Fraunhofer
FKIE

Verbesserung der Sicherheit von Personen in der Fährschifffahrt PLUS (VESPER^{PLUS})

Sicherheitsarchitektur und mehrstufiges Modell zur Fahrzeugüberprüfung

Abschlussbericht
FKZ: 13N11919
Laufzeit des Vorhabens:
01.09.2011 – 31.08.2014

E. Dalinger
H. El Mokni
J. Heinskill
D. Ley
G. Linkmann
F. Motz
O. Rassy
A. Wagner

**Alle Rechte vorbehalten,
einschließlich der Übersetzung in andere Sprachen.
Vorliegender Bericht darf – auch in Auszügen –
nur nach schriftlicher Genehmigung
vervielfältigt werden.**

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE
Fraunhofer Str. 20 | 53343 Wachtberg

Inhaltsverzeichnis

A. Einleitung

A.1 Aufgabenstellung

Vor dem Hintergrund einer wachsenden Bedrohung durch den internationalen Terrorismus hat sich die Sicherheitslage für die Bundesrepublik Deutschland in den letzten Jahren verschärft. Zukünftig muss damit gerechnet werden, dass verstärkte Maßnahmen zur Gefahrenabwehr nicht mehr nur über kurzfristige, sondern über mittel- oder langfristige Zeiträume aufrechterhalten werden müssen. Die Fährschifffahrt ist hiervon besonders betroffen, da Verzögerungen durch Sicherheitsmaßnahmen in den bereits stark optimierten Hafendurchläufen ihre Konkurrenzfähigkeit schwächen.

Das Forschungsprojekt VESPER^{PLUS} unterstützt Behörden und Endnutzer bei der Bewältigung ihrer Aufgaben zur Gewährleistung und Verbesserung der Sicherheit im Fährverkehr. Der gesamte Bereich ist ein interdisziplinäres Forschungs- und Anwendungsgebiet, das von der Entwicklung und Verbesserung einzusetzender Monitoring- und Detektionssysteme über die Kooperation verschiedenster Einheiten, wie Polizei, Reedereien und Schiffsbesatzung bis hin zu einer ganzheitlichen Analyse aller Elemente der Sicherheitsarchitektur reicht.

Im Einzelnen gehörte zu den Forschungsarbeiten in VESPER^{PLUS} eine ganzheitliche Analyse der Sicherheitsarchitektur, die sich aus den drei Teilen Schiff, Hafenanlage und Gesamthafen zusammensetzt, um durch eine optimale, vernetzte Architektur weitere Verbesserungen der Sicherheit erzielen zu können. Weiterhin waren dezidierte Kenntnisse der Risiken unerlässlich, um Präventiv- und Abwehrmaßnahmen geeignet entwerfen zu können. Daher wurden die bestehenden Methoden zur Risikobewertung ebenfalls einer Analyse und Überarbeitung unterzogen. Vor dem Hintergrund personeller und finanzieller Ressourcenplanung war die Effizienz der Sicherheitsarchitektur von Bedeutung. Daher stellten Aufwandsabschätzungen und die Unterstützung eines gemeinsamen Situationsverständnisses wichtige Forschungsaspekte dar.

Der Einsatz von Detektionstechnologien half bei der Gefahrstoffentdeckung. In der Regel sind Detektordaten in ihrer Rohform nicht direkt vom Anwender interpretierbar, sondern erfordern eine Nachbearbeitung. Durch geeignete Verfahren der Sensordatenfusion sollten die wesentlichen Informationen aus den Rohdaten extrahiert und aufbereitet werden. Insbesondere wurden Lösungen entwickelt, die es ermöglichen, Daten zu verknüpfen, die an verschiedenen Orten und Zeitpunkten gewonnen wurden und die sich idealerweise gegenseitig ergänzen. Die Ergebnisse unterstützen den Entscheidungsträger bei der Feststellung von Handlungsbedarf und ggf. bei der Einleitung geeigneter Gegenmaßnahmen.

Einen weiteren Forschungsschwerpunkt stellten Entscheidungsunterstützungssysteme (EUS) für den Einsatz in Krisensituationen dar. Sie unterstützen den Informationsverarbeitungsprozess und somit auch den Entscheidungsprozess des Menschen. Das Trainingspotential von Entscheidungsunterstützungssystemen darf dabei nicht unterschätzt werden. Das Lernen der notwendigen Fähigkeiten zur Entscheidungsfindung und Problemlösung mit Hilfe eines EUS führt zu einem effektiveren Nutzen des Systems. Ein EUS kann wiederum die Wirksamkeit des Trainings verbessern, indem es eine Unterstützung in Form von Instruktionen, Feedback und Dokumentation liefert. Daher wurde ein EUS mit integrierter Trainingskomponente entwickelt.

Im Vorgängerprojekt VESPER wurden die Methoden der Prozessanalyse sehr erfolgreich auf eine Übungsbegleitung und -analyse angewendet. Darauf aufbauend wurde in VESPER^{PLUS} ein Konzept in Form eines Handbuchs zur standardisierten Planung, Begleitung und Analyse schnittstellenübergreifender Übungen entwickelt.

Die nachfolgende Abbildung gibt einen Überblick über die Struktur von VESPER^{PLUS}.

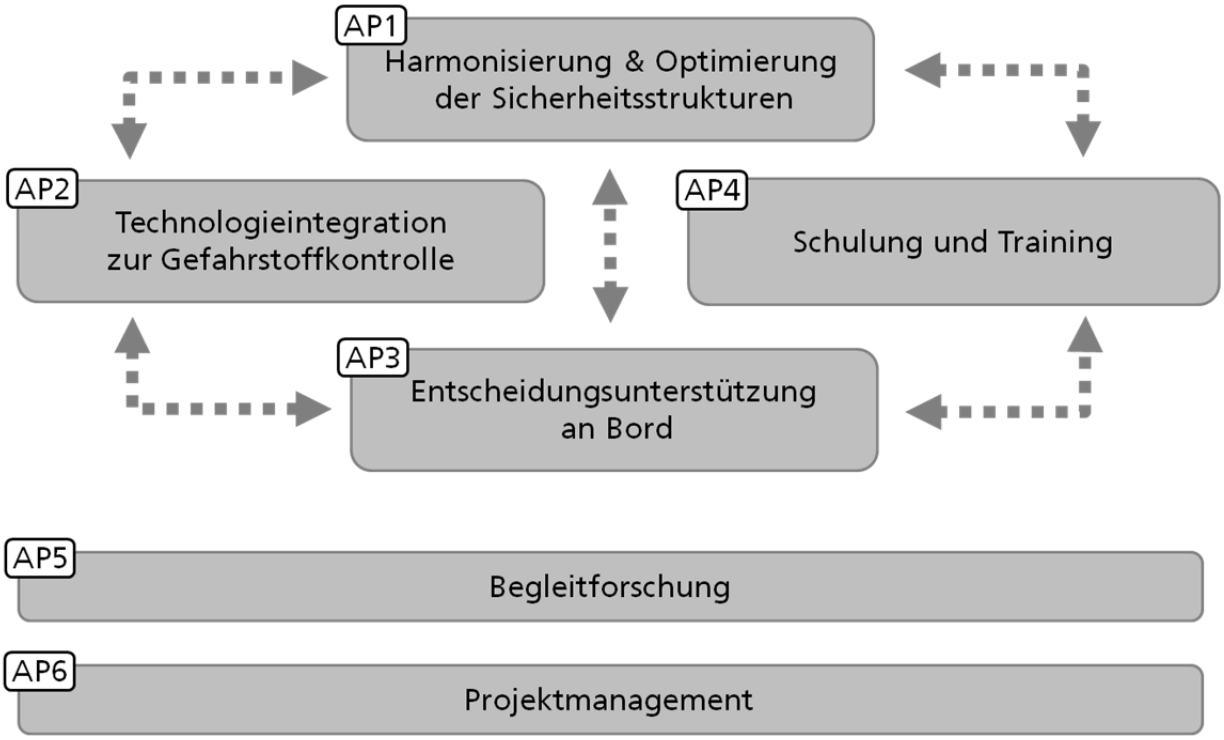

Abbildung 1: Arbeitspakete Vesper Plus

Das FKIE bearbeitete in VESPER^{PLUS} die folgenden Aufgaben:

- *AP1: Harmonisierung und Optimierung der Sicherheitsarchitekturen*
  Die Analyse der landseitigen Sicherheitsarchitektur hatte sich im Projekt VESPER auf ISPS-Hafenanlagen und damit ganz bestimmte Elemente eines Hafens bezogen. Hierbei wurde deutlich, dass für eine umfassende Beurteilung der Sicherheitsprozesse alle Elemente der Sicherheitsarchitektur mit einbezogen werden müssen. Dies betrifft die Sicherheitsarchitekturen von Schiff (ISPS-Code Schiff), Hafenanlage (ISPS-Code Hafenanlage) und Gesamthafen (Richtlinie EG/2005/65), wobei die Verzahnungen zwischen den einzelnen Sicherheitsarchitekturen bisher gering sind. Durch eine Analyse in VESPER^{PLUS} wurde die Identifizierung von Schwachstellen und Verbesserungspotentialen, eine Erhöhung der Handlungssicherheit der Beteiligten, die Redundanz in der Maßnahmenüberwachung, eine Verbesserung der Kooperation der beteiligten Akteure sowie eine Steigerung der Effizienz und damit der Effektivität der übergeordneten Sicherheitsarchitektur angestrebt. Da die zur Gefahrenabwehr zur Verfügung stehenden Ressourcen beschränkt sind, trägt ein geeignetes Ressourcenmanagement erheblich zur Verbesserung der Sicherheit bei. Die Arbeiten wurden in enger Zusammenarbeit mit den beteiligten Häfen, Reedereien sowie den zuständigen Behörden durchgeführt werden. Dabei wurden einerseits die in VESPER erprobten Methoden angewendet, so dass das FKIE seine diesbezügliche Expertise ausbauen und stärken konnte. Andererseits wurde im Bereich der Risikoanalyse, welcher eine enge Verwandtschaftsbeziehung zum Bereich der Prozessanalysen vorweist, eine neue Methode entwickelt.

- *AP2: Detektion von Explosivstoffen oder anderen Gefahrstoffen*
  Im Rahmen von VESPER wurden mögliche Lösungen für die Personenzugangskontrolle zur Lokalisierung von Gefahrstoffen untersucht, weiterhin wurden erste Ansätze zur stichprobenhaften Gefahrstoffkontrolle bei Fahrzeugen erprobt. Im Hinblick auf die Ergebnisse in der nicht-kooperativen Personenkontrolle wurde in VESPER^{PLUS} der Frage nach

der Übertragbarkeit des Ansatzes für die Fahrzeugkontrolle nachgegangen. Dabei wurde geprüft, ob es möglich ist, sowohl vor als auch im ISPS-Bereich geeignete Sensorik zu verteilen, deren Messungen mit den Fahrzeugen in Beziehung zu setzen und durch Kontextinformation zu ergänzen, um daraus einen Hinweis für das Sicherheitspersonal abzuleiten. Darüber hinaus wurde ein Tool zur Analyse von Substanzgemischen entwickelt, welches die Einbindung eines menschlichen Experten bei der Beurteilung der Gefährlichkeit eines Gemisches ermöglicht.

- *AP3: Anpassung und Erweiterung eines Entscheidungsunterstützungssystems für Fährschiffe zum Einsatz zu Trainingszwecken*
  Der in VESPER erstellte Anforderungskatalog für ein Entscheidungsunterstützungssystem (EUS) für Security-Vorfälle an Bord wurde in VESPER^{PLUS} um die Anforderungen an eine Trainingskomponente und an eine Komponente zur Koordination der Maßnahmen durch die Reederei erweitert. Ein EUS, das erfahrene Entscheidungsträger im Krisenfall unterstützen soll, kann auch zum Training der entsprechenden Expertise benutzt werden. Ein integriertes Konzept für das Design von EUS und Training wurde entwickelt. Voraussetzung für die Integration in den täglichen Routinebetrieb war die Überwindung der bereits aufgedeckten Schwachstellen: Die Diskrepanz zwischen den abstrakt formulierten Maßnahmen zur Gefahrenabwehr im ISPS-Code und deren praktische Umsetzung. Es wurden konkrete, schiffsbezogene Präventiv- und Notfallmaßnahmen und -abläufe für Security-Vorfälle auf dem Schiff definiert. Ferner wurde ein Konzept zur Koordination und Überwachung der Abläufe auf dem Schiff durch die Reederei mit Hilfe einer Datenübertragung vom EUS an Bord zur Landseite erarbeitet.

- *AP4: Schulung und Training*
  Wesentlicher Bestandteil einer Sicherheitsarchitektur ist ein hoher Ausbildungsgrad des Personals. Verbesserte Trainingskonzepte sollen die Wirksamkeit und Nachhaltigkeit des Trainings stärken. Das FKIE hat hierzu ein Konzept einer standardisierten Planung, Begleitung und Auswertung von Übungen erstellt. Die Ergebnisse flossen in ein Handbuch für Schulungen und Übungen ein.

A.2 Voraussetzungen

Auch die maritime Sicherheit ist seit dem elften September 2001 in den Fokus allgemeinen Interesses gerückt, da terroristische Aktivitäten im Seetransport schwerwiegende Folgen haben können. Dazu zählen beispielsweise der Verlust von Menschenleben, die Vernichtung hoher Sachwerte oder nicht abschätzbare Umweltschädigungen. Diese möglichen Auswirkungen werden begleitet von folgenschweren Beeinträchtigungen der Verkehrsinfrastruktur, Vertrauensverluste in den Verkehrsträger und insgesamt einer Schädigung des gesamten Wirtschaftszweiges. Um durch Terrorismus und Kriminalität induzierten Gefahren entgegenzuwirken, wurde im Jahr 2004 durch internationale Bemühungen der International Maritime Organization (IMO) der ISPS-Code (International Ship and Port Facility Security Code) zur Verbesserung der Gefahrenabwehr im internationalen Seeverkehr eingeführt.

Der in das SOLAS-Abkommen (Safety of Life at Sea) integrierte ISPS-Code fordert für Schiffe und Hafenanlagen, die international operieren, die Umsetzung von Maßnahmen zur Gefahrenabwehr. Dazu gehören neben konkreten Maßnahmen auch Kommunikationsvorgaben und die Einrichtung von Prüfbehörden. Verantwortlich für die Umsetzung der Vorgaben des ISPS-Codes sind die Hafenbetreiber und Reedereien selbst. Im Gegensatz zu Safety-Anforderungen gab es zur Einführung des ISPS-Codes 2004 kaum Erfahrungen oder Best-Practices im Bereich Security.

Die Implementierung von Präventiv- und Abwehrmaßnahmen im Bereich der Fährschifffahrt auf der Ostsee birgt darüber hinaus besondere Herausforderungen, da die meisten Fährlinien im Sinne eines Brückenersatzverkehrs in Konkurrenz zum Landweg stehen. Die Fährdienste sind unter anderem durch vergleichsweise kurze Überfahrten mit bereits optimierten Hafenaufenthalten gekennzeichnet. Die Herausforderungen betreffen hauptsächlich erhöhte Kosten sowie potentielle Verzögerungen in der Abfertigung aufgrund erhöhter Sicherheitserfordernisse. Die Einführung von Maßnahmen, wie sie im Personenflugverkehr oder der Kreuzschifffahrt vorhanden sind, würde für die Fährschifffahrt und den damit verbundenen Wirtschafts- und Industriezweigen zu immensen Störungen und Schädigungen führen.

Abteilung Mensch-Maschine-Systeme

In der Abteilung Mensch-Maschine-Systeme werden Konzepte, Methoden und Werkzeuge zur benutzerzentrierten Gestaltung von Informationssystemen erforscht, entwickelt und angewandt. Aufbauend auf ergonomischen Anforderungsanalysen werden innovative Mensch-Maschine-Schnittstellen konzipiert, in Form von Prototypen realisiert und hinsichtlich ihrer nutzergerechten Gestaltung in Feld- und Laborstudien evaluiert.

Bei der Gestaltung und Bewertung von Mensch-Maschine-Systemen werden auf der Grundlage von Aufgaben- und Tätigkeitsanalysen systematisch ergonomische Gestaltungsanforderungen ermittelt, unter Berücksichtigung ergonomischer Gestaltungsprinzipien umgesetzt sowie die resultierenden Systemkonzepte empirisch bewertet. Es wird weiterhin untersucht, auf welche Weise eine situations- und aufgabenangepasste Unterstützung des Informationsverarbeitungsprozesses und somit auch des Entscheidungsprozesses des Menschen bei der Visualisierung von und Interaktion mit komplexen dynamischen Daten realisiert werden kann. Besondere Bedeutung kommt hier der Optimierung des Informationsmanagements zur benutzer-, aufgaben- und situationsangepassten Bereitstellung und Darstellung von Informationen zu. Um das Informationsangebot von Systemen in Echtzeit an die situativen Erfordernisse anzupassen und in diesem zeitlichen Rahmen ein optimiertes Aufgabenmanagement zwischen den Operateuren untereinander sowie dem Führungssystem zu erreichen, werden adaptive Mensch-Maschine-Schnittstellen konzipiert. In kooperativen Arbeitsprozessen spielt außerdem sowohl das Situationsbewusstsein des einzelnen Operateurs als auch das gemeinsame Lageverständnis kooperierender Operateure eine wichtige Rolle für die Beurteilung der Leistungsfähigkeit und Gebrauchstauglichkeit von Führungs- und Arbeitssystemen.

Durch diese Kernkompetenzen wird die vorhandene Expertise der Abteilung zu relevanten Forschungsinhalten in Bezug auf das vorliegende Forschungsprojekt deutlich. Zusätzlich wird sie durch eine große Anzahl an laufenden und bereits abgeschlossenen Projekten konkretisiert und untermauert. So bestehen intensive Kontakte und Kooperationen im Bereich der Nautik hinsichtlich der ergonomischen Gestaltung von Informationssystemen auf Schiffen und durch die Mitarbeit in Gremien der Internationalen Schifffahrtsorganisation (IMO), welche den ISPS-Code verabschiedet hat. Dazu gehört auch die Leitung der IMO Correspondence Group „Integrierte Navigations- und Brückensysteme“. Diese und weitere relevante Arbeiten werden durch die folgende Auswahl an Projekten repräsentiert:

- Ergonomische Gestaltung von Navigationssystemen im Bereich der Schifffahrt
- Entwicklung und Gestaltung benutzerzentrierter Informationssysteme; u.a. Entwicklung eines Systems zur Entscheidungsunterstützung mittels regelbasiertem Inferenzsystem
- COMPRIS: „Consortium Operational Management Platform River Information Services“
- Durchführung von Prozessanalysen und Optimierung der Prozesse in verschiedenen Projekten, u.a. „SEDAN – Simulation und Evaluation der Aufklärung im Nahbereich“
- BMVI-Projekt „Ermittlung von Anforderungen an ein modulares Schiffsbrückenkonzept mit INS mit aufgaben- und situationsabhängiger Darstellung von Informationen zur Gewährleistung einer sicheren Schiffsführung“

- BMVI-Projekt: „Bewertung und Gestaltung der Präsentation von AIS-Informationen auf den Navigationsdisplays der Schiffsbrücke zur Gewährleistung einer sicheren Schiffsführung“
- BMVI-Projekt: „Ermittlung von Anforderungen an integrierte Navigationssysteme (INS) für eine aufgabengerechte Integration der Navigationsinformationen zur Erhöhung der Sicherheit in der Schiffsführung“
- Weitere fünf BMVBS-Projekte zur ergonomischen Gestaltung von Informationssystemen auf Schiffen in der Zeit von 1995 bis 2010
- Projekt „MEBS – Entwicklung eines Methodeninventars zur Erfassung und Bewertung des Situationsbewusstseins bei der Lagebewertung“
- Projekt „COPMEBS – Validierung eines Methodeninventars zur Erfassung und Bewertung des Situationsbewusstseins in kooperativen, vernetzten Systemen“
- Mitarbeit in Gremien der Internationalen Schifffahrtsorganisation (IMO) und Leitung der IMO Correspondence Group „Integrierte Navigations- und Brückensysteme“

Abteilung Sensordaten- und Informationsfusion

Die Abteilung Sensordaten- und Informationsfusion (SDF) verfügt über Kenntnisse und Erfahrungen im Bereich des Personentrackings und der Detektionstechnologien zur Abwehr asymmetrischer Bedrohungen durch unkonventionelle Spreng- und Brandvorrichtungen (USBV). Diese Kenntnisse wurden u.a. als Koordinator des Forschungsvorhabens HAMLeT (Hazardous Material Localization & Person Tracking) im Rahmen der vorbereitenden Maßnahmen zur Sicherheitsforschung der Europäischen Kommission (EU PASR 2006) und bei der Mitarbeit im Information Systems Technology (IST) Panel of the NATO Research and Technology Organisation (RTO) erworben.

Zu den Kernaufgaben der Abteilung SDF zählt die Entwicklung von Verfahren der Sensordaten- und Informationsfusion für die militärische Aufklärung. Im Rahmen des „Dual Use“ sind viele dieser Verfahren auch für zivile Anwendungen nutzbar gemacht worden. Sensordaten- und Informationsfusion bedeutet die Verdichtung von umfangreichen, einander ergänzenden Datenmengen zu Informationen von hoher inhaltlicher Qualität. Sensordaten, die Information über relevante Zielobjekte (wie z.B. Ort, Geschwindigkeit, Verhalten, u.a.) darstellen, dienen einer Lokalisierung, Klassifizierung und möglichen Identifizierung dieser Objekte. Die Daten sind in der Regel ungenau, unvollständig und mehrdeutig. Durch die in der Abteilung SDF entwickelten Verfahren ist es dennoch möglich, auf anhand der Daten zeitnahe „Lagebilder“ zu erstellen. Diese Lagebilder dienen als Grundlage für Entscheidungen. Die fusionierende Auswertetechnologie bildet die Schnittstelle zwischen Aufklärungssensorik und den handelnden und entscheidenden Menschen. Arbeiten hierzu gehen in zahlreiche militärische Aufklärungssysteme und Projekte ein, z.B. AWACS Mid-term Modernization, Sensor Data Fusion für die deutschen Fregattenklassen 124/125, Eurofighter, MAJIIC (Multisensor Aerospace-to-ground Joint Interoperabe ISR Coalition) und Sonar-Aufklärung für die U-Boot-Klasse 212.

A.3 Planung und Ablauf des Vorhabens

Seitens des Fraunhofer FKIE konnte das Projekt im Wesentlichen wie in der Projektbeschreibung geplant durchgeführt werden.

Zweimal jährlich fanden Workshops zur Vorstellung und Diskussion des Arbeitsstands der einzelnen Verbundpartner statt, an denen auch die assoziierten Partner teilnahmen. Darüber hinaus fanden zahlreiche Arbeitstreffen sowohl mit Verbund- als auch mit assoziierten Partnern statt.

A.4 Stand der Wissenschaft und Technik

Der International Ship and Port Facility Security Code (ISPS-Code) und die Gesamthafenrichtlinie 2005/65/EG

Im Jahr 2004 wurde der ISPS-Code zur Erhöhung der Gefahrenabwehr in der internationalen Seeschifffahrt in Kraft gesetzt (Verordnung (EG) Nr. 725/2004). Er schreibt für alle unter die SOLAS-Konvention (International Convention for the Safety of Life at Sea) fallenden Schiffe die Einhaltung von Sicherheitsstandards und Vorschriften vor, welche durch die jeweiligen Flaggenstaaten geprüft werden. Das zugrunde liegende Konzept stützt sich auf eine dreistufige Sicherheitsarchitektur für Schiffe und Hafenanlagen, die für die jeweilige Gefahrenstufe die Umsetzung von in einem Gefahrenabwehrplan festgeschriebenen Maßnahmen fordert. Die Festlegung der Gefahrenstufe obliegt den zuständigen Behörden, wobei eine grundsätzliche Einordnung in die Gefahrenstufe 1 festgesetzt worden ist. Der ISPS-Code schreibt neben Kontrollmaßnahmen unter anderem bestimmte Kommunikationsprozesse vor, darüber hinaus sind regelmäßige Risikobewertungen sowie Personalschulungen durchzuführen. Die Pflicht zur Ausführung der Maßnahmen der Gefahrenabwehr obliegt den privaten Unternehmen (Reederei, Hafenanlagenbetreiber) und wird von zuständigen Behörden und im Rahmen der Hafenstaatenkontrolle überprüft.

Aufgrund der lediglich 18 Monate andauernden Vorbereitungsphase zur Einführung des ISPS-Codes sind die Bestrebungen zur Erhöhung der Gefahrenabwehr in der Seeschifffahrt jedoch mit diesen Maßnahmen noch nicht vollständig ausgereift. Des Weiteren herrscht in Deutschland seit Einführung des ISPS-Codes durchgängig Gefahrenstufe I, daher liegen bisher kaum Erfahrungen hinsichtlich der Gefahrenstufen II und III vor. Es liegen keine gesicherten Erkenntnisse darüber vor, wie sich eine Gefahrenstufenerhöhung auf die Funktionsfähigkeit der Infrastruktur auswirken würde.

Die Gesamthafenrichtlinie ist als Ergänzung des ISPS-Codes zur Stärkung der landseitigen Sicherheitsarchitektur vorgesehen. Der ISPS-Code „beschränkt sich auf Maßnahmen zur Gefahrenabwehr an Bord von Schiffen und im unmittelbaren Bereich des Zusammenwirkens von Schiff und Hafen“ (vgl. Verordnung (EG) Nr. 725/2004), während die Gesamthafenrichtlinie sicherstellen soll, dass „in Anwendung der Verordnung (EG) Nr. 725/2004 getroffene Maßnahmen zur Gefahrenabwehr durch eine verbesserte Gefahrenabwehr in den Bereichen der Hafentätigkeit optimiert werden“ (vgl. Richtlinie EG/2005/65). Die Gesamthafenlinie sieht ebenfalls eine dreistufige Sicherheitsarchitektur vor.

Da sich der ISPS-Code in die Bereiche *Schiff* und *Hafenanlage* teilt, ergibt sich eine Unterteilung der Sicherheitsarchitektur in die Systeme Schiff, Hafenanlage und (Gesamt-)Hafen. Die Nutzung von Synergieeffekten wird durch unterschiedliche Zuständigkeiten behindert. Eine übergeordnete Analyse der Sicherheitsarchitektur unter Berücksichtigung aller Systembestandteile soll zur Verbesserung der Effektivität und Effizienz der Sicherheitsarchitektur beitragen

Prozessanalysen

Prozesse sind definiert als (chrono-)logische Aufeinanderfolge von Zuständen innerhalb eines Systems. Die Prozessanalyse ist eine Ist-Analyse von Prozessen, auf deren Basis Soll-Prozesse festgelegt werden. System- bzw. Prozessanalysen (Döring, 2005) strukturieren und erfassen die Vorgänge innerhalb eines bestimmten Betrachtungsraums unter Anwendung des Top-Down-Verfahrens, bei dem die Granularität der Prozessschritte immer weiter verfeinert wird. Eine Methode zur Systemstrukturanalyse bietet unter anderem die Hierarchical Task Analysis (Annett, 2004; Stanton et al., 2005), bei der Arbeitsabläufe hierarchisch etikettiert und so in immer kleinere Schritte unterteilt werden.

Zur konkreten Erfassung und Modellierung von Prozessen in den unterschiedlichsten Bereichen existiert eine Anzahl an Werkzeugen. So werden zum Beispiel durch erweiterte ereignisgesteuerte

Prozessketten (eEPK) logische Abläufe von Arbeitsprozessen semi-formal dargestellt. Weitere Darstellungsmöglichkeiten bieten unter anderem die Higraphs (Harel, 1987), deren bekannteste Anwendung Statecharts sind oder RFA-Netze (Rollen-, Funktions- und Aktionsnetze; Oberquelle, 1987). Speziell für Schwachstellenanalysen, deren Zweck die Optimierung von Verfahren und Prozessen darstellt, kann die Analysemethode „Failure Mode and Effects Analysis" (FMEA; Müller & Tietjen, 2003) angewendet werden. Auch Flussdiagramme der standardisierten Modellierungssprache „Business Process Modeling Notation" (BPMN, OMG, 2009) können der Erfassung und Analyse von Abläufen dienen.

Bei der Analyse der Sicherheitsprozesse in VESPER hat sich gezeigt, dass im vorliegenden Anwendungsbereich zwei grundsätzliche Prozessklassen zu finden sind: Chronologische Prozesse, die beispielsweise den Hafendurchlauf eines PKWs beschreiben und als stark strukturiert zu bezeichnen sind, und schwach strukturierte Sicherheitsprozesse, bei denen eine Menge von Maßnahmen vorliegt, die keiner logischen Abfolge unterliegen. Hier ist eine Zuordnung der Maßnahmen zu Örtlichkeiten und Gefahrenstufen möglich. Aufgrund dieser Problemstellung wurde in VESPER neben der BPMN zur Modellierung stark strukturierter Prozesse die im Hause entwickelte „Security Modeling Technique" (SMT; Ley & Dalinger, 2010) eingesetzt, die den oben beschriebenen Anforderungen schwach strukturierter Prozessklassen der maritimen Sicherheitsarchitektur gerecht wird. Die Modellierungstechnik SMT ermöglicht eine integrierte Modellierung von Gefahrenstufen, Bereichen, Maßnahmen und Ressourcen, Prozessen sowie Kommunikation.

Die ausgewählten Methoden ermöglichen eine partizipative Erhebung der Prozesse, denn nur unter Beteiligung von Experten kann eine Erfassung effizient ausgeführt werden. Durch eine anschauliche Visualisierung der Arbeitsabläufe wird ein gemeinsames Verständnis gefördert.

Die Anwendung von Prozessanalysemethoden zur Begleitung und Analyse von Übungen im Bereich der maritimen Sicherheit ist ein Novum und wurde vom FKIE erstmals im Rahmen von VESPER durchgeführt (Linkmann et al., 2011). Die Methodik basiert auf dem Gedanken, dass eine Übung ein einmalig stattfindender Prozess ist. Mit Hilfe von adaptierten Techniken aus der Prozessanalyse können Schwachstellen aufgedeckt und Optimierungspotentiale identifiziert werden.

Entscheidungsunterstützung an Bord

Neuartige Informationsvisualisierungen sollen die Entscheidungsfindung verbessern, indem sie dabei helfen, Entscheidungen schneller zu treffen und sie genauer, aber gleichzeitig auch flexibler zu machen. Um Faktoren wie unvorhergesehene Ereignisse, dynamische Änderungen einer Situation und Echtzeitreaktionen auf die Änderungen zu berücksichtigen, benötigt man Methoden, die menschliche kognitive Prozesse untersuchen und die Analyse auf den Arbeitsplatz erweitern. Das Cognitive Systems Engineering (CSE, Rasmussen et al., 1994) ist ein Design-Framework, das sich mit der Analyse der kognitiven Anforderungen beschäftigt. Methoden des CSE helfen zu verstehen, was Experten über ihr Arbeitsgebiet wissen, wie und warum sie bestimmte Entscheidungen treffen, welche Hinweise sie bei der Entscheidungsfindung benötigen, welches Wissen und Strategien sie dabei benutzen. Die Applied Cognitive Work Analysis (ACWA, Elm et al., 2003) ist eine Methode des CSE, die eine methodische Vorgehensweise liefert, um ein System zur effektiven Entscheidungsunterstützung zu entwickeln und zu evaluieren; darüber hinaus bietet sie ein analytisches Werkzeug an, um Design-Anforderungen zu entwickeln. Die Analyse beginnt mit der Identifizierung der kritischen Entscheidungen, die der Operateur treffen muss, und endet mit der Identifizierung der Designkonzepte zur Entscheidungsunterstützung und deren Umsetzung in einem Prototyp. Im Unterschied zu anderen Methoden des CSE verbindet ACWA kognitive Analyse und Design.

Der Zweck eines EUS auf Fährschiffen ist es, einem nautischen Offizier auf der Brücke Hilfestellungen bei der Krisenbewältigung zu geben. Durch die Visualisierung von komplexen Daten sollen diese Systeme den Informationsverarbeitungsprozess und somit auch den

Entscheidungsprozess des Menschen unterstützen. Der ergonomischen Gestaltung der Benutzungsoberfläche kommt dabei besondere Bedeutung zu. Um Design-Anforderungen zu definieren, muss man die Besonderheiten der Entscheidungsfindung in komplexen Krisensituationen verstehen. Krisensituationen an Bord eines Schiffes zeichnen sich vor allem durch eine dynamische Umgebung, eine Echtzeitreaktion auf Änderungen, schlecht definierte Ziele und schlecht strukturierte Aufgaben aus. Die Naturalistische Entscheidungstheorie (Naturalistic Decision Making, Klein, 1998; Orasanu & Connolly, 1993) betrachtet lebensnahe Entscheidungen in komplexen und sicherheitskritischen Situationen, die unter hohem Zeitdruck getroffen werden müssen. Im Gegensatz zur klassischen Entscheidungstheorie geht es dabei um Entscheidungen, die in dynamische Aufgaben eingebettet sind und nicht auf der Auswahl der Alternativen basieren. Sie eignet sich somit auch zur Definition der Anforderungen an die EUS in Security relevanten Krisensituationen.

Ein wichtiger Bestandteil einer effektiven Entscheidungsunterstützung ist die Bereitstellung einer geeigneten Navigation im System, die bei der Klassifikation eines Krisenereignisses und bei der Suche nach Gegenmaßnahmen und relevanten Informationen unterstützt. „Dynamische Taxonomien“ (Sacco & Tzitzikas, 2009) oder „facettierte Suche“ ist ein Wissensmanagementmodell, das auf multidimensionaler Klassifikation heterogener Daten basiert. Mit Hilfe der Facettenklassifikation wird die Suche in einer komplexen Informationsdatenbank erleichtert, wobei der Benutzer mittels einer gesteuerten Interaktion nicht nur die Möglichkeit hat, nach geeigneten Maßnahmen und weiteren unterstützenden Informationen im Krisenfall zu suchen, sondern auch die Maßnahmen im Falle einer Änderung der Situation jederzeit anzupassen oder zu ändern.

Eine Herausforderung bei der Entwicklung eines EUS ist seine Einbettung in alltägliche Arbeitsprozesse auf dem Schiff, so dass die Benutzer durch regelmäßige Verwendung mit dem System vertraut sind und dieses nicht erst im Krisenfall erstmalig zum Einsatz kommt. Deshalb muss das System so konzipiert werden, dass es für Trainings- und Simulationszwecke eingesetzt werden kann (Cohen et al., 1997; Morrison et al., 1998), z.B. im Rahmen vorgeschriebener regelmäßiger Übungen auf dem Schiff.

Risikobewertung

Ein fundiertes Verständnis des Risikos, dem ein Schiff oder eine Hafenanlage ausgesetzt ist, ist unabdingbar, um geeignete Präventiv- und Abwehrmaßnahmen aufsetzen zu können. Daher fordern sowohl der ISPS-Code als auch die Gesamthafenrichtlinie die Erstellung von Gefahrenabwehrplänen, die auf Risikobewertungen basieren. Beide Dokumente beinhalten jedoch keine festgelegte Methode, sondern fordern lediglich die Berücksichtigung verschiedener Aspekte. Dazu gehören beispielsweise bei der ISPS-Risikobewertung für Hafenanlagen die bauliche Sicherheit und Widerstandsfähigkeit, Personalschutzsysteme, Verfahrensgrundsätze, Kommunikationssysteme, Transport- Infrastruktur und Versorgungseinrichtung sowie weitere Bereiche, von denen ein Risiko ausgehen könnte (vgl. Verordnung (EG) Nr. 725/2004, Ziffer 15.3). Weiterhin werden sicherheitsrelevante Ereignisse beispielhaft aufgeführt. Laut Anhang III, Teil B, Ziffer 1.17 des ISPS-Codes muss die Risikobewertung folgende Bestandteile umfassen

- die Feststellung der empfundenen Bedrohung,
- die Feststellung möglicher Schwachstellen und
- die Berechnung der Folgen der Ereignisse.

