

Wissenschaft(f)t Sicherheit

Geförderte KIRAS-Projekte
2007 – 2009

Impressum: MEDIENINHABER UND VERLEGER: Bohmann Druck und Verlag GesmbH & Co.KG. > A-1110 Wien, Leberstraße 122
> Telefon: +43-1/740 95-0 > DVR: 0408689 > GESCHÄFTSFÜHRUNG: Dr. Gabriele Ambros – Gerhard Milletich > Herausgeber:
KR Dr. Rudolf Bohmann > Chefredakteur: Christian Klobucsar – DW 435 > Produktion: Markus Frühwirth, Thomas Weber > Druck:
Wograndl Druck GmbH, Druckweg 1, 7210 Mattersburg > Alle Rechte, auch die Übernahme von Beiträgen nach § 44 Abs. 1 und
2 Urheberrechtsgesetz, sind vorbehalten.

Fotos: SXC (S.5, 23, 42, 59, 62, 71), Bilderbox (S.35, 37, 44, 53, 58, 60, 66, 69), Photos.com (S.4, 13, 15, 16, 20, 25, 26,
28, 30, 45, 47), Photodisc (S.25, 46, 50, 51, 52, 55), ÖBB (S.18), Diamond Aircraft (S.32), BMLV (S.39), Pressebox (S.40)

Vorwort

Österreich ist nach wie vor eines der sichersten Länder der Welt und als EU-Mitglied zudem auch noch Teil des größten Friedensprojektes der Geschichte.

Dennoch wächst auch in der heimischen Bevölkerung zunehmend der Wunsch nach noch mehr Schutz und Geborgenheit. Wobei es in diesem Zusammenhang den Österreichern und Österreicherinnen nicht nur um terroristische Bedrohungsszenarien oder (Gewalt-)Verbrechen geht, sondern ganz generell um das Verhindern von Gefahren aller Art. Dazu zählen im Besonderen Umweltkatastrophen, wie etwa die schweren Überschwemmungen der letzten Jahre aber auch Lawinenkatastrophen, Tunnelbrände oder der Klimawandel. Und schließlich erhält – speziell in Zeiten globaler (wirtschaftlicher) Verunsicherung – das Thema Sicherheit zwangsläufig eine eigene Dynamik.

Im Rahmen des nationalen Sicherheitsforschungsprogramms „KIRAS“ sollen jene Antworten gefunden werden, die das Bedürfnis der Bevölkerung auf ein Mehr an Sicherheit gewährleisten. Dabei sind aber nicht nur die technischen Disziplinen gefragt: Die verpflichtende Einbeziehung der Geistes-, Sozial- und Kulturwissenschaften soll sicherstellen, dass neue Sicherheitstechnologien und -lösungen maßgeschneidert für die Bedürfnisse der Menschen entwickelt werden. Zugleich soll es gewährleisten, Sorgen vor einem Überwachungsstaat und dem gläsernen Menschen im Keim zu ersticken.

Während andere europäische Staaten in der Sicherheitsforschung erst jüngst erste Akzente zu setzen begannen, ist Österreich auf diesem Gebiet bereits seit vielen Jahren aktiv und hat zudem seit 2005 die Mittel dafür kontinuierlich gesteigert. Bis zum Jahr 2013 werden so mehr als 110 Millionen Euro in die heimische Sicherheitsforschung fließen.

Die vorliegende Broschüre soll Ihnen einen Überblick über sämtliche Forschungsprojekte verschaffen, die in der Zeit von 2007 bis 2009 innerhalb des Nationalen Sicherheitsforschungsprogrammes KIRAS gefördert wurden. Dieser Sammelband kann aber auch als Orientierungshilfe dienen, da er zeigt, in welchen Bereichen der Nationalen Sicherheit die österreichische Bundesregierung ihre Schwerpunkte setzt. Und schließlich soll das Werk dazu beitragen, den Diskurs rund um das Thema Sicherheit zu erweitern und auch jenseits der „klassischen“ Sicherheitsforschungsakteure im engeren Sinne (Bedarfsträger, Forscher, etc.) den Bekanntheitsgrad der erfolgreichen Marke „KIRAS“ zu steigern.

Im Namen des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT) möchte ich mich bei allen WissenschaftlerInnen, Konsortien aber auch sämtlichen ProjektmitarbeiterInnen für ihren Einsatz und ihr Engagement in diesem für Österreich so wichtigen Forschungsfeld herzlich bedanken. Unser Dank gilt auch den MitarbeiterInnen der Österreichischen Forschungsförderungsgesellschaft (FFG), die in professioneller Weise für die reibungslose administrative Abwicklung der ambitionierten KIRAS-Forschungsprojekte gesorgt haben und tagtäglich dafür sorgen.

Gemeinsam werden wir es auch in Zukunft schaffen, jenes Wissen zu generieren, das für den Schutz der österreichischen Bevölkerung, die Erreichung der sicherheitspolitischen Ziele sowie die wissenschaftliche Exzellenz der Forschungsnation Österreich erforderlich ist.

MR Dr. Gernot Grimm,
BMVIT – Stabsstelle für Technologietransfer und Sicherheitsforschung

Inhalt

Vernetzung- und Sondierungsmaßnahmen

BioWarDetect	4
<i>Mobiles System zur Detektion biologischer Kampfstoffe auf Fluoreszenzbasis</i>	
GÖPL-AUT	5
<i>Gemeinsames öffentlich-privates Lagebild</i>	
RescueNet	6
<i>Sondierung des Fluchtwegsanzeigesystems „Flexit“</i>	
SAFENET	8
<i>Austrian Transport Infrastructure SAFETY Research Network</i>	
SKIT	9
<i>Schutz kritischer Infrastruktur</i>	
StegIT	10
<i>Anti-Steganografie-Lösung für VoIP und GSM</i>	

FTE- und Demonstrationsprojekte

AREA-MUMOSIS	12
<i>Multimodales Sicherheitssystem zur Überwachung von Flughafen-Flächen</i>	
ASaP	13
<i>Airport Security and Productivity - Enhancing Airport Security based on Biometric Travel and Novel Methods to ease Airport Operations</i>	
C2DSAS	15
<i>Command and Control Decision Support and Advisory Services</i>	
CaR	16
<i>Connect and Rescue (moderne Rettungskonzepte)</i>	
DESTRail	18
<i>Vorbeugende Maßnahmen für Katastrophen durch Echtzeitschadenserkennung</i>	
DNA-TOX	20
<i>Methoden zum Schutz kritischer Infrastrukturektoren</i>	
emc2	22
<i>emergency mission control center</i>	
FEIS	23
<i>Failure Experience Improvement System</i>	
FUNCL-DEMO	24
<i>Functional clothing für Einsatzkräfte – Entwicklung flexibler multifunktionaler Demonstratoren</i>	
GEDES	26
<i>Gefährdung durch Deponien und Altablagerungen</i>	
iObserve	28
<i>Intelligente Videoüberwachung der nächsten Generation mit semantischen Templates</i>	
iObserve NG	30
<i>Verteilte Videoüberwachung in einer hochskalierbaren service-orientierten Architektur</i>	
MDL	31
<i>Multimedia Documentation Lab</i>	
PUKIN	32
<i>Periodische Überwachung kritischer Infrastrukturen</i>	
RetoMod	34
<i>REferenzszenarien TOxische Gase-MODelle</i>	
S.H.F.	35
<i>Sicherheit von Hohlrumbauteilen unter Feuerlast</i>	
SimRad.NBC	36
<i>Simulation- and information system to manage Rescue units at disaster</i>	
SimRad.COMP	37
<i>Simulations- und Informationssystem zum Administrieren von Hilfseinheiten bei Katastrophen - Erforschung von Systemkomponenten zur Überprüfen der Einsatztauglichkeit der SimRad-Technologie</i>	

SOSGuide	39
<i>Safety Monitoring System and Remote Guidance</i>	
STEG-IT 2	41
<i>Entwicklung von Abwehrmethoden gegen den verdeckten Informationstransfer über VoIP und Handy</i>	
tripleB ID	43
<i>Identifikation von Bedrohungsszenarien in Banken durch Bildanalyse</i>	
TULMON	44
<i>Monitoring der Ausbreitung des Tularämie-Erregers</i>	
VEI-3D	45
<i>Virtueller Einsatzort – Infrastruktur</i>	
VKT-GOEP	46
<i>Validierung von Konzepten und Technologien für ein gemeinsames öffentlich-privates Lagebild</i>	

Unterstützungsmaßnahmen und Studien

3S-VKI	48
<i>Strategische Security Szenarien für die Vernetzung Kritischer Infrastruktur</i>	
Cyberstalking	49
<i>Österreichweite Studie zum Cyberstalking Verhalten</i>	
GEO-IKT	50
<i>Geoinformation und Schutz kritischer Infrastrukturen</i>	
GoVAS	51
<i>Government Voice over IP Attack Study</i>	
Katastrophenmanagement im Gesundheitswesen	53
<i>Bestandsanalyse der Notfallplanung</i>	
Observer Algorithm	54
<i>Computer Vision-Algorithmen zur Detektion potenziell verdächtiger Gegenstände</i>	
OEPK	55
<i>Ortung eingeschlossener Personen nach Katastrophen</i>	
RoSkin	56
<i>Die Rolle des Menschen in ausgewählten Sicherheitssystemen kritischer Infrastruktur</i>	
SALOMON	57
<i>Segregationsanalyse und Methodenentwicklung</i>	
SALOMON Next Step	58
<i>Bedrohungswahrnehmung von Menschen mit Migrationshintergrund</i>	
SEHC	59
<i>Securing Extramural Health Care</i>	
SiLu – Sicherheit aus der Luft	60
<i>Sicherheit aus der Luft</i>	
SIM-SIC!	62
<i>Secure Intermodal Modes - Secure Intermodal Carriers Analyse von Risikopotenzialen einzelner Verkehrsträger intermodaler Transportketten</i>	
SkIG	63
<i>Sicherheit kritischer Infrastruktur bei Großveranstaltungen</i>	
SSC	64
<i>Secure Supply Chains</i>	
SUSI	65
<i>Subjektive Sicherheit im öffentlichen Raum</i>	
Trusted Computing i.d. österr. Verwaltung	66
<i>Abwehr von Angriffen und Schutz persönlicher Daten</i>	
UTSI	67
<i>Urbane Transitionsräume und ihre Sicherheiten</i>	
Zivilschutz	69
<i>Evaluierung von österreichischen Zivilschutzmaßnahmen hinsichtlich Akzeptanz und Zufriedenheit in der Bevölkerung und bei ExpertInnen</i>	

Vernetzungs- und Sondierungsmaßnahmen



BioWarDetect

Mobiles System zur Detektion biologischer Kampfstoffe auf Fluoreszenzbasis

Das vorliegende Forschungsprojekt „BioWarDetect - Mobiles System zur Detektion biologischer Kampfstoffe auf Fluoreszenzbasis“ bezieht sich auf die Programmlinie 1 des österreichischen Sicherheitsforschungsprogramms KIRAS.

Sensoren zur frühzeitigen Detektion biologischer Waffen sind wesentliche Systeme um rechtzeitig Maßnahmen gegen solche Attacken einleiten zu können.

Ziel ist die Sondierung und Evaluierung von Detektionsmöglichkeiten, welche eine schnelle und spezifische Erkennung biologischer Kampfstoffe möglich machen. Im Rahmen der Evaluierung solcher Methoden sollen grundlegende Konzepte zur Detektion untersucht werden.

Die Miniaturisierung der Real Time PCR Technologie ist ein erster Schritt zum mobilen Einsatz. Sie wird intensiv entwickelt, da sie eine Reihe von Vorteilen wie vollautomatische Durchführung, geschlossene Systeme und robuste Ausführung bei geringem Kosten-, Platz- und Energieaufwand bietet. Dadurch können Einschränkungen der klassischen Laborsysteme überwunden und ein mobiler Einsatz möglich gemacht werden. Ein wesentlicher Teil jedes mobilen Systems zum Nachweis von Nukleinsäurefragmenten und damit zur molekularen Feintypisierung infektiöser Materialien, der bisher nur mangelhaft gelöst ist,

sind hochselektive Detektionssysteme mit möglichst geringen Nachweisgrenzen und hoher Nachweissicherheit. Dazu eignen sich wegen der geforderten Spezifikationen in erster Linie Fluoreszenz - Detektionssysteme. Miniaturisierte Varianten zur Integration in Mikro-Fluidik-Systemen mit der Möglichkeit der Immobilisierung der fluoreszenzmarkierten Sonden sind in mehreren Integrationsstufen möglich.

Verschiedene Möglichkeiten zur Realisierung solcher Detektorsysteme sollen in diesem Projekt sondiert und die grundsätzliche Machbarkeit in mikrofluidischen Reaktionssystemen nachgewiesen werden. Den ganzheitlichen Ansatz dieses Projekts unterstreicht die Evaluierung der primären Detektionsmethoden, aber auch der dahinter stehenden Instrumentierung hinsichtlich optischer Anregung und Detektion sowie elektronischer Hardware und Algorithmen zur Auswertung der Messsignale.

ProjektleiterIn / Unternehmen:

JOANNEUM RESEARCH, Institut für chem. Prozessentwicklung und -kontrolle

Kontakt:

Univ.-Prof. Dr. Volker Ribitsch
Tel.: +43 316 876-1234
E-Mail: Volker.Ribitsch@joanneum.at



GÖPL-AUT

Gemeinsames öffentlich-privates Lagebild

Der Umgang mit modernen Sicherheitsrisiken erfordert von den staatlichen Behörden ein vernetztes gesamtstaatliches Vorgehen, das die Fähigkeiten und die Kapazitäten aller Ressorts systematisch aufeinander abstimmt und koordiniert zum Einsatz bringt. Ebenso bedeutend, jedoch konzeptionell erst in Ansätzen realisiert, ist die Zusammenarbeit von Staat und Wirtschaft bei der Gewährleistung staatlicher und unternehmerischer Sicherheitsvorsorge.

Zentrale Voraussetzungen des gemeinsamen öffentlich-privaten Handelns sind das gemeinsame Lagebewusstsein und -verständnis. Daher stellt die Fähigkeit, in einem Prozess die relevanten staatlichen und nichtstaatlichen Akteure zusammenzubringen und durch den gegenseitigen Austausch relevanter Informationen zu einem gemeinsamen Lagebewusstsein und Lageverständnis beizutragen, eine nationale Kernkompetenz dar. Der hohe Bedarf nach dieser Kernkompetenz wird insbesondere durch die Projektbeteiligung des Bundeskanzleramts, des Bundesministeriums für Inneres und des Bundesministeriums für Landesverteidigung unterstrichen.

Lagebewusstsein und Lageverständnis setzen die nutzer- und situationsgerechte Bereitstellung von führungs- und entscheidungsrelevanten Informationen an alle relevanten staatlichen und nichtstaatlichen Akteure voraus. Staatlicherseits wurde in Österreich ein Lagebildprozess etabliert. Gegen-

wärtig wird dieser im Hinblick auf seine Weiterentwicklung evaluiert. Weil staatliche und unternehmerische Sicherheitsvorsorge jedoch kaum noch voneinander zu trennen sind, schlägt das Forschungsprojekt vor, das gesamtstaatliche Lagebild durch ein rollenorientiertes, gemeinsames öffentlich-privates Lagebild (GÖPL AUT) zu ergänzen.

Folgende Inhalte werden im Projekt behandelt:

- Vergleichsstudien zum Aufbau und Einsatz von Lagebildern (und Lagebilelementen) in anderen Staaten sowie in der Privatwirtschaft
- Definition des öffentlichen und privaten Informationsbedarfs für ein gemeinsames öffentlich-privates Lagebild in Österreich
- Vorschlag für den Aufbau einer konkreten Arbeitsplattform für den strategisch relevanten öffentlich-privaten Informationsaustausch in Österreich
- Pflichtenheft für die Entwicklung eines GÖPL AUT-Demonstrators

ProjektleiterIn / Unternehmen:

KFEG GmbH, Koordinierungs-, Forschungs- und Entwicklungsgesellschaft, 1100 Wien, Daumgasse 3

Kontakt:

DI Martin LANGER

Tel.: +43 1 606 68 77-2151

E-Mail: martin.langer@fh-campuswien.ac.at

Web: www.fh-campuswien.ac.at





RescueNet

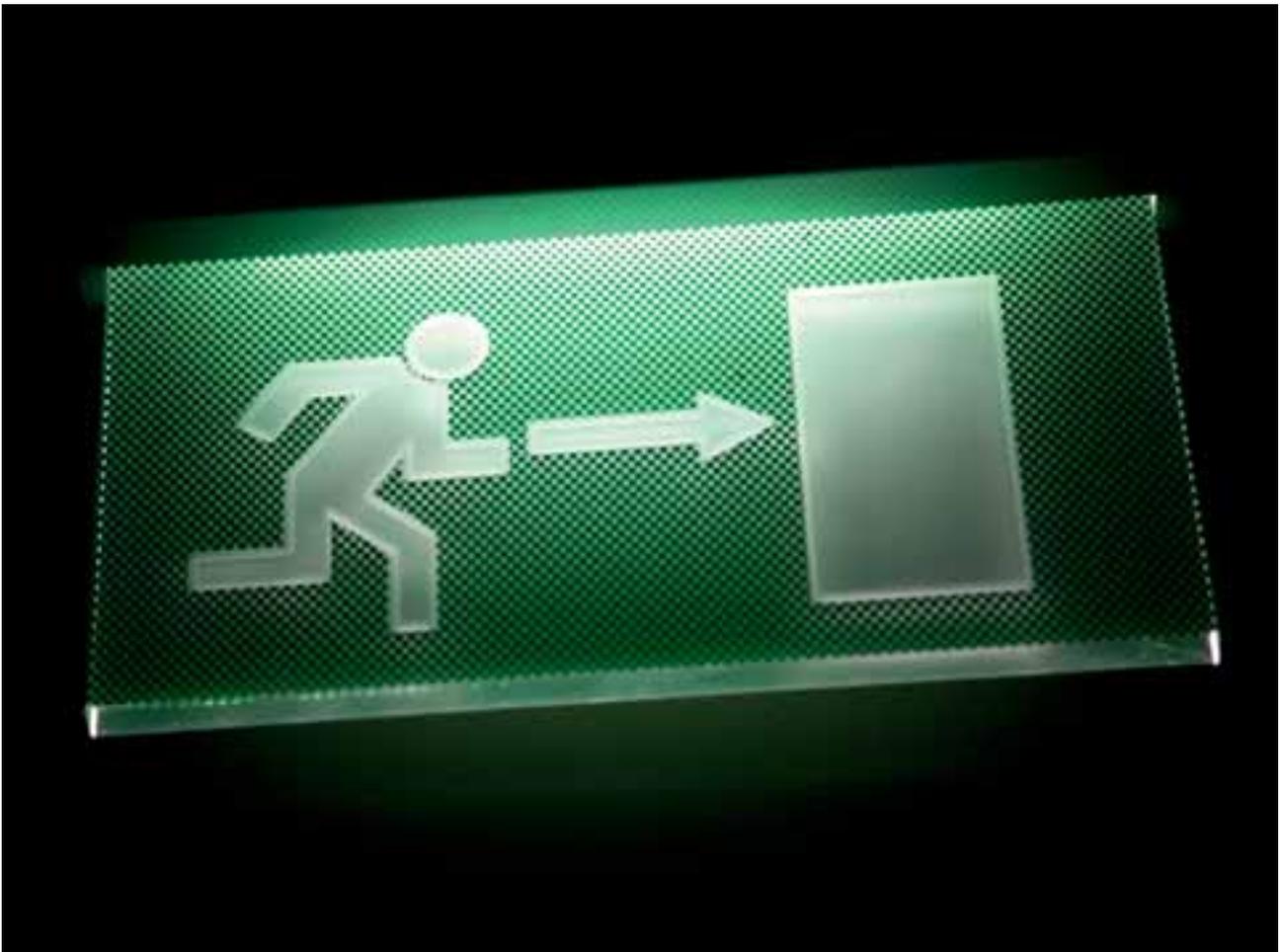
Sondierung des Fluchtwegsanzeigesystems „Flexit“

Sondierung des dynamischen Fluchtwegsanzeigesystems „Flexit“ mit konkretem Demonstrationsszenario.

RescueNET soll die einzigartige Chance nutzen, eine neue und innovative Lösung im Bereich der Fluchtleitsysteme zu sondieren. Die vorgeschlagene Sondierungsmaßnahme soll einen strategischen Beitrag bei der Anwendung eines dynamischen Rettungsmanagement in kritischen Infrastrukturen (z.B. einem Flugplatz) leisten. Ein österreichisches Unternehmen hat dieses innovative System entwickelt und patentiert. Die für die Prototypen erhaltenen Auszeichnungen und Bedarfsmeldungen gehen bereits über Europa hinaus.

Um eine möglichst schnelle Markt- und Betreiberpenetration zu erreichen, ist es erforderlich, die innovative technische Leistung mit Know-how für den realen Einsatzfall zu stärken.

So sollen die bereits identifizierten offenen Fragen auf dem Weg zu Einsatz und Vermarktung hinsichtlich der Lösungsmöglichkeiten analysiert und KIRAS- und EU-Projekte abgeleitet werden (Vernetzung für Konsortienfindung, Machbarkeitsaspekt „Kooperationen“ Technologietransfer, Standardgenerierung). Weiters werden durch eine breit angelegte Analyse – unter Einbeziehung von Sozialwissenschaft / Psychologie / rechtlicher Aspekte – die Faktoren Mensch und



Staat besser berücksichtigt. In Zusammenarbeit mit einem Betreiber (Flughafen Linz) werden mit Hilfe von Rapid Prototyping die potenziellen Nutzer mit einem Systemdemonstrator konfrontiert werden. Daraus können Hersteller und Betreiber wichtige Schlussfolgerungen für zukünftige Produkte ableiten.

Eine essentielle Maßnahme innerhalb einer kritischen Infrastruktur im Falle eines Anschlags, eines größeren Unfalls oder auch nur bei signifikanter Bedrohung ist das „in Sicherheit bringen“ der Menschen aus der Gefahrenzone. So muss jedes öffentliche Gebäude schon heute über ein Fluchtwegeschema, eine Kennzeichnung und passende Einrichtungen verfügen. Jedoch sind die Schemata einer Evakuierung aus einer Infrastruktur / Gebäude schon seit über 50 Jahren fast völlig identisch geblieben.

Bis heute verlässt man sich auf statische Fluchtwegekennzeichnungen. Diese beruhen auf standardisierten Bedrohungsszenarien und überlassen die Menschen in den ersten Minuten ihrer „Flucht“ sich alleine, ohne ihnen eine aktive Hilfestellung zu geben. So ergeben aktuelle Studien, dass z.B. behinderte oder ältere Menschen bei einer Flucht akute Nachteile haben. Ebenso sind die immer komplexer werdenden Infrastrukturen an sich ein Problemfaktor geworden; selbständiges Hinausfinden ist, auch ohne Stresssituation, oft nicht mehr möglich. Ein weiterer Faktor sind die immer mehr ins Blickfeld rückenden terroristischen Szenarien, die ein Vielfaches komplexer als herkömmliche Notfallsituationen sind.

Insbesondere bei solchen Schadensereignissen ergeben sich nicht nur Fragen nach schneller Situationserfassung und passenden Reaktionsmöglichkeiten, sondern auch nach Verantwortlichkeit und Haftung für die Folgeschäden. Empfindliche Störungen einer kritischen Infrastruktur übersteigen oftmals die Erfassungs- und Handlungsmöglichkeit privater, ja sogar staatlicher Akteure. Eine mögliche Lösung für diese Problematik wird

die Sondierung des Systems „Flexit“ zur dynamischen Fluchtwegelenkung aufzeigen.

ProjektleiterIn / Unternehmen:

DI Armin Veichtlbauer, Salzburg Research Forschungsgesellschaft mbH

PartnerInnen:

- Projektleiter DI Armin Veichtlbauer, Wiss. Leiter Prof. Dr. Ulrich Hofmann, Mag. Renate Steinmann, Salzburg Research Forschungsgesellschaft mbH, Jakob-Haringer Str. 5/III, 5020 Salzburg
- Geschäftsführer Ing. Gottfried Grundler, FLEXIT Group GmbH, Bräuhausstraße 14, 5020 Salzburg
- Geschäftsführer Ing. Franz Blohberger, ip&p projects & promotions GmbH, Bräuhausstraße 14, 5020 Salzburg
- Prof. Dr. Alexander Keul, Prof. Dr. Keul Hellbrunnerstr. 34, 5020 Salzburg
- Geschäftsführer DI (FH) Ulrich Wagner, Quantronic GmbH&CoKG, Ludwig-Ganghoferstr. 22, D-83471 Berchtesgaden
- Branddirektor DI Eduard Schnöll, Berufsfeuerwehr Salzburg, Jägermüllerstraße 3, 5020 Salzburg
- DI Gerhard Kunesch, Flughafen Linz, Flughafenstrasse 1, 4063 Hörsching

Kontakt:

- DI Armin Veichtlbauer, Projektleiter, Salzburg Research Forschungsgesellschaft mbH, Jakob-Haringer Str. 5/III, 5020 Salzburg
Tel.: +43 662 2288-448
Fax: +43 662 2288-222
E-Mail: aveichtl@salzburgresearch.at
Web: www.salzburgresearch.at
- Prof. Dr. Ulrich Hofmann, Einreicher, Wiss. Leiter, Salzburg Research Forschungsgesellschaft mbH, Jakob-Haringer Str. 5/III, 5020 Salzburg
Tel.: +43 662 2288-448
Fax: +43 662 2288-222
E-Mail: ulrich.hofmann@salzburgresearch.at
Web: www.salzburgresearch.at



SAFENET

Austrian Transport Infrastructure SAFETY Research Network

Bei dem Projekt SAFENET handelt es sich um ein Netzwerk zur Erforschung und Analyse der Sicherheitsaspekte, Risiken und Bedrohungen, welche in Österreich durch Erdbeben auftreten. Es soll die nationale Vernetzung von Wirtschaft, Wissenschaft und Bedarfsträgern ermöglichen.

Sicherheitsforschung bedeutet eine weitgehend fächerübergreifende Herausforderung. Zur gezielten Verbesserung des Ist-Zustandes ist eine Bündelung der nationalen Ressourcen und des Fachwissens notwendig. Einzelne, bisher zuwenig beachtete Fachgebiete, verdienen dabei besondere Aufmerksamkeit. Das SAFENET-Projekt hat das Thema seismische Gefährdung zum Mittelpunkt, welchem durch eine Neueinschätzung der Gefahren eine hohe Priorität zukommt.

Die Starkbeben von Northridge (U.S.A 1994), Kobe (Japan 1995), Kozaeli (Türkei 1999), Chi Chi (Taiwan 1999), sowie Umbrien (1998) und Athen (1999) haben zu einer Veränderung der Einschätzung des seismischen Risikos geführt. Dies ist bereits in den gültigen Eurocode 8 eingearbeitet und in die gültige österreichische Erdbebennorm (B4015) übernommen worden (gültig seit 2002). Erdbeben, bisher ein Thema ohne Relevanz in Österreich, werden nun zu entscheidenden Bemessungskriterien.

Aufgrund der bis 2002 gültigen Normenlage hat sich keine ausreichende „Erdbebenkultur“ in Österreich herausgebildet. Dieses Projekt soll die Integration seismischer Fragen in die allgemeine Sicherheitsbetrachtung ermöglichen. Das Thema Erdbeben betrifft sämtliche kritische Infrastrukturen und soll die nationale Vernetzung von Wirtschaft, Wissenschaft und Bedarfsträgern ermöglichen.

Mangels Aktualität hat der Wissens- und Technologietransfer zu den Bedarfsträgern nicht stattgefunden. Die neue Normenlage macht dies nun zwingend erforderlich. Dazu ist der Auf- und Ausbau von Humanressourcen erforderlich, um Syner-

gien nutzen zu können. Weiters betrifft das Thema Wissenschaftler/innen und Unternehmer/innen aus unterschiedlichsten Disziplinen. Auch hier herrscht ein großer Vernetzungsbedarf. Andererseits sollten die Bedarfsträger bei der Generierung innovativer Ideen für Forschungsprojekte einbezogen werden, um sehr gezielt arbeiten zu können. Die Verantwortlichen für die Infrastruktur sowie den Zivilschutz sollen eine Abschätzung der gesellschaftlichen Wirksamkeit von Maßnahmen abgeben, welche zu Neuentwicklungen führen sollen.

