

5th SECURITY RESEARCH CONFERENCE, BERLIN, SEPTEMBER 7th – 9th, 2010

SECURITY OF TRANSPORT SYSTEMS

BUILDING PROTECTION

SURVEILLANCE AND CONTROL

PROTECTION AND RESCUE OF PEOPLE

SECURITY-RELATED LEGAL AND ETHICAL PRINCIPLES

DETECTION OF HAZARDOUS MATERIALS

PROTECTION OF SUPPLY NETWORKS

SECURITY OF COMMUNICATION NETWORKS

5th SECURITY RESEARCH CONFERENCE BERLIN, SEPTEMBER 7th – 9th, 2010

CONFERENCE VENUE

Landesvertretung Baden-Württemberg
Tiergartenstr. 15

10785 Berlin, Germany

ORGANIZATION AND CONTACT

Future Security 2010
Fraunhofer IAF
Tullastrasse 72
79108 Freiburg, Germany
Phone +49 761 5159-458
Fax + 49 761 5159-71-458
contact.futsec@iaf.fraunhofer.de

www.future-security.eu

CONFERENCE HOST: FRAUNHOFER GROUP FOR DEFENSE AND SECURITY

- Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut EMI, Freiburg
- Fraunhofer Institute for High Frequency Physics and Radar Techniques FHR, Wachtberg
- Fraunhofer Institute for Communications, Information Processing, and Ergonomics FKIE, Wachtberg
- Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institut HHI, Berlin
- Fraunhofer Institute for Applied Solid State Physics IAF, Freiburg
- Fraunhofer Institute for Chemical Technology ICT, Pfinztal
- Fraunhofer Institute for Integrated Circuits IIS, Erlangen
- Fraunhofer Institute for Technological Trend Analysis INT, Euskirchen
- Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, Karlsruhe and Ettlingen

www.ws.fraunhofer.de

Future Security
Security Research Conference



FOREWORD

Welcome to the 5th Security Research Conference 2010 in Berlin. Today this fairly new conference series is already a well established building block in the emerging field of security research. The symposium will cover all relevant aspects of new technologies, thus serving as a unique communication platform for decision makers in politics and economy. Leading scientists will be presenting their latest results in the complex field of security research.

A number of outstanding presentations are scheduled this year. The scientific program features 3 plenary, 10 invited and about 50 oral contributions structured into 8 sessions. In addition, more than 50 posters will be presented. The wide range of topics addressed will give a detailed overview about the multi-faceted aspects of civil security.

My sincere thanks go to the German Federal Ministry of Education and Research (BMBF) for its patronage of this symposium and the reliable funding of important security research projects.

Security for Europe's citizens cannot be ensured based on isolated national activities but only in close international cooperation. In this spirit a number of bilateral German-Israeli projects have been launched recently. We are very proud to present these activities at our conference.

The organizers hope you will enjoy the conference and participate in fruitful discussions which will hopefully lead to new partnerships.

Oliver Ambacher
Future Security 2010 Conference Chair

GENERAL INFORMATION

TOWARDS A MORE SECURE FUTURE

One of Europe's main objectives is to preserve its values as an open society, including respect for fundamental rights and freedom, while counteracting increased and diversified security threats. Natural disasters and technological accidents, but also terrorism, organized crime and sabotage can cause serious damage and disruption with long-lasting consequences for economy and quality of life. Secure energy and transportation networks, internet and telecommunication services, provision of food and healthcare, are vital prerequisites for everyday life in our highly networked society.

Despite using robust technologies, our supply chains and networks are most vulnerable to even just small disruptions. Global mobility facilitates the spread of crime, terrorism and diseases and makes them challenging to control. To achieve sustainable success in civil security the development and implementation of new security technologies is mandatory.

SCOPE OF THE CONFERENCE

The symposium will cover all relevant aspects of modern security research. Decision makers in politics and economy are given the opportunity to meet scientists presenting their latest results in the field of security research.

The technical program consists of plenary and invited talks as well as of contributed oral and poster presentations. The conference will be opened on Tuesday, September 7, 2010, at 11:00 am, followed by three plenary talks and eight technical sessions which will run to the end of the conference on Thursday, September 9, 2010, at 5:30 pm.

PLENARY SPEAKERS

P. WEISSENBERG, EUROPEAN COMMISSION, BRUSSELS

H. MEY, EADS, UNTERSCHLEISSHEIM

P. HUSTINX, EDPS, BRUSSELS

INVITED KEYNOTE SPEAKERS

S1 – SECURITY OF TRANSPORT SYSTEMS

M. Hellenthal, Thales Deutschland, Stuttgart, D

S2 – BUILDING PROTECTION

A. Seyfried, Forschungszentrum Jülich, D

S3 – SURVEILLANCE AND CONTROL

A. Hampapur, IBM T. J. Watson Research Center, Yorktown Heights, NY, USA

J. Krüger, TU Berlin, D

S4 – PROTECTION AND RESCUE OF PEOPLE

S. Lechner, European Commission – JRC, Ispra, I

S5 – SECURITY-RELATED LEGAL AND ETHICAL PRINCIPLES

V. Schmid, Technische Universität Darmstadt, D

S6 – DETECTION OF HAZARDOUS MATERIALS

H. Ries, Smiths Detection, Wiesbaden, D

S. Waldvogel, Universität Mainz, D

S7 – PROTECTION OF SUPPLY NETWORKS

L. Sönnichsen, Kuehne + Nagel, Hamburg, D

S8 – SECURITY OF COMMUNICATION NETWORKS

G. Schäfer, Technische Universität Ilmenau, D

TIMETABLE

TUESDAY, 07 SEPTEMBER

9:45 - 10:30 Press Conference

10:00 - 14:00 Registration

11:00 - 11:30 Opening

Oliver Ambacher, Fraunhofer IAF
Helge Braun, BMBF
Rainer Krug, BMVg
Günther Leßnerkraus, Wirt.-Min. BW

11:30 - 13:00 Plenary Session

Chair: Klaus Thoma, Fraunhofer EMI
Paul Weissenberg, European Commission
Holger Mey, EADS
Peter Hustinx, European Data
Protection Supervisor

13:00 - 14:00 Lunch Break

14:00 - 15:30 Session 1

Chair: Jürgen Stock, BKA
Security of Transport Systems
Keynote: Markus Hellenthal, Thales Deutschland
German-Israeli Cooperation
Project RETISS
S 1.1 Ziehm, S 1.2 Henrique,
S 1.3 Arendt, S 1.4 Evers

15:30 - 16:30 Coffee Break – Poster Presentation

16:30 - 17:30 Session 2

Chair: Peter Elsner, Fraunhofer ICT
Building Protection
Keynote: Armin Seyfried, FZ Jülich
German-Israeli Cooperation
Project ACISS
S 2.1 Brenneis, S 2.2 Stolz

17:30 - 18:00 Break

18:00 - 19:30 Welcome Reception

WEDNESDAY, 08 SEPTEMBER	THURSDAY, 09 SEPTEMBER
<p>09:00 - 10:30 Session 3 Chair: Jürgen Beyerer, Fraunhofer IOSB Surveillance and Control I Keynote: Arun Hampapur, IBM German-Israeli Cooperation Project LiveDetect3D S 3.1 Beigang, S 3.2 Murtonen, S 3.3 Weiland, S 3.4 Hübers</p>	<p>09:00 - 10:30 Session 6 Chair: Maurus Tacke, Fraunhofer IOSB Detection of Hazardous Materials I Keynote: Hermann Ries, Smiths Detection Project IRLDEX S 6.1 Röseling, S 6.2 Scorsone, S 6.3 Le Tourneur, S 6.4 Bongartz</p>
<p>10:30 - 11:30 Coffee Break – Poster Presentation</p>	<p>10:30 - 11:30 Coffee Break – Poster Presentation</p>
<p>11:30 - 13:00 Session 3 Chair: Uwe Wiemken, Fraunhofer INT Surveillance and Control II Keynote: Jörg Krüger, TU Berlin German-Israeli Cooperation Project BEPE S 3.5 Künzner, S 3.6 Feierlein, S 3.7 Viitanen, S 3.8 Lopatka</p>	<p>11:30 - 13:00 Session 6 Chair: Joachim Ender, Fraunhofer FHR Detection of Hazardous Materials II Keynote: Siegfried Waldvogel, Univ. Mainz German-Israeli Cooperation Project ChipSenSiTek S 6.5 Wehner, S 6.6 Rosenstock, S 6.7 Hermanns, S 6.8 Woda</p>
<p>13:00 - 14:00 Lunch Break</p>	<p>13:00 - 14:00 Lunch Break</p>
<p>14:00 - 15:30 Session 4 Chair: Wilfried Gräfling, Landesbranddirektor Berlin Protection and Rescue of People Keynote: Stephan Lechner, IPSC German-Israeli Cooperation Project I-LOV S 4.1 Klein, S 4.2 Raskob, S 4.3 Felsenstein, S 4.4 Donner</p>	<p>14:00 - 15:30 Session 7 Chair: Jochen Schiller, FU Berlin Protection of Supply Networks Keynote: Lorenz Sönnichsen, Kuehne + Nagel German-Israeli Cooperation Project IRLSENS S 7.1 Schuchert, S 7.2 Eriksson, S 7.3 Peinel, S 7.4 Barrass</p>
<p>15:30 - 16:00 Coffee Break – Poster Presentation</p>	<p>15:30 - 16:00 Coffee Break</p>
<p>16:00 - 17:30 Session 5 Chair: Michael Friedewald, Fraunhofer ISI Security-Related Legal and Ethical Principles Keynote: Viola Schmid, TU Darmstadt German-Israeli Cooperation Project ESR S 5.1 Geisler, S 5.2 Vagts, S 5.3 Schnieder, S 5.4 Sellke</p>	<p>16:00 - 17:30 Session 8 Chair: Markus Ullmann, BSI Security of Communication Networks Keynote: Günter Schäfer, TU Ilmenau German-Israeli Cooperation Project EMSIN S 8.1 Schmidt, S 8.2 Jahnke, S 8.3 Adameit, S 8.4 Kirschnick</p>
<p>17:30 - 19:00 Break 19:00 - 23:00 Conference Dinner</p>	<p>17:30 - 17:40 Conference Closing</p>

TABLE OF CONTENTS

OPENING

	<i>O. Ambacher, Conference Chairman, Fraunhofer IAF, Freiburg, D</i>
p13	H. Braun, Federal Ministry of Education and Research BMBF, D
p14	R. Krug, Federal Ministry of Defense BMVg, D
p15	G. Leßnerkraus, Ministry of Economics of the State of Baden-Württemberg, D

PLENARIES

p16	P. Weissenberg	Future Security Research
p18	H. Mey	Future Security Challenges – A Strategic Assessment
p20	P. Hustinx	Making Data Protection More Effective in a Digital World

KEYNOTES

p22	M. Hellenthal	Security in Transportation Systems
p30	A. Seyfried	Rescue and Protection of People in Buildings – Understanding Crowd Movement Through Experiment and Simulation
p36	A. Hampapur	Information Analytics for Public Safety and Homeland Security
p44	J. Krüger	Secure Identity – A Source for Innovative IT-Systems and Processes
p52	S. Lechner	Remote Sensing for Damage Assessment in Humanitarian Disasters
p60	V. Schmid	German Privacy and IT-Security Law (IT'S Law) as a Contribution to the European Area of Freedom, Security and Justice
p68	H. Ries	Modern Sensors for Hazardous Materials
p76	S. Waldvogel	Detection of Peroxide-Based Explosives
p84	L. Sönnichsen	Security Based on Organization, Control and Technology
p92	G. Schäfer	Secure Overlay-Based Autoconfiguration of Complex IPsec VPN

GERMAN-ISRAELI COOPERATION PROJECTS

p24	S 1	RETISS: Real Time Security Management System for Road Infrastructures
p32	S 2	ACCIS: Automatic Cargo-Container Inspection System
p38	S 3, I	LiveDetect3D: Live Detection of Hidden Threats via Real-Time 3D Imaging
p46	S 3, II	BEPE: Biological Event Preparedness Evaluation
p54	S 4	I-LOV: MIXS and DETUS – Two Major Bilateral Technology Advances for Improving Capability Responses in Emergency Missions
p62	S 5	ESR: System Trust and Crisis Management – An Interactive Expert Exchange System for Enhancing Societal Resilience
p70	S 6, I	IRLDEX: Imaging Stand-Off Detection of Explosives by Quantum Cascade Laser Based Backscattering Spectroscopy
p78	S 6, II	ChipSenSiTek: Femtosecond Impulsive Laser Excitation and Quartz Enhanced Photoacoustic Spectroscopy for Explosive Detection
p86	S 7	IRLSENS: Infrared Fiberoptic Laser Sensor System for the Detection and Recognition of Hazardous Chemical Substances in Drinking Water
p94	S 8	EMSIN: Electromagnetic Protection of IT-Networks for Transportation-Infrastructures

SESSION 1 SECURITY OF TRANSPORT SYSTEMS

p25	S 1.1	Risk Analysis of Representative Terror Events on Airports Within the Project FluSs
p26	S 1.2	Passenger Flow at Hub Airports: Security, Retail and Infrastructure Investments
p27	S 1.3	The Requirement for Scanning Export Containers
p28	S 1.4	Visual Intelligence and Secure RFID Protect Road Tunnels Within the Framework of the SKRIBT Project

SESSION 2 BUILDING PROTECTION

p33	S 2.1	Protection of Critical Infrastructure-Buildings Against Dynamic Loads Caused by Attacks and Accidents
p34	S 2.2	Tunnel Structures Subjected to Explosions

TABLE OF CONTENTS

SESSION 3 SURVEILLANCE AND CONTROL

p39	S 3.1	TEKZAS THz Real-Time Camera (Two-Dimensional) for Application in Security Technology
p40	S 3.2	Development of BtoB Security Business – From Guarding to Knowledge-Intensive Expert Services
p42	S 3.3	Range-Gated Active Imaging Technology for Surveillance and Control of Areas
p43	S 3.4	Integrated Security Monitor for Control of Persons
p47	S 3.5	Integrated Mobile Security Kit
p48	S 3.6	European Border Surveillance: Solutions from the EUROSUR Technical Study
p49	S 3.7	Software Tools for the Development of Distributed Intelligence Surveillance Networks
p51	S 3.8	Improving Automatic Surveillance by Sound Analysis

SESSION 4 PROTECTION AND RESCUE OF PEOPLE

p55	S 4.1	Emergency Management in Large Infrastructures – the EU-Project EMILI
p56	S 4.2	SECURITY2People
p57	S 4.3	Challenges in Maritime Safety and Security Training Using a Specific Safety & Security Trainer (SST)
p59	S 4.4	IT-Supported Management of Mass Casualty Incidents: The e-Triage Project

SESSION 5 SECURITY-RELATED LEGAL AND ETHICAL PRINCIPLES

p63	S 5.1	A System Analysis Approach to Security
p64	S 5.2	New Approaches for Data Protection and Anonymization in Surveillance Systems
p65	S 5.3	Safety and Security; Two Sides of the Same Coin: Properties and Relations? Characteristics to Refine? Structure of Terminology and its Perception
p66	S 5.4	Public Information Responses After Terrorist Events (PIRATE)

SESSION 6 DETECTION OF HAZARDOUS MATERIALS

- p71** S 6.1 Evaluation of Explosive Detection Systems – Method Development, Testing, Benchmarking, Certification
- p72** S 6.2 Nanodiamond Coated SAW Platform for Sensing of Explosive and Warfare Gases at High Sensitivity
- p73** S 6.3 Neutron Technology Applied to Hazardous Materials Detection
- p74** S 6.4 Airport Related CBR Threat Analysis
- p79** S 6.5 Biosensors for Standoff-Detection of Mines and Explosives by Laser Induced Fluorescence
- p80** S 6.6 Prevention of Illicit Trafficking of Nuclear and Radioactive Material at Border Stations by Means of Highly Efficient Detection Systems
- p81** S 6.7 Public and User Acceptance of Unmanned Aerial Vehicles in Disaster Management and Prevention – Empirical Findings
- p82** S 6.8 Chip Cards as Fortuitous Individual Dosimeters after Nuclear Emergencies and Radiological Terrorism

SESSION 7 PROTECTION OF SUPPLY NETWORKS

- p87** S 7.1 A New Device for Monitoring Drinking Water Based on Image Analysis
- p88** S 7.2 Safety and Security of Drinking Water Distribution Systems
- p89** S 7.3 Deploying Process Management for Emergency Services Lessons Learnt and Research Required
- p91** S 7.4 Defending Food Supply Chains - a UK Approach

SESSION 8 SECURITY OF COMMUNICATION NETWORKS

- p95** S 8.1 A Hierarchical Framework for Quantitative Corporate IT Risk Management
- p96** S 8.2 Automatic Network Reconfiguration for Denial-of-Service Defense Using Dynamic Impact Estimation
- p97** S 8.3 Herold - Agent Oriented, Policy-Based Network Security Management
- p98** S 8.4 Usability of Biometrics on Mobile Phones

TABLE OF CONTENTS

POSTERS

p100	P 1	Prevention of Road Transports from Organized Crime
p101	P 2	Peer-to-Peer-Integration of Security-Oriented IT-Systems in Public Urban Transport
p102	P 5	A Reliable, Fast and Easy-to-Use Simulation Method for Blast Propagation in Urban Scenarios
p103	P 6	Tunnel Stability after Explosions From the Viewpoint of Dynamic Soil-Structure Interaction
p104	P 7	Advances on Chemical Gas Sensors for Detection of Explosives: From Concepts of Employment to Sensor-Array Systems
p105	P 8	Rapid Field Testing of Biological Threats With Lab-on-a-Chip Systems
p106	P 9	Liquid Screening by High- T_c Josephson Technology
p107	P 10	Concept of a Cooperation Project for the Development of a Chip-Based On-Site Detection System for Animal Diseases
p108	P 11	A New Approach for Dose Assessment in Urban Environments After Nuclear Emergencies and Radiological Terrorism
p109	P 12	Hidden Hazards – Appropriate Scanning Remains a Challenge
p110	P 13	EXAKT – Joint BMBF Research Project: Project Status Update on Near Real-Time Trace Analysis of Airborne Chemical Warfare Agents and Explosives
p111	P 14	Laser-Induced Breakdown Spectroscopy at the DLR Laser Test Range
p112	P 15	Photonic Sensors for Explosive Detection
p113	P 16	Contactless and Direct MS-Techniques for the Surveillance of Clandestine Production Facilities of Synthetic Drugs and Improvised Explosives
p114	P 17	An Integrated Approach to Deal With the CBRNE Threat Within the EU – DECOTESSC 1
p115	P 18	Immediate Identification of Single Bacteria - Novel Methods and Instrumentation
p116	P 19	Nanosize MOX Thin Film Gas-Sensitive Elements for Detection of Explosive Vapours
p117	P 20	The Project Safe inside – Trace Detection of Security Relevant Substances by Single Photon Ionization Ion Trap Mass Spectrometry (SPI-ITMS)
p119	P 21	CHORUS - Car Horns Used as Sirens
p120	P 22	Providing Dynamic Escape Routes to Support Self Rescue in Subway Systems
p121	P 23	Early Identification of Occurring Incidents at Big Events and Evacuation Modelling
p122	P 24	HERMES – Evacuation Assistant for Arenas
p123	P 25	Integrated Crisis Management for Disaster Relief - Communications, Navigation, Geo Information -
p125	P 26	SOGRO – Is Electronic Triaging the Solution to Fast Delivery of Patient Status in Case of an MCI?
p126	P 27	IDMA – How to Gain Efficiency by Means of Mobile Information Technology

p127	P 28	Landmarke Project: Development of Navigation Technology for Firefighters and Work Practices
p128	P 30	Social Scientific Expertise and Concomitant Research
p129	P 31	Private and Corporate Security Management: Introduction to a New Master-Programme
p130	P 32	Pro-Active and Effective Aviation Security Research Based on Stakeholders' Dialogue
p131	P 33	Limits, Rules and the Need for Transparency in Biosecurity Research
p132	P 34	Optimization of the Antenna Distribution of a Microwave-Based Body Scanner Profiting From an Automatic Quality Assessment of the Microwave Images
p133	P 35	A New Security Concept on Airports Using a Rotating W Band Person Scanner Within a Sensor Network
p134	P 36	Water-Fog-Generator Based on a Rocket-Burner to Dissolve Violent Demonstrations
p135	P 37	Non-Intrusive Continuous User Behavior Analysis Using Computerized Systems
p136	P 38	The Sensor Grid – An Integrated Security Solution
p137	P 39	Teams Rather Than Individuals: Collaborative Intrusion Detection
p138	P 40	Bi-Spectral Quantum-Effect Infrared Detectors for Security and Surveillance
p139	P 41	Integrated Circuits Beyond 100 GHz for Stand-Off Detection of Concealed Weapons
p140	P 42	PreBorderLane - Technology Must Adapt to People, Not People to Technology
p141	P 47	InfoStrom: Learning Information Infrastructures for Crisis Management in Medium to Large Electrical Power Breakdowns
p142	P 48	Context Adaptive Service Selection Within a SOA for Surveillance Applications
p143	P 49	Standardisation of Reports to Optimise Cooperation in the Domain of Public Safety and Security
p144	P 50	Cyber Defence in Future Communication Networks – A Multilayer Security Architecture
p145	P 51	MEVIM – Mobile Evidence Inventory Management
p146	P 52	Static Smartphone Malware Detection
p147	P 53	Secure Context-Aware Reconfiguration for Mobile Devices
p148	P 54	An Overview – Core Element for Interoperability in Networked Security
p149	P 55	SPIDER - Security System for Public Institutions in Disastrous Emergency Scenarios
p150	P 56	IP-Based Application and Services for Next Generation Networks
p151	P 57	The Emergency Misuse Problem: Detection and Prevention
p152	P 58	Security Assessment of the Evolved Packet Core

PROGRAM COMMITTEE

- Prof. Dr. Oliver Ambacher, Fraunhofer IAF
- Prof. Dr. Achim Bachem, Forschungszentrum Jülich GmbH
- Prof. Dr. Bernd Becker, Albert-Ludwigs-Universität Freiburg
- Prof. Dr.-Ing. Jürgen Beyerer, Fraunhofer IOSB
- Dr. Peter Boßdorf, Report Verlag GmbH
- Dr. Adam S. Cumming, DSTL, UK
- OTL i. G. Armin Dirks, Bundesministerium der Verteidigung
- Prof. Dr. Claudia Eckert, Fraunhofer SIT
- Prof. Dr.-Ing. Peter Elsner, Fraunhofer ICT
- Prof. Dr.-Ing. Joachim Ender, Fraunhofer FHR
- Reinhold Friedrich, Bundesministerium für Bildung und Forschung
- Dr. Jürgen Geisler, Fraunhofer IOSB
- Dr. Herve Graindorge, SNPE Matériaux Energetiques / CRB
- MinR Dr. rer. pol. Ehrentraud Graw, Wirtschaftsministerium Baden-Württemberg
- Prof. Dr. Jürgen Grosche, Fraunhofer FKIE
- Karsten Heidrich, Deutsche Bank AG
- Prof. Dr.-Ing. Albert Heuberger, TU Ilmenau
- MinR Rainer Krug, Bundesministerium der Verteidigung
- Monika Lieberam, Bundesanstalt Technisches Hilfswerk (THW)
- Prof. Markku Mesilaakso, Ph.D., Defence Forces Technical Research Center, Finland
- Prof. Dr. Bernd Michel, Fraunhofer IZM
- Dr. Joachim Schulze, Fraunhofer INT
- Dr. Alois J. Sieber, European Commission - Joint Research Centre
- Françoise Simonet, CEA Commissariat à l'Énergie Atomique
- Prof. Dr. Jürgen Stock, Bundeskriminalamt
- Christoph Stroschein, German European Security Association e.V.
- Prof. Dr. Maurus Tacke, Fraunhofer IOSB
- Prof. Dr. Klaus Thoma, Fraunhofer EMI
- Markus Ullmann, Bundesamt für Sicherheit in der Informationstechnik
- Dr. Albert C. van der Steen, TNO Defence, Security and Safety
- Dr.-Ing. Karin Wey, VDI Verein Deutscher Ingenieure e.V.
- Prof. Dr. Uwe Wiemken, Fraunhofer INT

OPENING



*Dr. Helge Braun, MdB
Bundesministerium für Bildung und Forschung
Hannoversche Straße 28 - 30
10115 Berlin
helge.braun@bmbf.bund.de*

Dr. Helge Reinhold Braun was born October 18th, 1972, in Gießen, Germany. He studied chemistry at the Philipps-University in Marburg and medicine at the Justus-Liebig-University in Gießen. From 2001 to 2009 he worked at the *Clinic for Anesthesiology, Critical Care and Pain Management* of the University of Gießen.

Dr. Braun has been a member of the Gießen Municipal Parliament since 1997. From 2002 to 2005 he was a member of the National German Parliament and a member of the Committee for Education, Research and Development. He was Chairman of the German CDU Parliamentary Group in the Regional Parliament of Gießen from 2006 – 2009.

Since 2009, Dr. Helge Braun has been member of the National German Parliament again. He works as Parliamentary State Secretary of the Federal Minister of Education and Research.

OPENING



*Ministerialrat Dipl.-Ing. Rainer Krug
Referatsleiter RÜ IV 2
Bundesministerium der Verteidigung
Fontainengraben 150
53123 Bonn
Rainer1Krug@BMVg.BUND.DE*

MinR Rainer Krug is Head of the Branch „Research and Technology Strategy and Planning, International Cooperation in R&T“ inside the Armaments Directorate.

Rainer Krug joined the German Armed Forces in 1974. From 1975 to 1978 he studied Communication and Electronics at the Armed Forces University in Munich. Between 1978 and 1986 Rainer Krug served in the German Army as Platoon Leader and Company Commander. He entered civil service in 1986, taking his Second State Examination in 1988. Between 1988 and 1996 Rainer Krug worked in different positions, such as Assistant Chief of the Section Sonar Technology and Underwater Weapons. In 1996 he became Assistant Chief of the branch Underwater Weapons, Torpedo Technology, Surface Ship Torpedo Defence in the Federal Ministry of Defence.

Rainer Krug was Head of the Section Sonartechnology, Hydroacoustic Systems and Project Realisation Support Vessels in the Federal Office for Defence Technology and Procurement (BWB) between 1998 and 2001. In 2001 he became Director Defence Technology of the Federal Academy for Defence Administration and Technology (BAKWVT), where he worked until he was transferred to the Federal Ministry of Defense in order to establish the branch Armament related Aspects of German Armed Forces Transformation (NEC, CD&E). He became Head of this branch in 2005. Since May 2008, Rainer Krug had been Head of the Branch „Research and Technology Strategy, International Cooperation in R&T“.



*Ministerialdirigent Günther Leßnerkraus
Wirtschaftsministerium Baden-Württemberg
Theodor-Heuss-Straße 4
70174 Stuttgart
leßnerkraus@wm.bwl.de*

Günther Leßnerkraus was born November 10th, 1956 in Esslingen, Germany. He studied law at the University of Tübingen (including First State Law Examination), followed by Legal Preparatory Training and Second State Law Examination. From 1986 to 1989 he worked as Judge and Public Prosecutor at the Local Court Riedlingen, the Regional Court Ravensburg and the Office of the Public Prosecutor Stuttgart.

From 1989 until 1996 Günther Leßnerkraus held various positions in the Ministry of Justice of Baden-Württemberg, the Federal Ministry of Justice and the Federal Foreign Office. In 1996 he joined the Ministry of Economics of Baden-Württemberg and worked in several positions, such as Head of Policy Coordination and Head of Department for Administration and Law. Since 2006, Günther Leßnerkraus has been Head of the Department for Innovation and Technology Transfer at the Ministry of Economics of Baden-Württemberg.

PLENARY

FUTURE SECURITY RESEARCH

In times when money is in short supply, we have to find more efficient ways to fulfil the obligations we have vis-à-vis the citizen who rightfully expects: -protection against terrorism, -protection of our EU borders and for our physical infrastructures, and better co-operation in European Crisis Management.

While it remains the responsibility of the EU Member States to guarantee security to its citizen, many of these obligations can only be fulfilled when done in the European way.

We have an EU Security research programme under FP7 with a budget of 1.4 Billion Euro. This helps European Security key players to learn to better co-operate. But we must go further. We need to get the good ideas coming from doing research together, to lead to a common European approach in providing security together to the citizen. Furthermore we must bridge the internal security / external security actions and the means needed to perform these.

In summary, we need to address 4 factors:

- we need to ensure the availability of knowledge,
- we need to address the fragmentation of the markets,
- we need to get rid of the artificial divide between internal and external, security and
- we need to explore dual use synergies as much as possible.

Facing the pressure of cuts in public spending, we have to find ways as to how – in the future – security research can be made part a holistic approach, ensuring a continuum from ideas to operations.



BIOGRAPHY

Dr. Paul Weissenberg studied law at the Universities of Würzburg and Freiburg (Germany), followed by post-graduate studies in European law in Geneva (Switzerland) and by a PhD (Docteur en droit) in European law at the University of Geneva.

Dr. Weissenberg started working for the European Commission in 1989 as Member of Cabinet of Dr. Martin Bangemann, Vice-President of the European Commission responsible for Industrial Policy. In 1996 he was appointed Head of Cabinet of Dr. Martin Bangemann.

From 2000 to 2005 he was Head of the Single Market Directorate responsible inter alia for automotive and pharmaceutical legislation. He was a Member of the Management Board of the European Medicines Agency (EMA).

Since January 2005 he has been in charge of the Directorate for Aerospace, GMES, Security and Defence and has been appointed Coordinator for Aerospace, GMES, Security and Defence within DG Enterprise and Industry.

Before joining the European Commission he worked in the Cabinet of the Minister of Economics of Germany. He started his career at the Ministry of Economics working in the department dealing with East-West economic relations and competition policy. Mr. Weissenberg was also posted to the German Permanent Representation to the OCDE in Paris and to the Chambers of Commerce in La Paz and Toronto.

Dr. Paul Weissenberg
Director for Aerospace, GMES,
Security and Defence
European Commission
DG Enterprise and Industry
1049 Brussels
paul.weissenberg@ec.europa.eu

PLENARY

FUTURE SECURITY CHALLENGES – A STRATEGIC ASSESSMENT

Assessing future challenges requires both a more traditional trend analysis, which is largely an extrapolation of comparatively stable and predictable trends, as well as a prescription of possible „wild cards“ or disruptive changes. In any case, sound planning needs to deal with uncertainty by making the planning robust enough to make the result largely insensitive against major assumption variations. In other words: No matter what happens, we need to be well prepared and to be able to maintain room for maneuver and freedom to act. There are a number of ways to do that which will be discussed in the presentation.

Future challenges are likely to be related to a number of „knowns“ (like proliferation of weapons of mass destruction, dissemination of high technology, failing states, terrorism, etc.) as well as „unkowns“ (like developments in the area of biotechnologies, nanotechnologies, robotics and artificial intelligence). Technology is part of both the challenge as well as the possible solution. However, technology has to be put into a political context. Usually, any technology is only as useful as the task or mission it serves. Furthermore, key is less technology as such but rather the skillful exploitation of opportunity it creates.



BIOGRAPHY

Holger H. Mey, born in 1958 in Flensburg, Germany, is Head of Advanced Concepts, Defence & Security, European Aeronautic Defence and Space Company (EADS), Munich, Germany.

Before joining EADS in June 2004, Prof. Mey worked for 12 years as a self-employed security policy analyst and consultant in Bonn, Germany. Among many other functions, Prof. Mey served as President & CEO of the Institute for Strategic Analyses (ISA) in Bonn, Germany. Over many years, he was a regular TV and radio commentator. Dr. Mey is an Honorary Professor at the University of Cologne, Germany.

Prof. Mey began his professional career 1986 as a Research Associate at the Stiftung Wissenschaft und Politik (Foundation for Science and Politics) then at Ebenhausen, Germany. From 1990 to 1992, he served as a Security Policy Analyst in the Policy Planning Staff of the German Minister of Defense. From 1992 to 1994, already self-employed, he became the Security Policy Advisor to the Chairman of the Defense Committee in the German Parliament. In 1992, he founded the ISA and became Chairman and Director. Prof. Mey directed over 30 studies for various Ministries and Government Agencies.

He is a member of many international and national foreign and security policy associations, including the International Institute for Strategic Studies (IISS, London) and the Deutsche Gesellschaft für Auswärtige Politik (the German Council on Foreign Relations, DGAP), Berlin.

Prof. Mey published well over 100 articles in major security policy journals, newspapers, and books. He is editor, co-author and author of many books, including „Deutsche Sicherheitspolitik 2030“, Frankfurt: Report Verlag, 2001 (English version: „German Security Policy in the 21st Century“, New York/Oxford: Berghahn Books, 2004).

*Prof. Dr. Holger Mey
Vice President
Advanced Concepts, Defence & Security
EADS
Landshuter Straße 26
85716 Unterschleissheim
holger.mey@eads.com*

PLENARY

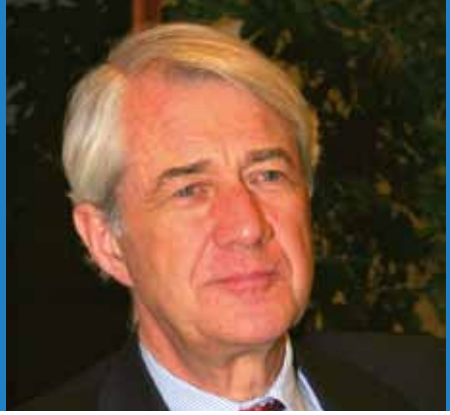
MAKING DATA PROTECTION MORE EFFECTIVE IN A DIGITAL WORLD

The need for data protection is increasingly relevant due to technological change, globalisation and conflicting public interests. However, as recently demonstrated, there is also a need to make data protection more effective in practice and to use more creative methods to reach this result.

