Jürgen Beyerer (Ed.)

Future Security

2nd Security Research Conference Karlsruhe
2007, 12th - 14th September

Fraunhofer Defense and Security Alliance

universitätsverlag karlsruhe

Jürgen Beyerer (ed.)

Future Security

2nd Security Research Conference
2007, 12th - 14th September
Karlsruhe, Germany
Fraunhofer Verbund für Verteidigungs- und Sicherheitsforschung

Future Security

2nd Security Research Conference
2007, 12th - 14th September
Karlsruhe, Germany
Fraunhofer Verbund für Verteidigungs- und Sicherheitsforschung

Jürgen Beyerer
(ed.)

universitätsverlag karlsruhe

Impressum

Universitätsverlag Karlsruhe
c/o Universitätsbibliothek
Straße am Forum 2
D-76131 Karlsruhe
www.uvka.de

Universitätsverlag Karlsruhe 2007
Print on Demand

ISBN: 978-3-86644-147-7

Future Security

2nd Security Research Conference, Karlsruhe

Preamble Prof.Dr.-Ing. Jürgen Beyerer, Fraunhofer IITB, Karlsruhe, Germany

The terrorist attacks made all over the world since the beginning of the new millennium have thoroughly altered the perception of threat and the need for protection and security in the free and democratic countries.

Besides the acute reaction to the events by politics and the executive this resulted in strengthening and expanding security-related research as a medium and long-term response to the changed situation.

In the more recent past, also natural disasters have become more and more important. As a consequence of ongoing climate change, they will be more frequent and more intense in the future. Research into safety and security will be required urgently also in this area, especially as quite a few technologies, particularly those employed to manage and cope with natural disasters and large-scale catastrophic events, are identical with those employed in crisis management after terrorist attacks. Obviously, *security* (from dangers caused intentionally) and *safety* (from accidental hazards or those produced by negligence) should not be separated. Instead, parallels should be taken into account in research.

2007 is characterized by a large number of new national and international events about security research. *Future Security*, organized in Karlsruhe for the second time after 2006 under the patronage of the German Federal Ministry for Education and Research (BMBF), has almost become a tradition in this field. *Future Security* is organized by the Association for Defense and Security Research (VVS) of the Fraunhofer Society, which combines the joint work of various scientific disciplines on all major problems of military and civil security research.

The Fraunhofer Society early on identified security research as a strategic topic under the heading of *Security – Safety through High Tech* one of its twelve Fraunhofer Topics of Innovation.

The dynamic nature of security research, and the political decisions driving it, are influenced by a variety of interrelated issues as well as external events. As the borderlines separating internal and external security are becoming more and more blurred, as parallels and potential synergies of civil and military technologies are becoming apparent and there is a growing need to make more effective use of limited resources, the German Ministries of the Interior, for Defense, and for Education and Research developed new, common perspectives.

Special mention must be made of the national Security Research Program of the Federal Government within the framework of High Tech Strategy published by the Federal Ministry for Education and Research (BMBF) in March 2007, which envisages investments into civil security research of 123 million euro in the period between 2007 and 2009. Its holistic approach joining users, industry, and research, combining scenario-oriented ness and cross sectional topics, also incorporating humanities and social sciences from the outset, makes this program embark on new ways. In particular, it makes security and guarantees of security an explicit subject of research.

Particularly in times of open borders in Europe, security is not only a national but a transnational problem. As a consequence, it requires specific international efforts as well. The 7th European Research Framework Programme meets this challenge, devoting approx. 200 million euro annually to security research on a European level in the 2007-2013 period.

Security research is highly multidisciplinary, requiring competences in all engineering and natural sciences in order to achieve the maximum of what is possible technically, but also needing humanities and social sciences so as to ensure, from the outset, ethical and societal compatibility and acceptance.

Technical solutions of civil security problems today are still characterized very much by a bottom-up approach involving individual specialized technologies. However, there is considerable unused potential in the well-coordinated joint action of different technologies towards systems serving specific purposes, thus answering security-related questions holistically in a top-down fashion. Systems of this kind require carefully considered architectures which can be designed only on the basis of a holistic scientific coverage of the entire security complex. Embedding the security topic in a systematic scientific framework able to work out the underlying abstract principles leads to a systems theory of security, which is a current object of research.

Against the backdrop of the multidisciplinary character of security, a specific systems theory as a scientific foundation constitutes a basis on which various individual technologies can be combined into powerful systems. In this regard, a special function as integrating disciplines is accorded to computer science and information and communication technologies.

Current security research is characterized, *inter alia*, by its community in part still being in a *status nascendi*.

Politics, potential users, industry, trade, and research, with both civil and defense-related backgrounds, are engaged in intense discussions in an effort to work out common points of departure, technological perspectives and, ultimately, commercially viable solutions for present and future security challenges.

It is this background against which *Future Security* attempts to establish an international platform for security research which will further a meeting of different interests and their merger into a fruitful community. It also wants to be a forum reflecting, in an interdisciplinary way and at a high level, the state of the art without neglecting the political perspectives and boundary conditions of security research. Finally, science wants to contribute, through *Future Security*, to creating a powerful market for security technologies on the basis of promising innovations.

This year's focus in *Future Security* is on the subject of *Critical Infrastructures*. This refers to structures which are indispensable for unrestricted functioning of our society, such as transport, finance and communication infrastructures, power and water supply systems etc. A characteristic feature in highly developed countries is the high level of optimization of these infrastructures as well as their close mutual interconnections. This results in excellent performance in regular operation, but also makes for increased susceptibility to disturbances and vulnerability. Typically, in optimized systems, minor causes (specific attacks) are able to cause major effects, i.e. considerable damage. *Critical Infrastructures*, in a way, are the Achilles' heel of our society.

Coupling Critical Infrastructures, in addition, can give rise to cascade and avalanche effects not properly understood or controlled to this day.

This volume of Proceedings contains the full versions of the papers and posters of the *Second International Conference on Future Security* in the order in which they are presented.

Program Committee

- Prof. Dr. Bachem, Achim
Forschungszentrum Jülich GmbH

- Bechtold, Bernd
b.i.g. bechtold INGENIEURGESELLSCHAFT mbh

- Prof. Dr.-Ing. Beyerer, Jürgen
Fraunhofer IITB

- Dr. Boßdorf, Peter
Report Verlag GmbH

- Cumming, Adam Stewart
DSTL

- Ebner, Jürgen
Bundeskriminalamt BKA

- Prof. Dr. Eckert, Claudia
Fraunhofer SIT

- Ministerialdirigent Ellinger, Dirk
Bundesministerium der Verteidigung

- Prof. Dr.-Ing. Elsner, Peter
Fraunhofer ICT

- Dr. Fonblanc, Gilles
SNPE Energetic Materials

- Dr. rer.nat. Geisler, Jürgen
Fraunhofer IITB

- Prof. Dr. Jürgen Grosche
FGAN-FKIE

- Dr. Helmbrecht, Udo
Bundesamt für Sicherheit in der Informationstechnik

- Dr.-Ing. Heuberger, Albert
Fraunhofer IIS

- Dr. Homburg, Axel
- Hupfer, Markus
EADS Deutschland GmbH

- Dr. Klee, Christian
Diehl BGT Defence GmbH & Co.KG

- Korting, Paul
TNO Defence

- Dr. Linnenkamp, Hilmar
European Defense Agency

- Dr. Mengel, Stefan
BMBF

- Menke-Südbeck, Christa
Deutsche Bank AG

- Dr. Michael, Karsten
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

- Nehm, Kay
Generalbundesanwalt i.R.

- Dr. Orama, Olli
VTT Technical Research Center of Finland

- Dr. Östmark, Henric
FOI Swedish Defence Research Agency

- Schneiders, Franz-Josef
BMVBS

- Dr. Sieber, Alois J.
European Commission - Joint Research Centre

- Prof. Dr. Stock, Jürgen
Bundeskriminalamt BKA

- Prof. Dr. Tacke, Maurus
FGAN-FOM

- Prof. Dr. Thoma, Klaus
Fraunhofer EMI

- Dr.-Ing. Tröster, Stefan
Fraunhofer ICT

- Prof. Dr. Weimann, Günter
Fraunhofer IAF

- Dr. Wiemken, Uwe
Fraunhofer INT

Index

Session 1:
Strategic Precaution »Staying One StepAhead«
Chair: Prof. Dr.-Ing. Jürgen Beyerer, Fraunhofer Institute for Information and Data Processing

Session 2:
Detection and Assessment of Threats and Dangers
Chair: Prof. Dr. Klaus Thoma, Fraunhofer Defense and Security Alliance

Session 3 (Part I):
Prevention, Protection and Defense
Chair: Maria Theresa Blattner-Zimmermann, Federal Office for Information Security

Poster Session

Session 3 (Part II):
Prevention, Protection and Defense
Chair: Prof. Dr.-Ing. Peter Elsner, Fraunhofer Institute for Chemical Technology

Session 4:
Security Management
Chair: Dr. Stefan Mengel, Federal Ministry for Education and Research BMBF

German Hightech-Strategy – The Role of Security Research

Dr. Wolf-Dieter Lukas, Director General, Federal Ministry of Education and Research BMBF, Germany

Germany's High-Tech Strategy establishes objectives for 17 cutting-edge fields of the future. Security research is one of the 17 areas. Cooperation between the Research Ministry and the other government departments which bear responsibility for the security and security research is an integral part of this approach. Research, legislation, regulatory support, international cooperation and procurement in the area of civil security are considered to form an integrated whole. An objective of the High-tech Strategy is to increase the competitiveness of companies which contribute to security and to achieve technological leadership in specific security technologies.

Security risks have changed: even minor interference with the vital supply networks in our society can lead to breakdown despite the robust technologies used. Small terrorist or criminal groups can achieve great impact and cause considerable damage. Global mobility facilitates the spreading of hazards. Natural disasters and technical accidents can cause great secondary damage in a closely networked world. Germany is an export-oriented economy and allows the free movement of information, people and goods. With its high population density and its complex high-tech infrastructure it is particularly exposed to new threats. Energy and transport networks, the Internet and telecommunications, food supply and public health are vital for our society.

The Federal Government's Programme “Research for civil security” aims to increase civil security without limiting the freedom of citizens. The programme is not entirely focused on technology. Innovation does not only mean technological innovation but also includes innovative organizational concepts and strategies for action. Interdisciplinary projects involving the humanities and social sciences, knowledge transfer to the general public, scientific support for critical issues and transparency are the prerequisites for successful security research. In addition, the programme operates in a European context. The Federal Government will make budget funds of approximately €123 million available for that purpose in the period 2007 up to and including 2010.

The Security Research Programme consists of two programme lines: The first programme line refers to scenario-based security research. This means that research considers the needs of users from the outset. The scenarios offer a platform on which authorities and private enterprises work together as operators and suppliers of security equipment. The focus is thus not on solutions to individual problems but on suitable system innovations. The main goals of funding are: protecting and saving human lives; protecting traffic infrastructures; preventing the breakdown of supply systems; and securing commodity chains.
The second programme line is aimed at the study of generic technologies within the framework of mixed-technology networks, which are needed in many scenarios.

These networks combine the technologies for quick and reliable identification of people, for quick and mobile identification of hazardous substances, for pattern recognition and for security and rescue capacity building.

For more information see www.sicherheitsforschungsprogramm.de

More Security Through Systematically Thinking Ahead

Christian Schmidt
Parliamentary State Secretary to the Federal Minister of Defence , Germany

Germany is faced with new opportunities and new challenges in the globalised environment of the twenty-first century. New risks and threats can have a destabilising effect on Germany and its neighbours and have consequences for the security of the international community as a whole. To meet these new challenges, we must use a broad range of foreign, security, defence and development policy instruments in order to identify, prevent and resolve conflicts at an early stage. The Bundeswehr makes an important contribution to this task across its entire capability spectrum as well as in the field of defence research.

The tasks of the Bundeswehr are based on constitutional guidelines and the mission and objectives of German security and defence policy. International conflict prevention and crisis management as well as the fight against international terrorism will be the most likely tasks in the foreseeable future. They will determine the structure of the Bundeswehr and significantly influence its capabilities and equipment.

If we are to prepare our future for the challenges of more security, we require advanced capabilities in all fields of science in order to closely monitor and evaluate the national and international military research and technology environment. We need a systematically approach of thinking ahead in the field of research and technology.

At the same time, accelerated technological change and the availability of state-of-the-art means of communication in asymmetric warfare are changing the capabilities of potential state and non-state adversaries. In view of future threats, risks, technologies and other developments, the Bundeswehr must develop a network of capabilities on a joint and Bundeswehr-unified basis.

The Federal Ministry of Defence takes an interdisciplinary approach to military security research that integrates military technology, military medicine, the humanities and the social sciences. Basic research in military history and the social sciences plays an especially important role. Together with the research institutes of the Fraunhofer Gesellschaft, the Research Establishment for Applied Science, the German Aerospace Centre, and the German- French Research Institute Saint Louis, the Bundeswehr research institutes for military medicine, military technology, military history, social sciences and geosciences are working towards improving the joint capability profile of the German armed forces.

The increasing interconnection between internal and external security is reflected in interministerial security research co-operation, particularly in the reciprocal transfer of knowledge and in the development of new applications that are significant for both civilian and military use.

In the context of armaments, the complex approach to security also includes synergies that are gained from defence research and used in civilian security research. This development can be seen in the increasing integration of defence research institutes into the general research landscape in Germany and above all the growth of research networks, for example the Fraunhofer Gesellschaft. Another important example is the integration of the Federal Ministry of Defence into the interministerial Security Research Working Group, which deals with the national and EU Security Research Programme.

Our international research is based on bilateral and multilateral co-operation projects with partner countries. The Bundeswehr has concluded agreements with a number of European and non-European countries on co-operation across the entire defence research spectrum. Projects include basic research, operational applications, and joint studies. International agreements with, for example, NATO or the EU – especially through the European Defence Agency (EDA) – are contributing to an efficient exchange of ideas and experience. They help avoid a duplication of efforts, establish mutual trust for the common security and defence efforts of allies, and pool scarce financial resources.

Security research - A Fraunhofer signpost to tomorrow's markets

Prof. Dr.-Ing. Hans-Jörg Bullinger, President of the Fraunhofer-Gesellschaft, Germany

Suicide bombings, organized crime, flood disasters – the nations of the western world are experiencing new threats to their security, and are becoming increasingly aware of the fact that they are vulnerable and dependent in many ways. This is largely due to their high level of industrialization as well as the increasing complexity of today's information society and the growing networks that link it, not to mention the growing population density in urban regions. If a critical infrastructure breaks down, this can trigger a crisis, placing people and the environment at risk.

The main challenge for scientists is to improve security in our increasingly networked societies. Researchers are helping to identify and assess potentially dangerous situations at an early stage, suggesting ways of minimizing or avoiding risk, and developing robust, resistant systems. Effective security research calls for an interdisciplinary approach and voluntary sharing of information, since many technologies can be put to a variety of different uses. Consequently, civil and military research groups are now working more closely together. Germany has a sound basis for this type of collaboration, but still lacks a systematic and strategic research policy for civil security. In 2006, the German government decided to set up a cross-departmental security research program for the first time. The German Federal Ministry of Education and Research (BMBF) has set aside 123 million euros to finance the program over the next four years. National security research now also constitutes an important part of the German government's high-tech strategy. On a European level, too, the issue of security is gaining in importance, and has become a thematic area in its own right for the first time in the 7th Framework Programme. In this program, the European Union intends to invest 1.4 billion euros in security research between 2007 and 2013.

The increased need for security is only one of the reasons behind this extensive funding. The other reason is that security technology is becoming an increasingly important business area for research and industry. In Germany alone, the market was valued at 10 billion euros in 2005 – and the tendency is rising, with a worldwide growth rate of 7-8 percent.

Protecting life and limb

A sufficient supply of energy, water and food is vital to our existence, and we depend on a fully functioning infrastructure. Healthcare, telecommunications, banking systems, transportation networks and industrial plants form the basis of our society. Information technology in particular has become a virtual necessity, and it is essential to modern society that we protect it. The institutes united under the Fraunhofer Information and Communication Technology Group are working on secure architectures for information systems, new encryption techniques and reliable methods of authentication. This is the only way of ensuring that all information reaches the intended addressee safely, confidentially and without being manipulated.

In order to act quickly and efficiently in the event of a disaster, crisis management teams, rescue forces, government authorities and aid organizations all need reliable information. An efficient information and communication infrastructure can help to save lives. One example is the digital planning desk developed by researchers at the Fraunhofer Institute for Information and Data Processing IITB. The system permits a team of experts to get together to assess the general situation in the affected region and if necessary obtain detailed information on a more local scale.

The aim of the EU SHARE project (Mobile Support for Rescue Services, Integrating Multiple Modes of Interaction), which is being coordinated by the Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS, is to develop new mobile communication services for on-site rescue missions. It will not be long before the walkie-talkies, printed maps, written orders and magnet boards currently used during large-scale operations can be replaced by PDAs or tablet PCs. But rescue workers don’t always have their hands free to operate a mobile terminal. They are already sufficiently encumbered with fireproof suits when they work in burning buildings. This is where ‘wearable computing’ – computers integrated in clothing and equipment – could provide useful support. Solutions like this are being worked on by researchers at the Fraunhofer Institute for Applied Information Technology FIT in collaboration with 36 European partners as part of the wearIT@work project. An additional source of data can be provided by self-organizing ad-hoc radio networks. The idea here is for the firefighters to distribute sensors in and around the burning building. These sensors measure the temperature and the composition of the air, and transmit their data over a radio link to the control center. Such self-organizing ad-hoc radio networks are being developed by the Fraunhofer Institute for Reliability and Microintegration IZM and the Fraunhofer Institute for Integrated Circuits IIS, among others.

In order to reliably secure an area, any potential sources of danger must be recognized and analyzed at an early stage. This is possible using surveillance and identification technologies. Satellite images of critical regions, video surveillance of public spaces, aerial photographs, and radar or infrared images can help to reconnoiter and monitor a particular area. However, this calls for the development of powerful systems. Scientists at the IITB are currently working on the computer-assisted analysis of aerial and satellite images, while the ‘Facedetector’ software developed by the IIS can quickly and reliably locate specific faces in a live situation or a video recording.

Biometric recognition techniques are a modern alternative to conventional means of authentication such as keys, PINs, passwords and cards. People themselves are now the key, and can be identified by their unique, unchanging physiological features: fingerprints, voiceprints, iris pattern, facial features and handwritten signature. The Fraunhofer Institutes for Computer Graphics IGD, Production Systems and Design Technology IPK and Integrated Circuits IIS have contributed significantly towards developing such biometric systems over the past few years.

Tracking down explosives

Terrorist attacks with explosives or biological, chemical or radioactive agents represent the greatest threat of all. Researchers across the globe are developing novel systems for detecting such weapons. Many sensors are based on microelectronic circuits that emit and measure microwave, millimeter-wave or terahertz radiation. A Fraunhofer initiative has now been set up to investigate the optical stand-off detection of explosives. The objective is to develop technical solutions capable of detecting the presence of explosives on people and in vehicles even at a distance of up to 100 meters. The researchers intend to identify the explosive substances in the gas phase, for instance in the form of a plume emanating from a potential terrorist. The presence of such a plume on surfaces like clothing or door handles can be revealed with the help of various spectroscopic techniques based on infrared lasers. The key to these techniques is terahertz radiation, which lies in the range between radar and infrared. It can easily penetrate paper, clothing, brick walls, plastic and ceramics without causing harm to people. For the last several years, researchers throughout the world – including scientists at the Fraunhofer Institute for Physical Measurement Techniques IPM – have been working on new technologies for the generation of terahertz waves and their use in practical applications. The development of actual systems is still in the fledgling stages, but numerous experts already consider terahertz metrology to be an important emerging technology. Such methods would even make it possible to detect a single individual wearing an explosive belt in a crowd of people.

New materials and processes can also help to reduce the effects of an explosion. Researchers at the Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institute, EMI and the Fraunhofer Institute for Solar Energy Systems ISE are developing multi-functional glass curtain walling that can dampen the impact of an explosion, while at the same time providing thermal insulation and filtering sunlight. A new type of polymer concrete, too, can reduce the impact of bomb attacks by absorbing the energy of the explosion.

More information:
Fraunhofer Defense and Security Alliance
www.vvs.fraunhofer.de

Dutch Approach Towards Security and Society

Mr. Drs. Dick Schoof, Directorate-general for Public Safety and Security
Ministry of the Interior and Kingdom Relations / The Netherlands

National Security Stategy, The Netherlands

Threats to our security are changing and becoming ever more intertwined. Relatively minor threats can through increasing interdependencies lead to societal disruption. Answers to existing and new threats can therefore no longer be formulated and implemented by a single ministry or organisation. We need an integrated and coherent approach that can look beyond current threats. Planning and policy should no longer be primarily based on individual (known) threats, but on the extent to which overall national security is or can be threatened.

In order to realise this approach, the Cabinet has drawn up a national security[*] strategy. The aim of the strategy is to protect society and citizens within Dutch territory against internal and external threats. Our national security, however, cannot be viewed in isolation from the security of other countries, in particular those of our European partners and NATO allies. This also explains why internal security policy, which this strategy mainly deals with, and Dutch international security policy are so closely linked.

National security is jeopardized when vital interests of the Dutch state and/or society are threatened to such an extent that one can speak of – potential – societal disruption. The following vital interests have been defined: territorial security (threatened through breach of territorial integrity), economic security (undisrupted trade), ecological security (living environment), physical security (public health) and social and political stability (e.g. respect for core values such as freedom of expression).

Using the working method described in the strategy, the Cabinet will be better able to determine which threats endanger our national security and how to anticipate those threats, irrespective of their origin or nature. In addition, the method not only enables the Cabinet to make better substantiated choices in determining priorities and acting upon them, but also to view these choices in their relationship with each other.

While new, the working method makes use of existing, more sector-oriented processes; these come together in the working method, thus enriching information and insights and increasing knowledge. Use of the working method should obviously not lead to duplication of existing processes.

From 2009 onwards, the working method will be applied across the full range of national security issues. The period up to 2009 will be used to roll out the working method. The introduction in stages is described in the 2007-2008 work programme.

The working method will generate a strategic (long-term) foresight report every two years, the yearly selection of threat themes requiring in-depth analysis and a twice-a-year government-wide horizon scan of shorter-term threats. This scan will result in the report 'Threat Assessment Netherlands'. Moreover, once a year the results of the national risk assessment will be presented in the report 'Risk Assessment Netherlands'.

(*) *In this document and in the working programme, the term ‘national security’ encompasses both security and safety.*

In order to make this possible, the working method starts by analysing the threats facing the Netherlands, assessing those threats in terms of risks to the vital interests and positioning these risks vis-à-vis each other: the national risk assessment. The Cabinet will then decide which risks will be prioritised for detailed treatment in the strategic planning stage. At that stage, the method will determine which capabilities the government would require to deal with the prioritised risks and which capabilities it already possesses and/or can expect from external parties, such as the business community, social organisations and international organisations. The Cabinet will then decide whether, and if so where and how, national security must be strengthened. The political/administrative choices will then be translated into policy, legislation and concrete measures.

The development of the choices made by the Cabinet is not only in the hands of the national government. Other public authorities, the business community and social organisations also play a role. In order to enable an integral approach, all parties involved must know and respect each other's role in strengthening national security, follow a shared doctrine, align their working methods to each other and be connected to the same communication network. In 2007 the Cabinet will come up with concrete proposals for optimizing the aforementioned aspects of authority and control by the government in the area of national security.

Another essential component of the integral approach is the structural exchange of knowledge and information and alignment between the public and private parties – both in a national and an international context – who play a role in protecting national security.

As many threats to national security do not originate in our territory but can have consequences here, a purely national approach will not suffice. Countries are dependent on each other if they wish to increase their resilience.

International cooperation, both at bilateral and multilateral level, is vital for reinforcing national security. The Cabinet is going to put security topics that require an international approach on the agenda. Wherever relevant, it will work in an international context to generate the capabilities deemed necessary to withstand threats. European programmes will also be leveraged to this aim. The goal of the Cabinet is to intensify the relationships with countries that use similar working methods to guarantee national security.

UK Approach to Security and Counter-Terrorism Science and Innovation

Dr. Mark Stroud, Sector Manager for Physical Security Sector, Home Office Scientific Development Branch, UK

The Challenge

Over the last decade, the world has witnessed brutal attacks by terrorists who seek to disrupt our way of life and to harm the public. The terrorist threat is ever-changing, it is innovative and it is inventive. In order to counter it, we need to stay well ahead of the terrorists, building and improving our capacity to combat terrorism. We have invested significant resources to make sure that the best people and organisations all over the UK and beyond are working to deliver cutting-edge science and innovation to do this.

The role of security and counter-terrorism science and innovation takes two forms. The first is about *forging an environment that fosters creativity and innovation in order to generate the knowledge and technologies that can reduce the risk from terrorism*. The second is about *providing the best available scientific evidence and advice to support Government's aims*. Science and innovation provide support, both at the strategic/policy level (Government departments) and at the end-user tactical level (e.g. emergency responders).

The UK Security and Counter-Terrorism Science and Innovation Strategy

The UK Security and Counter-Terrorism Science and Innovation Strategy brings together a range of technological, economic and social sciences to counter the increasingly diverse nature of the terrorist threat, both now and in the future. The programme includes a wide spectrum of research areas, for example: detecting, mitigating, and understanding the properties of chemical, biological, radiological and nuclear (CBRN) material and explosives; biometrics; forensics; information communication technologies and social science.

We aim to optimise the benefits of science and innovation to reduce the risk from terrorism so that people can go about their business freely and with confidence. We will do this in the following four ways:

- **Expanding a cross-departmental operational analysis approach** to identifying Government's research priorities;
- **Horizon-scanning** for future threats and new scientific developments and inventions to counter such threats;
- **Working more effectively with business and academia** to ensure that research is delivered and exploited through the cultivation of a strong and innovative counter-terrorism research market;
- **Collaborating with international partners**, allowing increased sharing of knowledge and technology.

Implementing the Strategy

It is essential to work closely with end-users, academia and business to encourage innovation and creative thinking, and to support clearly articulated requirements aimed at combating both current and future threats. We aim to provide greater transparency to suppliers of Government's research priorities and engage proactively with technology developers to ensure that emerging findings are exploited effectively and where appropriate, fed into the knowledge-base of research.

We work closely with international partners to share experience and solutions to combating terrorism. The UK has developed a number of valuable forms of international cooperation, including the European Union and its member states, the United States, Australia and Canada. We are also engaging with the security research element of the European Community's Seventh Framework Programme for Research and Technological Development (FP7) which provides a valuable opportunity for security research at a European level, and offers industry, academia and research the opportunity to be part of pan-European consortia sharing knowledge, skills and expertise; and access to new business markets.

http://security.homeoffice.gov.uk/science-technology/

Homeland Security Research in the USA

Dr. Starnes Walker, Director of Research, Science & Technology Directorate, U.S. Department of Homeland Security

Introduction

The S&T Directorate's mission is to improve homeland security by providing to our customers, the operating components of DHS and state, local, tribal and territorial emergency responders and officials, state-of-the-art technology that helps them accomplish their missions. A recent review of strategy and technology requirements resulted in a shift in the Directorate's focus to a new strategic approach. This new approach, reflected in a realigned organization and research portfolio management strategy, will allow us to better identify, enable, and transition new capabilities to our customers to better protect the Nation. To that end, the S&T Directorate develops and manages an integrated program of science and technology, from basic research through technology product transition. The managers of this program are predominantly active scientists and engineers in the technical disciplines relevant to Homeland Security. They are guided by a risk-diverse, multi-tiered investment strategy based primarily on the stated needs of our customers balanced with emerging technology opportunities.

The programmatic priorities outlined in this Plan are the result of a process that is largely driven and led by our customers. A majority of the S&T Directorate's investment will be in lower-risk projects dedicated to addressing a customer-defined capability need within three years. About 10 percent of the S&T investment will consist of higher risk innovative prototypical demonstrations, which, if successful, will place advanced technology in the operating components hands much more quickly than the incremental improvements typical of most acquisition programs. About 20 percent of the S&T Directorate's investment portfolio will be in long-term, basic research conducted primarily in universities and laboratories in areas of enduring homeland security relevance that could lead to revolutionary changes in the way we approach homeland security challenges.

The S&T Directorate's long-term success is dependent on the development of our workforce and on our leadership of the homeland security research enterprise. The leadership principles and management initiatives outlined in this plan support the priority we place on hiring, retaining and motivating a quality workforce. In leading the homeland security research enterprise outside of the S&T Directorate, we are proactively engaged with universities, research institutions, government laboratories, and private industry that conduct research and development in areas important to addressing our customers' homeland security requirements.

The S&T Directorate – Aligned for Success

The Directorate's R&D functions are aligned into six technical divisions along strategic and enduring functional disciplines. This, along with additional offices, allows us to better meet the Department's strategic goals. These Divisions and disciplines for research, development, testing and evaluation (RDT&E) programs include:

Explosives
Aviation Security; Mass Transit Security; Counter MANPADS

Chemical/Biological
Chemical and Biological Countermeasure R&D; Threat Characterization; Operations;
Agro-Defense; Biological Surveillance; and Response & Recovery

Command, Control, and Interoperability (C2I)
Information Management; Information Sharing; Situational Awareness; Interoperability and Compatibility; and Cyber Security

Borders & Maritime Security
Land Borders; Maritime; and Cargo Security

Human Factors
Social-Behavioral Terrorist Intent; Human Response to Incidents; and Biometrics

Infrastructure Protection & Geophysical Science
All Hazard Critical Infrastructure Protection; Regional, State and Local

These technical Divisions are linked to three research and development investment portfolio directors in a "matrix management" structure. These three portfolio directors – Director of Research, Director of Transition, and Director of Innovation/Homeland Security Advanced Research Projects Agency (HSARPA) – provide cross-cutting coordination of their respective elements (or thrusts) of the investment strategy within the technical Divisions. Each technical Division is comprised of at least one Section Director of Research who reports to the Director of Research in addition to the Division Director so that a crosscutting focus on basic and applied research capability is maintained and leveraged, and a Section Director of Transition who reports to the Director of Transition in addition to the Division Director to help the division stay focused on technology transition. The Director of Transition coordinates within the Department to expedite technology transition and transfer to customers. The Director of Innovation/HSARPA sponsors basic and applied homeland security research to promote revolutionary changes in technologies; advance the development, testing and evaluation, and deployment of critical homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities and works with each of the Division Heads to pursue game-changing, leap-ahead technologies that will significantly lower costs and markedly improve operational capability through technology application. This cross-cutting coordination facilitates unity of effort. The matrix structure also allows the S&T Directorate to provide more comprehensive and integrated technology solutions to its customers by appropriately bringing all of the disciplines together in developing solutions.

In addition to the six Divisions and the three Directors, the realigned organization features additional offices that support a range of critical missions. These include:

The Test and Evaluation and Standards Division that works to ensure independent objective testing of technology developments by the six Divisions and across DHS and oversees standards development for the effective operation and interoperability of technology; The Office of Special Programs that coordinates highly classified projects executed by the six Divisions; The Office of Operations Analysis that supports risk analysis and manages the Homeland Security Institute studies and analysis efforts which helps form the Department's basis for risk informed decision making; and the Interagency and International Programs Divisions that facilitate government-wide science and technology coordination and provides outreach to U.S. allies.

Summary

Our Nation's advantage in science and technology is a key to securing the homeland. To ensure we fully use this competitive edge, the S&T Directorate has undertaken major organizational changes designed to break down organizational barriers and foster greater inter-reliance among innovation, research, and transition programs. The strategy is to remain customer-focused and output-oriented – empowering customers to set priorities to meet the needs of tomorrow's homeland security – while proactively pursuing technology that could offer our DHS customers revolutionary means to better secure our Nation. With this focus, we can define what we will do for our customers, how we will do it, and how we will measure success.

Most importantly, we recognize our most valuable asset is not new equipment or technology, but rather our dedicated, flexible, and agile team of knowledgeable workers. Our workforce embraces personal characteristics of integrity, diversity, challenge to the ordinary, and brings diverse skill sets to the Directorate's mission. We must therefore create a work environment in which our people are encouraged and rewarded for using initiative to anticipate and improvise to changing circumstances or sudden opportunities.

This is a culture of organizational excellence that promotes a common identity, innovation, mutual respect, accountability and teamwork to achieve efficiencies, effectiveness and operational synergies.

This strategic plan outlines the four cornerstones of our strategic approach – our organization, our people, our financial systems, and the mixture of capability- and opportunity-based content of our programs that come to bear on fulfilling our responsibilities as established by the Homeland Security Act of 2002. They are the components of a business model and a strategy that allow us to address our customers' needs and pursue technology opportunities that eventually lead to capabilities that will make our Nation safer.

Proactive Assessment of Security Threats from the Police Point of View

Prof. Dr. Jürgen Stock, Bundeskriminalamt BKA, Germany

A security strategy is a vital element of a safe future for our society. A comprehensive security strategy must combine various perspectives to form a holistic overall strategy. This calls for security research which takes different areas into consideration.

Security research is a central tool for the police in the execution of the legal mandate to fight crime. In this context, the Bundeskriminalamt has been doubly-tasked, since it is both an end user of security research and also a research institution. For many years now the Institutes of Forensic Science and Criminalistics at the BKA have been pioneers in the field of police-relevant security research in Germany.

Threat situation

For the police as end users, the demands on security research arise from the prevailing threat situation.

There is no question that the high importance attached to long-standing "conventional" areas of crime such as violent and street crime, juvenile delinquency and sexual offences remains unchanged, Also the threats posed by organisied crime (OK) are ongoing. In this way, for example, the efforts of organised crime groups to use and control parts of the economic cycle for their criminal intent, must be seen as a significant risk for a fundamental element of our free societies in Europe - a functioning economy.

International terrorism

We are furthermore faced with new, to a great extent internationally-influenced forms of crime; of prime importance here is international religiously-motivated terrorism whose dimensions go way beyond any experience or concept which we have had up to now. The Madrid and London attacks are just as much proof of this as the attempted suitcase bomb attacks on regional trains in Germany at the end of July 2006. These offences clearly show that the terrorist threat has long since reached Europe. Terrorism increasingly focuses on so-called "soft" targets with the goal of spreading fear and terror by causing as much death as possible. It acts apparently as an internationally-operating network, which, however, increasingly presents itself as a worldwide propaganda element via Internet and aligns itself with the joint ideology of Jihad.

Crime on the Internet

In addition, the Internet is bringing about changes in numerous traditional fields of crime since it is opening up both new crime opportunities as well as a variety of possibilities for anonymisation. Fraud offences and the dissemination of child pornography are pertinent examples .

Meanwhile, offences which are committed by exploiting modern information and communications technologies or which are committed against these, in short, ICT crime, are exceptionally important. Information technology developments have led to new threat forms. If, for example, some years ago malicious software came into circulation through the exchange of infected data-storage media, today this would be spread at very high speed through the Internet. Through the networking of IT systems, global epidemics are caused within next to no time, with ensuing enormous impacts which are not only of a financial nature. Among other things, these threats are heightened through the criminal usage of remote-controlled computer networks, so-called bot-networks, which are connected via the Internet. These enable attackers to misuse a large number of computers simultaneously for illegal purposes.

At the same time, the Internet opens up new dimensions for corporate and competitor espionage. Classical targets are technology and know-how-theft as well as the obtaining of market advantages through espionage in respect of public tenders, contracts, price information, the spying out of corportate data.

The overall trend indicates that Internet crime is becoming more professional and commercial in character.

Threats for critical infrastructures,

Closely connected to the use of the Internet are also possible attacks on critical infrastructures (KRITIS), the lifeline of our society. They guarantee the supply of energy, water, health and communication services and mobility. Even if no concrete information is on hand with regard to attacks in connection with critical infrastructures, it should be noted that enterprises and facilities in the critical infrastructure branch should be considered particularly threatened by terrorism. If parts of these infrastructures are misused as targets of attacks or "crime weapons", this would not only have consequences which are difficult to assess at an objective level. Also the sense of security, the basic trust which people have in functioning systems would be strongly influenced.

Critical infrastructures also encompass the financial, monetary and insurance sector. Economic and financial crime alter competition structures and impact greatly on social structures, culminating in changes to the political structures.

For this reason, the security agencies compile separate analyses for the area of critical infrastructures. The leadership is held by the Federal Ministry of the Interior. A milestone in this context is the "Basic protection concept, protection of critical infrastructures“, which was developed interdisciplinarily and published by the Federal Ministry of the Interior in September 2005.

Early detection as a basis for effective concepts

The goal of police strategies has to centre around countering the developments outlined. This involves more than just reacting. Ultimately, we can only effectively prevent crime if we manage to "get in there first" and act proactively. We have to be able to assess crime developments on a timely basis in order to prevent damaging situations even occurring.
Thus, one of the tasks of the BKA International Coordination Division (IK), established in 2005, is information analysis from a prognostic viewpoint geared towards the early detection of potential crime and threat developments.
Security research is a further rudimentary element of this approach. Research projects have to be future-oriented and able to contribute to the development of prognoses on how crime phenomena and areas of crime will develop and what new forms of crime and modi operandi we have to be prepared for.

In this context, we require future-oriented analyses and substantiated hypotheses on interactions. We have to optimise our ability to make decisions by means of research into phenomena, monitoring and research into unreported/undetected crimes. We also require reliable situation analyses and proposals for modern crime- control concepts.
This means that sociological as well as technological aspects have to be taken into account and linked.

Security research as a contributory factor for prevention

In this way, etiology, - a classical sociological field of research - can make a significant contribution towards primary prevention. Primary prevention aims at influencing the conditions under which personal and personality-related crime develops: It is imperative that we elicit and get to the bottom of the roots of criminal behaviour in order to prevent somebody from becoming a criminal. In respect of extremist crimes of any genre, it is, for example, vital to establish how radicalisation processes can be effectively countered.

Secondary prevention deals with possibilities for minimising the opportunities for committing crimes. The central question here is how crimes can be prevented with the aid of technical means or how potential perpetrators can be deterred. Examples are the preventive use of video surveillance or the fast and precise detection of security-relevant substances, e. g. explosive materials (in this last connection your attention is drawn to the Bundeskriminalamt contribution in the Poster Session Determination of the Ionization Potentials of Security Relevant Substances within the cooperative project SAFE XUV).
Furthermore, the possibilities for misuse and the interests of security should not be neglected when new technologies are being developed. An example is the booming area of information and communications technology. Vigorous

efforts were made in the development to optimize the stability of the system or the quality of transmission - on the other hand, security aspects were often neglected, indeed, the concerns of the security agencies such as surveillance possibilities were disregarded.

Networking of security research

In the long run, security research can only be successful if interconnected. This involves the economic use of available resources as well as the achievement of possible synergy effects.

In order to effectively counteract highly complex phenomena such as international terrorism, we have to research it and approach it from various perspectives, i. e. on an interdisciplinary level. This results in the necessity for intensive co-operation between the research units of the various security agencies with universities and research institutes as well as an active exchange with commercial providers of security solutions.

For the further networking and optimization of security research, depending on the form and dimension of the research required, all the necessary protagonists must be incorporated and the financial aid structures utilized.

At national level, the Federal Ministry for Education and Research has taken up and promoted the subject of security research. As well as recording the existing potential solution approaches, the results thus far have demonstrated a great national need for security research.

In a Europe which is expanding and growing together, increasing consideration has to be given across national borders when it comes to security issues. The European security research programme demonstrates that central questions are not only of a national character but, depending on the dimension of the research project, necessitate a European approach including European sponsorship.

The so-called missions Protection against terrorism and crime, Security of infrastructures and public utility facilities (KRITIS), Border guard and rebuilding security following crisis situations, within the framework of which it is intended to plan and sponsor research projects are of interest for all the member states.

From the BKA point of view, especially the mission "Protection against terrorism and crime" is of great importance. Here, potential research projects show positive approaches both at national and EU levels.

The factors which influence the demand for security research do not, however, remain static. The gathering and coordination of information in respect of the need for security research therefore has to be an ongoing process.

Civil Emergency Prevention and Response by Others than the Police: A Challenge for Europe

Non-police Danger Prevention: An Important Security Function within the EU

Ortwin Neuschwander, Vice President of European Fire Academy, Germany

In all civilized states and in the EU in particular, „the protection of its citizens is the noblest and most important responsibility of the State”.

This protection is ensured in the following ways:

- Military intervention in case of a threat from outside the borders
- Police intervention in case of a threat from within
- Intervention by fire departments, emergency management and civil protection agencies in threats of a general nature

The ways in which these prevention measures are interconnected and the relative values assigned to the individual protection agencies depend on the legal regulations of each country. My lecture will focus exclusively on threats of a general nature in the daily lives of citizens.

The nature of these threats can be manifold. The following lists some of these:

1. War and defense-related dangers
2. Terrorism
3. Break-down or disruption of the infrastructure
4. Technical or industrial hazards
5. Weather and climatological events
6. Fires
7. Road/water/air traffic hazards

The above list of potential dangers can be classified in two distinct categories and must be viewed distinctly.

I have classified the list as follows:

- **Group 1: Military Events**
    - These include areas 1 to 7 from the above list of examples; they are subject to special legal parameters
    - To deal with these challenges, states rely on the civil defense agencies which are always a part of the overall national defense system

    - The relevant power structures are generally set up in such a way to prepare for and act preventatively if given adequate preparation time

- **Group 2: Civil Events**

    - These include areas 2 to 7 from the above list of examples
    - The structure of these danger-prevention organizations varies greatly - both quantitatively and qualitatively - in terms of organization and technical capabilities
    - The power structures must be enabled to act effectively from scratch and should be able to adapt dynamically from bottom to top to disastrous events

As already mentioned I limit my lecture to the group of civil events and organize these according to the following criteria:

- Who are the actors and what advantages and disadvantages do they
- present?
- What are the respective management structures?
- What research challenges do they present?
- What do we want from the EU?

Who are the actors and what advantages and disadvantages do they present?

In case of a civil disaster, local or communal bodies are primarily responsible; they, in turn, rely on aid organizations

- Professional Fire Departments
    - Within the entire EU, these generally exist in cities with more than 100.000.
    - Advantages: Optimally trained specialists, deployable instantly (approx. 1-2 minutes); they are familiar with their section of the city. In many states, they also are responsible for rescue and medical responses.
    - Disadvantages: For financial reasons, the team size is limited and, therefore, they can be deployed for quick and short responses only. For longer lasting deployments, the entire department must be activated

- Volunteer Fire Departments

    - There is a great disparity within the EU as to their existence, ranging from 0 to 100 %. In German-speaking states or regions, historically, they represent 90 to 100 %. Concerted efforts are under way to build up the system of volunteer firefighting in areas with few or no such systems.
    - Advantages: In a very short time (4 – 10 minutes in Germany), a good number of specially-trained citizens is available, who possess optimal knowledge of the place and social make-up in their assigned area.

Because of the heterogeneous background of these firefighters, the state has complete and free access to a wide spectrum of expertise, from skilled worker to professor.
  - Disadvantage: Because of social and occupational changes, fewer people will in future be able to provide these services

- Emergency Medical Services
  - e.g., the Red Cross, the Red Crescent, the Maltese Emergency Services, et al. are represented in various forms and numbers within the EU. They are available on request.
  - Advantage: Highly motivated people with a pronounced social conscience
  - Disadvantages: The same as with volunteer fire departments

- Civil Defense Units
  - Based on and structured according to military requirements. Subject to national government organizations. Units can be deployed outside the borders as well.
  - Advantages: Tightly organized specialists; as they are usually integrated into military organizations, they are well suited for long term deployment.
  - Disadvantages: The necessary manpower is usually not available immediately. State interests always have precedence over regional interests as far as deployment of units.

- Military
  - Available within the framework of its capabilities and legal circumstances
  - Advantages: A wide spectrum of competencies; tightly organized and deployable long-term
  - Disadvantages: Proportionate lead-time; military deployment always has precedence over civilian deployment

- Police
  - In the scenarios under discussion, the police are concerned with the policing of the situation and can, therefore, play only a tangential role. Discussion of advantages and disadvantages is superfluous here.

Examples of Management Structures

The management structures are based on and structured according to legal requirements. Since civil disasters, as a rule, occur unexpectedly in one, multiple or large-scale locations, the local powers are called upon to initiate the appropriate responses with the means at their disposal. The following priorities should always be maintained: rescue of humans and animals, salvaging of material assets. Safeguarding of public life should also be an important consideration.

At the same time, command channels must be established at the mid-and upper levels, depending on the nature of the disaster. Initially, this means that actions at the mid-and upper levels will lag behind; in case of a break-down of the communication infrastructure, this could present a serious problem.

Important Conclusions:

- Management structures must be set up in such a way that they can respond with optimal efficiency to hard-to-predict deployment situations. Management training
- Leaders at the various levels must know each other and build a climate of mutual trust over a long period of time
- Deployment planning for the various and sometimes unforeseen events as well as continuous updating of response strategies
- Establish and train back-up strategies in case of a collapse of modern technology in extreme case scenarios.
- Always be aware of the fact that volunteers should be motivated not ordered to do things.
- Management positions at all levels must be at least double-staffed.

Research Challenges

The example of military research shows how important it is that the future user, e.g. the military, be able very early on to formulate his requirements.

As I have tried to show, in the civilian sector, the real benefactor of this is difficult to identify. It is successful only when “lighthouse projects” are initiated, and are then adopted by many other users/clients.

The following could serve as examples:

- Adapt the advanced knowledge of the military to civilian areas
- Develop motivation-and solution models to help motivate people for public service or keep them motivated to continue to perform the service
- Establish planning models to preplan and train various scenarios
- Establish and develop preventative measures
- Develop models to enlighten politics that a successful civilian disaster prevention not only protects public property but is becoming an increasingly important economic factor

What Do We Want from the EU?

Europe must create unified security standards to be able to guarantee the optimal protection of its citizens

ΕΦΑ

www.europeanfireacademy.eu

Thwarted, failed and successful plots by Muslim extremists in the European Union

Prof. Dr. Rob de Wijk
Director of the The Hague Centre for Strategic Studies (HCSS) and professor of international relations and strategic studies,

Introduction

The attacks of in New York and Washington September 11, 2001 led the European Union (EU) to approve a common European policy to combat terrorism. This Plan of Action was supplemented with additional measures in the aftermath of the terrorist attacks in Madrid on 11 March 2004. The speed with which the policies were approved suggests that they were not founded on detailed analyses of the actual threat in Europe. It seemed as if the Madrid and London bombings were the archetypical terrorist acts in the European Union. Research by HCSS on dozens discovered, failed and successful plots by Muslim extremists from 1994 to 2007 reveals the true nature of the threat to the EU-member states. The findings shed new light on the intentions and modus operandi of extremists. Finally, the large number of foiled plots suggests that contrary to public belief intelligence services do their work better than commonly presumed. The main findings are summarized below:

During the mid-1990s the threat became manifest

Until 1994 most acts of terrorism were related to the Israeli – Palestinian conflict. The first plot linked to the international *salafi jihad*, an attempt to crash a plane into the Eiffel Tower in Paris in 1994, proved a watershed. This plot symbolised an important shift among Sunni Muslims. Until then, suicide attacks were perpetratd by Shiites. Yet in that period the Sunni jihad was extended from the Arabic peninsula to the Western world. The deployment of American troops on the Arabic peninsula during the first Gulf War was one of its main causes.

All but one plot until 9/11 was aimed at targets in France and linked to the Algerian Groupe Islamiste Armee (GIA) and its later splinter movement the Groupe Salafiste pour la Prédication et le Combat (GSPC). After 9/11 the number of terrorist incidents rose sharply. No less than 34 out of the 43 foiled plots were discovered after September 11, 2001, while all major successful and failed plots took place after that date. In particular 2004 shows a significant number of attacks (hoeveel?). One explanation for the large number of plots in 2004 is the mobilising effect of the successful 9/11 attacks. As did the interventions in Afghanistan and Iraq following

9/11. Furthermore, extremists may well believe that terrorism pays. After the Madrid bombings of March 11, 2004, Spain withdrew its forces from Iraq. By the end of 2004 the Philippines, the Dominican Republic, Honduras and Nicaragua withdrew their troops as well.

The rise in the number of plots and other incidents in 2004 cannot be attributed to the success of 9/11 alone, but also has to do with the skilful manipulation and exploitation of these and other attacks by the leaders of the international jihad. There is a clear correlation between messages from the (spiritual) leadership and the rise of terrorist incidents. Based on the proliferation of messages and intelligence in 2003 Europol concluded that the United Kingdom would be a priority target. It is substantiated by our research that the United Kingdom did become so.

Some countries run high risks

Almost all plots were discovered in Western European countries with a large Muslim minority (France, Italy, The Netherlands, Spain and the UK). Moreover, extremists were especially active in states with activist, pro-American foreign policies offering active support of the war on terrorism, including the US-led interventions in Afghanistan and Iraq. In other words, it seems there is a correlation between plots, foreign policy and the existence of a Muslim minority.

Targeting: strategically weak, tactically strong

The plots reveal two equally sized categories of targets. The first category includes targets symbolising a country’s political, military and economic power. The second category is composed of soft targets, including shopping malls and markets, cruise ships, entertainment facilities, sporting events, and groups of individuals. A subcategory consists of means of transport (trains, busses, and aircraft). This subcategory comprises 25 percent of the total number of failed and successful plots. Attacks on transportation systems seem to be the easiest and surest way to kill a lot of people. People are confined in small spaces, there is no easy exit and the attack creates chaos and destruction while rescue operations are difficult to carry out. One would expect extremists to target critical infrastructure. However, we found only one example, i.e. the attempted poisoning of a drinking water system in Rome. The economic base of a country also appears to be an important target. But we could only find two plots related to this type of attack. Among the few examples of economic targets was the plan by one of the Hofstad plotters in the Netherlands to attack a nuclear power plant.

Modus operandi: balancing effect against success

Extremists look for realistic targets. For example, after the 7/7 bombings, the British Transport Police and the Metropolian Police Service were on constant alert, so that the London plotters of 21 July 2005 evaded rush hour. An important finding is that extremists trade effect for success. They dream of dramatic targets, but end up planning for attacks on realistic targets.

For this reasons extremists rely on proven techniques. Most plots seem to require suicide attacks. The use of well-known and proven techniques such as car bombs and rucksack bombs also underscores the conclusion that plotters trade effect for success. Copycatting is common. All successful and failed plots involved multiple, synchronised attacks on transport systems. Multiple attacks, such as the Madrid and London bombings, are spectacular, have a higher chance of success and will result in much more damage than a single bomb and, consequently, will also create more chaos.

Finally, extremists generally use improvised weapons to decrease the chances of being caught. Consequently, most plots required little more than a few thousand euros. The London bombings cost approximately 8,000 pounds, a mere 2,000 pounds per terrorist.

Dreaming of catastrophic terrorism: the CBRN threat

Extremists find it technically and logistically difficult to plan and execute catastrophic attacks. Usually, they look for realistic targets and ultimately trade effect for success. We were surprised to find that approximately 25 percent of all plots involved attempts to use CBRN weapons. Better known examples are the attempt to poison the drinking water system of the U.S. embassy in Rome and the arrest in January 2003 of Islamic militants who may have been planning to poison the food supply of a British military base with ricin. In June 2006 a chemical bomb plot was foiled in the United Kingdom. One of the most interesting cases, however, is a plot discovered in 2004 involving an attempt to buy a nuclear device.

Conclusion

Some 50 foiled, failed and successful plots reveal an unpredictable and diverse threat by international and homegrown extremists. Extremists are willing to give up spectacular ideas if the chance of the successful execution of a plot then increases. Nevertheless, they will keep on dreaming up, and aiming for spectacular attacks. They will return to grand ideas, possibly with CBRN weapons. The threat of these weapons was much larger than expected. In short: catastrophic attacks cannot be ruled out for the future. The threat is complex and unpredictable, meaning that there is no magical solution. Intelligence is therefore the key to any successful antiterrorist strategy.

Risk Assessment and Avoidance Strategies of Terrorist Threats from an Insurance Point of View

Dr. Walter Tesarczyk (Directorate Allianz Insurance AG) Germany

The devastating attacks on the World Trade Center in New York and the Pentagon in Washington on 11 September 2001 demonstrated that terrorism risk has become virtually immeasurable in terms of both the severity and frequency of exposure. The new scope and dimensions of terrorism present a tremendous and lasting threat that has not changed significantly since the attacks and therefore has to be taken into account in the context of risk management. Both the regulatory framework and quantitative as well as qualitative characteristics of the terror risk have to be considered. The insurance industry can support this endeavour and offer financial protection within its capacity of coverage as well as help with questions regarding risk financing.

I. Regulatory Framework

Depending on the legal form of a company various risk assessment obligations have to be followed to identify and manage those risks that pose a threat to the existence of the company. The board of management of a public listed company is obliged to take appropriate measures, in particular to install a monitoring system (§9 Abs. 2 AktG). Details on the individual risk assessment obligations according to KonTraG can be found in the „Ausarbeitung des Prüfungsstandards des Instituts der deutschen Wirtschaftprüfer IDW PS 340“.

II. Qualitative Characteristics

Within a risk management framework the risk through terrorism and criminal acts has to be considered in its own right. An analysis of the specific risk a company faces can show whether and to which extent there is a threat through terrorism. In the commercially available fire policies these days the risk through terrorism is always excluded, it therefore also has to be analysed whether separate cover for terrorism is required. In this context it has to be considered whether such an event is so unlikely that market risks or other risks that cannot be insured are so dominant in relation to the terror risk that the cover against terrorism would not result in a significantly different risk exposure of the company as a whole.

It is also of interest whether and to what extent a company is free in its decisions or whether the evaluation through third parties has to be considered. The following criteria can be helpful when evaluating the above mentioned issues.

II. 1. Regional Characteristics

Is one of the risks within an urban conglomeration? Is one of the risks close to a flight corridor or a railway station? Is one of the risks in direct proximity to a secular or religious status symbol? Is one of the risks close to (domestic or foreign) governmental institutions?

II. 2. Risk increasing Criteria

Does the company itself represent a status symbol of western values? Could products the company manufactures or sells be the reason for terror attacks? Could stored substances cause spectacular damages through terror? Are there operational sites accessible to the public where access is not controlled? Could exports or cooperations cause terrorist activities? Could the ownership structure cause terrorist activities?

II. 3. Outside Influences

Do equity holders or lenders require insurance cover against terror? Is cover against terror customary within the industry?

III. Quantitative Characteristics

III. 1. Possible Maximum Loss

An important indication when estimating the possible maximum damage through terrorism could be the PML (probable maximum loss) which is determined by the fire insurer for his own risk management. The PML indicates the maximum loss that has to be expected when a fire spreads to the largest possible extent within an insured object.

The PML estimate of the insurer is however only a starting point for the determination of the maximum loss through terror and has to be adjusted where required for the following reasons:

1) The insurer’s PML is based on an accidental loss event where the loss-reducing measures of the insured take effect or at least they are not deliberately suspended. It therefore has to be assessed what extent a deliberately increased loss could take.

2) The PML is a measure for the insurer’s internal use only and does in no way affect the extent of the insurance cover. If the PML is estimated incorrectly this can result in insufficient reinsurance cover which only affects the insurer and not the insured. If however the possible maximum loss through terrorism is estimated incorrectly and consequently insufficient insurance cover is purchased this would be to the insured’s detriment.

3) Finally it has to be considered that a terror attack can have indirect consequential damage.

III. 2. Ratio of possible maximum loss to equity capital

The extent of the terror risk does not only depend on the maximum possible loss but also on the ratio of the latter to the company’s equity capital. The business continuity of a company with wide spread risks is less at danger than one with a large risk accumulation representing a large part of the equity. Companies where the operational sites are widely spread are less susceptible to business interruption through terror than companies where one central operational unit is critical to business continuity.

IV. Assessment

The board of management has to decide based on a thorough consideration of all surrounding factors which level of protection and risk transfer is appropriate. If assessment of all quantitative criteria of the terror risk shows that a maximum loss together with possible consequential losses could cause a shortage of equity the terror risk should be classified as a threat to the existence of the business. In this case insurance should be sought, even if the likelihood of occurrence of such an event is considered low.

V. Insurance cover

Terror coverage through Public-private-partnerships is increasingly becoming an integral part of economic policy in many western countries. Such coverage solutions exist in the US, in Great Britain, in France, Spain and in the Netherlands. In Germany the EXTREMUS Versicherungs-AG currently offers terror coverage with public support where the state provides a subordinate commitment on top of privately supplied capacity. This possibility of coverage exists for policies with a sum insured over € 25 Mio. For smaller risks coverage can normally be bought as part of the fire policy.

It is permanently discussed and re-evaluated whether coverage solutions with public support should be provided. Where such models don’t exist they failed because of the required high level of private contribution.

For the portfolio of the insurers the enormous loss potentials also pose a threat therefore the coverage that is given has to be limited. Primary insurers are however anxious to provide wherever possible extensive coverages and solutions. The joint assessment and determination of the exposure and related indemnity limit is key in order to sensibly limit both the premium for the insured and the exposure for the insurance.

Air-to-ground surveillance, a key capability for a secure Europe

Bob Moll, (Business Manager Space & Security, National Aerospace Laboratory NLR), The Netherlands

Abstract

The European Commission has addressed security as a dedicated theme under its 7th Framework Program. The priorities for security research have been outlined in the work programme (ref. [1]), which include the missions security of citizens, security of infrastructures & utilities, intelligent surveillance, enhancing border security, restoring security & safety in case of a crisis. These priorities reflect the shortfalls of today's state-of-the-art security systems, both for phases of preparedness as well as for response and recovery. A situational awareness and assessment (surveillance) function is needed in all these phases. In order to enhance security surveillance technology in these priority areas, development of adequate information supply together with analysis and dissemination tools are required to provide situational awareness. Air-to-ground surveillance systems are just a subset of possible contributors, however, have unique properties that complement and enhance alternative sources.

Application requirements

Security applications for surveillance systems (not just air-to-ground surveillance) include, but are not limited to

- border surveillance
- crisis management (natural, industrial disasters)
- special force operations, fight against terrorism
- crowd control (sports events, festivities, conferences of heads of state)
- VIP security

These applications can be characterised as

- joint (multi-agency)
- limited predictable (ad hoc, improvisation)
- dynamic and quick response (high operational tempo, critical time from deployment to required situational awareness)
- complex (many players and stakeholders)

What these applications have in common is a need to ***acquire and share information on the area of interest across all operational***

levels. Many different sensors and sources provide – at a high rate – data and information which need to be analysed and condensed into ***comprehensive and actionable information***. These sources range from mapping agencies, first responders in the field giving oral reports, ground based / vehicle mounted camera systems, police helicopters etc. These sources are selected based on their specific contribution to a shared situational awareness.

Quality / selection criteria for these sources are:

- reliability, accuracy, completeness
- relevance
- timeliness, update rate, currency, endurance
- accessibility, availability
- interoperability, integration
- spatial coverage
- resolution, spatial and spectral (for geo-spatial information)

The ***specific value of geo-spatial information lies in the reference grid and context*** that it provides for fusion with, analysis and visualisation of other information. Imagery produced by air-to-ground surveillance systems provides a bird's eye (over)view in a natural and easily understandable format.

In order to effectively and efficiently run security operations, a common operational picture is essential for the decision-makers and end users.

Common Operation Picture (COP)

The Common Operational Picture is a term widely used within the military domain. It has been defined in many ways. The first definition below addresses the information contained in a COP, the second addresses the joint, multi-service and interoperability aspects of the COP (ref. [2]).

1. The common operational picture is a distributed data processing and exchange environment for developing a dynamic database of objects, allowing each user to filter and contribute to this database, according to the user's area of responsibility and command role. ***The common operational picture provides the integrated capability to direct the collection, receive, correlate, and display a common tactical picture, including planning applications and the regenerated overlays and projections*** (i.e., force position projections). Overlays and projections may include location of friendly, hostile, and neutral units, assets, and reference points as well as data collection requirements and directives. The

common operational picture may include information relevant to the tactical and strategic level of command. This includes, but is not limited to, any geographically oriented data, planning data, intelligence (including imagery overlays), reconnaissance data, environmental, predictions of nuclear, biological, and chemical fallout.

2. A ***single identical display of relevant information shared by more than one command***. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness.

Current information sources

Today, much information is collected and used by the security forces on the street / field: oral and written reports, information provided by mapping agencies, force tracking data, ground based cameras etc. In addition, manned airborne platforms (e.g. police helicopters) and satellites provide imagery data. In many cases, these ways of collection of information are not adequate, because

- the object under observation is inaccessible (out of sight, in hazardous environment (fire, toxic gases ...))
- the acquired data is of insufficient quality / resolution
- the information collected is fragmented and does not provide the required overview for the operation
- the information is not provided in time or not sustained in order to be used for coordination of the operation
- it is hard to direct the information sources as to what information is needed where and when
- there is limited capability for analysis and integration of sensor data into actionable information

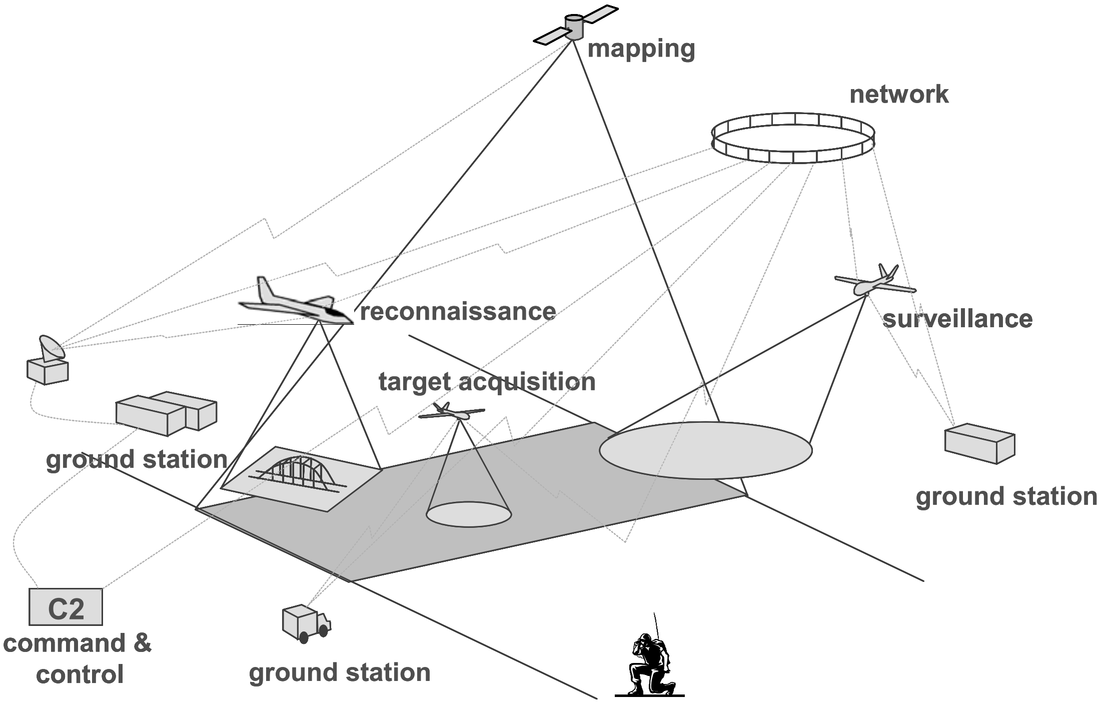


Figure 1. Functions provided by an integrated air-to-ground surveillance system

Geo-spatial information – e.g. maps and imagery – provides essential information and at the same time provides a reference grid, context and is an important carrier for other data sources. ***Commonly used geo-spatial information*** (maps of various types, archive imagery from satellites or aircraft, information contained in databases / geographic information systems) ***falls short on quality criteria: relevance, currency, endurance and spatial resolution***.

Air-to-ground surveillance, a key capability for a secure Europe

Figure 2. Long endurance UAV, 35m wing span

Air-to-ground surveillance systems can fill the capability gap as addressed above. The quality of imaging sensors for airborne and space borne platforms continuously improves. An even more significant development is the potential of unmanned aerial vehicles (UAV's) carrying those imaging sensors. For maritime and border surveillance, loitering large UAV's can provide a ***long endurance surveillance capability over wide areas***. For urban or local crisis management applications, the small UAV's can provide a ***flexible and rapidly deployable surveillance capability***. When fitted with state-of-the-art imaging and video sensors, combined with real-time processing technologies, UAV systems contribute to the common operational picture.

Essential, as for all contributions, is seamless interconnectivity and interoperability with existing security management systems in use. After all, the need is for ***shared*** situational awareness resulting from a ***common*** operational picture.

**Figure 3.
Rapidly deployable UAV, 5m wing span**

**Figure 4.
Shoulder launched UAV, 2,4m wing span**

References

[1]. Cordis website
http://cordis.europa.eu/security

[2]. Defense Technical Information Center (DTIC) website
http://www.dtic.mil/cjcs_directives/cdata/unlimit/3151_01.pdf

Technology for Intelligence, Surveillance, and Reconnaissance of Terrorists (ISRTA): From Interagency Collaboration to a protective Sensor Suite

Dr. Kay Pixius (The Federal Office of Defense Technology and Procurement BWB), Germany

Abstract

Underneath the umbrella of NATO's Programme of Work „Defence Against Terrorism (DAT)", Germany is the Lead Nation supported by the United States of America for „Technology for Intelligence, Surveillance, Reconnaissance, and Target Acquisition of Terrorists (ISRTA) ".

In fulfilling this mandate, a three-fold approach is followed comprising an interagency, cross-border effort against hijacked airplanes in Europe (denominated as "Information Protector"), contributions to NATO manoeuvres covering DAT scenarios, and a challenging "ISR Tech Demo", which aims at merging modern sensor technologies and data fusion methodologies to facilitate force protection and protection of a critical infrastructure, i.e. a harbour and/or a field camp.

The emphasis is on organisational and human factors aspects of the "Information Protector" effort, and technological challenges of the "ISR Tech Demo" effort, as both efforts have a strong relationship to the civil security domain.

It is concluded that doctrines and technologies applied for protection issues in the military are beneficial for civil organizations devoted to security assets.

NATO's PoW DAT

At their Istanbul summit in 2004 the Alliance approved the Programme of Work (PoW) Defense against Terrorism (DAT), which was prepared by NATO's Conference of National Armaments Directors.

The Defence Against Terrorism (DAT) Programme of Work is focused on the following ten items (lead nation in [brackets]):

1. Protection of large-body aircraft against man-portable air defence systems [GBR]
2. Protection of harbours and ports [ITA]
3. Protection of helicopters from rocket-propelled grenades [BGR]
4. Countering improvised explosive devices [ESP]
5. Precision air drop technology for special operations forces [USA]
6. Detection, protection and defeat of CBRN weapons [FRA]
7. Technology for intelligence, reconnaissance, surveillance and target acquisition of terrorists [DEU]
8. Explosive ordnance disposal and consequence management [SVK]
9. Defence against mortar attacks [NLD]
10. Critical infrastructure protection [BEL]

The PoW DAT is part of an enhanced set of measures to strengthen the Alliance's contribution to the fight against terrorism.