Durch Erdbeben hervorgerufene Krisen rangieren an oberster Stelle bei den Naturgefahren. Eine Abschätzung der gesamtstaatlichen Stabilität ist daher nur unter Einbeziehung aller betroffenen Disziplinen möglich. Andererseits können Vorsorgeprogramme gewünschte volkswirtschaftliche Effekte auslösen.

ProjektleiterIn / Unternehmen:

DI Dr. Helmut Wenzel, VCE Holding GmbH

PartnerInnen:

- Universität für Bodenkultur Wien, Institut für Vermessungswesen, Fernerkundung und Landvermessung – DI Dr. Werner Schneider
- Universität Innsbruck, Institut für Grundlagen der Bauingenieurwissenschaften, Arbeitsbereich für Festigkeitslehre Baustatik und Tragwerkslehre – DI Dr. Christoph Adam
- ÖBB Infrastruktur Bau AG – Mag. Karl-Eric Pumper
- APLICA Mess- und Prüftechnik GmbH – Ing. Robert Prethaler
- Arsenal Research - DI Dr. Rainer Flesch

Kontakt:

VIENNA CONSULTING ENGINEERS,
HOLDING GMBH

1140 Vienna, Hadikgasse 60

Tel.: +43 1 897 53 39

Fax: +43 1 893 86 71

E-mail: vce@atnet.at

Web: www.vce.at

SKIT

Schutz kritischer Infrastruktur

Die Bedrohung kritischer Infrastruktur durch Terrorismus und gewaltbereite, extremistische Gruppierungen.

Das vorliegende Forschungsprojekt „SKIT / Schutz kritischer Infrastruktur - Die Bedrohung kritischer Infrastruktur durch Terrorismus und gewaltbereite, extremistische Gruppierungen“ bezieht sich auf die Programmlinie 1 des österreichischen Sicherheitsforschungsprogramms KIRAS. Dieses Projekt dient der Erhebung und der Vernetzung österreichischer Bedarfsträger wie dem BMI, BMLV, BMWA und Bundesministerium für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft mit österreichischen Experten in Fragen der Sicherheits- und Terrorismusforschung und mit Vertretern der Wirtschaft.

Daraus soll eine Forschungsplattform entstehen und weitere Forschungsfragen bearbeitet werden. Die zentralen Forschungsaspekte werden durch Folgeprojekte abgedeckt. Damit fungiert das aktuelle Forschungsprojekt der Programmlinie 1 als Ausgangsbasis für eine weitere wissenschaftliche Bearbeitung des Themenfeldes „Schutz kritischer Infrastruktur“.

Als zentraler Aspekt für eine Folgebearbeitung wird die interdisziplinäre Erforschung bestimmter religiöser, ethnischer, soziologischer und ideologischer Strukturen in Österreich im Hinblick auf deren potenziellen Extremismusneigungen, sowie das daraus resultierende Gefährdungspotenzial für die kritische Infrastruktur angestrebt. Hierbei soll auch der Bewusstseinsbildung und Wissensgenerierung Rechnung getragen werden.

Im Kontext des vorgelegten Projekts wird insbesondere folgenden Forschungszielen besondere Bedeutung beigemessen:

- Erhebung des „State of the Art“ in der Terrorismus-Forschung
- Identifikation entsprechender Experten
- Identifikation möglicher Kooperationspartner und dauerhafter Netzwerkbildung

- Identifikation noch nicht oder nur ungenügend behandelter Forschungsfragen im Bereich der Terrorismusforschung
- Erarbeitung von Folgeprojekten

Der Wissensstand bezüglich gewaltbereiter Gruppierungen in Österreich ist gering und auf einen kleinen Personenkreis beschränkt. Im Rahmen des eingereichten Projekts soll vorhandenes Expertenwissen systematisch vernetzt werden, um forschungsrelevante Synergieeffekte zu erzielen. Dieses Netzwerk soll dazu dienen, bedarfsrelevante Fragestellungen zu erarbeiten und Möglichkeiten zu deren Beantwortung aufzuzeigen. Auf den Ergebnissen dieses Projekts basierend sollen weitere Projekte, welche die originäre Zielsetzung in einem umfassenden Ansatz verfolgen, entwickelt werden. Dieses Projekt soll interdisziplinär abgehandelt werden. Ziel ist eine Verbindung von sozialwissenschaftlichen mit naturwissenschaftlichen Ansätzen, sowie die Erschließung der europäischen Dimension als Andockstelle für die nationale Sicherheitsforschung.

Mit der vorliegenden Forschungskonzeption werden bislang nicht oder nur unzureichend behandelte Aspekte in der Terrorismusforschung wissenschaftlich abgedeckt. Mit diesem Projekt wird erstmalig der Versuch unternommen, vorhandene Expertisen weiterzuentwickeln und zu bündeln. Dadurch sollen Synergieeffekte in der österreichischen Terrorismusforschung erzielt und mittel- und langfristige Gegenstrategien entwickelt werden. Der Mehrwert wird darin gesehen, dass mittelfristig erwartbaren Sicherheitsproblemen proaktiv begegnet und dadurch den gesamtgesellschaftlichen und politischen Erfordernissen Rechnung getragen werden kann.

ProjektleiterIn / Unternehmen:

OIIP -Österreichisches Institut für Internationale Politik

Kontakt:

Mag. Nieves-Erzsebet Kautny
Tel.: +43 1 581 11 06
E-Mail: kautny@oiip.at



StegIT

Anti-Steganografie-Lösung für VoIP und GSM

Machbarkeitsstudie für Anti-Steganografie-Lösung für VoIP und GSM.

Die Steganografie ist die „Kunst“ geheime Informationen so zu vermitteln, dass ein nicht eingeweihter Dritter die Existenz dieser Information nicht bemerkt. Daher ist die Steganografie besonders gefährlich im Bereich der Wirtschaftsspionage, Vorbereitung von Terrorangriffen, Menschenhandel etc. Sie wurde nachweislich auch von Bin Laden und seiner Organisation eingesetzt.

Das Ziel des vorliegenden Projekts StegIT ist die Verhinderung von Steganografie in der Internettelefonie (VoIP) und Mobiltelefonie (GSM/UMTS). Die klassischen Methoden basieren darauf, dass zuerst im übertragenen Sprachsignal ein steganografischer Angriff (Einbettung von zusätzlichen Daten) erkannt und analysiert wird und dann der Angriff abgewehrt wird. Da es nach heutiger Sicht mit einem akzeptablen Aufwand nicht machbar ist, Verfahren und Lösungen zu entwickeln, die unbekannt bzw. neue steganografische Verfahren sicher erkennen und verhindern, wird im Rahmen dieses Projektes ein anderer Weg gegangen, der Angriffe über Transformationsmethoden abwehrt. Diese Methoden führen keine Steganalyse (Detektion eines steganografischen Angriffs) durch, sondern versuchen sofort einen möglichen Angriff durch eine geeignete Vorgangsweise abzuwehren, unabhängig davon, ob überhaupt ein steganografischer Angriff stattgefunden hat. Diese Abwehr von Angriffen darf aber die normale Sprachübertragung (und Bildübertragung bei MMS), insbesondere auch in Sprech- und Musikpausen, nicht stören. Es wird erwartet, dass dazu die Ergebnisse im eigenen Testlabor ausreichende Beiträge liefern.

Weiters werden auch Methoden und Konzepte nach Machbarkeit untersucht, die zusätzlich eine Durchlässigkeit eigener steganografischer Methoden erlauben. Diese Möglichkeit zur Einbettung kann zum Beispiel für das DRM (Digital Rights Management), wo Steganografie für positive Zwecke eingesetzt wird, Anwendung finden. Bei

dieser Durchlässigkeit kann es sich z.B. um ein hochsicheres Verfahren handeln, das nachträglich das originale Sprachmuster/Bitmuster wieder herstellen kann.

Für die erforderlichen Tests wird an der Fachhochschule St. Pölten ein Testlabor aufgebaut, in dem es möglich sein wird steganografische Einbettungsalgorithmen und Anti-Steganografie-Lösungen in VoIP und GSM zu testen.

Das gesamte Projekt dauert 8 Monate und ist in folgende Arbeitspakete unterteilt: Projektmanagement, Steganografie mit Bildern, Spezifikas von VoIP und GSM/UMTS, Steganografie mit VoIP und GSM/UMTS, Machbarkeitsstudien für Anti-Steganografie-Lösungen mit Bildern, VoIP und GSM/UMTS und mit einer Durchlässigkeit für DRM, Akzeptanzanalyse, Technologiefolgenabschätzung, Erstellung des Endberichtes.

Es werden im Rahmen dieses Projektes keine Verfahren und Lösungen vollständig entwickelt und implementiert, sondern geeignete Methoden und Konzepte ausgearbeitet, getestet und dafür Machbarkeitsstudien erstellt.

ProjektleiterIn / Unternehmen:

Fachhochschule St. Pölten GmbH, Projektleiter:
Univ.-Doz. D.I. Dr. Ernst Piller

PartnerInnen:

- Bundesministerium für Landesverteidigung
- Bundeskriminalamt (Bundesministerium für Inneres)
- internic Datenkommunikations GmbH

Kontakt:

Fachhochschule St. Pölten GmbH
Matthias Corvinus-Straße 15
3100 St. Pölten

z.H. Univ.-Doz. D.I. Dr. Ernst Piller

Tel.: +43 664 9200891 oder +43 2742 313 2280

Fax: +43 2742 313 228 209

E-Mail: lpiller@fh-stpoelten.ac.at

Web: www.fh-stpoelten.ac.at

FTE- und Demonstrationsprojekte



AREA-MUMOSIS

Multimodales Sicherheitssystem zur Überwachung von Flughafen-Flächen

Aufgrund der Wichtigkeit von Flughäfen als Hauptknotenpunkte für Transport und Verkehr können sich Störungen der Flughafen-Infrastruktur verheerend auswirken. Störungen können einerseits durch widerrechtliches äußeres Eindringen (Betreten oder Befahren der Flughafen-Flächen) oder durch unerlaubtes Abstellen von Fahrzeugen oder Gegenständen z.B. auf der Rollbahn erfolgen.

Dies ist vor allem bei starker Sichtbehinderung sehr kritisch, da die Überwachung der Flughafen-Flächen derzeit nur visuell von den Fluglotsen durchgeführt wird. Die derzeit verwendeten Systeme arbeiten meist nur unimodal, d.h., sie werten die Daten nur einer Art von Sensoren (z. B. Videokameras) aus. Signale zusätzlicher Sensoren werden derzeit kaum betrachtet.

Ziel des vorliegenden Projektes ist es deshalb, die Grundlagen für ein multimodales Monitoring-System zu entwickeln, mit dessen Hilfe die Flächen von Flughäfen effizient und effektiv überwacht werden können. Durch den Einsatz verschiedenartiger Sensoren und anschließender intelligenter Verarbeitung und Verknüpfung der Detektionsergebnisse soll zukünftig die Sicherheit der Flughafen-Flächen gewährleistet werden. Dadurch sollen auch komplementäre Informationsquellen erschlossen werden, um damit sowohl eine bessere Detektionsrate als auch eine höhere Stabilität und Zuverlässigkeit des Sicherheitssystems zu erreichen.

Im Projekt soll vor allem die technische Machbarkeit eines derartigen Systems, sowohl unter Berücksichtigung der wirtschaftlichen, als auch der gesellschaftlichen Aspekte, überprüft und erarbeitet werden.

Der Ablauf des Projekts kann wie folgt umrissen werden:

- AP 1: Erstellung System-Konzept, Definition der Schnittstellen, Nutzung bestehender Anlagen
- AP 2: Erarbeitung von Szenarien für die Durchführung von Testmessungen auf der Flughafen-Fläche

- AP 3: Erstellung eines Testplans, Durchführung von Testmessungen, Erstellung Signal-Datenbank
- AP 4: Algorithmenentwicklung für Videodetektion: robuste Personen- und Objektdetektion
- AP 5: Algorithmenentwicklung für akustische Detektion: Erkennung von alarmierenden Geräuschen, Lokalisierung von Schallquellen auch bei schlechten Sichtverhältnissen
- AP 6: Verknüpfung der Detektionsergebnisse der Modalitäten
- AP 7: Validierung der Ergebnisse
- AP 8: Dokumentation, Präsentation
- AP 9: Projektkoordination

Das vorrangige Ziel dieses Projekts ist es, die Funktionalität und die Vorteile eines multimodalen Monitoring-Systems aufzuzeigen und damit einen wesentlichen Beitrag zur Steigerung des subjektiven Sicherheitsgefühls der Bevölkerung zu leisten.

ProjektleiterIn / Unternehmen:

Dipl.-Ing. Dr. Franz Graf, JOANNEUM RESEARCH Forschungsgesellschaft mbH

PartnerInnen:

- JOANNEUM RESEARCH ForschungsgesmbH
Institut für Angewandte Systemtechnik
www.joanneum.at/ias,
Institut für Informationssysteme & Informationsmanagement, www.joanneum.at/iis
- Flughafen Graz Betriebs GmbH
www.flughafen-graz.at/
- Siemens AG Österreich Building Technologies
www.siemens.at/sbt

Kontakt:

JOANNEUM RESEARCH ForschungsgesmbH
Institut für Angewandte Systemtechnik
Dipl.-Ing. Dr. Franz Graf
Steyrergasse 17,
8010 Graz
Tel.: +43 316 876 - 1631
Email: franz.graf@joanneum.at
Web: www.joanneum.at

ASaP

Airport Security and Productivity - Enhancing Airport Security based on Biometric Travel and Novel Methods to ease Airport Operations

Im Rahmen dieses Forschungsprojektes sollen sicherheitsrelevante Ereignisse aus Videostreamen erkannt, ausgewertet und präsentiert werden, so dass Sicherheitspersonal unmittelbar und geeignet auf diese Ereignisse reagieren können. Durch Kombination von intelligenten Kamerasystemen mit leistungsfähigen Servern, sollen die hohen Anforderungen biometrischer Algorithmen kosteneffizient erfüllt werden. Wesentliche Ereignisse, die von diesem System erfasst werden sollen, sind stehen gelassene Gepäckstücke, hohes Personenaufkommen im Bereich der Check-In-Schalter, sowie unerlaubte Zutrittsversuche betriebs-

fremder Personen zu abgesperrten Bereichen. Begleitend zu diesen technischen Themen wird die Akzeptanz derartiger Kontroll- und Überwachungssysteme bei Passagieren und Flughafenpersonal erforscht und Verbesserungsvorschläge erarbeitet.

Videoüberwachungsanlagen nach dem heutigen Stand der Technik benötigen Personal, um sicherheitsrelevante Ereignisse zu erkennen. Turnusmäßiger Schichtwechsel ist an der Tagesordnung, da die Aufmerksamkeit schnell nachlässt. Diese Technologie erkennt sicherheitsrelevante Ereignisse





automatisch und zeigt vordefinierte Ereignisse dem Sicherheitspersonal automatisch an.

Die Anwesenheit bestimmter Personen ist am Flughafen unerwünscht oder wird als Sicherheitsrisiko eingestuft und soll dem Sicherheitspersonal unverzüglich gemeldet werden. Herkömmliche Videoidentifikationssysteme scheitern häufig an ungünstigen Lichtbedingungen, die eine zuverlässige Identifikation von Personen verhindern.

Ziel der Forschung in diesem Projekt wird die selektive Verbesserung der Lichtsituation im Bild sein, sodass das Potenzial der biometrischen Algorithmen voll ausgeschöpft werden kann.

Die folgenden sicherheitsrelevanten Themen werden im Detail behandelt:

- Durch die hohe Anzahl der Fehlalarme (verursacht meistens durch vergessene Gepäckstücke in der Abfertigungshalle) entsteht beim Sicherheitspersonal, aber auch bei den Passagieren unnötiges Konfliktpotenzial bzw. Ärgernis. Derzeit werden liegen gelassene Gepäckstücke erst so spät entdeckt, dass der Besitzer außer Reichweite ist und nicht bemerkt, dass sein Gepäckstück einen Alarm auslöst. Die häufige Konsequenz (200 - 300 Mal pro Jahr) ist ein Polizeieinsatz samt Sperre und Evakuation der Halle.
- Sicherheitskontrollen durch Personal und Metalldetektoren führen bei mehr als 30% der Passagiere zu unnötigen Nachkontrollen, meist aufgrund von Unkenntnis des Systems und schlechter Kommunikation der richtigen Vorgangsweise.
- Für Personen, die den Schengenraum verlassen, wird eine Datenbankabfrage beim Schengen-Informationssystem durchgeführt. Diese dauert im Schnitt 60-90 Sekunden und verlängert die Kontrollzeit und damit auch die Wartezeit der übrigen Passagiere. Frühzeitige Abfrage und Bereithaltung der Daten kann diese Wartezeit minimieren.

Unser Projektantrag geht auf diese technischen Problemstellungen ein und bietet detaillierte Lösungsansätze. Biometrische Systeme werfen aber auch sozialwissenschaftliche Fragen auf, die im

Rahmen dieses Forschungsprojektes beleuchtet werden sollen.

Derartige Systeme dienen einerseits der Erhöhung der Sicherheit aller Nutzer des Flughafens, andererseits schränken sie die Privatsphäre der Flughafenutzer ein. Ängste über vermutete Verletzungen des Datenschutzes, der Verletzung der Intimsphäre und vor einem Ausbau des Überwachungsstaates treten in Konflikt mit dem großen Sicherheitsbedürfnis und dem Wunsch, als Reisender den Flughafen in effizienter und rascher Weise vom Eingang über den Check-In Bereich bis zum Abflug-Gate zu nutzen.

In Österreich gibt es noch keine empirische Forschung über die Einstellung der Bevölkerung zu neuen computergestützten Identifizierungssystemen im öffentlichen Raum Flughafen. Weiters fehlen daher auch verlässliche empirische Daten über die überdurchschnittlich von Ängsten betroffenen Bevölkerungsgruppen und deren besondere Merkmale – sowohl Ängste in Bezug auf Sicherheitsrisiken, aber auch von Ängsten in Bezug auf Verletzung von Aspekten des Datenschutzes.

Die Sozialwissenschaftler des IFES Instituts unterstützen die Entwicklung im Rahmen der Erstellung der Konzepte und der praxisnahen Definition aller Anforderungen durch empirische Sozialforschung.

ProjektleiterIn / Unternehmen:

x-pin.com GmbH, Linke Wienzeile 4, Stiege 2, Tür 5, 1060 Wien

PartnerInnen:

x-pin.com - ARC - IFES - Flughafen Wien AG

Kontakt:

x-pin.com GmbH

DI Stefan Botond Borbely, MSc

Mobil: +43 650 9001615

E-Mail: s.borbely@x-pin.com

Web: www.x-pin.com

C2DSAS

Command and Control Decision Support and Advisory Services

Entwicklung neuer softwarebasierter Verfahren zur operativen Entscheidungsunterstützung, Ressourcenoptimierung und zur „Umplanung“ bei geänderten Rahmenbedingungen in komplexen Entscheidungssituationen.

Ziel des vorgeschlagenen C2DSAS-Projekts ist die Entwicklung neuer, softwarebasierter Verfahren zur operativen Entscheidungsunterstützung, Ressourcenoptimierung und insbesondere „Umplanung“ bei geänderten Rahmenbedingungen in komplexen Entscheidungssituationen im Störungs- und Krisenmanagement (z.B. bei Hochwasserkatastrophen, in der Einsatzplanung, bei Terror-Bedrohungen) sowie in der betrieblichen Prozessoptimierung im zivilen Bereich.

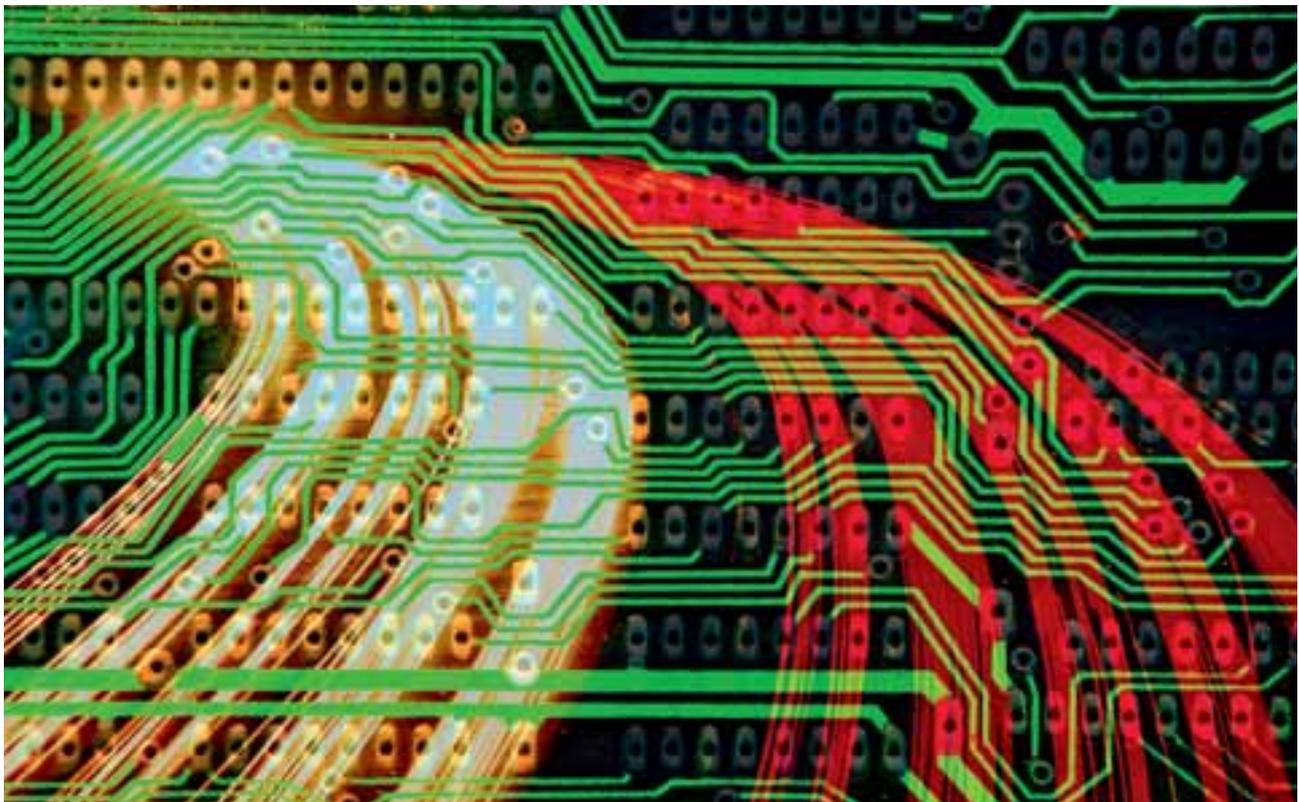
Im Bereich der Grundlagenforschung sollen neue Verfahren auf dem Gebiet von wissensbasierten Planungssystemen, der Prozessreparatur und -er-

klärung entwickelt werden. Anwendungsorientierung und Wirtschaftsorientierung werden durch detaillierte Evaluation der technischen Umsetzbarkeit und der dazu notwendigen Rahmenbedingungen bei den öffentlichen Bedarfsträgern erreicht.

Die zu erwartenden psychologisch-soziologischen Auswirkungen einer solcherart erweiterten IT-Unterstützung auf menschliche Entscheidungsprozesse in Krisensituationen werden in einer begleitenden Studie analysiert.

Kontakt:

Alpen-Adria Universität Klagenfurt -
Institut für angewandte Informatik
o. Univ.-Prof. DI Dr. Gerhard Friedrich
Universitätsstraße 65-67
9020 Klagenfurt
Tel.: +43 463 2700-3757
E-Mail: gerhard.friedrich@uni-klu.ac.at





CaR

Connect and Rescue (moderne Rettungskonzepte)

„Connect and Rescue“ hat das Ziel, eine innovative Lösung im Bereich moderner Rettungskonzepte zu entwickeln.

Ausgangspunkt ist die unzufriedenstellend geschlossene Lücke zwischen den Anforderungen an ein modernes Rettungssystem und den in der IKT-F&E erreichten Fortschritten bzgl. Sensortechnik, robusten, sicheren und leistungsstarken Kommunikationsnetzen, Informationssystemen für Retter und zu Rettende, Gestaltung offener Schnittstellen für die Interaktion der Rettungskräfte.

In einer ersten Phase wird „Connect and Rescue“ die Bedrohungspotenziale und Risiken erforschen, und daraus eine Anforderungsanalyse unter Einschluss aller technologischen und sozialen Aspekte ableiten.

Dabei werden die genauen Spezifikationen des in der zweiten Phase prototypisch zu entwickelnden Systems herausgearbeitet. In einer dritten Phase sollen die Ergebnisse mittels Labordemonstratoren optimiert und praxisnah gestaltet werden.

Die validierungsrelevante Anwendung wird die IKT-unterstützte Entfluchtung eines öffentlichen Gebäudes sein. Nach diesem „Proof of Concept“ werden die Testergebnisse wiederum nach technologischen und sozialen Kriterien interpretiert.

Es soll ein Kommunikationssystem entwickelt werden, das die digital vernetzte Koordination von Einsatzkräften vor Ort ermöglicht. So soll der bisherige schmalbandige Audio-Sprechfunk durch moderne IP-Konnektivität mit höherer Bandbreite ersetzt werden. Dieses System wird es ermöglichen, dass geographisch verortete Einsatzkräfte -



von einer mobilen Leitstelle unterstützt – wesentlich effektiver und sicherer arbeiten können. In einem weiteren Teil sollen generische Schnittstellen die vor Ort verwendbaren Systeme und Geräte (z.B. Entfluchtungseinrichtungen im Gebäude) übergangslos in das Gesamtleitsystem aufnehmen können.

Somit wird neben der von den Kräften „mitgebrachten“ neuen Funktionalität (z.B. digitales Netzwerk, GPS-Verortung, mobile Leitstelle) auch die Funktionalität des Gebäudes (z.B. dort integriertes Fluchtleitsystem) als Hilfsmittel für eine zielgerichtete Reaktion im Krisenfall verfügbar.

Dies spiegelt sich auch im Projektnamen wider: „Rescue“ steht für den Inhaltlichen Teil des Projektes, der die Rettungsaktivitäten durch eine innovative Kommunikationsinfrastruktur deutlich verbessern soll; „Connect“ für den Teil, der die Rettungskräfte mit der betroffenen Infrastruktur vernetzt und so in Folge das bisherige mühsame „Search“ durch die Einsatzkräfte drastisch mindern soll.