Die meisten Methoden zur Risikoanalyse basieren auf den folgenden Schritten (IMO, 2011):

1. Strukturierungsphase
2. Bewertung der Bedrohung
3. Bewertung der Auswirkungen
4. Bewertung der Angreifbarkeit/Anfälligkeit
5. Risiko-Scoring

6. Risiko-Management

In der ersten Phase ist ein Inventar der Anlage anzufertigen und das weitere Vorgehen festzulegen. Hier können klassische Methoden der Prozessanalyse wie Ablaufdiagramme und Methoden des Projektmanagements das Team unterstützen. In der darauffolgenden Phase sind Risikoszenarien und die davon betroffenen Organisationen zu ermitteln. Den Risikoszenarien sind Wahrscheinlichkeiten zuzuordnen, in deren Abhängigkeit eine Punktzahl (Score) vergeben wird. Hier wird ein Schwachpunkt aller Methoden ersichtlich, der sich auch durch die weiteren Phasen der Risikobewertung zieht: Die Wahrscheinlichkeiten lassen sich nicht eindeutig und objektiv berechnen, sondern werden unter Berücksichtigung festgelegter Aspekte, die von Methode zu Methode differieren können, von Experten festgelegt. Diese Festlegung bleibt subjektiv. Ziel muss es also sein, eine möglichst hohe Reproduzierbarkeit und Vergleichbarkeit zu erreichen. Dies könnte beispielsweise durch möglichst eindeutige Begriffsdefinitionen oder eine Kalibrierung der Skalen in Abhängigkeit des Experten geschehen.

Die dritte Phase ordnet den einzelnen Szenarien erwartete Auswirkungen zu. Meist werden dabei die Auswirkungen verschiedenen Kategorien zugeordnet, beispielsweise *Schaden für Personen oder Umwelt* und *Symbolwirkung des Anschlags*. Auch hier werden Punkte (Scores) vergeben, ebenso in der nächsten Phase. Zur Bewertung der Anfälligkeit werden zunächst mögliche Ziele und Schwachstellen der Infrastruktur aufgelistet und ihr Potential für Terrorzwecke beschrieben. Hier fließen auch Maßnahmen zur Minimierung der Auswirkungen mit ein. In der vorletzten Phase des Risiko-Scorings wird mit Hilfe der bisher gesammelten Informationen und vergebenen Scores ein Risiko ermittelt. Eine einfache Formel hierzu ist:

$$\text{Risiko} = \text{Bedrohung} \times \text{Auswirkungen} \times \text{Anfälligkeit}.$$

Je nach erreichter Punktzahl lassen sich Risiken damit in Kategorien einteilen. In Abhängigkeit dieser Kategorien werden weitere Maßnahmen ergriffen. Die letzte Phase des Risiko-Managements befasst sich mit dem Umgang mit dem ermittelten Risiko.

Weiterhin können Risikomatrizen (Threat and Risk Analysis Matrix, TRAM; IMO, 2000) eingesetzt werden, die eine verkürzte Vorgehensweise der Schritte 2 bis 5 darstellen.

Multisensorielle Assistenzsysteme für Zugangs- und Zufahrtskontrollen

In der Sensordatenfusion sind Assistenzsysteme für Zugangs- und Zufahrtskontrollen in das Gebiet der Bedrohungserkennung einzuordnen. Typische Szenarien sind durch eine komplexe Umgebungssituation und ein weitgehend unbekanntes Bedrohungsspektrum gekennzeichnet. Technische Systeme zur Unterstützung der Überwachungsaufgabe haben vor allem zwei Aspekte zu berücksichtigen: Erstens muss die Aufmerksamkeit des Sicherheitspersonals gerade in Massensituationen auf potentielle Bedrohungen fokussiert werden. Zweitens sollen Assistenzsysteme so verborgen wie möglich arbeiten, um die üblichen Abläufe nicht zu stören und potentiellen Angreifern keinen Hinweis auf die Überwachung zu geben. Neben den Sensordaten selbst sind „der Mensch als Sensor“ und in Datenbanken abgelegtes Hintergrundwissen wichtige Informationen, die mit der reinen Sensorinformation zu fusionieren sind.

Ein Beispiel für ein multisensorielles Assistenzsystem zur Zugangskontrolle ist das vom FKIE entwickelte System HAMLeT (Hazardous Material Localization and Person Tracking), welches im gleichnamigen EU-Projekt als Proof-of-Concept für die Überwachung von Personenströmen vorgestellt wurde (Wieneke et al., 2008b). Ziel der Überwachung ist es, chemische Gefahrstoffe im Zugangsbereich zu detektieren und die entsprechenden Trägerpersonen zu lokalisieren. Potentielle durch das System lokalisierte Träger können schließlich durch das Sicherheitspersonal gezielt angesprochen werden und einer gründlichen Kontrolle unterzogen werden. Da ein Gefahrstoffsensor zwar das Vorhandensein einer Substanz melden, jedoch aufgrund seiner begrenzten raumzeitlichen Auflösung diese nur sehr ungenau lokalisieren kann, ist ein solches

System ohne die gleichzeitige Verfolgung der Personen (Tracking) nicht denkbar. Im Rahmen von HAMLeT ist es gelungen, ein trackinggestütztes Klassifizierungsverfahren zu entwickeln (Wieneke et al., 2008a; Wieneke & Koch, 2009), das auf einem Zeitfenster die Signale verteilter chemischer Sensoren den Positionen der Personen zuordnet.

Grundsätzlich ist ein multisensorielles Sicherheitsassistenzsystem durch die folgenden Eigenschaften charakterisiert:

- Es arbeitet verdeckt, unbemerkt von der Öffentlichkeit,
- es bietet eine technische Unterstützung für das Sicherheitspersonal,
- die Erfahrung des Menschen bleibt unverzichtbar,
- es kombiniert die Stärken von Technik und menschlicher Erfahrung und
- ermöglicht eine Echtzeitanalyse großer Datenmengen und hohe Zuverlässigkeit in individuellen Situationen.

Allgemein basiert eine nicht-kooperative Überwachung auf:

- Überwachungssensoren
  - Detektion kinematischer Zustände: Erfassung von Position und Geschwindigkeit (wer/wann/wo?)
  - Attributdetektion (was/wann/wo?)
  - verfügbar oder derzeitig in der Entwicklung
- Fusion: Daten multipler Sensoren mit Hintergrundwissen
  - Überwachung von Personenströmen auf Attributmerkmale
  - Detektion auffälligen Verhaltens: z.B. Kontakte, Aufenthaltszeiten
  - Detektion verdächtiger mitgeführter Gegenstände
- Wissenstransfer: aus hochentwickelter militärischer Auswertetechnologie
  - Luft-Boden-Überwachung
  - Robotergestützte Überwachung im bebauten Gelände

A.5 Zusammenarbeit mit anderen Stellen

Dem Querschnittsthema „Sicherheit“ wurde im vorliegenden Vorhaben auch durch die Konsortialzusammensetzung Rechnung getragen.

Grundsätzlich erfolgte eine Zusammenarbeit in allen Arbeitspaketen mit den jeweils relevanten assoziierten Partnern:

- Bundesamt für Seeschifffahrt und Hydrographie (BSH)
- Hafen- und Seemannsamt Rostock (HRO)
- Landespolizeiamt Schleswig-Holstein, Dezernat 43, Behörde für Hafenanlagensicherheit (DA-SH)
- Lübecker Hafengesellschaft mbH (LHG)
- Scandlines Deutschland GmbH (SCA)
- TT-Line GmbH und Co. KG (TTL)
- Verband Deutscher Reeder (VDR)
- Verkehrsministerium Mecklenburg-Vorpommern, Hafensicherheitsbehörde (DA-MV)

Die Zusammenarbeit (ZA) des FKIE (Abteilungen MMS und SDF) mit anderen Verbundpartnern in den bearbeiteten Teil-Arbeitspaketen ist der folgenden Tabelle zu entnehmen.

AP 1	**Harmonisierung und Optimierung von Sicherheitsstrukturen**	**ZA**
AP 1.1	**Gefahrenabwehr in der Hafenanlage und im Gesamthafen**	
AP 1.1.1	Erfassung der landseitigen Sicherheitsarchitektur	HBRS
AP 1.1.2	Untersuchungen zum Wechsel von Gefahrenstufen	
AP 1.2	**Untersuchung der Schnittstellen zwischen landseitigen Organisationen, Behörden sowie der Schiffsseite**	
AP 1.2.1	Untersuchung der Kommunikationsprozesse	HBRS
AP 1.2.2	Unterstützung eines gemeinsamen Situationsverständnisses an der Schnittstelle Schiff-Hafen	HSW, MARSIG, HBRS
AP 1.3	**Untersuchungen zur Optimierung der Methode zur Risikobewertung von Hafenanlagen**	
AP 1.3.1	Ist-Analyse: Erfassung der Methodik zur durch den ISPS-Code vorgeschriebenen Risikobewertung; Analyse des bestehenden und ggf. alternativer Verfahren zur Risikoanalyse	
AP 1.3.2	Anpassung der bestehenden Methode zur Risikobewertung in enger Zusammenarbeit mit den Endnutzern	HBRS
AP 1.3.3	Entwicklung einer Informationsvisualisierung zur Unterstützung der Durchführung von Risikobewertungen evtl. unter Einbezug der SMT	
AP 1.3.4	Exemplarische Durchführung (Fallstudie) einer Risikobewertung einer Hafenanlage inklusive einer Visualisierung	

AP 2	**Technologieintegration zur Gefahrstoffkontrolle**	**ZA**
AP 2.1	**Überwachung Zugang Schiff und Hafen – Gefahrstoffkontrolle**	
AP 2.1.1	Machbarkeitsstudie zur Erstellung eines Fahrzeugprofils	
AP 2.1.2	Integration von Detektionssystemen für die Gefahrstoffkontrolle	HBRS

AP 3	**Entscheidungsunterstützung an Bord**	**ZA**
AP 3.1	**Definition von Präventiv-/Notfallmaßnahmen und -abläufen für Security-Vorfälle an Bord**	
AP 3.1.1	Situationsabhängige Spezifikation von Präventiv- und Notfallmaßnahmen und -abläufen	HSW

AP 3.3	**EUS für Trainingszwecke**	
AP 3.3.1	Entwicklung eines integrierten EUS-/Trainingskonzepts	
AP 3.3.4	Evaluation des Trainingskonzepts	HSW, ISV
AP 3.4	**EUS-Einsatz zur Koordination der Maßnahmen durch die Reederei**	
AP 3.4.2	Erstellung eines Konzepts	

AP 4	**Schulung und Training**	**ZA**
AP 4.2	**Übungen**	
AP 4.2.1	Konzeptentwurf für schnittstellenübergreifende Übungen	
AP 4.2.3	Zuarbeit zur Erstellung eines Handbuches für Schulungen und Übungen	

B. Projektergebnisse und Verwertung

B.1 Ergebnisse

B.1.1 AP 1.1: Gefahrenabwehr in der Hafenanlage und im Gesamthafen

In AP 1.1.2 wurde der Wechsel von Gefahrenstufen untersucht. Gefahrenstufe I bezeichnet den Normalbetrieb eines Hafens, in dem ein Minimum an Maßnahmen zur Gefahrenabwehr aufrechterhalten werden muss. Aufgrund eines sicherheitsrelevanten Ereignisses kann die für die Hafenanlage zuständige Sicherheitsbehörde Gefahrenstufe II ausrufen, in der für einen bestimmten Zeitraum zusätzliche Maßnahmen zur Gefahrenabwehr von zuständigen Personen in der Hafenanlage, vor allem dem Port Facility Security Officer (PFSO) als ersten Ansprechpartner der Sicherheitsbehörde, umzusetzen sind (zur Definition von Gefahrenstufen siehe Verordnung (EG) Nr. 725/2004, 2004, S. 26).

Die mit einer Erhöhung der Gefahrenstufe einhergehenden zusätzlichen Maßnahmen bedeuten einen zusätzlichen Aufwand, der abhängig von der jeweiligen Maßnahme Ressourcen wie Personal, Zeit und Kosten in Anspruch nimmt. Je nach Perspektive sind die unterschiedlichen betroffenen Parteien an unterschiedlichen Fragestellungen hinsichtlich des Aufwands einer Gefahrenstufenerhöhung interessiert:

- Hafenanlagenbetreiber, Mitarbeiter (inklusive Zulieferer und Handwerker) und Passagiere:
  Wie schnell können die geforderten Maßnahmen zur Sicherheit aller Beteiligten umgesetzt werden?
- Hafenanlagenbetreiber:
  Wie hoch sind die Kosten, die durch die zusätzlichen Maßnahmen verursacht werden?
- Mitarbeiter, welche die Maßnahmen umzusetzen haben:
  Wie hoch ist die zusätzliche Arbeitsbelastung während der Umsetzung von Maßnahmen?

Im Arbeitspaket (AP) 1.1.2 „Untersuchungen zum Wechsel von Gefahrenstufen“ wurden die Maßnahmen zur Abschätzung des zusätzlichen Aufwands, der bei der Erhöhung der Gefahrenstufe von I auf II verursacht wird, analysiert. Folgende aus der Aufgabenstellung abgeleitete Forschungsfragen werden durch die Analyse beantwortet:

Wie hoch wird der zusätzliche Aufwand eingeschätzt zur Umsetzung von Maßnahmen in Gefahrenstufe II hinsichtlich

- des notwendigen Zeitbedarfs zur Umsetzung von Maßnahmen?
- des Einsatzes zusätzlichen Personals?
- der zusätzlichen Beanspruchung vorhandenen Personals?

Wie im nächsten Abschnitt begründet, wurden als Datengrundlage für die Analyse zwei Gefahrenabwehrpläne verwendet, in denen die Maßnahmen für die unterschiedlichen Gefahrenstufen niedergelegt sind. Als zusätzliches Ergebnis der Analyse ergaben sich Verbesserungsvorschläge hinsichtlich der Darlegung von Maßnahmen für unterschiedliche Gefahrenstufen in Gefahrenabwehrplänen, welche ebenfalls in diesem Bericht aufgeführt werden.

<u>Auswahl der Daten zur Durchführung der Analyse</u>

Grundsätzlich kamen zur Bearbeitung des Arbeitspakets drei mögliche Datenquellen in Frage:

1. Gefahrenabwehrpläne,
2. ISPS-Code-Anforderungen (vgl. Verordnung (EG) Nr. 725/2004, 2004) und
3. erfasste Daten zu ISPS-Übungen in Hafenanlagen.

Zu 1: Gefahrenabwehrpläne repräsentieren die geforderten Maßnahmen in den drei Gefahrenstufen. Gefahrenabwehrpläne werden von Hafenanlagenbetreibern in Zusammenarbeit mit der zuständigen Sicherheitsbehörde erstellt und von letzterer zertifiziert. Die Umsetzung der Maßnahmen zu den Gefahrenstufen wird in Übungen erprobt. Die Daten in Gefahrenabwehrplänen werden als Grundlage zur vorgesehen Maßnahmen-Analyse als geeignet bewertet.

Zu 2: Die Anforderungen des ISPS-Codes bezüglich Maßnahmen in unterschiedlichen Gefahrenstufen sind zumeist nicht konkret dargelegt und oftmals nur als Vorschläge formuliert. Da aus diesem Grunde keine konkreten Aussagen bezüglich des Mehraufwands von Maßnahmen in Gefahrenstufe II im Vergleich zu Gefahrenstufe I zu erwarten sind, wird der ISPS-Code für eine Analyse als nicht geeignet bewertet.

Zu 3: Erfasste Daten zu konkreten Gefahrenstufenerhöhungen im Rahmen von Übungen bilden auch eine mögliche Quelle zur Analyse des Mehraufwands. Die in VESPERPLUS durchgeführte Datenerhebung im Rahmen einer Übung am 24.10.2012 in Puttgarden war jedoch in Bezug auf die Gefahrenstufenumsetzung aufgrund eines Missverständnisses nicht vollständig. Diese Daten kommen daher für eine Analyse nicht in Frage.

Aus der Bewertung der möglichen Datenquellen ergibt sich, dass die zur Verfügung stehenden Daten von Gefahrenabwehrplänen zweier Hafenanlagen für die grundlegende Analyse des Mehraufwands einer Gefahrenstufenumsetzung genutzt werden.

Die Vorgehensweise der quantitativen Inhaltsanalyse

Zur Auswertung der Daten zweier Gefahrenabwehrpläne (im Folgenden wird auf „GAP-1“ und „GAP-2“ referenziert, um die Vertraulichkeit der Inhalte zu wahren) wird eine quantitative Inhaltsanalyse (vgl. u.a. Bortz & Döring, 2006) durchgeführt. Die Auswertungsmethode der quantitativen Inhaltsanalyse ermöglicht abhängig vom Datenmaterial eine Beurteilung der Inhalte, welche sich auf die Erstellung eines individuellen Kategoriensystems stützt. Dabei wird entweder ein vorhandenes Kategoriensystem verwendet (deduktive Vorgehensweise), ein Kategoriensystem durch Sichtung des Datenmaterials vorbereitet (induktive Vorgehensweise), wobei eine Konkretisierung auch noch während der Analyse stattfinden kann, oder es wird eine Mischform aus deduktiver und induktiver Vorgehensweise gewählt. Bei der vorliegenden Analyse wurde die Mischform gewählt: Aus der Forschungsfrage abgeleitete Kategorien wurden bereits vor der Sichtung des Datenmaterials zu einem ersten Kategoriensystem zusammengefügt, jedoch durch Sichtung des Datenmaterials und im Laufe der Analyse ergänzt. Einzeldaten wird während des Einsatzes des Kategoriensystems für jedes Merkmal (ein Merkmal kann als Variable verstanden werden) ein Wert (Variablenausprägung) zugewiesen.

Vor einer Bewertung des Mehraufwands zu einzelnen Maßnahmen musste dieser identifiziert werden. Hierzu wurden einzelne Maßnahmen aus den Datenquellen zu den beiden untersuchten Gefahrenstufen extrahiert und in die ersten beiden Spalten einer Tabelle eingetragen. In der dritten Spalte wurde der Mehraufwand zur Umsetzung der einzelnen Maßnahmen der Gefahrenstufe II im Vergleich zur Gefahrenstufe I abgeschätzt und dargelegt (vgl. Tabelle 1).

Tabelle 1: Tabellenstruktur zur Identifizierung des Mehraufwands einzelner Maßnahmen bezüglich der Gefahrenstufen I und II mit Beispieleintrag

Maßnahmen in Gefahrenstufe I	Maßnahmen in Gefahrenstufe II	Mehraufwand zur Umsetzung der Maßnahmen in Gefahrenstufe II
Stichprobenartige Fahrzeugkontrolle	Kontrolle von 50% der Fahrzeuge	Erhöhung der Fahrzeugkontrolle von stichprobenartig auf 50%
…	…	…

Der Mehraufwand zur Umsetzung der einzelnen Maßnahmen in Gefahrenstufe II im Vergleich zur Gefahrenstufe I wurde als Grundlage für die Bewertung hinsichtlich verschiedener Merkmale verwendet. Einzelne zusätzliche und intensivierte Maßnahmen bilden somit die Textelemente, auf welche die Kodierung angewendet wird. Wie bereits erwähnt, wurde zur Kodierung ein Kategoriensystem vor und während der Analyse erarbeitet, welches in Tabelle 2 mit einem Beispiel dargestellt ist.

Tabelle 2: Kategoriensystem zur Bewertung des Mehraufwands einzelner Maßnahmen in Gefahrenstufe II im Vergleich zum Aufwand entsprechender Maßnahmen in Gefahrenstufe I

Mehraufwand (Übertrag der Spalte 3 aus Tabelle 1)	Zusätzliche Beanspruchung vorhandener Mitarbeiter	Einsatz zusätzlicher Mitarbeiter	Notwendige Zeitbedarf zur Umsetzung	Zusätzliche Kosten	Maßnahmendurchführung einmalig oder andauernd	Verzögerung bis zum Wirksamwerden der Maßnahme
Erhöhung der Fahrzeugkontrolle von stichprobenartig auf 50%	Hoch	Nein	Hoch	Nein	Andauernd	Gering
…	…	…	…	…	…	…

Die Qualität der Datenanalyse ist maßgeblich davon abhängig, wie die Merkmale des Kategoriensystems definiert und für die einzelnen Einträge kodiert (Zuordnung einer Maßnahme zu einer Merkmalsausprägung) werden. Dabei ist eine Kodierung „intersubjektiv nachvollziehbar, wenn die Kategorien eindeutig definiert, klar voneinander abgegrenzt und erschöpfend sind“ (Bortz & Döring, 2006, S. 153). Die Merkmale des Kategoriensystems und ihre Ausprägungen wurden wie folgt festgelegt:

- Zusätzliche Beanspruchung vorhandener Mitarbeiter
  Der Mehraufwand einer Maßnahme kann eine zusätzliche Beanspruchung der in der Hafenanlage eingesetzten Mitarbeiter bewirken. Die zusätzliche Beanspruchung wird mit einer der folgenden möglichen Ausprägungen bewertet:
  - Gering (Vorhandene Mitarbeiter werden durch die Umsetzung der Maßnahme nur geringfügig zusätzlich beansprucht, bspw. bei Anweisung der Benachrichtigung einer anderen Person.)
  - Hoch (Vorhandene Mitarbeiter werden durch die Umsetzung der Maßnahme stark zusätzlich beansprucht, bspw. weil eine Kontrolle von Fahrzeugen von stichprobenartig auf 100% erhöht wird oder eine Maßnahme immer wieder durchgeführt werden muss.)

- Einsatz zusätzlicher Mitarbeiter
  Der Mehraufwand einer Maßnahme kann den Einsatz zusätzlicher Mitarbeiter in der Hafenanlage bewirken. Der Einsatz zusätzlicher Mitarbeiter wird mit einer der folgenden möglichen Ausprägungen bewertet:
  - Nein (Es werden keine zusätzlichen Mitarbeiter zur Umsetzung des Mehraufwands der Maßnahme benötigt.)
  - Ja (zusätzliche Mitarbeiter werden zur Umsetzung des Mehraufwands der Maßnahme benötigt.)
- Notwendiger Zeitbedarf zur Umsetzung
  Die Umsetzung einer Maßnahme nimmt eine bestimmte Zeitdauer in Anspruch. Der Zeitbedarf zur Durchführung der Maßnahme wird mit einer der folgenden möglichen Ausprägungen bewertet:
  - Gering (wenn die Implementierung der Maßnahme bspw. lediglich die Schließung eines Zugangs zur Hafenanlage bedeutet und somit binnen weniger Minuten umgesetzt ist)
  - Hoch (wenn zur Implementierung der Maßnahme bspw. die ständige Überwachung eines Zugangs notwendig ist)
- Zusätzliche Kosten
  Die Umsetzung einer Maßnahme kann zusätzliche Kosten verursachen. Die zusätzlichen Kosten zur Implementierung einer Maßnahme werden mit einer der folgenden möglichen Ausprägungen bewertet:
  - Nein (Es werden keine zusätzlichen Kosten zur Umsetzung der Maßnahme verursacht, bspw. bei Anweisung der Erhöhung der Beobachtungsintensität, ohne dafür zusätzliches Personal einsetzen zu müssen)
  - Ja (Es werden zusätzliche Kosten zur Umsetzung der Maßnahme verursacht, bspw. beim Einsatz von zusätzlichem Personal, das vergütet werden muss, oder durch Schließung von Zugängen zur Anlage, welche den Schiffsverkehr beeinträchtigen und somit eine Gewinnsenkung verursachen.)
- Maßnahmendurchführung einmalig oder andauernd
  Eine Maßnahme kann entweder über eine einmalige Durchführung abgeschlossen sein oder muss andauernd (mehrfach bzw. über die gesamte Zeit der Gefahrenstufenerhöhung) durchgeführt werden. Die Durchführung einer Maßnahme wird mit einer der folgenden möglichen Ausprägungen bewertet:
  - Einmalig (Die Maßnahme muss lediglich einmal durchgeführt werden, um als abgeschlossen zu gelten.)
  - Andauernd (Die Maßnahme muss mehrmals bzw. solange durchgeführt werden, wie Gefahrenstufe II vorherrscht.)
- Verzögerung bis zum Wirksamwerden der Maßnahme
  Bis zur Umsetzung und somit Wirksamwerden einer Maßnahme kann entweder viel oder wenig Zeit vergehen. Die Dauer bis zum Wirksamwerden einer Maßnahme wird mit einer der folgenden möglichen Ausprägungen bewertet:
  - Gering (wenn die Implementierung der Maßnahme bspw. lediglich eines Anrufs bedarf und dadurch binnen weniger Minuten wirkungsvoll ist, wie beim Schließen von Zugangstoren)
  - Hoch (wenn zur Implementierung der Maßnahme bspw. zusätzliches Personal notwendig ist, welches erst kontaktiert und in den Hafen anreisen muss, bis es die Maßnahme umsetzen kann)

Zur besseren Übersicht sind die Merkmale und ihre Merkmalsausprägungen in Tabelle 3 noch einmal aufgeführt.

Tabelle 3: Übersicht über die Merkmale und ihre Merkmalsausprägungen des Kategoriensystems

Merkmal	Ausprägung 1	Ausprägung 2
Zusätzliche Beanspruchung vorhandener Mitarbeiter	Gering	Hoch
Einsatz zusätzlicher Mitarbeiter	Nein	Ja
Notwendiger Zeitbedarf zur Umsetzung	Gering	Hoch
Zusätzliche Kosten	Nein	Ja
Maßnahmendurchführung einmalig oder mehrfach	Einmalig	Andauernd
Verzögerung bis zum Wirksamwerden der Maßnahme	Gering	Hoch

Vorläufige Ergebnisse der quantitativen Inhaltsanalyse

GAP-1 und GAP-2 unterscheiden sich hinsichtlich der Struktur, mit der die Maßnahmen in den Gefahrenabwehrplänen niedergelegt sind.

In GAP-1 sind die Kapitel zu Maßnahmen nach Gefahrenstufen strukturiert: Ein Kapitel enthält alle Maßnahmen zu Gefahrenstufe I und ein Kapitel alle Maßnahmen zu Gefahrenstufe II. Entsprechungen der Maßnahmen zu den einzelnen Gefahrenstufen sind somit räumlich getrennt und nicht direkt zugeordnet. Dafür werden in jedem Kapitel alle Sicherheitsbereiche vollständig aufgeführt. Beide Kapitel sind in ihrem Aufbau unterschiedlich strukturiert. Unterkapitel zu einer Gefahrenstufe sind teilweise relevant auch für die andere Gefahrenstufe, in der jedoch nicht entsprechende Unterkapitel vorhanden sind.

In GAP-2 sind die Kapitel zu Maßnahmen nach Sicherheitsbereichen in zwei Kapitel strukturiert: Ein Kapitel enthält alle Maßnahmen zum Sicherheitsbereich der Ausweisordnung und ein Kapitel alle Maßnahmen zum Sicherheitsbereich der Zugänge. Entsprechungen der Maßnahmen zu den einzelnen Gefahrenstufen sind in einem der Kapitel räumlich direkt nebeneinander dargestellt, im anderen Kapitel jedoch über Unterkapitel voneinander getrennt. Dort, wo Unterkapitel nach Gefahrenstufen gegliedert sind, entspricht sich der inhaltliche Aufbau nur teilweise.

Eine Herausforderung ist, dass viele der Maßnahmen in GS II nicht konkret einzelnen Maßnahmen in GS I zugeordnet sind, so dass eine eindeutige Abschätzung des Mehraufwands nur dort möglich ist, wo eine eindeutige Zuordnung vorgenommen werden kann. Dort, wo die Zuordnung nicht eindeutig möglich ist (vor allem in Fällen, in denen eine Maßnahme in GS II mehreren in GS I zugeordnet werden können), käme diese einer Interpretation der Inhalte gleich, welche als fehleranfällig und subjektiv zu betrachten ist. Weitergedacht kann sich diese Fehleranfälligkeit auch im Einsatz von Gefahrenabwehrplänen zur Umsetzung von Gefahrenstufen fortpflanzen: Die vollständige Umsetzung von Maßnahmen ist bei Spielräumen in der Zuordnung nicht gewährleistet, zumal auch damit gerechnet werden muss, dass nicht nur der zuständige Port Facility Security Officer (PFSO), welcher den Gefahrenabwehrplan erstellt hat und die Hafenanlage kennt, den Gefahrenabwehrplan anwenden muss, sondern in Ausnahmefällen auch andere Personen, welche den PFSO bspw. in Krankheitsfällen vertreten. Bei der Inhaltsanalyse wurde so vorgegangen, dass nur bei einer möglichen eindeutigen Zuordnung diese auch vorgenommen wurde. Wo diese nicht vorgenommen werden konnte, wurden die Maßnahmen unabhängig von den Entsprechungen in GS I als zu kodierende Textelemente in die Tabellen eingetragen.

Eine weitere Herausforderung bei Ermittlung des Mehraufwands war die Anforderung an Gefahrenabwehrpläne, auf der einen Seite konkrete Maßnahmen zu den drei Gefahrenstufen aufzeigen zu müssen, auf der anderen Seite jedoch situationsabhängig adäquate Maßnahmen bereit zu stellen. Beide Anforderungen kann ein Gefahrenabwehrplan nicht erfüllen. Zumindest ist dies nicht mit vertretbarem Aufwand der Gefahrenabwehrplanerstellung und vertretbarem Umfang eines Gefahrenabwehrplans zu erreichen. Die gesichteten Maßnahmen in den beiden analysierten Gefahrenabwehrplänen weisen darauf hin, dass die Ersteller jeweils der Anforderung, situationsabhängig angemessen reagieren zu können, den Vorrang vor konkreten Einzelmaßnahmen gegeben haben. Diese Vorgehensweise kann nach derzeitigem Kenntnisstand als zweckmäßig erachtet werden, stellte jedoch aus folgendem Grund bei der quantitativen Inhaltsanalyse eine Herausforderung dar: Maßnahmen, deren Aufwand situationsabhängig unterschiedlich ist, können auch nicht eindeutig in ihrem Mehraufwand im Vergleich zu Gefahrenstufe I bewertet werden. In diesen Fällen wurde eine Abschätzung des durchschnittlichen Aufwands zwischen zwei Extremsituationen vorgenommen, welche der Kodierung des entsprechenden Merkmals zugrunde gelegt wurde.

Für GAP-1 wurden insgesamt 45 Maßnahmen der Gefahrenstufe II identifiziert, welche zusätzlich zu denen in Gefahrenstufe I durchgeführt werden müssen oder die der Gefahrenstufe I intensivieren. Für GAP-2 wurden 25 Maßnahmen identifiziert. Es kann vermutet werden, dass GAP-1 eine erheblich höhere Anzahl an Maßnahmen für Gefahrenstufe II enthält, da dieser die größere der beiden Hafenanlagen beschreibt.

Die Auswertung der beiden Gefahrenabwehrplandaten wurde in einer dreidimensionalen Kontingenztafel (vgl. Bortz & Döring, 2006, S. 152) zusammengefasst (vgl. Tabelle 4). Dabei wurden die Merkmalsausprägungen, welche einen geringeren Mehraufwand bedeuten (gering/nein/einmalig), und die, welche einen höheren Mehraufwand bedeuten (hoch/ja/andauernd), jeweils in einer Zeile zusammengefasst. Zusätzlich zu den addierten Merkmalskodierungen wurde die jeweilige Prozentzahl errechnet, um das Verhältnis zwischen hohem und geringem Aufwand pro Merkmal und Gefahrenabwehrplan besser einschätzen zu können. Es ist jedoch darauf hinzuweisen, dass alle Werte lediglich deskriptivstatistische Eigenschaften besitzen und keinesfalls inferenzstatistisch zu deuten sind. Die folgenden Ausführungen sind als Interpretationen und Mutmaßungen anzusehen.

Tabelle 4: Dreidimensionale Kontingenztafel zur quantitativen Inhaltsanalyse für GAP-1 und GAP-2

		Zusätzliche Auslastung vorhandener Mitarbeiter	Zusätzliche Mitarbeiter	Notwendige Zeit zur Umsetzung	Zusätzliche Kosten	Maßnahme einmalig oder andauernd	Verzögerung bis zum Wirksamwerden der Maßnahme
GAP-1	gering/nein/einmalig	20 (44%)	38 (84%)	30 (67%)	34 (76%)	24 (53%)	40 (89%)
	hoch/ja/andauernd	25 (56%)	7 (16%)	15 (33%)	11 (24%)	21 (47%)	5 (11%)
GAP-2	gering/nein/einmalig	11 (44%)	9 (36%)	7 (28%)	9 (36%)	4 (16%)	9 (36%)
	hoch/ja/andauernd	14 (56%)	16 (64%)	18 (72%)	16 (64%)	21 (84%)	16 (64%)

In Bezug auf die Auslastung vorhandener Mitarbeiter zeigt sich, dass sowohl in GAP-1 als auch in GAP-2 bei 56% der Maßnahmen vorhandene Mitarbeiter einer erhöhten Belastung beim

Hochsetzen der Gefahrenstufe von I auf II ausgesetzt sind (dies entspricht 25 der 45 Maßnahmen in GAP-1 und 14 der 25 Maßnahmen in GAP-2). Im Gegensatz zu GAP-2 wurden in GAP-1 häufig konkrete Rollen aufgeführt, welche Maßnahmen umzusetzen haben. Die Auswertung ergibt, dass in GAP-1 vor allem der PFSO von der zusätzlichen Auslastung betroffen ist.

In GAP-1 müssen zur Umsetzung von 7 der 45 Maßnahmen zusätzliche Mitarbeiter eingesetzt werden. Es werden insgesamt 9 zusätzliche Mitarbeiter benötigt. Im Vergleich dazu werden 10 zusätzliche Mitarbeiter in GAP-2 benötigt, um die Umsetzung von 16 der 25 Maßnahmen zu gewährleisten. An dieser Stelle wird – vor allem bei mittel- und längerfristigem Aufrechterhalten der erhöhten Gefahrenstufe – auch die Relevanz für das Merkmal „zusätzliche Kosten" sehr deutlich.

Bezüglich der notwendigen Zeit zur Umsetzung einer Maßnahme sind die Verhältnisse für GAP-1 (gering: 30 – hoch: 15) und GAP-2 (gering: 7 – hoch: 18) unterschiedlich. Auch hier kann nach Auswertung der Daten vermutet werden, dass die Größe der jeweiligen Anlage einen Einfluss auf dieses Merkmal besitzt: In GAP-1 sind viele der Maßnahmen, welche nur geringe Zeit zur Umsetzung benötigen, die Anweisung von organisatorischen Veränderungen und die Benachrichtigung zum Einsatz zusätzlichen Personals.

Für GAP-1 (11 von 45 Maßnahmen) ist die Minderzahl der Maßnahmen mit zusätzlichen Kosten verbunden. Die Auswertung zeigt, dass die überwiegende Zahl an kostenverursachenden Maßnahmen zwei Bereichen zuzuordnen sind: Der Einsatz von zusätzlichem Personal auf der einen Seite und – damit teilweise verbunden – die Schließung von Zugängen und somit Verzögerungen der Arbeitsabläufe. 16 der 25 Maßnahmen des GAP-2 und somit die Mehrzahl sind hingegen mit zusätzlichen Kosten verbunden.

Der Anteil einmaliger im Vergleich zu den andauernden Maßnahmen unterscheidet sich bei den untersuchten Gefahrenabwehrplänen: Der geringfügig höhere Anteil an Maßnahmen wird in GAP-1 über eine einmalige Durchführung erledigt (einmalig: 24 – andauernd: 21). Hingegen muss die überwiegende Anzahl an Maßnahmen in GAP-2 mehrfach oder andauernde durchgeführt werden (einmalig: 4 – andauernd: 21). Auch hier kann eine Verbindung zur Größe der Hafenanlage vermutet werden: In GAP-1 betrifft eine größere Anzahl an Maßnahmen infrastrukturelle Veränderungen, welche über eine einmalige Durchführung erledigt werden.

Die Mehrheit der Maßnahmen in GAP-1 (40 von 45 Maßnahmen) wird unmittelbar nach Anweisung der Gefahrenstufenerhöhung wirksam. Eine erhöhte Gefahrenstufe kann demnach größtenteils zügig umgesetzt werden. In GAP-2 (9 von 25 Maßnahmen) wird die Mehrheit der Maßnahmen nicht direkt wirksam. Das unterschiedliche Verhältnis bei GAP-1 (hohe Verzögerung: 11%) und GAP-2 (hohe Verzögerung: 64%) kann darauf zurückgeführt werden, dass in GAP-2 wesentlich mehr Maßnahmen mit dem Einsatz zusätzlichen Personals zusammenhängen und der Einsatz zusätzlichen Personals mit einer hohen Verzögerung kodiert wurde (zusätzliches Personal muss benachrichtigt werden und erst einmal bis zum Einsatzort gelangen, bevor es zur Sicherheit beitragen kann).