Within the scope of the PoW DAT is to develop new, cutting-edge technologies to protect troops and civilians against terrorist attacks. These technologies are aimed at preventing the kinds of attacks perpetrated by terrorists, such as suicide attacks with improvised explosive devices, rocket attacks against aircraft among others. Following findings of a NATO nations' assessment in early 2007, technologies of intelligence, surveillance, reconnaissance, and target acquisition (ISRTA) are regarded crucial to contribute and promote several of the other PoW DAT items.

Germany, supported by the United States of America as well as NATO's JISRCG[1], has taken the lead on item 7.

A threefold approach

The approach for item 7 pursue

1. the mutual support with NATO's JISRCG DAT efforts,
2. a contribution to air policing and security, and

[1] JISRCG: Joint Intelligence, Surveillance, Reconnaissance Capability Group

3. a technology demonstration for protection of objects and installations.

This set of activities is referred to as the threefold approach; while JISRCG's DAT activities have matured in the meantime from the R&D domain (and are reported elsewhere [1]), air policing and the technology demonstration reflect the German Federal Ministry of Defence effort to contribute to security issues within the given political and legal mandate.

"Information Protector": a means against Renegade

Following the "Weißbuch" [2], the Armed Forces' role in the concert of security authorities to provide protection to the public as well as to installations is gaining importance.

One important player within this concert is the national command center for air security (NFLZ SiLuRa). The „Information Protector 06" (IP 06) effort aimed at interagency collaboration with participation of three Federal ministries.

"ISR Tech Demo 2008": Technological Challenges

Based on a near-realistic scenario of the protection of a harbour as a critical infrastructure for the navy as well as for civil security authorities, the German Armed Forces' are presently planning for a technology demonstration in mid 2008.

The idea is to bring a set of "ISR-technologies" in the scene, and to combine and display the information provided by those sensors in a manner allowing for a quick analysis of the scene and – in the case of an incident – to allow for a rapid decision on potential and appropriate reactions.

The bunch of technologies to be investigated and to be demonstrated range from airborne (e.g. balloon and low-cost UAV) optical and/or IR-sensors to highly-sophisticated IR sensors mounted on protected vehicles. Besides, a self-organizing network with fixed optical/IR-sensors is used to perform area surveillance.

With respect to access control to the area of interest, most modern sensors in the mm-wavelength region and chemical sensors specialised on detecting explosives will be brought to the setting.

In order to provide an aide to the decision maker, it is relevant to bring all information in a concise way to attention. For this, a digital table technology developed by the Fraunhofer Institute IITB at Karlsruhe, is used.

Potential Synergies and Conclusions

From an organisational point of view, the “Information Protector” project with its approach to closely co-work among different national authorities by sharing information and by mutually to support the decision process in one location at the same time, can serve as a template for security related decision/ command centres.

From a more technical aspect, some of the technologies to be used for the “ISR Tech Demo 08” should find its way on the commercial market thus being available also for other stakeholders responsible for security matters. This holds especially true for mmW-radiometry technologies as well as for chemical sensors for explosives: these technologies seem appropriated also for the use by police and/or border control personnel.

For the time being, strengthening R&D efforts by collaboration of different stakeholders may serve to foster the market fielding of those technologies.

References

[1] http://www.nato.int/issues/dat/index.html

[2] http://www.weissbuch.de

[3] http://www.auswaertiges-amt.de/diplo/de/Aussenpolitik/FriedenSicherheit/Terrorismusbekaempfung/TerrorismusbekaempfungNATO.html

Urgent Need for Standards

Dr. habil. Alois J. Sieber, acting Director
Institute for the Protection and Security of the Citizen
Directorate General Joint Research Centre,
European Commission"
Chairman of the CEN BT Working Group "Protection and Security of the Citizen

Via Enrico Fermi 1
I-21020 Ispra (VA)

Abstract

The Competitive Council of the EU addressed in December 2006 the issue of the urgent need to reform the standardisation system in Europe. One of the conclusions was that the current standardisation system has to adapt to the needs of fast-moving markets, especially, in services and high-technology products. Further on the Council recommends to analysing the role of standardisation in research and new fields of technology.

An area where standardization is urgently required due to its societal relevance and pressing needs is security. In its advice to the EU on the implementation of a European security research program, the European Security Advisory Board (ESRAB) identifies as one of the five enabling areas standardisation. Efforts in the process of standardization for a secure Europe within a secure world are therefore of strategic importance. They will not only support the mandates of the EU in establishing an area of freedom, security and justice. At the same time these efforts will strengthen the industrial and market situation of European companies in the security and defence field.

CEN, one of the three standardisation entities in Europe, launched in 2004, a working Group BT WG 161 with the title "Protection and Security of the Citizen". The aim of this WG is to focus on needs for standards, standard-like documents, procedures, codes of practice and recommendations. It constitutes a powerful network of CEN Members, EC DGs (JLS, ENTR, ENV, RTD, JRC, INFSO, TREN), ISO/CS, Europol, the NATO standardisation body NSA, CLC, ETSI, EU Council, European Defence Agency, liaison ANSI HSSP and industry.

This WG started by defining the following definition of security:
"Security is the condition (perceived or confirmed) of an individual, a community, an organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such

as criminal activity, terrorism or other deliberate or hostile acts, and disasters (natural and man-made)".

This WG established a number of Expert Groups in which the specific needs for standards are identified and necessary processes are launched. At present the areas of investigation are:

- Integrated Border Management
- CBRN (Chem., Bio., Radio., Nuclear) incidents
- Critical infrastructure - Building and Construction
- Critical infrastructure - Energy supply
- Supply Chain Security
- Security of Water Supply
- Defence against terrorism
- Emergency services
- Reduction of crime risks in products and services

The presentation will focus on the urgent needs for standards in particular for critical infrastructure with an emphasis on networked infrastructure where IT is one crucial component.

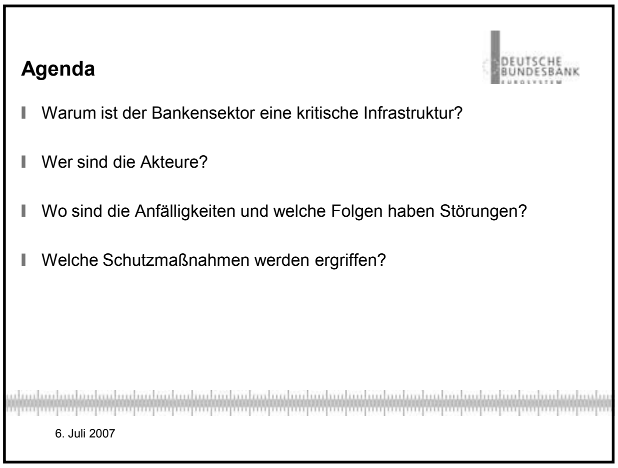
Information and communication technologies are being pervasively deployed by industry, with increasing exchange of data between production and administrative systems, remote access to installations, interconnections among companies, and services offered through public and private networks. In this panorama, cybersecurity gains a fundamental role, not considered until now. Cybersecurity of industrial installations is now a relevant issue for national security, and a potential key competitive factor in international markets. There is a need to adapt existing standards and to develop new ones taken cybersecurity into full consideration in the context of other existing regulation and standards (e.g. those related to safety and environmental conditions). Security standards are necessary for improving the protection of critical assets, developing a market of security products and services, and for spreading best practices across industry.

Protection of Critical Financial Infrastructures

Günter Jost (Deutsche Bundesbank, Head of the Security and Crisis Management Group, Germany

Schutz Kritischer Infrastrukturen im Bankenbereich

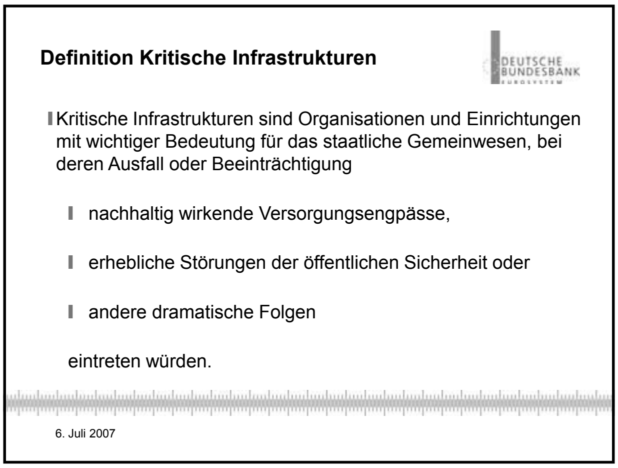
6. Juli 2007



Agenda

- Warum ist der Bankensektor eine kritische Infrastruktur?
- Wer sind die Akteure?
- Wo sind die Anfälligkeiten und welche Folgen haben Störungen?
- Welche Schutzmaßnahmen werden ergriffen?

6. Juli 2007

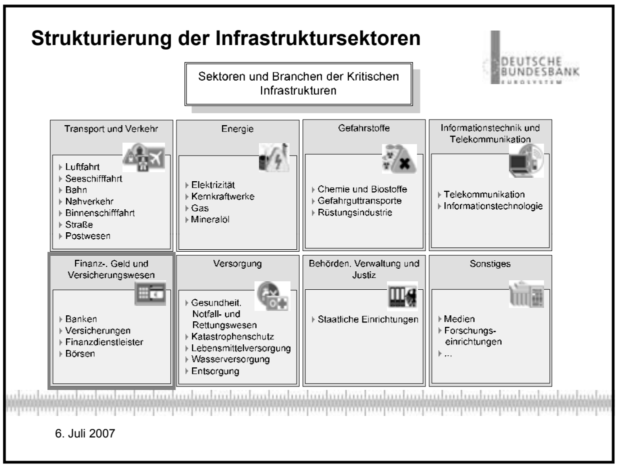


Definition Kritische Infrastrukturen

- Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung
  - nachhaltig wirkende Versorgungsengpässe,
  - erhebliche Störungen der öffentlichen Sicherheit oder
  - andere dramatische Folgen

eintreten würden.

6. Juli 2007

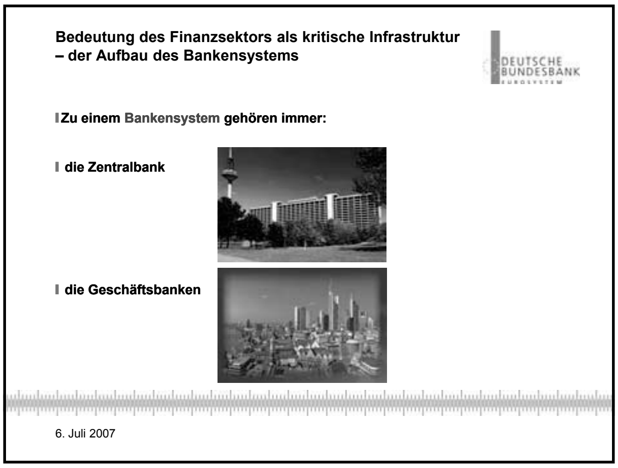


Strukturierung der Infrastruktursektoren

Sektoren und Branchen der Kritischen Infrastrukturen

Transport und Verkehr	Energie	Gefahrstoffe	Informationstechnik und Telekommunikation
Luftfahrt Seeschifffahrt Bahn Nahverkehr Binnenschifffahrt Straße Postwesen	Elektrizität Kernkraftwerke Gas Mineralöl	Chemie und Biostoffe Gefahrguttransporte Rüstungsindustrie	Telekommunikation Informationstechnologie
Finanz-, Geld und Versicherungswesen	Versorgung	Behörden, Verwaltung und Justiz	Sonstiges
Banken Versicherungen Finanzdienstleister Börsen	Gesundheit, Notfall- und Rettungswesen Katastrophenschutz Lebensmittelversorgung Wasserversorgung Entsorgung	Staatliche Einrichtungen	Medien Forschungs-einrichtungen ...

6. Juli 2007

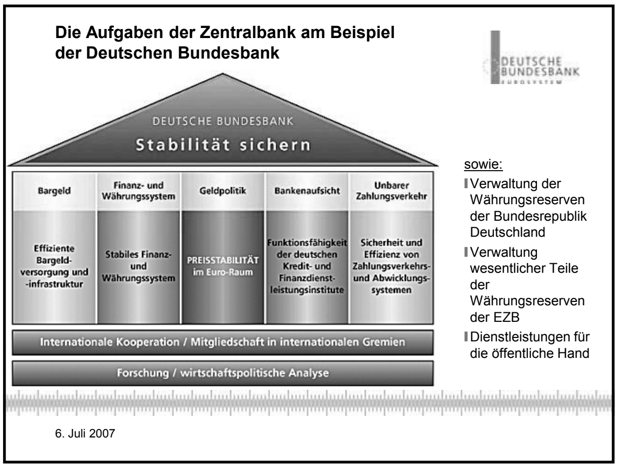


Bedeutung des Finanzsektors als kritische Infrastruktur – der Aufbau des Bankensystems

DEUTSCHE BUNDESBANK EUROSYSTEM

- **Zu einem Bankensystem gehören immer:**
- **die Zentralbank**
- **die Geschäftsbanken**

6. Juli 2007



Die Aufgaben der Zentralbank am Beispiel der Deutschen Bundesbank

DEUTSCHE BUNDESBANK EUROSYSTEM

DEUTSCHE BUNDESBANK

Stabilität sichern

Bargeld	Finanz- und Währungssystem	Geldpolitik	Bankenaufsicht	Unbarer Zahlungsverkehr
Effiziente Bargeld- versorgung und -infrastruktur	Stabiles Finanz- und Währungssystem	PREISSTABILITÄT im Euro-Raum	Funktionsfähigkeit der deutschen Kredit- und Finanzdienst- leistungsinstitute	Sicherheit und Effizienz von Zahlungsverkehrs- und Abwicklungs- systemen

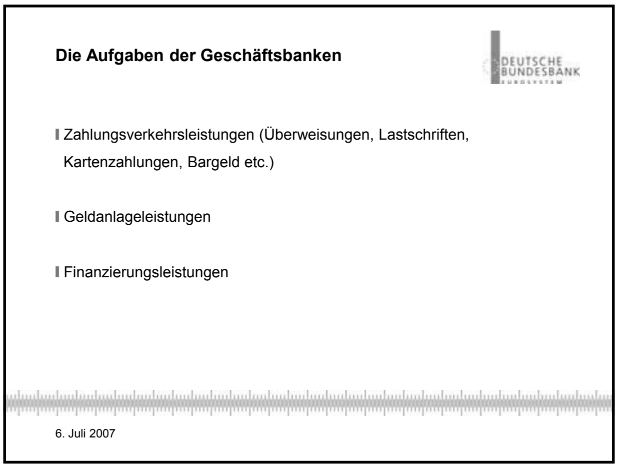
Internationale Kooperation / Mitgliedschaft in internationalen Gremien

Forschung / wirtschaftspolitische Analyse

sowie:

- Verwaltung der Währungsreserven der Bundesrepublik Deutschland
- Verwaltung wesentlicher Teile der Währungsreserven der EZB
- Dienstleistungen für die öffentliche Hand

6. Juli 2007

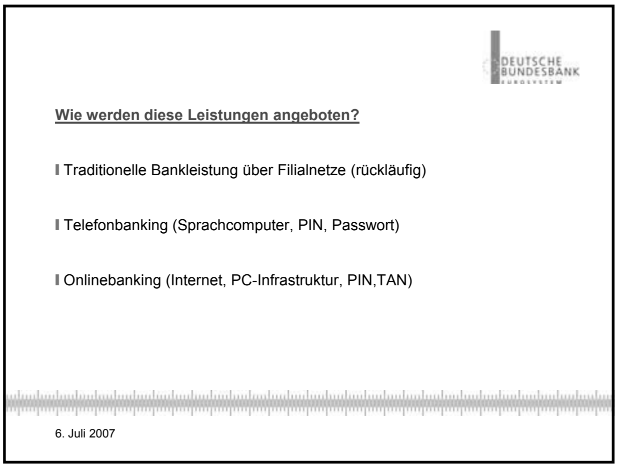


Die Aufgaben der Geschäftsbanken

DEUTSCHE BUNDESBANK EUROSYSTEM

- Zahlungsverkehrsleistungen (Überweisungen, Lastschriften, Kartenzahlungen, Bargeld etc.)
- Geldanlageleistungen
- Finanzierungsleistungen

6. Juli 2007

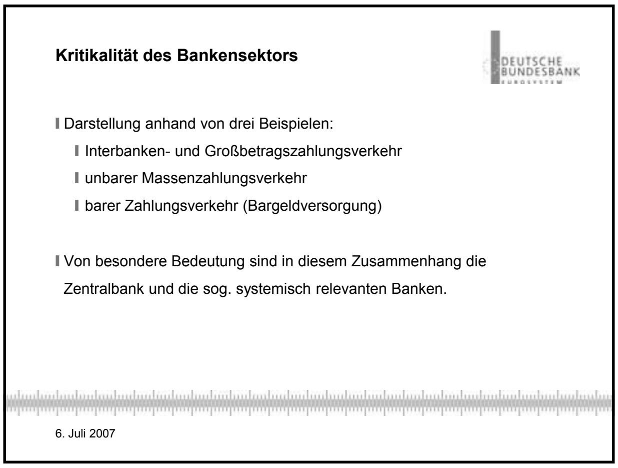


DEUTSCHE BUNDESBANK EUROSYSTEM

Wie werden diese Leistungen angeboten?

- Traditionelle Bankleistung über Filialnetze (rückläufig)
- Telefonbanking (Sprachcomputer, PIN, Passwort)
- Onlinebanking (Internet, PC-Infrastruktur, PIN,TAN)

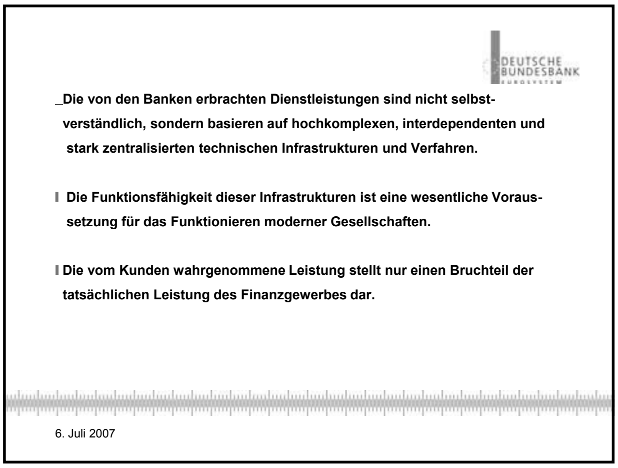
6. Juli 2007



Kritikalität des Bankensektors

- Darstellung anhand von drei Beispielen:
  - Interbanken- und Großbetragszahlungsverkehr
  - unbarer Massenzahlungsverkehr
  - barer Zahlungsverkehr (Bargeldversorgung)
- Von besondere Bedeutung sind in diesem Zusammenhang die Zentralbank und die sog. systemisch relevanten Banken.

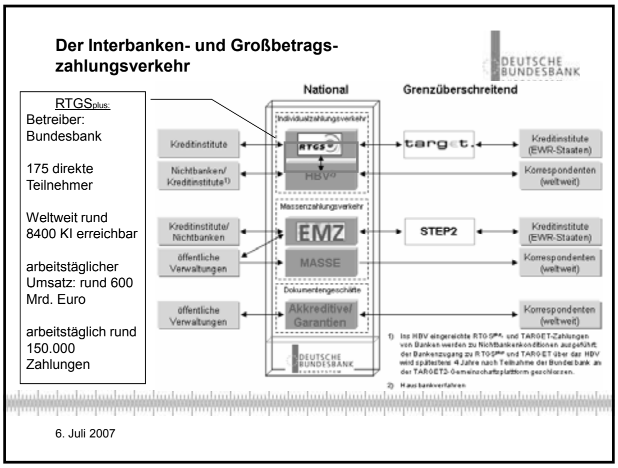
6. Juli 2007



_Die von den Banken erbrachten Dienstleistungen sind nicht selbstverständlich, sondern basieren auf hochkomplexen, interdependenten und stark zentralisierten technischen Infrastrukturen und Verfahren.

- **Die Funktionsfähigkeit dieser Infrastrukturen ist eine wesentliche Voraussetzung für das Funktionieren moderner Gesellschaften.**
- **Die vom Kunden wahrgenommene Leistung stellt nur einen Bruchteil der tatsächlichen Leistung des Finanzgewerbes dar.**

6. Juli 2007



Der Interbanken- und Großbetragszahlungsverkehr

RTGS$_{plus:}$
Betreiber:
Bundesbank

175 direkte Teilnehmer

Weltweit rund 8400 KI erreichbar

arbeitstäglicher Umsatz: rund 600 Mrd. Euro

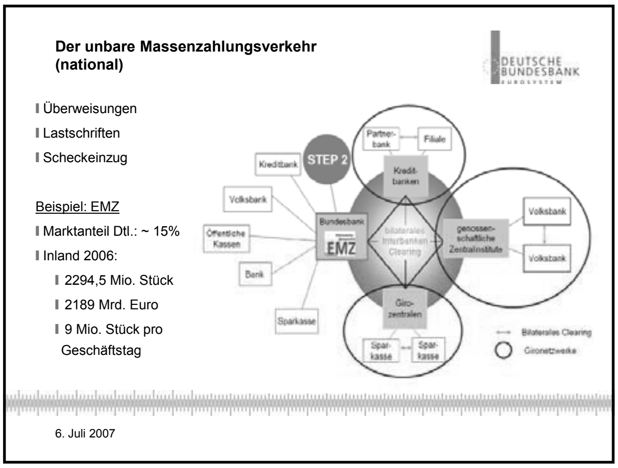
arbeitstäglich rund 150.000 Zahlungen

National
Grenzüberschreitend
Individualzahlungsverkehr
Kreditinstitute
RTGS
target.
Kreditinstitute (EWR-Staaten)
Nichtbanken/ Kreditinstitute1)
HBV2)
Korrespondenten (weltweit)
Massenzahlungsverkehr
Kreditinstitute/ Nichtbanken
EMZ
STEP2
Kreditinstitute (EWR-Staaten)
öffentliche Verwaltungen
MASSE
Korrespondenten (weltweit)
Dokumentengeschäfte
öffentliche Verwaltungen
Akkreditive/ Garantien
Korrespondenten (weltweit)
DEUTSCHE BUNDESBANK

1) Ins HBV eingereichte RTGS^{plus}- und TARGET-Zahlungen von Banken werden zu Nichtbankenkonditionen ausgeführt; der Bankenzugang zu RTGS^{plus} und TARGET über das HBV wird spätestens 4 Jahre nach Teilnahme der Bundesbank an der TARGET2-Gemeinschaftsplattform geschlossen.

2) Hausbankverfahren

6. Juli 2007



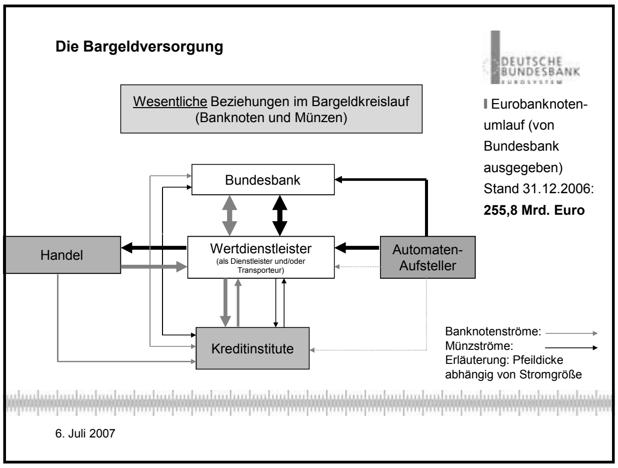
Der unbare Massenzahlungsverkehr (national)

- Überweisungen
- Lastschriften
- Scheckeinzug

Beispiel: EMZ

- Marktanteil Dtl.: ~ 15%
- Inland 2006:
  - 2294,5 Mio. Stück
  - 2189 Mrd. Euro
  - 9 Mio. Stück pro Geschäftstag

6. Juli 2007



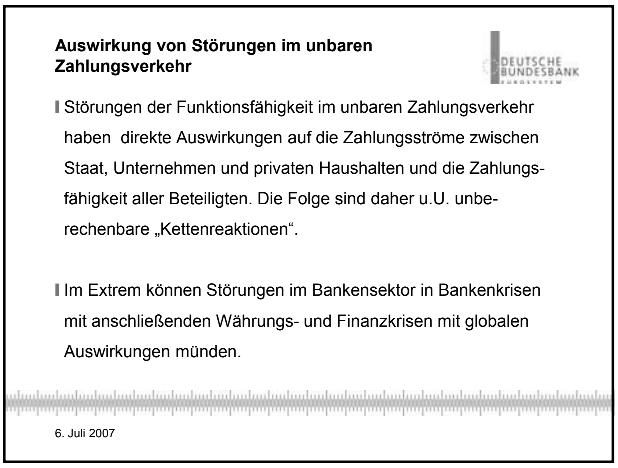
Die Bargeldversorgung

DEUTSCHE BUNDESBANK EUROSYSTEM
Wesentliche Beziehungen im Bargeldkreislauf (Banknoten und Münzen)
Bundesbank
Handel
Wertdienstleister (als Dienstleister und/oder Transporteur)
Automaten-Aufsteller
Kreditinstitute

- Eurobanknotenumlauf (von Bundesbank ausgegeben) Stand 31.12.2006: **255,8 Mrd. Euro**

Banknotenströme: →
Münzströme: →
Erläuterung: Pfeildicke abhängig von Stromgröße

6. Juli 2007

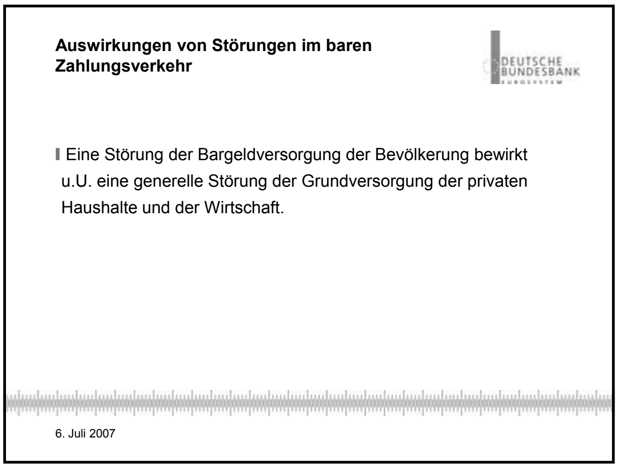


Auswirkung von Störungen im unbaren Zahlungsverkehr

- Störungen der Funktionsfähigkeit im unbaren Zahlungsverkehr haben direkte Auswirkungen auf die Zahlungsströme zwischen Staat, Unternehmen und privaten Haushalten und die Zahlungsfähigkeit aller Beteiligten. Die Folge sind daher u.U. unberechenbare „Kettenreaktionen".

- Im Extrem können Störungen im Bankensektor in Bankenkrisen mit anschließenden Währungs- und Finanzkrisen mit globalen Auswirkungen münden.

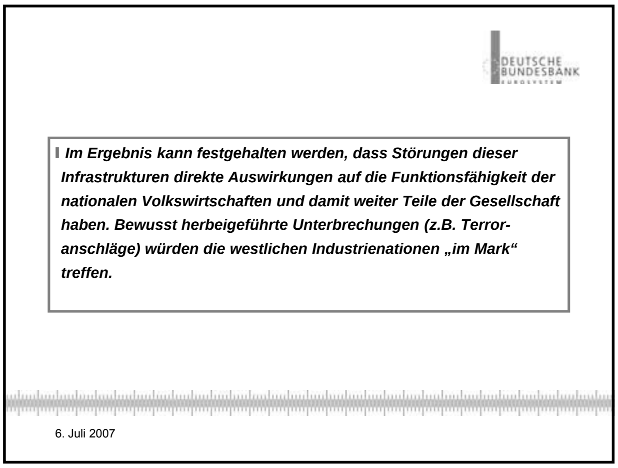
6. Juli 2007



Auswirkungen von Störungen im baren Zahlungsverkehr

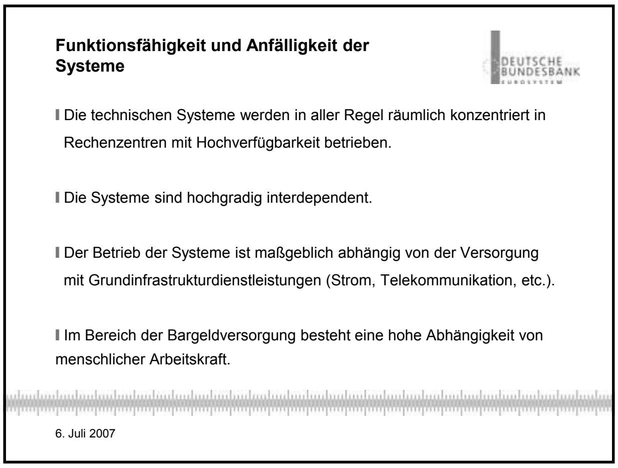
- Eine Störung der Bargeldversorgung der Bevölkerung bewirkt u.U. eine generelle Störung der Grundversorgung der privaten Haushalte und der Wirtschaft.

6. Juli 2007



- ***Im Ergebnis kann festgehalten werden, dass Störungen dieser Infrastrukturen direkte Auswirkungen auf die Funktionsfähigkeit der nationalen Volkswirtschaften und damit weiter Teile der Gesellschaft haben. Bewusst herbeigeführte Unterbrechungen (z.B. Terroranschläge) würden die westlichen Industrienationen „im Mark" treffen.***

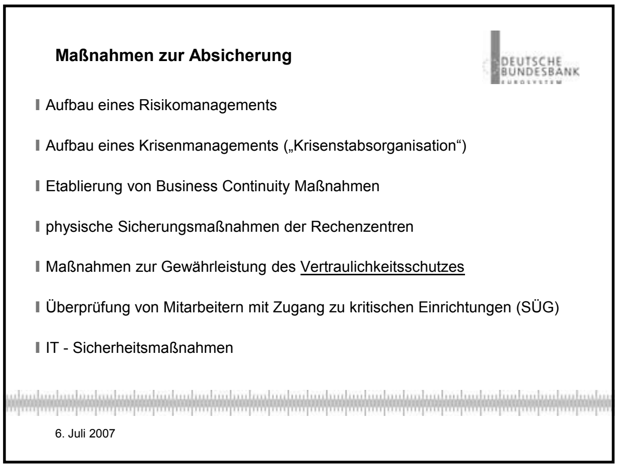
6. Juli 2007



Funktionsfähigkeit und Anfälligkeit der Systeme

- Die technischen Systeme werden in aller Regel räumlich konzentriert in Rechenzentren mit Hochverfügbarkeit betrieben.
- Die Systeme sind hochgradig interdependent.
- Der Betrieb der Systeme ist maßgeblich abhängig von der Versorgung mit Grundinfrastrukturdienstleistungen (Strom, Telekommunikation, etc.).
- Im Bereich der Bargeldversorgung besteht eine hohe Abhängigkeit von menschlicher Arbeitskraft.

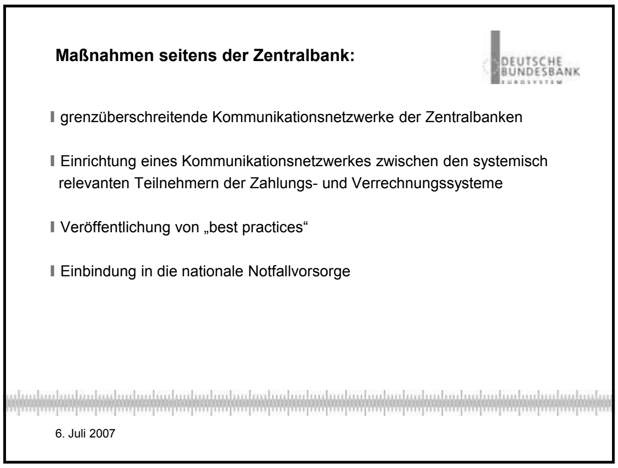
6. Juli 2007



Maßnahmen zur Absicherung

- Aufbau eines Risikomanagements
- Aufbau eines Krisenmanagements („Krisenstabsorganisation“)
- Etablierung von Business Continuity Maßnahmen
- physische Sicherungsmaßnahmen der Rechenzentren
- Maßnahmen zur Gewährleistung des Vertraulichkeitsschutzes
- Überprüfung von Mitarbeitern mit Zugang zu kritischen Einrichtungen (SÜG)
- IT - Sicherheitsmaßnahmen

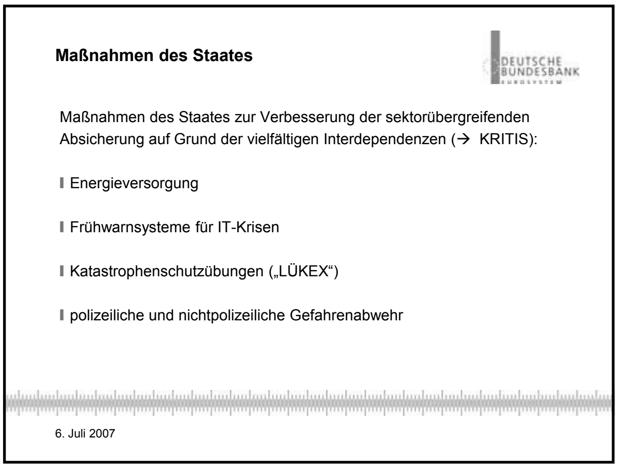
6. Juli 2007



Maßnahmen seitens der Zentralbank:

- grenzüberschreitende Kommunikationsnetzwerke der Zentralbanken
- Einrichtung eines Kommunikationsnetzwerkes zwischen den systemisch relevanten Teilnehmern der Zahlungs- und Verrechnungssysteme
- Veröffentlichung von „best practices“
- Einbindung in die nationale Notfallvorsorge

6. Juli 2007



Maßnahmen des Staates

Maßnahmen des Staates zur Verbesserung der sektorübergreifenden Absicherung auf Grund der vielfältigen Interdependenzen (→ KRITIS):

- Energieversorgung
- Frühwarnsysteme für IT-Krisen
- Katastrophenschutzübungen („LÜKEX“)
- polizeiliche und nichtpolizeiliche Gefahrenabwehr

6. Juli 2007

Semiconductor Sensors for Stand-off Explosives Detection

O. Tolbanov, O. Anisimov, V. Sachkov,
Tomsk State University, Tomsk, Russia
G. Sakovich, A. Vorozhtsov
Institute for Problems of Chemical and Energetic Technologies SB RAS, Biysk, Russia

The technology of manufacturing the new porous elements containing nanoparticles of semiconductors (In_2O_3:Sn, SnO_2:Sb, ZnO:Al) and of metals (Ag, Au, Pt, Pd) with the specified size of a specific surface (S=100-120 m^2/g) and the sol-gel specific technology of drawing porous ceramic films with catalyze nanoparticles on gas-sensitive has been developed. Activity of porous nanostructed elements in relation to explosives vapors of ammonium nitrate and nitrotoluene has been studied and today we create laboratory samples of multielement high-sensitive sensors of explosives (TNT, RDX, AN etc.).

It is the objective to develop nanotechnologies for an early warning and response system for explosion threats to buildings and infrastructures. It maintains surveillance also in case of a disaster and initiates emergency actions. It combines multi-sensor techniques, on-line communication and immediate alarm. Nanotechnologies enable the sensors to be of sufficient sensitivity and effective response. Sensor development includes nanotechnology based on semiconductor sensors for remote detection of explosives vapours as well as their location and, possible, type. Sensors are linked (wired or wireless) to a control unit, which enables analysis of the sensor signals, initiation of fast response and communication to the outer world. Continued surveillance especially in the case of disaster keeps emergency and counter measures under control. Existing communication channels have to be modified to work under these premises. The sensor system and its use to maintain control also during an event will be the main breakthrough application enabled by nanotechnologies. It leads to a new quality of security / safety also in private sites like sports arenas, production facilities, apartment houses, etc.

At development of safety system on the basis of semi-conductor thin-film sensors for explosives detection for prevention of terrorist acts, it is necessary, that used sensors had high sensitivity and selectivity in relation to trace amounts of explosives vapours which can present in under consideration medium.

Recently it has been proved that for developing the more efficient sensing element it is worthy to use Pt/SnO_2:Sb thin films with superthin layers of catalytic platinum, silver or gold deposited on the thin-film surface. However, such semiconductor thin-film sensors haven't high sensitivity for detecting explosives vapors.

The present research is aimed at creating hybrid sensing element of high sensitivity and selectivity to explosives traces and vapors. The main idea is to convert the complex molecules to more similar able to be detected by sensitive semiconductor surface.

$C_xH_yO_z \rightarrow nCO + m/2\ H_2O$

1) $C_xH_yO_z \rightarrow C_{xn}H_{ym}O_z * K * O$

2) $C_{xn}H_{ym}O_z * K * O \rightarrow CO * k * H_2O$

3) $CO * k * H_2O \rightarrow \underline{CO} + H_2O + K$

$C_xH_yN_nO_z \rightarrow N_mO_y + nCO + m/2\ H_2O$

These chemical reactions can't proceed spontaneously at room temperature. For efficient decomposition it is necessary to apply catalyst, for example, nanopalladium, nanosilver and nanogold. The nanoporous and transparent for vapors layer containing nanoparticles of the active component provides selective adsorption and transformation of explosives' molecules.

Sol-gel method is more suitable for generating highly porous selective catalyst. Sol-gel processes can proceed in the water solutions applying metal salts and in the alcoholic solutions applying.

Sol-gel transformation in metal alcoxides solutions is caused as a rule by hydrolysis and polycondensation reactions. The subsequent condensation leads to grow of metal-oxide oligomers which are combined to each other consecutively and form gel cells. Common reactions for silicon alcoxide $Si(OR)_4$ are below.

$$Si(OR)_4 + H_2O = Si(OH)(OR)_3 + ROH \quad (1)$$

$$Si\text{-}OH + Si\text{-}OH = -\overset{|}{\underset{|}{Si}}-O-\overset{|}{\underset{|}{Si}}- + H_2O \quad (2)$$

$$Si\text{-}OH + Si\text{-}OR = -\overset{|}{\underset{|}{Si}}-O-\overset{|}{\underset{|}{Si}}- + ROH \quad (3)$$

Silicon alcoxides have low rate of hydrolysis and polycondensation compared to alcoxides of other metals such as Ti, Zr, B and Al. Therefore, hydrolysis of silicon alcoxide is easier controlled, and gel samples of silicon could be transferred into different shapes such as spinning fiber of heavy-bodied gel, film obtained by depositing less heavy-bodied sol on the substrate and block structures.

The common reaction rate (1-3) depends on the water concentration, the kind of an alcoxi-group as well as on the kind and concentration of a catalyst. In the acid medium gel properties depends on the water concentration especially in the area where the water-alcoxide mole ratio changes from 2 to 4. The gels with low bound energy between structure units are obtained at water-alcoxide ratio < 2 and over a catalyst. These gels are applied for obtaining gel fiber and thin-films. The increase in water-alcoxide ratio up to 4 leads to getting the gels with high bound energy between structure units. Such gels keep its structure after thorough drying. The hydroxogroups predominate inside the gel cells. The pores are less than several nanometers in diameter.

When the process of macropores formation in silicon sol-gel system begins to compete with phase border formation and sol gel transformation the dynamic behavior of the system depends on the molecular weight distribution of silicon oligomers and on the length of gel cells. Thus, the content and concentration of a catalyst in precursor solution are the key parameters determining the morphology of obtained macropores.

Dehydration of humid gel samples proceeded in furnace with air circulation by slow evaporation of fugitive components. The most suitable temperature was in the range of 40 - 80^{0}C depending on dissolvent applied. Cockle and dehydration of samples varied from 50 to 70% of the initial size and depended mostly on oxide concentration and mesoporosity. The samples were annealed for eliminating the fugitive component and for thermal destruction of organic components aimed at obtain gel samples. The rate of annealing was 0,1 ^{0}C/min. and was maintained up to reaching the temperature of 550^{0}C during two hours. After that it was reduced to room temperature. Catalytic activity of the prepared systems was tested by catalytic installation of flow type with bed layer. The sample had been kept in the conditions of continuous catalytic reaction for two hours before sampling. Thus, at the present stage of the research the experiments have been carried out which showed the best synthesis approach of sol-gel method for obtaining more active system in catalytic process. The approach lies in simultaneous insertion of material components of the first stage of synthesis.

We have studied the changes of morphology of sol-gel materials at all stages of synthesis. The precision investigations have demonstrated (Figure 1) that the surface of the fresh prepared materials is smooth enough and the particles of 0.1 mkm are distributed uniformly.

It is difficult to presume the chemical content of the particle on the present stage of research, but this task is planned to be solved. Nevertheless, it is possible to state the sufficient homogeneity of the sample grounding on the character of particles distribution. To evaluate the thermostability of the sample to high temperatures it was annealed at 650 ^{0}C in the air. Morphology of the annealed sample is showed on the Figure 2. It has been determined that high temperatures doesn’t influence considerably on the sample’s morphology, the surface is of the same smoothness as before the treatment. But the decrease in the amount of particle caused probably by its melting was observed.

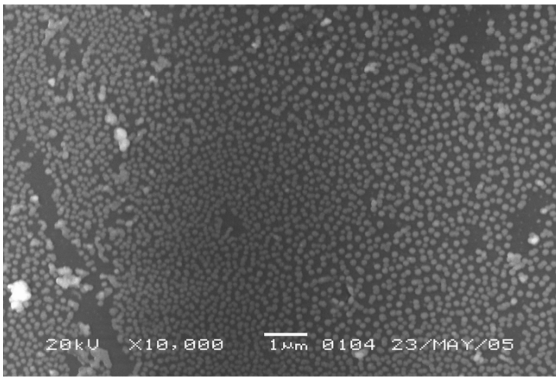


Figure 1: Fresh prepared sol-gel catalyst with nanoparticle of the metal.

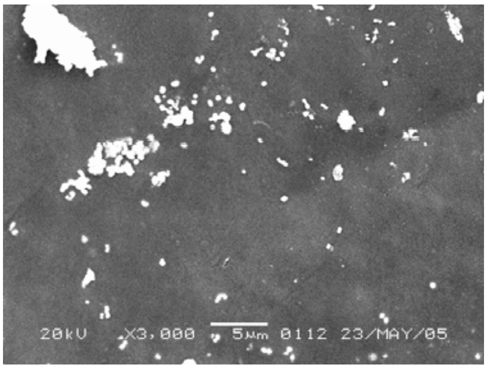


Figure 2: The surface of sol-gel material has been annealed for 2 hours at 650 °C in the air

The most important result is that the investigated material has thermal stability to high temperatures. Applying dip-coating method the porous gel structures were deposited on the surface of nanofilm sensors.

Activity of porous nanostructed elements in relation to explosives vapours of ammonium nitrate and nitrotoluene has been studied and today we create laboratory samples of multielement high-sensitivity sensors of explosives (TNT, RDX etc.).

The device consists of 16 single-type units and each of them has temperature stabilization and conductivity indicator of a semiconductor sensor. Units control and data reading are made by PC through RS232 port. The software provides controlling of every unit, data reflection and retention. Stabilization temperature could change in cycle according to program set up or be constant.

Figure 3 demonstrates sensor signal changes depending on the pumping time of the air with vapors of ammonium nitrate.

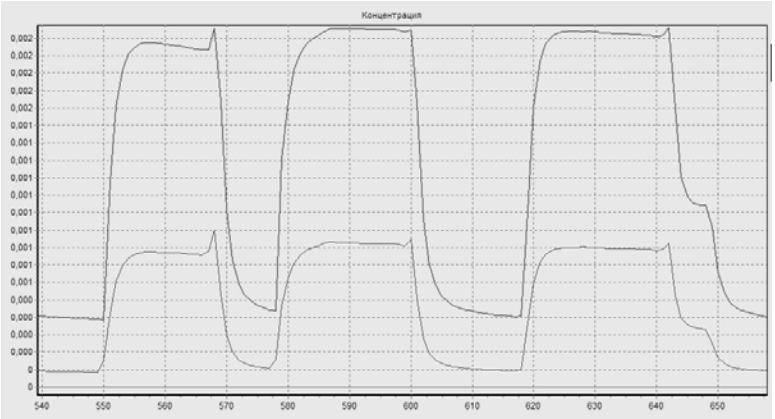


Figure 3: Sensors response to the effect of ammonium nitrate vapors.

Today, the algorithm of sensor signal processing has been developed for increasing the selectivity of the system if there is an interference of exhaust gases, cigarettes smoke, perfumery, synthetic aromatizers, hydrocarbons, etc.

This research was supported by NATO Grant NRCLG.982668.

Aspects of Integrated Safety and Security for the Built Infrastructure

Univ.-Prof. Dr.-Ing. Dr.-Ing.habil. Norbert Gebbeken, Institut für Mechanik und Statik, Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, 85577 Neubiberg, norbert.gebbeken@unibw.de

Abstract:

Automobiles, aircrafts and further technical systems have system inherent integrated safety and security components by law even for catastrophic events. These systems need to be inspected in close intervals. Dealing with the built infrastructure only for expected design loads a passive safety is enforced. Catastrophic loading scenarios need to be defined individually for critical infrastructures. In contrast to automotive industry there exists no standardized system for integrated safety and security for the built infrastructure.

Introduction

The built infrastructure is defined as buildings and structures which are planned, designed and executed by architects and/or civil engineers, e.g. office buildings, hospitals, high rise buildings, towers, bridges, tunnels, highways, railways, dams, dikes, sluices, ports, sewage plants. All these structures serve an intended purpose. Therefore, they are equipped with installations, instrumentations, equipment and devices. Owners and users expect structures and technical equipment to be safe, resistant, durable, robust, and integer at any time, and under all circumstances.

A well recognized threat is fire. Fire protection is always a combination of safety and security measures which are standardized. Safety measures are: selection of fire resistant materials, fire resistant design with respect to required time for fire resistance (e.g. F90, T30), design of fire compartments and design of escape routes. Security measures are heat and smoke detectors, sprinkler systems and the fire department.

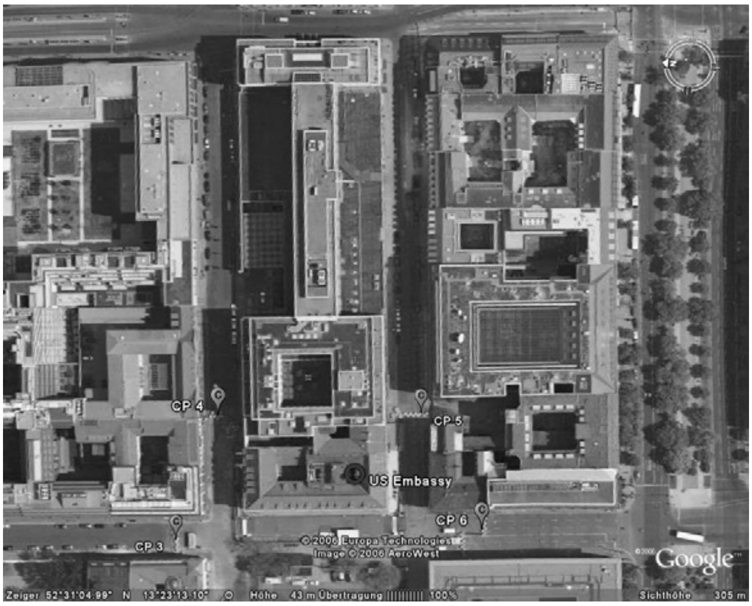
Analyses of past terrorist threats to infrastructures revealed that in more than 80% of the cases we have to expect explosive scenarios in combination with flying debris and splinter and after fire. Roughly 12%

were hand-gun or rocket or missile attacks. Because of these statistics, in the following, we will concentrate on explosion and impact.

Critical Built Infrastructures - Examples

Critical built infrastructures belong to the following areas: Government and administration, Finance, IT/Communication, Transportation, Health care system and interior safety, Trade and industry, Handling and storage and transportation of dangerous goods, Supply, Energy, Science, media and culture, Religion, Federal real estates abroad, military camps abroad. As the diversity of the areas is so is the complexity of the built infrastructures.

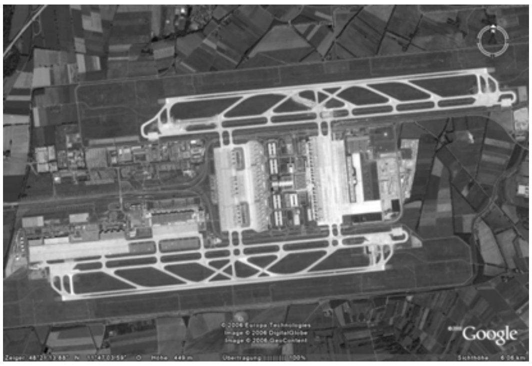
There are relatively simple office buildings or bridges, complex important underground traffic hubs, highly complex industrial plants, sea ports which are highly diverse and complex, air ports, “simple” telecommunication towers and others.


CP 4
CP 5
US Embassy
CP 6
CP 3
©2006 Europa Technologies
Image ©2006 AeroWest
©2006 Google
Zeiger 52°31'04.99" N 13°23'13.10" O Höhe 43 m Übertragung 100%
Sichthöhe 305 m

Embassy building complex (Google Earth image)

Bridge (Sessles Valley)

Sea port of Hamburg, tanks, vessels, containers



Air port of Munich

These infrastructures need to be protected against natural, technical or man made disasters.

Safety and security measures

In ports, industrial facilities and similar infrastructures safety and security measures are highly accepted by the public. This acceptance changes when people are entering concert halls, museums or industrial fairs. Consequently, safety and security measures have to take into account the perception and the acceptance of the society.

Safety measures are all measures of “passive” safety. Materials are chosen to be resistant and ductile, structural components are shaped and designed to be resistant and ductile and so is the entire structure. Buildings and facilities are arranged such, that they have stand-off distances and that they do not produce unfavourable multiple reflections. The landscape can be shaped and planted with bushes and trees in such a way that blast waves are directed, disturbed and partly reflected, and shootings with hand-guns can only be harmful at short distances. These passive safety measures will not be recognised as safety measures. They are system inherent and simply active in passivity.

Additional measures are fences, bollards and others. They ensure stand-off distances, force to drive slowly and prevent to climb or throw over. These measures are visible and can possibly constrict the freedom of movement.

Additional safety measures: sliding bollards

perimeter bollards

The above mentioned measures are complemented by active security measures, e.g. security personnel, check points, observation cameras, motion detector, chemical detector, luggage inspection, radioscopy, missile defence systems, and others. Some of these devices can be hidden, some might be perceived as obstruction.

Observation cameras

Fence and motion detector

Concluding remarks

All possible safety and security measures have to be coordinated in such a way, that one achieves a maximum of safety by minimizing costs and obstructions.

Lit.: Gebbeken et al.: BaU-Protect – Building and Utilities Protection, Berichte aus dem Konstruktiven Ingenieurbau, Nr.:06/4, Universität der Bundeswehr München, ISSN 1431-5122,

Passive Protection of Aircraft – Closing the Gap between Military and Civil Research

Christian Less, EADS Deutschland GmbH Military Air Systems
Klaus Thoma, FhG Ernst-Mach-Institut
Heinz Voggenreiter, Deutsches Zentrum für Luft- und Raumfahrt
Peter Middendorf, EADS Deutschland GmbH Innovation Works

Since the end of the cold war security scenarios have changed: Destabilization and conflicts have prepared the ground for terrorism and organized crime, moving civil aviation into the focus of new threats.

In the US capabilities have been joined, applying military analysis methods and expertise to civil platforms. Examples are FAA's Aircraft Hardening Program "regarding … implications of terrorism on … 800 to 1000 passenger jumbo jets", the Air Force's Large Aircraft Survivability Initiative or the FAA-funded Uncontained Engine Debris Damage Analysis Model, a civil version of US military vulnerability codes.

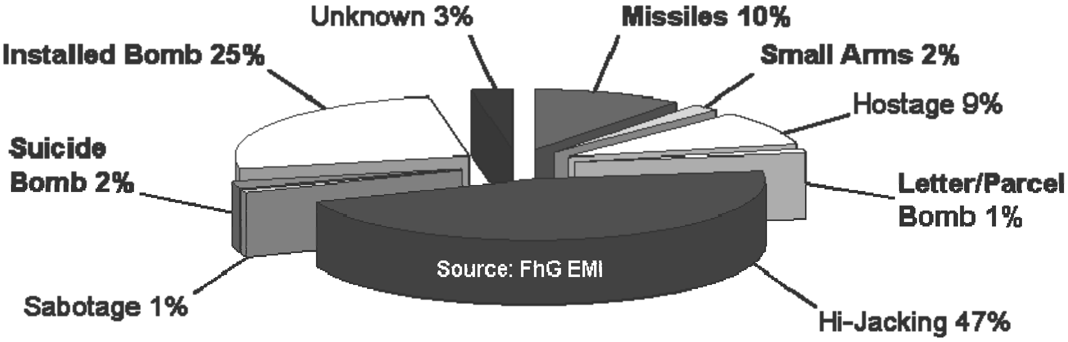
Guided by the ESRAB report, the European Security Research covers authorization, surveillance, communication and many more. Concerning risk assessment, modelling and impact reduction, current planning does not address the final element of the security chain – vulnerability analysis and reduction. This ranges from engagement analysis to improved configurations and to designed materials for optimum response to threat effects with minimized damage. Quantitative analysis based on appropriate metrics is a pre-requisite to trade-off studies, ensuring not only effectiveness but also efficiency of solutions for commercial applications.

For this ambitious goal civil and military research must develop synergies. The Alliance for Passive Protection of Aircraft is a first step into this direction.

Changing Threats

With the cold war, dominating security scenarios for more than forty years, disintegration of power structures lead to destabilization and local conflicts, thus preparing the ground for a yet unknown level of organized crime and terrorism. The single dominating risk was replaced by a number of new, asymmetric conflicts in a much more complex geo-political scenario. Furthermore the process of globalization, supported by sheer unlimited exchange of information via the internet, provided new possibilities of networking also to these detrimental developments.

Unfortunately, aviation is a prime target, especially for politically motivated terrorism, due to often catastrophic effects and the respective attention of media. Concerning aircraft, during the last 20 years about 40% of all attacks were based on the effects of projectiles or explosives – putting civil aircraft into a military environment.



Source: FhG EMI

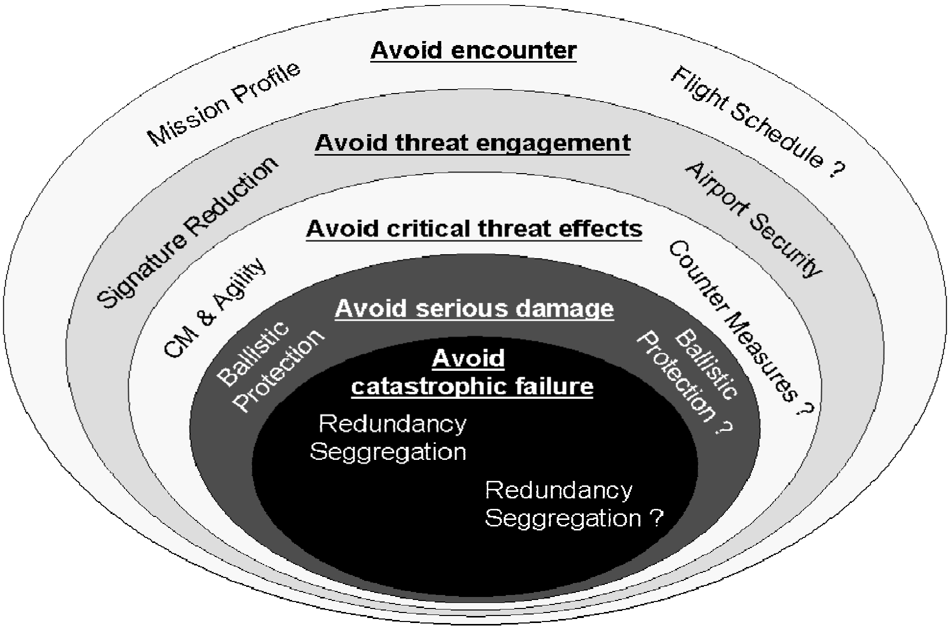
Attacks on aircraft by threats 1985-2006

The "Security Onion"

One of the key requirements in military applications is Survivability, being the capability of a system and crew to avoid or withstand a man-made hostile environment. The first part of Survivability is Susceptibility, which is the degree to which a system is open to effective attack. The second, complementary part is Vulnerability, being the characteristic of a system, which causes it to suffer a definite degradation as a result of having been subjected to a certain level of effects in an hostile environment.

Often Vulnerability and Susceptibility are presented more detailed in the so-called Survivability Onion, showing not only the concept of nested protection layers, but indicating also the decreasing space for solutions with the threat coming closer and becoming more defined. This approach can also be applied to civil scenarios using a different wording, extending Survivability to Security of passengers and crew.

Not all layers can be mirrored from the military domain to civil operations: Variations of flight schedule for achieving better tactics would be hard to implement by airliners. But the proposed solutions become the more similar the deeper the layer is nested.



The "Security Onion" for the military (left) and civil domain (right)

The US Approach

Consequently, in the USA not only funding for security research and technology was increased, but also cooperation between civil and military entities was intensified in order to realize synergies. Three examples for such cooperation can be found in open sources, which are of specific relevance for European aircraft manufacturers and airlines:

FAA's Uncontained Engine Debris Damage Analysis Model (UEDDAM) is capable of conducting rotor-burst assessment using military vulnerability codes FASTGEN/COVART modified with penetration equations being more suited to engine disk and blade fragments.

US Air Force's Large Aircraft Survivability Initiative (LASI) encourages government and industry collaboration to improve commercial and heavy military aircraft survivability against small missiles and recoverability of damaged commercial aircraft.

FAA's Aircraft Hardening Program intended to protect commercial aircraft from catastrophic structural or critical system failure due to an in-flight explosion. It also was to investigate vulnerability of the current and future fleet of commercial aircraft against missiles. Special emphasis is placed on assessing and recommending hardening actions regarding the long-term implications of terrorism on new commercial aircraft concepts such as the 800 to 1000 passenger jumbo jets and high speed civil transport aircraft. From the onset, the Aircraft Hardening program has used expertise from the U.S. Air Force, U.S. Army, and U.S. Navy.

European and German Activities

After formulation of the European Security Strategy in 2003, the Preparatory Action for Security Research (PASR) was conducted 2004-2006, accompanied by the formation of the European Security Research Advisory Board (ESRAB). Following, the European Security Research Program (ESRP) provides now substantial additional funding for respective projects within the 7th Framework Program (FP7).

Additionally, in Germany the BMBF has started a research program for civil security, harmonized with FP7 and focusing on specific needs and chances of the German security-related industry.

Both, ESRP and the BMBF program, claim that barriers between military and civil research shall be overcome, thus enabling technology transfer from the military domain. Both make security and protection of mass transport and specifically aviation a prime objective for research.

However, looking at the current programs and projects funded under PASR, the outer layers of the proposed Security Onion are strongly represented – the focus is set on Susceptibility issues, like detection, identification, authorization, surveillance or communication. Although topics like risk assessment, modelling and impact reduction provide a good framework to Vulnerability research, it seems that the security community was not yet ready to investigate scenarios, in which threat avoidance technologies have failed. Therefore, in future calls and proposals also the Vulnerability issues should be addressed and research should start at those points where operational analysis shows potential success of threat engagements.

The Alliance for Passive Protection of Aircraft

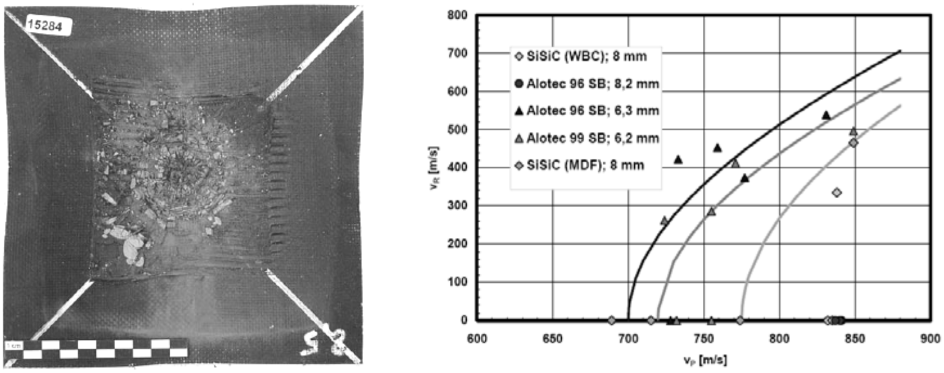
In March 2007 experts of Diehl BGT Defence, Eurocopter Germany, Fraunhofer EMI, DLR and EADS Germany Innovation Works and Military Air Systems have met in order to discuss their view on security research. They agreed to undertake a common effort – the Alliance for Passive Protection of Aircraft – to make the research community as well as political and industrial decision makers aware of the need to take a balanced approach and therefore to address the Vulnerability topics like response of structures and systems to blast and penetration. Vulnerability analysis and reduction is the final element in the Security chain and closes the still existing gap between military and civil research. When integrated in an operational analysis, it will enable trade-off studies, assessing the benefits of any protection measure against its penalties like additional weight and cost. Thus, not only effectiveness of solutions can be ensured, but also efficiency. Developing this capability will also be required by industry to discuss upcoming requirements and recommendations with global authorities and to sustain market success against global competitors.

In order to achieve the ambitious goal of substantial improvements at minimum drawbacks, the whole analysis sequence must be understood and the partners must have creativeness and the knowledge to propose, develop, validate and certificate new and alternative solutions.

While still being open to new partners, the Alliance for Passive Protection of Aircraft already covers many areas:

The DLR-Institutes of Structures and Design and Materials Research are concerned with the development and implementation of polymeric and ceramic composite materials in high performance structures with a special focus on energy absorption and improving the structural integrity of load bearing structures under ballistic impact or crash conditions.

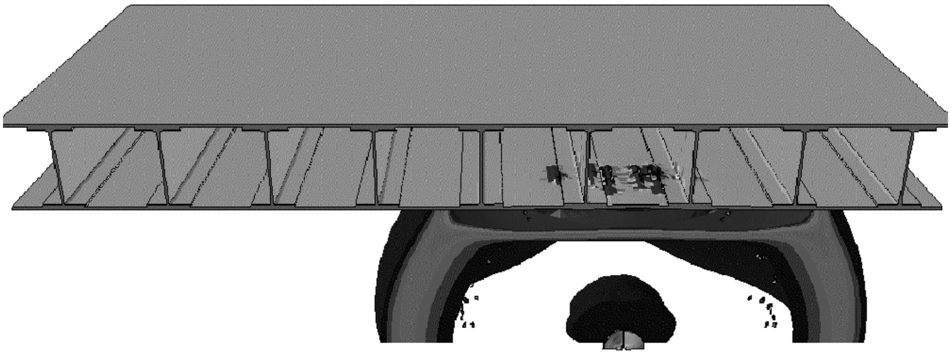
Recent development of biomorphic SiSiC-ceramics based on wooden preforms and advances in C/C-SiC-ceramics, both manufactured via the liquid silicon infiltration (LSI), are considered promising new armour materials due to their high potential for the manufacture of complex shaped structures – also load bearing – at low costs.



Ballistic performance of DLR's biomorphic SiSiC

The Fraunhofer Ernst-Mach-Institute (EMI) is dealing with physical-technical aspects of high-speed, mechanical and fluid-dynamic processes. This includes experimental and numerical analyses of shock waves in solids, fluids, and gases, flow and combustion processes, impact and penetration processes in a broad range of speeds from 10 m/s to 10.000 m/s, the response of structures to shock loads, dynamic material response at high strain and at high strain rates.

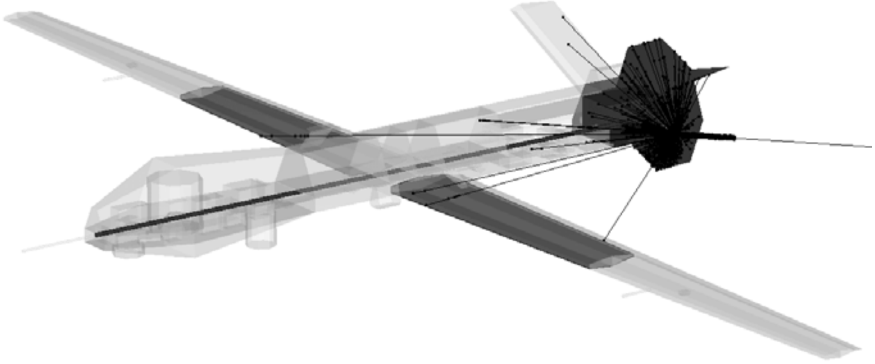
Recent application of these continuously developed capabilities comprise studies of CFRP wing structures exposed to fragmenting warheads, covering the coupled effects of blast, penetration of dry structures and hydrodynamic ram in fuel tanks.



EMI simulation of fragments and blast against a wing-like composite structure

EADS is a global leader in aerospace, defence and related services. The EADS Group includes the aircraft manufacturer Airbus, the world's largest helicopter supplier Eurocopter and the joint venture MBDA, the international leader in missile systems. EADS is the major partner in the Eurofighter consortium and develops the A400M military transport aircraft. EADS Military Air Systems is integrated business unit of EADS' Defence & Security Systems Division, representing the industrial end user of security technologies. The EADS Innovation Works (IW) are the corporate research facilities, supporting the research & technology strategy and covering the skills that are of critical importance to EADS.

In recent projects EADS has not only studied specific topics in vulnerability of composite structures, but MAS also developed a capability for system-level vulnerability simulation and analysis. This capability is based on, but not limited to use of the Swedish software AVAL from FMV/FOI, so far the only military Vulnerability code commercially available for industry without restrictions in use.



AVAL simulation of a missile attack on an unmanned surveillance aircraft

The Alliance for Passive Protection of Aircraft will progress Vulnerability topics in civil Security.

Protection against Malicious and Terrorist Attacks on Critical Infrastructures

Yves Guengant, Etudes Recherche et Développement, SME Environnement, GROUPE SNPE, France

Introduction

For many reasons, Global Security has become a major concern for Authorities and whole society. As regard to malicious and terrorist attacks, several actors conduct many actions. It is evident that the most important prevention is twice intelligence done by secret services or police and CBRNE substances detection by electronic sensors at critical locations. Nevertheless, the recent attacks have demonstrated that terrorist imagination is limitless. Then, it is difficult to anticipate threats using IEDs, Homemade Explosives … or simple craft knifes used for 9th/11 disaster. Then, it appears that prevention is not sufficient. It is also necessary to assess critical infrastructure vulnerabilities in the aim to identify completely possible threats, to attenuate attack effects, to improve the crisis management and to facilitate remediation.