Folgende grundlegenden Eigenschaften soll das im Projekt „Connect and Rescue“ zu entwickelnde System aufweisen (diese Eigenschaften spiegeln sich auch in der Beschreibung der einzelnen Arbeitsschritte wider):

- Sicherheit: Schutz vor Angriffen Außenstehender und Schutz der Zugriffsrechte und Systeminformationen. Beschränkung der Nutzbarkeit des Systems für Einsatzkräfte - Robustheit: Maximale Wirksamkeit der Lösung auch unter widrigsten Einsatzbedingungen
- Funktionalität: Ad-hoc-Verwendbarkeit (kein aufwendiges System-Setup vor Ort), Verständlichkeit (User-Interface), Performanz (ausreichend hohe Datenraten)
- Flexibilität: Schaffung einer universellen (System-) Schnittstelle („Open-CaR“), die die Anbindung an Third-Party Systemen erlaubt, Verwendung generischer Übertragungsprotokolle (TCP/IP basierend)
- Mobilität: Lange Netzunabhängigkeit und Handhabbarkeit (kleine / leichte Geräte)

ProjektleiterIn / Unternehmen:

DI Armin Veichtlbauer, Salzburg Research Forschungsgesellschaft mbH

PartnerInnen:

- Salzburg Research Forschungsgesellschaft mbH, Jakob-Haringer Str. 5/III, 5020 Salzburg
Projektleiter DI Armin Veichtlbauer
Wiss. Leiter Prof. Dr. Ulrich Hofmann
- Eurofunk Kappacher GmbH, Eurofunkstraße 2, 5600 St. Johann, Prokurist Ing. Christian Kappacher
- Universität Salzburg, FB Materialwissenschaften, Hellbrunnerstr. 34, 5020 Salzburg, Univ. Prof. Dr. Friedrich Steinhäusler
- Universität Salzburg, FB Psychologie, Hellbrunnerstr. 34, 5020 Salzburg, Univ. Prof. Dr. Alexander Keul
- FLEXIT Group GmbH, Bräuhäusstraße 14, 5020 Salzburg, Geschäftsführer Gottfried Grundler
- Berufsfeuerwehr Salzburg, Jägermüllerstraße 3, 5020 Salzburg, Branddirektor DI Eduard Schnöll
- Fachhochschule Salzburg, Urstein Süd 1, 5412 Puch, Studiengangsleiter Prof. Dr. Thomas Heistracher
- Quantronic GmbH&CoKG, Ludwig-Ganghoferstr. 22, D-83471 Berchtesgaden, Geschäftsführer DI (FH) Ulrich Wagner

Kontakt:

Salzburg Research Forschungsgesellschaft mbH
Jakob-Haringer Str. 5 / III
5020 Salzburg

DI Armin Veichtlbauer
Projektleiter
Tel.: +43 662 2288-448
Fax: +43 662 2288-222
E-Mail: aveichtl@salzburgresearch.at

Prof. Dr. Ulrich Hofmann
Einreicher, wiss. Leiter
Tel.: +43 662 2288-442
Fax: +43 662 2288-222
E-Mail: ulrich.hofmann@salzburgresearch.at
Web: www.salzburgresearch.at



DESTRail

Vorbeugende Maßnahmen für Katastrophen durch Echtzeitschadenserkennung

Prevention of Disasters from Earthquakes, Ship Impact and Terrorist Attack on Infrastructure of Rail Network. Ziel des kooperativen Projektes ist eine Eingrenzung der Risikozonen für Erdbebenauswirkungen im österreichischen Schienennetz und der Aufbau von Grundlagen für die Entwicklung eines Prototyps für ein Alarmsystem an ÖBB-Kunstbauten.

Die Verkehrsinfrastruktur ist das Rückgrat unserer Wirtschaft. Die Auswirkungen von Naturgefahren, Technologieversagen und menschlichem Fehlverhalten gefährden die Infrastruktur und können so zu erheblichen volkswirtschaftlichen Schäden führen. Dabei haben mehrere Ereignisse der letzten Jahre gezeigt, dass die indirekten Schäden die direkten bei weitem noch übertreffen.

Dieser Vorschlag konzentriert sich auf das Eisenbahnnetz. Störungen aus den oben erwähnten Einflüssen können zu Katastrophen führen, welche den Verlust von Menschenleben und erhebliche materielle Schäden bedeuten können. Der Inhalt des Projektes ist die Echtzeitschadenserkennung, die rechnerische Evaluierung und sub-

sequente automatische Zugbeeinflussung. Züge die sich schadhaften Stellen im Streckennetz nähern werden unverzüglich angehalten. Dieses ambitionierte Projekt deckt einen großen Bereich der Sicherheitsforschung ab. Es wird versucht, Methoden und Algorithmen zu finden, welche sowohl für terroristische Akte als auch Auswirkungen von Naturgefahren anwendbar sind. Den Erkenntnissen folgend, die bei Beinahekatastrophen wie dem Schiffsanprall an der Donaubrücke KREMS oder den Gleisverwerfungen beim Izmit-Erdbeben gewonnen wurden, konzentriert sich die Arbeit auf folgende Subthemen:

- 1) Eingrenzung der Risikozonen für Erdbebenauswirkungen im österreichischen Schienennetz. Dabei werden durch Fernerkundungsmethoden (Auswertung von Landsat, SAR, InSAR und Envisat Daten) jene Stellen im Schienennetz identifiziert, welche aktive tektonische Verwerfungen passieren oder tangential passieren. Dies führt unmittelbar zur Erstellung einer Gefahrenkarte für das österreichische Schienennetz. In Kombination mit der Auswertung von Erdbebenaufzeichnungen aus dem österreichischen Strong-



motion Network kann binnen Sekunden eine potenzielle Schädigung errechnet und der Zugverkehr gestoppt werden.

- 2) Durch Schiffsanprall (wie in Krems 2005/06) können Eisenbahnbrücken soweit geschädigt werden, dass ein passierender Zug zum Absturz kommen würde. Eine permanent arbeitende Kombination aus Sensoren und Detektoren soll entsprechende Hinweise auf derartige Ereignisse liefern. Diese Information wird in einem Decision Support System bewertet und entsprechende Haltesignale betätigt.
- 3) Terroristische Akte, welche in ihrer Natur der Auswirkung, dem Schiffsanprall ähneln, sind an allen Brücken und Kunstbauten des Bahnnetzes denkbar. Die gleiche Detektionsmethode wie zuvor wäre anwendbar und auf ihre Tauglichkeit zu untersuchen.

Der zuvor beschriebene technologische Ansatz wurde für andere Zwecke bereits beschrieben. In dem vorliegenden Projekt soll die Anwendbarkeit auf das österreichische Schienennetz untersucht und nachgewiesen werden. Entsprechende grundlegende Forschungs- und Entwicklungsarbeiten sind dazu notwendig.



Das Projekt beginnt mit der Grobeinschätzung der verschiedenen Risiken im ÖBB-Netz. Mittels Fernerkundung werden die Daten zur Beurteilung erhoben und über ein GIS-System mit dem Netz überlagert. Entsprechende Einflussbereiche sind zu definieren. Bezüglich technologischer Risiken wird untersucht, inwieweit eine Mustererkennung aus Beschleunigungsdaten Ziel führend ist. Dieses Konzept konnte bereits bei der Schadenserkenkung an Brücken in erfolgreichen österreichischen Projekten getestet werden. Die stabile Anwendbarkeit der bekannten Algorithmen ist zu prüfen und zu entwickeln. Der letzte Schritt ist der Transfer des Algorithmus auf allgemeine Anwendungsfälle von der Globalstruktur bis zum Risikoelement.

Das Ergebnis des Projekts soll als Grundlage für die Entwicklung eines Prototyps für ein Alarmsystem an ÖBB Kunstbauten dienen.

ProjektleiterIn / Unternehmen:

DI Dr. Helmut Wenzel, VCE Holding GmbH

PartnerInnen:

- Universität für Bodenkultur Wien, Institut für Vermessungswesen, Fernerkundung und Landvermessung, DI Dr. Werner Schneider
- Universität Innsbruck, Institut für Grundlagen der Bauingenieurwissenschaften, Arbeitsbereich für Festigkeitslehre Baustatik und Tragwerkslehre, DI Dr. Christoph Adam
- ÖBB Infrastruktur Bau AG, Mag. Karl-Eric Pumper
- APLICA Mess- und Prüftechnik GmbH – Ing. Robert Prethaler
- Arsenal Research, DI Dr. Rainer Flesch

Kontakt:

VIENNA CONSULTING ENGINEERS,
HOLDING GMBH
A-1140 Vienna
Hadikgasse 60
Tel.: +43 1 897 53 39
Fax: +43 1 893 86 71
E-Mail: vce@atnet.at
Web: www.vce.at



DNA-TOX

Methoden zum Schutz kritischer Infrastrukturektoren

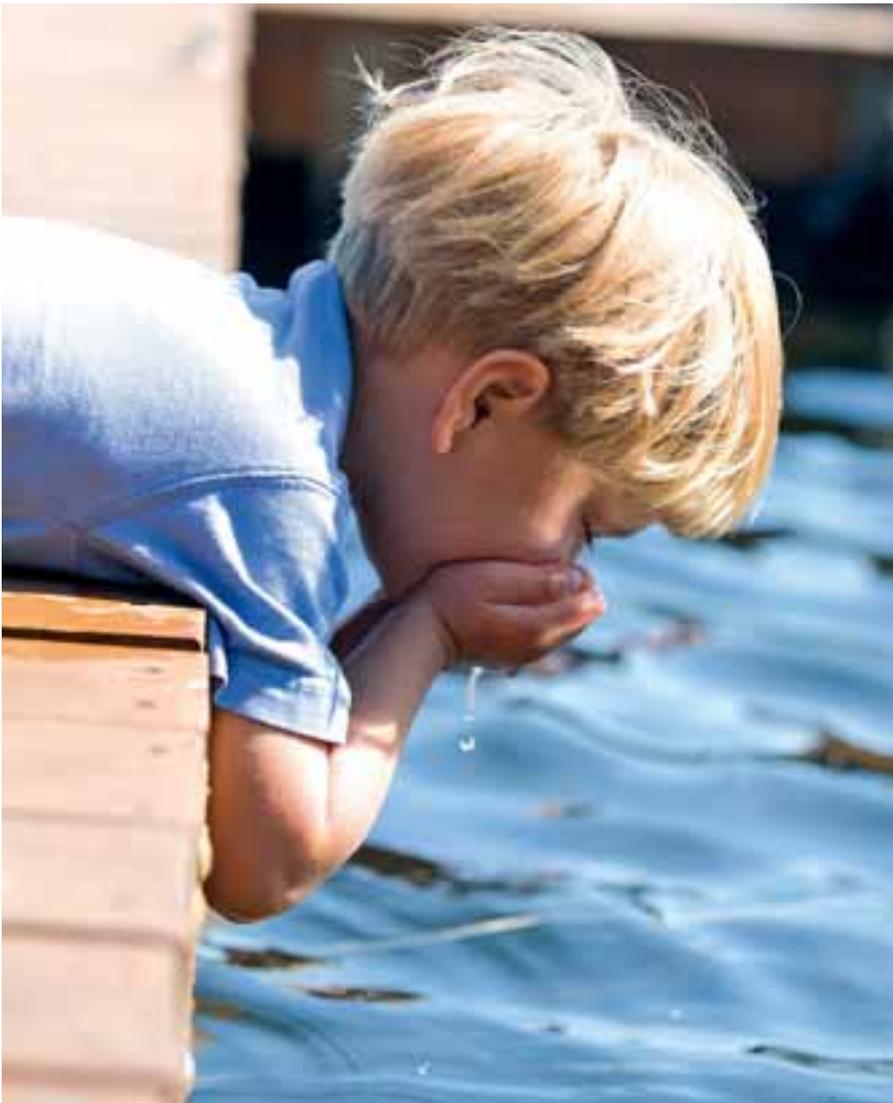
Die Kopplung der Flüssigkeitschromatographie mit der Massenspektrometrie als Werkzeug für die Toxin- und DNA-Analytik.

Infrastrukturen haben in unseren Gesellschaften die Funktion von Lebensadern und stellen daher Angriffsziele für kriminelle Handlungen dar. Die Reduzierung der Verwundbarkeit kritischer Infrastrukturen gegenüber natürlichen Ereignissen und Unfällen sowie gegenüber terroristischen Anschlägen und der Schutz der Bevölkerung vor die-

ser Bedrohung erfordert daher die besondere Aufmerksamkeit der Sicherheitsbehörden.

Im Rahmen des Projekts „dnatox“ sollen neue Methoden zum Schutz der kritischen Infrastrukturektoren „Wasser“ und „Lebensmittel“ und zur Terrorismusbekämpfung entwickelt werden. Es sollen Verfahren etabliert und weiterentwickelt werden, die basierend auf der Kopplung der Flüssigkeitschromatographie mit der Massenspektrometrie (LC-MS) einerseits zur raschen und sicheren

Identifizierung von Toxinen in Wasser und Lebensmitteln und andererseits zur raschen Personenidentifizierung mittels DNA-Profilen dienen. Das technologieorientierte Projekt hat zum Ziel die methodischen Ansätze so weiterzuentwickeln, dass sie in der Routineanalytik Anwendung finden. Im Vorfeld konnte bereits in durchgeführten Machbarkeitsstudien das große Potenzial dieser Techniken gezeigt werden. Die Optimierung der Probenvorbereitung ist für beide Anwendungsbereiche, Toxin-Identifizierung in Wasser und Lebensmitteln und Personenidentifizierung, von großer Bedeutung. Für die toxikologische Analyse müssen effiziente Extraktionsverfahren für die Aufreinigung und Aufkonzentrierung der Toxine erprobt werden. Im Bereich der DNA-Analytik müssen so genannte Multiplex-Polymerasekettenreaktionsansätze entwickelt werden, bei denen selektiv mehrere Loci gleichzeitig vervielfältigt werden. Während das



chromatographische Trennsystem für die effiziente DNA-Analytik bereits besteht, ist eine Entwicklung bzw. Optimierung dessen (monolithische Kapillarsäule, Laufmittel) für die toxikologische Analytik noch zwingend notwendig. Zur effizienten Charakterisierung bzw. Identifizierung von Substanzen und DNA-Sequenzvarianten kommt die „Hochleistungs-Massenspektrometrie“ zur Anwendung. Besonders die Entwicklung einer universell einsetzbaren, zwischen Instrumenten transferierbaren MS/MS-Spektrenbibliothek von toxikologischen Substanzen würde einen Meilenstein im Bereich der massenspektrometrischen Identifizierung von chemischen Verbindungen darstellen.

Eine besondere Bedeutung kommt der EDV-technischen Verarbeitung der massenspektrometrischen Daten zu. Im Rahmen des Projektes soll ein Softwarepaket erstellt werden, das es ermöglicht, auf einfache Art und Weise ein Spektrum mit einer Referenzdatenbank abzugleichen. Dem Endanwender soll sowohl ein spezifisches Programm, das möglichst transparent in die vorgegebene Auswertesoftware integriert wird, als auch ein generisches Webinterface zur Verfügung gestellt werden. Eine ebenfalls zu erstellende Serverapplikation übernimmt dann den Abgleich des Spektrums mit einerseits einer im Projektverlauf erstellten, zentralen Toxin-Referenzdatenbank zur Identifizierung von Substanzen, andererseits mit verschiedenen, vom Endanwender definierten Markersets zur Gewinnung eines DNA-Profiles.

Die rasche und sichere Identifizierung des „Unbekannten mit Gefährdungspotenzial“ (z.B. Gifte in Trinkwasser und Lebensmitteln; Verbrecher) ist von großer sicherheitspolitischer Bedeutung, denn nur dadurch kann sichergestellt werden, dass dessen schädliche Auswirkungen auf einzelne Personen bzw. auf die gesamte Gesellschaft frühzeitig unterbunden werden können. Beide Verfahren haben daher großes Potenzial, eine Steigerung der objektiven inneren Sicherheit zu bewirken und somit auch eine Steigerung des

subjektiven Sicherheitsempfindens in der Bevölkerung. Das Projekt kann einen enormen Mehrwert an Sicherheit generieren, da potenzielle künftige Anwender der zu entwickelnden Technologien, Umweltbundesamt GmbH und Bundesministerium für Inneres, von Beginn an am FuE-Prozess beteiligt sind und die Anforderungen der öffentlichen Bedarfsträger somit berücksichtigt werden können.

ProjektleiterIn / Unternehmen:

Institut für Gerichtliche Medizin der Medizinischen Universität Innsbruck, Prof. Dr. Richard Scheithauer, Institutsdirektor

PartnerInnen:

- Iplex IT Solutions KG, Ing. Martin Pircher, Innsbruck
- CEMIT Center of Excellence in Medicine and IT Dipl.Inf. Patricia Schirmer, Innsbruck
- Umweltbundesamt GmbH, Gerhard Thanner, Wien
- Bundesministerium für Inneres, Bundeskriminalamt, Dr. Reinhard Schmid, Wien
- Applera Austria Handels GmbH, Dr. Karin Wihsböck, Brunn am Gebirge
- Medizinische Universität Innsbruck, Institut für Gerichtliche Medizin, Müllerstrasse 44, 6020 Innsbruck, Tel.: +43 512 9003-70600
Fax: +43 512 9003-73600
Ansprechperson:
Prof. Dr. Richard Scheithauer
E-Mail: richard.scheithauer@i-med.ac.at
Web: www.gerichtsmedizin.at

Kontakt:

CEMIT Center of Excellence in Medicine and IT
Leopoldstrasse 1
6020 Innsbruck
Dipl.Inf. Patricia Schirmer
Programm- und Projektmanagement
Tel.: +43 512 576523-233
Fax: +43 512 576523-301
E-Mail: patricia.schirmer@cemit.at
Web: www.cemit.at



emc2

emergency mission control center

Informationsmanagement für Feuerwehreinsätze

Wie effizient die Feuerwehr ihre Einsatztaktik planen kann hängt sehr davon ab, in welcher Art und Qualität die richtigen Informationen verfügbar sind. Und zwar dort, wo die ersten Entscheidungen getroffen werden, direkt vor Ort bei der Einsatzleitung. Ein umfassendes Informationsmanagement, das die erforderlichen, zueinander sehr inhomogenen und großteils noch analogen, Daten zusammen fasst und in digitaler Form kontext-sensitiv dorthin bringt wo sie benötigt werden, ist das Ziel des Forschungsprojektes.

Die richtige Information zur richtigen Zeit am richtigen Ort zu haben ist somit ein ganz wesentlicher Faktor, damit Feuerwehreinsätze optimal ablaufen und Beschädigungen an einer betroffenen Infrastruktur vermieden werden. Auch die Wiederherstellung eines ordentlichen Betriebes dieser Infrastruktur hängt ganz wesentlich davon ab, auf welchen Informationen die Entscheidungen während einem Notfall-Einsatz beruhen.

Heute ist es so, dass in den Einsatzleitzentralen eine enorme Menge an Daten und Informationen vorhanden ist. In analoger und digitaler Form werden dort Daten in unterschiedlichsten Medienformaten gespeichert. Das gegenständliche F&E-Projekt möchte diese Daten dorthin bringen wo sie benötigt werden, zum Entscheidungsträger vor Ort, dem Einsatzleiter. Das F&E-Projekt nimmt sich darüber hinaus auch der Aufgabe an, einen Kulturwandel in der Arbeit der Feuerwehren nicht nur einzuleiten, sondern auch langfristig zu begleiten: zu mehr Mobilität des Wissens! Der Kulturwandel betrifft also die „Verlagerung des Zugriffes auf Informationen von der Einsatzleitzentrale an die Front“. Durch die Integration moderner Telekommunikationsmedien ist es dabei unwesentlich, wo die Daten physisch gespeichert werden bzw. über welche Schnittstellen sie empfangen werden. Dieser Kulturwandel wird auch in der Bevölkerung Auswirkungen haben. Nämlich in einem wachsenden Bewusstsein, dass jeder Notfall-Einsatz erfolgreicher, schneller und weniger destruktiv sein wird,

je besser die Informationen von einem Ernstfall aufbereitet werden. Ein Ansatz des Projektes ist deshalb auch, eine breite Akzeptanz dafür zu schaffen, dass die Einsatzkräfte den Zugriff auf bestmögliche Informationen brauchen. Dabei soll vor allem versucht werden, den mittelbaren und unmittelbaren Nutzen für die Gesellschaft zu evaluieren und entsprechend darzustellen.

Das Projektkonsortium bietet in seiner Zusammenstellung das Potenzial, dass das Problem des Informationsmanagements für Feuerwehren in einer umfassenden Problemstellung analysiert, bewertet und auf völlig neue Standbeine gestellt wird. In der Gegenwart stellt sich die Situation so dar, dass viele einzelne Lösungen (die meist auch noch sehr historisch belastete und technikgetriebene Ansätze verfolgen) existieren, die eine in sich abgeschlossene Teilaufgabe bedienen. Die Aufbereitung und der Umgang mit Informationen in einem umfassenden, strategischen und problemorientierten Fokus benötigt ein Projektteam, in welchem alle erforderlichen Exzellenzen entweder vorhanden sind, oder darauf aufbauend neu erzeugt werden. Das ist bisher nicht gelungen, durch die Zusammenstellung des Projektkonsortiums aber sichergestellt.

ProjektleiterIn / Unternehmen:

ROSENBAUER International AG

PartnerInnen:

- FH OÖ Forschungs & Entwicklungs GmbH
- mobilkom austria AG
- Österreichischer Bundesfeuerwehrverband
- SIEMENS IT Solutions and Services GmbH

Kontakt:

ROSENBAUER International AG

Ing. Gerhard Großberger

Leiter Telematik

Paschinger Straße 90, 4060 Leonding

Tel.: +43 732 6794-616

Fax: +43 732 6794-94616

E-Mail: gerhard.grossberger@rosenbauer.com

Web: www.rosenbauer.com

FEIS

Failure Experience Improvement System

Projekt zur Risikominimierung am Beispiel der kritischen Infrastruktur Trinkwasser

Ausgangslage: Fehler in der Wasserversorgung haben nicht nur Auswirkungen auf das System der Wasserversorger (betriebsinterne Prozesse, usw.), sondern auch auf die zu versorgende Bevölkerung (Brandbekämpfung, Hygiene bzw. Abwasserentsorgung, Ausfall von landwirtschaftlichen und industriellen Produktionsprozessen). In vielen Infrastrukturen gibt es ein noch nicht ausgeschöpftes Fehlervermeidungspotenzial, das mit Hilfe dieses Projektes nutzbar gemacht wird. In vernetzten Systemen, wie z.B. der Wasserversorgung, weist das lineare Fehlermodell naturgemäß eine eingeschränkte Gültigkeit auf, vernetzte Systeme, können mit Vereinfachungen nicht befriedigend erklärt werden. Daher spricht man in diesem Zusammenhang von multiplexen oder mehrdimensionalen komplexen Systemen.

Ziele: Das Hauptziel des Projektes ist die Entwicklung einer Datenbank mit integrierter Analysemöglichkeit (FEISTool, Failure Experience Improvement System), in der die Fehler des Unternehmens aufgenommen, kategorisiert, analysiert und mit einer entsprechenden Arbeitsanweisung versehen werden. Diese permanente Fehlerminimierung führt zu einer Erhöhung der Sicherheit der kritischen Infrastruktur Wasser (Risikominimierung, Versorgungssicherheit, Krisen- und Katastrophenprävention). Durch die einfache Duplizierbarkeit der entwickelten komplexen und integrativen Netzwerkstrukturanalyse des FEIS-Tools auf andere Infrastrukturbereiche (z.B. Energie, Finanzen, Verkehr usw.) entsteht ein nachhaltiger Mehrwert für die Sicherheit Österreichs und seiner Bevölkerung.

Erwarteter Nutzen durch das Projekt: Aufgrund der Analysemöglichkeit der Fehlernetzwerke werden die kausalen Zusammenhänge aufgedeckt und eliminiert. Dadurch werden einerseits die Eintrittswahrscheinlichkeiten bzw. die Auswirkungen und Schäden minimiert. Für das Krisenmanage-

ment und die Risikokommunikation bedeutet das, dass der Bedarfsträger auf bisherige Erfahrungen im Krisenmanagement zurückgreift, und sofort die Auswirkungen der Maßnahmen im eigenen System sieht. Dieses Projekt ist so aufgebaut und geplant, dass das FEIS-Tool in der Kiras Programmlinie 3 zur Marktreife weiterentwickelt wird.

ProjektleiterIn / Unternehmen:

Universität für Bodenkultur Wien, Department für Wasser, Atmosphäre und Umwelt, Institut für Siedlungswasserbau, Industrierwasserwirtschaft und Gewässerschutz

Partner

FAS.Research

Kontakt:

Dr. Reinhard PERFLER
Universität für Bodenkultur Wien, Department für Wasser, Atmosphäre und Umwelt, Institut für Siedlungswasserbau, Industrierwasserwirtschaft und Gewässerschutz
Muthgasse 18
1190 Wien
Tel.: +43 1 36006 5808
E-Mail: reinhard.perfler@boku.ac.at





FUNCL-DEMO

Functional clothing für Einsatzkräfte – Entwicklung flexibler multifunktionaler Demonstratoren

Im Projekt soll Einsatzkleidung für Katastrophenbekämpfung insbesondere hinsichtlich dreier technischer Funktionalitäten am Demonstrator verbessert werden: Gassensorik, Leuchten und Positionierung.

„Functional Clothing“ als Integration elektronischer Funktionen in Bekleidungsprodukte eröffnet als Forschungsfeld in den letzten Jahren die Möglichkeit, eine Reihe neuer Funktionalitäten, auch im Sicherheitsbereich, und hier vor allem für Einsatzkräfte in der Bekämpfung von Bedrohung und der Beseitigung von Katastrophen, zu entwickeln. Verfügbare Prototypen technischer Funktionalität auf dem Textil erlauben durch weitere Entwicklungsarbeit eine Demonstration und Erprobung nach den grundlegenden textilen Anforderungen an Bekleidung und den spezifischen Funktionalitäten aus den Anforderungsprofilen der First User BMLV und BMI.

Generelle Zielsetzung des Projekts ist die Optimierung von Labor-Prototypen für einen Praxiseinsatz unter realen Bedingungen. Dafür werden Demonstratoren in ausreichender Stückzahl konfektioniert. Die innige Verknüpfung der „harten“ Mikroelektronik mit der „weichen“ Textiltechnologie, die über das bisherige bloße Applizieren hinausgeht, erfordert industrielle Forschung hinsichtlich weiterer Miniaturisierung und Flexibilisierung auf der einen Seite und der Dauerhaftigkeit dieser Verbindung durch konfektionstechnische Belastungsminimierung auf der anderen Seite.

An den Demonstratoren wird die Interdependenz der elektronischen Komponenten mit den textiltechnologischen Prüfkriterien (Konfektionierbarkeit, Haltbarkeit, Reinigbarkeit, Bekleidungsphysiologie, Tragekomfort, Schadstofffreisetzung, etc.) untersucht. Die Erprobung der Demonstratoren im Feldversuch soll einerseits unter technischen Gesichtspunkten und andererseits unter besonderer Berücksichtigung der GSK Aspekte erfolgen.

Eine künstliche Nase als integrierter Sensor in der Einsatzkleidung erlaubt eine Frühwarnung ohne Behinderung der Mannschaft vor Gas (Brandgase, Sickergase, CO₂). Im Vorhaben muss dieser Sensor insbesondere für eine gefahrenabhängige Positionierung in Größe, Fixierbarkeit und Strombedarf optimiert werden.

Zielsetzung der Optimierung des eingebauten Ortungssystems ist es, die Kommunikation einer größeren Zahl von Einheiten unter Einsatzbedingungen mit einer Leitstelle sicherzustellen. Zusätzlich sollen integrierte Sensoren in der Lage sein, der Leitstelle auch Informationen über den Gesundheitszustand zu liefern. Dazu ist eine Softwareentwicklung zur gleichzeitigen Visualisierung und Koordinierung vieler Einheiten erforderlich.

Bei der geplanten Weiterentwicklung der Funktion Leuchten sollen zwei ähnliche Anforderungen mit divergierenden Rahmenkriterien vereint werden. Einerseits ist hohe aktive Sichtbarkeit bei Nachteinsätzen angestrebt, andererseits soll eine – allfällig wechselnde – Aufgabenstellung eines Mannes für alle Teammitglieder und auch für die betreuten Katastrophenopfer sichtbar sein. Für beides gibt es grundsätzlich kommerzielle Technologien, die jedoch für eine haltbare und bekleidungstechnisch vertretbare Integration noch angepasst und optimiert werden müssen.

Dabei kommt den Fragen der Energiebereitstellung und des Energietransports besondere Bedeutung zu, da der Tragekomfort und die Belastbarkeit des Kleidungsstücks weiterhin gewährleistet sein müssen. Dies kann unter anderem durch Fasermetallisierungen bzw. Metallbedruckungen erreicht werden.

Ergebnis des Projektes werden drei entscheidend verbesserte Demonstratoren und eine Empfehlungsliste sein, in der weitere für die Markteinführung notwendige Maßnahmen aufgezeigt werden.

ProjektleiterIn / Unternehmen:

Andrea Häußermann
ÖTI- Institut für Ökologie, Technik und Innovation
Spengergasse 20
1050 Wien

PartnerInnen:

- Bundesministerium für Inneres, Postfach 100, 1014 Wien, rechtsverbindlich vertreten durch Brig. Reinhard Schnakl
- Bundesministerium für Landesverteidigung Franz Josef Kai 7-9, 1010 Wien, rechtsverbindlich vertreten durch Brig. Obers. Klemens Hofmeister
- Integrated Microsystems Austria GmbH (IMA) Viktor Kaplan Straße 2/1, 2700 Wiener Neustadt
- Jarosch & Hass GesmbH, Guglgasse 8/2/12/95 Gasometer B, 1110 Wien

- Mobile Computing Solutions GesmbH (MCSA) Guglgasse 8/4/12/74, 1110 Wien
- MOONDIAL Innovation & Design Group GmbH Schottenfeldgasse 50/10, 1070 Wien
- PLATINGTECH Beschichtung GmbH & Co KG Parking 2, 8712 Niklasdorf
- SORA Institute for Social Research and Analysis Linke Wienzeile 246, 1150 Wien

Kontakt:

ÖTI- Institut für Ökologie, Technik und Innovation
Geschäftsbereich Innovation
Spengergasse 20, 1050 Wien
Andrea Häußermann
Tel.: +43 1 544 25 43-53
Fax: +43 1 544 25 43-10
Mobil: +43 699 17060170
E-Mail: haeussermann@oeti.at
Web: www.oeti.at



GEDES

Gefährdung durch Deponien und Altablagerungen

Gefährdung durch Deponien und Altablagerungen im Hochwasserfall – Risikoanalyse und Minimierung.