Bei der Analyse der beiden Gefahrenabwehrpläne wurden zwei grundsätzliche Möglichkeiten der Strukturierung von Maßnahmen zu unterschiedlichen Gefahrenstufen identifiziert. Zum einen kann nach Sicherheitsbereichen strukturiert werden. Dies bedeutet, dass für jeden Sicherheitsbereich die Maßnahmen für alle Gefahrenstufen in einem Kapitel aufgeführt werden. Der Vorteil dieser Methode besteht darin, dass schnell der Unterschied zwischen Maßnahmen verschiedener Gefahrenstufen erkannt wird. Der Nachteil ist, dass sich insgesamt die Maßnahmen über eine wesentlich höhere Seitenanzahl erstreckt. Zum anderen kann nach Gefahrenstufen strukturiert werden. Dies bedeutet, dass für jede Gefahrenstufe ein Kapitel angelegt wird, in dem für alle Sicherheitsbereiche die Maßnahmen hinterlegt sind. Der Vorteil dieser Methode ist, dass Maßnahmen zu einer Gefahrenstufe kompakt auf wenigen Seiten dargestellt werden. Der Nachteil ist, dass der Bezug zu den Maßnahmen anderer Gefahrenstufen verloren geht. Grundsätzlich wird jedoch keine Empfehlung für eine der beiden Strukturierungsmöglichkeiten ausgesprochen.

Ein weiterer Nachteil entsteht bei der Strukturierung nach Gefahrenstufen, wenn die Kapitel bezüglich der Unterteilung in Sicherheitsbereiche eine unterschiedliche Struktur aufweisen. In beiden untersuchten Gefahrenabwehrplänen ist keine eindeutige Zuordnung möglich. So werden beispielsweise teilweise für einen bestimmten Bereich Maßnahmen in Gefahrenstufe I angegeben, für Gefahrenstufe II existiert jedoch kein entsprechendes Teilkapitel. Die Maßnahmen sind hier für Gefahrenstufe II in einem anderen, allgemeingültigen Unterkapitel eingetragen. Andererseits werden im Unterkapitel zur Gefahrenstufe I teilweise Maßnahmen beschrieben, welche auch für Gefahrenstufe II relevant sind, jedoch in diesem Unterkapitel nicht aufgeführt sind. Auf diese Weise besteht die Gefahr, in Gefahrenstufe II diese Maßnahmen unberücksichtigt zu lassen. Aus diesen Gründen wird empfohlen, auf eine einheitliche Struktur für Maßnahmen zu unterschiedlichen Gefahrenstufen zu achten, um das Auffinden von Maßnahmen zu erleichtern und eine bessere Zuordnung von Maßnahmen zu gewährleisten. Zusätzlich wird empfohlen, dass Maßnahmen, die für alle Gefahrenstufen gelten, entweder auch in jedem einzelnen Kapitel aufgeführt werden, oder – platzsparend – ein eigenständiges Kapitel „Maßnahmen, die in allen Gefahrenstufen umzusetzen sind" erhalten. Im analysierten GAP-1 wurde zusätzlich für Gefahrenstufe II eine Checkliste hinterlegt, welche übersichtlich sämtliche Maßnahmen in einer priorisierten Reihenfolge zur Umsetzung der Gefahrenstufe II aufführt. Eine solche Checkliste wird als sehr hilfreich erachtet, um die Maßnahmen vollständig umzusetzen. Als weiteres Hilfsmittel zur Umsetzung von Gefahrenstufen kann die eigens dafür entwickelte Security Modeling Technique (SMT, vgl. z.B. Ley & Dalinger, 2010) angeführt werden.

Die eingangs gestellte Forschungsfrage lautete: Wie hoch wird der zusätzliche Aufwand eingeschätzt zur Umsetzung von Maßnahmen in Gefahrenstufe II hinsichtlich

- des notwendigen Zeitbedarfs zur Umsetzung von Maßnahmen?
- des Einsatzes zusätzlichen Personals?
- der zusätzlichen Beanspruchung vorhandenen Personals?

Hinsichtlich des Zeitbedarfs kann festgestellt werden, dass großer Zeitbedarf bis zum Wirksamwerden von Maßnahmen vor allem mit dem Einsatz zusätzlichen Personals verbunden ist. Insgesamt dürfte jedoch – wie die Erfahrungen mit bisher begleiteten Übungen zeigen – der gewährte Zeitraum von bis zu zwölf Stunden zur Erhöhung der Gefahrenstufe von I auf II normalerweise nicht benötigt werden. Die Analyse lässt jedoch auch vermuten, dass der Zeitbedarf, wie auch andere Merkmale einer Gefahrenstufenerhöhung, von der Größe der Hafenanlage beeinflusst werden. Vielleicht wäre hier eine Differenzierung der Zeitvorgabe in Abhängigkeit der Hafenanlagengröße sinnvoll.

Die Höhe zusätzlich anfallender Kosten steigt mit der Dauer, für die Gefahrenstufe II gilt. Dies wird aus den laufenden Betriebskosten für zusätzliches Personal und die Verzögerung der Arbeitsabläufe geschlossen. Für einen Hafenanlagenbetreiber wäre somit eine möglichst kurze Dauer einer Gefahrenstufenerhöhung vorteilhaft. Da jedoch die Sicherheit selbstverständlich eine höhere Priorität besitzt, wird nach Möglichkeiten der Entlastung von Hafenanlagenbetreibern gesucht. Hinsichtlich der Verzögerungen von Arbeitsabläufen wurde bereits eine Lösung in VESPER erarbeitet, welche teilweise bereits in Hafenanlagen Anwendung findet: Eine Verringerung der Anzahl an Zugängen zur Hafenanlage besitzt demnach keinen Einfluss auf die Sicherheit, solange diese Zugänge entsprechend der Gefahrenstufe gesichert werden. Dies bedeutet, dass Arbeitsabläufe nur geringfügig verlangsamt werden, wie in einer Simulation gezeigt werden konnte. Andererseits bedeutet die Öffnung aller Zugänge in Gefahrenstufe II jedoch auch den erhöhten Einsatz von Personal, welcher wiederum erhöhte Betriebskosten zur Folge hat.

Bezüglich der zusätzlichen Auslastung von Personal ist vor allem der PFSO betroffen, welche nicht zuletzt mit der hohen Verantwortung einhergeht. Jedoch sind auch andere Mitarbeiter einer erhöhten Belastung ausgesetzt. Die Gefahr von Fehlern – gerade auch bei lang andauernden Gefahrenstufenerhöhungen – ist gegeben. Aus diesem Grunde ist auf genügend

zusätzliches Personal zu achten. Die Belastungssituation einzelner Rollen in der Hafenanlage könnte im Zuge der Beobachtung zukünftiger Übungen bewertet werden.

Zusätzlich zur Analyse in Bezug auf die Forschungsfragen können weitere Vorschläge auf Grundlage der analysierten Gefahrenabwehrpläne gemacht werden:

- Maßnahmen zu spezifischen Gefahrenstufen sind oftmals sehr allgemein gehalten:
  - Vorteil: Maßnahmen können an die Situation angepasst umgesetzt werden.
  - Nachteil: Die Maßnahmen sind weniger konkret, was zu Verunsicherungen führen kann. Vorschlag: Es ist ggf. sinnvoll, Maßnahmen konkret zu benennen, jedoch situationsabhängig eine Priorität zu vergeben (bspw. hinsichtlich der Reihenfolge zu schließender Zugänge).
- Die Maßnahmen werden teilweise in langen Sätzen und Fließtext beschrieben. Kurze und stichpunktartige Anweisungen in Tabellen würden zum schnelleren Auffinden und Einleiten der Maßnahmen beitragen. Grundsätzlich wird hier auch auf die Möglichkeit des Einsatzes von SMT-Modellen (vgl. u.a. Ley & Dalinger, 2010) hingewiesen.
- Die meisten Maßnahmen werden beschrieben, ohne dass eindeutig eine verantwortliche Person/Rolle genannt wird. Mit der konkreten Benennung zuständiger Personen oder den Einsatz von Rollenkarten im Falle einer Gefahrenstufenerhöhung könnten Zuständigkeiten und Verantwortlichkeiten sichtbar und die Ausführung von Maßnahmen unterstützt werden.
- Nur in GAP-1 wurde situationsabhängig die Anzahl zusätzlich einzusetzenden Personals angegeben. Dies wird jedoch grundsätzlich als sinnvoll erachtet, um einen Überblick über die verfügbaren und benötigten Ressourcen zu erhalten.
- Es sollte darauf geachtet werden, dass Maßnahmen der Gefahrenstufe II eindeutig Maßnahmen oder Sicherheitsbereichen der Gefahrenstufe I zugeordnet werden, um eine vollständige Umsetzung zu unterstützen. Teilweise werden in Gefahrenstufe II Maßnahmen intensiver als in Gefahrenstufe I gefordert; die entsprechende Maßnahme ist jedoch in Gefahrenstufe I gar nicht aufgeführt.
- Teilweise ist nicht ersichtlich, ob Maßnahmen der Gefahrenstufe II die entsprechenden Maßnahmen der Gefahrenstufe I ersetzen oder ergänzen. Dies sollte jedoch grundsätzlich der Fall sein.
- Es fehlen teilweise Angaben, wo Ressourcen wie Telefonnummern, zus. Personal oder Hilfsmittel erhältlich sind zur Umsetzung der Maßnahmen in GS II. Dies würde die Gefahrenstufenerhöhung jedoch vereinfachen.

B.1.2 AP 1.2: Untersuchung der land- und wasserseitigen Schnittstellen

Zunächst werden die Arbeiten in AP 1.2.1 „Untersuchungen der Kommunikationsprozesse“ beschrieben:

Aufgabenstellung

Sowohl der Normalbetrieb als auch eine Gefahrenstufenerhöhung erfordern Informationsaustausch innerhalb von Hafenanlagen, Schiffen und Behörden ebenso wie Informationsaustausch zwischen diesen. Die Kommunikationswege sind dabei teilweise durch den ISPS-Code vorgegeben. Ziel der Arbeiten im Arbeitspacket 1.2.1: „Untersuchungen der Kommunikationsprozesse“ war es, die Kommunikationsprozesse zwischen landseitigen Organisationen, Behörden sowie der Schiffsseite zu untersuchen und zu verbessern. Die Arbeiten wurden in Zusammenarbeit mit den Häfen „Rostock“ und „Lübeck“, den Reedereien „TT-Line“ und „Scandlines“ sowie den zuständigen Behörden, dem „Bundesamt für Seeschifffahrt und Hydrographie“, dem „Landespolizeiamt Schleswig-Holstein“ (Behörde für Hafenanlagensicherheit) und dem „Verkehrsministerium Mecklenburg-Vorpommern“ durchgeführt.

Die Vorgehensweise

Die Arbeit in diesem Arbeitspaket lässt sich in drei Schritte gliedern:

1. Erfassung des Ist-Zustandes
2. Erfassung des Soll-Zustandes
3. Abgleich des Ist-Zustandes mit dem Soll-Zustand und Erarbeitung von Optimierungsvorschlägen

1. Erfassung des Ist-Zustandes

Im Zuge des Projektes Vesper^{PLUS} wurden jeweils eine Hafensicherheitsübung im Hafen Puttgarden und im Fährhafen Rostock durch das Fraunhofer FKIE begleitet. Die während der Übungen gesammelten Daten konnten in unterschiedlichen Arbeitspaketen verwendet werden, so auch hier zur Erfassung des Ist-Zustandes. Bereits für die Auswertung der Übungen wurden die Übungsdaten in Ablaufmodelle übertragen. Ein Beispiel für ein solches Modell findet sich in Abbildung 2. Da während der Hafensicherheitsübung in Puttgarden nur der Hafen involviert war, bei der Hafensicherheitsübung in Rostock sowohl der Hafen als auch die Schiffsseite beteiligt waren, wurde für die Auswertung der Ist-Daten die Hafensicherheitsübung in Rostock gewählt. Aus den Ablaufmodellen, die sämtliche Ereignisse und Handlungen beinhalten, wurden alle Kommunikationsverläufe extrahiert und in Kommunikationsmodelle übertagen. Ein Beispiel für einen Ausschnitt eines Kommunikationsmodells ist in der Abbildung 3 zu sehen. Als Darstellung wurde die Form einer Matrix gewählt. In der ersten Zeile sind alle Kommunikationspartner dargestellt. Für jeden Kommunikationspartner gibt jeweils eine Spalte für aktive Kommunikation, solche die von dieser Person ausgegangen ist, und eine Spalte für passive Kommunikation, die der Kommunikationspartner empfangen hat. Aktive Kommunikation wird mit einer dunklen Farbe dargestellt, passive Kommunikation mit einer hellen Farbe. Diese Unterscheidung wurde in die Tabellen aufgenommen, um den Soll-Ist-Vergleich genauer zu gestalten, da der ISPS-Code zum Teil die Richtung der Kommunikation genau vorgibt.

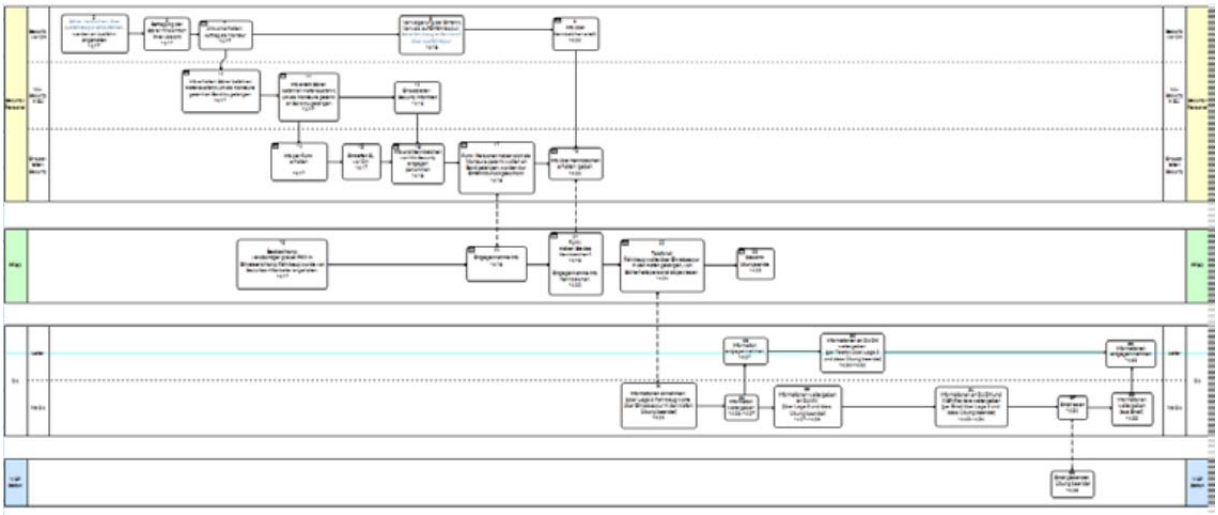

Abbildung 2: Beispiel für ein Ablaufmodell

Diese Form der Visualisierung ermöglicht die übersichtliche Darstellung der Kommunikationsinhalte, der Beteiligten und der Kommunikationsrichtung (von wem ging die Kommunikation aus, an wen war sie gerichtet). Um ein situationsabhängiges Verständnis zu ermöglichen, wurden die Kommunikationstabellen übungsnah strukturiert. Für jedes

Übungsszenario wurde eine eigene Kommunikationstabelle erstellt. Zusätzlich wurden Ereignisse definiert, die Kommunikation ausgelöst haben. Diese Angabe findet sich in der ersten Spalte. Die zweite Spalte beinhaltet die Kommunikation selbst.

Übung Rostock Szenario 1: Heraufsetzen Gefahrenstufe		DA MV		PFSO	
		IST	SOLL	IST	SOLL
GS II melden	DA MV meldet GS Erhöhung an PFSO	aktiv	Gefahrenstufe ändern (2_1-Regel-A)	passiv	Gefahrenstufe ändern (2_1-Regel-A)
	PFSO bestätigt GS Erhöhung	passiv	(für Schiff vorhanden)	aktiv	(für Schiff vorhanden)
	PFSO meldet GS Erhöhung an Leiter Sicherheitsdienst			aktiv	(nicht gefordert in 2, 4)
	PFSO meldet GS Erhöhung an weitere Einrichtungen und Firmen			aktiv	(nicht gefordert in 2, 4)
	PFSO meldet GS Erhöhung an Reedereien (CSO)			aktiv	(nicht gefordert in 2, 4)
	PFSO meldet GS Erhöhung an Deputy PFSO			aktiv	(nicht gefordert in 2, 4)
	CSO meldet Info über GS Erhöhung an SSO und Kapitän				
Ergreifen der ersten Maßnahmen	PFSO gibt Anweisung Personal zu schicken an EL Sicherheitsdienst			aktiv	(nicht gefordert in 2, 4)
	PFSO gibt Anweisung Kontrollstelle (KS) aufzubauen an Deputy			aktiv	(nicht gefordert in 2, 4)
	EL informiert PFSO, dass KS aufgebaut wird				
	PFSO erbittet um Info wenn KS fertig			aktiv	(nicht gefordert in 2, 4)
	Kapitän weist SSO an weitere Infos beim PFSO zu erfragen				
	EL informiert PFSO, dass KS fertig ist			passiv	(nicht gefordert in 2, 4)
	PFSO gibt Anweisung mit Kontrollen zu beginnen			aktiv	(nicht gefordert in 2, 4)
	PFSO meldet DA, dass KS fertig ist	passiv	(nicht gefordert in 2, 4)	aktiv	(nicht gefordert in 2, 4)

Abbildung 3: Ausschnitt aus einer Kommunikationstabelle für das erste Szenario

2. Erfassung des Soll-Zustandes

Um einen Vergleich zwischen Ist- und Soll-Zustand zu ermöglichen, wurden alle Soll-Vorgaben, welche die Kommunikation betreffen, aus dem ISPS-Code extrahiert.

Bereits die Analyse dieser Angaben für sich genommen hat gezeigt, dass es:

- Informationsredundanzen gibt,
- Kommunikationsprozesse teilweise stark unstrukturiert sind,
- Kommunikationsvorgaben für einzelne Akteure innerhalb des ISPS-Codes verstreut und unübersichtlich sind und
- Angaben zu weiterzugebenden Informationen teilweise nicht vorhanden sind.

Eine geeignete Methode zur Modellierung von unstrukturierten Kommunikationsprozessen konnte in der Literatur nicht identifiziert werden. Daher wurde für die Darstellung der Soll-Kommunikation (ISPS-Code-Vorgaben) eine eigene Modelliersprache entwickelt. Mit Hilfe der Communication Modeling Notation (COMON) wurden alle Vorgaben des ISPS-Codes in Flussdiagramme übertragen. Abbildung 4 zeigt die Grundelemente der COMON. Diese Grundelemente sind die Zeichenfläche mit Phasen- und Swimlane-Konzept, unterschiedliche Kontaktstellen in Form von Kreisen sowie verschiedene Kommunikationskontrollflüsse, um die unterschiedlichen Arten von Kommunikation darzustellen.

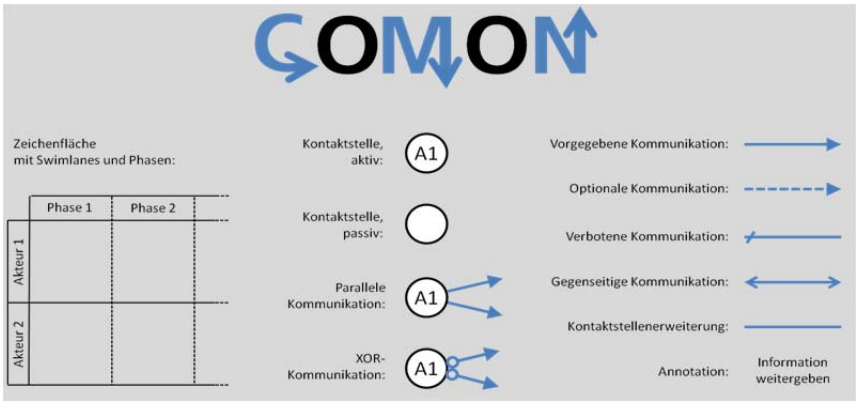

Abbildung 4: Die Grundelemente der COMON

Die zuvor extrahierten Kommunikationsvorgaben wurden in COMON-Modelle übertragen. Ein beispielhafter Ausschnitt aus einem Kommunikationsmodell ist in Abbildung 5 zu sehen. Dargestellt sind unterschiedliche Kommunikationspartner in den einzelnen Bahnen. Im vorliegenden Beispiel findet eine Kommunikation zwischen Schiffsseite und Landseite statt. Da diese übergreifende Kommunikation von besonderem Interesse in diesem Arbeitspaket ist, wird Kommunikation zwischen Land- und Schiffseite mit roten Pfeilen dargestellt. Kommunikation innerhalb von Land- oder Schiffsseite wird mit schwarzen Pfeilen abgebildet.

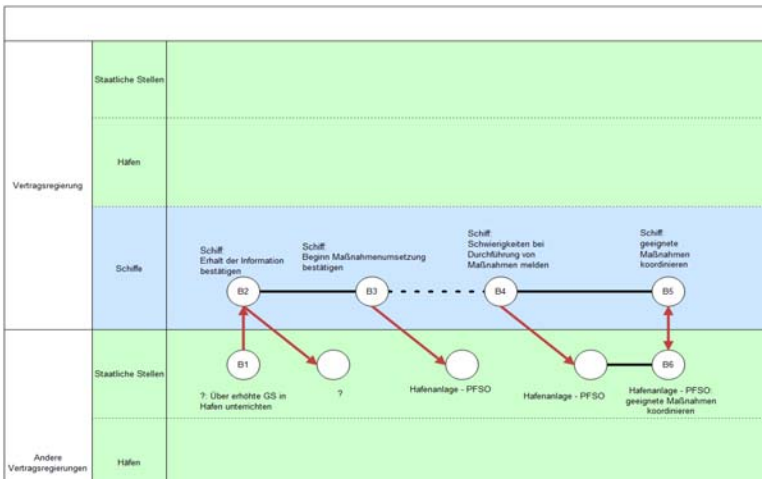

Abbildung 5: Ausschnitt aus einem COMON Modell

Zunächst wurden drei große COMON-Modelle erstellt, jeweils eines für die Regeln aus dem ISPS-Code sowie für die Teile A (verpflichtend) und B (empfohlen). Um diese Modelle zu strukturieren wurden acht Aufgabenbereiche identifiziert, über die eine Kommunikationskategorisierung ermöglicht wurde. Die Aufgabenbereiche wurden so gewählt, dass sich in einer bestimmten Situation möglichst schnell und valide identifizieren lässt, welche Kommunikationswege vorgegeben sind. Auch lassen sich Kommunikationsvorgaben für eine bestimmte Rolle/Person schnell finden. Abbildung 6 zeigt die acht Aufgabenbereiche und ihre mögliche aber nicht notwendige zeitliche Abfolge.

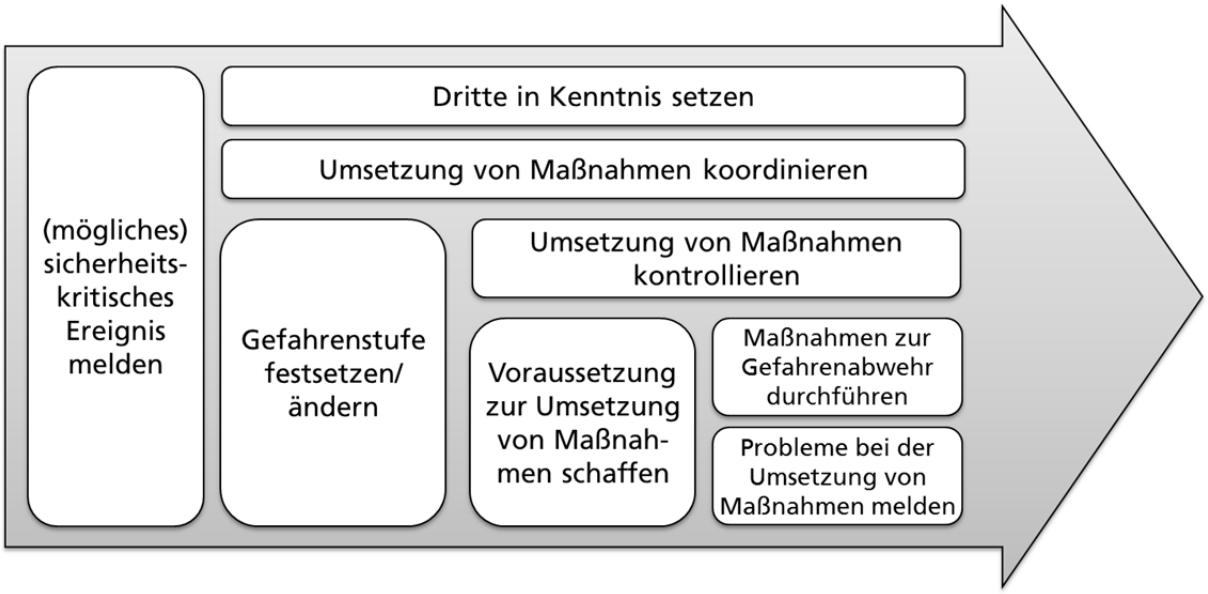

Abbildung 6: Die acht Aufgabenbereiche zur Strukturierung der Kommunikationsvorgaben

Im nächsten Schritt wurden alle Kommunikationsvorgaben den Aufgabenbereichen zugeordnet, sodass acht COMON-Modelle entstanden. Dabei gab es teilweise Unstimmigkeiten seitens der Vorgaben des ISPS-Codes, welche die Zuordnung der Kommunikationsvorgaben zu den Modellen erschwerten. Diese Unstimmigkeiten waren unter anderem:

- teilweise keine eindeutigen Akteur-Bezeichnungen,
- teilweise keine konkrete Benennung von Akteuren (aktiv und passiv),
- schwer zu verfolgende Ausnahmen (z.B. Teil A, Punkt 2 „Begriffsbestimmungen", 2.3: Der Ausdruck ‚Vertragsregierung' schließt in Verbindung mit einer Bezugnahme auf eine Hafenanlage und bei Verwendung in den Abschnitten 14, 15, 16, 17 und 18 eine Bezugnahme auf die ‚zuständige Behörde' ein.)

Die acht COMON-Modelle wurden zusätzlich strukturiert, sodass eine Kommunikationsvorgabe zu einem gegebenen Ereignis schnell identifiziert werden kann. Zusätzlich enthält jede Vorgabe einen Verweis auf die entsprechende Stelle im ISPS-Code.

3. Erfassung des Soll-Zustandes

Für einen Abgleich von Ist- und Soll-Zustand wurden die Vorgaben aus den COMON-Modellen mit den Kommunikationstabellen verglichen. Für jede Kommunikation wurde geprüft, ob es eine entsprechende Vorgabe gibt und ob diese erfüllt wurde. Das Ergebnis des Vergleichs wurde direkt in die Kommunikationstabellen übertragen. Die Bewertung des Vergleichs ist über die Farbe kodiert:

- grün (gefordert und vorhanden),
- gelb (nicht gefordert) oder
- rot (gefordert aber nicht vorhanden oder andere Gründe, die einer Diskussion bedürfen).

Ein Beispiel dafür ist bereits in der Abbildung 3. zu sehen.

Zuletzt wurden die Kommunikationstabellen mit Experten diskutiert. Dies waren die Designated Authority (DA) und der Port Facility Security Officer (PFSO) Mecklenburg-Vorpommern, DA und PFSO Schleswig-Holstein, der Kapitän der an der Übung beteiligten Fähre, Vertreter des BSH sowie die beiden CSOs der Reedereien „TT-Line" und „Scandlines".

Ergebnisse

Die Ergebnisse der Expertengespräche wurden direkt in die Kommunikationstabellen übertragen und den Endnutzern zur Verfügung gestellt. Diese können dazu beitragen, dass ein einheitlicheres Kommunikationsverständnis zwischen den unterschiedlichen Gruppen vorliegt und dass die Vorgaben des ISPS-Codes besser umgesetzt werden können.

Außerdem wurden den Endnutzern die COMON-Modelle zur Verfügung gestellt. Diese können genutzt werden, um die Kommunikationsvorgaben des ISPS-Codes situations- und rollenabhängig schnell und valide zu finden. Durch die bereits erwähnten Probleme in der Struktur des ISPS-Codes war es bisher schwierig, alle Kommunikationsvorgaben für eine bestimmte Situation oder eine bestimmte Person auf einen Blick zu haben. Die Modelle geben diesen Überblick über alle Kommunikations-Vorgaben. Die detaillierte Analyse des ISPS-Codes und Diskussionen mit den Endnutzern haben gezeigt, dass der ISPS-Code nicht nur hinsichtlich der Kommunikationsvorgaben überarbeitet und optimiert werden sollte. Dies ist jedoch nicht Teil dieses Projektes.

Die Ergebnisse dieses Arbeitspaketes in das Arbeitspaket 1.2.2 (Situationsverständnis) eingeflossen.

Nun werden die auf AP 1.2.1 aufbauenden Arbeiten des AP 1.2.2 „Unterstützung eines gemeinsamen Situationsverständnisses an der Schnittstelle Schiff-Hafen“ beschrieben:

Aufgabenstellung

Für eine optimale Prävention und Reaktion auf sicherheitskritische Ereignisse ist es notwendig, dass alle Beteiligten ein einheitliches Situationsverständnis besitzen. Insbesondere die bisher praktizierte getrennte Betrachtung von Schiff und Hafen hat sich hierbei als Schwachstelle herausgestellt, weshalb aufbauend auf die Kommunikationsanalyse (AP 1.2.1) ein Lösungsansatz für ein verbessertes Situationsverständnis bei sicherheitskritischen Ereignissen vor allem an der Schnittstelle Schiff/Hafen entwickelt werden sollte.

Vorgehensweise

Nach Diskussionen mit Endnutzern (DAs Hafen, DA Schiff, PFSOs und SSOs) wurde die Entwicklung von Kommunikations-Rollenkarten beschlossen, um das Situationsverständnis an der Schnittstelle Schiff/Hafen im Falle sicherheitskritischer Ereignisse zu unterstützen.

Die in Abbildung 6 dargestellten acht Aufgabenbereiche zur Strukturierung der Kommunikationsvorgaben aus AP 1.2.1 wurden als Grundlage verwendet, um Kommunikationsvorgaben in Kommunikations-Rollenkarten für zentrale Kontaktstellen, die an der Schnittstelle Schiff/Hafen tätig sind, zu überführen. Die Auswahl der Kontaktstellen fand auf Grundlage der ISPS-Code-Analyse in Übereinstimmung mit den Endnutzern statt. Insgesamt ergab die Analyse die in Abbildung 7 dargestellten, mit Endnutzern konsolidierten Kontaktstellen. Farblich hervorgehoben sind zentrale Kontaktstellen an der Schnittstelle Schiff/Hafen, für die jeweils eine Kommunikations-Rollenkarte entwickelt wurde. Dies sind:

- Behörden Hafen,
- Behörde Schiff,
- Hafenanlage/PFSO,
- Unternehmen/CSO und
- SSO.

Abbildung 7: Im ISPS-Code genannte und mit Endnutzern konsolidierte Kontaktstellen; farblich markiert sind Kontaktstellen, für die Kommunikations-Rollenkarten entwickelt wurden

Im Gespräch mit Endnutzern ergaben sich zudem folgende Informationsanforderungen an die Kommunikationsrollenkarten:

- Nennung der Aufgabenbereiche,
- Auflistung relevanter Kontaktdaten,
- Darstellung eines Kommunikationsdiagramms,
- Inhalte zur Kommunikation (aktiv) und
- allgemein vorgegebene Verhaltensweisen.

Nach Überführung der Informations-Anforderungen in ein erstes Konzept, wurde dieses mit den beteiligten Endnutzern besprochen und überarbeitet. Das Ergebnis wird exemplarisch im nächsten Abschnitt beschrieben.

Ergebnisse

In Abbildung 8 ist exemplarisch eine Rollenkarte (hier für den Company Security Officer, CSO) dargestellt, welche alle Informationsanforderungen berücksichtigt. Neben der Nennung des Kommunikations-Rollenkarteninhabers ist zunächst ein Kommunikationsdiagramm abgebildet, welches sämtliche Kontaktstellen visualisiert (blau = schiffsseitig, grün = hafenseitig), mit denen der Kommunikations-Rollenkarteninhaber situationsabhängig in Kontakt treten muss (Coastal State, DA Schiff, SSO usw.). Darunter ist ein Inhaltsverzeichnis aufgeführt, welches vor allem bei zahlreichen Kommunikationsvorgaben einen Überblick verschafft und die entsprechenden relevanten sicherheitskritischen Situationen nennt. Am unteren Ende der ersten Seite (links) ist die Möglichkeit zur Eintragung von Kontaktdaten gegeben, die teilweise vorgegeben sind. Auf der nächsten Seite (rechts) werden die Kommunikationsvorgaben für die einzelnen Aufgabenbereiche aufgeführt. Dabei sind die betroffenen Kontaktstellen (farblich) visualisiert und in Abhängigkeit der Kommunikationsvorgaben mit Pfeilen verbunden. Auf diese Weise können vom Kommunikations-Rollenkarteninhaber Abläufe leicht erkannt und befolgt werden. Eine Kommunikationsanweisung ist links neben den Abläufen vorhanden. Da der Kommunikationspartner entsprechende Kommunikations-Rollenkarten vorliegen hat, ist ein verbessertes Situationsverständnis möglich. Zu jedem Kommunikationsstrang wird der entsprechende Aufgabenbereich auf der rechten Seite erwähnt. Zudem ist ein Verweis auf die entsprechende Stelle im ISPS-Code links neben den Kommunikationsvorgaben vorhanden.

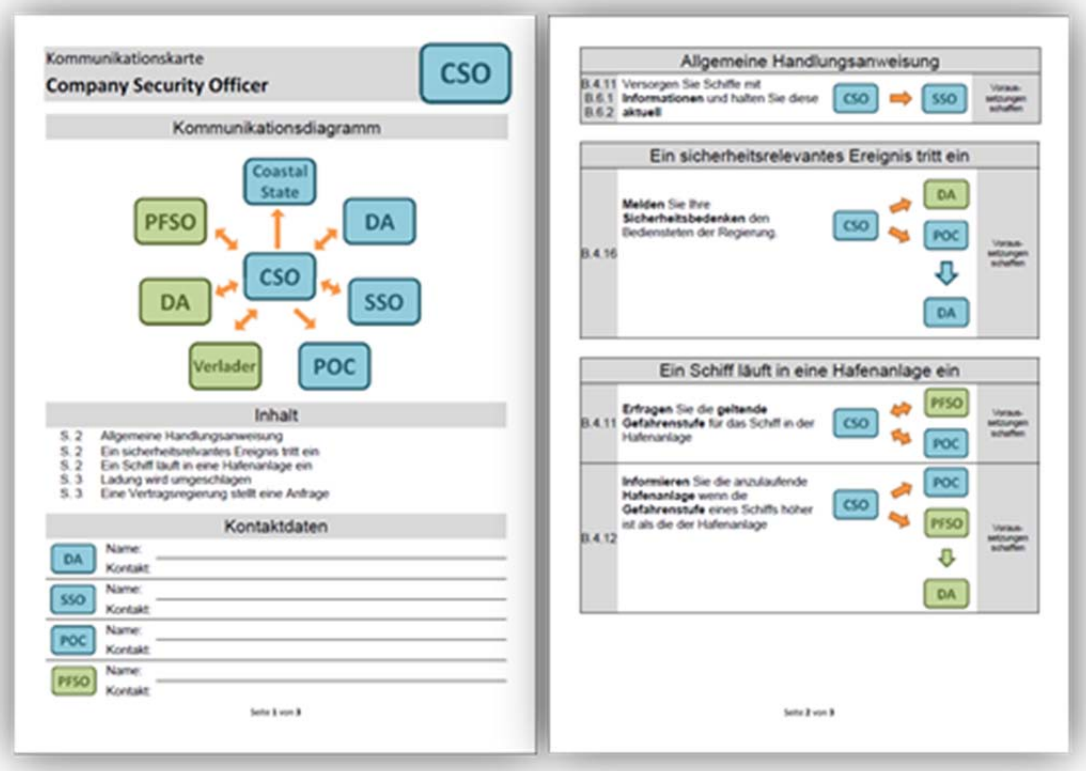

Abbildung 8: Beispiel einer Kommunikations-Rollenkarte für den Company Security Officer (CSO)

Im Zuge der Arbeiten und Diskussionen zur Verbesserung des Situationsverständnisses wurden inhaltliche Optimierungspotentiale bezüglich des ISPS-Codes gemacht. Hierbei zu nennen ist vor allem, dass der ISPS-Code nicht auf die Besonderheiten der Fährschifffahrt als Brückenersatzverkehr eingeht und keine Neudefinition von Kommunikationswegen erlaubt (vorgegebene Kommunikationspunkte müssen nach eigenen Möglichkeiten eingehalten werden). Ein Vorschlag zur vereinfachten Neudefinition von Standard-Kommunikationswegen ist in Abbildung 9 zu sehen.

