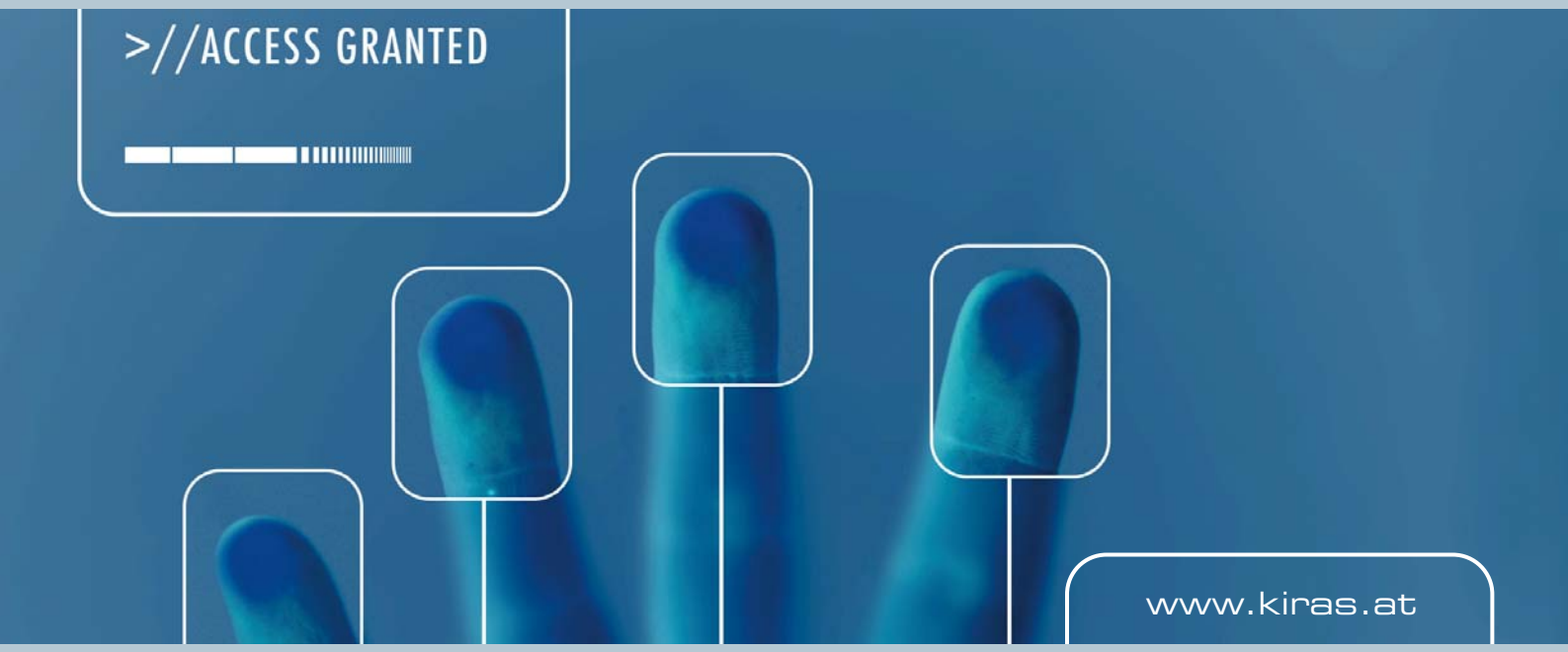
KIRAS
Sicherheitsforschung



Wissenschaf(f)t Sicherheit

Geförderte KIRAS-Projekte 2009 – 2011

FFG

bmvit
Stabsstelle für Technologietransfer und Sicherheitsforschung

Impressum: Medieninhaber, Herausgeber und Verleger:
Bundesministerium für Verkehr, Innovation und Technologie (bmvit)
Sektion III – Stabsstelle für Technologietransfer und Sicherheitsforschung
Renngasse 5, 1010 Wien

Alle Rechte, auch die Übernahme von Beiträgen nach § 44 Abs. 1 und 2 Urheberrechtsgesetz, sind vorbehalten.

Wir bitten im Sinne einer verbesserten Lesbarkeit um Verständnis, dass auf geschlechterspezifische Formulierungen verzichtet wird.
Selbstverständlich sind beide Geschlechter gleichermaßen angesprochen.

KIRAS
Sicherheitsforschung

Wissenschaf(f)t Sicherheit

Geförderte KIRAS-Projekte 2009 – 2011

bmvit
Stabsstelle für Technologietransfer und Sicherheitsforschung

KIRAS

Die Gewährleistung von Sicherheit für alle in Österreich lebenden Menschen ist eine staatliche Kernaufgabe. Die Notwendigkeit eines Beitrages von Forschung und Innovation bei der Begegnung dieser Herausforderung ist unbestritten. Österreich rief daher bereits im Jahr 2005 das Sicherheitsforschungsprogramm KIRAS ins Leben. Der vorliegende Projektsammelband stellt als zweiter seiner Art insgesamt 39 der bisher insgesamt 90 geförderten Projekte vor.

Sicherheit im Sinne von KIRAS

Der Sicherheitsbegriff (i.S.v. „security"), der KIRAS zugrunde liegt, ist umfassend angelegt. Er bezieht sich auf nichtmilitärische, ökonomische, ökologische, kulturelle und gesellschaftliche Gefahren und Risiken und alle Maßnahmen der öffentlichen Hand zur Erhaltung bzw. Verbesserung der öffentlichen Sicherheit einschließlich der Vorbeugung und Abwehr von Gefahren sowie der raschen Hilfe im Falle von Ereignissen, die die öffentliche Sicherheit maßgeblich beeinträchtigen. Sicherheitsforschung ist vor diesem Hintergrund technologieoffen, interdisziplinär und missionsorientiert, die beforschten Lösungen/Technologien sind eingebettet in den politisch-strategischen Gesamtkontext.

Strategische Zielsetzung

Diesem umfassenden Ansatz folgend gestalten sich die 6 strategischen Ziele von KIRAS breit gefächert und ambitioniert. Zur Überprüfung der Zielerreichung wurden bereits früh begleitende Evaluierungsmaßnahmen initiiert. Die unter dem jeweiligen Ziel dargestellten Erkenntnisse belegen das bereits bisher durchaus beachtliche Maß der Zielerreichung.

Ziel 1: *Erhöhung der Sicherheit und des Sicherheitsbewusstseins*
Mit der Vorgabe, die Sicherheit und das Sicherheitsbewusstsein der Bevölkerung zu erhöhen, wird die Sicherheitsforschung ihrer hohen gesellschaftlichen Relevanz gerecht. Wie die Ergebnisse der begleitenden Evaluierung von KIRAS bestätigen, adressiert die Sicherheitsforschung Themenbereiche, in denen ein konkretes Bedrohungspotenzial existiert. Repräsentative Umfragen belegen, dass 96 Prozent der Österreicherinnen und Österreicher die Aktivitäten des bmvit im Bereich der Sicherheitsforschung begrüßen.

Ziel 2: *Generierung sicherheitspolitisch erforderlichen Wissens*
Die Mehrzahl der Bedarfsträger, deren Einbindung in Kooperationsprojekte verpflichtend vorgeschrieben ist, um die Forschungsanstrengungen bedarfsorientiert (kundenorientiert) auszurichten, attestiert den hohen Innovationsbedarf bei Maßnahmen zur Begegnung konkreter Bedrohungsfälle. Für die Bedarfsträger sind die Inhalte der KIRAS-Projekte zu beinahe 90 Prozent neu für die Organisation, und in mehr als 75 Prozent der Fälle neu für Österreich.

Ziel 3: *Erzielung von Wissens-, Verfahrens- und Technologiesprüngen*
Die an der Sicherheitsforschung beteiligten Unternehmen verfügen insgesamt über eine höhere Innovationsleistung als der österreichische Durchschnitt. Im Vergleich zu den eigenen Forschungsaktivitäten der Unternehmen sind die 90 bisher durch das bmvit geförderten Sicherheitsforschungsprojekte technologisch komplexer, von höherer strategischer Bedeutung und mit einem höheren kommerziellen Risiko behaftet.

Ziel 4: *Wachstum der heimischen Sicherheitswirtschaft*
Bei Betrachtung der enormen volkswirtschaftlichen Schäden bspw. durch Kriminalität, Terrorismus und Naturkatastrophen und dem enormen Potenzial der globalen Sicherheitswirtschaft wird klar, dass die nationalen Sicherheitsforschungsanstrengungen einen Hebeleffekt für die heimische Sicherheitswirtschaft und damit – angesichts des stärkeren globalen Konkurrenzdrucks – einen Wettbewerbsvorteil darstellen. Die erzielten volkswirtschaftlichen Hebeleffekte durch die in der Sicherheitsforschung (KIRAS) bewilligten Fördermittel von rund 33 Millionen € bewirken zudem eine Wertschöpfung von 68 Millionen €. Darüber hinaus werden allein im Rahmen von KIRAS über 1.000 Arbeitsplätze gehalten und geschaffen. Ein ge-

rade in Zeiten der Wirtschaftskrise bedeutender Nachweis der Effektivität.

Ziel 5: *Auf- und Ausbau von Exzellenz im Bereich Sicherheitsforschung*
KIRAS-Projekte decken für einen Großteil der Fördernehmer zumindest teilweise einen neuen Forschungsbereich ab. Damit wird deutlich, dass in der Sicherheitsforschung erhebliches Potenzial für die Entwicklung von „Spitzentechnologie für Sicherheit" steckt, der Auf- und Ausbau von Exzellenz unterstützt wird.

Ziel 6: *Berücksichtigung gesellschaftlicher Fragestellungen in allen Aspekten der Sicherheitsforschung*
Durch die verpflichtende Einbindung von Geistes-, Sozial- und Kulturwissenschaften (GSK) in alle Sicherheitstechnologieprojekte wird sichergestellt, dass die entwickelten Technologien in einem interdisziplinären Ansatz gesellschaftspolitisch „verträglich" gestaltet werden und damit nur solche technologische Sicherheitslösungen entwickelt und eingesetzt werden, durch die sich die Bevölkerung auch sicherer fühlt.

Umsetzung

Zur Erreichung dieser Ziele werden bereits etablierte Governance-Strukturen unter Federführung des bmvit und unter breiter Einbeziehung von Bundesministerien, Sozialpartnern und FTI-Akteuren genutzt. Dadurch wird die Einordnung der Forschungsförderungsmaßnahmen in den breiten politisch-strategischen Kontext sichergestellt.

Die Programmlinien

KIRAS verfügt über vier Programmlinien, die sich gegenseitig unterstützen. Der Maßnahmenkatalog reicht von Vernetzungen und Sondierungen über kooperative F&E-Projekte bis hin zu Komponentenentwicklungen und Demonstrationsvorhaben sowie Unterstützungsmaßnahmen.

Thematische Ausrichtung

Der thematische Schwerpunkt der Förderaktivitäten liegt seit dem Programmstart auf dem Schutz kritischer Infrastrukturen. Entsprechend den jeweils aktuellsten Anforderungen der österreichischen Sicherheitspolitik werden zusätzlich für jede Ausschreibung sicherheitspolitische Schwerpunktfelder durch die im Nationalen Sicherheitsrat (NSR) vertretenen sicherheitspolitisch verantwortlichen Ressorts definiert. KIRAS steht somit für State-of-the-art-Sicherheitslösungen und adressiert Themenbereiche, in denen ein konkretes Bedrohungspotenzial existiert.

KIRAS als Türöffner für Europa

Österreich startete mit KIRAS im Jahr 2005 das erste Sicherheitsforschungsprogramm in Europa und sicherte sich damit einen entscheidenden Startvorteil in der europäischen Sicherheitsforschung. So wurde das Europäische Sicherheitsforschungsprogramm („FP7-SECURITY") nicht nur bei dessen Aufbau entscheidend durch das österreichische Vorbild geprägt, auch bei der Weiterentwicklung der europäischen Sicherheitsforschung nimmt Österreich unter der Federführung des bmvit eine entscheidende Rolle ein.

Die besondere Stellung Österreichs manifestiert sich in den Erfolgen heimischer Institutionen im Europäischen Sicherheitsforschungsprogramm. Österreich schneidet sowohl in den Beteiligungen, als auch in der Rückflussquote überdurchschnittlich gut ab und liegt damit im europäischen Spitzenfeld.

- Die Bewilligungsquote der Projekte mit österreichischer Beteiligung ist mit 24,8 Prozent deutlich höher als die Gesamtbewilligungsquote (16,4 Prozent) über alle bisherigen Ausschreibungen im Gesamtwert von rund 755 Millionen €.
- Die Bewilligungsquote der österreichischen Partnerorganisationen ist mit 24,7 Prozent deutlich höher als die Gesamtbewilligungsquote (nach Beteiligungen) der bisherigen Ausschreibungen (19,4 Prozent).
- Den bisher bewilligten Partnerorganisationen aus Österreich wurden bis dato in Summe rund 23 Millionen € an Fördermitteln zugesprochen.


Inhalt

KIRAS
Sicherheitsforschung

Kooperative F&E-Projekte

Programmlinie 2

EVIVA

Fluggestütztes Beobachtungs- und Analysesystem für den Eventschutz und für Krisensituationen mit videobasierter Verhaltensanalyse

EVIVA ermöglicht es, mit geringerem Personaleinsatz eine großräumige Überwachung von sicherheitskritischen Bereichen durchzuführen und Interventionen effizient zu steuern.

Der kombinierte Einsatz von terrestrischen und fluggestützten (Flugzeug, Hubschrauber, UAV's) Videosystemen bietet die Möglichkeit einer wesentlichen Effizienzsteigerung bei der Früherkennung kritischer Situationen etwa bei Großevents und bei der Durchführung, Steuerung und Beurteilung einer koordinierten Intervention.

Das Projekt EVIVA konzipiert, entwickelt und validiert Systemkomponenten für die fluggestützte Beobachtung und Analyse der Personenstromdynamik mittels Video- und Thermaldaten sowie ein dazugehöriges innovatives Management- und Führungssystem.

Die Innovationen des Projektes liegen in der

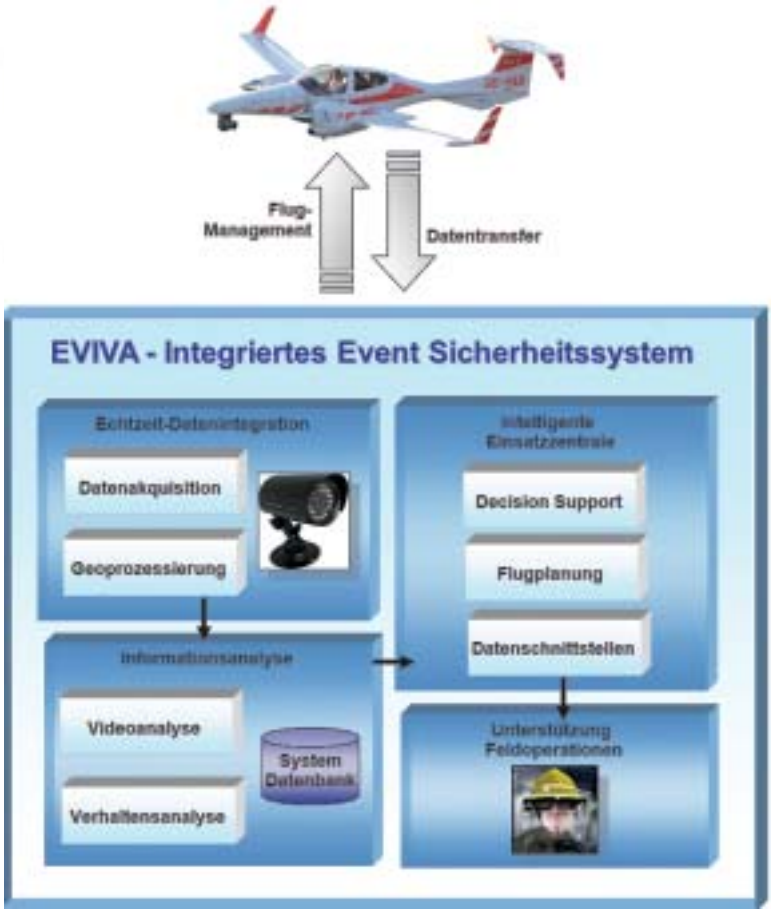
- Verwendung fluggestützter Sensorik;
- Entwicklung komplexer Algorithmen für die Auswertung von Video- und Thermaldaten zur Bewertung des Bewegungsmusters von Menschenströmen;
- automatischen Georeferenzierung von Videodaten sowie im
- Aufbau einer integrierten Managementzentrale, um den Einsatzkräften ein effektives Sicherheitsmanagement zu ermöglichen.

Durch die Funktionalität von EVIVA wird der Operator in der Einsatzzentrale in die Lage versetzt, größere Bereiche effektiv zu überwachen. Weiters können durch die Systemunterstützung mobile Sicherheitsteams wie auch luftgestützte und terrestrische Sensorsysteme effizient koordiniert werden. Die Integration von zusätzlichen Informationsquellen, von Methoden und Algorithmen zur gemeinsamen Auswertung der Datenebenen sowie eine intelligente, geo-orientierte grafische Repräsentation stellen eine wesentliche Unterstützung für die Beurteilung der Situation dar.

Ein weiteres wichtiges Instrument bei der Unterstützung der Überwachungsfunktion bildet die automatische Analyse der Videodaten in Bezug auf Personengruppen sowie Personenverhalten. Die Ergebnisse ermöglichen das automatisierte Erkennen potenziell kritischer Bereiche und das Generieren von Aufmerksamkeitsalarmen im Einsatzleitstand bei Überschreiten einstellbarer Schwellwerte. Dadurch wird die Aufmerksamkeit der Sicherheitskraft gezielt auf kritische Situationen gelenkt. Weiters wird der Informationsfluss in Richtung der mobilen Einsatzteams ausgebaut, um die Koordination der Einsatzkräfte zu erleichtern und die Einsatzkräfte selbst als mobile Lieferanten von Situationsberichten in die Einsatzzentrale einzubinden.

Gängige Videosysteme beschränken sich auf die Bereitstellung der Videodaten in Echtzeit und die Angabe von Positionskoordinaten der aktuellen Blickrichtung. Für das im Projekt EVIVA eingesetzte System werden zusätzlich Funktionalitäten für eine steuerbare, bedarfsorientierte Datenaufnahme sowie für eine flächendeckende, echtzeitnahe Generierung von ortho-rektifizierten Bildern bereitgestellt. Ortho-Bilder bieten durch den Zugang zu kartografischen Positionsinformationen relative und absolute Lageinformationen und sind somit unabkömmliche Voraussetzungen für die weiterführende automatisierte Datenanalyse und die Integration von zusätzlichen Informationen (terrestrischer Sensoren, Geoinformation etc.).

Für die Planung bzw. Anforderung bedarfsorientierter Datenaufnahmen können vom Benutzer die benötigten Parameter (Ausdehnung und Lage des aufzunehmenden Gebiets, Bildpunktauflösung, zu ver-



Oben: Datenvisualisierung von EVIVA in der Einsatzzentrale; rechts: die Systemkomponenten im Überblick

wendender Sensor etc.) definiert werden und dementsprechend eine genaue Konfiguration der Sensorplattform bzw. deren Kamerasteuerung berechnet werden. Die dafür erforderlichen Entwicklungen sind modular aufgebaut, entsprechende Schnittstellen gewährleisten die Integration von existierenden Softwarelösungen für die Flug- und Aufnahmesteuerung.

Für die fluggestützte Multisensorplattform wird eine äußerst leistungsfähige Videokamera mit Full-HD-Auflösung und effizienten optischen Zoomeigenschaften eingesetzt. Durch diese spezielle Aufnahmetechnik steht ausreichend „informative visuelle Textur" im Bild zur Verfügung, um den Einsatz leistungsfähiger Verfahren zur fluggestützten Videoanalyse zu ermöglichen. Die Videoanalyse extrahiert aus dem Videostream die für die Verhaltensanalyse relevanten Zielparameter wie Dichte, Richtung und Geschwindigkeit von Einzelpersonen sowie Personengruppen. Die Verhaltensmodellierung ermöglicht es, aufgrund dieser Parameter das Gefahrenpotenzial zu bewerten.

Für Bedarfsträger und Sicherheitsfirmen ergeben sich aus den in EVIVA angestrebten Entwicklungen Vorteile in folgenden Bereichen:

- Frühzeitiges Erkennen kritischer Situationen, raschere und effizientere Reaktion.
- Verbessertes Sicherheitsmanagement ohne Erhöhung des Personaleinsatzes.
- Im Fall eines Vorfalles: Perfekte Dokumentation für rechtliche Absicherung im Ermittlungsverfahren und für die Öffentlichkeitsarbeit.

Projektleitung:

JOANNEUM RESEARCH Forschungsgesellschaft mbH/DIGITAL

Projektpartner:

– Frequentis AG
– AIT Austrian Institute of Technology
– Diamond Aircraft Industries GmbH
– Bundesministerium für Landesverteidigung und Sport (BMLVS)
– Kooperationspartner: Bundesministerium für Inneres (BMI); Forschungsinstitut des Roten Kreuzes; G4S Security Services

Kontakt:

JOANNEUM RESEARCH Forschungsgesellschaft mbH
Dipl.-Ing. Alexander Almer
8010 Graz, Steyrergasse 17
Tel.: +43/316/876 17 38
Fax: +43/316/876 17 20
E-Mail: alexander.almer@joanneum.at
Web: www.joanneum.at

SECRET

Search for Critical Events in Video Archives

Ziel des Projektes SECRET ist die Erforschung von Algorithmen und Prozessen, um die Suche und Verfolgung von Personen in Videoarchiven für das Sicherheitspersonal zu erleichtern.

Sicherheit ist ein aktuelleres Thema denn je – gleichermaßen, ob diese beim Bürger subjektiv als solche empfunden wird oder ob diese durch staatliche Institutionen und Einsatzkräfte objektiv garantiert wird. Neue Bedrohungen globaler Art bis hin zu Attacken Einzelner an öffentlichen Einrichtungen mit gewollter Inkaufnahme größtmöglicher Schäden auch von unschuldigen Personen verstärken diesen Wunsch nach Sicherheit.

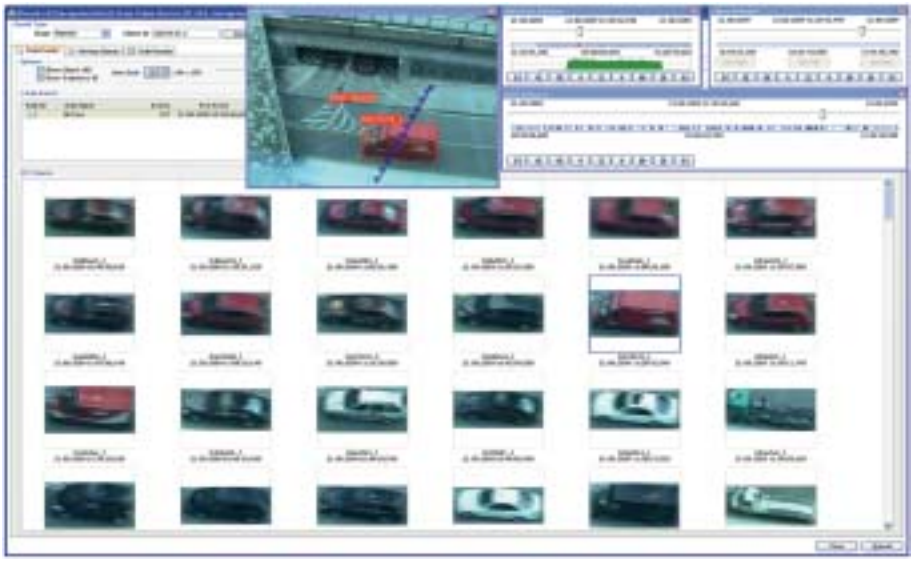
Ein wesentlicher Baustein zur Erhöhung der subjektiven und objektiven Sicherheit von kritischer Infrastruktur wie Bahnhöfen, U-Bahn, Flughäfen und anderer öffentlicher Plätze sind Videoüberwachungssysteme. Durch die Fülle von Videomaterial wird jedoch die Beobachtbarkeit und Nachverfolgbarkeit von Personen und Ereignissen nahezu unmöglich. So sind beispielsweise am Flughafen Wien 1.800 Kameras und bei den ÖBB ca. 3.000 + 700 für den neuen Bahnhof im Einsatz. Trotzdem sind Behörden häufig damit konfrontiert, eine bestimmte Person, die anhand optischer Kriterien (Größe, Farbe der Kleidung, Kopfbedeckung etc.) und/oder individueller Verhaltensmuster (Hinken, Herumschauen etc.) beschrieben wird, in den Videoaufnahmen eines großen Videoarchivs eines Infrastrukturbetreibers wiederzufinden. Diese Suche ist zeitlich extrem aufwendig, anstrengend und aufgrund der begrenzten Speichererlaubnis oft nicht erfolgreich. Die Folge ist, dass sehr häufig sicherheitskritische Ereignisse aufgrund der mangelhaften Videoanalyse nicht verhindert oder nicht nachverfolgt werden können.

Das Projekt „SECRET: Search for Critical Events in Video Archives" hat sich daher zum Ziel gesetzt, neue Methoden zur Segmentierung und zum Vergleich von Personen mit Personenbeschreibungen sowie Methoden zur Modellierung von Verhaltensmustern zu entwickeln. Gemeinsam mit Anwendungsexperten soll weiters ein Prozess erarbeitet werden, der die Suche nach Personen für das Sicherheitspersonal deutlich vereinfacht. Ziel ist die Reduktion der Suchzeit um einen Faktor zehn bis 100. Eine Suche, die jedoch weiter unter Berücksichtigung des für die Bevölkerung notwendigen Schutzes der Privatsphäre erfolgen muss.

Im Zuge einer automatisierten Videoauswertung erfolgt die Personenbeschreibungen einer gewünschten Person durch eine „Avatar-ähnliche" (also eine virtuelle) Beschreibungssprache oder ein Bildbeispiel, das in eine mathematische Beschreibung der optischen Eigenschaften einer Person umgesetzt wird. Diese Beschreibung wird mit den Videobildern aus dem Archiv verglichen. Dabei werden in einem ersten Schritt die Personenbilder aus den Videobildern des Archivs vereinzelt extrahiert. Das heißt, das Bild der Person wird aus einer Personengruppe und dem Hintergrund segmentiert.

Jeder Vergleich zwischen gesuchter Beschreibung und vereinzeltem Videoarchivbild ergibt einen Wert, der angibt, mit welcher Wahrscheinlichkeit die gesuchte Person mit der Person im Bild identisch ist. Durch einen interaktiven Prozess, der dem Benutzer (in der Regel eine Sicherheitskraft) unterschiedliche Resultate der Suche vorschlägt, kann der Suchraum zeitlich und örtlich eingeschränkt werden. Als Ergebnis werden die Personenbilder mit der höchsten Trefferwahrscheinlichkeit angezeigt. SECRET untersucht, ob eine solche automatische Auswertung der Videobilddaten tatsächlich die gewünschte Reduktion des Aufwandes für die Suche von Personen bringt. Unter Zugrundelegung der Bedürfnisse (im Projekt des Bundesministeriums für Inneres BMI) sowie den Möglichkeiten eines Infrastrukturbetreibers (im Projekt der Österreichischen Bundesbahnen ÖBB) soll anhand praktischer Beispiele ein labormäßiger Aufbau eines solchen Suchprozesses erfolgen. Die wesentlichen Forschungsthemen dabei sind:

- Detektion und Segmentierung von Personen aus Videobildern;



Ergebnisdarstellung für eine Suchanfrage nach roten Autos

- Vergleich und Wiederfinden von Personen in unterschiedlichen Videobildern anhand von mathematischen Kriterien sowie
- Analyse und Lernen von Verhaltensmustern.

Das Forschungsinstitut des Wiener Roten Kreuzes wird die industrielle Forschung begleiten und zwei relevante Themenbereiche abdecken: Zum Ersten soll mittels qualitativer Interviews die Einstellung der Bevölkerung gegenüber einer automatisierten Videoanalyse erfragt werden. Zum Zweiten soll darauf aufbauend ein Vorschlag für eine mögliche Richtlinie zur Durchführung solcher Suchvorgänge erarbeitet werden.

Weitere Resultate des Forschungsprojektes sind:
- Untersuchung bezüglich rechtlicher und datenschutzrechtlicher Aspekte zur automatischen Suche in Videoarchiven.
- Auswertung qualitativer Interviews mit ÖBB und BMI zum Thema Videoüberwachung mit Berücksichtigung ethischer und soziologischer Aspekte.
- Erstellung eines prototyphaften Systems zur Suche in Videoarchiven.
- Erstellung einer prototyphaften Anbindung an ein Videoarchiv zum Test.
- Darstellung möglicher Realisierungsvarianten (Blockdiagramme, Systemkonzept) in Verbindung mit einem realen Videosystem eines Infrastrukturbetreibers (ÖBB).

Zusammengefasst werden im Rahmen des Projektes SECRET neue Erkenntnisse im Bereich der automatischen Bildauswertungsverfahren generiert, die als algorithmischer Kern einer automatischen Videoarchivsuche dienen. Um den Nutzen der Bedarfsträger sicherzustellen, werden bereits während der Entwicklung Teile eines prototypischen Systems implementiert. Diese erlauben eine Validierung der Algorithmen bereits in einem frühen Stadium und optimieren die Chancen einer ebenso innovativen wie auch für Endanwender nützlichen Entwicklung eines neuen Frameworks für eine schnelle und effiziente Videoarchivsuche.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

– ÖBB-Infrastruktur Betrieb AG
– ÖBB-Personenverkehr AG
– ÖBB-Holding AG
– Bundesministerium für Inneres (BMI)
– ASE – Advanced Security Engineering
– FRK – Forschungsinstitut des Roten Kreuzes
– TU Graz – Institut für maschinelles Sehen und Darstellen

Kontakt:

AIT Austrian Institute of Technology
Dipl.-Ing. Bernhard Strobl
1220 Wien, Donau-City-Straße 1
Tel./Fax: +43/664/815 78 42
E-Mail: bernhard.strobl@ait.ac.at

SkyObserver

Autonome fliegende Drohnenschwärme zur schnellen Erfassung und Vorhersage möglicher Schadensauswirkungen bei großflächigen Gefährdungen

SkyObserver entwickelt ein Konzept zum Einsatz autonomer Drohnenschwärme zur Erfassung und Vorhersage möglicher Schadensauswirkungen bei großflächigen Gefährdungen.

Beim Auftreten von Gefahrenlagen, wie zum Beispiel dem unkontrollierten Austritt von flüssigen oder gasförmigen Schadstoffen jeglicher Art, ist die sichere und schnelle Erfassung und Vorhersage möglicher Auswirkungen von entscheidender Bedeutung. Weiters ist es entscheidend, dass Personen, die vor der Gefahr fliehen und bereits den Schadstoffen ausgesetzt waren, schnellstens gefunden werden.

Ziel des Projektes SkyObserver ist daher die Erforschung von neuen Methoden zur schnelleren und umfassenden Erfassung einer Gefahren- und Schadenslage, durch die die Gefährdung für Einsatzkräfte reduziert werden kann und die zudem kostengünstiger sind. Zur Veranschaulichung wurde das Referenzszenario „Chemieunfall mit Austritt toxischer Gase" gewählt, da es alle im Projekt behandelten Aspekte beinhaltet.

Die Hauptaufgaben im Projekt SkyObserver sind die Schadstoffmessung, Erstellung eines Lagebilds sowie die Detektion von Personen mittels Drohnen:

- Schadstoffmessung: Für die Prognose der Ausbreitung der toxischen Gaswolke muss dem Ausbreitungsmodell die Freisetzungsart und Freisetzungsrate vorgegeben werden. Laufende Messwerte der Schadstoffkonzentration ermöglichen eine realistische Prognose der Ausbreitung der Gaswolke. Je früher diese Messwerte zur Verfügung stehen, desto rascher liegt der Einsatzleitung eine abgesicherte Prognose vor. Dazu wird ein mit Schadstoffsensoren ausgestatteter Drohnenschwarm eingesetzt. Dieser fliegt das betroffene Gebiet autonom ab und übermittelt die gemessene Schadstoffkonzentration an die Bodenstation.
- Lagebilderstellung: Um den Einsatzkräften einen Überblick über die Gesamtsituation zu verschaffen und um die Befahrbarkeit der Zufahrtswege überprüfen zu können, wird ebenfalls ein Drohnenschwarm eingesetzt. Dieser ist mit Weitwinkelkameras ausgestattet, die Bilder mit einer Auflösung erstellt, die gewährleistet, dass Gesichter von Personen nicht erkennbar sind und somit keine Verarbeitung personenbezogener Daten erfolgt. Nach Rückkehr der Drohne werden diese Bilder in die Bodenstation geladen und zu einem hochauflösenden Lagebild zusammengesetzt.
- Personendetektion: Damit die Einsatzkräfte betroffenen Personen möglichst schnell helfen können, wird ein Drohnenschwarm mit einem „embedded system" zur Detektion von sich bewegenden Personen ausgestattet – sich nicht bewegende Personen sind von der Detektion ausgenommen. Auch hier bieten sich Optimierungsmöglichkeiten durch die Zahl der einzusetzenden Drohnen.

Eingesetzt werden sogenannte Miniaturdrohnen (Micro Aerial Vehicles), welche ein maximales Startgewicht von etwa zwei Kilogramm aufweisen. Die Drohnen sind in der Handhabung sehr robust und können durch ihr geringes Gewicht von einer einzelnen Person gestartet werden. Aufgrund der drei unterschiedlichen Aufgaben werden zumindest drei unterschiedlich ausgestattete Drohnen eingesetzt. Der Faktor Zeit oder die Größe des betroffenen Areals können es sinnvoll machen, mehr Drohnen einzusetzen. Hierfür ist die aufgabenspezifische Sensorik der Drohnen modular aufgebaut. Damit kann der Einsatzleiter vor Ort und nach Maßgabe entscheiden, welche und wie viele Drohnen für welche Aufgaben eingesetzt werden.

Um die Vorteile eines autonomen Drohnenschwarms nutzen zu können, wurde eine neuartige Schwarmintelligenz entwickelt, welche die Zahl und die Position der jeweils in der Luft befindlichen Drohnen berücksichtigt und auch eine autonome Aufgabenver-

Die Drohnen stimmen sich dank Autopilot (Bild re.) autonom ab und übernehmen unterschiedliche Aufgaben

teilung ermöglicht. Dabei wird von der Bodenstation ausschließlich die Gesamtaufgabe des Schwarms definiert. Die Aufteilung und Optimierung der Wege erfolgt zwischen den Drohnen und wird mit jeder Drohne die hinzukommt oder ausfällt, angepasst. Die Vorteile des Einsatzes mehrerer Drohnen sind damit offensichtlich:

- Bei Ausfall einer Drohne übernehmen die anderen Drohnen die Aufgabe der ausgefallenen.
- Effizientere Erledigung der Aufgabe, da diese auf mehrere Drohnen verteilt wird (Parallelisierung).
- SkyObserver muss nicht extra angefordert werden; ist mit den Einsatzorganisationen direkt vor Ort.
- Die Drohnen sind kostengünstiger in der Anschaffung und im Betrieb als Hubschrauber.
- Da die Drohnen unbemannt sind, wird kein Flugpersonal in Gefahr gebracht.

Da auch durch Einsatz von Miniaturdrohnen davon ausgegangen werden muss, dass betroffene Bürger sich in ihrer Privatsphäre verletzt fühlen oder Bedenken bezüglich der missbräuchlichen Verwendung zur Überwachung der Bürger bestehen könnten, wurde im Rahmen von SkyObserver eine Akzeptanzanalyse durchgeführt. Alle drei Aufgabengebiete des Referenzszenarios wurden bei der für die österreichische Bevölkerung repräsentativen Umfrage mit jeweils 93 Prozent positiv bewertet. Bedenken gab es nur bezüglich einer möglichen Verletzung der Privatsphäre (28 Prozent) und einer missbräuchlichen Verwendung (49 Prozent). Um diesen Bedenken Rechnung zu tragen, wurde die Auflösung der Kameras für die Lagebilderstellung und die Personendetektion auf eine Bodenauflösung von mindestens ein Zentimeter pro Pixel limitiert, wodurch keine Personen identifiziert und somit keine personenbezogenen Daten verarbeitet werden können. Dadurch kann ein Missbrauch für die Überwachung von Personen ausgeschlossen werden.

