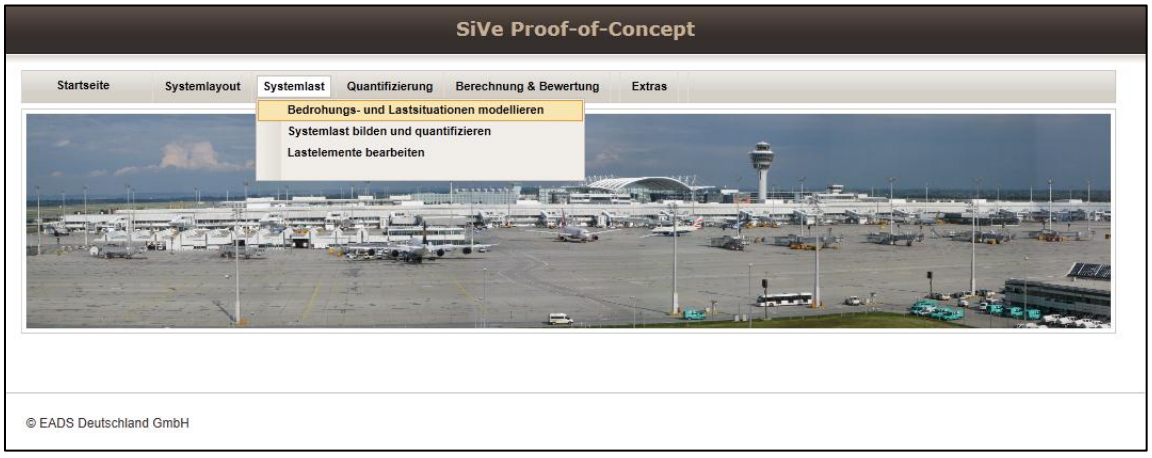


Abbildung 49: Auswahl Modellierung der Situationen.

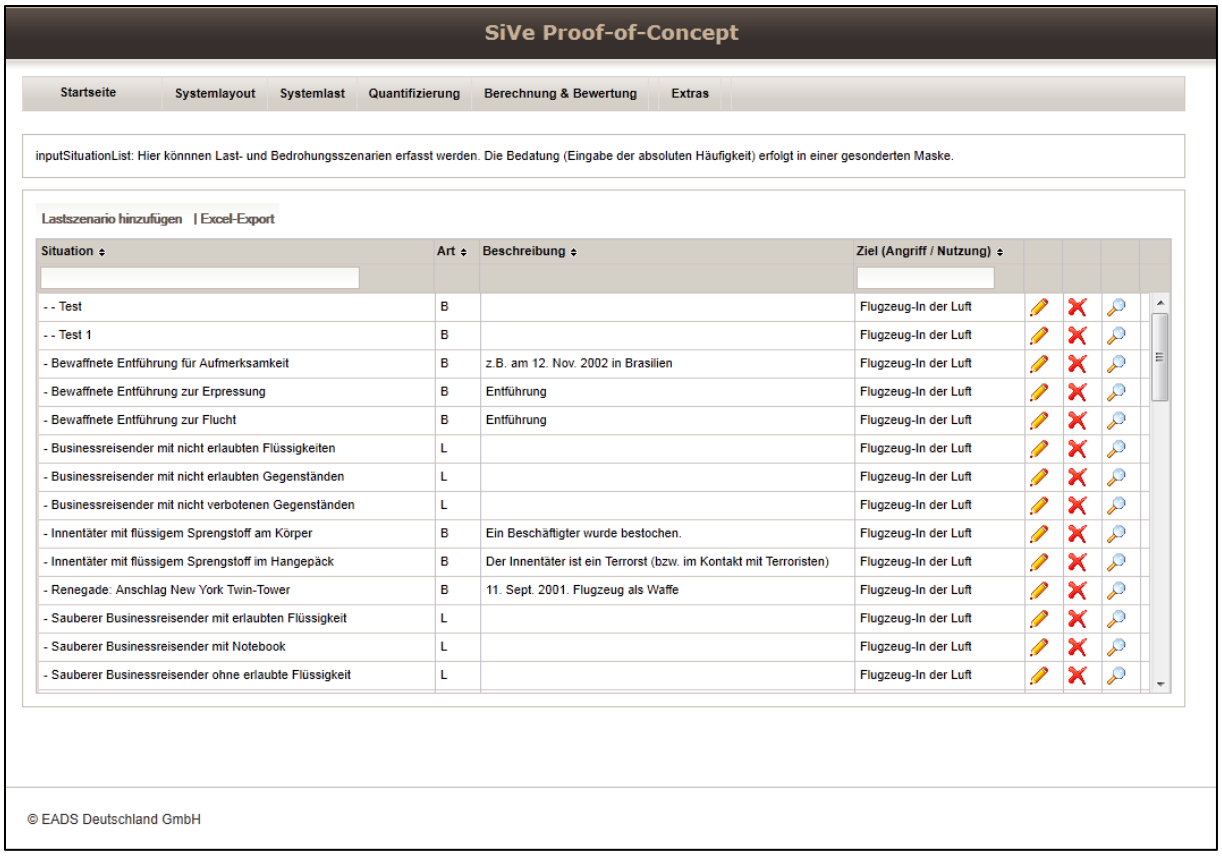


Abbildung 50: Die Situationsdatenbank mit allen möglichen Bedrohungs- und Lastsituationen. Historische Bedrohungsfälle sind auch eingetragen.

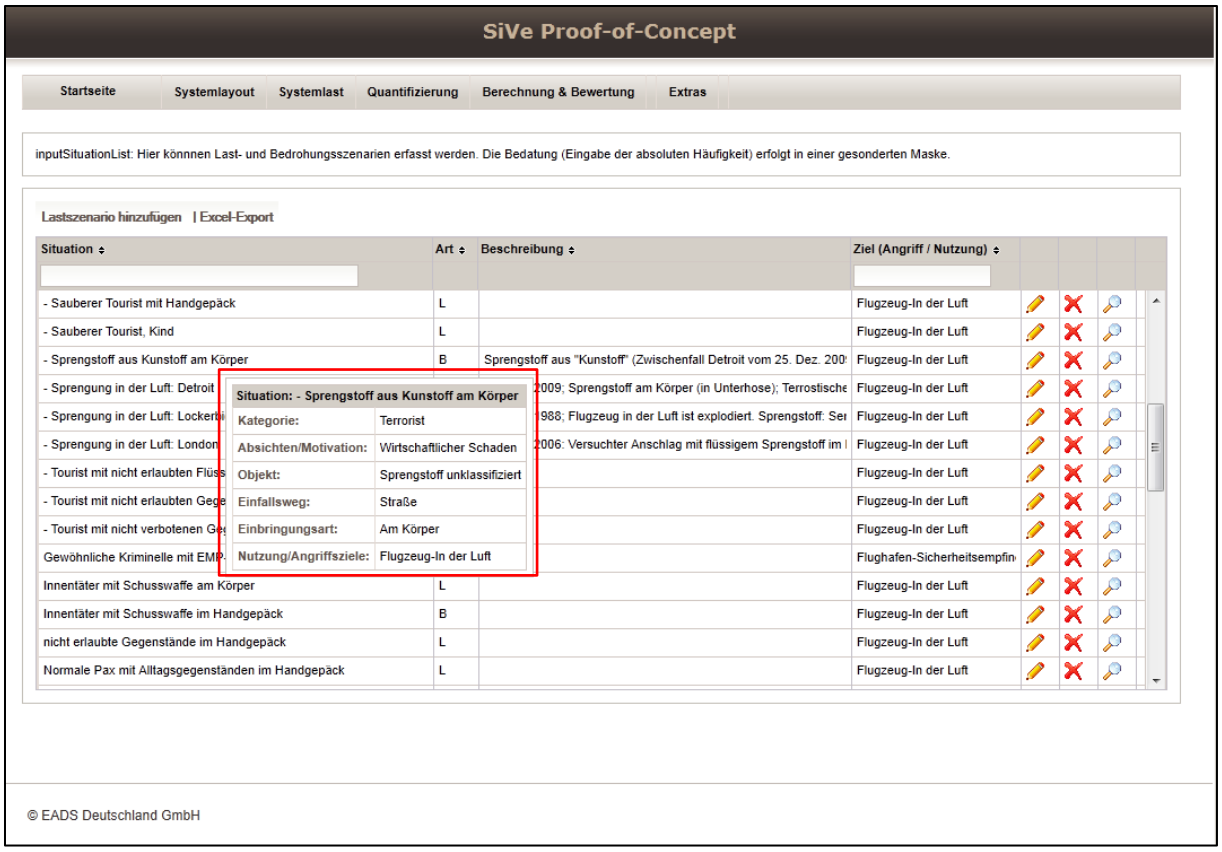


Abbildung 51: Die Aspekte, die eine Situation definieren, sind: Kategorie, Ziel, Absichten bzw. Motivation, Objekt bzw. Werkzeug, Einbringungsart des Objektes, Einfallsweg.