Die sich aus den Optimierungspotentialen resultierenden Wünsche an eine zukünftige Revision des ISPS-Codes sind, dass dieser

- auf die Besonderheiten von Linienverkehr eingehen sollte,
- die Möglichkeit bieten sollte, zwischen den verschiedenen Größen von Hafenanlagen bzgl. der Maßnahmen zu unterscheiden und
- nutzerfreundlicher und somit handhabbar gestaltet werden sollte.

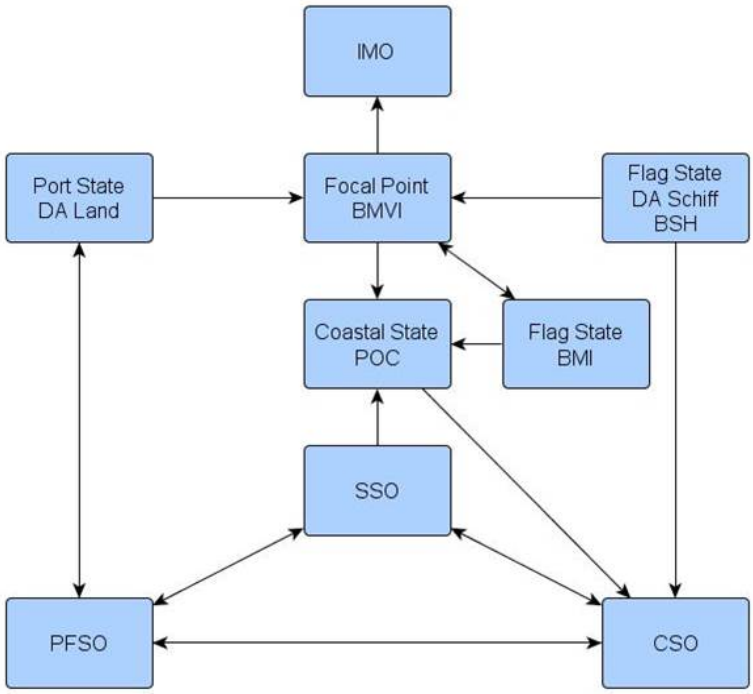

Abbildung 9: Vorschlag zur Optimierung der Standard-Kommunikationswege

B.1.3 AP 1.3: Untersuchungen zur Optimierung zur Risikobewertung von Hafenanlagen

Zur Ist-Erfassung der Methodik zur Risikobewertung fand eine Literaturrecherche im Bereich der Risikoanalyse im Allgemeinen statt, vertieft im Bereich terroristischer Risiken und ganz speziell für den Anwendungsfall der durch den ISPS-Code vorgeschriebenen Risikobewertung. Eine Auflistung der Literatur findet sich im Literaturverzeichnis. Verschiedene Methoden zur Risikoanalyse wurden erfasst und analysiert, wobei der Fokus auf der Bewertung terroristischer Risiken allgemein (Bundesministerium des Innern, 2011) und insbesondere in Bezug auf maritime Ziele lag. Darüber hinaus wurden die rechtlich bindenden Anforderungen des ISPS-Codes berücksichtigt. Literatur, die konkrete Ansätze zur Hafensicherheit diskutiert, konnte weitgehend nur in Bezug auf die US-amerikanische Methode MSRAM (Downs, 2010) gefunden werden. Aufgrund des schwierigen Umgangs mit verschiedenen Unsicherheitsfaktoren, die der vielfältigen Bedrohungslage zugrunde liegen, werden die Schwierigkeiten, ein risikobasiertes Konzept zur Entscheidungsunterstützung zu entwickeln, als „entmutigend“ bezeichnet (National Research Council, 2010).

Darüber hinaus wurden die von den deutschen Hafensicherheitsbehörden verwendeten Methoden analysiert und abschließend unter Anwendung einer hierarchischen Aufgabenanalyse domänenbezogene Informations- und Nutzeranforderungen ermittelt. Dies fand im Rahmen verschiedener Workshops, Interviews und Ortsbegehungen mittels der Methode „Cognitive Walk-Through“ statt. Es hat sich unter anderen gezeigt, das terroristische Risiken aus Mangel an Daten nicht mathematisch berechenbar sind, sondern von Experten geschätzt werden müssen. Diese Schätzer unterliegen subjektiven Einschätzungen und Beurteilungen (Linkmann et al., 2013) und eignen sich nicht als Eingangsdaten für statistische Verfahren. Die an die Bewertung technischer Systeme angelehnte Funktion zur Berechnung des Risikos enthält ungewollte Abhängigkeiten in ihren Parametern, da terroristische Aktivitäten stets intendiert sind und sich damit Eintrittswahrscheinlichkeit und Auswirkungen bzw. Schwere der Folgen nicht getrennt voneinander betrachten lassen. Auch dynamische Phänomene wie die Verschiebung von Risiken bleiben meist unberücksichtigt.

Die Bewertung von Gefahren, die aus terroristischen Aktivitäten erwachsen, unterscheidet sich von anderen Gefahrenanalysen (im Bereich Technik, Umwelt, etc.) im Wesentlichen durch zwei

Aspekte: Zum einen handelt es sich um intendierte Taten, zum anderen – insbesondere in Bezug auf maritime Ziele – um extrem seltene Ereignisse, so dass keine statistisch verwertbaren Daten vorliegen, die mathematischen Ansprüchen genügen.

Ebenso wurden die sich aus den gesetzlichen Vorgaben des ISPS-Codes (Verordnung (EG) Nr. 725/2004, 2004) ableitenden Anforderungen an eine Risikobewertung erfasst.

In mehreren Workshops wurde sowohl mit den am Projekt beteiligten Designated Authorities als auch in zwei Fällen mit den Designated Authorities aller Bundesländer der jeweilige Arbeitsstand besprochen. Dabei wurden Herausforderungen und Anforderungen diskutiert, Lösungsideen entwickelt und Richtungsentscheidungen getroffen. Die neue Methode wurde so iterativ in enger Zusammenarbeit mit den Endnutzern entwickelt.

Hinsichtlich der Informationsvisualisierung (AP 1.3.3) waren die Möglichkeiten eingeschränkt, da – wenn eine praxistaugliche Lösung angestrebt wird – auf die Verwendung von Software zurückgegriffen werden muss, die den Behörden standardmäßig zur Verfügung steht. Anforderungen wurden im Rahmen der Analyse der Informationsanforderungen erarbeitet. Eine SMT-Integration hat sich unter anderem als nicht sinnvoll herausgestellt.

Zur Durchführung der Fallstudie (AP 1.3.4) wurden Sachbearbeiter der Designated Authorities der Länder Mecklenburg-Vorpommern und Schleswig-Holstein gebeten, für eine Anlage eine Risikobewertung jeweils nach der alten und nach der neuen Methode durchzuführen. Im Anschluss wurden sie gebeten, einen Fragebogen auszufüllen, welcher entsprechend der Anforderungen erstellt wurde. Die Ergebnisse der Fallstudie sind in die Implementierung der neuen Methode eingeflossen.

Es wurde eine neue Methode zur Risikobewertung von Hafenanlagen (PFSA – Port Facility Security Assessment) entwickelt, die quantitative und qualitative Ansätze verbindet und den Anforderungen des ISPS-Codes genügt. Ziel ist nicht eine automatisierte Bewertung des terroristischen Risikos oder eine algorithmisch basierte Erstellung einer Sicherheitsarchitektur, sondern prozessgeführt zur Wissensbildung des Experten in Bezug auf die konkrete Hafenanlage beizutragen und somit ein fundiertes Expertenurteil zu ermitteln und zu dokumentieren. Ein wesentliches Ergebnis der Arbeiten ist, dass der Wert der Risikoanalyse in der Wissensgewinnung (Systemverständnis) bei ihrer Durchführung liegt und nicht in den numerischen Ergebnissen, vgl. Abbildung 10. Dieses Resultat wurde bereits veröffentlicht (Linkmann & Holder, 2012).

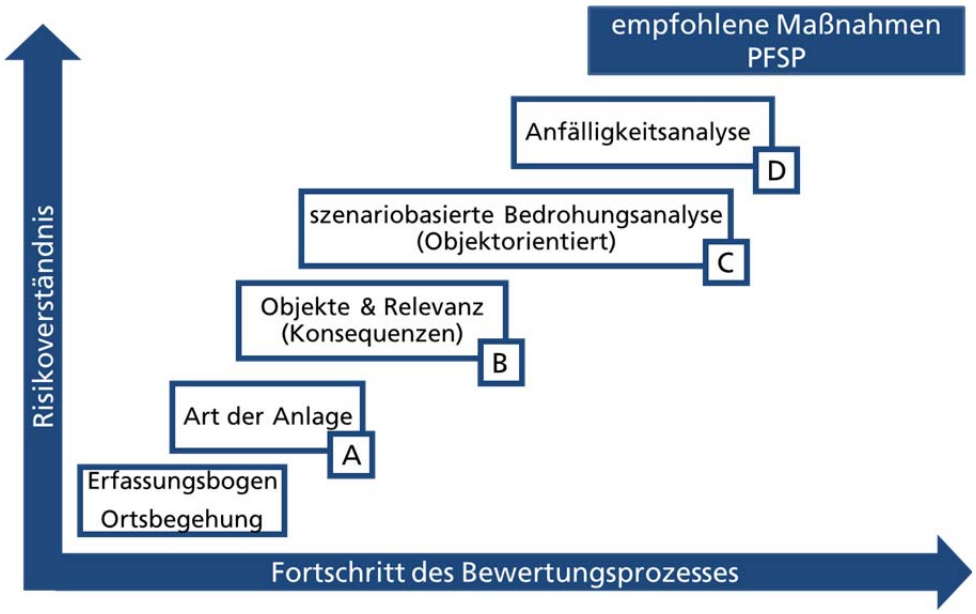

Abbildung 10: Verfeinerung des mentalen Modells mit Fortschreiten der Bewertung.

Der Analyst wird anhand von Fragen durch den Bewertungsprozess geführt. Es handelt sich dabei sowohl um Fragen, die mit „Ja" oder „Nein" beantwortet werden müssen, als auch um qualitative Fragen zu Vorhandensein und Eignung verschiedener Sicherheitsmaßnahmen. Begründungen und Erläuterungen zu diesen Antworten können bei Bedarf ebenfalls gegeben werden. Der Bewertungsprozess besteht den Vorgaben entsprechend aus den drei Komponenten Bedrohung, Auswirkungen und Schwachstellen. Darüber hinaus wird das geforderte Ranking der Objekte der Hafenanlage, beispielsweise des Gefahrgutplatzes, in Form einer dreistufigen Klassifizierung (geringes, mittleres und hohes Risiko) adressiert.

Das Vorgehen besteht grundsätzlich aus sechs Schritten:

- Ausfüllen eines Erfassungsbogen und Durchführung einer Ortsbegehung,
- Einschätzung der Art der Anlage (Ableitung einer Gewichtung),
- Auflistung der Objekte und Beurteilung der jeweiligen Bedeutung (Auswirkungen) in Bezug auf die vier Aspekte Mensch, Umwelt, Wirtschaft und Symbolik,
- Abgleich der Objekte mit vorgegebenen Bedrohungsszenarien (Exposition),
- Schwachstellenanalyse zur Bewertung der Sicherheitsarchitektur und
- Erstellen des Berichts mit Empfehlungen für den Hafenbetreiber.

Darüber hinaus wird anhand der quantifizierten Parameter „Auswirkungen" und „Exposition" jedes Objekt in einem Risikocluster (geringes, mittleres und hohes Risiko) klassifiziert.

Konkret trifft der Analyst im Bewertungsprozess zunächst Aussagen zur Art der jeweiligen Hafenanlage und den darin befindlichen Objekten in Form von Ja-/Nein-Antworten. Diesen Antworten unterliegt eine Matrix, anhand derer die Bedeutsamkeit der Aspekte Mensch, Wirtschaft, Umwelt und Symbolik, die klassischerweise zur Bewertung terroristischer Akte verwendet werden, gewichtet wird. Auf die sonst übliche Beantwortung mittels drei- oder mehrstufiger Skalen wurde aus den im Folgenden aufgeführten Gründen verzichtet: Auch wenn Risiko genau genommen ein Grenzrisiko bezeichnet, so ist die Toleranz im Falle terroristischer Risiken aus politischen Gründen sehr gering; beispielsweise wird das Schadensausmaß unter anderem nach der Höhe der Opferzahlen beurteilt. Vor dem Hintergrund einer „Null-Toleranz-Haltung" in Bezug auf Terrorismus ist eine Unterscheidung zwischen einem, fünf oder zehn Opfern bei der Beurteilung potentieller Auswirkungen damit nicht sinnvoll. Darüber hinaus werden nun reale Zustände bewertet und nicht mehr Auswirkungen potentieller Anschläge abgeschätzt. Es wird beispielsweise der tatsächliche Aufenthalt unbeteiligter Menschen an

einem Objekt bewertet oder ob sich dieses Objekt durch räumlicher Enge auszeichnet und nicht mehr, wie viele Menschen bei einem bestimmten Anschlagsszenario und einem bestimmten Grad des Gelingens zu Schaden kommen könnten. Diese Vorgehensweise wird von den Nutzern als wesentlich einfacher und plausibler empfunden und birgt darüber hinaus weniger Unsicherheitsfaktoren.

Im nächsten Schritt des Bewertungsprozesses wird jedes Objekt, über dessen Bedeutung und Eigenschaften sich der Analyst durch die vorangegangen Bewertungsschritte nun bewusst ist, gegen sieben vordefinierte Szenarien getestet und so die Exposition ermittelt. Hierbei soll der Analyst begründet einschätzen, ob bestimmte Szenarien als plausible Bedrohungen angenommen werden. Es ist zu betonen, dass hier bewusst das Dogma des „credible worst case" dem des „worst case" vorgezogen wurde, um Raum für eine differenzierte Einschätzung zu schaffen. Exposition und Objektbedeutung ergeben anschließend automatisiert die Zuordnung zum Risikocluster. Im letzten Schritt werden im Rahmen einer Schwachstellenanalyse – und wieder vor dem Hintergrund des während des Bewertungsprozesses erlangten Wissens über die Anlage und den darin befindlichen Objekten – rein qualitativ das Vorhandensein und die Eignung verschiedenster Sicherheitsmaßnahmen abgefragt. Eventuell notwendige zusätzliche Maßnahmen werden hier inklusive einer Begründung direkt dokumentiert. Unter anderem trägt dies der zentralen Anforderung nach Transparenz Rechnung. Das Thema Cybersicherheit fließt nun erstmalig in die Risikobewertung von Hafenanlagen ein. Die ermittelten administrativen Anforderungen, werden durch die neue Methode ebenfalls erfüllt.

Eine im Anhang verfügbare Tabelle enthält Anforderungen und Kritiken sowie ihre Umsetzung. Ebenfalls enthalten sind Auszüge der MS-Excel-Anwendung sowie die erstellte Verfahrensanweisung, die als Teil der Methode zu verstehen ist, da Erläuterungen und Hilfestellungen zu den einzelnen Einschätzungen sich als ein elementarer Teil der Vorgehensweise herausgestellt haben.

Die Informationsvisualisierung (AP 1.3.3) wurde ebenfalls im Rahmen der Anforderungsanalyse adressiert. Im Rahmen der Workshops mit den Endnutzern wurde eine Umsetzung der Methode in MS-Excel favorisiert. Die zentralen Anforderungen wie Transparenz und eine prozessgeführte, stringente Vorgehensweise wurden durch die Verwendung der folgenden Elemente umgesetzt:

- Ein Hauptarbeitsblatt, auf das die wesentlichen Ergebnisse automatisch übertragen werden,
- eine automatische Übertragung relevanter Bewertungen auf nachfolgende Arbeitsblätter,
- übersichtliches Arbeiten mit Excel-Arbeitsblättern, Listen und Tabellen,
- farblich unterlegtes, dreistufiges Risikocluster für alle Objekte „auf einen Blick",
- Drop-Down-Auswahlmenüs bei der Beantwortung von Ja/ Nein-Fragen,
- für den Nutzer einsehbare Formeln und hinterlegte Gewichtungen und
- in das Hauptarbeitsblatt integrierte administrative Elemente.

Mit der Erstellung einer neuen Methode zur Risikobewertung wurden die vorgegebenen Ziele erreicht. Die neue Methode wird bereits seit 2014 von den deutschen Hafensicherheitsbehörden verwendet.

B.1.4 AP 2.1: Überwachung Zugang Schiff und Hafen – Gefahrstoffkontrolle

Zunächst werden die Arbeiten zu AP 2.1.1 (Machbarkeitsstudie zur Erstellung eines Fahrzeugprofils) beschrieben:

Vorgehensweise

Für terroristische Anschläge werden Sprengstoffe oder andere gefährliche Stoffe wie beispielsweise leicht brennbare Flüssigkeiten bzw. giftige Stoffe eingesetzt. Diese können mit

Hilfe von Fahrzeugen an kritische Orte wie z.B. Häfen/Fähren transportiert werden. Jedoch stellen nicht nur von Attentätern mitgeführte Sprengstoffe oder gefährliche Stoffe ernste Gefahren dar, sondern ebenfalls der Missbrauch von bereits auf dem Betriebsgelände bzw. der Fähre vorhandenen gefährlichen Stoffen. Werden diese gezielt zur Explosion gebracht, in Brand bzw. freigesetzt, verursachen sie erhebliche Schäden (Verletzungen, Tod, Umwelt- und Materialschäden).

Nicht nur direkte Hinweise wie das nicht erlaubte Transportieren von gefährlichen Stoffen wie z.B. Sprengstoffen in Fahrzeugen, sondern ebenfalls das Verhalten von Personen/Fahrzeugen kann Hinweise auf geplante terroristische Angriffe geben.

Ermittlung von Verdachtsmerkmalen

Verdächtiges Verhalten bzw. verdächtige Objekte können frühzeitig Hinweise auf einen terroristischen Anschlag geben. Je früher Verdachtsmerkmale erkannt werden, umso schneller und effektiver können geeignete Maßnahmen zur Verhinderung eines Anschlages eingeleitet werden. Hierbei muss jedoch berücksichtigt werden, dass nicht jedes Verdachtsmerkmal zu einem direkten Eingreifen des Hafenbetreibers bzw. der Polizei führen muss. Erst nach Vorliegen einzelner gravierenden bzw. mehrerer „kleinerer" Verdachtsmomente kann ein Hinweis auf eine ernsthafte Gefahr erhalten werden.

Gefahren können erst bewertet werden, wenn sie bekannt sind. Im ersten Schritt werden am Fahrzeug, an den mitgeführten Gütern oder dem Verhalten von Personen Verdachtsmerkmale ermittelt, welche die Grundlage für eine Bedrohungsbeurteilung darstellen.

Sichtung auf dem Markt erhältlicher geeigneter Sensoren

Die Überwachung bzw. Kontrolle des gesamten Hafengeländes und der Fähren durch Sicherheitspersonal ist nur teilweise und mit erheblichem Aufwand und Kosten möglich. Nur durch den Einsatz geeigneter Sensoren könnten verdächtige Stoffe wie z.B. Sprengstoffe, radioaktives Material sowie verdächtige Verhaltensweisen erfasst werden. Aus diesem Grund wurden auf dem Markt zur Verfügung stehende Sensoren ermittelt, die in der Lage sind, gefährliche Stoffe zu detektieren bzw. verdächtige Verhaltensweisen zu erfassen.

Exemplarische Untersuchungen von im FKIE vorhandenen Sensoren

Neben der Recherche der auf dem Markt verfügbaren Sensoren wurden ebenfalls die im Fraunhofer-FKIE vorhandenen Sensoren

1. RFID,
2. Fahrzeugwaage und
3. Gammadetektoren – Detektion radioaktiver Stoffe (Gammastrahler)

auf ihre Eignung zur Identifizierung und Verfolgung von Fahrzeugen bzw. Erkennung von Bedrohungen untersucht.

Zu 1: RFID:

Ein wesentlicher Aspekt für die Hafensicherheit stellt die Identifizierung und Verfolgung von Fahrzeugen auf dem Hafengelände dar. Hierzu werden in das Gelände einfahrende Fahrzeuge mit RFID-Sensoren ausgerüstet.

Bereits im FKIE vorhandene RFID-Sensoren wurden auf ihre Eignung zur Identifizierung und Verfolgung von Fahrzeugen überprüft. Hierbei standen zwei Aspekte im Vordergrund:

- Kontrolle der Zufahrt auf das Hafengelände und Auffahrt auf Fähre

- Überwachung der Fahrzeuge auf dem Hafengelände; Abweichen von erlaubter Fahrroute wird durch RFID-Sensoren erkannt und an die Sicherheitszentrale automatisch gemeldet

Zu 2: Fahrzeugwaage:

Werden größere Mengen (z.B. 200 Kg) Sprengstoff in PKWs transportiert, sollte durch die Bestimmung des Gesamtgewichtes des Fahrzeugs und Vergleich mit dem Leergewicht des PKWs ein Hinweis auf das möglicherweise Mitführen von Sprengstoffen erhalten werden. Dies sollte mit Hilfe einer Fahrzeugwaage untersucht werden.

Zu 3: Gammadetektoren:

Radioaktive Stoffe, die u.a. auch zur Herstellung von „schmutzigen" Bomben verwendet werden, können mit Hilfe geeigneter Detektoren nachgewiesen und identifiziert werden. Radioaktive Stoffe senden abhängig vom Nuklid unterschiedliche Strahlung aus:

1. Alpha-Strahlung,
2. Beta-Strahlung und
3. Gamma-Strahlung.

Sowohl Alpha- als auch Beta-Strahlung werden schon durch relative geringe Mengen Materialien vollständig absorbiert und sind nicht bzw. nur mit erheblichem Aufwand aus einer bestimmten Distanz (> 50 cm) nachweisbar und werden deshalb im Rahmen dieses Projektes nicht näher untersucht.

Gamma-Strahlung wird abhängig vom Material nur in einem gewissen Maße absorbiert. Selbst durch Blei dringt ein Teil der Gamma-Strahlung durch. Durch Materialien wie Luft oder Papier wird die Gammastrahlung quasi nicht absorbiert.

Die Strahlungsintensität der Gamma-Strahlung nimmt mit $1/r^2$ (r= Abstand der radioaktive Quelle zum Messpunkt) ab. Im Rahmen dieses Projektes wurde untersucht, in welchem Abstand die im Fraunhofer FKIE vorhandenen radioaktiven Quellen (^{60}Co und ^{137}Cs) mit dem vorhanden Detektor (ICX: STRIDE DU 202) nachgewiesen werden können.

Im medizinischen Bereich werden zu Untersuchungszwecken ebenfalls radioaktive Stoffe wie ^{99}Tc eingesetzt. Diese Stoffe besitzen eine relativ kurze Halbwertzeit, so dass sie nach kurzer Zeit (mehrere Tage) nicht mehr nachgewiesen werden können. Personen, die mit diesen Stoffen behandelt wurden, können innerhalb der ersten Tage nach ihrer Behandlung einen Fehlalarm herbeiführen.

Wird ein radioaktiver Stoff nachgewiesen, bedeutet dies nicht zwangsläufig, dass es sich um verdächtiges Material handelt. Die Identifizierung der vorhandenen Nuklide erfolgt in einem zweiten Schritt mit Hilfe eines weiteren Gammadetektors „Identifinder 2" der Fa. Flir. Nur auf diesem Wege können Falschalarme beseitigt werden.

<u>Konzept: Erstellung eines mehrstufigen Datenfusionsmodells</u>

Die Ergebnisse der Recherchen bzw. Untersuchungen zu

- Verdachtsmerkmalen,
- auf dem Markt verfügbaren Sensoren zur Erkennung von Verdachtsmerkmalen,
- RFID,
- Fahrzeugwaagen und

- Gammadetektoren

wurden zur Erstellung eines Konzeptes eines mehrstufigen Datenfusionsmodells verwendet. Über den verfolgten methodischen Ansatz müssen solche Teilaspekte einer möglichen Bedrohung dann zeitlich und räumlich zu einem Gefahrenprofil fusioniert werden, um Verantwortlichen eine verbesserte Entscheidungsgrundlage zur Verfügung zu stellen.

Ergebnisse

In der Literatur sind zahlreiche Hinweise auf Verdachtsmerkmale beschrieben:

Übersicht möglicher Verdachtsmerkmale*

- Person klettert über Zaun bzw. Absperrung und verschafft sich Zugang zu Fahrzeugen auf Betriebsgelände, welche mit kritischen Gefahrstoffen beladen sind.
- Verstöße gegen Zugangsvorschriften
- Herumlungern einer/mehrerer Personen rund um Fahrzeuge
- Einbruch, Diebstahl, Hausfriedensbruch
- Ungewöhnliches bzw. auffälliges Fahrverhalten, z.B. Geschwindigkeit (zu schnell / ungewöhnlich langsames Fahren), Fahren ohne Licht
- Verdächtige Arbeiten in unmittelbarer Nähe zu Schiffen, an Fahrzeugen,…
- Unnötige Fahrten von Fahrzeugen im Hafenbereich
- Aufenthalt von Personen in Bereichen zu ungewohnter Stunde
- Aufenthalt von Personen in nicht erlaubten Bereichen (z.B. Lagerbereiche von Containern/Gefahrgütern,…)
- Parken an nicht erlaubtem Ort
- Personen benutzen Fernglas
- Personen machen Fotos/Videoaufnahmen von Überwachungsgeräten,…
- Lagekarten werden mit Informationen/Notizen versehen
- Personen verständigen sich mit verdächtigen Zeichen
- Unbekannte Personen versuchen, Informationen über Einrichtungen, Personal und Beschäftigungsmöglichkeiten zu erhalten
- Ungewöhnliche Fragen rund um Business-Operationen (z.B. wann sind die verkehrsreichsten Stunden,…)
- Unbeaufsichtigte Fahrzeuge an ungewöhnlichen Orten
- Unbeaufsichtigte Gegenstände/Objekte (z.B. Taschen, Rucksack,….)
- Fahrzeuge mit einem oder mehreren Personen parken zu einer ungewöhnlichen Zeit auf Betriebsgelände
- Flüssigkeit/Gas/Geruch tritt aus z.B. Fahrzeugen, Containern bzw. abgestellten Gegenständen aus
- Manipulierte Feuerlöscher
- Ungewöhnliche Geräusche wie z.B. Schüsse, Geschrei, Glasbruch,…
- Auffällige Benutzung von Gasflaschen

- Größere Mengen Blei vorhanden (Hinweis auf Transport von radioaktivem Material)
- Tragen von nicht witterungsbedingter Kleidung
- Unbekannte bzw. verdächtige Personen versuchen Arbeiten (z.B. Reparaturarbeiten) durchzuführen
- Wiederholte und verdächtige Telefonanrufe
- Verdächtige/verstellte Stimme
- Fahrzeug wird an Bord gefahren, Person verlässt entgegen den gemachten Angaben die Fähre/den Hafen
- Personen gehen weg, wenn Sie sich beobachtet fühlen bzw. Personen vermeiden Blickkontakt
- Anlieferung von Paketen durch private Paketzustelldienste
- Baulich verändertes Fahrzeug, z.B. hintere Stoßdämpfer wurden fixiert
- Fahrzeug überladen
- Auffällige Gewichtsverteilung im Fahrzeug
- Offene oder zerbrochenen Fenster und Türen an einem Fahrzeug
- Angaben zu Fahrzeugen/Gefahrgütern/Personen weichen von Realität ab
- Pakete/Gegenstände werden an wartendes Auto übergeben
- Auffällige Pakete im Fahrzeug (z.B. auffällige Verpackung/ungewöhnliche Beschriftung von Paketen, Ölflecken, Kabel sichtbar)
- Ungewöhnlich hohes Gewicht einer Postsendung
- Verdächtige Aufkleber auf Fahrzeug (Sprache der Aufkleber und Autokennzeichen weichen ab)

*Quellen:

- Suspicious Sea Port Behaviour
  http://www.psni.police.uk/index/advice-and-legislation/advice_small_ports/advice_suspicious_sea_port_behaviour.htm
  Reporting Suspicious Activity within the Port
  Port Community Information Bulletin # 06-02
  http://www.safetampabay.org/HSAlerts/pcib0602.pdf
- Maritime Domain Awareness
  Marine Safety Office St.Louis
  www.cgaux.net/marsec/mda.ppt
- Pre-Incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct
  Terrorism Research Center in Fulbright College
  https://www.ncjrs.gov/pdffiles1/nij/grants/214217.pdf
- Potential Indicators of Terrorist Activity Infrastructure Category: Chemical Storage Facilities
  http://info.publicintelligence.net/DHS-ChemStore-PI.pdf
- Indicators of Terrorist Attacks

http://www.bharat-rakshak.com/SRR/Volume11/anoop.html

- Eight Signs of Terrorism
  http://www.njhomelandsecurity.gov/press-room/publications/ohsp-pubs/8-terrorism-signs.pdf

Sichtung auf dem Markt erhältlicher geeigneter Sensoren (AP 2.1.1)

Nachfolgend werden die auf dem Markt verfügbaren Sensoren, die zur Überwachung von Häfen und Fährenbereich geeignet sind, dargestellt.

(1) Röntgenscanner

Auf Fahrzeugen können größere Mengen Gefahrstoffe wie z.B. Sprengstoffe, falsch deklarierte Produkte bzw. Waffen transportiert werden. Seit Jahren sind spezielle Röntgenscanner auf dem Markt, die in der Lage sind, ein „Röntgenbild" der Ladung bzw. des Fahrzeuges zu erstellen. Hierbei sind in der Regel nur Konturen sichtbar. Die in den letzten Jahren weiterentwickelten Röntgengeräte sind in der Lage, die im bzw. auf dem Fahrzeug vorhandenen Materialien bzw. Stoffe in drei unterschiedlichen Kategorien bildlich darzustellen:

a. Anorganisches Material, z.B. mineralische Stoffe, Salze,
b. Organisches Material, z.B. Gefahrgut, Sprengstoffe, leicht entzündliche Stoffe, Lebensmittel, und
c. Metalle.

Das Sicherheitspersonal kann anhand der farblichen Unterschiede im Röntgenbild erkennen, welche der oben beschriebenen Materialientypen (Kategorien) im Fahrzeug vorhanden sind. Hinweise auf mögliche gefährliche Stoffe bzw. Materialien sind beispielsweise:

- In einem mit Obst beladenen LKW, befindet sich ein Fass mit organischem Inhalt.
- Auf dem Fahrzeug befinden sich bleihaltige Verpackungen (Hinweis auf radioaktive Stoffe).
- Inhalte stimmen nicht mit deklarierten Produkten überein.

Liegen derartige Hinweise auf Röntgenbildern vor, sind weitere Kontrollen bzw. Maßnahmen zu veranlassen.

Zur Erstellung eines Röntgenbildes werden im Wesentlichen zwei unterschiedliche Röntgenverfahren eingesetzt:

- Backscatter-Verfahren:
  Bei diesem Verfahren werden Röntgenquellen niedriger Energie eingesetzt und die vom bestrahlen Objekt reflektierte Strahlung detektiert.
  Nachteil des Verfahrens: Die Strahlung dringt abhängig vom Material u.U. nicht so tief in das Fahrzeug/den Container ein, so dass unter ungünstigen Bedingungen nicht alle Objekte erkannt werden.
  Vorteil des Verfahrens: Es wird mit geringer Energie gearbeitet, so dass es in zahlreichen Ländern erlaubt ist, dass der Fahrer während des Scanprozesses im Fahrzeug sitzen bleiben darf.
  Materialien mit geringer Ordnungszahl (Dichte) (Sprengstoffe, Drogen,…) werden ebenfalls erkannt.
- Transmissions-Verfahren:
  Die gesamte Ladung wird mit Röntgenstrahlung höherer Energie durchstrahlt und die Reststrahlung wird detektiert.
  Vorteil: Es werden im Vergleich zum Backscatter-Verfahren u.U. mehr Objekte erfasst.
  Nachteil: Durch den Einsatz von Röntgenquellen mit höherer Energie darf der Fahrer

während des Scanvorgangs nicht im Fahrzeug bleiben bzw. muss vor der Strahlung geschützt werden (Siehe Abschnitt „Anbieter stationärer Röntgenscanner").

Für unterschiedliche Einsatzbereiche werden auf dem Markt

- stationäre und mobile Röntgenscanner
  - für LKWs
  - für PKWs
  sowie
- stationäre Scanner für Güterwagen

angeboten.

Die nachfolgend aufgelisteten, auf dem Markt erhältlichen Röntgenscanner sind in der Lage, zwischen unterschiedlichen Materialtypen (organisch, anorganisch, metallisch) zu unterscheiden. Die Anzahl der pro Stunde untersuchten Fahrzeuge variiert zwischen 25 bis 195. Die Durchsatzrate ist abhängig von der Art des Röntgenscanners, von dem erforderlichen Detaillierungsgrad der Röntgenaufnahme und Größe des zu scannenden Objektes.

Anbieter stationärer Röntgenscanner:

- CX-Gantry (Fa. L-3 Communications Security & Detection Systems)
- HCVS (Fa. Smiths Heimann)
  Objekte (LKW/Container) können gleichzeitig von oben und der Seite gescannt werden.
- HCVG (Fa. Smiths Heimann)
- HCVP 6030 (Fa. Smiths Heimann)
- Portal VACIS (Fa. SAIC)
- Z Portal (Fa. AS&E)
  Objekte (LKW/Container) können gleichzeitig von oben und der Seite gescannt werden.

In Deutschland dürfen nur Systeme verwendet werden, bei denen sichergestellt ist, dass der Fahrer während des Scanvorgangs keiner Röntgenstrahlung ausgesetzt ist.

Ein wesentlicher Unterschied zwischen den Anbietern von stationären Röntgenscannern besteht in der Möglichkeit, dass der Fahrer eines LKWs während des Scanvorgangs im Fahrzeug bleiben darf. Dies wird durch die nachstehenden Systeme sichergestellt:

- Das System HCVP 6030 startet den Scanvorgang erst, wenn das Ende der Fahrerkabine durch die Anlage automatisch erkannt wurde.
- Bei dem System Portal VACIS muss der Fahrer mit seinem LKW bis zu einem bestimmten Punkt fahren, die Fensterscheibe (Seite des Fahrers) herunterdrehen und den im Außenbereich befindlichen Schalter betätigen, um den Scanvorgang zu starten. Dies ist nur möglich, wenn sich die Fahrerkabine außerhalb des Scanbereiches befindet.

Neben stationären Röntgenscannern werden ebenfalls mobile Anlagen angeboten.

Anbieter mobiler Röntgenscanner

- CX-Mobile G3 (Fa. L-3 Communications Security & Detection Systems)
- HCVM L / HCVM T (Fa. Smiths Heimann)

Zur Untersuchung von Güterwagen werden spezielle Röntgenscanner angeboten. Personenzüge dürfen mit diesen Anlagen nicht gescannt werden.

Anbieter von Röntgenscanner für Güterwagen

- CX-RAIL (Fa. L-3 Communications Security & Detection Systems)
  Nur Güterwagen werden gescannt. Die maximale Scangeschwindigkeit beträgt 60km/h.
- EAGLE R90 (Fa. Rapiscan systems)
  Nur Güterwagen werden gescannt. Die maximale Scangeschwindigkeit beträgt 60km/h.
- VACIS® IR6500 (Fa. Saic)
  Mehr als 150 Güterfahrzeuge pro Stunde können gescannt werden.

Für kleinere Fahrzeuge wie z.B. PKWs wurden teilweise spezielle Röntgenscanner, z.B. CIP 300 (Fa. Smiths Heimann), entwickelt. Dieses System ist ebenfalls in der Lage, organische von anorganischen bzw. metallischen Gegenständen zu unterscheiden. In Deutschland dürfen diese Geräte jedoch nur eingesetzt werden, wenn vorher alle Insassen das Fahrzeug verlassen haben.