Projektleitung:

AIT Austrian Institute of Technology, Department Safety & Security, Business Unit – Safe and Autonomous Systems

Projektpartner:

– Aerospy Sense & Avoid Technology GmbH
– ZAMG – Zentralanstalt für Meteorologie und Geodynamik
– Johannes Kepler Universität Linz, Institut für Design und Regelung mechatronischer Systeme
– SG concepts gmbh
– NOVOTECH Elektronik GmbH
– market Marktforschungs-Ges.m.b.H. & Co.KG
– Bundesministerium für Landesverteidigung und Sport (BMLVS)
– Berufsfeuerwehr Linz
– Landes-Feuerwehrverband OÖ., Zentralleitung des Katastrophenschutzes der Oö. Landesregierung

Kontakt:

AIT Austrian Institute of Technology
Dipl.-Ing. Dr. Kristian Ambrosch
1220 Wien, Donau-City-Straße 1
Tel.: +43/50550-4176
Fax: +43/50550-4150
E-Mail: kristian.ambrosch@ait.ac.at
Web: www.ait.ac.at

NOTZERT

Notfalls-Zertifizierungsinfrastrukturen und -dienste

NOTZERT beschreibt die Vorgehensweise zur Erhaltung der sogenannten Public-Key-Infrastruktur (PKI) bei einem Ausfall des Zertifizierungsdiensteanbieters.

In Österreich, wie auch in vielen anderen europäischen Ländern, hat sich unter anderem als Folge der Umsetzung der Signaturrichtlinie sowie der Implementierung von eGovernment-Applikationen die Technologie der Public-Key-Infrastrukturen (PKI) zu einer kritischen Infrastruktur entwickelt. Das österreichische Signaturgesetz schreibt vor, dass im Falle des Ausfalls eines Zertifizierungsdiensteanbieters (ZDA) zumindest der Widerrufs- und der Verzeichnisdienst von einem anderen Anbieter weitergeführt werden kann oder von der Aufsichtsstelle (in Österreich die Rundfunk und Telekom Regulierungs-GmbH RTR) übernommen und weitergeführt werden muss. Derzeit ist auf dem österreichischen Markt aber nur ein Anbieter für qualifizierte Zertifikate tätig (A-Trust). Zieht man den Vergleich zur Versorgung mit Elektrizität würde ein Ausfall des Anbieters dem Abschalten des Stromnetzes gleichkommen.

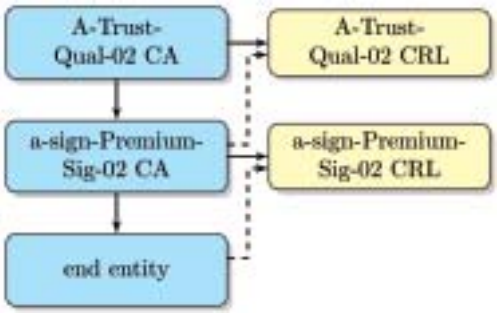
Das Projekt NOTZERT widmet sich daher der Frage, wie in einer Notfallsituation die notwendigste Public-Key-Infrastruktur erhalten bzw. weitergeführt werden kann. Den ersten und wichtigsten Schritt bei Einstellung des Betriebes eines ZDA stellt die Übernahme der Verzeichnis- und Widerrufsdienste dar. Dies ist essenziell, um bestehende Zertifikate weiter verwenden zu können, da man davon ausgehen muss, dass ein Zertifikat nicht gültig ist, solange man nicht zweifelsfrei das Gegenteil feststellen kann. Zu diesem Zweck wurde die Zertifizierungssoftware CAPSO („CA and PKI Solution“ ist eine am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz [IAIK] entwickelte Software zum Betrieb eines Zertifizierungsdienstes) um einen Importprozess erweitert, der es erlaubt, den Widerrufsdienst eines ZDA allein auf Basis der ausgestellten Zertifikate und der letztgültigen Widerrufslisten zu übernehmen.

Der Importprozess kann sich, je nach Kooperation des Aussteller-ZDA bzw. der technischen Voraussetzungen, sehr unterschiedlich gestalten. Prinzipiell können alle vom ZDA ausgestellten Zertifikate durch den oben genannten Importprozess übernommen werden, das ist aber weder sinnvoll (zum Beispiel aus Haftungsgründen), noch notwendig. Der Gesetzgeber sieht in diesem Zusammenhang nur die Übernahme von Zertifikaten „im öffentlichen Interesse“ vor. Qualifizierte Zertifikate müssen in jedem Fall übernommen werden.

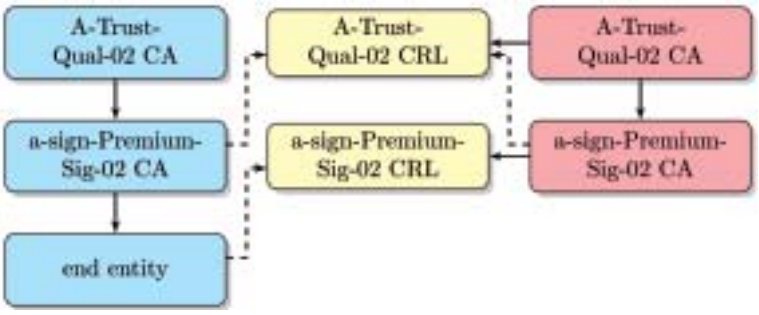
Ebenfalls übernommen werden sollten Serverzertifikate, deren Domänenname auf *.gv.at endet, um einen reibungslosen Betrieb der eGovernment-Dienste und der Verwaltungsaufgaben des Bundes zu ermöglichen. Weiters gibt es im Rahmen der Bürgerkartenaktivierung Zertifikate, die für die elektronische Identifikation mittels Bürgerkarte unerlässlich sind. Diese Zertifikate sind keine qualifizierten Zertifikate, sie können jedoch sehr einfach über eine spezielle Zertifikatserweiterung identifiziert werden. Letztendlich muss der Importprozess so flexibel gestaltet werden, dass man zusätzlich zu den oben genannten Gruppen auch einzelne Zertifikate besonderer Wichtigkeit importieren kann.

Ein funktionierender Widerrufsdienst ist eine essenzielle Vorraussetzung für die auf der Bürgerkarte basierenden Prozesse im österreichischen eGovernment. Die Übernahme des Widerrufsdienstes ist somit der kritischste Punkt der Notfall-CA und muss vor allen anderen umgesetzt werden. Der A-Trust ZDA bietet für seine qualifizierten Zertifikate Widerrufsdienste sowohl auf Basis von Zertifikatssperrlisten (CRLs) als auch auf Basis des Online Certificate Status Protocol (OCSP) an.

Beide Dienste sollen von der Notfall-CA übernommen werden. Je nachdem, ob die Schlüssel der CA Zertifikate weiter verwendet werden können und den Transport überstanden haben oder ob das nicht der Fall ist, gibt es unterschiedliche Möglichkeiten, die neuen Sperrlisten zu signieren.



Struktur direkter CRLs mit Verweisen auf Aussteller (durchgezogene Pfeile) und Sperrliste zur Prüfung (gestrichelt)



Struktur direkter CRLs mit neuen CA-Zertifikaten und den entsprechenden Verweisen (siehe links)

Beim Verzeichnisdienst handelt es sich um ein öffentlich zugängliches Register der ausgestellten Zertifikate. Entsprechend gestaltet sich die Übernahme auch einfacher. Das Verzeichnis wird beim A-Trust ZDA, genauso wie bei CAPSO, uber das Lightweight Directory Access Protocol (LDAP) zur Verfugung gestellt. Ein Import des Datenbestandes ist somit vergleichsweise einfach möglich.

Die gesetzlichen Rahmenbedingungen sind mit der Weiterfuhrung der Verzeichnis- und Widerrufsdienste erfullt. Fur den praktischen Einsatz eines Notfall-ZDA muss daruber hinaus jedoch auch sichergestellt sein, dass die Kernaufgaben von Bund und Ländern während des Betriebes des Notfalls-ZDA reibungslos weitergefuhrt werden können. Dazu kann es beispielsweise notwendig werden, neue Dienstausweise zu aktivieren. Die weiteren Forschungsarbeiten konzentrieren sich daher auf die Entwicklung des Prototypen in Richtung Aktivierung von Burgerkarten und mobile Signatur.

Das Arbeitspaket „Usability und Trust" umfasst drei wesentliche Bereiche. Im ersten Teil wird mittels einer qualitativen Studie und Focusgruppen untersucht, wie sich die Marke auf die Wahrnehmung des Produkts – der mobilen Signatur – auswirkt. Dazu werden die Eigenschaften eines optimalen Anbieters einer digitalen Signatur erhoben und mit den Eigenschaften des aktuellen Anbieters verglichen, um Übereinstimmungen sowie Defizite herauszuarbeiten. Auch die möglichen Auswirkungen eines Anbieterwechsels auf die Produktwahrnehmung werden diskutiert. Der zweite Teil umfasst die Recherche und Analyse der rechtlichen Auswirkungen und Datenschutzfragen, die bei Ausfall des Zertifizierungsdiensteanbieters und dem damit verbundenen Wechsel auf ein Notfallsystem zum Tragen kommen. Den Abschluss bildet schließlich eine Usability-Analyse der prototypisch umgesetzten Software fur den oben genannten Ausfall und Wechsel auf das Notfallsystem. Dabei werden Benutzerfreundlichkeit, etwaige Nutzungsbarrieren und der wahrgenommene Nutzen der Software mit einer Gruppe von Probanden erhoben.

Projektleitung:

Technische Universität Graz, Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK)

Projektpartner:

– A-SIT Zentrum für sichere Informationstechnologie – Austria
– Bundeskanzleramt Österreich
– evolaris next level GmbH

Kontakt:

Technische Universität Graz, IAIK
Dr. Peter Lipp
8010 Graz, Infeldgasse 16a
Tel: +43/316/873-5513
Fax: +43/316/873-105513
E-Mail: peter.lipp@iaik.tugraz.at
Web: www.iaik.tugraz.at

SafeCon

Sichere semi-autonome Konvoiführung

„SafeCon" entwickelt eine Technologie, die eine sichere und zuverlässige Führung von Nachschub- und Rettungskonvois in gefährdeten Zonen ermöglichen soll.

Bei internationalen Hilfseinsätzen sind Versorgungskonvois und Transportelemente sowie deren Bedienmannschaften relativ ungeschützt Angriffen, Überfällen, Entführungen und Hinterhalten ausgesetzt. Aktuell wird der Schutz des Personals in Konvois durch speziell gepanzerte Module sichergestellt – eine Zusatzausstattung, die sehr teuer ist, nur eine eingeschränkte Wirksamkeit aufweist und eine erhebliche Reduktion der Nutzlast bewirkt. Bei Naturkatastrophen setzt man in der Regel auf Luftbrücken. Allerdings handelt es sich auch dabei um eine sehr teure Lösung, die zusätzlich von der Verfügbarkeit des Fluggeräts und von der Wetterlage abhängig ist.

Das Projekt „Sichere semi-autonome Konvoiführung (SafeCon)" hat sich daher zum Ziel gesetzt, eine Technologie zu entwickeln, die es ermöglichen soll, einen Versorgungskonvoi zu bilden, der aus bemannten und unbemannten Fahrzeugen besteht.

Die besondere Herausforderung für das Projektteam besteht darin, dass solch ein Konvoi zu beliebigen Tages- und Nachtzeiten und bei jeder Witterung unterwegs sein muss und daher mit einer Sensorik auszustatten ist, die auch unter widrigen Bedingungen (Schlechtwetter, Störungen) zuverlässig funktioniert. Des Weiteren müssen die Konvoifahrzeuge in der Lage sein, miteinander zu kommunizieren, um einerseits einen Konvoi bilden zu können und andererseits flexibel auf geänderte Randbedingungen – etwa den Ausfall eines Fahrzeuges – reagieren zu können.

Im Rahmen von Hilfeleistungen bei Naturkatastrophen sollen die Transportgeräte – wenn es die jeweilige Gefährdungslage zulässt – gegebenenfalls auch bemannt eingesetzt werden können, da die physische Anwesenheit von Helfern das Sicherheitsgefühl der Bevölkerung stärkt. Aus diesem Grund wären die Konvoifahrzeuge so zu konzipieren, dass sie sowohl autonom als auch bemannt betrieben werden können, woraus sich der Arbeitsbegriff semi-autonome Konvoiführung ergibt.

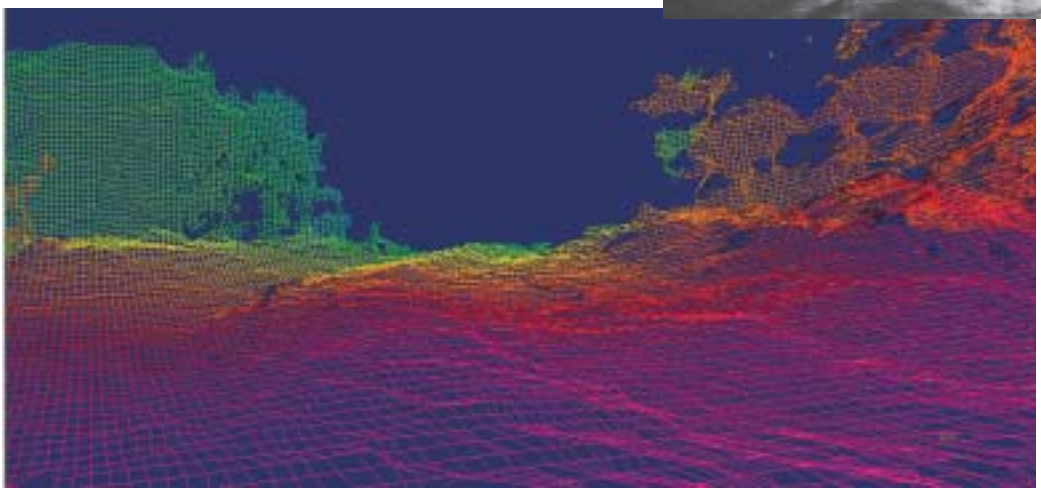
Die im Rahmen von SafeCon entwickelten Sensoren, Aktuatoren und Algorithmen können und sollen an Technologieträgern (Versuchsfahrzeugen) dargestellt und erprobt werden. Um die Interoperabilität sicherzustellen, werden alle Komponenten auf Basis allgemein anerkannter Standards zu konzipieren sein. Das Ergebnis stellt sich somit als „offene Architektur" dar, die vom jeweiligen Bedarfsträger gemäß seiner Erfordernisse adaptiert werden kann. Die Ergebnisse der gegenständlichen Studie können und sollen in Hardware umgesetzt werden. Dafür werden handelsübliche Fahrzeuge mit entsprechenden Sensoren, Prozessoren und Aktuatoren ausgerüstet werden, so dass die entwickelten Algorithmen im Feldversuch erprobt werden können.

Da es sich bei der zu entwickelnden sicherheitstechnologischen Innovation um ein zentrales Instrument für internationale Friedens- und nationale wie internationale Katastropheneinsätze handelt, ist eine rechtsethische begleitende Reflexion für das Projekt sinnvoll. Als zentrale begleitende Maßnahme ist daher die Erstellung einer rechtsethischen GSK-Studie vorgesehen.

SafeCon kann die Kosten für Versorgungsfahrzeuge signifikant reduzieren, da geschützte Fahrzeuge gegenüber den ungeschützten autonomen Systemen signifikant teurer sind. Damit kann die gegenständliche Technologie auf dem Wege der Kostenreduzierung auch über den Erfolg oder das Stattfinden einer Mission entscheiden. Humanitäre oder Katastrophenhilfseinsätze werden somit auch politisch und gesellschaftlich leichter argumentierbar.

Das erwartete Resultat des Projektes SafeCon ist eine zuverlässige Sensor- und Rechnerkonfiguration,

Navigation eines autonomen Fahrzeuges: Bild der Szene (Kamerarohdaten, die vom 3D-Sensor verarbeitet werden)



Darstellung, wie das Fahrzeug die Strecke vor sich sieht (3D-Abbildung der Szene als Gittermodell)

die in einem Konvoifahrzeug als eine Art Autopilot integriert werden soll. Diese Technologie unterstützt strategisch und taktisch internationale Hilfseinsätze in Gebieten hoher Gefährdung und ermöglicht Einsätze ohne Verluste an Menschenleben. Des Weiteren werden zukünftig Rettungsverfahren für Katastropheneinsätze möglich sein, die völlig neue Schutz-, Rettungs- und Versorgungsmöglichkeiten im Zivilschutz bieten.

Ein Verfahren, wie es im Rahmen dieses Projektes entwickelt werden soll, wird derzeit noch nirgends angewandt. Die Kooperation aus den verschiedenen Forschungsanstalten gemeinsam mit Unternehmen der österreichischen Wirtschaft ermöglicht zudem Ergebnisse, die durch die einzelnen Institutionen allein nicht erreicht werden können. Es entsteht daher eine Forschungs- und Umsetzungskompetenz auf dem Gebiet der autonomen Fahrzeuge, die national und wahrscheinlich auch international noch nicht erreicht worden ist.

Das Problem des Schutzes des eigenen Personals in humanitären Einsätzen ist für alle Staaten gleich. Der Bedarf an Lösungen, die bei geringstmöglichen Kosten optimale Sicherheit bieten, ist somit in hohem Maße gegeben. Die Entwicklung eines semi-autonomen Konvoisystems wie SafeCon eröffnet für die beteiligten Unternehmen einen internationalen Markt. Das Projekt wurde mit Jänner 2011 gestartet und die einzelnen Forschungsgruppen an den verschiedenen Instituten bzw. bei den Partnerfirmen haben die Arbeit aufgenommen.

Projektleitung:

Fachhochschule Technikum Wien, Institut für Mechatronics

Projektpartner:

– AeroSpy Sense & Avoid Technology GmbH
– AIT – Austrian Institute of Technology
– Bundesministerium für Landesverteidigung und Sport (BMLVS)
– NOVOTECH Elektronik GmbH
– Rheinmetall MAN Military Vehicles Österreich GesmbH
– TU Wien, Automation and Control Institute

Kontakt:

Fachhochschule Technikum Wien, Institut für Mechatronics
Dipl.-Ing. Dr. Wilfried Kubinger
1200 Wien, Höchstädtplatz 5
Tel.: +43/1/333 40 77-493
Fax: +43/1/333 40 77-459
E-Mail: kubinger@technikum-wien.at
Web: www.technikum-wien.at

Sis4you

Security Information System for Citizens

Das Forschungsprojekt „Sis4you" zielt darauf ab, erfolgreiche Präventionsmaßnahmen gegen Einbrüche in Wohnungen, Häuser und Geschäftslokale zu setzen.

In den letzten Jahren ist die Zahl der Einbrüche in Einfamilienhäuser und Wohnungen rasant angestiegen. Insgesamt finden laut einer Berrechnung des Security-Magazins in Österreich pro Tag 63 Einbrüche statt, das heißt, alle 24 Minuten werden irgendwo zwischen Vorarlberg und Wien Häuser bzw. Wohnungen aufgebrochen und ausgeräumt. Nicht zuletzt aufgrund dieser Entwicklung ist auch das subjektive Sicherheitsgefühl der Bevölkerung im Bereich der inneren Sicherheit im Sinne des Schutzes vor Kriminalität stark gesunken. Aus Sicht der Sozialforschung sind daher jegliche Maßnahmen, die die Ängste und Sorgen der Bevölkerung aufgreifen, begrüßenswert.

Inhalt und Ziel des Forschungsprojekts „Sis4you" ist die Entwicklung erfolgreicher Präventionsmaßnahmen gegen Einbrüche in Wohnungen, Häuser und Geschäftslokale. Mittels umfangreicher IT-Unterstützung soll die Bedrohungsanfälligkeit von Wohnobjekten reduziert und ein funktionelles Frühwarnsystem installiert werden.

Im Zuge des Projektes werden Faktoren und Rahmenbedingungen erforscht, die die Umsetzung von Informationen in konkrete sicherheitsrelevante Handlungen in der Bevölkerung fördern. Dies betrifft die Dimensionen Zugang, Usability und Vertrauen. Die angewandten Methoden stellen einen Technologiesprung in Bezug auf Awareness-Bildung dar. Zum anderen liegt die Herausforderung bei diesem Projekt in der Realisierung einer Pilotanwendung, mit der die Erwartungen der Bedarfsträger unter Berücksichtigung des Datenschutzes und der GSK-(geistes-, sozial- und kulturwissenschaftlichen)Aspekte in Bezug auf eine solche multifunktionale Sicherheitsplattform eingelöst werden können.

Die Betroffenheit ist sozial ungleich verteilt: Ältere Personen, Menschen mit geringerem sozioökonomischen Potenzial (Einkommen, Bildung etc.) und die Bevölkerung in den östlichen Bundesländern Wien, Niederösterreich und Burgenland sind stärker verunsichert als andere Personengruppen. Im Rahmen der Projektumsetzung sollten daher soziale Ungleichheiten analysiert und die Bedürfnisse der stärker Verunsicherten besondere Berücksichtigung finden. Die Information muss allerdings so aufbereitet werden, dass sie so umfassend wie möglich und so „Aufmerksamkeit erregend" wie notwendig ist, um die gewünschte Sensibilisierung der Bevölkerung auszulösen. Es ist wichtig, mögliche Barrieren im Vorfeld zu identifizieren und zu vermeiden. Darüber hinaus muss untersucht werden, welche Maßnahmen getroffen werden müssen, um das Vertrauen der Österreicher in die Plattform sicherzustellen. Hier ist zu klären, welche Erwartungen hinsichtlich der Transparenz der umgesetzten Vorkehrungen zum Schutz vor Missbrauch der Plattform bestehen. Die Thematik berührt daher insbesondere den Schutz persönlicher Daten, die von den Nutzern in der Anwendung der Plattform preisgegeben werden.

Resultat von Sis4you ist eine Plattform für Bürger zur Kriminalprävention und zur bi-direktionalen Kommunikation interessierter Bürger mit den Sicherheitsbehörden über standardisierte und IT-technisch sichere Kanäle.

Über einfache Interaktionsmöglichkeit bietet die Plattform Bürgern folgende Möglichkeiten:

- Informationen über die an ihrem Standort gegebene Sicherheitslage. Dabei werden die Tatortdaten der Ermittlungsbehörden in eine grafische Darstellung (eMap) konvertiert, aus der das jeweilige Gefahrenpotenzial am abgefragten Standort auf Basis einer leicht verstehbaren Logik und Symbolik abgelesen werden kann. Gleichzeitig sollen die Bürger durch Hinterlegung entsprechender semantischer Strukturen (Gefahrenpotenzial X erfordert Präventionsmaßnahme Y) in die Lage versetzt werden, Informationen über Abwehrmaßnahmen gegenüber

Sis4you schafft eine Plattform, die unter anderem neuralgische Sicherheitselemente von Wohnungen visualisiert

gegebenen Bedrohungsszenarien (Wahrscheinlichkeit eines neuerlichen Tateintritts in einem bestimmten Zeitraum; Modellrechnung auf Basis bisherige Tatortdaten nach Ort und Zeit) zu erhalten.

- Über die virtuelle Darstellung von Wohnungen und Eigenheimen mit entsprechenden Visualisierungstechnologien wird eine bildhafte Darstellung der neuralgischen Sicherheitselemente (Türen, Fenster, Balkone, Garageneinfahrten, Kellerfenster, Garten etc.) zur Verfügung gestellt. Durch interaktive Aktivierung dieser Elemente können relevante Maßnahmen zum Schutz des Eigentums und in Abhängigkeit von der gegebenen Sicherheitslage des Standorts präzise abgefragt werden.
- Bei eindeutiger Nutzeridentifizierung über geschützte Kommunikationskanäle können Bürger Eingaben über gemachte Beobachtungen an ihrem Standort bzw. in unmittelbarer Nähe ihres Standortes (z. B. Straßenzug) an die Sicherheitsbehörden weiterleiten.

Das Bundeskriminalamt (BK) kann mithilfe dieser Plattform nicht nur den Bürger beim Schutz seines Eigentums unterstützen, sondern bei erfolgreicher Nutzung des Systems eine Verbesserung bzw. Senkung der Einbruchsrate erreichen. Da das BK dem Bürger weiterhin die Sicherheitsthematik näher bringen wird, ist durch die Ergänzung durch dieses System eine noch höhere Reichweite der Informationen gegeben. Mittlerweile stehen fast in jedem Haushalt ein Fernseher und Computer, jedoch besteht nicht bei jedem Bürger ein Internet-Zugang. Eine mögliche Überlegung zur Weiterführung geht dahin, das sichere Eigenheim als Off-line-Version (DVD-/CD-Datenträger) dem Bürger zur Verfügung zu stellen, um die Informationen für den Bürger nachhaltig bereitzustellen.

Sis4you hat aber auch wirtschaftliches Potenzial. Die Sicherheitsempfehlungen auf der Plattform umfassen auch konkrete Produkte wie Alarmanlagen, Bewegungsmelder, Zeitschaltuhren, Sicherheitstüren, Fenstervergitterung. Handlungsempfehlungen, die von den Usern umgesetzt werden, tragen damit zur Wertschöpfung in Österreich bei. Da eine Plattform in dieser Dimension weltweit noch nicht existiert, besteht zudem auch eine Exzellenz und ein Wettbewerbsvorsprung in diesem Bereich.

Projektleitung:

AIT Austrian Institute of Technology GmbH, Safety & Security Department

Projektpartner:

– Bundesministerium für Inneres (BMI)
– Soroban IT – Beratungsgesellschaft mbH
– E-SEC Information Security Solutions GmbH
– IFES – Institut für empirische Sozialforschung GmbH

Kontakt:

AIT Austrian Institute of Technology GmbH
2444 Seibersdorf
Dipl.-Ing. Dr. Georg Neubauer
Tel.: +43/50550-2807
Fax: +43/50550-2813
E-Mail: georg.neubauer@ait.ac.at
Web: www.ait.ac.at

Dipl.-Ing. Thomas Bleier
Tel.: +43/50550-3115
Fax: +43/50550-2813
E-Mail: thomas.bleier@ait.ac.at
Web: www.ait.ac.at

CuteforceAnalyzer

Massivparalleler Computer-Cluster für kryptanalytische Anwendungen auf Basis GPU- und FPGA-Nodes

„CuteforceAnalyzer" schafft eine Entwicklungsplattform für den Einsatz neuer Koprozessortechnologien zur Analyse von Verschlüsselungssystemen.

In der Spionage, im organisierten Verbrechen oder bei der Vorbereitung von Terrorangriffen kommen Verschlüsselungssysteme zum Einsatz, die leicht anzuwenden, aber schwer zu knacken sind. Mit dem Forschungsprojekt „CuteforceAnalyzer – Massivparalleler Computer-Cluster für kryptanalytische Anwendungen auf Basis GPU- und FPGA-Nodes" soll ein Beitrag zum „präventiven Schutz vor Terrorismus und organisierter Kriminalität" geleistet werden.

Ob und wie neue Analysemethoden kryptografische Sicherheitsmechanismen wie Verschlüsselungsverfahren oder ein Authentifizierungsprotokoll überwinden können, kann vielfach nur durch experimentelle Methoden beurteilt werden.

Neue analytische Verfahren müssen zumindest ansatzweise ausprobiert werden, um eine Beurteilung ihres Bedrohungspotenzials zu ermöglichen. Durch Untersuchungen wurde festgestellt, dass „bösartige Software" (Malware) zur Tarnung, also zur Vermeidung von auffälligen Signaturen, eine Verschlüsselung der Schadroutinen verwendet. Eine Enttarnung und/oder Identifikation ist nur schwer möglich bzw. führt über die Kryptanalyse der verwendeten Algorithmen. Durch die Auswertung entschlüsselter

Kryptoanalytische Aufgaben stellen besondere Aufgaben an die Rechnerkapazität

Das Projekt Cuteforce-Analyzer liefert einen Beitrag zum „präventiven Schutz vor Terrorismus und organisierter Kriminalität"

Daten und Informationen kann damit ein wichtiger Beitrag zur Generierung von sicherheitspolitisch relevantem Wissen geleistet werden.

Kryptanalytische Aufgaben stellen jedoch besondere Anforderungen an die Rechenkapazität der involvierten Systeme. In der Regel werden für derartige Aufgaben speziell konstruierte Systeme verwendet. Durch eine direkte Integration des im Projekt entwickelten CuteforceAnalyzer in die vorhandene Rechnerumgebung des BMLVS kann ein großer Beitrag zur Erfüllung der sicherheitspolitischen Aufgabenstellungen der Republik Österreich und damit zur Sicherheit der Staatsagenden, Unternehmen und Staatsbürger geleistet werden.

Ein Ziel des Projektes CuteforceAnalyzer ist die Entwicklung eines skalierbaren, parallelen Rechnersystems, bestehend aus hochgradig spezialisierten Prozessoren – sogenannten Nodes – für die Implementierung von rechenzeitintensiven kryptanalytischen Algorithmen. Input-Nodes werden zur Verteilung von zu verarbeitenden Daten entwickelt, Compute-Nodes zur Durchführung von Berechnungen und Output-Nodes zur Zusammenfassung der Berechnungsergebnisse. Eine Management-Node erlaubt die Konfiguration, die Überwachung und die Steuerung der Aufgaben im Rechnersystem.

Ein weiteres Ziel des Projektes ist die Erforschung geeigneter Hardwareplattformen für kryptanalytische Algorithmen. Aufgrund der Erfahrungen aus Vorgängerprojekten wird bei den Compute-Nodes Hardware eingesetzt, die auf Field Programmable Gate Arrays (FPGAs) und Nvidia-Grafikprozessoren (GPUs) basiert. Insbesondere angestrebt wird die Integration des CuteforceAnalyzers in eine bestehende HPC-Rechneranlage. Dazu wird entsprechende Interfacehardware und -software entwickelt.

Ein weiteres Ziel des Projektes ist es, eine Weiterentwicklung und einen Ausbau des CuteforceAnalyzers durch den Benutzer zu ermöglichen. Hierzu werden eine Test- und Entwicklungsumgebung erstellt und marktübliche Komponenten verbaut. Durch die Erstellung von Schulungsunterlagen wird sichergestellt, dass das System neuen Aufgabenstellungen entsprechend angepasst werden kann.

Projektleitung:

FH OÖ Forschungs und Entwicklungs GmbH

Projektpartner:

– Bundesministerium für Landesverteidigung und Sport (BMLVS)
– DICE GmbH & Co KG
– market Marktforschungsgesmbh & Co KG

Kontakt:

FH OÖ Forschungs und Entwicklungs GmbH
FH-Prof. Dipl.-Ing. Robert Kolmhofer
4232 Hagenberg, Softwarepark 11
Tel.: +43/7236/3888-2510
Fax: +43/7236/3888-2599
E-Mail: robert.kolmhofer@fh-hagenberg.at
Web: www.cuteforce.at

SKILL

Prototypenentwicklung eines präzisen Verbringungssystems ballistischer multifunktioneller Körper mit veränderbarer Auftreffenergie für sicherheitsrelevante Aufgabenstellungen

Die heute für Ordnungs- und Sicherheitseinsätze verfügbaren ballistischen Systeme sind in ihrem Einsatz zu unpräzise und können oftmals gar nicht eingesetzt werden, da ihre Wirkung unbefriedigend und/oder mit einem hohen unerwünschten Sicherheitsrisiko behaftet ist. Aufbauend auf den von den Bedarfsträgern definierten Vorstellungen soll im Rahmen des Projektes SKILL ein System entstehen, welches bei der Verbringung ballistischer Körper eine hohe Präzision mit dosierbarer Wirkung im Ziel wie auch mit einer kurzen Reaktionszeit kombiniert. Weiters soll dieses System bei hoher Effizienz einen angemessenen Einsatz ermöglichen.

Mit diesem angestrebten technologischen Lösungsansatz entsteht eine Basis für eine Vielzahl von Einsatzmöglichkeiten. Neben sicherheitsrelevanten kann ein solches System eine Vielzahl weiterer Aufgaben im Katastrophen- und Rettungseinsatz, aber auch in anderen Bereichen erfüllen. So können etwa damit bei einer notwendigen Bergung Fangleinen mit daran angebrachten Rettungsmitteln präzise verschossen werden. Weitere Einsatzmöglichkeiten sind Lawinensprengungen oder das Verbringen von Sensoren im Veterinärbereich.

Die Systeme können im Einzelfall sehr unterschiedlich ausgeführt sein und benötigen weitere Entwicklungsschritte, welche über den derzeitigen Umfang des Projektes SKILL hinausgehen. Mit dem gegenständlichen Projekt sollen jedoch das grundsätzliche Funktionsprinzip und mögliche Arbeitsweisen erarbeitet werden.

Neben den technischen Aufgaben besteht ein bedeutsamer Teil des Projektes in der Erstellung einer begleitenden rechtsethischen GSK-Studie. Diese untersucht Aspekte wie die legitimatorische und normative Dimension dieser Entwicklung, inwieweit ethisch-moralische Anforderungen erfüllt werden bis hin zur Frage, welche Auswirkungen ein solches System auf die österreichische Sicherheitspolitik, das Sicherheitsbedürfnis der österreichischen Bevölkerung sowie deren Anwender hat. Erstellt wird diese begleitende Studie von der rechtswissenschaftlichen Fakultät der Universität Wien.

In der Startphase des Projektes wird von den Konsortialpartnern ein Pflichtenheft erstellt. Daran anschließend werden für den jeweiligen Verantwortungsbereich von den einzelnen Projektpartnern unterschiedliche Konzepte und Lösungsansätze untersucht und ausgearbeitet. Nach einer eingehenden Prüfung der gewählten technischen Lösungsansätze werden die einzelnen Komponenten entwickelt und in einem gemeinsamen Funktionsmuster zusammengeführt.

Projektleitung:

Photonic Optische Geräte GmbH & CoKG

Projektpartner:

– Steyr Mannlicher GmbH
– Versuchsanstalt Ferlach
– Bundesministerium für Inneres (BMI)
– Bundesministerium für Landesverteidigung und Sport (BMLVS)
– Universität Wien, Rechtswissenschaftliche Fakultät

Kontakt:

Photonic Optische Geräte GmbH & CoKG
Dipl.-Ing. (FH) Jörg Trautmann
1160 Wien, Seeböckgasse 59
Tel.: +43/1/486 56 91-15
Fax: +43/1/486 56 91-915
E-Mail: trautmann@photonic.at
Web: www.photonic.at

KIRAS
Sicherheitsforschung

Kooperative Komponenten-entwicklung und Demonstrationsvorhaben

Programmlinie 3

ACHILLES

Planungswerkzeug zur Identifikation von Schwachstellen im Regelbetrieb und Notfall für die urbane Wasserinfrastruktur

Der Softwareprototyp ACHILLES identifiziert Schwachstellen in der heimischen Wasserinfrastruktur und unterstützt bei der Planung von Gegenmaßnahmen.

Im Projekt „ACHILLES: Planungswerkzeug zur Identifikation von Schwachstellen im Regelbetrieb und Notfall für die urbane Wasserinfrastruktur" arbeitet daher ein Konsortium aus Partnern, die aus unterschiedlichen Bereichen kommen, an einem Analyseinstrument, mit dem mögliche Schwachstellen in der Wasserversorgung rascher und effizienter aufgedeckt werden können. Damit sollen die Risiken für Kontaminationen und Versorgungsausfall verringert und im Falle eines Schadens das Notfallmanagement verbessert werden.

Im Projekt berechnen die Forscher mithilfe mathematischer Modelle das Schadenspotenzial von Einwirkungen jeglicher Art auf die Wasserversorgungsnetze am Computer. Dabei können an jedem Punkt in den Leitungen die Druckverhältnisse und Stoffkonzentrationen verändert und Schadensfälle simuliert werden. Die daraus gewonnenen Erkenntnisse werden zusätzlich mit Informationen über Gefährdungspotenziale wie etwa durch Muren, Hochwasser oder Lawinen kombiniert.

Vor Projektstart wurden dazu alle vorliegenden Infrastrukturmodelle für den Einsatz im Regel- wie auch im Notfallbetrieb auf den neuesten Stand der Wissenschaft gebracht.

Aufgrund der Bedeutung von Haftungsfragen beinhaltet ACHILLES auch eine Erhebung der rechtlichen Rahmenbedingungen. Alle als relevant ermittelten rechtlichen Aspekte inklusive der Haftungsumfänge für das Risikomanagement wurden in einem Buch zusammengefasst.

Die praxisnahe Einbindung des entwickelten Softwareprototyps wird nicht nur im Rahmen der Planung von Rehabilitierungsstrategien an mehreren Bedarfsträgern getestet, sondern auch bei der Implementierung von Wassersicherheitsplänen (herausge–geben von der WHO) eingesetzt. Dies beinhaltet außerdem die Erprobung des Planungswerkzeugs für den Notfall.

Endresultat von ACHILLES ist ein Schwachstellenidentifizierungssystem inklusive Planungswerkzeug, das auf jeden Bedarfsträger anwendbar ist und mit dem eine erhöhte Versorgungs- bzw. Entwässerungssicherheit in der urbanen Wasserwirtschaft erreicht werden kann.