Deponien und Altablagerungen beinhalten ein großes Gefährdungspotenzial für Mensch und Umwelt. In Österreich lagern auf Deponien rund 50 Millionen Tonnen Hausmüll. Während der Regelbetrieb von Deponien und die dabei auftretenden Emissionen gut dokumentiert bzw. abschätzbar sind, ist das Verhalten von Deponien im Fall einer Überflutung weitestgehend unbekannt. Zahlreiche Studien belegen, dass die Umweltgefährdung, die von konventionellen Hausmülldeponien ausgeht, über Jahrhunderte andauert. Hauptverantwortlich dafür ist das große Inventar an abgelagerten Stoffen, das wegen der ausgeprägten Heterogenität der Wasserströmung in Deponien nur sehr langsam (über Jahrhunderte) abgebaut wird. Im Überschwemmungsfall ist davon auszugehen, dass sich die hydraulischen Verhältnisse drastisch ändern und es dadurch zu einer Mobilisierung des großen Schadstoffpotenzials kommt. Außerdem kann die Wassersättigung des Deponiekörpers Standsicherheitsprobleme nach sich ziehen, was zu Scher- und Gleitbrüchen mit Massenbewegungen ähnlich derer bei Hangrutschungen führen kann. Alle bisherigen Forschungsarbeiten zum Thema Deponien beschränkten sich aber auf den Regelbetrieb und ließen Ausnahmestände wie Überschwemmungen außer Acht. In Anbetracht der sehr langen Aufenthaltsdauer von Deponien in der Umwelt, ist das Auftreten eines Hochwassers in dieser Zeit aber durchaus wahrscheinlich, speziell unter dem Aspekt zukünftig geänderter klimatischer Verhältnisse. Das Ziel dieses Projektes ist es daher, das Verhalten von Deponien und Altablagerungen bei vollständiger Wassersättigung zu erforschen und Grundlagen für ein gesichertes Risikomanagement im Hochwasserfall zu erstellen.

Folgende Fragestellungen sollen im Zuge dieses Forschungsprojektes untersucht werden:

1. Wie viele Deponien und relevante Altablagerungen sind in Österreich mittel- bis langfristig als überschwemmungsgefährdet anzusehen?
2. Wie verändert sich der Wasser- und Stoffhaushalt von Deponien im Falle einer Überschwemmung?
3. Welche Konsequenzen hat das für den Deponiekörper, insbesondere für dessen Standfestigkeit und die flüssigen und gasförmigen Emissionen?
4. Welche Immissionen sind für die Schutzgüter Boden und Grundwasser im Schadensfall zu erwarten und wie sind diese zu bewerten?
5. Mit welchen technischen und organisatorischen Maßnahmen können negative Einflüsse auf Mensch und Umwelt rechtzeitig erkannt und behoben bzw. diesen vorgebeugt oder diese abgeschwächt werden?



6. Wie können die erwarteten monetären Schäden versicherungsmathematisch abgeschätzt und die potenziellen Risiken quantifiziert werden?

Das Projekt wird in fünf Phasen durchgeführt.

Im 1. Schritt wird das Potenzial an Deponien und relevanten Altablagerungen hausmüllähnlicher Zusammensetzung in Österreich erhoben, welches langfristig überschwemmungsgefährdet ist. Als Grundlage dazu dienen bestehende Gefahrenzonenpläne, Hochwasserabflusssimulationen, Informationen über die Standorte von Deponien und Altablagerungen sowie deren Schadstoffpotenzial.

In der 2. Phase werden anhand von Labor- und Feldversuchen an realen Deponien die Auswirkungen einer raschen Wassersättigung auf das Emissionsverhalten und die Standsicherheit des Abfalls untersucht.

Parallel dazu wird im 3. Schritt ein bestehendes mathematisches Deponiemodell für die Simulation der Fälle einer vollständigen und partiellen Wassersättigung adaptiert. Dieses Modell dient zukünftig zur Simulation verschiedenster Überflutungsszenarien.

Basierend auf den Resultaten der Labor- und Feldversuche sowie der numerischen Deponiemodellierung, werden im 4. Schritt die Auswirkungen auf die Schützgüter Boden und Grundwasser untersucht.

Abschließend werden die Resultate aus den ersten vier Phasen zusammengeführt, um die mit der Überschwemmung von Deponien verbundenen Risiken abschätzen und versicherungsmathematisch bewerten zu können, sowie um Strategien und Maßnahmen wie Notfallpläne zur Minimierung negativer Auswirkungen zu entwickeln. Darüber hinaus sollen Empfehlungen für den Bau neuer Deponien gegeben werden.

Die zu erwartenden Ergebnisse des Projektes sind:

1. Erkenntnisse und Ansätze um Überschwemmungen von Deponien bzw. Altlasten zu bewerten, die Risiken abzuschätzen und einzustufen.

2. Technische und organisatorische Empfehlungen für die Bewältigung des Problems im Überschwemmungsfall.

3. Aussagen über das langfristige Verhalten einer überschwemmten Deponie bzw. Altablagerung.

4. Handlungsanweisungen für die Planung, den Bau und Betrieb von neuen Deponien unter Berücksichtigung des Überschwemmungsfalles.

5. Grundlagen für Versicherungskonzepte für Deponien und Altablagerungen.

ProjektleiterIn / Unternehmen:

Univ. Ass. DI Dr. Johann Fellner

Technische Universität Wien

Institut für Wassergüte, Ressourcenmanagement und Abfallwirtschaft

PartnerInnen:

■ Univ. Prof. DI Dr. Hans-Peter Nachtnebel
Universität für Bodenkultur, Institut für Wasserwirtschaft, Hydrologie und konstruktiven Wasserbau

■ Mag. Christian Kolesar, Umweltbundesamt
Abteilung Altlasten

■ Dipl.-Ing. Dr. Fritz Reichel, Amt der Niederösterreichischen Landesregierung, Abteilung Wasserwirtschaft

■ Dr. Wolfgang Lantschbauer, Amt der Oberösterreichischen Landesregierung, Abteilung Umwelt- und Anlagentechnik

■ Univ. Prof. DI Dr. Uwe Schmock, Technische Universität Wien, Institut für Wirtschaftsmathematik

Kontakt:

Univ. Ass. DI Dr. Johann Fellner

Technische Universität Wien

Institut für Wassergüte,

Ressourcenmanagement

und Abfallwirtschaft

Karlsplatz 13/226

1040 Wien

Tel.: +43 1 58801-22654

Fax: +43 1 50422-34

E-Mail: j.fellner@iwa.tuwien.ac.at

Web: www.iwa.tuwien.ac.at



iObserve

Intelligente Videoüberwachung der nächsten Generation mit semantischen Templates

Videobasierte Überwachungssysteme sind in der Regel nicht in der Lage, das subjektive Sicherheitsempfinden der Bevölkerung zu steigern. Eine der Hauptursachen ist darin zu suchen, dass gegenwärtige Anlagen noch nicht intelligent genug sind, um als Supportsysteme für Behörden und Sicherheitspersonal in Echtzeit auf sicherheitsrelevante Ereignisse reagieren zu können. Vielmehr wird die immer vorhandene Aufzeichnungsfunktion verwendet, um nach einem Ereignis mögliche Auslöser, Sachverhalte etc. zu recherchieren.

Das Projekt iObserve hat sich zum Ziel gesetzt, die Basis für videobasierte Überwachungssysteme der nächsten Generation zu schaffen. Solche Systeme sollen in der Lage sein, detektierte Einzelereignisse auf einer semantischen Ebene zu Sachverhal-

ten komplexerer Bedeutung zusammen zu setzen um so eine höhere Ebene des Verständnisses einer potenziellen sicherheitsrelevanten Situation zu erhalten. Einen wichtigen Aspekt in solch einem System stellt dessen Bedienbarkeit und Konfigurierbarkeit dar. Die rapide steigende Systemkomplexität muss für den Benutzer in verständliche ‚Aktionen‘ übersetzt werden. Es ist die Frage zu klären bzw. zu erforschen, wie semantische Inhalte in Videos (‚eine Person legt einen großen Gegenstand in einen Papierkorb‘) mittels Benutzeroberflächen, auch für Laien verständlich, konfiguriert werden können. Der Benutzer muss für die Systemkonfiguration in die Lage versetzt werden, mit ‚Inhalten‘ effizient umzugehen.

Detektionsalgorithmen für Objekte, insbesondere Personen, Fahrzeuge und kofferähnliche Ob-



jekte, bilden die ‚Low-Level‘-Ebene des Systems. Die bei den Projektpartnern dafür bereits vorhandenen Detektionsalgorithmen werden einer gründlichen Bewertung unterzogen und auf ihre Tauglichkeit in Hinblick auf einen Einsatz im geplanten System getestet. Gegebenenfalls werden geeignete Module verbessert und angepasst.

Die „High-Level“-Ebene des Systems hat die Aufgabe, alle Informationen aus der Detektionsebene zu filtern, Statistiken zu berechnen und schlussendlich zu interpretieren. Als Schnittstelle zwischen beiden Ebenen dient ein Interpretationsmodul, welches die Low-Level-Information in semantische Informationen übersetzt. Dies geschieht durch Mustererkennung in einer Menge von (benutzer-)definierten Ereigniskriterien (beispielsweise Bewegungsmuster) und durch laufende statistische Analyse.



Die semantische Ebene ist damit in der Lage, Detektionen zu kombinieren und als Ereignisse mit neuem bzw. erweitertem Inhalt zu interpretieren. Aus dieser Interpretation kann im übertragenen Sinn eine primitive Sprache abgeleitet werden, die als interne Repräsentation von Ereignissen spezifiziert wird. Die Elemente dieser Sprache – so genannte semantische Templates – entsprechen Worten beziehungsweise Phrasen in einer klassischen Sprache. Sie dient als Vermittler zwischen den Aktionen auf der Benutzeroberfläche und den Ereignisdetektionen aus der Bildverarbeitung.

Die prinzipielle Funktion des Gesamtsystems wird im Rahmen der Installation eines Evaluierungsprototypen beim Bedarfsträger erprobt. Von Anfang an wird hoher Wert auf die Praktikabilität und Nützlichkeit für den Endbenutzer gelegt. Durch die enge Zusammenarbeit mit dem Bedarfsträger ist gewährleistet, dass die Entwicklung des Systems aktuellsten Sicherheitsanforderungen entspricht und mittelfristig in ein Industriesystem umgesetzt werden kann.

ProjektleiterIn / Unternehmen:

DI Martin Forster, Center Communication Systems GmbH, Abteilung Development Image Processing

PartnerInnen:

JOANNEUM RESEARCH Forschungsgesellschaft mbH, Institut für Informationssysteme & Informationsmanagement
Web: <http://www.joanneum.at/iis>

Kontakt:

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



iObserve NG

Verteilte Videoüberwachung in einer hochskalierbaren service-orientierten Architektur

Mit heutiger Technologie ist es möglich, Netzwerke bestehend aus tausenden Kameras aufzubauen. Mit herkömmlichen Systemarchitekturen ist es jedoch nicht möglich die notwendige Skalierbarkeit für ausgedehnte, intelligente Überwachungsnetzwerke zu erreichen.

Das Paradigma der verteilten Systeme hat in seiner Ausprägung der service-orientierten Architekturen in den letzten Jahren vor allem im Enterprise Computing große Popularität und Verbreitung gefunden.

Ziel des Projektes iObserve NG ist es die Prinzipien einer service-orientierten Architektur auf die verteilte, intelligente Videoüberwachung anzuwenden, um hochskalierbare, intelligente Videoüberwachungsanlagen zu realisieren. Mit der Umsetzung von Diensten („Services“) zur semantischen Interpretation von Videoinhalten und vollautomatischen Kalibrierung von Kameras werden modernste Entwicklungen der Videodetektion im Gesamtsystem integriert.



Aspekte der Skalierbarkeit, Integration, Datensicherheit, Verfügbarkeit, Erweiterbarkeit und Handhabbarkeit werden in der Systemarchitektur berücksichtigt und sind im praktischen Betrieb zu untersuchen und zu bewerten.

Definierte und offengelegte Schnittstellen nach innen und nach außen stellen sicher, dass in Zukunft auch Sensoren anderer Modalitäten (z.B. Audio oder Wärmebildtechnik) integriert und eingesetzt werden können, beziehungsweise mit Systemen anderer Betreiber interagiert werden kann. Die Integration zusätzlicher Komponenten erfolgt natürlich unabhängig vom physischen Medium der Anbindung.

Die Einsatztauglichkeit wird im Rahmen eines Testbetriebs validiert. Von Anfang an wird hoher Wert auf die Praktikabilität und Nützlichkeit für den Endbenutzer gelegt. Durch die enge Zusammenarbeit mit dem Bedarfsträger ist gewährleistet, dass die Entwicklung des Systems aktuellsten Sicherheitsanforderungen entspricht und in ein Industriesystem umgesetzt werden kann.

ProjektleiterIn / Unternehmen:

Center Communication Systems GmbH

PartnerInnen:

- JOANNEUM RESEARCH ForschungsgesmbH
- TU Wien
- BMI

Kontakt:

DI Martin Forster
Center Communication Systems GmbH
Ignaz-Köck-Straße 19
1210 Wien
Tel.: +43 1 90199-1304
Fax: +43 1 90199 -19
Mobil: +43 664 2341156
E-Mail: m.forster@centersystems.com
Web: www.centersystems.com

MDL

Multimedia Documentation Lab

Das MDL ist der Demonstrator eines Dokumentations- und Analysesystems für Multimediacontent. Es wird erstmals die Möglichkeit der Einbindung multimedialer Inhalte in die Analyse von sicherheitsrelevanten Themenbereichen wissenschaftlich erforscht und prototypisch umgesetzt. Es wird ein Architekturmodell entwickelt, dessen Ziel die musterhafte Umsetzung eines Systemprototyps bei den Endanwendern des Bedarfsträgers (Zentraldokumentation) ist.

Bislang konnte nationaler und internationaler Bild-, Ton- und Multimediacontent nicht oder nur unzureichend zu Analyse Zwecken herangezogen werden. Nun wird im Rahmen der österreichischen Sicherheitsforschung erstmals die Möglichkeit der Einbindung solcher multimedialen Inhalte erforscht.

Somit wird es möglich sein, neben Textdokumenten auch sicherheitsrelevante multimediale Inhalte nach neuesten Erkenntnissen zu durchsuchen und analysiefähig aufzubereiten. Unter Verwendung modernster Technologien und rezenter Forschungsergebnisse der Projektmitglieder aus Industrie und Wissenschaft sowie Erfahrungen des öffentlichen Bedarfsträgers, sollen multimediale Informationsquellen in unterschiedlichen Sprachen nutzbar gemacht werden. Die jederzeit wieder auffindbaren Inhalte dienen neben der sofortigen Kommunikationsmöglichkeit auch als Grundlage für die Erstellung von Trendanalysen und Lagebildern.

Der Gegenstand des Projektes MDL ist die Entwicklung und prototypische Umsetzung eines Demonstrators, der zielgerechte Suche und Analysen in Multimediacontent ermöglicht. Dazu müssen begleitend Terminologien und Ontologien sowie Retrieval- und Analysefunktionalitäten entwickelt werden.

Das MDL wird in die Infrastruktur des Bedarfsträgers integriert und wird in Zukunft das Problemlösungsspektrum der bereits vorhandenen Systeme ergänzen und erweitern. Diese Art der Einbin-

dung garantiert eine praxisnahe Anwendung der Ergebnisse und stellt ein Muster für andere Bedarfsträger dar. Ziel des Projektes ist es, multimediale Informationsquellen so nutzbar zu machen, dass diese in vorhandene Systeme bei dem Bedarfsträger eingebunden und bei Bedarf sofort („on demand“) durchsucht werden können.

Das System soll insbesondere in Krisensituationen Experten bei der Generierung eines realistischen und qualitativ hochwertigen Lagebildes unterstützen und als Kommunikationsmittel mit der Bevölkerung dienen. Somit erfüllt das Projekt eines der Hauptziele von KIRAS, nämlich die Sicherheit und das Sicherheitsbewusstsein der österreichischen Bevölkerung zu erhöhen.

Mögliche Einsatzszenarien sind:

- zivile Katastrophen
- wirtschaftliche Krisen
- andere sicherheitsrelevante Szenarien (etwa Großereignisse oder Versorgungsengpässe).

ProjektleiterIn / Unternehmen:

Sail Labs Technology AG

PartnerInnen:

- Landesverteidigungsakademie, ZentDok, Ing. Mag. Klaus Mak, ObstdhmfD
- Universität Wien, Fakultät für Informatik, Institut für Distributed and Multimedia Systems, Institut für Scientific Computing Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr
- Technische Universität Graz, Institut für maschinelles Sehen und Darstellen, Univ.-Prof. DI. Dr. Horst Bischof

Kontakt:

Sail Labs Technology AG
Mag. Dorothea Aniola
Mariannengasse 14
1090 Wien

Tel.: +43 1 58095-621

Fax: +43 1 58095-580

E-Mail: dorothea.aniola@sail-technology.com

Web: www.sail-technology.com



PUKIN

Periodische Überwachung kritischer Infrastrukturen

Entwicklung eines leistungsfähigen, preiswerten, modular aufgebauten und für viele Anwendungen nutzbaren luftgestützten Überwachungssystems zur Erfassung und Bewertung von Krisensituationen.

Die Infrastrukturen eines Landes (Verkehr, Versorgung, Kommunikation) stellen das Rückgrat einer jeden funktionierenden Volkswirtschaft dar. Werden diese Infrastrukturen nachhaltig außer Kraft gesetzt, brechen die geordneten und optimierten Prozesse einer Volkswirtschaft innerhalb kürzester Zeit zusammen. Dies kann durch Naturgewalten, menschliche Fahrlässigkeit (Aspekt Sicherheit - Safety) aber auch durch terroristische Anschläge (Aspekt Sicherheit - Security) geschehen. Wegen ihres vernetzten Wesens wird ein wie auch immer

gearteter Ausfall dieser Art von sicherheitskritischen Infrastrukturen immer zu einer starken Beeinträchtigung der Volkswirtschaft, den damit verbundenen hohen, wirtschaftlichen Schaden und eventuell zu nachhaltiger gesellschaftlicher Verunsicherung führen.

Während lokale Infrastruktureinrichtungen wie Verkehrsknotenpunkte, Kraftwerke, Staudämme etc. mit traditionellen Verfahren überwacht werden können, sind die zugehörigen Infrastrukturnetze wegen ihrer großen, räumlichen Ausdehnung weitgehend ungeschützt. Ziel einer periodischen Überwachung von kritischen Infrastrukturen ist es, bereits im Vorfeld die aktuelle Situation der Infrastruktur durch regelmäßige Observierung zu erfassen. Weiters ist es wichtig, im Schadens-



fall durch Bereitstellung aktueller Informationen die Erfassung der Krisensituation und das damit verbundene Krisenmanagement aktiv zu unterstützen.

Nur aus der Luft ist man in der Lage schnell und effizient Infrastrukturen weiträumig zu erfassen. Im Rahmen des PUKIN-Projektes soll deshalb die Leistungsfähigkeit luftgestützter Überwachungsverfahren (Erkennen von Bedrohungspotenzialen/ Erfassung von Krisensituationen zu akzeptablen Kosten) für kritische Infrastrukturen analysiert und demonstriert werden. Außerdem gilt es zu zeigen, wie die gewonnene Information an die Bedarfsträger weitergegeben wird bzw. wie die Bedarfsträger Einfluss auf die Durchführung der Beobachtungsmission nehmen können.

ERWARTETE ERGEBNISSE

Es wird prototypisch eine multisensorielle Überwachungsnutzlast entwickelt, deren Leistungsfähigkeit durch die Durchführung von repräsentativen Demonstrationsflügen validiert wird. Im Einzelnen werden folgende Ergebnisse erzielt: Entwicklung eines multispektralen Sensorikkonzeptes für die luftgestützte Infrastrukturüberwachung, Prototypische Realisierung der multispektralen Sensorik.

- Realisierung der notwendigen On-Board-Datenvorverarbeitungsverfahren, insbesondere zur Kompression der umfangreichen Bilddaten
- Prototypische Realisierung einer infrastrukturunabhängigen Datenkommunikation zwischen Beobachtungsplattform und Bodenkontrollstation
- Prototypische Realisierung der für die Überwachungsvorhaben notwendigen geometrischen Prozessierungsverfahren der aufgenommenen Bilddaten, welche im Wesentlichen die Geokodierung, die weiterführende Vorverarbeitung sowie Change Detection-Verfahren beinhalten
- Integration der multispektrale Sensorik in die Sensorplattform DA 42

- Durchführung von Evaluierungsflügen mit der Sensorplattform DA42
- Analyse charakteristischer Signaturen unter Berücksichtigung der verfügbaren Sensor-Spektralbereiche.
- Prototypische Realisierung von Algorithmen zur Ableitung von Indikatoren für Gefahren, welche weiterführend zur Erkennung von Bedrohungen bzw. Erfassung von Krisensituationen dienen
- Validierung des Verfahrens und Bestimmung der Zuverlässigkeit der Algorithmik

Gelingt dies, steht dem Konsortium ein Verfahren zur luftgestützten Infrastrukturüberwachung zur Verfügung, das weltweit in punkto Kosten-/Leistungsverhältnis und Universalität konkurrenzlos dasteht. Die positiven ökonomischen Auswirkungen bzgl. der österreichischen Sicherheitsindustrie liegen damit klar auf der Hand.

ProjektleiterIn / Unternehmen:

Dr. Elisabeth Gustenau,
Diamond Aircraft Industries GmbH

PartnerInnen:

- Diamond Aircraft Industries GmbH (Führung)
- Rheinmetall Defence Electronics GmbH
- JOANNEUM RESEARCH Forschungsges.mBH
- Technische Universität Graz
- Bundesministerium für Landesverteidigung
- Bundesministerium für Wirtschaft und Arbeit
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung
- Bundesministerium für Wirtschaft und Arbeit
- Niederösterreich

Kontakt:

Dr. Elisabeth Gustenau
Diamond Aircraft Industries GmbH
N.A. Otto-Straße 5
2700 Wiener Neustadt
Tel.: +43 2622 26700-107
Fax: +43 2622 26700-118
E-Mail: e.gustenau@diamond-air.at
Web: www.diamond-air.at

RetoMod

REferenzszenarien TOxische Gase-MODElle

Referenzszenarien für Verkehrsunfälle mit Freisetzung toxischer Gase – Schadstoffausbreitungsmodelle und ihre Praxistauglichkeit für die Feuerwehr

Die Feuerwehr benötigt bei unfallbedingtem Ausreten eines toxischen Gases, insbesondere bei Verkehrsunfällen mit Beteiligung eines Gefahrenguttransportes, vor Ort rasche Information

1. über die Richtung und Dimension der Ausbreitung der Gase und
2. über die Größe des Bereichs, in welchem adäquate Schutzmassnahmen getroffen werden müssen.

Ziel dieses Projektes ist die Auswahl und Nutzbarmachung eines Ausbreitungsmodells zur Berechnung dieser Informationen und die Festlegung der für die Ausbreitungsrechnung erforderlichen meteorologischen Informationen. Hierfür wird die Kurzfristprognose (für die nächsten 6 Stunden) der Zentralanstalt für Meteorologie und Geodynamik (ZAMG), welche mit einer horizontalen Auflösung von 1 km verfügbar ist, verwendet und die Nutzbarkeit dieser Daten für die Zwecke der Wiener Feuerwehr im gegenständlichen Projekt anhand von Vergleichsmessungen geprüft.

Als Anwendungsbereich werden Verkehrsunfall-szenarien mit möglicher Freisetzung toxischer Gase untersucht. Die Auswahl dieser Szenarien erfolgt mit Unterstützung der OMV Refining & Marketing GmbH und der Firma „Synex“ Ries & Greßlehner GmbH (im weiteren kurz Synex bezeichnet).

In Zusammenarbeit der Wiener Feuerwehr, der Firma Synex und der ZAMG werden geeignete Schadstoffausbreitungsmodelle hinsichtlich ihrer Praxistauglichkeit (Anforderungen an Eingangsparameter, Benutzerfreundlichkeit, Rechenaufwand) getestet. Unter Einbeziehung der bestehenden Erfahrungen der österreichischen Feuerwehren

sowie der C-Abwehr des österreichischen Bundesheeres wird eine optimale Vorgangsweise für den praktischen Einsatz durch die Feuerwehr erarbeitet.

ProjektleiterIn / Unternehmen:

Dr. Kathrin Baumann-Stanzer / Zentralanstalt für Meteorologie und Geodynamik

PartnerInnen:

- DI Dr. Manfred Hirnschall / Magistrat der Stadt Wien, Magistratsabteilung 68, Feuerwehr und Katastrophenschutz, Wien
- DI Gerhard Greßlehner / „Synex“ Ries & Greßlehner GmbH
- Dr. Silke Haupt-Herting / OMV Refining & Marketing GmbH, Wien

Kontakt:

Dr. Kathrin Baumann-Stanzer
Zentralanstalt für Meteorologie und Geodynamik,
Abteilung für Umweltmeteorologie
Hohe Warte 38
1190 Wien
Tel.: +43 1 36026 2405
Fax: +43 1 36026 74
E-Mail: k.baumann-stanzer@zamg.ac.at
Web: www.zamg.ac.at



S.H.F.

Sicherheit von Hohlrumbauteilen unter Feuerlast

Entwicklung eines realitätsnahen Berechnungsverfahrens zur Bestimmung der Struktursicherheit bestehender und in Planung befindlicher Hohlrumbauteile und Tragstrukturen unter Feuerlast.

Die Brandbelastung von Tragkonstruktionen aus Beton und Stahl, ausgelöst durch Unfälle, Terrorattacken oder Militäroperationen, verursacht erheblichen Schaden an der Tragstruktur von kritischen Infrastrukturbauten (z.B. Straßen- und Eisenbahntunnel, Brückentragwerke, unterirdische Kommunikationseinrichtungen, etc.) und beeinträchtigt dadurch die Gebrauchstauglichkeit und Tragsicherheit der Struktur. Die Bestimmung der Sicherheit derartiger bestehender und in Planung befindlicher Infrastruktur im Katastrophenfall Brand und im Zuge der Sanierung/Wiederherstellung ist das Ziel dieses Projekts. Derzeit werden Strukturen unter Brandbelastung unter Zugrundelegung von linearelastischem Materialverhalten dimensioniert, was besonders im Brandfall, der durch kombinierte thermische und mechanische Einwirkungen gekennzeichnet ist, die reale Belastung sowie das Tragverhalten der Stahlbetonstruktur in keinsten Weise wiedergibt. Die so genannte Nachbrandbemessung, die dem Tragverhalten nach erfolgter Abkühlung Rechnung trägt und die Bestimmung der Notwendigkeit etwaiger Stützmaßnahmen erlaubt, wird nach derzeitigem Stand der Technik nicht betrachtet und ist in der ganzheitlichen Betrachtung des gegenständlichen Forschungsprojekts (Brandlast ► Temperaturbelastung ► Strukturantwort) beinhaltet.

Das Ziel des Projekts ist die Bestimmung der Sicherheit von Hohlrumbauteilen und Tragstrukturen während, sowie nach einer Brandbelastung unter Verwendung realitätsnaher Analysemethoden und Materialmodelle. Letztere sollen im Rahmen des gegenständlichen Projektes entwickelt und experimentell validiert werden. Weiters sollen sie mit einem neuartigen Berechnungsschema in ein numerisches Berechnungsverfahren, basierend auf der Methode der finiten Elemente, zusammengeführt werden und somit erstmalig die reali-

tätsnahe Prognose der wesentlichen, das Tragverhalten der Struktur beeinflussenden Prozesse ermöglichen. Das neu entwickelte Berechnungsverfahren soll im Rahmen des gegenständlichen Forschungsprojekts auf drei Bauvorhaben angewendet werden.