Häufig sind mehrere unterschiedliche Prüfungen mit verschiedenen Sensoren gleichzeitig an einem Ort sinnvoll. Die Lieferanten von Röntgenanlagen bieten in der Regel den Ausbau der Röntgenanlage durch weitere Detektoren an. Optional werden häufig angeboten:

- radioaktive Detektoren,
- Systeme zur Erkennung von Autokennzeichen,
- Videoerfassung und
- Unterbodenscanner.

(2) Radardetektoren

Als Alternative zu Röntgenscannern wurde überprüft, inwieweit Radargeräte ebenfalls zur Scannung von Fahrzeugen geeignet sind und ob entsprechende Geräte auf dem Markt angeboten werden.

Auf dem Markt werden entsprechende Anlagen nicht angeboten.

(3) Detektoren zum Nachweis radioaktiver Stoffe

Radioaktives Material wird in zahlreichen Bereichen z.B. in der Medizin zu Prüfzwecken und in Reaktoren eingesetzt. Illegal beschafftes radioaktives Material kann zum Bau von „schmutzigen Bomben“ eingesetzt werden. Zum Nachweis radioaktiver Materialien werden spezielle Detektoren eingesetzt, die in der Lage sind, Gamma- und/oder Neutronenstrahlung zu detektieren. Im nachfolgenden Text werden sie als „Gamma-Detektoren“ bezeichnet. Die Gamma-Detektoren können sowohl allein als auch in der Kombination mit anderen Detektoren eingesetzt werden. So können z.B. Röntgenscananlagen für LKWs, PKWs und Züge mit Gamma-Detektoren (z.B. „Rambo“ der Fa. SEA) zur Erkennung von radioaktiven Stoffen ausgerüstet werden. Nach der Röntgenphase wird das Fahrzeug mit Hilfe eines Gammadetektors auf radioaktive Stoffe gescannt. Der Nachweis eines radioaktiven Stoffes führt zu einem Alarmsignal. Die Identifizierung des vorhandenen Nuklids muss anschließend mit einem speziellen Gamma-Detektor erfolgen.

Da in verschiedenen Produkten wie z.B. in Nahrungsmitteln (Bananen, Erdbeeren) oder in Kacheln/Fliesen aus natürlichen oder produktionsbedingten Gründen geringe Mengen radioaktiver Stoffe z.B. Kalium (^{40}K) enthalten sind, können durch die auf einem LKW vorhandene große Masse an Produkten Fehlalarme ausgelöst werden. Wurde das Fahrzeug vor der Untersuchung mit Gammadetektoren in einer Röntgenanlage durchleuchtet, können die Ergebnisse der Gammadetektion und Röntgenanlage fusioniert und die Fehlalarmrate reduziert werden. Ein beispielsweise mit Bananen beladener LKW ergibt ein quasi einheitliches Röntgenbild. Der Gehalt an Kalium (^{40}K) und die dadurch gegebene radioaktive Strahlung der gesamten Ladung kann u.U. so hoch sein, dass bereits ein Alarm ausgelöst wird. Die in

einzelnen Bananen enthaltene Menge an Kalium (^{40}K) unterschreitet den Grenzwert. Kombiniert man das Ergebnis eines erhöhten ^{40}K-Wertes (Alarmsignal) mit dem quasi einheitlichen Röntgenbild, erkennt das System automatisch, dass es sich um große Mengen sehr schwach radioaktiver Materialien handelt und der erhöhte Wert durch die große Masse an Bananen hervorgerufen wurde. Das System gibt die Ladung frei. Wären jedoch in der Ladung Bananen kleinere Mengen stark radioaktivem Material versteckt, würde kein einheitliches Röntgenbild entstehen. Die Bereiche, in denen radioaktives Material versteckt wurde, sind auf dem Röntgenbild farblich anders dargestellt. Dies wird automatisch durch das System erkannt.

Die verdächtigen Objekte im Fahrzeug müssen zusätzlich mit Hilfe eines speziellen Gamma-Detektors, welcher in der Lage ist radioaktive Nuklide zu identifizieren, untersucht werden.

Zur automatischen Überwachung einer größeren Anzahl von Fahrzeugen an unterschiedlichen Orten stehen ebenfalls mobile Gamma-Detektoren zur Verfügung. Anbieter solcher Anlagen sind z.B.:

- Detektor: FAMO
  Anbieter: Fa. SEA
- Detektor: Detective 200
  Anbieter: Fa. ORTEC

Diese mobilen Geräte liefern den Nachweis, dass radioaktives Material vorliegt, eine Identifizierung der Komponenten ist jedoch nicht möglich.

Zur Identifizierung radioaktiver Stoffe werden spezielle Gamma-Detektoren angeboten:

- Detektor: Identifinder 2
  Anbieter: Fa. Flir
- Detektor: Gamma-Analyzer LB 125
  Anbieter: Fa. Berthold

Diese Geräte eignen sich zur Überprüfung einzelner verdächtiger Objekte.

(4) Zaundetektoren

Nicht befugte Personen könnten sich durch Überklettern des Zaunes Zutritt zum Gelände und Fahrzeugen verschaffen. Auf diesem Weg können sie mit Gefahrgut beladene Fahrzeuge für kriminelle oder terroristische Zwecke verwenden. Eine frühzeitige Erkennung eines nicht erlaubten Zutritts kann durch verschiedene Sensorsysteme sichergestellt werden. Es werden unterschiedliche Systeme angeboten:

a RFID-System:

Am Zaun und an Toren werden RFID-Systeme (Beschleunigungstags) befestigt, die in der Lage sind, Bewegungen am Zaun/Tor zu erkennen und Alarm auszulösen.

Sensor: *PerimeterLocator*
Anbieter: *Fa. Novatec Sicherheit und Logisitk GmbH*

b Lichtwellenleiter:

In einem nicht belasteten Lichtleiter (LWL) erfolgt Totalreflexion des Lichtes. Tritt eine Belastung/Verbiegung auf, wird ein Teil des Lichtes reflektiert. Die Differenz des ankommenden zum ausgestrahlten Licht wird detektiert und ausgewertet.
Das System kann zur Absicherung von

- Zäunen,
- Mauerkronen und

- Bodenbereichen (Sensor befindet sich im Boden)

eingesetzt werden.

Sensor: *LWL-Detektionssystem*
Anbieter *Fa. degesa*

c Bodendetektionssystem:

Das Bodendetektionssystem (PPS) detektiert Druckveränderungen z.B. durch Begehungen über 2 unterirdisch verlegte und mit einer speziellen temperaturstabilen Flüssigkeit unter Druck gefüllte Sensorschläuche.

Sensor: *Bodendetektionssystem PPS*
Anbieter *Fa. degesa*

d Mikrofonkabel:

Das Mikrofonkabel (Intelli-FLEX) registriert kleinste Zaunbewegungen. Das System ist geeignet zur Überwachung von metallischen Zaunkonstruktionen wie z. B. Maschendraht- oder Stabgitterzäunen.

Sensor: *Intelli-FLEX*
Anbieter *Fa. Senstar-Stellar Corporation*

e Erdverlegtes Meldekabel mit Zielortung:

Ein verdecktes, erdverlegtes Sensorkabel (OmniTrax) detektiert Eindringlinge mittels eines unsichtbaren Radarfeldes. Wird das Feld durch einen Eindringling gestört, wird ein Alarm ausgelöst und die genaue Position des unbefugten Zutritts bestimmt.

Sensor: *OmniTrax*
Anbieter: *Fa. Senstar*

Bei der Auswahl der geeigneten Sensorik müssen die örtlichen Gegebenheiten berücksichtigt werden.

(5) Videoüberwachungssysteme

Videokameras werden seit vielen Jahren zur Überwachung von Gebäuden, Flächen und Personen eingesetzt. Hierbei werden unterschiedliche Überwachungsverfahren eingesetzt. Eine Auswahl der auf dem Markt verfügbaren Videoüberwachungssysteme und deren Leistungsfähigkeit wird in Abbildung 11 beschrieben.

Hersteller	Bosch	Siemens	AXIS	Dallmaier [1)]	Mobotix AG	Aimetis
Produkt	Kombination mehrerer Systeme	Sistore CX EDS Sistore CX ODR	Kombination mehrerer Systeme	PTZ Sedor	Mobitex M12	Smyphony
Verfolgung von Objekten	ja	ja	ja	ja	Ja	ja
Herumlungern	ja	ja	ja	auf Anfrage	nein	ja
Stehengelassenes Gepäck	ja	ja	ja	auf Anfrage	nein	ja
Erfassung von Objekten	ja	ja	ja	ja	ja	ja
Einrichten von Alarmzonen	ja	ja	ja	ja	ja	ja

[1)] Dallmaier liefert neben PTZ eine sehr leistungsfähige Kamera „Panomera", mit der Objekt z.B. Personen bis 180m, Winkel 180° identifiziert werden können.
Die Software zur Verfolgung, Erkennung von Objekten wird für das Kamerasystem Panomera in Kürze auf den Markt kommen

Abbildung 11: Anbieter: Systeme zur Videoüberwachung

Allgemein verfügbare Eigenschaften:

- Erkennen und Verfolgen von Objekten mit Hilfe von Videokameras:

  Unterschiedliche Objekte wie LKW, PKW und Personen können durch Softwaretools automatisch erkannt, verfolgt und auf dem Monitor dargestellt werden. Hierbei sind die Systeme in der Lage, die Größe der unterschiedlichen Objekte bei der Auswertung automatisch zu berücksichtigen. Das Sicherheitspersonal erhält automatisch Hinweise auf mögliche Bedrohungen.

- Einrichten von Alarmzonen:

  Bereiche, die nicht für alle Personen bzw. Fahrzeuge zu jedem Zeitpunkt betreten bzw. befahren werden dürfen, können elektronisch festgelegt werden (Alarmzonen). Beim unerlaubten Betreten bzw. Befahren dieser Zonen wird durch eine bzw. mehrere Videokameras dieses Fehlverhalten automatisch erkannt und ein Alarm ausgelöst.

Spezielle Eigenschaften:

Neben den Möglichkeiten, Fahrzeuge mit Hilfe von Videogeräten zu verfolgen, sind bestimmte Videoanlagen ebenfalls in der Lage, weitere kritische Verhaltensweisen wie z.B. das Herumlungern von Personen bzw. unbeaufsichtigtes Gepäck zu erkennen (Abbildung 11):

- Erkennen von verdächtigem Verhalten (Herumlungern von Personen):

  Bevor ein terroristischer Anschlag durchgeführt wird, können verdächtige Personen sich z.B. in der Nähe des Fahrzeuges „auffällig" verhalten („Herumlungern"). Moderne Videoüberwachungssystemen sind in der Lage „herumlungernde" Personen automatisch zu erkennen (Abbildung 11).

- Erkennen von verdächtigen Objekten (Unbeaufsichtigtes Gepäck):

  Werden chemische, biologische Gefahrstoffe bzw. Sprengstoff in einem Gepäckstück wie z.B. Koffer oder Tasche unauffällig abgestellt, so muss, um einen großen Schaden/Katastrophe abzuwenden, dieses Gepäckstück möglichst schnell erkannt werden. Auf dem Markt werden Videoüberwachungssystemen angeboten, die in der Lage sind, bei einer nicht zu hohen Anzahl an Personen/Bewegungen, unbeaufsichtigtes Gepäck zu

erkennen (Abbildung 11).

(6) Audiosignale

Im Hafenbereich können durch verschiedene akustische Signale wie z.B. die Abgabe eines Schusses oder das Zerbersten einer Glasscheibe Hinweise auf kriminelle oder terroristische Aktivitäten erhalten werden. Die Recherche nach geeigneten Audiosensoren ergab, dass zwei kommerzielle Systeme angeboten werden, die in der Lage sind, Schusssignale zu erkennen und zu orten:

1. **ShotSpotter Flex:** Einsatz in Städten (im Wesentlichen in der USA) zur Erfassung von Schussgeräuschen und Ortung des Schützen.
2. **PILAR MKII-w:** Einsatz im militärischen Bereich. Das System kann zusätzlich mit einem Kamerasystem (PIVOT) ausgerüstet werden. Unmittelbar nach Erfassung des Audio-Signals z.B. Schuss kann die Kamera automatisch in die Richtung des abgegebenen Audiosignals ausgerichtet werden und der Schütze, wenn nicht durch Objekte verdeckt, visualisiert werden. Dies ist ein entscheidender Vorteil dieses Systems gegenüber Shot-Spotter Flex.

Eine Erkennung und Klassifizierung weiterer charakteristischer Audio-Signalen wie z.B. der Bruch einer Fensterscheibe sind mit diesen Systemen zurzeit nicht möglich!

(7) Induktionsschleife

Fahren mit einem RFID-TAG ausgerüstete Fahrzeuge in einen *unerlaubten* Bereich, so können sie mit Hilfe einer RFID-Antenne automatisch erkannt werden und ggf. wird ein Alarm ausgelöst. Versteckt bzw. entfernt der Fahrer sein gültiges TAG, so ist eine Identifizierung des RFID-TAGs unmöglich. Ein verdächtiges Fahrzeug und somit eine mögliche Gefahr würde nicht erkannt werden. Durch die Installation einer Induktionsschleife (Abbildung 12) im Boden wird beim Überfahren der Induktionsschleife ein Signal erzeugt. Wird parallel zum Signal der Induktionsschleife kein RFID-Signal detektiert, fährt möglicherweise das Fahrzeug in einen unerlaubten Bereich. Durch die Kombination der beiden Informationen (Signal der Induktionsschleife und Fehlen des RFID-Signals) erhält man den Hinweis auf ein mögliches Fehlverhalten bzw. die Gefahr eines terroristischen Anschlages. Über die Identität des Fahrzeuges liegen, da die ID-Nr. des RFID-TAGs fehlt, keine Informationen vor. Durch den Einsatz eines Kennzeichenerkennungssystems (siehe unten) kann die Identität des Fahrzeuges (Kennzeichen) erfasst werden.

Hersteller/ Anbieter	Cat-Traffic	Simens	HINN	IBC	Recognitec GmbH	Vitronic [1)]	Schmitz GmbH / Mobotix AG/ Valeo IT	Horatio GmbH
Produkt	V-REX-Stationär	Sicore	Pollux		ACEN/Net	Poliscan surveillance	Car-Reader	Videowächter
Fahrzeugtypen	alle	alle	PKW, LKW, Omnibus	PKW, LKW, Kraftrad, Omnibus	PKW, LKW, Kraftrad, Omnibus	alle	alle	PKW, LKW, Omnibus, keine Motorräder
Kennzeichen - Länder	alle EU opt. Arab.	alle	alle EU, weitere auf Anfrage	alle EU, weitere auf Anfrage	diverse EU, Russland, Türkei, China ...	EU + weitere	ein-/zeizeilige EU-Zeichen	D, A weitere auf Anfrage
Position Kennzeichen	in der Regel von vorne	vorne bei Bedarf von hinten	beliebig	vorne bei Bedarf von hinten	Vorne u. hinten, seitlich (Gefahrgut)	vorn + hinten	vorn + hinten	vorne bei Bedarf von hinten
Erkennungssicherheit	> 95	98	> 95	97%	bis 98	99 / Referenz	> 95	bis 98
Erkennungsbereich	5 m - 17 m	5 m - 35 m	1m - 3 m	5 m - 35 m	7 m - 9 m	Bis 50 m	variabel	max. 10 m
Gefahrguterkennung	ja	ja	nein	Sonder-entwicklung	ja	ja	nein	nein
Bemerkungen	Kombination mit RFID möglich	Option: Verschlüs-selung des Kenn-zeichens	---	Erkennung Container-Nr.: bei Bedarf	- Container-Kennzeichen kann erfasst werden.	- Bis 6 Spuren gleichzeitig - Fahrzeugtyp-erkennung PKW, LKW, mit und ohne Anhänger		

Auswahl eines geeigneten Systems ist abhängig von der Anwendung
z.B.: nur Kennzeichen bzw. Kennzeichen und Gefahrguterkennung, zur Verfügung stehender Platz, ….

Abbildung 12: Anbieter: Systeme zur Kennzeichenerkennung

(8) Kennzeichenerkennungssysteme (Fahrzeuge)

Kennzeichenerkennungssysteme werden heute in vielen Bereichen zur Erfassung/Identifizierung von Fahrzeugen eingesetzt, so z.B. in Parkhäusern. Die auf dem Markt erhältlichen Systeme eignen sich zur Identifizierung von Fahrzeugen. Ein wesentlicher Unterschied zwischen den Systemen besteht in der Möglichkeit, das Kennzeichen dem Herkunftsland zuzuordnen. (Abbildung 13). Diese Information kann jedoch einen Hinweis auf eine mögliche Gefahr liefern. Beim Einsatz von Kennzeichenerkennungssystemen muss der Datenschutz berücksichtigt werden.

Hersteller	Bircher	Signalbau Blauert	Edmatec	Preiser	Cad traffic
Produkt	ProLoop2	Signalbau Blauert	Edmatec	Schleifen-detektor	AVC 100
PKW	ja	ja	ja	ja	ja
PKW - Anhänger	nicht eindeutig geklärt	nicht eindeutig geklärt	ja	nein	ja
LKW	ja	ja	ja	ja	ja
LKW-Anhänger	nicht eindeutig geklärt	nicht eindeutig geklärt	ja	nein	ja
Motorrad	ja	ja	ja	ja	ja

Auswahl eines geeigneten Systems ist abhängig von der Anwendung,
z.B.: nur Erkennung Fahrzeugen mit und ohne Anhänger

Abbildung 13: Anbieter: Systeme Induktionsschleifen

(9) Unterbodenscanner

Werden gefährliche Stoffe wie z.B. Sprengstoff bzw. Objekte wie Waffen unter einem Fahrzeug (LKW, PKW) versteckt, fallen diese in der Regel bei einfachen Kontrollen nicht auf. Durch den Einsatz hochauflösender Kamerasystemen (Scanner) ist es möglich, den Unterboden von fahrenden Fahrzeugen auf unerwünschte, sicherheitsgefährdende Gegenstände schnell und unkompliziert zu untersuchen, auszuwerten und das Ergebnis abzuspeichern.

Es werden sowohl stationäre als auch mobile Systeme für Fahrzeuge (LKW und PKW) von den nachfolgenden Firmen angeboten:

- UVIScan® (Fa. UVIScan)
- SecuScan (Fa. KTG Traffic Parking Secu)
- PlateCatcher (Fa. Topguard)

Die Aufnahmen der Fahrzeugunterböden können zusammen mit weiteren Daten wie beispielsweise den Kfz-Kennzeichen ausgewertet und in einer Datenbank gespeichert werden. Werden KFZ-Kennzeichen gespeichert, muss der Datenschutz berücksichtigt werden.

Für den Güterverkehr steht ein im Schienennetz integrierter Unterbodenscanner (GKH-TR11 der Fa. Gatekeeper Security) zur Verfügung. Die maximale Fahrgeschwindigkeit beträgt ca. 20 km/h.

Exemplarische Untersuchungen von im FKIE vorhandener Sensoren

(1) Untersuchung des Einsatzes der RFID-Technologie

Im FKIE wurde der Einsatz von RFID-Systemen zur Zufahrtskontrolle und als automatisches Kontrollsystem für Fahrzeuge im Hafenbereich (Aufenthalt von Fahrzeugen in unerlaubten Bereichen) im Rahmen mehrerer Messkampagnen untersucht. Hierzu wurden Antennen in verschiedenen Höhen aufgestellt und die TAGs an unterschiedlichen Stellen im und am Auto positioniert.

Im ersten Testversuch wurden ein RFID-Lesegerät und 4 Richtantennen mit einem Öffnungswinkel von (H:60°, V:45°) benutzt.

Die Antennen wurden wie folgt aufgestellt:

(1) 4 Antennen auf gleicher Höhe (ca. 1 m) (siehe Abbildung 14)
(2) 1 Antenne (Höhe ca. 2 m) und 2 Antennen Höhe ca. 1m) (siehe Abbildung 15)

Die TAGs wurden an unterschiedlichen Stellen im Fahrzeug positioniert:

a. Außenseite der Fahrzeugscheibe (Seite Fahrzeugtür)
b. Innenseite auf der Windschutzscheibe
c. Ablage Fensterbereich (Bereich Windschutzscheibe)
d. Auf dem Beifahrersitz

Fahrzeuggeschwindigkeit: ca. 10 km/h

Abbildung 14: Messaufbau: 4 Antennen in gleicher Höhe (ca. 1m)

Abbildung 15: Messaufbau: 2 Antennen in einer Höhe ca.1 m und eine Antenne in einer Höhe von ca. 2m

Versuchsergebnisse:

Zu (1): TAGs konnten bis zu einer Entfernung von

- a. ca. 7 m
- b. ca. 7 m
- c. ca. 2 m

erkannt werden.

- d. Der TAG wurde nicht in allen Fällen identifiziert.

Fahren zwei Fahrzeuge nebeneinander, so wird der TAG des weiter entfernten Fahrzeuges in der Regel nicht sicher erkannt.

Zu (2): TAGs konnten bis zu einer Entfernung von

- a. ca. 13 m
- b. ca. 13 m
- c. ca. 13 m

erkannt werden.

- d. Die TAGs wurde nicht in allen Fällen identifiziert.

Wird die Antenne in ausreichender Höhe (Sichtkontakt zum TAG) positioniert, ist eine Identifizierung der TAGs bis zu einer Entfernung von 13m möglich (Versuch (2) a, b, c).

Die Ergebnisse der Messkampagne zeigen, dass das RFID-System zur Identifizierung für PKWs im Hafen geeignet ist.

In einer weiteren Messkampagne wurde untersucht, ob LKWs auf dem Hafengelände identifiziert und verfolgt werden können. Hierzu fuhren Fahrzeuge unter einer Hebebühne (Höhe: ca. 4,5 m – simuliert Portalhöhe – siehe Abbildung 16) durch, welche mit RFID-Antennen ausgerüstet waren. Weitere Antennen waren seitlich positioniert (Höhe ca. 2,5 m – simuliert RFID-Antenne an einer Fahrbahnkreuzung/Abfahrt auf dem Hafengelände – siehe Abbildung 17).

Abbildung 16: Zwei RFID-Antennen an Hebebühne befestigt (Höhe ca. 4,5 m)

Abbildung 17: Zwei RFID-Antennen an Hebebühne befestigt (Höhe ca. 2,5 m)

Zusätzlich wurde der Einfluss des metallischen Untergrundes auf die Identifizierung unterschiedlicher TAGs untersucht.

Verwendete TAGs:

- TAGs mit einer Rückseite ohne spezielle Isolierung gegen Metall; TAG in Scheckkartengröße.
  Im weiteren Text als „TAG I" bezeichnet.
- TAGs mit spezieller Isolierung gegen metallischen Einfluss auf der Rückseite des TAGs; Größe des TAGs 150mm x 69mm x 8,6mm
  Im weiteren Text als „TAG II" bezeichnet.

Für die Versuche wurden ein Lesegerät und zwei Richtantennen eingesetzt.

Die Antennen wurden wie folgt positioniert:

(1) Jeweils 1 Antenne auf der Vorderseite und Rückseite einer Hebebühne in einer Höhe von ca. 4,5 m
(2) 1 Antenne in einer Höhe von ca. 2,5 m neben der Fahrbahn

Zur Identifizierung der TAGs wurden diese an unterschiedlichen Stellen im Inneren bzw. der Außenseite des Fahrzeugs positioniert:

a. Drei TAGs I (1 links, 1 Mitte, 1 rechts) auf der Innenseite der Windschutzscheibe festgeklebt. (Abbildung 18)
b. Drei TAGs I (1 links, 1 mitte, 1 rechts) auf der Ablage Bereich Windschutzscheibe (Abbildung 19)
c. Ein TAG II auf der Ablage Windschutzscheibe (Abbildung 19)
d. Außenseite: jeweils 1 TAG I und 1 TAG II oberhalb der Windschutzscheibe auf Metall und auf der Rückseite des Fahrzeugs auf Metall verklebt (Abbildung 20).

Fahrzeuggeschwindigkeit: ca. 10 km/h

Abbildung 18: 3 RFID-TAGs auf der Innenseite der Windschutzscheibe

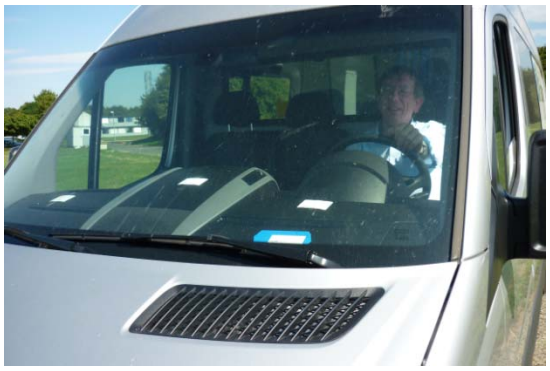

Abbildung 19: RFID-TAGs auf der Ablage des Fahrzeugs

Abbildung 20: 2 RFID TAGs auf metallischer Oberfläche fixiert

Ergebnisse:

Antenne oberhalb (1) und seitlich (2) positioniert:

1. Semipassive TAGs I und TAGs II auf der Ablage des Fahrzeuges (a)
   TAGs wurden aus einer Entfernung bis ca. 7m reproduzierbar erkannt.
   ➔ Semipassive TAGs I und TAGs II auf der Ablage der Windschutzscheibe positioniert sind geeignet zur Identifizierung und Kontrolle von Fahrzeugen.

2. Semipassive TAGs I (ohne Isolierung) auf Metall (c) wurden zu keinem Zeitpunkt erkannt.
   ➔ Semipassive TAGs I auf Metall sind nicht geeignet zur Identifizierung der Fahrzeuge.

3. Semipassive TAGs II (mit Isolierung) auf Metalloberflächen (c) wurden aus einer Entfernung bis ca. 7m reproduzierbar erkannt.
   ➔ Semipassive TAGs II (mit Isolierung) auf Metalloberflächen sind geeignet zur Identifizierung und Kontrolle von Fahrzeugen.

4. Semipassive TAGs I (ohne Isolierung) auf der Windschutzscheibe verklebt wurden abhängig von Fahrzeugmodell erkannt.
   ➔ Semipassive TAGs I (ohne Isolierung) auf der Windschutzscheibe verklebt (a) sind nur begrenzt geeignet zur Identifizierung und Kontrolle von Fahrzeugen.

Bei der Wahl eines geeigneten RFID-TAGs zur Identifizierung und Kontrolle eines Fahrzeuges auf dem Hafengelände müssen Parameter wie

- Fahrzeugtyp,
- metallischer Untergrund und

- Position des TAGs im bzw. am Fahrzeug

berücksichtigt werden.

Integration der Fahrzeugwaage

Zur Durchführung eines Bombenanschlags sind erhebliche Mengen an Sprengstoff erforderlich. Werden diese mit einem PKW transportiert, sollten abhängig von der transportierten Menge Sprengstoff deutliche Gewichtsveränderungen im Vergleich zum Leergewicht des Fahrzeuges nachweisbar sein.

Zur korrekten Beurteilung des gemessenen Fahrzeuggewichtes sind detaillierte Angaben zum

a. Leergewicht des PKWs,
b. Tankvolumen,
c. Anzahl und Gewicht der mitgeführten Gepäckstücke und
d. Umbau des Fahrzeuges

erforderlich.

Durch eine geschickte Ausnutzung dieser Parameter können unbemerkt große Mengen an Sprengstoff mitgeführt werden.

Zu a) Leergewicht des PKWs

Das Leergewicht eines Fahrzeuges wird laut Angaben des Kraftfahrt-Bundesamtes im ZBI (Fahrzeugschein) in Feld G „Masse des in Betrieb befindlichen Fahrzeugs in kg“ angegeben. In diesem Feld können abhängig vom Fahrzeug einzelne Werte, z.B. 1395 kg, jedoch ebenfalls Gewichtsbereiche z.B. 1367 kg – 1468 kg (z.B. KIA Ceed) angegeben werden. Wie groß die Gewichtsbereiche sein können, ist abhängig vom Fahrzeugmodell.
Die Angabe von Gewichtsbereichen kann zum unerkannten Transport von Sprengstoffen ausgenutzt werden, in dem man das leichteste Fahrzeugmodell (KIA Ceed 1367 kg) einsetzt und die Differenz zu 1468 kg (KIA Ceed) zum Transport von Sprengstoff benutzt.
Bei der Angabe des Leergewichtes (Feld G) ist eine Person mit 68 kg und 7 kg Gepäck berücksichtigt. Das Gewicht des Gepäcks bezieht sich auf normale alltägliche Fahrten. Urlauber führen in der Regel größere Mengen Gepäck mit sich, was berücksichtigt werden muss.

Zu b) Tankvolumen

Im Fahrzeugschein ist ein Feld (12) „Rauminhalt des Tanks bei Fahrzeugen in m³“ vorgesehen, welches jedoch nicht zwangsläufig ausgefüllt sein muss (z.B. KIA Ceed). Deutliche Schwankungen des Tankvolumens treten in Abhängigkeit des Fahrzeugmodells auf (ca. 40l – 80l). Wird ein Fahrzeug mit fast leerem Tank zum Transport von Sprengstoffen benutzt, kann anstatt des Kraftstoffs Sprengstoff geladen werden.

Zu c) Anzahl und Gewicht der Gepäckstücke

Bei der Benutzung einer Fähre durch Urlauber, muss das mitgeführte Gepäck berücksichtigt werden. Orientiert man sich am Flugverkehr mit seinen geringen zulässigen Gepäckmengen, so dürfen Einzelpersonen ca. 20 kg Gepäck mitnehmen. Befinden sich 4 Personen im Fahrzeug, könnten sie ca. 80 kg Gepäck mitführen bzw. anstelle von Gepäck 80 kg Sprengstoff.

Zu d) Umbau des Fahrzeuges

Wird das Fahrzeug umgebaut und Teile entfernt, verringert sich das Gewicht des Fahrzeuges. Angaben zu Gewichtsveränderungen sind sehr schwierig zu erfassen und werden in der weiteren Betrachtung nicht näher berücksichtigt.

Beurteilung; Einsatz der Fahrzeugwage

Unter Berücksichtigung der Punkte a–c bei der Planung des Transports von Sprengstoff können erhebliche Mengen an Sprengstoff mitgeführt werden, ohne dass man bei den Gewichtmessungen Hinweise darauf erhalten würde. Fährt der Terrorist mit einem quasi leeren Tank, benutzt er anstatt Gepäck jeweils Sprengstoff, verwendet er ein Fahrzeug, bei dem im Fahrzeugschein beim Leergewicht ein Gewichtsbereich von ca. 100 kg angegeben ist, so kann er durchaus, abhängig von der Anzahl an Personen im Fahrzeug ca. 150-200 kg Sprengstoff mitführen, ohne den geringsten Verdacht zu erwecken.

Unter Berücksichtigung dieser Aspekte ist der Einsatz der Fahrzeugwaage nicht zielführend und auf weitere Untersuchungen wurde verzichtet.

Beim Besuch des Hafens in Puttgarden am 23.10.2012 konnten zahlreiche überladene Fahrzeuge beobachtet werden. Als Ursache wurde die Mitnahme großer Mengen Getränke genannt. Überladene Fahrzeuge sind nach Angabe des PFSO in Puttgarden keine Seltenheit und eine Kontrolle dieser Fahrzeuge erfolgt in der Regel nicht.

Einsatz von Gammadetektoren: Nachweis radioaktiver Stoffe

Nachweis radioaktiver Materialien

Im Rahmen der im FKIE durchgeführten Untersuchungen wurde die Veränderung der Strahlungsintensität in Funktion des Abstandes zu den radioaktiven Quellen ^{137}Cs 3,7 MBq, ^{137}Cs 1.85 MBq und ^{60}Co 3,7 MBq mit Hilfe von „Stride DU 202"-Detektoren (Fa. ICX) gemessen. Die Ergebnisse dieser Untersuchungen lieferten Informationen über die Entfernung, in der radioaktive Quellen noch nachgewiesen werden können.

Mit Hilfe der Stride-Detektoren konnten die radioaktive Quellen, ^{137}Cs (3,75MBq und 1.85 MBq) sowie ^{60}Co (3,7 MBq), bis zu einer Entfernung von 5 Metern nachgewiesen werden. Mit Hilfe des „Identifinder 2" (Fa. Flir) wurden die einzelnen Nuklide eindeutig aus einer Distanz von ca. 1m identifiziert. Wird bei der Detektion ein starker Strahler nachgewiesen, muss die Person, welche die Quelle identifizieren muss, den Abstand zur Quelle berücksichtigen. Sie darf sich ggf. nicht bis in unmittelbarer Nähe der Quelle begeben. Die Identifizierung der Nuklide sollte nur von qualifizierten Personen durchgeführt werden.

Die Identifizierung zweier am gleichen Ort befindlichen unterschiedliche Quellen ^{137}Cs (3,7 MBq) und ^{60}Co (3,7 MBq) ist mit Hilfe des „Identifinder 2" möglich.

Die Ergebnisse zeigen, dass Gamma-Detektoren zur Detektion radioaktiver Quellen im Hafenbereich eingesetzt werden können. Aufgrund des relativ geringen Detektionsabstandes muss jedes Fahrzeug einzeln untersucht werden. Fahrzeuge, die nebeneinander fahren, werden aufgrund des zu großen Abstandes zwischen radioaktiver Quelle und Detektor nicht in allen Fällen sicher erkannt.

Einsatz von radioaktiven Stoffen im medizinischen Bereich wie z.B. Technetium (^{99}Tc)

Eine mit ^{99}Tc behandelte Person wurde direkt nach Verabreichung (ca. 2 Stunden) und 1 Tag später auf das Vorhandensein von radioaktivem Material mit Hilfe des „Identifinder 2" untersucht. Am ersten Tag konnte ^{99}Tc im Abstand von 4-5 Metern nachgewiesen und identifiziert werden. Ca. 24 Stunden später wurde nur in unmittelbarer Nähe (ca. 1 m) ^{99}Tc nachgewiesen und identifiziert. Das bedeutet aber, dass selbst noch nach einem Tag ein Fehlalarm ausgelöst werden kann.

Diese Ergebnisse zeigen, dass neben dem Nachweis von radioaktivem Material eine Identifizierung der Art der Quelle zwangsläufig notwendig ist.

Konzeption eines mehrstufigen Datenfusionsmodells

Durch den Einsatz geeigneter Sensoren werden frühzeitig erste Informationen über mögliche Gefahren bzw. geplante Anschläge erhalten. Durch die Kombination bzw. Fusion von Sensordaten und Kontextinformationen können frühzeitig weitere Bedrohungen erkannt werden. Da die Anforderungen an die Kontrollen und Überwachung auf einem Hafengelände unterschiedlich sein können wurden zwei Konzepte erarbeitet, die

1) sehr geringe Anforderungen (einfaches Konzept) und
2) höhere Anforderungen (erweitertes Konzept)

an die Sensorik und Auswertung beschreiben.

(1) Einfaches Konzept

Das in Abbildung 21 gezeigte einfache Konzept berücksichtigt im Wesentlichen die Zufahrt auf das Hafengelände und auf die Fähre. Als Zufahrtsberechtigung auf das Hafengelände und die Fähre ist ein gültiger RFID-TAG erforderlich. Die Fahrer erhalten vor der Einfahrt auf das Hafengelände Angaben, an welcher Stelle im Fahrzeug sie den RFID-TAG während der gesamten Aufenthaltszeit im Hafen aufbewahren müssen.