Für dieses Ziel werden themenspezifische „Vulnerabilitätskarten", die mit dem entwickelten Werkzeug erstellt werden, als Grundlage verwendet. Die Anwendungsmöglichkeiten dieser Karten sind weit umfangreicher als vor Beginn des Projektes erwartet. Allein zum Thema Kontamination lassen sich Karten bereitstellen, auf deren Basis Schutzzonen bei Bedrohung, Sensoren zur frühzeitigen Detektion, Stellen zur optimalen Ausspülung und Eintragsbereiche zur Desinfektion von Verunreinigungen etc. festgelegt werden können. Darüber hinaus wurden mit Hilfe der Vulnerabilitätskarten nicht nur neue Schwachstellen entdeckt, sondern auch die bekannten Achillesfersen von Versorgungssystemen bestätigt.

Bedarfsträger profitieren jedenfalls von dem im Rahmen von ACHILLES entwickelten Planungswerkzeug, das im Regelbetrieb ebenso zum Einsatz kommen kann wie im Notfallbetrieb. Daher ist zur Weiterentwicklung und Verbreitung auf regionaler Ebene (mit Deutschland und/oder Italien) die Durchführung von Interreg-Projekten geplant. Im Rahmen dieser Projekte soll die Methodik dahingehend weiterentwickelt werden, dass diese auch die spezifischen Anforderungen eines grenzübergreifenden Versor-

Der sonst friedliche Höttingerbach ist für die Wasserinfrastruktur der Stadt Innsbruck eine regelmäßige Gefahr

Überflutungen bringen in der Regel Kontamination und Ausfall der Wasserversorgung mit sich (Bild: Göfis/V)

gungsgebietes erfüllt und auf regionaler Basis strukturelle Anpassungen planen lässt.

Ferner ist im Anschluss von ACHILLES ein Forschungsprojekt geplant, das Risiken und Auswirkungen von Rohrschäden für die Bevölkerung im Detail untersuchen soll. Im Zuge dieses Projektes wird auch die Möglichkeit einer Erweiterung der Methodik auf die Fernwärme- und Gasinfrastruktur in Betracht gezogen. Bereits im Gange ist die Entwicklung eines Projektes zur Schnittstellenrealisierung mit einem von der Universität für Bodenkultur entwickelten Fehlermeldesystem (FEIS-Projekt).

Ein wesentliches Ziel des Projektkonsortiums ist auch die gemeinsame Vermarktung der Entwicklungsergebnisse. In Österreich gibt es rund 180 bis 200 größere Wasserversorgungsunternehmen. Ziel ist ein flächendeckender Einsatz in grenzübergreifenden Regionen. Als Erfolgsbeispiel kann das ORTIS Risikomanagementsystem (ein Projektpartner von ACHILLES) angeführt werden, welches in Tirol bei jeder Gemeinde implementiert wird.

Da das Sicherheitssystem ACHILLES auch international vertrieben werden soll, stellt Österreich aber nur einen Anteil am gesamten möglichen Markt dar. Da auch international die Versorger mit immer höher werdenden Ansprüchen der Konsumenten und Gewerbetreibenden konfrontiert sind, ist die Gewährung der Versorgungssicherheit in der Trinkwasserwirtschaft unumgänglich. Geografisch ist insbesondere in Osteuropa und in den Entwicklungsländern mit hohen Wachstumsraten für ein derartiges System zu rechnen.

Projektleitung:

Universität Innsbruck, Institut für Infrastruktur

Projektpartner:

– Universität Innsbruck, Institut für Öffentliches Recht, Staats- und Verwaltungslehre
– alpS – Zentrum für Naturgefahren- und Risikomanagement GmbH
– hydro-IT GmbH
– Ingenieurbüro Passer & Partner Ziviltechniker GmbH
– Stadtwerke Hall in Tirol GmbH
– Marktgemeinde Götzis
– Gemeinde Göfis
– Innsbrucker Kommunalbetriebe Aktiengesellschaft
– Amt der Tiroler Landesregierung, Abteilung Wasserwirtschaft

Kontakt:

Dipl.-Ing. Dr. techn. Michael Möderl
Universität Innsbruck, Institut für Infrastruktur
6020 Innsbruck, Technikerstraße 13
Tel.: +43/512/507-6918
Fax: +43/512/507-2911
E-Mail: michael.moederl@uibk.ac.at
Web: umwelttechnik.uibk.ac.at

AREA-MUMOSIS next

Multimodales Sicherheitssystem zur Überwachung von Flughafen-Flächen – Demonstrationssystem

Im Rahmen von AREA-MUMOSIS next soll ein Demonstrationssystem für ein effizienteres System zur Überwachung von Flughafenflächen entwickelt und installiert werden.

Ziel des vorangegangenen Projektes „AREA-MUMOSIS" war es, ein Pilotsystem für ein multimodales Monitoring-System zu entwickeln, mit dessen Hilfe Flächen von Flughäfen effizient und effektiv überwacht werden können.

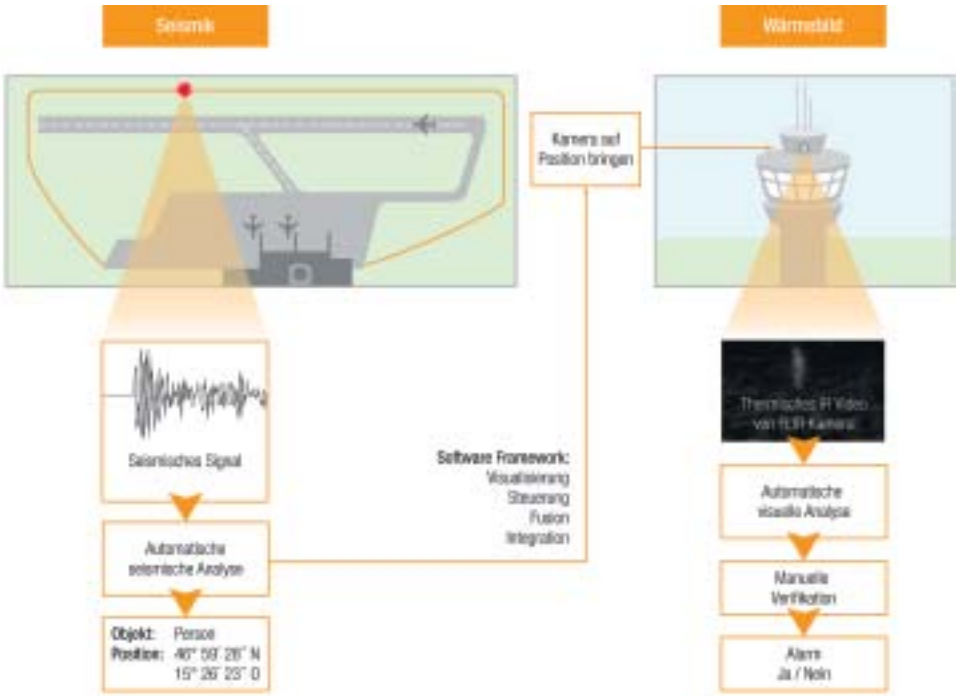
Durch den Einsatz verschiedenartiger Sensoren und einer anschließend intelligenten Verarbeitung und Verknüpfung der Detektionsergebnisse soll die Sicherheit der Flughafenflächen gewährleistet werden. Im Rahmen des Projektes „AREA-MUMOSIS next" soll auf den bisherigen Ergebnissen aufbauend auf dem Gelände des Flughafens Graz ein Pilotsystem installiert und im Rahmen eines Langzeittests evaluiert werden. Dabei werden gesellschaftliche und auch sozialwissenschaftliche Aspekte ausgewertet, die direkt in die Entwicklungsarbeiten einfließen.

Das mit AREA-MUMOSIS entwickelte Sicherheitssystem verarbeitet Signale von zwei Modalitäten bzw. Sensorarten:

- Der erste Sensor ist ein Lichtwellenleiter (LWL), der als seismischer Sensor arbeitet und in einer Tiefe von etwa 30 bis 50 Zentimetern und auf einer Länge von bis zu 40 Kilometern vergraben wird. Der seismische Sensor liefert Signale mit einer geografischen Genauigkeit von zehn Metern und ist durch das Vergraben weder durch Blitzschlag noch Sabotage gefährdet. Weiters kann das seismische Signal auch akustisch hörbar gemacht werden, wodurch Schritte oder dergleichen von anderen Geräuschen gut unterscheidbar sind. Zur weiteren Identifizierung eines Objektes wurden eigene Detektionsalgorithmen entwickelt, die zwischen Personen, Tieren und Fahrzeugen unterscheiden können.
- Ergänzt wird der seismische Sensor durch eine Thermalkamera, die auf die geografische Position des möglichen Alarms geschwenkt werden kann. Durch die Verwendung einer Wärmebildkamera wurden übliche Schwierigkeiten in der Bildverarbeitung auf ein Minimum reduziert. Ein Problem entsteht jedoch durch das ständige Monitoring bei Tag und Nacht und die sich kontinuierlich ändernde Hintergrundtemperatur. Durch ein ständiges Lernen von einem Hintergrundbild und Tracking (Verfolgen) der Vordergrundobjekte wird dieses Problem gelöst. Die Klassifizierung erfolgt durch die Geometrie der Region als Person, Fahrzeug, Tier oder als undefiniertes gefährliches Objekt (Trajektorienanalyse). Die Videodetektion der Thermalkamera ist aber nicht nur nach der Signalisierung durch den seismischen Sensor aktiv, sondern laufend, um Objekte zu sehen, die durch den seismischen Sensor nicht detektiert wurden.

Der große Vorteil des entwickelten Konzeptes liegt vor allem in der vergleichsweise kostengünstigen Installation. Darüber hinaus arbeitet das System aber auch bei Sichtbehinderung durch Dunkelheit oder Nebel (natürlich oder künstlich) zu 100 Prozent. Aufbauend auf AREA-MUMOSIS wurden daher im Zuge von „AREA-MUMOSIS next" gemeinsam mit dem Flughafen Graz als Bedarfsträger und in enger Kooperation mit allen Partnern die Spezifikationen für ein multimodales Sicherheitssystem für Flughafenflächen erarbeitet. Weiters wurden die Schnittstellen zwischen den einzelnen Systemen und Komponenten definiert und die ausgewählten Hardwarekomponenten im Labor ersten Funktionstests unterzogen.

Die für AREA-MUMOSIS entwickelten Algorithmen wurden für die Erfordernisse dieses Projektes adaptiert. Während im Vorgängerprojekt eine statische Kamera ein fixes Blickfeld beobachtete, wird die Kamera in AREA-MUMOSIS next so eingesetzt, dass sie



Schematische Darstellung des Konzepts für ein zukünftiges Sicherheitssystem für regionale Flughäfen

auf einer variablen Schwenk-Neige-Vorrichtung montiert ist und damit einen viel größeren Einsatzbereich einsehen kann. Mit diesem veränderten Ansatz ist es nun möglich, eine Rollbahn mit zirka fünf Kilometern Länge mit nur zwei Thermalkameras einzusehen, wobei alle notwendigen Blickfelder auf der Rollbahn in kurzer Zeit (ca. fünf Sekunden je Blickfeld) durchlaufen werden.

Auf Basis der extrahierten, seismisch-visuellen Merkmale können bestimmte Ereignisse detektiert werden, die für sich allein nicht ausreichend sind, um eine Alarmierungssituation zu erkennen, aber eine wesentliche Teilinformation darstellen. Diese werden daher als Elementarereignisse bezeichnet. Erst durch die Fusion der erkannten Elementarereignisse kann man auf Situationen rückschließen, die zu einer Alarmierung führen sollen. Als Schnittstelle zwischen den Detektoren, der Ereignisverarbeitung und der Alarmierung bzw. dem User-Interface wurde mit dem „RealtimeEventManager" ein spezifisches Softwaremodule entwickelt, implementiert und getestet. Etwaige Optimierungen werden vor Beginn des geplanten Langzeittests durchgeführt.

Weiters wurde ein Konzept für die Bedienungsoberfläche erstellt. Das Zentrum für Soziale Innovation führt dazu einen Usabilitytest mit dem Personal des Flughafens Graz durch, dessen Ergebnisse in das endgültige Design der Benutzeroberfläche einfließen.

Nach der Installation aller Hardwarekomponenten (in Summe werden 3,3 Kilometer LWL verlegt) erfolgt im Sommer 2011 ein erster Test der Anlage. Dieser dient vor allem dem Sammeln von seismischen und visuellen Daten zur Weiterentwicklung und Optimierung der Detektionsalgorithmen. Von Jänner bis Mai 2012 soll ein Langzeittest der Anlage stattfinden, bei dem das System im 24-Stunden-Betrieb eingesetzt werden soll.

Projektleitung:

JOANNEUM RESEARCH Forschungsgesellschaft mbH

Projektpartner:

– JOANNEUM RESEARCH Forschungsgesellschaft mbH
– Flughafen Graz Betriebs GmbH
– Siemens AG Österreich Building Technologies
– Bundesministerium für Landesverteidigung und Sport (BMLVS)
– Zentrum für Soziale Innovation

Kontakt:

JOANNEUM RESEARCH Forschungsgesellschaft mbH
Dipl.-Ing. Dr. Franz Graf
8010 Graz, Steyrergasse 17
Tel. +43/316/876-1631
E-Mail: franz.graf@joanneum.at
Web: www.joanneum.at

M²DynS

Multimodale Überwachung und Sicherung von Spezialobjekten durch dynamische Sensornetzwerke

Im speziellen Umfeld von Einrichtungen der Energieversorgung entwickelt das Projekt M²DynS ein System zur multimodalen Detektion sicherheitsrelevanter Ereignisse.

Kritische Infrastrukturen zeichnen sich durch einen hohen Vernetzungsgrad und damit einhergehender Komplexität aus. Ausfälle in einzelnen Bereichen können sich kaskadenartig ausbreiten und infolgedessen kaum abschätzbare Folgen nach sich ziehen. Dies gilt insbesondere für Einrichtungen der unmittelbaren und mittelbaren Energieversorgung.

Das Ziel eines multimodalen Ansatzes ist, die Detektionsgenauigkeit bei gleichzeitiger Verminderung der Fehlalarmrate in komplexen Umgebungen zu erhöhen. Außerdem sollen die zusätzlichen Informationen Ereignisse detektierbar machen, welche bisher nicht detektierbar waren. Im Rahmen des Projektes „M²DynS – Multimodale Überwachung und Sicherung von Spezialobjekten durch dynamische Sensornetzwerke" soll daher erstmalig eine Reihe unterschiedlicher Sensormodalitäten in Form eines dynamischen Sensornetzwerks zu einem multimodalen Sicherheits- und Überwachungssystem kombiniert werden.

Neben herkömmlichen Videokameras kommen auch Wärmebildkameras zum Einsatz. Auf die besonderen Eigenschaften von Wärmebildern wird mit der Erforschung und Entwicklung von spezieller Algorithmik für diesen Fall Rücksicht genommen. Im Verbund mit anderen Sensoren werden sogenannte Schwenk-Neige-Zoom-Kameras (SNZ-Kameras) eingebunden. Für diese Art der Kameras wird eine neuartige bildverarbeitende Algorithmik entwickelt.

Als Ergänzung zu den visuellen Sensormodalitäten werden zudem Kombinationen von Körper- und Luftschallsensoren eingesetzt. Je nach Art des Sensors werden entsprechende Verarbeitungsalgorithmen erforscht.

Bei SNZ-Kameras wird die Analyse von Videos durch die Eigenschaft erschwert, dass sich auch der Bildausschnitt dynamisch ändern kann und die Videoanalyse somit auf geänderte Kameraeinstellungen reagieren muss. Im Rahmen von M²DynS wird ein Algorithmus zur Detektion von ungewöhnlichen Ereignissen („Unusual Scene Detector") speziell für den Einsatz mit SNZ-Kameras weiterentwickelt. Bei diesem Verfahren wird ein Modell der Normalität eingelernt und über das Auftreten von Abweichungen informiert. Kombiniert mit Erkenntnissen, die von anderen Sensoren stammen – wie im Projekt auch aus der akustischen Detektion –, erfolgt in einem leistungsfähigen Fusionsmodul die Zusammenführung der unterschiedlichen Ergebnisse. Dieses Modul wurde auch für die Integration von weiteren Sensoren vorbereitet.

Weiters werden in Anbetracht der bekannten Vorbehalte gegenüber identifizierenden Sicherheits- und Überwachungstechnologien im Rahmen des Projektes M²DynS Anonymisierungstechniken in einem multimodalen Umfeld entwickelt und erprobt. In alle Projektphasen ist zudem ein unabhängiger Datenschutzexperte involviert.

Zur Erarbeitung der theoretischen Grundlagen wurde zunächst auf das umfangreiche Know-how zurückgegriffen, das die Projektpartner aus ihrer allgemeinen Forschungs- und Entwicklungsarbeit sowie aus ihrer Tätigkeit in den vorangegangenen Projekten im Sicherheitsforschungsprogramm KIRAS – iObserve und iObserve NG – beziehen. Zur Erhebung des aktuellen Standes der Wissenschaft wurde außerdem eine umfangreiche Recherche in aktuellen Publikationen aus dem Arbeitsbereich durchgeführt. In Kooperation mit dem Bedarfsträger wurden umfangreiche Testdaten sowohl im akustischen als auch im

M²DynS entwickelt ein multimodales System zur Überwachung von Spezialobjekten der Energieversorgung

bildgebenden Bereich gesammelt. Diese Daten werden für eine Evaluierung bestehender Verfahren und als Basis zur Entwicklung neuer Verfahren genutzt. Darauf aufbauend wird eine längerfristige Erprobung bei Anlagen des Bedarfsträgers vorbereitet.

Die bisherigen Ergebnisse des Projektes M²DynS haben gezeigt, dass der verfolgte Ansatz brauchbare Erkenntnisse liefert und somit zur Erhöhung der Sicherheit von kritischen Infrastrukturen der Energieversorgung beitragen kann. Zusätzlich wird die Betriebs- und Ausfallssicherheit erhöht. Weiters ergibt sich durch die automatisierte Überwachung der Anlagen und umgehende Alarmierung bei Abweichungen ein Kostenvorteil für die Betreiber der Anlagen.

Die Anforderungen für die Sicherung und Überwachung von Einrichtungen der Energieversorgung gelten auch für andere Bereiche der Energieversorgung. In der Stromversorgung treten Kraftwerke, Stauseen, Umformer und andere an die Stelle der infrastrukturellen Einrichtungen. Das generische Systemkonzept macht das System zudem auch im klassischen Überwachungsbereich (Public Safety) einsetzbar.

Daneben bietet sich die große Chance, an dem rapide wachsenden Markt der intelligenten Sicherheits- und Überwachungssysteme überdurchschnittlich zu partizipieren. Folgt man den einschlägigen Studien in diesem Bereich, ist mit einer Wachstumsrate von jährlichen 20 Prozent in diesem Marktsegment für die nächsten fünf Jahre zu rechnen. Das Nachfragepotenzial ist dabei nicht auf den nationalen Markt beschränkt.

Projektleitung:

Center Communication Systems GmbH

Projektpartner:

– JOANNEUM RESEARCH Forschungsgesellschaft mbH
– OMV AG

Kontakt:

Center Communication Systems GmbH, Abteilung Development Image Processing
Dipl.-Ing. Martin Forster
1210 Wien, Ignaz-Köck-Straße 19
Tel.: +43/1/90199-1304
E-Mail: m.forster@centersystems.com
Web: www.centersystems.com

MoSeS4eGov

Model-based Security System for eGovernment

In MoSeS4eGov werden modellbasierte Technologien entwickelt, um die Erstellung und Integration von Anwendungen in eGovernment-Systemen zu vereinfachen.

Aktuelle eGovernment-Systeme zeichnen sich durch eine hohe Funktionalitätsvielfalt, viele unterschiedliche Anwendungen und viele Schnittstellen zu den unterschiedlichen IT-Systemen aus. Diese Umstände erschweren nicht nur die Wartung bestehender Anwendungen, sondern behindern oder verhindern mitunter auch die Entstehung neuer Anwendungen. Änderungen an den Rahmenbedingungen (Gesetzesänderungen, Technologiewechsel etc.) resultieren in komplexen Folgeoperationen an den betroffenen Softwaremodulen.

Im Projekt „MoSeS4eGov – Model-based Security System for eGovernment" soll unter Verwendung von modellbasierten Ansätzen (MDA – Model Driven Architecture) ein Lösungsweg für dieses Problem aufgezeigt werden. Der Schwerpunkt liegt dabei auf der Kombination der Modellierung von fachlichen Anforderungen mit den Sicherheitsanforderungen.

Zusätzlich zu organisatorischen Maßnahmen muss die eingesetzte Software in Bezug auf Datensicherheit „state of the art" sein. Es bedeutet einen hohen Aufwand für den einzelnen Softwarehersteller bzw. -entwickler, in Bezug auf sicherheitsrelevante Aspekte auf dem letzten Wissensstand zu sein und alle Lösungen up to date zu halten. Im Projekt MoSeS4eGov wird daher an einer Lösung gearbeitet, um Sicherheitsanforderungen auf einer logischen Ebene zu formulieren, umfassend zu modellieren und einen professionellen Code zur Sicherstellung dieser Anforderungen zu generieren. Unternehmen, die diese Komponenten in ihren Lösungen einsetzen, sind wettbewerbsfähiger, da sie ihren immer sensibler werdenden Kunden einen Mehrwert in Bezug auf Sicherheit garantieren können. Softwareunternehmen (oder -abteilungen) werden wettbewerbsfähiger, weil sie ohne die derzeit erforderlichen erheblichen Zusatzaufwände in der Erstellung und Wartung von security-relevanten Codes in ihren Lösungen auskommen bzw. zum selben Preis qualitativ höherwertige Software herstellen können.

Das Projekt MoSeS4eGov leistet durch seinen integrativen Ansatz der Verknüpfung unterschiedlicher Datenquellen und neuer Modellierung von bestehenden eGovernment-Prozessen und deren Sicherheitsanforderungen einen wesentlichen Beitrag zum Schutz der kritischen Infrastruktur „Verwaltung".

Im ersten Schritt des Projektes erfolgt die Analyse und Definition der Anforderungen für den Anwendungsfall. Weiters wird eine Pilotapplikation entwickelt, um Einsatzorganisationen im Katastrophenfall schnelle, aktuelle und gesicherte Informationen auf Basis bestehender Standards und Protokolle zur Verfügung zu stellen. Diese soll die Einsatztauglichkeit unseres modellbasierten Ansatzes im Umfeld des Katastrophenmanagements zeigen. Konkret soll im Falle einer Katastrophe beispielsweise einem Einsatzleiter die Möglichkeit gegeben werden, über das zentrale Melderegister (ZMR) demografische Daten über die Bevölkerungsstruktur in einem gewissen Gebiet zu erhalten. Dazu zählen beispielsweise die Anzahl der gemeldeten Personen oder die Altersstruktur.

Ein wichtiger Aspekt im Projekt ist auch die datenschutzrechtliche Betrachtung von Anwendungsfällen. Dazu erfolgt im Rahmen des Projektes eine sozialwissenschaftliche Studie inklusive Befragung betroffener Bevölkerungsgruppen, um die Bereitschaft der Bevölkerung zu untersuchen, im Katastrophenfall auch eine teilweise Einschränkung beispielsweise von Privacyaspekten zu akzeptieren. Weiters untersucht ein juristisches Gutachten die im Projekt und in der Pilotapplikation implementierten Funktionalitäten in Bezug auf Datenschutz und andere rechtliche Aspekte.

In weiterer Folge wird eine Risikoanalyse durchgeführt, um mögliche Bedrohungspotenziale für die Art

Eine Pilotapplikation liefert im Katastrophenfall schnelle und gesicherte Informationen

von Applikationen im Allgemeinen und die Pilotapplikation im Speziellen zu ermitteln. Basierend darauf werden die Sicherheitsanforderungen für das System definiert. Auch dabei werden die spezifischen Aspekte der österreichischen eGovernment-Umgebung (PVP etc.) berücksichtigt.
Danach erfolgt in zwei Iterationen die Umsetzung der Technologien und der Pilotapplikation.

Nach Erstellung eines Metamodells und Entwicklung entsprechender Generatoren erfolgt die Modellierung und Umsetzung der Modelle. Die Entwicklung der Modellierungsmethode erfolgt auf der Plattform „Openmodels" (http://www.openmodels.at) der „Open Models Initiative". Dadurch können die erarbeiteten Modelle leicht ausgetauscht und wiederverwendet werden.

Das gesamte System wird dann zur Umsetzung der Pilotapplikation verwendet.

Ergänzend zur Modellierungsumgebung wird im Projekt auch ein Endpunktsimulator entwickelt, eine Komponente, die zum Testen und Zertifizieren von SOA-basierten eGovernment-Applikationen verwendet werden kann. Ziel ist das Sicherstellen der Einhaltung der Sicherheitsrichtlinien, die Protokollierung der Testabläufe sowie das Entdecken von Sicherheitslücken.

Schließlich erfolgt neben Erstellung einer Projektdokumentation eine Evaluierung der entwickelten Methoden, um diese in weiteren Entwicklungsprojekten effizient einzusetzen und die Nachhaltigkeit der Projektergebnisse sicherzustellen.

Projektleitung:

AIT Austrian Institute of Technology GmbH, Safety & Security Department

Projektpartner:

– Bundesministerium für Inneres (BMI)
– Bundesministerium für Landesverteidigung und Sport (BMLVS)
– PL.O.T EDV-Planungs- und Handels GesmbH
– Sphinx IT Consulting GmbH
– BOC Asset Management GmbH
– Secure Business Austria
– Donau Universität Krems
– JOANNEUM RESEARCH Forschungsgesellschaft mbH

Kontakt:

AIT Austrian Institute of Technology GmbH, Safety and Security Department
Dipl.-Ing. Thomas Bleier
2444 Seibersdorf
Tel.: +43/664/8251279
E-Mail: thomas.bleier@ait.ac.at
Web: www.ait.ac.at/it-security

Networked miniSPOT

On-the-spot-Ereigniskennung mit Low-cost-Minikameramodulen und Kommunikation über robuste Netzwerke der Gebäudeautomation

Das Projekt Networked miniSPOT verfolgt das Ziel, ein Gesamtkonzept umzusetzen, in dem Bilddaten ausschließlich ereignisgesteuert über Netzwerke der Gebäudeautomation weitergeleitet werden.

Bisher greifen Sicherheitszentralen auf Bilddaten zumeist über Analognetzwerke zu. Für den bevorstehenden Wegfall dieser Technologie muss ein Ersatz gefunden werden. IP-basierte Netzwerke als Alternative sind oftmals nicht oder nur durch erheblichen Kostenmehraufwand realisierbar. Das Projekt „Networked miniSPOT" liefert wertvolle Beiträge, um alternative Lösungen zu entwickeln.

Technologisch ermöglicht wird das Projekt durch Entwicklungen in der Videoanalyse, durch den Einsatz von Minikameramodulen sowie durch die Anpassung der zumeist schmalbandigen Netzwerke der Gebäudeautomation (Heizung, Lüftung, Klima, Elektrotechnik). Darauf aufbauend verfolgt Networked miniSPOT im Wesentlichen zwei Ziele:

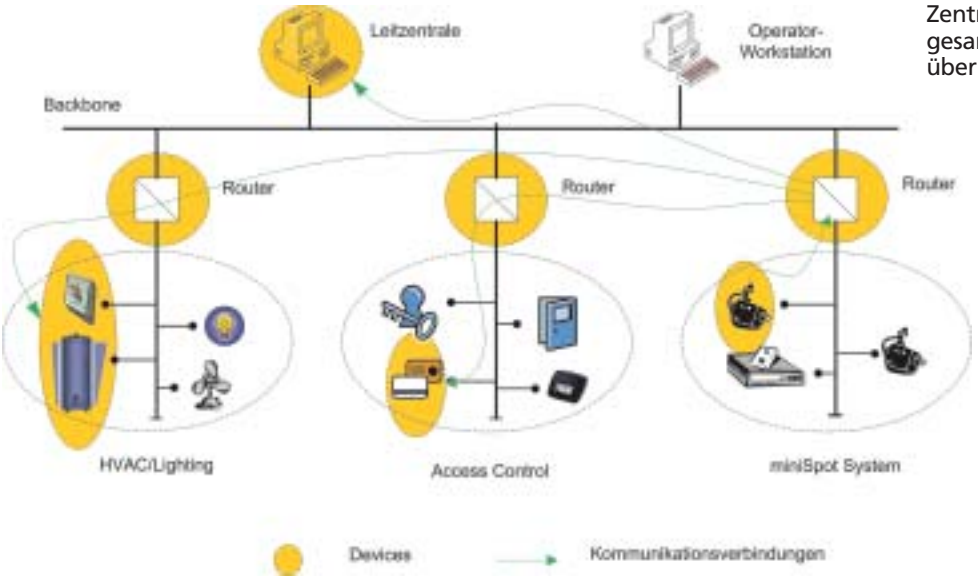
- Nutzung eines gemeinsamen Datenkanals für mehrere Anwendungen oder Aufgabengebiete und die Vor-Ort-Bildauswertung sowie
- Vor-Ort-Bildauswertung der Minikameras.

Als Anwendungsmöglichkeit seien zum Beispiel Zweckbauten zur Energieerzeugung, aber auch Kühlhäuser genannt, die allesamt üblicherweise bereits über einen hohen Grad an Gebäudeautomation verfügen und sich darüber hinaus hervorragend für eine Nachrüstung mit einem solchen System eignen. Ein weiteres wichtiges Anwendungsfeld für die entwickelten Hardwarekomponenten, insbesondere des Bildaufnahme und -verarbeitungssystems ist der Einsatz im Gesundheits- und Pflegebereich, in dem mit herkömmlichen Kameras oft ein Eindringen in die Privatsphäre assoziiert wird.

In einem ersten Schritt des Projektes wurden der aktuelle Stand der Forschung ermittelt und sicherheitskritische Szenarien definiert. Grundlage für die gemeinsame Erarbeitung der Szenarien stellten umfangreiche systematische, strukturierte Beobachtungen bei der Testinstallation der Firma Hel-Wacht im 9. Wiener Gemeindebezirk vor Ort sowie mithilfe des aufgenommenen Videomaterials dar. Die Testinstallation kam danach in zwei Szenarien zum Einsatz – einerseits in einem Personenlift und andererseits in einer Garage, wobei beides viel frequentierte Anwendungsbereiche sind.

Zusätzlich wurden im Rahmen des ersten Projektjahres sogenannte „Single Board Computer" als Hardwareknoten ausgewählt, die für die Vor-Ort-Bildauswertung zuständig sein werden. Im Bereich der automatischen Auswertung der Bilddatenströme wurde eine Analyse der bereits verfügbaren Algorithmen zur Personenerkennung und -verfolgung durchgeführt. Nach ausführlichen Tests stellte sich heraus, dass sich im konkreten Fall der Ansatz des „Histogram of Oriented Gradients" am besten eignet. Dieser muss im Unterschied zu anderen Methoden keine Hintergrundmodelle lernen. In einer Lernphase werden dabei verschiedene Personenmodelle trainiert, die in der Detektierungsphase im Video wiedergefunden werden. Da Personen in jedem Bild und in verschiedenen Größen vorkommen können, ergibt sich eine hohe Rechenintensität, die aber durch die Entwicklung von geeigneten Algorithmen drastisch gesenkt werden konnte, sodass auch der Einsatz am Single-Board-Computer sichergestellt war. Um die Redundanz der Bilddaten aus verschiedenen Blickrichtungen miteinander verbinden zu können, wurde ein Verfahren entwickelt, das die Daten fusioniert und in ein gemeinsames 3D-Koordinatensystem bringt.

Im Bereich der Netzwerktechnik wurden im ersten Abschnitt des Projektes zwei unterschiedliche Herangehensweisen in der Verkabelungstopologie getestet und analysiert. Sowohl der zentrale, als auch der dezentrale Ansatz wurden untersucht. In einer zentralen Netzwerktopologie ist die gesamte Kommunikation durch ein gemeinsames Kontrollzentrum ge-



Zentraler Netzwerkaufbau: Die gesamte Kommunikation wird über eine Leitzentrale organisiert

Personendetektion im Video unter Verwendung des „Histogram of Oriented Gradient"-Verfahrens

steuert. Alle miniSPOT.net-Knoten senden die Informationen an eine gemeinsame Anlaufstelle, die dann über die weitere Vorgehensweise entscheidet und mögliche Sicherheitsmaßnahmen einleitet. Im Gegensatz dazu erfolgt in einem dezentralen Ansatz die Kommunikation zwischen verschiedenen Knoten direkt und ohne gemeinsame, zentrale Anlaufstelle. Der Empfänger einer Nachricht entscheidet direkt, was in einem nächsten Schritt passieren soll. Beide Netzwerkausrichtungen wurden im Rahmen des Projektes getestet und sind in der Testinstallation zum Einsatz gekommen. Weiters wurden verschiedene Netzwerkprotokolle implementiert und auf ihre Einsetzbarkeit in Hinblick auf das Projekt analysiert.

Die sozialen und gesellschaftlichen Aspekte des vorgeschlagenen Konzeptes finden im Rahmen eines eigenen Arbeitspakets angemessene Berücksichtigung. Die Analyse konzentriert sich auf die Bestimmung der gesellschaftlichen Implikationen der zu entwickelnden automatischen Videoüberwachungs- und -auswertungssysteme. Dabei sind im Projekt besonders datenschutzrechtliche Aspekte relevant, die sich aus der geplanten tiefgreifenden Harmonisierung und Integration von Überwachungstechnik und Gebäudeautomation ergeben. Dies umfasst die Art der Verwendung der generierten Daten einschließlich der Möglichkeiten und Maßnahmen gegen Zugriff, Manipulation und missbräuchlicher Verwendung von Dritten. Vor diesem Hintergrund ergeben sich in Bezug auf die Eingliederung von Sicherheits- und Schutztechnologien in bestehende Systeme der Gebäudeautomation besondere und neue Herausforderungen, die im gesamtgesellschaftlichen Kontext zu diskutieren sind. Zusätzlich wird das bewährte sozialwissenschaftliche und ethnografische Methodeninventar durch Videografie bzw. -analyse und durch Interaktivitätsexperimente zwischen Mensch und technischem System erweitert. Um Platz für eine interdisziplinäre Gestaltung und Konfiguration soziotechnischer Systeme zu schaffen, werden diese Fragen bereits im Prozess der technischen Entwicklung durch die Einbeziehung nicht nur aller am Projekt unmittelbar beteiligten Institutionen und Personen, sondern auch eines erweiterten Kreises von Rechtsexperten, Gebäudenutzern und weiteren Akteuren der Zivilgesellschaft bearbeitet.

Projektleitung:

CogVis Software und Consulting GmbH

Projektpartner:

– TU Wien – AB Automatisierungssysteme
– TU Wien – AB Computer Vision Lab
– Hel-Wacht Holding GmbH
– Institut für Höhere Studien

Kontakt:

CogVis GmbH
Dipl.-Ing. Michael Brandstötter
1090 Wien, Pulverturmgasse 3
Tel.: +43/1/997 15 94-0
Fax.: +43/1/997 15 94-91
E-Mail: brandstoetter@cogvis.at

RSS

Railway System Security

Die Entwicklung und Erprobung einer neuartigen, einsatzoptimierten Schienenstahlgüte soll einen Beitrag zur Gewährleistung der Sicherheit im Bahnverkehr leisten.

Die Schiene mit ihren Aufgaben „Führen" und „Tragen" der Eisenbahnfahrzeuge ist die Grundlage für die hohe Sicherheit und die niedrige Unfallrate im Eisenbahnverkehr. Zukünftige Trends weisen klar in Richtung dichterer Zugfrequenzen, steigender Achslasten und höherer Reisegeschwindigkeiten, mit der Konsequenz, dass der Fahrweg deutlich erhöhte Belastungen ertragen muss. Versagt die Schlüsselkomponente des Fahrwegs – die Schiene–, so kann dies unmittelbar zu einer Gefährdung von Reisenden und Gütern sowie von den entlang von Bahnstrecken stehenden Gebäuden und deren Bewohnern führen.

International werden bereits in großem Umfang bisher noch wenig erforschte Schadensmuster an Schienen, wie z. B. Rollkontaktermüdungsschäden, festgestellt. Seit Kurzem treten derartige Schäden auch im Netz der ÖBB auf. Die ÖBB-Infrastruktur AG behebt diese Schäden dem Stand der Technik entsprechend und mit hohem Kosteneinsatz.

Um dieses Problem langfristig und nachhaltig zu lösen, werden im Rahmen des Projektes „RSS – Railway System Security" folgende Ansätze verfolgt:

- Entwicklung einer speziell angepassten Schienenstahlgüte. Schienenstahlgüten werden nach ihrer Härte – gemessen in Brinell (HB) – eingeteilt. Derzeit bestehen Standardgüten aus einem Phasengemisch aus Ferrit und Zementit (Perlit) und weisen eine Härte von 220 bis 260 HB auf. Diese kommen vor allem im Nahverkehr und bei Mischverkehr in der Geraden zum Einsatz. Für spezielle Anwendungsfälle wie in engen Bögen oder mit hohen Achslasten gibt es spezielle Güten, die bis zu 430 HB Härte aufweisen.