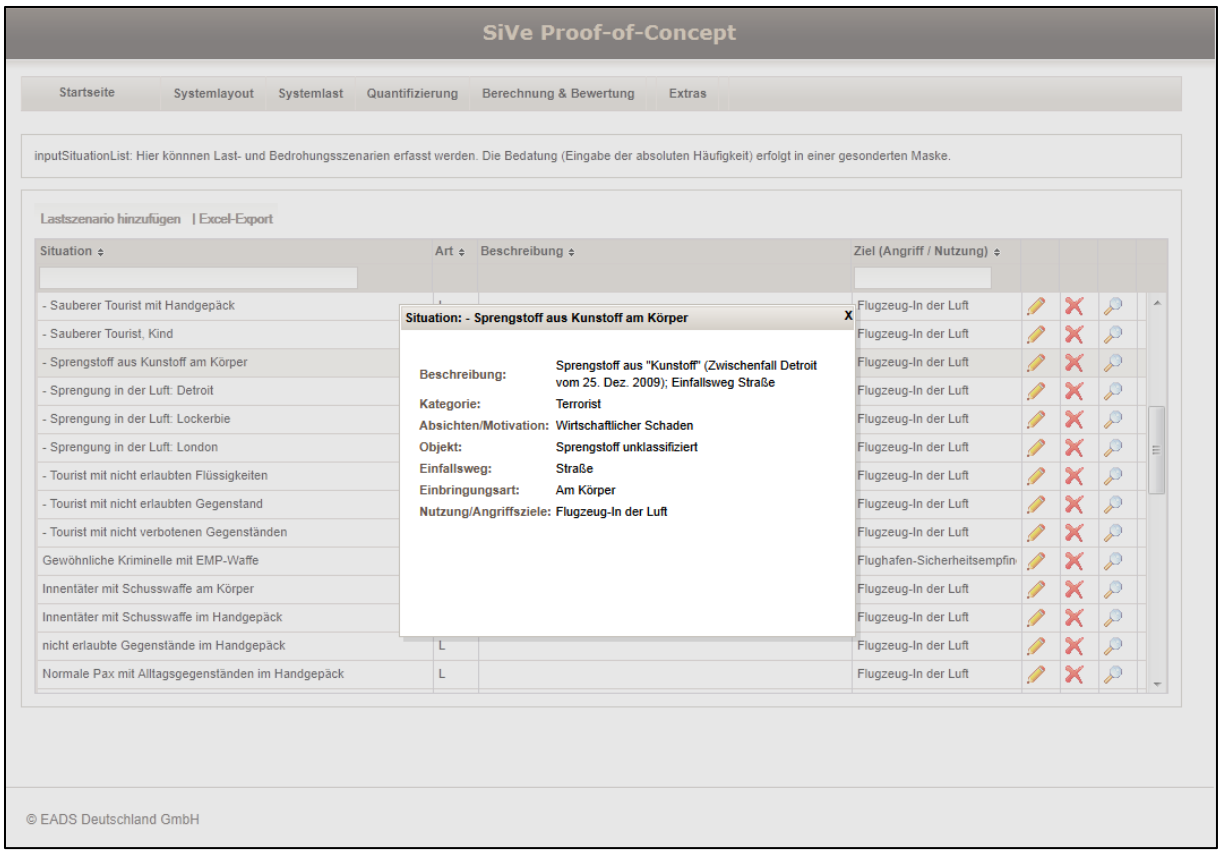


Abbildung 52: Wie Abbildung 51.

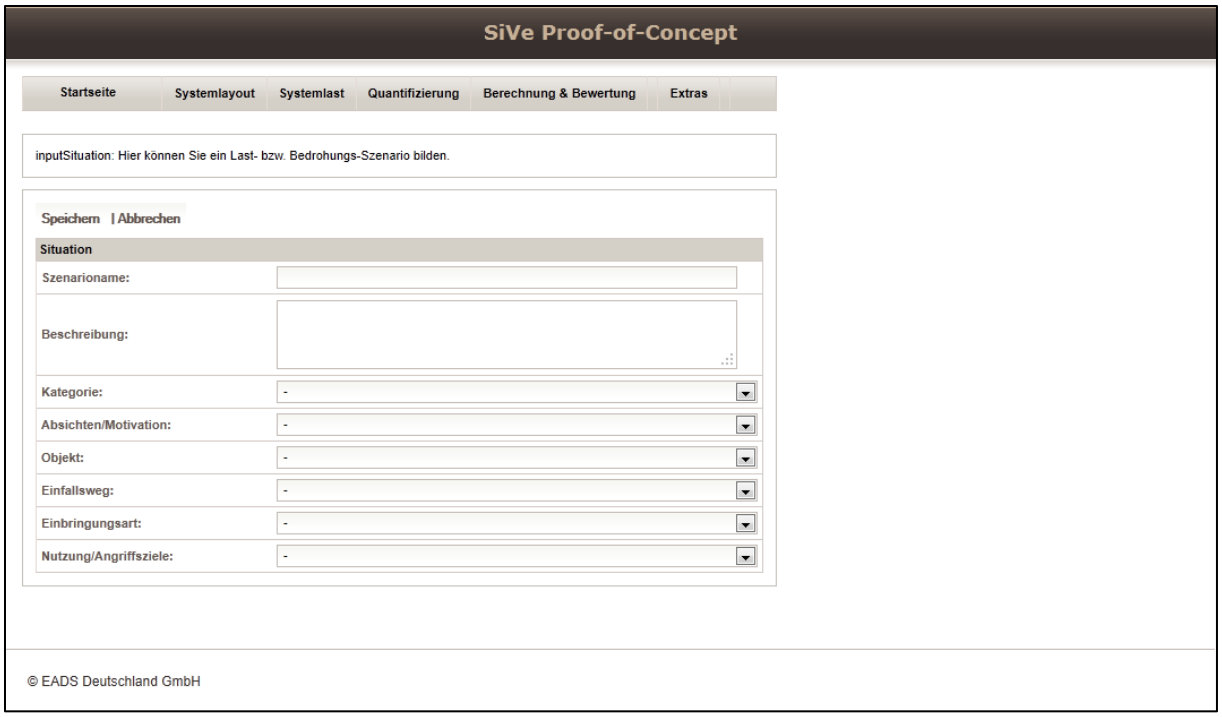


Abbildung 53: Die „Szenario“-Datenbank kann mit neuen Last-/Bedrohungssituationen ergänzt werden.