Although the challenges in this field are impressive, there are also some important opportunities that should be used well. The Lisbon Treaty has provided a new and much stronger perspective for data protection in the European Union. The right to data protection has become a binding fundamental right not only for EU institutions and bodies, but also for the member states when they are implementing European law.

Other elements of the Lisbon Treaty, such as stronger roles for the Parliament, the Commission and the European Court of Justice in the former „third pillar“ area of police and justice have also contributed to an increased focus on data protection in policy making. This focus is clearly visible in the new 5-year program for the area of Justice and Home affairs („Stockholm Program“) and in the activities of the new Commission, including its current Review of the existing legal framework for data protection and the Digital Agenda. Data protection is also an important part of the Transatlantic Agenda.

This presentation will look at the relevant trends and the prospects for more effective data protection in a more and more ICT dependent and globalised world, where concerns about privacy are increasing, as citizens discover how new technologies are impacting on their lives.



BIOGRAPHY

Peter Hustinx (1945) has been European Data Protection Supervisor since January 2004 and was re-appointed by the European Parliament and the Council in January 2009 for a second term of five years.

He has been closely involved in the development of data protection legislation from the start, both at national and at international level.

Before entering his office, Peter Hustinx was President of the Dutch Data Protection Authority since 1991. From 1996 until 2000 he was Chairman of the Article 29 Working Party.

He received law degrees in Nijmegen, the Netherlands, and in Ann Arbor, USA. Since 1986 he has been deputy judge in the Court of Appeal in Amsterdam.

*Peter Hustinx
European Data Protection Supervisor
Rue Wiertz 60 – MO 63
1047 Brussels
peter.hustinx@edps.europa.eu*

SESSION 1

SECURITY OF TRANSPORT SYSTEMS

KEYNOTE

SECURITY IN TRANSPORTATION SYSTEMS

Security, safety and mobility in an interconnected and networked world are among the global key challenges of the 21st century. The interdependency of these topics concerns nearly every sphere of private or business activity requesting answers from politics and industries. These answers vary from country to country and from one organization to another.

In this context the protection of intermodal transportation infrastructures becomes more and more a key issue from the security point of view, whereas traffic management and navigation aspects have to guarantee a smooth interaction between the different transport modes.

The range of possibilities offers today specific systems for access control and/or perimeter protection as well as sophisticated management solutions integrating information and communication systems in one platform. Today passengers and infrastructures security solutions (on-board and on platform) enable operators to monitor stations, line depots, equipment rooms, control rooms, platform, tracks, doors before departure, to control the access to stations, restricted areas, tracks, to detect: fire, abandoned objects, suspicious behaviour, person or object on the tracks, explosives, biological attacks, to quickly react in case of detected incident or threat, to facilitate rapid reaction through the use of decision aid system, to replay any incident for post analysis or training purposes and to centralise all the key data into one room in case of major crisis.

Thales's competencies cover the whole safety and security chain in terms of air, ground and maritime transportation needs with references worldwide.



BIOGRAPHY

Dr. Markus Hellenthal has served as CEO of Thales Deutschland and senior vice president of Thales since the beginning of 2008. Born in 1957, Dr. Hellenthal is a lawyer and former police official. Prior to joining Thales, he held leading positions in both the private and public sectors in Germany and abroad.

As senior vice president at EADS, he last had group-wide business development responsibility for civilian security solutions. Prior to that he was a partner at the consulting firm Accenture and had various managerial responsibilities at the Federal Ministry of the Interior and the federal police force.

Dr. Hellenthal has represented the interests of German industry as chairman of the European Security Research Advisory Board (ESRAB), the European Organization for Security (EOS) and as a member of other international committees.

After studying law and sociology, Dr. Hellenthal completed his postgraduate work in administrative sciences. He has published over sixty technical papers on security issues in various books and periodicals.

*Dr. Markus Hellenthal
CEO, Thales Deutschland
Lorenzstraße 10
70435 Stuttgart
markus.hellenthal@thalesgroup.com*

SESSION 1

SECURITY OF TRANSPORT SYSTEMS

RETISS: REAL TIME SECURITY MANAGEMENT SYSTEM FOR ROAD INFRASTRUCTURES

J. Krieger¹, I. Kaundinya¹, G. Mayer², W. Balz², and U. Degen³

¹ Federal Highway Research Institute (BASt), Bergisch Gladbach, Germany;

² PTV AG, Stuttgart, Germany; ³ NESS Technologies, Tel Aviv, Israel

kaundinya@bast.de

An effective and secure road network is of major importance to the economy and equally so to the mobility of citizens. Bridges and tunnels in particular, are key elements of the road network. Besides severe accidents, e.g. involving trucks carrying dangerous goods, terrorist attacks are one of the most dangerous threats for such key infrastructures. Restrictions of the availability of these infrastructures may lead to intense traffic interferences on the surrounding road network resulting in negative effects on the road user, high economic follow-up costs and negative environmental impacts. Due to the interdependence of the road transport network with other traffic modes like rail, air and shipping traffic, a failure of important connections could trigger a domino effect.

In order to improve the protection of critical road infrastructures a Real Time Security Management System (RETISS) will be developed and tested in the context of a cooperative research project with partners from Israel and Germany involved. The main objective of the Real Time Security Management System is to improve the security, and thereby the availability of road transport infrastructures, and to protect the users, especially against terrorist attacks and big accidents. RETISS will provide real time information on the current security situation of these infrastructures to the persons responsible for the operation. These data should help operators of road networks and infrastructures to take the best suitable preventative protection measures and, in the case of incidents, the best suitable reactive measures. This paper gives an overview about the content, structure and first results of the research project RETISS.

The project is funded as a German-Israeli cooperation under the programme „Research for Civil Security“ by the German Federal Ministry of Education and Research (BMBF) and the Israeli Ministry of Industry, Trade and Labor (MOITAL).

S 1.1

RISK ANALYSIS OF REPRESENTATIVE TERROR EVENTS ON AIRPORTS WITHIN THE PROJECT FLUSS

J. Ziehm, M. Voss, C. Roller, O. Herzog, and I. Häring

¹ Fraunhofer Institute for High-Speed Dynamics EMI, Freiburg, Germany

ivo.haering@emi.fraunhofer.de

Within the call “Protection of transport infrastructure” the project Airport Security System (acronym FluSS) is operated funded by the BMBF (German Federal Ministry of Education and Research). The aim of the project is to set up a demonstrator containing new and optimized security technologies and processes that will be tested at Frankfurt Airport. Our work starts off by setting up a database to accomplish an event analysis on terroristic events at airports focusing on conventional (explosive) events. The database is analyzed using different attributes, e.g. place of incident at the airport, used weapon, frequency of events and number of casualties. This allows deducing vulnerable points and relevant scenarios at an airport. For multiple relevant exemplary scenarios (in room and free field) a damage analysis is conducted using different software tools to quantify the damage to buildings and selected building components as well as fatalities and injuries mainly due to blast. In this case the damage is calculated as a function of the net explosive quantity of the explosive device for each scenario. Next we combine the results of the event and damage analysis in a semi-quantitative risk analysis. The probability and damages aspects of the scenarios are evaluated within different categories using a scale ranging from one (e.g. not likely) to five (e.g. very likely). Categories being evaluated are the probability using a certain weapon type, the probability of an event at a certain place, the number of effected persons, psychological effects, operative influences and crisis communication. This leads to risk tables and a risk ranking of the scenarios. By definition the approach identifies influence factors that determine the risk of the representative scenarios. Countermeasures are proposed and their effects on reducing the risk are shown. This means mainly reducing the explosive effects (blast) on buildings and building components.

SESSION 1

SECURITY OF TRANSPORT SYSTEMS

S 1.2

PASSENGER FLOW AT HUB AIRPORTS: SECURITY, RETAIL AND INFRASTRUCTURE INVESTMENTS

N. Henrique

European Center for Aviation Development – ECAD GmbH, Lise-Meitner-Str. 10, 64293 Darmstadt
nelson.henrique@ecad-aviation.de

Passenger related security measures at airports have continuously increased in number and complexity, and airport operators have to adjust passenger-related security processes making their operations suffer and their overall passenger flow change. In this context, understanding the airport as a dynamic system is crucial to making correct decisions leading to increased security operations, retail income and efficient investments in airport infrastructure with respect to airport connecting times.

In particular within hub-airport systems, security measures are part of complex, dynamic and interconnected processes. Dynamics in this type of complex system arise, at least in part, from the existence of non-linear passenger flows leading to corresponding peak times due to the specific geographical location of the airport (e.g., North America, Europe, and Asia) and due to their customer profiles (e.g., American, European and Asian airlines). Complexity results from the interactions produced by tens of inbound flights that may feed single outbound flights.

Interconnectivity, in complex systems such as hub airports, means that changing one process in any part of the airport, may impact other processes' performance. In particular, at peak times, potential bottlenecks at security checkpoints may impact connected processes resulting in potential security breaches and costs such as decreasing retail time and increasing number of lost-flight connections due to immediate actual increase in connecting time for passengers at the airport.

The paper explores airport dynamics focusing on the interaction of security measures, retailing and connecting times. First, relevant passenger related security processes and the importance of retailing and connecting times are presented. Secondly, an airport model based on the System dynamics methodology is presented. Finally, airport dynamics are explored. The overall passenger related, operative importance of security measures within the production system hub airport is analyzed and strategies that may lessen potential security problems are suggested.

S 1.3 THE REQUIREMENT FOR SCANNING EXPORT CONTAINERS

F. Arendt

Institute for Shipping Economics and Logistics (ISL), Universitätsallee 11-13, 28539 Bremen
arendt@isl.org

In 2007, a law named «House Resolution No. 1 (H.R.1)» was imposed by the US Congress saying that no container is allowed to enter the US territory from July 1st, 2012, unless it has been X-rayed (scanned) and checked on nuclear substances in the port of loading.

Container terminal operators, port and transport associations as well as political bodies heavily objected against the introduction of this law. If taking granted, implementation is complex: involved parties and responsibilities, legal aspects, locations, processes for truck, rail, inland waterway transport and transshipment (those being received and further shipped by sea), costs, technologies, IT integration, etc.

One port being especially affected by this law is the port of Bremerhaven. In 2007, more than 24% of all export containers from the European Union to the US passed that port, in figures : 617.000 TEU (twenty-foot equivalent units) – about more than 1.700 TEU per day!

A consortium of industrial players and research organisations lead by the Bremen/Bremerhaven-based Institute of Shipping Economics and Logistics (ISL) have successfully submitted an R&D proposal for a project named ECSIT (Erhöhung der Containersicherheit durch berührungslose Inspektion im Hafen-Terminal; Increase of container security by applying contactless inspections in port terminals) to the German Security Research Programme. ECSIT is likely to start in May 2010, will last for three years and will investigate all aspects mentioned above in a holistic approach.

ECSIT will develop transferable approaches and methodologies on the one hand applying them to the focus port of Bremerhaven on the other. Demonstrators for high speed detection systems, simulated processes to detect the optimum strategy for the integration of those technologies into the operational processes in the port including cost aspects, legal implications such as on data protection and liability, possible business models for operation, etc. form parts of this challenging project.

SESSION 1

SECURITY OF TRANSPORT SYSTEMS

S 1.4

VISUAL INTELLIGENCE AND SECURE RFID PROTECT ROAD TUNNELS WITHIN THE FRAMEWORK OF THE SKRIBT PROJECT

D. Evers¹, A. Heidenreich¹, F. Heimbecher², A. Hutter¹, I. Rönnau², and H. Seuschek¹

¹ Siemens AG München; ² Federal Highway Research Institute (BASt), Bergisch Gladbach
alla.heidenreich@siemens.com

The SKRIBT³ research project receives financial support from the Federal Ministry of Education and Research in the framework of Research program for Civil Security. The research project aims at the protection of road transport infrastructure by identifying possible threat scenarios which might have a direct impact on security of bridges and tunnels as part of roads and developing adequate precautions. An interdisciplinary consortium⁴ guarantees a holistic approach to the research project. Potential protection measures are identified and studied by means of risk and scenario analysis. Some of the most effective protective measures are implemented and their effectiveness is proven by the demonstration at a selected road tunnel. This publication also covers early overheated vehicle parts detection and hazards recognition systems developed by Siemens Corporate Research & Technologies within the project SKRIBT. These recognition systems are integrated into the strategy management of Siemens tunnel control center and tested in a real environment of a road tunnel near Munich.

For the prevention of accidents caused by vehicles, timely detection of overheated vehicle parts, initially brakes and tires, is necessary. Intelligent video algorithms recognize and classify vehicles. A 3D model of the vehicle is generated and thermal images projected on the model provide the assignment of temperatures measured and vehicle parts identified. Combination of secure RFID transponders and visual recognition of a hazardous goods plate enhances the confidence for detection of hazardous goods transports. A cryptographic chip to avoid interception and in particular to prevent the counterfeiting of transponders is used. Innovative methods used for energy effectiveness and a special wake-up feature are described. By means of these detection systems the contribution shows how innovative IT technologies can be used for securing transport infrastructures, especially road tunnels.

³ German acronym for "Protection of critical bridges and tunnels in the course of roads"

⁴ The consortium includes research partner – Federal Highway Research Institute (BASt), Fraunhofer Institute for High-Speed Dynamics, Ernst Mach Institute (EMI), Ruhr University Bochum, Stuttgart University and Julius Maximilian University Würzburg – as well as Federal Office of Civil Protection and Disaster Assistance (BBK) and manufacturer – HOCHTIEF GmbH, PTV AG, Schübler-Plan GmbH, Siemens AG.

5th SECURITY RESEARCH CONFERENCE
BERLIN, SEPTEMBER 7th – 9th, 2010

POSTER PRESENTATION

SESSION 2

BUILDING PROTECTION

KEYNOTE

RESCUE AND PROTECTION OF PEOPLE IN BUILDINGS – UNDERSTANDING CROWD MOVEMENT THROUGH EXPERIMENT AND SIMULATION

The trend towards large multifunctional buildings and also the size of public events today make new demands on the quality of security concepts. In case of emergency, all attendees present must be able to evacuate the danger area promptly. Although this is generally ensured by the application of building regulations, in case of overcrowding or if some of the emergency exits are blocked this can result in long queues or dangerous crushes.

In this talk an overview of rescue routes design in high occupancy buildings will be given. A discussion of problems with prescriptive regulations and the prospects for computer simulations of crowd movement follows. A critical review of experimental data shows that our knowledge about the dynamics of pedestrian streams is insufficient which hinders the improvement of legal regulations, design standards and the development of reliable models for crowd movement.

In the second part of the talk results from recent research activities are presented. In the Hermes project we develop a test system of an evacuation assistant. The aim is to support decision makers by producing online a forecast of the evacuation using information about the current risk situation. The project is funded by the Federal Ministry of Education and Research in the line of the program on „Research for Civil Security“.

To improve the experimental data base we performed experiments with up to 400 pedestrians and extract reliably the movement of all individuals. These data are used to examine regulations in building codes and to develop models for simulating pedestrian streams in complicated buildings.



BIOGRAPHY

Armin Seyfried studied Theoretical Physics at the Bergische Universität Wuppertal from 1988 to 1996. In the course of his diploma project and Ph.D. thesis, which he finished in 1998, he focused on many particle systems, high energy physics and parallel computing. After his Ph.D. he specialized in the fire safety field. Since 2004 he has been establishing a new research group for pedestrian dynamics and fire simulations at the Jülich Supercomputing Center of the Forschungszentrum Jülich. In 2010, he became Professor for computer simulations for fire safety and evacuation at the Bergische Universität Wuppertal.

With the main focus on the complex dynamics of pedestrian crowds Armin Seyfried is interested in safety and security research concentrating on fire and smoke simulations, crowd management as well as evacuation simulation. Furthermore his field of interest ranges from parallel computing to non equilibrium physics of traffic systems and their interdisciplinary application.

*Prof. Dr. Armin Seyfried
Institute for Advanced Simulation Science
Jülich Supercomputing Centre
Forschungszentrum Jülich GmbH
52425 Jülich
and
Computer Simulations for
Fire Safety and Evacuation
Dept. D – Division Civil Engineering
Bergische Universität Wuppertal
Pauluskirchstraße 7
42285 Wuppertal
a.seyfried@fz-juelich.de*

SESSION 2

BUILDING PROTECTION

ACCIS: AUTOMATIC CARGO-CONTAINER INSPECTION SYSTEM*

V. Dangendorf¹, A. Breskin², E. Giemulla³, I. Havardi⁴, O. Jagutzki⁵, T. Juergensohn⁶, K. Osterloh⁷, C. Piel⁸, W. Rehak⁹, and D. Vartsky¹⁰

¹ Physikalisch-Technische Bundesanstalt, Braunschweig, Germany; ² Weizmann Institute of Science, Rehovot, Israel; ³ Technische Universität Berlin, Germany; ⁴ Israel Police Bomb Disposal Division, Israel; ⁵ RoentDek GmbH, Kelkheim-Ruppertshain, Germany; ⁶ Human-Factors-Consult GmbH, Berlin, Germany; ⁷ Bundesanstalt für Materialforschung, Berlin, Germany; ⁸ Research Instruments GmbH (RI), Bergisch Gladbach, Germany; ⁹ OUT e.V., Berlin, Germany; ¹⁰ Soreq NRC, Yavne, Israel
volker.dangendorf@ptb.de

The threat to civil aviation, international trade and homeland security posed by illicitly-transported explosives and special nuclear materials (SNM) is of ever-increasing concern. Contemporary terror organizations have become highly skilled in devising bombs that are smaller, more potent than hitherto and progressively harder to detect. The ACCIS project encompasses an R&D program aimed at developing next-generation transmission-imaging systems that can detect standard and improvised explosives as well as SNM, concealed within items ranging in size from passenger bags to air-cargo containers, private and small-commercial vehicles. The method combines high-spatial resolution Fast-Neutron Resonance Radiography (FNRR) and Dual Discrete-Energy γ -Radiography (DDER), in a single, concomitant and automated screening sequence. Unlike conventional X-ray radiographic systems, FNRR and DDER do not rely on human operator skills to identify the threat objects. Instead, they rely on operator-independent identification of the concealed contraband, via few-view spatial-reconstruction of its elemental composition. An operational system combining these two state-of-the-art inspection methods will thus permit reliable and automatic detection of SNM and explosives.

The principal R&D tasks in this project will comprise development of novel, high-spatial-resolution neutron and γ -ray detectors, as well as prototyping new means for producing ns-pulsed neutron and gamma-ray beams. Subsequently, the capabilities of the combined neutron/gamma screening technique will be evaluated in a laboratory scale imaging facility, using realistic test objects defined by the participating end-users. In parallel to the investigation of the basic physical properties and technological requirements the socio-economic parameters for deployment in an air-cargo screening facility will be investigated. These include, among others, legal aspects of irradiating such cargo with penetrating high-energy neutrons and gammas, protection of privacy and commercially sensitive information, implementation of safety standards for operators and public, and questions of public acceptance.

** The project is a German-Israeli cooperation under the programme „Research for Civil Security“, funded by the German Ministry of Education and Research (BMBF) and the Israeli Ministry of Science and Technology (MOST).*

S 2.1

PROTECTION OF CRITICAL INFRASTRUCTURE-BUILDINGS AGAINST DYNAMIC LOADS CAUSED BY ATTACKS AND ACCIDENTS

C. Brenneis, O. Millon, C. Mayrhofer, W. Riedel, and K. Thoma

Fraunhofer Institute for High-Speed Dynamics – Ernst-Mach-Institute, Freiburg, Germany

christian.brenneis@emi.fraunhofer.de

The protection of critical infrastructure-buildings and its users against terrorist-attacks, industrial accidents and natural disasters is a major challenge of science and technology these days. Purpose of the project AISIS¹, funded by the BMBF², is to enhance the active and the passive safety of critical infrastructure-buildings with the development of a situational awareness-system, identifying the damage of a structure after a catastrophic event through a sensor-network inside the concrete-structure. Using the sensor-signals, an analysis of the residual load-carrying capacity of the whole system can be achieved. Accordingly an optimized and coordinated rescue operation can be carried out.

The active protection will be achieved by employing an energy-autonomous sensor-network identifying the intensity of a load. The passive protection, the focus of the proposed paper, will be reached by increasing the resistance of the used materials and structures:

- analysis of the dynamic soil-behavior
- development and analysis of a fire-resistant ultra-high performance concrete
- development and analysis of a sensitive coupling-system for tunnel-segments

The soil-behavior against impact loads will be investigated using a Split-Hopkinson-Bar. The overall behavior of the tunnel-construction can be calculated. The analysis of the residual load-carrying capacity allows a statement about the system-stability carrying the remaining loads. Furthermore an impact-sensitive coupling-system connecting the tunnel-segments which are made of a new type of concrete will be developed. Its parameters and behavior is analyzed through Hopkinson-Bar experiments.

A segmented tunnel-construction was modeled and used for numerical simulations. With the use of pressure-time and impulse-time histories, these experiments were dimensioned. The paper will provide an overview about the goals, the methods and first results of the investigations. The results of the numerical simulations and the experimental techniques are described.

¹ *Automatic information retrieval and protection of critical infrastructure in case of catastrophe*

² *German ministry of education and research*

SESSION 2

BUILDING PROTECTION

S 2.2

TUNNEL STRUCTURES SUBJECTED TO EXPLOSIONS

A. Stolz¹, W. Riedel¹, C. Mayrhofer¹, M. Nöldgen², and K. Dörendahl²

¹ Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institute, Freiburg

² Schübler-Plan Engineering Consultants, Düsseldorf

alexander.stolz@emi.fraunhofer.de

Explosions in tunnels caused by severe accidents or terroristic attacks may lead to local and/or global damage up to the complete loss of structural integrity or watertightness. While the event risk is usually comparatively low, the damage potential of such scenarios is very high.

The presenting authors have been working on analytical, numerical and experimental concepts for the evaluation of damage degrees caused by explosions in tunnels in context with national research projects:

Damage is identified by both, scaled experimental investigations and validated numerical simulations of tunnel (sub-) structures. The numerical simulation takes into account for shock wave propagation in the tunnel section, the reinforced concrete structure and the soil bedding. With the implementation of non-linear material behavior a satisfying prognosis of local and global damage state is achieved.

The integration of these results into a standardized method for the evaluation of damage degree enables for a generalized comparison of different structural systems. The standardized method furthermore allows for an objective evaluation of protective measure like damping materials which reduce shock wave intensities in the structure or high performance, energy absorbing concrete materials.

5th SECURITY RESEARCH CONFERENCE
BERLIN, SEPTEMBER 7th – 9th, 2010

WELCOME RECEPTION

SESSION 3

SURVEILLANCE AND CONTROL – PART I

KEYNOTE

INFORMATION ANALYTICS FOR PUBLIC SAFETY AND HOMELAND SECURITY

Public safety and homeland security agencies deal with a broad range of complex challenges ranging from law and order, to terrorism, to emergency response and disaster recovery. The traditional role and design of these agencies has been for deterrence and investigation. Today's geopolitical environment has broadened their mission from deterrence and investigation to include preemption in open societies where individual rights are sacrosanct. While many technologies from communications, to armaments, and command and control are critical to the public safety mission, information is at the very core of their mission. Like, most other large enterprises, public safety agencies are also challenged by the deluge of information, 1000's of video cameras streaming video in real time, web crawling and monitoring technologies generating information and many other public and tasked sources producing multiple layers of information.

This talk will explore various technologies that are becoming widely commercially available to addressing these challenges. Starting with the challenge of handling 1000's of streams of video information, to looking at information from sources like GPS and rfid, to more traditional sources like crime and intelligence reports, the talk will cover the use of information analysis and its role in these situations. By mapping the information availability to a time line, the talk will provide a perspective that illustrates the well know methodology using historical information to predict, prepare and preempt incidents. The talk will also look at the end to end spectrum, what is the information source, how should it be analyzed, how is it combined with other sources, what becomes of the insights gained by analysis, how do we measure the effectiveness of such technologies. While these technologies and processes have made significant progress, the open technical challenges offer many opportunities for the research community.



BIOGRAPHY

Dr. Arun Hampapur is an IBM Distinguished Engineer and Director in the Business Analytics and Math Sciences Department of IBM Research. In his current role Arun Hampapur is leading solution development and commercialization of Analytics and Optimization technologies across a broad range of industries. His role includes developing novel analytics offerings which combine structured and unstructured information analytics technologies into vertically integrated solutions. Arun's current projects are focused on enabling asset optimization, sustainability, advanced asset management, enhanced public safety and several additional smarter city topics thru the use of advanced reporting, predictive data analytics and optimization. Arun Hampapur has been in this role since 2009.

In 2008 Dr. Hampapur was on assignment to IBM Global Services as the CTO of Physical Security, where he led the technology commercialization of the IBM Smart Surveillance System. Arun Hampapur led the original research team which invented IBM Smart Surveillance System (S3) at IBM T. J. Watson Research Center prior to its commercialization. He has led the S3 effort from its inception as an exploratory research effort, thru the building of the first lab prototype, first customer pilot engagement, to the commercialization as a services offering. He has developed several algorithms for video analytics and video indexing.

Arun Hampapur has published more than 80 papers on various topics related to video analysis, pattern recognition, searchable video and video surveillance and holds 20 US patents and more than 70 patent applications.

Dr. Hampapur is a member of the IBM Academy of Technology, an IBM Master Inventor, and an IEEE Senior Member. He obtained his PhD from the University of Michigan in 1995.

*Dr. Arun Hampapur
IBM Distinguished Engineer & Director
Business Analytics and
Mathematical Sciences
IBM Research, Yorktown Heights
1101 Kitchawan Road, Route 134
Yorktown Heights, NY 10598 / USA
arunh@us.ibm.com*

SESSION 3

SURVEILLANCE AND CONTROL – PART I

LIVEDETECT3D: LIVE DETECTION OF HIDDEN THREATS VIA REAL-TIME 3D IMAGING

P. Haring Bolívar¹, A. Kolb¹, H. Wolf², T. Sprenger², H. G. Roskos³, T. Löffler⁴, J. Rosen⁵, J. Roulston⁶, R. El-Bahar⁷, A. Madjar⁸, E. Socher⁸, and B. Nadav⁹

¹ Universität Siegen, Germany; ² Huebner GmbH, Kassel, Germany; ³ Universität Frankfurt, Germany; ⁴ SynView GmbH, Bad Homburg, Germany; ⁵ Ben Gurion University, Beer Sheva, Israel; ⁶ NovaTrans, Herzelia, Israel; ⁷ Samsung Semiconductor, Ramat Gan, Israel; ⁸ Tel Aviv University, Israel; ⁹ Prime Minister Office, Israel

peter.haring@uni-siegen.de

Despite of intense international efforts, the global security situation remains critical, as demonstrated by continuous prevalence of terrorist attacks. Terahertz technology has an interesting potential for preventing such attacks. This potential follows from the intrinsic ability to detect security-related materials (metals, energetic materials, drugs, ...), in combination with the capability to see through many concealing materials such as polymers, paper, cardboard or clothing. Present worldwide efforts and, specifically, the existing R&D activities in Israel and Germany concentrate on the development of portal-like or close-range inspection solutions for security checks at airports, as this environment provides a well-controlled situation to inform and screen persons under ethically acceptable provisions. This scenario also represents the technologically simplest situation, as a portal-like imager operating at close distance to the screened person is sufficient.

The aim of this consortium is to develop an imaging system which allows screening of persons at a distance of more than five meters in order to detect hidden threats like weapons and explosives. The system is configured as a combined optical / THz system, in order to provide the technological basis for an ethically acceptable use in a less restricted environment. 3D imaging capabilities will be established, in order to allow the robust differentiation of threats. This project covers the full value chain, from the base technologies for the cost-effective mass market production of THz components and the provision of ultrafast algorithms for image processing, via the development of cost-performance optimized 3D tomographic visible and THz imaging subsystems, up to the development of a complete system prototype. Finally, as true evaluation, the prototype will be field tested at the end of the project. The project will integrate ethical evaluation, the development of training modules, and a public acceptance analysis, in order to ensure the applicability of the developed technologies on both the technical as well as the sociocultural level.

This German-Israeli cooperation project is proposed in the framework of the High-Tech Strategy programme „Research for Civil Security“ by the Federal Ministry of Education and Research in Germany and the Ministry for Science and Technology in Israel.

S 3.1

TEKZAS THZ REAL-TIME CAMERA (TWO-DIMENSIONAL) FOR APPLICATION IN SECURITY TECHNOLOGY

**R. Beigang¹, J. Jonuscheit², B. Cimander³, H. Wolf⁴, U. Kallmann⁵, J. Bartschke⁶,
R. Rösch⁷, H. G. Roskos⁸, J. Smet⁹, E. Giemulla¹⁰, and P. Lemke¹¹**

¹ Technical University Kaiserslautern; ² Fraunhofer Institute for Physical Measurement Techniques (IPM), Freiburg; ³ Flug- und Industriesicherheit Service- und Beratungs- GmbH, Kelsterbach
⁴ Hübner GmbH, Kassel; ⁵ Robert Bosch GmbH, Stuttgart; ⁶ Xiton Photonics GmbH, Kaiserslautern;
⁷ Fraunhofer Institute for Industrial Mathematics (ITWM), Kaiserslautern; ⁸ University Frankfurt /
Main; ⁹ Max Planck Institute for Solid State Research, Stuttgart; ¹⁰ ILB Internationale Luftfahrt- und
Verkehrsberatung GmbH, Berlin; ¹¹ Institute for Economy + Prevention, Munich

b.cimander@fisgmbh.de

Motivation

A growing terrorism threat in all its new variants and the resulting necessary legal regulations require additional and new security measures also in the field of transportation, above all in air traffic. Airlines, as well as airports, depend on efficient processes in all matters in order to be internationally competitive. These increased security requirements are met under this project with flexible and effective combined technology process solutions for security controls.

Project description and goals

The overarching objective of the project is to study and implement a multi-sensor system for the remote detection of hidden chemical, biological and explosive (CBE) hazardous substances carried directly on the body. Persons carrying such substances are moving in real time. The system to be developed will be based on terahertz (THz) technologies and include a surveillance camera and a two-dimensional camera in the THz spectral range. In addition a novel THz source with a high peak performance is to be studied which will make it possible to make two-dimensional pictures in real-time by means of a special detection method.

Innovations and applications

Both the THz source as well as the corresponding detection technique are innovative and have not been implemented in this form to date. The research project aims at developing a demonstrator as a starting point for a marketable system in the airport sector. Furthermore, technical innovations in the field of THz technology are expected which might be suitable for the surveillance of critical infrastructures, such as industrial facilities, stadiums and public institutions.

Founded by BMBF (Federal Ministry of Education and Research)

SESSION 3

SURVEILLANCE AND CONTROL – PART I

S 3.2

DEVELOPMENT OF BtoB SECURITY BUSINESS – FROM GUARDING TO KNOWLEDGE-INTENSIVE EXPERT SERVICES

M. Murtonen, H. Kortelainen, E. Kupi, and V. Rouhiainen

VTT Technical Research Centre of Finland, P.O. Box 1300, 33101 Tampere, Finland

mervi.murtonen@vtt.fi

Private security services is a globally growing business (van Steden and Sarre, 2007) that aims at preserving the security of persons, information and property using both manpower and alarm detecting and monitoring technologies (de Waard, 1999). As the main focus in this paper is in the business-to-business (BtoB) security services, the main security context is organizational security (or corporate security). Security services is a widely used form of organizational service that aims at protecting customer's business continuity and assets against security threats.

The aim of this paper is to explore both the service providers' and their customers' views on the evolution and the future trends in BtoB security business. This paper is based on two ongoing research projects, which will answer the following research questions:

- 1) What are the main business drivers in the security business?
- 2) How do service providers and their customers view the current development in security business?

This study has a qualitative research approach (Patton, 1990). The research data consists of interviews and results from several workshops and seminars. The interviews were conducted in 8 private security companies and in 3 customer companies. In total, 62 people (including 8 managing directors) were interviewed. In addition, informal conversations, several company visits, joint workshops and related documentation were used to illustrate the phenomena under study. The preliminary results were also discussed with the informants in the workshops.

In this paper we discuss the dynamics and the key business drivers in security. The private security service has originated in in-house guarding operations in large industrial plants, and it has evolved into the outsourced professional services that use different technologies and competencies as a key resource. The security business has had to adapt to and evolve along the changing global security environment. The current trend is towards more specialized and customized knowledge-intensive expert services where customer integration and value co-creation are among the key concerns.

Depending on the sector of activity, different customers have different needs and demands for the security services, and the need for customization is constantly increasing. Simultaneously, the alarming and surveillance systems have advanced substantially, what have created new opportunities for novel service concepts and more comprehensive security service offerings.

The tradition of academic security research in the areas of security business and services is very young, while the research has focused in threats and security technologies. We argue that BtoB security services and security business deserve more attention in current security research and that business-oriented studies have a lot to offer to the development of the whole security branch. This paper contributes to the discussion of security by revealing a structured view on perceptions of the security business among the service providers and their customers. At the branch level, more profound understanding of the dynamics in the security business will provide new opportunities to reinforce security service operations and to expand the knowledge on understanding of the customer needs in this field.