- Festlegung von Fahrzeugbelastungsgrenzwerten. Aufgrund der Interoperabilitätsanforderungen durch die EU sind diese aber nur bedingt oder nur sehr gut wissenschaftlich abgesichert durchsetzbar.

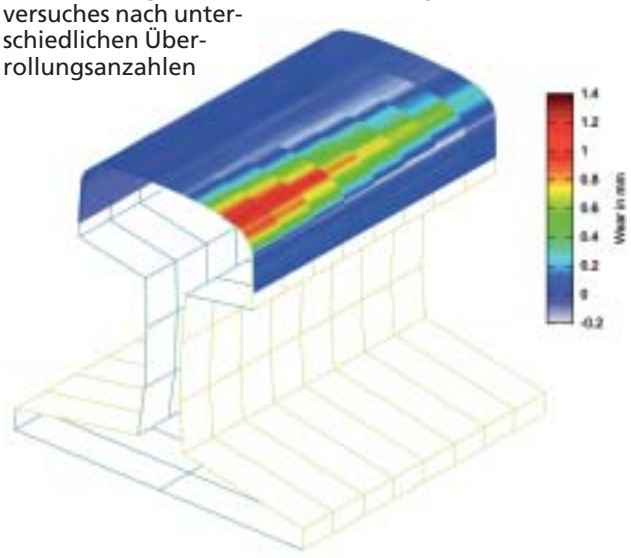
In einem ersten Schritt wurden vorhandene Hypothesen zur mathematisch physikalischen Beschreibung der Phänomene herangezogen, aus denen der Entwurf eines Systemmodells erstellt wurde. Dieser Prozess erstreckt sich über die ganze Länge des Projektes, da die Hypothesen aufgrund der aus dem Projekt gewonnenen Erkenntnisse ständig überprüft und redigiert werden und sich somit auch das Systemmodell verändert.

In einem weiteren Schritt wurde dieser erste Modellansatz an einer Standardschienenstahlgüte und an einer speziell entwickelten einsatzoptimierten Schienenstahlgüte unter Zuhilfenahme experimenteller Messtechnik auf einem speziellen Rad-Schiene-Prüfstand überprüft. Der spezielle Prüfstand stellt eine 1:1-Nachbildung des realen Rad-Schiene-Kontakts dar und ermöglicht so im Labor die Nachstellung realer Kontaktphänomene innerhalb einer sehr kurzen Zeitspanne.

Die Ergebnisse der Versuche haben klar die Überlegenheit der einsatzoptimierten Schienenstahlgüte im Vergleich zur Standardgüte in Bezug auf den Widerstand gegen Schienenverschleiß und Rollkontaktermüdungsschäden gezeigt. Die aus den Versuchen gewonnenen Mess- und Materialdaten wurden zur Überarbeitung und Verfeinerung des Systemmodells verwendet und auch zur Erstellung eines unterstützenden FEM-Simulationsmodells durch die TU Graz.

Der Vergleich zu den Prüfstandsversuchen erfolgt in einer ortsfesten Gleismessstelle, basierend auf dem Messsystem Argos® an einer hoch belasteten Strecke der ÖBB (Südbahn). Für diese spezielle Messstelle wurden von der voestalpine Schienen GmbH zwei spezielle Testschienen angefertigt, die beide Schienenstahlgüten (Standardgüte und einsatzoptimierte Güte) auf einem Schienenstück ohne Schweißung beinhalten. Der Einbau der mit spezieller Messtechnik

Visualisierung der Schienenabnutzung eines Prüfstandversuches nach unterschiedlichen Überrollungsanzahlen



Der erste Zug der ÖBB, der über die im Rahmen von Railway System Security entwickelte neue Messstelle fährt

bestückten Schienen und die Inbetriebnahme der In-Situ-Messstelle wurden vom Team Forschung & Entwicklung der ÖBB-Infrastruktur AG in enger Zusammenarbeit mit der Firma Hottinger Baldwin Messtechnik koordiniert und durchgeführt.

Die umfangreichen Signalverläufe der unterschiedlichen Sensortypen werden von der Firma BAMM mittels geeigneter Algorithmen in physikalische Größen umgewandelt, die die Fahrzeugwirkungen der Zugüberfahrt beschreiben. Die daraus generierten Daten werden strukturiert abgelegt und beschreiben detailliert für jede Messfahrt alle relevanten Parameter der Zugüberfahrt. Erst dadurch wird eine statistische Betrachtung von langfristigen Veränderungen der Schiene ermöglicht.

Aus den aus der Messstelle gewonnenen Daten und Erkenntnissen werden überarbeitete Prüfparameter für den Rad-Schiene-Prüfstand ermittelt, um reale Randbedingungen zu generieren, die einsatznahe Werkstofftests ermöglichen. Mit diesem neuen Parametersatz werden erneut Tests mit den beiden schon zuvor getesteten Schienenstahlgüten durchgeführt, um die Erkenntnisse zu verifizieren.

Im Anschluss daran soll ein neuer experimenteller Werkstoff auf dem Rad-Schiene-Prüfstand hinsichtlich seines Potenzials für ein deutlich verbessertes Einsatzverhalten untersucht werden. Begleitend wird auch das Simulationsmodell der TU Graz auf Basis der gewonnenen Daten verbessert werden, um die Vorgänge auf dem Prüfstand und im Gleis nachstellen zu können.

Schließlich sollen aus den aus Prüfstandversuchen und der In-Situ-Messstelle gewonnenen Erkenntnissen in Kombination mit der jeweiligen Schienenstahlgüte relevante Einsatzgrenzwerte erarbeitet werden. Diese werden herangezogen, um einerseits die Sicherheit des Systems weiter zu erhöhen und andererseits gleichzeitig eine Senkung des Instandhaltungsaufwands zu bewirken. Darüber hinaus werden die in diesem Zusammenhang definierbaren technischen Parameter als Basis für eine verursacherorientierte Verrechnung der Infrastrukturbeschädigung durch Fahrzeuge erarbeitet, die als Kalkulationsfaktoren für ein mögliches künftiges individuelles Infrastrukturbenützungsentgelt (IBE) verwendet werden können.

Projektleitung:

voestalpine Schienen GmbH

Projektpartner:

– ÖBB-Infrastruktur AG, Strecken- und Bahnhofsmanagement – Forschung und Entwicklung
– Dr. Mittermayr Scientific Consulting GmbH
– Technische Universität Graz, Institut für Leichtbau

Kontakt:

voestalpine Schienen GmbH
Dipl.-Ing. Richard Stock
8700 Leoben, Kerpelystraße 199
Tel.: +43/503 04 26-4148
Fax: +43/503 04 26-97
E-Mail: richard.stock@voestalpine.com

SHF2

Sicherheit von Hohlraumbauten unter Feuerlast – Entwicklung eines Struktursimulationstools

Das Forschungsprojekt „SHF2: Sicherheit von Hohlraumbauten unter Feuerlast – Entwicklung eines Struktursimulationstools" beschäftigt sich mit der Entwicklung eines realitätsnahen Berechnungsverfahrens zur Bestimmung der Struktursicherheit von Hohlraumbauten und Tragstrukturen bei einem Brand.

Die Sicherheit von Straßen- und Eisenbahntunnel oder Brückentragwerken wird nach der gängigen Ingenieurspraxis unter Zugrundelegung eines „linear-elastischen Materialverhaltens" bemessen. Dabei geht man davon aus, dass eine Belastung derartiger Baukörper zu einer elastischen Verformung führt, die proportional zu ihrer Einwirkung erfolgt. Die Feuerlast bei einem Brand kennzeichnet sich jedoch durch die Kombination aus einer thermischen und einer mechanischen Einwirkung. Die Annahme eines linear-elastischen Materialverhaltens gibt daher das Verhalten unter Feuerlast nicht realistisch wieder.

SHF2 setzt sich daher mit dem Lastfall Brand in einer ganzheitlichen Form auseinander: Brandlast, Temperaturbelastung sowie Strukturantwort. Ziel ist es, die Ingenieurpraxis hin zu einer realitätsnahen Analyse des Tragverhaltens von kritischen Infrastrukturbauten unter Feuerlast zu verbessern.

Um eine realistische Abbildung der wesentlichen Prozesse während und nach einem Brand darstellen zu können, werden dazu im Rahmen von SHF2 entsprechende Materialmodelle und Analysemethoden entwickelt und experimentell validiert. Diese werden anschließend mit einem neuartigen Berechnungsschema in ein numerisches Verfahren – das auf der im Ingenieurwesen verbreiteten „Methode der finiten Elemente" beruht – zusammengeführt.

Das derart entwickelte Struktursimulationstool soll in handelsüblichen Strukturprogrammen implementiert werden und damit in der Ingenieurpraxis die realitätsnahen Prognose des Strukturverhaltens unter Feuerlast ermöglichen.

Zur Darstellung des Mehrwertes für die Sicherheit kritischer Infrastruktur in Österreich wird das entwickelte Berechnungsverfahren im Rahmen von SHF2 auch auf konkrete Bauvorhaben angewandt. Damit wird das Verbesserungspotenzial gegenüber den derzeit üblichen (linear-elastischen) Berechnungsmethoden aufgezeigt.

Projektleitung:

Technische Universität Wien, Institut für Mechanik der Werkstoffe und Strukturen

Projektpartner:

– ARGE Bautech
– ASFiNAG Autobahn- und Schnellstraßen-Finanzierungs-Aktiengesellschaft
– Forschungsinstitut der Vereinigung der österreichischen Zementindustrie
– Ingenieurbüro Dr. Lindlbauer
– ÖBB-Infrastruktur Bau Aktiengesellschaft
– Schimetta Consult ZT GmbH
– Universität für Bodenkultur Wien, Institut für konstruktiven Ingenieurbau
– Universität Innsbruck, Materialtechnologie Innsbruck
– Wiener Linien GmbH & Co KG

Kontakt:

Technische Universität Wien, Institut für Mechanik der Werkstoffe und Strukturen
Dipl.-Ing. Dr. Matthias Zeiml
1040 Wien, Karlsplatz 13/202
Tel.: +43/1/58801-20240
Fax: +43/1/58801-920240
Mail: matthias.zeiml@tuwien.ac.at
Web: www.imws.tuwien.ac.at

SUEHC

Securing Urban Extramural Health Care

Securing Urban Extramural Health Care (SUEHC) entwickelt Modelle und Lösungsverfahren zur Touren- und Einsatzoptimierung mobiler Pflegekräfte in Krisen- und Katastrophenfällen.

Der steigende Bedarf an mobilen Pflegeleistungen erfordert eine effiziente Touren- und Einsatzplanung der Pflegekräfte

Sowohl der Bedarf an mobiler Pflege wie auch die Wahrscheinlichkeit von Naturkatastrophen soll in den nächsten Jahren steigen. Laut Statistik Austria (2011) bezogen in Österreich 2010 rund 430.000 Personen Bundes- oder Landespflegegeld. Da diese Zahl nur jene Personen beinhaltet, die staatliche Unterstützung erhalten, muss die tatsächliche Zahl Pflegebedürftiger deutlich höher eingeschätzt werden. Derzeit werden noch rund 80 Prozent der Pflegebedürftigen im Rahmen der informellen Pflege zu Hause durch nahe Angehörige oder Freunde versorgt. Der übrige Anteil entfällt auf den formellen Bereich der Pflege. Dieser beinhaltet die traditionellen Alten- bzw. Pflegeheime, Tageszentren sowie mobile soziale Dienste. Mit rund 80.000 betreuten Personen sind mobile Pflegedienste bereits zu einem vitalen Bestandteil des nationalen Gesundheits- und Pflegesystems geworden.

Aufgrund der derzeitigen demografischen und sozialen Entwicklungen ist in naher Zukunft nicht nur mit einem Anstieg des Pflegebedarfs, sondern auch mit einem drastischen Rückgang der informellen Pflegeleistungen zu rechnen. Dadurch ist im Bereich der formellen Betreuung, im Speziellen bei mobilen Diensten, ein weiterer Ausbau des Angebots zu erwarten. Laut einer Studie des Österreichischen Instituts für Wirtschaftsforschung (Mühlberger et al., 2008) weist das Szenario mit der größten Eintrittswahrscheinlichkeit dabei eine Gesamtausgabensteigerung von rund 159,7 Prozent auf. Der Anteil der Pflegekosten am realen BIP würde demnach zwischen 2006 und 2030 von 1,13 Prozent auf 1,96 Prozent steigen.

Sollte der bisherige Trend anhalten, ist in naher Zukunft aber auch mit einem Anstieg an Katastrophenereignissen zu rechnen. Pflegedienstleister stehen somit nicht nur vor den organisatorischen Herausforderungen, die sich durch den wachsenden Pflegebedarf ergeben, sondern müssen sich auch entsprechend gegen externe Störungen absichern. Trotz der großen gesellschaftlichen Bedeutung der mobilen Pflege, stellt diese im Bereich der Logistik und Katastrophenforschung immer noch ein relativ kleines Forschungsgebiet dar. Zur Touren- und Einsatzplanung in diesem Bereich gibt es bis dato nur eine überschaubare Anzahl wissenschaftlicher Arbeiten. Am bedeutendsten sind hier die Arbeiten von Eveborn et al. (2006 und 2009). Diese befassen sich mit der Tourenplanung für Pflegekräfte in Schweden und stellen die Tourenplanungssoftware „Laps Care“ vor. Diese kommt derzeit lediglich in skandinavischen Ländern zum Einsatz und ist aufgrund anderer Anforderungen (Arbeitsabläufe und gesetzliche Vorgaben) in Österreich nicht einsetzbar. Weitere wichtige Arbeiten stammen von Bräysy et al. (2007 und 2009), welche sich mit der Optimierung mehrerer mobiler sozialer Dienste (Essen auf Rädern, Heimpflege, Fahrtendienste) in einer finnischen Kleinstadt beschäftigen.

Arbeiten, die auch Aspekte des Risikomanagements berücksichtigen, konnten bislang nicht gefunden werden. Das Projekt „Securing Urban Extramural Health Care (SUEHC)“ und dessen Vorgängerstudie „Securing Extramural Health Care (SEHC)“ stellen daher – insbesondere durch die Kombination von quantitativen Optimierungsmethoden mit Elementen des Risikomanagements – ein Novum dar:

SEHC – Securing Extramural Health Care

Ziel des Projektes SEHC war es, gemeinsam mit dem Österreichischen Roten Kreuz (ÖRK), einen Softwareprototyp zu entwickeln, mit dem sich effiziente Touren- und Einsatzpläne für mobile Pflegedienste berechnen lassen. Dieser Prototyp sollte dabei sowohl im normalen Geschäftsbetrieb als auch in Katastrophenfällen anwendbar sein und dabei einen effizienten Einsatz der knappen Ressourcen sicherstellen. Weiters sollte er noch für Ex-ante- und Ex-post-Analysen von verschiedenen Katastrophenszenarien tauglich sein. Dazu wurden anhand von Testbezirken in Oberösterreich die Strukturen und Abläufe der mobilen Pflege erhoben und auf ihre Schwachstellen in Hinblick auf Naturkatastrophen untersucht. Danach wurden für die Testgebiete relevante Katastrophenszenarien identifiziert und die Auswirkungen dieser Szenarien auf relevante Attribute untersucht. In weiterer Folge wurde ein mathematisches Optimierungsmodell formuliert und mithilfe der Solversoftware Xpress verifiziert. Das direkte Ziel der Optimierung war es, die unproduktiven Zeiten (Fahr- und Wartezeiten) zu minimieren, gleichzeitig jedoch auch die Zufriedenheit der betreuten Personen sowie der Pflegekräfte zu maximieren. Da eine exakte mathematische Lösung nur für sehr kleine Probleminstanzen möglich ist, wurde in weiterer Folge ein eigenes Rechenverfahren basierend auf der Metaheuristik Variable Neighborhood Search implementiert und mit Realdaten umfangreich getestet.

SUEHC – Securing Urban Extramural Health Care

Im April 2010 startete das Nachfolgeprojekt SUEHC mit dem Ziel, die Ergebnisse aus dem Projekt SEHC auf den städtischen Raum zu übertragen. Gespräche mit dem Wiener Roten Kreuz ergaben, dass die Anforderungen in urbanen Regionen von denen in ländlichen Regionen abweichen. So nutzen in Städten mit guter öffentlicher Verkehrsinfrastruktur viele Pflegekräfte öffentliche Verkehrsmittel. Auch die sozialen Strukturen und die Bevölkerungsdichte sind nicht vergleichbar, diese beeinflussen aber maßgeblich die Auswirkungen von Katastrophenszenarien. Weiters wird der in SEHC entwickelte Prototyp in der Praxis getestet, um eine für den täglichen Einsatz geeignete Systemarchitektur zu erarbeiten. Zusätzlich soll die Akzeptanz eines solchen entscheidungsunterstützenden Systems untersucht werden.

Die Ergebnisse zeigen, dass es mit dem entwickelten SEHC-Prototypen möglich ist, trotz der hochgradigen Komplexität der Aufgabenstellung, die Touren- und Einsatzplanung von mobilen Pflegekräften effizienter zu gestalten. Der entwickelte Prototyp ist dabei in der Lage, auch für in der Praxis relevante Problemgrößen innerhalb kurzer Rechenzeit gute Ergebnisse zu liefern. Gerade in Katastrophenfällen lassen sich so die ohnehin knappen Ressourcen bestmöglich einsetzen und rasch auf neue Gegebenheiten reagieren. Neben der Berechnung von Touren- und Einsatzplänen lassen sich mit dem Prototyp aber auch Kapazitätsgrenzen und, in verschiedenen Katastrophensituationen, nicht versorgbare Klientinnen und Klienten ermitteln.

Projektleitung:

Universität für Bodenkultur Wien, Institut für Produktionswirtschaft und Logistik

Projektpartner:

– mobil data IT & Kommunikationslösungen GmbH
– Österreichisches Rotes Kreuz – Bereich Gesundheits- und soziale Dienste
– Salzburg Research Forschungsgesellschaft m.b.H.

Kontakt:

Universität für Bodenkultur Wien, Institut für Produktionswirtschaft und Logistik
Univ.-Ass. Mag. Dr. Patrick Hirsch
1180 Wien, Feistmantelstraße 4
Tel.: +43/1/476 54 44-19
Fax: +43/1/476 54 44-17
E-Mail: patrick.hirsch@boku.ac.at
Web: www.boku.ac.at

KIRAS
Sicherheitsforschung

Unterstützungsmaßnahmen

Programmlinie 4

BlackÖ.1

Blackouts in Österreich

Das Projekt „Blackouts in Österreich" (BlackÖ.1) analysiert die technischen, wirtschaftlichen und gesellschaftlichen Folgen von großflächigen Ausfällen im österreichischen Stromnetz.

Die zunehmende Belastung der Netze bei einem gleichzeitig zu geringen Ausbau der Infrastruktur lässt die Wahrscheinlichkeit großflächiger Stromausfälle mit katastrophalen Auswirkungen für die heimische Wirtschaft und Bevölkerung steigen. Während frühere Studien der Antragsteller (Brauner 2003; Reichl et al. 2006) nur Indizien für das Ausmaß und die Kosten derartiger großflächiger Stromausfälle geben konnten, gibt der erste Teil des Projektes „Blackouts in Österreich" (BlackÖ.1) eine hinsichtlich des Detailgrads sowohl für Österreich als auch im europäischen Raum einzigartige Bottom-up-Analyse der kaskadenartigen Ausfallswirkung, der Schadenskosten, der Betroffenenstruktur und der Wahrscheinlichkeiten großflächiger Stromausfälle.

Im ersten Projektschritt werden mögliche Ursachen von Blackouts spezifisch für die Ist-Situation in Österreich analysiert. Weiters wird analysiert, wie anfällig die Netze auf punktuelle Eingriffe sind. Solche Eingriffe können die Folgen von Umwelteinflüssen, von planmäßigen Außerbetriebnahmen von Leitungskapazitäten sowie auch von terroristischen Anschlägen sein. Neben den oben genannten Ursachen für Blackouts werden auch Einflussfaktoren wie der Ausbau der Windkraft, der weiträumige Stromhandel und extreme Wetterlagen infolge des Klimawandels auf ihr potenzielles Risiko für die Versorgungssicherheit hin analysiert.

Im zweiten Projektschritt wird die Risikoanalyse in Form einer szenarienbasierten Modellierung durchgeführt. Das Konsortium entwickelt Szenarien für mögliche Stromausfälle. Mögliche Ursachen für ihr Eintreten werden eruiert, die Ausfallskaskaden beschrieben und die jeweiligen Wahrscheinlichkeiten für den Katastrophenfall berechnet.

Im dritten Projektschritt wird die sozioökonomische Dimension von großflächigen Versorgungsunterbrechungen betrachtet. Entscheidend ist in diesem Zusammenhang die Frage, in welchem Ausmaß der soziale und wirtschaftliche Alltag der unterschiedlichen Betroffenengruppen beeinträchtigt wird und welche Schadenskosten entstehen.

Im vierten Projektschritt wird neben den kurzfristig eintretenden Verlusten infolge eines einzelnen Stromausfalls, eine Abschätzung der Folgen einer mittel- bis langfristigen Verschlechterung der Versorgungssicherheit für die österreichische Volkswirtschaft durchgeführt. Dabei wird auch jener volkswirtschaftliche Schaden ermittelt, der entstünde, wenn sich internationale Unternehmen aufgrund einer zu geringen Versorgungssicherheit gegen den Standort Österreich entscheiden würden.

Im Rahmen des Projektes wurde weiters unter Einbindung von mehr als 800 Haushalten, die Zahlungsbereitschaft zur Vermeidung von Stromausfällen ermittelt. Demnach wäre der durchschnittliche österreichische Haushalt bereit, 18,4 Euro zur Vermeidung einer 24-stündigen Versorgungsunterbrechung zu bezahlen. Festgestellt wurden auch signifikante Abweichungen von der durchschnittlichen Zahlungsbereitschaft aufgrund demografischer und anderer Faktoren:

- Wenn die Versorgungsunterbrechung im Winter auftritt. Dann ist die Zahlungsbereitschaft um 36 Prozent höher als im Sommer.
- Wenn der Umfrageteilnehmer männlich ist. Frauen weisen eine um 32 Prozent geringere Zahlungsbereitschaft als Männer auf.
- Wenn das monatliche Nettoeinkommen des teilnehmenden Haushalts höher/niedriger als der Durchschnitt ist. Ein wohlhabender Haushalt (Nettomonatseinkommen von 4.000 Euro) weist eine um 37 Prozent erhöhte Zahlungsbereitschaft auf als ein Haushalt mit Durchschnittseinkommen.

Die im Rahmen von BlackÖ.1 erstellte Datenbasis dient als Grundlage für künftige sicherheitspoliti-

Ausfallszenario: Ausgefallene Leitungen im österreichischen Übertragungsnetz

sche, wirtschaftspolitische und infrastrukturpolitische Entscheidungen. In einem Folgeprojekt sollen darauf aufbauend Strategien und Pfade zur Wahrung der bestehenden Sicherheitslage und der präventiven Abwehr von großflächigen Stromausfällen in Österreich entwickelt werden.

Projektleitung:

Energieinstitut an der Johannes Kepler Universität Linz GmbH

Projektpartner:

– Technische Universität Wien – Institut für Energiesysteme und Elektrische Antriebe
– Verein Energieinstitut an der Johannes Kepler Universität Linz
– Linz Strom Netz GmbH
– Wien Energie Stromnetz GmbH
– Austrian Power Grid AG (APG)
– Industriellenvereinigung
– Wirtschaftskammern Österreich – Bundessparte Industrie
– Bundeskanzleramt Österreich – Abteilung IV/6, Sicherheitspolitische Angelegenheiten

Kontakt:

Dr. Johannes Reichl
Energieinstitut an der Johannes Kepler Universität Linz GmbH
4040 Linz, Altenberger Straße 69
Tel.: +43/732/2468-5652
Fax: +43/732/2468-5651
E-Mail: reichl@energieinstitut-linz.at

GÖPL IFD

Gemeinsames öffentlich-privates Lagebild für internationale Flugdestinationen

Im Rahmen des Projektes „GÖPL IFD – Gemeinsames öffentlich-privates Lagebild für Internationale Flugdestinationen" sollen die konzeptionellen Grundlagen dafür erarbeitet werden, Gefahren für Luftfahrzeuge, Personal und Passagiere rechtzeitig erkennen und bewerten zu können, um gestützt darauf entsprechende Maßnahmen zu ergreifen, die der Verbesserung der Sicherheit dienen.

Wie in anderen Bereichen, wird auch im internationalen Luftverkehr zwischen Safety- und Security-Aspekten unterschieden. Beziehen sich die Safety-Überlegungen in erster Linie auf die Risiken, die sich aus den betrieblichen Kernprozessen der zivilen Luftfahrt ergeben, so versteht man unter Security-Aspekten eher die externen Gefahren, wie z. B. den internationalen Terrorismus, die Risiken für Flugzeuge, Personal und Passagiere darstellen können. Die Grenze zwischen Safety- und Security-Überlegungen ist allerdings fließend. Daher wurde beschlossen, dass der für das Projekt relevante Risikoraum beide Aspekte umfassen soll.

Im Vergleich zu den Instrumenten, die bislang für die Risikobewertung an internationalen Flugdestinationen eingesetzt werden, soll GÖPL IFD schwerpunktmäßig darauf ausgerichtet werden, die Aussagekraft und die Messbarkeit der genutzten Informationen zu verbessern. Dabei müssen allerdings die zeitliche Verfügbarkeit von Informationen und die direkte Beeinflussbarkeit von Ereignissen und Entwicklungen berücksichtigen werden.

In Hinblick auf die Erarbeitung eines Risikobewertungssystems müssen verschiedene Fragen beantwortet werden, um sicherzustellen, dass ein solches System optimal in die bestehenden betrieblichen Abläufe integriert werden kann: Wie sind die Abläufe im Unternehmen und der Informationsprozess gestaltet? Welche Risikodimensionen werden betrachtet? Wie können Risikodimensionen operationalisiert werden? Welche Rolle spielt Sicherheit in den betrieblichen Prozessen. Wie ist das Zusammenspiel von Prävention, Detektion, Reaktion?

Der für das Projekt relevante Risikoraum umfasst die Dimensionen politische Risiken, Kriminalitätsrisiken, Gesundheitsrisiken, ökonomische Risiken, technisch-infrastrukturelle Risiken und besondere Risiken wie beispielsweise Naturkatastrophen. Für jede dieser Dimensionen wurden einzelne Indikatoren erarbeitet, um Veränderungen erfassen zu können.

Darauf aufbauend geht es darum, für jeden Risikoindikator eine Skala zu erarbeiten, die es ermöglicht, erkannte Veränderungen zu bewerten und in weiterer Folge Sicherheitsmaßnahmen entsprechend abzustimmen.

GÖPL IFD schafft Grundlagen für eine umfassend definierte und systematisch hergeleitete Risikobewertung zur Führungs- und Entscheidungsunterstützung der Konzernsicherheitsverantwortlichen einer international tätigen Airline. Durch die gewählte Methodik werden Handlungsoptionen aufgezeigt, die in der Praxis effektiv umsetzbar wären und im Bedarfsfall ein schnelles und proaktives Handeln ermöglichen könnten.

Projektleitung:

Austrian Airlines AG

Projektpartner:

– Bundesministerium für Landesverteidigung und Sport (BMLVS)
– KFEG GmbH, Koordinierungs-, Forschungs- und Entwicklungsgesellschaft
– THALES Rail Signalling Solutions GmbH, 1210 Wien, Scheydgasse 41

Kontakt:

Austrian Airlines AG
Markus Christl
1300 Flughafen Wien, Office Park 2
Tel.: +43/51766-63500
E-Mail: markus.christl@austrian.com
Web: www.aua.com

BASE of ACE

Austrian Crime Explorer: Analyse, Identifikation und Quantifizierung kriminalitätsfördernder bzw. -hemmender Rahmenbedingungen

Die Studie „BASE of ACE – Austrian Crime Explorer" schafft Grundlagen zur objektivierten Betrachtung möglicher Ursachen von Kriminalität und ihrer statistischen Einschätzung.

Gefährden Nachtklubs, Wettbüros oder Großraumdiskotheken die öffentliche Sicherheit? Wie groß ist der Nutzen von Videoüberwachung bei der Kriminalitätsverhinderung? Wie hängt die Anzahl der Autobahnauffahrten mit der Häufigkeit von Einbruchsdelikten zusammen? Fragen, wie diese, finden sich in der strategischen Polizeiarbeit häufig, können aber selten umfassend oder zufriedenstellend beantwortet werden.

Gemeinsam arbeiten daher das Bundeskriminalamt und das Institut für Angewandte Statistik und Systemanalyse der JOANNEUM RESEARCH Forschungsgesellschaft seit mehreren Jahren daran, empirisch fundierte Werkzeuge zur Unterstützung lang- und mittelfristiger sicherheitspolitischer Entscheidungen zu schaffen.

Im Zuge dieser Zusammenarbeit wurde bereits ein Konzept für ein modulares Software- und Dienstleistungsprodukt erstellt, das den Namen Austrian Crime Information System (ACIS) trägt.

BASE of ACE untersucht den Einfluss bestimmter Rahmenbedingungen aus dem Bereich der nicht personenbezogenen Ursachenforschung auf die Kriminalität. Diese sogenannten kriminogenen Faktoren werden im Rahmen des Projektes identifiziert und quantifiziert. Dazu müssen die Verfügbarkeit von Rahmendaten für Österreich verbessert, statistische Modelle zur Datenanalyse entwickelt und letztlich die vorhandenen Daten im Sinne der Aufgabenstellung analysiert werden.

Nach der theoriegeleiteten Bestimmung der kriminogenen Faktoren werden daher entsprechende Datenbereiche und Indikatoren festgelegt. Je nach Art der Verfügbarkeit sind Daten einfach zu beschaffen oder es sind Maßnahmen zu treffen, um vorhandene Daten verfügbar zu machen.

Für verfügbare Daten wird die Art der Übermittlung festgelegt, es wird die Qualität der Daten geprüft und es wird letztlich deren Aufbereitung für die gemeinsame Analyse durchgeführt. Dazu werden eigene statistische Modelle entwickelt, die der besonderen Beschaffenheit der Datenstruktur Rechnung tragen und es ermöglichen, die erzielten Ergebnisse in einer für das Bundeskriminalamt verwertbaren Form aufzubereiten.

Ziel des Projekts ist die Entwicklung einer Daten- und Wissensbasis für die Prognose regionaler Unterschiede in der Kriminalität in Österreich.

Das wissenschaftliche Ziel besteht in der Identifikation und Quantifizierung kriminogener Faktoren. Die Ergebnisse dieser Studie sollen in der Folge als Grundlage für die Implementierung eines spezifischen Moduls des ACIS, das den Namen Austrian Crime Explorer (ACE) trägt, dienen.

Projektleitung:

JOANNEUM RESEARCH Forschungsgesellschaft mbH, POLICIES – Zentrum für Wirtschafts- und Innovationsforschung

Projektpartner:

– Bundesministerium für Inneres (BMI)
– Bundeskriminalamt (BK)

Kontakt:

JOANNEUM RESEARCH Forschungsgesellschaft mbH
Mag. Gerhard Neubauer
8010 Graz, Leonhardstraße 59
Tel.: +43/316/876-1557
Fax: +43/316/876-91557
E-Mail: gerhard.neubauer@joanneum.at
Web: www.joanneum.at/sta

SAFE TETRA2

Garantierte Sicherheit für die Bürger und Blaulichtorganisationen beim Einsatz von TETRA-Handfunkgeräten

SAFE TETRA2 stellt einen wichtigen Beitrag zur Sicherheit von Menschen dar, die in Kontakt mit drahtloser Kommunikationstechnologie für BOS in Österreich kommen.

Das Bundesministerium für Inneres (BMI) beabsichtigt, in den kommenden Jahren die gesamte Funkkommunikation in Österreich auf digitale Bündelfunktechnik umzustellen. Dieses neue System wird in Zukunft allen Blaulichtorganisationen wie insbesondere Exekutive, Feuerwehr und Rettungsorganisationen zur Verfügung stehen. Bei dieser Funkkommunikation handelt es sich um den dem Fernmeldewesen zuzuordnenden Digitalfunk BOS Austria (Behörden und Organisationen mit Sicherheitsaufgaben), der mit dem europäischen Standard TETRA umgesetzt wird. Bei der Verwendung von TETRA-Funksystemen („terrestrial trunked radio") entstehen jedoch elektromagnetische Felder.

Die in Österreich angewandten Grenzwerte zum Schutz der Bevölkerung gegenüber nachteiligen Wirkungen elektromagnetischer Felder garantieren keinen Schutz gegenüber möglichen Störungen von aktiven elektronischen Implantaten. Auch die bei manchen Funkgeräten angeführten maximalen „SAR-Werte" (Spezifische Absorptionsrate) sind nicht geeignet, um Aussagen über die mögliche Gefährdung von Implantatsträgern zu treffen. Dieses Thema wird zurzeit auf der Ebene der internationalen und nationalen Normung behandelt, im auch für Österreich relevanten vorliegenden Entwurf von CENELEC gibt es jedoch keine spezifischen Ausführungen für TETRA-Funkgeräte. Für die Relevanz der Studie „SAFE TETRA2: Garantierte Sicherheit für die Bürger und Blaulichtorganisationen beim Einsatz von TETRA-Handfunkgeräten" ist weiters anzuführen, dass die Zahl der Patienten mit aktiven elektronischen Implantaten in den letzten Jahren ständig zugenommen hat. Beispielsweise gibt es in Österreich zirka 50.000 Träger von Herzschrittmachern und pro Jahr finden im Durchschnitt etwa 7.500 Implantationen statt. Außer den Herzschrittmachern gibt es zusätzlich eine Vielzahl anderer aktiver elektronischer Körperhilfen.

Das Projekt SAFE TETRA2 stellt somit einen wichtigen Beitrag zur Sicherheit von Menschen dar, die in Kontakt mit drahtloser Kommunikationstechnologie für BOS in Österreich kommen. Es werden einerseits Maßnahmen zum Schutz von Bürgern mit elektronischen Implantaten und andererseits zum Schutz von Mitarbeitern der BOS untersucht. Weiters liefert das Projekt wichtige Informationen für den Betrieb der kritischen Infrastruktur Digitalfunk BOS Austria. Davon betroffen sind das BMI und dem Ministerium zugeordnete Organisationen sowie das Rettungswesen, die Feuerwehren und anderen BOS.

Das Projekt gliedert sich in zwei Hauptabschnitte, die parallel zueinander durchgeführt werden:

- Untersuchung der Möglichkeit der Störung von elektronischen Implantaten durch TETRA-Geräte: Dabei wird die Beeinflussung von 20 verschiedenen Herzschrittmachern, vier verschiedenen implantierten Defibrillatoren und einem implantierten neurologischen Impulsgenerator durch vier TETRA-Handgeräte und zwei TETRA-Autogeräte untersucht. Weiters werden Untersuchungen der Beeinflussung der Implantate bei zusätzlicher Exposition durch GSM- und Rundfunksignale sowie bei Exposition durch Hochspannungsleitungen durchgeführt. Die Messungen werden in Zusammenarbeit mit Kardiologen von der medizinischen Universität Wien durchgeführt.
- Maßnahmen zur Minimierung der Exposition von Benützern von TETRA-Funkgeräten: In diesem Arbeitspaket wird die Exposition von Personen bei der Verwendung von TETRA-Funk untersucht. Dazu wird im ersten Schritt via Fragebogen erhoben, wie die TETRA-Geräte bei Blaulichtorganisationen verwendet werden. Mit den Ergebnissen wird mittels

Von links: TETRA-Mobiltelefon, CAD-Modell für die numerische Simulation, simuliertes elektrisches Feld

numerischer Simulation die Exposition in verschiedenen Verwendungsarten berechnet.

Die Ergebnisse des Forschungsprojektes sind anwenderorientiert. Dies bedeutet, dass die Bedarfsträger die Ergebnisse der Studie als präventive Schutzmaßnahmen unmittelbar umsetzen können. Durch Broschüren, Informationen im Internet, aber auch durch Informationsveranstaltungen und Schulungen soll gewährleistet werden, dass die Forschungsergebnisse die potenziellen Nutzer auch tatsächlich erreichen. Außerdem dienen diese Maßnahmen der Erhöhung der Akzeptanz durch die Mitarbeiter der BOS, aber auch durch die Bevölkerung.