Erstellung und Quantifizierung einer Systemlast

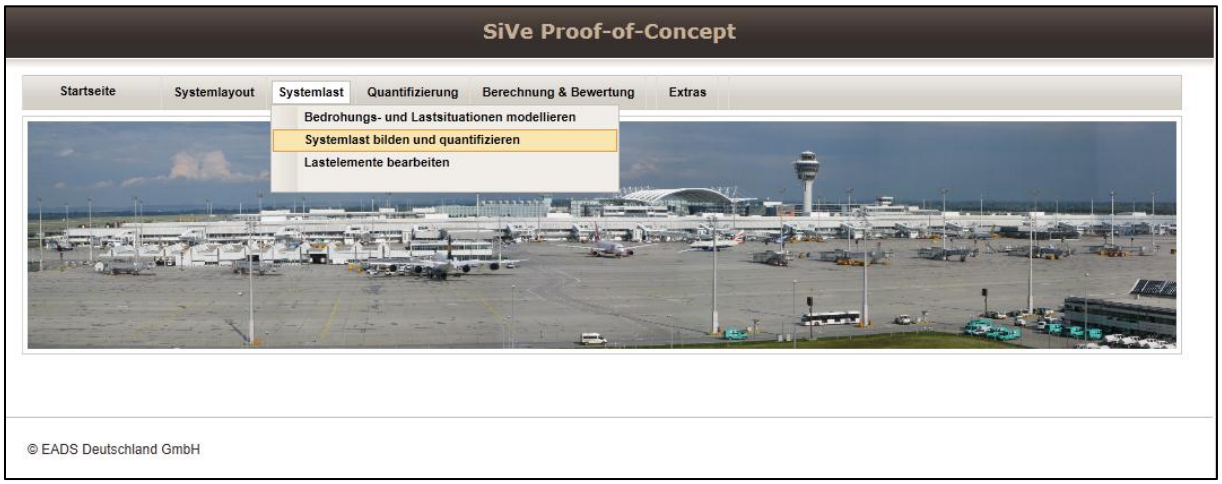


Abbildung 54: Auswahl situationsbezogene Quantifizierung der Schutzmechanismen (Vernetzung).

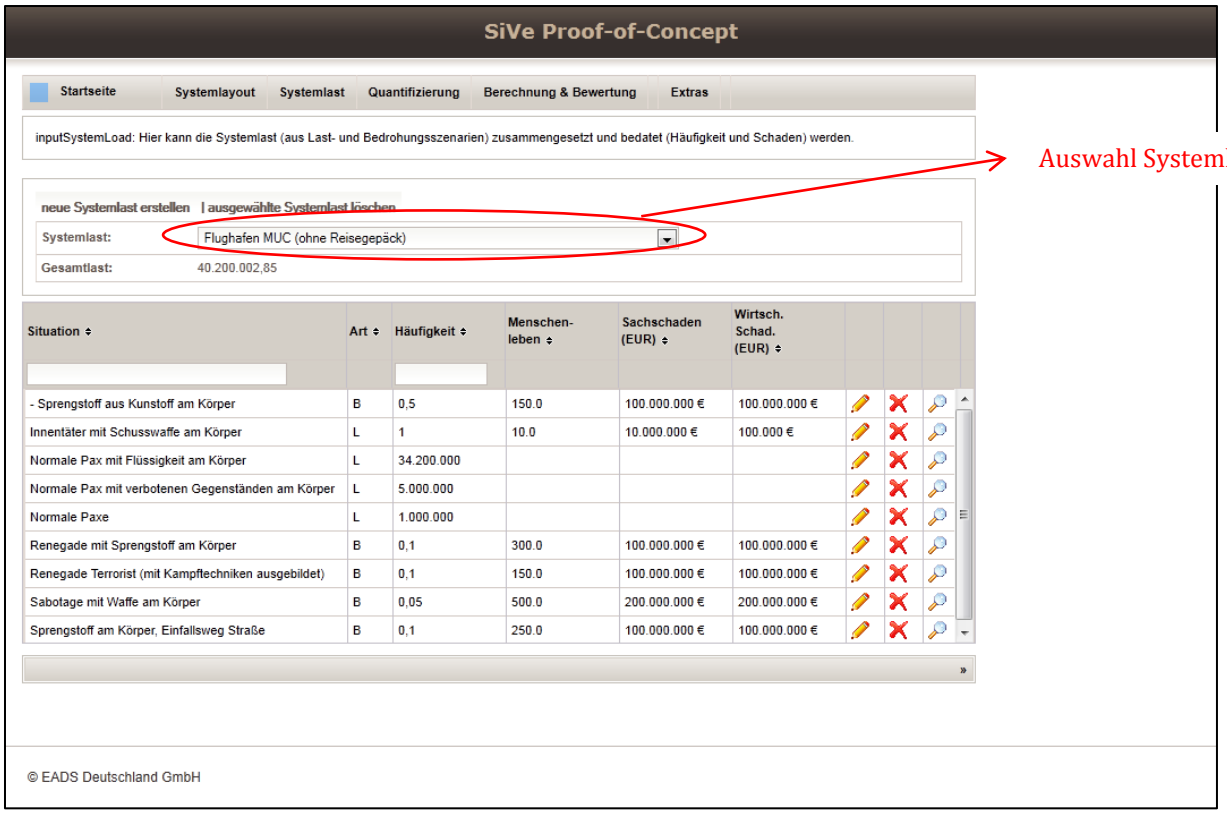


Abbildung 55: Systemlast.

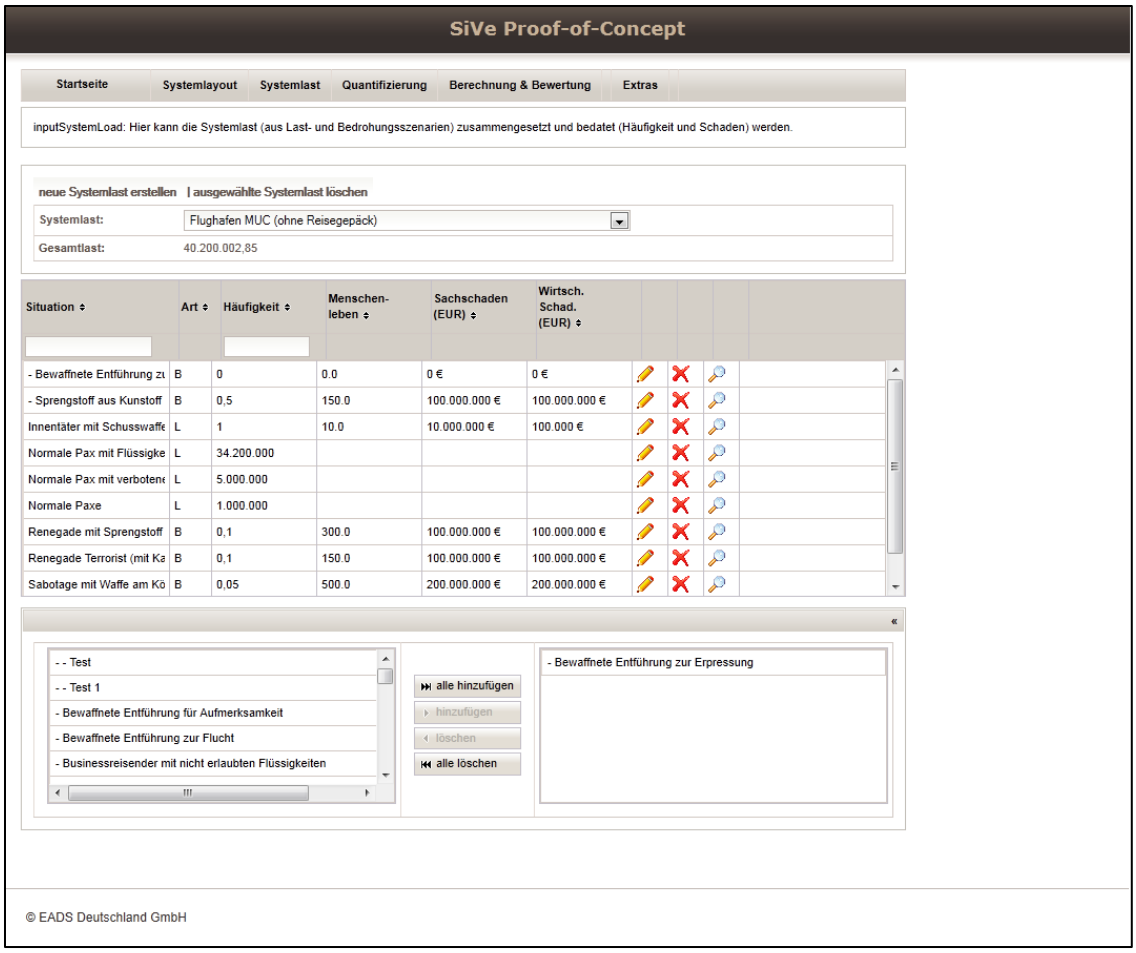


Abbildung 56: Auswahl von Situationen zur Bildung einer Systemlast.