Due to its activities in Chemicals and Energetic Materials as producer but also as R&T specialist, SNPE Matériaux Energétiques can bring significant contribution for improving the Global Security.

The aim of this paper is to underline several R&D axes that would be studied extensively concerning industrial sites and others critical infrastructures:

For example, not all precursors for homemade explosives can be eliminated for evident technical reasons (Acetone, Ammonium Nitrate …), nevertheless, these products could be marketed under chemical/physical form that is difficult to misuse (dilution, coating …) with complement of taggent agents.

Terrorists can attempt to reproduce major accidents (fire, explosion, toxic dispersion …) with possibly internal complicity getting round safety devices. This has been recently planned about kerosene tanks of JFK New York airport.

Complete knowledge of industrial safety management is necessary to identify these potential scenarios and to assess the vulnerabilities of these critical infrastructures. It is also necessary to quantify effects and consequences according to products, facilities, dominos effects …

Structural reinforcement of theses critical infrastructures would be done as high as possible. But these passive devices cannot allow reaching desirable protection level.

Design of active protection devices would be taken into account. For example, sprinklers are used for fire extinction but these could be used also for toxic smokes falling down. This device is not expensive because, it is only necessary to develop triggering system.

Industrial Risk management tools used in industry could be adapted to take into account of malicious and terrorist attacks. Up to know, industrial risk management tools run to prevent accident scenario (fire, explosion, BLEVE, VCE …), it is possible to use them extensively for Global Security. Through that way, the over costs for industry would be limited.

Thus, concerning security of critical infrastructures, crisis management is also facilitated if all scenarios are described, consequences are attenuated if adapted procedures are defined, and remediation costs are limited if facilities are specially designed.

Threat Hazard Assessment

Precursors & Others Substances

Not all precursors for homemade explosives can be eliminated for evident technical reasons and because they bring to all society some benefits. These precursors can be marketed themselves but these can be also some synthesis intermediate substances for medicines and others products.
If these precursors are marketed, it is possible to develop regulations to limit the misuses like recently for chlorate in France. The techniques consist to define chemical/physical form that is difficult to misuse (dilution, coating …), in complement some taggent agents can be added to facilitate detection.
On over hand, it is necessary to characterise all mechanisms that outcome violent or lethal effects (fire, explosion, toxic release ….):
For example, SNPE has conducted study in the aim to understand Toulouse AZF disaster (Ammonium Nitrate detonation of 300 tonnes stockpile). Indeed, chemical reaction with Sodium Dichloroisocyanurate can provoke Ammonium Nitrate Detonation through formation of Nitrogen Trichloride. SNPE can conduct also some studies to determine interactions between chemical substances and explosives / detonation gases in the aim to determine generated substances and their effects.

Accidental Events Reproducing

The SEVESO II plants have the maximum potential of danger due to the quantity and the nature of manipulated substances. Nevertheless, all safety concern is done to prevent accidental events. None action is performed to prevent specifically deliberate action, except access control and surrounding walls.

Terrorists can attempt to reproduce major accidents (fire, explosion, toxic dispersion …) with possibly internal complicity getting round safety devices. This has been recently planned about kerosene tanks of JFK New York airport. In France, during May 2007, LPG truck has been intentionally fired. The BLEVE (Boiling Liquid Expanded Vapour Explosion) has provoked missile projections; some have fallen down on houses at few hundred meters long.

Thus, it is important to consider accidental events that could be reproduced maliciously in the aim to set-up measure to prevent them.

Vulnerabilities of Critical Infrastructures

Critical infrastructures are numerous. Often, we consider firstly locations where lot of people are present (airport, railway station, stadium …). But it is also necessary to take into account SEVESO II plants have the maximum potential of danger due to the quantity and the nature of manipulated substances. And, these plants are not far form residential areas. A terrible example has been given by Enschede disaster (22 dead, 947 injured) in The Netherlands. A fireworks warehouse has exploded in little city and has provoked 22 dead, 947 injured.

Thus, complete knowledge of industrial safety management is necessary to identify these potential scenarios and to assess the vulnerabilities of these critical infrastructures. It is also necessary to quantify effects and consequences according to products, facilities, dominos effects …

Protection Measures

Structural Reinforcement

Structural reinforcement of the critical infrastructures would be done as high as possible. For example, it is possible to prevent glasses breaking for office building. Many studies have been done through defence R&T studies. SNPE has set-up numerical simulation tools based on experimental trials to design various protections. It is also possible to build concrete barricade to prevent missile projections or blast effects. But, this barricade has no efficiency on toxic release. So, these passive devices cannot allow reaching desirable protection level for all feared events.

Active Protection Devices

Design of active protection devices can be taken into account. For example, sprinklers are used for fire extinction but these could be used also for toxic smokes falling down. This device is not expensive because, it is only necessary to develop triggering system.
Others devices can be designed to activate safety measures as closing pipe, opening or closing barriers. Some of them can use pyrotechnic devises with the advantages to be triggered passively (temperature) or actively (sensors, remote …), to function without any external power supply and to be able to provide large power. Some of them have been designed by SNPE's subsidiary (Pyroalliance).

Organizational Measures

Risk Management

Industrial Risk management tools used in industry could be adapted to take into account of malicious and terrorist attacks. Up to know, industrial risk management tools run to prevent accident scenario (fire, explosion, BLEVE, VCE …), it is possible to use them extensively for Global Security. Through that way, the over costs for industry would be limited.
Many companies are certified ISO 14001 to control environmental impacts. It is possible to imagine some organizational procedures to prevent malicious and terrorist attacks and to reduce their effects & consequences for the company itself but also for neighbours and environment. SNPE is conducting such preliminary research.

Crisis Management & Remediation

Concerning security of critical infrastructures, crisis management is also facilitated if all scenarios are described, consequences are attenuated if adapted procedures are defined, and remediation costs are limited if facilities are specially designed. The risk management described in previous paragraph constitutes the entry data for such concerns.

Conclusions

This paper describes some R&D axes that would be studied especially concerning industrial sites and other critical infrastructures. Indeed, recent attacks have demonstrated that terrorist imagination is limitless. Then, it is difficult to anticipate threats using IEDs, Homemade Explosives, … . Then, it appears that the police investigation and check point controls are not sufficient. It is also necessary to assess critical infrastructure vulnerabilities in the aim to identify threats as completely as possible, to attenuate attack effects, to improve the crisis management and to facilitate remediation. Due to its activities in Chemicals and Energetic Materials as producer but also as R&T specialist, SNPE Matériaux Energétiques can bring significant contribution for improving the Global Security.

Immunisation of Buildings Against Chemical and Biological Threats: Remote Photocatalytic Decontamination

A.V. Vorontsov, Boreskov Institute of Catalysis, Novosibirsk, Russia
Tel. 7(383)3269447, Email: voronts@catalysis.ru
V. V. Nikulin, Lavrentyev Institute of Hydrodynamics, Novosibirsk, Russia
P. G. Smirniotis, University of Cincinnati, Cincinnati, USA

An approach has been suggested to treat the threat of distributing toxic substances or harmful biological microorganisms in buildings as a consequence of terrorist act or an unintentional incident. Minimum casualties are attained by minimizing the time of removal of harmful substances from air. Since the time of decontamination is limited by the speed of pumping air through filters an advanced approach is proposed for quick delivering air into the decontamination unit. Vortex method was shown to deliver contaminated air from remote parts of contaminated space. Photocatalytic destruction is used for irreversible on-site destruction of toxic compounds and biological agents.

Introduction

Terrorism is now generally recognized as one of the top priority threats to global security and peace. The number of terrorists act counts in hundreds per year and this number is increasing from year to year. Russia encountered continuously increasing terrorist activities in the latest years. Recent examples include very cruel and bloody terrorist acts. There are indications that future terrorist attacks in Russia will use not only explosives but also chemical and biological agents for increased effectiveness. While terrorist organizations need very high technologies and equipment to exercise nuclear terrorism (excluding the case of stealing ready nuclear weapons), chemical and biological terrorism is quite feasible with low level of knowledge and technology. There are many examples of recent chemical and biological terrorist acts. In 1994 the Japanese religious sect Aum Shinrikyo undertook an attack with sarin gas in streets of Japanese city Matsumoto. Sarin was released from a moving track. 7 people were killed and over 200 were injured. In 1995 the same sect repeated chemical attack in the Tokyo subway system. Sarin was released in many carriages through holes in plastic bags filled with 10 kg of 30% sarin solution. 12 people were killed and over 5500 were poisoned. During its operation, Aum Shinrikyo was able to produce about 30 kg of sarin without sophisticated technology. In November 2002, terrorists tried to undertake the release of the toxic agent cyan in London subway. Police prevented the act. In 2004, Jordanian authorities prevented the largest chemical terrorist act with 20 tons of various toxic chemicals linked to explosives. Therefore, the problem of prevention and neutralizing chemical and biological terrorist acts urgently requires developing response equipment.

Approach

One of the most probable scenaria of CB terrorist acts includes spraying volatile chemical or dispersed aerosolized biological agents near or in supermarkets, airports, railroad stations, and other public buildings. security against CB terrorism means effective measures not only to prevent the act but also to immediately remove CB agents from the air before they cause casualties and injuries. Thus, the targeted public buildings must become terrorist immune buildings. The concept of terrorist immune buildings provides measures for effective prevention and elimination of consequences of terrorist acts with CB. While dependable remote detectors for explosives are available or are close to be released to the market, remote detectors for CB agents that can work before their release are hardly to be as dependable in the near future. Moreover, the known CB detectors may not be able to detect a new agent. Consequently, prompt elimination of CB agents from the air immediately after any terrorist act becomes the key approach for terrorist immune building.

The proposed ultrafast decontamination setup is a modular construction that contains air delivery module, air filtration module and air pump module.

Remote air delivery

In a scenario of terrorist act in large rooms with many people inside, release of agents or generation of toxic smoke is directed towards lower layers of air. Simple suction of air by, e.g., tube of diameter d results in removal of air at a characteristic distance from tube d. Thus, parts of room at a significant distance from the decontamination unit cannot be quickly and efficiently cleaned by traditional methods.

A well known natural phenomenon – tornado – is capable of taking objects and transporting them for over kilometre distances. We managed to generate a laboratory-scale tornado and test it in a model situation of removal of cigarette smoke from the bottom of a chamber. The figure 1 in the next page shows moments t = 2.8 s, 4.4 s, 6 s and 7.6 s after switching on the vortex generator. One can see that the smoke was pumped through a tube at the bottom of the chamber and accumulated predominantly in the bottom layers of air. In about 5 seconds after switching on the vortex, the smoke at the bottom of the chamber was completely removed.

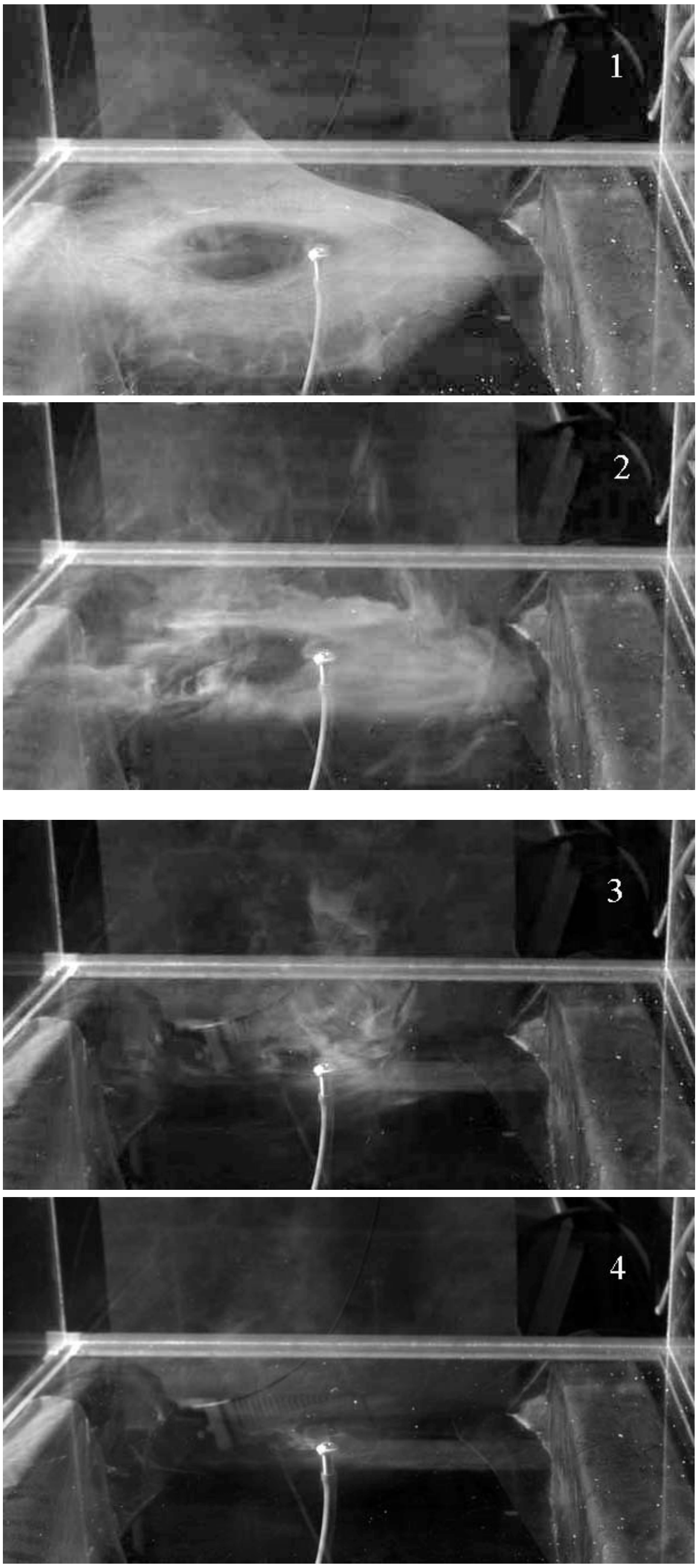


Fig. 1. Remote removal of smoke at the bottom of a closed chamber (volume 100 dm^3) with vortex generated at the top of the chamber

Thus, the proposed vortex approach is capable of selective air removal at determined locations without influencing air in other parts of space.

Photocatalytic filter

Contaminated air is delivered into a filter that should be capable of complete removal of contaminants and their irreversible destruction into less harmful products. Traditional filtration utilizes adsorbents for removal of chemicals and HEPA filters for removal of biological hazards. Both of these approaches just remove contaminants from gas phase into solid phase. If the decontamination unit based on these technologies is destroyed, the captured dangerous agents can be emitted back into air.

Recent research demonstrated that photocatalytic oxidation is capable of destroying both chemical agents and biological agents. Photocatalytic reactions over TiO_2 based materials proceed after absorption of quanta of UV light (□ < 400 nm).

TiO_2 + h□ → $h^+ + e^-$,

Photogenerated holes react with water vapor with formation of extremely reactive hydroxyl radicals

h+ + H2O → H+ + OH$^{\cdot}$.

These radicals destroy any organic materials including chemical and biological agents. The proposed decontamination setup utilizes carefullly designed photocatalytic material that reactively adsorbs chemical and biological agents and gradually destroy them into inorganic non-toxic compounds.

Thus, the problem of creating terrorist immune buildings is being solved by creating decontamination equipment utilizing ultrafast vortex air delivery and photocatalytic filters.

Acknowledgements

Support of NATO SfP Programme via grant 981461 and support of ISTC via project 3305 is gratefully acknowledged.

Novel photoacustic trace gas sensor for security applications

A. Miklós , J. Angster; Fraunhofer IBP, Stuttgart, Germany
Email: angster@ibp.fhg.de

Abstract

The danger of terrorist attacks using toxic industrial chemicals (TICs) or chemical warfare agents (CWAs) has exposed the need for reliable and early detection of trace amounts of such compounds in the air. Sensors for airports, railroad stations, large public and private office buildings, etc. would be required for the early detection of CWAs and TICs so that parts of buildings can be rapidly evacuated.

Photoacoustic (PA) spectroscopy is a powerful tool for trace gas detection. Most of the CWAs and explosives and many TICs absorb light in the wavelength region from 3 to 14 µm with absorption coefficients in the 30–60 cm^{-1} range. Thus, detecting CWAs and TICs at the necessary ppb to sub-ppb levels requires an absorption measurement capability as low as 10^{-8} cm^{-1}. Moreover, the sensor must have very few false alarms to avoid unacceptable social and economic disruptions. The problem of interference rejection is severe because the absorption features of many interferents may overlap with that of the target CWA. This paper presents a PA sensor based on a novel measurement method with excellent interference rejection properties for the selective and sensitive detection of trace amounts of CWAs and TICs in the air.

1. Introduction

Sensitive and selective detection of chemical warfare agents (CWAs) and toxic industrial chemicals (TICs) requires molecule-specific spectroscopic detection methods and sensors. To reach the required sensitivity and selectivity, mostly high-resolution laser techniques in the mid-infrared (MIR) are applied.

The rapid development of solid-state tunable laser sources, such as diode lasers, quantum-cascade lasers, and nonlinear optical devices open up new perspectives for the application of diverse spectroscopic methods (optical spectroscopy with multipass cell[1-2], cavity ringdown spectroscopy[3-5] (CRDS), integrated cavity output spectroscopy[6-8] (ICOS), photoacoustic spectroscopy[9-12], (PAS), quartz enhanced photoacoustic spectroscopy[13-15] (QEPAS), etc.) in trace gas detection. For security applications under atmospheric conditions the pressure-broadened absorption lines (0.1-0.3 cm^{-1}) of gases and the broad absorption features of CWAs and TICs with large molecular weight reduce the significance of the narrow linewidth of diode lasers. On the other hand, larger continuous tuning ranges are needed to achieve the necessary spectral selectivity in multicomponent mixtures. These requirements can be fulfilled by light sources utilizing nonlinear optical effects, e.g. the optical parametric oscillators (OPOs), sources with difference frequency generation (DFG), and optical parametric amplifiers (OPAs). Therefore, these laser sources are currently playing an increasing role in trace gas analysis.

2. Photoacoustic trace gas detection

Photoacoustic (PA) spectroscopy, which differs from optical absorption spectroscopy only in the method of detection, has already found wide-ranging applications in trace gas measurements. Since the photoacoustic signal is proportional to the power of the radiation sent through the PA detector, previous applications of this method have almost exclusively been confined to intense CO and CO_2 lasers in the IR[16-17]. These light sources, however, are only line tunable, and thus the laser and absorption lines must coincide to attain high sensitivities. Solid-state lasers, on the other hand, can be tuned to the peak of the selected absorption line, or they can be scanned over a broader range containing one or more lines of the relevant species. Utilizing these possibilities the drawback of a smaller light power may be overcome. In fact, PA sensitivities comparable to that achieved by CO and CO_2 lasers have been reported[9-15, 18] recently. A photoacoustic gas sensor based on a tunable OPO-DFG light source and an open-multipass PA detector[19] have been successfully applied for detecting CO_2 and methane in the atmosphere.

3. PA measurement of CWAs

High-sensitivity, high-selectivity photoacoustic detection of chemical warfare agents has been reported recently[20] by Pushkarsky *et al*. The applied sensor was a modified version of a practical field instrument that measures ambient ammonia using a line-tunable $^{13}CO_2$ laser with 5 W average output power and a resonant photoacoustic cell. The performance of the laser-photoacoustic sensor was demonstrated by measuring diisopropyl methylphosphate (DIMP), a relatively harmless surrogate for CWAs, in the presence of eight interfering species. A detection threshold of 1.2 ppb with a probability of false positive alarms of < 1:10^6 was determined from the measurements. However, the discrete tuning characteristics of the CO_2 laser is not optimum for obtaining detailed information about the shape of the absorption in the presence of interferents. The observed performance could be further improved by applying continuously tunable IR lasers[21].

4. A novel PA detector

A novel PA sensor based on a miniature IR emitter and a new photoacoustic measurement method[22] for sensitive and selective detection of several species in the atmosphere have been developed at the Fraunhofer IBP. An excellent selectivity has been achieved by a molecule specific modulation of the broadband IR light entering into the photoacoustic measuring cell of the PA sensor. Since the IR light intensity is modulated simultaneously at all absorption lines of the target gas, the PA signal is quite strong.

Interfering PA signal is generated by other species, if they have overlapping spectral features with the target molecule. This may happen in certain wavelength domains, but overlapping of complete absorption spectra of different molecules is unlikely. Therefore, interference by other components can hardly disturb the measurement.

The novel PA sensor has the following advantages:

- The selectivity of the method is very good.
- No modulation occurs at the water and CO_2 absorption lines. Therefore, the water and CO_2 content of the air sample does not contribute to the PA signal.
- Several (up to 15-20) different components can be measured sequentially with the same sensor.
- The sensitivity of the gas detector will be in the ppb concentration range for most of the important gas pollutants.
- The PA sensor contains only very simple and low-cost elements, thus it could be produced cost efficient.

The new PA sensor is intended for indoor air quality, environmental and security applications. It can also be applied for monitoring specific pollutants in process gases.

References

1. P.Weibring, D.Richter, A.Fried, J.G.Walega, C.Dyroff, Appl. Phys. B**85**, 207-218 (2006)
2. J.H. Shorter, D.D. Nelson, M.S. Zahniser, M.E. Parrish, D.R. Crawford, D.L. Gee, Spectrochem. Acta A, **63**, 994-1001 (2006).
3. S.E.Bisson, T.J.Kulp, O.Levi, J.S.Harris, M.M.Fejer, Appl. Phys. B**85**, 119-206 (2006)
4. J.T.Hodges, D.Lisak, Appl. Phys. B**85**, 375-382 (2006)
5. S.Stry, S.Thelen, J.Sacher et al., Appl. Phys. B**85**, 365-374 (2006)
6. J.H.Miller, Y.A.Bakhirkin, T.Ajtai, F.K.Tittel, C.J.Hill, Q.R. Yang, Appl. Phys. B**85**, 391-396 (2006)
7. V.L.Kasyutich, P.A.Martin, R.J. Holdsworth, Appl. Phys. B**85**, 413-420 (2006)
8. M.R.McCurdy, Y.A.Bakhirkin, F.K.Tittel, Appl. Phys. B**85**, 445-452 (2006)
9. C.Fischer, R.Bartolome, M.W.Sigrist, Appl. Phys. B**85**, 289-294 (2006)
10. M.Angelmahr, A.Miklos, P.Hess, Appl. Phys. B**85**, 285-288 (2006)
11. M.E.Webber, M.Pushkarsky, C.K.N.Patel, Appl. Optics **42**, 2119-2126 (2003)
12. J.P.Lima, H.Vargas, A.Miklos, M.Angelmahr, P.Hess, Appl. Phys. B**85**, 279-284 (2006)
13. A.A.Kosterev, Y.A.Bakhirkin, F.K.Tittel, Appl. Phys. B**85**, 133-138 (2006)
14. A.A.Kosterev, T.S.Mosely, F.K.Tittel, Appl. Phys. B**85**, 295-300 (2006)
15. M.D.Wojcik, M.C.Phillips, B.D.Cannon, M.S.Taubman, Appl. Phys. B **85**, 307-313 (2006)
16. S.Bernegger, M.W.Sigrist, Infrared Phys. **30**, 375-429 (1990).
17. P.L.Meyer, M.W.Sigrist, Rev. Sci. Instrum. **61**, 1779-1807 (1990)
18. A.Schmohl, A.Miklós, P.Hess, Appl. Opt. **41**, 1815-1823 (2002)
19. A.Miklos, S-C.Pei, A.H.Kung, Appl. Opt. **45**, 2529-2534 (2006)
20. M.B.Pushkarsky, M.E.Webber, T.Macdonald, C.K.N.Patel, Appl. Phys. Lett. **88**, 044103 (2006)
21. M.E.Webber, M.B.Pushkarsky, C.K.N.Patel, J. Appl. Phys. **97**, 113101 (2005)
22. A.Miklos, J.Angster, patent pending, FPL_Fallnummer: 06F47451-IBP

Explosive Detection: Development of a Chemical Gas Sensor Based on a Surface Acoustic Wave Device

A. Bardet, F. Parret, S. Besnard, P. Montméat and P. Prené, Laboratoire Synthèse et Formulation, CEA Le Ripault, BP 16, 37260 Monts

Abstract:

This work presents the comparison of detection performances of quartz crystal microbalance and surface acoustic wave sensors, coated with the same organic metalled macrocycle thin film, for the detection of explosive vapours. When nitroaromatics vapours, such as TNT explosive, are exposed to these two types of gas sensors, SAW sensor exhibits a large sensitivity of about 166 Hz/ppb against 17 Hz/ppb for QCM-sensor sensitivity. Moreover, for SAW sensor, when common solvents are used as interfering vapours, a different response (in comparison of nitroaromatics vapours exposure) is observed, which demonstrates the selectivity of this sensitive system. This study shows the interest to use SAW sensor performances to detect weak concentrations of explosives vapours.

Introduction

With the increased use of explosives such as nitroaromatics in terrorist attacks the development of an efficient, portable and low-cost explosive detection device has become an urgent worldwide necessity. Chemical sensors present a growing interest because of their high sensitivity and selectivity for various explosive detections such as nitroaromatics compounds. Previous works have demonstrated the interest of quartz crystal microbalances (QCM) as transducers for the detection of explosives such as nitroaromatics compounds, not only as highly sensitivity and selectivity detections, but also for the low-cost and the simplicity of integration. Nevertheless, according to the weak vapour pressure (< ppb) of several particular explosive landmines and in order to have a sufficient sensitivity, surface acoustic wave devices (SAW) are evaluated because of their high sensitivity to change of physical and chemical properties at near the transducer system surface.

The aim of this study is to compare the detection performances of these two transducers, QCM and SAW sensors, coated with the same metalled macrocycle thin film. The targeted explosive vapours are the 2,4 dinitrotoluene (DNT) and the 2,4,6 trinitrotoluene (TNT).

Experimental

The principle of a QCM sensor type is based on the frequency modulation of an oscillating piezoelectric crystal (Fig.1.a). The frequency of a QCM sensor coated with a sensitive layer decreases when molecules are adsorbed on its sensitive layer surface. The frequency variation is then proportional to the increase in mass, according to the Sauerbrey equation. The piezoelectric crystals used in this work are 9-MHz AT-cut quartz crystal with gold-plated metal electrodes on the both sides from AMETEK (model QA9RA-RO). The frequency determination is accomplished through a frequency measurement with a resolution of 0.1 Hz.

SAW sensors (Fig. 1.b) are composed of two interdigital transducers (delay line) on a quartz substrate permitting the generation and propagation of an acoustic wave. Those sensors are based on the reaction between the target gas and the coating modifies the acoustic wave velocity which implies, via the interdigital transducers, a frequency modulation. The SAW sensors used in this work are characterised by a resonance frequency of 100 MHz. this device is composed by two delay lines used as the sensing channel coated by a sensitive layer and the reference one without any film on it. To satisfy the Barkhausen conditions an integrated electronic feedback is inserted in the oscillator loop.

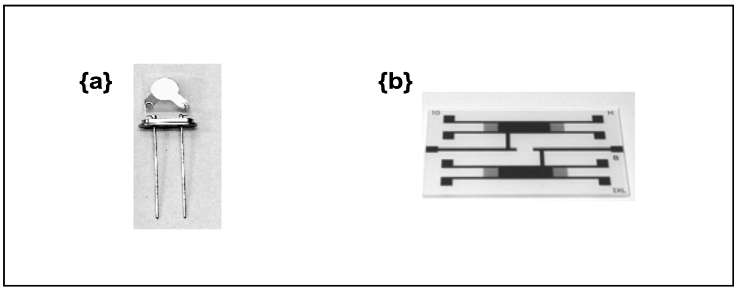


Fig. 1: Views of QCM sensor {a}, SAW sensor {b}.

The chosen sensitive material is an organic metalled macrocycle (a phtalocyanine for example) with a suitable affinity for explosive vapours. This compound is deposited by spray technique and induces a 10 KHz and 100 KHz frequency decreases for each QCM and SAW sensors respectively.

Dry DNT and TNT vapours are generated with a specific testing bench. The generated concentration is closed to the vapour pressure of DNT and TNT for a concentration of 120 ppb and 3 ppb respectively. The detection experiments consist in exposing each coated sensor type to DNT, TNT or interfering compounds for a 10 min duration at room temperature. Gas sensors are tested for a constant flow rate of 20 L/h, in a relative humidity (r.h) rate of 50%.

Results

When QCM and SAW sensors are exposed to several dry DNT vapours concentrations, the frequency responses are slowly decreasing (Fig.2) which implies a DNT adsorption at the surface of the metalled macrocycle thin film. The same behaviour is observed for the two transducers, the only difference concerns the frequency shift (ΔF). Indeed, for a DNT concentration of 12 ppb, a SAW device offers a ΔF of 550 Hz against 12 Hz for a QCM sensor. These Results show that the SAW sensor sensitivity (expressed by the ratio between frequency variation and concentration) is 40 times higher than the QCM response.

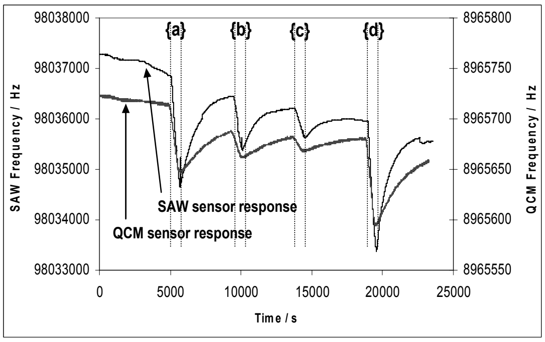


Fig. 2: Effects of 10-min of several concentrations of DNT exposure. {a} 60 pbb, {b} 24 pbb, {c} 12 pbb and {c} 60 pbb.

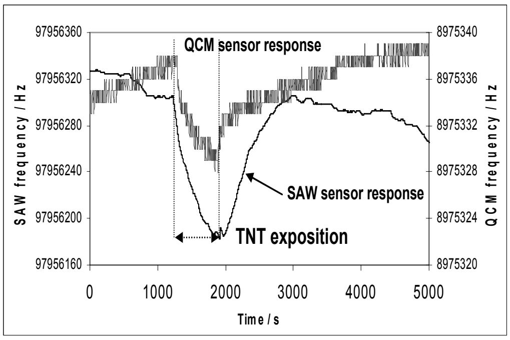


Fig. 3: Effect of 10-min of TNT 3 ppb exposure.

The effects of 50% of r.h on sensors performances are evaluated when gas sensors are exposed to DNT atmosphere at the operating temperature of 25°C. The results show that SAW and QCM sensors responses in dry air atmosphere are twice higher than the ones observed with the moisture conditions.

The SAW and QCM sensors expositions are performed for several TNT concentrations (Fig. 3). We can observe that frequency responses are slowly decreasing for a TNT exposure. When exposed to a TNT-concentration of 600 ppt, the SAW sensor offers a ΔF of about 100 Hz against 10 Hz for the QCM sensor response. SAW sensor offers a sensitivity of 166 Hz/ppb against 17 Hz/ppb for QCM sensor.

At last, the selectivity is tested on sensors performances (Fig. 4). Gas sensors are exposed to 3 interfering compounds. The interfering solvents exposures lead to a lower ΔF (inferior to 100 Hz and 10 Hz for SAW and QCM sensors respectively) for the two sensor types. Moreover, it appears clearly that the kinetic responses are different for DNT, TNT and interfering compounds vapours.

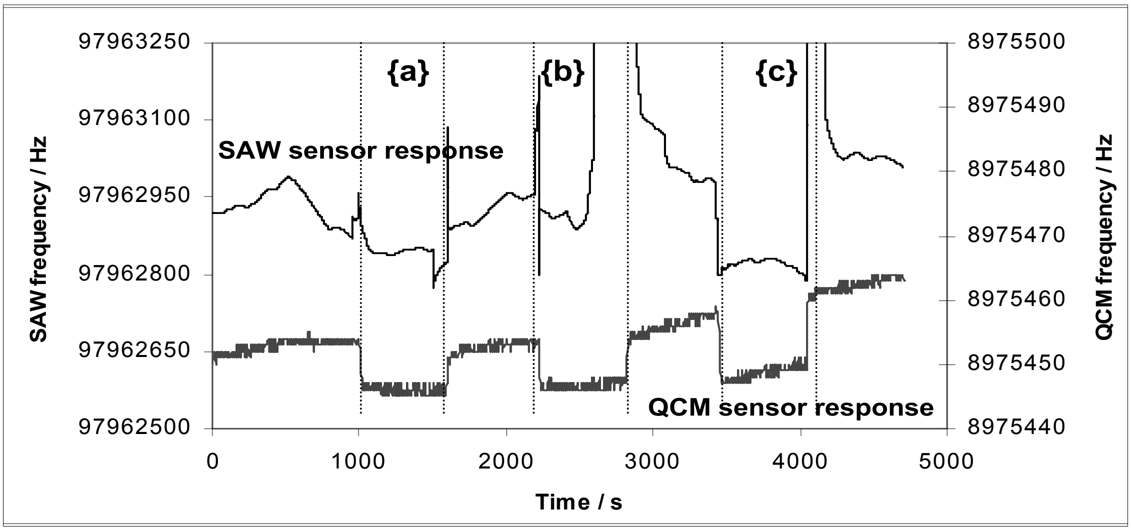


Fig. 4: Effects of 10-min MIBK (100ppm) {a}, C6H12 (600ppm) {b} and CH2CL2 (750ppm) {c} exposures.

Conclusion

A surface acoustic wave sensor, characterised by a resonance frequency of 100 MHz, offers a better sensitivity in comparison of the use of 9-MHz quartz crystal microbalance sensor, for the detection of explosive vapours. Sensitivity results, obtained on these two types of gas sensor, demonstrate the interest to use SAW sensors. Effectively, SAW device offers a DNT-sensitivity of 46 Hz/ppb against 1 Hz/ppb for QCM sensor. For TNT exposures, SAW sensor sensitivity is 10 times higher than a QCM sensor. This study demonstrates that a SAW device able to detect explosive vapours with suitable selectivity capability. We are now focusing on the time response, the stability of the device and the sensor life time before the design of a portable SAW detector.

Terahertz sensor for stand-off detection of explosives

R. Beigang, M. Theuer, J. Jonuscheit, Fraunhofer IPM, Germany

Abstract:

Terahertz radiation offers a high potential to be a useful technology for the detection of hidden explosives and related chemical substances by spectroscopic measurements. In particular, the frequency band between 100 GHz and 10 THz combines the advantages of the neighbouring spectral ranges: the transparency of dielectrics known from the microwaves and the spectral fingerprints of the infrared radiation. As a consequence, spectral features of most explosives in the terahertz range can be identified even under the surface of non-metallic packaging. Properties of terahertz radiation relevant to the detection of explosives are discussed and a standard terahertz system is presented.

Introduction

Different danger scenarios show threats hidden in e.g. cars, luggage or under clothing. So in military and civil security applications there is the urgent need to have an instrument for stand-off detection of explosives. But still there is no device to detect explosives or explosive related compounds (ERCs) with all the possible diversities like packaging, mixture, concentration, gas pressure etc. Detection in the terahertz (THz) spectral range is a feasible technique which offers solutions to some critical applications.

Properties of THz radiation

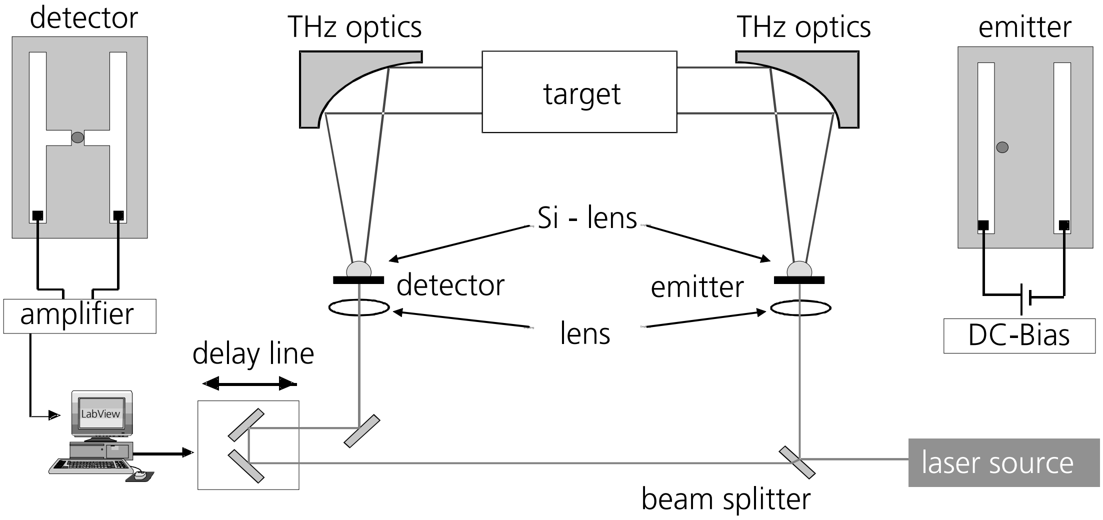
THz radiation covers the spectral range of 100 GHz up to 10 THz within the electromagnetic spectrum. The related wavelength range starts below 30 µm and reaches 3 mm. This band bridges the gap between microwaves and infrared radiation. The photon energy of one THz photon is less than 1% compared to a photon in the visible. Typical active THz systems use some microwatts to few milliwatts of optical power for illumination. This radiation is non ionizing and doesn’t change any chemical property. Therefore it’s completely safe for operator and target.

Possibilities and Limits

One major advantage of THz waves is their high transparency of most dielectrics. This allows for the detection in e.g. bags, packaging or under clothes. In addition the spectral characteristics of most explosives and ERCs are significant and specific [1]. Spectral fingerprints from chemical substances [2] are also known from the infrared range and are caused here by either inter or intra molecular vibrations.

THz radiation can not penetrate metals or liquid water. Also the humidity in compartment air has discrete absorption lines in the THz range. This limits the accessible distance for stand-off detection to some meters and cuts out some discrete lines within the bandwidth of the system.

Setup



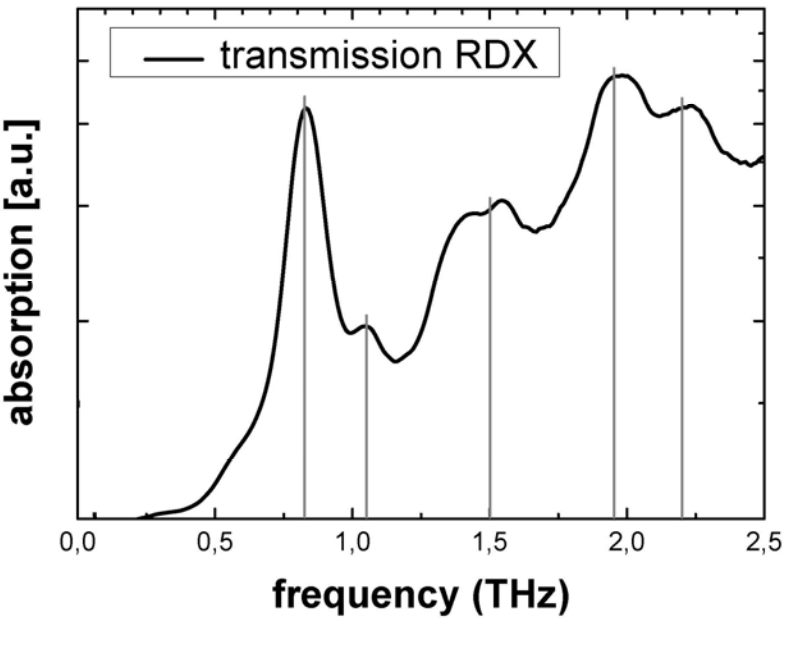
THz radiation can be generated electronically or optically. In the following we focus on pulsed THz systems which are pumped by ultra short laser pulses. This is an efficient way to generate and detect broadband THz radiation with a bandwidth which matches the region of specific absorptions of most explosives and ECRs but still allows for sufficient transmission through most dielectrics.

A typical THz setup consists of a laser source (e.g. Ti:Sapphire laser, fiber laser), optics including a delay line and a THz emitter/detector. These components define the spectral resolution and the scanning speed of the system. Typical data acquisition times are in the Hz range and spot sizes in the THz focus are approx 1 mm × 1 mm.

By measuring in the time domain (here as a function of optical delay) one gets the complete electric field of the THz pulse. This includes the amplitude, phase and time shift (tomography). A Fourier transformation leads to spectrum.

In principle THz systems can be used in reflection or transmission geometry. For applications in stand-off detection of explosives the THz systems have to work in reflection as transmission measurements are not practicable for this purpose.

Results



As example the measured THz absorption spectrum of RDX in transmission is shown. The broad attenuation bands are clearly identified and agree with the published data by X.-C. Zhang [3], as indicated by vertical grey lines. Various data is available from different sources, in reflection und transmission. Most ERCs show spectral features in the THz range. However, these features are strongly influenced by humidity, particle size, additives and surface shape. Therefore the raw data have to be analyzed carefully using known spectra from explosives, transmitted materials, different particles sizes etc.

In principle, even for raw data influenced by the above mentioned reasons filtering, oversampling or applying chemometric methods can reveal the content of the spectra.

Applications

The use of THz radiation does, of course, not allow for the detection of all hazards, especially in hydrous environments or under metallic surfaces. However, the possibility to do a spectroscopic analysis is a unique feature of this technique. The combination of THz spectroscopy together with other imaging techniques like microwaves or visible imaging can lead to a useful system for stand-off detection.

Thus, THz radiation offers the possibility to identify bulk ERCs in a reflection scheme by spectroscopy and in combination with other techniques this would be stand-off, non ionising, without artificial airflow and without the need to take a sample [4].

Outlook

THz spectroscopic systems are, in principle, well suited for the stand-off detection of explosives and ERCs. The development of pulsed laser sources will reduce the size of the systems. Improvements towards fiber coupled THz emitters and detectors will make the systems more flexible and stable. The overall costs will be reduced by using already available telecom components. These ongoing steps may eventually lead to complete commercially available THz systems that can be used as a security device at any check or control point.

[1]J. Federici, D. Zimdars et al, “THz imaging and sensing for security applications” Semicond. Sci. Technol. 20 (2005) S266-S280

[2]K. Kawase et al, “Non-destructive terahertz imaging of illicit drugs using spectral fingerprints”, Opt. Express, vol. 11, no. 20, pp. 2549-2554 (2003)

[3]H.-B. Li, X.-C. Zhang et al, “Detection and identification of explosive RDX by THz diffuse reflection spectroscopy”, Opt. Express, vol. 14, no. 1, pp. 415-423 (2006)

[4]M. Theuer, R. Beigang et al, “Detection of Explosives by Terahertz spectroscopy” (German), Workshop: Detection of Explosives, Fraunhofer ICT, Karlsruhe (2007)

IR modules and devices for security applications

Rainer Breiter (rbreiter@aim-ir.de), Dr. Mario Münzberg

AIM INFRAROT-MODULE GmbH, Theresienstr. 2, 74072 Heilbronn, Germany

Abstract

Key requirements for military and non military security tasks are early detection of threats, superior situation awareness and if inevitable precise weapon engagement on time.

IR-Detectors sensitive from the short (SWIR) to the long wave (LWIR) IR spectrum provide the solution to many of these requirements. Based on state of the art detector technology from AIM's portfolio, thermal imagers have been developed to fill the new capability gaps of the Bundeswehr and allied nations. AIM's thermal imager µCAM for the LUNA reconnaissance UAV provides invaluable real time information from various conflict areas. With HuntIR, AIM developed the only long range reconnaissance sight, which withstand the recoil of long range small arms for precise engagement of an identified threat. After international competition, HuntIR was selected for the German Army "Infanterist der Zukunft" (IdZ) programme.

The next member of the thermal imager family will be the RangIR sight with integrated laser range finder and 3 axis digital magnetic compass for accurate long range fire control and target location. A SWIR version providing daylight-like imaging to identify persons from available photographs will follow.

Most recent 3rd generation IR technology provides spectral information to detect e.g. agents. Missile approach warning systems to protect military or civil aircraft against the threat by manpads is another important application of this technology.

Introduction

As a supplier of state of the art IR technology AIM produces first and second generation linear arrays, dewars and cryocoolers since the late 1970's. AIM's most recent product family of IR detection modules covers a variety of two-dimensional focal plane arrays (FPA's) on the basis of mercury cadmium telluride (MCT), quantum well infrared photodetectors (QWIP's) and superlattice (SL) detectors providing 3rd generation dual-band and dual-color imaging capabilities. FPA detectors are mounted in integrated dewar cooler assemblies (IDCA's) with noiseless split linear cooling engines or integral rotary coolers for better efficiency ratio. Flexible programmable driving electronics with integrated analog to digital converter in miniaturized packages are available with each module. Miniaturized high speed video processors, which allow real-time non-uniformity correction with replacement of dead pixels according to AIM standard or customer specific procedures have been developed. In an additional integration level the IR detection modules and electronics are assembled to complete thermal imaging solutions e.g. for thermal weapons sights or UAV IR sensor payloads.

IR image taken with an reconnaissance UAV

Thermal Imaging Devices

AIM's choice for portable thermal imagers concentrate on mid-format FPAs due to the size, mass and power restrictions. In case of long range requirements the MCT 384x288 MWIR detection module is used providing even with slow F-numbers like F/7.5 an excellent performance. For shorter range applications AIM is developing thermal imaging devices based on uncooled microbolometer LWIR detectors with formats like 320x240 or 384x288.

The HuntIR / RangIR thermal weapons sights

The development of its HuntIR family of thermal imaging devices was launched by AIM due to demand of the German Infantry and Special Forces requiring a thermal weapon sight combining long range battlefield surveillance and target engagement purposes. State of the art small arms with ammunition from 12.7mm to 40mm provide engagement ranges beyond 1500m against various target classes. Sighting scopes provide excellent performance at day but even with image intensifiers only poor range performance at night is achieved. On the other hand the existing portable thermal sights for reconnaissance provide the required long range identification capability during night comparable to ranges of first generation systems in battle tanks. However they were not designed to be used on long range small arms i.e. to withstand the strong recoil of weapons and to provide the necessary line of sight stability to precisely hit targets in large distances. HuntIR is a thermal weapon sight for small arms with this unique feature of long range surveillance and targeting capability to fill this gap. During 2004 the final development and qualification phase has taken place and since November 2004 the device is in service for the German Army within the IdZ basic system program.

The HuntIR/RangIR devices make use of a modular architecture where most of the components are designed and fabricated by AIM. Core component of the HuntIR/RangIR devices is the AIM MCT 384x288 MWIR integrated detector dewar assembly. Even at a f-number F/7.5 a device NETD including lens transmission of typical 25mK with an integration time of 20ms is achieved. The lens is a fix focus assembly providing two field of views (FOV). The narrow field of view (NFOV) with 3.0°x2.3° provides and identification range of >1500m according to the FGAN-FOM TRM3 Range model even for bad weather condition. For the RangIR an additional electronics module was added to serve the new components LRF and DMC as well as providing a ballistics calculator for automatic fire control and new interfaces for video distribution and external control. The LRF allows eye-safe operation at 1.5µm and range measurement up to 2500m. Together with data of the 3-axis DMC automatic fire control is provided using results of the ballistics calculator.

HuntIR/RangIR performance data

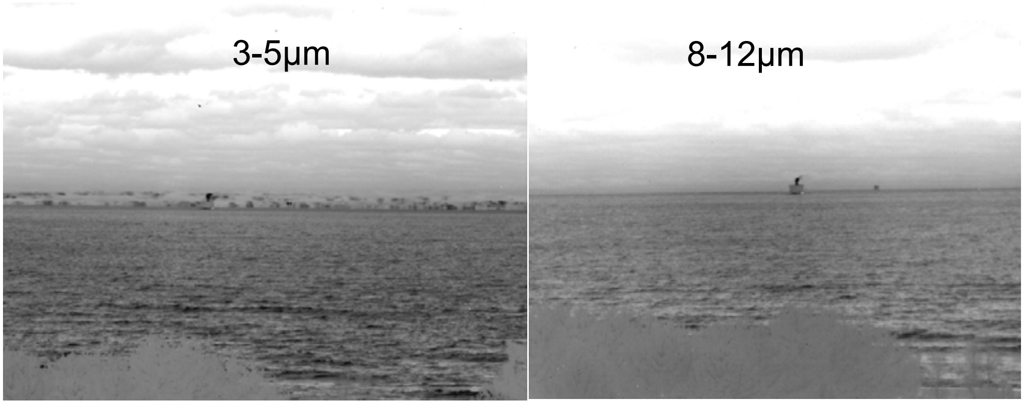
FOV	Dual FOV lens, NFOV 2.3°x3.0°, WFOV 6.8°x9.1°	
ID-Range	>1500m	
LRF	eye-safe 1.5µm	(RangIR only)
DMC	3-axis	(RangIR only)
Mass	<3kg	(RangIR <3.3kg)
Operation time	>3h	

HuntIR/RangIR thermal weapon sight

3rd Generation IR Technology

The 3rd generation of infrared detection module technology provides advanced features such as high resolution HDTV pixel formats of 1024x1024 or 1280x720, new functions like multi color or multi band capability, or higher frame rates with even better thermal resolution. Requirements for simultaneous detection of infrared radiation in different wavelength bands or spectral ranges within one band are driven by the significant increase in reconnaissance performance. Spectral detection is required for improved missile warning sensors to decrease reaction time and false alarm rates, other benefits are for automatic target recognition due to specific emissivity features or to find camouflaged targets. Specifically dual band detectors simply provide the benefit, that the pros and cons of both bands like smaller blur spot for longer ranges and better performance in hot humid areas for the MWIR on one side, and better performance in case of stray light or close to hot sources for the LWIR suddenly can be combined in one FLIR. These requirements pushed the development of multi color or multi band IR detectors. High frame rate detection modules are generally essential for the development of missile seekers and missile warning systems. Early warning stand-off chemical agent detection and mapping of contaminated terrain for force protection in a “dirty” battlefield environment as well as monitoring of surface pollution and contamination at toxic waste sites, chemical plants, ports and harbors is another field of spectral selective measurements in the infrared wavelength range between 2 and 11 µm. In this case high spectral resolution is reached with standard long linear FPA with a high number of pixels whereas the width of the pixels should be as small as possible.

QWIP and antimonide based superlattice modules are developed and produced in a work share between AIM and the Fraunhofer Institute of Applied Solid State Physics (IAF). The sensitive layers are manufactured by the IAF, hybridized and integrated to IDCA or camera level by AIM. In case of MCT based modules, all steps are done by AIM.



MWIR / LWIR image of naval environment

Concepts for low-cost sensors detecting gaseous explosives such as TNT

G. Bunte, J. Hürttlen, H. Pontius, D. Röseling, H. Krause,
Fraunhofer Institut für Chemische Technologie ICT
Joseph-von-Fraunhofer-Str. 7, D-76327 Pfinztal (Berghausen)

Abstract

Recent terrorist attacks like the bombing in New York at 11.9.2001, suicide bombings in the middle east or e.g. the London Underground bombing in July 2005 show that the today used detection techniques for explosives (Imaging by X-ray, neutron activation techniques, IMS, TeraHz-, MMwave, NQR,) are inadequate and have to be improved as well as new counter-action / detection concepts have to be developed. For the detection of explosives e.g. at airports, for humanitarian demining and in concerns with national security there are needs for inexpensive, rapid, high sensitive and selective sensors.

In this concern mass-sensitive devices coated with substance specific molecularly imprinted polymers (MIP) seem to provide promising low-cost detection devices for use in self-reporting sensor networks for the surveillance of public areas or as on-line / in-line sensors in different vehicle transportation systems (cars, trucks, containers etc.) in order to directly detect and warn for possible terrorist threats by hazardous components.

1 The technique of molecular imprinting

The technique of molecular imprinting allows the formation of specific recognition sites in macromolecules. In this process functional and cross-linking monomers are copolymerised in the presence of a target analyte (template). The functional monomers form a complex with the imprint molecule and in the following polymerisation the functional groups are held in position by the highly cross-linked structure. Subsequent removal of the template reveals binding sites that are complementary in size and shape to the analyte. The complex between monomers and template can be formed via reversible covalent bonds or via non-covalent interactions like hydrogen bonds.

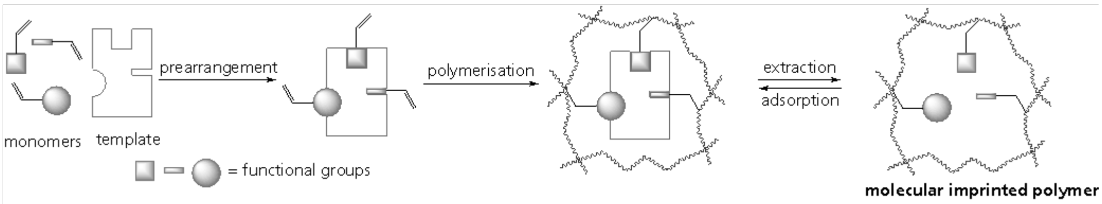


Figure 1: principle of molecular imprinting

For TNT as template it is not possible to use the covalent approach. Furthermore with the non-covalent approach we are able to use a large pool of functional monomers that are commonly used in the field of molecular imprinting. Because of the known problem that nitro-aromatics are weak hydrogen bond acceptors /1/ for the synthesis of layered MIPs we used several acrylates with different functional groups as monomers (Figure 2) and ethylene glycol dimethacrylate (EGDMA) as cross linking agent.

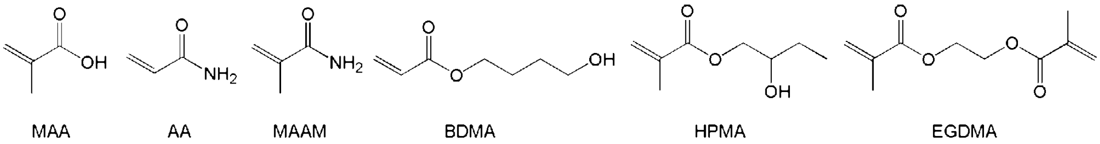


Figure 2: Tested monomers (MAA: Methacrylic acid, AA: Acrylamide, MAAM: Methacrylic amide, BDMA: Butandiolmonoacrylate, HPMA: 2-Hydroxypropylmethacrylate) and used cross linker EGDMA

2 Experimental

Synthesis and performance of TNT- and DNT-specific MIPs were achieved and tested as particulate material as well as thin film coatings on so called quarz crystal micro balances, QCMs. In the latter case synthesis was performed directly on the mass-sensitive sensor surfaces using a UV light for the polymerisation of the MIPs. For testing of performance of the MIPs (sensitivity, selectivity etc.) a special gas generator providing a certain TNT- or DNT gas concentration was used. In case of the thin film coatings the TNT uptake was directly measured via the decreasing QCM frequency of the treated MIP layers. For QCM measurements a commercial gaslab (ifak, Magdeburg) with quartzes having a ground frequency of 10 MHz were used.

3 Results and discussion

Despite the known inhibition of radical polymerisations by nitro groups and the known shrinkage of the polymer lattice during / after drying we were able to synthesize TNT- and DNT-specific particulate MIPs by suspension polymerisation as well as thin MIP coatings by direct surface polymerisation of spray-gunned QCMs. The best method to purify the porous beads was soxhlet extraction followed by supercritical carbon dioxide extraction (SFE with sc-CO_2) at mild conditions (150 bar, 50°C). At least a removal of > 99.7 % of the template was achieved. Performance tests of TNT imprinted polymer beads showed that acrylamide (AA) and more pronounced also methacrylic acid (MAA) possessed an enhanced adsorption tendency for gaseous TNT. An adsorption of 2,4-DNT by these MIPs was not detected. Using 2,4-DNT as template and methacrylamide, MAAM (only monomer tested until now), a positive imprint effect for gaseous DNT was achieved with no measurable cross-sensitivity for TNT.

The thin MIP coatings directly synthesized on the QCMs showed thicknesses of 20 to up to 500 nm. Preliminary screening experiments were done for five different monomers and three different solvents (acetonitrile, chloroform and dimethylformamide). Best adsorption properties for TNT vapour until now showed a PAA-MIP synthesized with chloroform. Direct measurements of the mass attachment, respectively frequency decrease of the coated QCMs during vapour treatment showed a TNT-uptake of about 150 pg per µg MIP per hour.

Results look worthy for further studies. For practical applications in principle different sensor platforms are thinkable such as cantilevers, field effect-transistors, surface acoustic waves and others providing all the possibility of mass-production. By this low-cost sensor elements for the substance selective detection of explosives are producible. Further work will be done to achieve pre-adjustable film thicknesses dependent on the frame conditions of the addressed different sensor platforms using improved coating procedures / techniques.

4 References

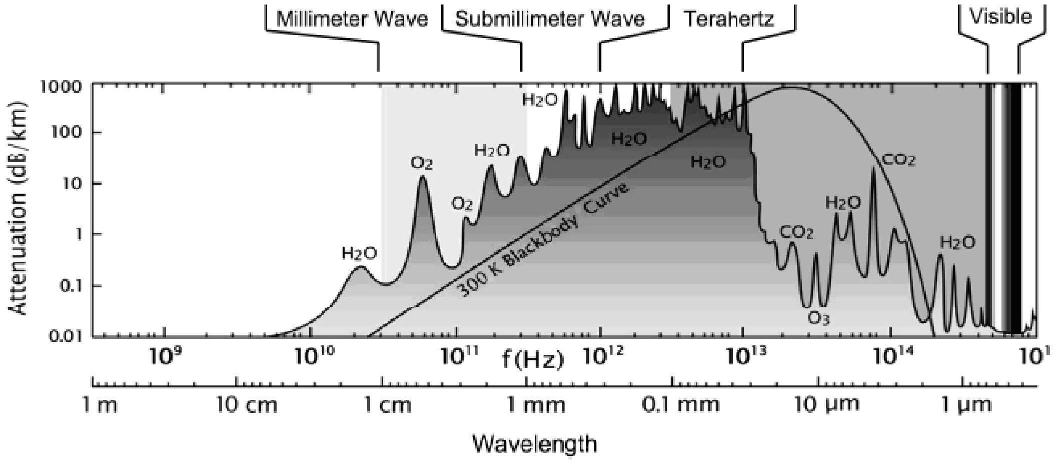
/1/ W. F. Baitinger, P. R. Schleyer, T. Murty, L. Robinson, Tetrahedron, 1964, 20,1635-1637

Millimeter-Wave Radar Sensorics for Security Applications

A. Dallinger, S. Bertl, J. Detlefsen
Technische Universität München, Lehrstuhl für Hochfrequenztechnik
Fachgebiet Hochfrequente Felder und Schaltungen
Arcisstr. 21, 80333 München, Germany
www.hfs.ei.tum.de

Abstract:

Security today plays a major role for technology improvement and systems development. For instance body scanners, commonly operated at critical infrastructures, are basically metal detectors and therefore are not able to detect other potential hazards like ceramics or explosives. Radar systems, working in the millimeter-wave (MMW) frequency range (30 GHz to 300 GHz) already showed applicability. MMW are non-ionizing and do not present a health hazard to people under surveillance. For security checkpoints these facts provide a save operation with respect to humans. MMW readily pass through many optically opaque materials such as clothing fabrics. In contrast to the THz region (300 GHz to 10 THz) atmospheric characteristics are appropriate for operating radar systems over several hundreds of meters distance. The costs of components increase dramatically with frequency and ready-to-use technologies for CCD like imaging are not available. Commercial systems for the civilian market thus have to manage with a reduced amount of subcomponents contrarily to real-time imaging concepts where usually many receivers in parallel are needed. Based on the work done towards the development of an active MMW Synthetic Aperture Radar imaging system this paper gives an overview about other existing sensor concepts and provides a comparative study, e.g. between active and passive systems with respect to image quality and expected limitations.



Introduction

The technology for MMW and THz security applications is expanding rapidly internationally. Yet there is insufficient technology available to develop a system capable of identifying concealed objects and threats. Effort is continued to be increased for security, but also medical, non-destructive inspection, and manufacturing quality-control applications. The THz range which is supposed to provide spectroscopic features is still under exploration, since only in the near past sources and appropriate receivers have been developed. The regarding equipment has reached laboratory standards but can not be integrated into a compact system due to bulky dimensions, high prized devices and their rather low availability. The attenuation of the electromagnetic spectrum caused by the earth's atmosphere is shown on the right. In contrast to the MMW region, which provides low attenuation and broad propagations windows, attenuation within the THz region rises up to 100 dB/km, i.e. medium and long-range applications become unrealistic.

MMW Imaging of Humans

The electromagnetic spectrum from MMW through THz is suited well both to create an image of an object by measuring the intensity of the scattered or emitted energy and to gather information on the physical properties, e.g. the dielectric constant of an object. It also provides transmission through optically opaque layers and passes through many materials such as clothing fabrics. In contrast to THz frequencies, the equipment required for the generation of MMW signals is less expensive while the wavelength is still small enough to obtain sufficient resolution.

Since the angular resolution of real aperture radars is inversely proportional to the operating frequency and proportional to the apertures size it would be desirable to use a frequency as high as possible and an aperture as small as possible. In fact there are limitations given by components, costs and atmospheric propagation.

We propose the usage of Synthetic Aperture Radar (SAR) systems, which overcome the necessity of big apertures in order to get good resolution by sampling the scattered field along a virtual big aperture just by moving a small sized real antenna. These systems have to be coherent and lateral resolution lies within the order of the antenna's dimensions. There are two general classes of imaging techniques: passive and active.

Passive Radar Sensorics

Passive means that the spectral distribution of natural radiation, which is emitted or reflected from a body at environmental temperatures, is captured (radiometry). Outdoors one can obtain acceptable, but weather dependent image quality from objects on human bodies. The radiometric temperature contrast between the objects reflecting radiation from the cold sky and the warm human body is relatively high. Indoors, however, the temperature contrast between the walls of the room, the hidden objects and the human body as the background is much lower and image generation usually is not possible due to today's limited receiver's sensitivity. Additional sources for illumination have to be installed [1]. Systems already on the market are mostly operated in Ka- (26.5 GHz … 40 GHz) or W-Band (75 GHz … 110 GHz) [2]. One type of systems is based on folded optics whereas a tilted rotating disc scanner focuses the scene mechanically. Systems from Qinetiq [3] and Smiths Detection (Farran Technologies) [4] are among those. Another class of systems belong to the focal plane principle where a sufficient amount of detectors are placed within the focus of an aperture, e.g. a lens. Due to a simultaneous readout of the detector's output real-time images are generated. There exists systems from Millivision [5] and Brijot Imaging Systems Inc.. A third class is based on a frequency scanned aperture and massive parallel readout of a Rotman lens, see. Trex Enterprises [6].

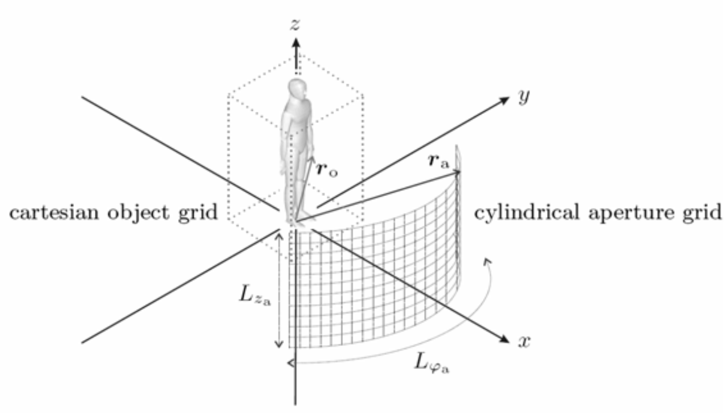
Active Radar Sensorics

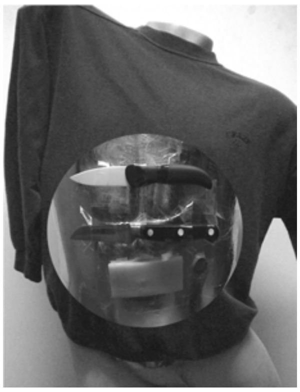
Active MMW imaging systems illuminate the detection space with a broadband beam of MMW power, either by illumination of the entire space or as a focused beam scanned over the object. The detectors preserve the phase information of the transmitted signal. This gives the active radar ranging capabilities. The range resolution is inversely proportional to the systems overall bandwidth. For instance in order to obtain a range resolution of 1.5 cm a system bandwidth of 10 GHz is necessary. Such a large bandwidth can be easier realized at higher operating frequencies, e.g. in W-Band.

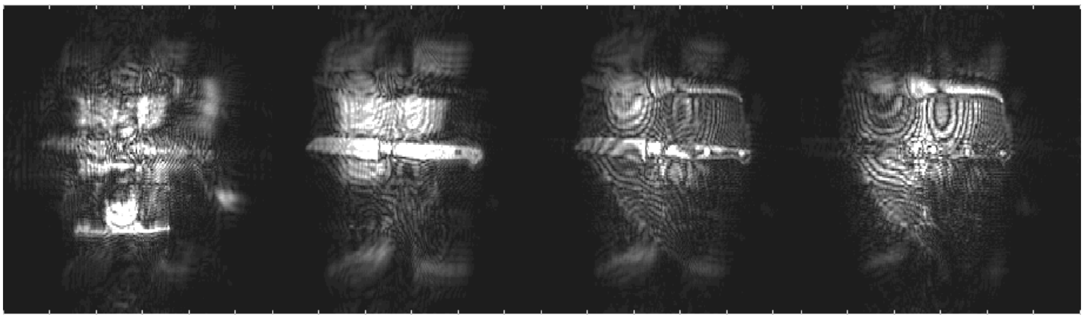
Systems developed are mostly in Ka-Band. The U.S. Department of Energy's Pacific Northwest National Laboratory (PNNL) has developed a broadband active and tomographic MMW scanner at around 30 GHz. PNNL has entered into a commercial relationship with SafeView Inc., a division of L-3 Comm. Agilent Technologies is developing a real-time MMW (raster-) imaging system based on a reflective array at 24 GHz. The beampattern of the reflective array can be electronically tuned in order to generate a confocal MMW lens. Smiths-Detection (Farran Techn.) developed an active system at 77 GHz based on the company's own passive radar system.