References

- [1] De Waard, J. (1999), „*The private security industry in international perspective*“, *European Journal on Criminal Policy and Research*, Vol. 7, No. 2, pp. 143-174.
- [2] Patton, M. Q. (1990), *Qualitative research & evaluation methods*, Sage Publications Ltd.
- Van Steden, R. and Sarre, R. (2007), „*The growth of private security: trends in the European Union*“, *Security Journal*, No. 20, pp. 222-235.

SESSION 3

SURVEILLANCE AND CONTROL – PART I

S 3.3

RANGE-GATED ACTIVE IMAGING TECHNOLOGY FOR SURVEILLANCE AND CONTROL OF AREAS

M. Weiland, W. Knorr, and M. Laurenzis

French-German Research Institute of Saint Louis, France

michael.weiland@isl.eu

For civilian as well as military scenarios surveillance and control of areas or borderlines is of great importance. Often this task is hampered by the climate conditions. Borders are often along rivers or seas with a high percentage of foggy days. Sometimes an observer is glared by sunlight in an against-the-light situation, which is particularly dazzling at water. In SAR scenarios it is necessary to fly with helicopters in sandy or snow-covered regions. There it is exceptionally difficult to touch down because of brown-out or white-out. In military scenarios it is often necessary to get a quick overview of the 3D topology of a scene to prepare the mission of special forces. Sometimes military or civilian forces have got to operate in a smoky environment where it could be helpful to look farther than only 2 meters.

A solution for all these surveillance and control problems is the range-gated active imaging technology. The French-German research institute of Saint Louis works since nearly 10 years in this domain. In international groups of scientists technologies have been developed which enable police and soldiers to observe zones which are covered with fog or dust. With new algorithms it is possible to generate in one minute a 3D picture of a scene with only two short laser-pulses.

The paper describes this technology, characterises the assets and drawbacks and shows by means of examples the capabilities of range-gated active imaging.

S 3.4 INTEGRATED SECURITY MONITOR FOR CONTROL OF PERSONS

H.-W. Hübers¹, S. Augustin¹, U. Böttger¹, H. Richter¹, A. Semenov¹, R. Bretfeld², H. Hirsch², M. Scheiding², S. Wörner², K. Schmalz³, J.C. Scheytt³, R. Schiffel⁴, W. Leonhardt⁵, D. Rondeshagen⁵, G. Arnold⁶, H. Dittmann⁶, and W. Schüler⁷

¹ Deutsches Zentrum für Luft- und Raumfahrt e.V., Rutherfordstr. 2, 12489 Berlin; ² Astro- und Feinwerktechnik Adlershof GmbH, Albert-Einstein-Str. 12, 12489 Berlin; ³ IHP GmbH, Im Technologiepark 25, 15236 Frankfurt (Oder); ⁴ IQ Wireless GmbH, Carl-Scheele-Str. 14, 12489 Berlin; ⁵ Institut für Umwelttechnologien GmbH, Volmerstr. 7B, 12489 Berlin; ⁶ Optotransmitter-Umweltschutz-Technologie e.V., Köpenicker Str. 325b, 12555 Berlin; ⁷ STEP Sensortechnik und Elektronik Pockau GmbH, Siedlungsstraße 5-7, 09509 Pockau

heinz-wilhelm.huebers@dlr.de

Fast end effective security detection systems for the checking up of persons are of prime importance in various locations like airports, government buildings, industrial facilities and public transportation as well as during public events such as major sport events or concerts. Since X-ray, gamma ray and neutron ray inspection cannot be applied due to radiation safety regulations new technologies are required. The state-of-the-art is the use of metal detectors, which do not allow explosive detection but detection of metallic weapons only. As a last instance only a physical search of a suspicious person can be performed by a security officer. Body scanners operating at mm-wavelengths might replace the hand search. However, these systems cannot identify explosives. Clearly, a contact free system is needed that can detect explosives worn at the body and non metallic weapons possibly at a large and safe distance.

We will present the development of an integrated security monitor. The system combines an ion mobility spectrometer for detection of explosives, a terahertz imaging system for detection of hidden objects and a detector for radioactive radiation. Two cameras, an optical and an infrared one, complete the system. Security scenarios for application of the security monitor will be discussed and the system design as well as first results will be presented.

SESSION 3

SURVEILLANCE AND CONTROL – PART II

KEYNOTE

SECURE IDENTITY – A SOURCE FOR INNOVATIVE IT-SYSTEMS AND PROCESSES

Secure identity is indispensable for electronic business processes. Security is also a precondition for the use of identity in various ways for the simplification of processes in economy, government and daily living. The fields of applications for new technologies for secure identity are widespread from the next generation of secure ID documents to new forms of communication between machines and vehicles. Another essential future domain for technologies for secure identity is the protection against product piracy.

In the Fraunhofer Cluster of Innovation 'Secure Identity Berlin-Brandenburg' five Fraunhofer Institutes cooperate with five Universities and twelve companies in order to develop new technologies for secure identity of persons, products and intellectual property. In the initial phase from 2008-2011 the R&D work of the partners concentrates on future ID-card systems and future ID-based communication. The special profile of expertise of the Cluster of Innovation is based on the complementary know-how of the Fraunhofer Institutes in the process chain of secure identity from acquisition to personalization and finally the verification of identity. The expertise comprises image processing technology, biometric identification, materials, mobile communication and micro systems.

In a globalized economy with its increasing exchange of goods, persons and data secure identity is a key element. It also contains a high potential for the automation of B2B-processes, transport or activities of daily living. Mobile communication in connection with the Internet provides instant access to many of these processes. For a broad acceptance of new technologies, not only a secure use and transfer of identity is essential but also the protection of privacy. Therefore the Cluster of Innovation closely links R&D for innovative technologies with societal research in an interdisciplinary structure.

The paper will give an overview about innovative technologies for and future domains of secure identity.



BIOGRAPHY

Prof. Dr.-Ing. Jörg Krüger, was born August 20, 1962 in Bielefeld, Germany. He holds a Master's degree in Engineering and a Doctor of Engineering from the Technical University Berlin.

Between 1992 and 1999 he worked at Fraunhofer IPK. In 1999, he founded the company reCognitec Gesellschaft für digitale Bildverarbeitung. In 2003 he joined TU Berlin as Full Professor of Industrial Automation Technology at the Institute for Machine Tools and Factory Management. In addition he became Director of the Division Automation Technology at Fraunhofer Institute for Production Systems and Design Technology IPK in 2004.

Between 2007 and 2008 he was Provisional Head of the Division Industrial Information Technology at TU Berlin. Since 2008 he has been Head of the Fraunhofer Innovation Cluster Secure Identity Berlin-Brandenburg, a research group of five Fraunhofer institutes and several universities and companies. Since 2009, he has been Provisional Director at the Department of Quality Sciences at the Technical University of Berlin.

Prof. Krüger's main areas of research include human-centered and image-based automation technologies, automatic handling and virtual reconstruction of partially destroyed documents, optical quality control of transparent and biogenic materials, as well as 2D and 2 ½ D object and position recognition. At TU Berlin and Fraunhofer IPK he develops safety-related applications for image processing and pattern recognition, which are used for instance in the domains of document security (biometry, digital water marks) and product and trademark protection.

Prof. Krüger has received several awards and is an active member of some major professional societies, such as the Wissenschaftliche Gesellschaft für Produktionstechnik (WGP). He is also a member of the Board of the Society for Secure Identity in Berlin.

*Prof. Dr.-Ing. Jörg Krüger
Technical University Berlin
Institute for Machine Tools
and Factory Management
Pascalstraße 8-9
10587 Berlin
joerg.krueger@iwf.tu-berlin.de*

SESSION 3

SURVEILLANCE AND CONTROL – PART II

BEPE: BIOLOGICAL EVENT PREPAREDNESS EVALUATION

B. Adini^{1,2}, W. Biederbick³, R. Brodt⁴, R. Cohen^{1,2}, R. Gottschalk⁶, D. Laor^{1,2}, B. Lev¹, R. Ringel¹, J. Sasse³, J. Schempf⁵, S. Schilling⁴, and L. Verbeek³

¹ Ministry of Health, Israel; ² Ben Gurion University of the Negev, Israel; ³ Robert Koch-Institute, Germany; ⁴ University of Frankfurt, Germany; ⁵ CSO GmbH, Pforzheim, Germany;

⁶ Centre of Competence for highly contagious diseases for the states of Hesse and Rhineland-Palatinate, Germany

verbeekl@rki.de

The overall aim of this project is to save as many lives as possible in case of a biological event due to natural or man-made causes. It is funded as a German-Israeli cooperation under the programme “Research of Civil Security” by the Federal Ministry of Education and Research (Germany) as well as the Ministry of Science and Technology (Israel) and the Ministry of Health (Israel), (BMBF contract No 13N11047)

A comprehensive web-based evaluation tool will be accomplished to identify strengths and weaknesses in the management of patients with highly contagious diseases, pandemics and epidemics. New propositions and guidelines acquired by the project team in collaboration with several experts will help to mitigate consequences for the public health and will improve the medical management of individual cases.

By means of existing experiences and a solid literature review emergency management parameters, checklists, guidelines and best practices will be developed. Experts in the relevant field will conduct a Delphi-study to validate and weight these parameters. Distribution of multiple choice tests, carrying out interviews, implementation of hospital drills and utilization of trained observers will enable an evaluation of performance and preparedness for a biological event. The project will identify benchmarks for the preparedness of hospitals for biological events. To these belong indicators and items such as knowledge of medical staff in diagnosing and managing a patient with a highly contagious disease, personal protection equipment, actualizing emergency plans, maintaining stockpiles of medications, reliability of infrastructure and coordination with neighbouring hospitals and governing authorities. Furthermore the project is focused on a responsible risk communication with regards to possible anxieties and demotivations of staff in this threatening situation.

The web-based evaluation tool will facilitate hospitals in improving and updating their preparedness for a biological event which differs from other catastrophes and seems to be more neglected despite present hazards. The appealing international synergism of this research project is based on the high-quality preparedness and real-life experience of the Israeli partner in managing mass-casualty incidents and on the excellent knowledge and experiences of the German partners in managing single patients with highly contagious diseases such as hemorrhagic fevers.

S 3.5 INTEGRATED MOBILE SECURITY KIT

N. Künzner¹ and K. Ekvall²

¹ Diehl BGT Defence GmbH & Co. KG, Alte Nußdorfer Str. 13, 88662 Überlingen;

² SAAB Microwave Systems, Göteborg, Sweden

karin.schroek@diehl-bgt-defence.de

The continuously evolving threat of unpredictable terrorist activity demands the innovative application of existing and developing technology for the protection of the EU's citizens. The Integrated Mobile Security Kit (IMSK) project will combine technologies for area surveillance; checkpoint control; detection of dangerous substances and support for VIP protection into a mobile system for rapid deployment at venues and sites (hotels, sport/festival arenas, etc) which temporarily need enhanced security.

This integrated project has been founded by the European Commission under the FP7 Security Research topic and started in March 2009.

The objective of presentation will be to provide an overview of the project and first results of the work already performed like the architectural framework of the security system, the involved technologies, and the scenarios identified during the operational analysis.

The project will employ legacy and novel sensor, C2, data fusion and knowledge fusion technologies, design an IMSK-system that will integrate sensor information to provide a common operational picture where information is fused into intelligence, adapt the system to local security forces, perform a field demonstration to validate the concept, and finally disseminate the results after accreditation by end-users. The development of IMSK will be heavily founded on advice derived from operational security professionals.

SESSION 3

SURVEILLANCE AND CONTROL – PART II

S 3.6

EUROPEAN BORDER SURVEILLANCE: SOLUTIONS FROM THE EUROSUR TECHNICAL STUDY

J. Feierlein

ESG Elektroniksystem- und Logistik GmbH, Fürstenfeldbruck

johannes.feierlein@esg.de

The European Commission outlines a three-phase common technical framework for setting up a „European border surveillance system“ (EUROSUR) designed to support the Member States in their efforts to reduce the number of illegal immigrants entering the European Union by improving their situational awareness at their external borders and increasing the reaction capability of their information and border control authorities. As a startup to this program, the ESG Group carried out a comprehensive technical feasibility study for the development of concepts for a border surveillance infrastructure, a secure communication network and a pre-frontier intelligence picture within the framework of a European border surveillance system. The presentation will focus its key objectives and main results.

National border surveillance systems of the European Member States emerged from different Concepts of Operations (CONOPS), and differ concerning the technical architecture and degree of maturity. Remaining under national control, border surveillance needs technical and organisational guidelines in order to ensure compliance to the requirements of the Schengen catalogue, and capability of being funded by the External Borders Fund (EBF). A classification scheme for border segment types (based on geomorphologic characteristics and related vulnerabilities) and the assignment of generic surveillance system architectures was developed and can now serve as a design toolbox for national planning authorities. The information exchange requirements for National Situation Pictures (NSP) and the new European Situational Picture (ESP) were reflected as well as the management of the EUROSUR system itself.

An Integrated Border Management approach requires a secure network of National Coordination Centers (NCC) and FRONTEX (as an equal node) to share relevant information on a voluntary and regular basis. The prerequisites and related technical requirements for this network enabled capabilities will be introduced.

The CPIP ensures situational awareness regarding the situation beyond the external borders of the EU to detect upcoming incidents and related threats. Relevant information from heterogeneous sources can be shared within the EUROSUR network and fused to a common/shared intelligence picture complementing the NSP/ESP. The prerequisites and related technical requirements for this CPIP will be introduced.

S 3.7

SOFTWARE TOOLS FOR THE DEVELOPMENT OF DISTRIBUTED INTELLIGENCE SURVEILLANCE NETWORKS

J. Viitanen and J. Jankkari

VTT Technical Research Centre of Finland

jouko.viitanen@vtt.fi

Scope

Future surveillance systems will perform a number of automatic image and signal analysis operations. When the area of surveillance increases and large numbers of cameras and sensors are installed, the limits of the processing power in a centralised computing system are rapidly exhausted. Therefore future surveillance systems will most likely be based on distributed processing. Another demand for the distributed processing rises from the fact that digital cameras rapidly replace analog cameras, therefore the compression and encryption of data, and local adjustments already necessitate major local processing power, in addition to local intelligence. Efficient software tools are needed for the assessment and building such distributed surveillance systems. This work will report some results from a European project SUBITO, where automated surveillance is being developed. One work package of the project was concentrating on supporting studies, and our task was to develop software tools for the support when future distributed systems are being designed.

Methods

The methods of the work consisted of an analysis based on an experimental surveillance system. In order to get a realistic view of the real bottlenecks and concerns for a large network, we have built a system based on current commercial state-of-the-art components, especially with respect to wired and wireless communication facilities and high resolution camera data rates, while the processing load was evaluated based on existing compression/decompression algorithms and the estimated automatic surveillance analysis task load distribution. The network and CPU loading analyses and measurements were performed using available commercial software tools. For wireless communication, a few typical RF interference situations were simulated. We assumed a typical situation where a central master surveillance station with a typical user interface was employed, with networked connections to the remote intelligent stations, basic recognition at the remote stations, but central command and data storage at the single master station.

Results

The results of the analysis were collected in table formats, containing parameters relevant to the surveillance setups, such as camera resolution and corresponding data rates, available wireless and wired network bandwidths, CPU performance

SESSION 3

SURVEILLANCE AND CONTROL – PART II

figures, and compression algorithm loads. The spare residual capacity left for the actual surveillance tasks was measured, and its sufficiency evaluated based on the estimated processing demand rising from the recognition tasks. Because the final automatic image analysis and recognition software modules to be delivered in the SUBITO project are still due, the analysis was based on just rough estimates on the loading by such typical modules. The results concluded concrete requests for the optimal digital surveillance camera interface requirements, in a situation where camera based compression and encryption algorithms are embedded within an intelligent camera. Features were also tested for the design on the communication principles between the remote stations and the master control station. Additionally, implementation principles were proposed for the master control station user interface in cases where large numbers of cameras are used, and human performance is not sufficient for the actual recognition, but still service for rapid requests of specific attention is required by the security personnel.

S 3.8

IMPROVING AUTOMATIC SURVEILLANCE BY SOUND ANALYSIS

K. Lopatka, J. Kotus, and A. Czyzewski

Gdansk University of Technology, Multimedia Systems Dept.

klopatka@sound.eti.pg.gda.pl

An automatic surveillance system, based on event detection in the video image can be improved by implementing algorithms for audio analysis. Dangerous or illegal actions are often connected with distinctive sound events like screams or sudden bursts of energy. A method for detection and classification of alarming sound events is presented. Detection is based on the observation of sudden changes in sound level in distinctive sub-bands or in parameter values. Among the parameters, there are specially defined features connected with the energy ratio in certain sub-bands of the spectrum and the shape of the signal around transients. The parameter set is completed with MPEG-7 descriptors chosen on the basis of experiments and statistical analysis.

For classification a Support Vector Machine classifier is implemented. The model is built using a test set of sounds recorded in real conditions. Separate classifiers are implemented for different classes of sound events. The length of the analysis frame and threshold values for event detection are set to fit the characteristics of a certain type of sound. The accuracy is then improved by the decision procedure. The final indication of the system is derived from decisions of all classifiers, compared in a number of adjacent analysis frames. The classifier yields high accuracy of detecting typical alarming sound events like gunshot, scream, explosion, broken glass or horn abuse. It also provides the possibility to retrain the model and add a new type of event to be recognized by the system. The described solution can be implemented in an automatic surveillance system together with image analysis. Processing both sound and image leads to a significant improvement of the event detection rate. The developed algorithms can be implemented to detect dangerous events in large public areas like stations, airports or stadiums.

SESSION 4

PROTECTION AND RESCUE OF PEOPLE

KEYNOTE

REMOTE SENSING FOR DAMAGE ASSESSMENT IN HUMANITARIAN DISASTERS

Remote sensing is a quick and reliable tool for damage assessment in disaster areas that are not easily accessible but need to be analysed as soon as possible to co-ordinate response activities. Satellite imagery alone, though, will not provide sufficient information to come to an accurate assessment of the situation, such that there is a need for the augmentation by additional information: Knowledge about vulnerabilities such as population density, settlement structures or critical infrastructure element locations can be added, and even and pre-calculated impact scenarios can be generated to make the picture more complete. Moreover, the assessment needs to be automated, as information should be communicated to the global first responder community as soon as possible and manual intervention is time-consuming.

The presentation will show in different examples how the European Commission's JRC (Joint Research Center) creates crisis management tools and turns its research results on information mining and pattern recognition into a reliable help for NGOs, first responders and policy makers in situation assessment after humanitarian disasters of different types (earthquake, tsunami, civil war). The JRC competencies range from image processing over open source information mining to modelling and risk assessment, and the capabilities of the JRC have been deployed internationally in several severe incidents such as the conflict between Georgia and South Ossetia, the Haitian earthquake or the Chile Tsunami. From post-disaster field missions, the JRC experts feed back their findings into scientific research, to continuously improve accuracy and performance of the automated situation assessment methods. Beneficiaries of the JRC work in this area are thousands of first responders in the EU member states and in the international community as well as the central Monitoring and Information Center of the European Commission in Brussels.



BIOGRAPHY

Since 2007 Stephan Lechner is the Director of the Institute for the Protection and Security of the Citizen at the European Commission's Joint Research Centre.

Before joining the European Commission, he worked from 1989 to 1993 at Siemens as project manager. In 1993 he joined E-plus, a start-up German Mobile Network Operator as IT Security Manager. In 1997 he became head of Corporate Security for O2 Germany, another Mobile Operator. From 2002 to 2007 Stephan Lechner worked at Siemens, where he profiled the Siemens Security research activities, including the successful start of Homeland Security and the company's internationalization by establishing a new research team in Beijing, China.

Stephan Lechner was member of the European Security Research Advisory Board (ESRAB) and member of the Permanent Stakeholder Group of the European Network and Information Security Agency (ENISA). He was also chairman of the Secure IST Advisory Board for the respective Coordination Action.

He used to work in European Standardization at ETSI (the European Telecommunications Standards Institute) and at ECMA (an industry association dedicated to the standardization of Information and Communication Technology and Consumer Electronics). He is also an active CISSP (Certified Information Systems Security Professional).

*Dr. Stephan Lechner
Director
Institute for the Protection
and Security of the Citizen
European Commission - JRC
Via E. Fermi, 2749
21027 Ispra (VA) / ITALY
stephan.lechner@ec.europa.eu*

SESSION 4

PROTECTION AND RESCUE OF PEOPLE

I-LOV: MIXS AND DETUS – TWO MAJOR BILATERAL TECHNOLOGY ADVANCES FOR IMPROVING CAPABILITY RESPONSES IN EMERGENCY MISSIONS

M. Loschonsky³, A. Ashkenazi⁴, U. Kaplan⁴, O. Rogall³, Y. Yankelevich^{3,5}, J. Henning³, D. Wiebeck², Q. Hamp³, L. M. Reindl³, H. Werner¹, and A. Kesar⁵

¹ THW – Bundesanstalt Technisches Hilfswerk – Referat E1, Bonn, Germany; ² THW – Bundesanstalt Technisches Hilfswerk – Ortsverband Breisach, Germany; ³ IMTEK – Institute for Microsystems Engineering, University of Freiburg, Germany; ⁴ NEMA – National Emergency Management Agency, Tel Aviv, Israel; ⁵ Soreq Nuclear Research Center, Pulsed Power Group, Yavne, Israel

marc.loschonsky@imtek.uni-freiburg.de

MIXS (Mobile Information Exchange System) and DETUS (Detection, recognition and Underneath Surveillance System) are two collaborative German-Israeli approaches within the German Project “I-LOV” funded by the German Ministry of Research and Education (BMBF) within the Research Program for National Security.

The collaboration intends to enable end-users as THW and NEMA to deploy a reliable, effective and comprehensive emergency management system with additional features and technical equipment that will be able to support their operation in the event of a national disaster. To guarantee bilateral benefit, major issues of I-LOV will be adapted to Israeli need in a common way, and potential Israeli need will be integrated into I-LOV.

MIXS represents a new approach of a highly cost-effective integrated mission overview and emergency management system, enabling continuous real-time information retrieval, monitoring and management of mobile and other resources in rescue operations and training.

DETUS represents an alternative technology-driven approach for the radar-based detection of human or animal creatures using pulse generator based ultra wide-band radar (UWB) as ground penetrating radar systems. This approach will allow the understanding of essential detection properties such as depth of penetration and clutter power.

S 4.1

EMERGENCY MANAGEMENT IN LARGE INFRASTRUCTURES – THE EU-PROJECT EMILI

R. Klein

Fraunhofer IAIS, Schloß Birlinghoven, 53754 Sankt Augustin
ruediger.klein@iais.fraunhofer.de

Emergency management in large infrastructures as public transportation, airports, or power grids is a challenge today and will be so even more tomorrow. It is critically based on an optimal information management and cooperation of many stakeholders. They have to share information, coordinate their plans and actions, jointly respond to changing conditions, etc.

Today's control systems process data in a pre-defined way. Especially in the case of emergencies they do not support the operators adequately. There is need for a higher level of flexibility and additional functionality. Operators need additional functionalities and sophisticated decision support.

The Internet is the ubiquitous information infrastructure. The EU FP7 Project EMILI will develop a new approach to crisis and emergency management in large infrastructures by next generation Web technology: complex event processing, Active Web technologies and Semantic Web.

These Next Generation Web technologies will be adapted and extended to a new generation of flexibly communicating control systems in Critical Infrastructures.

Three realistic but quite different use cases will guide the methodology development and provide proof of concept and demonstration capabilities:

- Airport security: the complex social, technical and IT systems of airports with their highly heterogeneous environments provide challenges for emergency and crisis management.
- Security in Metro systems show similarities and significant differences to airports – thus providing an interesting contrast and further validation and verification needs.
- Management of power grids: a completely different kind of Critical Infrastructures currently undergoing significant changes in technology (heterogeneous, distributed, renewable sources) and management (many stakeholders, large distances, trading).

SESSION 4

PROTECTION AND RESCUE OF PEOPLE

S 4.2

SECURITY2PEOPLE

W. Raskob⁵, E. Gers¹, R. Kaschow², U. Rickers, L. Tufte³, and F. Ulmer⁴

¹ BBK, 53127 Bonn, Germany; ² CAE Elektronik GmbH, 52220 Stolberg; ³ PRO DV Software AG, 44227 Dortmund; ⁴ Dialogik, 70176 Stuttgart, Germany; ⁵ Karlsruhe Institute of Technology, 76344 Eggenstein-Leopoldshafen

wolfgang.raskob@kit.edu

The integrated project SECURITY2People (Secure IT-Based Disaster Management System to Protect and Rescue People) that is part of the German Security Research initiative, aims at exploring the needs for and the structure of an integrated risk management system that is applicable for all types of emergencies and at all levels of emergency management from the local to the Federal Government. In addition operators of critical infrastructures and organisations dealing with security issues are also envisaged as future user of that system. The following functionalities should be included:

- Role-based information management;
- Decisions support at all levels of management;
- All types of simulation techniques;
- Applicability in training, exercises and operation.

An important feature of such a system is the appropriate information exchange between different actors and public communications. For this purpose, social and psychological aspects of risk communication have to be explored.

Finally the system has to be designed in such a way that existing specialised management tools can be integrated into SECURITY2People. As such a system can only be designed with the strong support of potential end users, ten associated partners from police, fire brigade, rescue services, operators of critical infrastructures and public administrations became associated partners of SECURITY2People.

The project started May 2009 and will last for three years. Work so far focused on the analysis of the current status in emergency management and the functional and technological requirements for such an integrated system. In the now starting second phase, the results of the analysis will be realised in a concept and a first demonstrator that will build the basis for the feedback from the associated end users. The paper presents the progress reached in the first year, in particular the first demonstrator designed for the continuous interaction with the potential end users.

changes in technology (heterogeneous, distributed, renewable sources) and management (many stakeholders, large distances, trading).

S 4.3

CHALLENGES IN MARITIME SAFETY AND SECURITY TRAINING USING A SPECIFIC SAFETY & SECURITY TRAINER (SST)

C. Felsenstein¹, K. Benedict¹, and M. Baldauf²

¹ Hochschule Wismar, University of Applied Sciences - Technology, Business and Design
Department of Maritime Studies Warnemünde, R.-Wagner-Str. 31, 18119 Rostock, Germany;

² World Maritime University Malmö, Citadellsvägen 29, 201 24 Malmö, Sweden

c.felsenstein@hs-wismar.de

There is a current major priority to train ship's officers and crew with sufficient skills and appropriate procedures which can provide adequate protection and ensure the safety of all passengers and crew especially on ferries and cruise ships. The best way to achieve experience and to gain corresponding skills are practice runs on specially designed simulators which realistically represent the complex board conditions on such vessels after emergency alerts.

Simulators have proved beneficial for ship handling training in real time on well equipped bridges throughout the last decades. A new type of simulator is in development which will train and research specific aspects of Maritime Safety and Security. Wismar University has been involved in the conceptual design and development of this new technology produced by Rheinmetall Defence Electronics (RDE) in Bremen. The Maritime Simulation Centre Warnemünde (MSCW) is one of the most modern simulation centres worldwide providing a full mission Ship Handling Simulators (SHS), Ship Engine Simulators (SES) and Vessel Traffic Simulators (VTS). Now this centre is completed by a new type of simulator called the Safety and Security Trainer (SST).

Apart from existing regulations as e.g. SOLAS, STCW, ISM, ISPS it is essential to adopt a permanent process of change and development with regard to new precautionary measures against terrorism both in port and on board vessels. Training human mentality and motivation is vital to create a permanent underlying security culture.

The SST simulator, designed for 2D and 3D visualisation, developed out of the research project „VeSPer“ and is dedicated to the „Enhancement of passengers' safety on RoRo-Pax-ferries“ and was developed thanks to initiatives from the German government such as „Research for civil safety“ and specifically „Protection of traffic infrastructures“. The project is supported by the Ministry of Education and Research, under the aegis of the Technology Centre Düsseldorf (VDI). One of the most challenging innovations developed during the research is the 3D-designed RoPax ferry “Mecklenburg-Vorpommern“ for the SST simulation system, available for stand alone developed scenarios and in integrated mode

SESSION 4

PROTECTION AND RESCUE OF PEOPLE

together with the SHS. An integrated support and decision system, called MADRAS, will be interfaced into the SST (one work station on bridge) and assist officers to cope with safety and security challenges during manoeuvres of the vessel (SHS). All decks of the RoPax ferry can be visualised in 3D including the integrated dynamic safety equipment. Functional tests of the developed system are in progress and running successfully.

The sophistication of simulation at the MSCW has achieved a new level of quality. This new and enhanced simulation facility allows for “in deep” study of the effects of the safety and security plans and procedures on board and enable more detailed evaluation of their effectiveness under varying conditions and during different courses of events by a different series of simulation runs.

This paper will introduce the basic concept of the safety and security training simulator and describe the work entailed for its integration into the complex environment of full mission ship-handling- and ship-engine-simulators. Selected results of a case study dealing with first basic implementation of training scenarios will be demonstrated and discussed (see attached poster).

S 4.4

IT-SUPPORTED MANAGEMENT OF MASS CASUALTY INCIDENTS: THE E-TRIAGE PROJECT

A. Donner¹, C. Adler², M. Ben-Amar³, and M. Werner⁴

¹ DLR, Institute of Communications and Navigation, Münchner Str. 20, 82234 Weßling-Oberpfaffenhofen, Germany; ² Ludwig-Maximilians-Universität München, Departement Psychologie, Leopoldstr. 13, 80802 München, Germany; ³ Euro-DMS Ltd., Anzengruberstr. 10A, 82140 Olching, Germany; ⁴ TriaGnoSys GmbH, Argelsrieder Feld 22, 82234 Weßling, Germany
anton.donner@dlr.de

Paper-based triage and registration systems for organizing mass casualty incidents (MCIs) are still state-of-the-art because they are robust and their usage is intuitive. Nevertheless the main drawback is that information about affected persons remains among the persons themselves, making disaster management considerably more difficult. Data can be duplicated/aggregated by manually copying triage tags only, which is a laborious and time-consuming manual process, and the normal medium for exchanging information are voice-based radio systems. Besides tracing single persons passing the different stations of the rescue chain is practically not possible. Since MCIs normally overwhelm the regularly available rescue resources (rescue personnel, vehicles, hospital capacity) a particularly effective crisis management has to be applied. Operational command centres, decision makers, and rescue forces need information as quickly as possible on the type and number of injuries so that each affected or injured person gets optimal care.

Within the e-Triage project, which is sponsored by the German Federal Ministry of Education and Research, an integrated concept for electronic registration of affected persons is under development. The approach consists of four main elements: autonomous communication infrastructure, electronic data recording, a distributed database system, and psychological acceptance research. In more details, the e-Triage system comprises a satellite-based communication system with terrestrial radio cells that can be installed locally, matching end devices with dedicated application software for the registration of victims, and a distributed, self-synchronising database system guaranteeing maximal availability without a single point of failure. Apart from the technical challenges the degree to which emergency forces accept the e-Triage system will depend primarily on psychological factors. A pre-emptive design of the technology, which accommodates the reduced cognitive abilities of emergency personnel operating under extreme stress, is crucial for a successful deployment.

SESSION 5

SECURITY-RELATED LEGAL AND ETHICAL PRINCIPLES

KEYNOTE

GERMAN PRIVACY AND IT-SECURITY LAW (IT'S LAW) AS A CONTRIBUTION TO THE EUROPEAN AREA OF FREEDOM, SECURITY AND JUSTICE

From a global perspective, Germany is the historical pioneer of data protection law. Not only was the German legislature a first, but also the decisions concerning privacy and IT security of the highest German court – the Bundesverfassungsgericht (Federal Constitutional Court) - may have the potential to become a model for (European) law. In its statement from 20.04.2010, the European Commission writes: "In a global society characterized by rapid technological change where information exchange knows no borders, it is particularly important that privacy must be preserved. The Union must ensure that the fundamental right to data protection is consistently applied. We need to strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations." (COM(2010) 171, p.3).

The contribution presents legal principles that the Bundesverfassungsgericht has developed in recent decisions ("Vorratsdatenspeicherung" ("traffic data retention", 2010), "Online-Durchsuchung" ("online search of computers", 2008), "Kennzeichen-Scanning" ("licence plate scanning", 2008), "Rasterfahndung" ("dragnet investigation", 2006), "Polizeirechtliche Telekommunikationsüberwachung" ("preventive telephone wiretapping", 2006) and "akustische Wohnraumüberwachung" ("acoustic residential surveillance", 2004)) and discusses how and whether these principles can become elements of the European area of freedom, security and justice. The Lisbon Treaty now establishes the relevance of fundamental rights of the 27 Member States: "The Union shall constitute an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States." (Article 67 of the Treaty on the Functioning of the European Union).



BIOGRAPHY

Viola Schmid was born (1960) and raised in Bavaria, Germany. She studied law in Germany (Friedrich Alexander Universität, Erlangen; First and Second State Examination) and in the USA (Harvard Law School, Cambridge, LL.M.). She was a business lawyer (Fries Rechtsanwälte, Nuremberg, Germany) and worked as a lecturer at the Freie Universität of Berlin, Germany.

In 2002 she accepted the chair of Public Law at the Darmstadt University of Technology. Since then Prof. Schmid's research interest is cyberlaw, the division of rights and obligations, chances and risks in cyberspace. Her publications include among others works to e-justice, privacy, commercial speech and energy demand side management.