Verwaltung der Szenario-Aspekte

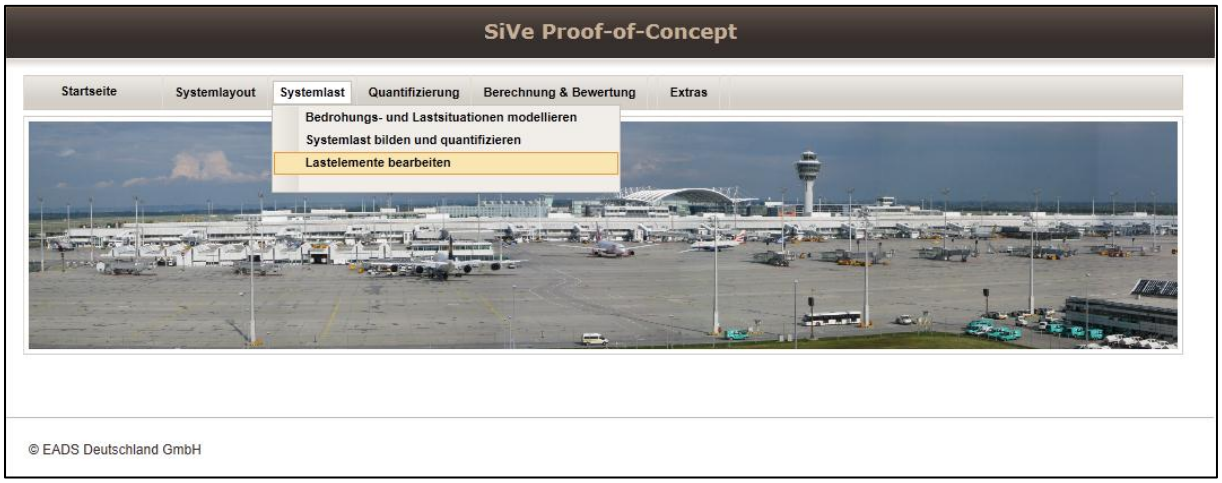


Abbildung 57: Auswahl zur Verwaltung der Situationselemente.

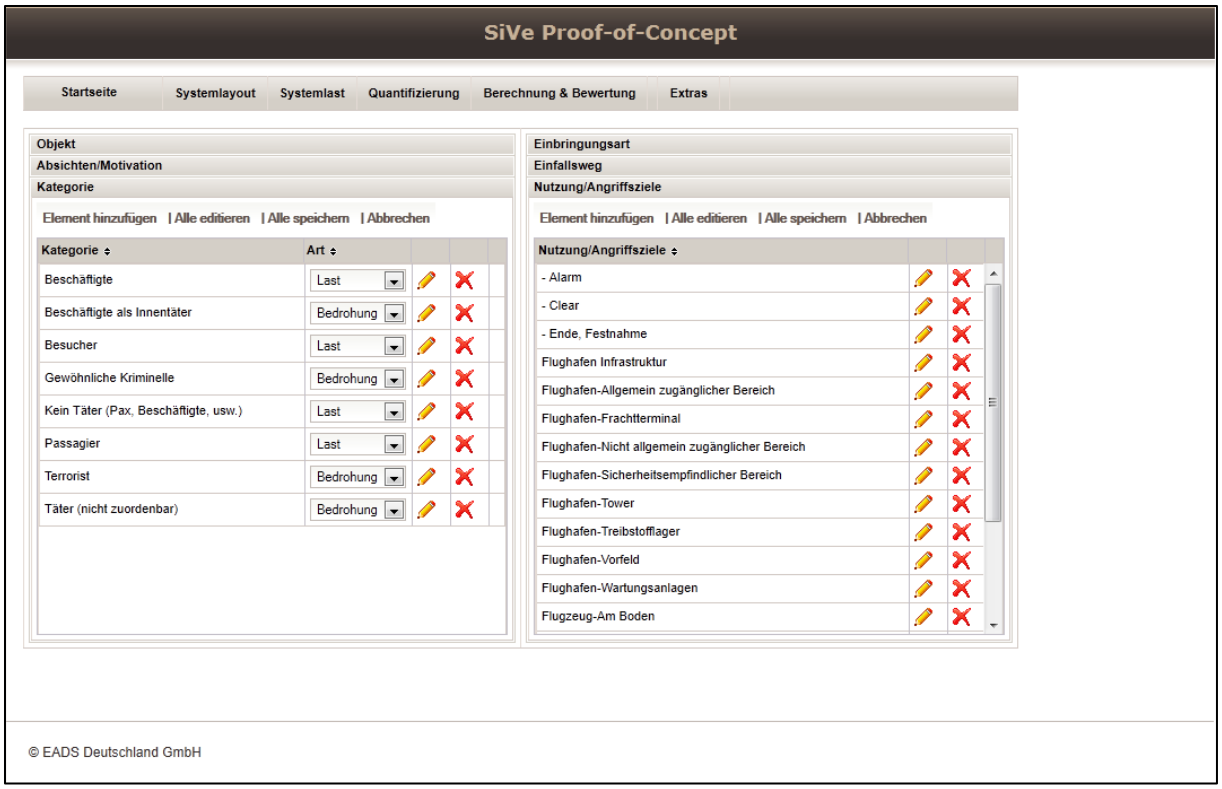


Abbildung 58: Verwaltung der Situationsaspekte Kategorie und Ziele.

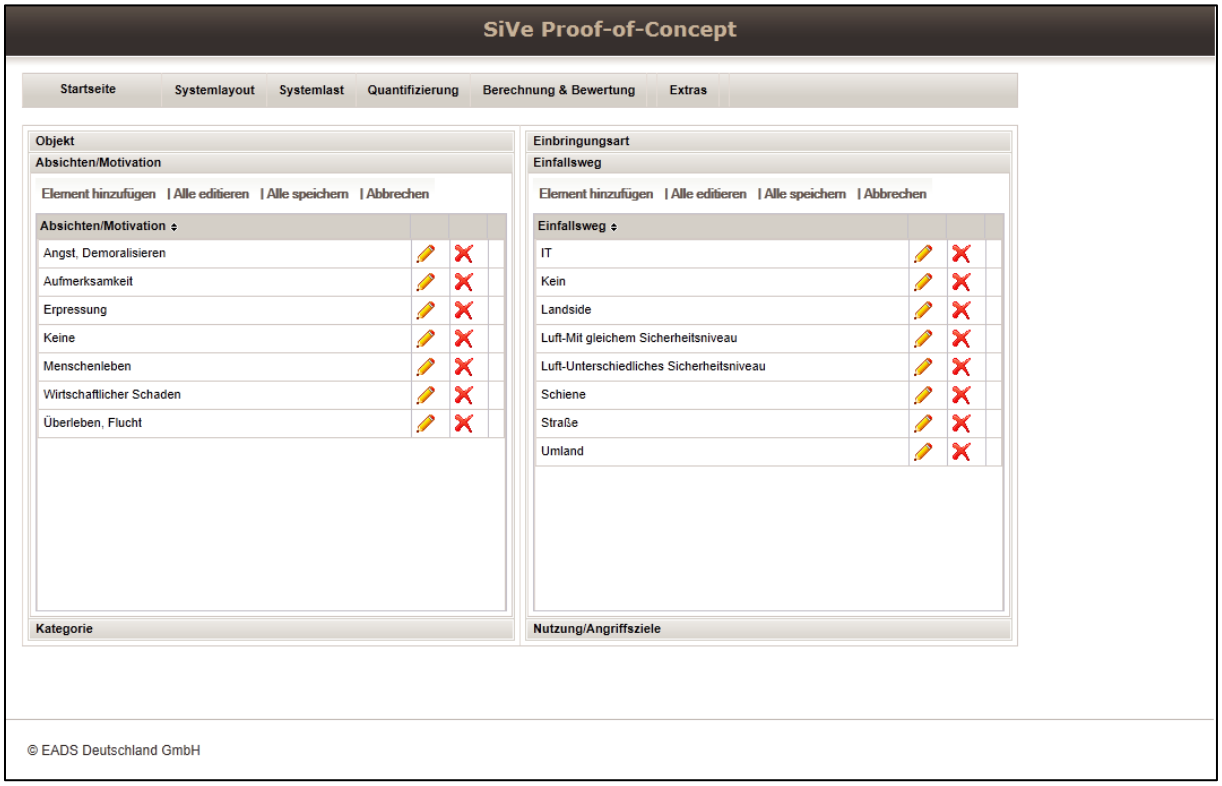


Abbildung 59: Verwaltung der Situationsaspekte Absichten und Einfallswege.