ProjektleiterIn / Unternehmen:

Institut für Mechanik der Werkstoffe und Strukturen, Technische Universität Wien – Prof. DI Dr. Josef Eberhardsteiner, Prof. DI Dr. Roman Lackner, DI Matthias Zeiml

PartnerInnen:

- Institut für konstruktiven Ingenieurbau, Universität für Bodenkultur Wien – Prof. DI DDR. Konrad Bergmeister M.Sc., DI Ulrich Puz
- Schimetta Consult ZT GmbH – DI Dr. Roman Geier, DI Slobodan Grbic
- Ingenieurbüro Dr. Lindlbauer – DI Dr. Wolfgang Lindlbauer, DI Rainer Waltner
- ZT Reismann – DI Dr. Wilhelm Reismann, DI Ulrich Puz
- ÖBB-Infrastruktur Bau Aktiengesellschaft – DI Dr. Hannes Kari, Mag. Karl-Eric Pumper
- ASFiNAG Autobahn- und Schnellstraßen-Finanzierungs-Aktiengesellschaft – DI Michael Steiner, Ing. Günter Ratte
- Wiener Linien GmbH & Co KG – DI Martin Hrupek
- ARGE Bautech – DI Dr. Peter Kremnitzer, DI Dr. Johannes Horvath
- Forschungsinstitut der Vereinigung der österreichischen Zementindustrie – DI Dr. Johannes Steigenberger, DI Dr. Jürgen Macht

Kontakt:

DI Matthias Zeiml
Institut für Mechanik der Werkstoffe und Strukturen, Technische Universität Wien
Karlsplatz 13/202
1040 Wien
Tel.: +43 1 588 01-20240
Fax: +43 1 588 01-20298
E-Mail: matthias.zeiml@tuwien.ac.at
Web: www.imws.tuwien.ac.at



SimRad NBC

Simulation- und Informationssystem zum Management von Rettungseinheiten bei Katastrophen

Simulations- und Informationssystem zum Management von Rettungseinheiten bei Katastrophen- im Fokus auf ABC-Bedrohungen

Die Bedrohung durch NBC-Katastrophen wächst ständig. Im Katastrophen-Fall werden vor allem freiwillige aber auch hauptberufliche Katastrophen-Schutztrupps (z.B. Strahlenschutztrupp der Feuerwehr, ABC-Kommando) eingesetzt, um die Auswirkungen der Katastrophen zu minimieren.

Um den immer neuen Anforderungen gerecht zu werden brauchen Katastrophen-Schützer ein neues System, mit dem sie Katastrophen-Situationen effizient trainieren und in weiterer Folge den Katastrophen-Fall optimal bewältigen können. Zurzeit ist ein realistisches Training nicht möglich (vergleichbar mit einer Führerschein-Ausbildung am Übungsgelände – und nicht im Verkehr).

Das Projekt SimRad.NBC erschafft erstmals eine Technologie (die wissenschaftliche Basis eines Systems) für eine effektive Bewältigung von Katastrophen entstanden aus atomaren, biologischen und chemischen Zwischenfällen (z.B. AKW-Explosion, Giftgas-Anschlag, ...) und zum Schutz kritischer Infrastrukturen (z.B. Krankenhaus).

Dabei werden Simulationstechnologien eingesetzt um die menschlichen und technischen Abhängigkeiten von wesentlichen Einflussfaktoren herauszufinden und deren Zusammenspiel zu erforschen.

Die geschaffene Technologie ermöglicht in weiterer Folge die Herstellung neuer Produkte im Bereich des Katastrophenschutzes und dessen Training sowie die Ableitung effektiver Strategien für den Katastrophenschutz und erhöht damit die Sicherheit und das Sicherheitsempfinden der europäischen Bevölkerung.

Die NBC-Bedrohung wächst ständig – im Gegensatz dazu stagnieren die Maßnahmen im Katastrophenschutz!

ProjektleiterIn / Unternehmen:

Creative BITS Mihalits und Roth OEG, Traun

PartnerInnen:

- Ziehesberger Elektronik, Neuhofen /Krems
- J.K. Universität Linz
- Rotes Kreuz Landesverband Oberösterreich
- Forschungsinstitut des Wiener Roten Kreuzes
- Freiwillige Feuerwehr Schwechat Mitte
- EMPL Fahrzeugwerk Gesellschaft m. b. H. Kaltenbach/ Tirol

Kontakt:

Creative BITS Mihalits und Roth OEG

Markus Roth

Assistenz: Michèle Wiesmair

Zaunermühlstrasse 2

4050 Traun

Mobil: +43 676 846024 400

Fax: +43 732 65125922

E-Mail: roth@creativebits.com;

E-Mail: wiesmair@creativebits.com

Web: www.creativeBITS.com



SimRad.COMP

Simulations- und Informationssystem zum Administrieren von Hilfeinheiten bei Katastrophen - Erforschung von Systemkomponenten zur Überprüfen der Einsatztauglichkeit der SimRad-Technologie

SimRad.COMP entwickelt Komponenten zur Verifikation der im Rahmen von SimRad.NBC (KIRAS PL.2) erforschten Technologien für effektives Management von Einsatzorganisationen in Katastrophensituationen. SimRad.COMP liefert für die Simulation von Katastrophen, aber auch für ein realistisches Training von Krisensituationen und

den Realfall Komponenten, die als Vorstufe zu Prototypen für Geräte zum optimierten Katastrophenmanagement betrachtet werden können. In weiterer Folge können durch SimRad.COMP Geräte und Vorgehensweisen entwickelt werden, die die Effizienz von Einsatzorganisationen maximieren und sie optimal unterstützen.





Im Rahmen des Projektes SimRad.COMP wird die mit SimRad.NBC gestartete Initiative zur Erhöhung der Kooperation und Effizienz von Einsatzorganisationen (EO) in Katastrophensituationen fortgeführt.

Während SimRad.NBC eine Technologie zum effektiven Katastrophenmanagement mit Fokus auf nukleare, biologische und chemische Katastrophen erforscht, ist das Ziel von SimRad.COMP die Umsetzung und Erweiterung dieser innovativen Technologien, um neuartige, nachhaltige Systeme zu erschaffen, die die Effektivität von Einsatzorganisationen erhöhen.

SimRad.COMP soll in Simulation, Training und Realfall wesentliche Verbesserungen bringen:

Katastrophensituationen sollen realitätsnah simuliert werden und dadurch ein realistisches Training ermöglicht werden. EO und deren Kommandanten sollen von einem IT-Führungssystem so unterstützt werden, dass sie – im Zusammenspiel mit den anderen Verbesserungen – Katastrophen mit optimaler Effizienz bewältigen können.

Dabei werden Einsatzfahrzeuge mit der Technologie bestückt um als Sender von Sensoren- und Statusdaten zu dienen; Mobile Leitstellen und Einsatzleitung werden damit ausgerüstet, um Einsatzkräfte und Fahrzeuge optimal und effizient koordinieren zu können und ein Maximum an verwertbaren Informationen zu haben.

Einsatzpersonal wird damit ausgestattet, um Statusinformationen an die Einsatzleitung senden zu können und optimal eingesetzt werden zu können.

SimRad.COMP verwendet dabei die Ergebnisse aus SimRad.NBC, um auf verschiedene Katastrophenszenarien sowie ein spezifisches Regelwerk zugreifen zu können.

Das SimRad-System und seine Prozesse sollen dabei selbstlernend/optimierend sein und mit steigender Anzahl an realen Einsätzen, Katastrophenübungen und Simulationen wachsen, um damit eine immer effektivere Bewältigung von Katastrophen zu ermöglichen. Der in SimRad.COMP unterstützte PDCA-Zyklus dient dabei einerseits einer immer effektiveren Krisenbewältigung, andererseits einem nachhaltigen und ständigen Wachstum der Modulbibliotheken wie sie im Rahmen von KIRAS Programmlinie 2 mit SimRad.NBC entstanden sind. Vorgesehene Schnittstellen zu Sensoren und bestehenden Systemen ermöglichen eine maximale Kompatibilität mit bestehenden und in Entwicklung befindlichen Systemen und Vorgehensweisen.

SimRad.COMP trägt somit nachhaltig zu einer Optimierung von Kooperation und Bewältigungspotenzial beim Einsatzpersonal sowie dadurch zur Verminderung der Unsicherheitsperzeption der betroffenen Gesellschaft bei.

ProjektleiterIn / Unternehmen:

Creative BITS Mihalits und Roth OEG, Traun

PartnerInnen:

- J.K. Universität Linz, Institut Telekooperation
- Rotes Kreuz Landesverband Oberösterreich
- Forschungsinstitut des Wiener Roten Kreuzes
- Freiwillige Feuerwehr Schwechat Mitte
- Ziehesberger Elektronik, Neuhofen /Krems
- OÖ Ferngas AG, Linz

Kontakt:

Creative BITS Mihalits und Roth OEG

Markus Roth

Assistenz: Michèle Wiesmair

Zaunermühlstrasse 2

4050 Traun

Mobil: +43 676 846024 400

Fax: +43 732 65125922

E-Mail: roth@creativebits.com;

E-Mail: wiesmair@creativebits.com

Web: www.creativeBITS.com

SOSGuide

Safety Monitoring System and Remote Guidance

Im Projekt SOS Guide geht es um ein Konzept und eine Teststellung für ein um Elemente der Navigation erweitertes Notrufsystem des Roten Kreuzes zur Ortung und Zielführung von Hilfe suchenden Personen.

Im Zuge des Projekts soll eine Machbarkeitsstudie für eine Modernisierung der Notrufsysteme von Einsatzorganisationen durch Erweiterung um Elemente aus der Navigation durchgeführt werden. Derzeitiger Stand der Technik bei der Durchführung eines Notrufes ist, dass die Rettung per Telefon alarmiert wird und die Hilfe holende Person die Position des Verletzten für den Rettungseinsatz selbst beschreiben muss. Erst wenn in der Rettungsleitstelle hundertprozentige Gewissheit über die Position des Verletzten herrscht, wird das

Rettungsteam losgeschickt. Dies ist jedoch oft mit einem Zeitverlust verbunden, da die Position des Verletzten in vielen Fällen nicht genau beschrieben werden kann, unter anderem weil der Anrufer meist unter Stress steht.

Um bei Risikogruppen die Kommunikation zu vereinfachen bietet das Rote Kreuz das System „Rufhilfe“ an. Bei diesem System kann auf Knopfdruck über ein Funkarmband eine Kommunikation über das Festnetztelefon mit der Rettungszentrale aufgenommen werden. Da dieses System an das Festnetz gebunden ist, ist zwar die Position bekannt, es kann aber nur innerhalb einer Wohnung verwendet werden. In Zukunft sollen GPS-taugliche Mobiltelefone die Position des Verunglückten an die Zentrale übermitteln.





Durch SOSGuide soll diese Technologie nun erweitert werden: Bei einem Notruf soll nicht nur die GPS-Position an die Zentrale gesendet werden, sondern auch die aktuelle Gehrichtung der hilfeschuchenden Person. Diese Richtung kann nicht durch GPS alleine oder von diesem nur sehr unzuverlässig bestimmt werden, insbesondere dann, wenn sich die Person nicht oder nur sehr langsam fortbewegt. Durch Einsatz zusätzlicher Sensoren würde es ermöglicht, etwa blinden oder sehbehinderten Personen, die sich verirrt haben, den Weg per „Remote Guidance“ von zentraler Stelle aus zu weisen. Damit kann man sie entweder zurück an einen sicheren Ort führen oder zu einem nahe gelegenen Treffpunkt, von dem aus sie abgeholt werden können.

Potenzieller Anwenderkreis sind insbesondere auch Menschen, welche altersbedingt oder durch eine Behinderung gefährdet sind, sich aber dennoch ihre Mobilität bewahren wollen. Als Anwender denkbar sind aber auch Kinder oder Touristen. In der Umsetzung soll berücksichtigt werden, ob die betroffene Person noch im Stande ist, von der zentralen Einsatzstelle Informationen entgegenzunehmen. Bei einem Notruf soll ein Rettungsteam bzw. ein Helfer beim Auffinden der Person durch Routenplanung und Zielführung unterstützt werden.

Das System soll so weit entwickelt sein, dass die Rettungsmannschaft bei unverletzten, ansprechbaren Personen vorerst nicht sofort ausrücken muss, wenn es genügt, der Person durch gezielte Anweisungen zu helfen, sich zurechtzufinden. So kann etwa durch Zielführungsinstruktionen aus der Zentrale versucht werden, eine verirrte Person über Remote Guidance auf einem für diese Person optimalen Weg wieder nach Hause zu führen, während ihre Fortbewegung kontinuierlich mitverfolgt werden kann. Sollte jedoch dringend Hilfe nötig sein, kann zuerst auch ein in der Nähe anwesender Helfer mit einer speziell dafür entwickelten mobilen Einheit auf gleiche Weise zu einem Patienten geführt werden. Zusätzlich wird er

durch ein visuelles Benutzerinterface mit Routenplanung und Zielführung unterstützt.

Bei der Positionsbestimmung der mobilen Einheiten sollen Ausfälle von Satellitensignalen durch Sensoren der Fußgängernavigation oder GSM-Zellortung überbrückt werden können. Dies hat den Vorteil, dass entgegen herkömmlichen GPS-Mobiltelefonen auch innerhalb von Gebäuden eine Position verfügbar ist. Durch die Verwendung eines digitalen Kompasses soll – als wichtige Komponente des Systems – die Bestimmung der Orientierung (Gehrichtung) möglich sein.

Durch ein derartiges Gesamtkonzept können die Ausfahrten der Rettungsmannschaften auf das notwendigste beschränkt und die Anzahl der Fehlalarme reduziert werden. Insgesamt betrachtet liegt der innovative Aspekt der Entwicklung in der Zielführung von verirrtten Personen von einer Leitzentrale aus, aber auch in der Zielführung von Sanitätern, Pflegern und Angehörigen zu der hilfesuchenden Person, wenn diese verletzt ist.

ProjektleiterIn / Unternehmen:

Institut für Navigation und Satellitengeodäsie
Technische Universität Graz
<http://www.inas.tugraz.at>

PartnerInnen:

- SOLVION information management
<http://www.solvion.net>
- Österreichisches Rotes Kreuz, Landesverband Steiermark, <http://www.st.rotekreuz.at>

Kontakt:

Ao.Univ.-Prof. Dipl.-Ing. Dr.techn.
Manfred Wieser
Institut für Navigation und Satellitengeodäsie
TU Graz
Steyrergasse 30, 8010 Graz
Tel.: +43 316 873-6348
Fax: +43 316 873-8888
E-Mail: wieser@geomatics.tu-graz.ac.at
Web: www.inas.tugraz.at

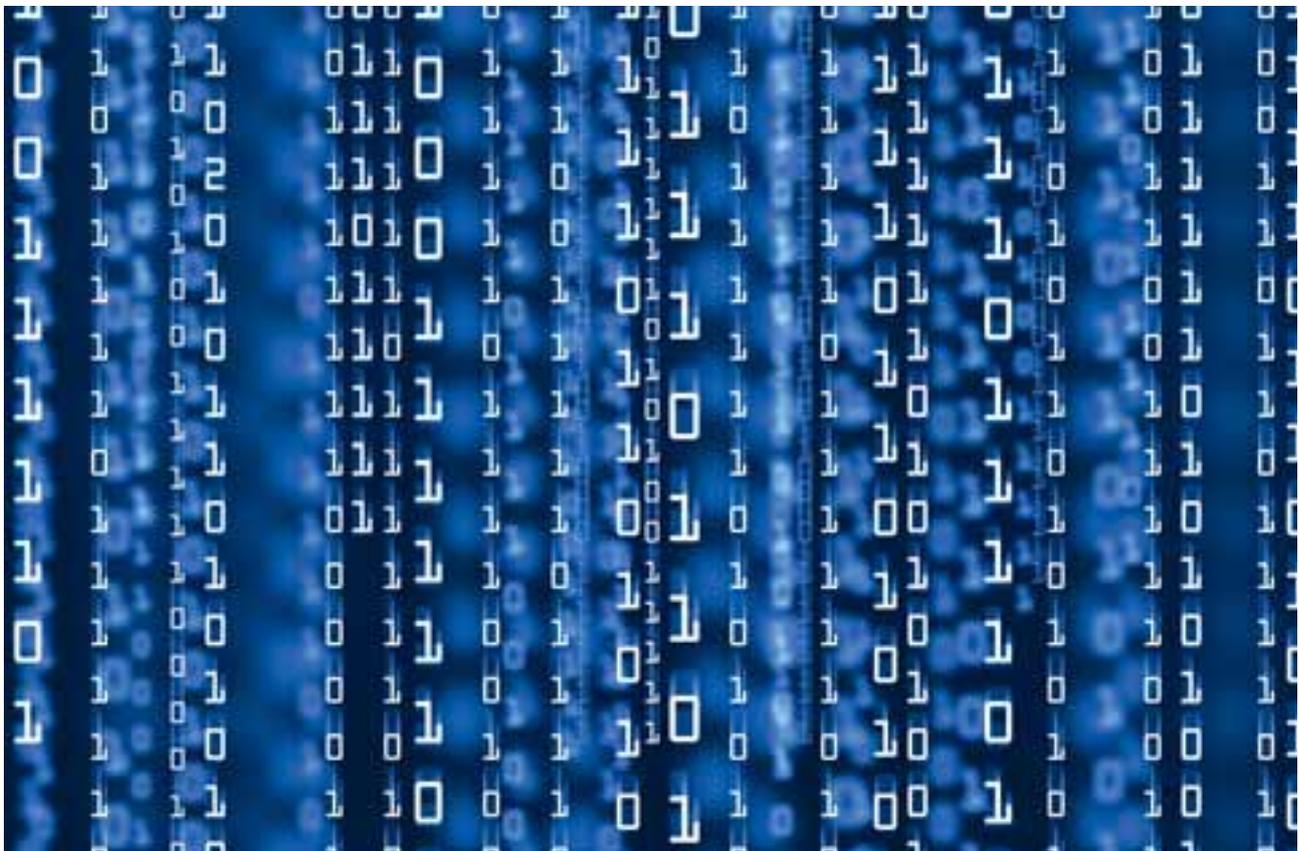
STEG-IT 2

Entwicklung von Abwehrmethoden gegen den verdeckten Informationstransfer über VoIP und Handy

Durch gezielte Veränderung von Datenpaketen wird die erfolgreiche Übermittlung geheimer Nachrichten in Audio- und Bilddateien verhindert, ohne die normale Sprach- und Bildübertragung zu stören. Das ist die effizienteste, sicherste und günstigste Methode, um den unbemerkten Transfer verschleierte Botschaften – die so genannte Steganografie – zu erschweren. Im Forschungsprojekt SteglIT haben Mitarbeiter der FH St. Pölten gemeinsam mit dem Bundesministerium für Landesverteidigung und dem Bundeskriminalamt erste Methoden und Verfahren ausgearbeitet, die wirksam spezifische steganografische Angriffe verhindern. SteglIT wurde Ende 2007 abgeschlossen. In einem Folgeprojekt sollen weitere Verfahren entstehen und ein Prototyp entwickelt werden, der gegen eine Vielzahl möglicher steganografischer Angriffe robust ist.

Eine Informationsgesellschaft lebt vom Austausch und der Speicherung von Informationen. Es besteht dabei oftmals auch Interesse daran Daten geheim zu halten. Während mit der Kryptografie Daten verschlüsselt werden, erlaubt die Steganografie eine versteckte (verborgene) Übertragung und Speicherung von Daten. Dieses Verbergen eines Informationstransfers bzw. einer Datenspeicherung gewinnt zunehmend an Bedeutung. Dies ist z.B. dann wichtig, wenn Kryptographie verboten, unerwünscht oder verdächtig ist oder wenn, etwa aus strategischen Gründen, eine Kommunikation oder Datenspeicherung überhaupt verborgen bleiben soll. Daher ist Steganografie gefährlich in den Händen von Kriminellen und Terroristen.

Die Fachhochschule St. Pölten beschäftigt sich seit 2007, wo das erste Forschungsprojekt SteglIT





durchgeführt wurde, mit der Theorie und den Anwendungen der Steganografie und der Abwehr steganografischer Angriffe. Das Ziel des Folgeprojektes STEGIT ist es, während seiner Laufzeit von 22 Monaten, konkrete Verfahren und Prototypen zur Abwehr moderner steganografischer Angriffe für die Internettelefonie (VoIP) industriell zu erforschen und zu entwickeln. Damit die Abwehrmaßnahmen getestet und Schwächen optimal erkannt werden können, beschäftigt sich das Projekt auch mit der versteckten Datenübertragung in VoIP.

Die Experten haben Abwehrmethoden entwickelt, die auf der „unhörbaren“ Datenveränderung mit Hilfe von Zufallszahlengeneratoren und mathematischen Operationen in Verbindung mit speziellen Optimierungsmethoden basieren. So werden LSB-Einbettungen wirkungsvoll abgewehrt. Die Daten werden dabei prophylaktisch verändert, unabhängig davon, ob sie geheime Informationen tragen oder nicht. Bei einer Echtzeit-Übertragung würde beispielsweise ein unhörbares Rauschen hinzugefügt werden, damit der Empfänger eine versteckte Botschaft nicht mehr dechiffrieren kann. Die normale Sprach- und Bildübertragung wäre dabei nicht gestört. Die Transformation der Daten übernimmt eine Hardware, die beim Internetservicebetreiber bzw. GSM-Netzbetreiber eingesetzt ist; die Gesprächsinhalte bzw. gesendeten Informationen selbst würden bei diesem Prozess weder abgehört bzw. gesichtet werden.

Es ist ungeheuer aufwendig, die Existenz einer versteckten Information nachzuweisen. Um diese extrahieren zu können, muss zudem die Einbettungstechnologie erkannt werden. Hier stoßen die bestehenden Verfahren schnell an ihre Grenzen, da sie auf Erkenntnissen von vorhandenen Steganografie-Algorithmen beruhen und neue Entwicklungen nicht berücksichtigen. Die Detekti-

on in Echtzeitübertragung ist besonders schwierig, da die Einbettung der Daten in unregelmäßigen Zeitabständen geschieht und damit die Zeitpunkte, wann die geheimen Nachrichten-Bits gesendet werden, unbekannt sind.

Für die nächsten Jahre erwarten die IT-Security-Experten einen starken Anstieg von Steganografie-Angriffen. Gründe dafür sind die zunehmende Verbreitung der Internettelefonie und der „Intelligenz“ der Mobiltelefone hin zu „Mini-PCs mit mobiler Telefonfunktion“. Durch SteGIT und das Folgeprojekt können schon frühzeitig Strategien und Methoden zur erfolgreichen Abwehr entwickelt und die dafür notwendigen rechtlichen Rahmenbedingungen geschaffen werden.

ProjektleiterIn / Unternehmen:

Fachhochschule St. Pölten
Matthias Corvinus-Straße 15, 3100 St. Pölten
Univ.-Doz. D.I. Dr. Ernst Piller,
Tel.: +43 2742 313 228 – 636
E-Mail: ernst.piller@fhstp.ac.at

PartnerInnen:

- Bundesministerium für Inneres, Mag. Leopold Löschl, Bundeskriminalamt, +43 1 248 36 - 865 20, E-Mail: leopold.loeschl@bmi.gv.at)
- Bundesministerium für Landesverteidigung, Bgdr. Mag. Klemens Hofmeister, Leitung F&E, +43 1 5200 23541
E-Mail: mgp.forschung@bmlv.gv.at
- Kapsch CarrierCom AG, D.I. Sanja Boltek, 050811-3324, E-Mail: sanja.boltek@kapsch.net

Kontakt:

FH-Prof. Dipl.-Ing. Johann Haag,
Studiengangsleiter IT Security,
Fachhochschule St. Pölten
Tel.: +43 2742 313228-632
E-Mail: johann.haag@fhstp.ac.at
Web: www.fhstp.ac.at

tripleB ID

Identifikation von Bedrohungsszenarien in Banken durch Bildanalyse

Das Ziel dieses Projektes ist die Entwicklung eines Softwaresystems zur Erkennung kritischer Ereignisse in Bankenumgebungen.

Das Erkennen von bestimmten Aktivitäten in einer Szene erfolgt durch die Analyse der aufgenommenen Bilder.

Das geplante System konzentriert sich auf die Bewegungsverfolgung und Analyse in mehreren, auch nicht überlappenden Kameras mit einer anschließenden Szenarioerkennung, sowie die optimierte Datenkompression mit einer effizienten Archivierung.

Ein weiteres Ziel ist ein real time Demonstrator mit herkömmlichen IP Kameras und Standard Computerhardware in einem Foyer der Ersten Bank.

ProjektleiterIn / Unternehmen:

CogVis Software und Consulting GmbH

PartnerInnen:

- Technische Universität Wien, Institut 183 (PRIP)
Dr. techn. Dipl. Ing. Martin Kampel, Favoritenstr. 9, 1040 Wien
E-Mail: kampel@prip.tuwien.ac.at
- sOM Objektmanagement GmbH, Johann Sattler, Geschäftsführer, Traungasse 12 / 6.Stock, 1030 Wien
- Institut für höhere Studien, Stefan Vogtenhuber, Stumpergasse 56, 1060 Wien
- Bundesministerium für Inneres, Bundeskriminalamt Büro 1.6, Abteilung Kriminalprävention und Opferhilfe, Mag. Herwig Lenz, Abteilungsleiter, Josef Holaubek Platz 1, 1090 Wien

Kontakt:

CogVis Software und Consulting GmbH,
DI Michael Brandstötter, Geschäftsführer
Pulverturmstraße 3, 1090 Wien
Tel.: +43 1 9971594-0
Fax: +43 1 9971594-91
E-Mail: brandstoetter@cogvis.at





TULMON

Monitoring der Ausbreitung des Tularämie-Erregers

Untersuchungen zur natürlichen Verbreitung der Tularämieerregers in Österreich und deren Differenzierung vom biologischen Kampfstoff.

Tularämie (Hasenpest, Nagerpest, Lemmingfieber, Hirschfliegenfieber, Ohara-Krankheit) ist eine seit langem bekannte, durch das Bakterium *Francisella tularensis* ssp. verursachte Zoonose, mit zyklisch aktiven Naturherden in verschiedenen Ländern der nördlichen Hemisphäre inklusive Gebieten im Nordosten Österreichs. Weiters handelt es sich bei der Tularämie neben Anthrax (Milzbrand, Erreger: *Bacillus anthracis*) um einen der beiden bei uns natürlich vorkommenden potenziellen B-Kampfstoffe. Der Krankheitsverlauf und die Symptome der Tularämie sind von der Dosis, dem vom Stamm bestimmten Grad der Virulenz sowie der Art und dem Ort (Eintrittspforte in den Körper) der Infektion abhängig. Unbehandelt kann die Krankheit beim Menschen tödlich verlaufen und deshalb hat *Francisella tularensis* die Bedeutung als potenzielles biologisches Kampfmittel. Bei frühzeitiger und richtiger Diagnose ist eine Behandlung mit Antibiotika jedoch erfolgversprechend. Der Nutzen dieses Projektes ist vielschichtig. Erstmals soll in Österreich ein punktuell Monitoring der Ausbreitung des Tularämie-Erregers in Kleinnagetieren, Zecken sowie in Wasser- und Schlammproben durchgeführt werden. V.a. die Kleinnager spielen als Reservoirtiere bei der Aufrechterhaltung und der Übertragung der Tularämie innerhalb des Na-

turherdes und auf den Menschen eine wichtige Rolle. Somit können neue Erkenntnisse über mögliche Infektionsquellen gewonnen werden. Die biochemische und molekularbiologische Differenzierung von Bakterienisolaten bis hin zur Stufe unterschiedlicher Subspecies bzw. Biovare ermöglicht bei gehäuftem Auftreten von Humanfällen in der Zukunft die rasche Unterscheidung einer Naturherd-Infektion von einer Infektion durch willkürlich freigesetzte Tularämie-Erreger.

Der Benefit dieses Projektes umfasst somit wissenschaftliche, gesundheits- und sicherheitspolitische Aspekte sowohl im zivilen als auch im militärischen Bereich.