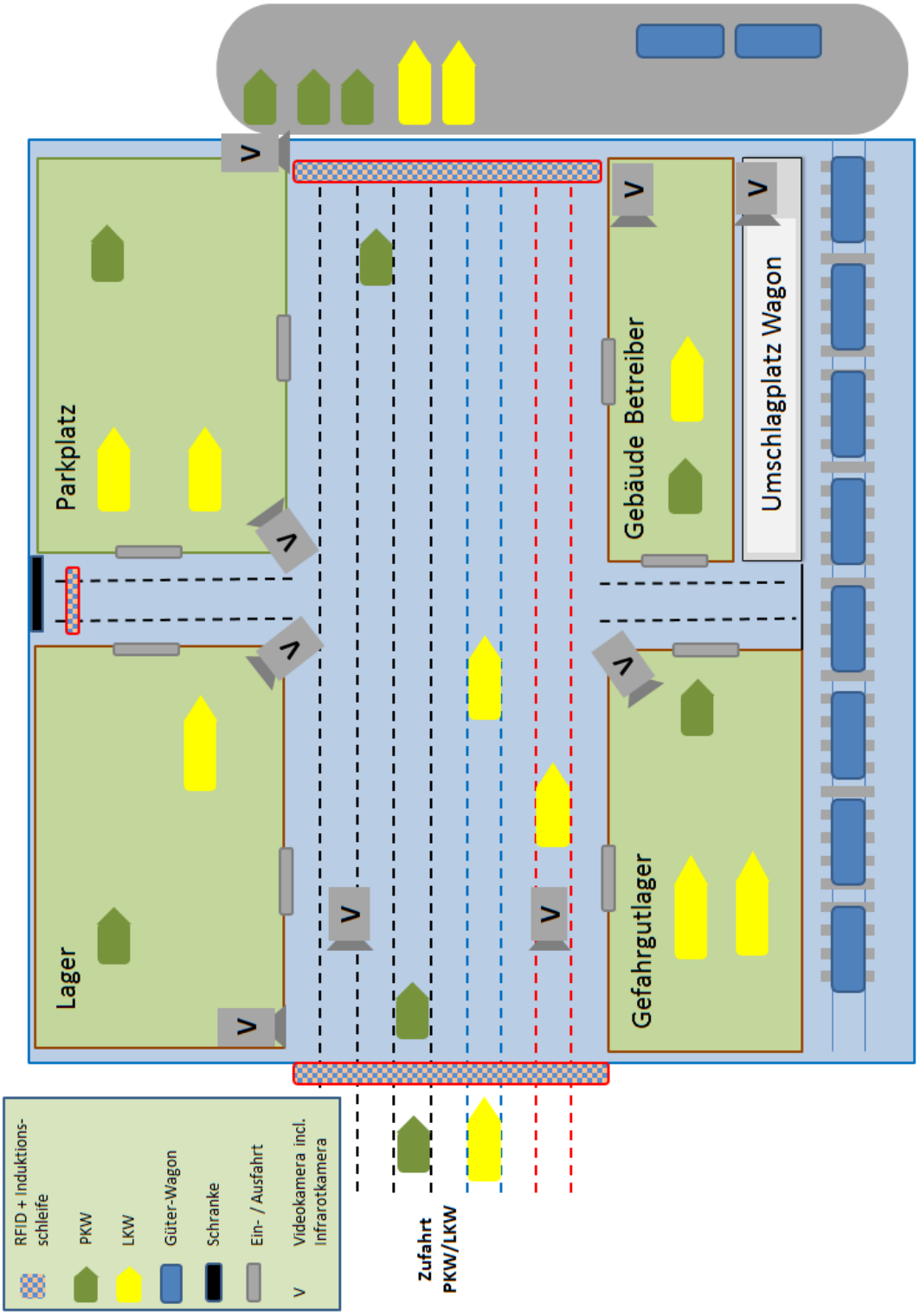

Abbildung 21: Einfaches Konzept

Im Bereich der Hafeneinfahrt sind RFID-Sensoren und Induktionschleifen installiert. RFID-Antennen überprüfen die Zufahrtsberechtigung auf das Hafengelände, während mit Hilfe der Induktionsschleife überwacht wird, ob ein Fahrzeug mit oder ohne Anhänger auf das Hafengelände fährt.

Fahrzeuge von eigenen Mitarbeitern bzw. Fremdfirmenmitarbeitern, welche nicht auf die Fähre fahren, sondern nach der Arbeit das Gelände wieder verlassen, erhalten ebenfalls einem RFID-

TAG als Zufahrtsberechtigung. Die auf den TAGs gespeicherten ID-Nummern sind ebenfalls auf dem Sicherheitssystem des Hafenbetreibers hinterlegt. Neben der ID-Nummer sind die unterschiedlichen Zufahrts- bzw. Ausfahrtsberechtigungen für Kunden und eigene Mitarbeiter bzw. Fremdfirmenmitarbeiter auf diesem System gespeichert.

Im Bereich der Ausfahrt vom Hafengelände auf die Fähre wird mit Hilfe der RFID-Sensoren und Induktionsschleifen überprüft, ob das Fahrzeug mit oder ohne Anhänger eine Zufahrtsberechtigung für die Fähre hat. Duch die zusätzliche RFID-Kontrolle im Bereich der Zufahrt auf die Fähre wird automatisch überprüft, ob alle gebuchten Fahrzeuge auf der Fähre sind oder Fahrzeuge ohne gültigen TAG auf die Fähre gelangt sind. Im letzteren Fall würde ein Warnsignal abgegeben, da das zwar die Induktionsschleife eine Ausfahrt meldet, aber das RFID-Signal fehlt (kein oder ungültiges TAG im Fahrzeug). Das Fehlen einer gültigen ID- Nummer wird sofort der entsprechenden Stelle gemeldet.

Automatische Überwachungen in anderen Bereichen auf dem Hafengelände erfolgen nicht. Die auf dem Gelände installierten Videokameras werden vom Sicherheitspersonal verwendet, um Fehlverhalten bzw. Hinweise auf kritische, kriminelle oder terroristische Aktivtäten zu verfolgen.

Fremdfirmen- und Hafenmitarbeiter dürfen eine getrennte Ausfahrt benutzen. Das System erkennt anhand der ID-Nummer die Fahrzeuge, die berechtigt sind das Hafengelände zu verlassen.

Die für die Zugangkontrollen und Überwachung des Hafengeländes und der Fähre eingesetzten RFID-TAGs sind für die Fährkunden nur einmal verwendbar. Bei der Einfahrt auf das Hafengelände wird die ID-Nummer erkannt und im Sicherhheitssystem hinterlegt. Diese ID-Nummer wird nach Verwendung nicht mehr neu vergeben. Bei dem Versuch diesen RFID-TAG nochmals zu verwenden, würde das System automatisch erkennen, das diese ID- Nummer nicht mehr gültig ist und die Einfahrt auf das Betriebsgelände sperren. Ein Mißbrauch durch Wiederverwendung des RFID-TAGs ist somit nicht möglich.

Eigene Mitarbeiter erhalten TAGs, die sie während ihrer gesamten Vertragsdauer verwenden müssen. Mit diesen können sie jederzeit auf das Betriebsgelände fahren und es wieder verlassen.

Fremdfirmenmitarbeiter erhalten je nach Dauer ihrer Tätigkeiten für einen oder mehrere Tage einen TAG mit entsprechenden Zufahrts- bzw. Ausfahrtsberechtigungen. Nach beendeter Tätigkeit erlischt die Zufahrtsberechtigung zum Hafengelände.

Diese Regelungen gelten für alle Nutzergruppen, die zuvor genannt wurden, für das gesamte Hafengebiet und die Zufahrt zu den Fähren.

(2) Detailliertes Konzept

Sind umfangreichere automatische Kontrollen gewünscht, ist der Einsatz weiterer Sensoren erforderlich. Dies wird im detaillierten Konzept (Abbildung 22) dargestellt.

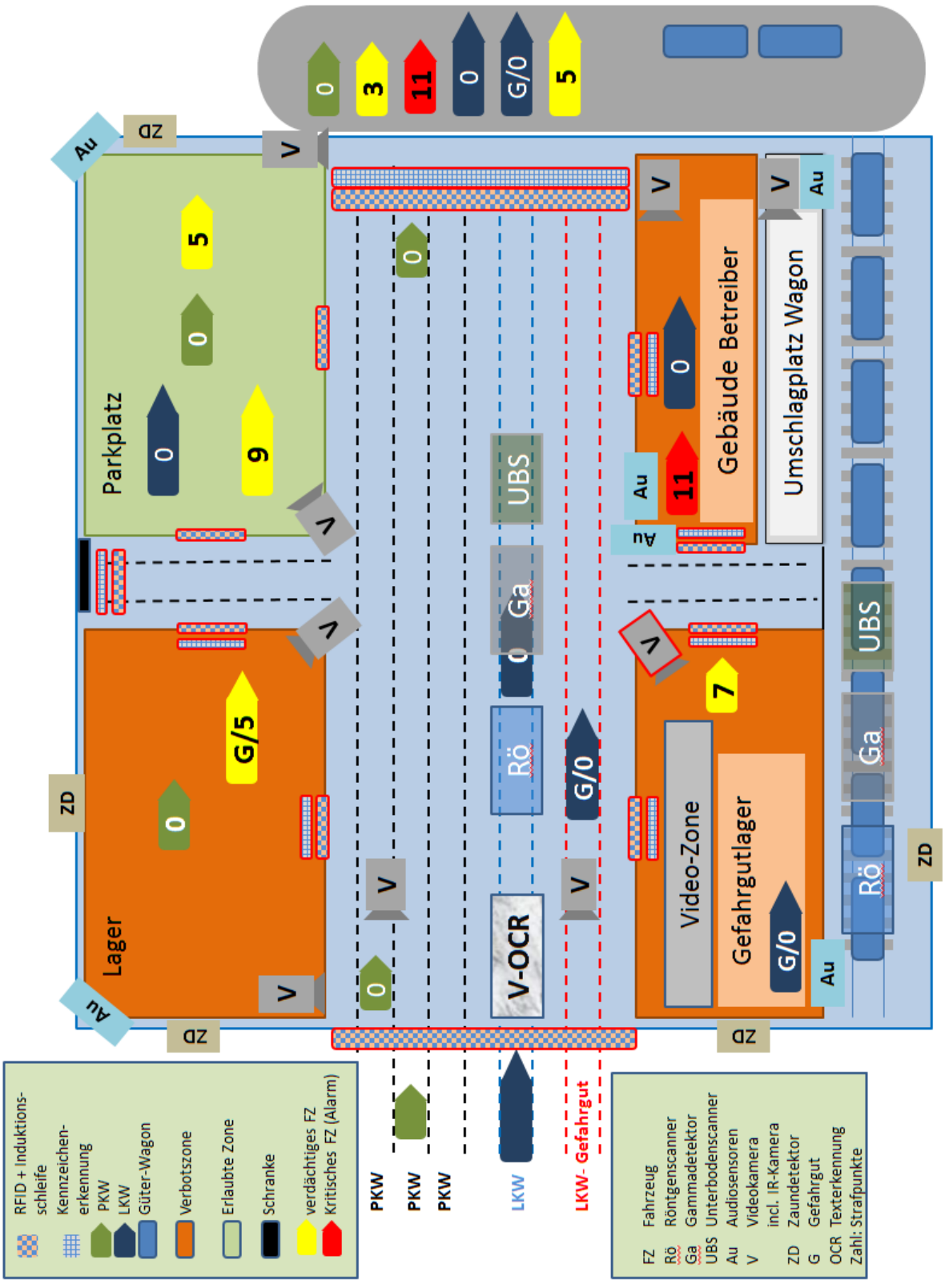

Abbildung 22: Detailliertes Konzept

Erläuterungen zum Konzept:

Die in den Fahrzeugensymbolen (Pfeilen) enthaltene Buchstaben bzw. Zahlen bedeuten:

G: Fahrzeug befördert Gefahrgut

Zahl: Anzahl Strafpunkte auf dem Strafkonto
(Erläuterung zu Strafpunkten siehe Text unten)

G/Zahl: Fahrzeug befördert Gefahrgut und hat [Zahl] Strafpunkte

Farbliche Markierung der Fahrzeuge:

- Grün: PKW ohne Strafpunkte
- Blau: LKW ohne Strafpunkte
- gelb: (PKW bzw. LKW) hat > 0 und < 10 Strafpunkte
  (verdächtiges Fahrzeug).
- rot: (PKW bzw. LKW) hat $\geq$ 10 Strafpunkte
  (kirtisches Fahrzeug – Alarm!!)

Das detaillierte Konzept hat in Bezug auf die RFID-Tags und die Fahrzeug-IDs die gleiche Funktion wie im einfachen Konzept.

Zusätzlich können aber spezielle Überwachungsregeln für einzelne Teilbereiche im Hafengelände gelten.

Die Zufahrtsberechtigungen in verschiedene Bereiche des Betriebsgeländes bzw. auf die Fähre können unterschiedlich sein. So dürfen beispielsweise Fahrzeuge

- von Kunden, welche auf die Fähre fahren,
- von Fremdfirmen und
- eigener Mitarbeiter

nur in die für sie freigegebenen Bereiche fahren bzw. das Hafengelände wieder verlassen. Die im Sicherheitssystem hinterlegten Zufahrtsberechtigungen werden über die ID-Nummer mittels RFID-Antennen auf dem Hafengelände überwacht. So kann der Hafenbetreiber festlegen, dass sich alle eigene Mitarbieter mit ihrem Fahrzeug auf dem gesamten Betriebsgelände aufhalten dürfen. Kunden, welche auf die Fähre fahren, dürfen nur auf den Zufahrtswegen und für sie erlaubten Bereiche fahren. Wird Gefahrgut auf das Hafengelände transportiert, wird dieses in speziellen hierfür zugelassenen Bereichen abgestellt. Diese Fahrzeuge erhalten für das Gefahrgutlager eine Zufahrtsberechtigung, während für andere Fahrzeuge dieser Bereich eine Verbotszone sein kann.

Fremdfirmenmitarbeiter erhalten für ihre Tätigkeiten Zufahrtsberechtigungen für einzelne Bereiche oder im speziellen Fällen für den gesamten Hafenbereich.

Die Zugangsberechtigungen in unterschiedlichen Zonen werden automatisch mit Hilfe von RFID-Antennen überprüft. Fährt ein Fahrzeug in einen nicht für ihn zugelassenen Bereich, wird dies automatisch über die Auswertung der ID-Nummer und den im Sicherheitssystem hinterlegten Daten überprüft. Da keine Zufahrtsberechtigung vorliegt, werden im Sicherheitsystem automatisch Strafpunkte auf ein Strafkonto dieser RFID-Nummer hinterlegt. Die Anzahl der Strafpunkte ist abhängig von der durch das Fahrzeug verusachten möglichen Gefahr, die durch das unerlaubte Fahren in eine Verbotszone entsteht. Hierbei werden Parameter wie z.B.

1. PKW (ohne bzw. mit Anhänger),
2. LKW (ohne bzw. mit Gefahrgut) und
3. Herkunftsland (sofern im System hinterlegt)

berücksichtigt. Weitere Parameter können jederzeit ergänzt, bestehende gelöscht oder verändert werden.

Fährt ein PKW in einen nicht erlaubten Bereich, kann zunächst davon ausgegangen werden,

dass es sich um ein „harmloses“ Vergehen (falsche Abfahrt) handelt und es werden nur wenige Strafpunkte (3) vergeben. Hat das gleiche Fahrzeug jedoch durch mehrere Verstöße einen kritischen Punktestand (z.B. ≥10 Punkten) erreicht, wird ein Alarm ausgelöst und das Fahrzeug wird auf einem Überwachunmgsmonitor rot dargestellt.

Da die Fahrzeuge mit Strafpunkten für das Sicherheitspersonal von Bedeutung sind, werden Fahrzeuge mit

- 1-9 Strafpunkte in gelb und
- ≥10 Strafpunkte: in rot

dargestellt. Fahrzeuge ohne Strafpunkte werden nicht dargestellt, um die Übersicht über die aktuelle Gefahrensituation nicht zu beeinträchtigen.

Die Sicherheitskräfte erkennen sofort anhand der Farbe, welche Gefahr besteht, und können z.B. bei Erscheinen eines gelb bzw. rot dargestellten Fahrzeugs auf dem Gelände die verdächtigen Fahrzeuge mit vorhandenen Videokameras zusätzlich manuell überwachen; das Zuweisen einer Kamera zu einem verdächtigen Fahrzeug ist ebenfalls automatisierbar. Ein mögliches Gefahrenpotential wird frühzeitig erkannt und kann sofort beurteilt werden. Bei rot markierten Fahrzeugen muss unverzüglich gehandelt werden.

Beseitigt bzw. versteckt der Fahrer sein TAG, würde er nicht mehr durch die RFID-Antennen erfasst und könnte möglicherweise unerkannt seine nicht erlaubten Aktivitäten (Einholen von Informationen, Vorbereitung eines Anschlages) umsetzen. Um dies zu verhindern, werden neben den RFID-Antennen ebenfalls an der gleichen Stelle Induktionsschleifen im Boden installiert. Fährt ein Fahrzeug ohne TAG in einen unerlaubten Bereich, meldet die Induktionsschleife zwar ein Fahrzeug, jedoch fehlt das RFID-Signal. Durch die Kombination der Daten dieser beiden Sensoren kann automatisch erkannt werden, dass jemand mit einem Fahrzeug in einen möglicherweise nicht erlaubten Bereich fährt. Eine derartige Meldung wird an das Sicherheitspersonal weitergegeben. Da keine Information über die Identität des Fahrzeuges mehr vorliegt (RFID-TAG nicht vorhanden/nicht identifiziert) kann durch die zusätzliche Installation eines Kennzeichenerkennungssystems (KES) automatisch ermittelt werden, um welches Fahrzeug es sich handelt. Dieses KES wird nur dann aktiviert, wenn die Induktionsschleife eine Fahrzeug meldet und kein RFID-Signal vorhanden ist. Eine systematische Überwachung der Kennzeichen soll nicht erfolgen. Das Kennzeichen des Fahrzeuges wird im System abgespeichert. Die Dauer und der Umfang der gespeicherten Daten muss den Vorgaben des Datenschutzes entsprechen.

Der Versuch, mit einem Fahrzeug, an dem nach der Einfahrt der TAG entfernt wurde, an unterschiedlichen Tagen in unterschiedliche verbotene Bereiche zu fahren und diese auszukundschaften, kann ebenfalls durch die Auswertung der verdächtigen Kennzeichen über einen bestimmten Zeitraum erkannt werden. Datenschutzrechtliche Aspekte, wie die Dauer der Aufbewahrung von Kennzeichendaten, müssen berücksichtigt werden.

Die Vergabe von Strafpunkten beruht auf der Gefährdungsbewertung der einzelnen unerwünschten Verhaltensweisen ab. Fährt etwa ein LKW mit gefährlichem Gefahrgut in einen nicht erlaubten Bereich, werden deutlich mehr Strafpunkte vergeben als bei der Einfahrt eines PKWs in einen aus allgemeinen Gründen gesperrten Bereich. Abhängig vom möglichen Schaden, der im Falle eines Anschlages angerichtet werden kann, werden in den unterschiedlichen Bereichen mehr oder weniger Punkte vergeben. Hierbei können ebenfalls die Gefahrgutklassen als Kriterium herangezogen werden. Beim Transport von Gefahrgütern müssen die Firmen Angaben wie z.B. Gefahrgutklassen zu den transportierten Gefahrgütern machen. Da diese Angaben bereits beim Kauf eines gültigen RFID-TAGs vorliegen, können diese automatisch in der Vergabe von Strafpunkten einbezogen werden. Die Risikobeurteilung und somit Festlegung der Anzahl an Strafpunkten erfolgt durch den Betreiber.

Werden durch das Sicherheitspersonal weitere nicht durch Sensoren erkannte Gefahren beobachtet, können manuell Punkte auf das entsprechende Konto des Fahrzeuges im System hinzugfügt werden.

Ein „kritisches“ Fahrzeug (≥ 10 Strafpunkte) sollte nach Möglichkeit daran gehindert werden, auf eine Fähre zu fahren. Gelangt das Fahrzeug trozdem auf die Fähre, wird dies durch die im Bereich Ausfahrt Hafen/Auffahrt Fähre installierten Sensoren (RFID-TAG, Induktionsschleife, Kennzeichenerkennungssystem) erkannt. Der Kapitän und die Sicherheitskräfte erhalten unverzüglich Informationen über das kritische Fahrzeug.

Neben der nicht erlaubten Zufahrt in verbotene Bereiche kann die Aufenthaltsdauer in diesen Zonen Hinweise auf verdächtige Handlungen liefern. Hat sich ein Fahrzeug in eine nicht erlaubte Zone verfahren, ist die Aufenthaltsdauer in der Regel relativ kurz. Werden jedoch vom Fahrzeugfahrer Informationen z.B. über vorhandene Sicherheitsanlagen in diesen verbotenen Bereichen eingeholt oder andere nicht erlaubte Handlungen durchgeführt, hält sich das Fahrzeug in der Regel länger in diesem verbotenen Bereich auf. Die Aufenthaltsdauer liefert mögliche Hinweise auf Bedrohungen und kann bei der automatischen Vergabe von Strafpunkten berücksichtigt werden.

Fährt ein auf dem Hafengelände mit einem gültigen Fahrschein (RFID-TAG) ausgestattetes Fahrzeug nicht auf die Fähre, wird dies durch einen Abgleich der Zufahrtsdaten auf das Hafengelände mit den Zufahrtsdaten auf die Fähre erfasst und Reederei und Hafenbetreiber automatisch mitgeteilt.

Ein Teil der Fahrzeuge transportiert Gefahrgüter, welche in speziell dafür vorgesehene Bereiche z.B. Gefahrgutlager zwischengelagert werden. Für diese Bereiche besitzen die Gefahrguttransporter eine Zufahrtsberechtigung (Abbildung 22 – Fahrzeug G/0) während für normale Fahrzeuge wie z.B. PKW dies eine Verbotszone (Abbildung 22 – Fahrzeug mit 7 Strafpunkten) darstellt. Das Sicherheitssystem erkennt anhand der ID-Nr, wer eine Zufahrtsberechtigung für diesen speziellen Bereich hat und wer nicht. Dürfen in bestimmten Zeitabschnitten (Nacht/Wochenende) im Gefahrgutlager keine Fahrzeuge mit Gefahrgut abgestellt werden, kann der Bereich zusätzlich durch Videokameras mit Zonenüberwachung kontrolliert werden. Der Betreiber kann die Zonen, in denen zu bestimmten Zeitpunkten keine Fahrzeugbewegungen stattfinden dürfen, selbst festlegen. Finden im Gefahrgutlager nicht erlaubte Veränderungen/Fahrzeugbewegungen in der festgelegten Video-Zone statt, erkennt das spezielle Video-Überwachungssystem (Abbildung 22 – rot umrandetes Videosymbol) dies und informiert automatisch das Sicherheitspersonal. Das Videoüberwachungssystem kann zwischen unterschiedlichen Fahrzeuggrößen (PKW bzw. LKW) und Personen unterscheiden.

Der Aufenthalt mehrerer verdächtiger Fahrzeuge in einem erlaubten Bereich könnte eine Gefahr darstellen. Hält sich ein verdächtiger LKW mit z.B. 9 Strafpunkten und ein PKW mit 5 Strafpunkten auf dem Parkplatz (erlaubter Bereich) auf, können von den Fahrern der verdächtigen Fahrzeuge Waren bzw. Gegenstände übergeben oder ausgetauscht werden, die zu einem späteren Zeitpunkt für eine kriminelle Handlung verwendet werden können. Durch die vorhandene Information, dass sich zwei verdächtige Fahrzeuge in einer erlaubten Zone aufhalten, kann das Sicherheitspersonal durch eine gezielte Kontrolle mit Hilfe von Videokameras den Bereich genauer überwachen.

Beim Gütertransport (LKW) können kritische Stoffe zwischen unkritischen versteckt werden. Diese können mit Hilfe von zusätzlichen Sensoren wie

- Röntgenscannern (Rö) oder
- Gammadetektoren (Ga) (Detektion radioaktiver Stoffe)

erkannt werden (Abbildung 22). Die modernen Röntgenscanner sind in der Lage, zwischen den Kategorien organischen, anorganischen Materialien und Metallen zu unterscheiden. Selbst innerhalb einer Kategorie, z.B. „organische Materialien“, sind beispielsweise Unterschiede zwischen Bananen und organischen Sprengstoffen in Kunststoffgebinden farblich dargestellt. Hinweise auf nicht deklarierte bzw. verdächtige Objekte und Produkte können mit Hilfe der Röntgenscanner sichtbar gemacht werden. So können Hinweise auf bleihaltige Objekte ebenfalls auf radioaktive Stoffe hindeuten. Blei wird als Schutzmaterial gegen radioaktive

Strahlung eingesetzt.

Werden radioaktive Substanzen mit Hilfe von Gammadetektoren nachgewiesen, müssen diese, um das Gefahrenpotential zu ermitteln bzw. Fehlalarme auszuschließen, mit Hilfe spezieller Gammadetektoren identifiziert werden.

In der Medizin werden radioaktive Substanzen mit kurzer Halbwertzeit eingesetzt. Fährt ein mit radioaktivem Material (^{99}Tc) behandelte Person in den Hafenbereich, so würde ein Alarm abhängig vom Zeitpunkt der medizinischen Behandlung ausgelöst. Erst nach der Identifizierung des Nuklids wird der Fehlalarm erkannt.

Werden verdächtige Objekte bzw. Stoffe unter dem Fahrzeug versteckt, sind sie nicht ohne zusätzliche Prüfverfahren erkennbar. Hinweise bzw. Nachweise auf unter dem Fahrzeug versteckte Objekte können mit Hilfe von speziellen Spiegeln oder Unterbodenscannern (Ubs) erhalten werden. Unterbodenscanner liefern detaillierte Bilder bzw. Videos des Unterbodens von Fahrzeugen. Die Auswertung dieser Bilder/Videos erfolgt durch entsprechend geschultes Personal.

Die Kontrolle verdächtiger LKW-Fahrzeuge kann durch die Detektoren Rö, Ga und Ubs auf einer Fahrspur erfolgen. Sollte ein Röntgengerät für LKWs eingesetzt werden, bei dem die Fahrerkabine ebenfalls gescannt wird, müssen alle LKW-Insassen vor dem Scan-Vorgang aussteigen.

Sind Hinweise bei PKWs auf verdächtige Stoffe bzw. Objekte vorhanden, können auch PKWs in diesen Anlagen (Rö, Ga und Ubs) untersucht werden. Alle Insassen müssen vorher aussteigen.

Mit Hilfe von Videosystemen incl. OCR-Erkennung ist es möglich, LKWs von aussen optisch zu erfassen und mit Hilfe von OCR-Erkennung Infomationen über das Fahrzeug im System abzuspeichern. Wenn erforderlich, können diese Informationen zur Bedrohungserkennung im Zusammenhang mit weiteren Daten genutzt werden.

Eisenbahnwagons können ebenfalls auf eine Fähre verladen werden. Die Kontrolle der Wagons kann durch den Einsatz von Röntgenscannern, Gammadetektoren und Unterbodenscannern auf den Gleisen erfolgen (Abbildung 22).

Versuchen Personen sich über einen Zaun Zutritt zu Fahrzeugen, die Gefahrgüter geladen haben, zu verschaffen, kann durch die Installation von Zaundetektoren diese Bedrohung automatisch erkannt und an das Sicherheitspersonal gemeldet werden.

Werden bei einem Anschlag auf dem Hafengelände Schüsse abgegeben, können diese mit Hilfe von akustischen Sensoren (Mikrofonen) erfasst werden. Die Systeme erkennen, dass es sich um einen Schuss und nicht um ein anderes Geräusch handelt. Eine Differenzierung zwischen mehreren unterschiedlichen Geräuschen ist derzeit nicht mit auf dem Markt erhältlichen Sensoren möglich. Durch den Einsatz von mindstens drei Mikrofon-Arrays kann der Ort des Schusses berechnet und die Koordinaten des Schützen automatisch an das Sicherheitspersonal weitergegeben werden.

Das detaillierte Konzept ist modular aufgebaut und kann jederzeit erweitert oder vereinfacht werden, ohne dass das Überwachungtool neue programmiert werden muss. Dies ermöglicht es, kurzfristig Anpassungen ohne großen Aufwand vorzunehmen.

Nun werden die Arbeiten zu AP 2.1.2 (Integration von Detektionssystemen für die Gefahrstoffkontrolle) beschrieben:

Vorgehensweise

Tritt bei einer Kontrolle der Verdacht eines unerlaubten Transports bzw. Besitzes von Gefahrstoffen wie z.B. Sprengstoffen auf, sollten die verdächtigen Stoffe sofort und nach Möglichkeit vor Ort analysiert werden, um ggf. unverzüglich geeignete Maßnahmen einzuleiten. Zur Identifizierung von Reinsubstanzen bzw. Gemischen stehen spektroskopische Verfahren wie Infrarot (Günzler & Gremlich, 2003) und Raman-Spektroskopie (Hesse et al., 2011) zur Verfügung. Die Auswertung der IR- bzw. Raman-Spektren führt nicht in allen Fällen direkt vor Ort zu eindeutigen Ergebnissen. Einige Gerätehersteller bieten den Service an, die nicht eindeutig interpretierbaren Spektren zur Auswertung an ihre Serviceabteilung zu schicken. Der Kunde erhält innerhalb von 24 – 48 Stunden eine Antwort mit dem Ergebnis, dass das Produkt möglicherweise identifiziert wurde. Dieser Zeitraum für die Interpretation der Spektren ist im Ernstfall zu lang. Mit Hilfe des entwickelten Tools können Experten vor Ort in weniger als eine Stunde weitere Informationen über die Zusammensetzung eines unbekannten Gemisches liefern. Hierfür wurden spezielle Algorithmen entwickelt, welche die IR- bzw. Ramanspektren auswerten und dem Spezialisten zusätzlich die Möglichkeit einer manuellen Auswertung geben. Liegen komplexe Gemische vor, können diese nicht in allen Fällen durch IR- bzw. Raman-Spektroskopie identifiziert werden. In solchen Fällen müssen weitere Analysen durchgeführt werden.

Im Rahmen dieses Projektes wurden folgende mobile Infrarot- bzw. Raman-Spektrometer eingesetzt:

- Infrarot-Spektrometer *TruDefender FT (Fa. Thermo Scientific)* und
- Raman-Spektrometer *FirstDefender RM* (*Fa. Thermo Scientific*).

Der Vorteil der modernen mobilen IR- und Raman-Geräte besteht darin, dass die Analyse ohne große Probenvorbereitung direkt vor Ort erfolgen kann. Es werden sehr geringe Mengen an Probenmaterial benötigt, so dass keine ernsthaften Gefahren für die Person, welche die Analyse durchführt, zu erwarten sind.

Die im Rahmen dieses Projektes für die Entwicklung von Algorithmen erforderlichen IR- und Raman-Daten von Sprengstoffen (Reinstoff und Stoffgemische) wurden vom Projektpartner Hochschule Bonn Rhein Sieg (HBRS) mit den oben genannten Geräten aufgenommen und dem Fraunhofer FKIE als TXT-Dateien zur Verfügung gestellt.

Auswertung der Spektren

Zur Auswertung von IR- und Raman-Spektren wurde ein Verfahren entwickelt, das die von den Spektrometern aufgenommenen Daten in ein Auswertetool einliest, die IR- bzw. Raman-Spektren graphisch darstellt und die Peaks mit einem speziellen Algorithmus automatisch erkennt.

IR- bzw. Raman-Spektren von Reinsubstanzen geben charakteristische Spektren für die jeweiligen Substanzen. Das IR- bzw. Raman-Spektrum der Reinsubstanzen ist vergleichbar mit einer Art Fingerabdruck. Eine Identifizierung eines Stoffes kann somit nur dann erfolgen, wenn die IR- bzw. Raman-Spektren von unbekannten Substanzen mit den Spektren bekannter Verbindungen verglichen werden, die z.B. in einer Datenbank gespeichert sind. Liegen keine Vergleichsspektren vor, ist in der Regel eine Identifizierung der unbekannten Substanz mit Hilfe der IR- bzw. Raman-Spektroskopie nicht möglich.

Es wurde ein Algorithmus entwickelt, der es ermöglicht, die Spektren von Einzelsubstanzen mit denen aus einer Spektrendatenbank automatisch zu vergleichen und ggf. zu identifizieren. Die Zusammensetzung eines Stoffgemisches wird durch einen automatischen Vergleich der Peaks

aus dem Stoffgemisch mit denen aus der Datenbank enthaltenen Spektren der Einzelsubstanzen ermittelt. Für die Identifizierung mehrerer Stoffe in einem Gemisch müssen im Wesentlichen alle Peaks der einzelnen Stoffe ebenfalls im Spektrum des Gemisches enthalten sein. Bei einer automatischen Auswertung schlägt das Programm im Gemisch enthaltene Stoffe vor. Dieses Ergebnis muss jedoch von einem Experten auf Plausibilität überprüft werden. Das Softwaretool ermöglicht des Weiteren eine zusätzliche manuelle Auswertung. Hierbei kann der Experte für die Auswertung weitere Spektren aus einer Datenbank mit dem aufgenommenen Spektrum vergleichen und prüfen, ob das vorgeschlagene Ergebnis korrekt ist bzw. weitere Stoffe enthalten sind. Das Ergebnis wird auf einer vom Fraunhofer FKIE entwickelten Benutzeroberfläche dargestellt.

Die Entwicklung des Softwaretools erfolgte in mehreren Stufen:

1) Entwicklung eines Verfahrens, mit dem die in den Messgeräten erzeugten Daten automatisch in ein geeignetes Format konvertiert und graphisch auf der Benutzeroberfläche angezeigt werden.
2) Entwicklung eines Algorithmus zur Identifizierung von Sprengstoffen bzw. Sprengstoffgemischen.
   a) Automatische Erkennung und Speicherung der in den Spektren vorhandenen Peaks.
   b) Automatische Identifizierung der Einzelkomponenten bzw. des Stoffgemisches. Das Softwaretool unterbreitet Vorschläge bzgl. der Zusammensetzung der untersuchten Probe.
   c) Manuelle Auswertung durch einen Experten:
      Der Experte kann zur Auswertung der IR- bzw. Raman-Spektren weitere Spektren aus der Spektrenbibliothek verwenden.
3) Darstellung des Ergebnisses auf einer Benutzeroberfläche.

Einsatz des Softwaretools

Die Messdaten (IR- und Raman-Spektren) werden von den Personen, die die Messung durchführen, in ein vom Projektpartner GITZ entwickeltes WEB-Tool eingestellt. Der Experte erhält eine Information über Telefon, SMS bzw. E-Mail, dass IR- und Raman-Daten zur Auswertung bereit stehen. Der Erhalt der Information muss vom Experten bestätigt werden. Der Experte kann aus dem WEB-Tool die Datei herunterladen, analysieren und das Ergebnis der Analyse ins WEB-Tool hinterlegen. Die Personen vor Ort erhalten automatische Nachricht, dass das Analysenergebnis vorliegt und können sich das Ergebnis im WEB-Tool ansehen.

Ergebnis

Konzeption und Entwicklung von Datenstrukturen und Algorithmen zur Identifizierung von Gefahrstoffen

Mit Hilfe der mobilen IR- bzw. Raman-Spektrometer wurden vom Projektpartner HBRS Spektren unterschiedlicher Sprengstoffe aufgenommen. Die Daten werden u.a. in ein TXT-Format im Spektrometer abgespeichert und werden auf eine externe Speicherkarte übertragen und in das von GITZ entwickelte WEB-Tool eingelesen. Das Fraunhofer FKIE verwendet diese Daten zur Auswertung.

Hinweis zur Nomenklatur von Sprengstoffen:

Die Nomenklatur gleicher Sprengstoffe bzw. von Sprengstoffgemischen können unterschiedlich sein. So werden z.B. für die Reinkomponente „Oktogen“ ebenfalls die Namen

- HMX
- LX 14-0

- HW 4

verwendet. Dies gilt ebenfalls für zahlreiche andere Sprengstoffe.

Im ersten Schritt wurde ein Verfahren entwickelt, das die in der TXT-Datei enthaltenen Daten extrahiert und für eine weitere Auswertung in ein geeignetes Datenformat konvertiert und graphisch darstellt (siehe Abbildung 23).

Für die Identifizierung von Stoffen anhand der Spektren muss die Lage und Größe der Peaks ermittelt werden. Ein weiterer entwickelter Algorithmus erkennt automatisch die Lage und Größe der Peaks (siehe Abbildung 23).