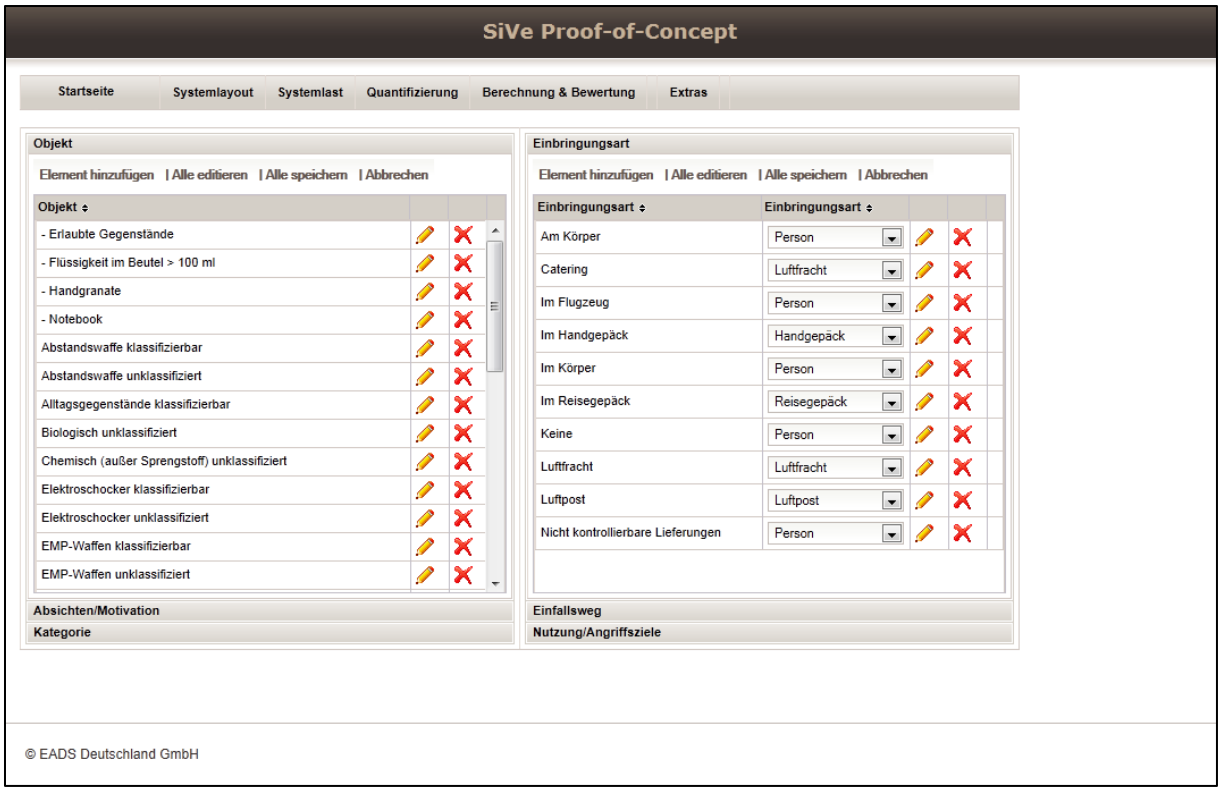


Abbildung 60: Verwaltung der Situationsaspekte Objekt (Werkzeuge) und Einbringungsart.

BERECHNUNG & BEWERTUNG

Berechnung der Kosten-/Nutzen und Rest-Risiken

Abbildung 61: Auswahl zur Erstellung von Berechnungsstudien.

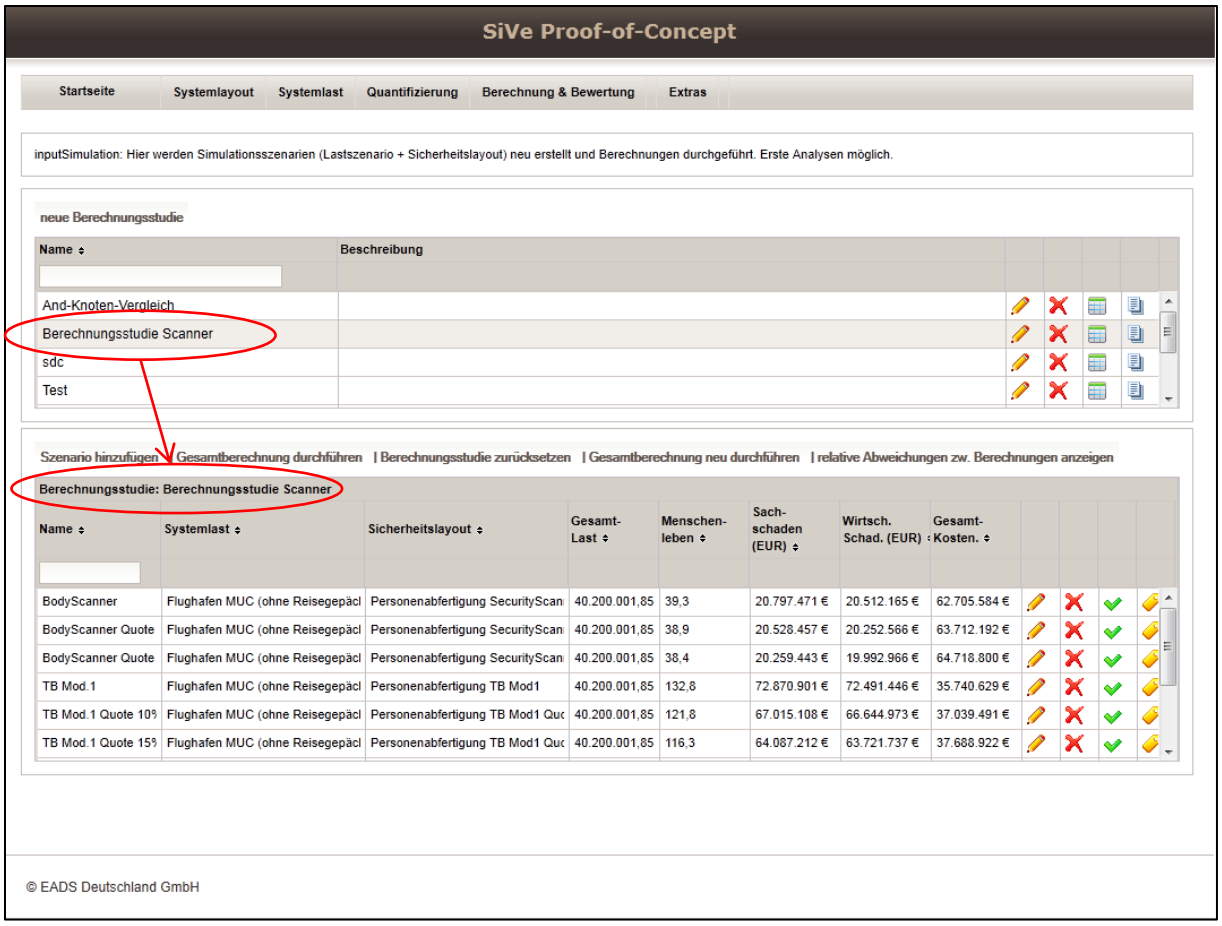


Abbildung 62: Berechnungsstudie als Zusammenstellung von Szenarien. Ein Szenario stellt sich aus einer Systemlast und einem Layout zusammen.