*Prof. Dr. Viola Schmid, LL.M. (Harvard)
Technische Universität Darmstadt
Fachgebiet Öffentliches Recht
Hochschulstraße 1
64289 Darmstadt
schmid@jus.tu-darmstadt.de*

SESSION 5

SECURITY-RELATED LEGAL AND ETHICAL PRINCIPLES

ESR: SYSTEM TRUST AND CRISIS MANAGEMENT – AN INTERACTIVE EXPERT EXCHANGE SYSTEM FOR ENHANCING SOCIETAL RESILIENCE

H.-L. Dienel¹, C. Henseler¹, R. Peperhove¹, W. Dombrowsky², N. John³, S. Rosenberg³, and Y. Sharan³

¹ nexus Institute for Cooperation Management and Interdisciplinary Research, Berlin;

² KFS Katastrophenforschung an der Universität Kiel; ³ ICTAF Interdisciplinary Center for Technology Analysis & Forecasting at Tel Aviv University

henseler@nexusinstitut.de

While the negative impact of social and economic conditions – the vulnerability of societies – is widely known and accepted in disaster research, the more upbeat notion of societies' resilience is quite a recent development. Drawing on an evocative metaphor and based on concepts from environmental research and psychology, a recent definition of societal resilience describes it as "a process linking a set of adaptive capacities to a positive trajectory of functioning and adaptation after a disturbance" (Norris et al.), or, as put more simply by Maguire and Hagan, "a resilient social entity absorbs, responds and recovers from the shock; and improvises and innovates in response to disturbances". Of the many factors determining a population's resilience – such as community competence, participation in policy decisions, economic development, etc. – we will focus on the role of trust in emergency management. Citizens' trust in emergency management organizations along with the trust of those organisations in people's capabilities to react adequately are among the most important assets for a society's resilience. With the aim of detecting successful methods for increasing trust and integrating people in emergency management, as well as assessing resilience-enhancing measures, this project employs a comparative and dialogue-centred approach. The cases of Israel, with its lengthy experience with terrorism on the one hand, and Germany, with its experiences and competencies in dealing with natural and industrial disasters on the other, offer a promising pair for mutual comparisons and learning. To enable crisis managers from both countries to share their good (and bad) experiences and practices in integrating citizens and strengthening societal resilience, a platform for knowledge sharing and dialogue will be developed. The concept for this interactive expert exchange system will be based on interviews and focus groups with prospective users, to whom the concept of the system will be presented. The preliminary concept as developed so far will be presented.

The research is funded by the BMBF under the support code 13N10409. A joint project of the nexus Institute for Cooperation Management and Interdisciplinary Research and the Interdisciplinary Center for Technology Analysis & Forecasting at Tel Aviv University (ICTAF) funded as a bilateral cooperation under the programme „Research of Civil Security“ by BMBF (D) and MOST (IL).

S 5.1

A SYSTEM ANALYSIS APPROACH TO SECURITY

J. Geisler and J. Beyerer

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung,

Fraunhofer-Str. 1, 76131 Karlsruhe

juergen.geisler@iosb.fraunhofer.de

Whoever is in charge to design a system has first of all to define a clear boundary between the system and its environment and the interactions crossing this boundary. For systems with the purpose to ensure security, what means to protect a certain entity, this is no trivial exercise. On the one hand the »Security-System« interacts with the »Entity-To-Protect«. On the other hand it has to interact with those entities that are assumed to jeopardize the security of the Entity-To-Protect: the »Source-Of-Hazard«. Furthermore the Entity-To-Protect naturally interacts with the Source-Of-Hazard and the Security-System has to be aware of this interaction. Finally the Security-System itself is a target for the Source-Of-Hazard and therefore also an Entity-To-Protect.

The system analysis approach to security introduced by the authors defines a basic interaction scheme between the three entities mentioned above. All three entities are thought as roles and not as physical distinct objects. So one human who protects himself is Entity-To-Protect as well as a Security-System. But the roles are strictly distinct and so it is possible to define clear interactions between them.

The interaction is modeled as flow of value from sink to source where the Source-Of-Hazard is a potential sink for value that causes loss to the Entity-To-Protect that itself is a source of benefit for the Security-System to pay its protection effort. This economic interaction is fundamental to all safety and security problems so far as human activity is the Source-Of-Hazard. Expressed with different functions of benefit over hazard the only distinction is made between utilizing the hazard as a means to gain economic benefit (e. g. robbery), regarding it as a purpose (gun rampage) or taking the hazard into account to save effort to prevent it (negligence). Being able to describe those economic interactions is a precondition to design properly working technical systems to ensure security.

SESSION 5

SECURITY-RELATED LEGAL AND ETHICAL PRINCIPLES

S 5.2

NEW APPROACHES FOR DATA PROTECTION AND ANONYMIZATION IN SURVEILLANCE SYSTEMS

H. Vagts and J. Beyerer

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung,
Fraunhofer-Str. 1, 76131 Karlsruhe, Germany

hauke.vagts@iosb.fraunhofer.de

Modern surveillance systems collect a massive amount of data. In contrast to conventional systems that store raw sensor material, modern systems take advantage of smart sensors and improvements in image processing. They extract relevant information about the observed objects of interest, which is then stored and processed during the surveillance process. Such high-level information is, e.g., used for situation analysis and can be processed in different surveillance tasks.

Modern systems have become powerful, can potentially collect all kind of user information and make it available to any surveillance task. Hence, direct access to the collected high-level data must be prevented. Each surveillance task should only access information that is required to fulfil its specified objective. Multiple approaches for anonymization exist, but they do not consider the special requirements of surveillance tasks. Furthermore surveillance systems can be used for varying reasons, e.g., thievery protection or location-based services for social networks. Hence, the specification of sensitive data is strongly connected to the objective of a surveillance task. This work identifies different classes of surveillance tasks and the according sensitive data. Based on these classes existing approaches for anonymization are examined and it is shown to what extent they can be used. Afterwards the existing approaches are extended to fulfil the requirements of the specific classes of surveillance tasks. Anonymization strategies cannot be seen isolated. They must interact with an identity management system, which handles all objects that should be anonymized, and with other components of the surveillance systems. Thus a framework is presented that enforces the anonymization strategies and realizes privacy-aware access to personal data related to the objects.

S 5.3

SAFETY AND SECURITY; TWO SIDES OF THE SAME COIN: PROPERTIES AND RELATIONS? CHARACTERISTICS TO REFINE? STRUCTURE OF TERMINOLOGY AND ITS PERCEPTION

L. Schnieder, E. Schnieder, and C. Stein

Technische Universität Braunschweig, Institute for Traffic Safety and Automation Engineering,
Langer Kamp 8, 38106 Braunschweig, Germany

l.schnieder@iva.ing.tu-bs.de

In many different standards and publications the subject matter of dependability, including reliability, availability, maintainability and especially safety/security, RAMS(S) for short, is defined by various concepts and terms. Their unambiguous definition can lead to a clear interpretation which facilitates communication of all persons involved in the development of safety-critical applications. By means of concise communication during specification, subsequent implementation as well as the preparation of operating and maintenance manuals negative legal, financial human or social impacts can be avoided. This is the purpose of the IGLOS- project (acronym for intelligent glossary), which is a totally new terminology management system on a solid differentiated linguistic basis. This system is intended to facilitate the development of a consistent, unambiguous and multilingual technical terminology which improves especially security relevant communication in scientific or commercial applications. This paper introduces a method for terminological disambiguation and applies it to the terms "safety" and "security". In the future this helps to improve communication in the domain.

Keywords

risk management, standardization, terminology, communication

SESSION 5

SECURITY-RELATED LEGAL AND ETHICAL PRINCIPLES

S 5.4

PUBLIC INFORMATION RESPONSES AFTER TERRORIST EVENTS (PIRATE)

P. Sellke¹, R. Amlot², B. Rogers³, J. Rubin⁴, J. Pearce³, F. Mowbray²

¹ Dialogik non-profit research Institute, Stuttgart, Germany; ² Health Protection Agency, Centre for Emergency Preparedness and Response, London, UK; ³ The King's Centre for Risk Management, King's College London, UK; ⁴ King's College London, UK
sellke@dialogik-expert.de

The threat western societies face through terrorist attacks became much more apparent than ever before through the attacks of 9/11 (New York and Washington 2001), 11-M (Madrid, March 11, 2004) and 7/7 (London, July 7, 2005). The new quality of those attacks comprised the deliberate attempt to cause as many fatalities as possible and to disrupt economic and social life. Not least the ruthlessness and sophistication of the attacks carried out made the use of radiological or biological substances for attacks conceivable, if not likely. How the public reacts to biological or radiological terrorism will help to determine how extensive the attack's medical, economic and social impacts are. Yet our understanding of what the public is likely to do in case of a radiological and/or biological attack is limited. Will they spontaneously evacuate affected areas? Are they willing to attend mass treatment centers? Will unaffected people demand treatment and monitoring? Will people avoid affected areas even after clean-up operations have been completed? As yet, we do not know. While emergency plans and simulations dealing with these scenarios assume a relatively compliant public with easily understood behaviors, evidence from previous incidents suggests that the reality may be different. As such, a first step to preparing better plans to protect the public is to identify actions they intend to take in the event of one of these scenarios occurring, and to assess how prevalent such intentions are in society.

In this presentation results from a two-year research project will be presented, addressing the questions outlined above and comparing them between Germany and the United Kingdom. In a first set of 20 focusgroups (10 in Germany, 10 in UK) participants were confronted with a fictive news broadcast either on a terrorist attack with smallpox or an attack with a radiological embedded device (RED). Results of the focus groups were being used to design representative surveys for Germany and the UK. In a second set of 40 focusgroups (20 per country), the news broadcast stimulus has been altered according to the information needs and behavioural responses articulated in the initial focusgroups and according to the results of the surveys. The presentation will emphasize the question of whether behavioral intentions of the public can be influenced by tailored emergency communication and the satisfaction of public's information needs and what possible differences in the response to terrorist attacks exist between Germany and the United Kingdom.

5th SECURITY RESEARCH CONFERENCE
BERLIN, SEPTEMBER 7th – 9th, 2010

CONFERENCE DINNER

SESSION 6

DETECTION OF HAZARDOUS MATERIALS – PART I

KEYNOTE

MODERN SENSORS FOR HAZARDOUS MATERIALS

This non-comprehensive overview concentrates on three typical applications: Sensors for First Responders, for cargo scanning and for aviation security. A few examples of chemical, of nuclear and of explosives detectors illustrate the large variety of technologies in use today.

First responders need to be highly flexible and equipped with portable detectors which do not only provide the capability of fast detection but also of a first and reliable identification. Vapour and trace detectors, e. g. based on ion mobility spectroscopy, and portable Raman spectrometers are examples of modern detection systems.

Dirty bombs or radioactive materials hidden in cargo containers have created a substantial need for radiation detection capabilities. Radioactivity detectors as portals are available; due to natural radioactivity like in tobacco false alarms are an issue. Expensive spectroscopic portals are available but also portable sensors for re-check purposes.

Most recent discussions in aviation security refer to liquid detection and to passenger screening. For liquids scenarios are rated in levels a to d in Europe. Various technologies are proposed for these categories Raman spectroscopy and multi-view x-ray evaluation are two examples. For scanning of passengers two major technologies are under test today, x-ray backscatter and mm-waves. Besides technical also privacy considerations are essential design criteria.



BIOGRAPHY

Dr. Hermann Ries is Chief Technology Officer for Security and Inspection products at Smiths Detection. In this position he has been responsible for R&D activities on security related detection systems in various competence centres since 2008. He joined the former Heimann GmbH in 1989 to work on explosives detection after having worked on novel detectors at the universities of Giessen, Heidelberg and at the European Research Centre CERN.

*Dr. Hermann Ries
Chief Technology Officer
Smiths Heimann GmbH
Im Herzen 4
65205 Wiesbaden
hermann.ries@smiths-heimann.com*

SESSION 6

DETECTION OF HAZARDOUS MATERIALS – PART I

IRLDEX: IMAGING STAND-OFF DETECTION OF EXPLOSIVES BY QUANTUM CASCADE LASER BASED BACKSCATTERING SPECTROSCOPY

F. Fuchs¹, S. Hugger¹, M. Kinzer¹, Q. K. Yang¹, W. Bronner¹, R. Aidam¹, K. Degreif², S. Rademacher², F. Schnürer³, and W. Schweikert³

¹ Fraunhofer Institute for Applied Solid State Physics (IAF), Tullastraße 72, 79108 Freiburg;

² Fraunhofer Institute for Physical Measurement Techniques, Heidenhofstr. 8, 79110 Freiburg;

³ Fraunhofer Institute for Chemical Technology, Joseph-von-Fraunhofer-Str. 7, 76327 Pfinztal;

frank.fuchs@iaf.fraunhofer.de

Due to the threat of terrorist bomb attacks, reliable stand-off detection of trace explosives at save distances has become an important issue. Optical detection techniques based on IR-laser spectroscopy represent a promising approach as organic chemical compounds typically exhibit strong characteristic absorbance patterns in the mid-infrared spectral range. Quantum cascade lasers are robust, compact and wavelength-versatile semiconductor lasers and therefore ideal illumination sources for spectroscopy in the mid-infrared spectral range.

We present the results of an imaging stand-off detection system based on a mid-IR external-cavity quantum cascade laser (EC-QCL) with a broad tuneable range of 200 cm^{-1} . Traces of TNT (trinitrotoluene) and PETN (pentaerythritol tetranitrate) as well as various non-hazardous substances such as flour or skin cream on different substrate-materials (Aluminum, standard car-paint, cloth) were investigated by illuminating them with the EC-QC laser and collecting the diffusely backscattered light. By tuning the EC-QCL across the significant absorption spectra we were able to detect the explosives and evaluate the possibility of false alarms caused by non-hazardous contaminations.

Keywords

stand-off detection, remote sensing, tuneable infrared laser, quantum cascade laser, external cavity laser, explosives, CBRNE detection

S 6.1

EVALUATION OF EXPLOSIVE DETECTION SYSTEMS – METHOD DEVELOPMENT, TESTING, BENCHMARKING, CERTIFICATION

D. Röseling, F. Schnürer, G. Bunte, and H. Krause

Fraunhofer ICT, Joseph-von-Fraunhofer-Straße 7, 76327 Pfinztal

d.roeseling@ict.fraunhofer.de

The European Commission aims to remove the current liquids restrictions that came into force in August 2006. Along with several incidents happened in the field of civil aviation security the intention has been drawn towards the need of reliable and certified bottled liquid detection systems. So far, only the liquid test methodology developed by the European Civil Aviation Conference (ECAC) task force offers the opportunity to benchmark the various detection systems present today. The CTM was assessed at the Fraunhofer ICT within two major testing campaigns from 2008-2009. This year, on behalf of the Federal Ministry of the Interior, the Fraunhofer ICT has been officially nominated as German test centre for liquid explosive detection. Beside the performance of official test campaigns according to the ECAC common test methodology initiated by the Federal Police the Fraunhofer ICT has developed a similar test method adapted to the needs of the different available detection methods of current detection systems such as x-ray, IR, IMS etc. The Fraunhofer ICT-Test offers a secure test infrastructure and includes standardised threat and benign samples, an objective test methodology as well as an intensive data evaluation. Manufacturers of detection systems have the chance to test their well-established or new developed devices against real explosive samples before participating in an official certification trial.

SESSION 6

DETECTION OF HAZARDOUS MATERIALS – PART I

S 6.2

NANODIAMOND COATED SAW PLATFORM FOR SENSING OF EXPLOSIVE AND WARFARE GASES AT HIGH SENSITIVITY

E. Scorsone, E. Chevallier, and P. Bergonzo

DRT/DETECS/SSTM/LCD, CEA de Saclay, Gif-sur-Yvette, France

emmanuel.scorsone@cea.fr

SAW sensors are known as promising platforms for the detection of toxic volatile chemicals due to their high sensitivity. However, the selective coating (often a polymer) deposited on such transducers is generally a limiting element in terms of selectivity, sensor to sensor repeatability and long term stability. We have developed a novel approach where we use modified NanoDiamond particles (NDs) as an alternative sensitive layer solving several of the issues often encountered on such sensors. Indeed, NDs can be found in nanometre sizes and be deposited as single or multiple layers on a variety of sensor surfaces with uniform thicknesses and high surface area, which is in favour of high sensitivity. NDs also feature attractive properties for chemical detection: (i) they are made of sp³ carbon which is very stable in time, and (ii) the carbon terminated surface of diamond offers wide perspectives from organic chemistry and biochemistry for covalent attachment of specific receptors.

The sensors were implemented in a very versatile detection platform consisting of a semi-industrial 8 channel SAW sensor system enabling high performance detection of gases or VOCs. In this contribution, we have optimised the NDs coatings for warfare gas detection. We report the detection of traces of dinitrotoluene, a precursor for the fabrication of TNT, and dimethyl methylphosphonate (DMMP), a simulant for sarin gas. We achieved detection thresholds in the low ppb range for both gases with high signal to noise ratio. The sensitivity for DNT was in the order of 200 Hz per ppb and over 5 Hz per ppb in the case of DMMP. Detection limits are below all values reported in the literature, together with improved stability, reproducibility and response time.

S 6.3

NEUTRON TECHNOLOGY APPLIED TO HAZARDOUS MATERIALS DETECTION

P. Le Tourneur, J. L. Dumont, I. Lefesvre, C. Groiselle, J. S. Lacroix, M. J. Lopez-Jiménez, P. Paul, and K. Soudani

EADS/SODERN, 20 Avenue Descartes, 94451 Limeil-Brévannes, France

philippe.letourneur@sodern.fr

In the framework of homeland security, there is a need for a clear assessment of vulnerabilities in threats that include explosive, chemical, radiological, and nuclear attacks (NRBCE). The most effective prevention against such attacks is detection and identification of the threats before it triggers. To meet this challenge, neutron technology could provide some help analyzing and identifying materials in a non intrusive way inside objects like parcels, pieces of luggage, containers or cars. Manufacturing leader in neutron tubes and generators for years, Sodern has developed a cutting edge “associated particle” tube (API) to meet the demanding requirements of the detection of hazardous materials.

Neutron tubes have been used for many years in industrial systems to scan materials. The material composition is determined by analyzing the secondary emission of gamma rays produced by the interaction of the neutrons inside the materials.

Sodern’s API (Associated Particle Imaging) tube enhances this analysis technology by adding a spatial resolution giving the capability to determine the location of identified elements within the object being analysed, a key requirement in security applications. Using the alpha position information and the time of flight of neutrons and gammas, spectral and 3D imaging algorithms provide composition and location of simple elements as carbon, oxygen, nitrogen, ... (present in explosives), arsenic, chlorine, sulphur, ... (could be components of toxic materials).

The ULIS (Unattended Luggage Inspection System) that has been developed for the need of bomb squads to analyze suspicious and abandoned objects will be presented with respect to the technology and to the operational conditions. Starting from that modest portable product and its achievements and referring to previous Sodern’ studies about EDS (Explosives Detection System: the INES project) the paper will discuss how the neutron technology could help solve in the future more difficult hazardous material detection problems.

SESSION 6

DETECTION OF HAZARDOUS MATERIALS – PART I

S 6.4

AIRPORT RELATED CBR THREAT ANALYSIS

A. Bongartz and A. Dörr

Industrieanlagen-Betriebsgesellschaft mbH (IABG), Defence and Security,
Department Vulnerability and NBC-Threats, Ottobrunn, Germany
bongartz@iabg.de

This unclassified presentation describes mainly the approach along with some general results of a CBR threat analysis within the framework of the joint research project FluSs (Flughafensicherungssystem = Airport Security System). The ongoing project, incorporating 12 research partners, is sponsored by the German Ministry for Education and Research (BMBF).

The basis for future security measures requires a comprehensive threat analysis. For the purpose of the joint research project this threat analysis has been structured into “event analysis”, “damage analysis”, “risk assessment”, and “gap analysis” for conventional (firearms, explosives) and CBR threats .

In case of CBR threats, the “event analysis” could not be based on a large record of incidents. Instead, the “event analysis” for CBR threats comprised a judgement on availability/producibility of agents, the technical feasibility of agent related release/dissemination scenarios, the required scientific/technical skills, and the accordance with offenders (terroristic) goals.

This view on possible agents and dissemination scenarios has than been combined with the specifics of the target infrastructure (airport) to yield a short-list of threat scenarios with defined location and time of the event. For the “damage analysis”, the effects of the incidents are described in figures for contaminated areas, possible victims, estimated times of closure and decontamination efforts.

Based on these figures, the “risk assessment” has been performed with results documented in tabular format. The tables comprise estimates for the probability of occurrence of an incident on one hand and for casualties, structural and operational effects, psychological impact, public relations efforts, and efforts in case of a false incident (fake) on the other hand. In this way a scenario ranking with respect to the mentioned effect categories was achieved.

Finally this analysis opened the fields for subsequent actions of the other project partners.

5th SECURITY RESEARCH CONFERENCE
BERLIN, SEPTEMBER 7th – 9th, 2010

POSTER PRESENTATION

SESSION 6

DETECTION OF HAZARDOUS MATERIALS – PART II

KEYNOTE

DETECTION OF PEROXIDE-BASED EXPLOSIVES

Inexpensive and mass producible sensors represent one of the keys to affordable security applications. A part of my group focuses on the development and application of high fundamental frequency quartz microbalances (HFF-QMB). The high frequency combined with appropriate affinity coatings on these QMBs allow a fast determination of airborne analytes. In particular, the tracing of home-made peroxides like TATP and HMTD is usually challenging but can be performed with our HFF-QMB system. The advantages are an on-line measurement of the desired analytes. Identification of the peroxides explosives is achieved by an array of at least three micro balances equipped with orthogonal affinities. Most remarkably, the system operates not only in a closed laboratory system but can be exploited for an application close scenario as an open system. With appropriate affinity coatings on the QMBs the scope of the method can be expanded to the continuous and direct detection of 2,4,6-trinitrotoluene (TNT).

In addition, a novel way for the safe handling of authentic material of peroxide explosives will be demonstrated representing the key for the evaluation of novel detection systems such peroxide explosives.



BIOGRAPHY

Prof. Dr. Siegfried R. Waldvogel was born in Constance, Germany, in 1969. He studied Chemistry at the University of Constance and obtained his PhD from the University of Bochum and the Max-Planck-Institute for Coal Research. He spent two years at the The Scripps Research Institute in La Jolla, California, to finish his post-doc. From 1998 – 2004 he was Assistant Professor at the University of Münster. Between 2004 and 2010, Siegfried Waldvogel was Professor for Organic Chemistry at the University of Bonn.

Since 2010, Siegfried R. Waldvogel has been full professor for Organic Chemistry at the University of Mainz. His fields of research include Supramolecular Sensing, Electroorganic Synthesis, Energy Storage Systems and the Synthesis of Complex Molecular Targets

*Prof. Dr. Siegfried R. Waldvogel
University of Mainz
Institute of Organic Chemistry
Duesbergweg 10 – 14
55128 Mainz
waldvogel@uni-mainz.de*

SESSION 6

DETECTION OF HAZARDOUS MATERIALS – PART II

CHIPSENSITEK: FEMTOSECOND IMPULSIVE LASER EXCITATION AND QUARTZ ENHANCED PHOTOACOUSTIC SPECTROSCOPY FOR EXPLOSIVE DETECTION

W. Schade¹, W. Schippers¹, J. Burgmeier¹, O. Katz², Y. Silberberg², and S. Rosenwaks³

¹ Technische Universität Clausthal, Germany; ² Weizmann Institute of Science, Rehovot, Israel;

³ Ben-Gurion University of the Negev, Israel

w.schade@pe.tu-clausthal.de

The objective of this joint German-Israeli research project is to provide a new compact sensor technology for multi-compound explosive detection in the gas phase that can be applied in security gates for sensitive infrastructure, such as airports, sports arenas, public buildings or power plants. The sensor combines photoacoustic detection technology with visible impulsive Raman femtosecond excitation, with the potential of producing a versatile, simple multi-component sensor. In a first step, triacetoneperoxide (TATP) which frequently is used by terrorists and which is a mixture of acetone and peroxide will be used as a test substance. These molecules have extreme high vapor pressure; therefore they can relatively easy be detected by spectroscopic methods. On the other hand, they show strong absorption bands in the mid-infrared spectral range (5-10 μm) that are accessible by quantum cascade lasers but because of broad absorption structures a wide tuning range is required. Also, sensitive mid-infrared detectors operating at room temperature are still a technological problem.

Therefore we develop and test novel nonlinear femtosecond laser spectroscopy, in particular so called impulsive femtosecond laser excitation, which offers the possibility for excitation of vibrational levels of molecules over a broad spectral range. Moreover, in combination with pulse shaping and coherent control techniques, impulsive excitation can be used for selective molecule excitation. Recently the Israeli partner has demonstrated that such impulsive excitation could be used for standoff detection of explosives. Impulsive laser excitation offers a very interesting new concept for a sensor device when combined with a new type of spectroscopy – the so called quartz enhanced photoacoustic spectroscopy (QEPAS). A QEPAS sensor combines sensor element and detector in the same device. In combination with impulsive femtosecond laser excitation QEPAS becomes a very attractive multi-compound analysis tool for routine inspections of dangerous materials, e.g. explosives. First results will be reported and discussed.

This project is funded as a German-Israeli cooperation under the programme „Research of Civil Security“ by BMBF (D) and MOST (IL).

S 6.5

BIOSENSORS FOR STANDOFF-DETECTION OF MINES AND EXPLOSIVES BY LASER INDUCED FLUORESCENCE

**M. Wehner¹, S. Schillberg², K. Hund-Rinke³, C. Kühn², N. Raven², H. Meurer⁴,
T. Wirtz¹, and R. Poprawe¹**

¹ Fraunhofer-Institute for Laser Technology, Aachen; ² Fraunhofer-Institute for Molecular Biology and Applied Ecology, Aachen; ³ Fraunhofer-Institute for Molecular Biology and Applied Ecology, Schmallenberg; ⁴ GeoTec GmbH, Brühl

martin.wehner@ilt.fraunhofer.de

Genetically engineered but environmentally safe soil bacteria are tailored to function as specific and sensitive whole-cell biosensors for landmines. This technique exploits the well known fact that all explosive devices constantly leak very minute traces of their explosive content into the environment. The biosensors react to substances that are present as vapours, diluted in water, or bound to soil particles in the surrounding of landmines. Upon contact with TNT or its derivatives the biosensor amplifies the signal by producing a large number of fluorescent proteins. Therefore the short range chemical contact signal is transformed into a long ranging optical fluorescence signal. When excited by a scanning laser beam the detection at great distance and mapping of large areas become feasible. Biosensors have the same capability to detect landmines as a mine detection dog – however, a large area can be monitored at a short time without entering the mine-field.

Within a feasibility study we generated a bacterial biosensor containing a TNT-specific promoter driving the expression of a red fluorescent protein when induced by the explosive. We have demonstrated that the biosensor detects TNT and ADNT in soil samples. The detection limit for an ADNT induced fluorescence response can be estimated at 10 mg/L. To excite and detect the fluorescent signal produced by the bacterial biosensor over a large distance a modified laser scanner was generated. Signal calibration by comparing dye solutions revealed a production rate in excess of 105 fluorophores per cell for artificially activated biosensors. Signal bacterial colonies could be detected at a distance of 10 m using a laser scanning device with a numerical aperture of NA ~ 0.6 mrad. These results demonstrate that standoff-laser detection of whole cell biosensors could be a powerful tool to detect explosives and landmines employing ground-based or airborne vehicles.

SESSION 6

DETECTION OF HAZARDOUS MATERIALS – PART II

S 6.6

PREVENTION OF ILLICIT TRAFFICKING OF NUCLEAR AND RADIOACTIVE MATERIAL AT BORDER STATIONS BY MEANS OF HIGHLY EFFICIENT DETECTION SYSTEMS

W. Rosenstock, W. Berky, S. Chmel, H. Friedrich, T. Köble, M. Risse, and O. Schumann

Fraunhofer-Institute for Technological Trend Analysis (INT), 53879 Euskirchen, Germany

wolfgang.rosenstock@int.fraunhofer.de

In the context of the possible threat of proliferation of nuclear material by groups of terrorist and non-state actors reliable detection techniques of such material are of great importance at points of interest such as airports, harbors, railway stations, and border crossing points. The opportunity to detect nuclear material is given at border stations in particular because vehicles and pedestrians potentially carrying such material are forced to drive or walk slowly in lines, thus providing well-defined measuring conditions. Gamma and neutron detectors with a high efficiency are required for this task. As consortium leader of the current TACIS (Technical Assistance to the Commonwealth of Independent States) project "Ukrainian Border Security" of the European Union our institute is involved in setting up modern stationary portal monitor systems at selected Ukrainian border stations in order to provide adequate detection techniques for the prevention of illicit trafficking of nuclear material at these borders.

The current status of the project will be presented. Furthermore, Fraunhofer-INT operates a mobile portal monitor system manufactured by Thermo based upon our institute's requirements and specifications. It comprises two pillars containing large-volume NaI crystals which can be used separately or combined, then forming a portal of variable width. Besides providing the option to localize radioactive or nuclear material, the system also allows for the discrimination between naturally occurring radiation and artificial material by means of the implemented NBR method. The measured count rate data are transferred to a PC by radio transmission. A series of measurements was performed with this portal monitor system to test its ability to detect both radioactive and nuclear material. An overview of the measurement results will be presented as an example of the capabilities and performance of current portal monitor systems.

S 6.7

PUBLIC AND USER ACCEPTANCE OF UNMANNED AERIAL VEHICLES IN DISASTER MANAGEMENT AND PREVENTION – EMPIRICAL FINDINGS

A. Hermanns

Technische Universität Berlin, FG Innovationsökonomie, Sekr. VWS 2,
Müller-Breslau-Straße, 10623 Berlin
andre.hermanns@tu-berlin.de

The Federal German Government is funding national civil security research to develop a variety of technical solutions for public safety & security, strongly acknowledging social science research and end user demands as well.

Project „AirShield“ (Airborne Remote Sensing for Hazard Inspection by Network-Enabled Lightweight Drones) develops a swarm of mini drones (5kg quattrocopters), that are equipped with gas sensors and artificial intelligence, in order to detect and continuously measure toxic clouds, e.g. after a fire in a chemical plant, and to deduce counter-measures for the population, e.g. evacuation.

One of TU Berlin's tasks in this project is to investigate public as well as end user acceptance of this technology and its application. The empirical findings will now be presented. To investigate public opinion, 400 interviews were conducted on three public events (2x Hanover Fair and Open Science Day at TU Berlin) over a one year time period.

Analysis of the surveys compared support for different technologies, for alternative drone applications and compared the importance of different acceptance factors and socio-demographic factors. The results showed a high degree of support by 71% for drone technology in general. However, though the AirShield system neither collects nor stores or processes personal data, the paper reveals the perception and concerns that such a technology might affect privacy. Technological, regulatory and application based proposals are made to overcome that barrier.

End user acceptance was collected based on an adapted Unified Theory of Acceptance and Use of Technology model. Factors like utility, reliability, usability but also cost-effectiveness, innovation climate and the legal framing were investigated. More than 40% of the German professional fire departments gave their feed back. The analysis includes a comparison with potential “special” users in the BBK's Analytical Task Forces, the German Landesfeuerweherschulen and company fire departments.

SESSION 6

DETECTION OF HAZARDOUS MATERIALS – PART II

S 6.8

CHIP CARDS AS FORTUITOUS INDIVIDUAL DOSIMETERS AFTER NUCLEAR EMERGENCIES AND RADIOLOGICAL TERRORISM

C. Woda¹ and T. Spöttl²

¹ Helmholtz Center Munich, German Research Center for Environmental Health, Institute of Radiation Protection, Ingolstädter Landstr. 1, 85764 Oberschleissheim, Germany

² Infineon Technologies AG, Wernerwerkstraße 2, Regensburg, Germany

clemens.woda@helmholtz-muenchen.de

The increasing risk of a mass casualty scenario following a large scale radiological accident or attack necessitates the development of appropriate dosimetric tools for emergency response. Here we demonstrate that contact based chip card modules with a translucent globe top covering have high potential to be used as individual dosimeters for rapid assessment of the radiation exposure received by the individual. These modules find use in credit cards, cash cards, health identity cards and SIM cards and are thus carried by a larger part of the general population. The radiation sensitive component is traced to silica in the covering layer of the chip, added to control the properties of the epoxy encapsulation.

Luminescence properties turned out to be complex due to the presumed thermo-optical release of electrons from the epoxy and transfer into the silica during measurement. Nevertheless, a suitable measurement protocol could be developed using optically stimulated luminescence (OSL) without any preheat treatment. The dose response of the chip card modules is then linear up to almost 10 Gy and a minimum detectable dose as low as 10 mGy one day after exposure could be achieved. The signal is not stable at room temperature but irradiation trials indicate the applicability of a universal signal decay function for fading correction. Processing time of a single module is less than 30 minutes.

In addition, we also report on first investigations on contact based and contactless modules using mold encapsulation, the contactless version finding potential use in electronic documents.

Keywords

Nuclear emergency, radiological terrorism, emergency response, fortuitous dosimeter, chip card modules, luminescence dosimetry.

SESSION 7

PROTECTION OF SUPPLY NETWORKS

KEYNOTE

SECURITY BASED ON ORGANIZATION, CONTROL AND TECHNOLOGY

As global operating logistic service provider Kuehne + Nagel has a long lasting experience in organizing supply chains for high value products under special security requirements.

Actually Kuehne + Nagel knows two different main aspects of security:

First, the the state-required aspects, driven by target to avoid terrorism and crime with laws and regulations. Results are for instance the 9/11 Commission Act of 2007 by the USA, ISPS, CTPAT, AEO and so on. We call these aspects "Macro Security".

"Micro Security" in our understanding means security requirements, driven by customers' requirements, as part of contracted logistic services. Micro security procedures have to be "tailor-made", covering individual needs and risks of customer and his products.