ProjektleiterIn / Unternehmen:

Univ. Prof. Dr. Walter ARNOLD
Forschungsinstitut für Wildtierkunde und Ökologie (FIWI) der Veterinärmedizinischen Universität Wien

PartnerInnen:

- FIWI: Ass. Prof. Dr. Theodora Steineck (Veterinärmedizinische Forschung), Mag. Erich Klansek (Ökologie, Wildtiermanagement, Naturschutz), Dr. Christoph Beiglböck (Veterinärmedizinische Forschung)
- Österreichische Agentur für Gesundheit und Ernährungssicherheit GmbH (AGES), Institut für veterinärmedizinische Untersuchungen Mödling, Dr. Erwin HOFER
- Bundesministerium für Landesverteidigung (BMLV), ObstVet Dr. Michael KREINER (FGG 8), MjrA Dr. Herbert Tomaso (FGG 8), Mag. Georg Ecker (ABC-Abweherschule), HptmVet Mag. Katharina Faulkal (ABC-Abweherschule)

Kontakt:

Univ.Prof. Dr. Walter ARNOLD, Forschungsinstitut für Wildtierkunde und Ökologie
Savoyenstr. 1
1160 Wien
Tel.: +43 1 4890915
Fax: +43 1 4890915-333
E-Mail: walter.arnold@vu-wien.ac.at



VEI-3D

Virtueller Einsatzort – Infrastruktur

Ein virtuelles Modell des Einsatzortes ermöglicht der Einsatzleitung das Treffen der richtigen Maßnahmen und die effektive Unterstützung und Vorbereitung der Einsatzkräfte noch vor dem Eintreffen am Einsatzort.

Infrastrukturen mit großer geographischer Ausdehnung werden heute meist von wenigen Zentralen aus überwacht. In Krisen- und Katastrophenfällen benötigen die Mitarbeiter in der Zentrale, speziell bei komplexen Situationen, einen umfassenden und klaren Überblick über die Gegebenheiten am Einsatzort und in seiner Umgebung mit allen verfügbaren Informationen, um rasch und effektiv die richtigen Entscheidungen zur Krisenbewältigung und bestmöglichen Rettung von Leben sowie Abwendung weiterer Schäden treffen zu können. In den ersten Minuten, noch bevor Einsatzkräfte vom Einsatzort weitere wichtige Informationen über die Lage melden können, werden wichtige Entscheidungen wie die zeitgerechte Verfügbarkeit von notwendigen Ressourcen, die Auswahl von Zufahrtswegen oder die Bedachtnahme auf weitere mögliche Risiken, getroffen. Andernfalls verstreichen die lebenswichtigen ersten Minuten ergebnislos bis die ersten Einsatzkräfte direkt vor Ort eintreffen.

Ein virtuelles Modell des Einsatzortes, vergleichbar einem Sandkastenspiel früherer Militärs, mit zusätzlicher Darstellung aller sichtbaren aber auch

unsichtbaren Gegebenheiten (Kanäle, Leitungen, andere Verkehrswege, Bevölkerungsdichte u.s.w.) am Bildschirm, mit Interaktionsmöglichkeiten wie z.B. dem Messen im Modell, ermöglicht der Einsatzleitung das Treffen der richtigen Maßnahmen und die effektive Unterstützung und Vorbereitung der Einsatzkräfte noch vor dem Eintreffen am Einsatzort.

Zusätzlich könnte das System für die Planung sicherheitsrelevanter Einsätze, für Schulungen und das Überprüfen von Taktiken genutzt werden.

Der virtuelle Einsatzort hilft somit die entscheidenden ersten Minuten nach einem Schadensereignis bestmöglich zu nutzen, um das Richtige rechtzeitig zu veranlassen, optimal zu retten und Schäden an Menschen und Gütern abzuwenden oder zumindest zu minimieren.

ProjektleiterIn / Unternehmen:

ÖBB-Infrastruktur Bau AG

PartnerInnen:

DI Dr. Stefan Maierhofer/VRVis Forschungs-GmbH, Wien; DI Paul Fried/Eydolon GmbH, Wien

Kontakt:

Ing. Friedrich BRIMMER

Tel.: +43 664 6171030

E-Mail: friedrich.brimmer@bau.oebb.at





VKT-GOEPL

Validierung von Konzepten und Technologien für ein gemeinsames öffentlich-privates Lagebild

Das Projekt VKT-GOEPL strebt den Aufbau einer neuen kollaborativen öffentlich-privaten Führungsfähigkeit an. Diese basiert auf der Einsicht, dass öffentliche und private Akteure für eine erfolgreiche Sicherheitszusammenarbeit über ein gemeinsames Lagebewusstsein und Lageverständnis verfügen müssen. Diese soll durch ein gemeinsames öffentlich-privates Lagebild (GOEPL) hergestellt werden. Als Anknüpfungspunkt dafür dient das KIRAS-Projekt GÖPL AUT.

Neue Sicherheitsherausforderungen verlangen nach einer neuen Wissensgrundlage, um die Ursachen von Sicherheitsrisiken korrekt beurteilen

und die zur Bekämpfung erforderlichen Maßnahmen in der erforderlichen Zeit treffen zu können.

VKT-GOEPL ist ein umsetzungsorientiertes industrielles Forschungsvorhaben, in dessen Mittelpunkt die Erforschung technischer Konzepte und die Prüfung ihrer Realisierbarkeit stehen, um eine neue, bislang nicht verfügbare kollaborative öffentlich-privete Führungsfähigkeit in Form eines gemeinsamen öffentlich-privaten Lagebilds bereitzustellen. Das beantragte Projekt untersucht die technische Machbarkeit ausgewählter Aspekte, prüft die Einsatzfähigkeit unterschiedlicher relevanter Konzepte und Technologien und stellt das damit verbundene Entwicklungspotenzial dar, es skizziert die GOEPL-Architektur und bildet die Funktionsfähigkeit gemeinsam mit staatlichen und privatwirtschaftlichen Akteuren anhand eines Experiments unter Realbedingungen ab.

ProjektleiterIn / Unternehmen:

Frequentis AG

PartnerInnen:

- Bundeskanzleramt
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung
- KFEG GmbH
- SAS Institut Software GmbH
- Thales Rail Signalling Solutions GmbH
- TU-Wien - Institut für Computertechnik
- VRVIS GmbH

Kontakt:

DI Dr. Christian Flachberger
Frequentis AG, Corporate Research
Innovationsstrasse 1
1100 Wien
Tel.: +43 1 81150-0
Mobil +43 664 608502942
Fax +43 1 8115077-2942
E-mail: christian.flachberger@frequentis.com
Web: www.frequentis.com



Unterstützungsmaßnahmen und Studien



3S-VKI

Strategische Security Szenarien für die Vernetzung Kritischer Infrastruktur

Globale Methodologie und Modell für infrastrukturübergreifende Bedrohungsbilder und Schutzmassnahmen.

Das Thema Security ist in den letzten Jahren eine feste Größe in der Öffentlichkeit geworden. Ob Anschläge, wie am 11. September 2001, auf die Londoner „Tube“ und in Madrid, die wachsende Anzahl an Naturkatastrophen oder drohende Pandemien, sie bewahren diesem Thema die Aktualität, sowohl in Medien als auch in den Köpfen der Zivilbevölkerung. Alle genannten kritischen Ereignisse für die öffentliche Sicherheit beeinträchtigen oder schädigen auch die öffentliche Infrastruktur und damit die ökonomischen und sozialen Abläufe des Alltags. Dies führt zum Gedanken, diese Träger von potenziellen Bedrohungen verstärkt zu schützen. Zusätzlicher Schutz von (kritischer) Infrastruktur führt zu der Gefahr einer Kostenexplosion durch zusätzliche notwendige Anschaffungen, wie technische Sicherheitseinrichtungen und Anlagen sowie zusätzlichem Personal. Um so mehr ist es von vorrangiger Bedeutung, einerseits potenzielle Risiken zu evaluieren und andererseits Kosten für zusätzlichen Schutz und Schaden im Eintrittsfall in die Waagschale zu legen. Das Projekt „3S-VKI - Strategische Security Szenarien für Vernetzung Kritischer Infrastruktur“ soll diesem Aspekt (Schutz, Nutzen und Kosten) im Rahmen einer Studie zur Ausarbeitung einer Methode zur Beschreibung und Bewertung von infrastrukturübergreifenden Bedrohungen Rechnung tragen. Die Bearbeitung der Thematik erfolgt in enger Zusammenarbeit mit den betroffenen Bedarfsträgern bzw. Infrastrukturbetreibern und unter Einbeziehung deren inhaltlicher Inputs. Der Beitrag für die Gesellschaft ist durch die Möglichkeit des sinnvollen Mitteleinsatzes (möglicherweise auch

von Steuergeldern) und dem gezielten Schutz gegeben.

Die Inhalte des Projektes „3S-VKI – Strategische Security Szenarien“ für Vernetzung Kritischer Infrastruktur sind eindeutig dem Schutz kritischer Infrastruktur im Verkehrs- und Transportbereich zuzuordnen, da dieses Projekt die übergreifende Betrachtung von Infrastrukturbereichen betrifft, die eine elementare Lebensgrundlage der Bewohner des Landes Österreich darstellt.

Als übergeordneter Projektteil der Ermittlung kritischer Infrastrukturen werden in diesem Projekt die Akteure (Straße, Schiene, Wasser, Energie) aber auch Bedarfsträger (z.B. bmvit, BMI, BMLV) zur Mitarbeit (im Zuge von Workshops) eingeladen und integriert.

ProjektleiterIn / Unternehmen:

L.O.B Logistik- und Organisationsberatung GmbH
Landstraßer Hauptstraße 81/40, 1030 Wien

PartnerInnen:

- bachler & partners crisis and security consulting GmbH – Mag. Michael Madreiter
- Herry Consult GmbH – DI Norbert Sedlacek
- L.O.B Logistik- und Organisationsberatung GmbH – Mag. (FH) Andreas Fohringer

Kontakt:

L.O.B Logistik- und Organisationsberatung GmbH
Landstraßer Hauptstraße 81/40
1030 Wien
Mag. (FH) Andreas Fohringer (L.O.B)
Tel.: +43 1 71307-19
Fax: +43 1 8174955-1688
E-Mail: fohringer@lob.co.at
Web: www.lob.at



POLIZEIABSPERRUNG

Cyberstalking

Österreichweite Studie zum Cyberstalking-Verhalten

Neue Medien verändern unser gesamtes Leben. Sie helfen Kindern dabei, Neues zu lernen, mit dem Mobiltelefon sind wir überall erreichbar und der Laptop erlaubt es uns, überall zu arbeiten. Trotzdem werden wir immer häufiger vor den Folgen der missbräuchlichen Nutzung des Internets gewarnt. Hacker stehlen Kreditkartennummern und Computerviren werden verschickt.

Das Bedrohen und Schikanieren anderer Personen ist kein neues Phänomen. In den vergangenen Jahren wurden diese Handlungen unter dem Begriff Stalking zusammengefasst. Personen fühlen sich durch Telefon-, SMS- und Internetterror in ihrer Lebensführung beeinträchtigt. Das Stalken, die üble Nachrede und Geschäftsschädigung über das Internet werden als Cyberstalking bezeichnet. Cyberstalking umfasst also einen Teil der Handlungen, die sonst oft unter dem Begriff Cybercrime subsumiert und somit in diesem Projekt als Bedrohung verstanden werden. Opfer von Cyberstalking können nicht nur Einzelpersonen, sondern auch Organisationen werden. Für Unternehmen etwa können Schäden in Millionenhöhe entstehen. Im Zeitalter des Web 2.0 wächst der Handlungsspielraum aller InternetuserInnen. Dadurch steigt aber auch die Gefahr der missbräuchlichen Nutzung des Internets.

Der Forschungsgegenstand Cyberstalking wurde in Österreich bislang von der Medienforschung noch nicht untersucht. Außerdem gibt es in der Fachliteratur noch keine einheitliche Definition des Begriffes Cyberstalking. Ein Ziel der Forschung ist es deshalb, eine Definition des Begriffes zu erarbeiten, die die unterschiedlichen Zugänge und Betrachtungsweisen integriert und die unterschiedlichen Stakeholdergruppen zur Verfügung gestellt werden kann. Der oft als „Anti-Stalkingparagraph“ bezeichnete §107 StGb deckt nicht alle Aspekte des Stalkings ab, die von WissenschaftlerInnen beschrieben werden. Definitionen des Stalkings umfassen auch Handlungen, die über die im §107 StGb genannten hinausgehen und juristisch an anderer Stelle behandelt

werden. Es gilt daher, im Rahmen der Studie eine juristische Analyse durchzuführen, um alle rechtlichen Bereiche, die durch Cyberstalking zur Anwendung kommen, zu prüfen. Ein weiteres Ziel des Forschungsprojektes ist es, die Frage zu klären, ob, beziehungsweise inwiefern technische Entwicklungen das Verhalten von Stalking-TäterInnen beeinflussen. Ein zusätzliches Forschungsinteresse ist es, mit Hilfe einer repräsentativen Umfrage aufzuzeigen, wer sich in Österreich als Opfer beziehungsweise TäterIn sieht. Außerdem stellt sich die Frage, mit welchen elektronischen Mitteln Cyberstalking in Österreich betrieben wird. Schließlich sollen die Forschungsergebnisse im Rahmen eines Symposiums an die wesentlichen Stakeholder und die Community of Science weitergegeben werden.

ProjektleiterIn / Unternehmen:

Donau-Universität Krems

PartnerInnen:

- Institut für Publizistik und Kommunikationswissenschaft der Universität Wien
- Universitätslehrgang für Informationsrecht und Rechtsinformatik

Kontakt:

Mag. Edith Huber, Zentrum für Praxisorientierte Informatik, Donau-Universität Krems

Dr. Karl-Dorrek-Straße 30
3500 Krems

Tel.: +43 2732 893-2306

E-Mail: edith.huber@donau-uni.ac.at





GEO-IKT

Geoinformation und Schutz kritischer Infrastrukturen

Erhebungsstudie als Grundlage weiterführender Aktivitäten im Bereich Geoinformation und Sicherheit kritischer Infrastrukturen.

Ereignisse der jüngsten Vergangenheit wie Terroranschläge und Naturkatastrophen haben gezeigt, dass Geoinformation einen entscheidenden Faktor im Krisen- und Katastrophenmanagement darstellt - 80% aller katastrophenrelevanten Informationen haben räumlichen Bezug. Für eine gewinnbringende Einbindung von Geoinformation in Bereiche der Sicherheit bzw. des Zivil- und Katastrophenschutzes gilt es, die Interoperabilität der Daten im größtmöglichen Umfang zu erweitern. Dies erfordert mehr Kooperation und Zusammenarbeit zwischen den beteiligten Akteuren. Handlungsbedarf liegt in der Definition kritischer Infrastrukturen im Sinne deren Identifikation und Dokumentation sowie im Ausloten von Möglichkeiten eines Monitoring, das zeitnahe Reagieren erlaubt.

Die Studie GEO-IKT identifiziert österreichische Akteure in Wissenschaft, Wirtschaft und öffentlicher Hand, die zum Aufbau von Geoinformation für die Sicherheitsforschung beitragen und stärkt und vernetzt eine entstehende community im Bereich Geoinformation und Sicherheitsforschung. Erster Schritt ist die Bestandsaufnahme der österreichischen Situation unter Einbindung internationaler Best-Practice. Relevante Akteure, Stakeholder und Forschungseinrichtungen, sowie deren Aktivitäten, Bedürfnisse und Problemstellungen werden identifiziert und in einer räumlichen



Übersicht (einer so genannten Kompetenzlandkarte) als web-basierte Lösung dargestellt.

Meilensteine und erwartete Ergebnisse von GEO-IKT:

- Definition, Identifikation und Dokumentation der notwendigen Geoinformation für das Monitoring relevanter kritischer Infrastrukturen in Österreich
- Erhebung derzeitiger Aktivitäten in Österreich und Erstellung einer Kompetenzlandkarte
- Aufzeigen internationaler Best-Practice aus den Bereichen GIS, GMES und INSPIRE
- Untersuchung potenzieller Anwendungsfelder im Bereich kritischer Infrastrukturen, in denen durch den Einsatz von Geoinformationssystemen, Methoden der Fernerkundung und Monitoring eine Verbesserung der Sicherheit zu erwarten ist.
- Kritische Analyse des Informationsflusses zwischen beteiligten Akteuren

Die wesentlichen Inhalte und Erkenntnisse werden aufgearbeitet, in Empfehlungen für weiterführende Maßnahmen überführt und dienen als Vorbereitung für künftige Vernetzungsaktivitäten. GEO-IKT ist eine Voraussetzung, um eine leistungsstarke Community im Bereich Geoinformation und Sicherheit in Österreich herauszubilden und aufzubauen.

ProjektleiterIn / Unternehmen:

Z_GIS Zentrum für Geoinformatik, Universität Salzburg

Partner

- HiTec Marketing
- Austrian Research Centers - arsenal research

Kontakt:

Prof. Dr. Thomas Blaschke
Universität Salzburg, Zentrum für Geoinformatik
Hellbrunner Str. 34, 5020 Salzburg
Tel.: +43 662 908585-216
E-Mail: thomas.blaschke@sbg.ac.at

GoVAS

Government Voice over IP Attack Study

In Hinblick auf die fortschreitende Transformation herkömmlicher Sprachtelefonie (POTS) in Richtung Internet-basierender Technologien ist die Zielsetzung des Projekts Government Voice over IP Attack Study (GoVAS) zum einen durch gezieltes Monitoring des österreichischen Internet-Verkehrs, zum anderen durch Analyse der relevanten Protokollfamilien ein Bild potenzieller Angriffsvektoren und deren Gefährdungspotenzial als Basis für einen zukünftigen Aktionsplan zur Absicherung der relevanten Infrastrukturen zu entwerfen.

Die Notwendigkeit eines solchen Projekts ergibt sich aus der Tatsache, dass in den letzten Jahren innerhalb eines relativ kurzen Zeitraums mehr und mehr Internet- (i.e. TCP/IP-basierende) Infrastrukturen für Zwecke verwendet wurden und werden, die ursprünglich durch abgeschlossene und gut abgeschirmte Strukturen (Closed Circuit Netze) unterstützt wurden. Diese basieren auf langjährig etablierten und ausgereiften Technologien und formen die Basis grundlegender Kommunikationskanäle, die





sich durch beinahe 100%-ige Verfügbarkeit, auch in Krisenfällen, auszeichnen. Ein Beispiel eines solchen, bislang abgeschlossenen Systems, stellt die Sprachtelefonie dar, die, nicht zuletzt aufgrund ihrer technologischen Reife, extrem hohe Verfügbarkeit (i.e. äußerst niedrige Ausfallswahrscheinlichkeiten) bietet.

Aus verschiedenen technischen, wie nicht zuletzt auch ökonomischen, Erwägungen werden diese Dienste nun vermehrt auf Internet-Protokoll-basierende Technologien umgestellt, was zum einen zu einer Vereinheitlichung (und damit Vereinfachung) der Kommunikationsinfrastrukturen, zum anderen aber zur Abhängigkeit einer Basiskomponente der Kommunikation von Technologien, die ihre Reife und Ausfallssicherheit bislang nur beschränkt unter Beweis stellen mussten, mit sich bringt.

Vereinfacht gesagt unterwirft sich die bislang als relativ ungefährdet geltende Sprachtelefonie durch ihre Verlagerung von einem Closed Circuit Netz in ein nach allen Seiten offenes System damit den selben Gefährdungen durch verschiedene Attacken (Hacker-Angriffe, Denial-of-Service-Attacken, bis hin zu Viren und trojanischen Pferden), wie jedwede sonstige Internet-Dienste.

Selbiges gilt ebenso für die Telefonie-Infrastruktur (Endgeräte, Vermittlungsanlagen, etc.) in Analogie zu beispielsweise der Infrastruktur des World Wide Web (i.e. Server, Client-PCs, etc.).

GoVAS (Government VoIP Attack Study) beschäftigt sich mit der Analyse potenzieller Gefahren, die sich aus der Transformation der Sprachtelefonie auf VoIP (Voice over Internet Protocol) Technologien und der damit einhergehenden Abhängigkeit von Internet-Basis-Infrastrukturen ergeben.

Dabei wird der Fokus nicht nur auf die Angreifbarkeit der Technologien bzw. Infrastrukturen selbst, sondern auch auf die potenziell

zu erwartenden Auswirkungen solcher etwaiger Angriffe gelegt.

Zur Erreichung dieser Zielsetzung besteht das Projekt aus 3 Hauptteilen:

- Monitoring des Internetverkehrs und Analyse der erfassten Daten hinsichtlich potenzieller Angriffsmuster
- Analyse sowohl der VoIP-Protokolle per se, als auch der für VoIP unabdingbaren Internet-Basisprotokolle (auf Anwendungsebene), wie DNS, NTP, etc., bzw. deren Zusammenspiel
- Analyse und Bewertung der aus den beiden o.a. Punkten resultierenden Bedrohungspotenziale

Die aus diesen Teilen gewonnenen Erkenntnisse sollen letztlich als strukturierte Basis für zukünftige Arbeit im Bereich Schutz von Internet Infrastrukturen mit besonderem Fokus auf kritische Bereiche dienen. Derartige zukünftige Aktivitäten können die Prozessentwicklung für eine Alarmierungsinfrastruktur oder den Aufbau eines umfassenden Monitoring- bzw. Frühwarnsystems beinhalten.

ProjektleiterIn / Unternehmen:

FH JOANNEUM, ASE/ITM
Dipl.-Ing. Takashi Linzbichler

PartnerInnen:

- FH JOANNEUM GmbH, Studiengänge
- Advanced Security Engineering (ASE)
- Internettechnik (ITM)
- Informationsmanagement (IMA)
- Datentechnik GmbH

Kontakt:

Studiengangs- und Transferzentrumsleitung:
FH-Prof. Mag. Dr. Sonja Gögele
FH Joanneum – Datentechnik
Alte Poststraße 149
8020 Graz
Tel.: +43 316 5453
E-Mail: sonja.goegele@fh-joanneum.at

Katastrophenmanagement im Gesundheitswesen

Bestandsanalyse der Notfallplanung

Bedarfsplanung für Krisen und Katastrophenmanagement – unter Berücksichtigung von gesundheitlichen Bedrohungen, chemischen und atomaren Gefahren, Bioterrorismus und Naturkatastrophen.

Die bioterroristischen Anschläge mit Milzbrandbriefen in den USA, die SARS-Epidemie, das jüngste Auftreten der Vogelgrippe in Asien sowie aktuelle politische, gesellschaftliche sowie technologische Entwicklungen bergen eine Vielzahl an Risiko- und Gefährdungspotenzial, die als Quelle außergewöhnlicher Schadenereignisse fungieren können.

Die von ihnen potenziell verursachten Katastrophen implizieren eine wesentliche Zerstörung bzw. Schädigung der örtlichen Infrastruktur, eine Gefährdung des Lebens sowie der Gesundheit der Menschen und sorgen für gravierende ökologische aber auch ökonomische Folgen.

Die Zielsetzung des Projekts ist es, auf Basis klar definierter Gefahren, eine Bestandsanalyse der medizinischen und psychologischen Notfallhilfeplanung in Österreich in behördlicher, operativer, materieller und juristischer Hinsicht durchzuführen.

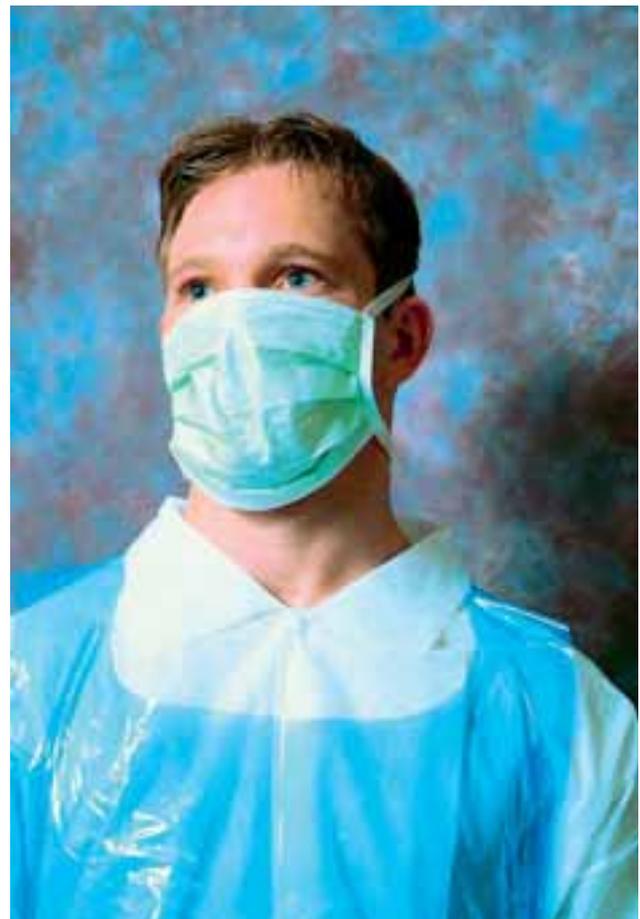
Zudem soll ein Status quo bereits ergriffener Initiativen auf nationaler und europäischer Ebene ermittelt werden. Die dabei gewonnenen Erkenntnisse sollen im Zusammenhang mit möglichen Folgen eines Katastropheneintritts bestehende Engpässe und Mängel aufdecken. Dieses Projektvorhaben liefert einen Beitrag zur Bedarfsermittlung im Gesundheitswesen im Katastrophenfall und dient zur Vorbereitung künftiger Maßnahmen. Das Projekt wird unter der Leitung des Institutes für Pharmaökonomische Forschung in Kooperation mit AGES, Foresee, Med-Consult und dem Österreichischen Ökologie Institut durchgeführt.

ProjektleiterIn / PartnerInnen:

- Institutes für Pharmaökonomische Forschung (IPF)
- Österreichische Agentur für Gesundheit und Ernährungssicherheit (AGES)
- Foresee
- Österreichisches Ökologie Institut (ÖI)
- MED-CONSULT, Dr. Evelyn Walter (IPF)

Kontakt:

Mag. Anamarija Batista (IPF),
Tel.: +43 1 5132007-12,
E-Mail: a.batista@ipf-ac.at





Observer Algorithm

Computer Vision-Algorithmen zur Detektion potenziell verdächtiger Gegenstände

Im Rahmen des Projektes Observer Algorithm soll ein bildverarbeitendes System zur Erkennung von verlorenen oder abgestellten Gegenständen erforscht werden, um sicherheitskritische Zustände zu erkennen.

Das Projekt Observer Algorithm umfasst die Erforschung von Computer Vision - Algorithmen zur Detektion potenziell verdächtiger Gegenstände. Bildverarbeitende Kamerasysteme sollen in Zukunft zur Erkennung von verlorenen oder abgestellten Gegenständen verwendet werden, um sicherheitskritische Abläufe nicht vertrauenswürdiger Personen zu erkennen.

Ziel des Algorithmus ist es, eine Person mit Gepäck zu erkennen, zu verfolgen und das Abhandkommen des Gepäckstückes zu bemerken. Erkannte Vorfälle (abgestellte Koffer, verlorene Handtaschen, etc.) sollen protokolliert und an eine überwachende Stelle weitergeleitet werden.

Das Ermitteln von Bewegungen über Korrelationen, über optischen Fluss und weitere neue Methoden werden im Rahmen dieses Projektes analysiert und erprobt.

Für den Einsatz dieser Algorithmen werden handelsübliche Digitalkameras verwendet, welche Farbbilder an einen zentralen Rechner übermitteln wo die Objekterkennung und das Verfolgen von Personen (Tracking) durchgeführt werden.

Mehrere Kamerasysteme, auf einem zu observierenden Gebiet, dienen zur Verfolgung von Personen über unterschiedliche Gebäudebereiche und ermöglichen es, relevante Bilder an eine Sicherheitseinrichtung zu übermitteln.

Ansätze für diesen Algorithmus sind die im folgenden Absatz erklärten Verfahren: Eine denkbare Lösung ist das Zulassen von variablen Formen, um einen Mensch darzustellen und bei Änderungen der Form eine Trennung von Mensch und Objekt zu erkennen.