3D-SAR Imaging at TUM

At Technische Universität München several active SAR approaches have been considered. Based on a cylindrical synthetic aperture a three-dimensional image can be resolved. Data is taken at 90 GHz to 100 GHz. The Figure below shows slices of the three-dimensional reconstructed data of a PVC dummy clothed with an ordinary pullover. The image's resolution is better than 5 mm. Objects worn beneath clothes are clearly visible. These are a ceramic knife, a metallic knife and a wax plate (used as an explosive simulant material).


z
y
$\boldsymbol{r}_\mathrm{o}$
$\boldsymbol{r}_\mathrm{a}$
cartesian object grid
cylindrical aperture grid
L_{z_a}
x
L_{φ_a}





Conclusion

MMW/THz technology can contribute to overall security, but its limitations need to be recognized and it will be most effective when used in conjunction with sensor technologies that provide detection capabilities in additional frequency regions. MMW/THz technology in portal applications has been demonstrated for detecting and identifying objects concealed on people. MMW are well suited for small, medium and long range perimeter and intrusion detection applications providing features like localization, tracking, classification and detection of hidden objects during day and night, at bad weather conditions and can see through optical barriers like smoke.

Bibliography

1. Coward, P.R. and R. Appleby. *Development of an illumination chamber for indoor millimeter-wave imaging*. in *Passive Millimeter-Wave Imaging Technology VI and Radar Sensor Technology VII*. 2003: Proceedings of SPIE.
2. Lüdi, A., *Passive Abbildende Systeme im mm-Wellen Bereich*, in *IAP Research Reports*. 2000, Institut für angewandte Physik, Universität Bern: Bern, Switzerland.
3. Sinclair, G.N., R.N. Anderton, and R. Appleby. *Outdoor passive millimetre wave security screening*. 2001.
4. Doyle, R., et al. *Low Cost Millimetre Wave Camera Imaging up to 140GHz*. in *34th European Microwave Conference*. 2004. Amsterdam: Horizon House, EuMA.
5. Huguenin, G.R., *The Detection of Hazards and Screening for Concealed Weapons with Passive Millimeter Wave Imaging Concealed Threat Detectors*. 2005, Millivision Technologies: South Deerfield, Massachusetts. p. 9.
6. Clark, S., et al. *A real-time wide field of view passive millimeter-wave imaging camera*. 2003.

Hilbert spectroscopy of liquids for security screening

Y. Divin, U. Poppe, K. Urban
Institute of Solid State Research, Research Centre Juelich, 52425 Juelich, Germany

An unambiguous identification of liquids could be realized by measurements of their dielectric permittivity functions ε(*f*) in a broad frequency range between sub-GHz and THz ranges, but this range cannot be covered by any single conventional technique. A new type of spectroscopy, Hilbert transform spectroscopy, demonstrated a spectral range from a few gigahertz to a few terahertz with a scanning time as low as several milliseconds. We describe our approach to liquid identification, its comparison with other possible techniques and planned realization with Hilbert transform spectroscopy.

Introduction

After recently uncovered terrorist plots involving the mid-flight detonation of liquid explosives, it became clear that an additional screening of passenger's luggage is required. The goal of this screening should be to find and identify particular sorts of liquids, which might be dangerous themselves or could be used as components for fabrication of explosives on board. The screening should be so fast and specific that it should not disturb a normal flow of passengers and operate with low frequency of false alarms.

Among various discussed ways of explosive detection, the techniques using electromagnetic radiation (i.e. microwave and terahertz imaging and spectroscopy), are considered as having a great potential, and intensive research activities are recommended in this field by experts of US National Academy [1]. In this paper we present our approach to identification of liquids, based on Hilbert-transform spectroscopy [2].

Dielectric function

From the point of view of electromagnetic theory, the electric displacement-field response of a substance to a rapidly varying electrical field is defined by a complex dielectric permittivity

$$\varepsilon(f) = \varepsilon_1(f)+i\cdot\varepsilon_2(f), \qquad (1)$$

which is determined by the internal dynamics of the molecules [3]. Therefore a substance can in principle be identified by measuring the dielectric function ε(*f*) of this substance over a wide range of frequency *f* and comparing it with available reference data.

The internal dynamics of liquids can be considered to a first approximation as an alignment of dipoles by the local electric field following a Debye relaxation process [4]. In this case the dielectric permittivity function can be written as

$$\varepsilon(f) = \varepsilon_\infty + (\varepsilon_0 - \varepsilon_\infty)/(1+i2\pi f\tau), \qquad (2)$$

where ε_∞ is the “infinite frequency permittivity”, ε_0 is the static permittivity and τ is the characteristic relaxation time. The dielectric functions of some pure liquids, which were calculated using Eq.2 and available data [4-6], are shown in Fig. 1. In real liquids, due to the interplay of orientational, intramolecular, kinetic, H bonding, diffusional and migrational modes, the dielectric function ε(f) is more complicated. This is favourable for detection purposes since the frequency dependence is more specific to a particular liquid [4-6].

The techniques to measure the dielectric properties of liquids in the frequency range of up to about 100 GHz have recently been reviewed [7]. The reflection, transmission and resonator microwave techniques at fixed frequencies are the main conventional approaches in the field. However, due to non-monotonous behavior of the permittivity of two-component solutions with increase of a concentration of one component [5,6], the measurement of the dielectric function at fixed frequency, or even at a few preset spot frequencies cannot distinguish unambiguously between some solutions and the liquids of concern. This makes such approaches unreliable, and since the safety system must react in both, harmless and safety-relevant cases, this should give rise to a high rate of false alarms.

To study fast dynamics in liquids, continuous measurements in the terahertz frequency range have been performed using time-domain spectroscopy (TDS) [8-10].

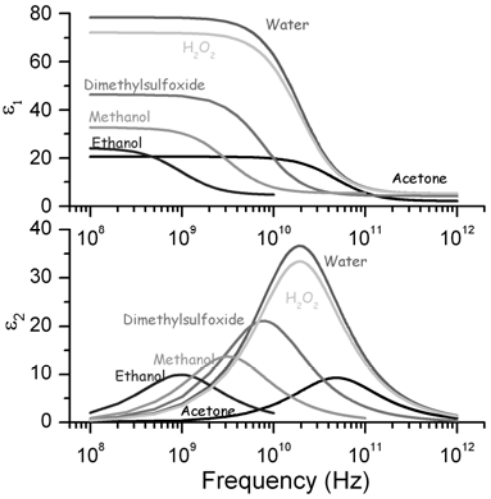


Fig. 1. Real and imaginary parts of the dielectric functions of various pure liquids at 25 °C [4-6]

Transmission spectra of some inflammable liquids like benzene and kerosene, stored in conventional beverage plastic bottles, have been measured in the frequency range from 300 GHz to 1.8 THz [10]. From this measurements a crude inspection principle was derived following the rule *“If liquids transmit terahertz radiation, it is dangerous, if not - it* *is water"*. With this criterion in practice, acetone and hydrogen peroxide would clearly escape detection, due to their large absorption in the terahertz range. We note also that terahertz TDS involves extended measurement times, typically of a few minutes, since a mechanically driven optical time-delay line is used for gated operation [8,9].

Hilbert-transform spectroscopy

In contrast to the conventional techniques, Hilbert-transform spectroscopy [2] (in the following abbreviated by HITRAS) represents a fast technique operating in the frequency range of a few GHz to a few THz, and thus can make an unambiguous identification of dangerous substances within short times.

The central part of the Hilbert spectrometer is a nanoelectronic device, a Josephson tunnel junction. Special bicrystal Josephson junctions, made from the high-temperature superconductor $YBa_2Cu_3O_{7-x}$, were developed for HITRAS [2]. A nanostructure and a microphotograph of the junction with an Ag broadband sinuous antenna are shown in Fig.2.

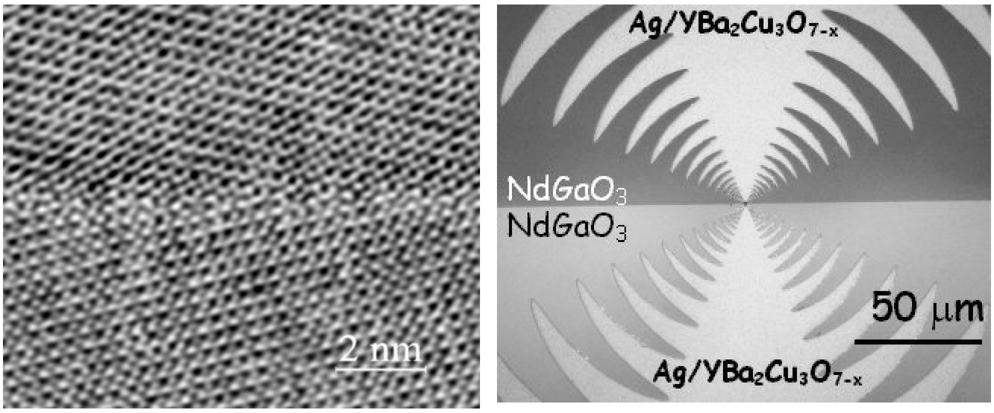


Fig. 2. High resolution transmission electron microscopy image of a grain boundary of a $YBa_2Cu_3O_{7-x}$ bicrystal Josephson junction (left) and micrograph of the junction (point-like contrast in the centre) with integrated broadband antenna for Hilbert spectroscopy (right).

If a Josephson junction in the resistive state is irradiated by electromagnetic radiation the electrical response function $H(V) \propto \Delta I(V) \cdot I(V) \cdot V$ (where V is the voltage across the junction, $I(V)$ is a current through the junction and ΔI(V) is a current response of the junction to radiation) is proportional to the Hilbert transform of the spectrum *S(f)* of the incident radiation [2]. Applying an inverse Hilbert transformation to the measured response *H(V)* the spectrum *S(f)* can be recovered as

$$S(f) = \left(\frac{1}{\pi}\right) P \int_{-\infty}^{\infty} \frac{H(f_j) \cdot df_j}{f_j - f} \qquad (3)$$

where $f_j = 2eV/h$ (h is Planck’s constant). HITRAS is similar to Fourier-transform spectroscopy (FTRAS) or TDS. The important distinction, however, is that a direct transformation of the spectrum into an electrical signal in HITRAS is achieved by a nanoelectronic device, the Josephson junction, while in FTRAS or TDS this procedure requires a bulky optical-mechanical device, an interferometer or optical delay line, together with a broadband detector.

An example of a spectral measurement by HITRAS in a frequency range relevant for the spectroscopy of liquids is presented in Fig. 3.

The spectral range of Hilbert spectroscopy lies in the range of frequencies where the liquids of concern have characteristic signatures in their electromagnetic response. Total scanning times amount to only several milliseconds and demonstrators of Hilbert spectrometers were developed to show the potential of the technique in spectral characterization of various terahertz sources and substances including vapours of liquids such as methanol and acetone [11,12].

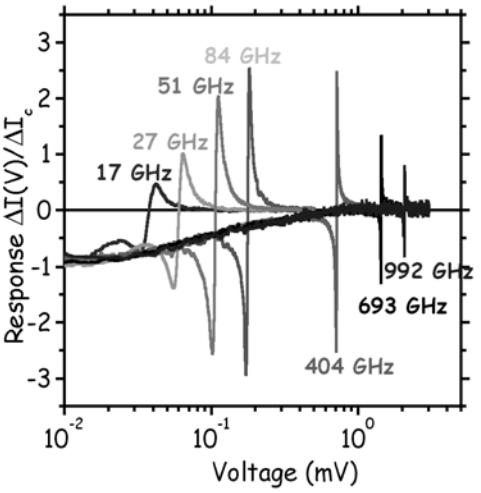


Fig. 3 Voltage dependences of the response of high-T_c Josephson junction to monochromatic radiation with the frequencies in the range from 10 GHz to 1 THz. The junction is placed in a Stirling cryocooler at a temperature of 85 K [2].

References

[1] *Existing and Potential Standoff Explosives Detection Techniques*, Nat. Academies Press, Washington, D.C., 2004.

[2] Y. Divin et al., Advances in Solid State Physics, vol. 41, ed. B. Kramer (Springer, Berlin, 2001) pp. 301-313.

[3] L.D. Landau, E.M. Lifshitz. *Electrodynamics of continuos media*, Pergamon Press, Oxford, 1963

[4] J. Barthel, R. Buchner. Pure & Appl. Chem., vol. 63, pp.1473-1482 (1991).

[5] A.K. Lyashchenko, V.S. Goncharov, P.S. Yastremenko. J. Struct. Chem., vol.17, pp.871-876 (1976).

[6] A.A. Potapov, I.Yu. Parkhomenko. Russ. J. Phys. Chem., vol.72, pp.1469-1474 (1998).

[7] U. Kaatze, Y. Feldman. Meas. Sci. Technol., vol.17, pp.R17-R35 (200 6)

[8] C. Ronne, L. Thrane, P.-O. Astrand, A. Wallqvist, K. V. Mikkelsen, S. R. Keiding. J. Chem. Phys., vol. 107, pp.5319-5331 (1997).

[9] D. S. Venables, C. A. Schmuttenmaer. J. Chem. Phys., vol. 113, pp. 11222-11236 (2000).

[10] T. Ikeda et al. Appl. Phys. Lett., vol. 87, 034105 (2005).

[11] V. Shirotov et al. IEEE Trans. Appl.Supercond. vol.13, pp.172-175 (2003)

[12] V. Shiritov. PhD Thesis, IRE RAS Moscow, 2004

Standoff detection of dangerous and illegal objects and substances concealed beneath clothes on the basis of electromagnetic centimetre- and millimetre-waves and electronic nose

$_1$I. Altpeter, $_1$G. Dobmann, $_1$M. Kröning, $_2$B. Ratius, $_1$C. Sklarczyk,
$_1$Fraunhofer-Institute Nondestructive Testing (IZFP),
Saarbrücken, Germany
$_2$Ministerium for Interior, Family, Women and Sports of Saarland, Police Department, Saarbrücken

The concept of a system for standoff detection of concealed hazardous objects like explosives, weapons or drugs is presented. It is based on a combination of three-dimensional imaging of innocuous electromagnetic waves and a spectrometer integrated into the system ("electronic nose"). The imaging method detects the suspicious object according to contrast and shape, the electronic nose provides for a targeted analysis and identification. For the latter, several methods come into question, like the Ion Mobility Spectrometry (IMS) or the spectrometry with Quantum Cascade Laser (QCL). The complete scanning time of the system will be in the range of a few seconds.

Introduction

Facing the change of exterior and interior security situation the challenges for the security authorities of the german federation and of the federal states have considerably evolved, forcing to reflect the future tactical and strategic mission concepts to preserve the public security and order. The task of the federal states in the national federation is e.g. to combat illegal border crossing, internet crime, terrorism, asymmetric threats, among other, the threatening activities of non governmental organizations and the protection of critical infrastructures (e.g. water and power supply, nuclear power plants, traffic infra structure like airports, public institutions,…). Also counterproductive trends like budgetary shortages and reduction of personal resources have to be balanced by the usage of an avant-garde technique for special police duties of high risk and of hazardous potential.

System description

Millimetre-wave technology

The microwaves and millimetre-waves detection belongs to the outstanding future technologies of the 21st century for effective person and danger property control, its possibilities offer a considerable assistance, especially in the protection of critical infrastructures, as well as in individual cases, e.g. detection for the purpose of a reliable danger estimation and assessment for preparation of police countermeasures.

The portal systems currently in procurement, e.g. for the improvement of the airport security, already partially use the millimetre-wave detection technique. However, in view of system-conditional weakness they only incompletely cover the risen demands of current safety engineering standards. Certainly, they clearly outbid the currently installed old systems. However, they must be understood as transitional systems in the absence of the future detection bandwidth demanded by experts.

Active imaging

Electromagnetic waves in cm- and mm-range are able to penetrate most clothes. At lower wavelengths (sub-mm range) the absorption in the clothes and in the air especially in presence of humidity gets more and more severe. Presently, multi-pixel systems similar to digital cameras are still too complex and expensive. Therefore imaging with a sufficient pixel count has to be executed by means of mechanical scanning or at least by a combination of mechanical scanning and an array of several antennas.

In active imaging systems the algorithms of synthetic aperture can be used to improve the lateral resolution. With increasing frequency and thus decreasing wavelength the lateral resolution of the gained image is improved. However, the number of required pixels and thus the scan duration is increased with decreasing wavelength. Therefore, in order to minimize the number of necessary scan steps or antennas, the lowest millimetre wavelength which produces a sufficient lateral resolution of the image must be used. Nearly optimal results can be gained with steps of about one wavelength.

In order to obtain a further improvement of the recognizability of hidden objects, in particular such with straight edges, waves with same or different polarization can be used.

Hidden objects in the clothes, which cover dangerous items like weapons may produce only a few glint points if they are irradiated from only a few aspect angles. This will inhibit object recognition in most cases. To get a better, more complete three-dimensional view of the object it is necessary to irradiate it from many aspect angles and to reconstruct it with the algorithms of synthetic aperture as applied since several tens of years in the remote sensing domain.

Integration of substance-specific and other methods

To get substance-specific information from the object under test, other methods have to be applied, like infrared spectroscopy, ion mobility spectroscopy (IMS) or molecular imprinted polymer (MIP) method. They use the gaseous components outgoing from the hidden substance and therefore work particularly well for substances with high steam pressure. Infrared spectroscopy based on quantum cascade lasers (QCL) is promising concerning the detector response in relation to traces of explosives and can be further developed to a compact, durable and robust component of the detection system. The person screening system to be developed will be modular, both with regard to hard- and software and can be expanded easily with regard to additional detection methods and biometry.

NIVEGOS-partner consortium

A consortium of partners competent in their respective research areas has put the task to itself to develop a personal screening system for detection and identification of dangerous and illegal hidden objects. The partners are:

Partner	Task
FHG-Heinrich-Hertz-Institute (HHI), Berlin	Visualization, 3D modelling, object separation and identification
FHG-Institute Applied Solid State Physics (IAF), Freiburg	Integrated radar modules, high frequency switches
FHG-Institute Nondestructive Testing (IZFP), Saarbrücken	Scanner, experimental investigations, system integration
FGAN-FHR, Research Institute High Frequency Physics and Radar Technology, Wachtberg	Innovative Antennas and millimetre wave modules, scanner
Institute Low Temperature Plasma	IR spectroscopy based on quan-

Physics (INP), Leibnitz-Society, Greifswald	tum cascade laser, substance identification
German Research Institute for Artificial Intelligence (DFKI), Saarbrücken, Kaiserslautern, Bremen	Object and substance identification, pattern recognition, data fusion, alarms
University Kassel, Theoretical Electrophysics, Kassel	Object reconstruction from imaging data
Ministery of Interior, Family, Women and Sports of Saarland (MfIFFS) as end user	Consulting, definition of threat scenarios, providing explosives

FHG: Fraunhofer-Society, FGAN: Research Society for Applied Nature Sciences

Industrial partners are intended for commercialization in the diverse relevant application fields. The development project was called **NIVEGOS** (**N**achweis und **I**dentifikation **ve**rborgener **g**efährlicher **O**bjekte und **S**ubstanzen = Detection and Identification of hidden dangerous objects and substances).

Application ranges

The ranges of application of NIVEGOS firstly cover the protection of all kinds of traffic. In a later development phase NIVEGOS is to be developed further to a unique mobile system with multiple detection capabilities, so that it is also applicable for everyday police work (Ad-hoc controls, strip service, personal searches), for control of big events and for traffic control tasks. The NIVEGOS user spectrum can successfully cover not only specific police requirements according to expert opinions of the Ministry, but also offers a wide range of applications of a military nature (dual use principle). The same applies to the range of civilian, population and disaster control, as well as the equipment of private safety officers.

Advanced radiological technologies for imaging and characterisation of threats

Uwe Ewert, Kurt Osterloh, Andreas Kupsch, Axel Lange, Jörg Beckmann, Mannfred P. Hentschel
Federal Institute for Materials Research and Testing, Unter den Eichen 87, D-12205 Berlin, Germany

Abstract:

Radiological technologies are the primary tool for bulk detection. Traditionally, their strength is to allow estimating the actual amount of a dangerous substance inside of cases, containers, luggage etc. or carried by a person or in a bag. Due to the vast range of putative objects to be scanned and the various requirements from penetrability to radiation safety, different technologies are required involving not only X-rays but also other kinds of radiation as mm-waves and THz-radiation. Reliable threat detection requires the combination of 2- and 3-dimensional imaging as well as spectral characterisation for identification of dangerous sub-stances. The capabilities of X-ray and THz-inspection are compared.

Threats shall be detected in an early state when scanning systematically at certain checkpoints as in airports or in other critical infrastructures. Normally, the equipment for this purpose is fixed installed and designed for scanning in large numbers. A different situation may be encountered when a suspicious object (e.g. IED) is found somewhere. Mobile (portable) devices are needed for radiographic inspection, that nevertheless produce informative images sufficient to guide further actions. New fast laminographic techniques are presented for mobile 3D-inspection.

Introduction

Among the detection technologies currently applied, radiology is the primary one to obtain information about the bulk of dangerous substances such as explosives within a suspected object. Moreover, trigger, fuses or detonators can be detected and how they are connected to each other. Equally indispensable are devices and methods to convert radiation into visible information. Fig. 1 gives an overview on the requirements for security applications and on the different kinds of radiation suitable for this application.

Radiological inspection of hand baggage had been introduced after the bomb attack of the fight PA103 over Lockerbie (1988) in UK (http://www.flugzeug-absturz.de). In addition, passengers had been checked for metallic items. The September 11th attack to the world trade centre in New York in 2001 forced the need for automated control of the shipped baggage. Germany has joined the corresponding agreement since 2003.

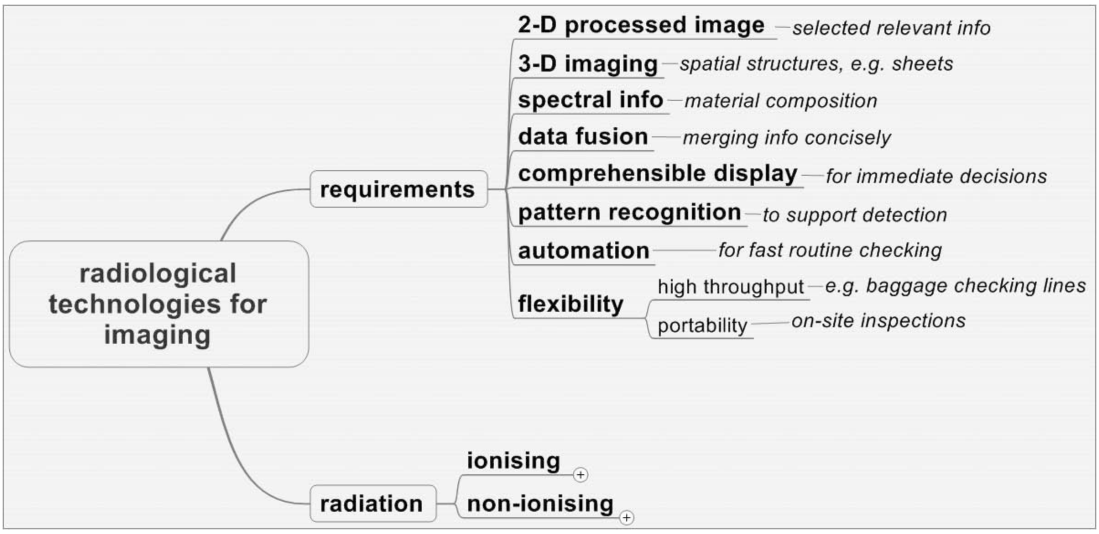


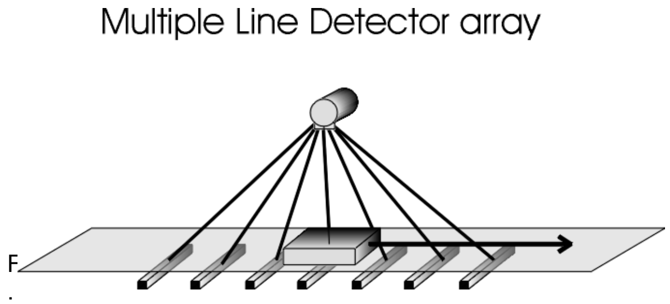
Fig. 1: Requirements and types of radiation for threat detection

Dual Energy Radioscopy

Hand and shipped baggage control is carried out whenever passengers enter the plane. Two major items are searched for: weapons, dangerous objects and explosives. The classical radioscopic inspection is sensitive for metals and was an essential tool for location of illegal metallic objects. Explosives are more difficult to detect. Therefore, it was necessary to improve the classical radioscopy. Baggage is inspected now with two different X-ray energies. The change of the attenuation at different energies is related to the atomic number of the compounds in the inspected material. Explosives are identified by this procedure. Nevertheless, this method does not provide reliable information if sheet explosives are hidden behind highly attenuating objects as e.g. notebook computers. This is one reason, why they are inspected separately.

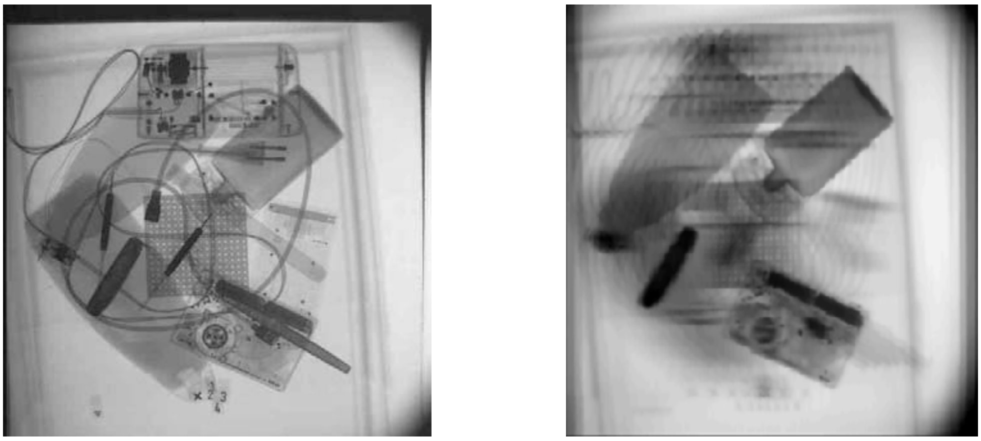
Multiple view inspection vs. tomography

Nowadays the technology has been improved by multiple view inspection. Due to confidentiality reasons the principle can be described only. A bag is transported on the conveyer belt beneath an X-ray tube (fig. 2). Seven detector lines are used to generate seven radioscopic projections as basis for a tomographic reconstruction. The reconstruction follows the principles of tomosynthesis and coplanar translational laminography. The single energy reconstruction of a complex test object is shown in fig. 3 (b). Due to the limited number of the projections the layers are not separated completely, but the camera view through the object gives more detail information than the digital radiograph of fig. 3 a, where all objects are sequentially overlapped.



Special statistic order reconstructions as maximum or minimum reconstruction improve the images [1].

Similar methods are also applicable for mobile inspection of IEDs (improvised explosive devises). Fig. 4 shows a typical manipulator based scenario. Reconstructions are possible from different views. This is important to localise the ignition unit (fuse) and deactivate it in a controlled way.



a) Digital radiograph of a test object

b) Laminographic reconstruction of the central layer

Fig. 3: Digital radiography of a baggage test object and its reconstruction of the central layer based on the test assembly of fig. 2

mm-waves and THz radiation

Body scan are also possible with X-rays. Penetrating body scanner and back scatter body scanner are commercially available. Due to restrictions and concerns of radiation protection this technology is unsuitable for routine testing of passengers. A fast development of mm-wave technology (40 – 100 GHz) and THz technology (100 GHz – 10 THz) is presently observed. The first mm-wave scanners were introduced at exhibitions. THz scanners are under development. The techniques are preferred for several reasons: they penetrate isolators (clothes, paper, plastics) and are reflected by metals, they are not harmful for human and provide additional specific spectral information on materials within a wide spectral range. From a physical point of view they probe the material’s dielectric properties, i.e. the material’s ability to align its (molecular) dipoles ac-cording to the oscillating external electric field of given frequency.

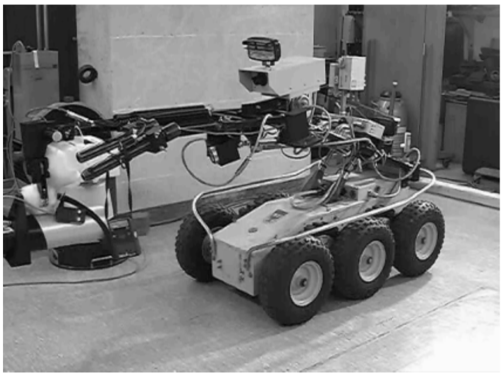


Fig. 4: Manipulator Theodor of TeleRob with X-ray tube inspecting an IED.

Fig. 5 displays a THz scanning topogram obtained from sampling a plane arrangement of explosives. The according measurement had been performed in the THz Time Domain Spectroscopy (TDS) mode, i.e. sampling the temporal electrical field after traversing the material. Fourier transformation (FT) provides the decomposition into the complex spectral components (since the phase information is conserved). In the depicted sample of explosive pellets the greyscale represents the derived index of refraction averaged in a 0.3 to 1.5 THz interval. The derivation implies a fully automated algorithm including FT and phase matching in order to obtain the spectrally resolved index of re-fraction. It can be seen from Fig. 5 that the different species of explosives can be quantitatively distinguished from each other. For the purpose of better presentation image processing has been applied in order to avoid poor contrast and coarse scanning pattern.

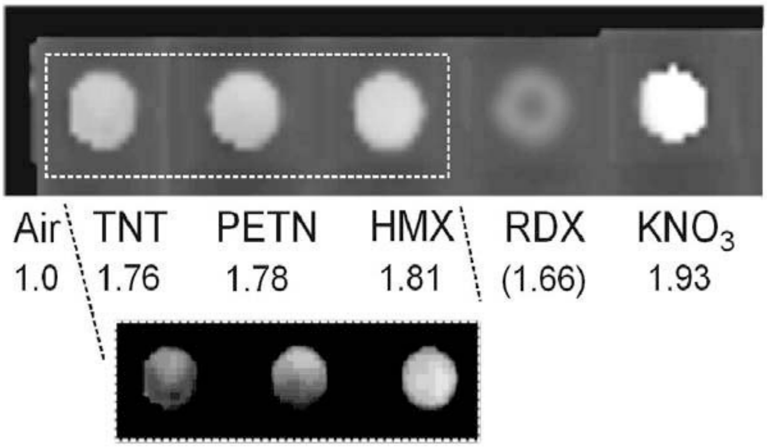


Fig. 5: THz scanning topogram of selected explosives and determined refractive indexes (insert contrasted).

Methods for high power EM pulse Measurement

P. Fiala, M. Steinbauer, P. Drexler, (Brno University of Technology, Faculty of Electrical Engineering and Communication), Czech Republic

abstract

There are some suitable methods for the measurement of ultra-short solitary electromagnetic pulses that can be generated by high power pulsed generators. The measurement methods properties have to correspond to the fact whether we want to measure pulses of voltage, current or free-space electromagnetic wave. The need for specific measurement methods occured by the development of high power microwave pulse generator [1]. Applicable methods are presented in this paper. The method utilizing Faraday's induction law allows the measurement of generated current. For the same purpose the magneto-optic method can be utilized, with its advantages. For measurement of output microwave pulse of the generator, the calorimetric method was designed and realized.

Introduction

The Fig. 1. shows the basic principle of microwave pulsed power generator. It consists of three stages – the primary source of electrical energy, the pulsed power generator and the microwave pulsed power generator (load in the Fig. 1). The primary source supplies the pulsed power generator, which ensures the pulse current amplification. After transformation to the high voltage and pulse shaping (not shown in Fig. 1), the pulse is fed to the microwave pulsed power generator. The detailed description of pulsed power generation can be found in [2]. For example, the peak level of current pulse achieves the value of I_p = 100 kA with the pulse duration t_d = 70 μs typically in the second stage. After high voltage transformation and using pulse shaping element we can get voltage pulse with the peak value U_p = 400 kV and with the rise time t_r = 0,1 ns. Following microwave source (vircator [3]*)* emits electromagnetic pulse (EMP). The characteristic of EMP is high power level (P_max = 250 MW [1]) and very short time duration ($t_\mathrm{p} \in \langle 1, 60 \rangle$ ns). For the pulsed power generator evaluation is essential to obtain an idea about the qualitative and quantitative processes during the generator operation. Important measurement points are shown in Fig. 1. Special requirements for measurement methods have to be considered because of the specific pulses properties.

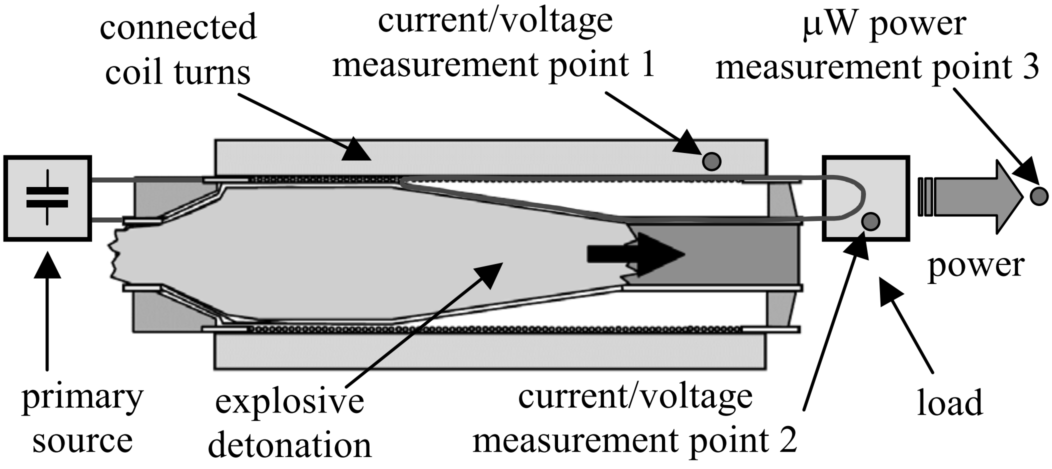

connected coil turns
current/voltage measurement point 1
μW power measurement point 3
power
primary source
explosive detonation
current/voltage measurement point 2
load

Fig. 1. The basic principle of microwave pulsed power generator

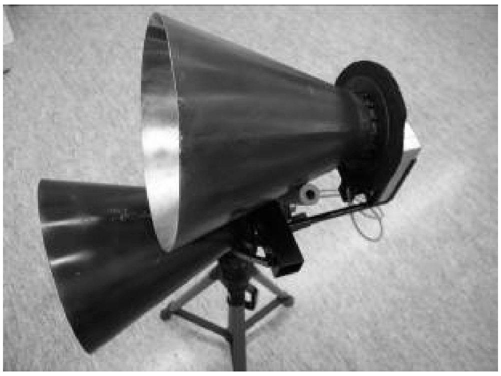
Methods for pulses identification

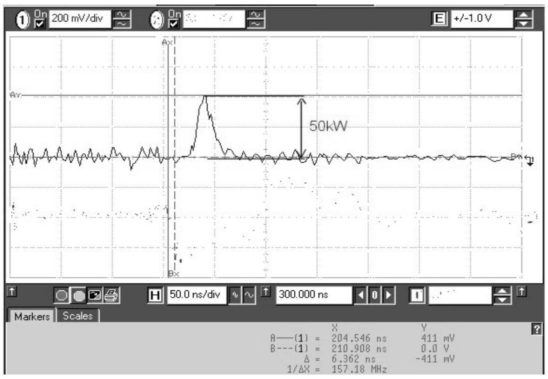
The basic quantity is the current of the pulsed power generator. It is quite difficult to use the classical methods for current measurement (shunt) because of the high current level. The measurement of the induced magnetic field has been proposed, according to Faraday's induction law. The most straightforward way for the voltage pulse measurement is the method using high voltage divider. It has been developed inductance-free high voltage divider.The final product of the relativistic vircator effect [3] is the electromagnetic pulse, which can be guided in a cylindrical waveguide or emitted in to the free-space. However, it was not possible to use microwave probe or antenna for first vircator test. The frequency range and the mode distribution were unknown. The calorimetric measurement method was proposed for the vircator tests. On the other side, it allows physically correct power and energy measurement. The power of the EMP is the crucial parameter, which gives an idea about vircator optimal design.

Free-space combined calorimetric sensor

The realization of the combined sensor is shown in Fig. 2. Both parts are equipped with Horn antennas to ensure the matching of the free-space EMG wave to the sensor input. The parameters of the antenna obtained by the help of numerical simulation are following:

Gain: G = 19 dB , 3dB beam angle: θ_{3dB} = 21°, 6dB beam angle: θ_{6dB} = 30°, Front-to-back ratio: FBR = 69,4 The sensor was calibrated with an RF generator in an semi-anechoic room. The calibration was performed for microwave pulses with defined duration and power level, with the frequencies f =3, 4, 5, and 6 GHz. The power level and pulse duration relation were set for emitted energy $F_{test} \in$ <0,1; 10> J.





```
          X             Y
A——(1) =  204.546 ns    411 mV
B---(1) =  210.908 ns   0.0 V
     Δ =  6.362 ns     -411 mV
  1/ΔX =  157.18 MHz
```

Fig. 2. Realization of optimized combined calorimetric sensor

Fig. 3. Measured waveform of small microwave power, P_{max} = 50 kW

Method based on magneto/electro optic effect

The second method presented – the magnetooptic method - uses the Faraday's magnetooptic effect as a sensor principle. There are three basic types of the possible active sensors. The first type is a garnet with high Verdet constant, the second one is an optic fiber and the third one is based on magnetooptic properties of ferromagnetic mono/multi thin film. Other types of sensors are based on the magnetooptic Kerr's effects (MOKE), or surface MOKE (SMOKE) effect. By an available measuring devices application we can measure pulses with the limit length up to T_{max} = 0.1 ns [4].

Design of the magnetooptic method

The magnetooptic (MO) method is proposed for further experiments. The magnetooptic method allows ultra-short pulses waveform measurement because of its high bandwidth. The polarization rotation of light passing the MO sensor is affected by the magnetic part of EM pulse. The rotation is due to the magnetic field and properties of the sensor material (Verdet constant). For the measurement the MO garnet, glass or thin film may be used [5] and [6] .The absolute measurement method utilizing the MO glass element was experimentally realized with low frequency magnetic field. Laser beam with linear polarization passes the MO glass placed in Helmholtz coil. The laser beam is subsequently fed through an analyzer and the polarization rotation is converted to intensity modulation. The intensity of light is sensed by a photodiode. The magnetooptic glass FR-5 by Hoyoa Optics was used in this experiment. Next, the differential method was experimentally realized [7]. The differential method utilizes

Wollaston prism and offers better sensitivity. It is proposed for the next pulse current sensor development. The experiment for the measurement of high frequency magnetic field is in development – Fig. 3.

Conclusion

The overview of several methods suitable for the measurement of short solitary pulses with high power level was given. The characteristics of the designed method were discussed. Some methods were experimentally tested and evaluated. A combined calorimetric sensor for free-space measurement was built and the functionality of the calorimetric sensor was proved by real measurement of vircator-emitted EMP.

Acknowledgements

The paper was prepared within the framework of the research plan No. MSM 0021630513 of the Ministry of Education, Youth and Sports of the Czech Republic.

References

[1] FIALA, P. *Non-conventional sources of electrical energy*. BUT FEKT, Brno, 2003.

[2] FIALA, P., DREXLER, P., RYCHNOVSKÝ, J. Pulsed power generator with output power up to 20GW, research report. HS Prototypa a.s., 18580001.

[3] BARKER, R. J., SCHAMILOGLU, E. *High-Power Microwave Sources and Technologies*. IEEE Press, 2001.

[4] RIORDAN, J. A., SUN, F.G., LU, Z.G., ZHANG, X.-C. Free-space transient magneto-optic sampling. *Applied Physics Letters*. 1997, vol. 71, p. 1452-1454.

[5] ŠUNKA, P. Verbal information. UFP AV ČR, Praha 6, 2003.

[6] CRAIG, A. E., CHANG, K. *Optical modulation: Magneto-optical devices. Handbook of Optical Components and Engineering*. New Jersey: John Wiley & Sons, Inc., 2003. 1380 pages. ISBN 0-471-39055-0

[7] DREXLER, P. *Methods for the measurement of ultrashort electromagnetic pulses*. Treatise on the Ph.D. thesis. BUT FEKT, Brno, 2006.

High-speed Computed Tomography: Potentials and Physical Limits

Dr. Theobald Fuchs, Dr. Randolf Hanke, Petra Keßling

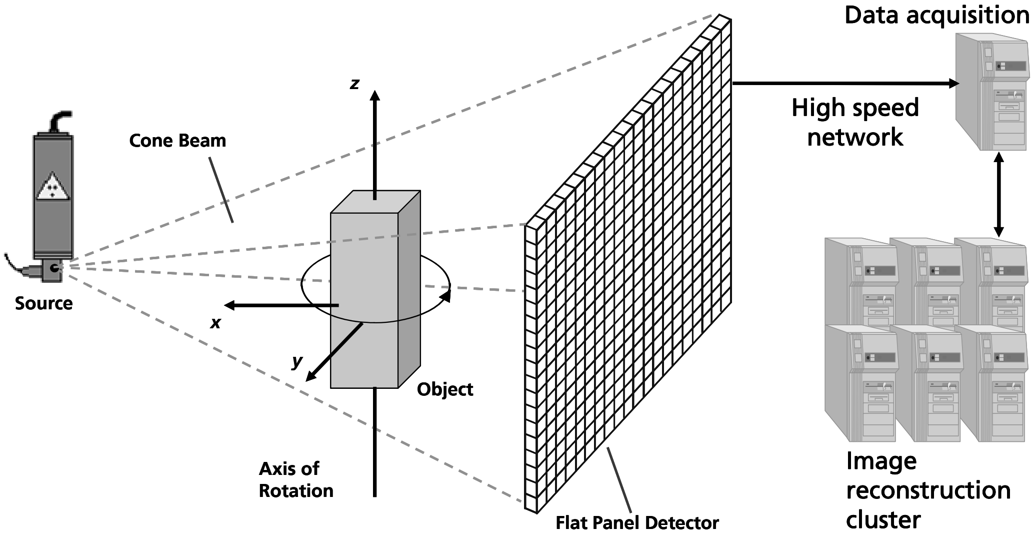
Fraunhofer Development-Center X-ray Technology, a common department of the Fraunhofer-Institutes IIS and IZFP

Dr. Mack-Str. 81, 90762 Fürth, Germany

The request for fast and reliable methods for the inspection of luggage has grown in the past and is still growing today. This contribution intends to estimate the potentials of X-ray Computed Tomography (CT) as a tool to improve security in the world wide transportation of passengers and goods. We try to evaluate the limits of 3D-imaging by means of X-rays. Today, the inspection of objects with a size between some ten centimeters and a few meters still poses various challenges to the development of an adequate CT system.

The Principles of Computed Tomography

X-rays can penetrate matter due to their extremely short wavelengths. Depending on the properties of the matter (density, atomic number) and the object’s geometry (path length) they are more or less attenuated. The X-rays are usually detected with digital flat panel detectors.



Set-up of a CT system and scheme of measurement

Computed Tomography (CT) is the process of generating a 3D-image from many 2-dimensional X-ray projections with the assistance of a computer. Thereby the object is X-rayed from all directions while being rotated between the X-ray source and the detection system. The individual layers or a complete 3D-volume image are calculated from the projection data by means of a numerical reconstruction algorithm.

Physical Limits

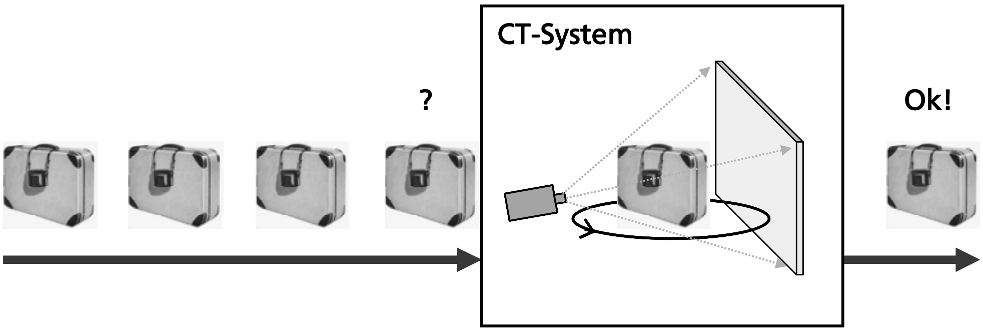
Components & System Design

The crucial image quality parameter with respect to fully automatic evaluation of the reconstructed CT-volume data is the signal to noise ratio. Thus, the power of the X-ray source available for a real 24/7 inspection system determines the fundamental limitation of the inspection rate.

Today's state-of-the-art X-ray tubes provide several 10 kW of electrical power for non-stop operation. In order to obtain quantitative information at each point of the inspected volume, the reconstruction algorithm requires at least 200 up to more than 1000 projection images of the object. A higher intensity of the tube's radiation allows for a respective decrease in integration time of the detection system and in consequence helps to reduce the total data acquisition time.

Data Processing & Reconstruction

The data read-out is another technological bottleneck of a CT-system. Today, flat panel detectors are available that provide an active imaging area of 40 by 40 cm whereby the spacing of the pixels is as small as 200 microns. Since the integration time of each projection image is of the order of magnitude of 100 ms, the resulting data rate can reach 800 MByte per second. Thereby we assume 16 bit resolution of each measured intensity value and an acquisition of 500 two-dimensional projection images within 5 seconds.



Scheme of an inline CT-inspection system

The projection data are transferred to the reconstruction system while keeping pace with the ongoing measurement. The subsequent algorithms of the image reconstruction and evaluation of the primary volume data are performing inline, too.

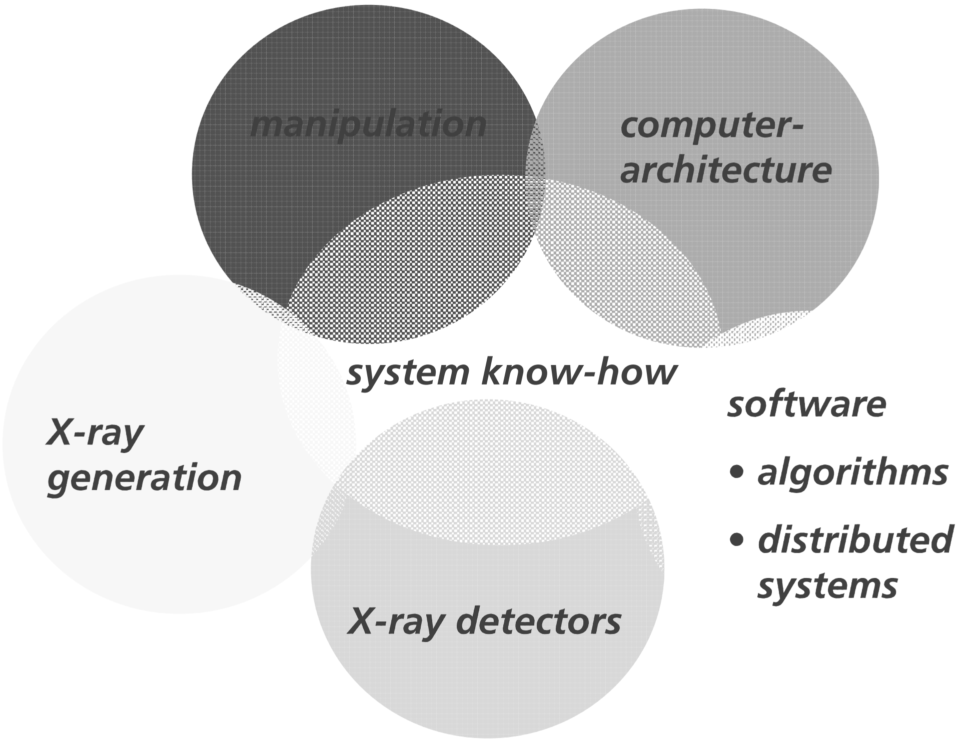
Potential Applications

The advantages of CT-inspections of any kind of test objects are obvious: CT provides full information on the internal structure of an object and the 3-dimensional distribution of the material density. This allows for the fully automatic evaluation of the volume data and subsequently for the detection and visualization of defects and hidden details.

Today, CT has become fast enough to be used as a fully 3D inline inspection tool of parts that are relevant for safety in surface and air travel. Already, the first CT-systems for quality testing in industrial mass production have been introduced. An inspection cycle time of less than 30 s can be achieved. This time period includes highly optimized and parallelized post-processing algorithms and a fully automated evaluation.

The efforts in research and development at the Fraunhofer EZRT aims at innovations in the field of highly efficient, very fast and radiation-hard sensor systems. Amongst others, the development of technologies and complete systems for X-ray inspection can include multi-energy reconstruction techniques for the detection of different materials or fully automatic detection of contaminations in packed goods like food, plastics, bulk materials and fluids.

For more than 10 years running, the Fraunhofer EZRT is having a broad knowledge in X-ray component development, process control and object manipulation, as well as final system set-up of fully automated inline 2D- and 3D-inspection systems.



Necessary know-how of components for the design of a CT-system

Reference Architecture for Protection Systems

Dr. Gunther Grasemann, Fraunhofer IITB, Karlsruhe

Abstract

For the protection of large sites with high values that are continuously threatened by attacks and accidents, complex sensing and decision systems are necessary for an efficient protection. Examples for such sites are airports, harbours, railway stations, power plants, critical research facilities and all public areas. Based on the data from many different sensors, like video cameras, microphones, mechanical, chemical sensors and many others, information about the actual situation must be delivered by means of automatic and interactive evaluation. For the realisation of systems for this purpose, a general applicable architecture for the construction shall be defined. The organisation of devices, services and applications will be organised in a web based service oriented architecture. For the operation, interaction, decision and handling, three application layers are defined. The first is the top level decision layer, the second is the guidance layer and the third the fields operation layer. In each layers, systems for visualisation, interaction and simulation are required. For the top level decisions, the complete information has to be condensed in order derive the best solution for an adequate reaction. In addition to tasks matching services, ergonomic optimised interaction devices are required.

Security does not exist – that is sure.

Total Security is just an imagination that there cannot happen anything at all, everywhere and always. That is not realistic - and do we really want that?

What we want and what we should do as good as possible is to provide the best protection. That means detection of possible threats as early as possible, in order to avoid an accident or an attack. In addition, if an accident or attack could not be avoided it should be tried to attenuate the consequences. The last aspect is nearly independent of the reasons for the situation.

The actual technological state of the relating to sensors, computer ..... and communication allows oftentimes a rapid detection and notification of threatening situations and close reactions. However, in complex situations there are constraints due to lacking cooperation of the concerned subsystems. An optimal detection and characterisation of complex scenes, taking into consideration all available sources of information can only be performed by humans.

Figure 1: Karlsruhe Main Railway Station

Endangered buildings and sites are e. g. all public buildings where lots of people are present like airports, railway stations and public places, but also temporary crowds at special events (e.g. “Tour de France”) or political demonstrations (e.g. transport of nuclear material). Sadly, there is a long list of examples where terrible consequences where not avoidable by protection systems due to their not sufficient or wrong functionality.

The Fraunhofer Society is actually focusing on the development of integrated protection systems in the scope of the network for defence and security research. The task of the IITB is the field of sensors and sensor data evaluation, the decision finding and the acting to combine inside a information technology oriented reference architecture.

For the detection of dangerous situations and threats, many different sensors are provided. The most important sensor type is video. But it is critical in the field of human and civic rights and in privacy aspects. Especially therefore, a almost complete automatic interpretation of the images and image sequences is necessary so that nobody has a look on the images while no dangerous situation is detected. Only in case of critical situations recorded images are displayed and viewed by people. An extended video surveillance will only be accepted in public and by private persons if the private and civic rights are being respected (“aware of the image”).

To achieve an aiming usage of the huge amount of different sensors, an integration of them into a complex over-all-systems is required. With that, a close and comprehensive analysis and valuation of the dangerous base on all available information. For that, efficient interfaces between the information sources and the analysing parts of the system. Very important is a task oriented information condensing from the respective data up to the over-all view which is the basis for the decision process. For that, many automatic and interactive components and tools are necessary in order to give wide assistance for the security stuff. The realisation of this complex and currently changing task can only be accomplished by use of a variable and easily scaleable system architecture. A web-based service architecture is suitable for that because new sensing systems can be integrated without the need of a manual reconfiguration of the system when the sensor are able to report there facilities after having been found in the system ("plug and protect").

A central aspect in the conception of protection systems are the interaction components for the operation by the stuff. The central process is the continuous monitoring process, the evaluation of the situation and the reaction on special events. Always has to be proved whether more information is necessary and the requirement has to be reported to the systems. After every performed action it has to be found out what effects has been taken place, if more information is required and if more actions are suitable.

For this continuous process, display and interaction components are required that are able to give an overview and to show all detailed information when it is required. Fig. 2 shows the "large situation table".

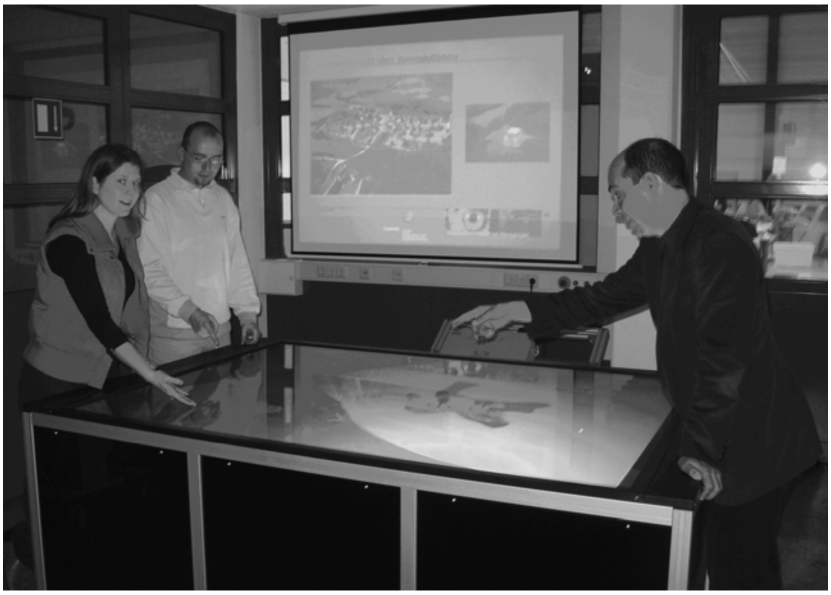


Figure 2: The "Large Situation Table "

Early Warning and Protection of Installations under RAM Threats

Markus Graswald, Ilya Shaydurov, Hendrik Rothe
University of the Federal Armed Forces, Hamburg

Rockets, artillery projectiles, and mortar grenades (RAM) are nowadays serious threats to military installations in out-of-area missions. A high percentage of terrorist attacks on field camps in Afghanistan or Iraq are undertaken with mortars. Mortars of 60, 82, and 120 mm caliber are distributed all over the world, relatively easy to obtain and handle, and therefore frequently chosen for attacks.

Two different approaches to withstand this asymmetric threat are investigated and requirements are given for: (1) an early warning system that alerts people depending on the predicted impact point of the mortar shell on the ground, and (2) a counter RAM weapon system that intercepts the approaching shell in a safe distance.

The investigations reveal that very precise radar sensors are required for tracking the mortar shell. Provided that standard deviations of the azimuth, elevation, and range measurements are small enough, reasonable warning squares can be defined by the circular error probability (CEP) of the predicted impact point in the field camp. Furthermore, simulated frontal attacks against 82 mm grenades show significant differences in the hit probability and ammunition consumption of 35 mm Ahead and 155 mm HE ammunition.

Requirements for early warning of camps

Exterior ballistics and trajectory determination

The determination of the grenade’s trajectory is principally based on a simple physical model of its motion with an experimentally determined reference function for the velocity-dependent part of the air drag and several radar measurements of its flight path. The drag coefficient of the grenade is determined by the drag function that corresponds to the difference in kinetic energy between two averaged points of the trajectory and refers to their distance. This drag coefficient consists of the mentioned velocity-dependent part, an atmospheric part assumed to be constant, and a projectile-depending part called the ballistic coefficient.

This estimated ballistic coefficient allows to solve the nonlinear differential equations of motion iteratively and to calculate the trajectory from an averaged radar location to either the firing or impact point on the ground. This mathematical model consists of path-dependent

2-DOF equations of motion with the mortar shell as a point mass and gravitation and air drag as external forces.

Error propagation and CEP simulations

The well-known methods of error propagation are applied to the mathematical model in order to find variations of the point of impact depending on the sensor accuracy, i. e. variations in range, deflection, and the CEP. All systematic errors shall be eliminated by calibration or adjustment, while the measurements of the radar azimuth, elevation, and time (range) are subject to normally distributed random errors. Variations of the radar measurements propagate with the ballistic coefficient to the predicted point of impact and thus determine its desired variation.

The scenario for the CEP simulations consists of the commissioned Russian air search radar MWRL-SWK and the counter battery radar COBRA as sensor systems and a Russian 82 mm-mortar grenade O-832 (No. 6) as typical RAM threat. The simulation results are shown in Fig. 1 for confidence levels (C. L.) of 50%, 90%, and 99%. For an early warning system, the estimation of CEP allows the definition of the edge length of plane squares in order to enable specific areal warnings to soldiers. Since a clear threat direction is usually unknown, the camp shall be divided into squares with their edge length given by double CEP. For a precise radar system like MWRL-SWK, the edge length is already 46 m, while for COBRA it is 269 m (both at 50% C. L.). These distances cannot be covered by soldiers in warning times of roughly 10 s. Therefore, a more precise tracking radar is required and physical measures in the field camp like shelters and dugouts have to be considered.

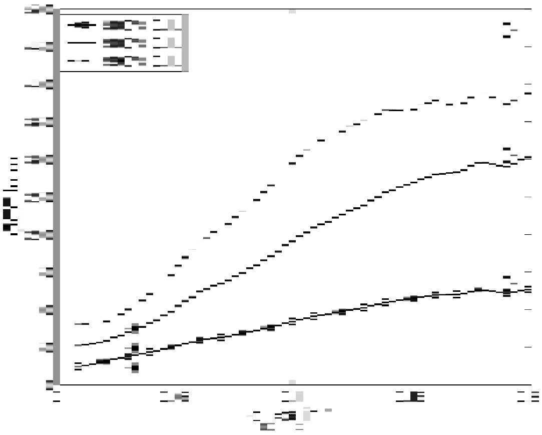


Figure 1: CEP of impact point on the ground (σ_t = 200 ns, ∗ MWRL-SWK, À COBRA).

Protection against mortar attacks

For this purpose, 35 mm Ahead ammunition and a typical 155 mm HE-projectile is examined in the following sections. Two conditions are required to successfully intercept a RAM target: at first, the kinetic energy of the sub-projectile or fragment is sufficient to destroy the mortar grenade, and secondly, at least one pellet hits the shell. A frontal attack by pellets is considered as ideal case leading to a high kinetic energy for destruction. However, the chance of hitting the fuze and a resulting ignition of the explosive is not observed here.

Penetration and activation energy considerations

For the sake of simplicity it is assumed that the minimum energy to destruct a grenade is compounded by the kinetic energy to penetrate the shell and the potential energy to activate the explosive. The minimum impact velocity of an Ahead sub-projectile at an angle of 0° (NATO) is determined by the formula of *de Marre* for the maximum thickness of an 82 mm mortar shell. This minimum kinetic energy and the potential energy of TNT determined by its impact sensitivity lead to the required overall minimum energy of 1160 J. At this stage of the investigations, this minimum energy is also used for the following calculations with the HE ammunition.

Ammunition consumption

The normally distributed hit probability of a single pellet is both calculated in the plane of the grenade’s symmetric axis and the plane normal to this axis. The destruction probability is calculated with the internal energy provided through a rigid body impact of a pellet with the target and the determined minimum energy. Finally, the kill probability of a single pellet is the product of these three probabilities.

Calculating the kill probability of *N* effective pellets hitting the target area, it is assumed that the base area of the fragment cone equals the area of the radar CEP at the target location. This leads to the kill probability of *N* pellets and the desired number of rounds to destroy the target.

As intercepting ammunition the air defense version of Ahead consisting of 152 sub-projectiles and experimentally determined static data superposed with the velocity vector of the HE projectile is used for the simulation. The interception and radar distance is supposed to be 1000 m. The number of rounds required to destroy an 82 mm grenade with Ahead or HE ammunition depends strongly on the radar precision.

As Fig. 2 reveals, distinctly one-digit ammunition consumptions can be realized with 155 mm HE due to its high number of effective fragments, a wide fragment cone angle, and high fragment velocities.

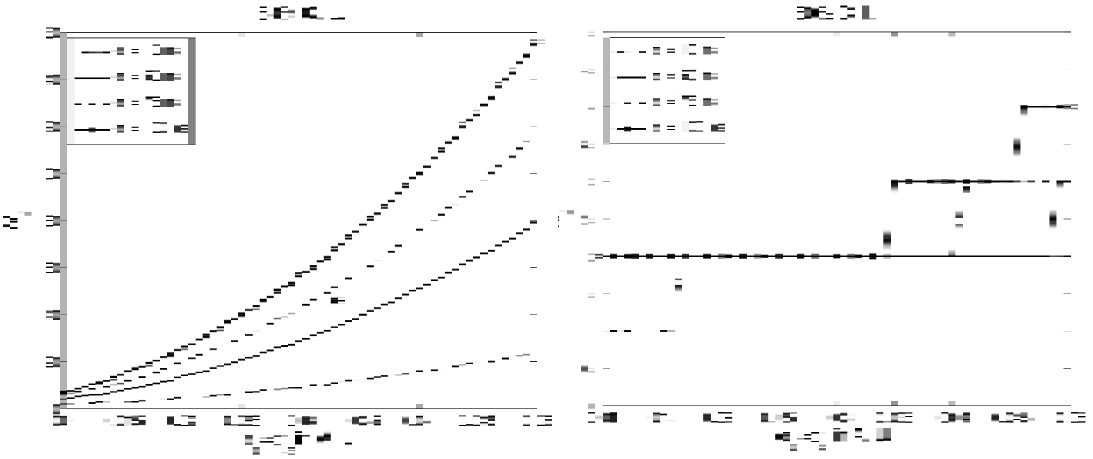


Figure 2: Ammunition consumption for 35 mm Ahead (left) and 155 mm HE (right), ∗ MWRL-SWK.

Conclusions

The procedure for evaluating sensor and ammunition requirements is described for the protection of field camps and military installations underlying the asymmetric threat of mortar grenades. Early results of the study yield that

- the precision of the radar sensor for trajectory tracking of the target is essential for the success of both early warning systems and counter RAM systems,
- the type of ammunition for intercepting the mortar shell, low-caliber projectiles with submunition or high-caliber HE, decides on the effectiveness of the system and the ammunition consumption, and
- the ammunition consumption limits operational durations, affects service intervals and therefore the overall costs of the counter RAM system strongly.

A necessary future task is to consider the overall error budget of counter RAM systems and their effect on the ammunition consumption. Furthermore, the terminal ballistics of fragments and sub-projectiles against mortar shells need to be investigated theoretically in more detail as well as experimentally. The selection of the ignition point of the intercepting projectile has a major influence on the number of fragments hitting the target due to non-uniform spatial distributions of the fragment masses and velocities. Last but not least, multiple threats especially those coming from short distances, in short sequences, and different directions demand an intelligent strategy with optimal fire distributions to several artillery weapons.

Autonomously Controlled Robot Systems – Solutions for Homeland Security

Dr. Jens Hanke, Robowatch Technologies GmbH, Berlin.

Terrorist attacks and rising international tensions greatly influence perceptions of safety in Europe, so politicians and businesses alike are faced with the task of integrating preventive and defensive measures into security concepts. Industry in particular is called on to off er technical solutions that meet security needs while taking due account of cost pressures.

Mobile, autonomously navigating robots are an effective response to the challenges of this new millennium.

Robowatch Technologies GmbH develops and markets autonomously controlled robot systems, termed AUGVs, or Autonomous Unmanned Ground Vehicles. These bundle proven elements of hazard warning technology, video surveillance and detection of persons onto autonomously navigating robot platforms. When so equipped, AUGVs issue warnings in dangerous situations in good time, support surveillance of high-risk zones or extensive areas, and optimize reconnaissance for disaster control and civil protection. Thanks to its stock of unique expertise, Robowatch is the key driving force for international security projects, too.

Distance creates security

Experience today from the world’s crisis regions indicates that asymmetric conflict situations in unknown terrain and the need to conduct operations in inhabited environments are on the rise, presenting entirely new threats. At the same time, the risk closer to home of acts of violence motivated by terrorism is increasing.

Robowatch develops and markets AUGVs for the military defence markets and for homeland security tasks. The objective is to minimize dangers to persons in situations for which otherwise a mission would only be possible at high risk. In fulfilment of this aim, Robowatch offers AUGVs for reconnaissance, detection of chemical, radioactive and nuclear hazards (CBRN), defusing explosive devices and transporttation. If needed, they can also operate under remote control. Thanks to these capabilities, the AUGVs of Robowatch raise performance while enhancing protection of military personnel and other task forces for a wide range of missions.

Autonomous Unmanned Ground Vehicles (AUGVs)

OFRO+detect can be used for monitoring purposes as well as the CBRN analysis. The robot - by means of its integrated ther-mal camera system, which rotates 360 degrees - reliably recognises human heat sources. It transmits data continuously using the radio standards GPRS, UMTS and WLAN. **OFRO+detect** not only transmits type and concentration of the detected gas, but also simultaneously delivers video recordings of the location of the accident to the control unit.

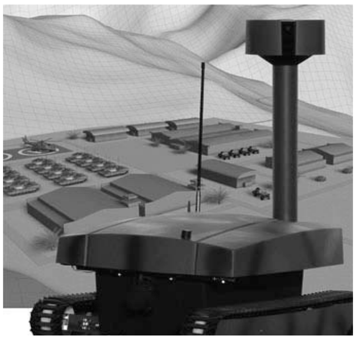


Figure 1: Reconnaissance robot OFRO+detect

Due to its modular concept **ASENDRO** operates as reconnaissance or defusing system, especially in critical areas like the metro, buses or aircrafts. The robot consists of a manoeuvrable platform and two mission-specific payload modules with a reconnaissance or manipulator arm which can be exchanged without much trouble. Due to its small size (40 x 60 cm) and its relatively high speed (up to 10 km/h) it is suited for missions indoors and outdoors.