Starting with micro security aspects the presentation will give an example for an operating security system, covering the entire supply chain, developed in cooperation with a high sophisticated customer, based on 3 reliable pillars:

- Organization under security aspects
- Control
- Technology for additional security

The presentation will show details from daily operational business as well as results.

Based on proven technology the company developed in a joint project with two partners (Bosch Sicherheitssysteme and Koch Kommunikation) a new system for global container monitoring and tracking + tracing. After some years experience in operating business with that system the discussion started if such a system would be applicable to fulfill state requirements/macro security aspects as well as micro security needs. The presentation will give a short spot on actual discussion and research projects, Kuehne + Nagel involved.

Some remarks regarding experiences, problems and prospective developments will close the view on protection of supply networks from a logistic service provider perspective.



BIOGRAPHY

Lorenz W. Sönnichsen was born in Landshut, Germany, in 1947. He graduated as Diplom-Kaufmann at the University of Hamburg, where he studied economics with a focus on industrial economics, operations research and logistics.

Before joining Kuehne + Nagel's headoffice in Hamburg in 1984, Lorenz Sönnichsen worked as management consultant with a focus on logistics for different industrial companies.

His responsibilities at Kuehne + Nagel include loss prevention management, general security projects and facility management.

*Lorenz Sönnichsen
Kuehne + Nagel AG & Co. KG
Großer Grasbrook 11-13
20457 Hamburg
lorenz.soennichsen@kuehne-nagel.com*

SESSION 7

PROTECTION OF SUPPLY NETWORKS

IRLSENS: INFRARED FIBEROPTIC LASER SENSOR SYSTEM FOR THE DETECTION AND RECOGNITION OF HAZARDOUS CHEMICAL SUBSTANCES IN DRINKING WATER

F. Fuchs¹, W. Konz², D. Richter³, G. Biber⁴, A. Simon⁵, A. Katzir⁶, T. Würtenberger⁷, and S. Kaufmann⁸

¹ Fraunhofer Institute for Applied Solid State Physics, Tullastraße 72, 79108 Freiburg;

² Fraunhofer Institute for Physical Measurement Techniques, Heidenhofstr. 8, 79110 Freiburg;

³ DVGW-Technologiezentrum Wasser, Karlsruher Straße 84, 76139 Karlsruhe; ⁴ Zweckverband Wasserversorgung Kleine Kinzig, Berneckstrasse 100, 72275 Alpirsbach-Reinerzau; ⁵ Bruker Optik, Rudolf-Plank-Str. 27, 76275 Ettlingen; ⁶ Tel Aviv University, School of Physics and Astronomy, Ramat Aviv, Tel Aviv 69978, Israel; ⁷ Universität Freiburg, Institut für Öffentliches Recht, Platz der Alten Synagoge 1, 79110 Freiburg; ⁸ Universität Freiburg, Institut für Soziologie, Rempartstr. 15, 79085 Freiburg

frank.fuchs@iaf.fraunhofer.de

Among possible scenarios of terrorist attacks the poisoning of the central water supply is considered to be extremely critical. The protection of drinking water is of major public interest. Water supply units typically are enclosed; however, they are not under permanent surveillance. In order to reduce the impact of a terrorist attack, fast localization of the place where the poison has been released as well as the identification of the chemical species are of utmost importance for the reaction forces.

The technical goal of the IRLSENS project is to develop a fiber-optic sensor system with a broad band tuneable infrared laser, based on quantum cascade laser technology, serving as the spectroscopic infrared source. From the Israeli side the focus is on the development of the fiber-optic sensors, the German contribution comprises the development of the infrared laser system. For the tuneable laser module, a modified Littman-Metcalf configuration is envisaged, making use of the principle of wavelength-coupling in an external resonator. This scheme is configured for an ultrafast time-multiplex fiber-based spectroscopy without moving mechanical parts, enabling sampling well above typical acoustic noise frequencies. This system will operate fully automated for the on-line control of the water supply system. Since a semiconductor-based solution is proposed, there is a big potential for cost reduction and downsizing of the measuring unit. A demonstrator system for real-time in-situ detection of the most relevant chemical species will be realized and subsequently evaluated in field tests performed in drinking water supply units.

The project is funded as a German-Israeli cooperation under the programme „Research of Civil Security“ by the German Federal Ministry of Education and Research (BMBF) and the Israeli Ministry of Science and Technology (MOST).

S 7.1

A NEW DEVICE FOR MONITORING DRINKING WATER BASED ON IMAGE ANALYSIS

T. Schuchert, T. Müller, and M. Höpken

Fraunhofer Institute of Optronics, System Technologies and Image Exploitation,
Fraunhoferstraße 1, 76131 Karlsruhe, Germany

tobias.schuchert@iosb.fraunhofer.de

Fast and reliable detection of drinking water contamination is essential in order to take counteractions in time, e.g. warning population. Therefore drinking water quality is tested on special germs and chemical substances on a regular basis. In most cases the analytical techniques are carried out offline in special laboratories. These methods are time-consuming and limited to known and expected substances. Recently several techniques have been developed, which allow analyzing water online. These techniques are based on devices directly connected to the drinking water supply. The devices contain microbiological organisms, which react on contaminations in the water. The changes of the organism's behavior are detected by image processing methods. The main drawback of these methods is an increased number of fail alarms due to changes in water, e.g. increased temperature or oxygen, which lead to changes in the behavior of the organisms but is no harm for humans.

In this work we present a device which allows fast development and prototyping of new image processing algorithms for detection of drinking water contamination based on motion analysis of biological microorganisms. The device designed at Fraunhofer IOSB consists of an imaging sensor unit which acquires images of two cuvettes containing the same biological organism. Cuvette pairs of different sizes allow monitoring of different biological species, e.g. Brine shrimps, Paramecium, Turbatrix aceti or Daphnia. A cuvette pair consists of one cuvette filled with "good" drinking water and one cuvette filled with water to be tested. The behavior of the organisms in both cuvettes is then analyzed by image processing tools and differences in behavior coming from contaminated water are detected. The combination of two separated cuvettes helps to filter out motion behaviors, which do not rely on current water quality, i.e., changing behavior due to growth of the organisms.

SESSION 7

PROTECTION OF SUPPLY NETWORKS

S 7.2

SAFETY AND SECURITY OF DRINKING WATER DISTRIBUTION SYSTEMS

M. Eriksson

S-SENCE and Laboratory of Applied Physics, Linköping University, Sweden

mats.eriksson@liu.se

A national Swedish collaborative project is presented, that aims at strengthening and developing existing crisis management systems by incorporating a detector for unexpected events due to biological and chemical substances, leading to faster actions in case of an emergency. The municipal drinking water distribution system is used as a test bed for the development of such an event detector, but the sensor network could also be applied to ensure safe drinking water in critical buildings. In the project the whole chain from the sensor to the end user is taken into account. Therefore both sensors that detect changes in the water properties, algorithms that distinguish between normal variations of the drinking water properties and anomalies, communication of the evaluated sensor data to a crises management system and presentation of information that is relevant for the end users of the crises management system are considered.

Several technologies have been considered for local event detection in drinking water distribution systems. In this project we have chosen to focus on a technique based on a „voltammetric electronic tongue“. By utilizing this type of non-selective sensor, we will be able to detect a plurality of anomalies without the need of a specific sensor for each type of event.

One aim of the project is to supply an early warning, due to e.g. terrorist attacks, sabotage or accidents. This will facilitate fast initial decisions which can be followed up with careful investigations leading to optimized actions. In order to achieve this goal a project consortium with complementary competences has been formed. It consists of the S-SENCE group at Linköping University, the security group of the municipality of Linköping, who serves as an end user, the drinking water supplier Tekniska Verken i Linköping AB, Saab Security, supplier of the crisis management system ISAK.

S 7.3

DEPLOYING PROCESS MANAGEMENT FOR EMERGENCY SERVICES LESSONS LEARNT AND RESEARCH REQUIRED

G. Peinel¹, and T. Rose^{1,2}

¹ Fraunhofer Institute for Applied Information Technology, Schloss Birlinghoven, 53757 Sankt Augustin, Germany; ² Information Systems, RWTH Aachen University, Ahornstr. 55, 52056 Aachen, Germany

gertraud.peinel@fit.fraunhofer.de

TRescue organizations have intensified their efforts to prepare for major emergency events. Typically each preparation compasses a planning phase, a reconciliation phase among affected organizations and a training exercise for evaluation. The latter often causes a re-planning since bottlenecks of resources or coordination short-comings have been identified based on exercises in field trials. Currently, this preparation process is dominated by the use of paper-based documents. Yet, knowledge represented in simple flowcharts and textual process descriptions is ambiguous and not formally processable. But, process management has proven to be instrumental for the engineering and assessment of courses of actions to meet specific objectives.

In this presentation we want to give a summary of our work and experiences made when introducing the concept of process management to the domain of emergency services in tight collaboration with rescue organisations.

In this process modelling endeavours we have identified major process modelling issues and research challenges:

Customisation of modelling language and environment – Emergency management processes have to be modelled according mindset and peculiarities of emergency services.

Deliberation of design rationales of processes – Operations of rescue organisations are driven by tactical and operational goals. Hence, the design rationales of counter actions have to be exposed explicitly rather than merely setting relationships among goals and activities as in prevailing process management tools.

SESSION 7

PROTECTION OF SUPPLY NETWORKS

Traceability of concepts – To prepare for large-scale disasters contributions from different organisations have to be merged. Thus, traceability of decisions – also for legal reasons – has to be provided.

Organisational model – Organisations have to be modelled rather detailed in order to assess feasibility of plans since capabilities and privileges of dynamic organisational units are decisive.

Informal representation of processes – Informal representations such as Excel or drawings are recommended to capture the initial skeleton of the process envisioned. Once initially reconciled, formal representations can be expanded.

Our projects' experiences unveil a minor importance of direct workflow support, since most of the actions to be planned are not embedded in ICT environments. However, we faced an interesting research challenge with regard to control structures for simulation purposes. Many processes are defined for different alarm levels. Hence, means for process escalation and relaxation are required to accommodate shifts among levels of alarm.

can be reached and an attack may result in enormous negative economic implications. The WHO (2002) stated that "the malicious contamination of food for terrorist purposes is a real and current threat, and deliberate contamination of food

S 7.4

DEFENDING FOOD SUPPLY CHAINS - A UK APPROACH

S. Barrass

Centre for the Protection of National Infrastructure (CPNI), London, UK

steveb@cpni.gsi.gov.uk

This paper will examine approaches to prevent the malicious disruption of food supply, and the ill-health, public concern, economic loss and media reaction which this could cause.

Strong commercial competition within the food industry together with the wide diversity of supply mechanisms, not least those involving global trade, provide built-in resilience to disruption. The high level of intrinsic vulnerability of the industry means that malicious attack is conceivable, but the consequences are unlikely to be widespread. That said, even the rumour of an attack could cause significant public discontent, economic disruption and criticism by the media.

Following the 9/11 attacks, the World Health Organisation charged governments to work with food industries to build protection against possible terrorist attack and improve recovery and continuity procedures in the event of a successful incident. This is now widely termed 'food defence'. The United States has publicised 'CARVER+Shock', the French Government has Vulnerability Analysis Critical Control Point (VACCP) and the British Government has supported development of Publicly Available Specification (PAS) 96 - Defending food and drink. PAS 96 has been reviewed in 2010 and now describes Threat Assessment Critical Control Point (TACCP) as the proportionate approach to food defence.

These are all risk management tools and share many common features. The paper will look at some of the underpinning theory and practical implications of food defence.

SESSION 8

SECURITY OF COMMUNICATION NETWORKS

KEYNOTE

SECURE OVERLAY-BASED AUTOCONFIGURATION OF COMPLEX IPsec VPN

G. Schäfer¹, M. Roßberg¹, and K. Martius²

¹ Technische Universität Ilmenau; ² secunet Security Networks AG

Virtual private networks (VPN) offer services for secure data exchange over public networks and are steadily gaining importance for commercial organizations, private individuals as well as governments and military. However, growing VPN sizes and a dynamic behavior of VPN gateways and clients, e. g., for mobility reasons or perhaps reactions due to denial-of-service attacks, make a manual configuration of large, dynamic VPN complicated and expensive. First, the administrative overhead grows quadratically with the number of VPN devices, if each VPN device shall be able to communicate with every other VPN device. This will not only lead to higher expenses, but also to more errors caused by human failure. Second, the robustness of the VPN is not as high as it could be, e.g., in case of partial failures of the transport network some VPN devices could redirect traffic for other devices that cannot reach each other directly anymore. Even though IPsec could support such a resilient behavior by utilizing nested security associations, manual reconfiguration prohibits a timely reaction. Third, manually configured security associations cannot be adopted with sufficient flexibility to support mobile VPNs appropriately. It is not possible to just configure security associations between two mobile devices as both regularly change the IP addresses that they are reachable over. In consequence, a number of diverse VPN auto-configuration approaches have been invented, implemented, and – at least partially – deployed over the last decade. This talk will motivate and explain a comprehensive set of objectives to be fulfilled by such mechanisms, give a brief overview of existing mechanisms and present our own approach Secure OverLay for IPsec Discovery (SOLID) that allows for fully automated configuration of IPsec VPN, scales well with respect to the number of IPsec gateways, reacts robust to network failures, and supports the configuration of nested networks with private address spaces.



BIOGRAPHY

Prof. Dr.-Ing. Günter Schäfer studied Computer Science at the University of Karlsruhe (TH) and worked as research assistant at the Institute of Telematics. After finishing his PhD thesis in 1998 he joined the Ecole Nationale Supérieure des Télécommunications in Paris, where he dealt with issues of network security and the capacity of access networks of mobile communication networks of the third generation.

In August 2000, he joined the Technical University Berlin in the department of telecommunication networks. He worked in the domains of network security, mobile communication and active network technologies. He was appointed Head of the department of Telematics/Computer Networks at the Technical University in Ilmenau in 2005.

His main areas of interest are the domains of network security, safety of communication infrastructures and communication protocols and architectures. Günter Schäfer is a member of the Association of Computing Machinery (ACM), of the Institute for Electrical and Electronics Engineers (IEEE) and of the Gesellschaft für Informatik (GI).

*Prof. Dr.-Ing. Günter Schäfer
Fachgebiet Telematik/Rechnernetze
Technische Universität Ilmenau
Postfach 100565
98684 Ilmenau
guenter.schaefer@tu-ilmenau.de*

SESSION 8

SECURITY OF COMMUNICATION NETWORKS

EMSIN: ELECTROMAGNETIC PROTECTION OF IT-NETWORKS FOR TRANSPORTATION-INFRASTRUCTURES

N. Sonnenberg¹, H. Garbe², M. Koch³, R. Rambousky⁴, C. Pistor⁵, and N. Sharfi⁶

¹ THALES Defence Deutschland GmbH, Pforzheim; ² Gottfried Wilhelm Leibniz Universität Hannover; ³ Fachhochschule Hannover; ⁴ Wehrwissenschaftliches Institut für Schutztechnologien, Munster; ⁵ Flug- und Industriesicherheit Service- und Beratung, Kelsterbach; ⁶ Netline Communications Technologies Ltd (NCT), Tel Aviv, Israel

Werner.Kranzpiler@thalesgroup.com

The aim of this project EMSIN is the technical and organizational protection of critical traffic infrastructure against intentional electromagnetic field interferences. The collaborative project is based on scenarios for asymmetric threats applying electromagnetic sources (so-called HPEM-sources) to induce a planned impact on electronic components of critical infrastructures. Private and public partners are going to develop an integral approach to ensure the proper function of critical infrastructure (in this case: airports) by technological and organizational means and threat detection as well as alerting.

Modern communication-systems are the backbone for secure and smooth proceedings. Fast information-transmission, continuous access to databases as well as the management of air traffic are most important for effective and safe operation. Malfunctions, a breakdown, damages or destruction of parts of the system may lead to a breakdown of the whole communication-system thus leading to severe failures in the system and eventually even causing catastrophic accidents.

Planned innovations and developments:

- Sensor for immediate detection and location of attacks by electromagnetic pulses.
- Investigation and modelling of the electronic infrastructure of real arrangements (German and/or Israeli airport), Identification of weak points.
- Set-up of a test-network. Recommendations for structural concepts of networks based on simulations and measurements performed with the test network.
- Early threat detection and evaluation of immediate measures after a HPEM-attack
- Strategies and concepts for risk assessment and danger prevention
- Examination of the developed concepts under societal and legal aspects.

The project is funded as a German-Israeli cooperation under the programme „Research of Civil Security“ by BMBF (D) and MOITAL (IL).

S 8.1

A HIERARCHICAL FRAMEWORK FOR QUANTITATIVE CORPORATE IT RISK MANAGEMENT

S. Schmidt and S. Albayrak

DAI-Labor, Technische Universität Berlin

stephan.schmidt@dai-labor.de

Risk management and business process management play an increasingly vital role in contemporary corporate infrastructures due to a multitude of operational, technical and regulatory reasons. Increasingly complex interdependencies as well as flexibility demands in rapidly changing networked environments make this effect even more pronounced for companies which are strongly based in the IT domain.

Current risk management methodologies are often static in nature and can not meet the demands of operational practices. Risk assessment is often not integrated into the business process management process but rather executed in parallel. A systematic modeling approach is needed which captures the relationships between vulnerabilities and associated threats with their effect on the business assets as well as the interdependencies between assets and threats. The latter aspect is often disregarded in current practice but has huge implications in practice, for example cascading failures.

Within the presented framework, we are aiming to quantify the „virtual“ value of a IT infrastructure (hardware) component with respect to how much its continuous operation contributes to the value generated by the business processes it supports. This value does not necessarily coincide with the conventional asset value, which might be computed as the sum of acquisition, deployment and operational costs. We develop a quantitative framework where, given business process revenue information and dependency assessment, we can determine these virtual asset values using mathematical tools from graph and control theory. Subsequently, we can correlate this asset value with the threat assessment information to get a complete picture of risk dissemination on the lowest level of abstraction, the actual IT hardware infrastructure.

In this domain, we are able to use various mathematical tools, such as graph, game and control theory, to compute optimal risk management strategies which include mitigation and transfer of identified IT risks. Due to the required flexibility and rapid changes in topology or assessed input values, we develop algorithms which select optimal security strategies from a given portfolio of available actions for predefined time periods.

SESSION 8

SECURITY OF COMMUNICATION NETWORKS

S 8.2

AUTOMATIC NETWORK RECONFIGURATION FOR DENIAL-OF-SERVICE DEFENSE USING DYNAMIC IMPACT ESTIMATION

M. Jahnke, G. Klein, and J. Tölle

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE,
Neuenahrer Str. 20, 53343 Wachtberg, Germany
marko.jahnke@fkie.fraunhofer.de

Defending computer systems and networks against the ever increasing number of cyber attacks needs different strategies and their reliable implementation in terms of technical, physical, and procedural measures. This means that both the root causes of attacks and their actual symptoms in terms of threat and damage need to be investigated. While recent research results on in-depth analysis of malware and botnets gained significant progress in understanding the internals and the underlying structures of cybercrime tools, these are of limited use to defend a network against ongoing attacks once they occur.

Various examples for severe Denial-of-Service (DoS) attacks against large-scale network infrastructures (e.g., Estonia 2007, Georgia 2008) have shown that without proper countermeasures, a complete shutdown of national IT infrastructure might be the ultimate consequence of these attacks, leading to serious damage in several areas like national economy, energy, healthcare, public administration and transport. In cases like these, appropriate near-real-time mechanisms for reconfiguring parts of the network or services would contribute significantly to a mitigation of the attacks. Knowledge of effects of an attack countermeasure is very important to avoid unwanted harmful impact.

GrADAR (Graph-based Automated DoS Attack Response) is a methodology for assessing the effects of attack countermeasures on the availability of resources in a networked scenario by evaluating their effects prior to their real-world application in a model that is updated during run-time. The availability of the key resources is measured using distributed sensor components in the network. Based on these values, GrADAR suggests the most appropriate alternative from a given set of network reconfiguration actions. Different metrics for quantifying the attack and response effects may be used, including the expected response success, application costs and durability.

This has been shown to work well for known and explicitly specified countermeasures and for reliably measurable resource availability values. Current research focuses on establishing a common operational picture (COP) of network resources' availability even with incomplete and potentially disturbed observations. Additionally, approaches for exploring previously unknown combinations of elementary response actions, based on well-known optimization technologies in the response action space are being investigated.

S 8.3

HEROLD – AGENT-ORIENTED, POLICY-BASED NETWORK SECURITY MANAGEMENT

S. Adameit¹, T. Betz¹, F. Hars², M. Hewelt¹, D. Moldt¹, J. Quenum¹, A. Theilmann², T. Wagner¹, T. Warns², and L. Wüstenberg¹

¹ Theoretical Foundations of Computer Science, University of Hamburg

² PRESENSE Technologies GmbH, Hamburg

warns@pre-sense.de

Computer networks are getting more and more complex. Common use cases span multiple subnetworks under different administrative control and integrate external networks for grid and cloud computing. Classical approaches to network security, which focus on security enforcement at the network perimeter, are no longer sufficient in this context.

The BMBF-funded project Herold addresses these challenges by developing a new, agent-based approach for managing network security components (NSCs) such as firewalls or intrusion detection systems. Herold allows to define policies at a global level while enforcing them locally. The approach relies on three cornerstones: cooperative creation of security policies, automatic transformation from abstract policies to technical configurations, and cooperative policy enforcement.

Administrators use local, autonomous software agents for defining a security policy for the subnetwork under their administrative control. The administrators can resort to high-level abstractions in order to keep policies concise and easy to understand and inspect. The different agents that form the overall management system interact to determine a common global policy.

The agents transform the global policy to technical configurations and deploy these on the NSCs they have been assigned to. An agent may also delegate parts of the policy enforcement to other agents. A particular goal of the policy transformation is to obtain a high degree of compartmentalization: The NSCs are configured such that the overall network is separated into small cells that are secured from each other.

Together, the agent-managed NSCs enforce the global policy as a cooperative effort. All NSCs only enforce the parts of the global policy that are relevant at their respective location, which improves efficiency. Additionally, as part of a defense in depth strategy, a policy for a subnetwork may, for example, be enforced by its own NSCs as well as by NSCs in other subnetworks.

SESSION 8

SECURITY OF COMMUNICATION NETWORKS

S 8.4

USABILITY OF BIOMETRICS ON MOBILE PHONES

N. Kirschnick, H. Sieger, and S. Möller

Quality and Usability Lab, Deutsche Telekom Laboratories, TU Berlin

niklas.kirschnick@telekom.de

Not long ago, mobile phones had only limited capabilities and were mainly used for phone calls and SMS. With advances in technology, smart phones have evolved to small computers, and usage now includes online banking, social networks, internet access, calendars, address books, and more.

All these private data and sensitive applications are mostly only secured by a PIN code. If this PIN code is used properly it would give acceptable protection, but unfortunately many users choose a too easy PIN code (like 1234) or write it down with their phone. Furthermore, entering the PIN code in public is very prone to shouldersurfing. These issues lead to the fact that the PIN code is quite insecure.

To increase the security of mobile phones, biometric authentication mechanisms can be used. There are different biometric authentication mechanisms that could be imagined on a mobile phone: face, iris and voice recognition, fingerprint scans and signature and gesture authentication.

Our research focuses the on perceived security and usability of biometrics on mobile phones. To evaluate these aspects we combined two user research methods:

- (1) Supervised focus groups where concepts and mock-ups have been presented to potential users and group discussions have been moderated; and
- (2) Online surveys to reach more users in their natural environment. The results of these evaluations will be analyzed in the talk. They show that most users would like to use biometrics on their mobile phones, and that the fingerprint scan is the most favoured one.

To further evaluate the usability of biometric authentication methods on mobile phones, we currently design a demonstrator which combines several of the formerly mentioned methods. It will be used for controlled laboratory experiments which will more detailed information on the advantages and inconveniences of biometric authentication on mobile phones from a usability perspective.

5th SECURITY RESEARCH CONFERENCE
BERLIN, SEPTEMBER 7th – 9th, 2010

CONFERENCE CLOSING

POSTERS

P 1 PREVENTION OF ROAD TRANSPORTS FROM ORGANIZED CRIME

L. Axelsson

Lindholmen Science Park

leif.axelsson@lindholmen.se

Crimes against the road transports have increased in both number and size in recent years. According to recent statistics the stolen cargo amount to about 8 B€ in EU every year. As the truck and trailer are much easier targets compared to for example banks, thefts have transferred to the transport business. Economic gain from these activities is furthermore utilized in heavier organized criminal activities. With this in mind there is an urge for solutions making the transports more secure. The road transport is often divided into driver, vehicle and cargo and in order to make the transports more secure, all three parts have to be considered to minimize weak points.

This project has been carried out by Volvo Technology, Lindholmen Science Park and Datachassi at Security Arena Lindholmen, Sweden, where close collaboration between industry, society and academia, so called triple-helix, is fundamental. The early involvement of end-users and different stakeholders has enabled research and development in an innovative living-lab environment.

A field pilot has been developed for proof-of-concept of developed security services and tested at a Volvo test track. The platform in the project is a wireless sensor network that enables flexible connection of different types of sensors. In order to cover the above-mentioned parts of the road transport, the following services have been developed – wireless panic button (driver), remote immobilization (vehicle) and wireless electronic seal (cargo). These components are certainly not sufficient to secure the transport, but enough to initiate discussions around legal constraints and responsibilities in the supply chain. During 2010 the project will take the next step towards providing a complete set of services to enable a secure road transport and investigate the requirements put on securing information sharing.

P 2

PEER-TO-PEER-INTEGRATION OF SECURITY-ORIENTED IT-SYSTEMS IN PUBLIC URBAN TRANSPORT

W. Engelbach, S. Frings, H. Roßnagel, and J. Zibuschka

Competence Team Informationsmanagement, Universität Stuttgart IAT, Fraunhofer IAO,
Nobelstr. 12, 70569 Stuttgart

wolf.engelbach@iao.fraunhofer.de

Large events such as city festivals or sport championships pose stress on the institutions that care about transport and security in the urban environment. They already use different IT-Systems to improve the preparedness and response capacities in case of unexpected incidents such as terroristic attacks or heavy weather. A detailed analysis of the stakeholders and their situation in Cologne within the BMBF-supported project VERSIERT (www.versiert.info) elaborated three core conditions for a supportive IT-infrastructure:

- 1) The IT-infrastructure needs to enable the cooperation of many institutions and persons that are even changing for each event.
- 2) The overall solution must offer significant improvements also for the everyday business of large events and urban activities without incidents.
- 3) The individual IT-systems have to be flexibly combinable in order to manage increasingly complex challenges in a cooperative manner.

On this basis, we developed an integration concept without a central middleware that allows peer-to-peer cooperation with stepwise extendable IT-interfaces. The starting points are business demands of the involved stakeholders and interests for cooperation and information. Existing standards are used to simplify data exchange and political communication issues. Relevant for the acceptance has been a common role model within the event and incident management as well as for the operation of the ITsystems. Starting with solutions for specific but representative events, incident scenarios and locations reduced complexity. This has been elaborated and evaluated together with City of Cologne, Kölner Verkehrsbetriebe (KVB) and project coordinator Nahverkehr Rheinland (NVR).

The approach is implemented and has been tested in July 2010 for the annual city firework „Kölner Lichter“, among others for the IT-components information and cooperation portal, video analytics, real-time-securityquestionnaires, agent based simulation and mobile services for staff and participants. Also a multi-touch collaboration environment exists that supports event managers, traffic operators and security organisations.

POSTERS

P 5 A RELIABLE, FAST AND EASY-TO-USE SIMULATION METHOD FOR BLAST PROPAGATION IN URBAN SCENARIOS

A. Klomfass and O. Herzog

Fraunhofer EMI, Eckerstr. 4, 79104 Freiburg, Germany

klomfass@emi.fhg.de

The assessment of blast effects on people and infrastructure is demanded in several occasions. One example is the investigation of potential hazards and resilience in an early design phase of a new infrastructure. The determination of evacuation requirements for the planning of bomb disposals is another example.

Most of the existing simulation tools for such purposes are based on simplified calculation models, which limit either their accuracy or the spectrum of permitted applications. As an alternative general-purpose hydrocodes may be used which offer both accuracy and broad applicability. They are however difficult to use and require long set-up and calculation times. Given this situation we have developed a fast and accurate approach specifically for the simulation of blast propagation in urban scenarios. This method allows the simulation of blast propagation both outside and inside of one or more buildings and can be easily coupled to damage models for the assessment of blast effects. An automated simulation setup makes the software easy to use.

The method is based on the fluid dynamic conservation laws, which are solved on a Cartesian grid with an explicit finite volume scheme and a particularly designed automatic mesh refinement strategy. The method includes a state-of-the art detonation model contained in a pre-processor. The automatic set-up determines suitable computational domains and grid resolutions based on the given scenario geometries.

The paper gives a survey about the fundamentals and specific aspects of the method, its present state of development and examples of applications including validation by experimental data for various test cases.

P 6 TUNNEL STABILITY AFTER EXPLOSIONS FROM THE VIEWPOINT OF DYNAMIC SOIL-STRUCTURE INTERACTION

P. Kudella, V. Osinov, and T. Triantafyllidis

Karlsruher Institut für Technologie (KIT), Institut für Bodenmechanik und Felsmechanik,
Postfach 6980, 76128 Karlsruhe, Germany

peter.kudella@kit.edu

Explosions due to terrorist attacks in suburban road or railway tunnels, where large explosive loads may be carried in trucks, are a nightmare scenario. Such tunnels are often shallow, embedded in soil, under groundwater and made of reinforced concrete tubbings. After an explosion the main focus is paid to the damage of the concrete lining. Less attention, if any, is paid to changes in the soil behind when struck by an explosion wave. Tunnels are always supported by a joint resistance of structural parts and surrounding soil. For shallow tunnels, the lining acts as a sprocket chain supported by subground reaction. Tubbings are designed to withstand sectional forces resulting from simplified assumptions for the soil-structure-interaction.

Considering the soil as a three-phase medium, a one-dimensional wave front due to a given explosion pressure in the tunnel was examined. Due to nonlinear soil behaviour, the elastic pressure wave entering the soil transforms into a shock wave. Deformations within the next milliseconds change the soil state depending on its density and degree of saturation. With a few volume percent of air trapped in the soil, a higher residual pore water overpressure develops compared to full saturation, resulting in a partial or even complete loss of residual shear strength.

As a consequence, the soil's ability to support the (eventually damaged) lining may be reduced, after the wavefront has passed. The loads on the lining and its distribution have changed as well which can lead to an upward movement of the tunnel. The following pore water pressure dissipation may take hours to weeks until a new equilibrium state is reached. This will be further examined employing finite element models. In order to evaluate the danger of structural collapse or water inrush during rescue activities, the checking of all transient states is required.

POSTERS

P 7 **ADVANCES ON CHEMICAL GAS SENSORS FOR DETECTION OF EXPLOSIVES: FROM CONCEPTS OF EMPLOYMENT TO SENSOR-ARRAY SYSTEMS**

P. Montméat, C. Barthet, P. Prené

CEA, DAM, Le Ripault, 37260 Monts, France

philippe.prene@cea.fr

With the increased needs of explosives detection for various applications such as safety or military and civilian security or surveillance for mass-transport, the development of efficient devices has become an urgent worldwide necessity. The classical laboratory techniques (GPC, HPLC, Mass Spectrometry, FTIR, NMR,...) present high sensitivities (in order of ppb to ppt), but their uses are limited due to their high cost, their poor mobility and the fact that only experts are able to make them function. For 10 years, many studies have been performed on the detection of explosives compounds using chemical gas sensors as highly sensitive and selective detectors because of their capability to be low-cost portable systems. We will begin our presentation on the potential concepts of employment the chemical gas sensors could be used for detection of explosives. Secondly, we will show the recent advances on chemical gas sensors based on various transducers such as fluorescence and Surface Acoustic Wave we are developing, in term of sensibility, selectivity, robustness with environmental conditions, durability and reliability for detection of explosives. Finally, we will present the performances of a sensors-array system which allows to give a first linked-threat alarm in a few seconds and to identify the chemical nature of explosive after one minute of detection.

P 8

**RAPID FIELD TESTING OF BIOLOGICAL THREATS
WITH LAB-ON-A-CHIP SYSTEMS**

T. van Oordt¹, D. Mark¹, M. Focke², S. Lutz¹, F. von Stetten^{1,2}, and R. Zengerle^{1,2}

¹ HSG-IMIT - Institut für Mikro- und Informationstechnik der Hahn-Schickard-Gesellschaft e.V., Wilhelm-Schickard-Strasse 10, 78052 Villingen-Schwenningen, Germany; ² Laboratory for MEMS Applications, Department of Microsystems Engineering (IMTEK), University of Freiburg, Georges-Koehler-Allee 106, 79110 Freiburg, Germany

thomas.van.oordt@hsg-imit.de

The world's increasing mobility, mass tourism but also possible terrorist activities increase the risk of a fast distribution of infections. Today's procedures for pathogen detection involve complex, stationary devices and may be too time consuming for a rapid and effective response. A robust, mobile field diagnostic system is required. A microfluidic system that includes a mobile centrifugal platform and a disposable cartridge enabling complex biochemical analysis is currently being developed within the BMBF funded project SONDE.

In case of a pathogenic threat fast and automated field test systems are required. This need is not met by the state-of-the-art diagnostic procedures which rely on either labour-intensive and slow laboratory tests performed by skilled specialists or highly integrated but large and immobile pipetting robots.