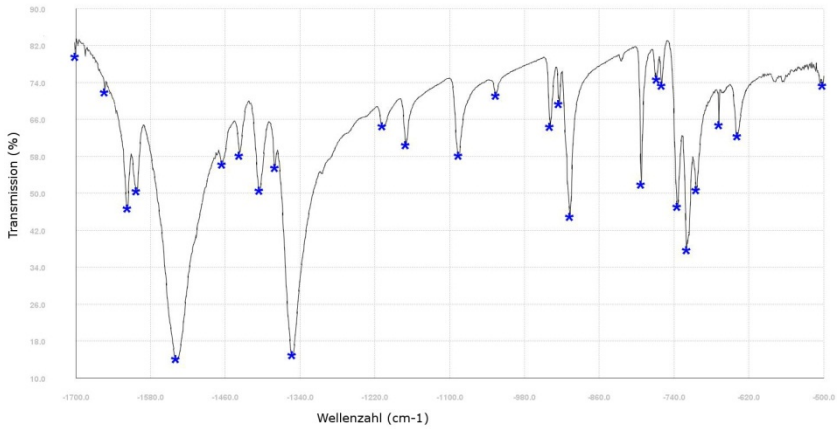

Abbildung 23: IR-Spektrum TNT – Ergebnis eines automatischen Einleseprozesses sowie graphische Darstellung und Erkennung der Peaks (* vom Algorithmus erkannte Peaks)

Diese Daten bilden die Grundlage der Entwicklung von Algorithmen zur Identifizierung von Stoffen. Bei den zu untersuchenden Stoffen kann es sich um einzelne „Reinstoffe“ wie z.B. TNT (Trinitrotoluol) oder um Stoffgemische wie z.B. TNT + RDX handeln. Eine Identifizierung von Stoffen ist in der Regel nur möglich, wenn die Spektren der Reinstoffe vorliegen. Die Spektren der Reinstoffe und Stoffgemische wurden vom Projektpartner HBRS aufgenommen und dem Fraunhofer FKIE zur Verfügung gestellt. Die Spektren der Reinstoffe werden in einer Datenbank (Spektrenbibliothek) im Softwaretool hinterlegt. Zunächst wurde ein Algorithmus programmiert, der die Peaks des Reinstoffs analysiert und mit den Peaks von Reinstoffen in einer Datenbank vergleicht. Im Falle einer Übereinstimmung der Peaks (Lage und Größe) zwischen Reinstoff und untersuchtem Stoff ist der Stoff eindeutig identifiziert. Dieses Prinzip der Auswertung kann sowohl für die IR- als auch die Raman-Spektren angewendet werden, so dass der entwickelte Algorithmus sowohl für die Auswertung von IR- und als auch für Raman-Spektren eingesetzt werden kann.

Für die Analyse von Stoffgemischen vergleicht der Algorithmus automatisch die Peaks von Stoffgemischen mit den Peaks von Reinsubstanzen und überprüft sie auf Übereinstimmungen. Hierbei muss berücksichtigt werden, dass in zwei verschiedenen Reinsubstanzen ein Teil der Peaks sich an der gleichen Stelle (Wellenzahl cm^{-1}) befinden können, während andere Peaks nur in einer Substanz enthalten sind. In Abbildung 24 sind beispielsweise charakteristische Signale für TNT mit einem blauen und für Tetryl mit einem grünen Pfeil markiert. Der überwiegende Teil der restlichen Peaks kommt durch eine Überlagerung der Peaks aus den Einzelsubstanzen bei gleicher Wellenzahl zustande. Zur Identifizierung der einzelnen Substanzen müssen alle Peaks herangezogen werden. Diese werden mit den Daten der Einzelkomponenten in der Datenbank verglichen. Der Algorithmus berücksichtigt dies und unterbreitet dem Experten Vorschläge über

die in der untersuchten Probe enthaltenen Substanzen.

Die in Frage kommenden Sprengstoffe werden zusammen mit dem Spektrum des unbekannten Stoffes graphisch dargestellt. Der Experte muss das vorgeschlagene Ergebnis überprüfen, indem er das Spektrum der Probe mit den Spektren der vom Tool vorgeschlagenen Stoffe vergleicht. Erkennt der Experte, dass möglicherweise bestimmte Stoffe nicht erkannt wurden, kann er selbst Spektren von Sprengstoffen aus der Bibliothek laden und mit dem gemessenen Spektrum vergleichen. Liegt eine Übereinstimmung des Spektrums aus der Bibliothek mit dem Spektrum der Probe vor, ist Substanz ebenfalls in der Probe enthalten.

Das gleiche Verfahren wird zur Auswertung von Raman-Spektren eingesetzt. In Abbildung 25 ist das Raman-Spektrum eines Gemisches von Ammoniumnitrat und Zucker dargestellt. Die charakteristischen Signale für Ammoniumnitrat sind mit grünen Pfeilen markiert. Alle wesentlichen Peaks des blauen Spektrums (Reinsubstanz Zucker) sind im Spektrum der Probe enthalten, so dass in der untersuchten Probe Ammoniumnitrat und Zucker enthalten ist.
Eine Quantifizierung einzelner Komponenten ist unter diesen Bedingungen nicht bzw. nur mit sehr hohem Aufwand möglich. Eine Voraussetzung hierfür ist, dass die Substanzgemische als homogene Mischungen vorliegen müssen bzw. eine hohe Anzahl an Messungen für eine statistische Auswertung erforderlich ist. Der Aufwand ist sehr hoch und stellt sehr hohe Anforderung an den Experten, die in der Regel nur bei Personen vorhanden ist, die häufig Quantifizierungen vornehmen. Der qualitative Nachweis von Sprengstoffen reicht in der Regel aus, um weitere Maßnahmen zu veranlassen.

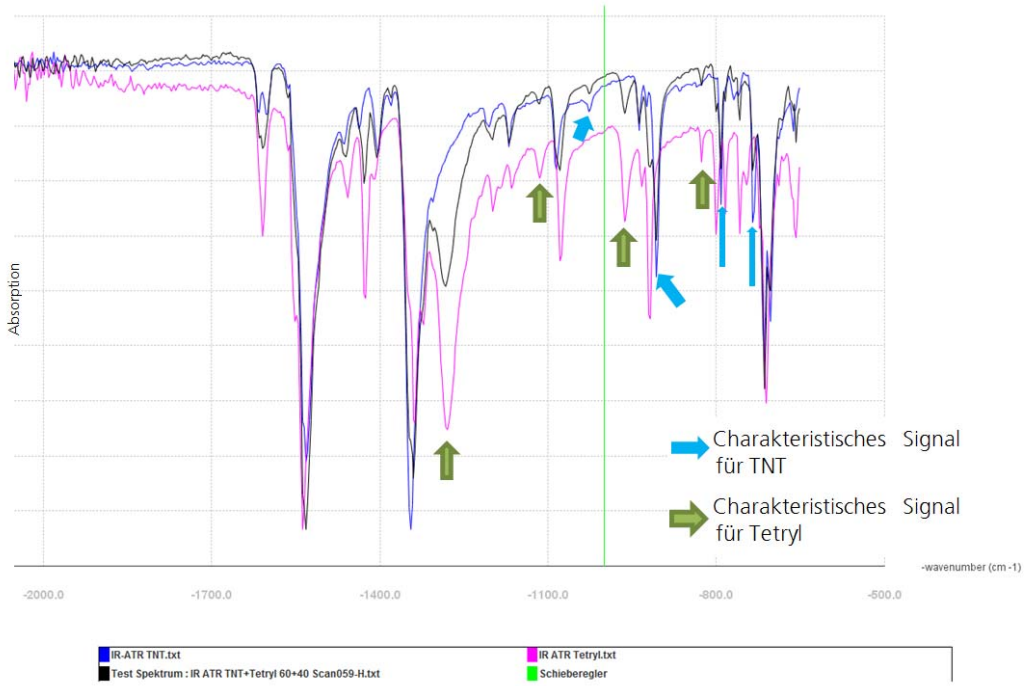

Abbildung 24: IR-Spektrum TNT-Tetryl-Gemisch sowie Spektren der Reinsubstanzen „TNT“ und „Tetryl“

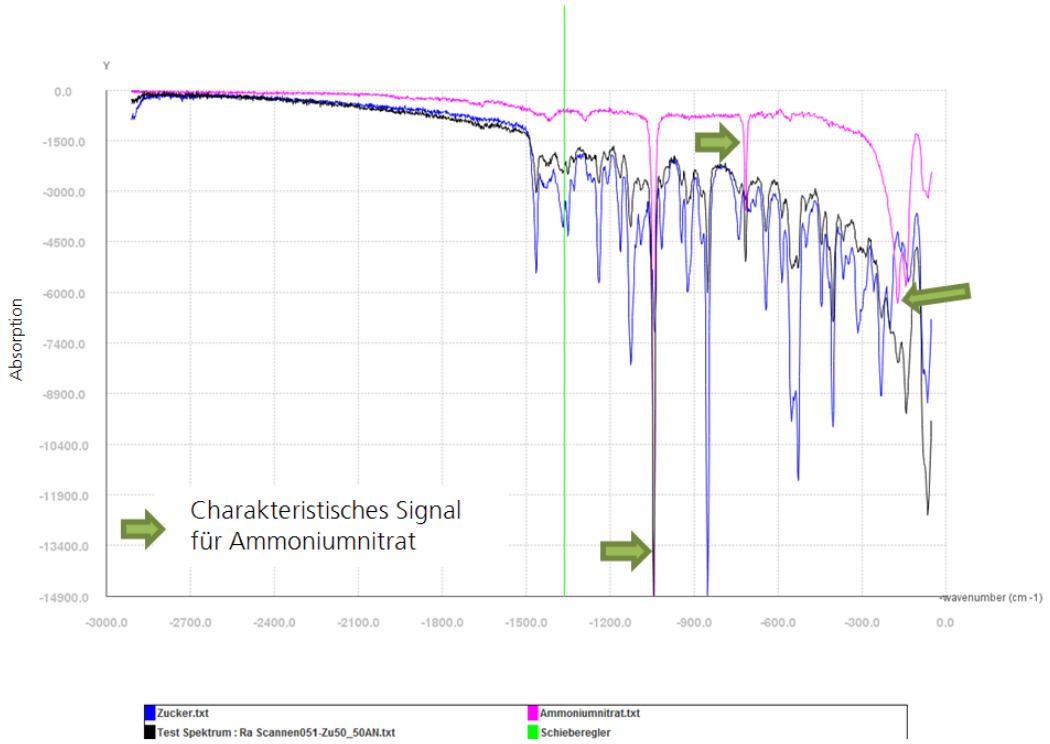

Abbildung 25: Raman-Spektrum Ammoniumnitrat-Zucker-Gemisch und Reinsubstanzen „Ammoniumnitrat“ und „Zucker“

Die Analyse der Spektren erfolgt in zwei Schritten. Im ersten Schritt werden die Peaks aus dem IR- bzw. Raman-Spektrum extrahiert und in einer Datenbank gespeichert. Werden reine Stoffe bzw. charakteristische Stoffgemische untersucht, können die in der Datenbank gespeicherten Daten als Referenzspektren für spätere Auswertungen genutzt werden. Bei der Analyse unbekannter Reinstoffe werden die einzelnen Peaks der unbekannten Verbindung im Spektrum extrahiert und mit denen in der Datenbank verglichen. Hierbei erfolgt ein Peak-zu-Peak-Vergleich (Probe/Referenzmaterial in der Datenbank). Der Algorithmus schlägt anschließend maximal fünf mögliche Substanzen vor. In diesem Schritt werden ausschließlich einzelne Peaks verglichen.

Für die Identifizierung von Stoffgemischen reicht ein Vergleich der Lage der einzelnen Peaks nicht aus. Es wurde ein Partikelfilter zur Schätzung der im Gemisch enthaltenen unbekannten Stoffe eingesetzt. Das speziell entwickelte statistische Verfahren wird in El Mokni (2014) im Detail erläutert.

Entwicklung einer Benutzeroberfläche zur Auswertung von IR- und Raman-Spektren

Es wurde eine Benutzeroberfläche zur Auswertung von Spektren entwickelt (siehe Abbildung 26). Die Daten von Infrarot- bzw. Ramanspektren werden über den Button „öffnen“ (Abbildung 26 – Nr.1) automatisch in das Auswertungstool eingelesen und grafisch dargestellt. Durch Betätigen des Buttons „Auswerten“ (Abbildung 26 – Nr.2) wird das IR- bzw. Raman-Spektrum ausgewertet und Vorschläge über in der Probe enthaltene Substanzen in der Tabelle (Siehe Abbildung 26 – Nr. 3) dargestellt. Die Spektren der Probe und die vorgeschlagenen Substanzen werden in unterschiedlicher farblicher Darstellung angezeigt (Abbildung 26 – Nr.5). Der Anwender kann sich die einzelnen Spektren durch Aktivierung bzw. Deaktivierung „Auswertung“ (Abbildung 26 – Nr. 3) anzeigen bzw. aus der Gesamtansicht entfernen. Es

können max. 5 Spektren automatisch aus der Datenbank angezeigt werden. Bei Bedarf kann der Anwender sich zusätzlich ein Spektrum aus der Datenbank „Beliebiges Spektrum anzeigen" darstellen lassen (Abbildung 26 – Nr. 4) und somit evtl. weitere, nicht automatisch erkannte Substanzen identifizieren.

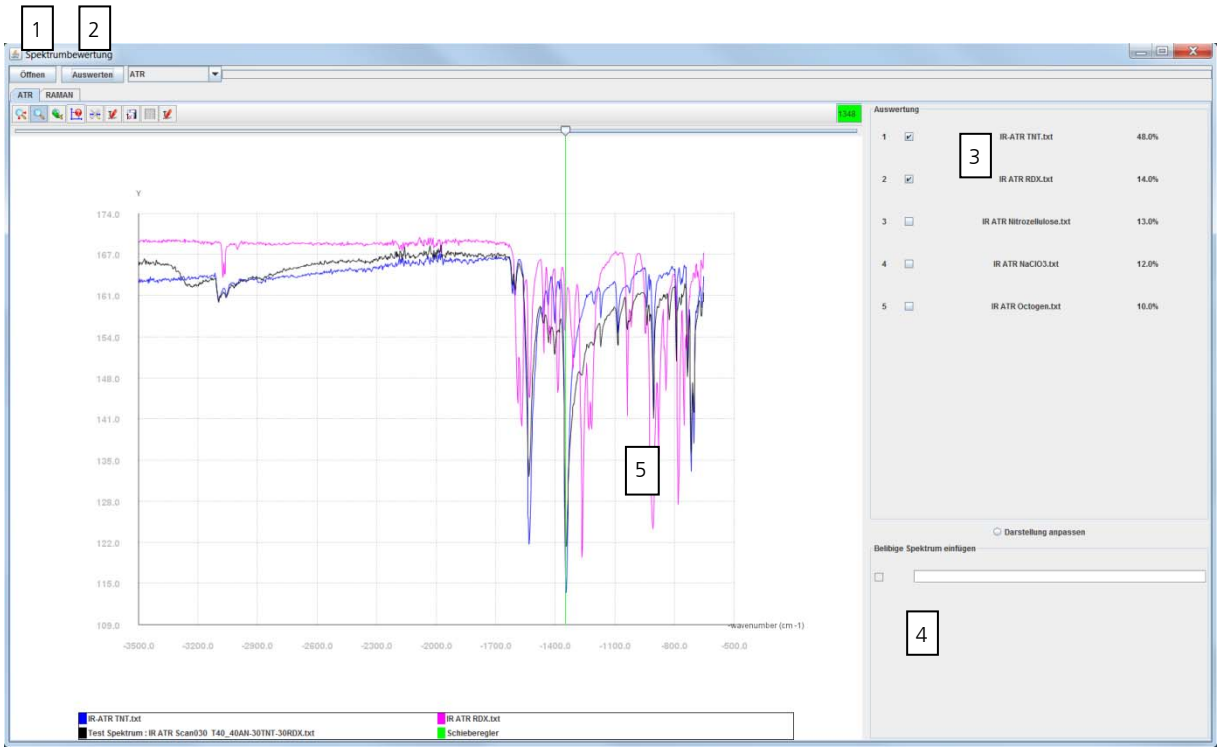

Abbildung 26: Benutzungsoberfläche – Auswertung und Darstellung von IR- bzw. Raman-Spektren

Test, Evaluierung und Demonstration des Unterstützungssystems

Test

Während der Entwicklung der Algorithmen wurden zahlreiche IR- und Raman-Spektren unterschiedlicher Sprengstoffe verwendet. Beim Test der Algorithmen wurden IR- und Raman-Spektren unterschiedlicher Sprengstoffe und Sprengstoffgemische ausgewertet. Die Ergebnisse dieser Tests wurden zur Weiterentwicklung und Optimierung der Algorithmen verwendet.

Evaluierung

Zur Evaluierung wurden Sprengstoffgemische unterschiedlicher Zusammensetzung untersucht. Hierbei zeigte sich, dass die Hauptkomponenten der Sprengstoffe in der Regel identifiziert werden konnten. Einzelkomponenten in geringen Konzentrationen (<15%) in Sprengstoffgemischen konnten nicht in allen Fällen nachgewiesen werden.

Präzise Angaben, ab welcher Konzentration welche Sprengstoffe nicht mehr nachweisbar sind, können nicht gemacht werden, da dies von der Zusammensetzung der gesamten Probe abhängig ist. Ein weiterer Einflussparameter stellt die Homogenität der Probe dar. Homogene Feststoffgemische selbst herzustellen ist relativ schwierig. Da die für die Untersuchung benötigte Probenmenge sehr gering ist, können bei nicht homogenen Gemischen die Messergebnisse unterschiedlicher Proben aus dem Gemisch zu Abweichungen in der Größe der Peaks führen. Die Größe der Peaks ist ein Maß für die in der Probe enthaltene Menge an einer oder mehreren Substanzen. Dies kann dazu führen, dass eine Identifizierung aufgrund der sehr geringen Menge nicht mehr möglich ist, wenn ohnehin eine Komponente in geringen Mengen im Gemisch

enthalten ist und zufällig eine Probe an der Stelle genommen wurde, wo die Mischung noch weniger an dieser Verbindung enthält.

Demonstration

Das Fraunhofer FKIE hat in Zusammenarbeit mit dem Projektpartner HBRS eine Datenbank mit IR- und Raman-Spektren von Sprengstoffen und Zusatzstoffen wie z.B. Mehl und Zucker angelegt. Im Rahmen des Projektes konnten nur die gängigen Sprengstoffe in die Datenbank aufgenommen werden. Diese wurden für die Auswertung verwendet.

Der Projektpartner HBRS hat dem Fraunhofer FKIE die Messdaten (IR- und Raman-Spektren) von zehn Proben im WEB-Tool zur Verfügung gestellt. Diese Proben konnten nur mit Hilfe der Messgeräte nicht identifiziert werden. Der Projektpartner HBRS hat dem Fraunhofer FKIE telefonisch über das Vorliegen von Spektren zur Analyse informiert. Dem Fraunhofer FKIE lagen keine Informationen seitens des Projektpartners HBRS über die Zusammensetzung der Proben vor.

Das Fraunhofer FKIE hat die Spektren aus dem Internet heruntergeladen und mit Hilfe des entwickelten Tools ausgewertet. Das Ergebnis wurde über das Web-Tool zurückgemeldet und ist in der Abbildung 27 dargestellt. In der Spalte „Ergebnis SDF-Tool-IR“ bzw. „Ergebnis SDF-Tool-Raman“ wurde das vom Fraunhofer FKIE ermittelte Ergebnis eingetragen.

Die Auswertung der IR-Spektren lieferte präzisere Ergebnisse als bei den Raman-Spektren. Beim IR-Spektrum „Scan011“ (Fahrzeug 333) konnte Ammongelit nachgewiesen werden, während die Auswertung des Raman-Spektrums „Scan009“ lediglich Hinweise auf Ammongelit bzw. Ammoniumnitrat gab. Bei der Analyse des IR- und Raman-Spektrums konnten bei der Auswertung des IR-Spektrums 3 Substanzen (TNT/RDX/PETN) nachgewiesen werden, während es bei der Auswertung des Raman-Spektrums nur einen Hinweis auf TNT gab. Beim Ergebnis „kHS“ konnte das Tool keine Substanzen nachweisen, da sie nicht in der Datenbank enthalten waren. Das Raman-Spektrum „Scan16“ (Fahrzeug 999) konnte nicht ausgewertet werden. Das automatische Einlesen der Daten in das Softwaretool war nicht möglich. Die Datei war möglichweise beschädigt oder unvollständig.

Die Auswertung der 10 Proben hat ergeben, dass in 5 Proben, in denen Sprengstoffe enthalten waren, diese nachgewiesen werden konnten. In den restlichen 5 Proben (enthielten keine Sprengstoffe) wurden keine Sprengstoffe nachgewiesen. Eine Identifizierung der „Nicht-Sprengstoffe“ war nicht möglich, da diese Verbindungen nicht in der Datenbank enthalten waren.

Nummer Fahrzeug	Substanz	FT-IR Spektrum	Raman-Spektrum	Ergebnis SDF-Tool IR	Ergebnis SDF-Tool Raman
111	2-Amino-4,6-Dinitrotoluol	Scan010	Scannen007	kHS	kHS
222	Ammongelit (Dynamit)	Scan009	-	Ammongelit[1)]	---
333	Ammongelit (Dynamit)/2A-4,6-DNT (80/20 ww)	Scan011	Scannen009	Ammongelit[1)]	Hinweis auf Ammongelit[1)]/ Ammoniumnitrat
444	$KClO_4/NaClO_3$ (50/50, ww)	Scan012	-	$NaClO_3$	---
555	$Ca(NO_3)_2/KClO_4/NaClO_3$ (20/40/40, ww)	Scan013	Scannen012	$NaClO_3$	$NaClO_3$
666	TNT/RDX/PETN/2A-4,6-DNT (30/30/30/10)	Scan014	Scannen014	TNT/RDX/PETN	Hinweis auf TNT
777	$KClO_4$ (Kaliumperchlorat)	-	Scannen10	---	kHS
888	Harnstoffnitrat (feucht)	Scan15	Scanen15	kHS	Daten nicht auswertbar
999	CL-20	Scan16	Scanen16	kHS	kHS
1000	Dimethylnaphtalin (Isomerengem.)	Scan17	-	kHS	---

[1)] Wenn typische Sprengstoffgemische in der Datenbank berücksichtigt werden, erkennt das Tool diese Stoffe als Stoffgemisch

kHS = Datenbank: Kein Hinweis auf Sprengstoff

Abbildung 27: Untersuchung von in Testmischungen enthaltenen Sprengstoffen/sonstige Stoffe

B.1.5 AP 3.1: Definition von Präventiv-/Notfallmaßnahmen und -abläufen an Bord

Das Ziel der Arbeiten in AP 3.1.1 (Situationsabhängige Spezifikation von Präventiv- und Notfallmaßnahmen und -abläufen) war es, im Gegensatz zu abstrakt formulierten Maßnahmen zur Gefahrenabwehr im ISPS-Code konkrete Präventiv- und Notfallmaßnahmen und -abläufe für Security-Vorfälle an Bord zu definieren, mit dem Zweck, diese in einem Entscheidungsunterstützungssystem (EUS) umzusetzen.

Folgende Arbeiten wurden durchgeführt:

- Der Katalog der Präventiv- und Notfallmaßnahmen und -abläufe wurde erstellt,
- Anforderungen an die Integration der Maßnahmen in ein EUS wurden spezifiziert und der Anforderungskatalog entsprechend ergänzt,
- Szenarien, die für die Spezifikation der Maßnahmen definiert wurden, wurden entwickelt und für den Einsatz im Trainingsmodul eines EUS angepasst.

Maßnahmen wurden situationsabhängig, basierend auf ausgewählten Szenarien zu verschiedenen Security-Vorfällen spezifiziert. Folgende Szenarien wurden verwendet:

- Sprengsatz in einem Fahrzeug,
- Bombendrohung/Bombensuche,
- ein sich auffällig verhaltender Passagier,
- Schiffsentführung durch Passagiere.

Diese Szenarien sind dazu vorgesehen, in einem EUS integriert und beim Training eingesetzt zu werden. Hierfür werden zu jedem Szenario verschiedene Verläufe definiert sowie Trainingsziele zugeordnet. Die Zuordnung der Trainingsziele zu den Szenarien/Maßnahmen soll es ermöglichen, das Training entsprechend den jeweiligen Trainingszielen zu gestalten.

Für jedes Szenario wurden benötigte Maßnahmen und Abläufe zur Vorfallbekämpfung basierend auf einschlägigen Dokumenten definiert. Die Szenarien wurden in einem Gespräch mit den Sicherheitsbeauftragten der Reedereien Scandlines und TT-Line validiert und an die Anforderungen der Reedereien angepasst.

Der Maßnahmenkatalog beinhaltet folgende Informationen für jedes Szenario:

- Beschreibung eines Szenarios,
- Mögliche Verläufe/Modifikationen des Szenarios,
- Maßnahmen und Abläufe zur Vorfallbekämpfung, die dem Szenario zugeordnet werden,
- Trainingsziele laut des ISPS-Codes (Verordnung (EG) Nr. 725/2004, 2004), die dieses Szenario unterstützt.

Maßnahmen wurden den vier Gruppen zugeordnet:

- Vorbeugende Maßnahmen,
- Maßnahmen bei verdächtigen Personen, Handlungen, Gegenständen,
- Maßnahmen bei Drohungen, erhöhter Gefahr eines kritischen Ereignisses,
- Maßnahmen bei akuten Gefahren für die Menschen/das Schiff.

Anforderungen an die Visualisierung der Maßnahmen im EUS wurden an die konkret definierten Maßnahmen angepasst und im Maßnahmenkatalog festgehalten.

Der Maßnahmenkatalog befindet sich im Anhang.

B.1.6 AP 3.3: EUS für Trainingszwecke

Das Ziel der Arbeiten im Arbeitspaket AP 3.3.1 (Entwicklung eines integrierten Design-Konzepts für ein Entscheidungsunterstützungs- und Trainingssystem) war es, ein EUS-/Trainingskonzept zu erstellen, um das EUS für den Einsatz beim Training anzupassen. Es sollte untersucht werden, wie ein EUS auf Schiffsbrücken für das Training eingesetzt werden kann.

Es wurde eine methodische Vorgehensweise entwickelt, um ein System zur effektiven Entscheidungsunterstützung und zum Training entwickeln und evaluieren zu können. Der im Projekt VESPER entstandene Anforderungskatalog für ein Security-EUS wurde um die Anforderungen an eine Trainingskomponente ergänzt.

Problembeschreibung

Ein EUS, das Entscheidungsträger im Krisenfall unterstützen soll, kann auch zum Training der entsprechenden Expertise benutzt werden: ein Konzept, das bislang nur im militärischen Bereich Anwendung fand (Cohen et al., 1997, Morrison et al., 1998). Das Modul für Training wurde als Bestandsteil eines Security-EUS konzipiert, um vom Ship Security Officer (SSO), Kapitän oder einer anderen für das Training auf dem Schiff verantwortlichen Person benutzt zu werden.

Training zur Bewältigung von Krisensituationen besitzt eine große Bedeutung, da hierdurch Kenntnisse und Fähigkeiten erlernt werden, die im realen Leben nicht ohne weiteres zu erwerben sind. Design von EUS für eine schnelle und effektive Reaktion in kritischen Situationen sowie das Design von Trainingsmethoden, um Entscheidungsfertigkeiten zu entwickeln und auszubauen, müssen aufeinander abgestimmt sein. Einerseits führt das Training der Fertigkeiten zur Bewältigung sicherheitskritischer Entscheidungssituationen mit Hilfe eines EUS dazu, dass der Umgang mit dem System gelernt wird und somit in realen Situationen ein sicherer Umgang mit ihm gewährleistet ist. Andererseits kann ein EUS das Training unterstützen, indem es als interaktives Werkzeug Krisensituationen simuliert und somit einen Trainingseffekt bewirken kann. Über die Möglichkeit der Aufzeichnung von Benutzerinteraktionen mit dem System ist zudem eine lückenlose Evaluation und Nachbereitung der durchgeführten Szenarien möglich. Zusammenführen vom EUS und Trainingssystem in einer Anwendung bringen außerdem Vorteile mit sich, wie das Nutzen der gleichen Funktionen sowie der Zugriff auf den gleichen Datenbestand. Daher wird die Entwicklung eines integrierten Konzepts für das Design von EUS und Training angestrebt.

Entwicklung eines integrierten Konzepts (Vorgehensweise)

Um ein integriertes Konzept für EUS und Training zu entwickeln, wurde als erstes untersucht, wie Methoden des Cognitive Systems Engineering (CSE, Rasmussen et al., 1994) angewandt werden können, damit die Anforderungen an ein EUS um die Anforderungen an ein Trainingssystem ergänzt werden können und somit ein ganzheitliches Konzept zur Entscheidungsunterstützung an Bord erarbeitet werden kann. CSE ist ein Design-Framework, das sich mit der Analyse kognitiver Anforderungen beschäftigt. Methoden des CSE helfen zu verstehen, was Experten über ihr Arbeitsgebiet wissen, wie und warum sie bestimmte Entscheidungen treffen, welche Hinweise sie bei der Entscheidungsfindung benötigen, welches Wissen und Strategien sie dabei benutzen.

CSE-Methoden werden meistens in Arbeitsdomänen angewandt, die seit geraumer Zeit existieren und wo Expertenwissen abgefragt werden kann und es lange bestehende Arbeitsabläufe gibt. In neuen, sich in Entstehung befindlichen Arbeitsdomänen gibt es selten Expertenwissen, Informationen über diese Domänen beschränken sich auf Vorschriften und Arbeitsanweisungen. Solche Dokumente können keinen Einblick in die Arbeitsweise eines Entscheidungsträgers geben, darüber wie er denkt und welche Strategien er verfolgt. Um dies zu verstehen wurden nachfolgend beschriebene Methoden angewandt.

Work Domain Analysis (WDA) ist eine Methode des CSE, die eine funktionale Beschreibung einer Arbeitsdomäne liefert und benutzt werden kann, um ein System zu entwickeln, das nicht

nur Unterstützung in einer konkreten Situation sondern auch in unvorhergesehen Situationen liefert. Mit Hilfe der WDA kann man darüber hinaus sowohl den Trainingsbedarf als auch die Anforderungen an das Trainingssystem definieren (Naikar & Sanderson, 1999).

Um ein Vorgehen zur Definition von Anforderungen an ein Trainingssystem entwickeln zu können, wurden die Besonderheiten des Trainings zur Entscheidungsfindung in Krisensituationen betrachtet. Um in Krisensituationen richtig zu reagieren, braucht man Techniken, die nicht auf die Ausführung bekannter Handlungen basieren, sondern die kognitiven Anforderungen der Krisensituationen berücksichtigen. In unvorhergesehenen Situationen können Menschen nicht immer auf vordefinierte Handlungsanweisungen zurückgreifen. Um effektiv mit solchen Situationen umgehen zu können, sind Fähigkeiten zur kreativen Problemlösung und Entwicklung neuer Verhaltensmuster notwendig. Das Training muss dabei mehr beinhalten, als nur den beschriebenen Handlungsanweisungen zu folgen und einzelne Maßnahmen sowie deren Reihenfolge zu lernen. Es muss gelernt werden, wie Änderungen der Situation rechtzeitig erkannt, wie auf sie reagiert werden kann und wie Maßnahmen entsprechend angepasst werden können. Das Design des Trainingssystems muss daher die kognitiven Anforderungen der Arbeitsumgebung beachten (Naikar, 2006). Ein Trainingsprogramm soll sich in diesem Fall nicht auf Routinehandlungen fokussieren, sondern vielmehr ein flexibles Problemlösungsverhalten fordern.

Um eine WDA durchzuführen, wurde die Abstraktionshierarchie nach Rasmussen (1994), welche die menschliche Informationsverarbeitung beschreibt, verwendet. Die Abstraktionshierarchie beinhaltet folgende Ebenen (beginnend mit der obersten Hierarchie-Ebene):

- Funktionaler Zweck (wozu dient das System?)
- Abstrakte Funktion (kausale Struktur des Prozesses)
- Generalisierte Funktion (grundlegende Funktionen des Systems)
- Physikalische Funktion (Beschreibung einzelner Komponenten und der Verbindungen zwischen ihnen)
- Physikalische Form (physisches Erscheinungsbild und Lage einzelner Komponenten)

Zum besseren Verständnis der Anforderungen der Arbeit in Krisensituationen wurde die Naturalistische Entscheidungstheorie (Naturalistic Decision Making, NDM; Klein, 1998, Orasanu et al., 1993) herangezogen. NDM betrachtet lebensnahe Entscheidungen in komplexen und sicherheitskritischen Situationen, die unter hohem Zeitdruck getroffen werden müssen. Sie eignet sich somit nicht nur zur Definition der Anforderungen an ein EUS in Security relevanten Krisensituationen, sondern auch zur Definition der Anforderungen für ein Trainingssystem zum Erlernen der Entscheidungsfindung in Krisensituationen. Eines der Modelle des NDM ist das Recognition-Primed Decision Model (RPD, erkennungsbasierte Entscheidungsfindung, Klein, 1998), das den Prozess der Entscheidungsfindung in Krisensituationen beschreibt. Der Prozess der Situationserkennung beinhaltet folgende Phasen:

- Erkennen der Ziele (Prioritäten setzen),
- Auswählen der relevanten Hinweise,
- Prüfen der Erwartungen (was als Nächstes zu erwarten ist, um sich vorzubereiten),
- Ableiten der Handlung (typische Reaktion in dieser Situation).

Die Handlungsweise wird mit Hilfe der mentalen Simulation evaluiert. Wenn durch die mentale Simulation klar wird, dass Schwierigkeiten bei der Durchführung der Handlung zu erwarten sind, muss die Handlungsweise angepasst werden oder eine neue Handlungsalternative überlegt werden.

Mit Hilfe des RPD-Modells können die Phasen des Prozesses der Entscheidungsfindung, die vom System unterstützt werden sollen, identifiziert werden und so die kognitiven Anforderungen einer neuen Arbeitsdomäne beschrieben werden. Auf der anderen Seite liefert die WDA eine

Struktur der Arbeitsdomäne und damit auch Verständnis wie ein RPD-Modell implementiert werden soll. Mit der Hilfe der WDA und RPD wurde eine methodische Vorgehensweise für das Design eines Entscheidungsunterstützungs- und Trainingssystems entwickelt. Die Kombination dieser beiden Techniken macht es möglich, eine Analyse einer sich noch in Entstehung befindlichen Arbeitsdomäne zu machen. Um Design-Anforderungen zu definieren wurde die Applied Cognitive Work Analysis (ACWA, Elm et al., 2003, Potter et al., 2003) verwendet.

Ergebnisse

Folgende Ergebnisse wurden im Projekt erzielt:

- Mit Hilfe des CSE-Ansatzes wurde eine methodische Vorgehensweise entwickelt, um ein System zur effektiven Entscheidungsunterstützung und zum Training entwickeln und evaluieren zu können.
- Eine funktionale Beschreibung der Arbeitsdomäne „Bewältigung von Security relevanten Vorfällen auf Fährschiffen" (Dalinger & Motz, 2010, Dalinger & Ley, 2011), die als Basis zur Definition von Design-Anforderungen an ein Security-EUS diente, wurde erweitert und angepasst, um Anforderungen an ein Trainingsmodul definieren zu können. Eine Beschreibung der Arbeitsdomäne "Entscheidungsfindung in kritischen Situationen" (s. Tabelle 5) wurde erstellt. Damit wurden Anforderungen an das EUS und an den Trainingsbedarf definiert. Eine Beschreibung der Arbeitsdomäne "Training der Entscheidungsfindung in kritischen Situationen" (Tabelle 6) diente dazu, Design-Anforderungen an das Trainingssystem zu definieren.
- Basierend auf Ergebnissen der Analyse wurde ein Anforderungskatalog für ein Trainingsmodul eines Security-EUS an Bord von Schiffen erstellt (s. Anhang) und vom Projektpartner „MARSIG" in einem Demonstrator umgesetzt.

Tabelle 5: Beschreibung der Arbeitsdomäne "Entscheidungsfindung in kritischen Situationen".