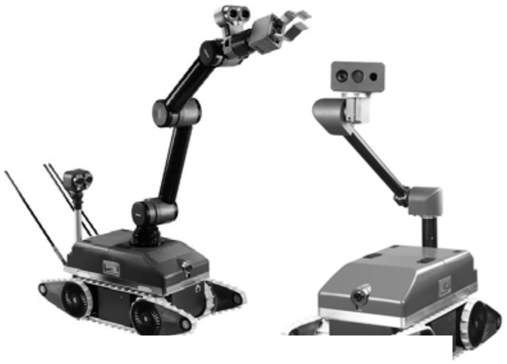


Figure 2: Modular robot ASENDRO

With the **AUG-V8** a conventional mission vehicle was upgraded by integrated robotics functions. The vehicle can be driven autonomously on given distances as reconnaissance, transport or effect system. In addition, as with UGV' s usually, it also can be steered over radio from a command centre. Thereby obstacles are recognized automatically. The advanced digital communication system installed on the **AUG-V8** relays video and sensor readings back to the headquarters and to a forward command post.

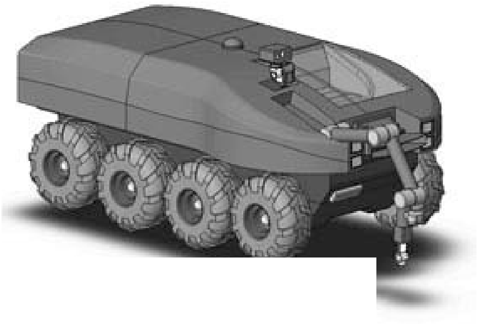


Figure 3: Multimission Vehicle

Algorithms for autonomous vehicle control

The navigation processes acquire data and analyze the vehicle's environment, so that it can drive to its destination independently even in unstructured surroundings. Robowatch develops processes for intervening autonomously in part or in full in the vehicle's propulsion and control systems, that is for acceleration and braking.

For autonomous vehicle control, Robowatch has developed a robust vehicle-independent route planning process (see Figure).

For trajectory planning, various navigation techniques are combined: track detection, object detection and orientation. Likewise, non-holonomous vehicle equations of motion and real-time criteria of the entire trajectory planning algorithm are factored in. So as to be able to react, for example, to unknown obstacles detected by the sensors, deviations from this ideal trajectory are made by planning special manoeuvres as a differential motion from the ideal route. The result of this planning is the vehicles desired motion, which is realized by the vehicle's control system in the form of actuator settings.

Mission planning with visualization for autonomous vehicles

Robowatch's route planning procedure works out the current vehicle position by applying various navigation techniques.

Changes in direction are computed by comparing the actual with the target position. The reference direction is received by the trajectory planning process from the mission planning program specially developed for this purpose. Serving as the basis for this is a digitized map, through which the logical reference to the vehicle position is created. The trajectory planning process fixes the precise position through the *mission planning program* and its integrated reconciliation with the map.

The mission planning program is made up of GPS visualization tools, a communication interface to the vehicle, route and mission planning functions as well as import functions for geo-referenced map material.

Detection and bypassing of obstacles

Essential for collision-free and automatic navigation are detection of obstacles and, if necessary, a real-time strategy for driving round these, provided by the autonomous vehicle system. Today, obstacles and objects in the vehicle's surroundings can be recognized by a range of sensors, like video camera, laser scanner, radar, ultrasonic sensor, photonic mixer device (PMD), etc.

In accordance with application specifications, Robowatch offers *software libraries* for obstacle detection and bypassing. Visualization tools for checking and modelling the sensor data help the user to interpret the vehicle's environment and its behaviour.

Recognition of routes and tracks

When navigating in unstructured terrain, unmanned vehicles require precise control through the trajectory planning system. Representing a key software component is the *track recognition algorithm*.

With the aid of colour and object classifiers as well as a smart shadow compensation process, tracks, roads, intersections as well as known elements in the surroundings, like traffic signs, meadows, trees, beacons, cars and non-natural colours, are recognized. From this information, the vehicle receives its current position in relationship to the detected path as well as a significance value for the subsequent path that is fed into the trajectory planning function.

Smart detection of persons indoors and outdoors

Substantial emphasis with the realization of person detection with mobile robots is the recognition of foreign movements in the surrounding field of the robot, also - and above all - during its own movement.

The moving target recognition works both ways - with a resting robot as well as during a forward or a possible backward motion of the robot. A distinction will be made between fixed objects, which induce themselves if applicable relatively to the sensors, and foreign movement, as they are produced e.g. by a moving person. The latter arrives at the evaluation.

The moving target recognition is based on a double signal processing. Thus the sensor technology is conceptional able to measure radial velocities, whereby the measured radial velocity enters an angle dependence between object and sensor adjustment. Robowatch develops mobile video and radar monitoring systems.

Fast sensors for detection and recognition of flying threats at short distances

I. Kaufmann, L. Doktorski (FGAN Research Institute for Optronics and Pattern Recognition FOM), Germany

Abstract

An active protection for buildings and vehicles could expand the range of avertable flying threats and reduce the necessary amount of passive armour. We compared different sensor types (IR, UV, Laser-Radar, etc.) for their ability to distinguish threats from background features and to track their flight paths. We evaluated the ability of the sensor concepts to provide data like size, trajectory, and velocity, the latter being the best criterion to discriminate a fast projectile against possible false alarms.

Introduction

In different situations buildings and vehicles have to be protected against armour breaking threats like RPGs or unpropelled grenades. Especially for vehicles passive armour is limited to a reasonable weight. An active protection system would reduce the necessary amount of armour as only smithereens of defeated threads have to be absorbed. Sensors of active systems like the Israelian Trophy [1] or the Russian Arena [2] need a minimum detection range of a few tens of meters to have sufficient time to initiate a reaction. On the other hand, an RPG e.g. [3] can be fired from a distance below 20 m. Therefore a sensor system is needed to allow a short distance detection and recognition. The major problem in such an effort is to discriminate between threads and false alarms from the background.

Physical features of projectiles

Velocity and trajectory

The velocities of flying threats vary between 70 m/s for unpropelled grenades, 200 m/s for guided missiles and up to 300 m/s for certain RPGs. These very high velocities would make up a perfect discrimination criterion between threads and unperilous objects, that can be supplemented by the trajectory.

Geometry

The resolution of a sensor has to be adopted at the expected thread sizes. Diameters start at about 5 cm for grenades and end at about 15 cm for certain missiles. Using a sensor view that is not directly head on it might be possible to determine the length of an approaching object, varying between a few centimeters for grenades and about 1 m for missiles.

Heat emission

Three heat sources have to be discussed concerning flying threads: The firing of grenades causes an initial but decaying heat emission of the projectile. The plume of a rocket is a strong source of heat emission, but different threads are propelled only during the first phase of their flight. Due to cooling effects and heat distribution, aerodynamic heating becomes relevant above about Mach 1 (333 m/s). But most projectiles won't fly long enough to reach a temperature that causes significant more thermal radiation than the background.

Plume

In addition to the IR visible heat, the plume of most propelled threats does emit visible and also UV radiation. The latter depends on the used propellant.

Evaluation of different sensor systems

IR

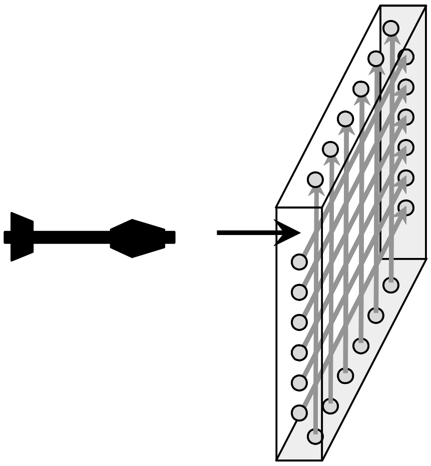
A big advantage of an IR system is the ability of night vision. Nowadays, IR sensors are available providing a frame rate of up to several 10 kHz [4]. Therefore, depending on their latency, it would be possible to use IR sensors for the detection and classification within the last view meters of a projectiles flight. Because some threats lack an intense IR signature it would be necessary to perform a time consuming image analysis to distinguish them from the background. In addition there are too many possible false alarm sources like sun reflections, fire and any sort of machine. An image from a single sensor will not provide distance information for the calculation of a trajectory. Using triangulation from images of two sensors with a sufficient base would further increase the computing time.

UV

Because UV from the solar radiation is blocked by the atmosphere, the background would be dark at this spectral range. Therefore it is easy to spot each UV source. On the other hand, not all threads do have an UV signature. In many cases the UV radiance derives from a backward located plume being hidden by the head of the threat in the case of a head on view. In addition many technical devices, especially devices that use high electric current or voltage, cause hard to distinguish false alarms.

Light barriers

In the context of UV and IR we have discussed imaging systems. An alternative realisation for short distance recognition could be a curtain like system of light barriers in front of the threatened object. Different arrangements were proposed in the past for such purposes. A double row of skyward orientated sensors [5] uses the projection of a projectile to calculate velocity and trajectory in azimuthal orientation. A rectangular grid of light barriers [6] estimates the exact position where it is penetrated by a projectile. All those approaches would need a construction in front of the threatened object.



Schematic drawing of the defending system proposed by [6] using a rectangular grid of light barriers.

Laser Radar

Laser radar provides a detailed, geometrical mapping of the environment. The measured distances make it easy to distinguish between the background and objects by a simple threshold. Velocity and trajectory of a possible threat can be calculated from the distances derived from a sequence of laser radar data. Unfortunately, up to now, there are no laser radar or 3D-camera systems available, that offer a sufficient high frame rate and low latency to meet the requirements. This problem may be solved by using a line of sensors or multiple single point range finders instead of a 2 dimensional detection array. Using an adequate geometry, threats could be detected at appropriate positions to calculate the necessary parameters for classification and estimation of the trajectory.

Conclusion

We evaluated different sensor concepts regarding their potential to detect fast flying threats. It should be possible to detect and characterise threads approaching with up to Mach 1 (333 m/s) within the last 10 m of their flight. UV and IR sensors provide significant features for the classification of certain threats and modern IR sensors have a sufficient frame rate. However, the computing time to analyse complete 2D images to determine the trajectory of a heading threat will not meet the claims of the required system. A light barrier system would need a sensor construction in front of the protected object. Range finding sensors would provide data which are easy to analyse regarding the trajectory and geometry of an approaching object. To ensure the detection and proper classification to avoid false alarms a combination of different concepts and sensors is worth considering.

References

1. Trophy Active Protection System (http://www.defense-update.com/products/t/trophy.htm)
2. ARENA-E Active Protection System (http://www.defense-update.com/products/a/arena-e.htm)
3. RPG Rocket Propelled Grenade Launcher (http://www.defense-update.com/products/r/rpg.htm)
4. IRCAM-KAMERAS (http://www.ircam.de/produkte/ir_kameras_d.php)
5. Schutzvorrichtung für Zielobjekte immobiler und mobiler Art gegen Zerstörung durch angreifende Munition, M. Held, Patentschrift DE 26 12 673 C1, 1976
6. Armament system and explosive charge construction therefor, F. Thomanek, United States Patent 4,051,763; 1977

Surveillance of Security-critical Compounds and Buildings Using a Team of Autonomous Robots

Frank Kirchner, Markus Eich, Dirk Spenneberg, German Research Centre for Artificial Intelligence, Robotics Laboratory, Bremen, Germany, {frank.kircher, markus.eich, dirk.spenneberg}@dfki.de

Abstract:

The surveillance of security-critical compounds and buildings requires large amounts of human and financial resources. Office buildings and industrial compounds are targeted frequently by theft, sabotage, or industrial espionage. Even higher costs can be expected, if security systems have to be upgraded. In general, most customers from the security business don't want to replace an existing security system, but prefer to enhance it in order to make it more efficient. Therefore, consequential costs for maintenance and personal training have to be reduced, as these factors are a criterion for customers to invest into a security system.

As a solution to the described problem, the DFKI Laboratory in Bremen is developing a team of autonomous mobile security robots which can be seamlessly integrated into existing security systems. These mobile security robots are able to navigate autonomously and are not limited by battery-life, because they can recharge their batteries without any user assistance. The robot team is self-organizing and provides an intuitive interface via voice control. As part of the SentryBot project, a co-operative team of five different robots is being developed which is able to secure buildings and industrial compounds. Four identical systems are designed for a co-operative surveillance approach in indoor environments; one system is designed for outdoor security missions.

Introduction and Related Work

Research regarding security robots is primarily driven forward in the USA, which plays a leading role regarding security robots. One of the security robot producing companies is ActiveMedia, which manufactures the robots *Patrolbot* and *P3-AT* [Patrol]. These systems have the ability to navigate autonomously and can be equipped with a variety of application sensors, like thermal vision or passive infrared sensors. For military applications, the robots Talon from Foster-Miller [FMTAL] and the *Packbot* by iRobot [Packbot] show the state of the art regarding mobility in rough terrain. All of these systems are tele-operated and are used for remote surveillance and reconnaissance missions. In Germany only a few companies are working on security robots [Mosro, Securo]. All security robots that are on the market are able to navigate between manually defined waypoints, but lack the ability to dynamically plan the optimal path or work as a team of interacting robots. All systems mentioned above are non-cooperating systems. The drawbacks of such single robot systems are that they have a much higher risk of failure, because there is simply no backup system that can overtake the patrol of a lost system. Also they are not able to communicate with each other or “work together” on a given mission plan, i.e. monitor a compound or a building. Another drawback of existing systems is that they are tele-operated or simply operated on pre-defined waypoints. In this work we present a concept of how a team of mobile autonomous robots can be used to secure and monitor compounds and buildings in a co-operative approach. In contrast to existing mobile security systems, our approach uses the aspects of a robot team that is superior to an individual robot. Another focus of our work is on the seamless integration of our system into existing security concepts, which means that existing alarm systems in buildings are considered. Additionally, the security personnel are regarded as part of a human-robot team.

Surveillance and Security Robotics at the DFKI

The robotics lab at the DFKI is developing an autonomous team of robots to fulfil the needs of a highly integrated robot system, which can be integrated into existing security concepts. By integration we mean not only deploying a robot that is able to trigger an alarm by its motion sensors, but a robot system which extends an existing alarm system and supports security personnel in their tasks. Our focus with security robots is on the cooperation of the individual robots to form a team in order to fulfil their mission, and on easy and intuitive user interaction. The operator, i.e. the security guard from our lab, is included in the development process and is therefore able to evaluate constantly the usability of the security robot team.

The Autonomous Security Robot Team “SentryBot”

With the SentryBot project, we have undertaken the first step towards an autonomous team of security robots. The current indoor security team, which consists of four autonomous robots, is equipped with security relevant application sensors, which are able to sense an intrusion into a building along with its motion sensors and its camera. The applied sensors consist of passive infrared sensors as well as radar sensors, which are able to detect motions even through walls up to a distance of 12 meters. This allows one, to monitor rooms behind closed doors, in an indoor environment, which arises from the situation that office doors are generally locked during non-working hours. Each robot is also equipped with a laser range finder, which allows for fully autonomous self-localization and path planning. The robots are able to dynamically re-plan their path from the current position. Every robot has a full-scale embedded computer on board, which allows autonomous map-based navigation. With the given energy resources the system can operate around 5 hours. With the ability to reach a recharging station fully autonomously, the operating time is extended to 24 hours, 7 days a week.

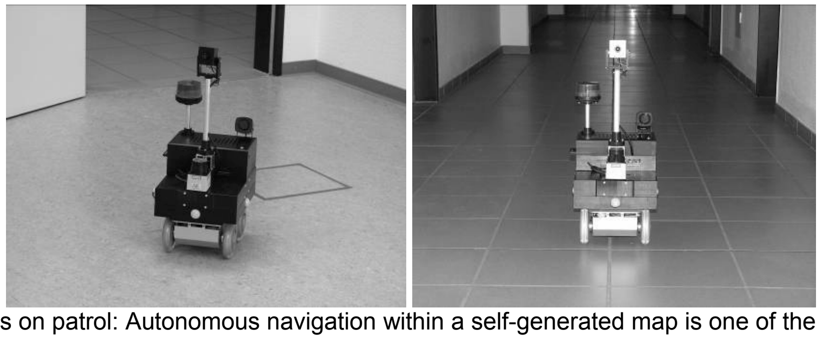


Fig. 1: SentryBots on patrol: Autonomous navigation within a self-generated map is one of the key aspects of the system.

Architecture

In order to reduce the time of development, the communication architecture is partly based on the Carnegie Mellon Robot Navigation Toolkit [CARMEN], which provided basic algorithms for self-localization and single robot communication. CARMEN also provided a message based inter-process communication (IPC), which was used in the SentryBot project. We enhanced this architecture with modules relevant for security robots, like application sensor processing and transmission. We also enhanced it to make it usable for multi-robot systems and interaction with a human operator. Beside direct joystick control, the user can give patrol points or regions of interest via the graphical user interface. It is also possible to select waypoints via voice control to the input layer. The security personnel are therefore able to give commands via a voice interface, while they are on patrol themselves. Figure 2 gives a compact overview over the SentryBot software architecture.

User Interaction and Interfaces

The current implementation of the graphical user interface allows an individual control of each of the four indoor systems. The user can interact with the system directly by controlling each robot individually or by setting waypoints within an obstacle map, which is provided by the control system. Another way of interacting with the system is by selecting certain regions of interest inside the given map and assigning a numbered relevance to it. The planning system will assign the available robots to fulfil this task, based on the available resources, the available energy of each system, and the current position of the individual system within the map.

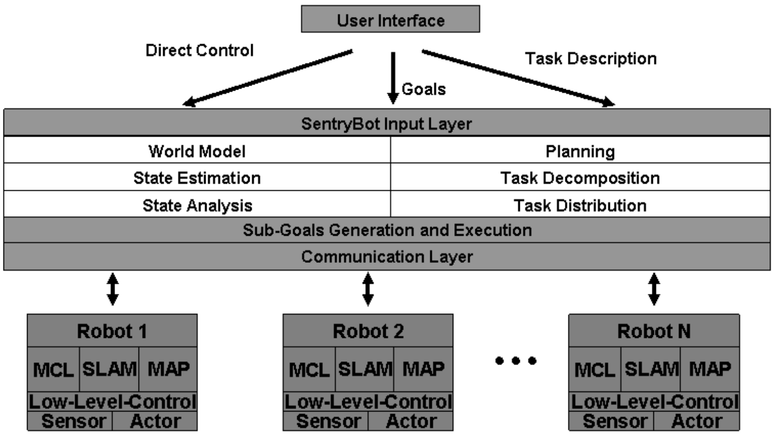


Fig. 2: The software architecture of SentryBot team: It contains the user interface, a planning architecture and a module for task decomposition and distribution. The modules needed for navigation, mapping and control are distributed on the individual robots, which allows an autonomous navigation if the connection to the control system is lost.

Conclusion and Further Work

In this work we presented our approach of using a co-operative team of robots to secure and monitor buildings. The presented software architecture, which allows deploying a team of autonomous robots, makes use of a centralized planning approach. Each system is able to navigate and trigger an alarm fully autonomously at given waypoints. The waypoints within the common map are set by the centralized planning system which holds the high-level mission plan. The drawback of such a centralized control architecture is that there is no robot interaction when the communication to the central control computer is lost. In this case, individual waypoint updates will no longer be possible. To solve this problem, we are researching a distributed planning approach that is based on individual communications between the systems. In this case the robots must communicate directly and can also serve as relay stations for the other robots.

Another ongoing work at our lab is to extend the existing team of indoor robots with an autonomous outdoor platform. The outdoor system will be equipped with suitable intrusion-sensing sensors, which are processed on board. Research in our lab will focus on how to expand our planning architecture in order to combine indoor and outdoor systems in order to provide complete autonomous surveillance of compounds and buildings using a common mission planning system.

References

[CARMEN]	http://carmen.sourceforge.net
[FMTAL]	http://www.fostermiller.com/lemming.htm
[MOSRO]	http://www.robowatch.de
[PACKBOT]	http://www.irobot.com/sp.cfm?pageid=109
[PATROL]	http://www.mobilerobots.com/PatrolBot.html
[SECURO]	http://www.neobotix.de

Optical Stand-off Detection of Explosives and Improvised Explosive Devices

Fraunhofer-Initiative OFDEX

Frank Fuchs, Joachim Wagner, Christoph Wild, Fraunhofer Institute for Applied Solid-State Physics IAF, Freiburg, Germany

Horst Krause, Frank Schnürer, Wenka Schweikert, Fraunhofer-Institut für Chemische Technologie ICT, Pfinztal, Germany

Cord Fricke-Begemann, Peter Jander, Reinhard Noll, Fraunhofer-Institut für Lasertechnik ILT, Aachen, Germany

Raimund Brunner, Jürgen Hildenbrand, Armin Lambrecht, Fraunhofer-Institut für Physikalische Messtechnik IPM, Freiburg, Germany

The Fraunhofer Society is the leading European organisation for applied research. It pooled its know-how in the fields of explosives, laser spectroscopy, semiconductor-laser design and manufacture, and system integration in order to develop optical technologies for the stand-off detection of explosives. Within the framework of a comprehensive research and development project called OFDEX, four Fraunhofer institutes are working jointly towards the development of a demonstrator remote detection system which will be tested in realistic scenarios.

For specific scenarios, the limits of detection required are estimated from both simulations and experiments. Various spectroscopic methods including infrared spectroscopy and laser-induced breakdown spectroscopy (LIBS) are currently being assessed for inclusion into the system.

The OFDEX initiative will improve the most promising among these technologies with regard to their detection limit and cross-sensitivity towards changing environmental conditions. The most suitable technologies will be integrated into a field-deployable demonstrator system. The poster will focus on the optical methods used and present some preliminary results.

The Growing Threat of Terrorism

The threat of terrorism has been increasing worldwide for some years now. Media reports about suicide bombers, car bombs, and explosions have become commonplace, with the greatest threat emanating from suicide bombers in crowds and car bombs in traffic. The societal, economic, and political sphere are equally interested in having all technological options exhausted to prevent such attacks.

So far, no remote-detection devices are available that will detect potential assassins from a safe distance. In the field, well-trained sniffer dogs are the best alternative for sensing explosives remotely, albeit at distances of no more than a few metres. Portal technologies and sampling detection systems are similarly unsuited for remote detection.

Development Needs

To identify potential suicide bombers effectively, the following conditions must be met:

– Remote detection (‘standoff detection’) of explosives on persons and in cars over a distance of up to 100 metres

– Identification of infinitesimal traces of explosives

– Dependable measurement results within seconds

– Very low incidence of false alarms

– Detectability of a wide range of possible explosive configurations

Together, these performance requirements demonstrate clearly the magnitude of the technical challenge involved in developing suitable measuring systems for the remote detection of explosives.

The Fraunhofer OFDEX initiative

Within the framework of a comprehensive research and development project, four Fraunhofer institutes are working jointly on this development goal. When the Fraunhofer OFDEX initiative was launched, the Fraunhofer Society pooled its competences in the fields of explosives knowhow, laser-spectroscopy processes, semiconductor-laser production, and system integration.

The initiative’s four partner institutes, the Fraunhofer IAF, the Fraunhofer ICT, the Fraunhofer ILT, and the Fraunhofer IPM will be jointly developing technical solutions for the remote detection of explosives from now on.

The OFDEX Approach

Many explosives can be detected because they exude gas which may form a "vapour cloud" (plume) above a potential assassin. Moreover, as most explosives are absorbed well by surfaces of many kinds, it is likely that persons (e.g. their clothing) or parts of cars (e.g. door handles) will be contaminated, a fact that is similarly useful in remote detection.

The detection process itself will involve a variety of spectroscopy technologies based on IR lasers. The OFDEX initiative will improve the most capable among these technologies with regard to their detection limit and cross-sensitivity towards fluctuating environmental conditions, and combine them to create a mutually-complementary orthogonal system.

Development activities aim to produce demonstrators that permit the remote detection of explosives in realistic sample scenarios.

AMROS – an Autonomous Mobile Robotic System for Multisensor Surveillance of Real Estate

T. Emter, E. Monari, Ch. W. Frey, T. Müller, H.-B. Kuntze, A. Laubenheimer, M. Müller

Fraunhofer Institute for Information and Data Processing (IITB)
Fraunhoferstr. 1, 76131 Karlsruhe, Germany

Multisensor service robots operating in indoor and outdoor environments of endangered public and industrial objects (e.g. stadiums, waterworks, power plants, chemical facilities, etc.) are able to make an essential contribution to combating terrorist and criminal threats. More efficient and reliable than human guards, robots have the ability to patrol nearly autonomously, detect and diagnose suspicious situations automatically and execute adequate protection measures. The AMROS (Autonomous Mobile Robots for Security Applications) system, developed at the Fraunhofer Institute IITB, is an autonomous mobile robotic system for multisensoric outdoor surveillance of real estates. The AMROS system concept will be presented in this paper.

Introduction

For security surveillance of endangered public and industrial objects (e.g. stadiums, waterworks, power plants, chemical facilities, etc.) autonomous outdoor inspection robots can be more efficient and reliable than human guards since they are able to automatically patrol and perform adequate protection operations.

While for the automatic inspection of indoor environments powerful robotic systems are commercially available for the outdoor inspection of estates only a few suitable systems are on the market. Thus, there is a considerable demand for the development of autonomous multi-sensor based robot systems which can comply with the more complex and varying outdoor surveillance scenarios.

The **AMROS** (**A**utonomous **M**obile **Ro**bots for **S**ecurity Applications) system, developed at Fraunhofer Institute IITB, is an autonomous obile robotic system for multi sensor outdoor surveillance of real estates

AMROS System Overview

AMROS is intended as a system consisting of multiple mobile robot platforms and one or several control rooms (Fig. 1). The concept is to provide a modular development and demonstration platform for fast prototyping of innovative hardware and software components required for autonomous navigation and path planning, exploration of the environment, detection and identification of threats as well as their elimination.

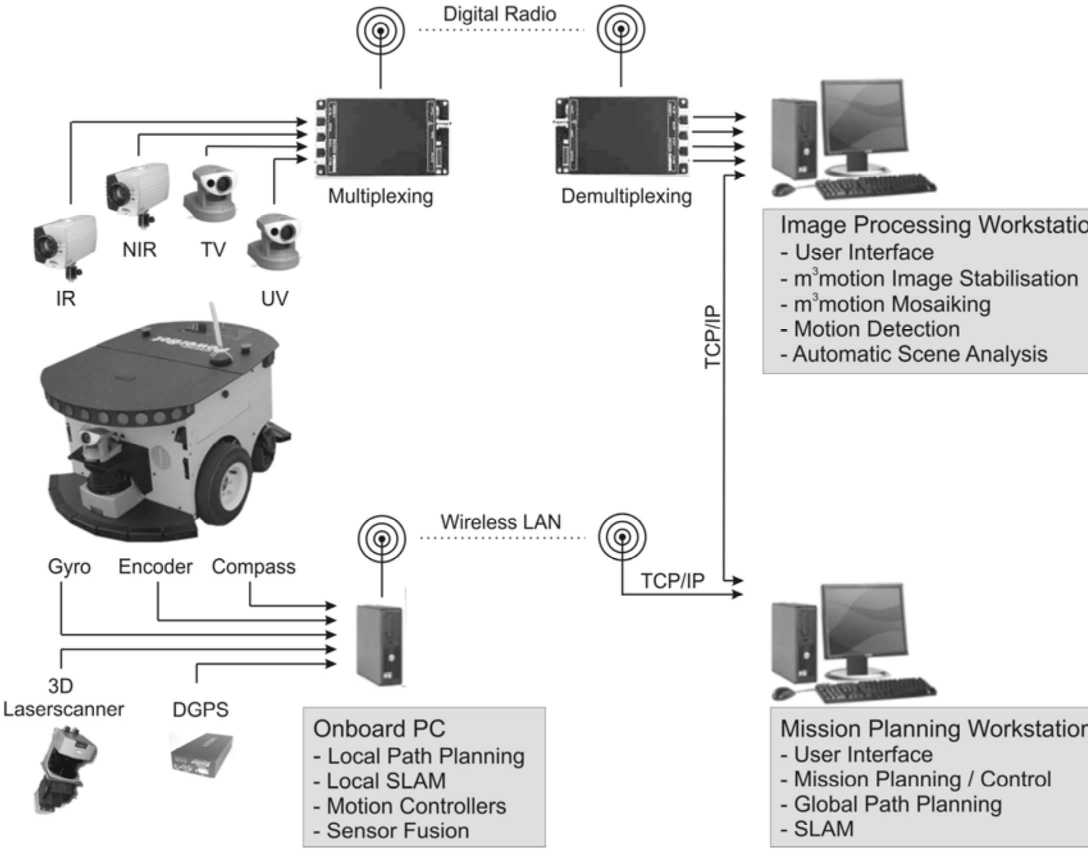


Fig. 1: AMROS System Overview

As a development and demonstration platform, the AMROS mobile robots are equipped with various heterogeneous sensors for fast adaptation to different scenarios and environments. In order to cope with changing light conditions the robots are equipped with different vision sensors with a spectra range from ultraviolet to far infrared (UV, TV,NIR, IR) and include monocular as well as stereo camera systems. For the navigation and path planning the robot is equipped with various position sensors as e.g. DGPS, 3D laser scanner, odometer, compass, a laser gyroscope, bumpers and acoustic sensors. Additionally the information from a stereo-camera system is evaluated for obstacle detection and further improvement of navigation and route planning. The upper level of the AMROS system hierarchy comprises the image processing modules and the mission planning and control modules.

For mission planning a user interface has been implemented which allows the operator to interactively plan surveillance mission. Based on this task the global path planning algorithm automatically generates the robot trajectories and transmits them via WiFi to the local path planning modules on the robot. With respect to the map of the estate the path is then executed by motion control algorithms which also provide a dynamic obstacle avoidance mechanism.

For automatic vision-based surveillance of the estate (motion detection, human detection and tracking) the several video streams from the vision sensors are transmitted by a digital video link (OCFDM) to the image analysis modules in the control room. Additionally the existing WiFi link is used for transmission of meta data, control commands to pan/tilt cameras and image sequences with low data rates (e.g. MJPEG / MPEG4).

Outdoor Localization, Mapping and Navigation

In order to patrol autonomously around a building on a given path it is essential for the robot platform to locate itself precisely in a map of the estate. In contrast to a structured indoor environment with predominately straight walls and perpendicular structures in an unstructured outdoor environment without clear contours (e.g. hedges, bushes) enhanced strategies have been implemented for the SLAM (Simultaneous Localization and Mapping) task. As uncertainties in the odometry sensors (dead-reckoning) accumulate over time also the absolute position from an additional DGPS sensor underlies errors due to multi-path propagation in the proximity of large buildings. In order to ensure a robust localisation of the robot in an outside environment Kalman-Filter and Particle-Filter methods have been implemented to ensure a reliable estimation of the robot position in the unstructured outdoor environment.

Visual Surveillance

For automatic scene analysis several up-to-date image analysis methods are available for the fused output of the vision sensor data. Based on a real-time image-to-image registration algorithm, motion detection can be performed, even while the robots are in motion themselves. The applied m^{3}motion$^®$ real time image stabilisation allows a detailed analysis of the video streams even when the robot is moving on rough ground. With the integrated m^{3}motion$^®$-mosaiking module it is also possible to generate mosaics in real time which provide the operator with an extended view of the area and the objects under investigation.

For object tracking the system provides several different tracking algorithms (blobclustering, particle filter and feature based correlation approaches). Furthermore all approaches are sensor independent. With respect to the surveillance task and environment the operator can select the suitable data source (NIR-, IR- or video) and process the data with the appropriate algorithms. In future the output of these mechanisms will be used for the automated pursuit of suspicious objects by means of visual servoing.

Summary and Outlook

Due to its dynamically reconfigurable software and hardware components the AMROS system is adaptable to various surveillance scenarios and environments. The current research is focused on additional vision based surveillance capabilities and enhanced SLAM functionalities.

Threat Detection and Characterisation by Spectroscopic THz-Imaging

A.Kupsch, J.Beckmann, U. Ewert, A. Lange, M.P. Hentschel
Federal Institute for Materials Research and Testing, Unter den Eichen 87,
D-12205 Berlin, Germany

Abstract

The emerging technology of generation and detection of Terahertz waves (1 THz = 10^{12} Hz) is a promising candidate for the future threat detection in areas where X-rays cannot be applied for several reasons.

There are three reasons for application of THz radiation: (i) as non-ionizing radiation it is harmless for the human body, (ii) it penetrates isolators and materials of low electrical conductivity (such as plastics and clothes) which are opaque in the visible spectral range, and (iii) the enhanced spatial resolution in comparison with mm-waves, due to the smaller wavelength. Moreover, THz time domain imaging supplies additional spectral information which may be utilized for materials identification.

Advantages of THz imaging are demonstrated in comparison to conventional X-ray radiographs at two examples: (1) Small structural details of a mock-up letter bomb hidden in a paper envelope are resolved in the sub-mm range. (2) A plane arrangement of different explosives exemplifies the spectral sensitivity up to 2.0 THz in order to distinguish them from common packaging (masking) material, or even some explosives from each other.

Why Terahertz waves? - Introduction

The challenge of future threat defence technologies in sensitive areas of public domain means to do the splits: The people’s freedom should not be restricted, their health must not be hazarded – neither by inspection nor by terrorist threats – ,and threats must be detected with the highest probability possible.

The developing technology of THz waves is a promising candidate to meet these requirements to a high degree, in particular with respect to stand off screening of persons. Illicit items like weapons (fire arms, knives etc.) or contraband (explosives, drugs) can be detected without any radiation harm even if they are concealed beneath the clothes.

The term ‘THz band’ refers to the spectral range between 100 GHz and 10 THz of electro-magnetic waves. It closes the gap between technically mature applications of the adjacent ranges: high-frequency electronics in the GHz band (millimeter waves) used for radar, broadcasting and communication and techniques in the infrared optical range on the high-frequency side.

The potential of the THz range is its superiority to other parts of the spectrum regarding certain aspects: the better spatial resolution and broad-band spectral information compared to millimeter waves, the transparency of clothes and packaging material which are opaque at optical frequencies, and its inherent harmlessness to biological tissue (like the human body) compared to X-rays. A disadvantage of THz practical applications is the considerable absorption in humid atmosphere due to the polarity of water molecules.

Imaging by THz Time-Domain Spectroscopy (TDS)

Measuring in the TDS mode means direct sampling of the THz wave's *temporal electrical field* (designated as 'wave form' below, see Fig. 1, left), i.e. the wave's phase information is conserved, contrary to optical spectroscopy techniques which usually measure the wave's (spectrally resolved) *intensity*. This allows for straight forward Fourier transformation (FT) of the measured temporal wave form, and eventually provides the complete complex-valued (magnitude *and* phase) spectral components (Fig.1, right). From the point of view of physics the THz wave samples the dielectric material properties, i.e. the polarizability of molecular dipoles on the microscopic scale. The measurable, macroscopic phenomenon is equivalently described by the complex-valued dielectric function or the refractive index, respectively. The desired broad band THz waves are generated by optical rectification in biased electro-optic crystals which are irradiated by pulsed femtosecond lasers (1 fs = 10^{-15} s).

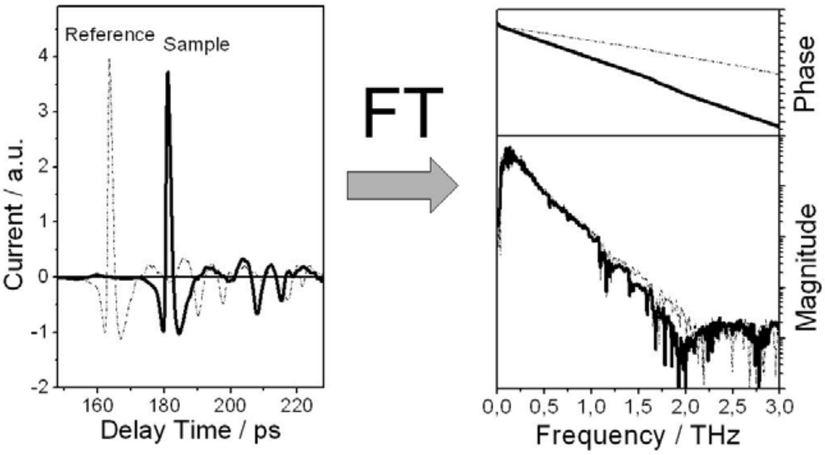


Figure 1: Measured raw data of a polyethylene sample and reference (air) in the time domain (left), and the respective magnitude and phase of frequency components as obtained by Fourier transformation (right).

In practice any material penetrating wave is compared to a reference wave which is assumed to travel the respective path length in air ($n_{\mathrm{Air}} = 1$). In order to extract spectral physical properties both waves are Fourier transformed followed by further procedures. For the purpose of imaging the entire wave form is sampled within 50 ms and stored at each position. This kind of collecting raw data is highly time and storage consuming. On the other hand, a huge variety of measured or derived scalars can be selected for imaging. They are subdivided into three classes referring to their origin in time or frequency domain, as well as derived physical parameters. Possible characteristics are listed in Table 1. The final choice of the appropriate scalar to elucidate the respective problem depends on the operator's decision.

Table1: Classification of THz images according to their origin.

Class	Examples
Time domain	maximum/minimum pulse amplitude, temporal position of pulse maximum, integrated pulse absolute
Frequency domain	integrated FT magnitude in selected intervals, FT phase
Physical parameters	penetrated thickness; refractive index, absorbance, transmittance (slope, curvature, averaged or selected frequencies)

Spectral information – Explosives

In order use the spectral information we apply a THz radiograph of explosive pellets. The spectra do not exhibit significant features such as absorption lines. The greyscale in Fig. 2 represents the local index of refraction $n(\omega)$ averaged in a 0.3 to 1.5 THz interval. Different explosive substances are well distinguished quantitatively since the error limits of $n(\omega)$ amount to 0.01 or less except for the RDX pellet which is too heterogeneous (although differences are not recognizable in greyscale). The derivation of the physical parameter $n(\omega)$ is based on a fully automated algorithm.

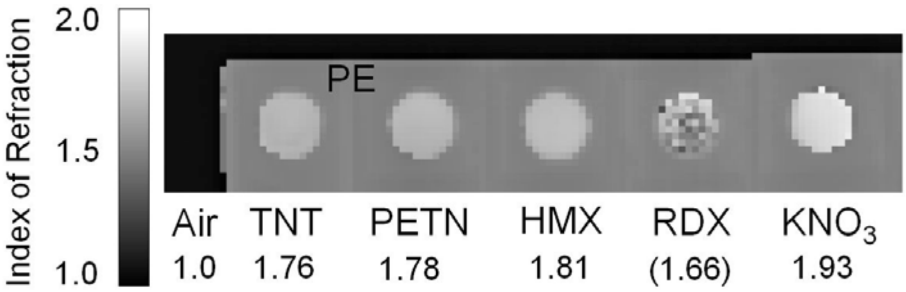


Figure 2: THz image of a planar arrangement of explosives embedded in a polyethylene (PE) sample holder. The numbers represent the pellets' index of refraction as a local average.

Spatial resolution – Mock-up letter bomb

The example of a mock-up letter bomb illustrates the capabilities of THz imaging with respect to the perceptibility of small structural details. At the first glance the THz radiograph of Fig. 3 (D) reveals the highly contrasted metal constituents (battery, wires, conductor paths, gear wheel) as bright areas due to the metal's reflectance. Since high frequency components (1.0-1.5 THz) are applied the according spatial resolution (small focus ~300 µm) even allows for perception of the integrated circuit's inner details. The plastic constituents are identified by their outer shapes created by scattering effects. The circular details in the explosive dummy and traces of the adhesive tape emphasize the THz wave's high sensitivity to thickness variations.

Two X-ray images – a radiograph (B) and a back-scatter topograph (C) – demonstrate that THz cannot compete with respect to resolution due to wavelength. Since the radiograph is sensitive to atomic numbers and material's density the soft matter details are missed, the back-scatter topograph is a well competing alternative.

In spite of mentioned drawbacks the harmless character of THz waves should be kept in mind as a big advantage. Improvised explosive devices worn by a person can be detected safely with THz waves in contrast to X-rays.

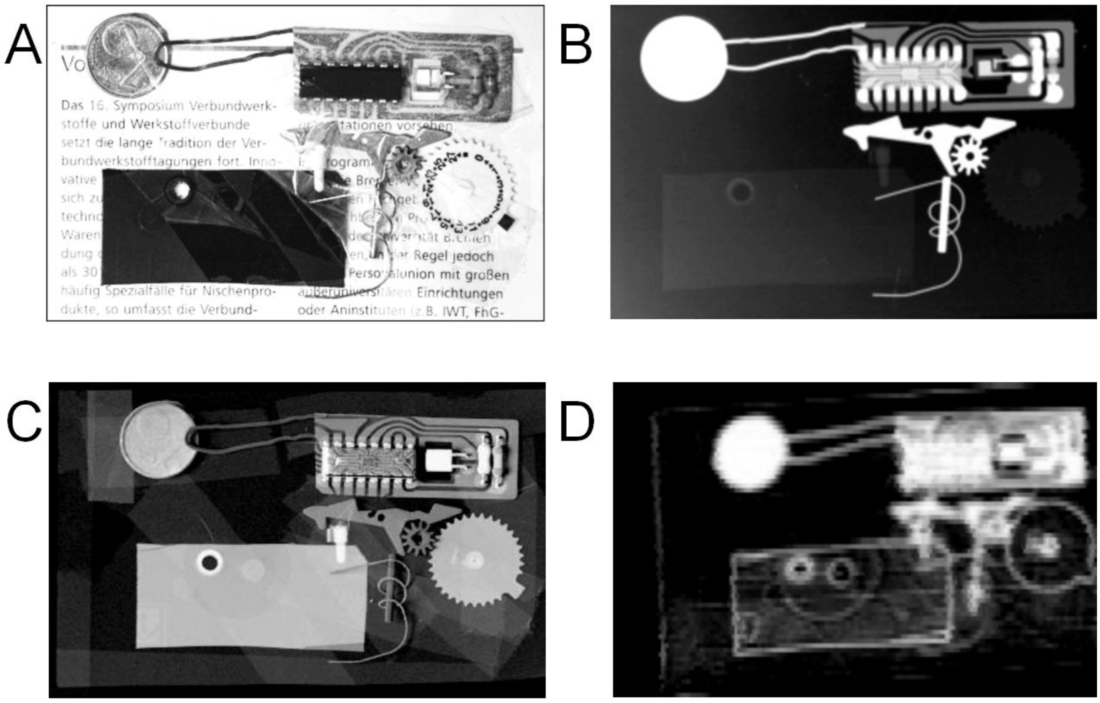


Figure 3: Photograph of a home made mock-up letter bomb incl. battery, electronics and trigger (A), conventional X-ray radiograph (flash tube, 150 kV) (B), back-scatter X-ray topograph (pencil beam, 18keV) (C), and a THz radiograph obtained from integrated Fourier amplitudes (1.0-1.5THz) (D).

Karlsruhe Generic Agile Ground Station

S. Leuchter, T. Partmann, L. Berger, E. J. Blum & R. Schönbein

Fraunhofer Institute for Information and Data Processing (IITB), Karlsruhe, Germany

The Karlsruhe Generic Agile Ground Station is an adaptable prototype system for managing sensors and mobile sensor platforms. The main task of the ground station is to work as an ergonomic user interface and a data integration hub between multiple sensors mounted on light UAVs (unmanned aerial vehicles) or UGVs (unmanned ground vehicles), stationary platforms (webcams), ad hoc networked sensors, and a super-ordinated control centre.

Task Description

The application scenarios for such a surveillance system range from safety to security related settings. Examples for such scenarios are emergency management and securing sites with critical infrastructure. These application scenarios include the demand for real-time information supply in order to support operation personnel quickly acquiring situation awareness.

The system uses multiple sensors and different mobile platforms to bring them to potentially interesting locations in order to cope with large or not beforehand sensor equipped areas. The actual prototype demonstrator is focused on light UAVs as mobile platforms.

The tasks of such a human-machine system include:

- task management
- mission planning
- control of mobile platform (without line of sight through a virtual cockpit)
- sensor control
- dynamic situation display/situation awareness
- fusion of sensor data
- sensor data exploitation
- reporting, generation of alarms
- archiving

Empirical evidence shows that the control of a light UAV is such a demanding task that it is not possible to evaluate and exploit all incoming sensor data in parallel. Thus two operators are needed to achieve surveillance goals in such a setting.

System Design

The Karlsruhe Generic Agile Ground Station consists of two operator workstations with three monitors (the middle one is used by both operators, see fig. 1). It is designed to be moveable. The workstations feature ergonomic software for supporting operators' tasks.

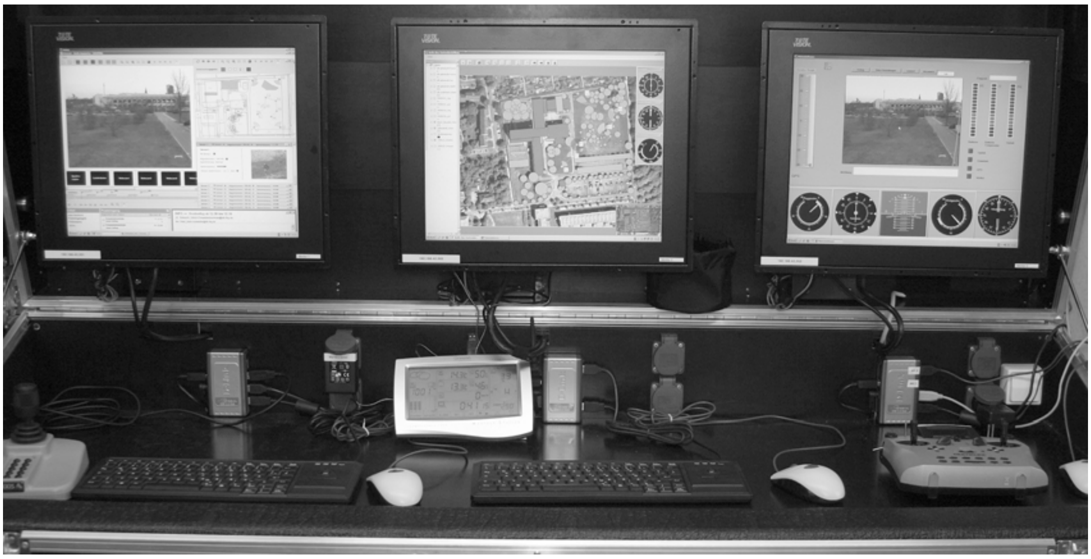
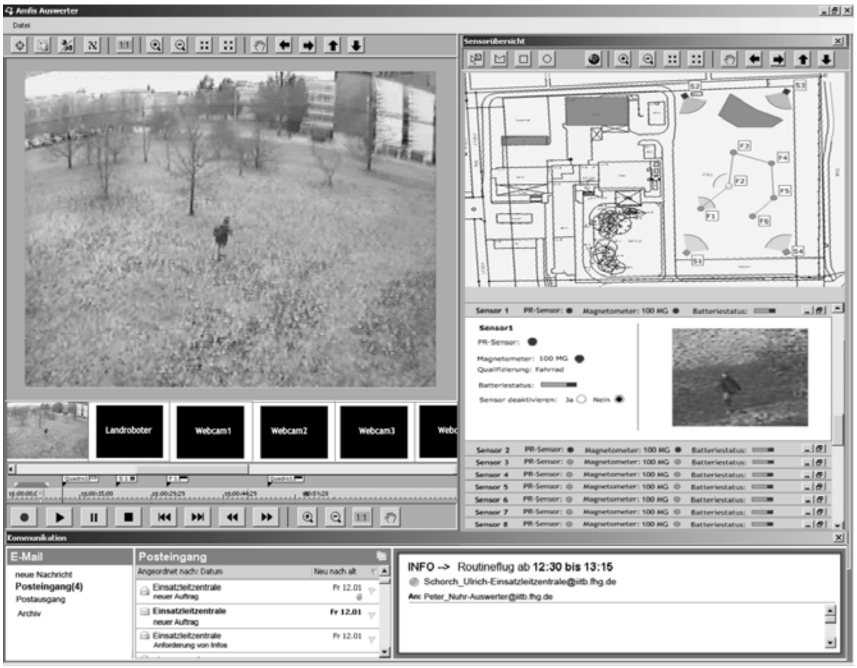


Fig 1: Karlsruhe Generic Agile Ground Station

One Operator receives data streams from sensors (e.g. video) and is responsible for sensor data interpretation, sensor data fusion, communication, and coordination with the control centre. He or she uses a specific software tool that displays sensor streams (see fig. 2). It is possible to apply image sequence processing algorithms e.g. to stabilize a video coming from a moving platform. The user can switch between different sensor streams. Alarm messages from event sending sensors are displayed together with their locations. The software also has a message oriented communication interface to get tasks from and to report events to a super-ordinated control centre.

The other operator is responsible for mission planning, flight/vehicle control, supervision, and camera control. He or she uses a virtual cockpit which is specific to the vehicle and sensory. Fig. 3 shows the virtual cockpit for control of a light UAV that carries a video camera on board.

Both operators use the situation display on the workstation in the middle (see fig. 4). This display contains instruments showing the weather conditions (mainly for supporting the UAV pilot), sensor alarms, positions of static sensors and mobile platforms and view angles of video cameras. Both operators need this display to communicate about the situation and to build up their mental representations of the situation, which they need to interpret incoming sensor data and control the UAV respectively.



Sensor 1 PR-Sensor: ● Magnetometer: 100 MG ● Batteriestatus:

Sensor1
PR-Sensor: ●
Magnetometer: 100 MG ●
Qualifizierung: Fahrrad
Batteriestatus:
Sensor deaktivieren: Ja ○ Nein ●

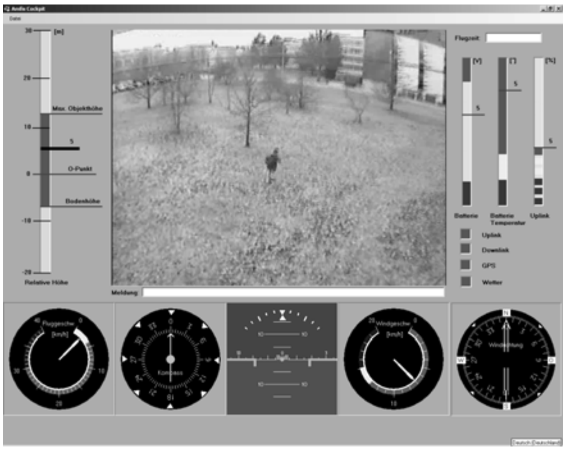
Sensor 2 PR-Sensor: ● Magnetometer: 100 MG ● Batteriestatus:
Sensor 3 PR-Sensor: ● Magnetometer: 100 MG ● Batteriestatus:
Sensor 4 PR-Sensor: ● Magnetometer: 100 MG ● Batteriestatus:
Sensor 5 PR-Sensor: ● Magnetometer: 100 MG ● Batteriestatus:
Sensor 6 PR-Sensor: ● Magnetometer: 100 MG ● Batteriestatus:
Sensor 7 PR-Sensor: ● Magnetometer: 100 MG ● Batteriestatus:
Sensor 8 PR-Sensor: ● Magnetometer: 100 MG ● Batteriestatus:

Einsatzleitzentrale neuer Auftrag Fr 12.01
Einsatzleitzentrale neuer Auftrag **Fr 12.01**
Einsatzleitzentrale Anforderung von Infos Fr 12.01

INFO --> Routineflug ab **12:30 bis 13:15**
Schorch_Ulrich-Einsatzleitzentrale@iitb.fhg.de
An: Peter_Nuhr-Auswerter@iitb.fhg.de

Fig 2: screenshot of the software for sensor data interpretation and coordination with control center

The actual prototype demonstrator is used for intrusion detection of a spacious outdoor area. In order to achieve this the external fence is equipped with mobile ad hoc networked sensor nodes carrying visual and movement detection sensors. Alarms from this sensor net are displayed at the ground station on the GIS based view in the middle. The sensor data operator uses different stationary video cameras and movement sensor detectors to determine what is happening. The UAV pilot plans a flight mission and brings video sensors to the required location. From there the UAV will then be following the intruder.



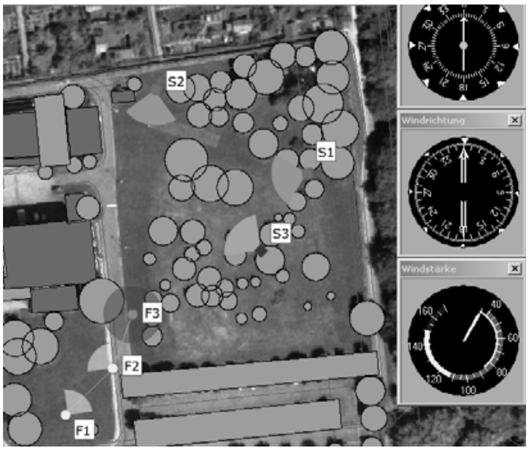


Fig 3: virtual cockpit for UAV control with display for on board video

Fig 4: clipping of a screenshot with the situation display software

System Implementation

The ground station is realized as a modular framework allowing for adaptation to different operational needs. Figure 5 illustrates the components of the system. The ground station has the function to integrate the data streams coming from a range of sensors. It is also used to control the different platforms. Data links (either wireless LAN or radio) connect sensor, sensor platform, and ground control station.

The underlying software architecture has a generic connector for interfacing the ground control station with the different sensor types and other streaming data sources. As a basis for visualization and data integration a GIS based landscape model is used.

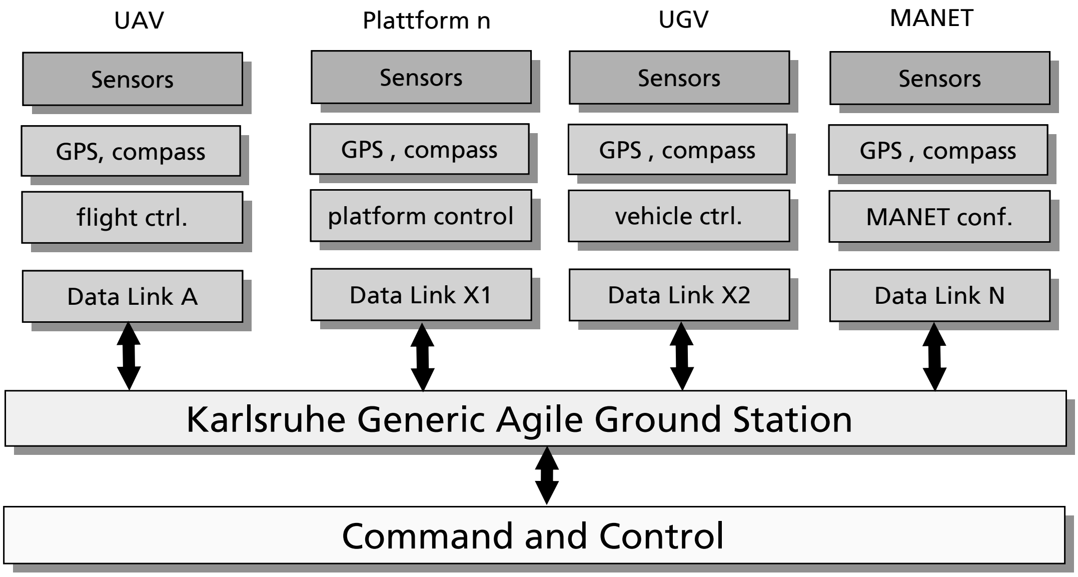


Fig 5: component oriented system implementation

The generic approach of this surveillance solution makes it possible to adapt it to the operational needs of different scenarios. We use the NATO Architectural Framework (NAF) to design a concrete system with the existing components. NAF distinguishes operational, systems, and technical aspects of a system. For each of these areas a number of descriptions have to be created.

One key aspect for the process of adapting the surveillance system with NAF is the system functionality description (NSV-4). For that purpose we create a task model of the mission as a business process model description with BPMN (business process modelling notation). This makes it possible to use standard business process simulation tools to simulate timings and to estimate the overall performance of the designed surveillance system in different situations.

Blast-Optimised Construction Component: Polymer concrete for energy absorption

Dr. Christoph Mayrhofer, Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, Germany Email: mayrhofer@emi.fraunhofer.de

Introduction

In many areas explosive attacks on buildings cannot be excluded. Common targets of terrorist actions are government buildings or banking and financial institutions. Chemical industry and nuclear power plants also have to consider a risk potential. The kind of loading in the event of an explosion is basically dependent on charge size and standoff. Figure 1 shows the extreme cases of contact and far field explosion. Deformation modes of walls and columns, which are similar to a horizontal static loading, occur in case of a larger distance. The impact loading can be supported with a reinforcement arrangement similar to a conventional bending design. This method is not applicable in the case of a contact detonation, because the load is concentrated and exhibits very high pressure amplitudes (up to several GPa). Shock waves are formed which may lead to spalling, scabbing and the formation of a punching shear cone. Even if loads are limited to a small area of a structure, the consequences can be considerable. The failure of loadbearing structural members reduces the stability of the global structure, for example of a high-rise building, and might lead to a »progressive collapse«. In order to protect these critical structural elements, the impacting shock waves have to be damped. To achieve this goal, an absorbing material, based on renewable primary products has been developed at the Fraunhofer-Institute for High-Speed Dynamics.

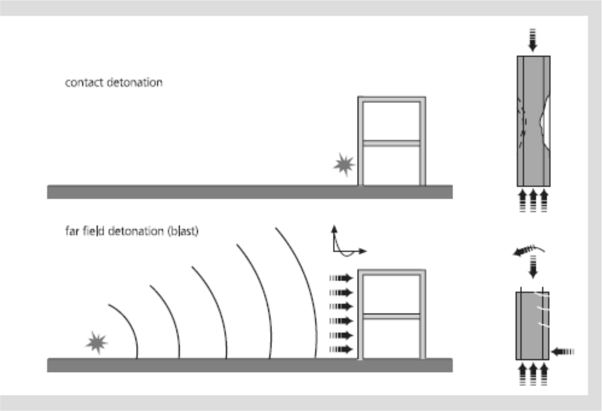


Figure 1: Difference between a contact detonation and a detonation in the far field.

Polymer concrete

Polymer concrete consists of filler materials and binder, supplemented by auxiliary materials or additives. The role of the filler is damping the arriving shock waves. Therefore materials have to be chosen which exhibit a high plastic deformation capability under high pressures. Porous materials with high pore volumes have these material properties. For the polymer concrete developed at EMI waste products from corn cobs are used as filler material. They show a very high pore volume. Besides the filler materials, reinforcements in the form of flax fibers are added. They increase the ductility and the plastic deformability, respectively. In the case of large deformations, as occurring during shock loading, fibers are pulled out of the matrix and energy is absorbed. An epoxy resin consisting of resin and hardener with high deformation capacity is used as an appropriate binder material. The constituent parts of the polymer concrete are shown in figure 2.

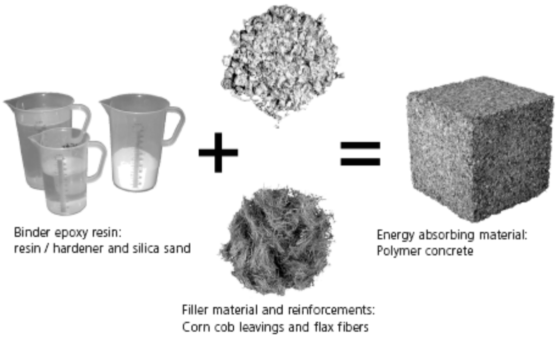

+
=
Binder epoxy resin:
resin / hardener and silica sand
Energy absorbing material:
Polymer concrete
Filler material and reinforcements:
Corn cob leavings and flax fibers

Figure 2: Constituent parts of the polymer concrete.

Properties under shock wave impact

For the damping of shock waves, the plastic volumetric deformation via compaction is of importance. Figure 3 show the behavior under dynamic loading, using an impactor. Thereby strain rates of 52 1/s have been achieved. Show is the large area below the curve, representing the absorbed energy. The maximum plastic compression of conventional concrete is reached at 0.2 while 0.7 are reached for polymer concrete.

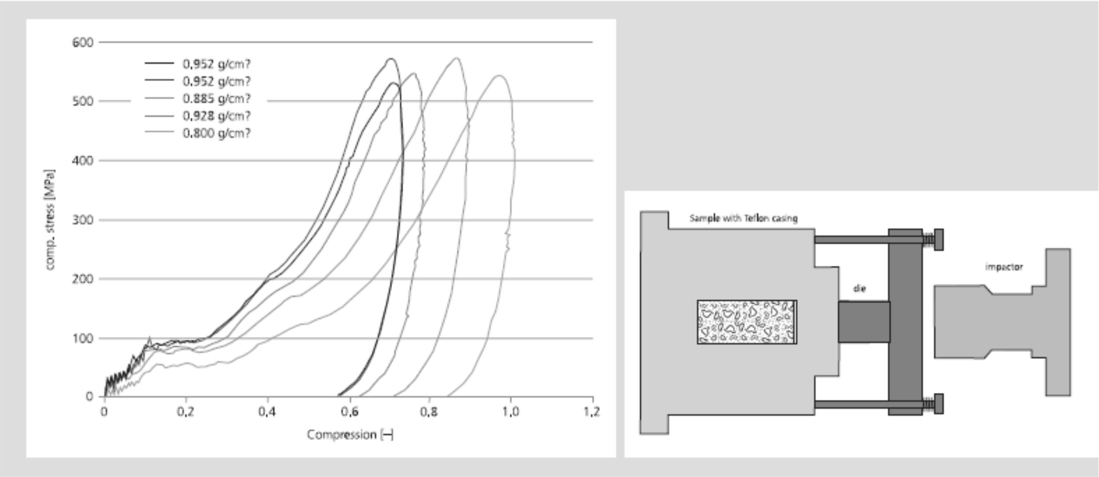


Figure 3: Dynamic compression of polymer concrete.

The compression rates, achieved by the impact tests are 3 to 4 decades below those of shock waves. In plate impact experiments the Hugoniot-properties, or compression behavior under shock loading, are measured. With plate impact experiments, the relationship between compression and stress up to several GPa can be derived. Comparing to the stresses in impact testing, the Hugoniot-stresses are higher at identical compressions. This points to a dependency of the compression curve on the loading velocity, which has to be considered in constitutive equations. Figure 4 shows the Hugoniot-properties and the polymer concrete sample in a planar-plate impact test.

Polymer concrete in application

The damping principle is shown figure 5. The maximum blast pressure p_0 is reduced to the stress σ_p by the damping layer in front of the reinforced concrete wall. Thus crack initiation and propagation is prevented. Especially for brittle materials like concrete, a high amplitude even with a small energy input leads to crack propagation and fragmentation.

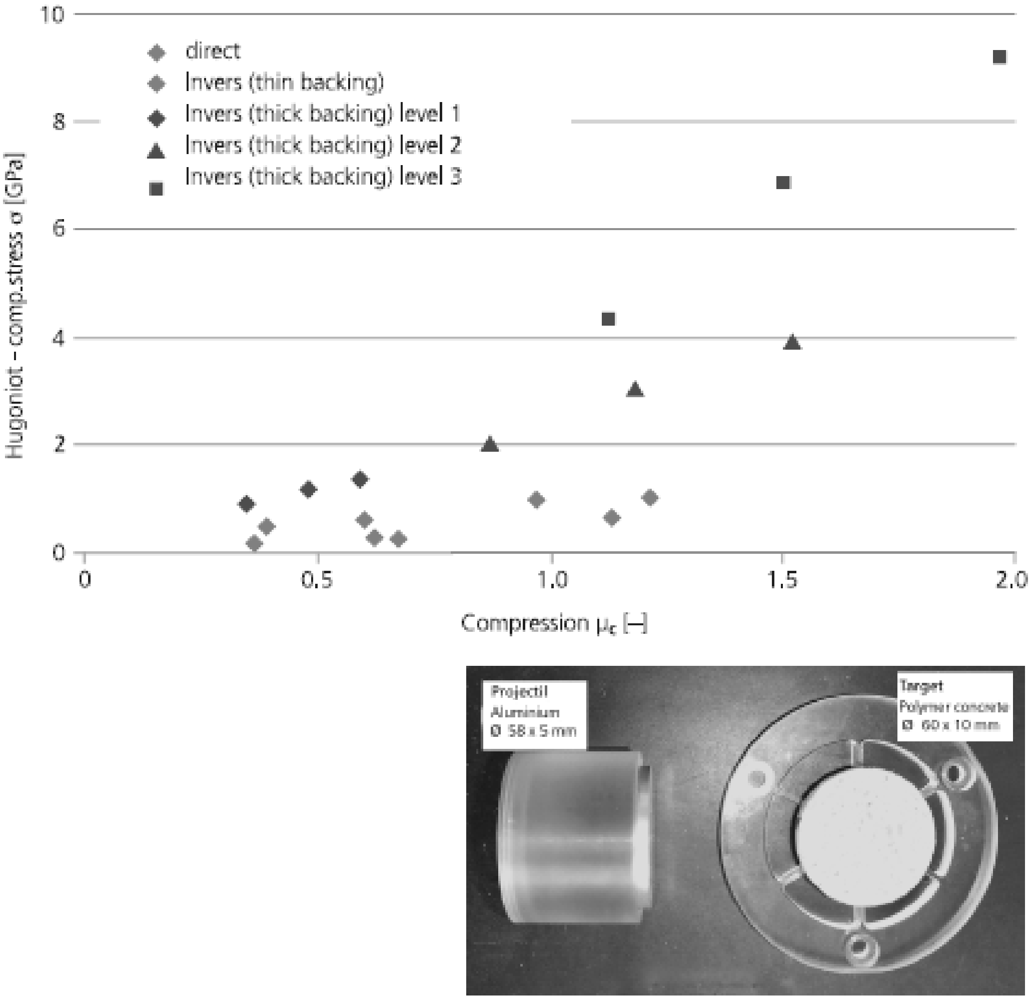


Figure 4: Results of planar-plate impact trials and used polymer concrete samples.

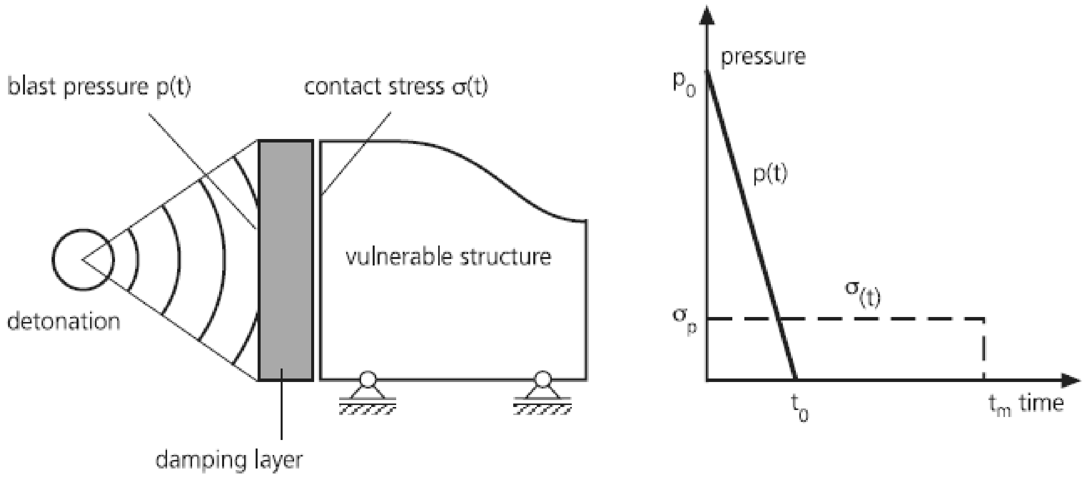


Figure 5: Principle of damping in case of detonation at close range.