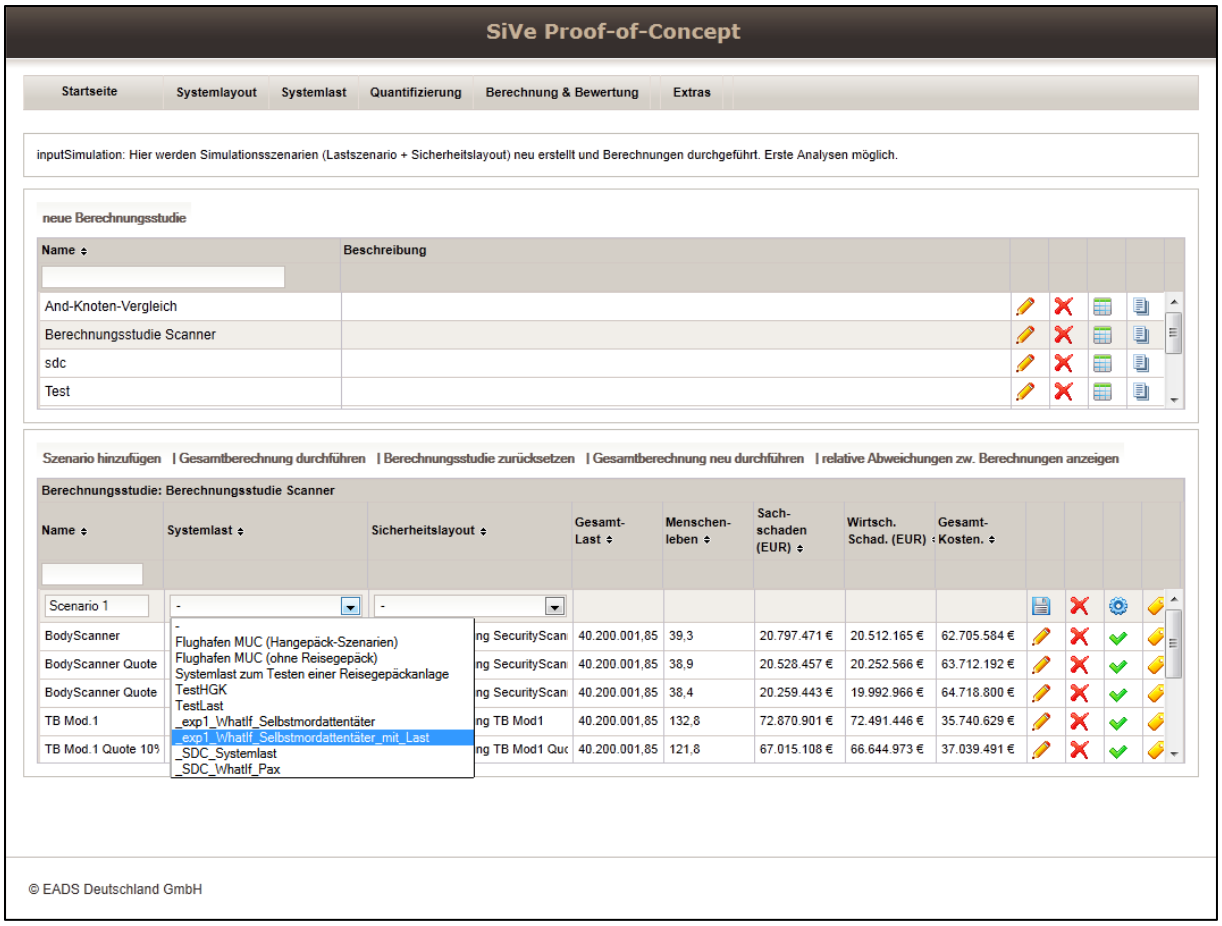


Abbildung 63: Erstellung eines Szenarios aus Systemlast und Layout (s Abbildung 64) (aus den Dropdown-Listen auswählbar)..

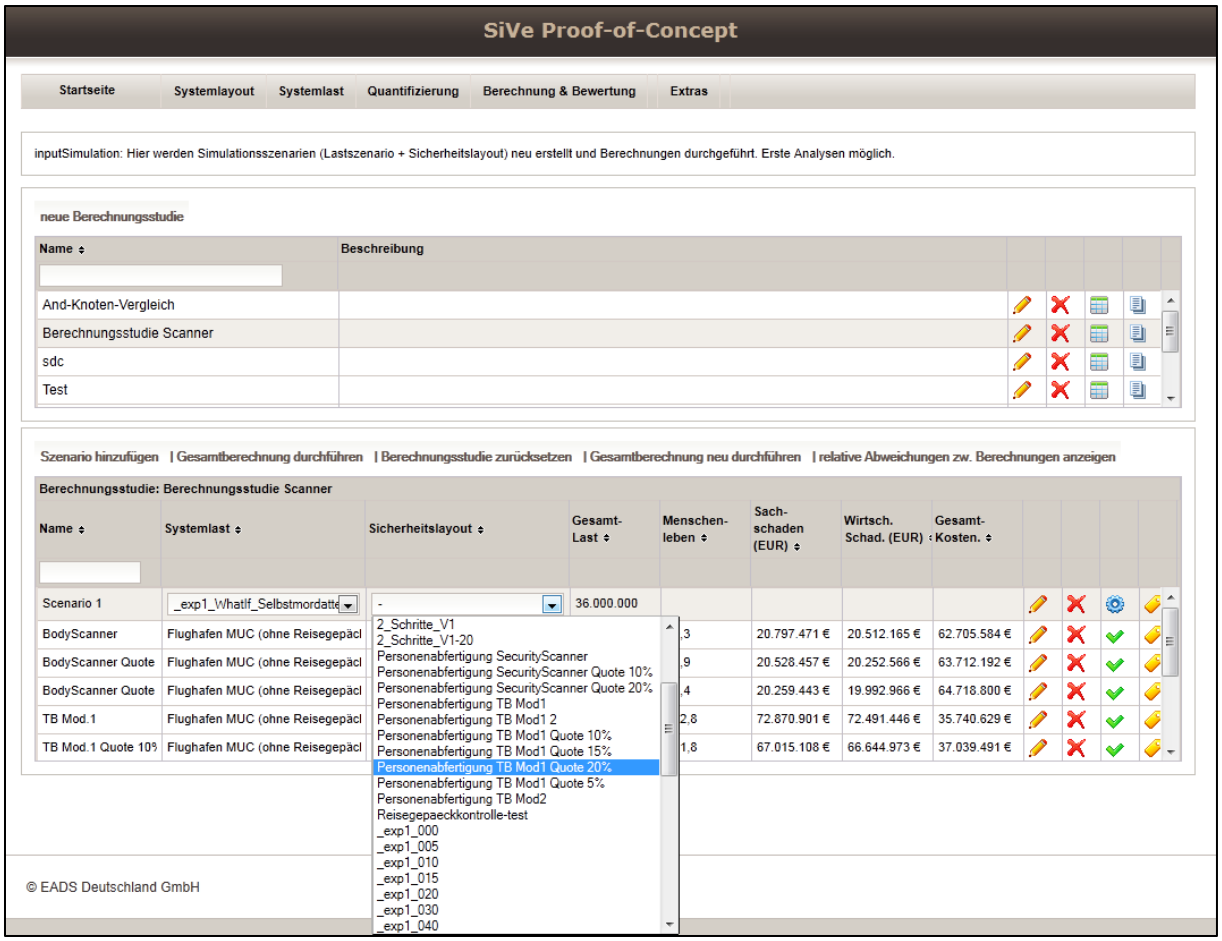


Abbildung 64: Fortsetzung Abbildung 63.