A mobile and fully integrated diagnostic system for the detection of B-agents such as anthrax and *Y. pestis* is about to be developed and field-tested within the project SONDE. Centrepiece of the detection system is a disposable test carrier in which reagents are pre-stored and fluidic structures are integrated to perform all required operations.

Preliminary work includes the introduction of a novel foil-based fabrication method for test carriers as well as the successful implementation of analytical assays including DNA extraction from whole blood and real time PCR. The foil based approach reveals unique features like low thermal resistance for efficient thermocycling and low material consumption which is attractive for cost-efficient large-scale production of disposables.

The SONDE consortium combines its competences in microbiology and microsystem technology to integrate diagnostic protocols for the automated detection of B-threats. The novel foil based fabrication technology enables both, the fast prototyping and implementation of individual analytical assays as well as the potential for a high throughput production of the disposable test carriers.

POSTERS

P 9

LIQUID SCREENING BY HIGH- T_c JOSEPHSON TECHNOLOGY

Y. Divin¹, M. Lyatti^{1,2}, U. Poppe¹, and K. Urban¹

¹ Forschungszentrum Juelich GmbH, 52425 Juelich, Germany; ² Kotel'nikov Institute of Radio Engineering and Electronics of RAS, Moscow 125009, Russia

y.divin@fz-juelich.de

One of future checkpoint screening techniques will be related with non-invasive, fast and reliable detection of liquids. To distinguish between benign and threat liquids, we have suggested an electromagnetic-wave concept based on our Hilbert spectroscopy and high- T_c Josephson detectors [1]. This spectroscopy covers a frequency range of main dispersions of liquids, from a few GHz to a few THz, and thus significantly enhances reliability of identification. The high- T_c detectors, due to a power dynamic range of more than five orders, guarantee fast operation of the identifier [1]. Several demonstration set-ups of liquid identifiers, consisting of Hilbert spectrometers, integrated in Stirling coolers, and polychromatic radiation sources, have been developed and characterized. Reflection polychromatic spectra of various liquids in plastic containers have been measured at the spectral range of 15 - 400 GHz with total scanning time down to 0.2 second [2]. Examples of identification of liquids, both benign and threat, by developed demonstration set-ups will be presented.

[1] Y. Divin, U. Poppe, V. Gubankov, K. Urban. *IEEE Sensors J.*, v.8, pp.750-757 (2008) (invited).

[2] M. Lyatti, Y. Divin, U. Poppe, K. Urban. *Supercond. Sci. Technol.*, v.22, 114005 (2009).

P 10

CONCEPT OF A COOPERATION PROJECT FOR THE DEVELOPMENT OF A CHIP-BASED ON-SITE DETECTION SYSTEM FOR ANIMAL DISEASES

C. Seyboldt¹, M. Heller¹, M. Lange¹, C. Schnee¹, E. Schubert¹, B. Haas², K. Brehm², T. Selhorst³, H. Lenz³, R. Möller⁴, A. Brinker⁴, B. Seise⁴, J. Weber⁵, M. Koge⁵, T. Hillebrand⁵, and F. Pauly⁶

¹ Friedrich-Loeffler-Institute, Federal Research Institute for Animal Health, Institute of Bacterial Infections and Zoonoses, Jena; ² Institute of Diagnostic Virology, Insel Riems; ³ Institute of Epidemiology, Wusterhausen; ⁴ Friedrich Schiller University of Jena, Jenaer BioChip Initiative; ⁵ Analytik Jena AG, Jena; ⁶ Tecart GmbH, Erfurt

christian.seyboldt@fli.bund.de

Agriculture forms part of critical supply-related infrastructures which are particularly affected by biological hazards. Animal diseases can have severe economic consequences and may considerably upset the general public. Efficient protective and remedial measures as well as outbreak control depend on the rapid identification of potential biological agents. However, the detection of pathogens on the spot is only possible to a limited extent so far.

For this reason, a new system is to be developed which enables the on-site detection of different animal diseases e.g. FMD, blackleg and CBPP. The approach includes three main modules: The first module is the on-site sample processing. The second comprises a PCR chip which allows the highly sensitive amplification of target DNA without requiring much space or energy. The third module is a DNA chip which enables the highly specific identification and differentiation of pathogens. Such an innovative miniaturized lab-on-a-chip system will ensure a quick and flexible response to potential hazards caused by epizootic pathogens. To make the diagnostic data available to an immediate analysis and crisis management a web based online data management tool is developed. Accompanying network analysis of trade connections between farms is performed to develop models for the possible spread of pathogenic agents. The Project is funded by the Federal Ministry of Education and Research within the programme „Research for Civil Security“, part of the High-Tech Strategy of the Federal Government of Germany.

POSTERS

P 11

A NEW APPROACH FOR DOSE ASSESSMENT IN URBAN ENVIRONMENTS AFTER NUCLEAR EMERGENCIES AND RADIOLOGICAL TERRORISM

J. C. Kaiser and C. Woda

Helmholtz Center Munich, German Research Center for Environmental Health, Institute of Radiation Protection, Ingolstädter Landstr. 1, 85764 Oberschleissheim

clemens.woda@helmholtz-muenchen.de

In the event of a nuclear emergency or a terrorist attack with radiological material in an urban environment a reliable overview on the radioactive contamination is crucial for decision making. To assess the radiological situation, we use here measurements of the cumulative dose. These are derived from passive luminescent BeO detectors, which are placed at pre-selected positions of high importance (i.e. public squares). BeO is characterized by a low minimum detectable dose (10 μ Gy or less), linearity of dose response up to 10 Gy, long term signal stability and, in combination with a suitable packaging, an essential flat photon energy response. The dose measured by the dosimeter however strongly depends on the detector environment. To account for this dependence, each dose is multiplied by a location factor, which quantifies the deviation of the recorded dose from the hypothetical dose obtained over a reference surface of an infinitely extended lawn. Furthermore, the data originate from geo-referenced points but do not provide full spatial information. We present an approach to produce maps of reference gamma dose rate, air kerma or surface contamination in urban areas from localised dose measurements. For pre-processing of the measurements and for geo-statistical interpolation, the Inhabited Areas Monitoring Module (IAMM) is applied. IAMM is an operational module of the European decision support systems RODOS and ARGOS. Our approach is demonstrated in a hypothetical scenario based on the explosion of a radioactive dispersion device.

Keywords

nuclear emergencies in urban environments, radiological terrorism, mapping of the radioactive contamination, dose assessment, luminescence dosimetry.

P 12

HIDDEN HAZARDS – APPROPRIATE SCANNING REMAINS A CHALLENGE

K. Osterloh, N. Wrobel, U. Zscherpel, and U. Ewert

BAM Federal Institute for Materials Research and Testing, Berlin

kurt.osterloh@bam.de

Hazardous materials are encountered in various forms and conditions, as highly energetic, toxic, flammable, caustic, corrosive or even contagious substances, as solids, granules, powders, plasticines, gels, liquids, fumes, dusts or gasses. They may be sophisticatedly wrapped, concealed, stowed deeply into a container, disguised or even carried by a person underneath the clothing. All these different occurrences and appearances make a scanning appropriate for detecting a hidden hazard anything else than trivial. An immediate threat emerges from such materials in conjunction with a fuse. This makes radiological scanning technologies to serve as a most effective preventive measure as to detect the full hazard consisting of substances and a device. This means a double challenge, to identify the hazardous material as far as possible and to spot any appliance operating as a fuse. An update will be given on current approaches and some recent developments in this area. This includes supporting activities such as image processing and evaluation.

It is quite evident that a single technology cannot be applied in any situation. Some may be even inappropriate; others do not cope with the size and restricted mobility of the specimen to be interrogated. Cargo may be inspected with ionising radiation, but not necessarily human. A suitcase can be easily brought to a dedicated inspection line, but the situation with containers is different. As a consequence, scanning requirements seem to be nearly as diversified as the threats to be detected themselves. The question remains not only how to identify the appropriate means but also to evaluate the versatility of a given technology. A link counting matrix is proposed to provide impartial scaling parameters that may contribute either to support pursuing certain technologies or to suggest reconsideration. Versatile solutions may not only be economical but also may improve the efficiency of providing security.

POSTERS

P 13

EXAKT – JOINT BMBF RESEARCH PROJECT: PROJECT STATUS UPDATE ON NEAR REAL-TIME TRACE ANALYSIS OF AIRBORNE CHEMICAL WARFARE AGENTS AND EXPLOSIVES

G. Bunte¹, J. Hürttlen¹, J. Ringer², F. Rietz², P. Boeker³, J. Leppert³, T. Etterer⁴, and G. Horner⁵

¹ Fraunhofer Institut für Chemische Technologie, Joseph-von-Fraunhoferstrasse 7, 76327 Pfinztal-Berghausen; ² Wehrwissenschaftl. Institut für Schutztechnologien - ABC-Schutz, Postfach 11 42, 29623 Munster; ³ Universität Bonn, IfL-Abt.Sensorik, Nussallee 5, 53115 Bonn; ⁴ SECURETEC Detektionssysteme AG, Eugen-Sänger-Ring 1, 85649 Brunnthal;

⁵ five technologies GmbH, Frauenstr. 22, 80469 München

gudrun.bunte@ict.fraunhofer.de

The actual presentation will address the concept and objectives of the joint project EXAKT, which is financed by the German BMBF under the security related CBRNE research programme. EXAKT comprises a new concept in on-line, near real time (NRT) analysis of trace level (airborne) chemical warfare agents and explosives using a continuous sampling Thermal Desorption (TD) system and a new bench top Time of Flight (TOF) mass spectrometer. TD adsorption is achieved using standard wide range and novel selective adsorption materials. The selective adsorption materials are newly developed molecularly imprinted polymers (MIPs), which are synthesized, tested and evaluated for the selective adsorption of explosives and direct desorption into the TOF-MS. Preliminary results will be presented.

P 14

LASER-INDUCED BREAKDOWN SPECTROSCOPY AT THE DLR LASER TEST RANGE

C. Pargmann, F. Duschek, and J. Handke

DLR (German Aerospace Center), Institute of Technical Physics, Im Langen Grund,
74239 Hardthausen
carsten.pargmann@dlr.de

A basic set-up for laser-induced breakdown spectroscopy (LIBS) at the DLR laser test range in Lampoldshausen and first LIBS spectra of selected samples are presented. The test range allows measurements in free atmosphere under daylight conditions at distances up to 130 m.

With the help of a Cassegrain type telescope a pulsed Nd:YAG laser has been used to produce plasma on different samples at distances exceeding 50 m. The scattered light of the plasma was collected by a Newtonian telescope and analysed and detected by a gated spectrometer with an attached CCD camera.

The plasma generating laser yields a maximum pulse energy of 800 mJ at a wavelength of 1064 nm and a pulse width of 8 ns. It also has the option to extract the second and third harmonics.

LIBS spectra from 10 nm layers of gold on a silicon wafer, as well as from black powder and one of its main components, potassium nitrate, were recorded. The spectra are compared with respect to the laser wavelength, pulse energy, and energy density on the target.

POSTERS

P 15

PHOTONIC SENSORS FOR EXPLOSIVE DETECTION

W. Schade^{1,2}, P. Lützow¹, R. Orghici¹, M. Mordmüller², M. Angelmahr¹, and S. R. Waldvogel³

¹ Fraunhofer-Institut für Nachrichtentechnik, Heinrich-Hertz-Institut, Berlin; ² Technische Universität Clausthal, LaserAnwendungsCentrum, Energie Campus, Am Stollen 19, 38640 Goslar;

³ Universität Bonn, Kekule-Institut Organische Chemie und Biochemie

w.schade@pe.tu-clausthal.de

The detection of improvised explosive devices (IEDs) in conflict areas as well as the threat posed on common welfare by terrorist attempts increasingly became focal points of interest in recent years. Novel photonic sensor devices applying evanescent field spectroscopy and nano-dimensioned waveguides in combination with miniaturized lasers such as microchip- and quantum cascade lasers reveal entirely new possibilities for insitu and real-time diagnostics. In this context evanescent-field laser spectroscopy is a very promising method for extreme sensitive detection of low-vapor pressure explosives, e.g. TNT (Trinitrotoluene). TNT is highly toxic and carcinogenic and the detection of this explosive is very difficult due to its extreme low vapour pressure, resulting in concentrations down to the ppt level.

A new concept is developed which allows the identification of TNT by using microring resonators coated with a specially engineered receptor film (triphenylene-based ketals). This opens new possibilities for miniaturized and high sensitive photonic sensor devices, e.g for application on robotic platforms. A second photonic sensor device is developed applying photoacoustic spectroscopy. Instead of a conventional photoacoustic cell just a simple quartz tuning fork is used as sensor element. Miniaturized laser technology and fibre optics enable engineering a smart handheld sensor, e.g. for the detection of TATP (tri-acetone tri-peroxide). A third approach is pulsed laser fragmentation (PLF) in combination with high-resolution mid-infrared laser absorption spectroscopy which offers new possibilities for sensitive and selective stand-off analysis of surface contaminations under real-time operation conditions. The detection of NO_x production rates emitted from contaminated surfaces after interaction with an infrared PLF laser beam allows analysis of different surface contaminations, e.g. distinguishing between energetic and non-energetic materials but also between molecules with similar atomic composition. The concepts and miniaturization of such technologies are discussed.

P 16

CONTACTLESS AND DIRECT MS-TECHNIQUES FOR THE SURVEILLANCE OF CLANDESTINE PRODUCTION FACILITIES OF SYNTHETIC DRUGS AND IMPROVISED EXPLOSIVES

J. Rittgen^{1,2}, M. Pütz¹, T. Rößler¹, R. Schulte-Ladbeck¹, and R. Zimmermann²

¹ BKA – Bundeskriminalamt, Forensic Science Institute, Wiesbaden; ² University of Rostock, Rostock

michael.puetz@bka.bund.de

Illicit amphetamine derivatives are clandestinely produced in large-scale facilities (e.g. MDMA for Ecstasy tablets) or in “kitchen laboratories” (typical for methamphetamine). The latter small-scale production is also observed for home-made explosives, used in IED’s. For action forces who firstly have to observe and then to safeguard such labs it is very important to know which kind of chemical reactions are arranged in the concerning objects. The fast, mobile and at best contactless analysis of hazardous materials at trace levels is able to improve the danger estimation to protect action forces and the population.

Solid phase microextraction in combination with gas chromatography-mass spectrometry (SPME-GC/MS) is a promising method for air sampling and subsequent analysis of drugs, their precursors, process chemicals or explosives. In contrast to conventional extraction techniques the integration of sampling, extraction (including matrix removal), reconcentration and sample introduction within only one step is the major advantage of SPME. Vapour phase sampling with SPME-fibres is fast, contactless and not limited to any specified environment. Desorption electrospray ionization mass spectrometry (DESI-MS) is well suited for the direct mass spectrometric examination of solid materials. It provides near time detection and identification of synthetic drugs and explosives on contaminated surfaces and wipe samples.

In our work we performed a small-scale amphetamine production via the Leuckart synthesis route with seized chemicals under controlled conditions. We successfully identified amphetamine, its precursors, process chemicals and by-products in the environmental air of the laboratory by SPME-GC/MS and volatile components by a mobile infrared spectrometer. It was possible to reconstruct details of the arranged synthesis by analysing contaminated laboratory equipment (e.g. magnetic stir bars, glass rods) and laboratory waste (filter paper, gloves) with DESI-MS. Additionally we monitored the synthesis of selected improvised explosives (TATP, HMTD) with the named techniques.

POSTERS

P 17

AN INTEGRATED APPROACH TO DEAL WITH THE CBRNE THREAT WITHIN THE EU – DECOTESSC1

M. S. Nieuwenhuizen and M. van den Brink

TNO Defence Security and Safety, CBRN Protection, PO Box 45, 2280 AA Rijswijk

maarten.nieuwenhuizen@tno.nl

Within the 7th Framework Programme Security the EU is heading for a demonstration project on CBRNE counterterrorism. The scope of this project will be the demonstration of a consistent portfolio of countermeasures for CBRNE along the chain from prevention to response and recovery. The call for this demonstration project will be issued during Summer 2011.

The project DECOTESSC1, led by TNO, is tasked to develop a roadmap for this demonstration project and beyond.

The basic idea is an analysis and prioritization of the gaps between the current situation and the ideal situation of CBRNE system-of-systems counterterrorism. To achieve this a thorough understanding of the system-of-systems' structure will be developed, the requirements for an ideal system will be proposed as well as a description of the current state-of-the art. A gap analysis will reveal the differences between the current situation and the ideal situation. Finally, in order to fill the gaps a strategic roadmap will be developed. The strategic roadmap will address the full concept of an EU counterterrorism system-of-systems against CBRNE and outlines all the necessary missions, tasks, capabilities, systems, technologies, etc. to be considered. As a result the focus will be on the enhancement of the integrated operational competences.

In addition, to achieve all this, the DECOTESSC1 project will, on top of the efforts of the Core Group, consider the needs of the various stakeholders by direct interaction. This will be achieved by involving the stakeholders (Expert Group) continuously by organizing workshops at relevant moments during the work of DECOTESSC1, by organizing a mid-term stakeholders meeting and well as a final symposium. All interactions above will not only provide input for DECOTESSC1's work but also provide dissemination of its findings throughout the EU community and raise awareness for this very important subject area in the mean time.

P 18

IMMEDIATE IDENTIFICATION OF SINGLE BACTERIA – NOVEL METHODS AND INSTRUMENTATION

O. K. Valet and M. Lankers

rap.ID Particle Systems, Köpenicker Str. 325, 12555 Berlin

oliver.valet@rap-id.com

Microorganisms, such as bacteria, must be identified quickly in order to minimize possible health risks. We will discuss the results taken from several investigations in which a micro-Raman instrument combined with modern software classification algorithms performed analysis on single particles. The combination of both technologies provides quick, reliable, and non-destructive identification methods of single bacteria.

This revolutionary device identifies single particle microbial strains from micro-contamination in just seconds. The combined analysis technique enables one to determine and identify the viability of a single microorganism. Quick germ detection facilitates the user to respond with timely and pertinent countermeasures in just minutes.

This custom approach could be applicable, for example, in antibiotics which fight against sepsis and other kinds of diseases.

Conventional methods for identifying bacteria are much slower and can take days or weeks. More modern methods still take days and require a particular search strategy in order to identify microorganisms. Quicker methods such as PCR are able to obtain DNA fingerprints of bacteria as well as make special mixtures of reactants which are optimized for a particular type of bacteria

All the painstaking steps of conventional methods such as special isolation material, staining processes and integrated fluorescence microscopy have been eliminated so that every user can quickly determine the entire viable bacteria count and the hazardous potential of such germs. The device can identify particles at a speed of 4 particles per minute and accurately determine pathogenic bacterial contamination in even troublesome pathogenic germs.

POSTERS

P 19

NANOSIZE MOX THIN FILM GAS-SENSITIVE ELEMENTS FOR DETECTION OF EXPLOSIVE VAPOURS

O. Tolbanov¹, O. Anisimov¹, G. Sakovich², and A. Vorozhtsov²

¹ Tomsk State University, Tomsk, Russia; ² Institute for Problems of Chemical and Energetic Technologies SB RAS, Biysk, Russia

abv@mail.tomsknet.ru

Concerns associated with the potential for future terrorist attacks have prompted investigations into effective methods for sensitively detecting a wide range of explosive vapours.

Due to the many advantages associated with nanosize thin films gas-sensitive elements, manufactured by microelectronic technology, including portability, ease of integration and low cost, high sensitivity and rapid response time, there has been significant interest in research such MOX (metal oxide) gas sensors and the development of portable devices for explosive detections.

In present work, metal oxide thin film technology is used to engineer a small, sensitive and selective sensor elements in relation to trace amounts of explosive vapours.

The nanosize (grain size is 15÷20 nm) WO_3 and SnO_2 thin films were deposited on sapphire substrates by reactively sputtering a pure tungsten or tin targets in argon-oxygen atmosphere using an RF magnetron sputtering system. The sensitivity of the thin films to nitrogen dioxide and nitroaromatics vapours, such as TNT explosives, was studied at different temperatures: steady mode – in range 170÷350 °C, pulsing mode – in range 100÷450 °C.

We concluded that the best stable and sensitive sensors are based on WO_3 and SnO_2 (Au catalyzed). Furthermore, the low-concentration sensitivity level increased for detectable gases up to 200 ppt NO_2 . The sensors characteristics analyzed include the response and recovery times, dynamic range, sensitivity, repeatability and selectivity.

P 20

THE PROJECT SAFE INSIDE – TRACE DETECTION OF SECURITY RELEVANT SUBSTANCES BY SINGLE PHOTON IONIZATION ION TRAP MASS SPECTROMETRY (SPI-ITMS)

R. H. Schultze¹, R. Laudien¹, N. Rüssmeier¹, J. Wieser¹, A. Walte², M. Pütz³, J. Rittgen³, R. Schulte-Ladbeck³, E. Schramm⁴, J. Hölzer⁴, S. Schindler⁵, G. Törber⁵, A. McNeish⁶, H. Ries⁶, P. Schall⁶, T. Dantl⁷, T. Heindl⁷, A. Ulrich⁷, S. Ehlert⁸, M. Sklorz⁸, and R. Zimmermann^{4,8}

¹ Optimare GmbH, Wilhelmshaven, Germany; ² AIRSENSE Analytics GmbH, Schwerin, Germany;

³ Bundeskriminalamt, Wiesbaden, Germany; ⁴ Helmholtz Zentrum München, Germany;

⁵ Schindler Endoskopie Technologie GmbH, Gutach, Germany; ⁶ Smiths Group; ⁷ Technische Universität München; ⁸ University of Rostock

rainer.schultze@optimare.de

Threats from terrorism, organized crime or technical disasters lead to a persistently tense security situation worldwide. A fast, selective and sensitive on-site detection of hazardous substances with minimized impact on the supervised activities is required. Within the collaborative research project SAFE-Inside, an analytical system for a fast detection of security relevant substances is developed, based on an ion trap mass spectrometer (ITMS) with single photon ionization (SPI).

For SPI, an electron beam pumped excimer lamp (E-Lux) is used, providing emission wavelengths in the range from 116 nm to 176 nm depending on the employed gas. With this source, a soft ionisation with minimized fragmentation of security relevant organic substances is possible. Typical carrier gas components like N₂, O₂, H₂O, CO₂ are not ionized. Characteristic ions (often molecular ions) are generated and isolated inside the ion trap. The subsequent collision induced dissociation (CID) in MS/MS-experiments allows an unambiguous analyte identification.

Time consuming separation or sample preparation steps are not required. The analytical technique allows a design as a mobile system suited for on-site operations.

POSTERS

A flexible employment of the SPI-MS system is aspired. An endoscopic sampling system was developed, allowing the minimally invasive investigation of e.g. containers or luggage. The endoscope consists of a camera for a visual surveillance. Via a fibre optics, a laser beam is used for the desorption of low volatile analytes. Besides the endoscopic sampling, the on side investigation of substances, adsorbed on wipe pads or SPME fibres and introduced into the ITMS via a thermal desorption system, is possible.

Present activities are focused on an increase of light intensity, the optimization of the MS detector and the implementation of an enrichment unit in order to improve the sensitivity of the entire system. Operation conditions are supervised and additional analyte information are obtained by the implementation of a FTIR-detector.

P 21

CHORUS - CAR HORNS USED AS SIRENS

G. Huppertz

Fraunhofer INT, Appelsgarten 2, 53879 Euskirchen

guido.huppertz@int.fraunhofer.de

In Germany, an extensive siren system was used in the past to warn the population against disasters: in case of natural hazards, industrial accidents or other disaster scenarios, situation centres could trigger the loud siren alarm. Detailed information about the danger situation was provided by radio and television. However, after the end of the Cold War, most sirens were dismantled in the mid-nineties. Today there exists a satellite-based warning system SatWaS, which distributes warning messages via radio and television. But if TV and radio are off, the warning goes unheard.

A reinstallation of the former siren system would cost several hundred million Euros plus additional millions per year for maintenance. This is why German federal and state governments since years are searching for alternative solutions. Cell-broadcast systems can send mass SMS messages to mobile phones. Smoke detectors, radio-controlled clocks and weather stations with radio receiver can also trigger alarm. Despite the high distribution rate of some of these devices, it cannot be ensured that a warning reaches the entire population. Only individual persons or households can be warned, and only if the devices are on standby 24/7/365.

The Fraunhofer INT develops a new warning system based on the use of car horns. In case of disaster the situation centres can define a region inside which every parked car will start to honk its horn corresponding to a predefined warning signal. To activate the cars they have to be equipped with a radio receiver, based on e.g. RDS, eWarn, GSM or different technology. The system will exploit the data of a GPS receiver coming with the introduction of the telematics platform eCall. Besides sirens this system is the only one based on broadcast signals. It is independent from power lines and allows the free definition of alarm zones.

POSTERS

P 22

PROVIDING DYNAMIC ESCAPE ROUTES TO SUPPORT SELF RESCUE IN SUBWAY SYSTEMS

M. Plaß and R. Koch

University Paderborn, Fakultät Maschinenbau / C.I.K.

m.plass@uni-paderborn.de

Subways are an indispensable part of mass transportation in modern cities. Every day millions of people use them to reach their destination quickly and inexpensively. A large number of passengers are continuously staying in trains and underground stations. In case of a fire, a lot of people will be affected and the peoples self-rescue has the highest priority. But various factors make it difficult to take action. Few possible escape routes, the lack of clarity and familiarity with the complex infrastructure causes disorientation and stress to those affected. Possible obstructions by smoke increase the stress and block the view to evacuation plans and signage of escape routes. To support the self-rescue it makes sense to point the passengers individually in the right direction depending on their current location, and thus facilitate the appropriate action. Doing that technical challenges arise in the area of detection / sensor technology, calculation of the spread, escape route calculation based on it, as well as individual transportation of the information to the passengers. Our approach is presented and technical limitations are discussed.

P 23

EARLY IDENTIFICATION OF OCCURRING INCIDENTS AT BIG EVENTS AND EVACUATION MODELLING

A. Blanc¹, L. Deimling¹, N. Eisenreich¹, R. Könnecke², and D. Oberhagemann³

¹ Fraunhofer ICT, 76327 Pfinztal; ² I.S.T GmbH, 60325 Frankfurt; ³ vfdb e.V., 48341 Altenberge
ne@ict.fraunhofer.de

The effective protection and rescue of people attending big events requires early recognition of a developing incident, analysis of its origin and its expected impacts, as well as the initiation of adequate counter measures. Such big events include cultural and sports activities, public viewing or crowded infrastructures like metro, railway or bus stations. The combination of localisation, measured densities and movements of the crowds with the existing building layouts and the emergency routes can enable an optimal response and evacuation if needed.

The real time incident localisation and the record of crowd densities and movements resolved in time and position use various techniques of image processing like auto and cross correlation methods. The temporal changes in densities and paths of the crowd are interpreted by physical models of the behaviour of individual persons and anonymous crowds to predict the progress of the incident. This information might allow the most effective reactions and activities of the first responders like fire brigades, police and paramedics. In the future, additional innovative devices or measures might be used for guiding an evacuation by visual and acoustic signalling or even by flexible, rapidly deployed physical barriers for route marking which takes into account the actual situation.

The methods to be applied are tested in some big events like a football match and a public event of temporally varying crowd densities. The analysis of the results shows the advantages for lay-outs of buildings and for involved first responders who currently rely mainly on their intuitive comprehension and experience.

POSTERS

P 24

HERMES – EVACUATION ASSISTANT FOR ARENAS

H. Klüpfel¹, A. Seyfried², S. Holl², M. Boltes², M. Chraibi², U. Kemloh², A. Portz², J. Liddle², T. Rupprecht³, A. Winkens³, W. Klingsch³, C. Eilhardt⁴, S. Nowak⁴, A. Schadschneider⁴, T. Kretz⁵, and M. Krabbe⁶

¹ TraffGo HT GmbH, Bismarckstraße 142a, 47057 Duisburg; ² Forschungszentrum Jülich GmbH, Wilhelm-Johnen-Straße, 52525 Jülich; ³ Bergische Universität Wuppertal, Pauluskirchstraße 11, 42285 Wuppertal; ⁴ Universität zu Köln, Inst. für Theor. Physik, Zülpicher Straße 77, 50937 Köln; ⁵ PTV Planung Transport Verkehr AG, Stumpfstraße 1, 76131 Karlsruhe; ⁶ ESPRIT arena, Arena Straße 1, 40474 Düsseldorf

kluepfel@traffgo.ht

The Hermes project³ focuses on the improvement of safety at mass events. It is an evacuation assistant for security services in case of emergencies and fore-casts the emergency egress of large crowds in complex buildings. This requires realistic and faster than real-time simulation of pedestrian dynamics.

Multifunctional arenas and large-scale public events present new challenges for the quality of security concepts. A safe egress is in general based on prescriptive regulations specifying minimal width and maximal length of escape routes. If part of an escape route is lost due to fire or other risks, dangerously high crowd densities and bottlenecks can occur. To prevent such critical situations crowd management is necessary based on accurate and up-to-date information about the current status. Usually the decision makers do not know the number of people in the danger zone and are confronted with uncertainties: where are dangerous congestions causing long waiting times? How does the loss of escape routes influence the evacuation time?

The evacuation assistant will close this gap. It helps decision makers to assess the actual danger, decide on a successful evacuation strategy, and optimally employ the security staff. The ESPRIT arena in Düsseldorf (Germany) provides a venue for testing. It is a multifunctional arena with a capacity of 60,000. A test system of the assistant will be installed in 2011.

More details: <http://www.fz-juelich.de/jsc/appliedmath/ped/projects/hermes>.

³ *Funded by the German Federal Ministry of Education and Research, BMBF, under grants 13N9952 – 13N9960*

P 25

INTEGRATED CRISIS MANAGEMENT FOR DISASTER RELIEF – COMMUNICATIONS, NAVIGATION, GEO INFORMATION –

S. Baumann¹, T. Sichert¹, and M. Berthold²

¹ IABG mbH, Ottobrunn; ² THW Ortsverband München-Mitte

baumanns@iabg.de

Nowadays various crisis situations occur almost every day all over the world. All types of crisis situations like earth quakes, tsunamis, floodings, forest-fires, terrorism etc. have a common challenge with respect to telecommunications the crisis reaction forces have to cope with: terrestrial communication infrastructures are not available, because they are either destroyed, overloaded, or the crisis takes place in a region without any communication capabilities.

This fact is extremely harmful, because effective crisis management requires reliable, robust and secure telecommunication capabilities for multiple purposes, like:

- operational command and control
- reconnaissance of the area of operation
- situation awareness
- emergency calls
- logistics
- search and rescue, etc.

This paper will outline the role of various user communities involved in crisis management scenarios (e.g. the German Federal Agency for Technical Relief (THW), police, fire-brigades, Red Cross), the telecommunication needs of these organisations and finally a summary of their current and future telecommunication demands. Based on these analyses a generic design for an “integrated crisis management system”, which consists of the following components, will be presented:

- Headquarters and data centre in the home country
- Regional headquarters in the deployment area
- Long distance communications using satellite links
- Autonomous Ad Hoc Networks
- Mobile networks like TETRA
- Various sensors and types of user terminals (stationary, nomadic, mobile) in the deployment area

POSTERS

The derived crisis management system will be used to support the disaster relief forces by various applications like:

- Voice and data communications
- Tracking of rescue forces
- Fleet management
- Emergency call for rescue forces
- GIS / Remote Sensing applications
- Dedicated operations applications
- Dedicated operation documentation, etc.

This generic system represents a “tool box”, providing standardised of-the-shelf products and services, which are pre-selected and suitable for the needs of the relevant user communities. It supports interfaces to external stakeholders and can be adopted by specific measures to a tailored solution for a specific crisis management application.

As an example a dedicated system set-up, adopted to support the rapid deployment task force of the THW has been developed and tested in a field-campaign in November 2009 in the South of Munich.

P 26

SOGRO – IS ELECTRONIC TRIAGING THE SOLUTION TO FAST DELIVERY OF PATIENT STATUS IN CASE OF AN MCI?

L. Latasch

Amt für Gesundheit, Frankfurt am Main

leo.latasch@stadt-frankfurt.de

Triaging outdoors at the scene of a mass casualty incident (MCI) still bears a lot of problems. One of these is that patient information, especially the status of the patient, actually arrives too late at the dispatch center and/or hospital. Time consuming is also the amount of data taken from the patient a question of necessity in case of an MCI. Our project called SOGRO (funded by the German federal ministry of education and research) tries to eliminate both of these problems by using modern technology (RFID and PDA) to transfer the first data immediately after the triage of the patient. Using a rugged PDA, only the status of triage, gender, adult or children and a photo of the face are transferred on to a coloured (red, yellow or green) wristband which holds an RFIF-chip, so that these data stay with the patient. At the same time these data are also send to a server, the user defines the location of this server. In case of medical treatment, infusions and/or medication and if needed also physiological data can be stored on the patient wristband. Once the patient is ready for transportation, the ID of the ambulance is stored and also transferred.

In several smaller exercises, we were able to demonstrate that basic triage (using the START-system) and done by paramedics, takes about 45 sec. per patient. Approximately 1 min later, triage data were already available on the server. This way, the status of the patient is available immediately after the triage. Only absolute necessary medical data is stored on the wristband. Patients can be tracked from the scene of the MCI until arriving in the hospital, so that no patient gets "lost". In an exercise which will be held this year (500 patients), also unmanned aerial vehicles will be used for aerial overview of the disaster area.