Weiters ist es denkbar die Bewegungen im Bild so zu überwachen, dass man erkennt, dass bestimmte, bewegte Regionen zusammenhängen. Trennen sich diese, wurde ein Objekt vom Menschen getrennt. Eine weitere Möglichkeit bietet ein kinematisches Modell, welches ab dem Zeitpunkt des Erkennens der Person alle ihr zugehörigen Objekte auf Grund der unterschiedlichen kinematischen Bewegungen erkennt und zwischen Mensch und Objekt differenzieren kann.

Im Rahmen des Projektes Observer Algorithmus sollen die erläuterten Ansätze erforscht und weitere Möglichkeiten evaluiert werden. Im Laufe des Projektes werden die erdachten Konzepte implementiert und getestet.

Außer einem Einsatz auf öffentlichen Plätzen mit starren Kameras ist es außerdem denkbar diese Algorithmen im Bereich der Servicerobotik auf Sicherheitsrobotern einzusetzen und Überwachungsaufgaben automatisch durchzuführen.

ProjektleiterIn / Unternehmen:

Firma DI (FH) Roland Ambrosch

Kontakt:

DI (FH) Roland Ambrosch

Leopold-Moses-Gasse 4/2/33

1020 Wien

Tel.: +43 660 5555 435

E-Mail: roland@ambrosch.co.at

Web: www.ambrosch.co.at

OEPK

Ortung eingeschlossener Personen nach Katastrophen

Das Lawinenunglück in der Tiroler Wintertourismusgemeinde Galtür führte der österreichischen Öffentlichkeit in besonders drastischer Weise vor Augen, wie wichtig eine rasche Ortung verschütteter Personen ist, um möglichst viele Opfer lebend bergen zu können. Das Projekt OEPK hat sich zum Ziel gesetzt, Methoden zur Ortung von Personen zu entwickeln, die nach Katastrophen (Erdbeben, Lawinen, Murenabgänge etc.) verschüttet werden.

Gegenwärtig vermögen trainierte Suchhunde Spuren von flüchtigen Verbindungen zu riechen – das Projekt OEPK entwickelt demgegenüber eine „elektronische Nase“. Im Vergleich zu Hunden können technische Lösungen mittels Massenspektrometrie wesentlich mehr flüchtige Substanzen „riechen“ und eignen sich auch für lang andauernde Katastropheneinsätze.

Im Atemgas, Schweiß und Urin sind hunderte flüchtige Substanzen nachweisbar, die theoretisch für die Ortung von Personen infrage kommen. Die Konzentrationen von Aceton, Isopren, Acetaldehyd, Methanol, Dimethylsulfid, Allylsulfid oder Butanon könnten etwa für die räumliche Ortung von lebenden Menschen ausgenutzt werden. OEPK erforscht charakteristische Konzentrationsmuster von verschütteten Menschen, um mit diesem Know-how eine Ortungsgerätegeneration von hohem Innovationsgrad zu begründen.

Österreich soll in dieser Marktnische eine international führende Rolle in der zunehmenden Professionalisierung des Katastrophenmanagements einnehmen.

Zur Erreichung des Projektziels werden spurenanalytische Methoden eingesetzt; für die Entwicklung der Methode werden folgende Geräte benützt:

- Protonen Transfer Reaktions Massenspektrometrie (PTR-MS),
- Selected Ion Flow Tube Massenspektrometrie (SIFT-MS),

- Gaschromatographie mit massenspektrometrischer Detektion (GC-MS);

Diese analytischen Techniken werden vom OEPK-Projektteam zur Analyse von Ausatemgas und Urin und auch – in Ergänzung zum Projekt – zur Entwicklung entsprechender medizinischer Diagnostik benützt. Die Empfindlichkeit geht bis in den ppt-Bereich (ppt = parts per trillion = 1 Teil Substanz auf 10¹² Luftteilchen).

Für den Einsatz am Katastrophenort ist Ionenmobilitätsspektrometrie (IMS) vorgesehen. Die entsprechenden Geräte sind schon jetzt an Flughäfen (Detektion von Sprengstoff) oder im Kriegsgebiet (Detektion von chemischen Kampfstoffen) im Einsatz.

Es handelt sich grundsätzlich um portable Geräte – mit großem Potenzial für Miniaturisierung. Wesentlich für OEPK ist die Entwicklung eines Sets von verschiedenen Substanzen mit einem für verschüttete Personen charakteristischen Konzentrationsmuster.

ProjektleiterIn / Unternehmen:

Direktor Univ.-Prof. Doz. (ETH) Dr. Anton Amann, Forschungsstelle für Atemgasanalytik der Österreichischen Akademie der Wissenschaften

PartnerInnen:

- Branddirektor Mag. Erwin Reichel, Berufsfeuerwehr Innsbruck

Kontakt:

Mag. Mag. Marco Freek
Forschungsstelle für Atemgasanalytik der Österreichischen Akademie der Wissenschaften
Dammstraße 22
6850 Dornbirn
Tel.: +43 664 80515-60000
Fax: +43 512 50424683
E-Mail: marco.freek@oeaw.ac.at
Web: www.oeaw.ac.at/aa



RoSkIn

Die Rolle des Menschen in ausgewählten Sicherheitssystemen kritischer Infrastruktur

Moderne Technologien spielen eine große Rolle bei der Überwachung kritischer Infrastrukturen. Operatoren von Sicherheitssystemen sind unmittelbar an der Mensch-Maschine Schnittstelle von hochkomplexen technischen Einrichtungen (Verkehrs-Leitstellen, Kontrollsystemen in Kraftwerken, Tunnel-Überwachungsanlagen, Überwachung der Wasserversorgung, etc.) tätig. Dementsprechend kommt ihnen eine zentrale Rolle im Management von Krisen und Zwischenfällen zu. Das bedeutet aber zugleich, dass Fehlentscheidungen mit massiven Konsequenzen verbunden sein können. Ein umfassendes Verständnis aller Aspekte der Mensch-Maschine Interaktion in derartigen Sicherheitssystemen ist für die nationale Sicherheit von großer Bedeutung. Im Projekt „Die Rolle des Menschen in ausgewählten Sicherheitssystemen kritischer Infrastruktur“ werden Operatoren derartiger Sicherheitssysteme in ihrem Arbeitsumfeld untersucht.

Projektphase 1: Theoretischer Hintergrund

In der ersten Forschungsphase wird der aktuelle Stand wissenschaftlicher Forschung zum Untersuchungsobjekt dargestellt. Zunächst werden mögliche Bedarfsträger identifiziert. Parallel dazu wird in einer umfassenden Literaturanalyse der wissenschaftliche State of the Art erhoben. Eine Analyse der rechtlichen Reglementierung der Arbeit der

Operatoren ist ebenfalls Teil dieser ersten, explorativen Phase der Untersuchung.

Projektphase 2: Soziologische Analyse und psychologische Testungen

Die zweite Stufe des Projektes ist wiederum in mehrere Ebenen gegliedert. Zunächst werden, auf den Erkenntnissen aus Projektphase 1 aufbauend, sozialwissenschaftliche Erhebungsinstrumente für den spezifischen Einsatz in diesem Projekt adaptiert. Mittels Analyse von Sekundärdaten, Expertenbefragungen und Beobachtungen vor Ort wird die Arbeitspraxis der Operatoren untersucht. Psychologische Testungen sollen Aufschluss über die Persönlichkeitsmerkmale der Operatoren geben.

Projektphase 3: Selektionskriterien und Ausbildungsguidelines

Durch die interdisziplinär verschränkte Vorgehensweise kann ein umfassendes Verständnis der arbeitspraktischen Prozesse sowie der psychologischen Voraussetzungen der Operatoren entwickelt werden. Aus den Ergebnissen der empirischen Untersuchungen können anschließend Selektionskriterien sowie Ausbildungsguidelines für dieses Berufsfeld abgeleitet werden. Darüber hinaus wird dargestellt, welche Voraussetzungen für das rechtzeitige Erkennen und damit Verhindern von Störfällen gegeben sein müssen und welche Maßnahmen zur Auswahl und Schulung des Personals dafür erforderlich sind.

ProjektleiterIn / Unternehmen: Kuratorium für Verkehrssicherheit

Kontakt:

Mag. Thomas Völker
Schleiergasse 18
1100 Wien
Tel.: +43 577077-1218
Fax: +43 577077-1499
E-Mail: thomas.voelker@kfv.at
Web: www.kfv.at



SALOMON

Segregationsanalyse und Methodenentwicklung

Entwicklung einer Forschungsmethodik zur Erfassung individueller und kollektiver Bedrohungswahrnehmungen in der Bevölkerung.

Um die Sicherheit von Bevölkerungen zu gewährleisten, sind Informationen und Daten wesentlich, die Aufschluss über Bedrohungsbilder und Ängste geben. Dieses Wissen kann dazu beitragen, Unterschiede bei spezifischen gesellschaftlichen Gruppen (Geschlecht, Alter, ethnische Herkunft, Religion, soziale Lage, ...) zu erkennen und Maßnahmen zur Verbesserung der Sicherheit der Bevölkerung gezielt weiterzuentwickeln. Hierbei sind politische, wirtschaftliche, organisatorische und kulturelle Aspekte zu integrieren. Derzeit existiert im europäischen Raum kein Instrumentarium, mit dem Bedrohungswahrnehmungen von Menschen mit Migrationshintergrund methodisch valide erfasst werden können.

Ziel von SALOMON ist es, eine Forschungsmethodik zu entwickeln, mit der individuelle und kollektive Bedrohungswahrnehmungen und Ängste in der Bevölkerung – im Speziellen von Menschen mit Migrationshintergrund – erfasst werden können. Insbesondere sollen Fragen des Feldzugangs und der praktischen Durchführbarkeit berücksichtigt werden.

SALOMON wird in vier Schritten umgesetzt: Aufbauend auf (1) einer umfassenden Literaturrecherche und (2) ExpertInnen-Gesprächen zur Erkenntnisgewinnung über geeignete Forschungsmethoden sollen (3) valide Methoden entwickelt werden, die geeignet sind, Bedrohungswahrnehmungen von MigrantInnen zu erfassen. In der abschließenden Projektphase werden (4) die Ergebnisse aufbereitet und Empfehlungen für die Sicherheitsforschung abgeleitet. Die Projektarbeit wird im Rahmen des eingerichteten „Think Tank“ – einer Gruppe von ExpertInnen aus Wissenschaft, Politik und Praxis – begleitend unterstützt.

SALOMON wird von 1. Mai 2007 bis 30. April 2009 unter der Leitung des Forschungsinstituts

des Wiener Roten Kreuzes in Kooperation mit der Sigmund Freud Privat-Universität durchgeführt.

ProjektleiterIn / Unternehmen:

Mag^a. Ingrid Spicker, Forschungsinstitut des Wiener Roten Kreuzes

Weitere Projekt- bzw. KooperationspartnerIn

■ Univ. Prof. Dr. Alfred Pritz, Sigmund Freud Privat-Universität Wien GmbH (SFU), Schnirchgasse 9a, 1030 Wien

Kontakt:

Mag^a. Ingrid Spicker
Forschungsinstitut des Wiener Roten Kreuzes
Nottendorfer Gasse 21
1030 Wien
Tel.: + 43 1 79580-2426
Fax: + 43 1 79580-9730
E-Mail: ingrid.spicker@w.rotekreuz.at
Web: www.w.rotekreuz.at/forschungsinstitut





SALOMON Next Step

Bedrohungsperzeption von Menschen mit Migrationshintergrund

Bedrohungsperzeption in der Bevölkerung - Studie um Aufschluss über die Bedrohungsperzeption insbesondere von Menschen mit Migrationshintergrund zu erhalten.

Das Projekt SALOMON Next Step, aufbauend auf SALOMON, liefert wissenschaftlich fundierte Erkenntnisse in Bezug auf die individuellen und kollektiven Ängste, handlungsanleitende Motivationen sowie die Bedrohungsperzeptionen von Menschen mit Migrationshintergrund in Österreich. Auf einer breiten Basis werden die Ergebnisse mit ExpertInnen diskutiert und Empfehlungen für die Sicherheitspolitik in Österreich formuliert. Damit kann eine solide Hintergrundinformation für Maßnahmen zur Verbesserung der Sicherheit der österreichischen Bevölkerung geliefert werden. Bedrohung und ihre Wahrnehmung gehen dabei in beide Richtungen: in Paris starben Kinder in den Flammen eines Wohnhauses, weil sie und ihre Familien die Anweisungen der Feuerwehr entweder nicht verstanden haben oder für eine Falschinformation hielten, während die Familien der U-Bahn-Attentäter von London als integrierte britische Staatsbürger der zweiten Generation aus den ehe-

maligen Kolonien die individuellen Karrieren der Gewalttäter nach Auslandsaufenthalten in fundamental religiösen Zentren nicht adäquat bewerteten. Dies mag für die sozial motivierten Unruhen in den Banlieus Frankreichs analog gelten. Zusätzlich ist in der Bedrohungsperzeption die oft unmittelbar erinnerte reale Bedrohung durch Kriegs- oder Bürgerkriegsszenarien zu beachten. So ist verständlich, dass bosnische Muslime aus Srebrenica die Behandlung ihrer Religion anders konnotieren als serbische Einwanderer aus dem Kosovo Polje. Dies gilt umso mehr, wenn eine reale individuelle oder familiäre Verstrickung in derzeit noch andauernde Konflikte besteht.

SALOMON Next Step, aufbauend auf SALOMON, ist daher von Relevanz für sämtliche Themen und Aufgaben der Sicherheitsforschung sowie darüber hinaus für die Präzisierung sozialer, ökonomischer und hoheitlich sicherheitsbezogener Maßnahmen (und ist insbesondere auch in Zusammenhang mit den Einreichungen der Forschungsinstitute der LVAK in die Programmlinien des KIRAS zu betrachten).

ProjektleiterIn / Unternehmen:

Forschungsinstitut des Wiener Roten Kreuzes

PartnerInnen:

- Univ. Prof. Dr. Alfred Pritz, Sigmund Freud Privat-Universität (SFU), Schnirchgasse 9a, 1030 Wien
- Günther Ogris, M.A., SORA Institute for Social Research and Analysis, Ogris & Hofinger GmbH Linke Wienzeile 246, 1150 Wien

Kontakt:

Mag^a. Ingrid Spicker
Forschungsinstitut des Wiener Roten Kreuzes
Nottendorfer Gasse 21
1030 Wien
Tel.: +43 1 79580-2426
Fax: +43 1 79580-9730
E-Mail: ingrid.spicker@w.rotekruz.at
Web: www.w.rotekruz.at/forschungsinstitut



SEHC

Securing Extramural Health Care

Die Sicherung der extramuralen Versorgung hilfs- und pflegebedürftiger Menschen im Krisen- und Katastrophenfall.

In Österreich sind derzeit etwa 600.000 Menschen hilfs- und pflegebedürftig. 480.000 davon werden informell im Rahmen des familiären Verbandes gepflegt und betreut. Weitere 60.000 Menschen befinden sich in Alten- und Pflegeheimen. Den übrigen 60.000 wird durch das Angebot der formellen mobilen Pflegedienste ein Leben in den eigenen vier Wänden ermöglicht.

Die mobilen Dienste ermöglichen den betroffenen Personen, so lange als möglich zu Hause zu verbleiben, wobei das Angebot von qualifizierter Pflege über Hilfe zur Weiterführung des Haushaltes bis zur Aufrechterhaltung sozialer Kontakte reicht. Der Kernbereich der Leistungen, die Hauskrankenpflege, die Heimhilfe und die Betreuung durch AltenfachbetreuerInnen, wird mittels Besuchsdiensten, Essen auf Rädern und Fahrtdiensten ergänzt.

Noch nicht eingehend untersucht sind in diesem Zusammenhang Auswirkungen komplexer Krisen- und Katastrophenszenarien auf die formellen Betreuungs- und Versorgungsstrukturen dieser 60.000 hilfs- und pflegebedürftigen Menschen. Dieser Frage soll sich die geplante Studie widmen: Derzeit erscheinen insbesondere drei Gefahrenquellen als besonders relevant. Erstens der Anstieg von Naturkatastrophen durch den Klimawandel und damit assoziierter Gefahren. Die Berechnungen des „International Panel on Climate Change“ prognostizieren einen Anstieg der Klimavariabilität und Änderungen in der Frequenz, Intensität und Dauer von Extremereignissen. Beispiele sind die Zunahme von Hitzewellen und außerordentlichen Niederschlagsereignissen. Ein zweites Bedrohungsszenario stellen Katastrophen dar, die durch technisches Versagen, Fahrlässigkeit oder Vorsatz hervorgerufen werden. Beispiele hierfür sind gezielte Anschläge auf die Infrastruktur und Störfälle in Atomkraftwerken. Darüber hinaus soll drittens im Rahmen dieser Studie auch auf die Auswirkungen von Pandemien eingegangen werden. Im Falle einer Pandemie wäre in Folge der zu erwartenden Erkrankungsrate damit

zu rechnen, dass nicht alle Erkrankten hospitalisiert werden könnten und es massive Ausfälle beim Schlüsselpersonal gibt. Alle genannten Szenarien bedrohen die kritische Infrastruktur und können auch in Kombination auftreten.

Dieses Projekt wird sich dabei mit der Logistik der Versorgungsdienste auseinandersetzen, mögliche Störfaktoren evaluieren und darauf aufbauend ein ausführliches Verbesserungskonzept erstellen. Am Beginn steht eine Analyse des IST-Zustandes des vorhandenen Logistiknetzwerks und der damit verbundenen Humanressourcen. Es folgt eine Untersuchung der gegebenen Infrastruktur und die Identifikation von kritischen Punkten. Im nächsten Schritt werden Szenarien simuliert und mögliche notwendige Modifizierungen aufgezeigt. Methodisch wird dabei auf computergestützte Simulationstechniken und Optimierungstechniken zurückgegriffen. Ergebnisse dieser Studie sollen eine umfassende Darstellung der kritischen Infrastruktur in der formellen extramuralen Pflege und Betreuung, und die Bereitstellung von leistungsfähigen, computerunterstützten Planungsverfahren für die Organisation der Versorgungsdienste sein.

In Verbindung mit den dargestellten Bedrohungsszenarien sind derartige Studien sehr wichtig, um eine möglichst effiziente und effektive Betreuung der formell extramural betreuten PatientenInnen im Krisen- und Katastrophenfall gewährleisten zu können und einen Anstieg der Mortalitäts- und Folgeschadensrate bestmöglich zu verhindern.

ProjektleiterIn / Unternehmen:

Universität für Bodenkultur Wien,
Inst. f. Produktionswirtschaft u. Logistik

Partner:

Österr. Rotes Kreuz

Kontakt:

Univ. Ass. Mag. Dr. Patrick Hirsch, Universität für Bodenkultur Wien, Institut für Produktionswirtschaft und Logistik
Feistmantel Str. 4, 1180 Wien
Tel.: +43 1 47654-4419
E-Mail: patrick.hirsch@boku.ac.at



SiLu

Sicherheit aus der Luft

Bedingungen, Chancen und Risiken für ein Intellectual Property Cluster „Sicherheit aus der Luft“ zum Schutz von Österreichs Bevölkerung und kritischer Infrastruktur.

Ziel der Studie ist der Entwurf eines integrativen Ansatzes für ein Intellectual Property Cluster „Sicherheit aus der Luft“ (SiLu) mit Schwerpunkt in Wiener Neustadt. Es soll dem Aufbau einer diesbezüglich national leistungsfähigen und international wettbewerbsfähigen Industrie und Forschung dienen, indem es die Akteure von Staat und Industrie, Wissenschaft und Forschung in Österreich vernetzt, eine bessere Abstimmung der Kooperation mit internationalen Partnern fördert und die Voraussetzung für eine wirksame internationale Kooperation schafft. Österreichs Bürgerinnen und Bürger haben Anspruch auf wirksamen Schutz und die ungestörte Funktionsfähigkeit kritischer Infrastruktur. Dies gilt ebenso für sicherheitsbezogene Aspekte

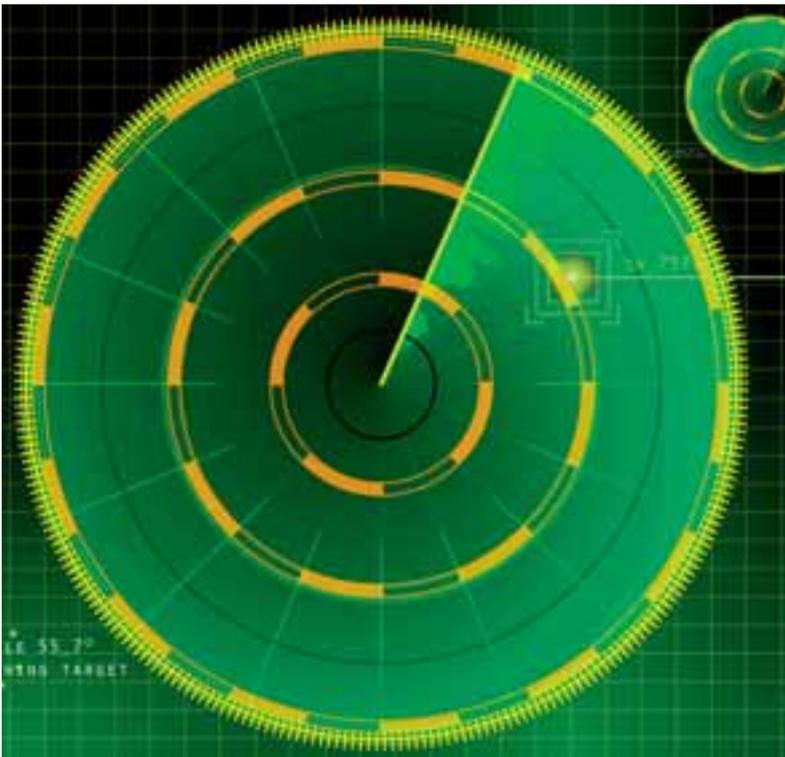
von Klima und Umwelt. Die Umsetzung dieses Verständnisses erfordert im Schwerpunkt „Sicherheit aus der Luft“, d.h. die Nutzung luftgestützter Technologien einschließlich des zugehörigen Informations- und Wissensmanagements.

Die Zukunft industrieller Wertschöpfung wird in erster Linie von „Intellectual Properties“ bestimmt. Eine enge Zusammenarbeit aller „Stakeholder“ ist unerlässlich – nicht nur mit Blick auf die zu leistenden Sicherheitsaufgaben, sondern auch hinsichtlich hart umkämpfter nationaler und internationaler Märkte.

Dieser Ansatz muss gegenüber einer kritisch nachfragenden Öffentlichkeit nachhaltig kommuniziert werden können.

Im Inhalt der Studie sollen dazu die Bedingungen, Chancen und Risiken unter Berücksichtigung folgender Teilaspekte untersucht werden:

- Erhebung der national vorhandenen Expertise im technologischen Bereich rund um das Thema Fernerkundung, luftgestützte Aufklärungssysteme, UAV, Systemintegration etc.
- Klärung des Zugang zu internationaler Technologie und zu Trends und Vorhaben bei staatlichen und EU-Gremien für die österreichischen Akteure
- Aktivierung und Unterstützung der Kommunikation zwischen den unterschiedlichen Bedarfsträgern und Bedarfsdeckern in Österreich
- Erwerb einer Kooperationsfähigkeit – z. T. Vorreiterrolle – mit internationalen F&E Einrichtungen generell und im Rahmen der zwischenstaatlichen Forschungsk Kooperation bei gleichzeitiger Einbindung der nationalen Industrie



- Entwurf einer Kollaborationsstruktur für nationale Akteure auch hinsichtlich internationaler Kooperationserfordernisse
- Identifizierung von relevanten lösungsbedürftigen politischen, wirtschaftlichen, technologischen, ökologischen, sozialen, rechtlichen und ressourcenbezogenen Fragestellungen
- Identifizierung von konkreten Programmen einschließlich kooperativen F&E-Projekten zur Realisierung des IPC „Sicherheit aus der Luft“; nationale Programme sollen dabei globale Nachfrage antizipieren (z.B. in Verbindung mit der Fußballeuropameisterschaft 2008)
- Entwurf von Grundzügen eines integral angelegten Kommunikationskonzeptes für die Vermittlung des IPC-Konzeptes einschließlich seiner Produkte
- Evaluierung der Möglichkeiten von Bündelung, Weiterentwicklung und Vernetzung technologischer Kompetenz
- Aufbereitung der Grundlagen für die strategische Ausrichtung der Kooperation und Kollaboration
- Identifizierung des möglichen Beitrages zur Förderung von Exzellenz und Wachstum der österreichischen Sicherheitswirtschaft

Zum Projektablauf ist vorgesehen, unter Führung und Mitarbeit einer Strategieguppe der „Stakeholder“ in einer 12-monatigen Studie die Expertise ausgewiesener österreichischer und weiterer Fachleute zur Recherche, konzeptionellen Aufbereitung und kommunikativ wirksamen Zusammenfassung zu nutzen. In drei Workshops werden unter Beteiligung möglichst vieler Partner eines künftigen IPC bereits bestehende/entstehende Kompetenzen erfasst, in einem zweiten Schritt Weiterentwicklungs-, Ergänzungs-, Kooperationsbedarf analysiert und abschließend in einem dritten Schritt Handlungsempfehlungen abgeleitet.

Begleitend zur Studie soll das Thema „Sicherheit aus der Luft“ beispielhaft in einer künstlerischen Anwendung (Video) über einen Wettbewerb konstruktiv-kritisch und öffentlichkeitswirksam reflektiert werden.

Als Ergebnis der Studie wird eine Beschreibung der erforderlichen Bedingungen, Chancen und Risiken für die Bildung eines Intellectual Property Cluster „Sicherheit aus der Luft“ vorgelegt, darunter

- Identifizierung und Klärung der Vorbedingung für die Vernetzung von Expertise in Administration, Industrie, Wissenschaft und Forschung

Die Studie wird aufzeigen, wie sich mit Hilfe eines Intellectual Property Cluster „Sicherheit aus der Luft“ auf der Grundlage bestehender Kompetenzen ein sogenannter „nationaler Diamant“ gestalten lässt, in dem sich Faktorbedingungen, Unternehmensstrategie, Struktur und Wettbewerb, die Präsenz bzw. Ansiedlung fähiger Unternehmen und Lieferanten in „Sicherheit aus der Luft“ bezogenen Branchen sowie die Nachfragebedingungen gegenseitig positiv dynamisch beeinflussen.

ProjektleiterIn / Unternehmen:

emer. o. Univ. Prof. Dipl.-Ing. Dr.-techn. Dr.-Ing.e.h. Helmut Detter, Österreichische Gesellschaft für Mikrosystemtechnik, Wien

PartnerInnen:

- Österreichische Gesellschaft für Mikrosystemtechnik (Führung)
- Technische Universität Graz
- Johannes Kepler Universität Linz
- JOANNEUM RESEARCH Forschungsgesellschaft mbH
- Aerospy Kleinstflugzeuge GmbH
- Diamond Aircraft Industries GmbH

Kontakt:

emer. o. Univ. Prof. Dipl.-Ing. Dr.-techn. Dr.-Ing.e.h. Helmut Detter
Öst. Gesellschaft für Mikrosystemtechnik
Floragasse 7/2
1040 Wien
Tel.: +43 1 58801-36680
Fax: +43 1 58801-36698
Mobil: +43 664 3079607
E-Mail: dolenc.stz@ogms.at



SIM-SIC!

Secure Intermodal Modes - Secure Intermodal Carriers Analyse von Risikopotenzialen einzelner Verkehrsträger intermodaler Transportketten

Das Projekt SIM-SIC! beschäftigt sich mit der Bewertung des Risikopotenzials (insbesondere, aber nicht nur, der Störanfälligkeit) einzelner Verkehrsträger unter dem Ziel der Minimierung des Gesamtrisikos intermodaler Transportketten und somit des Supply Chain Risikos.

Die Wichtigkeit der Thematik des präventiven Schutzes und somit der Abschätzung und Bewertung des Risikopotenzials der einzelnen Verkehrsträger intermodaler Transportketten und Supply Chains zeigt sich beispielsweise bei in den letzten Jahren vermehrt zu beobachtenden Störungsfällen in intermodalen Transportsystemen und -ketten.