DATENANALYSE

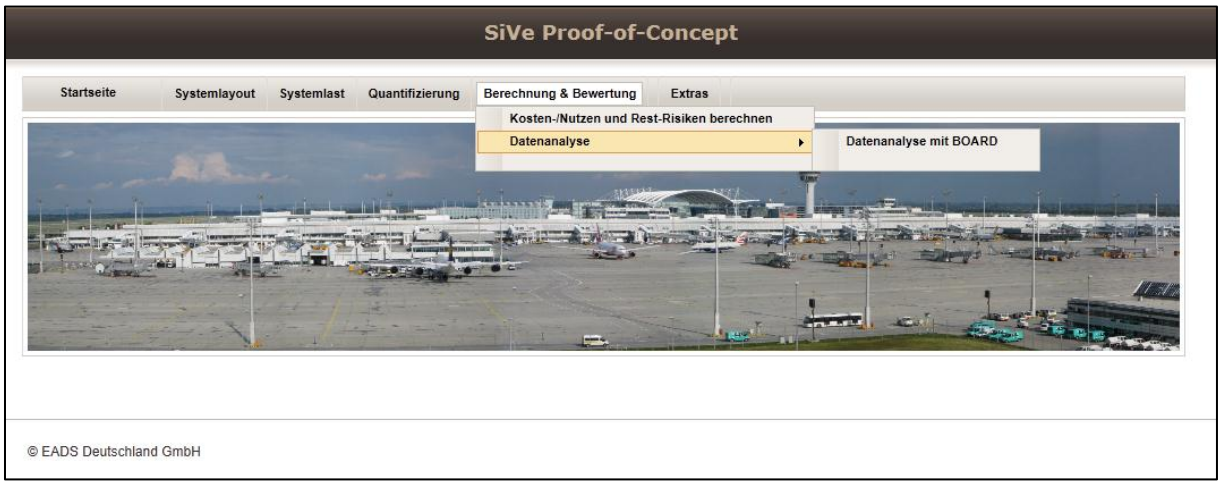
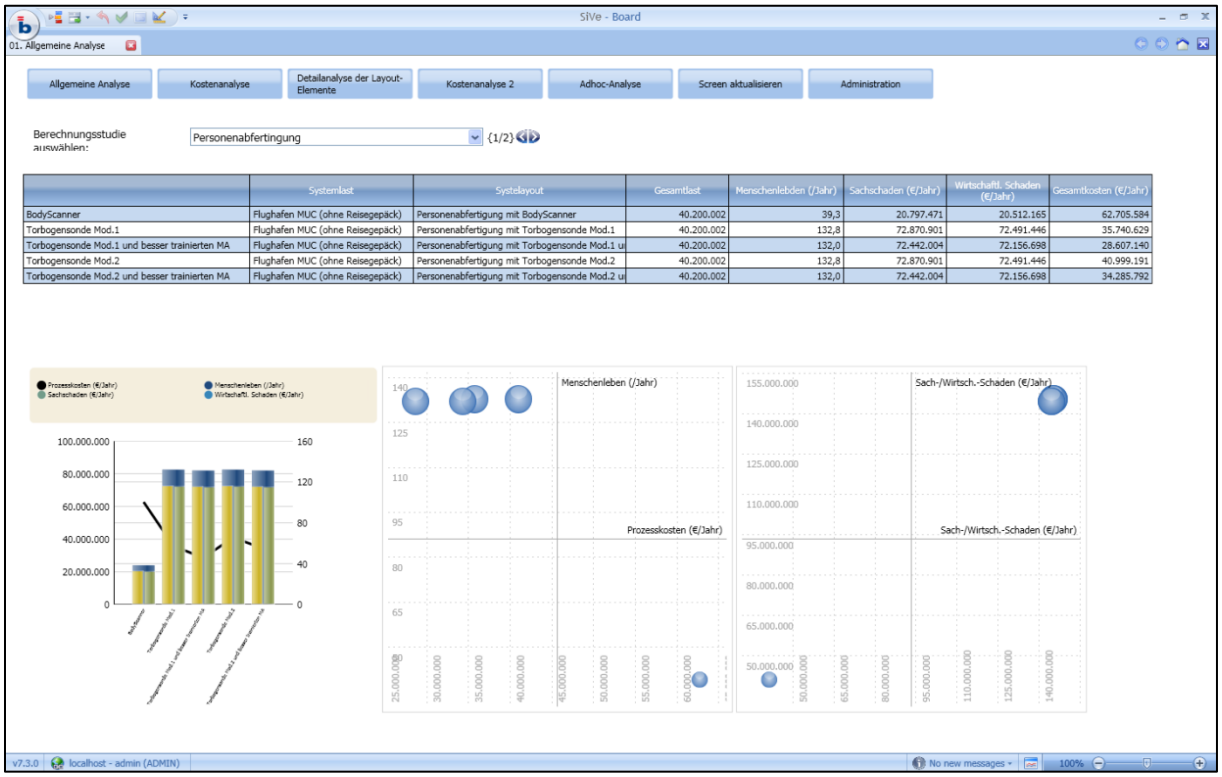


Abbildung 65: Auswahl eines externen Werkzeugs zur Datenanalyse (derzeit wird das BOARD Toolkit zur Datenanalyse gestartet).

Die Berechnungsstudien produzieren große Mengen an Daten, die weiter analysiert werden müssen, um Entscheidungen daraus zu treffen. Aus den Daten sollen Informationen gewonnen werden. Im PoC werden Datenanalyse und Reporting mit externen Werkzeugen durchgeführt.

U.a. werden Cristall-Reports, BIRT und BOARD verwendet, die direkt aus dem PoC aufgerufen werden (können).

Folgende Beispiele wurden mit BOARD (www.board.de) erstellt. Dafür werden die Ergebnisse der Berechnungsstudie über eine Datenintegrations-Schnittstelle in die multidimensionale Datenbank von BOARD geladen. Diese Datenbank ermöglicht eine „Navigation“ durch Daten, um Informationen aus verschiedenen Sichten über die Berechnungsstudien zu gewinnen.



	Systemlast	Systemlayout	Gesamtlast	Menschenleben (/Jahr)	Sachschaden (€/Jahr)	Wirtschaftl. Schaden (€/Jahr)	Gesamtkosten (€/Jahr)
BodyScanner	Flughafen MUC (ohne Reisegepäck)	Personenabfertigung mit BodyScanner	40.200.002	39,3	20.797.471	20.512.165	62.705.584
Torbogensonde Mod.1	Flughafen MUC (ohne Reisegepäck)	Personenabfertigung mit Torbogensonde Mod.1	40.200.002	132,8	72.870.901	72.491.446	35.740.629
Torbogensonde Mod.1 und besser trainierten MA	Flughafen MUC (ohne Reisegepäck)	Personenabfertigung mit Torbogensonde Mod.1 u	40.200.002	132,0	72.442.004	72.156.698	28.607.140
Torbogensonde Mod.2	Flughafen MUC (ohne Reisegepäck)	Personenabfertigung mit Torbogensonde Mod.2	40.200.002	132,8	72.870.901	72.491.446	40.999.191
Torbogensonde Mod.2 und besser trainierten MA	Flughafen MUC (ohne Reisegepäck)	Personenabfertigung mit Torbogensonde Mod.2 u	40.200.002	132,0	72.442.004	72.156.698	34.285.792

Abbildung 66: Beispiel eines Cockpits.

Abbildung 67: Beispiel einer Portfolio-Analyse.