POSTERS

P 27

IDMA – HOW TO GAIN EFFICIENCY BY MEANS OF MOBILE INFORMATION TECHNOLOGY

C. Schmitt^{1,2}, D. Mosemann^{1,2}, and K. Fischbach²

¹ Ambient Innovation, Pohligstr. 1, 50969 Cologne; ² Dep. of Information Systems and Information Management, University of Cologne, Albertus-Magnus-Platz, Cologne, Germany

idma@ambient-innovation.com

The Department of Information Systems and Information Management at the University of Cologne has developed the mobile computing system IDMA that makes the victim identification process in disaster operations more accurate and efficient without replacing it. The system is based on marking corpses with RFIDtransponders. With the help of wireless communication and modern mobile devices (such as tablet PCs), the digital processing of victim data speeds the process up and improves its reliability.

The identification of casualties in the aftermath of large catastrophes such as tsunamis or terror attacks is a complex and partly unreliable, error-prone and mostly paper-based procedure. The current disaster victim identification process includes three steps: after the victim recovery, corpses are examined by the mortuary branch and finally transported to the identification centre. Although progress has been made in the field of automating the matching of ante and post mortem data, most processes include the manual collection of information about both corpses and missing people. As a consequence, disaster victim identification is usually delayed, to the detriment of relatives not knowing about the fate of their beloved ones.

The authors name several procedural flaws that could be overcome by introducing mobile information technology for emergencies. Taking into consideration the described deficiencies, the authors propose a solution based on a sophisticated mobile information system that improves the status quo without replacing it. The current process undergoes refinements but no impairments.

P 28

LANDMARKE PROJECT: DEVELOPMENT OF NAVIGATION TECHNOLOGY FOR FIREFIGHTERS AND WORK PRACTICES

V. Wulf^{1,2}, T. Dyrks^{1,2}, and L. Ramirez^{1,2}

¹ Universität Siegen; ² Fraunhofer Institute for Applied Information Technology, Schloss Birlinghoven, 53754 Sankt Augustin
volker.wulf@uni-siegen.de

Quickly building a reliable assessment of an incident is a key skill for firefighters. Navigation under extremely rough conditions and very poor visibility is an agency in which experience, senses and training play an extremely important role. Technology supporting navigation must take into account these factors to provide the required levels of safety. The Landmarke Project is an initiative funded by the Federal Ministry of Education and Research for developing a navigation support infrastructure enhancing the cognitive abilities of firefighters. In the vision of the project, firefighters mark relevant points of reference using interactive landmarks while performing their missions. These landmarks are small, deployable wedges containing sensing and networking technology. An interaction unit integrated in the equipment of the firefighter exchanges information with the landmarks, providing a layer of information that enhances the perception of the environment. The design space posed by the Landmarke project is particularly complex. Designing an interactive ubiquitous computing service for people crawling on the floor inside a building full of smoke confronts technology designers with complex constraints that demand exceptional solutions. While it is relatively easy to imagine visions of ubiquitous computing providing support to this work, designing practicable solutions is always a very complex challenge. To deal with this complex design space, we use in Landmarke a participatory design approach (Ehn 1992) focused on fostering an organic grow of technological artifacts from inside the work practices and intertwined with them. We use a collection of methods and tools, such as ethnographic studies (Randall et. al. 2007), triggering artifacts (Mogensen et. al. 1995) and experience prototyping (Buchenau et. al. 2000) to collaboratively search for opportunities to mediate or improve practices in navigation.

References

- [1] Ehn, P. (1992) *Scandinavian design: On participation and skill*. In: *Usability: Turning technologies into tools* (Eds, Adler, P. and Winograd, T.), pp. 96-132. Oxford University Press, Oxford.
- [2] Randall, D., Harper, R. & Rouncefield, M. (2007) *Fieldwork for Design: Theory and Practice*, Springer.
- [3] Mogensen, P. & Robinson, M. (1995) *Triggering artefacts*. *AI & Society*, 9, 373 - 388.
- [4] Buchenau, M. & Suri, J. F. (2000). *Experience prototyping*. In: *Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques*, pp. 424 - 433. ACM, New York City, New York.

POSTERS

P 30

SOCIAL SCIENTIFIC EXPERTISE AND CONCOMITANT RESEARCH

J. Pohl, J. Mayer, and S. Runkel

Universität Bonn, Geographisches Institut, Meckenheimer Allee 166, 53115 Bonn

pohl@giub.uni-bonn.de

1. Risk and security perception

The perception of risks, hazards and security/safety is a challenge for every technological innovation. We put risk perception and management in relation to the needs of practice and technology. Thus, the perspectives of engineering could be combined with social scientific studies on risk for the greater good of usability and acceptance through (downstream) users. We look upon a broad experience in projects on early warning systems (ILEWS), evacuation (HERMES) and risk management (InterRisk).

2. User-technology interface

With the objective of an optimized communication between different stakeholders we will identify them to moderate between the levels of developers, administrators and users in the process of the development and implementation of a technology. The focus is on the acceptance of new technologies as well as potentials and constraints of controlling. Administrative conditions have to be identified and analyzed. We work with a broad set of methods (Delphi, workshops etc.) to make communication possible.

3. Systemic social social research

The intrinsic logic of participating actors could lead to conflicts. We offer not just evaluation, but strategies to avoid barriers for innovations. The project would gain economic and organizational efficiency. Further we back our work with a wide range of theory-based research (f.e. system theory, etc.).

The poster will feature the two BMBF-funded projects 'HERMES' in which we research on evacuation of mass events as well as 'ILEWS', which has a focus on the development of an early warning system.

P 31

PRIVATE AND CORPORATE SECURITY MANAGEMENT - INTRODUCTION TO A NEW MASTER-PROGRAMME –

R. Stober

Deutsche Universität für Weiterbildung, Germany

rolf.stober@duw-berlin.de

“Not Freedom, equality or solidarity are the guiding principles of the current politics but security any-time and anywhere. The modern State is above all, a state dealing with security” (Wolfgang Sofsky, Security as a Principle, 2005, p. 84) In this context private security firms are being called upon more and more to assist states and their public authorities in providing the protection of people, buildings, goods and different other values. The growing private security sector, the reduction of public protection and the increasing private responsibility to corporate and infrastructure security produces a need of security learning and training system in consideration of the Bologna-Process and the security constitution, which allows different cooperations with the private security sector.

The presentation gives an introduction to a new established professional Master Programme “Private and Corporate Security Management” offered by the Berlin University for Professional Studies, a daughter of the Free University Berlin and the KLETT-Group. The unique selling points of the Programme are:

- Integration of different Security-Markets (Private Security, Corporate Security, Public Security, Public-Private Partnership)
- Distance Learning Model for Academic Professionals
- University based Training
- Interdisciplinary Approach (legal, social, Economic and technical competence)
- Process orientated schedule
- Focused on General Security Management
- Counterpart of academic Police Management Training

The blended learning concept consists of course books for training at home, Online-Units, Tutorial Support, Presence Phases and a Field Trip with the aim to get a reflective practitioner.

POSTERS

P 32

PRO-ACTIVE AND EFFECTIVE AVIATION SECURITY RESEARCH BASED ON STAKEHOLDERS' DIALOGUE

T. Hecker and N. Lombardo

National Competence Center Aviation Security Research (NCAS), Lise-Meitner-Str. 10,
64293 Darmstadt

torben.hecker@ncas-research.de

In the last decades, the requirements on aviation security have been raised in ever shorter time intervals. Combined with the forecasted increasing demand, the aviation sector has an ever growing “high pace” need for innovative security measures and therefore depends on the rapid development, certification and implementation of security innovations. As these innovations must be application oriented and appropriate for masses, it is essential to actively involve end users (public authorities, airports and airlines) and to include their operational requirements and practical experience at an early stage of development. Furthermore, instead of merely reacting to new regulations, entering in a close dialogue beforehand enables to pro-actively discuss current and future challenges and make use of emerging opportunities.

Utilizing dialogue platforms expedites the development processes and implementation of application oriented security innovations. Thus, financial and personnel related resources as well as complementary expertise can be allocated in a goal-oriented manner and the international competitiveness of the German respectively the European aviation industry can be safeguarded.

The proposed paper will discuss the difficulties concerning the perspectives and communication of aviation security related stakeholders and will present a holistic concept for a pro-active and effective dialogue platform. Further, different dialogue instruments which promote information/experience exchange will be presented. These instruments are the operational tools of dialogue platforms giving means to connect a wide and diverse network of stakeholders. In addition, the paper will inform about the experiences gathered while implementing the concept in Germany resulting in the National Competence Center Aviation Security Research (NCAS). The NCAS - constituted by end users and aiming for a productive exchange of stakeholders - is a dialogue platform which has received positive feedback from the aviation sector with first demonstrable successes such as the initiation of research consortiums and the identification of research requirements of end users.

Keywords

security research, end users, dialogue platform, aviation security

P 33

LIMITS, RULES AND THE NEED FOR TRANSPARENCY IN BIOSECURITY RESEARCH

I. Hunger

Research Group for Biological Arms Control, Carl Friedrich von Weizsäcker Centre for Science and Peace Research, University of Hamburg

iris.hunger@uni-hamburg.de

One of the areas in the life sciences, where the dual use potential – the potential to use the results of peaceful activities for hostile purposes – is particularly pronounced, is biodefence and biosecurity research. Such research activities frequently involve particularly dangerous agents such as anthrax and aim at threat assessment such as identifying gaps in biopreparedness. This often creates knowledge and materials that, if misused for hostile purposes, could have massive negative consequences. Biodefence and biosecurity research has proliferated in recent years; funding has increased, in some states dramatically, and there is a rapidly growing number of people and places involved in such research.

The proliferation of biodefence and biosecurity research has created several problems. There has been a recognizable change in research focus away from basic health needs towards very specific pathogens of bioterrorism concern. Research culture has changed; in particular the openness of the scientific enterprise has been questioned and at times been restricted. And last but not least, questions have arisen whether some of the activities in biodefence and biosecurity research may have crossed the border into territory prohibited by the international norm against biological weapons.

There is an urgent need for common understandings on where the limits of biodefence activities are. Biodefence scientists should receive training to recognize the misuse potential of their work and how to deal with it; there would also be use in thinking about a code of conduct for this area of research. And lastly, in order to avoid misinterpretation, biodefence activities need to be understandable to others, i.e. they need to be open and transparent as far as possible, and debate must be possible on a national and international basis.

P 34

OPTIMIZATION OF THE ANTENNA DISTRIBUTION OF A MICROWAVE-BASED BODY SCANNER PROFITING FROM AN AUTOMATIC QUALITY ASSESSMENT OF THE MICROWAVE IMAGES

C. Sklarczyk, A. Bevetskij, and R. Pinchuk

Fraunhofer-Institut für Zerstörungsfreie Prüfverfahren, Saarbrücken

christoph.sklarczyk@izfp.fraunhofer.de

In the area of homeland security real-time methods to detect dangerous and illegal items such as weapons or explosives hidden under clothing are sought. Methods harmless to humans and based on cm- and mm-waves are suitable for this purpose, since these waves penetrate clothing and are scattered back from the object. To achieve the required real-time capability of the scanner system, the person has to be scanned with an electronically controlled antenna array since scanners working mechanically are too slow.

In a conventional antenna array the antennas must be located very closely to each other to ensure a good spatial resolution and to avoid image artifacts. This results in a very high number of antennas and measuring channels. Using the principle of the Sampling Phased Array (SPA), in which all the antennas are interconnected with each other, the number of required antennas can be reduced decisively making the overall system more cost-effective.

The method developed at the Fraunhofer IZFP enables a fully automated optimization of the SPA-antenna array based on simulations. The quality of two- and three-dimensional images can thus be determined quantitatively. In each iteration step of the optimization method one reference image that has been generated with a fully occupied conventional antenna array and one image generated with a thinned array according to the SPA principle are compared with each other, making a decision in accordance with a predefined quality threshold. In each iteration a software module creates a new antenna arrangement after a given scheme resulting in an antenna arrangement optimized to the respective inspection task and geometry.

P 35

A NEW SECURITY CONCEPT ON AIRPORTS USING A ROTATING W BAND PERSON SCANNER WITHIN A SENSOR NETWORK

S. Hantscher¹, S. Lang¹, M. Hägelen¹, H. Essen¹, and A. Tessmann²

¹ Fraunhofer Institute for High Frequency Physics and Radar Techniques, Neuenahrer Straße 20, 53343 Wachtberg, Germany; ² Fraunhofer Institute for Applied Solid State Physics, Tullastr. 72, 79108 Freiburg, Germany

sebastian.hantscher@fhr.fraunhofer.de

After the failed terror attack on a flight to Detroit on December 25th, the security systems on airports are currently under close scrutiny. Common metal detector systems require time-consuming manual inspection and are just able to detect metal objects. Emerging person scanners like X-ray scanners or full body scanners seem to be harmful or are questionable regarding the privacy of the passenger. Moreover, single sensor concepts do not have the reliability which is required from the airport security personnel.

That is why a new security concept is introduced based on the fusion of different sensors. It foresees two imaging sensors, an active 94 GHz radar in the W band and another radar in the band from 15 GHz to 35 GHz. Furthermore, active and passive GSM or Wifi based sensor nodes will be installed in the airport area in order to track suspicious people. These sensors should operate almost invisible for the persons such that the natural passenger flow on the airport will be influenced as little as possible.

In this contribution, a W band person scanner is proposed enabling a 360 degree scan from the person under test. With this full-body measurement, a comprehensive detection of hidden objects is possible within a few seconds. For obtaining a sufficient resolution, the principle of the synthetic aperture is applied to simulate a narrow beam antenna by moving a broad beam antenna around the person. In the current version, the radar data are mapped and focused onto a cylindrical surface which shows suspicious objects on a test person. Tests measurements show – without affecting the privacy of the person – that metal objects such as guns are detectable as well as ceramic knives which cannot be discovered by using conventional scanners. These data might be utilised as the input for forthcoming radar systems.

POSTERS

P 36

WATER-FOG-GENERATOR BASED ON A ROCKET-BURNER TO DISSOLVE VIOLENT DEMONSTRATIONS

H. Schmid

Fraunhofer-Institute for Chemical Technology (ICT), Joseph-von-Fraunhofer-Str. 7, 76327 Pfinztal
helmut.schmid@ict.fraunhofer.de

Violent demonstrations must be fought with adequate means in order to ensure de-escalation. Today armoured vehicles equipped with water cannons are widely used to generate physical impacts. This procedure is relatively safe, but complex, expensive and low effective. Pepper spray cartridges fired from pistols or rifles can put attackers out of action in advance – but a health risk must be considered. The legality according to international chemical weapon control is still under discussion.

A new approach is the use of a water-fog-generator based on a smart rocket-burner. These small, lightweight and autarkic device can be used as a de-central solution. The water-fog generators produce micro droplets so that large areas can be covered very fast. The fog impedes the view and simultaneously works as a very efficient fire extinguishing-system, e.g. against "Molotow-Cocktails". The apparatus can be easily operated and handled by one person, is mobile, non-human-toxic, environmental-friendly and low in price.

P 37

NON-INTRUSIVE CONTINUOUS USER BEHAVIOR ANALYSIS USING COMPUTERIZED SYSTEMS

A. Messerman, T. Mustafić, A. Camtepe, and S. Albayrak

Technische Universität Berlin, DAI-Labor, Ernst-Reuter Platz 7, 10587 Berlin

arik.messerman@dai-labor.de

There are different ways to authenticate humans to a computerized system as an essential prerequisite for access control. An authentication process consists of the validation of the authorization by any subset of three factors: something someone i) know (e.g. password), ii) have (e.g. smart card), and/or iii) is (biometric features). Besides classical attacks on password solutions and the risk that identity-related objects can be stolen, traditional biometric solutions have their own disadvantages such as the requirement of expensive devices, risk of stolen bio-templates etc. Moreover, existing approaches provide the authentication process usually performed only once initially. Nonintrusive and continuous monitoring of user activities emerges as promising solution in hardening authentication process: (iii-2) how someone is doing something. In recent years various keystroke dynamic behavior-based approaches were published that authenticate humans based on their typing behavior. The major part focuses on so-called static text approaches, where users are requested to type a previously defined text. Relatively few techniques are based on free text approaches that allow a transparent monitoring of user activities and provides continuous verification. Unfortunately only few solutions are deployable in real application environments under real conditions, because of scalability reasons, too high response times and error rates. The aim of this work is the development of behavioral-based verification solutions that can be deployed under real conditions in existing environments in order to enable a transparent and free text-based continuous verification of active users with low error rates and response times. Regarding this, based on a web mail application, various solutions were developed, implemented and evaluated, which guarantee that verified objects represent in truth current acting humans. Such solutions, resistant against so-called unlocked workstation-attacks, achieved a FAR of less than 1% and a FRR of less than 10% after only few characters typed using standard keyboard input devices. Since the user's behavior is analyzed during the interaction through a standard input devices such as the keyboard, no additional hardware equipment is required.

References

[1] *Moskovitch R., Feher C., Messerman A., Kirschnick N., Mustafic T., Camtepe A., Löhlein B., Heister U., Möller S., Rokach L., Elovici Y. Identity Theft, Computers and Behavioral Biometrics. In IEEE Intelligence and Security Informatics, 2009. ISI, 09., 2009*

POSTERS

P 38

THE SENSOR GRID – AN INTEGRATED SECURITY SOLUTION

J. Weijman

American Science and Engineering, Inc., AS&E Europe B.V., Amsterdam

jweijman@as-e.com

Security in Europe is facing increasing challenges. Acts of terrorism, organized crime, smuggling of contraband and weapons of mass destruction are posing a serious threat to our open society. In order to protect ourselves against these threats many individual security measures are taken at Air and Seaports, Border crossings and critical infrastructure. Most of the security systems work stand-alone or at best integrated in the local IT infrastructure. Transmission and Backscatter X-ray technology are important detection capabilities. Our vision, that we call "The Sensor Grid" is a three layered security model.

- Layer one: The sensor layer
X-ray scanners, mmWave and under vehicle cameras should produce the images in a uniform and vendor independent format.
- Layer two: The communication layer
All elements in the sensor layer should act as a uniform IP network element. This ensures proper (international) communication while using the highest encryption standards.
- Layer three: The presentation layer

Every national and international government organization has its own security application and databases. The layered integrated solution allows using the existing application to evaluate images that are produced by transmission or backscatter X-ray system across the world. This means that an X-ray image from a container in Hamburg can be presented for evaluation to a CSI officer in Washington DC, USA. Or a backscatter X-ray image from mobile police unit can be evaluated by an officer from the regional justice department before deciding to enter a building and issuing an electronic warrant.

The combination of transmission and backscatter X-ray technology provides the highest grade of detection and fits perfectly in this layered model like the proven Omniview system in the Port of Venice in Italy. The images from this system are evaluated in Rome using the existing applications. We will see more of those examples. It does require co-operation from all technology providers. Ideally this must be promoted by central European organizations like EU, WCO, Eurotracks, Interpol, OLAF and EAASP.

P 39

TEAMS RATHER THAN INDIVIDUALS: COLLABORATIVE INTRUSION DETECTION

R. Bye, A. Camtepe, and S. Albayrak

DAI-Labor, Technische Universität Berlin

rainer.bye@dai-labor.de

There are many challenges for current intrusion detection approaches such as zero-day attacks, high false-alarm rates or architectural drawbacks, e. g., centralized designs exposing the Single-Point-of-Failure. From the field of sociology, we learn that teams respectively groups cope with complex tasks by their inherent cooperative character. Accordingly, there exist intrusion detection systems, that work cooperatively, bypassing the aforementioned shortcomings of the conventional approaches. However, these systems remain limited to very specialized scenarios and do not take configuration and grouping of participants into account.

We propose CIMD (Collaborative Intrusion and Malware Detection), a scheme for the realization of collaborative intrusion detection approaches [1]. We argue that teams, respectively detection groups with a common purpose for intrusion detection and response, improve the measures against malware. By enabling participants to state their objectives (i.e. the aim of a detection group) and interests (i.e. the desired properties of the team members) an intrusion detection overlay is realized.

We introduce the main aspects of Collaborative Intrusion Detection, and show related work as well as the influences from other research fields on this school of thought. Then, we outline challenges such as the group formation process and show how the CIMD approach provides solution. In two case-studies, we present the relevance and applicability of the approach to „real life“. This includes a group set-up that benefits from the homogeneity of the members to enable a collaborative anomaly detection approach. In contrast, the applicability and benefit of a heterogeneous group set-up is shown. Here, the shortcomings of individual members are compensated and the nodes exchange signatures to reduce the window of opportunity of zero-day attacks.

References

- [1] Rainer Bye, Ahmet Camtepe, and Sahin Albayrak. *Collaborative Computer Security and Trust Management, Chapter Teamworking for Security: The Collaborative Approach, page 342. Reference. Information Science Reference, 1 edition, November 2009.*

POSTERS

P 40

BI-SPECTRAL QUANTUM-EFFECT INFRARED DETECTORS FOR SECURITY AND SURVEILLANCE

F. Rutz¹, R. Rehm¹, M. Walther¹, J. Schmitz¹, J. Niemasz¹, L. Kirste¹, and R. Scheibner²

¹ Fraunhofer-Institut für Angewandte Festkörperphysik, Tullastraße 72, 79108 Freiburg;

² AIM Infrarot-Module GmbH, Theresienstraße 2, 74072 Heilbronn

frank.rutz@iaf.fraunhofer.de

Bi-spectral infrared imaging systems with the ability to detect infrared radiation in two different wavelength regions are key elements for the next generation of infrared detectors for security and surveillance. Modern quantum effect infrared detectors, based on type-II InAs/GaSb short-period superlattices (SLs) have proven their great potential for high performance bi-spectral infrared detectors and are now emerging from the development stage into field applications. This new class of infrared detectors exhibit high quantum efficiency and offer simultaneous and spatially coincident detection in two different spectral channels.

In the past years, the development of the infrared detector technology at the Fraunhofer-Institute for Applied Solid State Physics (IAF) has been focused on achieving series-production readiness for bi-spectral dual-color superlattice detector arrays for the mid-wavelength infrared spectral range. The mature III-V process technology is ideally suited for airborne missile threat warning systems, due to the ability of low false alarm remote imaging of hot carbon dioxide signatures at very short integration times.

One essential point for the performance of two-dimensional focal plane infrared detectors is the crystallographic defect density of the substrate and the epitaxial layer structure. Permanent improvement of the material quality and the development of suitable techniques to monitor the quality of substrates and epitaxial layers are important. The detector structures are grown in a multi-wafer molecular beam epitaxy system on 3" GaSb substrates. With a full wafer process technology, focal plane array detectors with 288 x 384 detector elements are processed and hybridized with a silicon based integrated read-out circuit. The detectors are then integrated into a detector cooler assembly, which is part of an infrared camera system. Very uniform detector arrays with high quantum efficiency and excellent thermal resolution are obtained with this technology. The performance data of this new class of infrared imaging systems clearly demonstrate the capability of this enabling technology.

P 41

INTEGRATED CIRCUITS BEYOND 100 GHz FOR STAND-OFF DETECTION OF CONCEALED WEAPONS

A. Hülsmann, A. Tessmann, A. Leuther, I. Kallfass, M. Schlechtweg, and O. Ambacher

Fraunhofer Institute Applied Solid State Physics (IAF), Tullastr. 72, 79108 Freiburg

axel.huelsmann@iaf.fraunhofer.de

Suicide Bombers are an increasing problem for the security personal at check points and entrance portals. To detect concealed weapons, explosives or hazardous substances, millimeter wave is a probate technology to penetrate clothing of suspicious persons. Body scanners, working at low frequency millimeter waves, are already at a high technological level.

Such scanners operate at the limit of the well known Rayleigh resolution ($Res \sim \lambda / NA$), where λ is the wavelength and NA is the numerical aperture ($NA = \sin f$, and f is the aperture acceptance angle). Commercial scanners are limited by the frequency of available millimeter wave circuits, but the NA can be increased to unit if the sensor is moved $f = 90^\circ$ around the person. Assuming a millimeter wave frequency of 30 GHz, wavelength and resolution are at 10 mm.

For stand-off detection the situation is somewhat different. The distance to a potential suicide bomber should exceed 30 m. On the other hand the real aperture of a stand-off detection system will hardly exceed 2 m. Thus NA is a problem and the resolution of a 30 GHz system will be unacceptable. Thus increasing frequency is the only solution for stand-off-detection.

At Fraunhofer IAF we have developed several integrated circuits working at frequencies between 100 and 300 GHz and above. These circuits have been tested in active and passive working systems based on radar or radiometer technology.

POSTERS

P 42

PREBORDERLANE – TECHNOLOGY MUST ADAPT TO PEOPLE, NOT PEOPLE TO TECHNOLOGY

J. Köplin¹, K. Hops¹, and A. Nouak²

¹ w/o aff.; ² Fraunhofer-Institut für Graphische Datenverarbeitung IGD, Darmstadt

alexander.nouak@igd.fraunhofer.de

In Border Control in many cases delays are generated by confronting officers with documents they do not have qualifications for.

Passengers are subject to either a minimum check or a detailed check which is determined by the traveller's nationality. Within the Schengen area border control distinguishes between EU citizens and non- EU citizens but also non-EU citizens that hold a residence permission.

And non-EU citizens may carry a passport that does not apply to the current standards. In order to accelerate the border crossing process also a distinction is required between casual and frequent travellers as well as people that need special assistance like physically impaired, persons with small children, families and the such.

To improve the process we propose the concept of a PreBorderLane that runs a holistic approach (in contrast to current systems like Rapid or EasyPass). The inevitable waiting time may already be used to start the interaction with the passenger. By scanning the machine readable zone of the identification document we get enough information to welcome the passenger in his mother tongue instructing him on how to proceed. If his document already holds the new biometric features the biometric characteristics can be compared. The relevant databases (AFIS, black lists, VIS) can be contacted and necessary measurements can be taken at an early stage. In the end the passenger can be assigned an official with the suitable qualifications to communicate with the traveller and check his specific documents.

The Pre-Border Lane incorporates a more efficient use of manpower as it can be dynamically adjusted to meet current passenger flows. It enhances therewith the security despite a faster throughput of passengers. Since passengers cannot wait in the wrong queue border control personnel is not confronted with documents or situations they are not qualified to examine.

P 47

INFOSTROM: LEARNING INFORMATION INFRASTRUCTURES FOR CRISIS MANAGEMENT IN MEDIUM TO LARGE ELECTRICAL POWER BREAKDOWNS

N. Balduin⁴, J. Brand⁴, M. Görden⁴, M. Hannappel¹, P. Hasenfuß⁵, B. Ley¹, C. Neuhaus¹, V. Pipek¹, F. Probst³, C. Reuter¹, T. Rose², G. Rusch¹, T. Wiedenhöfer¹, and A. Zinnen³

¹ Universität Siegen; ² Fraunhofer-Institut für Angewandte Informationstechnik FIT, Sankt Augustin; ³ SAP Research - CEC Darmstadt; ⁴ RWE AG, Essen; ⁵ PSI Transcom GmbH, Berlin
volkmar.pipek@uni-siegen.de

One of the most important infrastructures in modern industrialized societies is the electricity network. Due to its fundamental role for many aspects of our everyday life, power infrastructures lead to a strong dependence between power suppliers and customers. Customers take the infrastructure for granted; it appears mostly invisible to them as long as it works, but in the case of breakdowns in power supply customers become aware of the dependence on electricity. They join professional actors in the recovery and coping work with regard to the electricity breakdown: Maintenance workers of the power provider, police, firefighters, red cross, etc. These institutions are professionalized to deal with such situations, but the people affected by a power outage also need to be considered as actors.

The goal of the InfoStrom Project is to develop a "Security Arena", a communication and information platform that aims to continuously improve cooperation for electricity supply recovery between power supplier, firefighters, police, country administration and citizen. It focuses on designing effective interorganizational communication, information and coordination processes and on the development of new innovative technologies in the fields of situation illustration, reliability, information quality visualization, flexibility and public participation. All technologies, concepts and methods will be developed and evaluated in cooperation with RWE, SAP Research, Fraunhofer FIT, PSI Transcom and the County Siegen-Wittgenstein and Rhein-Erft County.

The use of information and communication technologies should empower the actors to improve planning, observation and management of and in crisis situations. Based on a rich technological foundation of mobile technologies, service-oriented architectures and semantic technologies, we focus on the development socio-technical concepts, demonstrators and media concepts, which allow to include existing technologies of crisis management and infrastructure maintenance into processes to improve inter-organisational communication and collaboration in scenarios of medium to large electrical power breakdowns. One important aspect will be to improve the integration of citizens as active participants in managing crisis situations.

POSTERS

P 48

CONTEXT ADAPTIVE SERVICE SELECTION WITHIN A SOA FOR SURVEILLANCE APPLICATIONS

E. Kannegieser and S. Leuchter

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung, Abt. Interoperabilität und Assistenzsysteme, Fraunhoferstr. 1, 76131 Karlsruhe

sandro.leuchter@iosb.fraunhofer.de

In the last years service oriented architectures (SOA) have been used to integrate newly developed and already existing surveillance resources such as sensors, databases, and information processing capabilities (e.g. Finland Network-Enabled Defence, or US Coast Guard's Long Range Identification and Tracking).

The paradigm of SOA is to decouple the implementation of the overall application and utilized function implementations (services). This is realized by introducing a service registry instance where each service provider registers its functions together with the syntax of the invocation protocol. This allows for late binding: The creator of an application that will use such service resources does not have to know the specific service providers at system development time but delays the decision which implementation to use until run time when the application uses the service registry to find feasible service providers that can be utilized by a standardized protocol. Making an application on top of a SOA means to orchestrate the sequence of such service calls. Due to late binding SOA applications can be changed ad hoc. Service providers can be easily replaced without touching the orchestrated application.

The advantage of this approach can turn into a weakness: Large SOAs can consist of a plethora of such service providers from internal as well as external sources. Thus service discovery (interactive and automated) may become a problem because the service registry has only syntactical information about service names and interfaces but knows nothing about performed function, constraints, or quality of the implementation. A solution to this problem is to enrich the representation of services in the registry semantically. This exposes service discovery processes to reasoning, automated matchmaking, and dynamic generation of orchestration.

We have developed a new semantics aware service discovery component that fits into SOAs. It is based upon the SOAR rule engine. In a proof of concept a perimeter control application has been built with some simple service enabled sensors. The new service discovery component uses an ontological representation of attributes and capabilities of deployed sensors and a custom rule set that uses context information to deduce constraints of the current situation and proposes sensor services best suited to current task and context.

P 49

STANDARDISATION OF REPORTS TO OPTIMISE COOPERATION IN THE DOMAIN OF PUBLIC SAFETY AND SECURITY

C. Lindemann, C. Held, J. Pottebaum, and R. Koch

Universität Paderborn, Computeranwendung und Integration in Konstruktion und Planung (CIK),
Pohlweg 47-49, 33098 Paderborn

held@cik.uni-paderborn.de

In large scale incidences communication systems in the domain of public safety and security require the intra- and interorganizational exchange of messages and reports. Because of the wide variety of systems, uniform standards are not available. To enhance the efficiency of crisis management and emergency response it is necessary to support the actors in their intrinsic ambition to get an overview of all relevant information and to get a collective understanding of processes and structures.

The evaluation of established processes, the analysis of directives and guidelines as well as former studies in research (cp. various ISCRAM papers) and commerce (cp. BITKOM publications) led to the conclusion that the exchange of reports plays a decisive role for the generation of an operational picture. The standardized exchange of data based on a common vocabulary among the public safety authorities and organizations promises high potential. Ongoing initiatives like CAP and EDXL underline this result. It tends to the analysis of organisations considering psychological, sociological and technical aspects to get an increased understanding of existing and required communications.

This contribution focuses on both the organisational and the semantic level of interoperability. Following a scenario based approach a specific group of players was set up. Within the user oriented methodology workshops of this "Round Table" are used besides interviews to identify goals and restrictions of communications. Results of this intensive approach to requirements engineering are available: On the one hand the results illustrate communication problems and a lack of common understanding between the players. On the other hand the power of established workflows is highlighted and has to be taken into account carefully.

The described results represent the basis for a standard "xHelp" will be defined in close cooperation with an extended group of players. The results will be transferred to the technological level of interoperability; they will be evaluated comparatively and illustrated by a demonstrator. In doing so no new information system will be created: Better access to information transferred in established workflows will be used to get a networked operation.

POSTERS

P 50

CYBER DEFENCE IN FUTURE COMMUNICATION NETWORKS – A MULTILAYER SECURITY ARCHITECTURE

M. Kretzschmar, B. Stelte, and R. Koch

Institut für Technische Informatik, Universität der Bundeswehr, München Neubiberg

michael.kretzschmar@unibw.de

Future communication networks (FCN) will be highly dynamical, flexible, and scalable designed to support any kind of missions. The provision of security, privacy, and trust will be the most challenging tasks for network providers in inter- and intra-domain communications.

Cyber defence requires mechanisms, procedures, and capabilities to prepare for, prevent, detect, respond to, recover from and learn lessons from attacks affecting the confidentiality, integrity and availability of information and supporting system services and resources.

Well-known and today available state-of-the-art Cyber Defence systems and algorithms for Intrusion Detection and Early Warning are not able to cope with these challenges. These systems are based on data provided by sensors in the network which are not able to handle upcoming challenges such as trillions of fixed as well as mobile devices, huge amounts of data, encrypted payloads or complex security strategies.

Based on current research we present a multilayer security architecture that addresses these security challenges. The primary task of an Early Warning System (EWS) is its capability to detect cyber attacks and the distribution of malicious software as early as possible. Attack signatures can be detected and classified by Intrusion Detection and - Prevention Systems (IDS / IPS) based on data from sensor agents. A detection of ongoing cyber attacks can initiate the activation of additional, specialized sensor agents or re-configuration of certain sensor agents for further investigation. The network provider's Security Management Infrastructure (SMI) will take this task in our architecture.