Die bisherigen Ergebnisse der Studie zeigen, dass TETRA-Geräte grundsätzlich in der Lage sind, Implantate zu stören. Während jedoch einige Implantate keine Beeinflussung zeigten, konnte bei anderen Implantaten Störungen bis zu einem Abstand von 40 Zentimetern zwischen TETRA-Gerät und Implantat beobachtet werden. Bei der Erhebung der Exposition der Anwender von TETRA-Funkgeräten konnte ermittelt werden, dass der Großteil der TETRA-Anwender mit dem Funkgerät vor dem Mund spricht (wie mit einem klassischen Funkgerät) und die überwiegende Trageweisen in der Brusttasche und am Gürtel sind. Auf diesen Ergebnissen aufbauend, werden die numerischen Simulationen der Exposition der TETRA-Anwender konzipiert und durchgeführt. Nach heutigem Kenntnisstand ist bei Einhaltung der bestehenden Grenzwerte zur Begrenzung der Exposition durch elektromagnetische Felder mit keinen gesundheitlich nachteiligen Effekten zu rechnen, allerdings bestehen in einigen wissenschaftlichen Bereichen relevante offene Fragen, wie zum Beispiel die über mögliche Langzeitwirkungen bei Exposition durch Hochfrequenzfelder. Sollte sich in Zukunft herausstellen, dass es unterhalb der heutigen Grenzwerte gesundheitsrelevante Effekte gibt, so hätte man durch die im Rahmen dieses Projektes erarbeiteten Maßnahmen bereits Vorsorge getroffen.

Aufgrund der Ergebnisse von SAFE-TETRA2 können künftig mögliche Gefährdungen oder Belästigungen von Personen durch den Einsatz der Infrastruktur Digitalfunk BOS Austria verhindert werden. Durch die Umsetzung des Konzeptes der umsichtigen Vermeidung werden zudem Maßnahmen zu einer Erhöhung der Akzeptanz bei den Mitarbeitern der BOS wie auch in der Bevölkerung getroffen. Dies reduziert zeitliche und finanzielle Aufwendungen sowohl beim BMI als auch bei allen BOS-Organisationen. Solche Probleme sind bei der Etablierung von GSM- und UMTS-Netzen sehr häufig aufgetreten und haben zu beträchtlichen Verzögerungen beim Rollout des Netzes und entsprechend erhöhten Kosten sowie Verzögerungen bei den Einnahmen geführt. Ein weiterer Vorteil ist, dass bei der Einführung zukünftiger Funktechnologien wie Wimax, UWB, DVB-H auf die Erfahrungen von SAFE-TETRA2 zurückgegriffen werden kann.

Projektleitung:

Seibersdorf Labor GmbH

Projektpartner:

– Bundesministerium für Inneres (BMI)
– Österreichisches Rotes Kreuz
– Projektmitarbeit durch das Landesfeuerwehrkommando Niederösterreich

Kontakt:

Seibersdorf Labor GmbH, EMC&Optics
Dipl.-Ing. Stefan CECIL
2444 Seibersdorf, Austria
Tel.: +43/50550-3138
Fax: +43/50550-2881
E-Mail: stefan.cecil@seibersdorf-laboratories.at
Web: www.seibersdorf-laboratories.at

SFI@SFU

Entwicklung eines disziplinenübergreifenden nationalen Sicherheitsforschungsinstitutes an der Sigmund Freud PrivatUniversität Wien

SFI@SFU verfolgt einen transdisziplinären Ansatz, um internationale Wissensstände systematisch zu erschließen, zu bündeln und fachübergreifend in angewandte Forschung umzusetzen.

Die Entwicklung eines nationalen Institutes für umfassende Sicherheitsforschung im Rahmen des Projektes SFI@SFU findet in ständiger Praxiserprobung und auf der Grundlage selbstgeleisteter, empirisch-analytischer ebenso wie theoretisch-konzeptueller Forschungsarbeiten statt. Zudem werden wissenschaftliche Dienstleistungen erbracht, wie Durchführung von Fachtagungen und fachwissenschaftliche Beratung in der Konzeptionsphase von Sicherheitsforschungsprojekten.

Das Projekt SFI@SFU setzt eine pluralistische Methodologie um. Dazu gehören politologische, soziologische und naturwissenschaftliche (z. B. Risikoanalysen, Naturgefahrenmanagement) Analysen, strukturierte Workshops und Erhebungen, vergleichende Auswertungen von nationalen und internationalen Sicherheitsforschungsprojekten und der zusammenführende Abgleich von Forschungsständen. Über ein Beratungsgremium werden relevante Bedarfsträger in die laufende Arbeit eingebunden.

Insgesamt wurden bisher 37 Ergebnisdokumente (Deliverables), Studien, Berichte, Leitfäden, Infotexte und Dokumentationen verfasst. Die Eigenveranstaltungen des Projektes umfassten bisher insgesamt acht Konferenzen und Workshops mit insgesamt 380 Teilnehmern. Acht Umfragen und Expertenkonsultationen wurden durchgeführt. Mit bisher gehaltenen 17 Fachvorträgen im In- und Ausland trugen die Projektmitarbeiter zur Verbreitung der erzielten Ergebnisse und zur Einbettung des sich entwickelnden Institutes in die wissenschaftliche Gemeinschaft bei. Darüber hinaus wird in Form einer Summer School ein wissenschaftlicher Fachkurs zu Methoden der Sicherheitsforschung abgehalten. Ein Methodenhandbuch zur Sicherheitsforschung steht ebenfalls in Erarbeitung, genauso wie das erste deutschsprachige Lehrbuch zur Katastrophenforschung.

Folgende ausgewählte inhaltliche Ergebnisse von SFI@SFU sind bisher besonders hervorzuheben:

- GSK-Aspekte in Definition und Schutz kritischer Infrastruktur: Im Rahmen einer Befragung wurden Einschätzungen von Experten zur Risikobewertung von Sektoren kritischer Infrastrukturen erhoben. Die Ergebnisse sollen Relevanzbereiche zur Weiterentwicklung von KIRAS definieren, in denen GSK-Forschung (Forschung in den Geistes-, Sozial- und Kulturwissenschaften) dezidiert ansetzen sollte, um „weiche" oder „soziale" Aspekte von Kritikalität näher zu untersuchen.

- Politik umfassender ziviler Sicherheit: Der „umfassende Ansatz" (comprehensive approach) ist in Europa von einem Leitbild der Außen- und Sicherheitspolitik zu einem allgemeinen sicherheitsstrategischen Modell geworden, das auch Sicherheitsforschungsprogramme wie KIRAS leitet. Mit seiner zunehmenden Verbreitung ist das Konzept aber immer diffuser geworden und seine Inhalte sind weitgehend intuitiv. Um das Konzept für die Sicherheitsforschung zu präzisieren, wurden zahlreiche Definitionen aus unterschiedlichen Kontexten auf internationaler und nationaler Ebene gesammelt und vergleichend ausgewertet.

- Krisen- und Katastrophenforschung: Erstmals wurde ein strukturierter Dialog zwischen Bedarfsträ-

Podiumsdiskussion auf der Sicherheitstechnologie-Tagung – organisiert von SFI@SFU und Austria Tech

gern und Geistes-, Sozial- und Kulturwissenschaften (GSK) umgesetzt, der aus kombinierter Forschungs- und Praxissicht Richtlinien und weiteren Forschungsbedarf für bevölkerungszentrierte Kommunikation im Krisen- und Katastrophenmanagement erarbeitete. Es zeigte sich, dass Kommunikation mit der Bevölkerung als spezifisches Katastrophenmanagementtool für die Akutphase zu kurz greift: Wesentlicher Faktor für gelingende Kommunikation in Katastrophenfällen ist Kommunikatorenvertrauen aufgrund vorangegangener gelebter Kommunikation im Alltag. In Österreich fällt dabei die verhältnismäßig geringere Glaubwürdigkeit von Wissenschaft und die überproportionale Glaubwürdigkeit von Regierung, Journalisten, Familie und Bekanntenkreis, aber auch – wenngleich in geringerem Ausmaß – EU-Institutionen auf.

- Dienstleistungen für die wissenschaftliche Gemeinschaft und Bedarfsträger: Das Projekt erstrebt hier u. a. die Stärkung der Potenziale GSK-Forschung, Technologieentwicklung integrativ zu begleiten. Hierzu wurde bereits ein Weiterbildungsplan für GSK-Forscher entwickelt. Insbesondere wurde eine breit angelegte Studie zur Erhebung von Ansprüchen der Bedarfsträger und der wissenschaftlichen Gemeinschaft an künftige nationale Sicherheitsforschung erstellt. Bedarfsträger wünschen sich demzufolge vor allem Aufklärung über die zukünftigen Bedrohungslagen, um Erfordernisse innovativer Sicherheitstechnik sowie weiterentwickelter Informations- und Kommunikationstechnologie frühzeitig einschätzen zu können.

Mit einer ausführlichen Website schuf das Projekt die erste fachwissenschaftliche Internetpräsenz österreichischer Sicherheitsforschung, die dazu beiträgt, Sicherheitsforschung als akademische Disziplin greifbarer zu machen. Diese findet sich unter der Internetadresse: www.sfi-sfu.eu.

Projektleitung:

Institut für Sicherheitsforschung der Sigmund Freud PrivatUniversität Wien

Projektpartner:

– Sigmund Freud PrivatUniversität Wien GmbH
– Dr. Alexander Siedschlag

Kontakt:

Sigmund Freud PrivatUniversität Wien,
Institut für Sicherheitsforschung
Prof. Dr. Alexander Siedschlag
1030 Wien, Schnirchgasse 9a
Tel.: +43/1/798 62 90-50
E-Mail: alexander.siedschlag@sfu.ac.at
Web: www.sfi-sfu.eu

SICHER AKTIV

Entwicklung eines bedarfs- und bedürfnisorientierten Zivilschutzkurses zum Schutz kritischer Infrastruktur in Österreich

SICHER AKTIV beinhaltet die Entwicklung eines bedarfs- und bedürfnisorientierten Zivilschutzkurses zum Schutz kritischer Infrastruktur im Bereich Gesundheitswesen.

Derzeit werden Informationen zum Zivil- und Selbstschutz vonseiten des Österreichischen Zivilschutzverbandes und den jeweiligen Zivilschutzverbänden der Bundesländer für die Bevölkerung angeboten. Dies geschieht in Form von Aktionen und Projekten, kostenlosen Kursvorträgen, Informationen im Internet sowie Stellungnahmen zu aktuellen Geschehnissen in den Medien. Das Projekt „Sicher Aktiv: Entwicklung eines bedarfs- und bedürfnisorientierten Zivilschutzkurses zum Schutz kritischer Infrastruktur in Österreich" ergänzt diese Inhalte und legt den Schwerpunkt auf die Thematik Gesundheitswesen.

Ziel ist die Entwicklung eines bedarfs- und bedürfnisorientierten Zivilschutzkurses für die Bevölkerung. Dieser knüpft am Bedarf der Betreiber von Anlagen der kritischen Infrastruktur im Bereich Gesundheitswesen an, um diese Anlagen im Falle einer Krise nicht zusätzlich durch falsche Handlungsweisen der Bevölkerung zu belasten, sondern durch richtiges Verhalten zu entlasten.

Interessen und Informationsbedürfnisse der Bevölkerung werden in die Gestaltung des Kurses ebenfalls mit einbezogen. Ein modularer Aufbau ermöglicht die Vertiefung von thematischen Schwerpunkten für die Teilnehmer sowie das Eingehen auf regionale Besonderheiten. Ergebnis des Projektes ist ein umfassendes, bedarfs- und bedürfnisorientiertes Kurskonzept, das vollständig als Curriculum mit Lehr- und Lernunterlagen vorliegt und in weiterer Folge eine Methode darstellt, um das Sicherheitsgefühl der Bürger einerseits und die Sicherheit der kritischen Infrastruktur andererseits zu steigern.

Insgesamt konnten fünf große Themen und mehrere kleinere Themenbereiche als Inhalte konkretisiert werden. Diese wurden innerhalb des Kursentwicklungsprozesses zu folgenden Modulen ausgearbeitet:

- Katastrophen. In diesem einleitenden Kursteil wird einerseits die „Katastrophe" definiert, ein kurzer Überblick über das staatliche Krisen- und Katastrophenschutzmanagement gegeben, die Aktualität der Thematik durch Beispiele verdeutlicht und der Regelkreis einer Katastrophe erarbeitet. Dadurch wird ein Problembewusstsein geschaffen.
- Organisationsinformationen über das österreichische Gesundheitssystem und dessen Kapazitäten im Krisenfall. In diesem Modul werden die Zuständigkeiten der Institutionen des österreichischen Gesundheitssystems, ihr Tätigkeitsspektrum und ihre Kapazitäten im Alltag und im Falle einer Krise erklärt.
- Krisenszenarien und persönliche Maßnahmen zum Zivil- und Selbstschutz. Dieser Teil des Kurses wird in den Pilotkursen von Den Helfern Wiens und dem Niederösterreichischen Zivilschutzverband übernommen. Durch diese Kooperation können den Kursteilnehmern sowohl adäquate Empfehlungen zum Selbstschutz als auch zur Entlastung des Gesundheitswesens gegeben werden.
- Planspiel als Übung für den Katastrophenfall. Als praktische Übung wurde ein kartenbasiertes Planspiel entworfen. Es teilt die Teilnehmer in Kleingruppen ein, die Nachbarschaften darstellen. Die vier Gesundheitsstationen Apotheke, Arzt, Krankenhaus und Rettungsdienst werden von Spielern übernommen und haben entsprechende Funktionen. Ziel ist es, als Gruppe eine gewisse Anzahl von Tagen im Spiel zu bleiben und sich dementsprechend mit Ressourcen gegenseitig zu unterstützen. Einerseits soll das Bewusstsein für Nachbarschaftshilfe und Bevorratung in einer Notsituation gefördert werden. Andererseits werden entstehende Engpässe aufgezeigt, die den Spielern die Bedeutsamkeit von richtigem Handeln aufzeigen.

Die Kurse von SICHER AKTIV berücksichtigen die Interessen der Bürger und der Betreiber kritischer Infrastruktur

Wichtiges Element der Kurse von SICHER AKTIV ist ein kartenbasiertes Planspiel als Übung für den Katastrophenfall

● Gesundheitsbildung mit Praxisanleitung. Dieses Modul beinhaltet Praxistipps sowie vorbeugende Maßnahmen zum Selbstschutz im Alltag, Krisen- und Katastrophenfall – von Symptomerkennung und einfachen Anwendungen von Hausmitteln bis hin zu Vorsorgeuntersuchungen oder Warnungen vor Medikamentenfälschungen.

Die im Rahmen des Projektes in Wien und Niederösterreich durchgeführten Pilotkurse wurden ausgiebig beworben. Drei Lehrbeauftragte des Ausbildungszentrums des Wiener Roten Kreuzes wurden auf die Inhalte des Kurses geschult und unterstützende Kursmaterialien wurden produziert. Begleitet werden die Kurse vom Sicher-Aktiv-Projektteam, das Beobachtungsprotokolle verfasst. Weitere Informationsbedürfnisse und Änderungsvorschläge werden in einer Evaluation mit den Teilnehmern berücksichtigt.

Nach den ersten durchgeführten Pilotkursen lässt sich jedenfalls ein großes Interesse der Teilnehmer attestieren. Insbesondere das Themengebiet der Katastrophen erweist sich als wichtiges Element, das in der folgenden Adaption noch erweitert wird. Von Interesse ist etwa, wie Katastrophenhilfe konkret gestaltet ist, was bevorratet ist oder welche Institutionen und Organisationen wie zusammenarbeiten. Auch Übungen für derartige Ereignisse wären für Teile der Bevölkerung interessant und würden das Bewusstsein sowohl für eigene Vorsorgemaßnahmen (auch im Gesundheitsbereich) als auch für die Vorsorge, die ein Land für seine Bevölkerung trifft, deutlich steigern.

Ein bedarfs- und bedürfnisorientierter Zivilschutzkurs, wie in dem Projekt erarbeitet, trägt dazu bei, Informationsbedarf zu decken, das Bewusstsein für das eigene Handeln zu erhöhen und Verständnis für das Gesundheitswesen in Österreich zu verbessern. Für die Zukunft wäre es interessant und wichtig, auch neue Wege in der Vermittlung dieser Inhalte zu beschreiten, um die Thematik dadurch in das tägliche Leben der Bevölkerung zu integrieren. Denn nur durch die Erreichung einer gewissen „Selbstverständlichkeit" können nachhaltig die „resilient society" (die „Widerstandsfähigkeit der Gesellschaft") gestärkt und im Falle einer Katastrophe zusätzliche Schäden verhindert werden.

Projektleitung:

Forschungsinstitut des Roten Kreuzes

Projektpartner:

– ABZ Ausbildungszentrum des Wiener Roten Kreuzes GmbH

Kontakt

Forschungsinstitut des Roten Kreuzes
Mag.a Nadine Sturm
1030 Wien, Nottendorfer Gasse 21
Tel.: + 43/1/795 80-7425
Fax: + 43/1/795 80-9730
E-Mail: nadine.sturm@w.roteskreuz.at
Web: www.frk.or.at

StratfüSys

Strategisches Führungssystem für die öffentlich-private Sicherheitszusammenarbeit

„StratfüSys" definiert die Anforderungen an ein strategisches Führungssystem zur Unterstützung der öffentlich-privaten Sicherheitszusammenarbeit.

Die Globalisierung hat zu einem höchst komplexen politischen und wirtschaftlichen Umfeld geführt, das eine große Zahl neuer Sicherheitsrisiken birgt. Im politischen Umfeld sind diese Risiken z. B. Terrorismus, organisierte Kriminalität, Weiterverbreitung von Massenvernichtungswaffen etc. Ein einzelner Akteur – sei es ein Staat, ein Ministerium oder eine Sicherheitsbehörde – allein wäre mit der Bewältigung dieser Risiken, ihrer Ursachen und ihrer Folgen überfordert. Daher müssen verschiedene staatliche und nicht-staatliche Akteure sowie militärische, zivile, wirtschaftliche und gesellschaftliche Mittel systematisch in einem vernetzten Ansatz miteinander kombiniert werden.

Im wirtschaftlichen Umfeld ist die Ausgangslage vergleichbar. Zusätzlich hat die Informationsrevolution die Intensität des Wettbewerbs verstärkt. Vielgliedrige unternehmerische Wertschöpfungsprozesse entstehen, in denen zahlreiche Akteure laufend koordiniert werden müssen. Dieser ausgeprägt arbeitsteilige Prozess ist durch technische Verzögerungen, durch Anschläge an wichtigen Standorten oder durch die Unterbrechung strategisch wichtiger Versorgungswege (wie etwa durch Piraterie oder Naturkatastrophen) extrem störanfällig geworden.

Vor diesem Hintergrund wird die Sicherheitsvorsorge immer mehr zu einer Gemeinschaftsaufgabe von Staat und Wirtschaft. Wenn privatwirtschaftliche Betreiber und Eigentümer kritischer Infrastrukturen unzureichend in ihre eigene Sicherheit investieren, wirkt sich dies unmittelbar auf die staatliche Sicherheitsvorsorge aus. Umgekehrt können staatliche Sicherheitsvorschriften die Rahmenbedingungen wirtschaftlichen Handelns beeinflussen.

Damit eine öffentlich-private Sicherheitszusammenarbeit erfolgreich gestaltet werden kann, bedarf es eines umfassenden Führungssystems, das aus vier Komponenten bestehen sollte:

- Einem gemeinsamen Lagebild;
- einem Prozess der strategischen Zukunftsanalyse, um Chancen und Risiken frühzeitig erkennen zu können;
- der Fähigkeit zur Modellbildung und Simulation als entscheidendem Beitrag zur Führungsunterstützung sowie
- aus einem kollaborativen Wissensmanagementumfeld, das den Austausch von Daten, Informationen und Wissen zwischen den beteiligten Akteuren ermöglicht.

Der zentrale Beitrag des Projektes „Strategisches Führungssystem für die öffentlich-private Sicherheitszusammenarbeit" (StratfüSys) liegt darin, die wesentlichen Komponenten eines solchen Systems zu identifizieren und in ihrer Ausgestaltung zu präzisieren.

Die sicherheitspolitischen Herausforderungen verlangen nicht nur nach neuen Wissensgrundlagen, sondern auch nach kollaborativen Verfahren, um dieses Wissen zu erarbeiten und weiterzuentwickeln. Dem Kompetenz-Networking kommt dabei eine zentrale Funktion zu. Dieses ist ein Expertenmanagement, das zur Identifizierung der relevanten Kompetenzträger dient und den vernetzten Erfahrungsaustausch zwischen diesen unterstützt.

Die Konzeptstudie im Rahmen des Projektes StratfüSys ist so angelegt, dass Ergebnisse konkret realisiert werden können. Mit der strategischen Zukunftsanalyse entsteht ein neuer gesamtstaatlicher Führungsprozess, der die gegenwartsbezogene Arbeit der Ministerien durch systematisch erarbeitete Infor-

Sicherheitsvorsorge wird zunehmend zu einer Gemeinschaftsaufgabe von Staat und Wirtschaft

mationen über künftig mögliche Entwicklungen und ihre Konsequenzen ergänzt und dabei auch den Akteuren aus der Wirtschaft offensteht. Weiters soll durch die aufzubauende Expertise im Bereich Modellbildung und Simulation mittelfristig eine eigenständige Institution entstehen (Arbeitstitel: Austria Lab), die analytische Werkzeuge zum Umgang mit Komplexität entwickelt und deren Anwendung in den Dienst von Bedarfsträgern aus dem öffentlichen und privaten Umfeld stellt. Schließlich wird mit der kollaborativen Wissensmanagementumgebung das daten-, informations- und wissensbasierte „Rückgrat" des strategischen Führungssystems geschaffen. Alle drei Bausteine von StratfüSys sind inhaltlich aufeinander abgestimmt und unterstützen gemeinsam das „Gemeinsames öffentlich-privates Lagebild zur Verbesserung der staatlichen und unternehmerischen Sicherheitsvorsorge" (GÖPL). Damit leistet StratfüSys einen entscheidenden Beitrag zur Erweiterung der sicherheitspolitischen Handlungsfähigkeit staatlicher und wirtschaftlicher Akteure in Österreich.

Neben einer fundierten Analyse und Konzeption zur öffentlich-privaten Sicherheitszusammenarbeit sollen aber auch konkrete Produkte generiert werden, die sowohl für die am Projekt beteiligten Bedarfsträger, aber auch für weitere Betroffene und Interessenten von Nutzen sein können. Zwei solche Produkte gibt es bereits:

- Generische Risikomatrix. Die Risikomatrix ist eine Auflistung möglicher Gefahren für Österreich, die nach Wirkungsgrad und Eintrittswahrscheinlichkeit differenziert werden und von natürlichen Katastrophen über kriegerische Auseinandersetzungen, bis hin zu technischen Bedrohungsszenarien wie etwa durch einen Nuklearunfall reichen. Ursprünglich vom Bundesministerium für Landesverteidigung und Sport erstellt, wird es gerade im Rahmen von StratfüSys ausgebaut und verfeinert.
- RiskPanel (Risikoperzeptionsbarometer). Das RiskPanel stellt eine Alternative zu einer umfassenden Zukunftsanalyse dar und ist eine direkte Weiterentwicklung des Panel 50. In regelmäßigen Abständen wird die Einschätzung wesentlicher Entscheidungsträger zu sicherheitsrelevanten Themen abgefragt und ausgewertet.

Projektleitung:

Industriellenvereinigung

Projektpartner:

– Borchert Consulting & Research GmbH
– Thales Rail Signalling Solutions GmbH
– KFEG GmbH Koordinierungs-, Forschungs- und Entwicklungsgesellschaft
– Institut für Wirtschaftsmathematik, TU Wien
– Institut für Höhere Studien
– RiskRe Agentur für Risikoforschung
– Bundeskanzleramt (BKA)
– Bundesministerium für Landesverteidigung und Sport (BMLVS)
– Bundesministerium für Inneres (BMI)

Kontakt:

Industriellenvereinigung
Dipl.-Ing. Roland Sommer
1031 Wien, Schwarzenbergplatz 4
Tel.: +43/1/711 35-2408
E-Mail: r.sommer@iv-net.at

AFOR

Studie zu digitaler Forensik –- Erfordernisse der Beweissicherung und Möglichkeiten der Verknüpfung von Daten

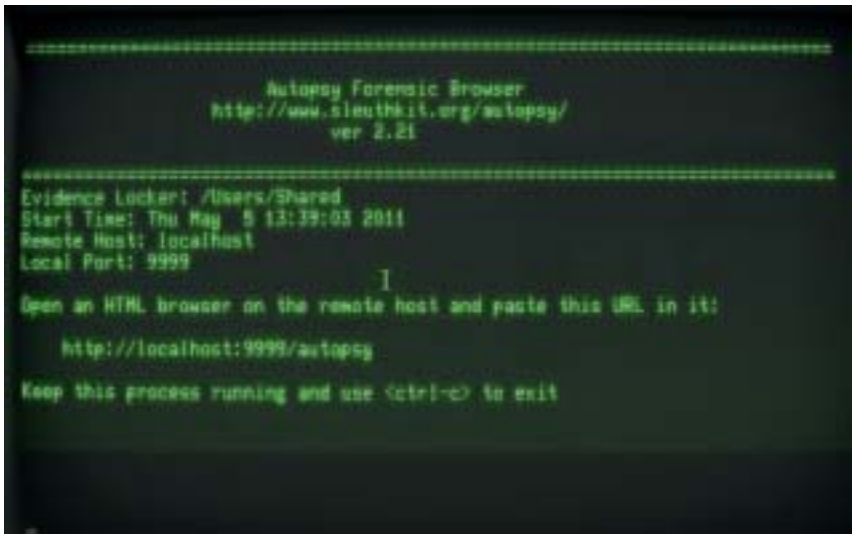
Die „Studie zu digitaler Forensik" in Österreich untersucht Erfordernisse der digitalen Beweissicherung und Möglichkeiten der Verknüpfung von Daten.

Da Computer und Netzwerke nicht nur im täglichen Leben, sondern auch bei illegalen und kriminellen Aktivitäten immer häufiger zum Einsatz kommen, gewinnt auch die digitale Forensik bei der Ermittlung durch Behörden zunehmend an Bedeutung.

Grundlage der Untersuchungen im Rahmen von „AFOR: Studie zu digitaler Forensik – Erfordernisse der Beweissicherung und Möglichkeiten der Verknüpfung von Daten" ist eine Erhebung des Ist-Stands der momentan gängigen Praxis in der digitalen forensischen Beweisermittlung. Darauf aufbauend sollen neue Methoden und Werkzeuge entwickelt werden, die der sich ständig verändernden Bedrohung Rechnung tragen. Außerdem sollen Methoden erarbeitet werden, die eine sicherere und effizientere Abwicklung der Beweisübermittlung ermöglichen. Zudem wird durch die Schaffung einer einheitlichen Vorgehensweise für die Beweisermittlung mittels digitaler Forensik die Vergleichbarkeit von Gutachten und Beweismaterial aus verschiedenen Quellen ermöglicht.

Die Vielzahl an teilweise inhomogenen Teilbereichen der digitalen Forensik macht eine holistische Herangehensweise erforderlich. Daher beinhaltet die Studie eine Zahl parallel laufender Projekte:

- Im ersten Projektabschnitt wurde die Problemstellung der Verknüpfung von Daten aus unterschiedlichen Quellen behandelt. Dabei wurde die Anwendbarkeit von forensischen Methoden für Web2.0/Cloud Systeme evaluiert. Gemeinsames Merkmal dieser Dienste ist die Tatsache, dass Systemkomponenten vermehrt bei externen Dienstleistern ausgelagert werden und ein physischer Zugriff auf diese Komponenten wie heute üblich nicht möglich ist.
- Im Rahmen des Projektes „Onlinestorage/Dropbox" wurde der Onlinespeicherdienst Dropbox auf die Anwendbarkeit von forensischen sowie anti-forensischen Methoden analysiert. Als Ergebnis der Forschungsarbeiten entstehen zwei Publikationen über Onlinestorage, die zum einen die sogenannte Hashwert-Manipulation (Hashwerte sind Algorithmen, die eine nahezu eindeutige Kennzeichnung einer größeren Datenmenge ermöglichen) bei Dropbox beschreiben. Zum anderen wird ein verbessertes Übertragungsprotokoll entwickelt, das die Vorteile des gemeinsamen Speichers behält, jedoch Hashwert-Manipulationen verhindert.
- „Enterprise Rights Management (ERM)" beinhaltet die Adaptierung sogenannter DRM-Technologien, die zur digitalen Rechteverwaltung eingesetzt werden, für den Einsatz in Unternehmen. Die Tatsache, dass ERM-geschützte Dokumente verschlüsselt abgespeichert werden, erzeugt erhebliche Schwierigkeiten bei forensischen Untersuchungen. In diesem Projekt wird analysiert, welche Schritte eingehalten werden müssen, um digitale Forensik in ERM-Systemen zu ermöglichen und welche Maßnahmen getroffen werden müssen, damit der Zugriff auf ERM-geschützte Dokumente nach Ablauf ihrer Gültigkeitsdauer verhindert werden kann.
- Soziale Netzwerke wie facebook enthalten jede Menge Informationen zu verdächtigen Personen, die bei forensischen Untersuchungen verwertbar sein können. Allerdings werden diese Informationen in der Regel nur einem kleinen Nutzerkreis (sogenannten Freunden) zur Verfügung gestellt. Im Zuge des Projekts „Soziale Netzwerke/facebook" wird ein Forensik-Tool entwickelt, das das automatisierte Auslesen von facebook-Profilen ermöglicht.
- Die Storage-Engine InnoDB für das Datenbankmanagementsystem MySQL speichert Daten in einer sogenannten B*-Baum-Struktur. Die Forschungsarbeiten auf diesem Gebiet befassten sich mit der



AFOR entwickelt Techniken zur Beweissicherung von kriminellen Aktivitäten in der digitalen Welt

Annahme, dass der Aufbau eines B*-Baums Rückschlüsse auf die Reihenfolge von INSERT-Statements und DELETE-Statements ermöglicht. Mithilfe dieser Informationen könnten in weiterer Folge Manipulationen in Datenbanken erkannt werden.

- Um digitale Forensik effizient durchführen zu können, müssen eine Reihe organisatorischer Rahmenbedingungen erfüllt sein. Hierbei stehen Institutionen vor der Herausforderung, Prozesse zu identifizieren und umzusetzen, die forensische Untersuchungen ermöglichen und gegebenen Rechtsanforderungen hinreichend entsprechen. Im Rahmen des Projektes „Computer Forensik Management System (CFMS)" soll evaluiert werden, welche Strukturen und Richtlinien umgesetzt werden sollten, um forensische Analysen bestmöglich zu unterstützen. Ein weiteres Ziel der Forschungsarbeiten in diesem Bereich ist die Entwicklung eines Best-Practice-Guides zur Schaffung eines forensischen Managementsystems. Dabei gilt es, besonderes Augenmerk auf die Integration in bestehende und etablierte Managementsysteme wie beispielweise das Information Security Management System (ISMS) oder das Business Continuity Management System (BCMS) zu legen.
- Das Betreiben und Verbessern eines Computerforensik-Managementsystems innerhalb einer Institution ist grundlegende Voraussetzung für koordinierte und verwaltete Aktivitäten. Die Studie will noch einen Schritt weitergehen und beleuchten, ob ein institutionsübergreifendes Managementsystem sowie einheitliche Prozesse und Vorgehensweisen sinnvoll sind. Dabei ist im Besonderen zu berücksichtigen, ob Institutionen autonom handeln sollen oder ob übergeordnete Gremien wie beispielsweise ein Computerforensik-Board oder Computerforensik-Response-Team einen erhöhten Nutzen bringen.
- Ein sekundäres Ziel stellt schließlich die Betrachtung der Kommunikation nach außen dar. Hierbei soll analysiert werden, zu welchem Zeitpunkt welche Informationen an die Öffentlichkeit gebracht werden sollen, dürfen bzw. müssen.

Bei Vorfällen, in welchen die getroffenen Sicherheitsmaßnahmen nicht ausreichend waren und sich eine kriminelle Handlung auf einem Computersystem oder in einem digitalen Netzwerk abgespielt hat, ist die digitale Forensik der nächste logische Schritt. „AFOR: Studie zu digitaler Forensik – Erfordernisse der Beweissicherung und Möglichkeiten der Verknüpfung von Daten" schafft Grundlagen, um für diesen Schritt standardisierte Abläufe und Vorgaben zu entwickeln, die künftig eine nachträgliche Auswertung digitaler Daten ebenso ermöglichen wie auch die Vergleichbarkeit von Gutachten und Beweismaterial aus verschiedenen Quellen.

Projektleitung:

SBA Research

Projektpartner:

– Bundesministerium für Landesverteidigung und Sport (BMLVS)

Kontakt:

SBA Research
1040 Wien, Favoritenstraße 16
Dr. Edgar Weippl
Tel.: +43/1/505 36 88
E-Mail: eweippl@sba-research.org

Dipl-Ing. Sebastian Schrittwieser
Tel.: +43/1/505 36 88
E-Mail: sschrittwieser@sba-research.org

HASIF

Handlungsorientierte Sicherheitsforschung im Wohn- und Lebensraum

Das Projekt HASIF entwickelt ein wissenschaftlich fundiertes Modell zur Steigerung des subjektiven Sicherheitsempfindens in Wohnsiedlungen im städtischen Raum.

Das Thema „Sicherheit" ist in den vergangenen Jahren auch in Graz zunehmend zum Gegenstand öffentlichen, medialen und politischen Interesses geworden.

Im Unterschied zu Wien oder anderen Städten im deutschsprachigen Raum, gibt es jedoch keine etablierte Strategie für Gemeinwesenarbeit oder Siedlungsbetreuung. Auch eine wissenschaftliche Untersuchung des Zusammenhangs von aktivierender Bürgerarbeit und einer daraus resultierenden Steigerung des subjektiven Sicherheitsempfindens und der objektiven Sicherheitssituation in Wohn- und Lebensräumen existiert bis dato nicht.

Ausgangspunkt des Projektes HASIF war die Annahme, dass subjektive Lebenslagen und Lebenswelten in einem räumlichen Kontext in einem hohen Ausmaß die Vorstellungen von Sicherheit prägen und darüber hinaus auf die empfundene Lebensqualität abfärben. Im Mittelpunkt der Forschung steht eine gründliche Bestandsaufnahme mit wissenschaftlicher Begleitung auf lokaler Ebene ebenso wie die Entwicklung gezielter Präventionsmaßnahmen unter aktiver Beteiligung der Betroffenen selbst.

HASIF liegt eine gesamtheitliche Sicht von Sicherheit zugrunde. Das wird unter anderem dadurch deutlich, dass im Rahmen des Projektes ein interdisziplinäres Team (von der Polizei über Wohnungsamt, Sozialamt, Jugendamt bis hin zu Siedlungsgenossenschaften) daran arbeitet, Bewohner von Siedlungen für Fragen der erweiterten Sicherheit zu sensibilisieren und gemeinsam mit ihnen Aktivitäten zur Verbesserung zu setzen. Sicherheit wird als ein Themenbereich betrachtet, der eine Vielzahl von Ebenen und Adressaten berücksichtigt.

Die Zielgebiete der Forschung sind zwei konkrete Siedlungen in den Grazer Bezirken Jakomini und Lend, die zu jenem Stadtbereich zählen, in dem viele Migranten leben, und die als eher unattraktive Wohngebiete bzw. benachteiligte Bezirke gelten. Zusätzlich wurde in die Forschungsarbeit eine Vergleichssiedlung in der postindustriellen Zone der Stadt (Bezirk Eggenberg) einbezogen. In der Siedlung im Bezirk Lend wurden zudem nach der Erhebung auch gemeinwesenorientierte Maßnahmen gesetzt, während die beiden anderen Siedlungen nicht weiter betreut wurden.

In einem ersten Schritt wurden im Rahmen einer Regionalanalyse vorhandene Daten aufbereitet. Weiters wurden Interviews mit Vertretern relevanter Organisationen und Institutionen durchgeführt. Parallel dazu erfolgte eine explorative Annäherung, bei der auch die Bewohner befragt wurden. Zusätzlich wurde eine repräsentative Sicherheitserhebung in Form einer schriftlichen Befragung durchgeführt. Weiters wurden Kontakte und Kooperationen mit für das Projekt wichtigen Institutionen initiiert. Am Ende dieser Phase wurde in beiden Siedlungen ein Siedlungsfest zum Thema „Sind Sie sicher?" veranstaltet. Sowohl die Aktivierungsarbeit in der betreuten Siedlung wie auch die Vernetzungsarbeit wurden danach fortgesetzt.