The effectiveness of the damping layer becomes apparent if an unprotected and a protected plate with polymer concrete are viewed in comparison. The energy balance in the upper right figure shows the lower energy input into the concrete (5 instead of 8 kJ) in the case of an added damping layer. Figure 6 shows the protected plate with polymer concrete in scaled experiments 1:4.

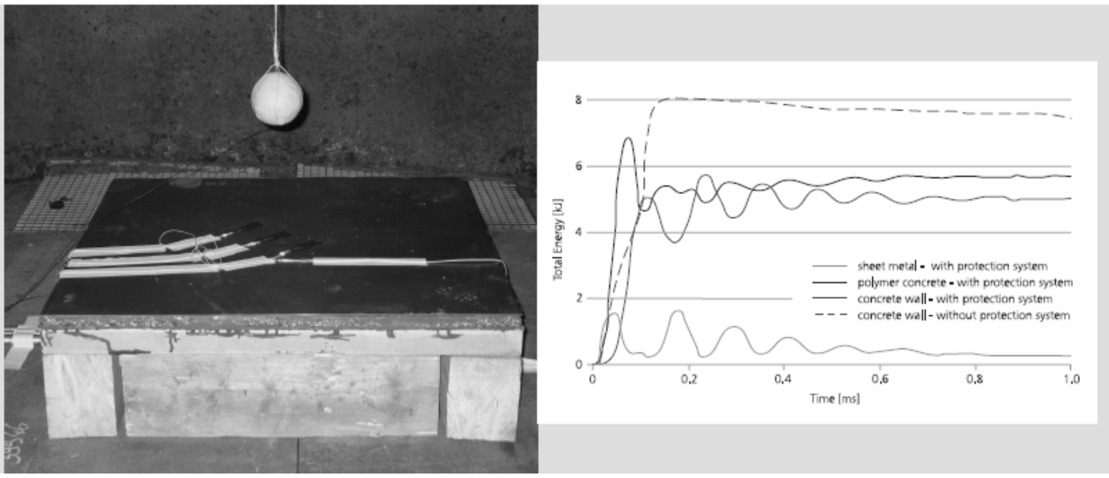


Figure 6: Left: Reinforced concrete plate protected by a damping layer out of polymer concrete - right: energy input into an unprotected plate (dotted) and a protected plate.

The consequences regarding the degree of damage are shown in figure 7. Due to the damping layer, no breaching occurs in the plate. In summary, the degree of damage of a wall or column can be reduced significantly by means of damping. With adequate design of the layer, the original load-bearing capacity is nearly preserved. Damping layers out of polymer concrete are flexibly adapted to the geometry and therefore suitable as a subsequent retrofitted protection measure.

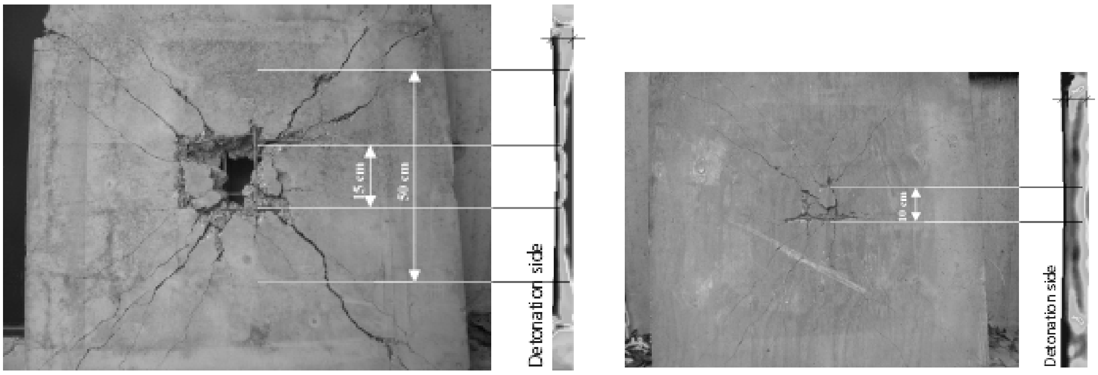


Figure 7: Damage level of unprotected (left) and protected (right) plate.

A Comparative Survey of Emergency Management in Australia, New Zealand and Europe – Findings on Information and Communication Technology Use

Andreas Meissner
Fraunhofer Institute for Information and Data Processing - IITB
Fraunhoferstrasse 1, 76131 Karlsruhe, Germany
andreas.meissner@iitb.fraunhofer.de

The 2006 EMANZE survey study looked into "Emergency Management in Australia, New Zealand, and Europe". In the regions covered, a large number of experts were interviewed and asked about organizational matters, the role of technology, and the handling of certain emergency scenarios. This short paper reports specifically on study findings related to the use of information and communication technology (ICT), which is, while still less widely deployed than in other industry sectors, often regarded as critical for the organizations' ability to cope with emergency events.

Introduction and Scope

"In the past ten years, technology has improved our ability to cope with emergencies." When representatives of emergency management organizations were confronted with this statement in the course of a recent international survey, a large majority indicated that they agreed or even strongly agreed that it did in fact apply to them. Advances in communication technology were among the most frequently mentioned technological breakthroughs. This short paper reports on selected ICT related results of the EMANZE survey research project, jointly carried out by Germany's Fraunhofer-Gesellschaft and National ICT Australia (NICTA) in 2006, covering Australia, New Zealand, two South Pacific islands, as well as Germany, Austria, Switzerland and the UK. In Australia, New Zealand, the Cook Islands, and Germany, both the national level and the state (or respective) government levels were covered, and additionally, selected regional and local organizations involved in emergency mitigation, preparedness, response and/or recovery were included in the form of personal interviews with senior representatives. Reflecting regional particularities, both metropolitan and remote areas were researched, including Aboriginal communities in Australia's Outback; moreover, non-government organizations such as the Royal Flying Doctor Service of Australia (RFDS) were asked for participation. In the other countries, interviews were carried out at the

National level only. For all 56 interviewees representing emergency management organizations, the same structured interview guide was applied, yielding a solid basis for a comparison. While EMANZE, in its entire setup, looked into “Emergency Management in Australia, New Zealand, and Europe” with a broader approach including organizational and management issues (Meissner 2006, 2007) apart from technology related questions, among the most tangible results are findings on ICT that is either already deployed or on the “wish list” of the organizations interviewed for the project. This subset is the focus of this paper.

Critical Infrastructure and ICT Use

The survey asked about critical infrastructure the organization relied upon for its own tasks in emergency response operations, both on a general basis and with particular regard to ICT. While the list of general infrastructure facilities referred obviously varied according to the specific role of the organizations, *communication networks* was a common answer. As fallback options applied in case of failure of the default communication path(s), *satellite phones* were frequently mentioned, with little distinction between countries and government levels. Asked more specifically about information and communication technology used at their headquarters and, separately, in the field, answers were more varied. In Australia, only four out of 26 interviewees, including the Federal Emergency Management Agency (EMA), identified specific IT systems applied as mobile solutions in the field, ranging from mere *email access* to a *web based information system* client. Australia, with its rather heterogeneous organizational structure observed in the emergency management sector of the seven states researched, has a potential for ICT deployment that, as also found in the study, is only now being addressed by the academic community, e.g. in the SAFE project (Robinson & Indulska 2006, Iannella 2005). In New Zealand, five out of eleven interviewees use some kind of mobile information technology, mainly a *web based information system* or an *incident management system*. There is, however, an issue with the interoperability of such systems between so-called CDEM (Civil Defence Emergency Management) Groups, i.e. the organizational layer just below New Zealand’s National CDEM Ministry (MCDEM). Such systems are not in use at all in the two South Pacific island countries, i.e. Cook Islands and Fiji, with the remarkable exception of the regional post of the United Nations’ Office for the Coordination of Humanitarian Affairs (OCHA), who use the UN’s *Virtual On-Site Operations Coordination Centre*. In Germany, the Länder are better equipped with mobile IT, as a majority of interviewees referred to either *vehicle based* or *“out-of-the-box” mobile data communication* equipment available for use in the field, e.g. Bavaria’s *Kommunikationskoffer*.

Demand for New Technology

Interviewees had a chance to disclose their “wish list” for ICT to be used at the headquarters and in the field, and, with a more long-term perspective, suggest a “homework” to academia that would, if completed successfully, make their job an easier one. As it turned out, all interviewees did not have a clear concept of what ICT is commercially already available (and thus a realistic entry for a short-term wish list) and what is still so remote that a long-term research effort is required. Thus, in this paper, the answers for both questions are combined; it should also be noted that homework suggestions unrelated to ICT were also given but are not generally mentioned here. For the purpose of supporting the work of frontline response organizations, “anytime-anywhere” communication systems are frequently mentioned especially in Australia, e.g. *a holistic communication system that works anytime anywhere* or *an online information sharing system to be used in the field, for live video, yielding an analysis of what is going on in the field*, whereas in Fiji and the Cook Islands, wish list items are more basic, such as *easier-to-use satellite phones*, *Inmarsat based data communication*, or *better international roaming capabilities* for GSM phones. Another technology challenge frequently mentioned in this context in all countries researched is a *better system for warning the public of imminent danger*. Several interviewees expressed concern that increased use of ICT may result in information overload, and it was suggested that academia do research into *how people deal and cope with information overload, having a natural tendency to deviate from the big picture to small details if exposed to too much information*.

Relevance of Technology Advances

As mentioned earlier, a further technology related EMANZE question asked interviewees to comment on the statement: *“In the past ten years, technology has improved our ability to cope with emergencies.”* All but seven (out of 56) indicated that they *agreed* or *strongly agreed* (on a 5-point scale also allowing for *neutral*, *disagree* or *strongly disagree* as answers). All but a handful of interviewees mentioned some kind of communication technology as a “breakthrough” that helped them get their job done in a better way, and more specifically, *mobile and satellite phone technology* was a frequently given answer. *Remote sensing*, or *access to remotely sensed data*, was often mentioned. While, in an overall assessment, the benefits of technology were acknowledged by most interviewees, it should be noted that, particularly in states and countries with coastal areas in the Oceania region, a Tsunami warning system, including a solution for the “last mile” to the public, is an unresolved issue. Several approaches were mentioned, however, interestingly, the director of Fiji's National Disaster Management Organization (NDMO) still suggested that *traditional warning systems* such as the interpretation of unusual animal behaviour should not be neglected over a belief in the accomplishments of technology.

Conclusion and Outlook

This paper reported on ICT related findings of the EMANZE project on Emergency Management in Australia, New Zealand and Europe. While there is still a tremendous potential for the introduction of enhanced ICT, it has become evident that ICT, in particular: communication networks, are, in many cases, already critical to the success of emergency response operations. Further analysis of the 2006 data is ongoing, and it is planned to conduct additional interviews in order to investigate lessons learned from more recent disasters in the region.

References

Emergency Management Agency of Australia, EMA, www.ema.gov.au

Iannella, Renato (2005). “Incident Notification: Requirements and Frameworks. Recent advances in counter-terrorism technology and infrastructure protection.” Proc. 2005 Science, Engineering and Technology Summit, Canberra, Australia, 12-14 July 2005.

Meissner, Andreas (2006). "Emergency Management and Security Research in Australia, New Zealand and the South Pacific: Survey and Comparison to Europe”, in: Recent advances in security technology, Proc. 2006 RNSA Security Technology Conference, Canberra / Australia, 21-23 Sept 2006, published by Australian Homeland Security Research Centre, pp 372-381, ISBN 0-9757873-4-9

Meissner, Andreas (2007). "Emergency Management in Australia, New Zealand and Europe - The 2006 EMANZE Survey", Proc. IEEE Int'l Conference on Intelligence and Security Informatics 2007 (ISI 2007), May 23-24, 2007, New Brunswick NJ, USA, ISBN 1-4244-1329-X

Robinson, Ricky, and Indulska, Jadwiga (2006). “Adaptive and resilient systems for emergency response”, in: Recent advances in security technology, Proc. 2006 RNSA Security Technology Conference, Canberra / Australia, 21-23 Sept 2006, published by Australian Homeland Security Research Centre, 2006, pp 423-430, ISBN 0-9757873-4-9

Ministry of Civil Defence and Emergency Management of New Zealand, MCDEM, www.civildefence.govt.nz

Detection Features of the Chemically Active Gas Impurities in the Atmosphere by Semiconductor Chemical Sensors

Obvintseva, L., Belikov I.B., Avetisov A.K., Chibirova, F.Kh. Elansky N.F., (Karpov Institute of Physical Chemistry), Russia

Abstract

The problems and the aspects of semiconductor chemical sensor use for active atmospheric chemical impurity measurements are discussed. The main features of detecting of small (maximum permissible) concentration of O_3, $C1_2$, ClO_2, HCl in the air are considered.

Gas analyzers based upon semiconductor chemical sensors (SCS) are perspective devises for gas analysis different fields. Its action is based on conductivity change of the semiconductor sensitivity layer when ambient air composition is changed. Sensitivity of semiconductor sensors allows to apply them for measurement of a wide range of impurities concentrations, from those that are lower than the maximum permissible concentration (m.p.c.) and up to high concentrations under the conditions of emergency outbursts. The advantages of semiconductor sensor also include its small size and high performance at a low cost.

Sensor is represented isolating substrates the size of 1.5 x 1.5 mm^2. On one of substrate sites there is a Pt- heater covered with SiO_2 layer, on the other there are meander Pt- measuring electrodes. Sensitivity layers as think films of ZnO, In_2O_3 or In_2O_3:Fe_2O_3(3%) were prepared. Sensor is in the teflon cell.

The enhanced model of the gas analyzer based on chemical sensors is elaborated. This model is purposed for measurements of gas impurities under the field working conditions as well as in laboratories. According to laboratory researches sensor sensitivities towards investigated gases are the follows: O_3>ClO_2>$C1_2$>HC1 [1-3]. The results of surface atmospheric ozone measurements obtained both by semiconductor sensor and with DASIBI 1008 optical gas analyzer are presented on the fig. It is revealed that the semiconductor sensor measured daily variations of ozone in the atmosphere synchronously with the DASIBI 1008, but with higher sensitivity (< 1 ppb) and faster operation (< 1 s). As a result of these measurements it is concluded that semiconductor sensors would provide a good opportunity for both ozone monitoring during long periods and small and fast ozone pulsation measurements in the atmosphere.

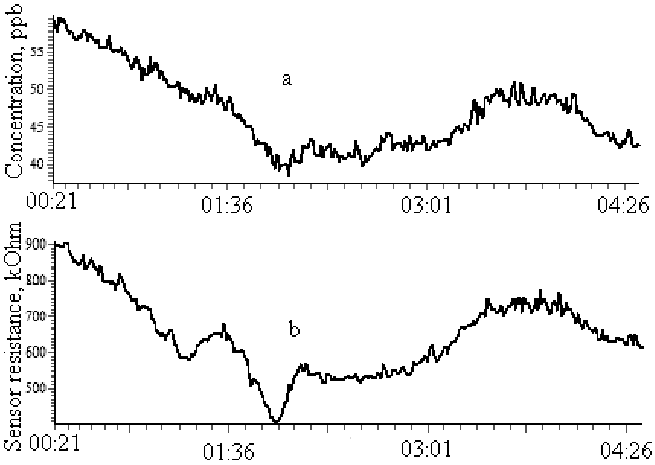


Fig. Measurement of ozone concentration during 4 h. Average time is 1 min. a) ozone concentration (ppb) for DASIBI; b) data from semiconductor ozonemeter (kOhm). Tsimlyansk scientific station of Obukhov Institute of Atmospheric Physics, Russian Academy of Sciences August, 12, 2006.

Gas analyzers based upon semiconductor sensor can work both in an autonomic mode and as a part of multifunctional instrumental complexes. This device may be used not only for stationary stations of atmosphere control, but also for measurements at distant territories and on the moving platforms.

This work was supported by International Science & Technology Center (ISTC) – project no. 3288.

References

1. Obvintseva L.A., Gubanova D.P. “Determination of Chlorine and Chlorine Dioxide in Air with Semiconductor Sensors”. *Russian Journal of Analitical Chemistry* 2004. vol. 59. no. 8. p. 871.

2. Obvintseva L.A., Oksengoit–Gruzman E.A., Kuchaev V.L., Avetisov A.K., Chibirova F.Kh., Dmitrieva M.P. “Specific Features of Hydrogen Chloride Detection in Air with Semiconductor Sensors”. *Russian Journal of Analitical Chemistry* . 2008. vol. 63. in press.

3. Obvintseva L.A., Chibirova F.Kh., Avetisov A.K., Elansky N.F., Skorokhod A.I., Shumsky R.A. “Capability of the Semiconductor Ozonometer in Monitoring Ozone in the Atmosphere”. *Atmosoheric and Oceanic Optic*. 2005. 18. no. 11. p.1007.

Information Fusion Concepts in Anti Asymmetric Warfare

Felix Opitz, Josef Filusch, Defence and Communications Systems,
EADS Deutschland GmbH,
felix.opitz@eads.com, josef.filusch@eads.com

Abstract:

The asymmetric adversary poses a serious threat to civil and military facilities. Hence, the defence against such adversaries, the so-called anti asymmetric warfare, is of interest in various environments: air traffic control, air defence, force protection in out of area missions, harbour protection, coastal surveillance, or the security of naval platforms operating in critical environments, like littoral. A vital factor in anti asymmetric factor is to ensure information superiority and intervention capability. This is addressed by information fusion and visualisation.

What is Anti Asymmetric Warfare?

The classical situation of symmetric conflicts is determined by uniformed forces. The utilisation of weapons is assumed to comply with international treaties and conventions and with national laws. All targets one has to fight are assumed to comply with the principles of the laws of armed conflict, which implies requirements for any legal response, e.g.: military necessity, discrimination between civil environment and aggressor, proportionality of response, and minimization of unnecessary suffering. The tactics are based on military superiority, e.g. high quantity of own entities, mobility, and efficiency of weapon systems.

The asymmetric scenario is different to the classical battlefield, e.g. in the following aspects: Here, the objective of an adversary is to create instability using irregular forces. These may include prohibited weapons, improvised devices, the use of civilian facilities and equipment as weapons, or the use of legitimate weapons in an unlawful way. Civilian and protected targets (both inside the conflict area and elsewhere) may be attacked by the adversary if such actions serve his objectives. The asymmetric adversary may utilise low cost platform and weapons: micro light planes, hang gliders, airliners, divers, mines, UAVs, UUVs, dinghies, car bombs, bazookas, grenades, artillery fire or snipers. The asymmetric scenario is guided by the willingness to use to advantage irregular forces and unconventional weapons.

Solutions for Anti Asymmetric Warfare

For legal defence against asymmetric threats information superiority is a vital factor: In general one has to observe complicated situation with numerous involved civil or military entities over a long duration. Only by detection of critical situation at an early stage, one is able to reobtain the own escalation dominance and to fight off such threats by legal response.

Applications may be found in the civil and military area, like

- Air defence systems,
- Air traffic control,
- Force protection in out of area missions,
- Urban surveillance,
- Border control,
- Protection of assets and events,
- Combat management systems for naval ships, and
- Coastal surveillance.

The answer to these threat scenarios is different. Both, operational concepts and technical solutions have to interlock.

Technical solutions address the issues of information superiority and intervention capability by realising situation awareness and decision support even in situations where the operator is under stress.

Information Sources

The information about symmetric as well as asymmetric targets is collected by sensor systems or by other internal and external sources. These may be sensors like primary radar, passive radar, over-the-horizon radar (OTH), secondary radar (IFF), synthetic aperture radar (SAR), automatic identification system (AIS), electro optical sensors (EO), electronic support measures (ESM), acoustic sensors, seismic sensors, and chemical sensors.

Often it is only a sensor suite which is able to satisfy the requirement with respect information demand, i.e. detection, accuracy, coverage, classification, diversity, etc. Further, the sensor suite has to take into account various operational restriction and climatic conditions.

Tracking

The requirements for target tracking in the anti asymmetric warfare are similar to those of the known symmetric world.

Here one has to be able to track dense scenarios consisting of numerous participating objects. Asymmetric aggressors may use geographic constraints and civil shields to their own advantage. Further, anti asymmetric warfare has to deal with threats launched from the nearest neighbourhood. Hence short reaction times has to be considered. And one has to cover the wide spectrum of possible platforms and weapons usable for asymmetric threats. However, this means that the tracking algorithms which are applied in the symmetric warfare, are also required by the asymmetric one.

Classification and Automatic Target Recognition

A more detailed automatic classification of asymmetric platforms is required due to the possible large and different object spectrum to ensure an optimal effector choice against asymmetric threats.

Because it is not always possible to keep objects off distance, this often has to be done in scenarios consisting of multiple object. Advanced recognition techniques may help to distinguish between adversaries and objects abused as civil shield. Therefore automatic target recognition based on TV, IR or SAR image recognition methods is a benefit and can decrease the load of the operator and increase the situation awareness. Very applicable for surveillance applications within anti asymmetric warfare is also the automatic detection of people.

Hence the classification capability is a technical functionality addressing the requirements of a legal response, like proportionality and discrimination.

Identification

Identification in anti asymmetric warfare has to ensure to distinguish between civil parties and the adversaries. This seems to be a bigger challenge as in the symmetric situation. Often the knowledge of the platform type doesn’t contribute to the identity of the platform. Question and answer systems (IFF) are often not applicable and other identity sources usable in symmetric warfare are also not suitable.

Often the asymmetric adversary is identified by an assessment of the ongoing situation or by the prediction of this situation into the future. It is the interaction between objects, which characterises the object under observation as a potential origin for an asymmetric threat. One has to take into account the own possibilities for countermeasures, like warning or the usage of non-lethal and lethal weapon systems bearing in mind the constraint of legal response. Hence, there is an interlock between the identification, and situation and threat assessment.

However, there is no unique realisation, which automatically covers all aspects of situation and threat assessment. Hence, new techniques have been developed, like traffic flow evaluation or behaviour analysis.

Sensor Management

Another aspect of anti asymmetric warfare is the sensor management. An example specific for anti asymmetric warfare is the data acquisition with various sensor types and data processing techniques.

Visualisation

Very important for anti asymmetric warfare is the optimisation of the human machine interface and cognitive refinement, such that operator interaction is supported in an optimal way.

Asymmetric threats may happen during peace keeping operations, where the attention of the operator is decreased through long term missions. The asymmetric threat may happen spontaneously and may occur in a civil environment. Therefore, it is important to focus and also defocus the attention of the operator, especially in multi target scenarios.

Also the decision of an operator concerning effector usage may lead to consequences for the civil population, e.g. collateral damage has to be taken into account. Hence, it is difficult for the operator to predict all the consequences of his decisions. Here decision support tools are believed to be helpful.

Further anti asymmetric warfare is characterised through the uncertainty of identification resulting from the normal uncertainty of the intention prediction. One has to find methods to symbolise this uncertainty to the operator, so that the operator is able to interpret the fusion results in an adequate manner.

Asymmetric threats may be executed in an confusing or unclear environment, like the urban or littoral. Special display techniques are required to visualise the operator these environmental constraints.

Also use of automatic recording, including the decision process and other relevant data may lead to juristic applicability of the process output.

Threat detection and imaging

Kurt Osterloh, Uwe Zscherpel, Uwe Ewert

Bundesanstalt für Materialforschung und –prüfung (BAM), 12205 Berlin, Germany

Abstract:

Clandestine threats are frequently recognised by image generating technologies such as radiography allowing an insight into a suspect object without opening or even touching it. Those images are supposed to show detailed features sufficient to guide rendering safe procedures, i.e., they have to visualise existing risks. This is rarely achieved by simply displaying raw detector signals on a screen since the capability to recognise relevant details may be impeded by noise or by contrast ranges exceeding human perceptibility. Some features only become visible after adequate adjustments and image processing. Tuning the pertaining parameters by hand and under stress (IED) can often consume valuable time and may lead to less optimal or even biased results.

This contribution provides an overview how to bridge the gap between the image detector signals and a perceivable presentation ensuring that any existing relevant detail has a chance to be visualised properly. For this purpose, digital image processing and stereo techniques provide a large toolbox from brightness and contrast adjustment to sophisticated methods such as edge enhancements and spatial presentation meeting the physiological requirements of the human vision.

Introduction

The kinds of threats to be detected before harming are improvised explosive devices (IEDs) in the first place, but also encompass any other subject assembled with malicious intention, e.g. to distribute noxious substances and the like. An inspection of the interior of a suspect item is required to determine if it may entail a threat, and if so, how it could be rendered safe. Therefore, as an essential first step, an insight is achieved by radiological methods, in general by X-ray. Due to unforeseeable risks the specimen to be interrogated should not be moved, nor even touched, so portable equipment is required such as the portable X-ray flash generator shown in Figure 1. The classical X-ray film to obtaining an image is replaced by digital technologies using either phosphor imaging plates (computed radiography) or flat panel detectors (digital detector arrays) converting radiation directly into an electronic signal. In the course of threat detection, it is important to achieve fast and reliable results for immediate decisions. This excludes trying various image processing procedures one after the other that might even involve tedious parameter adjustments by hand. The subject of this contribution is the appropriate conversion of the received signals into visible and perceivable images while minimising operator interactions due to the situational stress.

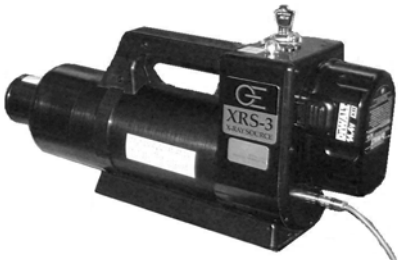


Figure 1: Portable X-ray source: flash generator by Golden Engineering

Imaging: displaying relevant information

The conversion of the signals from the digital imaging device rarely results in an perceptible image. The most obvious reason are the dynamics of the digital systems as compared to the physiological capability of the human vision. Technically, the images come with at least with 12 bit grey scale resolution in a picture element (pixel), today even with 14 or 16 bit. This converts into 4096, 16384 or 65536 intensity values per pixel while the human eye is capable to differentiate between some 60 or 80 grey levels in one view (equivalent to 6 - 7 bit). As a consequence, a digital image entails much more information than viewable, and a selection of the ranges of interest has to be made, i.e., the image has to be processed. Some pivotal steps are shown in Table 1. The specimen interrogated can be seen in Figure 2, it is an “improvised” laboratory sample. It demonstrates items that could occur, in one or the other form, in an IED.

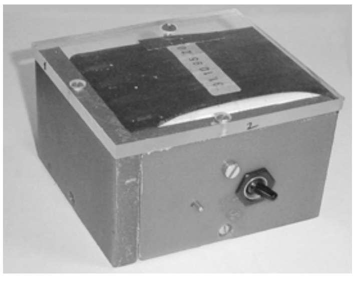


Figure 2: laboratory sample resembling something like an “IED”, but without any functionality

A radiograph of the sample shown in Figure 2 has been taken with the portable X-ray flash generator (5 flashes) of in Figure 1 and a phoshpor imaging plate (Fuji ST-V_N, reading device: Lumisys ACR 2000) from a very close distance (25 cm).

Table 1: From the raw image data to comprehensible images

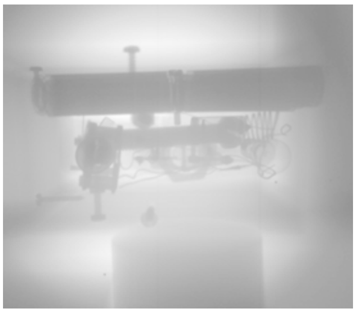
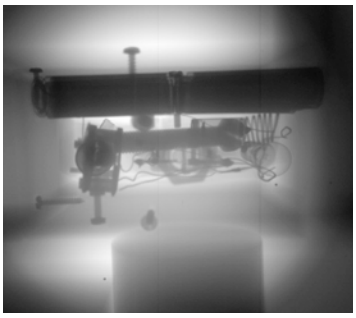
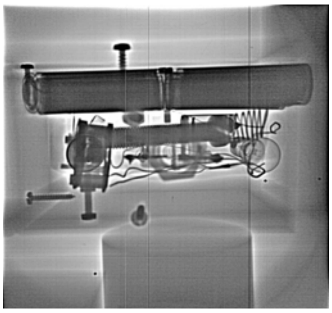
Raw image	First adaptation	Processed image
whole digital range of the detector signal (focus-detector distance: 25 cm), positive presentation	brightness and contrast adjusted (minimum and maximum grey values)	advanced band pass filtering with automatic noise recognition
		

Table 1 pricipally demonstrates two essential steps in viewing the digital information as it may come with a 12 bit depth in the left column. It is obviously faint because the whole dynamic range of 4096 grey values is transferred to an 8 bit range encompassing 256 levels as in most displaying devices such a monitors etc. This even exceeds the capability of human perception (s.a.). As a first step in selecting the information of interest, only the true range of grey values from minimum to maximum is transformed into the 8 bit viewing scale. While showing up more details, another limiting effect becomes obvious: the specimen contains items of high and low densities with wires inbetween, and the image shows a shading with a bright centre and a lesser exposed margin. This is due to the narrow cone beam of the close distance between the source and the object (chosen purposely to demonstrate this kind of problem).

In the course of rendering safe, material densities are of minor interest as compared to connecting leads between the parts such as cables and wires (eventually suitable to interrupt). These structures should be seen as a whole, regardless if they are running through dense or light zones of the object. Appropriate methods to achieve adequate visibility could be edge enhancement procedures (Laplace kernel or embossed presentation) or high pass filtering. The latter one has been chosen to be adequate in most cases, however, this method also enhances any existing noise, blotches of dirt and scratches on the image media. Though not all artefacts can be removed swiftly, there is at least a chance to reduce the noise that hampers detecting fine structures within the image, particularly in low dosed exposures. In such cases, the noise is distributed equally over the whole image plane so it may be regarded as a feature common to any part of the resulting picture. However, the degree of noise is a parameter hard to determine, particularly under situational stress as it is the case in rendering safe measures. In order to ease the imaging procedure in the course of threat detection, an algorithm has been developed to detect automatically the degree of the inherent noise in each individual image and to define an appropriate filter for compensation. The result of such a procedure is shown in the third column of Table 1 – just a mouse-click away from the original raw image.

Conclusion

Among numeous existing possibilities to process a digital image, two consecutive essential steps have been demonstrated with an “improvised” laboratory sample. First of all, the kind of information required has to be defined, i.e. fine structures representing connecting leads between the parts rather than differences in densities. Then, the two subsequent measures in image processing demonstrated here should reveal any of the relevant information entailed in a radiographic image in almost all cases as shown above, i.e. brightness and contrast adjustment first followed by a powerful filtering method. Finally, it has to be taken into account that field conditions are profoundly different to those in a laboratory. Any operator has neither the time nor the temper to try many possibities in image processing with tedious parameter adjustments – a result is needed almost immediately, ideally with just a mouse click.

A final remark should be allowed that processing digital radiographic images requires specialised programs capable to handle both, the dynamic of 16 bit grey values and large, uncompressed image formats in difference to those obtained with a digital photo camera. Therefore, most photo processing programs are not suitable for this purpose. The program BAM provides for such applications (“ISee!”) can be found at: http://www.kb.bam.de/~alex/ic.html.

PCs Vulnerability Assessment

Libor Palisek, Jiri Kusala
VOP-026 Sternberk, s.p., division VTUPV Vyskov,
V. Nejedleho 691, 682 03 Vyskov, Czech Republic, l.palisek@vtupv.cz

Abstract

Assessment of electromagnetic threats such as NEMP (Nuclear Electromagnetic Pulse), UWB (Ultra Wide Bandwidth) and HPM (High Power Microwave) to personal computers (PCs) is considered in this paper. Possible and suitable ways for PCs vulnerability verification are recommended. Some practical results achieved during relevant experiments related to PCs vulnerability are provided in this study. Conclusion with recommendations for possible PCs protections countermeasures is done at the end of presented study.

1 Introduction

It is well known electronics equipments are sensitive to electromagnetic irradiation. Personal computers (PCs) are one of the most sensitive equipments. The criticality of it's reliable function is very important when PCs are used in the infrastructures. There are a lot of possible electromagnetic threats to them such as NEMP (Nuclear Electromagnetic Pulse), UWB (Ultra Wide Bandwidth) and HPM (High Power Microwave).

The aim of this study is to present the area of electromagnetic threat to PCs according to known possibilities for intentional electromagnetic field generation.

This investigation is a part of study of project "PCs protection against real electromagnetic threat - ELEKTROOCHRAN" (CEP: OPVTUPV200601) supported by Ministry of Defence, Czech Republic

2 Electromagnetic Threats Assessment

Non-lethal weapons on various principles are more and more attractive during past years. An important group of these technologies is represented by weapons which use power electromagnetic field destructive effects. These weapons are mainly used for electronic equipments function disturbance or damage.

Next electromagnetic environments are considered according to electronic equipment threat:

- NEMP – Nuclear Electromagnetic Pulse, (EMP - Electromagnetic Pulse or HEMP - High Altitude Electromagnetic Pulse): pulse with rice time typically several nanoseconds and with duration typically from 10's up to 100's nanoseconds, electromagnetic strength at the place of target 10's kV/m, electromagnetic strength 50 kV/m is considered according to valid EMC standards (electromagnetic strength is relatively uniform over distances of 1 000 km), there are a lot of standards including NEMP environment like MIL-STD-461E (military standard), EN 61000-2-9 (civilian standard) and many others.
- HPM: High Power Microwave, narrowband signals in frequency range 100's MHz up to several GHz, electromagnetic strength at the place of target typically up to 10's kV/m (strong dependence on range).
- UWB: Ultra Wide Bandwidth, pulses with rice time typically 100's picoseconds and with duration several nanoseconds, electromagnetic strength at the place of target typically up to 10's kV/m (strong dependence on range). HPM and UWB technologies are often used as directed due to its frequency range so these technologies are called Direct Energy Weapons (DEW).

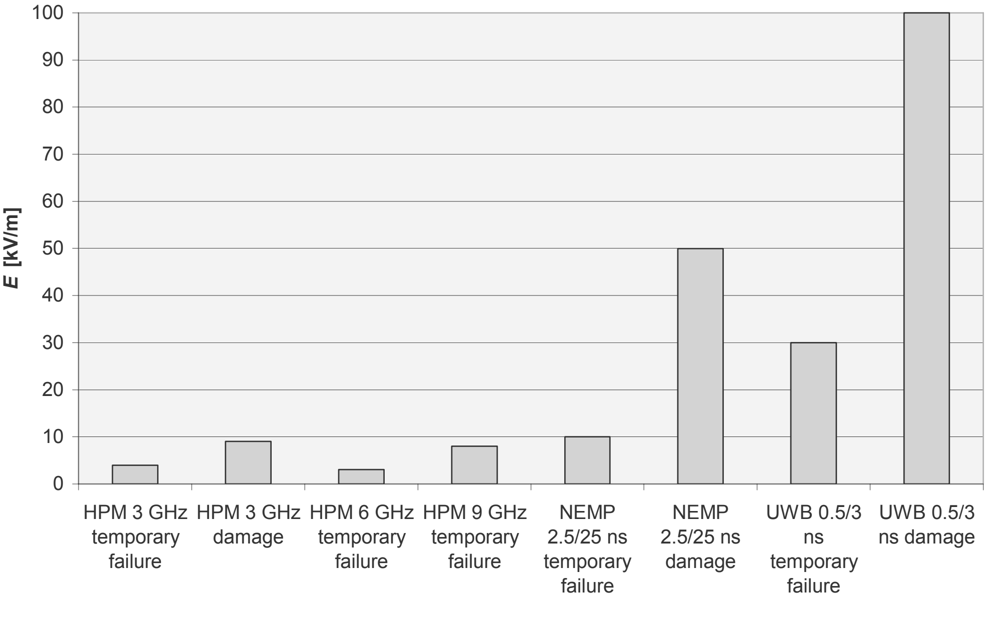
Because HPM and UWB environment is strongly dependent on range and moreover these environments may have a wide variety of waveshapes, their standardization is much more difficult than standardization of NEMP environment. Now there are only few standards which describes HPM and UWB environment generally (for example IEC 61000-2-13). Possible approach is to consider various types of HPM and UWB environments that have been produced and consider their possible use in the future against sensitive targets (PCs). It is always necessary to make relevant analysis of electromagnetic threat where very important parameter is the shortest possible distance from HPM or UWB source.

3 PCs Vulnerability Verification

For electromagnetic vulnerability it is necessary first of all to make analysis where electromagnetic threat assessment is done (see previous chapter). Moreover it is necessary to consider criticality of relevant system. Finally testing plan and testing can be done. For the testing it is usually the best way to start with transfer function measurements (shielding effectiveness measurement, induced currents and voltages measurement) which is possible to carry out in wide frequency range up to few GHz or higher. After that it is necessary to choose possible critical frequencies according to transfer function measurements and according to analysis. Chosen frequencies can be used for final high power electromagnetic field measurement with HPM, UWB and NEMP simulator use. Possibilities of these simulators are restricted to parameters which can not be changed or changing these parameters is too much time consuming so it is necessary to choose suitable parameters according to analysis and transfer function measurement results for this testing.

4 Practical Results

A lot of experiments related to PCs vulnerability are planned for year 2007 in project Elektroochran. First of all PCs immunity to radiated continuous wave signals were tested in frequency range 80 MHz - 7 GHz for setups with USB or PS/2 keyboards and mice with more kind of computers. Regular keyboards and mice were used as well as wireless technology. After that transfer function measurements will be carried out (shielding effectiveness of the case, induced currents in data and power cable). Finally high power electromagnetic testing will be done. As an example we can present some results from previous testing with HPM, UWB and NEMP effects on computer P75 (see Picture 1). From this picture it is obvious real electromagnetic threat 10’s kV/m for HPM, UWB and NEMP can cause not only temporary failures but PCs damage too.



Picture 1 HPM, UWB and NEMP effects comparison

5 Conclusions

Electromagnetic threat to PCs is real and considered high power electromagnetic fields can cause temporary failures as well as equipment damages. So it is necessary to consider this threat for crucial systems where sensitive electronics like PCs are used. In case the result of analysis with relevant necessary testing is: "crucial system immunity is not good enough", it is necessary to find out suitable countermeasures (protections) like keeping minimal distance from potential electromagnetic wave source. Other way is to place sensitive equipments to shielded rooms or shielded boxes or to use equipments or parts with higher electromagnetic immunity. Other possibility of hardening can be protection device installation (overvoltage protectors, filters), using optical cables where ever it is possible instead of metal ones. Redundancy can be useful too. Suitable solution is to realize the most important functions by other way (e.g. manually etc.).

6 References

[1] AEP-41, Unified Electromagnetic Environmental Effects (UE 3) Protection, Philosophy, and Methodology, 1. 2. 2004

[2] CLAYBORNE D. TAYLOR, D. V. GIRI High-Power Microwave Systems and Effects, Taylor and Francis, Washington, 1994

[3] IEC 61000-2-13, First edition, 2005-03, Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic (HPEM) environments – Radiated and conducted

[4] MIL-STD-461E, Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, 20 August 1999 (vojenský EMC standard)

[5] MIL-STD-464, Electromagnetic Environmental Effects, Requirements for systems, 18.3.1997, (vojenský EMC standard)

[6] ROBERT J. BARKER, EDL SCHAMILOGLU High-Power Microwave Sources and Technologies, IEEE Press Series on RF and Microwave Technology, New York, 2001

Simulation of HPM Threat to PCs

Libor Palisek, Lubos Suchy
VOP-026 Sternberk, s.p., division VTUPV Vyskov,
V. Nejedleho 691, 682 03 Vyskov, Czech Republic, l.palisek@vtupv.cz

Abstract

First of all electromagnetic threat to PCs according to known possibilities for intentional electromagnetic field generation is considered. Consideration is focused on HPM area in this study. HPM threat is simulated with FDTD software use and achieved calculated results comparison with results from measurement is provided. Results related to critical frequencies assessment is presented too.

1 Introduction

Personal computers (PCs) are one of the most sensitive equipments to electromagnetic irradiation. The criticality of it's reliable function is very important when PCs reliability can have significant influence on mission performance. When PCs are used in the infrastructures it is very important to consider it's vulnerability. There are a lot of possible electromagnetic threats to PCs such as NEMP (Nuclear Electromagnetic Pulse), UWB (Ultra Wide Bandwidth) and HPM (High Power Microwave).

The aim of this study is to present HPM threat to PCs simulation and to compare results achieved with simulation use with results from measurements.

This investigation is a part of study of project "PCs protection against real electromagnetic threat - ELEKTROOCHRAN" (CEP: OPVTUPV200601) supported by Ministry of Defence, Czech Republic.

2 Electromagnetic Threats

There are quite a lot of high power electromagnetic threats to PCs such as mainly LEMP (Lightning Electromagnetic Pulse), NEMP, HPM and UWB. Our consideration is focused on HPM area. These signals are narrowband signals in frequency range 100’s MHz up to several GHz, electromagnetic strength at the place of target is typically up to 10’s kV/m and there is strong dependence on range (see (1)).

$$E = \frac{\sqrt{30.P.D}}{r} \qquad (1)$$

where *E* is electromagnetic strength,
P is radiated power,
D is antenna directivity,
r is distance from antenna.

Because HPM environment is strongly dependent on range and moreover this environment is expected in wide frequency range and can have variety of waveshapes, it's standardization is much more difficult than standardization of NEMP or LEMP environment for example. Now there are only few standards which describes HPM environment generally (for example IEC 61000-2-13).

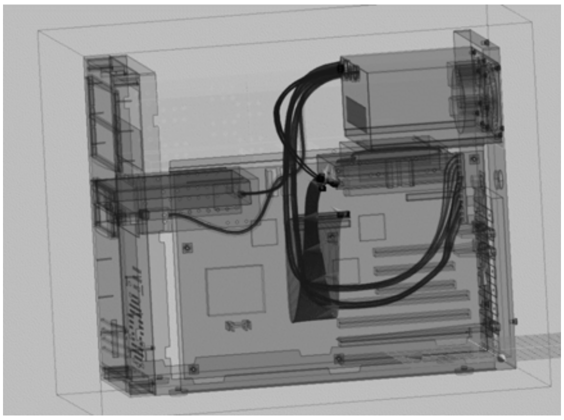
Possible approach is to consider various types of HPM environments that have been produced and consider their possible use in the future against sensitive targets like PCs. It is always necessary to make relevant analysis of electromagnetic threat where very important parameter is the shortest possible distance from HPM.

3 HPM Threat Simulation

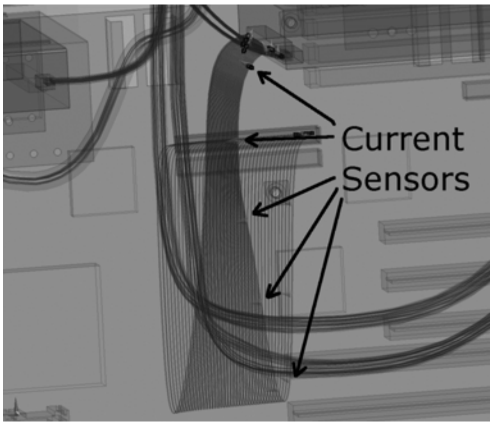
For HPM threat simulation detailed model was used (see picture 1). All details of metal box and barriers as well as studied cables were included. The model was imported to software SEMCAD X where FDTD (Finite Difference Time Domain) method is used. The wire number 1 of IDE cable was chosen for this investigation. 9 current sensors were equidistantly defined around wire 1 of IDE cable (see picture 2). Parameters of incident electromagnetic field were: CW (Continuous Wave), frequencies 250 MHz, 450 MHz and 1 GHz, electromagnetic strength E = 1 V/m. Monitored currents for 9 defined sensors were found. Low electromagnetic strength was chosen because of possibility of simulation and measurement comparison. For expected HPM electromagnetic strength around 10 kV/m, relevant currents would be 10,000 times higher than for electromagnetic strength 1 V/m (it is possible to consider linear behaviour for this structure).

4 Simulation vs. Measurement

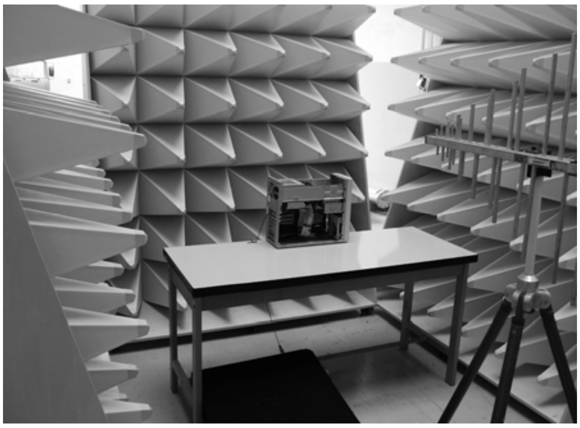
Results gained from simulation were verified by measurement (see picture 3 and picture 4).



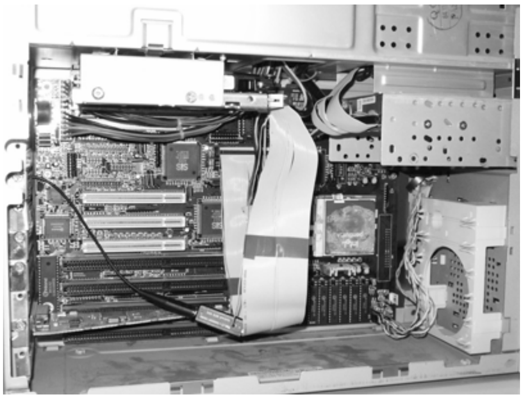
Picture 1 Model used in simulation



Picture 2 Defined 9 current sensors



Picture 3 Test setup



Picture 4 Test setup - detail, current probe in position 4

For electromagnetic strength E = 1 V/m relevant currents flowed in wire 1 of IDE cable of typical values 100's μA were found by simulation. For electromagnetic strength typical for HPM threat 10,000 kV/m it is possible to expect currents values few Amperes. Simulation was supported by measurement where similar currents were found as during simulation. The difference between results from measurement and results from simulation was typically up to 6 dB (2 times) only for some positions the difference was up to 15 dB. It was possible to expect quite big difference between results from measurement and results from simulation because it was impossible to guarantee absolutely the same structure - setup during measurement and during simulation. For example when measured cable was diverted approximately 2 cm beside it caused difference more than 3 dB. When we compared average values from all 9 positions for relevant measurement and simulation, the difference was less than 5 dB.

4 Conclusions

Results gained from simulation were compared with results from measurement. The difference was usually up to 6 dB (extremely in some cases for some positions up to 15 dB). For many purposes this difference is low enough for HPM threat assessment. So simulation methods can be very useful for HPM threat area. It is useful to use them during first considerations. It can give us good explanation of possible expected effects and it can give us reasonable results during vulnerability analysis.

It is obvious the crucial parameter for electromagnetic field coupling to cables is a frequency. For frequencies with wavelengths comparable with the cable length the coupling of electromagnetic field is the most effective and induced currents are the highest. The most crucial are longer cables used in equipment (system) when lower frequencies are used. For personal computers it is possible to expect the highest vulnerability in frequency range 100's MHz.

5 References

[1] AEP-41, Unified Electromagnetic Environmental Effects (UE 3) Protection, Philosophy, and Methodology, 1. 2. 2004

[2] CLAYBORNE D. TAYLOR, D. V. GIRI High-Power Microwave Systems and Effects, Taylor and Francis, Washington, 1994

[3] IEC 61000-2-13, First edition, 2005-03, Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic (HPEM) environments – Radiated and conducted

[4] MIL-STD-461E, Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, 20 August 1999 (vojenský EMC standard)

[5] MIL-STD-464, Electromagnetic Environmental Effects, Requirements for systems, 18.3.1997, (vojenský EMC standard)

[6] ROBERT J. BARKER, EDL SCHAMILOGLU High-Power Microwave Sources and Technologies, IEEE Press Series on RF and Microwave Technology, New York, 2001

Microwave radiometer systems for security applications

Markus Peichl, Stephan Dill, Matthias Jirousek, Helmut Süß
DLR, Microwaves and Radar Institute
Oberpfaffenhofen, 82234 Wessling, Germany
Phone +49-8153-28 –2352, -2390, -2372, Fax +49-8153-28-1135
E-mail markus.peichl@dlr.de, stephan.dill@dlr.de, matthias.jirousek@dlr.de, helmut.suess@dlr.de

Abstract

Microwaves in the range of 1-300 GHz are used in many respects for remote sensing applications. The imaging of persons and critical infrastructures for security purposes is of increasing interest particularly for transportation services or public events. Personnel inspection with respect to weapons and explosives becomes an important mean concerning terrorist attacks. Microwaves can penetrate clothing and a multitude of other materials and allow the detection of hidden objects by monitoring dielectric anomalies. Passive microwave remote sensing allows a daytime independent non-destructive observation and examination of the objects of interest under nearly all weather conditions without artificial exposure of persons or areas. Imaging and profiling systems have been developed in the past for a multitude of applications. The development of suitable high-resolution and real-time capable instruments is supported by the extensive use of adequate experimental sensors as precursors for advanced operational equipment. An application of radiometric sensors for wide area monitoring is illustrated.

1 Introduction

International terrorism has reached a level where adequate countermeasures to protect the population have to be provided by the authorities. Similarly, the improved surveillance and protection of sensitive infrastructures, like for instance nuclear power plants, attracts increased attention. Hence, research on new sensors addressing these new challenges had been animated through various organizations. A millimetre-wave (MMW) radiometer is a potential candidate to construct detectors, which are both reliable and convenient to use [1].

Radiometer systems are purely passive sensors measuring the natural thermally generated radiation. The imaging is rather achieved like in optics or infrared technology by moving a focused antenna beam across the desired field of view and measuring the incident radiation power. The moving is either achieved by a mechanical motion of the antenna structure or by electronic steering. Range measurements cannot be performed, but the output image geometry and the image form of appearance are similar to photographs.

Today many different physical sensors are available for the monitoring of sensitive areas. Each sensor type already has demonstrated its capabilities, usefulness and strengths for certain environments and situations it has been developed for. Due to physical limitations none of the sensor technologies on its own is able to provide 24 hours operation and all weather coverage. For instance optical cameras cannot be operated during night. Infrared can be operated during day and night times but also dust and fog are limitations. Doppler radar sensors only detect signals due to the motion of objects, which can be humans, animals, plants or vehicles, above a predefined threshold. Hence false alarm rates are rather high. Laser scanners as well are affected by atmospheric obstacles and the discrimination of detected anomalies being an intruder or just a false target is impossible.

In general, the advantages of passive MMW techniques are a) day and night operation capability, b) penetration through atmospheric obstacles like rain, fog, dust, and smoke, c) covert operation, d) no exposure of observed objects (e.g. persons), and e) quasi-optical image appearance. Hence an imaging MMW radiometer system can be a suitable completion for an advanced surveillance system. In order to demonstrate potential applications some results using an experimental system are outlined next.

2 Experimental radiometer system

The imaging principle of our ground-based imager ABOSCA is shown in fig. 1. The main goal of this development was the capability to image a full hemisphere and have a high flexibility concerning modifications. A rotating parabolic mirror provides an image line, and the azimuth movement of the whole unit delivers the second image dimension. The system is operated at 90, 37 and 9.6 GHz with about 0.6°, 1.5°, and 5.8° of angular far-field resolution, but it can be extended to any frequency band where ever a receiver is available and the spatial resolution is still sufficient. The measurement duration for the complete hemisphere is less than 5 minutes and the sensitivity is in the order of 0.1 K depending on the over-sampling rate used.

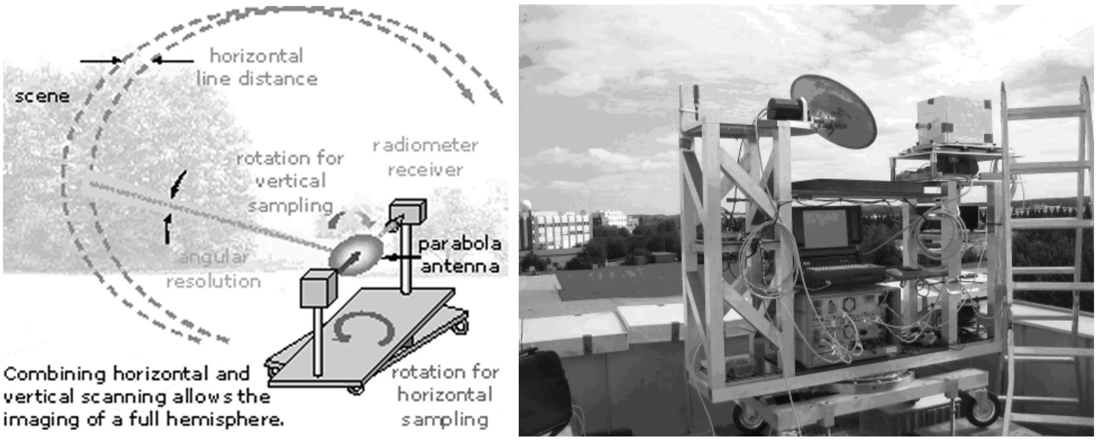

horizontal line distance
scene
rotation for vertical sampling
radiometer receiver
angular resolution
parabola antenna
Combining horizontal and vertical scanning allows the imaging of a full hemisphere.
rotation for horizontal sampling

Figure 1: Schematic drawing and photograph of the experimental radiometer system.

3 Surveillance experiments

The ABOSCA system was installed outside in the corner and in front of a right-angled building alignment. This position allowed approximately 90° of clear view in azimuth and almost 90° in elevation with respect to the scenario located in front. A big portion of the sampled solid angle belongs to the sky region being not the main object of interest. However, this comprehensive characterization of the sky is valuable for calibration and the interpretation of contrast behavior within the scene part of interest. Another large portion is adopted by the building complex.

A sequence of images of the identical scene was measured at 90 GHz in time lags of about 15 minutes. The only intended difference in the scenes was a single person located at different distances with respect to the sensor. The experiment should show the detection capabilities for such a sensor type with respect to spatial resolution, sensitivity, contrast, and stability of the ambient conditions.

Figure 2 shows a photograph and several radiometric images for different distances of about 5 m, 10 m, and 20 m between the sensor and the person. For the photograph the distance was 10 m. Compared to the photograph the optical similarity of the radiometer image stands out. The building structures, the concrete area of the yard, some further distant buildings, some vegetation, and the cold sky region can be clearly recognized. More important, the person can be clearly identified even for the larger distances keeping in mind the spatial resolutions of about 5, 10, and 20 cm according to the as well increasing distances.

Note that the signature of the person is reflected in the concrete, since at millimeter-waves such materials act as an optical mirror. The same is valid for many other objects. It could be shown that even for larger distances of up to 50 m the person can be clearly detected if the images are subtracted from a reference image without the person.

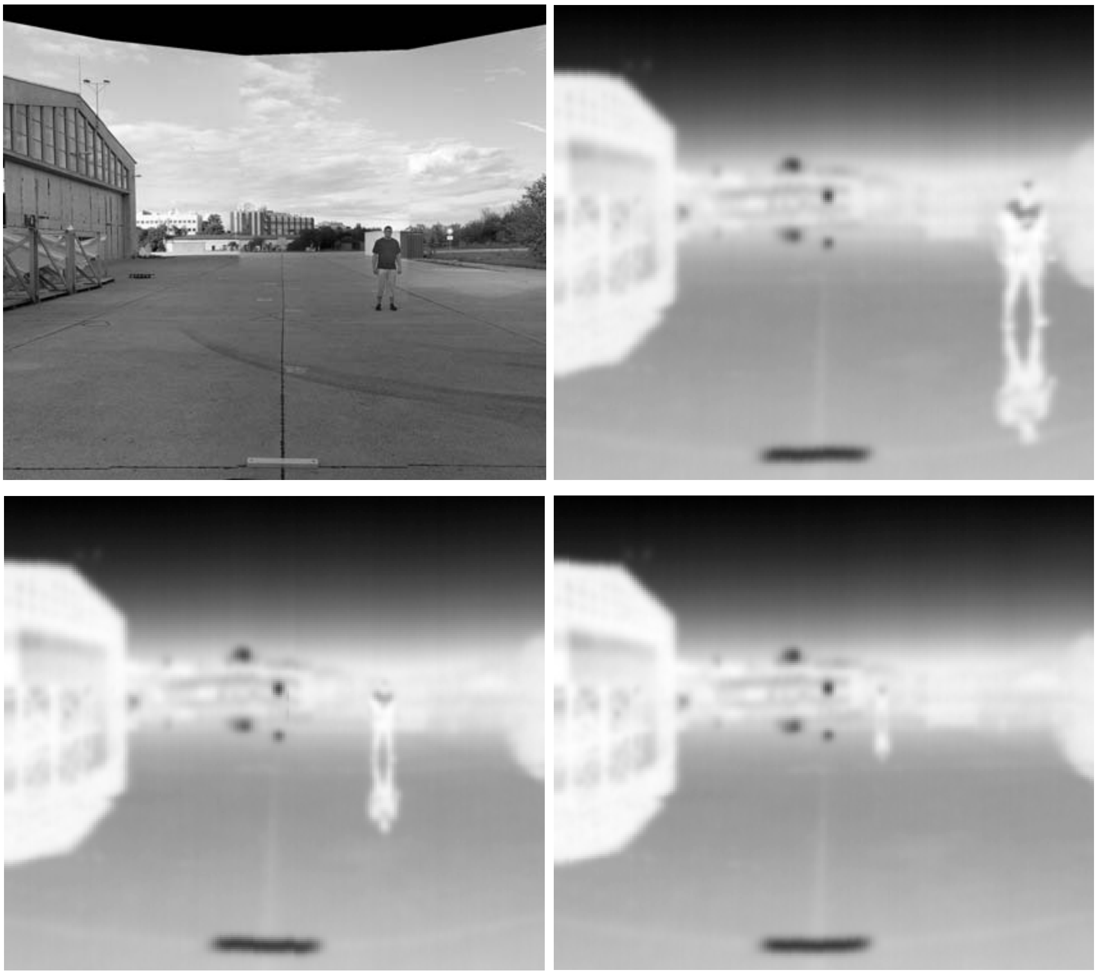


Figure 2: Photograph and a sequence of 90 GHz images of a scene with a person located at different distances. As far as possible the other scene composition was kept identical.

The experiments show that by the use of simple change detection processing a reliable detection and identification of a person is possible for distances of up to many ten meters. This is even valid for situations where no optical or infrared sensor can be used due to a bad visibility.

4 References

[1] Peichl M., Dill S., Jirousek M., Süß H., Security applications of microwave radiometry, Proc. of Fraunhofer Symposium "Future Security", 1. Sicherheitskonferenz Karlsruhe, Karlsruhe, Germany, 04.-05. July 2006.

Public-Private-Partnership – The contribution of the private security services to the strengthening of the infrastructural security

Prof. Dr. Stober, R. (University of Hamburg - Faculty of Law) Germany

Insiders suppose that private security services attain "a accentuated security-policy relevance" in Europe in the long term. Because regardless of the different security-mandates of private services and the police, both security-service providers are lined up in the legally protected interest "security".

The **EU-Commission** also certifies this classifying commercial enterprises as potential prevention-actors in a communication to the council. Accordingly the **Council of the European Union** ascertains in a recommendation regarding "cooperation between the competent national authorities of Member States responsible for the private security sector" among other things:
"The activities of the private security sector have a bearing on the prevention of crime and the safeguarding of public security."
"The stream of information generated by the activities of private security firms is of significance in these fields."

Also the **Minister's of the Interior conference** considers the activity of the private security services as a reasonable supplement to the police work. After the events of September 11th 2001 states have to develop new security models. For it is necessary to protect freedom using security, because freedom has no continuance without security. In consequence of the generally constricted budgetary and personnel position all states will concentrate their security efforts upon certain aspects like counter-terrorism and upon a definite personal protection and object protection. The **security gaps** arising out of this signify new challenges and new requirements for the private security services. In this connection it is discussed between trade and authorities which additional preventive security tasks can be incured by private service providers.

Besides, it involves in the core the regulatory and legal political orientations which confine themselves not at all to the trade permission law. They cover in fact the basic relation between all security actors, because state and private prevention do not coexist isolated in a cooperative state model. For the **cooperation principle** aims at a widest possible participation of all social groups at the conception and implementation of criminal-preventive objectives as a guideline of the state action. It substantiates the **dual security responsibility** of citizen and state on condition that the state has, indeed, a monopoly on force, but no **security monopoly**. In this context police, citizens, companies, federations and social groups form a whole-social security architecture, which is qualified as **security network** or as **security partnership**. This modern view is at the same time a starting point for a mulitfaceted collaboration between police and private security services which proceeds in different forms of **Police-Private-Partnership** as a specification of Public-Private-Partnership. (see specified: Stober, in: Stober/Olschok (Hrsg.), Handbuch des Sicherheitsgewerberechts, 2004 S. 1 ff.)

Countering the threat from Improvised Explosive Devices

Dr B. Reck, Dr M. Sturtzer, F. Rondot, R. Allen, Dr JF Legendre
ISL – French-German Research Institute of Saint-Louis,
5 rue du Général Cassagnou, BP70034, Saint-Louis Cedex, France
reck@isl.tm.fr, legendre@isl.tm.fr

Abstract:

The French–German Research Institute of Saint Louis (ISL) is conducting research programmes investigating current and emerging Improvised Explosive Devices (IED) threats that concern both the European Homeland Security and the security of Armed Forces while deployed overseas for military peacekeeping operations.
The programme has the following aims :

- to identify emerging threat devices,
- to understand the physical lethality mechanisms,
- to assess and predict the on-target effects,
- to define standard reference devices for repeatable studies,
- to develop and assess physical protection strategies.

The studies at ISL address both blast and kinetic effects. The work is, to date, primarily focused on three types of devices which are currently considered to be major threats :

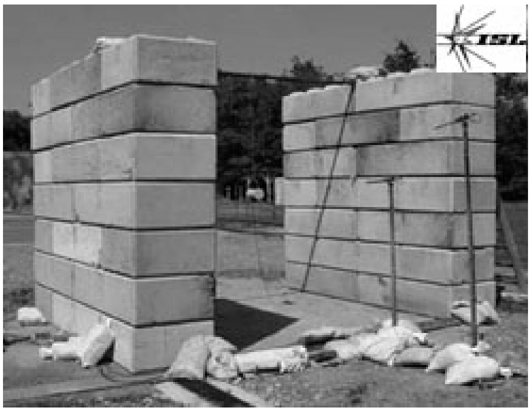
- Homemade explosives with enhanced blast effects,
- Improvised devices with Explosively Formed Projectile (EFP),
- Improvised devices with fragments projection (road-side bombs and suicide belt bombs).

Both 3D numerical simulations and full scale experiments with real IEDs are conducted on ISL Explosive Test Range.
The results detailing the characteristics of the IED threats and protection strategies remain classified and therefore are not presented in this paper.

Homemade explosives with enhanced blast effect.

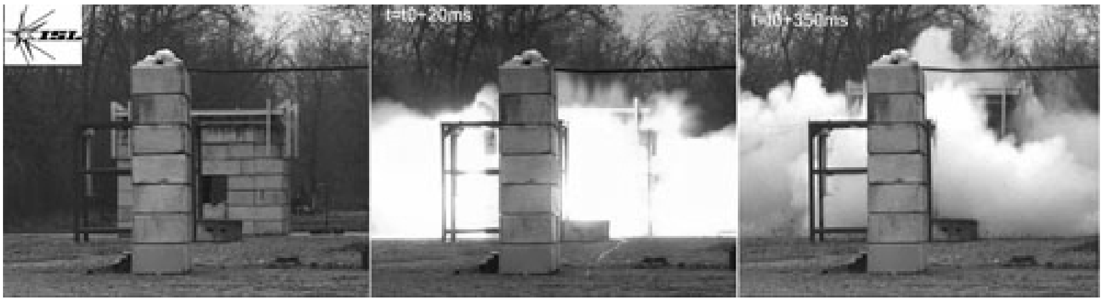
Homemade thermobaric mixtures are designed to increase blast and thermal efficiency in comparison to conventional non-metallized high explosives.

Academic studies are conducted to understand the various reaction mechanisms encountered for the different environment scenarios such as free-field, semi-confined area and fully enclosed buildings.



Two-wall semi-confined configuration.

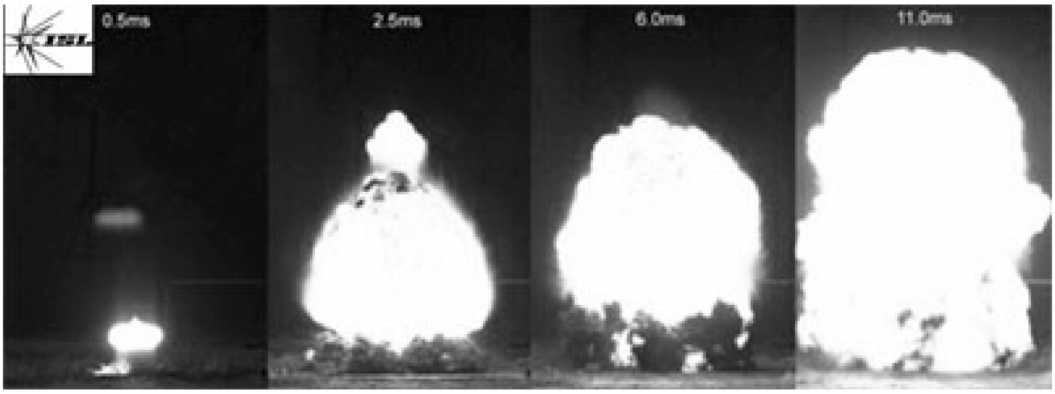
Effects on personnel of home-made charge detonated between 2 walls



Effects of enhanced blast homemade explosives detonated inside building

Mitigation of the damage effects can be achieved in two ways; either by protecting the target to prevent failure or by containing the explosive effects close to the point of detonation.