Das intermodale Transportsystem mit seinen Verkehrsträgern selbst weist Charakteristiken auf, die es für Störungen aller Art (natürlich, menschlich herbeigeführt, politisch, technisch etc.) anfällig macht. Im Projekt werden die einzelnen Modi für Güterverkehr (Strassen-, Schienen- und Wasserstrassenverkehre) auf ihre Risikopotenziale analysiert und klassifiziert. Dadurch wird die Basis der Absicherung der funktionierenden intermodalen Güterversorgungsstruktur des Landes verbreitert und die intermodalen Netze und einzelnen Verkehrsträger auf ihre Risikopotenziale und Störungsausbreitungsreichweiten, eventuell zugrundeliegende strukturelle Defekte und Möglichkeiten von Ausweichstrategien (Coping and Mitigation) und Wiederherstellungsfähigkeiten zu einem „Normal-Zustand“ (Resilience of the System) untersucht.

Gegenüber dem Fall der Modellierung von Teilausfällen von Knoten des Netzes (wie derzeit vom Konsortium in einer Vorstudie bearbeitet), gilt es nun in diesem Projekt ein wesentlich komplexeres Zusammenspiel der verschiedenen Verkehrsträger innerhalb multi- und intermodaler Transportketten abzubilden, auf Schwachstellen und Risikopotenziale zu analysieren, vielschichtige Szenarien von Störanfälligkeiten zu modellieren und zu simulieren, um einen Risikokataster für österreichische intermodale Transportketten zu erstellen.

Mit den Ergebnissen ist das Projekt sodann in der Lage, einen Katalog von Risikopotenzialen und ihre jeweiligen, zu planenden Coping-, Mitigation- und Antwortstrategien sowie Möglichkeiten zur Hebung der Resilience des Systems zu erarbeiten, um somit die gesamte intermodale Transportkette (Vorlauf-Umschlag-Hauptlauf-Umschlag-Nachlauf) für alle Verkehrsträger und Modi, Umschlagsknoten sowie auch für die Ebene der Ladungsträgereinheiten abzubilden und das entsprechend erarbeitete Wissen zu bündeln.

Als Adressaten dieser Studie sind alle Akteure der intermodalen Supply Chains, politische Entscheidungsträger, Infrastrukturbetreiber, Terminalbetreiber, Dienstleister, Verloader, Spediteure und Betreiber verkehrsträgerpezifischer Unternehmen zu verstehen.

ProjektleiterIn / Unternehmen:

Universität für Bodenkultur, Department für Wirtschafts- und Sozialwissenschaften, Institut für Produktionswirtschaft und Logistik

PartnerInnen:

- h2 projekt.beratung Mag. Hans Häuslmayer KG, 1030 Wien
- Wirtschaftsuniversität Wien, Department für Informationsverarbeitung und Prozessmanagement, Institut für Produktionsmanagement, 1090 Wien

Assoziierte Projektpartner (über Letter of Interest)

- Rail Cargo Austria AG
- ÖBB Infrastruktur Betrieb AG
- Erste Donau-Dampfschiffahrts-Gesellschaft m.b.H., 1020 Wien
- via donau Österreichische Wasserstraßen-Gesellschaft mbh

Kontakt:

Univ.-Prof. Mag. Dr. Manfred Gronalt
Tel.: +43 1 47654-4411, Fax: +43 1 47654-4417
E-Mail: manfred.gronalt@boku.ac.at

SkIG

Sicherheit kritischer Infrastruktur bei Großveranstaltungen

Großveranstaltungen und deren Sicherheit stellen ein immer größer werdendes Problem dar. Ausschreitungen durch Fans bei Konzerten oder Sportveranstaltungen werden zur alltäglichen Realität. Überwachungssysteme sollen den Schutz von Menschen bei solchen Großveranstaltungen gewährleisten.

Nichtsdestotrotz sind solche Techniken bei der Bevölkerung nicht immer beliebt. Es stellt sich daher die Frage, wie man die Technik so anpassen kann, dass ihre Akzeptanz und das Vertrauen der Menschen in diese Techniken erhöht wird und auch die gewünschte Schutzfunktion gewährleistet werden kann, um mögliche Ausschreitungen zu reduzieren. Es gilt daher, eine soziologische und psychologische Analyse in diesem Forschungszusammenhang durchzuführen.

Durch das Zusammentreffen einer großen Anzahl von Menschen sind Handlungen und Reaktionen nicht immer vorhersehbar. Um eine adäquate technische Lösung zu entwickeln ist es nötig, das menschliche Verhalten und das Empfinden von und in unsicheren Situationen näher zu beleuchten.

Basierend auf diesen Erkenntnissen sollen Technologien und Szenarien zum Schutz von Menschen, speziell bei Großveranstaltungen, erstellt werden. Die Wissenschaft, insbesondere die Psychologie, versucht „Sicherheit“ bzw. „Unsicherheit“ an objektiven Messkriterien festzumachen. Daher sollte man den Prozess der Erfahrungsbildungen (Ungewissheit) näher beleuchten. Menschliches Handeln ist eine Abfolge von Beobachten, Identifizieren relevanter Sachverhalte, Interpretieren vorliegender Daten, Handlungsauswahl und Handlungsführung. Jeder dieser Schritte kann mit Ungewissheit einhergehen. So kann z.B. durch das Vorhandensein von Videoüberwachung die Wirklichkeit verzerrt sein und ein starkes Unsicherheitsgefühl entstehen.

Ob eine Situation als „sicher“ oder „unsicher“ eingestuft wird, hängt also im Wesentlichen von den Erfahrungen der Person, der geschätzten Häufigkeit des Eintretens eines Ereignisses, der geschätzten Wahrscheinlichkeit des Eintretens und der Möglichkeit, das Ergebnis des Ereignisses vorauszusagen, ab.

Im Rahmen des Forschungsvorhabens wird die Frage des Empfindens von Unsicherheit von Individuen bei Großveranstaltungen, unter der Berücksichtigung von eingesetzter Technologie gestellt. Generell soll beurteilt werden, ob das Empfinden in der Gruppe anders ist als im Einzelfall. Ein weiterer Forschungsaspekt soll die Untersuchung der sozialen Urteilsbildung sein.

Es geht im Wesentlichen um die Frage der sozialen Mitbedingtheit des Wahrnehmens von anderen Personen bzw. Gefahrenpotenzialen sowie die Prozesse der Informationsgewinnung und -verarbeitung im Hinblick auf soziale Phänomene und Prozesse.

Die Ergebnisse der Forschung sollen nachhaltig die Technologieentwicklung von Sicherheitstechnik, insbesondere die Überwachungstechniken, beeinflussen.

ProjektleiterIn / Unternehmen:

Donau-Universität Krems, Department für Governance & Public Administration, Zentrum für praxisorientierte Informatik

PartnerInnen:

■ Center Communication Systems GmbH

Kontakt:

Mag. Edith Huber, zPM
Donau-Universität Krems
Dr. Karl-Dorrek-Straße 30, 3500 Krems
Tel.: +43 2732 893-2306
E-Mail: edith.huber@donau-uni.ac.at

SCC

Secure Supply Chains

Secure Supply Chains erstellt eine Risikoanfälligkeitsanalyse der österreichischen Güterverkehrsinfrastruktur und damit der Basis der funktionierenden Versorgung des Landes mit Gütern.

Anhand der Beispiele mehrerer Knoten des österreichischen Infrastrukturnetzes (multi-modaler Binnenterminals) in ihrer Funktion als wichtigste Bindeglieder zwischen verschiedenen Transportmodi der Supply Chain werden Risikoanalysen durchgeführt und Schwachstellen und Potenziale zur Hebung der Sicherheit im österreichischen Güterverkehr erhoben. Diese Risikoanalysen werden auf der Ebene gesamter beispielhafter Supply Chains, auf der Ebene einzelner wichtiger Umschlagsknoten der betrachteten Supply Chains, sowie auf Ebene der betroffenen Ladungseinheiten durchgeführt. Die erforschten Inhalte bilden die Basis, um Risikoszenarien zu definieren. Diese Szenarien bilden die Basis, um mittels Modellierung und Simulation Planspiele durchzuführen, um den (Teil-)Ausfall verschiedener Knoten in der

österreichischen Versorgungskette (Disruption Risks) im Falle von Natur- oder Terrorkatastrophen sowie operationaler Risiken zu bewerten. Ein wichtiger Aspekt hiervon ist die Frage, welche Teile der Güterversorgungskette im Falle eines Teil- oder Totalausfalls von einem oder mehreren Knoten des Netzes in welcher Tiefe mit welcher Reaktionsgeschwindigkeit einspringen und Versorgungsengpässe kompensieren können. Dazu werden bestehende Güterströme und betriebliche Leistungsdaten von Container Terminals erhoben, abgeglichen und auf ihre, aus logistischer Sicht, Tauglichkeit zur Aufrechterhaltung einer Notversorgung Österreichs bei Ausfall wichtiger Versorgungslinien durch Katastrophen geprüft. Ein weiterer wichtiger Teil des Projekts ist die Erarbeitung von Auswirkungen und Praxis-Umsetzungsmöglichkeiten von auf europäischer und einzelstaatlicher Ebene zu verabschiedenden legislativen Maßnahmen, die auf eine Erhöhung der Sicherheit in der Transport- und Lieferkette Europas abzielen. Das Projekt trägt somit zu einem höheren Sicherheitslevel für Österreichische Güter Supply Chains bei und, durch die Erarbeitung von Antwort- und Risiko-Deeskalations-Strategien, zu einem besseren und effizienteren Umgang mit knappen Ressourcen im Notfall.

ProjektleiterIn / Unternehmen:

Universität für Bodenkultur Wien, Institut für Produktionswirtschaft und Logistik

Partner

- Wirtschaftsuniversität Wien, Institut für Produktionsmanagement
- CTS Container Terminal Salzburg Ges.m.b.H.

Kontakt:

Univ.-Prof. Mag. Dr. Manfred Gronalt
Universität für Bodenkultur Wien, Institut für
Produktionswirtschaft und Logistik
Feistmantel Str. 4
1180 Wien
Tel.: +43 1 47654 4410
E-Mail: manfred.gronalt@boku.ac.at



SUSI

Subjektive Sicherheit im öffentlichen Raum

Subjektive Sicherheit im öffentlichen Raum - im Mittelpunkt steht die Frage, welche Faktoren zu einer Erhöhung der subjektiv wahrgenommenen Sicherheit verschiedener Bevölkerungsgruppen beitragen.

Die subjektive Wahrnehmung von Sicherheit/Unsicherheit hängt nur bedingt mit „objektiven Bedrohungen“ etwa „Gefährdungen auf Leib und Leben“ zusammen. Vielmehr speist sie sich aus einem intra- und intersubjektiven Prozess, bei dem „objektive Bedrohungen“ wohl eine entscheidende, aber eben nicht die einzige Determinante darstellt: Menschen fühlen sich in bestimmten Situationen sicher oder unsicher, weil sie diese selbst als sicher/unsicher definieren. Diese Definitionen unterscheiden sich von Individuum zu Individuum. Sicherheitsspezifische Studien zeigen, dass diese Definitionen eben nur bedingt auf objektive nachweisbare Sicherheitsrisiken oder tatsächliche erlebte Verbrechen Situationen zurückzuführen sind, ja sich teilweise sogar konträr zu tatsächlichen objektiven Sicherheitslagen entwickeln (vgl. Polizeipräsenz und Sicherheitsgefühl, Feltes 2003).

Ziel & Anlauf des Forschungsprojektes

Das vorliegende Forschungsprojekt möchte einen Beitrag dazu leisten, das Wissen über den subjektiven Definitionsprozess von Sicherheit/Unsicherheit im öffentlichen Raum zu erhöhen. Da präventive Sicherheitsmaßnahmen nur erfolgreich sein können, wenn sie das subjektiv wahrgenommene Sicherheitsgefühl erhöhen, stellt das Verständnis dieses Definitionsprozesses einen entscheidenden Faktor bei der Konzeption und Durchführung von erfolgreichen Instrumenten einer präventiven Sicherheitsstrategie dar. Dazu werden sowohl Aneignungskonflikte im öffentlichen Raum, als auch Auswirkungen von Kriminalpräventiven Maßnahmen (Schutzzonen, Videoüberwachungen, Polizeipräsenz, etc.) untersucht. Darüber hinaus sollen aus der beantragten Studie konkrete Empfehlungen und Schulungskonzepte entstehen, die in der Aus- und Weiterbildung von

Exekutive, SozialarbeiterInnen (evt. MentorInnen, aber auch VertreterInnen von politischen Körperschaften) Anwendung finden.

Der Forschungsablauf gliedert sich in drei Forschungsphasen: In einer explorativen Forschungsphase werden mittels qualitativer ExpertInneninterviews und teilnehmender Beobachtung die Grundlagen der subjektiven Definitionsprozesse erhoben. Diese werden dann in einer anwendungsorientierten Forschungsphase über die Vignettenanalyse zu einer Struktur der Definitionsprozesse verdichtet. In einer abschließenden verwertungsbezogenen Forschungsphase sollen diese Erkenntnisse dann aufbereitet und für Fort- und Weiterbildungsprozesse weiterentwickelt werden.

Um einen möglichst großen Bereich potenzieller Determinanten subjektiver Sicherheit/Unsicherheit erheben zu können, wurden als Forschungsfeld „öffentliche Räume“ gewählt, die sich hinsichtlich ihrer BenutzerInnen, ihres Konfliktpotenzials und dem Ausmaß bereits etablierter präventiver Sicherheitsmaßnahmen stark unterscheiden:

- a. Wiener Karlsplatz (Schutzzone, Suchtszene)
- b. Fleischmarkt (Wegweiserecht, Klinik für Schwangerschaftsunterbrechungen)
- c. Schwedenplatz/Morzinplatz (Videoüberwachung)
- d. Brunnenmarkt (Ottakring, keine präventiven Sicherheitsmaßnahmen)

ProjektleiterIn / Unternehmen:

Kompetenzzentrum für Soziale Arbeit GmbH
Daumegasse 5/2
1100 Wien

Kontakt:

Mag. Dr. Tosca Wendt
Tel.: +43 1 6066877-8300
Fax: +43 1 6066877-109
E-Mail: toska.wendt@fh-campuswien.ac.at
Mag. Dr. Katharina Miko
Tel.: +43 1 6066877-8300,
Fax: +43 1 6066877-109
E-Mail: katharina.miko@fh-campuswien.ac.at



Trusted Computing in der österreichischen Verwaltung

Abwehr von Angriffen und Schutz persönlicher Daten

Herausforderungen und Möglichkeiten von Trusted Computing für das Public Management.

Trusted Computing, die neue Technologie in der Sicherheitstechnik für PCs, Server und Netzwerke, eine Kombination aus Software-Sicherheit und kryptographischer Hardware-Verschlüsselung, zeichnet sich in allen Ebenen ab. Intel und AMD arbeiten intensiv mit Kryptographen an der Vorbereitung gesicherter PC und Serverplattformen für Trusted Computing Lösungen.

Ziel ist die Abwehr von Angriffen durch z.B. Viren, Phishing oder Root-Kit Attacken und das bei gleichzeitigem Schutz der Integrität der persönlichen Daten auf dem höchsten erzielbaren Sicherheitsniveau. Betriebssysteme, wie Microsoft VISTA, diverse UNIX- oder Linux-Derivate unterstützen und nützen künftig Trusted Computing als Basis für die Gewährleistung von Sicherheit. Die TC-STUDIE vereint ein technisch-wissenschaftliches Team bestehend aus der Technikon Forschungsgesellschaft mbH, der TU Graz (Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie – Univ.-Prof. Dr. R. Posch) und der Fachhochschule Kärnten (Studiengang Public Management – Prof. (FH) Dr. Dietmar Brodel).

Dieses Konsortium hat sich zum Ziel gesetzt, die derzeitige Vorreiterrolle von Österreich im Bereich e-Government in Europa durch eine frühzeitige Bewusstseinsbildung und Migrationsstrategie in Richtung Trusted Computing für die öffentliche Verwaltung nicht nur zu festigen sondern auch wesentlich auszubauen. Die TC-STUDIE analysiert die spezifischen Eigenschaften der öffentlichen Verwaltungsstrukturen in Österreich in Hinblick auf die Kompatibilität mit Trusted Computing, generiert erforderliches Wissen im sicherheitspoli-

tischen Bereich und erstellt konkrete Migrations-szenarien für Schlüssel Anwendungsbeispiele. Im konkreten werden folgende Ziele verfolgt:

- a) Die wesentliche Erhöhung der Sicherheit und des Sicherheitsbewusstseins der Bürgerinnen und Bürger durch Absicherung der kritischen IT-Infrastruktur der öffentlichen Verwaltung
- b) Erzielung von Technologiesprüngen im IT-Security-Bereich der öffentlichen Verwaltung in Österreich durch rechtzeitige Analyse und gezielte Ausarbeitung von Migrationsszenarien

Gleichzeitig werden die Aktivitäten und Ergebnisse das Wachstum der Sicherheitswirtschaft und – Forschung stimulieren. Zu erwarten sind:

- c) erhöhte Forschungsaktivitäten an Universitäten und Fachhochschulen zum Bereich Trusted Computing,
- d) ein rechtzeitiger Aufbau von notwendigem Know-how am österreichischen Berater-Markt, und
- e) gezielte Produktentwicklungen mit Trusted Computing Funktionalität bei zahlreichen österreichischen CRM, e-Government, oder e-Banking Solution Providern.

Die Arbeiten zur TC-STUDIE werden die herausragenden österreichischen Beziehungen zur internationalen Trusted Computing Sicherheitsforschung nützen und weiter ausbauen.

ProjektleiterIn / Unternehmen:

TECHNIKON Forschungsgesellschaft mbH

Kontakt:

Herbert Petautschnig

Tel.: +43 4242 233 55

Fax: +43 4242 233 55 77

E-Mail: coordination@technikon.com

Web: www.trusted-computing.at

UTSI

Urbane Transitionsräume und ihre Sicherheiten

Erst eine genaue Analyse potenzieller Gefahren und Bedrohungen an Transitionsräumen ermöglicht es, zielführend Sicherheitsvorkehrungen für diese Orte treffen zu können. Die geplante Studie soll deshalb einen Überblick über Gefahrenquellen „neuralgischer Orte“ bieten. Ziel der Studie ist es, typische Gefährdungen und Bedrohungen zu eruieren und Anregungen und Lösungsmöglichkeiten aufzuzeigen, um diese zu entschärfen.

In einer globalisierten Welt, sind die Orte, an denen die Kommunikationsströme der Güter, Informationen und Menschen aufeinander treffen, sich überschneiden und einander durchdringen, sicherheitspolitisch von besonderer Bedeutung. Als Schnittstellen, Knotenpunkte, Umschlagorte, Transformationsorte lassen sich allgemein Räume des Übergangs, der Transition beschreiben, in denen sich der routinemäßige Ablauf (des Transports, des Verkehrs, der Kommunikation) in einer

kritischen Phase befindet. Die Flüchtigkeit, Wandelbarkeit und Beschleunigung dieser Vorgänge gerät mit der Festigkeit gebauter Strukturen in Konflikt.

Um zielführend Sicherheitsvorkehrungen treffen zu können, bedarf es einer genauen Analyse potenzieller Gefahren und Bedrohungen dieser Transitionsräume. Die geplante Studie soll einen Überblick über Gefahrenquellen „neuralgischer Orte“ (die auch Angstorte für die Bevölkerung darstellen können) bieten. In der Vergangenheit zeigte sich, dass gerade diese Orte, an denen viele Menschen, Güter und Transportmittel aufeinander treffen und die als wichtige Drehscheiben für die Mobilität der Bevölkerung gelten, Ziel von Bedrohungen und auch terroristischen Angriffen sind. Ziel der Studie ist es, typische Gefährdungen und Bedrohungen (Bedrohungsszenarien) zu eruieren und in einem zweiten Schritt Anregungen





und Lösungsmöglichkeiten aufzuzeigen, um diese zu entschärfen - mit dem Zweck die Sicherheit der Bevölkerung zu erhöhen. Um der Vielschichtigkeit und Vielfältigkeit transitorischer Orte und ihrer Bedrohungslagen gerecht zu werden, ist es notwendig, Sicherheit (in seinen verschiedenen Facetten) als ein Produkt, räumlicher, technischer und sozialer Interaktionsmuster zu analysieren.

Das Forschungskonzept stellt durch die Kombination von kriminologischen, raum- und techniksoziologischen Gesichtspunkten sowie städte- und raumplanerischen Perspektiven eine wesentliche Grundlage für künftige Maßnahmen dar, die darauf abzielen, transitorische Orte sicherer zu gestalten.

Das Projekt ist in vier zentrale Forschungsschritte gegliedert:

TEIL A: Vorphase

Erarbeitung des theoretischen Hintergrunds sowie Durchführung einer umfassenden Literaturrecherche

TEIL B: Fallstudien

Interviews mit ExpertInnen:
Im Rahmen der Studie werden drei Verkehrsknotenpunkte einer detaillierten Analyse im Hinblick auf potenzielle Bedrohungsszenarios unterzogen. Die Auswahl der Orte erfolgt anhand deren Frequenz, bestehender Disorder-Phänomene, krimineller Vorfälle bzw. deren Attraktivität für (terroristische) Angriffe. Die Analyse eines Flughafens, einer hochfrequentierten U-Bahnstation sowie eines Bahnhofs ist geplant. In dieser Phase werden pro neuralgischem Ort n=10 qualitative Interviews mit ExpertInnen (z.B. Sicherheitsbeauftragten) bzw. BenutzerInnen (z.B. Geschäftstreibenden) durchgeführt. Ziel dieser Erhebungsphase ist, Informationen über die jeweiligen Sicherheitsvorkehrungen, potenzielle Wahrnehmungen über den Ort und eventuell kriminelle Ereignisse zu sammeln.

TEIL C: Dokumentenanalyse:

Die Analyse von Systemanfälligkeiten und potenzieller Schwachpunkte wird durch eine Analyse von Notfallhandbüchern und Sicherheitsprotokollen (Prozessdaten) der untersuchten Verkehrsknotenpunkte ergänzt. Diese Analyse dient als Vorbereitung für gezielte Beobachtungen in der Feldphase.

TEIL D: Beobachtungsphase:

Die drei untersuchten Verkehrsknotenpunkte werden einer fallbezogenen Analyse unterzogen. In der ethnographisch ausgerichteten Analyse werden Raum, soziales Handeln und der Einsatz sicherheitstechnischer Instrumente in ihrem Zusammenspiel zur Herstellung und Aufrechterhaltung von Sicherheit herausgearbeitet. Gemeinsam mit Stadt- und RaumplanerInnen werden Beobachtungskriterien aufgestellt anhand derer die ausgewiesenen Orte untersucht werden. Unter Berücksichtigung kriminologischer sowie raumplanerischer Aspekte werden kritische Punkte im Hinblick auf Sicherheitsvorkehrungen und Problembereiche identifiziert. In einem weiteren Schritt werden Lösungsvorschläge aufgezeigt, um potenzielle Schwachstellen zu kompensieren und Konflikte und Gefahren an diesen Orten zu entschärfen.

ProjektleiterIn / Unternehmen:

Kuratorium für Verkehrssicherheit (KfV)

PartnerInnen:

- Österreichisches Institut für Raumplanung (ÖIR)
- ÖIR-Projekthaus GmbH

Kontakt:

Mag. Birgit Zetinigg
Schleiergasse 18
1100 Wien
Tel.: +43 577077-0
Fax: +43 577077-1499
E-Mail: birgit.zetinigg@kfv.at
Web: www.kfv.at

Zivilschutz

Evaluierung von österreichischen Zivilschutzmaßnahmen hinsichtlich Akzeptanz und Zufriedenheit in der Bevölkerung und bei ExpertInnen

Das vorliegende Forschungsprojekt zielt darauf ab, österreichische Zivilschutzmaßnahmen einerseits hinsichtlich Akzeptanz und Zufriedenheit innerhalb der Bevölkerung zu evaluieren bzw. andererseits ExpertInnen bezüglich Status quo und ge-

planter Maßnahmen zu befragen, um die Resultate dieser Erhebungen in die Aus- und Fortbildungsmodule der Zivilschutzschule einfließen lassen zu können.





Ein Schwerpunkt im Bevölkerungs-Fragebogen wird auch dem subjektiven Sicherheitsempfinden bzw. den Sicherheitsbedürfnissen, dem Vertrauen in die Organe bzw. die Technologie sowie der Technikakzeptanz und dem Kommunikations- und Informationsprozess im Krisenfall gewidmet sein.

In den ExpertInnen-Interviews werden die aktuellen Aus- und Weiterbildungsmodule der Zivilschutzschule evaluiert sowie die allgemeinen Gefahrenpotenziale. Der Stellenwert der Prävention auch in Bezug auf deren wirtschaftliche Bewertung soll von den ExpertInnen geschätzt werden.

ExpertInnen-Ebene:

Unterschiedliche Akteure werden interviewt: Spezialisten in der öffentlichen Verwaltung, Praktiker in Einsatzorganisationen wie Feuerwehr, Bundesheer, Rettung, Polizei, etc.) sowie ExpertInnen auf Universitätsebene.

Es ist angedacht, auf dem Sektor öffentliche Verwaltung und auf Universitätsebene rund 10-15 ExpertInnen in einem persönlichen Gespräch mit einem strukturierten Fragebogen (Gesprächsleitfaden) zu interviewen. In den Einsatzorganisationen wird die Befragung mit einem standardisierten Fragebogen durchgeführt. Die Fallzahl wird hier aufgrund der Gruppengröße erweitert: Das Sampling sieht hier eine Stichprobe von 200 vor, wobei hier ExpertInnen auf Länder- und Gemeindeebene kontaktiert werden.

Einsatzorganisationen	Polizei	BH	FW	Rettung	Sonst.
Bundesländer					
Wien	40	40	40	40	40
NÖ/Bgld	12	12	12	12	12
Stmk/K	7	7	7	7	7
OÖ/Sbg	7	7	7	7	7
T/Vbg	7	7	7	7	7

Bevölkerungs-Ebene:

Die repräsentative Bevölkerungsbefragung (Stichprobe: 1.500) sieht vor, dass alle maßgeblichen Gruppen in der Bevölkerung vertreten sein werden: Repräsentativ nach Geschlecht, Alter, Bildungsniveau, beruflichem Status (berufstätig: Branche, arbeitslos, karenziert, StudentIn/SchülerIn, etc.), sozialer Stellung im Beruf, geographischer Lage des Wohnumfeldes (Stadt, Land, Bundesland), privatem Status: Single, Lebensgemeinschaft, Familie. Diese detaillierte Stichprobe lässt es zu, dass tiefergehende Aussagen bezüglich Informationsniveau und Sicherheitsempfinden seitens der Bevölkerung getroffen und seitens des BM.I. bedarfsgerechte Informationsmaßnahmen gesetzt werden können.

Die Studie hat damit zum Ziel das Gemeinwesen in Österreich durch die Evaluierung von konkreten Maßnahmen im Bereich Zivilschutz zu verbessern und sicherer zu gestalten. Dies wird durch die Mehrebenenstruktur der Erhebung bei unterschiedlichen zu befragenden Gruppen - einerseits auf organisatorischer Ebene in den Ländern und Gemeinden bzw. im Bund (ExpertInnen-Befragung) und andererseits auf individueller Ebene (Bevölkerungsbefragung, siehe oben) gewährleistet.

ProjektleiterIn / Unternehmen:

IHS, Institut für Höhere Studien und wissenschaftliche Forschung, Wien, Stumpergasse 56, 1060 Wien

PartnerInnen:

■ SIAK im BM.I, Sicherheitsakademie, Institut für Wissenschaft und Forschung, Wien

Kontakt:

Mag. Dr. Susanne Kirchner
 Tel.: +43 1 59991-306
 Fax: +43 1 59991-555
 E-Mail: Kirchner@ihs.ac.at
 Web: www.ihs.ac.at



Kontakte

Programmverantwortung

Bundesministerium für Verkehr, Innovation und Technologie (BMVIT)

Stabsstelle für Technologietransfer und Sicherheitsforschung

1010 Wien, Renngasse 5

Ansprechpartner: MR Dr. Gernot Grimm

Tel.: +43 1 711 62 – 653128

Fax: +43 1 711 62 – 653130

E-Mail: gernot.grimm@bmvit.gv.at

www.kiras.at

www.bmvit.gv.at

Programmabwicklung und -management

Österreichische Forschungsförderungsgesellschaft – FFG

1090 Wien, Sensengasse 1

Ansprechpartner: DI Johannes Scheer

Tel.: +43 (0) 5 77 55 – 5070

Fax: +43 (0) 5 77 55 – 95070

E-Mail: johannes.scheer@ffg.at

www.ffg.at