Die große Bedeutung der räumlichen Strukturen für die Sicherheitswahrnehmung wurde in den drei Siedlungen im Zuge der Erhebung klar ersichtlich. In den beiden Siedlungen, in denen die Gemeinde ein Zuweisungsrecht hat, sind im Zusammenhang mit dadurch bedingten strukturellen Merkmalen der Mieter (hohe Fluktuation, Probleme zwischen alteingesessenen und neuen Mietern, verstärkt sozial hilfsbedürftige Menschen) andere Bedrohungsszenarien vorhanden als in der Vergleichssiedlung mit einer eher homogenen, mittelständischen Bewohnerschaft. Gewisse öffentliche Räume, Gruppen von Personen und Anzeichen von Verwahrlosung fördern das Gefühl einer hohen Sicherheitsgefährdung. In dieser Hinsicht bewirken vor allem Vandalismus, Verunreinigun-

Subjektive Lebenslagen und Lebenswelten in einem räumlichen Kontext prägen die Vorstellung von Sicherheit

Siedlungsfeste zum Thema „Sind Sie sicher?" waren Teil des Grazer Projektes HASIF

gen, Verschmutzung, „wild" entsorgter Sperrmüll, beschädigte Anlagen und öffentliche Räume, herumstehende zerstörte Fahrzeuge, verkommene Eingangsbereiche sowie alkoholisierte Menschen, Gruppen von (ausländischen) Jugendlichen oder (unbeaufsichtigten) Kindern in den beiden Übertragungsbauten vermehrte Unsicherheit.

Aus den Ergebnissen der Sicherheitserhebung lässt sich daher der Einfluss räumlicher und sozialer Strukturen auf die Sicherheitsempfindung und die Kriminalitätsfurcht deutlich ablesen. Konzentrierte soziale Probleme auf kleinräumiger, lokaler Ebene können zu massiven Veränderungen in der Sicherheitswahrnehmung führen. Besonders jene Menschen die mit ihrer Lebensqualität in der Wohnumgebung unzufrieden sind, bringen auch ihren Nachbarn weniger Vertrauen entgegen und fühlen sich an öffentlichen Orten in der Dunkelheit überproportional unsicher. Genau da setzen die Aktivitäten in der Umsetzungsphase an und haben bereits erste Erfolge gebracht. So berichtet der Hausverwalter über eine signifikant geringere Beschwerdetätigkeit aus der betreuten Siedlung – „entweder gibt es keine Probleme mehr oder es wurden andere Wege gefunden, sie zu behandeln".

Das im Projekt erarbeitete Modell zur Aktivierung der Ressource „BürgerInnen" in der Gestaltung des subjektiven Sicherheitsempfindens und der objektiven Sicherheitssituation soll übertragbar auf ähnliche Wohn- und Lebensräume sein. Da in diesem Bereich Subjektivität eine große Rolle spielt, deckt das Projekt einen Bereich ab, der durch strukturelle Maßnahmen von Politik und Sicherheitseinrichtungen nicht oder nur wenig gestaltbar ist. Das am Ende des Projektes vorliegende „Handbuch" soll die Vorgehensweise, Ergebnisse und Erfolge im Überblick aufzeigen und will Anregungen und übertragbare Ansätze zur Diskussion stellen. Es liefert damit eine gute Basis für eine direkte Umsetzung im Bereich der Kommunalpolitik, der Kommunalverwaltung und der Wohnbaugenossenschaften.

Projektleitung:

Grazer Büro für Frieden und Entwicklung

Projektpartner:

– IFA Steiermark – Institut für Arbeitsmarktbetreuung und -forschung in der Steiermark
– GEFAS – Akademie für Generationen

Kontakt:

Grazer Büro für Frieden und Entwicklung
8011 Graz, Wielandgasse 7/1
Mag. Jutta Dier
Tel: +43/316/872-2180
Fax: +43/316/872-2189
E-Mail: jutta.dier@friedensbuero-graz.at
Ursula Hauszer-Ortner
Tel: +43/316/872-2182
Fax: +43/316/872-2189
E-Mail: ursula.hauszer@friedensbuero-graz.at
Web: www.friedensbuero-graz.at

IDEMÖ

Identifikation mit Österreich bei jungen StaatsbürgerInnen mit und ohne Migrationshintergrund als Beitrag zur Sicherheit in Österreich

„IDEMÖ" untersucht, auf welche Weise junge Staatsbürger mit und ohne Migrationshintergrund Zugehörigkeits- und Loyalitätsgefühle gegenüber Österreich entwickeln.

Aktuell haben bereits 17,8 Prozent der österreichischen Bevölkerung einen direkten oder indirekten Migrationshintergrund. Dieser Anteilswert umfasst Einwohner mit nicht-österreichischer Staatsbürgerschaft, Personen, die im Ausland geboren sind und mittlerweile über die österreichische Staatsbürgerschaft verfügen, sowie Personen, deren Eltern im Ausland geboren sind. Zudem waren im Jahr 2009 bereits 24 Prozent der in Österreich geschlossenen Ehen bi-kulturell bzw. bi-national (Österreichischer Integrationsfonds 2010). Diese Zahlen legen nahe, dass für einen erheblichen Teil sowohl der Bevölkerung heute und künftig mehrfache ethnische, kulturelle oder nationale Bezüge und vielfältige Zugehörigkeits- und Loyalitätsgefühle zum alltäglichen Lebenszusammenhang gehören.

Zugehörigkeits- und Loyalitätsgefühle zur österreichischen Gesellschaft stellen nicht nur biographisch bedeutsame Themen für Staatsbürger dar, sondern sind auch grundlegende Elemente für den Zusammenhalt Österreichs. Dieser Zusammenhalt, der als „Systemintegration" bezeichnet wird, bildet eine Basis für die gesellschaftliche Konfliktprävention und -bewältigung und kann somit als wesentlicher sicherheitsrelevanter Aspekt von Integration verstanden werden. Sicherheit muss in diesem Kontext jedoch in einem weiteren Sinn verstanden werden.

Eine umfassende Sicherheitskonzeption ist auf die Stabilität der Gesamtgesellschaft gerichtet und berücksichtigt daher sowohl die Sicherheit von Personen mit Migrationshintergrund als auch von Angehörigen der Mehrheitsbevölkerung.

Integrationsdynamiken können dann problematisch werden, wenn auf Migrantenseite eine Entfremdung gegenüber der Aufnahmegesellschaft entsteht, aber auch dann, wenn die Mehrheitsgesellschaft auf einem monokulturellen Österreich-Bild beharrt, das nicht mehr der gesellschaftlichen Realität entspricht.

Die Gefahr solcher Entwicklungen darf daher nicht einseitig (d. h. mit Blick auf Migranten) gesehen werden. Gerade die im öffentlichen Diskurs häufige Unterstellung, dass Personen mit Migrationshintergrund potenziell radikaler oder gefährlicher seien als der Rest der Bevölkerung, erweist sich für Integrationsbestrebungen als kontraproduktiv und kann Auslöser für Rückzugstendenzen jenes Teiles der Bevölkerung darstellen. Ebenso trägt aber auch die Missachtung der als solche empfundenen Überforderung der Mehrheitsbevölkerung durch gesellschaftliche Veränderungen, die unter anderem Migration mit sich bringt, nicht zur Förderung einer integrierten Gesellschaft bei. Es stellt sich daher die Frage, inwiefern sich Staatsbürger mit Migrationshintergrund im vorherrschenden Bild von Österreich wiederfinden können und inwiefern die Mehrheitsgesellschaft in der Lage ist, soziale Tatsachen wie Zuwanderung anzuerkennen.

IDEMÖ widmet sich daher der Fragestellung, auf welche Weise junge Staatsbürger mit und ohne Migrationshintergrund sowie mit kulturell heterogenem Hintergrund Zugehörigkeits- und Loyalitätsgefühle zur österreichischen Gesellschaft entwickeln. Dabei sollen identifikationsförderliche Dynamiken ebenso ermittelt werden wie identifikationshinderliche Dynamiken und ihre jeweiligen gesellschaftlichen Bedingungen und Einflussfaktoren. Auf Basis der Ergebnisse sollen Empfehlungen abgeleitet werden, wie jene gesellschaftliche Prozesse gefördert werden können, die eine konfliktfähige und solidarische Gesellschaft stärken.

Ein erheblicher Teil der österreichischen Bevölkerung hat bereits heute mehrfache ethnische, kulturelle oder nationale Bezüge

Konkret behandelt IDEMÖ folgende Fragestellungen:

- Gibt es charakteristische Phasen und Prozesse in der Herausbildung eines Zugehörigkeitsgefühls zu Österreich?
- Welche Bedingungen und Faktoren (Personen, Institutionen oder Ereignisse) beeinflussen maßgeblich diese Prozesse?
- Gibt es diesbezüglich unterschiedliche Verläufe bei unterschiedlichen Personengruppen und lassen sich diese aufgrund von soziodemografischen Eigenschaften oder anderen Merkmalen zu Typen zusammenfassen?
- Lassen sich Verläufe identifizieren, die im Sinne eines umfassenden Sicherheitsbegriffes als besonders problematisch oder aber als besonders förderlich zu werten sind, und was sind deren Merkmale?
- Wie können die als besonders förderlich erachteten Verläufe gefördert werden?

Den Kern der Forschung von IDEMÖ bilden qualitative Interviews mit jungen österreichischen Staatsbürgern. Befragt werden Personen im Alter zwischen 18 und 30 Jahren. Da Zugehörigkeit in sehr verschiedenen Lebensbereichen eine Rolle spielen kann, werden fünf ausgewählte Bereiche der Lebenswelt als Ausgangspunkte für die Befragung genommen.

Der Innovationsgehalt von IDEMÖ liegt vor allem darin, das zunehmend aktuelle Thema der subjektiven Zugehörigkeit zur österreichischen Gesellschaft aus einer sozialwissenschaftlichen Perspektive aufzugreifen: Wie können angesichts von globaler Mobilität, (Trans-)Migration und bi-kulturellen Familienkontexten Verbindlichkeiten und Loyalitäten zu einem Staat und einer Gesellschaft entstehen? Was steht ihrer Entwicklung entgegen? Wie können solche Verbindlichkeiten und Loyalitäten gefördert werden? Was trägt zur Stärkung des Zusammenhalts auf der gesamtgesellschaftlichen Ebene bei? Indem das Forschungsprojekt den Blick sowohl auf die Dynamik als auch auf die konkreten Situationen und Zusammenhänge richtet, in denen sich Gefühle der Zugehörigkeit zur österreichischen Gesellschaft entwickeln, lassen sich Empfehlungen ableiten, wie der soziale Zusammenhalt in Österreich gestärkt werden kann.

Projektleitung:

Forschungsinstitut des Roten Kreuzes

Projektpartner:

– Österreichisches Rotes Kreuz
– in Kooperation mit dem Österreichischen Integrationsfonds

Kontakt:

Forschungsinstitut des Roten Kreuzes
1030 Wien, Nottendorfer Gasse 21
Edith Enzenhofer
Tel.: +43/1/795 80-2423
E-Mail: Edith.Enzenhofer@w.roteskreuz.at

ISKOS

InformationsSystemKonzeptOeffentlicheSicherheit

Das Projekt ISKOS erforscht Möglichkeiten zur Schaffung eines gesamtheitlichen Informationssystems für den Bereich der öffentlichen Sicherheit.

Die Entwicklung der letzten Jahre zeigt, dass die Schere zwischen den Anforderungen im Bereich der öffentlichen Sicherheit und der Komplexität der verfügbaren Hilfsmittel zunehmend auseinandergeht. Neue Herausforderungen ergeben sich durch die sich ständig ändernden gesellschaftlichen Rahmenbedingungen in Österreich, die immer stärker werdende Vernetzung der Staaten Europas, aber auch durch immer häufigere und komplexere Katastrophenszenarien aller Art. Schließlich stellen auch die gestiegene Mobilität von Kriminellen und deren verbesserte Fähigkeit zur Selbstorganisation und die daraus resultierende Effizienzsteigerung in ihren Handlungen ein junges Problem dar.

Für die Bewältigung der neuen Herausforderungen ist für die zuständigen Stellen der öffentlichen Sicherheit neben einer ausreichenden Zahl von personellen Ressourcen auch die Ausstattung mit adäquaten technischen Hilfsmitteln unerlässlich. Eine zentrale Rolle nehmen dabei Mittel zur Generierung, Aufbereitung und Verbreitung von Informationen aller Art ein. Gerade im Bereich der öffentlichen Sicherheit mit sich permanent ändernden Anforderungen und einem volatilen Umfeld ist der effiziente Umgang mit authentischen Informationen von großer Bedeutung.

Eine Aufgabe, die mit sogenannten Informationsservicesystemen realisiert wird. In solchen Systemen werden, gestützt auf Informations- und Kommunikationstechnologien (IKT), Informationen gesammelt, aufbereitet und an spezifische Abnehmer übermittelt. Leider sind Entscheider und Anwender dabei mit einer überaus heterogenen IKT-Systemlandschaft konfrontiert. In gleichem Maß wie der Bedarf an Leistungen im Bereich der öffentlichen Sicherheit in den letzten Jahren angewachsen ist, ist auch die Auswahl an technischen Lösungen im Bereich von IKT gestiegen. Neben der Anzahl an technischen Hilfsmitteln sind auch deren Komplexität und dadurch die Anforderungen an die Nutzer drastisch angestiegen. Unterschiedliche Standards sowie herstellerspezifische Eigenheiten verhindern oftmals die notwendige Integration verschiedenster Lösungen zu einem umfassenden und leistungsfähigen Gesamtsystem.

Im Zuge der Basis- bzw. Machbarkeitsstudie „ISKOS: Potenziale eines integrierten Informationssystemkonzepts für den Bereich der öffentlichen Sicherheit am Beispiel von Sonderlagen/Besonderen Lagen" wird vom Institut für Maschinenbau- und Betriebsinformatik (MBI) in enger Kooperation mit der Organisations- und Einsatzabteilung des Landespolizeikommandos für Steiermark ein synergetisches, integriertes und zukunftssicheres Konzept für ein solches Informationssystem erarbeitet.

Die Erarbeitung des Konzeptes erfolgt anhand eines Frameworks für die Auswahl, Bewertung und Integration von IKT-Lösungen auf Basis technologiefreier Schnittstellen. Auf Basis der Analyse von Tätigkeitsprofilen, Abläufen und Prozessen bei sogenannten „Sonderlagen" – darunter sind organisierte Kriminalität, Großveranstaltungen, Katastrophen- und Terrorszenarien etc. zu verstehen – werden Nutzenhebel definiert, die im Abgleich mit verschiedenen technologischen Lösungen eine Bewertung derer Effektivität im Hinblick auf die gestellten Anforderungen ermöglichen.

Darauf aufbauend wird unter Nutzung von Erkenntnissen aus bereits bestehenden techno-ökonomischen Frameworks zur Gestaltung von Informationsservicesystemen und unter Einbeziehung der speziellen Rahmenbedingungen und Anforderungen im Bereich der öffentlichen Sicherheit ein Informationssystemkonzept entwickelt, das die Umsetzung eines Gesamtsystems ermöglichen soll, das folgende Kriterien erfüllt:

Komplexe Sicherheitsanforderungen benötigen ein gesamtheitliches Informationssystem

nologien an definierten Sollbruchstellen kann ohne Beeinträchtigung der Gesamtfunktionalität des Gesamtsystems erfolgen.

Das geplante Informationssystemkonzept eröffnet damit künftig die Möglichkeit, Planungen und Entscheidungen in Hinblick auf die Integration neuer IKT-Komponenten nach den Anforderungen des Zielsystems (Organisation, Nutzer, Anwendungen) und weitgehend losgelöst von technischen Zwängen abwickeln zu können. Weiters sollen in Hinblick auf die geplante Weiterführung und Implementierung die Potenziale einer systematischen und standardisierten Planung von IKT-Serviceleistungen in speziellen Bereichen der öffentlichen Sicherheit wie beispielsweise der Bewältigung von Sonderlagen erhoben werden. Als Basis- bzw. Machbarkeitsstudie ist ISKOS zudem als Vorstufe für eine technische Prototypenentwicklung (PL3) zu sehen.

Anforderungen und Hilfsmittel der öffentlichen Sicherheit haben sich in den letzten Jahren auseinanderentwickelt

- Synergetisch. Das Gesamtsystem ist von unterschiedlichen (internen und externen) Stellen nutzbar.
- Integriert. Das Gesamtsystem ist auf die jeweiligen Anforderungen zugeschnitten und fügt sich in die Systemlandschaft ein.
- Zukunftssicher. Ein partieller Austausch von Tech-

Projektleitung:

TU Graz, Institut für Maschinenbau- und Betriebsinformatik

Projektpartner:

– Landespolizeikommando Steiermark (LPK)

Kontakt:

TU Graz, Institut für Maschinenbau- und Betriebsinformatik
Univ.-Prof. Dipl.-Ing. Dr. Siegfried Vössner
8010 Graz, Kopernikusgasse 24/III
Tel.: +43/316/873-8001
E-Mail: voessner@tugraz.at


Optimale Sicherheit

Subjektive Sicherheit der österreichischen Bevölkerung versus Dienststellendichte der Polizei

Das Projekt „Optimale Sicherheit" untersucht, ob und welcher Zusammenhang zwischen der Dichte an Polizeistellen und dem Sicherheitsgefühl der Österreicher besteht.

Im Mittelpunkt des Projektes „Optimale Sicherheit" stand die Frage, ob zwischen der Dienststellendichte der Exekutive und dem subjektiven Sicherheitsgefühl der Bevölkerung ein Zusammenhang hergestellt werden kann. Davon ausgehend, wäre es im Rahmen der strategischen Polizeiarbeit wichtig, zu wissen, ob man von einer optimalen Dienststellendichte der Polizei ausgehen kann.

Weitere Fragestellungen betrafen das Sicherheitsgefühl im Zusammenhang mit Dienststellenschließungen und der Wichtigkeit von öffentlicher Präsenz der Polizei sowie in Relation zur Sicherheitslage. In diesem Zusammenhang wurden im Rahmen von „Optimale Sicherheit" auch allgemeine Kriminalitätsängste der Bevölkerung erhoben. Weiters wurde das öffentliche Auftreten und die Präsenz der Exekutivbeamten (also die Arbeit der Polizei) aus der Perspektive der Bevölkerung bewertet, um im Bedarfsfall interne Qualitätsstandards im Rahmen der Aus- und Weiterbildung der .SIAK im BMI optimieren zu können.

Repräsentative Bevölkerungsbefragungen lieferten die Basis für weiterführende Regressionsanalysen und Modellrechnungen, die mit Kriminalitätsdaten aus dem BMI verknüpft wurden. Zusätzliche tiefergehende Erkenntnisse wurden aus österreichweiten qualitativen Interviews gewonnen. Die Daten beider Befragungen wurden anschließend mit regionalen Daten über die Arbeitslosigkeit, Kriminalitätsentwicklung und Dienststellen auf Ebene der politischen Bezirke bzw. der Bundesländer sowie Daten über die befragte Person verknüpft.

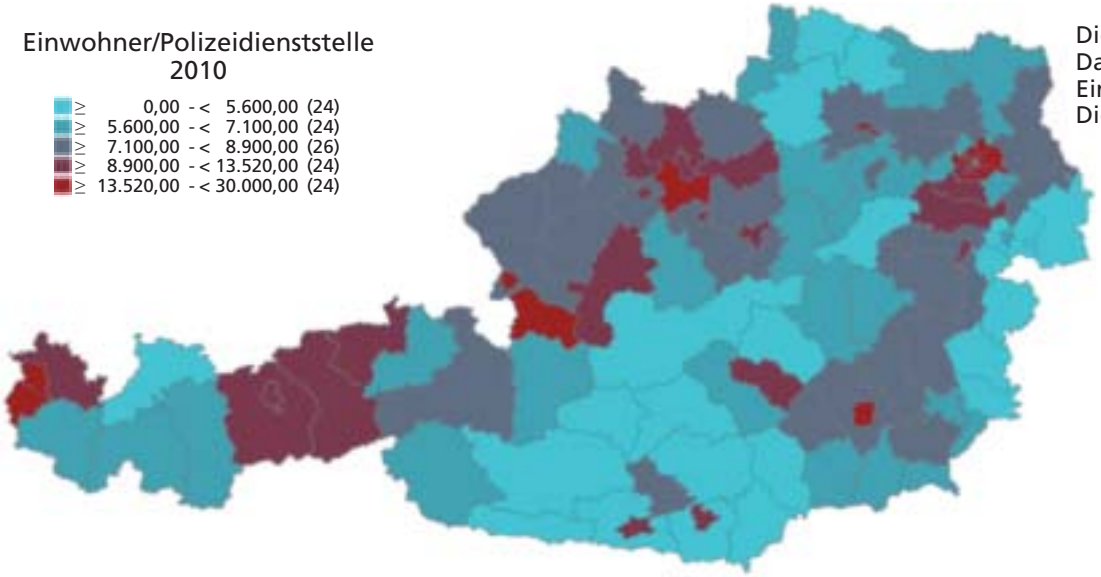
Im Allgemeinen kann ein statistisch signifikanter Zusammenhang zwischen polizeilicher Dienststellendichte und dem subjektiven Sicherheitsgefühl festgestellt werden. Die Effekte auf das Sicherheitsgefühl sind im Allgemeinen jedoch sehr klein. So würde eine österreichweite Eröffnung von 121 zusätzlichen Dienststellen das Sicherheitsgefühl der Bevölkerung (Wahrscheinlichkeit sich sicher zu fühlen) von 76 auf 76,5 Prozent erhöhen. Bei Opfern vergangener Straftaten würde sich das Sicherheitsgefühl von 78 auf 78,7 Prozent (Opfer schwerer Straftaten) bzw. von 70 auf 70,7 Prozent (Opfer leichterer Straftaten) erhöhen.

Um das Sicherheitsgefühl der Wiener Bevölkerung, das im österreichweiten Vergleich am geringsten ist, auf das gesamtösterreichische Niveau zu heben, wäre eine Erhöhung der Dienststellendichte um 12,5 Prozent nötig, was einer Eröffnung von 13 neuen Dienststellen entsprechen würde.

Anhand dieser Beispiele wird deutlich, dass eine Erhöhung der Dienststellendichte wahrscheinlich ein kostenintensives, aber wenig effizientes Instrument ist, um das Sicherheitsgefühl der österreichischen Bevölkerung zu steigern.

Unterschiede im Sicherheitsgefühl können bei verschiedenen Untergruppen der Bevölkerung festgestellt werden. Es zeigt sich, dass Ältere im Allgemeinen unsicherer sind und dass sich das Sicherheitsgefühl der österreichischen Bevölkerung mit steigender Ausbildung erhöht. Ein weiterer „robuster Effekt" ergibt sich bei Opfern von Straftaten, deren Sicherheitsgefühl im Vergleich zur Gesamtbevölkerung niedriger ist. Dieser Effekt ist auch in den einzelnen Untergruppen der Bevölkerung (Frauen, unterschiedliche Bildungsgruppen, Ältere) nachzuweisen.

Weiters ergaben sich im Rahmen einer Bevölkerungsbefragung, die repräsentativ auf die politischen Be-



Diensstellendichte: Darstellung nach Einwohnern pro Dienststelle

zirke (N=12.100) erhoben wurde, signifikante Effekte der aktuellen Kriminalitätslage auf das subjektive Sicherheitsgefühl der Bevölkerung. So senkt eine einprozentige Erhöhung der Delikte pro Einwohner die Wahrscheinlichkeit sich sicher zu fühlen, um 0,02 Prozentpunkte. Die Schätzungen ergaben zudem, dass eine Erhöhung der Zahl der Arbeitslosen pro Erwerbsfähigem um einen Prozentpunkt zu einem Sinken der Wahrscheinlichkeit sich sicher zu fühlen, um 0,01 Prozentpunkte führt. Im Rahmen eines kleineren Datensatzes (N=1.500) konnten diese Effekte allerdings nicht nachgewiesen werden.

Das Vorhandensein einer Polizeidienststelle hat damit auf der einen Seite zwar hohe Priorität für die österreichische Bevölkerung, auf der anderen Seite fühlen sich die Österreicher zum Großteil wenig durch Polizeidienststellenschließungen in ihrem Sicherheitsgefühl beeinträchtigt. Wichtiger für das subjektive Sicherheitsgefühl scheint bei näherer Betrachtung der Daten nicht die unmittelbare geografische Erreichbarkeit einer Polizeidienststelle zu sein, sondern das schnelle Eingreifen der Polizei im Alarmfall. Man erwartet, dass die Polizei rund 12,5 Minuten von der Alarmierung bis zum Eintreffen benötigt. Optimal wäre ein Wert von sieben Minuten.

Nur eine einfache Erhöhung von Polizeidienststellen bzw. Polizeiinspektionen (MW 2,45) würde nicht so stark zu einem erhöhten Sicherheitsgefühl beitragen, als die öffentliche Präsenz und die Reaktion der Polizei. Insgesamt würde das Sicherheitsgefühl am stärksten erhöht werden, wenn die Polizei nach Alarmierung schneller vor Ort eintreffen würde (MW 1,85), es auf der Straße präsentere Polizisten (MW 2,10) sowie Patrouillen (MW 2,12) gäbe. Diese Faktoren tragen zum Sicherheitsgefühl entscheidend bei. Ebenfalls wären eine effiziente „Rund-um-die-Uhr-Besetzung" der Polizeidienststellen (MW 2,21), eine bessere Beleuchtung auf Straßen und in Garagen (MW 2,22) und eine verstärkte polizeiliche Kontrolle (MW 2,27) Maßnahmen, die das subjektive Sicherheitsempfinden der Österreicher stark erhöhen würden.

Projektleitung:

Institut für Höhere Studien, Dr. Susanne Kirchner

Projektpartner:

– Institut für Wissenschaft und Forschung der .SIAK im BM.I
Kontakt: Dr. Katharina Weiss, Mag. Linda Jakubowicz

Kontakt:

Institut für Höhere Studien (IHS)
Dr. Angleitner, B./Dr. Kirchner, S./
MMag. Schwarzbauer, W.
A-1060 Wien, Stumpergasse 56
Tel.: +43/1/599 91-0
Fax: +43/1/599 91-555
E-Mail: Barbara.Angleitner@ihs.ac.at
E-Mail: Susanne.Kirchner@ihs.ac.at
E-Mail: Wolfgang.Schwarzbauer@ihs.ac.at
Web: www.ihs.ac.at

ORESP

Organizational Response to Heat Waves

Das Rote Kreuz Österreich entwickelt im Rahmen von ORESP Konzepte, um die Betreuung und Versorgung von Risikogruppen im Falle einer Hitzewelle zu optimieren.

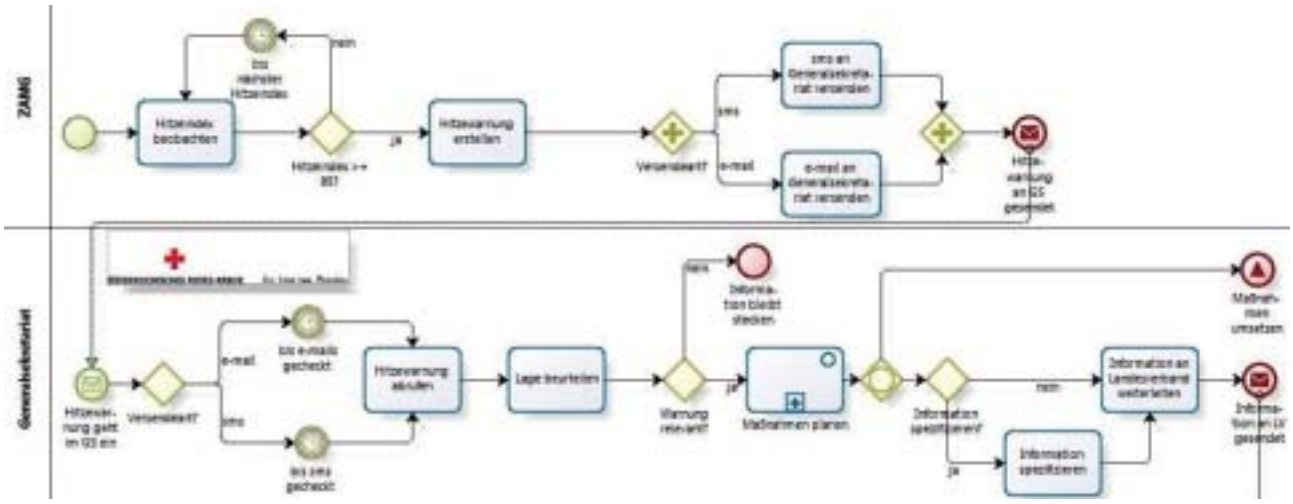
Hitzewellen stellen für sozial benachteiligte Personen in der Gesellschaft eine große Bedrohung dar. Vor allem alte und gebrechliche Menschen, die sozial isoliert sind, gelten als besonders gefährdet. Die Hitzewelle im Jahr 2003, die in Europa mehr als 30.000 Menschenleben gekostet hat, zeigte in dramatischer Weise die Mängel hochentwickelter Gesundheitssysteme hinsichtlich der adäquaten Betreuung sozialer Randgruppen. Maßnahmen kamen zu spät und im Bereich der Prävention wurde zu wenig unternommen, wodurch erst die Notaufnahmen der Krankenhäuser und später die Leichenschauhäuser überfüllt wurden. Andererseits sind laut Statistik Austria vor allem bei über 60-jährigen Menschen deutliche Bevölkerungszuwächse zu erwarten. Bis ins Jahr 2030 wird mit einem Plus von 52 Prozent (gegenüber 2007) gerechnet. Folglich wird ein vermehrter Bedarf an extramuraler Pflege und Betreuung, auch von alternden Menschen mit Migrationshintergrund, entstehen.

Das Österreichische Rote Kreuz spielt im Falle einer Hitzewelle eine tragende Rolle und ist gemeinsam mit den verantwortlichen Behörden und anderen Hilfsorganisationen für den Katastrophenschutz verantwortlich. Das Österreichische Rote Kreuz ist außerdem aktiv in die Erstellung der nationalen Klimawandelanpassungsstrategie involviert und stellt dort seine Expertise in Fragen zu den Aktivitätsfeldern Gesundheit, Naturgefahren und Wasserwirtschaft zur Verfügung. In Hinblick auf das Szenario häufigerer Hitzewellen bei einer steigenden Zahl gefährdeter Personen stellte sich die Frage, in welcher Form das Rote Kreuz darauf reagieren muss und ob die derzeitigen Verfahrensprozesse adäquat gestaltet sind, um potenziell Bedürftigen die notwendige Hilfe zuteil werden lassen zu können.

Im Rahmen der Recherchen für das Projekt hat sich herausgestellt, dass es in Europa bereits zahlreiche Projekte und Initiativen gibt, die sich mit Hitzewellen im engeren und weiteren Sinn beschäftigen. Alle Projekte und Forschungsinitiativen gehen davon aus, dass Hitzewellen und Hitzetage massiv zunehmen werden. Den meisten Studien ist zudem gleich, dass sie als Hochrisikogruppe Personen im Alter von über 65 Jahren definieren. Im Projekt „Prevention of acute Health Effects of Weather conditions in Europe" wurde diese Zielgruppe hinsichtlich der Mortalitätsrate in 15 Städten europaweit untersucht (Matthies et al., 2008). Diese Population liegt in Österreich 2010 bei 1.475.065 Personen. Diese Zahl steigert sich bis 2035 auf 2.379.574 Personen. Unter Berücksichtigung der Steigerung der Hitzetage ist sogar mit mehr als einer Verdopplung zu rechnen.

Ein wesentlicher Bestandteil des Projektes ist die Erstellung eines Kommunikationskonzeptes, um die identifizierten Risikogruppen erreichen zu können. Eine Medienanalyse hat dabei ergeben, dass zum Beispiel das Radio bei älteren Menschen ein stark genutztes Medium darstellt. Die Erreichbarkeit liegt hier bei 77,7 Prozent (Alter 60 bis 69) beziehungsweise 84,2 Prozent (älter als 70 Jahre). Die Tophörzeiten liegen zwischen 07:00 und 08:15 und zwischen 12:00 und 12:15 (Teletest 2006). Für die Erreichbarkeit älterer Menschen via Radio bieten sich diese Zeiten in Bezug auf Hitzewellen an, um zum Beispiel Hitzewarnungen zu kommunizieren. Die Erreichbarkeit älterer Personen über das Internet ist eher gering. Nur acht Prozent der Menschen älter als 80 und elf Prozent der Menschen älter als 70 Jahre haben Zugang zum Internet. In der Gruppe der Menschen im Alter von 60 bis 69 sind es 24 Prozent (Medianalyse 2008/09). Diese Zahlen werden allerdings auf lange Sicht massiv ansteigen. Für eine langfristige Strategie ist also das Internet auf jeden Fall in den Mediencocktail aufzunehmen.

Ein Medium mit sehr hoher Reichweite bei älteren Menschen ist das Fernsehen. Vor allem im Bereich der Menschen im Alter von über 70 Jahren wächst



Prozessanalyse: Darstellung wie im Falle einer Hitzewelle Risikogruppen infomiert und Maßnahmen gesetzt werden

der Anteil der Nutzung dieses Mediums. 60- bis 69-Jährige werden laut Mediaanalyse 2009/08 zu 77,7 Prozent erreicht und Menschen älter als 70 Jahre zu 82,2 Prozent. Das Fernsehen strahlt auch ein Begleitmedium aus: den Teletext. 45 Prozent der Menschen älter als 50 Jahre nutzen den Teletext regelmäßig (Kubitschke et al. 2002). Die Medienanalyse lässt darauf schließen, dass eine Meldung über Hitzewellen und Maßnahmen zum Schutz vor deren Auswirkungen im TV am besten über ORF 2 rezipiert würde. Hier wiederum in den Sendungen der ZIB 1 und in Bundesland Heute. Diese Sendungen sind tagesaktuell und werden sehr häufig von der Personengruppe älter als 65 Jahre konsumiert.

Ein weiterer Bestandteil des Projektes ist die Analyse Rot-Kreuz-interner Prozesse, die im Rahmen von Hitzewellen ablaufen. Im Rahmen der Prozessanalyse wird es möglich, die Strukturen, Abläufe und Schnittstellen darzustellen und zu evaluieren. Dies wird für das vorliegende Projekt mittels einer Prozessmodellierung durchgeführt, die dazu dient, den derzeitigen Fluss der Information „Hitzewarnung" darzustellen. Vor allem in Hinblick auf eine Reorganisation des Prozesses „Weiterleitung der Information Hitzewarnung" ist eine Erhebung des Ist-Zustandes unumgänglich, dabei werden alle relevanten Abläufe auf den Prüfstand gestellt. Es wird nach einem dem Total-Cycle-Time ähnlichen Problemlösungskreislauf vorgegangen, der mit der Auswahl des Problems beginnt, weiter über dessen Analyse verläuft, anschließend eine Lösungssuche und deren Umsetzung vorsieht ebenso wie die Wirkung der Lösung und abschließend eine Standardisierung vorschlägt.

Die Ergebnisse aus den Arbeitspaketen werden zusammengeführt und fließen in eine Optimierung der Rot-Kreuz-internen Prozesse und des externen Schnittstellenmanagements ein. Dies führt letztlich zu einer Adaptierung der Prozesse, die Instrumente der Qualitätskontrolle beinhalten. Dem Abschluss des Projektes folgt die Planung spezifischer Maßnahmen für Hitzewellen innerhalb des Roten Kreuzes. Die Ergebnisse des Projektes werden in Form eines Endberichts allen Einsatzorganisationen und Behörden zur Verfügung stehen.

Projektleitung:

Österreichisches Rotes Kreuz

Projektpartner:

– Universität für Bodenkultur
– Österreichischer Rundfunk – Hitradio Ö3,
– Forschungsinstitut des Roten Kreuzes

Kontakt:

Österreichisches Rotes Kreuz
Dipl.-Ing. Clemens Liehr
1040 Wien, Wiedner Hauptstraße 32
Tel.: +43/1/589 00-134
Fax: +43/1/589 00-139
E-Mail: clemens.liehr@roteskreuz.at
Web: www.roteskreuz.at

DaMon

Der Informationskrieg im Internet: Monitoring zur Datensicherheit in Österreich

Die Studie liefert erstmals einen unabhängigen und repräsentativen Forschungsbeitrag zum Thema Cybersicherheit in Österreich mit Fokus auf kritische Sektoren.

Behörden, Unternehmen aber auch Privatpersonen sind mit regelmäßigen Bedrohungen aus dem virtuellen Raum konfrontiert: Hackerangriffe, Viren, Malware, Trojaner, Datenspionage, Datenlecks, Datenhandel. In wenigen Fällen steckt Ernstzunehmendes dahinter. Meistens besteht der Schaden in der zeit- und ressourcenaufwendigen Klassifizierung einzelner Vorfälle. Ähnlich wie bei der Spam-Abwehr ist der daraus resultierende volkswirtschaftliche Schaden jedoch enorm.