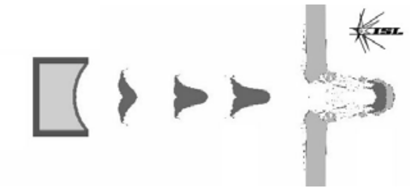
The mitigation research programme has two main objectives – firstly to determine whether current protection systems are appropriate to counter the blast effects and secondly, if required, to develop new protection strategies.

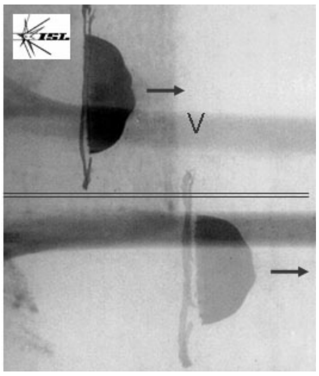


Evaluation of commercial bomb-proof bin containing homemade explosives

Improvised Devices with Explosively Formed Projectile (EFP)

Explosively Formed Projectiles (EFP) represent a major threat in the field of stand-off IEDs. Researches at ISL primarily involve the understanding of the relative effects of the charge architecture parameters. Both numerical simulations and experiments on ISL Test Range are conducted. While different real IED performances are assessed against various types of targets, laboratory reference charges are also designed and are involved for the research on target protections.



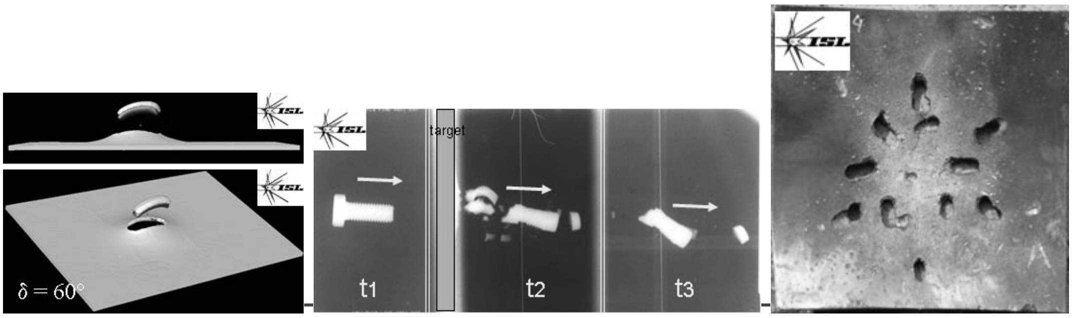


Numerical simulation of EFP projectile formation and target interaction
Flash X-Rays of an EFP projectile in flight
Terminal effects of EFP on armoured-glass

Improvised charges with fragment projection

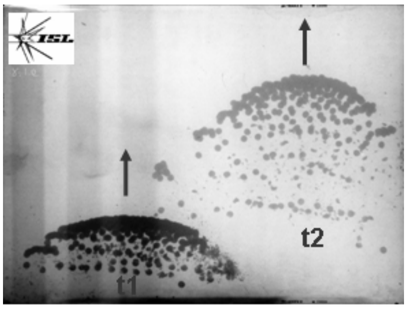
A number of different research programmes are conducted to determine the on-target effects of stand-off IEDs like Road-Side bombs, and also Body-Worn suicide belts containing explosively driven fragmentation. Various types of explosively driven fragments (balls, screws, nuts, bolts, nails, etc…) and natural fragmentation of metallic containers (pipe bombs, pressure cookers, …) are taken into account. While the terminal effects of various reference charges are assessed, specific add-on target protection and also mitigation systems are evaluated and further developed. Both numerical simulations and experiments are involved in this research programme. On-target effects and protection strategies are assessed both with full-scale detonation experiments and simultaneous blast, as well as multi-hits scenarios. For preliminary studies single impact of real fragments are conducted in the terminal ballistics lab with a powder-gun.

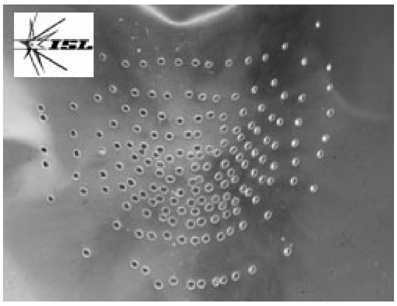
Road-side Bomb with explosively driven screws :



Numerical simulation of target interaction -Flash X-Rays of target interaction of single screw launched by powder -gun-IED interaction with armoured target

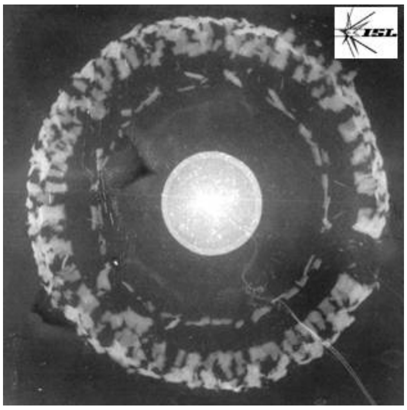
Suicide-belt Bomb with explosively driven balls.





Flash X-Rays of explosively driven ballsIED interaction with vehicle target

Pipe-bomb with fragmenting envelope.



Flash X-Rays of explosively fragmented steel pipe. IED interaction with ballistic protection aramid fabrics.

Airborne Sensor System for near Real-Time Monitoring of Disaster Situations

P. Reinartz, F. Kurz , R. Bamler
German Aerospace Center (DLR), Remote Sensing Technology Institute,
PO Box 1116, D-82230 Weßling, Germany
peter.reinartz@dlr.de

KEY WORDS: disaster situations, aerial cameras, rapid mapping, image time series, near real time processing

Abstract

Near real time monitoring of natural disasters, mass events, and other man-made disasters with optical cameras is the focus of a research and development project at the German Aerospace Center (DLR). For this project, a new airborne camera system is applied and tested. It consists of three non-metric off-the-shelf cameras which are aligned in an array with one camera looking in nadir direction and two in oblique direction, which leads to an increased wide area monitoring capability. With this camera combination, a high resolution, colour and wide-area monitoring task even at low flight altitudes, e.g. below the clouds, is achievable. The goal is to develop a complete system for near real time monitoring of large areas including data transmission from an airborne platform and establishment of an image data evaluation tailored to the specific needs of the civil security authorities and relief organisations. The applications are e.g. infrastructure monitoring including change detection, large flooding situations, monitoring of mass events and, through the usage of image time series (up to 5 images / second), traffic monitoring and also the monitoring of people movements during critical situations. The German Technisches Hilfswerk (THW), the fire brigades of Munich and German police authorities are users and supporters of the project. First results show the direct mapping capabilities through georeferencing without ground control and data integration into the GIS system of the fire brigades of Munich, the traffic monitoring possibilities through image time series and the 3D change detection capabilities through stereo viewing.

Introduction

Airborne imaging sensors like digital cameras and SAR-systems become of increasing importance for near real time monitoring of extreme events in heavily populated areas. These events can be natural disasters like the Elbe flood in April 2006, mass events like the pope visit in Cologne in summer 2005 or traffic congestions after disastrous accidents. Airborne image data can contribute to an area wide situation overview. For the management of such situations the data have to be directly transmitted to a situation awareness centre where they can be utilized for decision makers and planning of the civil security authorities.

The camera system described below was selected for this purpose because it allows image sequences of up to 3Hz, which is very essential for e.g. traffic monitoring to determine vehicle velocities.

For operational use of the image data automatic georeferencing with knowledge of exterior and interior orientation is necessary. To accomplish the georeferencing in near real time only the camera calibration parameters and the recorded GPS/INS navigation data have to be used. Therefore, a method was developed for georeferencing which avoids the utilisation of GCPs. The main part of this method is the determination of the boresight misalignment angles only with tie points.

The investigations of this paper are part of an overall DLR project (ARGOS) to develop a near real time airborne situation monitoring system with data transmission to a situation information centres.

THE DLR 3K-CAMERA SYSTEM

DLR operates an optical sensor suite for experimental and operational flight campaigns. An important part of the sensor suite plays the recently developed optical wide angle 3K camera system (3K = “3Kopf”), which consists of three non-metric off-the-shelf cameras (Canon EOS 1Ds Mark II, 16 MPix). The cameras are arranged in a mount with one camera looking in nadir direction and two in oblique sideward direction (Figure 1), which leads to an increased FOV of max 110°/ 31° in across track/flight direction. With this camera configuration, a high resolution, colour and wide-area monitoring task even at low flight altitudes, e.g. below the clouds, becomes feasible. The camera system is coupled to a GPS/IMU navigation system, which enables the direct georeferencing of the 3K optical images.

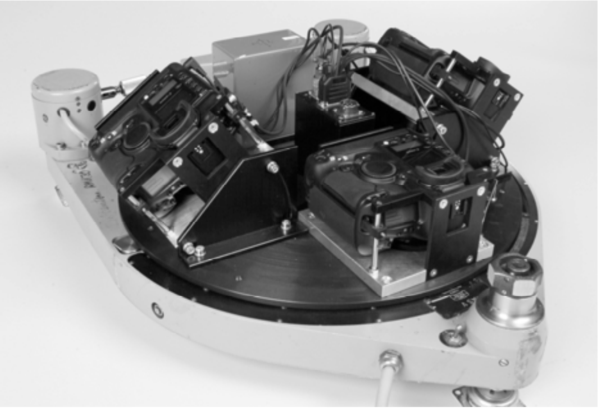


Figure 1. DLR 3K-camera system consisting of three Canon EOS 1Ds Mark II, integrated in a ZEISS aerial camera mount

The Canon EOS 1Ds Mark II camera is the flagship model of the Canon EOS line and captures up to 32 consecutive frames with an image size of 4992x3328 pixels using a full frame CMOS sensor (24x36mm). The highest tested repetition rate for image acquisitions was 3Hz.

As a limitation for contiguous monitoring at this high repetition rates the internal buffer size of 165 MB was identified, i.e. the camera must pause some seconds during flight campaigns to write the data from the internal buffer to the

SD memory cards. If the repetition rate is below 0.5 Hz, contiguous capturing is possible.

Thus, for the planning of flight campaigns with this camera the internal buffer size and the file sizes must be taken into account. The lossless compressed file size for images in the highest resolution is 15 MB, which can be reduced using e.g. JPEG compression grade 10, 8, or 6 to 12, 9, or 4 Mbytes respective.

The onboard data link to a PC, which is required for near real processing of images, could be achieved based on a Firewire connection with a data rate of 1.5 frames/s. Further, an online connection to the navigation system is required for near real time processing based on GPS/IMU measurements.

Figure 2 illustrated the image acquisition geometry of the DLR 3K-camera system. Based on the use of 50 mm Canon lenses, the relation between airplane flight height, ground coverage, and pixel size is shown, e.g. the pixel size at a flight height of 1000 m above ground is 15 cm and the image array covers up 2.8km in width.

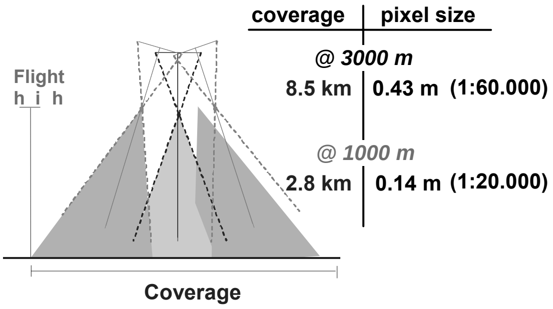


Figure 2. Illustration of the image acquisition geometry, the tilt angle of the sideward looking cameras is approx. 35°.

APPLICATIONS

The applications range from pure image data acquisition and data geocoding with the transmission of the data directly to the situation centres of the involved users, up to real time traffic monitoring with high frequency image time series and traffic data fusion within a traffic management system. Within this wide field the following application examples, including the near real time processing and data transmission, are envisaged:

- Repeated rapid mapping of large areas prone to natural or man made hazards (within 2 minutes an area of 10 km x 8 km can be covered)
- Surveillance of mass events
- Extraction of actual flooding layers containing the information of the flooding extent in a format usable for the civil security authorities
- Change detection of involved infrastructure after a disaster/crisis: Houses, industrial plants, streets bridges a. o.
- Traffic monitoring: extraction of vehicle velocities, congestion and other information, data fusion with traffic information from other sources

- Extraction of digital surface models and 3D change detection using the measured parallaxes in subsequent images

Figure 3 shows an example for the mapping of an ongoing landslide in Austria. In this case the data are used for change detection of the movement of the landslide for a certain time period.

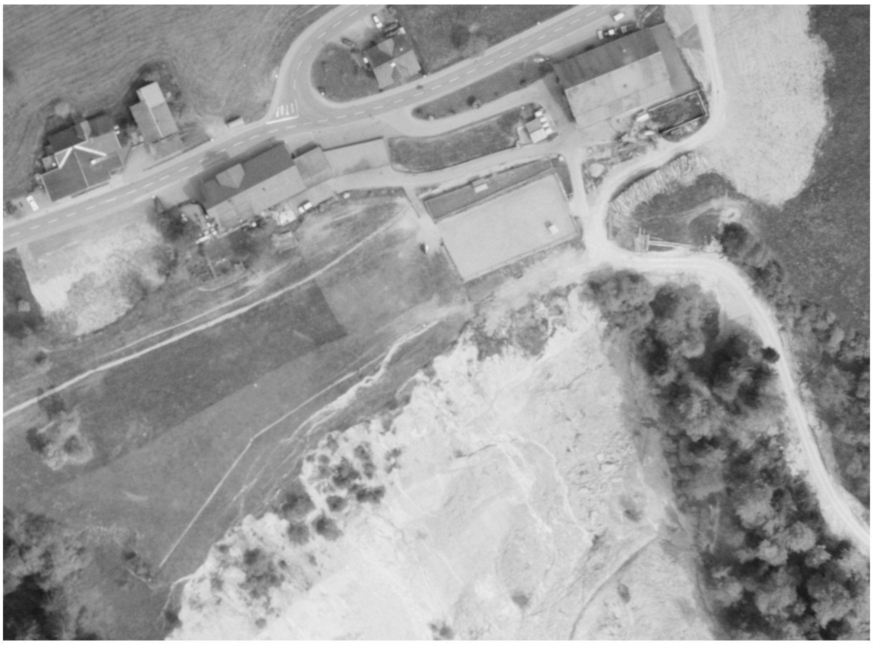


Figure 3: Part of a 3K-camera image showing a landslide area close to buildings in Austria

Structural Behaviour of Masonry and Strengthening against Explosion Loading

M. Romani, FhI for High-Speed Dynamics, Ernst-Mach-Institute (EMI), Germany, Email: romani@emi.fhg.de

Abstract

In this paper the structural behaviour of un-strengthened masonry for blast loads is described. Furthermore, an overview of strengthening methods for masonry structures and their applications will be given.

Introduction

A large part of buildings in Germany consists of masonry. Besides complying with the building physical requirements, masonry is used to provide the structure of a building. For this reason, the masonry must carry and transmit all permanent and variable loads to the ground. The most frequent are self weight, service, wind and snow loads. Apart from these, accidental actions such as earthquakes or explosions can occur. Masonry structures are endangered by out-of plane loads that are typical for explosion loads. Along with the analysis of the masonry resistance, a retrofit measure is often necessary for buildings exposed to explosion hazard.

Un-strengthened Masonry

Masonry has high compressive strength in relation to bending. While the failure in compression occurs through crushing of the bricks, the ultimate bending strength is limited by tensile adhesion in the mortar joints (Figure 1), leading to a much smaller load capacity in the latter case. The strength of masonry is influenced by several effects like material properties, normal forces, structural system, masonry dimensions and support conditions. The load-carrying capacity for out-of plane loads increases if arch effects occur. They are only possible if the support rotation is constrained by the adjacent floors. Normal forces pre-stress the bed joints. Thus higher out-of plane loads can be applied until the bending strength of the masonry is reached (Figure 1). If the masonry is supported as a two way system by the floors and lateral constraints, the out-of-plane load carrying capacity is much higher than for a one way system (vertical floor support only).

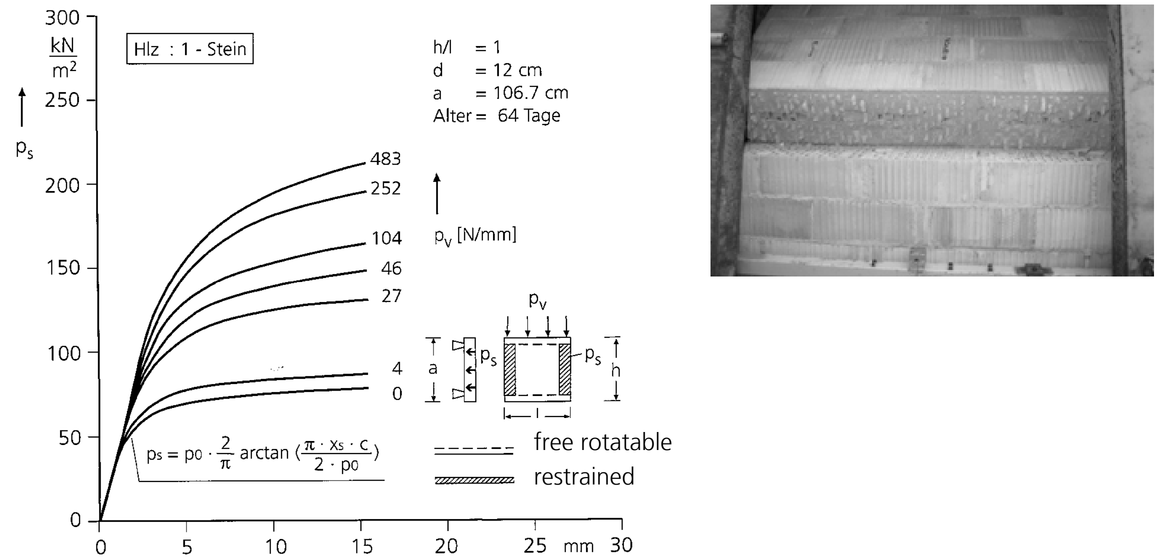


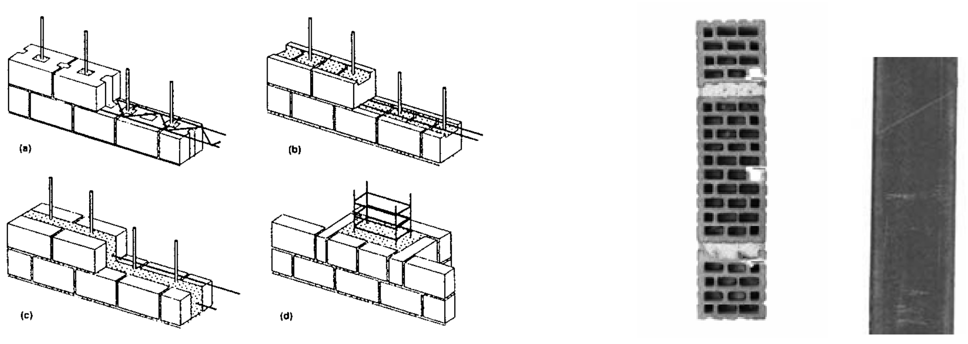
Figure 1: Influence of the normal forces and support condition Mayrhofer /2/ (left) and un-reinforced masonry, one sided spanned after a dynamic shock tube test; tensile bending failure (right).

Retrofit Methods

Reinforcement concepts can be divided in structural strengthening concepts (e.g. additional reinforced plaster layers or Carbon Fiber Reinforced Plastic (CFRP) strips) and fragment mitigation measures (geotextiles, polymer coating, etc.). A summary of materials and components for structural reinforcement and debris ejecta protection based on high potential fibers is given in Figure 1. The aim of the structural strengthening is to reduce the deflection and to avoid structural failure of the masonry and potentially a collapse of the building. The fragment mitigation is used to avoid dangerous flying debris. Failure of the masonry structure will be accepted in the latter case.

Structural Strengthening

Generic steel bars can only be used as an internal reinforcement (see Figure 2). For structural reinforcement materials also materials with a high tensile stiffness are preferably used, like sheets and strips of carbon or aramid fibers. CFRP strips can be applied externally and internally (see Figure 2). Sheets will be glued onto the masonry as an external reinforcement. In the case of a full-surface reinforcement of a wall component, a layer is applied over the entire wall surface. Fabrics like carbon fibers (CF) or aramid fibers (AF) are frequently used. They are applied via a full-surface bonding of the fabric at the opposite side of the detonation. In order to achieve a strong bonding, the top side of the wall must be cleaned and primed, if necessary. There should be a sufficient anchoring of the fabric, so that a membrane effect can be achieved after a peeling of the fabric.



Reinforcement methods with steel bars

Internal glued CFRP-strips (left);
used CFRP-strip (right)

Figure 2: Internal reinforcement by steel bars and internal glued CFRP strips (structural reinforcement).

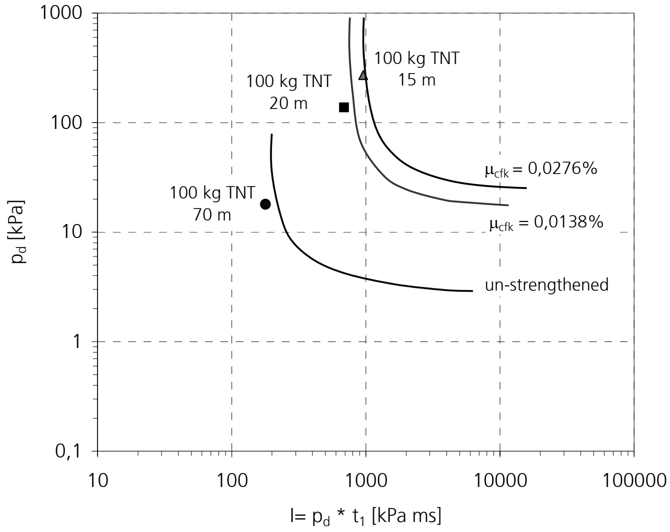


Figure 3: Damage curve for CFRP-strips glued into milled slits.

In the case of a local reinforcement, only a small part of the component surface is retrofitted with the material. As a rule, the local reinforcement consists of one-dimensional bars or strips. Due to the local limitation of the reinforcement, much less effort is required for component preparation. While reinforcement concepts involving steel provide a high ductility, their lack of high tensile strength requires a relatively large part of the cross section. Alternatives are high-strength composites. The fibers are arranged unidirectional in a matrix so that the highest tensile strength and modulus of elasticity is achieved in longitudinal direction of the strips.

Mitigation of Flying Debris

A failure may lead to a hazard to individuals in the interior of the room, caused by the wall fragments. Reinforcement by means of geotextiles and composites are generally available in order to implement a fragment protection (ROMANI ET AL. /1/). A method is the use of geotextiles acting behind the wall a as a tensile membrane in the event of a failure. They only exhibit a high tensile strength in one direction. In the orthogonal direction they have a significant lower strength. In order to achieve a membrane effect in two axes, the geotextile must have similar load and deformation characteristics in both directions, The wall geometry must be suited for its application as well. In addition, the design of the side structural elements must ensure that the loads can be transmitted and supported. The use of composite materials is another option for preventing debris of a masonry wall from entering the room to be protected. Fibers or fabrics with high tensile strength are applied at the rear side. The materials used for the matrix and the high tensile strength materials must be tailored to the construction to be reinforced and to the operational environment. Since high energy absorption capability and breaking extension are required, high-stiffness carbon or glass fibers are often less suited.

Summary

Un-strengthened masonry loaded out-of plane has only a small load carrying capacity in relation to it compressive strength. Thus the resistance of not strengthened masonry is in relation to other materials like reinforced concrete low. Detonations are out of this reason a critical load case. The load-carrying capacity is influenced by the support conditions, the possibility of formation of arching and normal forces. If the resistance of the un-strengthened masonry is not sufficient, strengthening methods are necessary to avoid structural failure with perhaps the consequence of the collapse of the building. Several strengthening methods are possible for the structural strengthening and fragment mitigation.

Literature

/1/ Romani, M., Richter, R.: Bauliche Reduktion der Wirkung von Beanspruchungen durch Blast und nachträgliche Bauteilverstärkung; In: Proceedings 2. Workshop „BAU-PROTECT“, Band 2, Neubiberg, ISSN 1431-5122, 2006, S. 365-378/2/ Mayrhofer, C.: Wirkung vertikaler Auflasten auf das dynamische Tragverhalten von horizontal belastetem Mauerwerk; Bericht E 2/90, Fraunhofer Institut für Kurzzeitdynamik, 1990

Compliance and Security Management

Dr. Andreas Schaad, Dr. Orestis Terzides, SAP Research, Karlsruhe

Abstract

Recent legal guidelines und regulations such as SoX, Basel II and HIPAA do require the stakeholders and owners of an organisation to demonstrate how they exercise control over assets, people, business processes and supporting IT systems. This requires (among others) support for business rules allowing for the specification of separation of duty constraints. This document provides a summary and discussion about current work at SAP Research in the area of modeling and enforcing separation of duty controls (SoD) in workflows. We provide:

- **A brief summary on the notion and importance of separation of duties;**
- **A discussion of SoD properties in the context of an SAP Banking loan origination process;**
- **A report on the technical feasibility for realizing such properties in a workflow management system, based on our successful efforts to couple a rule-based engine with a workflow management system.**

1. Introduction: Compliance and Separation of Duties

Recent legal guidelines und regulations such as SoX, Basel II and HIPAA do require the stakeholders and owners of an organisation to demonstrate how they exercise control over people, business process and supporting IT systems. From an IT perspective, this can be supported by various technologies that allow to achieve a higher and demonstrable degree of control over business activities and the resources of an enterprise. Over the last years we witnessed the shift from “low-level” controls such as database audit logs or other integrity preserving mechanisms towards more application-centric controls that closely resemble the needs and lingo of the solution architects and end users. Business rules, application-level policies and constraints that had previously been hidden in the code started to be defined outside the application in a declarative instead of previously programmatic fashion.

Separation controls are probably the so far best understood type of application-level constraint. The two main application areas are the prevention of fraud due to the misuse of powers and the preservation of integrity. Specifically research in the areas of role-based access control and distributed systems management has led to the definition of several taxonomies and frameworks. Although the origins of this principle cannot be clearly identified, it is obvious that the development of organisational theory and internal control and accountancy frameworks helped in their definition and possible ways of implementation.

One classic example when talking about separation controls is that of preventing fraud committed by the purchasing officer in a company If he could perform all the necessary steps of creating and authorising an order, recording the arrival of the item, recording the arrival of the invoice and finally authorising the payment, it would be easy for him to place an order with a fictitious company he owns, record a non-existing arrival, pay to the company, and add the non-existing goods to the books. Only the end-of-the-year inventory would reveal the discrepancy between the books and the physical stock. One way of enforcing a separation control in this context would be to not let a principal have all the necessary authorisations for each required step in this process. A more relaxed variation may be to not allow him to perform all the steps on his own. This is sometimes referred to as a dual control since two or more people are needed for the execution of a critical process. Another example of separation as an integrity preserving control could be in the context of a software company. Here a programmer may be required to not test his own code. Likewise, when considering the previous cheque processing example, a single programmer should not be involved in the programming of all the necessary transactions of an accounting application, since he might install some hidden backdoors.

2. Case Study: Loan Origination and Separation of Duties

Loan origination is about customers demanding a loan form a Bank and roughly consist of the customer requesting a loan from his bank; the management of his master data; evaluation of external and internal ratings; the bundling / pricing of the product; and final approval and signature. In this context, a static separation of duty property could be that a customer must not be an employee of the bank. Another static property would be that the same person must never be assigned to the cross-check and final approval tasks.

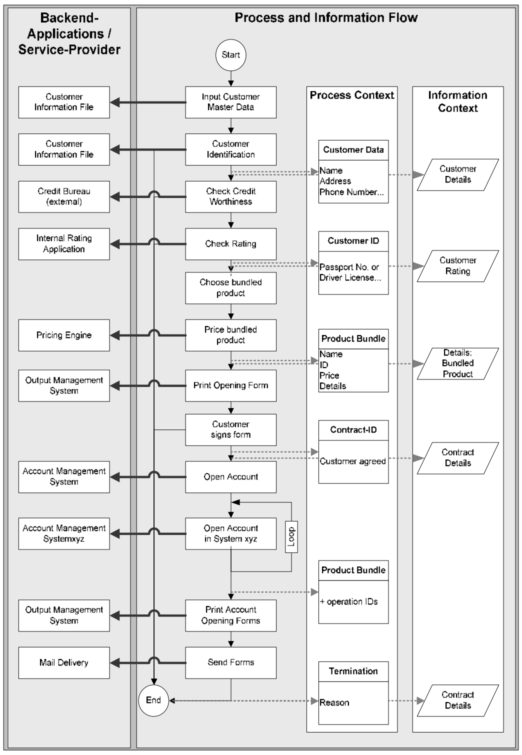


Figure 1: Loan origination process and possible static and dynamic SoD properties

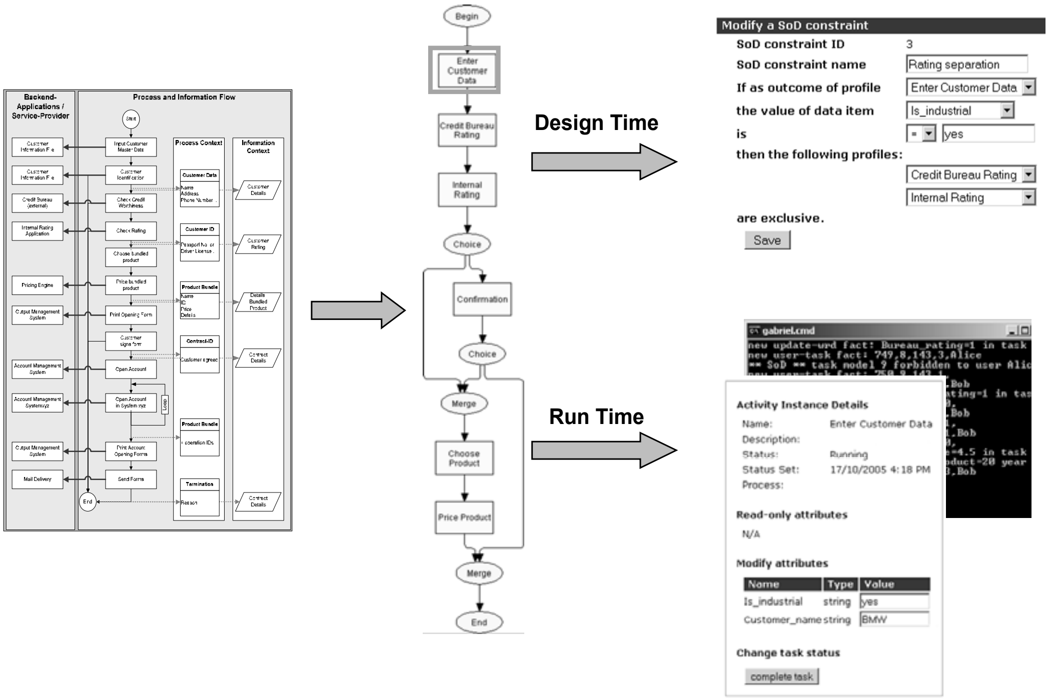
Dynamic properties may be dependent on some process variables. For example, we may require that if the requesting customer is an industrial costumer, a separate clerk must be responsible for verification of the master data. We could also imagine that the four steps of internal / external rating, choosing and pricing the product may be exclusive. That would imply that a clerk may perform any of these steps but not all of them in the same workflow instance.

It is clear that some of these properties could equally be defined in the workflow model context. We would, however, argue that it makes more sense to keep the model as simple as possible and separate from the business rule logic.

Another dimension of complexity will be the materialization of virtual organisations and collaborative business processes. This requires rethinking current control paradigms due to heavily decentralized systems management.

3. Concept Verifying Prototype

To further analyse SoD properties and validate some of our assumptions we coupled a SAP Research workflow management tool suite with a java-based rule engine (JESS) (Figure 2).



Modify a SoD constraint

SoD constraint ID 3

SoD constraint name: Rating separation

If as outcome of profile: Enter Customer Data

the value of data item: Is_industrial

is: = yes

then the following profiles: Credit Bureau Rating, Internal Rating

are exclusive.

Save

gabriel.cmd

```
new update-urd fact: Bureau_rating=1 in task
new user-task fact: 749,8,143,3,Alice
** SoD ** task model 9 forbidden to user Alic
                                       .Bob
                                       ating=1 in tas
                                       0,
                                       .Bob
                                       1,
                                       1.Bob
                                       0,
                                       e=4.5 in task
                                       oduct=20 year
                                       3.Bob
```

Activity Instance Details

Name: Enter Customer Data

Description:

Status: Running

Status Set: 17/10/2005 4:18 PM

Process:

Read-only attributes

N/A

Modify attributes

Name	Type	Value
Is_industrial	string	yes
Customer_name	string	BMW

Change task status

complete task

Figure 2: Coupling a Workflow System and Rule Engine

This allowed us to specify and relate SoD properties to a loan origination workflow model and enforce the constraints at runtime. Enforcement in this context would mean that once a user has worked on some critical task or object, he may then not be able to see and pull a subsequent task into his worklist as a security enforcement point does control the worklist based on the runtime results of the rule-engine.

In a simple case we could thus define that if the customer asking for a credit is an industrial customer, then the external credit bureau rating and internal rating must be performed by two different clerks. More dynamic properties would specify that the steps of rating the customer, choosing and pricing the product must be performed by different clerks. In essence, all the properties as defined in the table in figure 1 can be modeled and enforced. We can even bind duties, thus forcing a clerk to continue working on a case he initiated.

We broadly distinguish between design and run time in our prototype. At design time we manipulate the rule base via an accessible user interface. Predefined and generic separation templates then get instantiated with the workflow model context. At run-time, a task management engine will query the rule engine over a security enforcement point. Based on context data like previously accessed objects or previously exercised tasks etc., the rule engine will provide feedback and the task manager will decide whether a task will be visible in the task list of a user or not. We have also integrated iLog's jRules instead of the JESS rule engine.

Experiences and Trends on Critical Infrastructure Protection (CIP)

Rudi Schäfer, InfoCom, IK11, IABG mbH, Germany

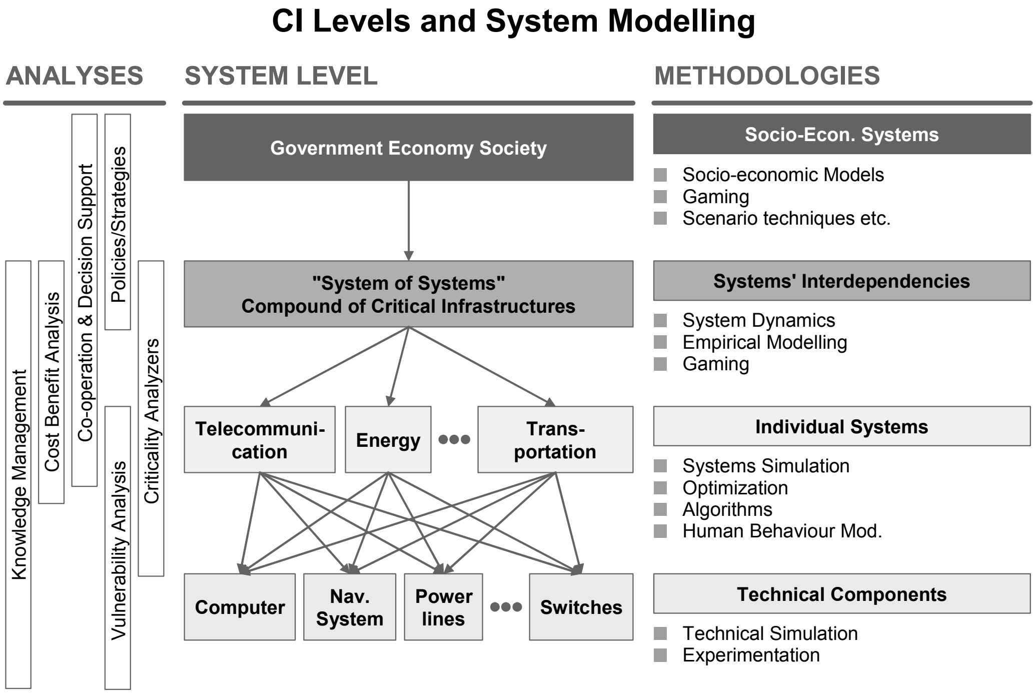
Abstract

Recent national and international projects have identified important requirements and measures to improve the security of critical infrastructures. Experiences and results of projects within the European Research Programmes (FP6 and PASR) may help CI providers to achieve more effective and efficient protection against new threats. Some trends which are decisively driven by activities of the European Commission like the EPCIP will have significant consequences for stakeholders from private and public sectors. Simultaneously new research and development activities within the military domain may contribute to civil security, covering in particular simulation and exercising models to analyse and develop appropriate response to new threats and scenarios. These trends will require new collaboration methods between the involved parties.

Introduction

"Critical Infrastructures" (CI) can be considered as the backbone of modern industrial societies. Most of these highly networked infrastructures are mutually dependent and operate trans-nationally. Disruption of them is critical to Europe's security, to the well-being of the European citizens, and to the functioning of the economy. The term covers a wide range of abstraction levels, addressing socioeconomic interdependencies, system of systems relationships down to individual technical components like sensors or control equipment (see fig. 1). Whilst the latter is rather tangible in terms of technical specifications there are neither common standards nor formal methods to describe the architecture and behaviour of critical infrastructures on e.g. the system of systems or the sector levels. Moreover, human behaviour has a significant impact on the dependability of critical infrastructures, in particular in respond to disruption events. Therefore different practicable methods and models are needed to analyse and describe vulnerabilities and the impact of corresponding protection measures.

Recent national and international projects have provided different attempts to model critical infrastructures on the sector and system of systems level, covering as well human behaviour aspects. Simultaneously activities on national and international level like the European Program on Critical Infrastructure Protection (EPCIP) will have significant consequences for national and European stakeholders from private and public sectors.



Source: IABG

Figure 1

Experiences from recent CIP research projects

Compared with the military research, which is conducted since more than 50 years with budgets of multi billion Euros per year, research in the field of CIP is, like others in the (civil) security research, a young discipline. Important prerequisites like appropriate methods, standards and simulation models are still missing. The European Commission has addressed this challenge since 2002 by various programs, e.g. within the 6th and 7th Framework Programme and the Preparatory Action on Security Research (PASR). One of the most recent CIP research projects was VITA (Vital Infrastructures Threats and Assurance), which has successfully finalized in 2006. VITA, a PASR 2004 project (http://vita.iabg.eu) provided:

- Methods to raise awareness and the sense of urgency on the need for vital infrastructure protection
- An approach on methods, tools and technologies required for the protection improvements
- A demonstrator experiment by a scenario exercise with focus on electrical energy
- Recommendations for future focused R&D in this domain

The demonstrator experiment was the first one of its kind in Europe addressing the phenomena of CIs under severe threats, and the behaviour of systems and involved organisations. In a synthetic, however realistic scenario, Stakeholder representatives covered all levels of an international CI environment: The individual operators; the management of individual infrastructures; end users like health, rescue and transportation systems; local crisis management and cross-border coordination.

Other examples for European CIP research projects are:

- IRRIIS (Integrated Risk Reduction of Information-based Infrastructure Systems), see www.irriis.org
- CI2RCO (Critical Information Infrastructure Research Co-ordination), see www.ci2rco.org

It is important to note that the EU research funding schemes provide only a grant between 50 to 75% of the total project budget. The remainder is from the industrial viewpoint to be considered as an investment, for which a return strategy is required. Whilst a significant gain of technical and commercial Know How can be expected from participation in an EU research project, a realistic evaluation and tracking of opportunities for (commercial) exploitation of results should be a key driver for any decision to participate.

Significant obstacles for progress within the CIP domain are

- The responsibility gap between government and industry. Whilst private stakeholders have a direct responsibility only for the threat category of technical or human failure, it is not clear who is paying for protection measures against natural disasters, technical cascading effects on different CIs and deliberate disruptions, which are considered either as an act of God or as a government business
- The progressive liberalisation in different sectors and the corresponding competition, forcing CI providers to reduce cost for security measures.

Trends and recommendations

Various nations, in particular the United States and some EU member states have independently initiated national CIP studies and work programmes in the last years, most of which are dealing with confidential content. On EU level the EPCIP has been launched in 2005, consisting of e.g. the CIWIN and the Green Book initiative. The new proposal for a European CIP directive issued by the Commission in December 2006 could become a milestone on CIP in Europe, although being attended by conflicting opinions.

The proposed directive establishes the necessary procedure for the identification and designation of European Critical Infrastructure (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructure.

ECI are defined as infrastructures that, if disrupted or destroyed, would significantly affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State.

The Directive lays down a procedure by which the Commission, Member States and relevant stakeholders need to develop sector specific criteria for the identification of ECI. It is then up to each Member State to actually identify the ECI in their country. The Directive proposal further sets out two obligations for owners and operators of ECI. On the one hand operators and owners would have to establish an Operator Security Plan (OSP) which would identify the ECI owners' and operators' assets and establish relevant security solutions for their protection. The estimated timeframe for the implementation of the directive is about five years.

One of the challenges of the implementation of the directive will be to take into account the many and diverse existing regulation frameworks, which deviate significantly between countries and sectors.

Taking into account the experience and trends addressed above some key recommendations for efficient CIP measures are:

- The establishment of an appropriate and integrated threat and risk management process.
- Establish efficient crisis management plans including regular (computer aided) training & exercises covering relevant scenarios and involving operators and decision makers and take into account

dependencies of other (external and cross border) CI, in particular Electricity & Telecommunication / IT providers.

- Deploy methods and/or models to address of human behaviour aspects
- Consider to conduct an independent third party evaluation in order to identify internal shortfalls.
- Be informed on and consider participation in most recent EU CIP research projects (e.g. FP7)

Conclusions

VITA and other European and national CIP research projects have revealed the dimensions of interdependencies of critical Infrastructures on national and cross border level and confirm the necessity of European activities like the EPCIP. Critical Infrastructure stakeholders are highly recommended to participate actively in the discussion and implementation of the EC directive since this will significantly contribute to an improved and efficient business continuity process. More information can be obtained via www.iabg.de.

Small Rovers for Rescue and Monitoring Applications

Klaus Schilling, Daniel Eck
Universität Würzburg, Am Hubland, D-97074 Würzburg, Germany
Steinbeis Transferzentrum ARS, D-97082 Würzburg, Germany
k_schi@t-online.de

Abstract:

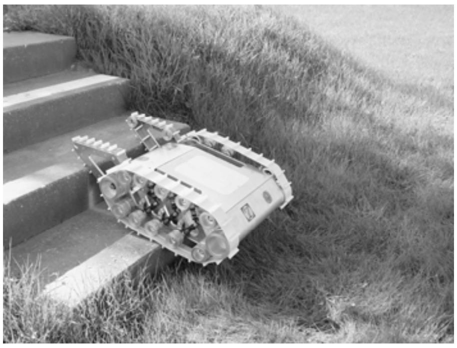
Compact rovers offer interesting potential in security applications related to search and rescue, as well as for monitoring and exploration missions. Since the 90ies the MERLIN (Mobile Experimental Rovers for Locomotion and Intelligent Navigation) vehicles have been used in exploration as well as in monitoring missions. The MERLIN types of mobile robots for rough environments include robust 4-wheeled as well as tracked rovers in the weight class below 20 kg. Modular sensor system configurations for navigation and environment characterisation purposes are provided for typical operation scenarios.

In this contribution a specific application scenario in the security domain is described, addressing the operations of mixed teams of fire fighters and rovers in hazardous environments to perform rescue operations at minimum risk. A system design enabling efficient cooperation between rovers, fire fighters and remote tele-operators has been established and tested. In particular an efficient support system to optimize the data flow and the efficient coordination between the different actors has been provided. To be able to explore and characterize a dangerous area before human rescuers follow, the rovers offer a scalable combination of autonomous reaction capabilities with user-friendly tele-operation on basis of on-board sensor data processing.

1 Introduction

In dangerous environments mobile robots should replace as far as possible the human personal for exploration, monitoring, surveillance, search and rescue tasks in order to reduce risks. Currently the development focuses on small, versatile tele-operated vehicles due to advantages in accessing unstructured environments. On the basis of modern miniaturisation techniques in electronics, especially in data processing and sensorics, this can be realized without reduction in capabilities.

The Outdoor MERLIN



The Tracked MERLIN

The MERLIN (Mobile Experimental Rovers for Locomotion and Intelligent Navigation) family of mobile vehicles for rough environments includes 4-wheel drive rovers, as well as tracked vehicles. While the wheeled robots are fast (up to 50 km/h) and energy efficient, the tracked robots are specialized for difficult areas, where obstacles or stairs are to be passed. Both robots have a weight below 20 kg and a length of about 50 cm, they share modular components, and are designed for the application in rough and hazardous environments [2].

The MERLIN rovers for search and rescue scenarios were designed and tested in typical situations related to fire fighting [1], [5]. A mixed team of human fire fighters, robots and a remote coordinator had to perform rescue operations at a minimum risk. The task of the robots in these teams is the exploration of an unknown, dangerous environment. Appropriate sensors enable the robot to localize its position and to characterize the area by sensors.

More details about the MERLIN robots follows in the next chapter, followed by the discussion of application scenarios in the security domain.

2 MERLIN Rovers

The development of the MERLIN family of rovers started in the beginning of the 90ies as test vehicles for sensor configurations and for operational techniques combining autonomous / tele-operations strategies in the context of the European Mars rover MIDD [Schilling].

The MERLIN rovers are designed as modular systems and easily re-configurable system with respect to sensor configurations and control software. These rovers offer a standard CAN-Bus sensor interface to provide a high degree of flexibility to adapt sensor configurations according to mission needs. Sensor systems employed so far include sensors, such as ultrasonics, infrareds, GPS, laser scanners, inclinometers, encoders, gyroscopes, cameras, active light sensors. The MERLIN Control Software (MCS) provides the servo level control of the different classes of MERLIN robots.

A human operator is challenged by the remote control of such a fast mobile robot in an outdoor environment. Therefore the MERLIN drive assistance system offers a scalable range of autonomous navigation functionalities, as well as data processing functions to display the sensor data in a suitable form for a tele-operator. These capabilities are based on inherent kinematical and dynamical models of the vehicle.

Thus by example in case of an obstacle detected on path either a warning of the operator can be issued, a deceleration of the speed related to the distance guaranteeing a stop in front of the obstacle or initialization of an autonomous obstacle avoidance and detour maneuvers returning to the initially planned path after the obstacle has been passed. Another helpful implemented feature addresses the autonomous return to the start location in case the radio link to the tele-operator has been lost. Here, too, obstacles on the way must be avoided.

3 Application Scenario

The MERLIN vehicles have been optimized for application in search and rescue scenarios to find injured humans in dangerous, quickly changing environments.

A mixed team of fire fighters and robots in the emergency area, as well as tele-operators, coordinating the activities from a distant safe location, has to perform the rescue operations in a most efficient way. The rover assistance system supports the local or remote operators to take advantage of the rover autonomy features with minimum detraction from other urgent tasks and by reducing risks for the human fire fighters by doing a first exploration with the robots. With the cameras and the sensors of the mobile robot, the operator localizes victims and characterizes hazardous areas, before the fire fighters are prepared to perform the rescue activity. The information transmitted by the rover is integrated into maps provided to the rescue team.

In comparative tests in a fire fighter training centre, the increased performance of the fire fighter teams supported by mobile robots has been documented.

4 Conclusions

The MERLIN rovers provide robust and versatile vehicles with a mass below 20 kg for harsh environments. According to the application scenario, wheeled and tracked vehicles can be flexibly equipped via standard interfaces with appropriate sensors to provide good performance for the specific given emergency scenario. The operation of the rovers, either locally or remotely, is supported by a scalable drive assistance system. In the extreme case, also specific autonomous reaction capabilities are implemented in order to return the vehicle safely, in case the radio contact to the operator has been lost. The vehicle performance has been tested in detail for search and rescue scenarios, as well as for remote reconnaissance applications.

References

[1] Driewer, F., Baier, H., Schilling, K. Robot/Human Rescue Teams: A User Requirement Analysis, *Advanced Robotic* 19 (2005), p. 819-838.

[2] Eck, D., Stahl, M., Schilling, K.: “The Small Outdoor Rover MERLIN and its Assistance System for Tele-Operations”, Field and Service Robotics FSR 2007, Chamonix, France

[3] Frank, M., Busch, S., Dietz, P., Schilling, K.: „Teleoperation of a Mobile Outdoor Robot with Adjustable Autonomy“, Proceedings 2nd ACIDCA-ICMI'2005, International Conference on Machine Intelligence, Touzeur, Tunisia 2005

[4] Schilling, K., L. Richter, M. Bernasconi and C. Garcia-Marirrodriga. The European Development of Small Planetary Mobile Vehicles, *Space Technology* **17** (1998), p. 151 - 162.

[5] Schilling, K., Driewer, F. Remote Control of Mobile Robots for Emergencies. *Proceedings of the 16th IFAC World Congress*, Prague, Czech Republic, 2005.

Determination of the Ionization Potentials of Security Relevant Substances within the cooperative project SAFE XUV

E. Schramm[1], A. Görtler[2], T. Heindl[3], A. McNeish[4], S. Mitschke[1],
A. Morozov[3], F. Mühlberger[1], M. Pütz[5], G. Reichardt[6], H. Ries[4], P. Schall[4],
R. Schulte-Ladbeck[5], R. Schultze[7], R. Trebbe[8], A. Ulrich[3], J. Wieser[2],
R. Zimmermann[1, 9, 10]

1. GSF – National Research Center, Neuherberg
2. Coherent GmbH – München
3. Technische Universität München
4. Smiths Group – Wiesbaden
5. BKA – Wiesbaden
6. BESSY – Berlin
7. Optimare GmbH – Wilhelmshaven
8. BBK – Bonn
9. BIfA – Augsburg
10. University of Augsburg

Abstract

The objective of the BMBF-financed SAFE XUV project is to show that single photon ionization (SPI) can be used as a powerful detection method for security relevant substances in complex matrices at very low concentrations. A prerequisite is that the ionization potentials (IPs) of the substances of interest are lower than the IPs of the background gases. This enables the use of intermediate photon energy, low enough not to ionize the matrix elements. Since the IPs are not known from literature for many of these substances, several IPs were determined by single photon ionization time of flight mass spectrometry (SPI TOF MS) using monochromatized synchrotron radiation from the "*B*erliner *E*lektronen*s*peicherring-Gesellschaft für *S*ynchrotronstrahlung" (BESSY). It was found that the analyzed security relevant substances showed IPs significantly below the IPs of common matrix compounds like nitrogen, oxygen, water, argon or CO$_2$. Therefore it is possible to find photon energies where the molecules of interest can be detected with SPI in very low concentrations due to the absence of the matrix ions.

1. Introduction

To identify lowest concentrations of substances like explosives, narcotics and their precursors as well as **c**hemical **w**arfare **a**gents (CWAs) not only in public transit terminals but also for identifying illegal drug laboratories or to discover land mines is an important task for agencies responsible for public security.

The main difficulty is that most of these security relevant substances appear in very low concentrations due to their low vapor pressures. One possibility to increase the concentration in a gaseous matrix is to increase the temperature of the samples. This implies that solid samples have to be collected and vaporized at high temperature. Wipe test desorbers, known from airports, are based on this technique. Thereby the surface of a suspicious object is wiped with a swab. This swab is put inside a thermal desorber where it is heated up and the substances on the swap vaporize into a hot flushing gas like nitrogen. As a result relatively high concentrations of the substances can be generated.

Unfortunately, not only the trace substances are collected on the swab but also a large amount of other substances in much higher concentrations leading to a complex matrix containing, besides the flushing gas, e.g. also oils and fats. Separation of the relevant trace compounds from the matrix is therefore necessary for a sensitive detection.

A possibility to detect low concentrations of different substances in complex matrices is **s**ingle **p**hoton **i**onization **m**ass **s**pectrometry (SPI-MS). This method uses **v**acuum **u**ltra**v**iolet (VUV) photons for soft photon ionization. A single photon is absorbed by the molecule and if the photon energy is higher than the **i**onization **p**otential (IP) of the molecule, an electron is separated. The charged molecule can then be detected by a **m**ass **s**pectrometer (MS). Substances with an IP higher than the photon energy are not ionized and not detected. Most matrix molecules like nitrogen (IP = 15.58 eV), oxygen (IP = 12.06 eV), carbon dioxide (IP = 13.77 eV) and water (IP = 12.62 eV) [1] have relatively high IPs. If the IPs of the security relevant substances IP_{sample} are all below the IPs of the matrix elements IP_{matrix}, it is possible to use an intermediate photon energy E_p, with $IP_{sample} < E_p < IP_{matrix}$, so that the sample molecules are ionized but not the matrix elements. This is very favorable since a high density of ions causes unwanted ion scatter and space charge effects in the MS resulting in an increase of the **l**imit **o**f **d**etection (LOD) for the trace compounds due to high noise signals.
Choosing a photon energy just above IP_{sample} has another advantage. Only little excess energy is transferred to the molecule resulting in a low probability for fragmentation (soft ionization) because the **a**ppear- were used for that purpose.

ance **e**nergy (AE) of many fragments is not reached. The advantage of such a soft ionization technique is that the number of unwanted fragment signals in mass spectra is reduced. The possibility to label signals of complex mixtures is therefore greatly increased.

The IPs of most security relevant substances are unfortunately not known from the literature. Therefore, the IPs of several security relevant substances were determined in this work. To measure the IPs, SPI spectra at various photon energies between 7 eV and 11.8 eV (177 nm–105 nm) were recorded and the onsets of the molecular ion peaks of 10 different drugs and drug precursors, 12 explosives and related substances as well as DIMP and DMMP as simulants for CWAs were determined.

2. Experimental Method

To obtain SPI spectra at different wavelengths, a **t**ime **o**f **f**light **m**ass **s**pectrometer (TOFMS) was installed behind a monochromator at the beamline U125/2-NIM of BESSY ("Berliner Elektronenspeicherring-Gesellschaft für Synchrotronstrahlung") [2]. The 10 m normal incidence monochromator was designed for photon energies from 10 eV to 40 eV, but for the measurements performed here energies between 7 eV and 11.8 eV were used. Unfortunately, some light intensity appeared in higher order of the grating and had to be blocked using a LiF-window. The experimental setup is shown in Fig. 1. The gas streamed effusively through a heated capillary (200 °C) into the ion source where the security relevant substances were ionized by the VUV photons provided by the synchrotron. The ions were mass separated and detected with a reflectron time of flight mass spectrometer[3]. To determin the IPs, it was necessary to maintain a constant concentration of the substances while recording the spectra. Two home made standard gas generators

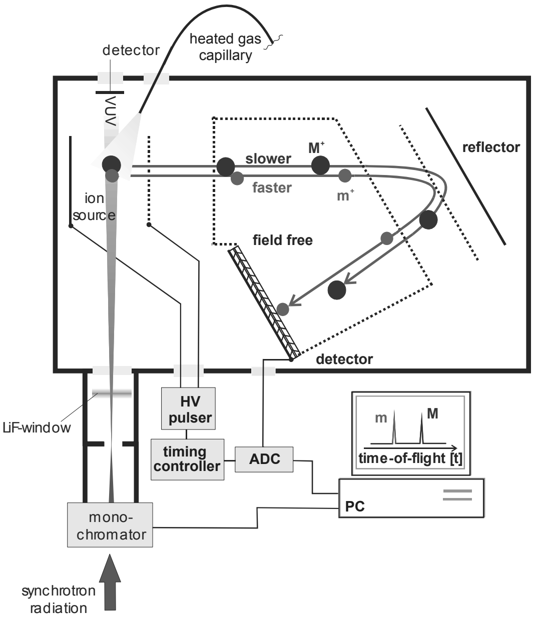


Fig. 1: Measurement Setup

3. Results and Discussion

For data analysis, **p**hoto **i**onization **e**fficiency plots (PIEs) were generated by integrating single spectra at different wavelengths, then dividing them by the respective VUV light intensity and displaying them vs. photon energy. The lowest photon energy where the molecular ion could be detected was taken as IP.

Unfortunately, for some substances the molecular ion peak could not be seen. However by determining the AE of a main fragment a rough estimate of the IP could be found. For the selection of the fragment it had to be ensured that it is a photo ionization fragment and not a thermal decomposition product. Therefore only peaks which could be found in high levels in the EI (**el**ectron **i**mpact ionization) spectrum as well were selected.

Due to a rather low signal to noise ratio and the finite width of the wavelength steps the IPs and AEs are only accurate to within ± 0.1 eV. This could be improved by averaging more spectra at each wavelength and reducing the step width. However, the beam time and the availability of the security relevant substances were limited and therefore the averaging time at every wavelength step was chosen to 10 s with 0.1 eV steps. Fig. 2 exemplarily shows a 70 eV EI spectrum[1], a SPI spectrum measured at BESSY and the PIE plot of 2,4-DNT which is a decomposition product of TNT. Due to its higher vapor pressure it is used to detect TNT.

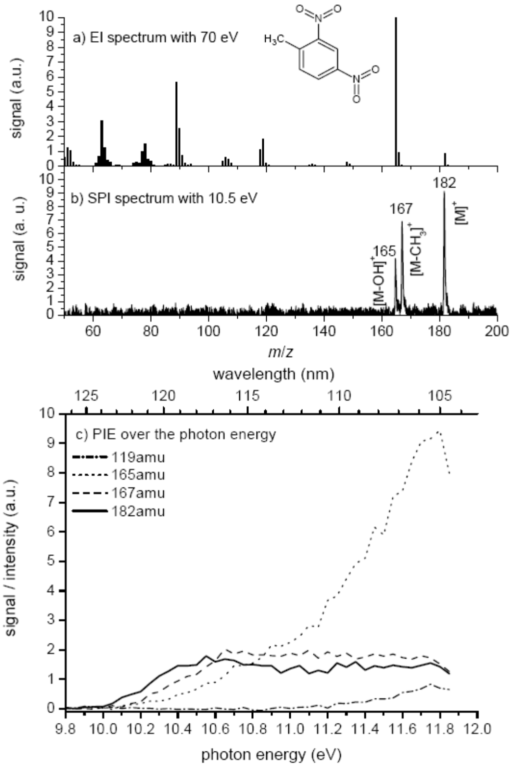


Fig. 2: Results for 2,4-DNT
a) EI spectrum [1],
b) SPI spectrum and
c) PIE plot.

The molecular ion peak (182 amu) appears at 10.0 eV which is therefore assigned as its IP (Fig. 2c). At higher photon energies three fragments at *m*/*z* = 119, 165 and 167 appear. All three fragments are present in the EI-Spectrum as well. The signal at *m*/*z* = 119 is caused by separation of NO_2 and OH from the molecule. The fragment *m*/*z* = 165 results from the loss of OH and the one at *m*/*z* = 167 from the loss of a CH_3-group.

In summary we were able to determine 12 new ionization potentials and to verify 6 known ones in our measurements despite the low concentrations which are due to the low vapor pressure of the security relevant substances. None of the measured IPs is in discrepancy with available data from the NIST data base [1]. For 7 substances only the AEs of fragments could be determined.

It can be concluded, that all IPs from security relevant substances known at this time are below the IPs of the most common matrix molecules including oxygen with the lowest IP of 12.06 eV [1]. According to this it is possible to find a photon energy so that substances of interest can be detected in very low concentration due to the absence of the matrix ions.

4. References

[1] G. Mallard et al., National Institute of Standards and Technology (NIST): http://webbook.nist.gov/chemistry, Vol. 2000, NIST database

[2] G. Reichardt et al., Nuc. Inst. a. Meth. in Phys. Res. Sec. A, Vol. 467-468, Part 1, 21 July 2001, P. 462-465.

[3] F. Mühlberger et al., Analytical Chemistry 2005, Vol. 77, P. 7408-7414.

Columns under Explosion Loadings

Harald Schuler, Fraunhofer Institute for High-Speed Dynamics
79588 Efringen-Kirchen, Germany

Abstract

Columns are parts of a bearing structure which are subjected to very high vertical loads. If these elements fail the consequences can be fatal up to a progressive collapse of the complete structure. The access to exposed columns or to columns in underground garages and the high extent of damage in the case of an incidence makes it inevitable to protect them. Standard concrete is not really suitable to resist against explosions. Its brittle behaviour makes structures vulnerable against shock loadings. Due to reflection of waves crack propagation and spalling occur. A reduction of the bearing cross section and uncovered reinforcement are the result. This leads to a loss of the load carrying capacity. To mitigate this loss, an increase of the ductility is required. It can be achieved with ductile Concrete (DUCON), a micro reinforced concrete, which is attached around columns as a retrofit measure. The break-up and the blow out of standard concrete can be avoided. The material is kept together by the micro reinforcement. Another column type with high resistance is a composite set-up. With steel jackets and box girders the concrete is protected and the damage level is reduced.

Introduction

Loads on structures resulting from detonations can be distinguished into **close-in detonations** and far field detonations (**blast loading**). While close-in detonations act very local, blast loadings subject larger parts of a structure. Figure 1 shows two different scenarios. In the left figure a typical exposed column loaded by high dead load is additionally subjected by a close-in detonation. If this column fails and there is no redundancy in the structure, the complete façade can collapse. For the assessment of such close-in detonations to structural elements, HYDROCODE analyses are suitable.

For design of elements against detonations with a higher distance to the structure, typically, pressure-impulse diagrams (P-I curves) are used. The design curves are based on analysis using a Single-Degree of Freedom System (SDOF). In this article, the focus is set on detonations in the close-in range. Numerical analyses, experimental investigations and retrofit measures are addressed.

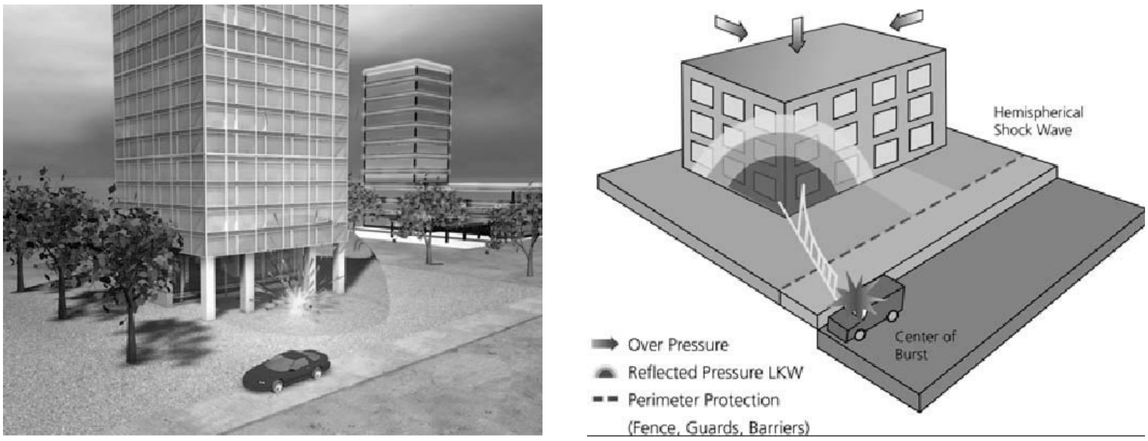


Figure 1: Close-in detonation on a column (left) and blast loading on a building (right).

Numerical Analyses

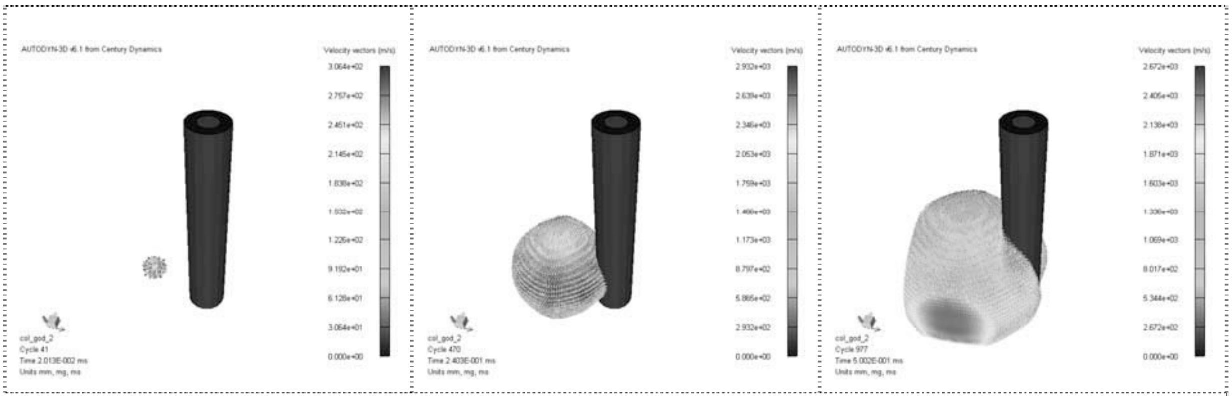


Figure 2: Wave propagation in the air and around a column for 100 kg explosive in a distance of 1.3 m.

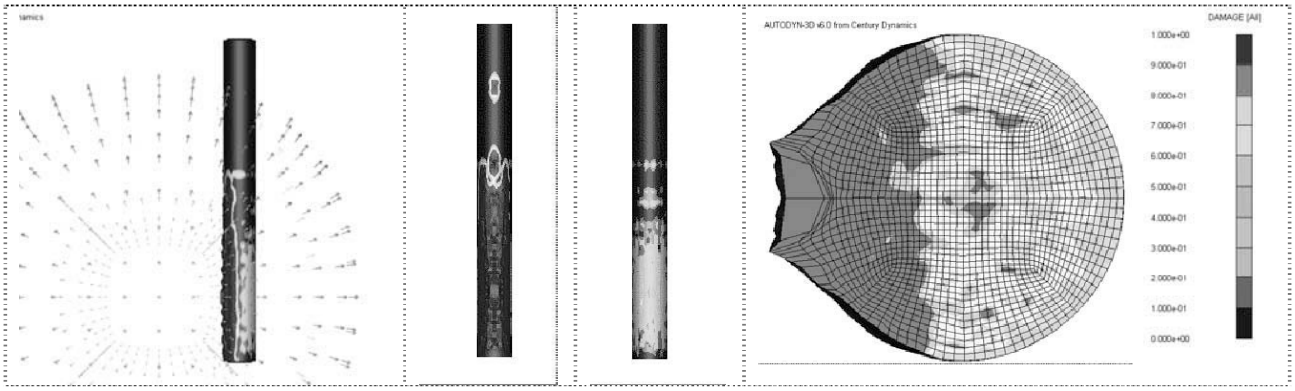


Figure 3: Damaged column after a close-in detonation: side view, front side, rear side, cross section.