By sharing information about detected attacks or by combining information from different providers to enable the detectability of attacks, the Cyber Defence System can isolate ongoing attacks and prevent further dissemination. Therefore, the SMI coordinates the collaboration in general and the degree of information exchange between the network providers.

P 51

MEVIM – MOBILE EVIDENCE INVENTORY MANAGEMENT

D. Mosemann^{1,2}, C. Schmitt^{1,2}, and K. Fischbach²

¹ Ambient Innovation, Pohligstr. 1, 50969 Cologne; ² Dep. of Information Systems and Information Management, University of Cologne, Albertus-Magnus-Platz, Cologne, Germany
University of Cologne, Pohligstr. 1, 50969 Cologne

mevim@ambient-innovation.com

Throughout Germany police authorities prosecute more than 1 million serious criminal actions annually. Therefore many traces have to be documented in detail in order to reconstruct the progression of events. Analyzing the necessary communication, numerous media disruptions crop up: Investigating the crime scenes, observations are documented manually written. Afterwards these observations are keyed in the local information systems at the police station. In order to share findings of an investigation with forensic laboratories or the public prosecutor's offices, corresponding reports are printed and composed as paper file again. Especially, extra time-consuming effort for manual assignment of copious photographs to secured evidence has to be taken into account.

The Department of Information Systems and Information Management at the University of Cologne develops a mobile computing system called MEVIM that supports the investigators during crime scene investigation and reduces overhead for compiling records at the police station.

Investigating the crime scene, traces are labeled distinct with RFID and corresponding details or evidences are captured intuitively using rugged mobile devices. So, user input can be verified and new information can immediately be used for prosecution without further recording. Therefore the mobile application automatically synchronizes with the local intranet application whenever the mobile devices are linked to their cradles at the police station. Copious photographs are assigned to covered traces automatically and reports are generated from stored information. With MEVIM the stored information can easily be changed or supplemented with proofed evidence using web form. Also, you can trace corresponding court exhibit while passing them to criminological inspections and analysis.

POSTERS

P 52

STATIC SMARTPHONE MALWARE DETECTION

A.-D. Schmidt, A. Camtepe, and S. Albayrak

Technische Universität Berlin – DAI-Labor, 10587 Berlin

aubrey.schmidt@dai-labor.de

Malwares (e.g. virus, worms and Trojan horses) have been threats to computer systems for many years and it was only a question of time when the first malicious software writers would get interested in increasingly popular mobile platforms, such as Symbian OS. In 2004, the first articles about malware for smartphones appeared, cf. [1-2], stating that the next generation of targets are mobile devices. Since then, the number of malwares increased every month and variants for various smartphone platforms appeared. Commercially available countermeasures to smartphone malware suffer from weaknesses since they mostly rely on signatures. This approach leaves users exposed to new malware until the signature is available. Bulygin [3] showed that in worst case a MMS worm targeting random phone book numbers can infect more than 700000 devices in about three hours. Additionally, Oberheide et al. [4] state that the average time required for a signature-based anti-virus engine to become capable of detecting new threats is 48 days. These numbers request extended security measures for smartphones as a malware can seriously damage an infected device within seconds. In this context, the new smartphone platform Android gained special interest among developers. Since it set open source, security tools can be developed even at kernel level. This allows comprehensive security mechanism to be deployed on Android handsets only being limited by the typical resource constraints of mobile devices. Due to these constraints, we focus on static and light-weight mechanisms for detecting malware presence on Android devices. Our static approach for detecting malware allows us to use simple classifiers which are not very resource consuming and therefore fit very well to mobile needs. Additionally, these classifiers tend to have high detection rates while keeping false positive rate low.

[1] D. Dagon, T. Martin, and T. Starner, "Mobile phones as computing devices: The viruses are coming!", *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 11–15, 2004.

[2] M. Piercy, "Embedded devices next on the virus target list," *IEE Electronics Systems and Software*, vol. 2, pp. 42–43, Dec.-Jan. 2004.

[3] Y. Bulygin, "Epidemics of mobile worms," in *Proceedings of the 26th IEEE International Performance Computing and Communications Conference, IPCCC 2007, April 11-13, 2007, New Orleans, Louisiana, USA. IEEE Computer Society, 2007*, pp. 475–478.

[4] J. Oberheide, E. Cooke, and F. Jahanian, "Cloudiv: N-version antivirus in the network cloud," in *Proceedings of the 17th USENIX Security Symposium (Security'08), San Jose, CA, July 2008*.

P 53

SECURE CONTEXT-AWARE RECONFIGURATION FOR MOBILE DEVICES

L. Batyuk and S. Albayrak

Technische Universität Berlin – DAI-Labor, 10587 Berlin

leonid.batyuk@dai-labor.de

Over the past ten years, the trend in user applications has definitely moved towards autonomous mobile devices, and wireless networks. More and more applications rely on various physical and logical sensors. The computing environments of today have become highly heterogeneous and spontaneous, but the models and methods for software development remained mostly the same as for desktop computers and wired networks. These models do not allow software to adapt to the current situation of the user.

A novel approach to solving this problem is context-awareness, where software is enabled with knowledge about its environment and adapts itself to the current needs of the user. During the last decade, numerous context-awareness frameworks have evolved on both infrastructure-level and device-level. Most context-aware systems rely on predefined settings which invoke a certain action upon a change in the environment. However, in several works an attempt has been made to overcome the fixed model and implement a generic approach. The concepts of context proximity and context familiarity have been introduced, which, to some extent, enable reasoning upon context without having a precise set of rules and predefined conditions.

These approaches provide more flexibility, but less control due to inability of such methods to annotate context information with semantic data, enabling full-edged reasoning. As such, automated semantic recognition and annotation of context is a fundamental problem we address.

Utilizing contextual information for autonomous secure self-configuration is an example of a use case where manual rule-based management is unfeasible, but also current heuristics fail due to their shortcomings. We contribute to existing heuristic approaches with methods of artificial intelligence, utilizing techniques known from the field of anomaly detection to identify, predict and annotate context information, allowing to make more precise and reliable security decisions upon sensor data.

POSTERS

P 54

AN OVERVIEW – CORE ELEMENT FOR INTEROPERABILITY IN NETWORKED SECURITY

K. Mertins¹ and A. Groth²

¹ Fraunhofer Institute for Production Systems and Design Technology, Pascalstraße 8-9, 10587 Berlin; ² Ampersystems, Margeritenstraße 5, 82256 Fürstenfeldbruck

kai.mertins@ipk.fraunhofer.de

The networked application is the essential means to manage successfully military deployment, emergencies of internal security and catastrophes by the EU, NATO or also national in a group of various military forces und civil organizations in sense of „joined, combined as well as within a strategy of networked security. In order to realize networked application interoperability is required. Interoperability enables to net fast and agile as well as effective and economical a network of various forces and services for a specific mission over a limited period of time.

Interoperability as an “essential tactical element” requires in sense of Clausewitz the “superelevation” in condition of a “better overview”. “The overview”, in other words the situation picture, empowers a group of forces to estimate jointly the given situation based on current and secured information in order to make a well-founded decision and to come to an appropriate decision as well as to reliable supervision of the following actions.

Nowadays there is no need of further systems or other functionalities for the interoperability of a networked application but rather the competency to design an information hub to integrate existing organizations structures, processes and systems as well as technology in sense of the strategy of networked security.

At the FHG IPK in cooperation with the industry this competency was used to establish the concept of an information hub to application maturity in order to empower fast and agile interoperability for the networked application to existing organizations, processes and systems. For the respective application an individually adjusted, matured and appropriate interoperability is quickly established, assured and conducted in order to be able to execute and operate tactical, operational and strategical command levels.

In the presentation the concept of an information hub for interoperability in networked application will be performed and with the aid of real examples the application to manage emergencies of internal security and catastrophes in sense of the strategy of networked security will be demonstrated.

P 55

SPIDER - SECURITY SYSTEM FOR PUBLIC INSTITUTIONS IN DISASTROUS EMERGENCY SCENARIOS

L. Tufte¹, S. Subik², and T. Tran²

¹ PRO DV Software AG, Hauert 6, 44227 Dortmund; ² Communication Networks Institute, TU Dortmund

lars.tufte@prodv.de

Various organisations are involved in large-scale disaster management operation, for instance with several hundred injured people. One of the big challenges is an efficient information management that gives the people in the field ubiquitous access to the right information during the whole operation and support them in their emergency response tasks. The SPIDER project tackles this challenge by facilitating interoperability of existing IT systems (e.g. GSL.net, XENIOS, deNIS Ilplus) using novel web services and a new XML based Protection and Rescue Markup Language (PRML). Moreover, a high reliability, high availability mobile communication network will be provided at the emergency location allowing ubiquitous information access and exchange. This network will enable the emergency services to communicate even if public networks are broken down as a result of panic calls of the involved parties. IT security aspects are of high relevance considering that personal data, e.g. the name and state of health of a person, will be exchanged.

The SPIDER security solution is based on a Public Key Infrastructure (PKI) in combination with an extended set of roles and rules, which are the foundation of the rights management. To increase the flexibility a peer to peer network will be used to enable a service discovery even in local incident area networks without an interconnection to other public networks. As an addition, even interfaces to on-scene computer-aided facility management systems are defined to enable fire fighters a dynamic control of escape routes and other building infrastructure components (like door controls)

Our concepts and solutions as well as first results of an early demonstrator will be presented in the paper.

POSTERS

P 56

IP-BASED APPLICATION AND SERVICES FOR NEXT GENERATION NETWORKS

Y. Rebahi

Fraunhofer Fokus, Kaiserin-Augusta-Allee 31, 10589 Berlin

yacine.rebahi@fokus.fraunhofer.de

The transition to Next Generation Networks is often coupled with the vision of innovative services providing personalized and customizable services over an all-IP infrastructure. To enable a smooth transition, next generation all-IP networks need not only support more services but also support current vital services, namely emergency services. The PEACE project is a research project funded by the European Commission that aims to provide a general emergency management framework addressing extreme emergency situations, such as terrorist attacks and natural catastrophes as well as day-to-day emergency cases based on the IP Multimedia Subsystem (IMS).

To achieve its goals, the PEACE project will be addressing two major technological challenges:

First, a general solution for secure multimedia communication in extreme emergency situations will be provided. This will often involve the establishment of an ad-hoc networking environment for communication among first responders. In this context, the PEACE project will be devising mechanisms for fast and lightweight establishment of keying material between members of first responders in order to ensure the security of their communication. Furthermore, to enable multimedia communication in such environments, current centralized services, such as VoIP call routing and name translation, need to be supported in an adhoc networking environment.

Secondly, the PEACE project will investigate the provision of day-to-day emergency communication in Next Generation All-IP networks. Due to the different structure of IP and PSTN networks, it is not possible to simply reuse PSTN emergency services standards for emergency services communication in IP networks. This involves location information management, emergency calls identification and routing, emergency calls prioritization, and support for disabled persons.

In our presentation, we will describe the progress as well as the results being achieved within the PEACE project.

P 57

THE EMERGENCY MISUSE PROBLEM: DETECTION AND PREVENTION

Y. Rebahi

Fraunhofer Fokus, Kaiserin-Augusta-Allee 31, 10589 Berlin

yacine.rebahi@fokus.fraunhofer.de

The top priority of a Public Safety Answering Point (PSAP) is to answer to emergency calls as fast as possible and to ensure that the appropriate emergency assistance is initiated. However, it is possible that a call taker answers to a call and determines afterwards that it is not of an emergency nature. It might be possible that there is no bad intention behind this kind of calls, however, it is important to mention that these calls present a major problem for the emergency services as they can cause some delay to respond to the genuine calls and initiate wrong decisions. It is worth to mention that the European average of hoax calls is around 70% of the overall amount of calls that the PSAPs answer. This can result in overloading the PSAP with false calls in addition to the fact that the call takers can do the wrong decision by answering a given call if they have been receiving only false calls during the last hour. Reducing the percentage of misuse or hoax calls is very important and will save lives. In our presentation, we will discuss the emergency misuse problem, its scope, and the potential solutions being investigated within EENA 112 and the PEACE (<http://www.ict-peace.eu/>) project that Fraunhofer Fokus is currently running.

The SPIDER security solution is based on a Public Key Infrastructure (PKI) in combination with an extended set of roles and rules, which are the foundation of the rights management. To increase the flexibility a peer to peer network will be used to enable a service discovery even in local incident area networks without an interconnection to other public networks. As an addition, even interfaces to on-scene computer-aided facility management systems are defined to enable fire fighters a dynamic control of escape routes and other building infrastructure components (like door controls)

Our concepts and solutions as well as first results of an early demonstrator will be presented in the paper.

POSTERS

P 58

SECURITY ASSESSMENT OF THE EVOLVED PACKET CORE

Y. Rebahi, T. Q. Tran, and T. Magedanz

Fraunhofer Fokus, Kaiserin-Augusta-Allee 31, 10589 Berlin

yacine.rebahi@fokus.fraunhofer.de

The Evolved Packet Core (EPC) is the new all-IP mobile core network for the Long Term Evolution (LTE). It provides a converged framework for packet-based real-time and non-real-time services. The EPC promotes the introduction of innovative services and applications and can be accessed through trusted and untrusted (WiFi, Femtocells, ...) access networks, which makes security as a must in this kind of environments. The Evolved Packet Core already includes some building security mechanisms such as authentication and authorization based on the DIAMETER standard, unfortunately, this might not be sufficient when the EPC is being accessed from untrusted networks. The objective of our presentation is to give an assessment of the EPC from the security point of view in addition to the progress being achieved regarding the protection mechanisms being developed within the internal Fraunhofer Fokus project "OpenEPC".

5th SECURITY RESEARCH CONFERENCE
BERLIN, SEPTEMBER 7th – 9th, 2010

AUTHOR INDEX

- Adameit, S. S 8.3
Adini, B. Project BEPE
Adler, C. S 4.4
Aidam, R. Project IRLDEX
Albayrak, S. P 37, P 39, P 52, P 53, S 8.1
Ambacher, O. P 41
Amlot, R. S 5.4
Angelmahr, M. P 15
Anisimov, O. P 19
Arendt, F. S 1.3
Arnold, G. S 3.4
Ashkenazi, A. Project I-LOV
Augustin, S. S 3.4
Axelsson, L. P 1
Baldauf, M. S 4.3
Balduin, N. P 47
Balz, W. Project RETISS
Barrass, S. S 7.4
Barthet, C. P 7
Bartschke, J. S 3.1
Batyuk, L. P 53
Baumann, S. P 25
Beigang, R. S 3.1
Ben-Amar, M. S 4.4
Benedict, K. S 4.3
Bergonzo, P. S 6.2
Berky, W. S 6.6
Berthold, M. P 25
Betz, T. S 8.3
Bevetskij, A. P 34
Beyerer, J. Chair Session 3 I, S 5.1, S 5.2
Biederbick, W. Project BEPE
Biwer, G. Project IRLSENS
Blanc, A. P 23
Boeker, P. P 13
Boltes, M. P 24
Bongartz, A. S 6.4
Böttger, U. S 3.4
Brand, J. P 47
Braun, H. Opening
Brehm, K. P 10
Brenneis, C. S 2.1
Breskin, A. Project ACCIS
Bretfeld, R. S 3.4
Brinker, A. P 10
Brodt, R. Project BEPE
Bronner, W. Project IRLDEX
Bunte, G. P 13, S 6.1
Burgmeier, J. Project ChipSenSiTek
Bye, R. P 39
Camtepe, A. P 39, P 52
Chevallier, E. S 6.2
Chmel, S. S 6.6
Cimander, B. S 3.1
Cohen, R. Project BEPE
Czyzewski, A. S 3.8
Dangendorf, V. Project ACCIS
Dantl, T. P 20
Degen, U. Project RETISS
Degreif, K. Project IRLDEX
Deimling, L. P 23
Dienel, H.-L. Project ESR
Dittmann, H. S 3.4
Divin, Y. P 9
Dombrowsky, W. Project ESR
Donner, A. S 4.4
Dörendahl, K. S 2.2
Dörr, A. S 6.4
Dumont, J. L. S 6.3
Duschek, F. P 14
Dyrks, T. P 28
Ehlert, S. P 20
Eilhardt, C. P 24
Eisenreich, N. P 23

Ekvall, K.	S 3.5	Hasenfuß, P.	P 47
El-Bahar, R.	Project LiveDetect3D	Havardi, I.	Project ACCIS
Elsner, P.	Chair Session 2	Hecker, T.	P 32
Ender, J.	Chair Session 6 II	Heidenreich, A.	S 1.4
Engelbach, W.	P 2	Heimbecher, F.	S 1.4
Eriksson, M.	S 7.2	Heindl, T.	P 20
Essen, H.	P 35	Held, C.	P 49
Etterer, T.	P 13	Hellenthal, M.	Keynote Session 1
Evers, D.	S 1.4	Heller, M.	P 10
Ewert, U.	P 12	Henning, J.	Project I-LOV
Feierlein, J.	S 3.6	Henrique, N.	S 1.2
Felsenstein, C.	S 4.3	Henseler, C.	Project ESR
Fischbach, K.	P 27	Hermanns, A.	S 6.7
Focke, M.	P 8	Herzog, O.	P 5, S 1.1
Friedewald, M.	Chair Session 5	Hewelt, M.	S 8.3
Friedrich, H.	S 6.6	Hillebrand, T.	P 10
Frings, S.	P 2	Hirsch, H.	S 3.4
Fuchs, F.	Project IRLDEX, Project IRLSENS	Holl, S.	P 24
Garbe, H.	Project EMSIN	Hölzer, J.	P 20
Geisler, J.	S 5.1	Höpken, M.	S 7.1
Gers, E.	S 4.2	Hops, K.	P 42
Giemulla, E.	Project ACCIS, S 3.1	Horner, G.	P 13
Görgen, M.	P 47	Hübers, H.-W.	S 3.4
Gottschalk, R.	Project BEPE	Hugger, S.	Project IRLDEX
Gräßling, W.	Chair Session 4	Hülsmann, A.	P 41
Groiselle, C.	S 6.3	Hund-Rinke, K.	S 6.5
Groth, A.	P 54	Hunger, I.	P 33
Haas, B.	P 10	Huppertz, G.	P 21
Hägelen, M.	P 35	Hürttlen, J.	P 13
Hamp, Q.	Project I-LOV	Hustinx, P.	Plenary
Hampapur, A.	Keynote Session 3 I	Hutter, A.	S 1.4
Handke, J.	P 14	Jagutzki, O.	Project ACCIS
Hannappel, M.	P 47	Jahnke, M.	S 8.2
Hantscher, S.	P 35	Jankkari, J.	S 3.7
Haring Bolívar, P.	Project LiveDetect3D	John, N.	Project ESR
Häring, I.	S 1.1	Jonuscheit, J.	S 3.1
Hars, F.	S 8.3	Juergensohn, T.	Project ACCIS

AUTHOR INDEX

Kaiser, J. C.	P 11	Krüger, J.	Keynote Session 3 II
Kallfass, I.	P 41	Kudella, P.	P 6
Kallmann, U.	S 3.1	Kühn, C.	S 6.5
Kannegieser, E.	P 48	Künzner, N.	S 3.5
Kaplan, U.	Project I-LOV	Kupi, E.	S 3.2
Kaschow, R.	S 4.2	Lacroix, J. S.	S 6.3
Katz, O.	Project ChipSenSiTek	Lang, S.	P 35
Katzir, A.	Project IRLSENS	Lange, M.	P 10
Kaufmann, S.	Project IRLSENS	Lankers, M.	P 18
Kaundinya, I.	Project RETISS	Laor, D.	Project BEPE
Kemloh, U.	P 24	Latasch, L.	P 26
Kesar, A.	Project I-LOV	Laudien, R.	P 20
Kinzer, M.	Project IRLDEX	Laurenzis, M.	S 3.3
Kirschnick, N.	S 8.4	Le Tourneur, P.	S 6.3
Kirste, L.	P 40	Lechner, S.	Keynote Session 4
Klein, G.	S 8.2	Lefesvre, I.	S 6.3
Klein, R.	S 4.1	Lemke, P.	S 3.1
Klingsch, W.	P 24	Lenz, H.	P 10
Klomfass, A.	P 5	Leonhardt, W.	S 3.4
Klüpfel, H.	P 24	Leppert, J.	P 13
Knorr, W.	S 3.3	Leßnerkraus, G.	Opening
Köble, T.	S 6.6	Leuchter, S.	P 48
Koch, M.	Project EMSIN	Leuther, A.	P 41
Koch, R.	P 22, P 49, P 50	Lev, B.	Project BEPE
Koge, M.	P 10	Ley, B.	P 47
Kolb, A.	Project LiveDetect3D	Liddle, S.	P 24
Könnecke, R.	P 23	Lindemann, C.	P 49
Konz, W.	Project IRLSENS	Löffler, T.	Project LiveDetect3D
Köplin, J.	P 42	Lombardo, N.	P 32
Kortelainen, H.	S 3.2	Lopatka, K.	S 3.8
Kotus, J.	S 3.8	Lopez-Jiménez, M. J.	S 6.3
Krabbe, M.	P 24	Loschonsky, M.	Project I-LOV
Krause, H.	S 6.1	Lutz, S.	P 8
Kretz, T.	P 24	Lützow, P.	P 15
Kretzschmar, M.	P 50	Lyatti, M.	P 9
Krieger, J.	Project RETISS	Madjar, A.	Project LiveDetect3D
Krug, R.	Opening	Magedanz, T.	P 58

Mark, D.	P 8	Piel, C.	Project ACCIS
Mayer, G.	Project RETISS	Pinchuk, R.	P 34
Mayer, J.	P 30	Pipek, V.	P 47
Mayrhofer, C.	S 2.1, S 2.2	Pistor, C.	Project EMSIN
McNeish, A.	P 20	Plaß, M.	P 22
Mertins, K.	P 54	Pohl, J.	P 30
Messerman, A.	P 37	Poppe, U.	P 9
Meurer, H.	S 6.5	Poprawe, R.	S 6.5
Mey, H.	Plenary	Portz, A.	P 24
Millon, O.	S 2.1	Pottebaum, J.	P 49
Moldt, D.	S 8.3	Prené, P.	P 7
Möller, R.	P 10	Probst, F.	P 47
Möller, S.	S 8.4	Pütz, M.	P 16, P 20
Montméat, P.	P 7	Quenum, J.	S 8.3
Mordmüller, M.	P 15	Rademacher, S.	Project IRLDEX
Mosemann, D.	P 27, P 51	Rambousky, R.	Project EMSIN
Mowbray, F.	S 5.4	Ramirez, L.	P 28
Müller, T.	S 7.1	Raskob, W.	S 4.2
Murtonen, M.	S 3.2	Raven, N.	S 6.5
Mustafic, T.	P 37	Rebahi, Y.	P 56, P 57, P 58
Nadav, B.	Project LiveDetect3D	Rehak, W.	Project ACCIS
Neuhaus, C.	P 47	Rehm, R.	P 40
Niemasz, J.	P 40	Reindl, L. M.	Project I-LOV
Nieuwenhuizen, M. S.	P 17	Reuter, C.	P 47
Nöldgen, M.	2.2	Richter, D.	Project IRLSENS
Nouak, A.	P 42	Richter, H.	S 3.4
Nowak, S.	P 24	Rickers, U.	S 4.2
Oberhagemann, D.	P 23	Riedel, W.	S 2.1, S 2.2
Orghici, R.	P 15	Ries, H.	P 20, Keynote Session 6 I
Osinov, V.	P 6	Rietz, F.	P 13
Osterloh, K.	P 12, Project ACCIS	Ringel, R.	Project BEPE
Pargmann, C.	P 14	Ringer, J.	P 13
Paul, P.	S 6.3	Risse, M.	S 6.6
Pauly, F.	P 10	Rittgen, J.	P 16, P 20
Pearce, J.	S 5.4	Rogall, O.	Project I-LOV
Peinel, G.	S 7.3	Rogers, B.	S 5.4
Peperhove, R.	Project ESR	Roller, C.	S 1.1

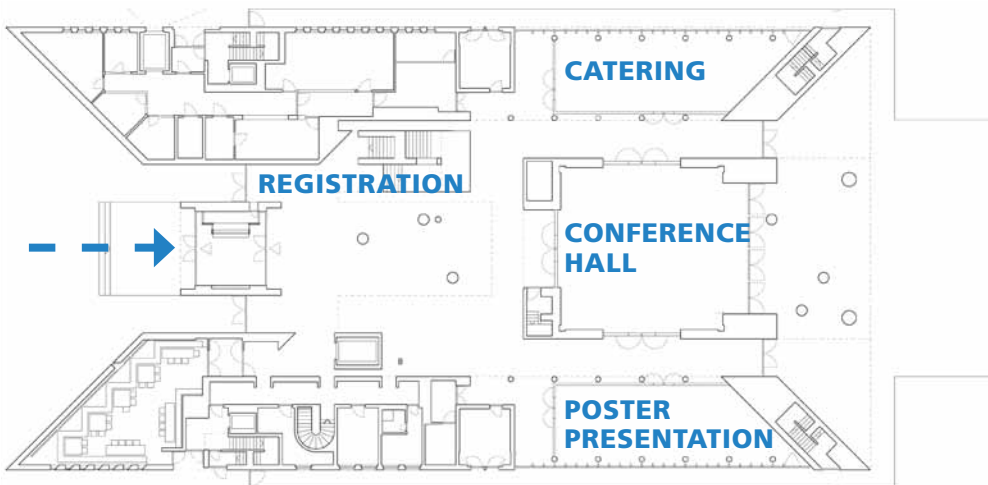
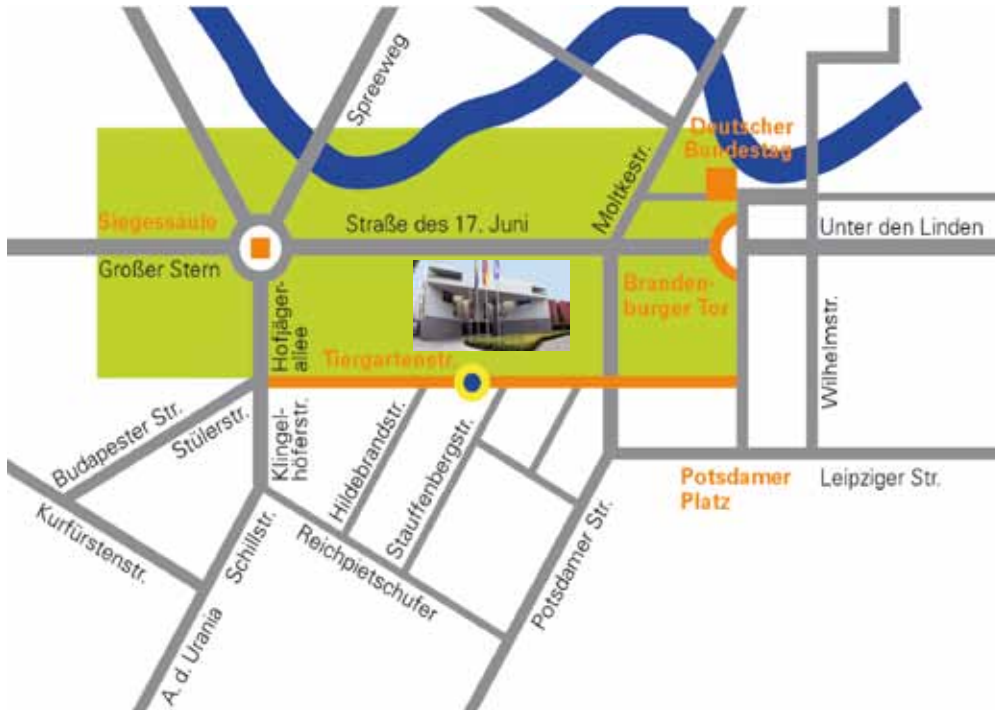
AUTHOR INDEX

- Rondeshagen, D. S 3.4
Rönnau, I. S 1.4
Rösch, R. S 3.1
Rose, T. S 7.3, P 47
Röseling, D. S 6.1
Rosen, J. Project LiveDetect3D
Rosenberg, S. Project ESR
Rosenstock, W. S 6.6
Rosenwaks, S. Project ChipSenSiTek
Roskos, H. G. S 3.1, Project LiveDetect3D
Röbber, T. P 16
Roßnagel, H. P 2
Rouhiainen, V. S 3.2
Roulston, J. Project LiveDetect3D
Rubin, J. S 5.4
Runkel, S. P 30
Rupprecht, T. P 24
Rusch, G. P 47
Rüssmeier, N. P 20
Rutz, F. P 40
Sakovich, G. P 19
Sasse, J. Project BEPE
Schade, W. Project ChipSenSiTek, P 15
Schadschneider, A. P 24
Schäfer, G. Keynote Session 8
Schall, P. P 20
Scheibner, R. P 40
Scheidung, M. S 3.4
Schempf, J. Project BEPE
Scheytt, J. C. S 3.4
Schiffel, R. S 3.4
Schillberg, S. S 6.5
Schiller, J. H. Chair Session 7
Schilling, S. Project BEPE
Schindler, S. P 20
Schippers, W. Project ChipSenSiTek
Schlechtweg, M. P 41
Schmalz, K. S 3.4
Schmid, H. P 36
Schmid, V. Keynote Session 5
Schmidt, A.-D. P 52
Schmidt, S. S 8.1
Schmitt, C. P 27, P 51
Schmitz, J. P 40
Schnee, C. P 10
Schnieder, E. S 5.3
Schnieder, L. S 5.3
Schnürer, F. Project IRLDEX, S 6.1
Schramm, E. P 20
Schubert, E. P 10
Schuchert, T. S 7.1
Schüler, W. S 3.4
Schulte-Ladbeck, R. P 16, P 20
Schultze, R. H. P 20
Schumann, O. S 6.6
Schweikert, W. Project IRLDEX
Scorsone, E. S 6.2
Seise, B. P 10
Selhorst, T. P 10
Sellke, P. S 5.4
Semenov, A. S 3.4
Seuschek, H. S 1.4
Seyboldt, C. P 10
Seyfried, A. Keynote Session 2, P 24
Sharan, Y. Project ESR
Sharfi, N. Project EMSIN
Sichert, T. P 25
Sieger, H. S 8.4
Silberberg, Y. Project ChipSenSiTek
Simon, A. Project IRLSENS
Skłarczyk, C. P 34
Sklorz, M. P 20

Smet, J.	S 3.1	von Stetten, F.	P 8
Socher, E.	Project LiveDetect3D	Vorozhtsov, A.	P 19
Sonnenberg, N.	Project EMSIN	Voss, M.	S 1.1
Sönnichsen, L.	Keynote Session 7	Wagner, T.	S 8.3
Soudani, K.	S 6.3	Waldvogel, S. R.	Keynote Session 6 II, P 15
Spöttl, T.	S 6.8	Walte, A.	P 20
Sprenger, T.	Project LiveDetect3D	Walther, M.	P 40
Stein, C.	S 5.3	Warns, T.	S 8.3
Stelte, B.	P 50	Weber, J.	P 10
Stober, R.	P 31	Wehner, M.	S 6.5
Stock, J.	Chair Session 1	Weiland, M.	S 3.3
Stolz, A.	S 2.2	Weijman, J.	P 38
Strohmeier, O.	P 8	Weissenberg, P.	Plenary
Subik, S.	P 55	Werner, H.	Project I-LOV
Tacke, M.	Chair Session 6 I	Werner, M.	S 4.4
Tessmann, A.	P 35, P 41	Wiebeck, D.	Project I-LOV
Theilmann, A.	S 8.3	Wiedenhöfer, T.	P 47
Thoma, K.	S 2.1	Wiemken, U.	Chair Session 3 II
Tolbanov, O.	P 19	Wieser, J.	P 20
Tölle, J.	S 8.2	Winkens, A.	P24
Törber, G.	P 20	Wirtz, T.	S 6.5
Tran, T.	P 55	Woda, C.	S 6.8, P 11
Tran, T. Q.	P 58	Wolf, H.	Project LiveDetect3D, S 3.1
Triantafyllidis, T.	P 6	Wörner, S.	S 3.4
Tufte, L.	P 55, S 4.2	Wrobel, N.	P 12
Ullmann, M.	Chair Session 8	Wulf, V.	P 28
Ulmer, F.	S 4.2	Württemberg, T.	Project IRLSENS
Ulrich, A.	P 20	Wüstenberg, L.	S 8.3
Urban, K.	P 9	Yang, Q. K.	Project IRLDEX
Vagts, H.	S 5.2	Yankelevich, Y.	Project I-LOV
Valet, O. K.	P 18	Zengerle, R.	P 8
van den Brink, M.	P 17	Zibuschka, J.	P 2
van Oordt, T.	P 8	Ziehm, J.	S 1.1
Vartsky, D.	Project ACCIS	Zimmermann, R.	P 16, P 20
Verbeek, L.	Project BEPE	Zinnen, A.	P 47
Viitanen, J.	S 3.7	Zscherpel, U.	P 12

VENUE

LANDESVERTRETUNG BADEN-WÜRTTEMBERG
TIERGARTENSTR. 15
10785 BERLIN, GERMANY





Bundesministerium
für Bildung
und Forschung

*This conference series is
organized by the Fraunhofer
Group for Defense and
Security and under the
patronage of the German
Federal Ministry of Education
and Research (BMBF).*

WWW.FUTURE-SECURITY.EU