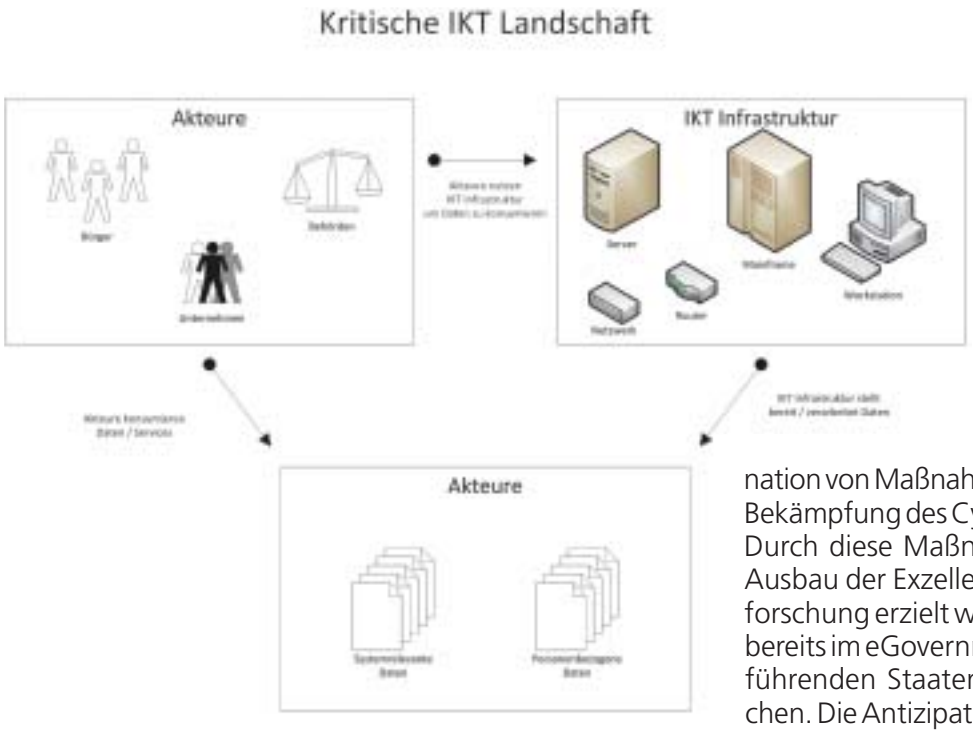
Einzelne Vorfälle können sogar zur Existenzbedrohung für Unternehmen und sogar ganzer Staaten werden. Estland war im Jahr 2007 Ziel eines groß angelegten Angriffs, der die Unerreichbarkeit von Regierungs- und Verwaltungssystemen zur Folge hatte. Die größte Bank Estlands musste den internationalen Zahlungsverkehr einstellen und Krankenhäuser und Energieversorgungssysteme waren in Mitleidenschaft gezogen. Unter Verwendung von über 160.000 „Zombie"-Rechnern wurden im Juli 2009 Südkorea und die USA das Ziel mehrerer „DDoS-Angriffe".

Vor diesem Hintergrund und den damit verbundenen Herausforderungen an Behörden, Unternehmen und Bürger sowie unter Berücksichtigung der derzeitigen und zukünftigen Bedeutung von Datensicherheit für die Gesamtwirtschaft, widmet sich die Studie „DaMon – Der Informationskrieg im Internet: Monitoring zur Datensicherheit in Österreich" folgenden Punkten:

- Design einer Langzeitstudie, die in regelmäßigen Abständen durchgeführt werden kann, um die Entwicklung und Veränderung der Sicherheitslage erheben und die Auswirkungen von Maßnahmen auf die Akteure analysieren zu können.
- Erfassung der Wahrnehmung und Bedeutung von Datensicherheit bei Bürgern, Behörden sowie in der betrieblichen Praxis heimischer Unternehmen und der sich daraus ergebenden Anforderungen unter besonderer Berücksichtigung der Situation in kleinen und mittleren Unternehmen (KMU).
- Umfassende Analyse des Umgangs mit Datensicherheit in österreichischen Behörden und Unternehmen sowie Darstellung der Hintergründe, die zum Einsatz und zur Nutzung entsprechender Schutzmaßnahmen führen.
- Erarbeitung eines Maßnahmenkatalogs zur Stärkung des nationalen IKT-Sicherheitsbewusstseins und zum Ausbau nationaler technologischer Abwehrmaßnahmen.
- Formulierung von Schlussfolgerungen und Handlungsempfehlungen in Hinblick auf (wirtschafts-) politische Maßnahmen zur Unterstützung von Schutzmaßnahmen.

Für die Durchführung der Studie wird eine Kombination aus qualitativen und quantitativen Erhebungsinstrumenten der empirischen Sozial- und Wirtschaftsforschung verwendet. Dieser Ansatz erlaubt eine differenzierte Analyse der formulierten Forschungsfragen:

- Wie hoch und wie aktuell ist das IKT-Sicherheitsbewusstsein („Awareness") bei österreichischen Bürgern, Behörden sowie Entscheidungsträgern in österreichischen Unternehmen in Bezug auf Datensicherheit und entsprechende Schutzmaßnahmen?
- Welche Bedrohungen liegen grundsätzlich vor und warum?
- Welche Faktoren sind für die Implementierung von Datensicherheitsmechanismen in Unternehmen ausschlaggebend?
- Wie sehr vertrauen Bürger den Datensicherheits- und Datenschutzmaßnahmen von Unternehmen und Behörden?
- Wie gut sind Unternehmen und Behörden für den Krisenfall (z. B. eine Cyberattacke auf kritische Infrastrukturen) vorbereitet?
- Wie hoch ist die Akzeptanz von Sicherheitsmaßnahmen durch die Gesellschaft?



Cybersicherheit: Darstellung der Akteure und der betroffenen Infrastruktur

- Wie kann die gesellschaftliche Dimension von Cyberattacken bewertet werden: Was löst das Vorliegen der Gefahr in der Bevölkerung und in Unternehmen aus?

DaMon stellt die erste Umfrage zum Thema Cyberterrorismus in Österreich dar. Die Unabhängigkeit und Repräsentativität macht sie zu einem elementaren Element für die Sicherheitsanalyse des Gesamtsystems. Die Studie erlaubt erstmalig die Erfassung der Risikolage in Österreich, die Analyse von Schwachstellen im Gesamtsystem sowie die Definition von Schutzmaßnahmen in Form von Prävention.

Zudem ermöglicht sie die Generierung sicherheitspolitisch erforderlichen Wissens über langfristig relevante Trendentwicklungen und liefert somit eine grundlegende Entscheidungsbasis für Behörden und Unternehmen in Bezug auf die Regulierung des Internets. Die Erforschung der gesellschafts- und wirtschaftspolitischen Auswirkungen bei Ausfall von kritischen Infrastrukturen stellt darüber hinaus eine wesentliche Grundlage für die Definition entsprechender Schutz- und Sicherungsmaßnahmen der Behörden dar.

Die Studie kann aber nicht nur zur Erhöhung der Sicherheit und des Sicherheitsbewusstseins beitragen, sondern dient auch als Basis für die bessere Kooperation und Koordination von Maßnahmen und Akteuren, die zur Bekämpfung des Cyberterrorismus beitragen. Durch diese Maßnahmen kann der weitere Ausbau der Exzellenz im Bereich Sicherheitsforschung erzielt werden und Österreich (wie bereits im eGovernment-Sektor) zu einem der führenden Staaten auf diesem Gebiet machen. Die Antizipation mittelfristiger Entwicklungen in Bezug auf die nationale Sicherheit kann einen wesentlichen Beitrag zur nationalen Wertschöpfung liefern. Die Erzielung von Wissens-, Verfahrens- und Technologiesprüngen bringt zudem eine Verbesserung der globalen Wettbewerbsfähigkeit des Wirtschaftsstandorts Österreich.

Projektleitung:

TU Wien, Institut für Softwaretechnik und Interaktive Systeme

Projektpartner:

– Technische Universität Wien, Institut für Softwaretechnik und Interaktive Systeme
– Universität Wien, Fakultätszentrum für Methoden der Sozialwissenschaften
– Wirtschaftskammer Österreich, Bundessparte Information und Consulting
– Bundeskanzleramt

Kontakt:

TU Wien, Institut für Softwaretechnik und Interaktive Systeme
Prof. Dr. A Min Tjoa
1040 Wien, Favoritenstraße 9/188
Tel.: +43/1/58801-18801
Fax: +43/1/58801-18899
E-Mail: amin@ifs.tuwien.ac.at

link-up

Verknüpfung von Fehlernetz- und Risikoanalyse mit Vulnerabilitätsbetrachtungen in der Trinkwasserwirtschaft

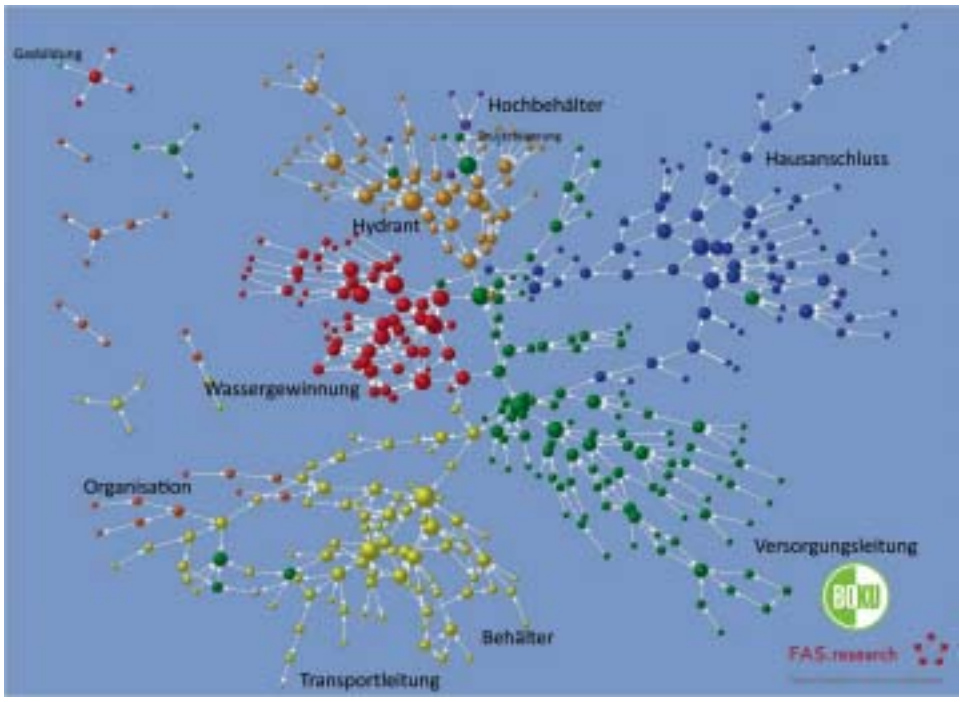
link-up verbindet die zwei bereits entwickelten Werkzeuge ACHILLES und FEIS zu einem integralen Risikomanagement für die Trinkwasserversorgung in Österreich.

Im Rahmen des KIRAS Sicherheitsforschungsprogramms führten sowohl die Universität für Bodenkultur (BOKU-SIG) als auch die Universität Innsbruck bereits zwei Projekte zur Risikominimierung im Trinkwasserbereich durch. Der grundlegende Unterschied zwischen den beiden daraus entwickelten Anwendungen FEIS und ACHILLES liegt in den angewendeten Risikobetrachtungen.

ACHILLES basiert auf quantitativer sowie lokaler Risikobetrachtung. Die quantitative Risikobewertung hat zum Ziel, objektive numerische Werte für alle Komponenten der Risikoanalyse zu berechnen. Der Vorteil der quantitativen Risikobetrachtung besteht vor allem darin, dass die Ergebnisse für Entscheidungsträger gut verständlich als absolute Werte vorliegen. Der Nachteil liegt in der Notwendigkeit, Daten wie die Eintrittswahrscheinlichkeit von Ereignissen sowie das Ausmaß des dadurch verursachten Schadens quantifizieren zu müssen. Diese Daten sind jedoch oft nur unter größerem Aufwand ermittelbar. Bei der lokalen Risikobetrachtung wird hauptsächlich die externe Gefahrenlage (Muren, Terroristen, Unfälle etc.) erhoben und örtlich referenziert. ACHILLES führt eine solche Betrachtung durch. Der Vorteil dieser Betrachtung besteht durch die Referenzierung des Ortes, von dem eine Gefahr ausgeht bzw. wo der Schaden am größten ist. Nachteil dabei ist, dass funktionale Zusammenhänge und die Anzahl von Szenarien begrenzt sind.

Im Gegensatz dazu basiert FEIS auf der qualitativen und funktionalen Risikobetrachtung. Bei der qualitativen Analyse werden – anders als bei der quantitativen Risikobetrachtung – nur relative numerische Werte berechnet. Dies gilt auch für die Berechnung der möglichen Auswirkungen eines eingetretenen Risikos. Der Vorteil einer qualitativen Herangehensweise liegt darin, dass keine umfangreiche Ermittlung von Eintrittswahrscheinlichkeiten und Schadensausmaß erfolgen muss, um eine Prioritätenreihung zu erstellen und Wissen zu den einzelnen kritischen Punkten zu sammeln. Der Nachteil einer qualitativen Risikobetrachtung besteht darin, dass die resultierenden Zahlen auf subjektiven Schätzungen basieren und nicht absolut sind. Durch das Einbringen einer systematischen Methodik und von Erfahrungswerten, wie zum Beispiel durch FEIS, kann die Subjektivität reduziert und die qualitative Risikobetrachtung zu einem Expertensystem ausgebaut werden. Bei der funktionalen Risikobewertung in FEIS werden hauptsächlich Betriebserfahrung (Erfahrungen, Ereignisse, Fehler etc.) erfasst und funktionale Zusammenhänge im Wasserversorgungssystem analysiert.

Durch die Verknüpfung von qualitativer und quantitativer sowie von funktionaler und lokaler Risikobetrachtung wird zusätzliche Information gewonnen, mit der die Risikobewertung besser angepasst werden kann. Einerseits werden aus der funktionalen Objektanalyse Szenarien ausgegeben, die als Ausgangspunkt für die numerische Systemanalyse dienen. Für die vorliegende Kombination bedeutet das, dass FEIS kritische Fehlerursachen und deren Fehlerketten als Input für die Modellierung in ACHILLES liefert. Somit wird die Information aus den gesammelten Erfahrungen vieler Wasserversorger anderen Nutzern zur Verfügung gestellt und für die individuelle numerische Systemanalyse bei einzelnen Wasserversorgern angewendet. Andererseits werden aus der quantitativen Systemanalyse numerische Werte aus einzelnen Szenarien ausgegeben, die zur Kalibrierung der funktionalen Objektanalyse dienen. Dabei dient die Bewertung der Auswirkungen von konkreten



Visualisierung von Fehlerketten

Fällen bei einzelnen Wasserversorgern aus der ACHILLES-Modellierung als Input für die Kalibrierung verschiedener Parameter in FEIS. Darüber hinaus werden Szenarien bzw. Vulnerabilitätskarten aus ACHILLES als Input für neue Gefährdungen und Auswirkungen im Wasserversorgungssystem in die FEIS-Datenbank importiert.

Durch diesen Informationsaustausch können insbesondere kleine Wasserversorger mit begrenzten Personalressourcen auf die Erfahrungen der allgemeinen Wissensdatenbank zurückgreifen. Da fast zwei Drittel der österreichischen Bevölkerung in kleinen und mittleren Gemeinden mit weniger als 50.000 Einwohnern leben, ist für die Erhaltung der Funktionsfähigkeit der Wasserversorgung in Österreich daher in besonderem Maße auf die kleinräumige Siedlungsstruktur Bedacht zu nehmen.

Beim Entwurf der Schnittstelle für den Informationstransfer zwischen FEIS und ACHILLES wurde sichergestellt, dass numerische Bewertungen von konkreten Fällen immer aggregiert und in anonymisierter Form in die allgemeine Wissensdatenbank fließen. Die technischen Kriterien und die Schnittstellenbeschreibung für den Informationstransfer in beide Richtungen wurden bereits in der Studie berücksichtigt und stellen die Grundlage für die Umsetzung dar.

Durch eine Verknüpfung der beiden Anwendungen FEIS und ACHILLES können eine gegenseitige Ergänzung der beiden Systeme und ein Mehrwert für den Wasserversorger als Nutzer einer kombinierten Anwendung erreicht werden. Ziel des integralen Risikomanagements ist eine gemeinsame Lösung, bei der FEIS und ACHILLES vor Ort implementiert werden und beide Systeme für den hier beschriebenen Informationstransfer miteinander kommunizieren. Die damit erzielte Kombination von quantitativer und qualitativer Risikobetrachtungen ist besonders für die dezentrale Versorgungsstruktur und die damit einhergehenden begrenzten Personalressourcen von großem Nutzen.

Projektleitung:

Universität für Bodenkultur Wien, Institut für Siedlungswasserbau (BOKU-SIG)

Projektpartner:

– Universität Innsbruck, Institut für Infrastruktur, Fachbereich Umwelttechnik
– Universität Innsbruck, Institut für Informatik, Quality Engineering

Kontakt:

Universität für Bodenkultur Wien
Dr. Reinhard Perfler
1190 Wien, Muthgasse 18
Tel.: +43/1/476 54-5808
Fax: +43/1/368 99 49
E-Mail: reinhard.perfler@boku.ac.at
Web: www.wau.boku.ac.at

RITA

Risiko des Herzkammerflimmerns bei Taser-Applikation

Das Projekt RITA schafft erstmals fundierte quantitative Grundlagen zur Risikoabschätzung des Einsatzes von Tasern, insbesondere in Bezug auf das Auslösen von Herzflimmern.

Die Funktion von Tasern beruht darauf, dass an den Körper kurze Hochspannungspulse bis zu einer Höhe von 50.000 Volt abgegeben werden, die eine Verkrampfung der Skelettmuskulatur auslösen. Der Einsatz erfolgt entweder aus der Distanz durch das Abfeuern zweier pfeilartiger Elektrodenspitzen (Distanz-Applikation) oder indem der Taser direkt in Kontakt mit dem Körper gebracht wird (Kontakt- Applikation). Aus Sicht der Exekutive ist der Taser derzeit die einzige Alternative zur Schusswaffe, mit der die Angriffs- und Widerstandsfähigkeit einer Person unmittelbar unterbunden werden kann.

In der Öffentlichkeit besteht aber aufgrund berichteter Todesfälle die Angst, dass diese durch die Einwirkung von Tasern verursacht worden sein könnten. Es wird befürchtet, dass der Einsatz von Tasern Herzkammerflimmern auslösen kann, da ein Teil des elektrischen Stromes auch über das Herz fließen kann. Herzkammerflimmern ist eine Herzrhythmusstörung, bei der sich der Herzmuskel nicht mehr geordnet kontrahiert und die ohne rechtzeitige Behandlung unmittelbar zum Tod führt.

Im Rahmen des Projektes RITA soll dieses Gefährdungspotenzial anhand der beiden typischen Anwendungsfälle Distanz- und Kontakt-Applikation und anhand der drei unterschiedlichen Taser-Gerätetypen X26, X3 und XREP erstmals umfassend untersucht werden.

Durchgeführt werden die Untersuchungen am Institut für Health Care Engineering der Technischen Universität Graz, das über die erforderliche Ausrüstung zur messtechnischen Untersuchung von Taser-Pulsen verfügt. Darüber hinaus verfügt das Institut über die Möglichkeit, die derzeit modernsten und genauesten Rechenverfahren zur Untersuchung der Auswirkungen im Körperinneren einzusetzen – ohne ethisch und methodisch problematische Versuche an lebenden Tieren oder an Menschen durchführen zu müssen. Dazu stehen verschiedene „numerisch-anatomische Humanmodelle“ von Männern, Frauen und Jugendlichen, einer Schwangeren und eines Herzschrittmacherpatienten zur Verfügung, die anatomische Verhältnisse bis zu Details von zwei Millimeter Größe berücksichtigen. Damit ist es möglich, den elektrischen Stromfluss im und am Herzen quantitativ so zu untersuchen, dass die Gefährlichkeit der Taser-Impulse in Hinblick auf das Auslösen von Herzkammerflimmern genauer und umfassender bestimmt werden können, als dies durch Humanexperimente möglich wäre. Die Schwellen zum Auslösen von Herzkammerflimmern hängen wesentlich vom zeitlichen Verlauf der Reize ab. Belastbare Daten über die Flimmergefahr beziehen sich bisher allerdings vor allem auf die Ströme der Energieversorgung. Es ist daher erforderlich, auch die Reizwirkung verschiedener Taser-Pulsformen zu untersuchen. Auch dazu können numerische Modelle – von einzelnen Herzzellen – eingesetzt werden.

Ziel von RITA ist es, nachvollziehbare quantitative Grundlagen für die Risikoabschätzung der Taser-Anwendung zu erarbeiten. Aufbauend auf den bisherigen Ergebnissen soll in weiteren Untersuchungen auch untersucht werden, wie weit die Ergebnisse auch auf neue Taser-Modelle mit anderen Ausgangswerten übertragen werden können. Insbesondere sollen Taser-Modelle untersucht werden, bei denen mit einem Taser mehrere Elektrodenpaare auf dieselbe Person abgefeuert werden können. In diesem Fall könnten sich komplexe Durchströmungsmuster ergeben, die eine Abschätzung des Herzkammerflimmernrisikos wesentlich beeinflussen könnten. Die dafür notwendigen Untersuchungen sollen auch Mehrfachanwendungen wie wiederholte Auslösungen von Impulsen in Form von Impulszyklen umfassen.

Durch die unabhängige wissenschaftliche Untersuchung werden Wissenslücken und Unsicherheiten

Die Erkenntnisse von RITA erhöhen die Sicherheit im Einsatz von Tasern – sowohl für Bürger als auch für die Einsatzkräfte

in Bezug auf den Einsatz von Tasern beseitigt. Die gewonnenen Erkenntnisse ermöglichen die Erhöhung der Sicherheit im Einsatz sowohl für Bürger als auch für die Einsatzkräfte. Zusammengefasst dient das Projekt RITA zur

- fundierten und verantwortungsbewussten politischen Entscheidungsfindung;
- Minimierung von Risiken und Gefahren in Bezug auf Verletzungen und Todesfolgen;
- Optimierung in Bezug auf verhältnismäßige und möglichst schonende Vorgangsweise der Exekutivbeamten;
- Erhöhung der Sicherheit der Einsatzkräfte;
- fundierten und professionellen Erstellung von Einsatz- und Ausbildungsvorschriften;
- professionellen Durchführung der Aus- und Fortbildung;
- auf verbesserten und auf gesicherten Fakten basierender Kommunikation mit der Bevölkerung;
- Entkräftung unbegründeter Ängste und Besorgnis;
- Richtigstellung bestehender Mythen und Legendenbildungen;
- Erhöhung der gesellschaftlichen Akzeptanz.

Von den Ergebnissen von RITA wird auch abhängig gemacht werden, ob ein Taser-Modell als Dienstwaffe bei der heimischen Bundespolizei, der Justizwache oder dem Bundesheer eingeführt werden kann. Das Projekt dient somit dem integrativen Ansatz der Sicherheitsforschung und entspricht den thematischen Anforderungen der sicherheitspolitischen Schwerpunktsetzung. Das Aufgreifen von Befürchtungen der Bevölkerung und die umfassende und unabhängige wissenschaftliche Untersuchung ist zudem eine wichtige Voraussetzung für eine glaubwürdige Risikokommunikation und zur Erarbeitung risikominimierender Maßnahmen.

Die positiven Aspekte von RITA liegen schließlich in der Erarbeitung von Rahmenbedingungen zur sicheren Anwendung von Tasern und damit der Einschränkung von wesentlich risikoreicheren Schusswaffen. RITA trägt somit zur Vermeidung von schweren Unfällen mit ihren menschlichen und ökonomischen Folgewirkungen bei.

Projektleitung:

Technische Universität Graz, Institut für Health Care Engineering

Projektpartner:

– Bundesministerium für Inneres (BMI)
– Bundesministerium für Justiz (BMJ)
– Bundesministerium für Landesverteidigung und Sport (BMLVS)

Kontakt:

TU Graz, Institut für Health Care Engineering
Univ.-Prof. Dipl.-Ing. Dr. Norbert Leitgeb
8010 Graz, Kopernikusgasse 24
Tel.: +43/316/873-7397
Fax: +43/316/873-4412
E-Mail: norbert.leitgeb@tugraz.at

Sicherheitstypologie

Entwicklung einer österreichischen Sicherheitstypologie zur Analyse und Stabilisierung der Sicherheit in der Bevölkerung

Im Projekt „Sicherheitstypologie" wird die österreichische Bevölkerung ab 16 Jahren einer Typologisierung nach ihrem Sicherheitsgefühl unterzogen.

Sicherheitsempfinden entsteht im Wirkungsgefüge der persönlichen Lebenswelt, gesellschaftlicher Strukturen und des öffentlichen Diskurses. Um die Einflussfaktoren von subjektiver Sicherheit wissenschaftlich erklären zu können, müssen daher die Wechselwirkungen einzelner Dimensionen des Sicherheitsbegriffs identifiziert werden.

Das Projekt „Sicherheitstypologie" verfolgt daher einen multidimensionalen Ansatz. Das ist neu: Wechselwirkungen und Konstruktionsprozesse zwischen den einzelnen Komponenten eines umfassenden Sicherheitsbegriffs wurden bisher noch nicht in diesem Umfang analysiert. Zudem gibt es international noch keine Typologienbildung im Bereich der Sicherheit. Im Detail umfasst „Sicherheitstypologie" folgende Inhalte:

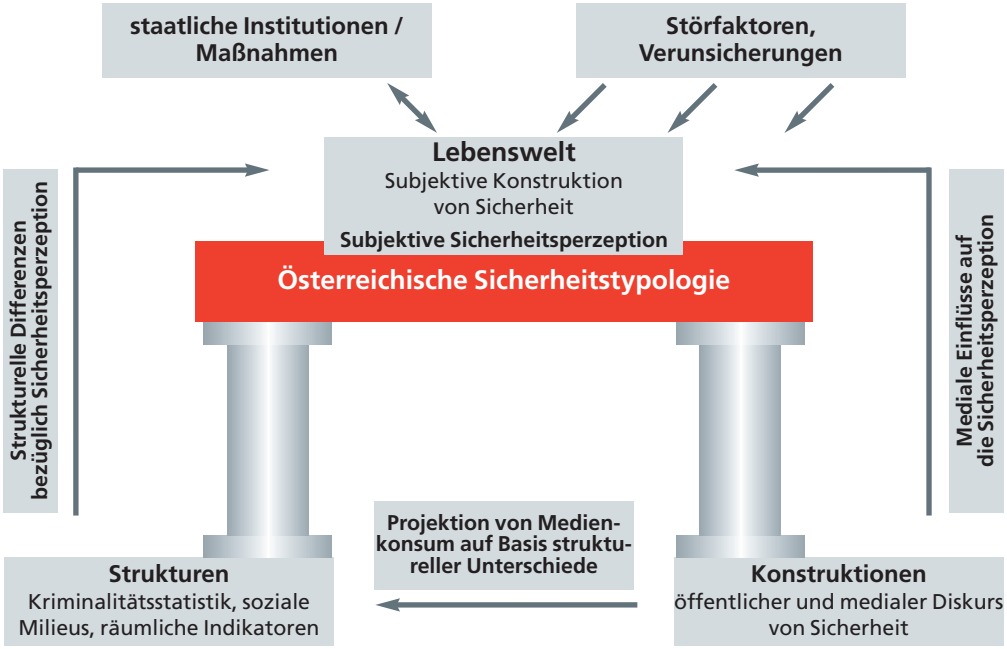
- Integration bisheriger Studienergebnisse.
- Analyse der Zusammenhänge zwischen den drei Kontexten Lebenswelt, Strukturen (objektiver sozialer Hintergrund) und Konstruktionen (Aufarbeitung des Themas Sicherheit in den Medien).
- Identifikation der Faktoren, die zur Entwicklung eines positiven Sicherheitsempfindens beitragen.
- Identifikation der Stabilisierungsfaktoren subjektiver Sicherheit für die Sicherheitstypen.
- Entwicklung eines Indikatorensets für die empirische Erhebung zur leichten Anwendung in anderen Studien.
- Nutzbarmachung der Ergebnisse für die KIRAS-Evaluierung bzw. GSK-Begleitforschung.
- Erstellung einer räumlichen Sicherheitstypologielandkarte.

Durch die erzielte Typologisierung, in der statt einem Aspekt („allgemeines subjektives Sicherheitsempfinden") viele Aspekte berücksichtigt werden, wird neues Wissen darüber generiert, welche Wirkungsmechanismen das Sicherheitsgefühl in Österreich beeinflussen. Dieses neue Verständnis stellt die Grundlage für die Entwicklung neuer Maßnahmen dar bzw. ermöglicht, diese Erkenntnisse in der Planung verschiedenster Vorhaben des öffentlichen und privaten Sektors zu berücksichtigen.

Die analysierten Beziehungen zwischen den einzelnen Kontexten werden auf eine österreichische Landkarte übertragen. Dies gelingt durch die Strukturfaktoren, die für die einzelnen Regionen vorliegen und die in der quantitativen Erhebung ebenfalls erfasst werden. Sie stellen die Basis für die Analyse von Unterschieden in der Sicherheitsperzeption dar. Von der strukturellen Zusammensetzung der Bevölkerung in einer Region wird auf die Ausprägung der sicherheitsrelevanten Faktoren geschlossen: Sicherheitsperzeption, Störfaktoren, Maßnahmenakzeptanz und Vertrauen in politische Institutionen.

Die Größe der räumlichen Einheiten ist dabei von den Bedürfnissen potenzieller Bedarfsträger sowie von der Verfügbarkeit struktureller Informationen abhängig. Dadurch ergeben sich geschätzt zirka 200 räumliche Einheiten, auf die die Ergebnisse projiziert werden. Für jede diese Einheiten sind spezifische Informationen abrufbar:

- Wie sicher fühlt sich die Bevölkerung?
- Welche Ängste, Unsicherheiten überwiegen?
- Welche Bedürfnisse zur Hebung des Sicherheitsgefühls bestehen?
- Welche Fragen stehen im Vordergrund? Zum Beispiel Information über Schwerpunktaktionen der Polizei, Produktberatung durch Sicherheitsfirmen, Fördermöglichkeiten für Sicherheitsmaßnahmen in der Wohnung/im Haus?
- Wie sieht die soziale Zusammensetzung aus? Kaufkraft, Migrationshintergrund, Einkommensverteilung etc.
- Welche Kommunikationsstile sind bevorzugt anzuwenden? Regionale Zeitungen, Print allgemein, In-



formationen durch kommunale Politik, Aktionen der Polizei etc. Die Landkarte wird in einer elektronischen Datenbank dargestellt, sodass durch Auswahl der Region einfach auf die Informationen zugegriffen werden kann.

Die Entwicklung einer Sicherheitstypologie in Österreich auf Basis eines breiten Sicherheitsbegriffs ist auch europaweit eine Innovation. Angesichts der Relevanz des Themas für die Nationalstaaten vermag die Studie durchaus, Impulse im europäischen Forschungsbereich auszulösen und als Musterbeispiel eines umfassenden Ansatzes zu dienen. Innerhalb Österreichs ist davon auszugehen, dass insbesondere der öffentliche Bereich – wie Länder, Städte und Kommunen – von den Erkenntnissen profitieren wird, da auf eine regionale Betrachtung der Sicherheitstypen großer Wert gelegt wird. Auf Basis der österreichischen Sicherheitstypologie lassen sich konkrete Maßnahmen im sozial- und wirtschaftspolitischen Umfeld entwickeln.

Neben einem umfassenden Bericht, der die Entwicklung und die Ergebnisse zur österreichischen Sicherheitstypologie dokumentiert, stellt ein kürzer gefasstes Kompendium die Sicherheitstypen und deren spezifische Charakteristika in anschaulicher Form und überblicksmäßig dar. Darüber hinaus enthält das Kompendium Indikatoren, die für die Rekonstruktion der Sicherheitstypen in anderen empirischen Studien notwendig sind, sowie eine Anleitung zur Berechnung der Typologie. Die österreichische Sicherheitstypologie basiert auf einer Vielzahl von Indikatoren, deren Erhebung langwierig ist. Mithilfe statistischer Analysen soll jedoch ein Set von Indikatoren entwickelt werden, anhand dessen ein Nachbauen der Typologie mit möglichst geringem Informationsverlust möglich ist. So wird es möglich sein, je Aspekt des Sicherheitsbegriffs einen und in gewissen Fällen zwei Indikatoren auszuwählen, die die übrigen möglichst gut repräsentieren bzw. mit den anderen stark zusammenhängen, sodass auf die konkrete Ausprägung (Information) der nicht erhobenen Indikatoren verzichtet werden kann. Darüber hinaus können charakterisierende Variablen (Soziodemografie und sozioökonomisches Potenzial), die in den meisten empirischen Studien erfasst werden, als Hilfsvariablen bei der Rekonstruktion der Sicherheitstypologie verwendet werden.

Projektleitung und Kontakt:

Institut für empirische Sozialforschung (IFES) GmbH
MMag. Dr. Reinhard Raml
1010 Wien, Teinfaltstraße 8
Tel.: +43/1/546 70-321
Fax: +43/1/546 70-312
E-Mail: reinhard.raml@ifes.at
Web: www.ifes.at

Silicon Malware

Studie zu Schadroutinen in Hardware-Komponenten

„Silicon Malware" beschäftigt sich mit den Gefahren, die mit schädlicher Funktionalität in Hardwarechips einhergehen, und erforscht geeignete Gegenmaßnahmen.

Die Verbreitung von Informationstechnologie in nahezu allen Lebensbereichen der industrialisierten Zivilisationen bietet ein breites Feld an Angriffsvektoren. Doch während bisher hauptsächlich softwarebasierte Angriffe in Betracht gezogen und untersucht wurden, haben hardwarebasierte Angriffe bisher vergleichsweise wenig Interesse geweckt. Wenn man sich aber vorstellt, dass Mikroprozessoren Schadcodes (Malware) enthalten, über die Unberechtigte auf sie zugreifen können oder die sie bei Bedarf sogar fernsteuern können, lässt sich ein düsteres Szenario für die Zukunft ausmalen.

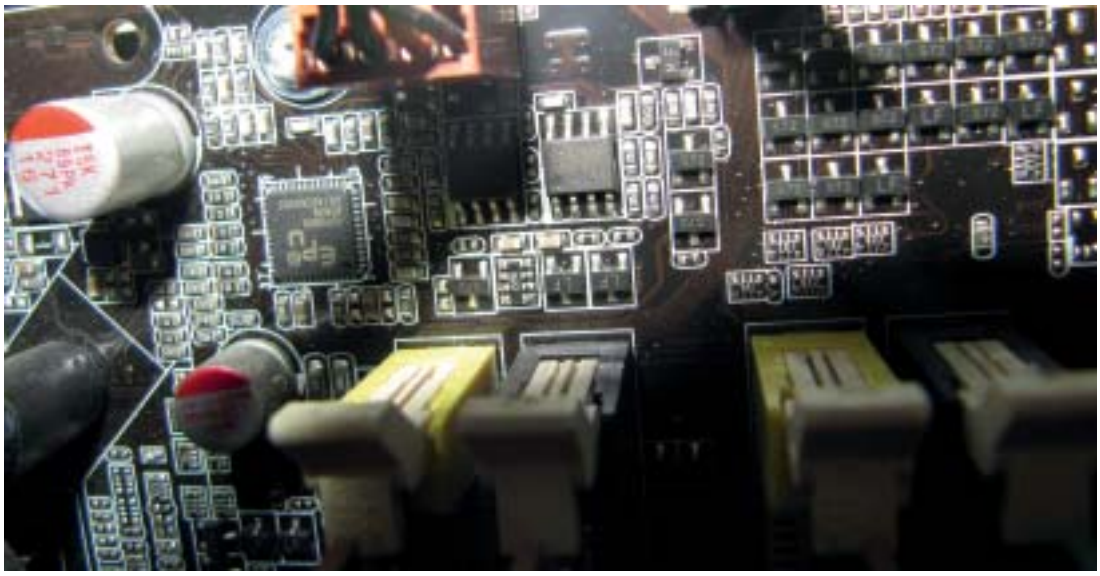
Ein Angriff auf Hardwareebene unterscheidet sich grundlegend von einem Angriff auf Softwareebene. Anders als Software ist Hardware ein materielles Gut, das nach seiner Fertigung nur noch bedingt verändert werden kann. Auch lässt sich Hardware nicht in so einfacher Weise vervielfältigen wie Software, mitunter ist hier sehr großer Sach- und Personalaufwand und in weiterer Folge finanzieller Aufwand vonnöten.

Das Projekt „Silicon Malware" widmet sich den Gefahren, die sich aus kompromittierter Hardware ergeben. Es werden systematisch die Schwachstellen erforscht, die sich aus dem Entwicklungs- und Produktionsprozess für die gefertigte Hardware ergeben. Weiters werden Strategien zur Verhinderung dieser besonderen Form von Angriffen erforscht werden. Bisherige Bemühungen, der Gefahr durch bösartige Hardware zu begegnen, beschränken sich auf akademische Modelle und Hypothesen. Da der Markt zurzeit auf wenige Bereiche beschränkt ist (militärische Anwendungen), sind bis dato keine massenfähigen, allgemein anwendbaren Lösungen entwickelt worden, um manipulierte Chips entdecken und verhindern zu können.