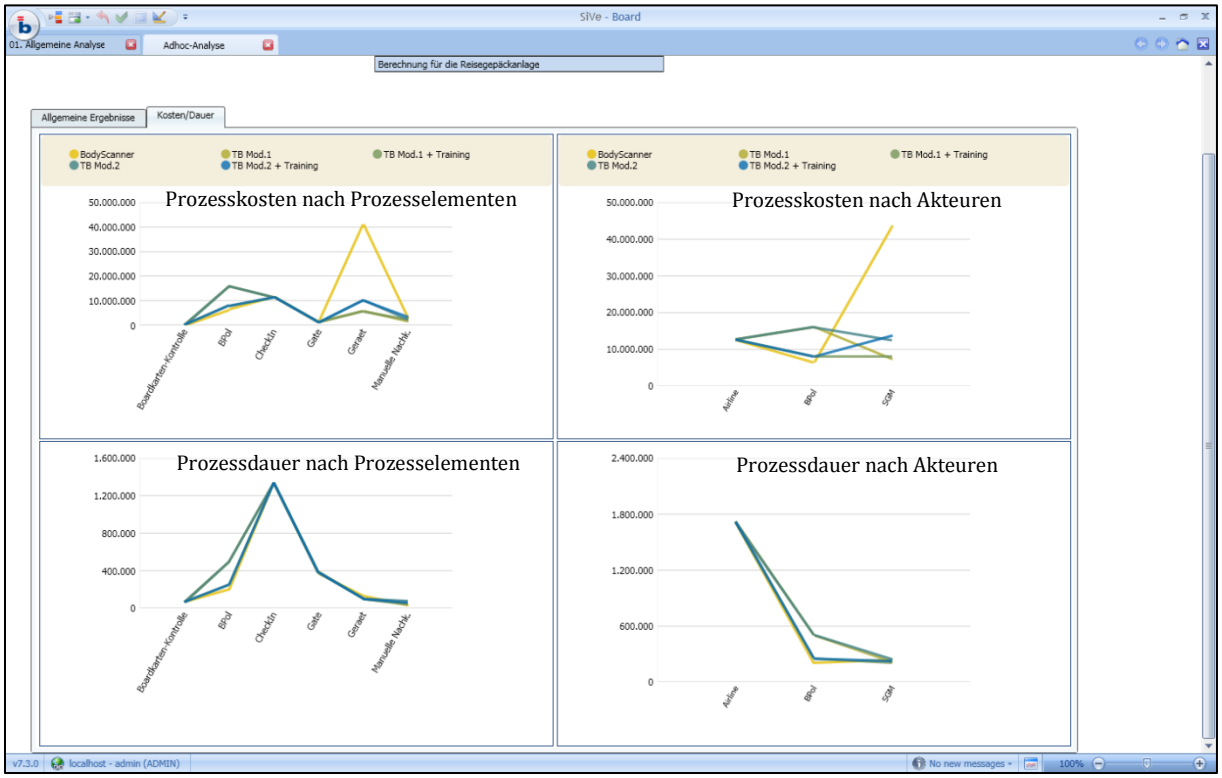


Abbildung 68: Darstellung der Prozesskosten und –dauer nach Prozesselemente und Prozess-verantwortlichen.

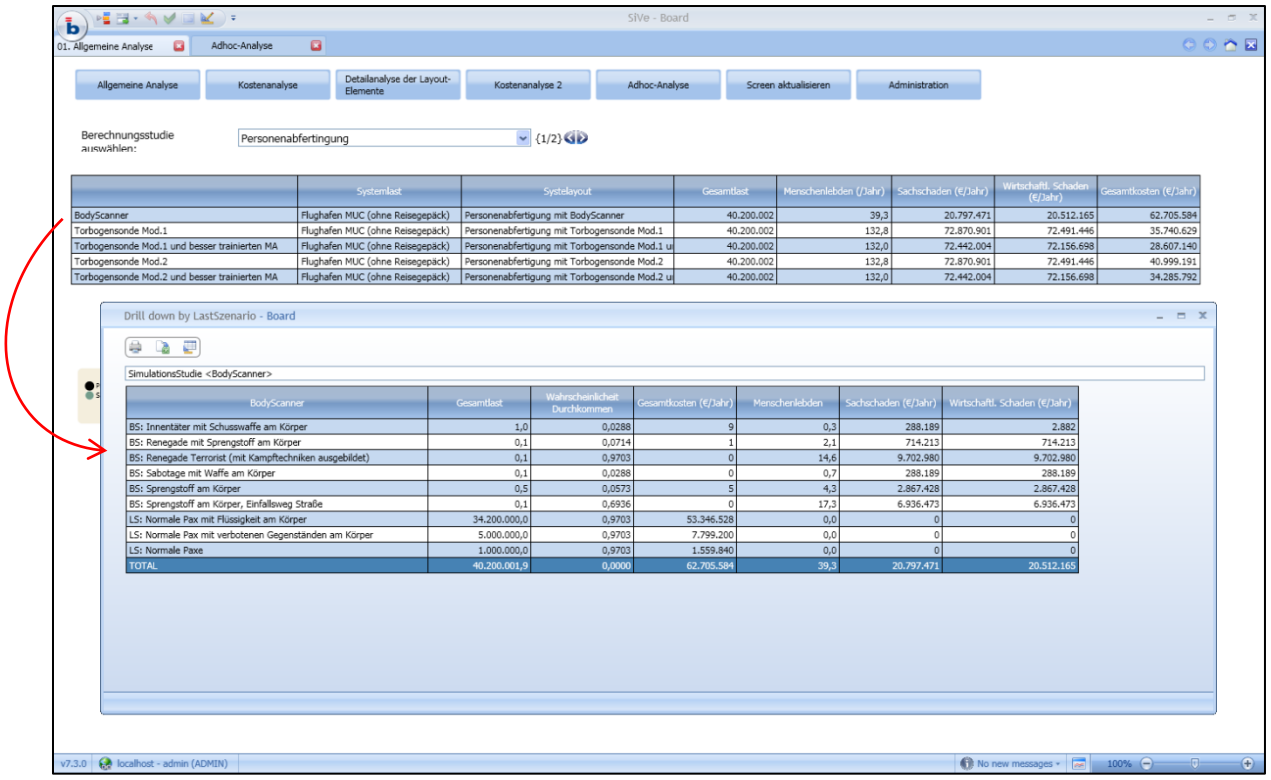


Abbildung 69: Beispiel einer „Navigation“ durch die Daten (Drilldown von aggregierten nach detaillierten Informationen).

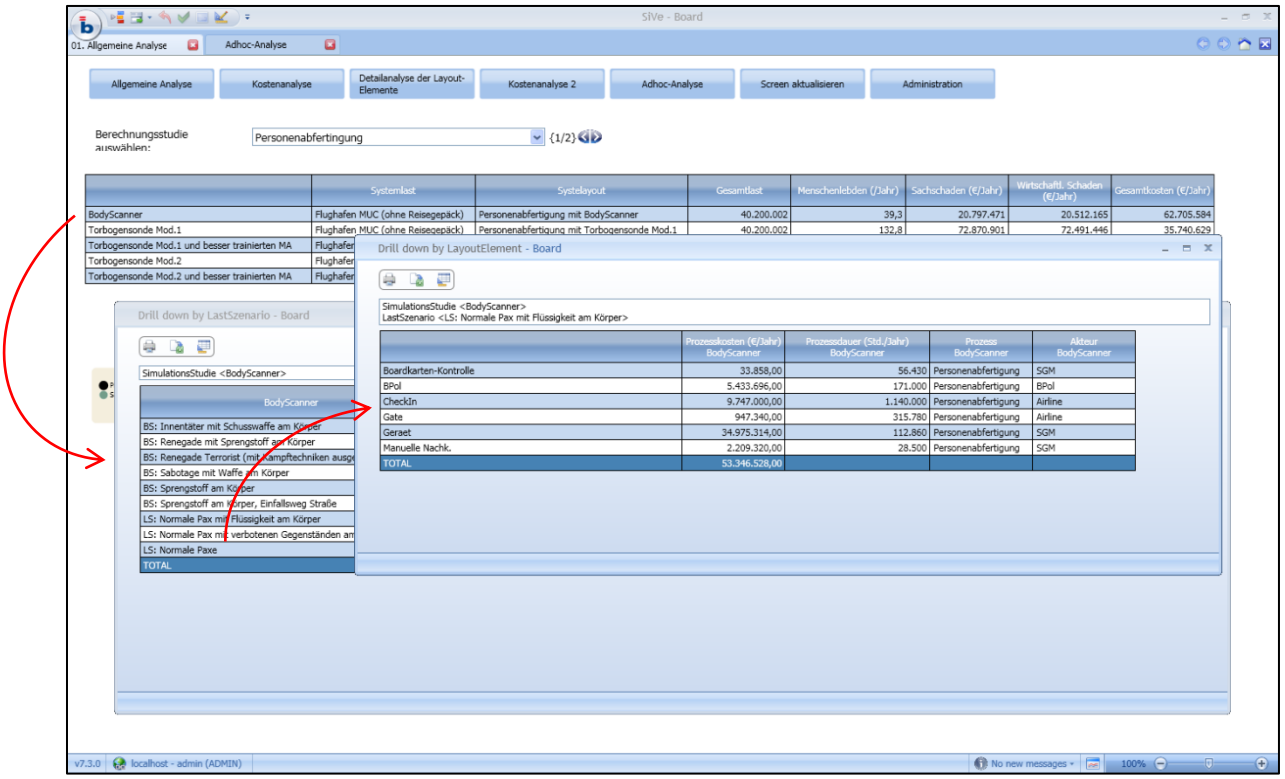


Abbildung 70: Fortsetzung Abbildung 69.