RPD-Modell / Abstraktionshierarchie	Erkennen der Situation				Mentale Simulation
	Ziele	**Erwartungen**	**Hinweise**	**Handlungen**	
Zielsetzung	Ziele beachten (wie z.B. Sicherheit des Lebens gewährleisten)		Vorgaben der Reederei und Behörden erfüllen	Gefahrenabwehr planen	Gefahrenabwehr evaluieren
Vorrangige Maßnahmen	Situation und deren Änderungen erfassen	Erwartungen definieren	Relevante Hinweise wählen	Handlungsplan implementieren	
Überwachung, Planung, Kontrolle	Maßnahmenumsetzung beobachten	Verlauf des Vorfalls überwachen	Probleme mit dem Handlungsplan feststellen	Handlungsplan ausarbeiten	Handlungsplan evaluieren
Informationsverarbeitung, Analyse, Kommunikation	Informationen verwalten Security-Ereignis klassifizieren Dokumentation erstellen			Kommunikation erfolgreich bewältigen Handlungsmöglichkeiten bestimmen/Ressourcen verwalten	Plan anpassen
Komponenten	Sensorinformationen/Informationen über die Infrastruktur liefern				

Tabelle 6: Beschreibung der Arbeitsdomäne "Training der Entscheidungsfindung in kritischen Situationen"

<table>
<tr><th rowspan="2">RPD-Modell
Abstrak-tionshierarchie</th><th colspan="4">Erkennen der Situation</th><th rowspan="2">Mentale Simulation</th></tr>
<tr><th>Ziele</th><th>Erwartungen</th><th>Hinweise</th><th>Handlungen</th></tr>
<tr><td>Trainingsziele</td><td>Klassifikation der Schlüssel-ereignisse lernen</td><td>Reaktion auf Änderungen der Situation trainieren</td><td>Lernen, wie man Hinweise erkennt</td><td>Lernen, wie man Handlungen/ Ressourcen auswählt</td><td>Treffen von Entschei-dungen üben</td></tr>
<tr><td>Entwicklung von Szenarien</td><td>Schlüssel-ereignisse für ein Szenario auswählen</td><td>Änderungen des Szenarios generieren (zusätzliche Ereignisse oder besondere Bedingungen)</td><td>Informationen über den Vorfall liefern</td><td>Maßnahmen wählen, die zu trainieren sind, Ressourcen wählen, die benutzt werden sollen</td><td>Entschei-dungspunkte definieren</td></tr>
<tr><td>Leistungs-bewertung</td><td>Ereignisse richtig erkennen</td><td>Änderungen der Situation rechtzeitig erkennen</td><td>Hinweise richtig erkennen</td><td>Maßnahmen rechtzeitig implementieren,
adäquate Ressourcen benutzen</td><td>Notwendige Entschei-dungen treffen</td></tr>
<tr><td rowspan="2">Datenerfassung</td><td colspan="3">Erfasse Hinweise zum Erkennen der Situation</td><td>Vordefinierte und umgesetzte Handlungen vergleichen
Bestimmen der Fertigstellung/ Reihenfolge der Handlungen</td><td>Erfasse getroffene Entschei-dungen</td></tr>
<tr><td colspan="5">Erfasse Daten über Zeitpunkt/Zeitfenster/Dauer der Maßnahmen</td></tr>
<tr><td>Simulierte Komponenten, Ressourcen</td><td colspan="3">Notwendige Simulationen bereitstellen</td><td>Menschliche/ technische Ressourcen zuweisen</td><td></td></tr>
</table>

Zur Entwicklung eines integrierten EUS-/Trainingskonzepts wurde als erstes eine Bestandsaufnahme zur Erfassung des Ist-Standes der vorhandenen Trainingsabläufe durch die Begleitung von Übungen an Bord und durch die Analyse der Anforderungen des ISPS-Codes (Verordnung (EG) Nr. 725/2004), sowie anderer relevanter Dokumente durchgeführt. Außerdem wurden Interviews mit den Sicherheitsbeauftragten der Reedereien Scandlines und TT-Line durchgeführt, um die Trainingsabläufe an Bord zu erfassen. Anschließend wurden der Trainingsbedarf und die Trainingsanforderungen mit Hilfe der oben vorgestellten Methode definiert. Dabei galt es, diverse Faktoren wie organisationale Ziele, Ressourcen und Besonderheiten der Krisenereignisse zu berücksichtigen. Die notwendigen kognitiven Schlüsselfähigkeiten und Kenntnisse, die einen erfahrenen Entscheidungsträger ausmachen, z.B. Situationsverständnis, Fähigkeit zur Problemlösung, Wissen über Gegenmaßnahmen, Infrastruktur, Dokumentations- und Kommunikationsroutinen, wurden identifiziert.

Es wurden folgende Möglichkeiten der Anwendung eines Trainingsmoduls identifiziert:

- Computerbasiertes Training (Simulation) für Entscheidungsträger (Verantwortliche Offiziere, wie Ship Security Officer, sein Stellvertreter, Kapitän). Dieses Training setzt eigenständiges Lernen voraus.
- Unterstützung des SSO beim Organisieren/Vorbereiten des Trainings für die Schiffsbesatzung. Dieses Training kann als ein Seminar oder eine Planübung, in der bestimmte Situationen durchgesprochen werden, ablaufen.
- Einsatz bei Übungsplanung und -durchführung (bei vorgeschriebenen Security-Übungen an Bord).

Der Schwerpunkt der Untersuchung wurde auf den Einsatz bei Übungsplanung und -durchführung gelegt, da die Notwendigkeit der Unterstützung in diesem Bereich als groß angesehen wurde.

Folgende Trainingsphasen wurden identifiziert, die vom System unterstützt werden können:

- Planung des Trainings,
- Durchführung des Trainings (Simulationen, Datenerfassung für die Leistungsbewertung, Überwachung des Trainingsablaufs),
- Dokumentation und Evaluation des Trainings.

Besonders wichtig ist sowohl für das EUS als auch für das Trainingssystem die Bereitstellung von Informationen. Informationen sollen leicht zu finden sein, entsprechende Suchroutinen sollen implementiert werden. Die Funktionen, die im EUS implementiert sind, können vom Trainingssystem benutzt werden. Zum Beispiel können im EUS vorhandene Informationen über mögliche Ereignisse und Gegenmaßnahmen genutzt werden, um Trainingsszenarien zu entwickeln und Handlungen, die trainiert werden müssen, zu bestimmen. Außerdem kann man während des Trainings die Handhabung des EUS verbessern. So können Kommunikations- und Dokumentationsanforderungen gelernt werden, indem man während des Trainings die im EUS implementierten Funktionen nutzt.

Ein Trainingssystem soll insbesondere folgende Funktionen bereitstellen:

- Definition der Trainingsszenarien,
- Auswahl der Trainingsszenarien über die Trainingsziele,
- Feststellung der Gegenmaßnahmen, die zu trainieren sind,
- Definition der Leistungskriterien, um die Trainingsergebnisse zu erfassen,
- Auswahl der Ressourcen, die für das Training notwendig sind.
- Datenerfassung für die Leistungsbewertung.

Im Arbeitspaket 3.3.4 (Evaluation des Trainingskonzepts) wurde das Trainingskonzept evaluiert. Der Einsatz eines EUS beim Training soll die Trainingsqualität und die Handhabung von EUS verbessern. Der Akzent bei der Evaluation des Trainingskonzepts lag auf der Untersuchung der Unterstützung bei der Planung, Durchführung und Auswertung von vorgeschriebenen ISPS-Übungen an Bord.

Es wurde eine Usability-Evaluation mit potentiellen Nutzern durchgeführt. Ein EUS-Demonstrator mit einem integrierten Trainingsmodul wurde für die Evaluation genutzt. Die Gebrauchstauglichkeit des Systems wurde getestet, um das Design zu verbessern. Folgende Methoden wurden dabei angewandt:

- Methode des Lauten Denkens, Beobachtung,
- Usability-Fragebögen: System Usability Scale (SUS), Isometrics,
- ZEIS-Fragebogen zum Grad der Beanspruchung.

Die bei der Untersuchung benutzten Fragebögen findet man in Anhang.

Folgende Anforderungen wurden an Testpersonen gestellt: nautische Offiziere mit Brückenerfahrung, Kenntnisse des ISPS-Codes.

Evaluiert wurden drei Trainingsphasen, die durch das EUS unterstützt werden:

- Planen einer Übung,
- Durchführen einer Übung,
- Evaluation der Ergebnisse und Dokumentation.

Die Versuchspersonen hatten die Aufgabe, als Ship Security Officer (SSO) eine ISPS-Übung an Bord mit Hilfe des EUS zu planen, auszuführen und zu evaluieren. Das benutzte Szenario war „Bombendrohung" mit einem simultanen Ereignis „verdächtige Person". Die Aufgabe wurde in zwei Teile eingeteilt:

- Planen einer Übung,
- Durchführen einer Übung mit Evaluation der Ergebnisse.

Dabei wurden die von den Versuchspersonen durchgeführten Aufgaben mit einer Musterlösung verglichen und Abweichungen dokumentiert, um mit deren Hilfe eventuelle Fehler/Inkonsistenzen im System zu finden und notwendige Änderungen am System zu definieren. Diese werden vom Projektpartner „MARSIG" umgesetzt.

B.1.7 AP 3.4: EUS-Einsatz zur Koordination der Maßnahmen durch die Reederei

Im Teilarbeitspaket 3.4.2 (Erstellung eines Konzepts für den EUS-Einsatz zur Koordination der Maßnahmen durch die Reederei) wurde untersucht, wie ein EUS zur Koordination der bordseitigen Maßnahmen durch die Reederei eingesetzt werden kann. Das System soll bei der Notfallbekämpfung die Kommunikation und die Koordination der Abläufe auf dem Schiff durch die Reederei mit Hilfe der Online-Datenübertragung zwischen dem EUS an Bord und einem Modul des EUS in der Reederei ermöglichen. Dazu wurden Anforderungen für die Anpassungen am bordseitigen EUS, sowie für ein Modul des EUS zum Einsatz in der Reederei definiert.

Folgende Arbeiten wurden durchgeführt:

- Ein Anforderungskatalog für den EUS-Einsatz zur Koordination der Maßnahmen durch die Reederei wurde erstellt. Dabei wurden zusätzliche Komponenten, um die ein Security-EUS erweitert werden soll (wie z.B. Anzeige der Verbindungsdaten) beschrieben und Anforderungen an die Benutzungsoberfläche definiert. Diese werden vom Projektpartner „MARSIG" umgesetzt.
- Anforderungen an die Datenübermittlung, wie Zeitpunkt, Art der Daten, Anzeigemöglichkeiten, wurden definiert.
- Anforderungen an das bordseitige EUS wurden entsprechend den Änderungen, die durch die Interaktion mit dem Reederei-Modul entstehen, angepasst.

Zur Beschreibung der Arbeitsdomäne „Hilfestellung in kritischen Situationen" (Tabelle 7) wurde die bereits beschriebene Vorgehensweise verwendet.

Tabelle 7: Beschreibung der Arbeitsdomäne "Hilfestellung in kritischen Situationen".

RPD-Modell / Abstraktionshierarchie	Erkennen der Situation				Mentale Simulation
	Ziele	Erwartungen	Hinweise	Handlungen	
Zielsetzung	Unterstützung des Schiffs bei der Krisenbewältigung		Zusammenarbeit mit den verantwortlichen Behörden		Gefahrenabwehr evaluieren
Vorrangige Maßnahmen	Ermöglichung des Datenaustausches mit dem Schiff	Erwartungen definieren	Empfehlungen den Verantwortlichen auf dem Schiff geben	Handlungsplan implementieren	
Überwachung, Planung, Kontrolle	Verfolgung der Maßnahmenumsetzung auf dem Schiff	Verlauf des Vorfalls überwachen	Informationen vom Schiff analysieren	Handlungsplan ausarbeiten	Handlungsplan evaluieren
Informationsverarbeitung, Analyse, Kommunikation	Aktuelle Informationen zum Vorfall vom Schiff empfangen Informationen vom Schiff an die Behörden weiterleiten Informationen von den Behörden an das Schiff weiterleiten			Kommunikation erfolgreich bewältigen	Plan anpassen
Komponenten	Verschiedene Kommunikationswege bereitstellen Verwaltung und Auswahl geeigneter Kommunikationskanäle Daten senden und empfangen			Kontakt mit den Behörden ermöglichen	

Das Reederei-Modul soll folgende Aufgaben unterstützen:

- Verfolgung der Maßnahmenumsetzung auf dem Schiff:
  - Aktuelle Informationen zum Vorfall vom Schiff empfangen,
  - Informationen vom Schiff analysieren.
- Zusammenarbeit mit den verantwortlichen Behörden:
  - Kontakt mit den Behörden ermöglichen,
  - Informationen vom Schiff an die Behörden weiterleiten.
- Unterstützung des Schiffs bei der Krisenbewältigung:
  - Empfehlungen den Verantwortlichen auf dem Schiff geben,
  - Informationen von den Behörden an das Schiff weiterleiten.
- Ermöglichung des Datenaustausches mit dem Schiff:
  - Verschiedene Kommunikationswege bereitstellen,
  - Verwaltung und Auswahl geeigneter Kommunikationskanäle,
  - Daten senden und empfangen.

B.1.8 AP 4.2: Übungen

Verordnung (EG) Nr. 725/2004 schreibt die regelmäßige Durchführung von Übungen zur Gefahrenabwehr in Hafenanlagen vor. Zweck solcher Übungen ist das Überprüfen von Kommunikation (Nachrichtenverkehr), Koordination, Verfügbarkeit von Hilfsmitteln und Reaktionen. Diese können in Form von Großübungen unter realen Bedingungen, Simulationen

oder einer Kombination mit anderen Übungen durchgeführt werden. Zu einer optimalen Planung, erfolgreichen Durchführung und aussagekräftigen Auswertung gehören viele Schritte und Details, die beachtet werden sollten. Zur Unterstützung der Hafenanlagenbetreiber und der Behörden sollte daher in AP 4.2.1 „Konzeptentwurf für schnittstellenübergreifende Übungen" ein Konzept für eine standardisierte Planung, Begleitung und Auswertung von komplexen Übungen, durchgeführt von mehreren Organisationen, erarbeitet und in Form eines Handbuches für Hafensicherheitsübung umgesetzt werden (AP 4.2.3: „Zuarbeit zur Erstellung eines Handbuchs für Schulungen und Übungen").

Grundlage für das Handbuch sind nicht nur theoretische Überlegungen. Im Rahmen des Projektes wurden zwei Hafensicherheitsübungen begleitet. Dabei war das Fraunhofer FKIE in jeweils unterschiedlichem Umfang in die Planung, Vorbereitung, Durchführung und Auswertung involviert.

Bereits während der ersten Übung im Hafen Puttgarden am 24.10.2012 konnten viele praktische Erfahrungen gesammelt werden. Die hier gewonnen Erkenntnisse zur Planung und Durchführung einer Hafensicherheitsübung konnten in der zweiten Übung im Fährhafen Rostock am 05.06.2013 teilweise direkt umgesetzt und validiert werden. Weiterhin wurden neue Erkenntnisse gewonnen. Insbesondere der intensive Austausch mit der Übungsleitung während der Planungs- und Vorbereitungsphase, aber auch die Beobachtung während der Übung ermöglichte eine ganzheitliche Sicht auf den gesamten Übungsprozess. Wichtige Erkenntnisse wurden außerdem in der Nachbereitung der Übung gewonnen. Dazu haben am 04.09.2013 in einem ersten Validierungstreffen alle landseitigen Übungsteilnehmer die Übung gemeinsam anhand der vom Fraunhofer FKIE erstellten Ablaufmodelle diskutiert. In einem zweiten Treffen am 08.10.2013 wurde die Übung mit dem Kapitän und dem SSO aus Sicht des Schiffes besprochen.

Bei der Planung, Durchführung und Auswertung der Hafensicherheitsübungen wurden wichtige Erkenntnisse für die Optimierung der Sicherheitsarchitektur der beteiligten Hafenanlagen gewonnen. Diese Erkenntnisse wurden an den entsprechenden Stellen teilweise bereits umgesetzt.

Im Zusammenhang mit den durchgeführten Hafensicherheitsübungen konnte weiterhin auch der Umgang mit Gefahrstoffdetektionssystemen untersucht werden (AP 4.2.2).

Die Auswertung der Übungen hat gezeigt, dass es bei der Planung, Durchführung und Auswertung von Hafensicherheitsübungen vieles, teilweise trivial scheinendes, zu beachten gibt. Ein zu erstellendes Handbuch soll dem Verantwortlichen für Hafensicherheitsübungen in jeder Phase unterstützen. Die beigefügten Checklisten sollen dem Verantwortlichen helfen, alle notwendigen Punkte vor, während und nach der Übung zu berücksichtigen. Die Checklisten sind so gestaltet, dass sie als Vorlage in jeder Übung eingesetzt werden können. Die Archivierten Checklisten dienen dem Nachweis der Übungen vor Behörden und der Vergleichbarkeit der Übungen untereinander. Ein Beispiel für eine Checkliste findet sich in Abbildung 28.

Insbesondere für die Planung und Vorbereitung beinhaltet das Handbuch Leitfragen, die sich der Verantwortliche stellen soll, um eine optimale Übung auszuarbeiten.

Insgesamt soll das Handbuch dazu beitragen, dass Hafensicherheitsübungen standardisiert und strukturiert geplant und vorbereitet und optimal durchgeführt werden können. Daher beinhaltet das Handbuch Beispiele und Tipps, wie in der Übung vorgegangen werden sollte, auch wenn es zu ungeplanten Schwierigkeiten kommt. Eine gute Hafensicherheitsübung sollte nicht nur das Erfüllen der ISPS-Vorgaben sein, sondern ein Gewinn für alle Beteiligten.

Das fertig gestellte Handbuch beinhaltet Erkenntnisse aus den Übungen sowie Wünsche und Anregungen aus Diskussionen mit den Endnutzern. Das Handbuch wird den Endnutzern zur Verfügung gestellt und in Zukünftigen Übungen eingesetzt. Es wird im gesonderten Anhang dieses Berichts bereitgestellt.

Phase	Aufgabe	Anmerkung	Erledigt
Planung	Übungszeitpunkt bestimmen	__.__.____ __:__ - __:__ Uhr	
	Übungsziele bestimmen	- - -	
	Übungsteilnehmer bestimmen Sicherheitsdienst, Hafen, Reederei, Behörden, Polizei …		
	Übungsbereiche definieren	- - -	
	Szenarien planen		
	Zeitlichen Übungsablauf festlegen In Tabelle 3 eintragen		
	Übungsbegleitung bestimmen Übungsleitung, Schiedsrichter, Störer, Beobachter (in Tabelle 4 eintragen), weitere Personen		
Vorbereitung	Instruktionen, Übungs- und Störeranweisung schreiben		
	Equipment organisieren		
	Informieren von Behörden etc.		
	Einweisung der Übungsbegleitung		
	Dokumentation vorbereiten Dokumentationsbögen (Tabelle 5), Fotos, Kameras, …		

Abbildung 28: Beispiel einer Checkliste für die Phasen „Planung“ und „Vorbereitung“

B.2 Wichtigste Positionen des zahlenmäßigen Nachweises

Die wichtigsten Positionen des zahlenmäßigen Nachweises bilden die gesamten unmittelbare Vorhabenkosten (0855) bzw. die Zuwendung (0884) und entsprechen den Selbstkosten des Vorhabens (0991). Sie setzen sich wie folgt zusammen:

- 0837: Personalkosten
- 0838: Reisekosten
- 0850: Sonstige unmittelbare Vorhabenkosten

B.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die durchgeführten Arbeiten wurden alle stringent auf die im Projektantrag beschriebenen Ziele hin ausgerichtet und durchgeführt. Dazu wurden stets möglichst effiziente und effektive Vorgehensweisen gewählt, um unnötigen und nicht angemessenen Aufwand zu vermeiden.

B.4 Voraussichtlicher Nutzen

Die Untersuchung maritimer Sicherheitsarchitekturen hat insbesondere Aufgrund ihrer Nähe zur Praxis bereits jetzt einen Beitrag zur Verbesserung der Sicherheit geleistet, insbesondere, da einige Ergebnisse von den Bedarfsträgern bereits umgesetzt werden konnten. Weitere sollen folgen. Damit tragen die Ergebnisse des Projekts aktiv zu einer Verbesserung der Sicherheit beim Zugang im RoRo-Verkehr bei. Da die Lösungen in enger Zusammenarbeit mit den Bedarfsträgern erarbeitet wurden, ist von einer besonderen Nachhaltigkeit der Ergebnisse auszugehen. Auch die entstandenen Netzwerke zwischen den beteiligten Akteuren werden über den Abschluss des Projekts hinaus einen nachhaltigen Beitrag zur kontinuierlichen Verbesserung der Sicherheit leisten.

Mit dem Ausbau der Expertise im Bereich der Analyse von Sicherheitsprozessen konnte das FKIE seinen Standpunkt als Sicherheitsforschungsinstitut weiter stärken. Dies beinhaltet auch zukünftige Beratertätigkeiten zur technischen und organisatorischen Gewährleistung eines adäquaten Sicherheitsniveaus auf RoRo-Fähren sowie die Entwicklung von Technologien im Bereich der zivilen Sicherheit. Eine Anwendung auf den nicht-zivilen Bereich ist ebenfalls denkbar.

Der Vorstoß im Bereich der Anpassung von Prozessanalysemethoden zur Übungsbegleitung und die Entwicklung eines Übungshandbuchs hat das Potential, einen wichtigen Beitrag zur diesbezüglichen Forschung zu leisten. Das fertig gestellte Handbuch beinhaltet Erkenntnisse aus den Übungen sowie Wünsche und Anregungen aus Diskussionen mit den Endnutzern. Dieses wurde den Endnutzern zur Verfügung gestellt und wird in Zukunft bei der Planung und Durchführung von Hafensicherheitsübungen eingesetzt werden.

Zusätzlich sind die Arbeiten zur Kommunikationsanalyse und zum Situationsverständnis mit rollenspezifischen Kommunikationskarten eine Grundlage zur Optimierung bisheriger Abläufe, vor allem an der Schnittstelle Schiff-Hafen.

Die erarbeitete Methode zur Risikoanalyse wurde in Deutschland ab 2014 in Kooperation mit den Designated Authorities der durch den ISPS-Code betroffenen Bundesländer Schleswig-Holstein, Hamburg, Bremen, Nordrhein-Westfalen, Mecklenburg-Vorpommern und Niedersachsen flächendeckend eingeführt. Eine Übertragung des Rahmenwerks auf andere kritische Infrastrukturen ist denkbar und sollte für konkrete Anwendungsbeispiele geprüft werden. Eine Übertragbarkeit der Methode auf die maritime Sicherheit anderer europäischer Länder sollte ebenfalls geprüft werden. Hier können strukturelle und systemische Unterschiede bestehen, die insbesondere die Finanzierung der Umsetzung des ISPS-Codes betreffen. Ein erster

Vorstoß in diese Richtung war die Vorstellung der Methode vor dem MARSEC-Ausschuss der Europäischen Kommission im Februar 2014. Andere Mitgliedsstaaten und die Kommissionsvorsitzenden haben sich sehr interessiert gezeigt.

Bezüglich der Arbeiten zur Entscheidungsunterstützung stehen der Katalog der Security-Maßnahmen zur Gefahrenabwehr auf dem Schiff, der Anforderungskatalog und der vom Projektpartner „MARSIG“ umgesetzte Demonstrator für weitere Forschungsarbeiten zur Verfügung. Zudem kann eine Übertragung der Anforderungen auf Safety-Bereich als Verwertungsmöglichkeit in Betracht gezogen werden.

Hinsichtlich der Gefahrstoffkontrolle bilden Ergebnisse wie die Ermittlung von Verdachtsmerkmalen, der Sensor-Marktüberblick, die stichprobenartigen Untersuchungen von Einzelkomponenten sowie das mehrstufige Datenfusionsmodell zur Bedrohungserkennung bei anschließenden Projekten die Basis für weiterführende Forschungsarbeiten. Das Softwaretool zur Identifizierung von Sprengstoffen soll zur Identifizierung gemischter radioaktiver Quellen weiterentwickelt werden, ebenso die Datenbank zur Identifizierung von Drogen. Mögliche Einsatzbereiche können hierbei neben Häfen auch Flughäfen, öffentliche Einrichtungen und industrielle Bereiche sein.

Sämtliche Ergebnisse werden – soweit keine Geheimhaltungsaspekte entgegenstehen – für weitere wissenschaftliche Untersuchungen zur Verfügung gestellt und gehen damit als Gemeingut in zukünftige Forschungsprojekte ein. Eine Übertragbarkeit der Methoden auf andere Sicherheitsarchitekturen soll weitere Anwendungsfelder eröffnen.

B.5 Fortschritte auf dem Gebiet des Vorhabens bei anderen Stellen

Forschungsarbeiten, die sich mit der Risikobewertung von Hafenanlagen in Deutschland beziehen, sind nicht bekannt. Aktuelle Forschungsarbeiten, die die amerikanische Methode zur Risikobewertung von Hafenanlagen betreffen, sind eingeflossen.

Forschungsarbeiten, die sich mit Security-Entscheidungsunterstützungs- und Trainingssystemen für zivile Schifffahrt beschäftigen sind nicht bekannt. Ähnliche Forschungsarbeiten zu EUS im militärischen Bereich wurden berücksichtigt.

Darüber hinaus sind keine Fortschritte auf dem Gebiet des Vorhabens bei anderen Stellen bekannt.

B.6 Veröffentlichungen im Rahmen des Projekts

- Dalinger, E. (2013): A Framework for Design of an Integrated System for Decision Support and Training. Proceedings of the 31st European Conference on Cognitive Ergonomics (ECCE). Toulouse, Frankreich: ACM, 2013.
- Ley, D. (2014): Methoden und Werkzeuge zur Unterstützung sicherheitskritischer Prozesse in der zivilen Schifffahrt. Eingeladener Vortrag beim VfS-Kongress 2014: Gemeinsam gegen Kriminalität 2.0 und "Underground Economy", Leipzig, Verband für Sicherheitstechnik e.V.
- Linkmann, G. & Holder, E. (2012): ISPS Port Risk Assessment: Is the True Value in the Numbers or in the Process? In N. Aschenbruck, P. Martini, M. Meier & J. Tölle (Hrsg.), Future Security, 318, (S. 522-525). Springer.
- Linkmann, G., Holder, E. & Motz, F. (2013): ISPS port risk assessment: Getting the most out of the process? In R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia, & A.C.W.M. Vrouwenvelder (Hrsg.), Safety, Reliability and Risk Analysis: Beyond the Horizon. Florida, USA: CRC Books.
- Wagner, A. & Motz, F. (2014): A guide for preparing and executing an effective port security exercise. 9. Sicherheitsforschungskonferenz “FUTURE SECURITY” in Berlin. Proceedings, S. 353-359.

C. Literatur

Annett, J. (2004): Hierarchical Task Analysis. In: D. Diaper & N. Stanton (Hrsg.): The Handbook of Task Analysis for Human-Computer Interaction (S. 67-82). Mahwah, New Jersey: Lawrence Erlbaum Associates.

APEC (2012): Manual of maritime security drills & exercises for port facilities.

Bortz, J. & Döring, N. (2006): Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler. Berlin, Springer.

Bundesministerium des Innern (2011): Schutz Kritischer Infrastrukturen: Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden).

Cohen, M.S., Freeman, J.T. & Thompson, B.B. (1997): Integrated critical thinking training and decision support for tactical anti-air warfare. 3rd International Command and Control Research and Technology Symposium Proceedings, 1997.

Dalinger, E. & Ley, D. (2011): A Reference Model for Designing Decision Support Systems in Novel Work Domains, IEEE International Conference on Systems, Man, and Cybernetics Proceedings, S. 1615 – 1620, Anchorage, Alaska, Oktober 2011.

Dalinger, E. & Motz, F. (2010): Designing a decision support system for maritime security incident response. In: O. Turan, J. Boss, J. Stark & J.L. Colwell (Hrsg.): International Conference on Human Performance at Sea Proceedings, 181-188, University of Strathclyde, Glasgow, United Kingdom.

Döring, B. (2005): Systemanalyse. In: H. Schmidtke (Hrsg.): Handbuch der Ergonomie. Koblenz: Bundesamt für Wehrtechnik und Beschaffung.

Downs, B. (2010): Maritime Security Risk Analysis Model (MSRAM): Overview. Presentation at the Electronic Power Grid Resilience Workshop 17-19 May 2010 in Monterey, California. Abgerufen am 11.06.2012 von http://www.chds.us/?player&id=2478.

El Mokni, H. (in Druck): IR and RAMAN Spectrum Analyst. Technischer Bericht Fraunhofer FKIE.

Elm W., Potter S., Gualtieri J., Roth E. & Easter J. (2003): Applied cognitive work analysis: a pragmatic methodology for designing revolutionary cognitive affordances. In: E. Hollnagel (Hrsg.): Handbook for Cognitive Task Design, London: Lawrence Erlbaum Associates, pp. 357-382.

Günzler, H. & Gremlich, H.-U. (2003): *IR-Spektroskopie: Eine Einführung*. 4. Auflage. Wiley-VCH, Weinheim.

Harel, D. (1987): Statecharts: A visual formalism for complex systems. Science of Computer Programming, Vol. 3, No. 8, 231-274.

Hesse, M., Meier, H. & Zeeh, B. (2011): Spektroskopische Methoden in der organischen Chemie, 8. überarb. Auflage.

IMO (2000): Adoption of Amendments to the International Convention for the Safety of Life at Sea (SOLAS) 1974, Revision to Chapter V – Safety of Navigation. IMO Resolution MSC.99 (73). London: International Maritime Organization.

IMO (2011): Maritime Security Manual: Guidance for port facilities, ports and ships. Draft (01/2011) London: International Maritime Organization.

Klein, G. (1998): Sources of Power: How People Make Decisions. Cambridge, MA: MIT Press, 1998.

Ley, D. & Dalinger, E. (2010): Entwicklung einer Security-Modellierungstechnik zur

Entscheidungsunterstützung in der Fährschifffahrt. USEWARE 2010: 5. VDI Fachtagung. Grundlagen – Methoden – Technologien, Baden-Baden.

Linkmann, G. & Holder, E. (2012): ISPS Port Risk Assessment: Is the true value in the numbers or in the process? In: N. Aschenbruck, P. Martini, M. Meier & J. Tölle (Hrsg.): Future Security, 318 (S. 522-525), Springer.

Linkmann, G., Holder, E. & Motz, F. (2013): ISPS port risk assessment: Getting the most out of the process? In R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia, & A.C.W.M. Vrouwenvelder (Hrsg.): Safety, Reliability and Risk Analysis: Beyond the Horizon. Florida, USA: CRC Books.

Linkmann, G., Ley, D. & Salzig, J.-S. (2011): Adapting Process Analysis Methods for the Evaluation of Exercises in the Maritime Domain. ErgoShip 2011 Göteborg, Schweden.

Morrison, J.G., Kelly, R.T., Moore, R.A. & Hutchins, S.G. (1998): Implications of Decision-Making Research for Decision Support and Displays. In: J.A. Cannon-Bowers & E. Salas (Hrsg.): Decision Making Under Stress: Implications for Training and Simulation. American Psychological Association.

Müller, D.H. & Tietjen, T. (2003): FMEA-Praxis, 2. Aufl., Carl Hanser Verlag, München.

Naikar, N. & Sanderson, P.M. (1999): Work domain analysis for training system definition and acquisition. International Journal of Aviation Psychology, 9(3), 271-290.

Naikar, N. (2006): Beyond interface design: Further applications of cognitive work analysis. International journal of industrial ergonomics 36, S. 423-438.

National Research Council (2010): Review of the Department of Homeland Security's Approach to Risk Analysis. Washington, DC: The National Academies Press.

Oberquelle, H. (1987): Sprachkonzepte für benutzergerechte Systeme. Berlin: Springer-Verlag

OMG (2009): Business Process Modeling Notation (BPMN). Version 1.2, Object Management Group (OMG) document number: formal/2009-01-03. Standard document URL: http://www.omg.org/spec/BPMN/1.2/.

Orasanu, J. & Connolly, T. (1993): The Reinvention of Decision Making. In: G.A. Klein, J. Orasanu, R. Calderwood, & C.E. Zsambok (Hrsg.): Decision Making in Action: Models and Methods. Norwood, NJ: Ablex, 3-20.

Port of Antwerp (2012): European handbook of maritime security exercises and drills.

Potter, S., Gualtieri, J. & Elm, W. (2003): Case studies: applied cognitive work analysis in the design of innovative decision support. In E. Hollnagel (Hrsg.): Handbook for Cognitive Task Design. London: Lawrence Erlbaum Associates, 653-678.

Rasmussen, J., Pejtersen, A.M. & Goodstein, L.P. (1994): Cognitive systems engineering. New York: Wiley, 1994.

Richtlinie EG/2005/65 des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen (Gesamthafenrichtlinie).

Sacco, G.M. & Tzitzikas, Y. (2009): Dynamic Taxonomies and Faceted Search: Theory, Practice, and Experience, Dordrecht: Springer.

SOLAS, 1974: International Convention for the Safety of Life at Sea.

Stanton, N.A., Salmon, P.M., Walker, G.H., Baber, C. & Jenkins D.P. (2005): Human Factors Methods. A Practical Guide for Engineering and Design. Burlington, USA: Ashgate.

Verordnung (EG) Nr. 725/2004: des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ISPS-Code).

Wieneke, M. & Koch, W. (2009): Combined Person Tracking and Classification in a Network of

Chemical Sensors. In: Elsevier Journal of Critical Infrastructure Protection, Vol. 2.

Wieneke, M., Safenreiter, K. & Koch, W. (2008a): Hazardous Material Localization and Person Tracking (Artikel und Poster). In: Proceedings SPIE Conferences on Defence and Security, Signal and Data Processing of Small Targets, Orlando (FL), USA.

Wieneke, M., Varela, M., Lorenz, F.P. & FKIE-HAMLeT-Team (2008): Hazardous Material Localization and Person Tracking, Supporting Activity Final Workshop & Demonstration Proposal/Grant Agreement no.:204400.

D. Abkürzungsverzeichnis

Abkürzung	Beschreibung
ACWA	Applied Cognitive Work Analysis
AMSS	Advanced Multisensor Surveillance Systems
ANN	Artificial Neural Network
BMBF	Bundesministeriums für Bildung und Forschung
BPMN	Business Process Modeling Notation
CP	Conducting Polymers
CSE	Cognitive Systems Engineering
DA	Designated Authority
dt	Zeitintervall
EID	Ecological Interface Design
EUS	Entscheidungsunterstützungssystem
FAN	Funktionales Abstraktionsnetzwerk
GUI	Graphical User Interface
HAMLeT	Hazardous Material Localization and Person Tracking
HMI	Human-Machine-Interface
HTA	Hierarchical Task Analysis
IMO	International Maritime Organization
IMS	Ionenmobilitätsspektrometrie
IMDG-Code	International Maritime Code for Dangerous Goods
IR	Infrarot
ISPS-Code	International Ship and Port Facility Security-Code
IST	Information Systems Technology
ISV	Institut für Sicherheitstechnik/Schiffssicherheit
KNN	K-Nearest-Neighbor-Algorithmus
LF	Relative Luftfeuchtigkeit
MLE	Maximum Likelihood Estimation
MOS	Metal Oxide Semiconductor
MOSFET	Metal Oxide Semiconductor Field Effect Transistors
mV	Milli-Volt
NDM	Naturalistic Decision Making
PASR	Preparatory Action for Security Research
PCA	Principal Component Analysis
PDA	Personal Digital Assistant
PFSO	Port Facility Security Officer
ppm	Parts per million
ppb	Parts per billion
ppt	Parts per trillion
ppq	Parts per quadrillion
QMB	Quartz Micro Balance
RFID	Radio-frequency identification
RFID-TAG	RFID-Transponder
RoRo	Roll on Roll off
RPD	Recognition-Primed Decision
RTO	Research and Technology Organization
SDF	Sensordaten- und Informationsfusion
SMT	Security Modeling Technique
SSO	Ship Security Officer
SOLAS	Safety of Life at Sea

SVM	Support Vector Machines
T	Temperatur
TATP	Triacetontriperoxid
TDM	Task Decomposition Method
TP	Taupunkt
UA	Unterauftragnehmer
USBV	Unkonventionelle Spreng- und Brandvorrichtungen
WLAN	Wireless Local Area Network

E. Verweis auf nicht-öffentliche Anlagen

In diesem Bericht wird auf Anlagen verwiesen, die nicht öffentlich zugänglich gemacht werden können. Nachfolgend sind diese zum Überblick aufgeführt. Sie sind verfügbar im gesonderten Dokument „Nicht öffentlich zugängliche Anlagen zum Abschlussbericht".

E.1 Risikobewertung für Hafenanlagen

E.2 Katalog der Security-Maßnahmen

E.3 Anforderungskatalog an ein Trainingssystem

E.4 Anforderungskatalog für ein Reederei-Modul

E.5 Bericht zur wissenschaftlichen Evaluation

E.6 Handbuch zur Übungsbegleitung