Der moderne Hardwareproduktions- und -entwicklungsprozess besteht aus zahlreichen Schritten und dazugehörigen Schnittstellen. Es ist leicht einzusehen, dass jeder dieser Prozessschritte sowie jeder Übergang zwischen den Prozessschritten verwundbar ist. So können bösegesinnte Entwickler schadhafte Funktionalität direkt als Code in der Hardwarebeschreibung einbringen. Weiters besteht die Möglichkeit, dass zugekaufte Funktionalität in Form sogenannter IP-Cores (IP – Intellectual Property) neben der gewünschten Funktionalität auch schadhafte, ungewünschte Funktionalität implementiert. Außerdem ist nicht auszuschließen, dass die Fehler bzw. zusätzliche Funktionalität von Softwaretools wie Synthetisierern oder Place-and-Route-Werkzeugen eingeschleust werden.

Während in der Entwurfs- und Entwicklungsphase eingeschleuste schadhafte Funktionalität durch Formalverifikation oder Simulation ausfindig gemacht werden kann, ist ein Erkennen nach der Fertigung ausschließlich durch Logiktests und Nebenkanalanalyse möglich:

- Formalverifikation. Formalverifikation ist eine Methode, um die Gleichwertigkeit zweier Repräsentationen eines Entwurfs zu überprüfen (Beispiel Hardwarebeschreibung und Netzliste).
- Simulation. Durch Simulation kann durch Annehmen von Zuständen und Eingangsbedingungen und anschließendem Beobachten der Zustände und Ausgänge das Verhalten eines Systems überprüft werden.
- Logiktests. Bei Logiktests werden an Chipeingängen Testmuster angelegt, an den Ausgängen werden die tatsächlichen Ergebnisse mit den erwarteten Ergebnissen verglichen. Das Problem dabei ist eine nahezu unendliche Anzahl von Testmustern.
- Nebenkanalanalysen. Nebenkanalanalysen untersuchen die nicht vordergründig zum Informationsaustausch vorgesehenen physikalischen Größen eines Chips wie beispielsweise Energieversorgung, Temperatur und elektromagnetische Abstrahlung. Durch Vergleich mit Referenzchips können manipulierte Chips aufgefunden werden.



Auch die Hardware eines Computers kann Opfer eines Hacker-Angriffes sein

Die meisten bislang bekannten hardwarebezogenen Angriffsvektoren beschäftigen sich mit der Frage, wie geistiges Eigentum derart geschützt werden kann, dass integrierte Schaltungen durch Konkurrenten nicht nachgebaut werden können. Hierbei handelt es sich jedoch stets um Angriffe von außen unter Ausnutzung von Schwächen in Übertragungsprotokollen bzw. Testvorrichtungen. Ein weitaus interessanterer Angriffsvektor ist der sogenannte Hardwaretrojaner bei dem zusätzliche, nicht-spezifizierte Funktionalität in Hardware eingefügt wird. Da Hardware materielles Gut ist, muss dies während des Entwicklungs- und Produktionsprozesses stattfinden. Ein Angriff sollte so unerkannt wie möglich bleiben. Da mit dem Produktionsprozess intensive Testphasen einhergehen, muss ein Hardwaretrojaner Mittel und Wege ergreifen, die ein Entdecken während dieser Phasen verhindern. Dies wird bewerkstelligt, indem die eigentliche Funktionalität – die Nutzlast – durch ein seltenes Ereignis – einen Auslöser – aktiviert wird.

- Auslöser: Auslöser haben die Aufgabe, die Nutzlast eines Hardwaretrojaners zu aktivieren. Dies geschieht auf Basis seltener Ereignisse, wie z. B. das Verstreichen von 10.000 Sekunden, das Anlegen ganz bestimmter Bitmuster oder das Erreichen eines bestimmten Spannungswertes innerhalb einer elektronischen Schaltung. Weiters ist eine Aktivierung von extern über ein Funksignal denkbar.
- Nutzlast. Nach Aktivierung kann die eigentliche Funktionalität eines Trojaners in Erscheinung treten. Denkbar ist hier das Abhören von Passwörtern oder das vollständige Ausschalten bzw. Zerstören des Geräts.

Um Hardwaretrojaner zu kategorisieren, gibt es mehrere Möglichkeiten, beispielsweise nach ihren physikalischen, topologischen Eigenschaften oder auch nach deren Auswirkungen. Anhand der Art der Implementierung können analoge Trojaner von digitalen unterschieden werden, wobei Auslöser und Nutzlast auch unterschiedlicher Natur sein können. Digitale Trojaner können wieder in kombinatorische und sequenzielle unterteilt werden.

Zusammengefasst zeigt sich, dass Hardware in vielfältiger Weise manipuliert werden kann. Das Projekt Silicon Malware schafft eine Expertise auf dem Gebiet, um anschließend eigene Ansätze zur Problemlösung beizutragen. Der Nutzen liegt klar auf der Hand: Erlangen von Spezialwissen über ein Fachgebiet, das von globaler Relevanz und hoher Aktualität ist, sowie die Chance, Österreich auf diesem Gebiet zu einem gewichtigen Proponenten zu machen.

Projektleitung/Kontakt:

SBA Research
Christian Krieg, PD Dr. Edgar Weippl
1040 Wien, Favoritenstraße 16
E-Mail: eweippl@sba-research.org
E-Mail: ckrieg@sba-research.org

Der Szenekundige Dienst

Ausbildung und Professionalisierung von Szenekundigen Beamten im internationalen Vergleich (European Best Practice Manual)

Fußball gehört zu den populärsten Sportarten weltweit und hat daher auch in sicherheitspolitischer Hinsicht eine hohe Bedeutung. Dabei stehen sowohl die Vertreter der einzelnen Bundesligavereine, die Bundesliga selbst als auch insbesondere die staatlichen Sicherheitsbehörden auf der Exekutivebene vor der Herausforderung, bestmögliche Sicherheitsstandards für Besucher und Spieler bei den einzelnen Spielpartien zu gewährleisten. Ein Hauptaugenmerk liegt insoweit auf strategischen Sicherheitsmaßnahmen in und rund um die Fußballstadien, wenn es durch das Verhalten von konflikt- und gewaltbereiten Fangruppierungen zu gewalttätigen Auseinandersetzungen kommt.

Um sicherheitspolitischen Überlegungen Rechnung zu tragen, wurde durch die Antragstellerin 2009 erstmals eine empirische Untersuchung der österreichischen Bundesliga für die Saison 2007/2008 durchgeführt. Es handelt sich um eine explorative Studie, die sich im Besonderen auf den Istzustand sicherheitsrelevanter Faktoren und strategischer Maßnahmen zur Eindämmung von Zuschauergewalt konzentriert. Denn bisher liegen auch im internationalen Vergleich nur wenige bis gar keine empirisch begründeten Erkenntnisse zu den gängigen Reaktionsmöglichkeiten oder über die Entwicklung effektiver Kontrollstrategien vor.

Das Sicherheitspolizeigesetz (SPG) stellt die rechtliche Grundlage für die Sicherheitsbehörden und deren Organe, also die Polizei, dar. Außerdem regelt das SPG die Organisation und Aufgaben der Sicherheitsbehörden und des Wachkörpers. Bei Spielen mit internationalem Bezug und den Fußballbegegnungen der beiden höchsten Spielklassen werden regelmäßig zusätzlich zur uniformierten Polizei sogenannte Szenekundige Beamte (SKB) eingesetzt, um Risikoanalysen als Grundlage für jeweilige Lagebilder erstellen und alle präventiven Maßnahmen setzen zu können, die gefährliche Angriffe bereits im Vorfeld vermeiden. Für jeden Sportverein, bei dem es aufgrund der Größe und des Gefährdungspotenzials der Fangruppen notwendig erscheint, ist unter Einbindung der Landespolizeikommanden ein SKB als Koordinator und allenfalls ein Stellvertreter einzusetzen. Die SKB bewegen sich im Bereich der Fanszenen und treten im offenen Dialog zu den Fans als nicht uniformierte Fanpolizisten vor, während und nach Sportgroßveranstaltungen auf. Sie sind als permanente Ansprechpartner – immer nur eines Vereins – mindestens zu zweit im Einsatz. Bezüglich der Auswahl und der Ausbildung der SKB berichteten Experten der Polizei noch bei einer Befragung im Rahmen der Studie Fußball und Sicherheit (Winter/Klob 2009), dass die Rekrutierung auf freiwilliger Meldung interessierter Kollegen zum Szenekundigen Dienst basiere. Zur Selektion würden zwar keine psychologischen Auswahlverfahren angewendet werden, die Fachvorgesetzten und Leiter der SKB würden aber sehr wohl auf eine persönliche Eignung achten.

Basierend auf der Einrichtung hauptamtlicher Szenekundiger Beamter bei Sportgroßveranstaltungen im Rahmen des neuen SKB-Erlasses (GZ.: BMI-EE1910/0012-ZSA/2009) soll nunmehr auch eine Ausbildung der SKB in der Zukunft angedacht werden. Entsprechende Ausbildungs- bzw. einheitliche Schulungsrichtlinien mit professionellen Aufbaumodulen bestehen jedoch bisher noch nicht in Österreich. Im Rahmen der Projektstudie „Der Szenekundige Dienst – Ausbildung und Professionalisierung von Szenekundigen Beamten im internationalen Vergleich (European Best Practice Manual)“ werden daher sowohl nationale wie auch einschlägige Erfahrungen aus dem europäischen Raum in die Studie einbezogen, um bei einer Bestandsaufnahme alle etwaigen Maßnahmen, Ausbildungsmodule und Modelle vergleichend zu verifizieren. Unter der Prämisse „What works, what doesn’t work“ soll diese Bestandsaufnahme (Best-Practice-Analyse) im direkten Zusammenhang zur österreichischen Sicherheits-

Szenekundige Mitarbeiter sollen Ausschreitungen und sonstige Sicherheitsrisiken im Fußball verhindern

lage aktiv die Entwicklung und Ausarbeitung landesweiter, einheitlicher Ausbildungsrichtlinien implementieren und eine ausgewiesene Professionalisierung des Berufsbildes gewährleisten.

Ziel der Forschungsstudie ist es, zukünftig im Sinne einer umfassenden nationalen Sicherheitspolitik sicherheitsrelevante Vorfälle bei Sportveranstaltungen durch ein optimiertes Einsatzmanagement der österreichischen Polizei bestmöglich zu verhindern. Zu diesem Zweck werden die folgenden Punkte im Rahmen des Projektes wissenschaftlich erhoben:

- Die Erhebung des nationalen Ausbildungsbedarfs der Polizei (SKB).
- Die Erhebung internationaler Ausbildungsstandards der Polizei (SKB) im Vergleich.
- Die Entwicklung entsprechender – bisher nicht bestehender – Ausbildungsprogramme und berufsbildfördernder Maßnahmen für SKB.
- Die Entwicklung qualitativ hochwertiger Ausbildungsstandards und fachlich fundierter Richtlinien für Schulungen der SKB.
- Die Entwicklung eines European Best Practice Manuals.

Eine Forschungsstudie dieser Art ist bisher weder national noch international durchgeführt worden. Die wissenschaftlichen Ergebnisse, die vorrangig für die Sicherheitsentwicklung und die polizeiliche Einsatzstrategie Österreichs von immenser Relevanz sind, könnten aber in Anbetracht der Europäischen Sicherheitslage bei Sportgroßveranstaltungen auch international von organisatorischer Bedeutung sein

Das SKB-Umfeld

und versprechen auf politischer Ebene ein großes Umsetzungspotenzial. Die Antizipation der Weiterentwicklung gilt vor allem, wenn aufgrund der empirischen Untersuchungen einheitliche Richtlinien und Module in der Ausbildung definiert und umgesetzt werden können. Des Weiteren eröffnen die Ergebnisse Einsparungspotenziale durch Regulierung der uniformierten Einsatzkräfte bei verstärktem Einsatz von ausgebildeten SKB (Personal- und Sachressourcen) und bilden die Grundlage zur Optimierung von Einsatzstrategien und Prozessabläufen in Kooperation mit privaten Sicherheitsdiensten sowie zur Optimierung von internationalen Kooperationen und Wissens- und Erfahrungsaustausch.

Projektleitung:

Universität Wien

Projektpartner:

– Bundesministerium für Inneres (BMI)

Kontakt:

Universität Wien, Institut für Strafrecht und Kriminologie
Univ.-Ass. Dr. iur. Ireen Christine Winter
1010 Wien, Schenkenstraße 8–10
Tel.: +43/1/4277-34623
Fax: +43/1/4277-9346
E-Mail: ireen.winter@univie.ac.at
Web: www.univie.ac.at/kriminologie

AQUASEC-AUT

Kriseninterventionslabor für die österreichische Wasserversorgung

Die Erfahrung zeigt, dass bei Unfällen mit in der Wasseranalytik weniger gängigen Substanzen (beispielsweise Beimischungen in Pestiziden und Düngemitteln), das schnelle Auffinden eines kompetenten analytischen Partners und der toxikologischen Expertise oftmals sehr schwer ist.

Das Projekt „AQUASEC-AUT: Kriseninterventionslabor für die österreichische Wasserversorgung" verfolgt daher zwei Hauptziele:

- Im Rahmen des Projektes wird ein virtuelles, nationales Kriseninterventionslabor konzipiert werden. Ein solches Labornetzwerk soll jederzeit und rasch unbekannte chemische und mikrobiologische Substanzen, die durch unvorhergesehene Ereignisse, Unfälle oder aber durch erpresserische/terroristische Handlungen in die Wasserversorgung gelangen, identifizieren können.

- Zum anderen will AQUASEC-AUT einen Überblick schaffen, wie die Zusammenarbeit der beteiligten Akteure im Krisenfall funktioniert und welche zusätzlichen Bedürfnisse diese zur Bewältigung der Krise haben.

Dazu findet eine Erhebung der Erfahrungen und Anforderungen aller relevanten Akteure im Krisenfall statt. Aus dem geschärften Bild der Kommunikationspfade, Entscheidungshierarchien und Abhängigkeiten lassen sich relevante Schlüsselpositionen ermitteln. Deren konkreter Bedarf an bestimmten Informationen, Unterstützung und Leistungen bilden die Basis für das zu konzipierende Netzwerk.

Auf analytischer Seite wird der Bedarf eines Kriseninterventionslabors charakterisiert, durch die Art der benötigten Leistung, die Mindestansprüche an die Datenabsicherung sowie das Zeitfenster. Weiters widmet sich das Projekt der Frage, welche Informationen und Expertisen (toxikologisch, medizinisch u. a.) in ungeregelten Sonderfällen abseits der Analytik benötigt werden, um sichere Entscheidungen zu ermöglichen.

Sind diese Basispunkte des Bedarfs definiert, wird aufgrund der in Österreich bestehenden analytischen Ressourcen das Konzept des virtuellen, nationalen Kriseninterventionslabors erstellt. Dazu werden im Vorfeld die grundsätzlich vorhandenen Laborressourcen erhoben. Dabei liegt der Fokus nicht auf dem Medium Wasser, sondern auf der Schadstoffkompetenz der einzelnen Labors. Für diese werden die angebotenen Leistungen, die Verfügbarkeit und die Reaktionszeit ermittelt.

Durch die Gegenüberstellung des zu deckenden Bedarfs und des analytischen Angebots kann schließlich der Grad der Bedarfsdeckung bestimmt und etwaige Defizite aufgedeckt werden.

Angestrebt wird eine detaillierte Darstellung eines umsetzbaren Laborkonzeptes und sonstiger eventuell notwendiger Expertisen.

Weiters sollen Kommunikationswege, Entscheidungshierarchien und Informationsflüsse in verschiedenen Krisensituationen dargestellt werden.

Projektleitung:

Umweltbundesamt GmbH

Projektpartner:

– Österreichische Agentur für Gesundheit und Ernährungssicherheit (AGES)
– Bundesministerium für Landesverteidigung und Sport, Zentraler Technischer Dienst
– Bundesministerium für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft, Sektion VII

Kontakt:

Umweltbundesamt GmbH
DI Verena Stingl
1090 Wien, Spittelauer Lände 5
Tel: +43/1/313 04-5127
E-Mail: verena.stingl@umweltbundesamt.at
Web: www.umweltbundesamt.at

Standsicherheit der Ortsbrust im Tunnelbau

Grundlagen für Teilsicherheitsbeiwerte für Boden und Stützmittel sowie Bewertung der Stützmaßnahmen

Eine wichtige Aufgabe beim Tunnelbau ist die Bestimmung des erforderlichen Stützdruckes der sogenannten Ortsbrust. Dabei handelt es sich um die Stelle, an der der bergmännische Vortrieb stattfindet. Experimentelle Untersuchungen zur Ortsbruststabilität in geotechnischen Zentrifugen blieben bisher fast ausschließlich auf Modelle beschränkt, die die Flexibilität der Tunnelschale vernachlässigen. Außerdem wurde bisher vorwiegend die Stabilität von vollflächiger Ortsbrust (wie im maschinellen Tunnelbau üblich) untersucht.

Beim zyklischen Tunnelvortrieb („Neue Österreichische Tunnelbauweise") wird die Stabilität der Ortsbrust auch vom Erhärtungszustand der Spritzbetonschale im Bereich der Ortsbrust beeinflusst. Das Projekt „Standsicherheit der Ortsbrust im Tunnelbau" schafft Grundlagen für Teilsicherheitsbeiwerte für Boden und Stützmittel und zur Bewertung von Stützmaßnahmen. Dazu wurde – mit Unterstützung der Österreichischen Gesellschaft für Geomechanik – ein Versuchsprogramm ausgearbeitet, bei dem der Einfluss der Steifigkeit der Schale auf die Stabilität untersucht werden kann.

Die Versuche wurden an der 400-Gramm-Tonnen-Zentrifuge der University of Colorado in Boulder, USA, durchgeführt. Das dabei eingesetzte Modell besteht aus einem Aluminium-Acryl-Behälter, der mit feinem Quarzsand gefüllt wurde. Durch die transparente Vorderseite kann der Versuchsablauf mit Hilfe einer Digitalkamera beobachtet werden. Die halbzylindrische Tunnelschale besteht ebenfalls aus Acryl und ist so gelagert, dass sie sich wie eine echte Tunnelschale im Boden verschieben und deformieren kann. Eine Abschlussfläche (bzw. zwei im Fall eines unterteilten Vortriebes) simuliert die Ortsbruststützung und wird nach Erreichen der gewünschten Geschwindigkeit der Zentrifuge verschiebungsgesteuert vom Boden wegbewegt, bis sich im Boden Verformungen ausbilden.

Die Verschiebungen und Verzerrungen der Tunnelschale und des Bodens wurden messtechnisch aufgezeichnet, ebenso wie die Kraft, die der Boden auf die Abschlussfläche(n) ausübt. Vier Varianten wurden dabei simuliert:

- Tunnelschale bis zur vollflächigen Ortsbrust in voller Stärke;
- Tunnelschale endet 0,25 Durchmesser hinter der vollflächigen Ortsbrust;
- Tunnelschale bis zur in Kalotte und Strosse unterteilten Ortsbrust in voller Stärke sowie
- Tunnelschale endet 0,25 Durchmesser hinter der unterteilten Ortsbrust.

Für jede Variante wurde der Versuch mit zwei unterschiedlichen Höhen der Bodenüberlagerung gefahren und zweimal wiederholt, um Aussagen über die Streuung der Ergebnisse zu erhalten. Die Versuchsergebnisse zeigen deutlich die Auswirkungen der Varianten auf die Belastungen der Tunnelschale und die Ausbildung der Versagensflächen im Boden.

Die Ergebnisse des Projektes „Standsicherheit der Ortsbrust im Tunnelbau" dienen als Grundlage zur Ermittlung von Teilsicherheitsbeiwerten für Boden und Stützmittel. Die im Versuch erzielten Resultate sind ein wichtiger Schritt auf dem Weg zu wissenschaftlich begründeten Werten für Boden und Stützmittel.

Projektleitung und Kontakt:

Herbert Walter
5020 Salzburg, Dr.-A.-Altmann-Straße 24
Tel.: +43/662/82 06 44
E-Mail: enzi-walter@aon.at
Web: www.zthw.at

Projektpartner:

University of Colorado, CEAE-Department, Boulder, CO 80309, USA

SIDE

Sicherheitsrisiko Deponiegas: Abschätzung des Gefährdungspotenzials und Analyse von Abwehrmaßnahmen

Das Projekt „SIDE" stellt das Gefährdungspotenzial von Deponiegas für Österreich dar und bewertet geeignete Abwehrmaßnahmen.

Werden organische Abfälle in Deponien abgelagert, entsteht beim mikrobiellen Abbau im anaeroben Milieu ein Gasgemisch, das im Wesentlichen aus Kohlendioxid CO_2 und Methan CH_4 besteht. Neben der hohen Treibhauswirksamkeit, verursacht Methan ein direktes Sicherheitsrisiko für Mensch und Umwelt. Die direkte Gefährdung von Menschen durch Deponiegas besteht aber hauptsächlich in der Erstickungsgefahr. Außerdem ist auch kritische Infrastruktur wie Autobahnen, Eisenbahnlinien oder Stromleitungen durch die mögliche Explosion von Deponiegas gefährdet.

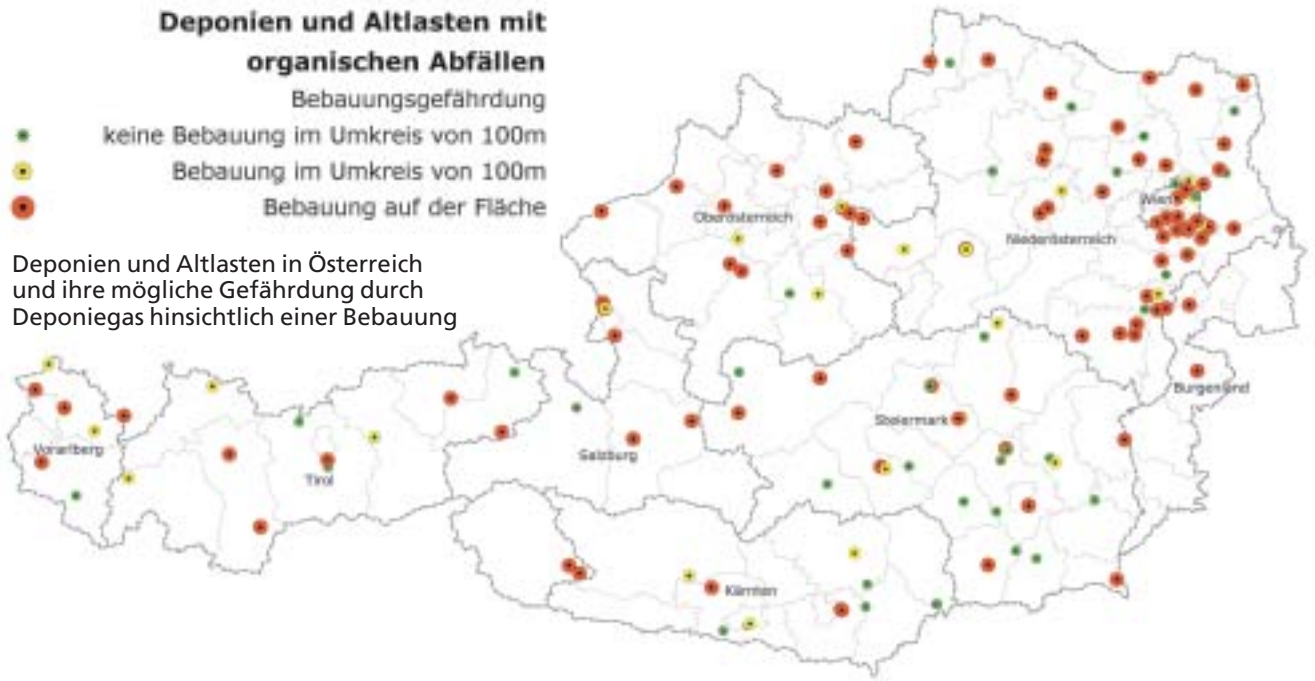
Bisher existieren in Österreich weder eine flächendeckende Erfassung aller Altablagerungen, von denen eine Gefährdung durch Deponiegas ausgehen kann, noch eine Handlungsempfehlung für den Umgang mit dem Sicherheitsrisiko. Ziel des Projektes „SIDE – Sicherheitsrisiko Deponiegas: Abschätzung des Gefährdungspotenzials und Analyse von Abwehrmaßnahmen" ist daher eine Abschätzung des Gefährdungspotenzials und die Analyse von Abwehrmaßnahmen. Diese Ziele sollen ihre konkrete Umsetzung in Form von Gefährdungskarten und eines Maßnahmenkataloges finden.

Zunächst wurde in einem ersten Erhebungsschritt das Gefährdungspotenzial für Österreich erhoben. Dazu wurden alle Deponien und Altlasten mit organischem Inhalt >25.000 Kubikmeter ermittelt und eruiert, ob und welche Bebauung bzw. kritische Infrastruktur sich auf oder im Umkreis der Flächen befindet und diese Ergebnisse anhand von Gefährdungskarten visualisiert. Im einem nächsten, vertieften Erhebungsschritt wurden für das Bundesland Salzburg neben den Deponien und Altlasten auch alle Verdachtsflächen und registrierten Altablagerungen mit organischem Inhalt erhoben und wiederum ermittelt, ob und welche Bebauung bzw. kritische Infrastruktur sich auf oder im Umkreis der Flächen befindet und die Ergebnisse wiederum anhand von Gefährdungskarten visualisiert.

Die Abschätzung des gesamten Gefährdungspotenzials für Österreich ergibt folgendes Bild:

- Von 7.400 Ablagerungen in Österreich muss bei der Hälfte (3.700) mit der Bildung von Deponiegas gerechnet werden.
- Bei 2.850 deponiegasbildenden Ablagerungen muss von einer Bebauung im näheren Umkreis und bei 1.600 sogar von einer Bebauung auf der Fläche ausgegangen werden.
- Bei 2.150 deponiegasbildenden Ablagerungen muss von Infrastruktureinrichtungen im näheren Umkreis und bei 500 von Infrastruktureinrichtungen direkt auf der Fläche ausgegangen werden.

Bei den Überlegungen zur Vermeidung des Gefährdungspotenzials durch Deponiegas ist unbestritten, dass es langfristig der beste Weg wäre, die Ablagerung organikhaltiger Abfälle zu vermeiden. Dies wird auch durch die Gesetzgebung seit rund 20 Jahren stark forciert. Es hat sich jedoch gezeigt, dass der Restmüll trotzdem noch reich an biologisch abbaubaren Substanzen ist. Daher wurde in Umsetzung der EU-Deponierichtlinie (1999/31/EG des Rates vom 26. April 1999) in der österreichischen Deponieverordnung 2004 (Deponieverordnung 1996 idF 2004) die Verpflichtung zur Vorbehandlung von Restmüll vorgesehen, mit dem Ziel, Gehalt und Reaktivität der Organik von abzulagernden Abfällen zu minimieren. Diese Maßnahmen sind sicher langfristig die besten, wirksamsten und auch vermutlich die billigsten Lösungen, das Gefährdungspotenzial durch Deponiegas zu minimieren.



Deponien und Altlasten in Österreich und ihre mögliche Gefährdung durch Deponiegas hinsichtlich einer Bebauung

Ist die Ablagerung der Deponiegas-produzierenden Abfälle nicht mehr zu verhindern, weil es sich um alte Ablagerungen handelt oder weil ja auch bei neueren Deponien noch eine gewisse Menge an Deponiegas entsteht, dann gilt es langfristig durch übergeordnete Maßnahmen der Raumplanung und auch der Politik eine Bebauung in einem relevanten Umkreis zu verhindern.

Ist es weder möglich das Deponiegas und den Ort der Gefährdung grundsätzlich zu verhindern, bieten sich Abwehrmaßnahmen an, die an unterschiedlichen Punkten im Gefahrensystem ansetzen können:

- Zum einen kann direkt im Deponiekörper die Entstehung von Deponiegas verhindert oder stark reduziert werden, z. B durch eine In-Situ-Belüftung der Deponie. Dabei handelt es sich jedoch um aufwendige, zeit- und kostenintensive Maßnahmen.
- Weiters besteht die Möglichkeit, den unkontrollierten Austritt des Gases aus dem Deponiekörper durch Entgasungsmaßnahmen zu verhindern oder stark zu reduzieren. Diese Maßnahmen sind in der Regel weniger aufwendig, jedoch länger zu betreiben, da nur das entstehende Gas kontrolliert wird.
- Darüber hinaus kann eine unkontrollierte Migration des Gases an die Stelle der Gefährdung unterbunden werden, z. B durch eine Umschließung der Deponie. Diese Maßnahme stellt zwar eine mittelfristig wirksame Lösung zur Reduktion des Gefährdungspotenzials dar, jedoch wird an der Gefahrenquelle nicht eingegriffen.
- Durch eine entsprechende Bauausführung der Gebäude kann ein möglicher Eintritt des Gases in die Gebäude verhindert werden. Bei neu zu errichtenden Bauwerken stellt diese Vorgehensweise eine gute und relativ einfache Möglichkeit dar. Bei älteren, bestehenden Gebäuden, Schächten, sind nachträglich Abdichtungsmaßnahmen schon deutlich aufwendiger.
- Direkt in den Gebäuden kann durch betriebliche Maßnahmen die Sicherheit stark erhöht, nicht aber die grundsätzliche Gefährdung beseitigt werden.

Darüber hinaus sind langfristige, übergeordnete Maßnahmen anzudenken, wie der Eintrag der Ablagerungen in das Grundbuch mit einem möglichen Bebauungsverbot, damit mögliche Gefahren auch noch Jahrzehnte nach der Ablagerung erkannt werden können.

Projektleitung und Kontakt:

blp GeoServices gmbh
Dipl.-Ing. Dr. Roman Prantl
1070 Wien, Schottenfeldgasse 63/2
Tel.: +43/732/99 70 04-14
Fax: +43/732/99 70 04-19
E-Mail: r.prantl@blpgeo.at
Web: www.blpgeo.at


UDS9

Ultraleichte Drohnenstruktur optimiert auf Einsatzdauer mittels Highend-Composite-Engineering-Technologie

Weltweit sind mehr als 2.000 Projekte in Arbeit, die sich mit der Weiterentwicklung und Verbesserung von Drohnen (UAV) auseinandersetzen. Von diesen hebt sich das Projekt UDS9 durch sein interdisziplinäres Herangehen an die Entwicklung einer ultraleichten Composite-Struktur mit modernsten Simulationsmethoden ab. Entsprechend den Anforderungen an Leichtbau, Mobilität und Herstellbarkeit wurde ein Grundkonzept für die Drohnenstruktur erarbeitet. Diese wurde in der Gesamtstruktur integriert und hinsichtlich der Konzeptprüfung in einem ersten Funktionsprototypen umgesetzt.

Die Grundstruktur des UAV lässt sich mit dieser Konstruktion in einem Rohr mit rund dia 180x500 Millimeter Länge zum Transport und zur Lagerung unterbringen. Das skalierbare Konzept ist aktuell auf ein Höchstabfluggewicht (MTOW) von 1,5 Kilogramm bei einem Eigengewicht von einem Kilogramm ausgelegt. Die auf Flexibilität und Erweiterbarkeit konzipierte Elektronik bietet mit ihrer hochsensiblen Sensorik eine solide Basis jeglicher Applikationsintegration für ein breites Anwendungsspektrum. Die Flexibilität des Konzeptes wurde weiters durch den, in wenigen Sekunden möglichen Nutzlastwechsel umgesetzt. Ein Landegestell, das den Erfordernissen der Mobilität und dem Leichtbau entsprechen sollte, wurde konstruiert, berechnet und gebaut. Das Gesamtgewicht von rund zehn Gramm und die für das mit dem UAV kompatiblen Transportmaß erreichten Abmessungen waren sehr positiv.

Der Einsatz modernster Simulationsmethoden und Entwicklungswerkzeuge, ermöglichte in diesem Sinne mit dem interdisziplinären Herangehen an die Anforderungen, mit relativ geringem Aufwand die weitestgehende Umsetzung des angestrebten Konzeptes beziehungsweise der gesetzten Projektziele. Noch nicht erreicht wurde die angestrebte Flugdauer mit Nutzlast von 25 Minuten, derzeit beträgt diese zirka 13 Minuten.

Bezüglich der Flugzeit zeigte das Projekt auf, dass in weiterer Folge an dem Antriebsstrang intensiv entwickelt werden muss, um das UAV auf dem Markt entsprechend weit vorne positionieren zu können. Parallel zum Projekt entstand ein Patent für den Verriegelungsmechanismus der Nutzlast, welches auch schon für die EU angemeldet wurde. Dieses stellt am wachsenden UAV-Markt künftig eine strategische Alleinstellung von SG concepts sicher. Bei einschlägigen Messen und Fachevents wurde jedenfalls ein reges internationales Interesse an dem von UDS9 verfolgten Ansatz festgestellt. Sogar konkrete Anfragen auf Liefertermine (!) für das UAV gingen bereits ein.

Auch das KIRAS-Projekt SkyObserver zeigt, wie wichtig die bei UDS9 erworbenen Erfahrungen sind. Bei SkyObserver ist SG concepts ein Projektpartner und für die Entwicklung und Prototyplieferung einer „kardanischen Aufhängung" (Gimbal) zur Aufnahme eines Kamerasystems verantwortlich, welches auch künftig bei dem in UDS9 entwickelten UAV in ähnlicher Form eingesetzt werden kann.

Geplant ist, 2011 die Serienreife für den Vertriebsstart des UAV zu erreichen. Zielgruppen für den Einsatz der Drohne sind Blaulichtorganisationen sowie Sachverständige, welche ein Werkzeug zur Begutachtung aus der Luft von schwer zugänglichen Einsatzorten suchen. Parallel erfolgt der erste Schritt zur kommerziellen Nutzung durch ein erweitertes Dienstleistungsangebot von SG concepts mit UAV-Einsätzen auf Abruf.

Projektleitung und Kontakt:

SG concepts gmbh
Gregor Schnoell
4432 Ernsthofen, Neubauring 29
Tel.: +43/664/141 85 64
E-Mail: gregor.schnoell@sgconcepts.at
Web: www.sgconcepts.at

Kontakt

Programmverantwortung

Bundesministerium für Verkehr, Innovation und Technologie (bmvit)
Sektion III – Innovation und Telekommunikation
Stabsstelle für Technologietransfer und Sicherheitsforschung
Renngasse 5, 1010 Wien
Web: www.bmvit.gv.at/

Kontaktpersonen :

Dr. Ralph Hammer
Tel.: +43/1/711 62-65 2109
E-Mail: ralph.hammer@bmvit.gv.at

Dipl.-Ing. Michael Brugger
Tel.: +43/1/711 62-65 3126
E-Mail: michael.brugger@bmvit.gv.at

Programm- und Schirmmanagement

Österreichische Forschungsförderungsgesellschaft mbH (FFG)
Sensengasse 1, 1090 Wien
Web: www.ffg.at

Kontaktpersonen :

DIpl.-Ing. Johannes Scheer
Tel: +43/5/7755-5070
E-Mail: johannes.scheer@ffg.at

Christian Brüggemann
Tel.+43/5/7755-5071
E-Mail: christian.brueggemann@ffg.at

Abbildungen:

Auf den linken Seiten: Touchscreen©reinobjektiv, fotolia; iris scan ©Patrizia Tilly, fotolia
Seite 1 © Mark Aplet, shutterstock; Seite 84 Photosani, shutterstock

Seite:	Abbildung:
9	Frequentis AG, JOANNEUM RESEARCH
11	AIT-2011
13	AeroSpy
15	TU Graz, IAIK
17	AIT
19	E-SEC GmbH
20/21	FH Hagenberg
25	Innsbrucker Kommunalbetriebe AG, Gemeinde Göfis
27	JOANNEUM RESEARCH
29	Center Communication Systems
31	AIT, Safety & Security Department
33	TU-Wien
35	Dr. Mittermayr Scientific Consulting GmbH, ÖBB-Infrastruktur AG
37	RK Salzburg, RK OOE
41	AUSTRIAN POWER GRID, Foto C. Schiller – www.fotolia.de
45	Seibersdorf Labor GmbH
47	SFI@SFU
49	Forschungsinstitut des Roten Kreuzes
51	Tommy Windecker – Fotolia.com
53	SBA Research
55	Friedensbüro
57	Jason Stitt/Pixmac
59	Siegfried Vössner
61	Quelle: BMI, Statistik Austria, IHS Berechnungen und Illustration
63	M.Schweiger/ORESP
65	TU Wien, Institut für Softwaretechnik und Interaktive Systeme
67	FAS.research, 2009
69	Schaub-Walzer/ PID
73	SBA Research
75	Ireen Christine Winter, Bernhard Jäger
79	blp GeoServices gmbh