For the assessment of structures loaded by close-in detonations, HYDROCODEs are useful. The pressure propagation in the air can be simulated and the effects to a structural element analysed. Figure 2 shows the pressure propagation in the air at different point of times. The loading is in the lower part of the column. There, the damage extent is analysed in detail. Figure 3 shows the calculation of the damaged concrete. The main damage occurs at front side (cp. plot of the cross section). With the results of the simulation, an assessment of the residual load carrying capacity is possible.

Reinforced Concrete Structures

The resistance of reinforced concrete against close-in detonations is small due to the brittle behaviour of the concrete. The failure of concrete is under tension because of its small tensile strength. Cracks and spalling occur and the reinforcement looses its bonding to the concrete. This leads to a heavy reduction of the load carrying capacity. Figure 4 shows two damaged columns. The left column was loaded by a car bomb (real size configuration: Ø 50 cm column/100 kg TNT in a distance of 1 m). The residual load carrying capacity after this explosion was only 9 % of the original load carrying capacity. In the right figure, the result after a contact explosion (bag bombe) is illustrated. In both cases, the concrete cover is destroyed and the concrete in the core is multiple cracked.

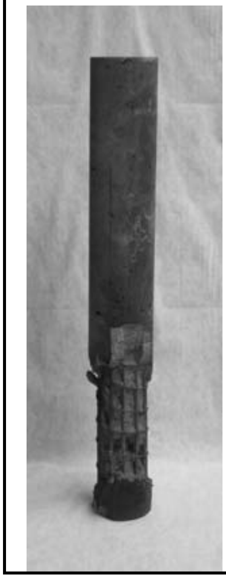
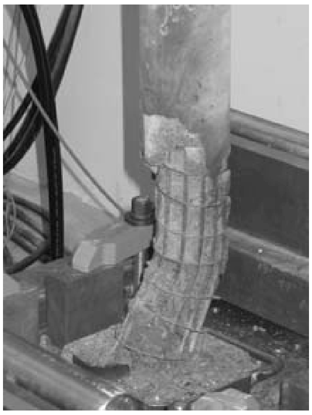
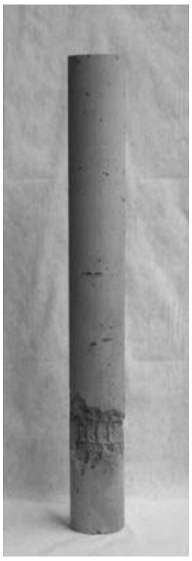
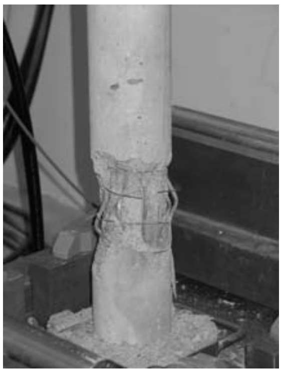
close-in detonation		**contact detonation**	
	Axial loaded column after a close-in detonation 		Axial loaded column after a contact detonation 

Figure 4: Reinforced concrete columns after a close-in detonation (left) and contact detonation (right).

Hardening Measurements

The main task to enhance the resistance of columns against explosions is to increase the ductility. There are two effective concepts to reach this goal. The first one is suitable in particular for new buildings. Composite columns including a steel core and jacket or a filed box girder are very effective solutions. Figure 5 shows different types in the cross section on the left side. On the right side, a tested column in model scale is shown. The deformation of the steel jacked, is high but it still covers the concrete. The residual load carrying capacity of this column was 60 % compared to an undamaged column. A plain reinforced concrete column would fail completely at a comparable contact explosion. The second hardening method is to cover the concrete columns with a micro reinforced concrete (e.g. DUCON). Through a fine mesh of wires, the concrete is kept together in the core (cp. Figure 6). The effect is the same as for the columns with a steel jacket. Micro reinforced concrete can be applied as a retrofit material on already existing buildings. Additionally, there is no corrosion sensitivity as it is with composite constructions.

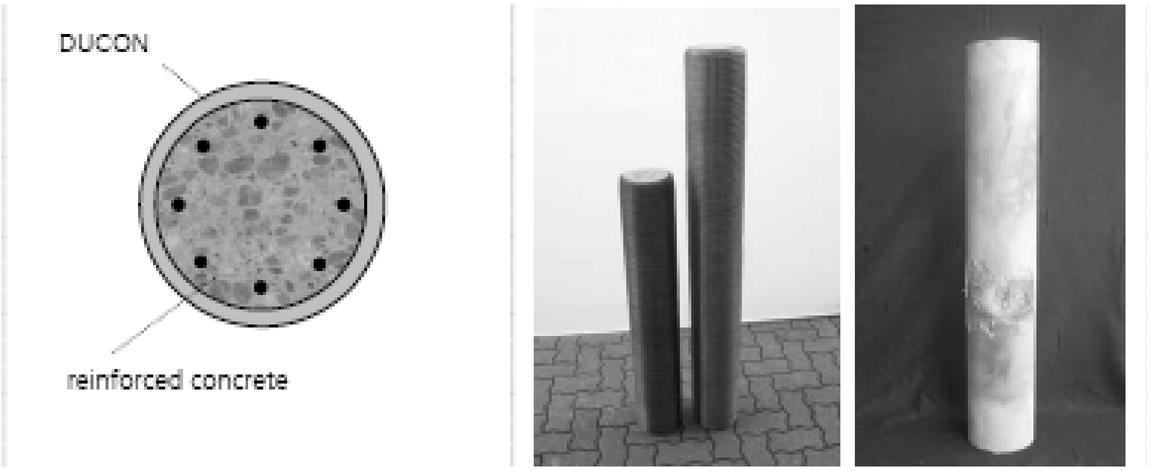


Figure 5: Different types of composite columns (left) and a composite element loaded by a contact explosion (right).

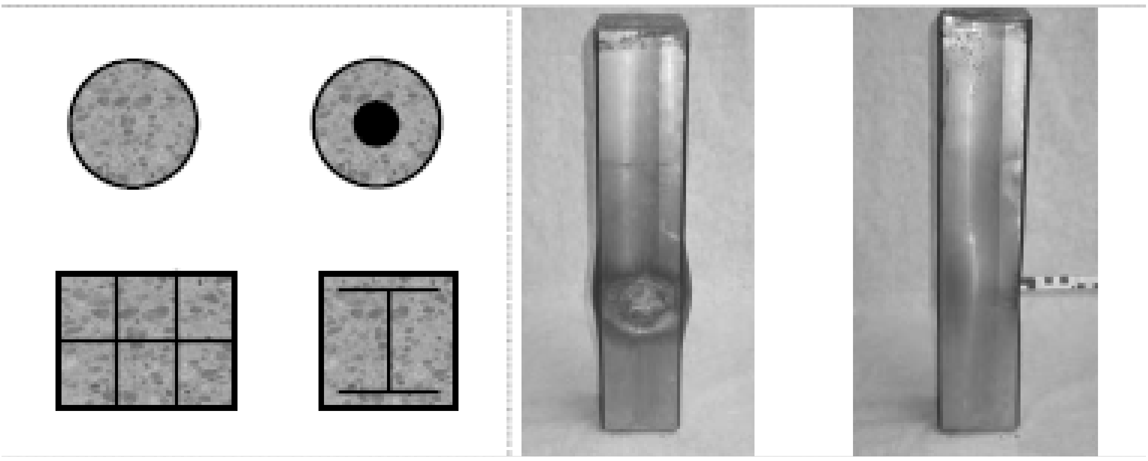


Figure 6: Concrete column surrounded by micro reinforced concrete (DUCON) as a retrofit measurement (left), small damage of a hardened column (right).

Synthesis of Emi Filter Models

J. Sedlácek, Z. Szabó, (Brno University of Technology, Faculty of Electrical Engineering and Communication), Czech Republic

abstract:

In present time the world is becoming more densely populated with devices that are increasingly sensitive to electromagnetic disturbances. In industrial spheres, electronic control systems, data processing equipment and other sensitive devices play an increasingly important role. Therefore solution of problems coupled with problematic of EMC (electromagnetic compatibility) is very important. In electrical engineering practice now are used many new circuit elements for electromagnetic interference (EMI) suppression. In area of EMC there are very often used EMI filters. Their using can be differed to solution of two different problems. At first it is the essential decreasing of undesirable electromagnetic pollution, on the other hand are used to increase electromagnetic immunity of any electrical equipments. Unfortunately, many of these methods cannot be applied directly to power electronics, which has it own peculiarities[1].

EMI Filters

Electromagnetic interference (EMI) can be reduced to acceptable level using filter circuits usually referred as EMI or RFI filters. EMI filters are usually lowpass filter circuits with serial choke coils and parallel capacitors. These filters can be generally divided to two different groups. First group are named as data filters - are used namely in telecommunication systems. EMI data filters are performed as well known lowpass filter configurations (LC ladder circuits). Because these filter are constructed for constant load and generator impedances, design and optimization of filters can be realized according known design and optimization procedures. The second group of EMI filters are filters used in power electronic. In comparison to EMI data communications filters EMI power filters operate typically under mismatched impedance conditions. This major problem of EMI filter design for power electronic equipment is caused by the arbitrary generator and load impedances. These impedances are really arbitrary because neither their value can be known, filters are installed in different equipments and supply network. The design of power EMI filters is different then well known procedures of classical filter design and requires some special view and procedures. EMI filters are generally two - ports characterized by insertion loss (IL) rather then voltage attenuation. An insertion loss definition and measurement method is clear from Fig.1. The difference between the measured voltage appearing beyond the insertion point before (switch position1) and after the filter insertion (switch position 2) can be expressed as :

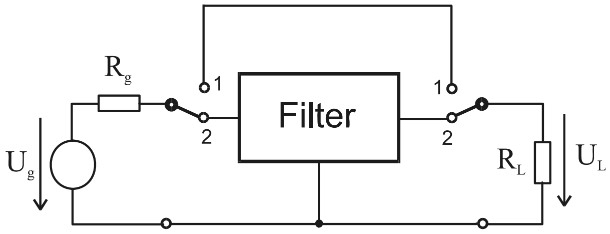


Fig.1. Insertion loss definition and

$$IL = 20\log\left(\frac{U_{L1}}{U_{L2}}\right). \qquad (1)$$

The voltage U_{L1} can be expressed using resistances of load and generator , then insertion loss is given :

$$IL = 20\log\left(\frac{U_g}{U_{L2}}\frac{R_L}{R_g + R_L}\right). \qquad (2)$$

Assuming that the resistance of generator Rg and load RL are in practice most often identical, the value of the insertion loss can be simplified as :

$$IL = 20\log\left(\frac{U_g}{2U_{L2}}\right). \qquad (3)$$

The requirement of insertion loss value must be fulfil in wide frequency range from DC to frequencies about hundred MHz. Thus analysis and measurement of the insertion loss must be made by filter design process in wide frequency range for many frequencies. The chart in Fig.2 presents typical frequency characteristic of insertion loss of EMI filters. In the pass band insertion loss must be negligible, from cut-off frequency fc it monotonically increases. After determining the required insertion loss in the stop bandpass, the next step of filter design is to choose a circuit configuration. Important factors may include a limitation on capacitive current for grounded equipments or the acceptable voltage drop across power line filters. For stringent suppression requirements must be also consider the mismatched impedance conditions.In area of power electronic EMC filter most often areused lowpass LC ladder filters in L, PI or T configurations(see Fig.3). To suppress EMI on all wires, filter prototypes from Fig.3 must be inserted in every wire of power lines. Thus power filter network becomes more complex with an increase in the number of wires to be filtered. According of used measurement system (symmetric, asymmetric or non – symmetric) the unused terminal pairs must be connected together to obtain the lowest insertion loss value. These specifications require the unused terminals to be grounded, ungrounded, or linked to ground through a specific impedance [4].

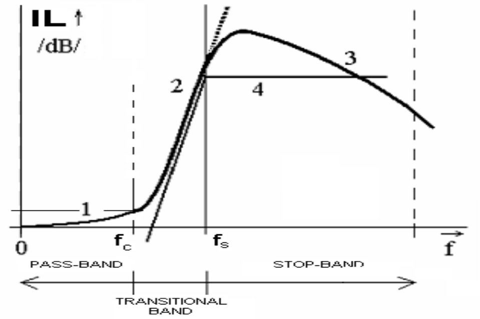


Fig.2. Typical frequency charakteristic of EMI filter insertion loss

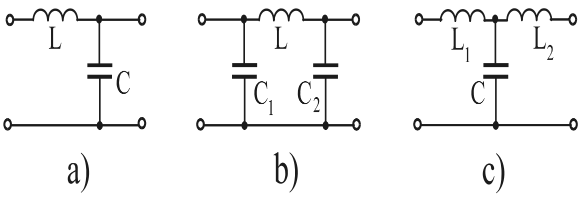


Fig.3. Basic EMI low pass filter configurations:
a) L circuit, b) PI circuit, c) T circuit

Modeling of Emi Filters

The synthesis of proper filter models (equivalent circuits) including function elements as well as parasitic elements is one from important parts of successful EMI filter design and optimization. Using modeling techniques can be analyzed the effects of parasitic phenomena and impedance mismatch. Three major modeling techniques for passive components including their parasitic effects have been developed: direct calculation, engineering approximation and analytical approximation. The EMI filter models can be synthesized using basic filter elements. To express filter performance in required wide frequency range, the basic filter elements must be assumed not ideal. Basic electrical element must be replaced by equivalent circuit including their parasitic elements.

Synthesis of Emi Power Filter Model

As an example of EMC filter model synthesis and optimization a filter model for three phase power FN 256 -64-52 is here presented. The first step of filter model synthesis was grown from known basic filter topology, Fig.4. In the second step the given topology with ideal basic elements was for each from three lines replaced by real models of each (R,L,C) filter elements. After circuit analysis obtained frequency curve of insertion loss was compared with frequency curve presented by the same measuring conditions in manufacturer’s data sheet. Using optimizer routines from analyzers was processly optimized frequency curve of filter model. Using created filter model an influence of resistance of generator R1 and resistance load R2 on insertion loss of filter was investigated to determine worst case of operation. How it is seen from curves, effect of mismatch conditions in worst case can decrease initial insertion loss about 20dB in entire working frequency range what must be by filter design assumed.

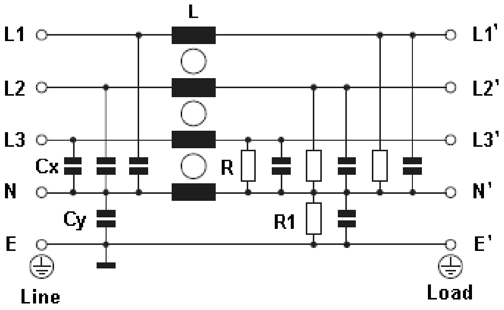


Fig.4. Typical electrical PI topology of power four – wire EMI filter

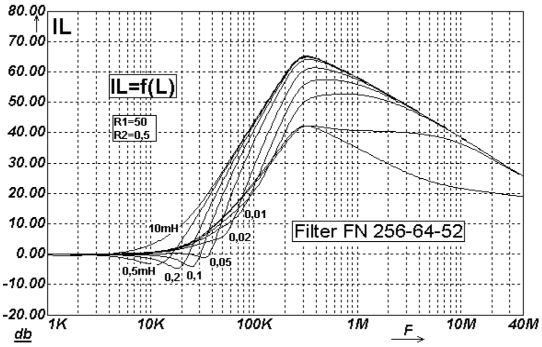


Fig.5. Insertion loss characteristics as function of load inductance

We can see from Fig.5, that in a practice operating filter conditions must be to mismatch conditions, which are leading to worst case operating stage of filters taken in account not only resistances, but also inductances of loads and generators.

Conclusion

In the paper was shortly discusses problems of power EMC filter design and optimization. In a practical example of the power EMC filter was prescribed a synthesis method which enable to set and optimise equivalent filter model including their element value parameters.

Acknowledgment

This work has been supported by the Research Projects : MSM 0021630513 and Grant Agency of the Czech Republic under Grant 102/03/1181, 102/04/0442.

REFRENCES

1. Tihanyi L.: *Electromagnetic Compatibility in Power Electronics.* IEEE PRESS, J.K.Eckert, Sarasota, USA, 1995,2004.
2. Wiliams T, Armstrong K.: *EMC for Systems and Installations.* Newnes, Butterworth-Heineman, Oxford, Great Britain, 2000.
3. Rybak T,Steffka M.: *Automotive Electromagnetic Compatibility (EMC)*.Kluwer Academic Publishers, Norwell, Massachusetts , USA 2004.

4. Dřínovský J, Svačina J.: *Estimation of EMI Filter Performance for the "Worst-Case" system*. Radioengineering, vol.15,no.4. ISSN 04-510-79.Brno 2006.

Standoff imaging of suspicious and hidden objects with electromagnetic waves in the centimeter and millimeter range

[1]C. Sklarczyk, [2]K. Mayer, [1]V. Melev
[1]Fraunhofer-Institut Zerstörungsfreie Prüfverfahren (IZFP), Saarbrücken, Germany
[2]Universität Kassel, FB 16 Elektrotechnik / Informatik, Fachgebiet Theoretische Elektrotechnik

Abstract

Dangerous and illegal objects like metallic and non-metallic weapons, explosives or drugs worn by a person and hidden beneath its clothes can be detected and imaged by means of non-ionizing electromagnetic waves in the centimetre and millimetre range. Experimental investigations have been performed at frequencies of 94 GHz and 24 GHz. Scanning of the hidden objects is done with compact radar modules with standoff distances in the range of several decimetres. The objects are reconstructed three-dimensionally in short time with aperture synthesis using Fourier transform. Some examples are given for imaging of suspicious objects hidden beneath different types of clothes.

Introduction

Electromagnetic waves in cm- and mm-range can penetrate for the most part clothing. Dangerous objects like weapons or explosives worn by humans and concealed under clothing exhibit a reflection behaviour which differs from the human skin. Therefore these objects can be detected with cm- and mm-waves by evaluation of their shape and contrast. Since they are non-ionizing and only low power is needed they are harmless to humans. IZFP has performed experimental investigations concerning detection of different concealed and non-concealed metallic and nonmetallic objects. In cm- and mm-wave range the penetration depth in human body is very low (only a few mm or less). Therefore screening of the human body with the objective to detect hidden objects can only be done in reflection mode.

Experimental setup

Experiments have been performed with a very compact 94 GHz FMCW-radar sensor (**f**requency **m**odulated **c**ontinuous **w**aves) with a band width of about 5 GHz based on a microchip developed by Fraunhofer-IAF, Freiburg. One single chip contains all radio frequency building elements. Only one antenna was used for both emission and reception (monostatic measurement). The radar sensor was mounted on a mechanical two-axis scanner which scanned the object under test. Additionally an industrial low-cost 24 GHz transceiver with small bandwidth (about 0.15 GHz) and with an integrated patch antenna was used. The emitted powers of both sensor types were in the range of a few mW.

Experimental results

If the raw data are evaluated in simple way by only determining the amplitude of the reflected signal the existence of an object may it be hidden or not can be ascertained but the object cannot be recognized due to a lack of lateral resolution. By application of the algorithms of synthetic aperture focusing the resolution can be essentially improved (theoretically up to half wavelength). Reconstruction calculations at 94 GHz have been performed by University Kassel using a three-dimensional Fourier-transformation synthetic aperture focusing algorithm (3D FT-SAFT).

Fig. 1 shows the reconstruction result of a non-concealed ceramic knife containing no metallic parts (distance between antenna and object 40 cm). The ceramic blade can be recognized very well while the grip made from plastics can be discerned not as good like the blade due to the lower permittivity of the plastics compared with the ceramics. In order to simulate the reflection properties of the human body the object was fixed on a plastics torso covered by a wet towel to simulate the properties of the human skin. The object was attached to the towel and then covered by some clothes. Fig. 2 shows the ceramic knife fixed at the torso and covered by a shirt. The blade can still be recognized well but there are some disturbances due to the shirt and the wet towel. In Fig. 3 the knife was covered by a coat and its zipper. The image of the knife blade is disturbed considerably but nevertheless an object resembling to a knife can be discerned.

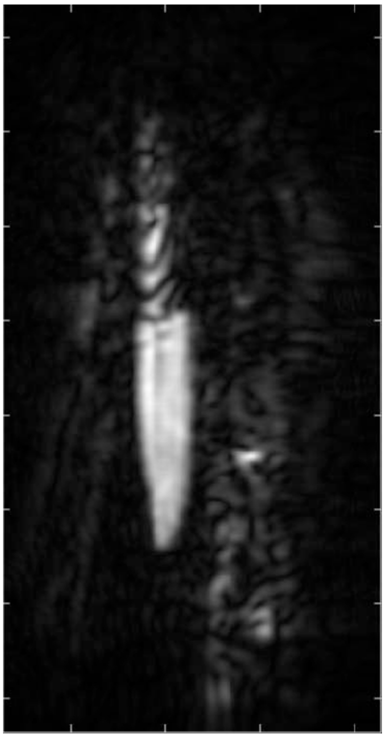


Fig. 1: Non-concealed ceramic knife, knife grip on the top, 94 GHz

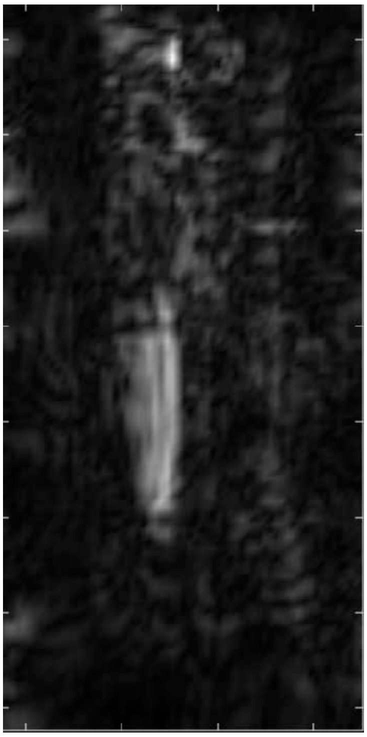


Fig. 2: Ceramic knife hidden under a shirt

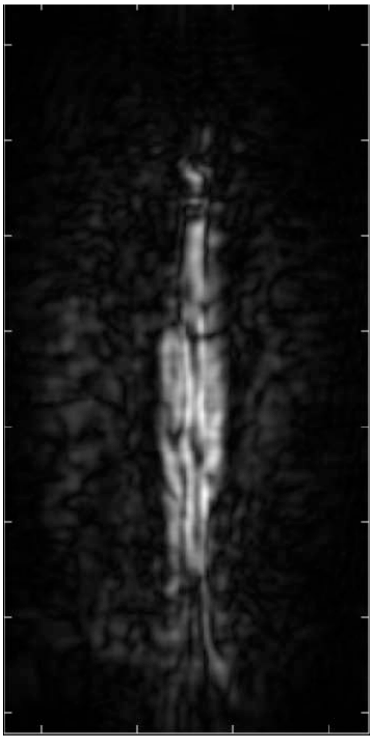


Fig 3: Ceramic knife hidden under a coat with zipper

It has been found that a scanning step of one wavelength delivers a reconstruction image which is approximately as good as an image gained with a scanning step of half wavelength or less. However for bigger scanning steps than one wavelength (to save scan duration) the quality of the image worsens considerably due to some artefacts.

By using a 24 GHz low-cost sensor, objects like a revolver or the ceramic knife can be recognized quite well at a distance of about 60 cm (Fig. 4). The lateral resolution however is inferior to the images at 94 GHz due to the bigger wavelength (about 12.4 mm vs. 3.2 mm). The axial resolution is much lower compared to the 94 GHz sensor due to the lower frequency bandwidth. It is a question of the respective application if this restriction is essential or not.

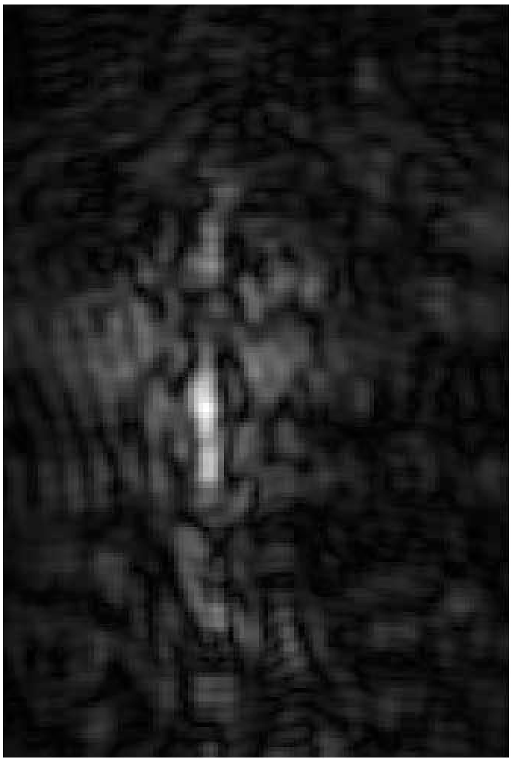


Fig. 4: Ceramic knife hidden under jacket, 24 GHz, scan area 400 x 600 mm²

Conclusions

The experimental investigations have shown that non-metallic objects hidden under clothing can be detected and recognized with millimetre waves. With increasing frequency the object resolution increases, but the number of necessary scanning positions (pixels) is also increasing resulting in longer duration of the object scan. Therefore, an optimum trade-off must be found between high resolution of the image and the number of scanning positions. One possibility to improve the recognisability of many objects is to scan the object with different polarizations of the electrical field vector and to combine the respective images.

Non-Lethal Weapons – A Contribution to the Security of Critical Infrastructures

K.-D. Thiel, J. Neutz, S. Zettl, W. Liehmann, N. Eisenreich, W. Eckl
Fraunhofer Institut für Chemische Technologie,
76327 Pfinztal

Abstract

Additionally to the detection of aggressors the protection of critical infrastructures needs a reaction potential. Non-Lethal Weapons (NLW) could be an innovative part of a staged security system combining the detection of aggressors and the staged, adequate response. Non-Lethal Weapons impact on the aggressors by warning, refusing the access to the infrastructure, deterring and affecting the physical condition. Non-Lethal Weapons avoid or reduce collateral damage compared to conventional systems. A variety of NLW have been developed and tested at Fraunhofer ICT during the last years. Fast deploying barriers based on gas generators, acoustic weapons e.g. infra pulse generators and NLW dispensers are a few examples, which are presented.

Introduction

Non-Lethal Weapons are means to incapacitate opponents or technical equipment. They will prevent severe and enduring injury or damage during and after their deployment. NLW close the gap between the two options security forces are facing today – to do nothing or to shoot. They are more than alternatives to the established systems, because they enable the security forces to react adequately on the different steps of escalation. Main applications of NLW are in the area of counter terrorism, riots, ethnic conflicts and border security. ICT started its research on NLW in 1996, is leading partner in the European Working Group on Non-Lethal Weapons and organizer of the European Symposium on Non-Lethal-Weapons. ICT is active in the creation of concepts for new NLW, the development and testing of NLW prototypes and basic research on different NLW technology areas e.g. mechanical or acoustical effects.

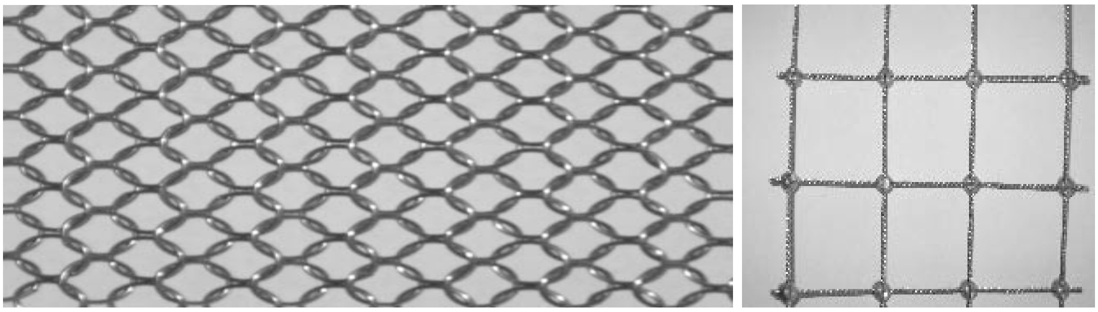
Research Topics on Non-Lethal Weapons at Fraunhofer ICT

Rapid deployable Mechanical Barriers based on Gas Generators

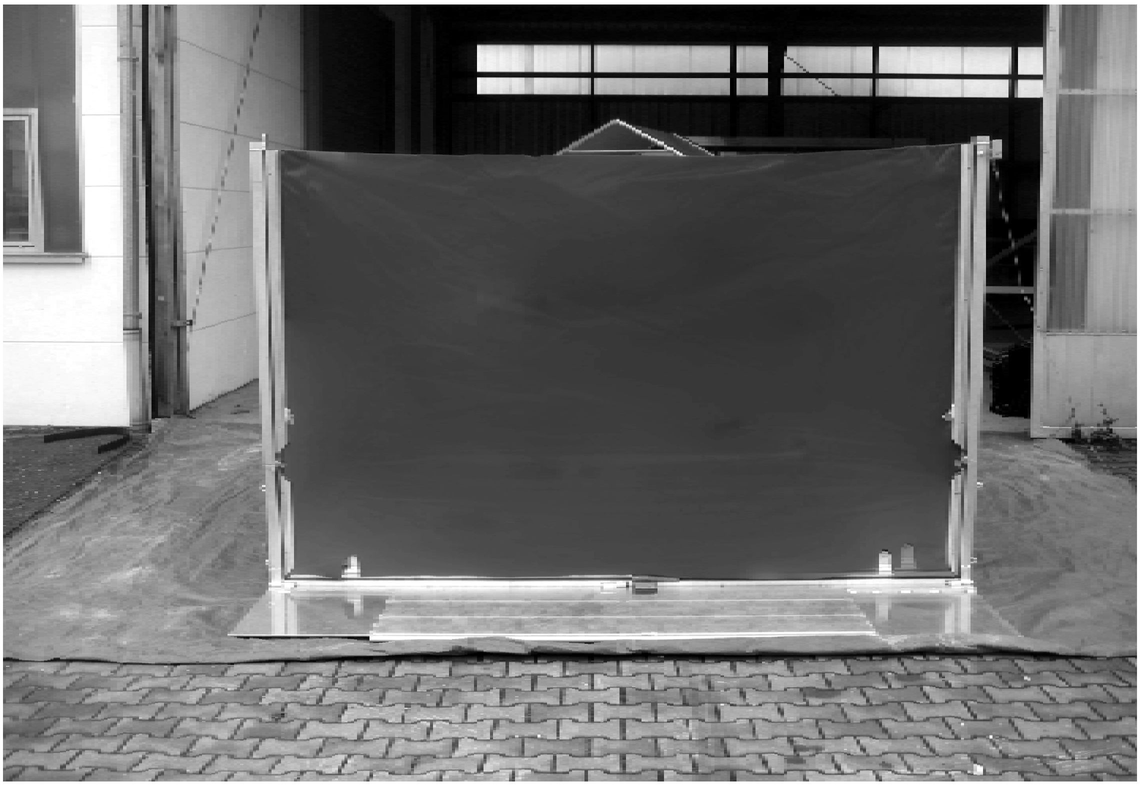
The rapid deployable barrier was developed to protect buildings or areas. The system is able to detect and identify approaching single person or crowds and to deny access to defined areas. In addition, the system can be applied as mobile barrier for special areas at borders, which have to be controlled and protected on demand of the situation. The rapid deployable barrier in combination with other non-lethal means enables an adaptive reaction to the escalation situation.

The barrier is designed in a modular way and consists of telescoping pillars, which can be connected with resistant nets or fabrics. The modular light weight design enables easy adaptation to the local requirements. The pillars can be ejected driven by different energy sources e.g. pneumatics or gas generators. Additionally, the barrier system can be equipped with non-lethal means like an integrated aerosol dispenser, and further useful equipment to repel aggressive persons.

The rapid barrier is used to redirect or distance people and light vehicles from the protected area to avoid the application of conventional weapons or not proportionate application of force in early escalation stages. Furthermore it can contribute to maintain public law and order in case of ethnic or social conflicts with a minimum risk of serious injuries or lethality.



Chain mail (left) or steel net (right) lining of the barrier

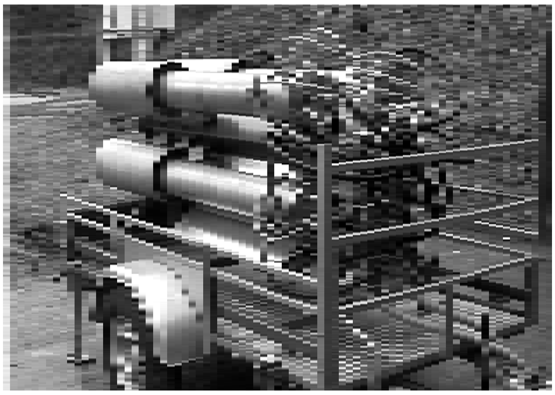


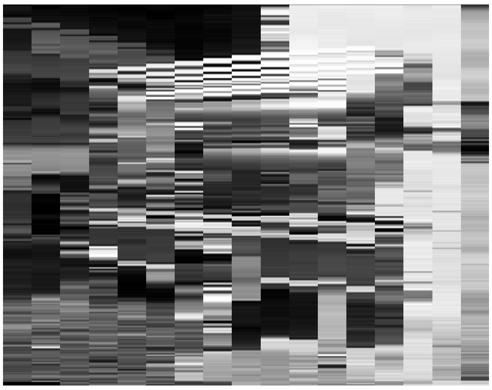
Prototype of the Rapid Deployable Barrier with fabric lining

Infra Pulse Generator

The Infra Pulse Generator is a stand alone system, which can be integrated in an overall concept for the protection of critical infrastructures. The basic working principle is the generation of low frequency acoustic emissions by the combustion of a gas mixture inside a tube. The hot gases form a vortex ring after leaving the tube and the vortex ring propels over a distance of 60 meters. These vortex rings have also mechanical impact on the target and are able to transport irritating agents e.g. OC or tear gas.

The prototype design consists of four tubes, which could be activated subsequently at different frequencies with a maximum acoustic emission of around 140 dB. The Infra Pulse Generator is able to suppress communication between aggressors and to cause malaise in the riot crowd by a periodic noise. The transport of irritating or marking agents in combination with the vortex impulse enables discriminating action on ringleaders.





Prototype of the Infra Pulse Generator

NLW Dispenser

The NLW dispenser is a highly agile mini UAV, which is able to deliver non-lethal means on a distance of 100 to 1000 meters with high accuracy. The NLW dispenser consists of two components, which are connected during the flight mission. At the final approach the NLW dispenser is discharged to deliver the non-lethal means on the target. The maximum weight of the non lethal means is up to 1 kg. Additionally the remaining carrier is able to control the effect on the target via video systems. The NLW dispenser could be applied to incapacitate ringleaders or small vehicles carrying explosives or toxic agents.

Prototype of the NLW dispenser.

Summary

Three different NLW prototype systems were presented and described. All systems are applicable for the protection of critical infrastructure as an additional mean for the security forces to react adequately on the different stages of escalation.

European Working Group on Non-Lethal Weapons (EWG-NLW)

K.-D. Thiel (Chairman of the EWG-NLW)
Fraunhofer Institut für Chemische Technologie,
76327 Pfinztal

Abstract

Many emerging and non-traditional threats should be countered with an innovative response based upon non-lethal capabilities. The foundation of the European Working Group on Non-Lethal Weapons (EWG-NLW) in 1998 is to be seen as a response to this challenge. Non-Lethal Weapons are of interest as well to the military as to law enforcement agencies. The EWG-NLW is the scientific organizer of the biggest Symposium in this field worldwide. This year the European Symposium on Non-Lethal Weapons took place the fourth time – in May 2007-. The Symposium acts as a forum to review current and future Non-Lethal Weapons technologies, to represent new results and to discuss contributions to improve the understanding of the widespread and interdisciplinary phenomena of Non-Lethal Weapons.

Introduction

Several European organisations are currently developing and implementing non-lethal capabilities.

This enables many emerging and non-traditional threats (which may appear in low intensity, asymmetric conflicts, peace support-, and anti-terrorism operations) to be countered with an innovative solution.

Non-Lethal Weapons are of interest to both the military and to law enforcement agencies as, in many cases, the character of the scenarios might be similar. Non-Lethal Weapons can be seen as having dual-use application and they provide armed forces, law enforcement agencies, and policies with additional options to respond in a tailored and graduated manner.

Background

The EWG-NLW was founded in autumn 1998. Present Members are from Austria, Czech Republic, France, Germany, Italy, Netherlands, Russia, Sweden, and The United Kingdom. The working Group is open to all European organisations working in the area of Non-Lethal Weapons.

Aims of the EWG-NLW

There are two complementary strategies of the EWG-NLW to improve awareness of Non-Lethal Weapons. On the one hand there is a holistic approach, i.e. by considering all essential aspects (legal, ethical, sociological, technological, medical etc) and on the other hand High Tech solutions.

Activities of the EWG-NLW

Activities of the group include:

- Exchange of information and harmonisation of activities
- Promote Research & Development of Non-Lethal Technologies to meet future European requirements
- To encourage the European defence industry to become more innovative and more competitive in designing, developing and validating new Non-Lethal Technologies
- To include related activities on law enforcement and homeland security
- Independent operational expertise of the NL Technology development and deployment

Definition of Non-Lethal Weapons

The following definition of Non-Lethal Weapons is that of NATO:

Non-Lethal Weapons are weapons which are explicitly designed and developed to incapacitate or repel personnel, with a low probability of fatality or permanent injury, or to disable equipment, with minimal undesired damage or impact on the environment.

Mission Statement

The EWG-NLW supports the development and use of technologies, devices and tactics which are intended to preserve life whilst enabling lawful and appropriate use of force in response to threats, be they individual or crowd based.

Furthermore the EWG-NLW advocates full co-operation between European partners to share information, scientific advancement and recommended operational practise.

Why NLW are needed?

New means have to be found to address threats whilst minimising the risk of fatalities and harm to the environment or other critical infrastructure.

Who uses them?

Non-Lethal Weapons are employed by authorised civilian and military organisations.

Where should they be used?

They should be used at any place and during any situation whereby the relevant authority may seek to resolve a situation using lawful and appropriate force, possibly supported by conventional, lethal options.

When should they be used?

In case that it deemed safe to do so and it is believed any life maybe saved.

The benefits of using non-lethal technologies must be balanced against the risks to military or law enforcement personnel and the general population. It should be recognized that no technology or device can be guaranteed to be completely non-lethal and injuries may still occur, even when used with minimal force according to the rules of proportionality.

What types of NLW should be used?

Any option should be used which is considered to be appropriate, acceptable and lawful given the situation. Development of new non-lethal technologies will allow military and law enforcement personnel to exploit alternative means of countering potentially hazardous threats, expanding their capability with new options that offer an acceptable alternative to lethal force.

European Symposium on Non-Lethal Weapons

The respective national Points of Contact to the European Working Group on Non-Lethal Weapons serve as the Programme Committee of the European Symposium on Non-Lethal Weapons (http://www.non-lethal-weapons.com/).

To receive an impression as to the relevance of the last Symposium:

At the Symposium in May 2007 there attended about 170 participants from 16 countries.

There were given 30 oral presentations and about 40 posters. The Symposium included topics such as

- Current and desired Capabilities
- Advanced Technologies
- Operational and Tactical Aspects
- Effects on Targets & Evaluation of Effects
- Legal and Public Acceptability

Summary

The employment of Non-Lethal Weapons has arguably saved many human lives in a variety of different situations in recent times.

Numerical Simulation of Windows Subjected to Blast Loading

S. Vetter, W. Riedel, D. Fürbas

FhI for High-Speed Dynamics, Ernst-Mach-Institute (EMI), Germany
Email: vetter@emi.fhg.de; riedel@emi.fhg.de

ABSTRACT

This paper describes how numerical modelling based on finite element simulations and the mathematical model of the single degree of freedom system are used to examine windows. The numerical simulation offers the opportunity to examine almost arbitrary component geometries and complex blast phenomena. The influence of model parameters like dimensions and support conditions on the shape of damage curves is investigated. Numerical simulation as an additional tool to experimental testing and engineering judgment is demonstrated.

1. Introduction

The glazing of sensitive infrastructure and buildings with increased safety risk has to fulfil particular requirements with respect to explosion protection. The efficiency of explosion-proof windows is generally verified by »shock tube« or »free range« tests. As only a restricted amount of tests is feasible, statements for arbitrary loading conditions are derived by the mathematical model of the single degree of freedom system. By comparing strength and natural frequency with peak pressure and duration of the blast loading, damage curves for pi-diagrams are developed from failure predictions. These pi-diagrams can be established for combinations of explosive charge weight and stand-off.

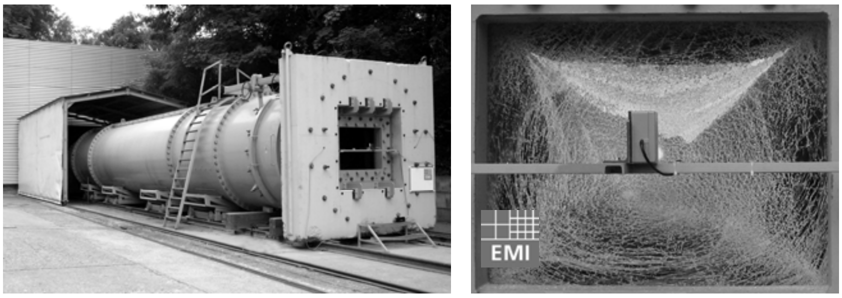


Fig.1: Shock tube test facility and test specimen.

2. Methodology

Window panes and complete window systems can be examined by the mathematical model of the single degree of freedom (SDoF) system. The system can be described by the following equation:

$$k_m \frac{m}{A}\ddot{x} + k_l p_s(x) = k_l p(t)$$

$$\omega = \sqrt{\frac{k_l}{k_m}\frac{c}{m}} = \frac{2\pi}{T} \qquad c = \left.\frac{\partial p_s}{\partial x}\right|_{x=0}$$

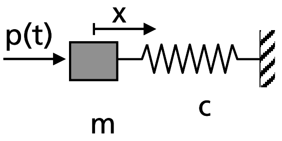


Fig. 2: SDoF model.

k_m and k_l are load factors for equivalence of strain energy, kinetic energy and the work of external forces. ω and c are defined as natural frequency and stiffness of the element respectively.

The resistance function p$_s$(x) can be derived from experimental test data or from a numerical simulation. With the resistance function at hand, free field blast with arbitrary charge and distance combinations can be analyzed. The dimension afflicted SDoF approach can be transferred into a normalised dimensionless formulation to obtain pi-

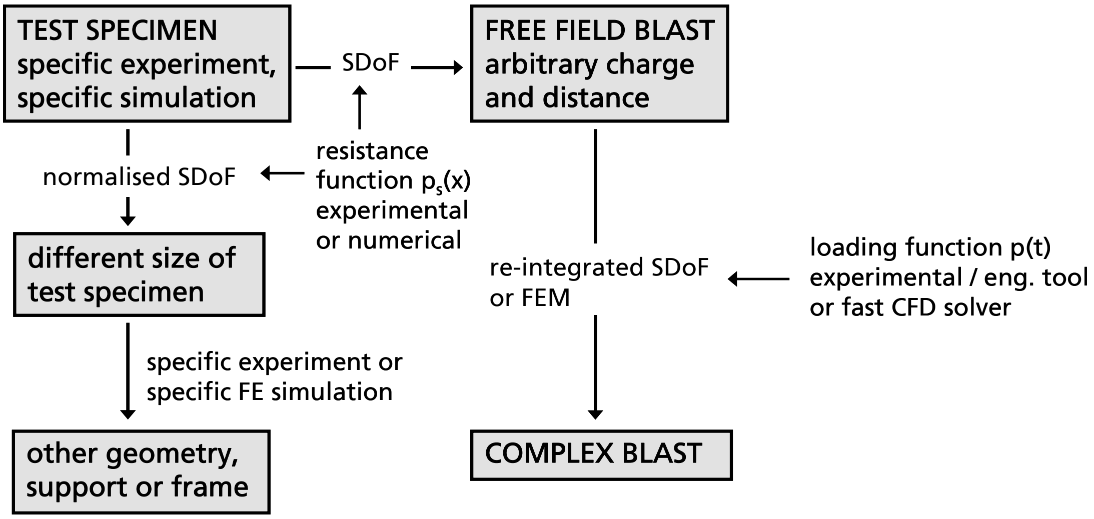


Fig. 3: Analysis scheme of structural elements.

diagrams for different window dimensions. The pi-diagrams can also be generated by multiple finite element simulations with varying pressure-impulse combinations.

3. Numerical Simulation

3.1 Resistance Function

The resistance function $p_s(x)$ can be derived from numerical simulations, in which the influence of different boundary conditions, like simple or fixed support as well as the interaction of glass pane and window frame can be analyzed.

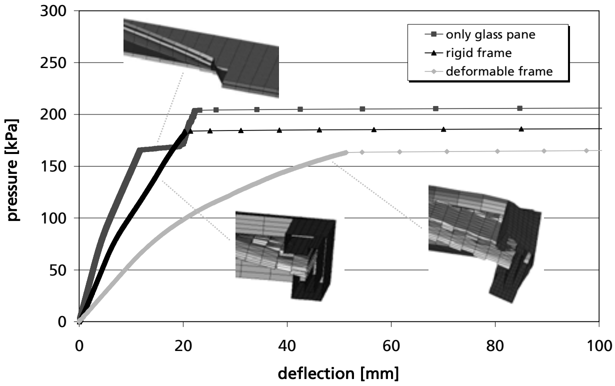


Fig. 4: Resistance function for different system configurations.

3.2 PI-Diagram

A pi-diagram for an arbitrary geometry and frame design can be generated by a series of numerical simulations with varying combinations of pressure and impulse. Below the resulting boundary line, the structural component stays intact, whereas above the line, a distinct failure criterion has been reached.

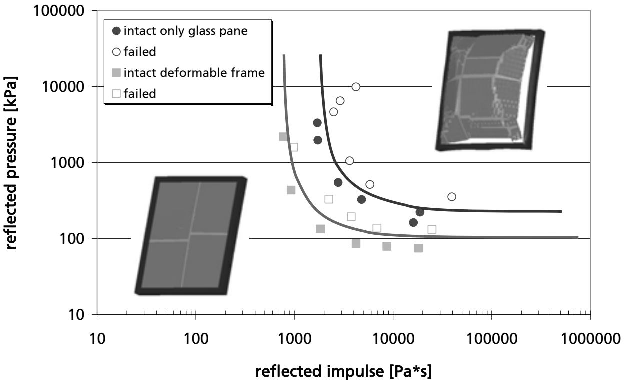


Fig. 5: PI-diagram generated by numerical simulation.

3.3 Arbitrary Blast Loading

With numerical simulations or the re-integration of the SDoF, arbitrary blast loading that is different from free blast wave propagation, can be examined. Such »complex« blast loading occurs for example in urban areas where narrow streets and dense building development

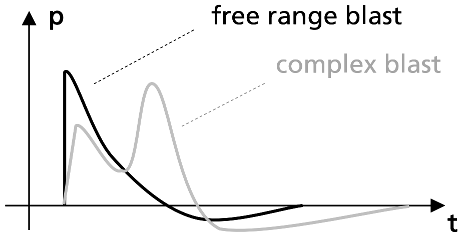
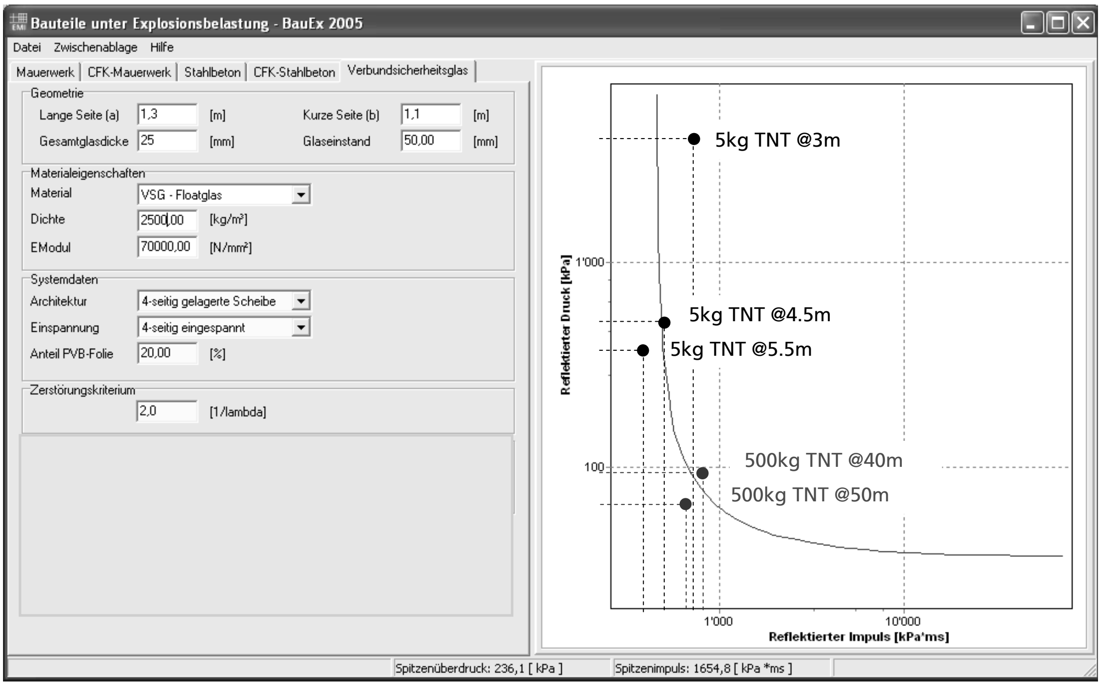


Fig. 6: Complex blast.

lead to multiple reflections and focussing effects. Therefore duration of blast loading and peak pressure can vary significantly.

4. Engineering Tool

For a quick and first assessment of a structural element like window glazing, masonry or reinforced concrete engineering tools are used. The EMI engineering tool BauEx for example is based on the normalized SDoF approach to evaluate structural elements. Figure 7 shows an example of two different explosive loads with sub- and supercritical stand-off distances.



Geometrie
Lange Seite (a) 1,3 [m]
Kurze Seite (b) 1,1 [m]
Gesamtglasdicke 25 [mm]
Glaseinstand 50,00 [mm]

Materialeigenschaften
Material VSG - Floatglas
Dichte 2500,00 [kg/m³]
EModul 70000,00 [N/mm²]

Systemdaten
Architektur 4-seitig gelagerte Scheibe
Einspannung 4-seitig eingespannt
Anteil PVB-Folie 20,00 [%]

Zerstörungskriterium
2,0 [1/lambda]

Spitzenüberdruck: 236,1 [kPa]
Spitzenimpuls: 1654,8 [kPa *ms]

Fig. 7: Engineering tool BauEx, developed by EMI.

5. Summary

Instead of experimental testing, the finite element method was used to determine the resistance function $p_s(x)$ of a structural element. PI-diagrams have been derived by a series of numerical simulations. The numerically derived resistance functions can be implemented into easy to use engineering tools. The advantage of the numerical simulation, in comparison to experimental testing, is the possibility to examine arbitrary geometries and blast loading that is different from idealized free field blast conditions.

New, high-energy anti-terrorist equipment

Authors: Dominique Vinci – Michael Mamou - PyroAlliance Company (SNPE Group) France

SUMMARY:

**PyroAlliance, an advanced pyrotechnology subsidiary of the SNPE Group, uses its technological expertise in countering terrorism threats.
Within the scope of the ATLAS project, involving special police units from the European Community, PyroAlliance's contribution involves the design and supply of high-energy equipment and tools for rapid-response forces.**

Based on a modular design for rapid and easy system deployment, the technical solutions proposed by PyroAlliance are particularly innovative and very robust.

**The equipment defined easily adapts to a wide range of operational configurations. The ruggedness of their design ensures a very high level of reliability and safety.
To illustrate this, PyroAlliance presents this poster of the SORMA and CIBA systems as an example.**

**The SORMA system is designed for rapid and accurate breaching of all types of walls made of various materials and thicknesses, including metal, composite, glazed, and masonry walls, etc.
The CIBA system is a cutter designed to slice through metal bars.
These systems use cutting detonating cord technology in a modular architecture whose geometry adapts to the configuration encountered.**

Overview of the cutting detonating cord technology

Cutting detonating cords were originally developed to cut metal or composite structures for the needs of the space industry. For example, they are used on the ARIANE 5 launcher to separate the strap-on boosters from the main stage and to ensure functions dedicated to the launcher's safety.

They can be adapted to the requirements of various defence, safety and industry sectors in general, and allow for intervention in extreme, inaccessible and hostile environments.

The cutting detonating cords consist of a metallic part or sheath in close contact with an explosive substance. The metal sheath completely surrounds the explosive charge forming a dihedral.

The sheath features a V-shaped cross-section.

Operating principle: The detonation of the explosive charge projects the two faces of the sheath into the dihedral's plane of symmetry where their collision initiates a two-dimensional metallic jet, in the shape of a blade, projected at very high velocity (several thousand m/s). When the jet encounters a nearby material, it produces a groove which causes the part to be severed.

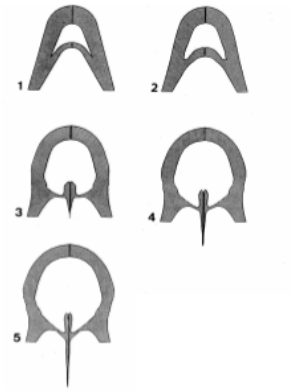


Figure 1 – Dynamic operation of a cutting detonating cord

In comparison with other products available on the market having the same cutting capacity, the cutting detonating cords manufactured by PyroAlliance feature significantly weaker explosive linear charges (3 to 5 times less). PyroAlliance offers a wide range of cords featuring a metal sheath (lead, copper or silver). The size is selected according to the intended application. PyroAlliance uses secondary explosives such as octogene, hexogene, hexocire, and hexanitrostylbene. For applications requiring a very high cutting capacity, PyroAlliance proposes cords charged with plastic-bonded explosives in a copper sheath.

Overview of SORMA and CIBA systems

The SORMA and CIBA systems were designed in close collaboration with ATLAS European task force to meet the needs of special police response units. These systems integrate cutting detonating cord technology.

SORMA is a pyrotechnic system designed for rapid and precise breaching of all types of walls made of various materials and thicknesses, including metal, composite, glazed, and masonry walls, etc.
The system is modular in design.
System deployment in the field is very easy.
The geometry of the frame can be adapted to the requested dimensions of the opening.
SORMA is presented in kit form, consisting of pre-equipped angular and linear modules.
The modules are assembled into plastic cutting frames.
The operator set the frame's dimensions by adjusting the length of the linear modules with a special tool.
The frame is transported and installed on the target by means of an innovative carrying device using a vacuum-based gripping pad.
The SORMA system is ultra-lightweight, weighing less than 5 kg.
SORMA currently exists in 5 different models to cover a wide range of applications

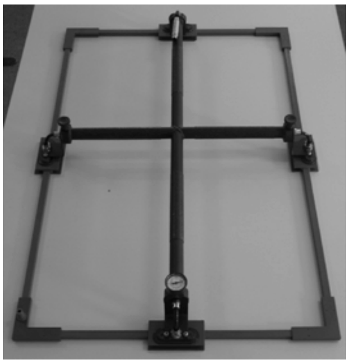


Figure 2 –SORMA equipped with is carrying system.

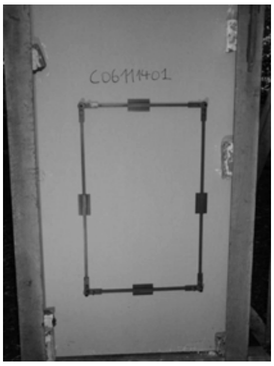


Figure 3–SORMA installed on its target

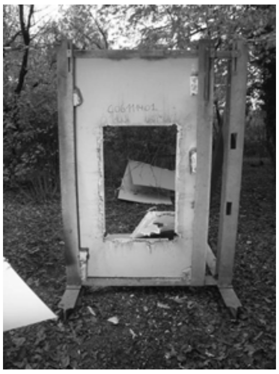


Figure 4– Opening made by the SORMA system

CIBA is a system designed to cut metallic bars.

The system resembles plastic cutting pliers equipped with V-shaped cutting detonating cords.

CIBA systems are capable of cutting mild steel bars up to 30 mm in diameter.

The CIBA system features a mechanism that automatically locks it to the metal bar to be cut.

Several CIBA can be interconnected for simultaneous operation.

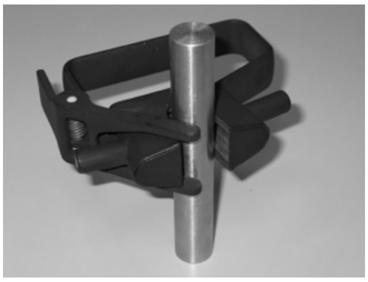


Figure 5: CIBA installed on a metallic bar

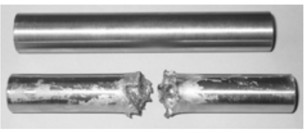


Figure 6: Metallic bar before and after a CIBA is fired

A new generation of high-energy systems

PyroAlliance participates in counter-terrorism operations by making its technological expertise available to European special police units.
PyroAlliance contributes to the development of high-energy equipment designed to enhance the intervention efficiency of special units conducting particularly sensitive and strategic missions.
By proposing rugged, modular and adaptable concepts, PyroAlliance enables special forces to intervene with efficient operational resources.
Through in-depth assessment of the needs of these units, a pragmatic approach and with over fifty years of experience in the field of pyrotechnics, PyroAlliance capitalises on its know-how to propose technological innovations.
The SORMA and CIBA systems have led to the creation of a new generation of anti-terrorist systems better adapted to the needs of special forces units.

Advanced technology for photocatalytic degradation of C/B agents resulted from terrorist attacks

G.Sakovich, V.Komarov, A.Vorozhtsov, S.Bondarchuk
Institute for Problems of Chemical and Energetic Technologies SB RAS, Biysk, Russia
A.Vorontsov, Boreskov Institute of Catalysis SB RAS, Novosibirsk, Russia
S.Bobrovnikov
Institute of Atmospheric Optics SB RAS, Tomsk, Russia
N.Eisenreich, Fraunhofer ICT, Karlsruhe, Germany

The method for degradation of dangerous substances generated from terrorist attacks and man-caused catastrophes is discussed. In the paper LIDAR is suggested for stand-off detection of poison gas cloud. The results of deactivation process mathematical modeling are presented.

Scientific background of protection against terrorist acts and struggle against consequences of man-caused catastrophes implies development of methods of dangerous substances neutralization and destruction to reduce the level of hazardous impact on humans and environment. One of the ways for neutralizing the poison C- and B-agents dispersed in air can be catalytic and photochemical degradation reactions catalyzed by nanosized particles of oxides of TiO_2, etc. Such catalysts can be preliminary produced in stationary industrial devices and then be atomized with the help of gas generators. A different way for nanocatalysts generation is the nanooxides synthesis by explosion or combustion of special energetic condensed systems (ECS). The key issue is that when using the last method the nanocatalysts can be generated in the given point (e.g., in the location of the terrorist attack) and in specified instant of time. Explosion synthesis might be preferable for solution of the problem. First of all the temperatures reached during explosion (~3000÷4000 K) as well as cooling rate of detonation products is maximal, consequently the solidification rates are maximum because of fragments separation high speed (~3000÷4000 m/s). Secondly, under the condition of inclusion of the metal atoms into the explosive’s molecule, primary products of explosion are in atomic state and oxide synthesis is proceed at this level. The following oxide condensation upon cooling provides minimal sizes of synthesized oxide particles. Synthesis of such metal-contained explosives may be conducted via complexing reactions of the urea nitro-derivatives with metal salts.

The UV or visible light energy for photochemical reaction can be taken from the natural sun illumination (day time) or be produced by a special design pyrotechnic charge functioning simultaneously with nanooxide catalysts generation. We investigated problems connected with photocatalytic degradation (oxidation) of carcinogenic and toxic organic substances on the titanium dioxide TiO_2 surface. Experimental and computational results testify to effectiveness of generating nano-sized oxides in air with the aid of combustion or explosion of metal-containing explosives for removal of toxic gases. From the point of view of photocatalysis electronic theory, different metal oxides (e.g. ZnO, MgO, Fe_2O_3, CaO) or their combination with each other or "inert" supports like SiO_2, Al_2O_3 can be used are can be more effective.

One of the important aspects of C-agents deactivation task is the nessesity of preliminary detection of terroristic attack and the assessment of the efficiency of the countermeasures undertaken. In the case of a closed space of a chemical reactor one can monitor the chemical reaction by use of standard means of chemical analysis. However, the use of standard means under real conditions is too problematic because of large scales and fast rates of the actions. In this connection, it obviously becomes quite urgent to consider the application of the means of remote monitoring of the environment that are capable of following up the deactivation process in time and space. Among such means there are laser radars (lidar) for sounding the atmosphere that use standard lasers and photodetectors.

Lidar is an instrument that, in principle, is capable of: 1) detecting a contamination source, 2) to generate the target guidance signal for the means delivering the deactivation load, 3) to control the deactivation process in time and space. Differential absorption and scattering can serve the device capable of remotely detecting and identifying the contents of chemical agents. The differential absorption and scattering LIDARs (DAS-LIDARs) possess the highest operation speed and the largest operative range among known LIDAR detectors of the contaminants. The principle of operation of DAS-LIDARs is in measurement of the difference between the atmospheric attenuation of sounding laser radiation at two wavelengths. For that, two LIDAR returns are compared, one of which is obtained using sounding radiation at a wavelength within an absorption band of a substance of interest and the other one at a wavelengths off this band. The ratio between the on-

and off-line LIDAR returns is related to the absorption coefficient of the substance sounded and thus to its concentration in the atmosphere. In principle, a DAS-LIDAR specially designed for detecting PS in the atmosphere is capable of detecting, during few minutes, a cloud of a poison substance determine its size, location, direction, and speed of its transport in the atmosphere, as well as the distribution of the substance concentration over the cloud. It is important that the minimum detectable concentration of the substances can be about 35mg/m^3 as low, what well fits the minimum PS concentration according to the median lethal dose (LD_{50}).

Mathematical simulation of the processes under study provides tools for description of aerosol cloud evolution and catalytic operation under different environmental conditions. The simulation was conducted on the basis of 3D equations of chemical gas dynamics and combustion.

The results of planned researches are of significant social value from the point of view of searching the effective methods to fight against consequences of different kind catastrophes and terrorist acts. They also lead to developing new knowledge. In particular, it regards elaborating scientific background for purposed production of the metal oxide particles with varied characteristics in the explosion or combustion wave. Catalytic studies are intended to derive new information about the catalyst activity in aerosol and powder suspended state and to compare the oxide performance in different states.

The comparative analysis of efficiency of different schemes of poison gas cloud neutralization was performed on initial volume of generated TiO_2 nanoparticles cloud and characteristic time of poison gas neutralization. Initial volume of generated nanoparticles cloud estimation was performed for the following schemes.

1. Generation by an explosion, when nanoparticles are generated in the process of detonation.
2. Nanoparticles generation in the process of open combustion (under the atmospheric pressure) of the solid propellant containing 16% of titanium.
3. Nanopowder dispersion by means of gas generator on the double-based solid propellant containing 30% of TiO_2 particles with the size of 8 nm (TiO_2 powder of type Hombikat UV-100). The total weight of the working substance was the same as for the schemes 1 and 2.

TiO_2 particles concentration fields are represented on figures 1-3 for schemes 1-3 respectively. Volumes of generated nanoparticles clouds for these schemes are related as 1 : 0.5 : 1.2. It's necessary to note that for all nanoparticles generation schemes the gas phase carrier of the *TiO_2* cloud is represented by the combustion (detonation) products that pushed the initial environment (contaminated air) aside.

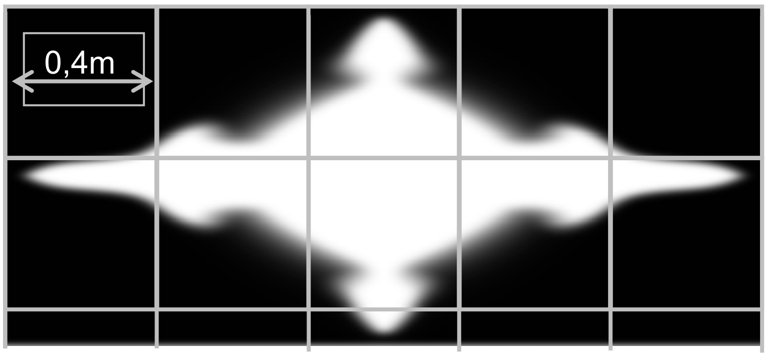


Figure 1: Particles concentration field for scheme 1

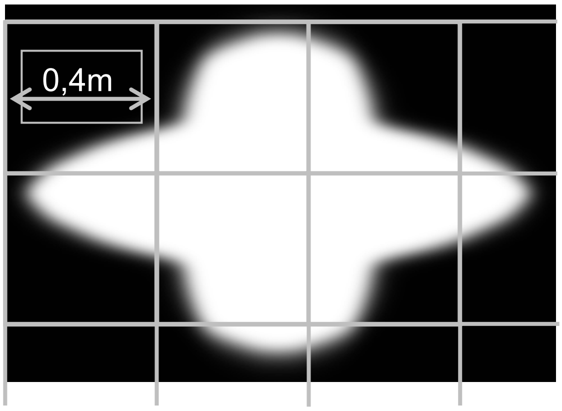


Figure 2: Particles concentration field for scheme 2

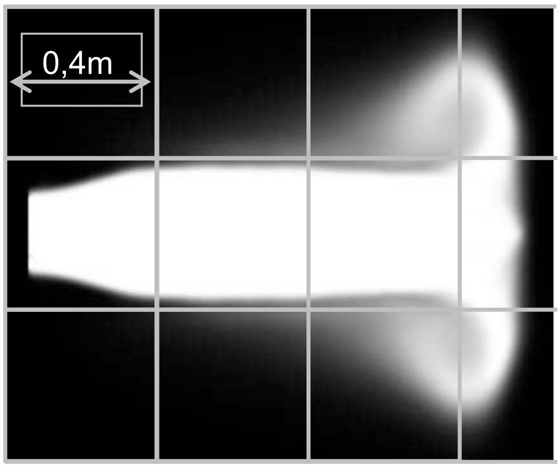


Figure 3: Particles concentration field for scheme 3

Efficiency analysis of contaminant neutralization was performed based on the assumption that photocatalytic activity of the particles is the same, and the rate of contaminant neutralization (concentration decrease) can be estimated by its relaxation time during the interaction with the environment (the same volume for each scheme).

This research was supported by ISTC Grant#3305.

Security Research at Fraunhofer Society: An Overview

Prof. Dr. Klaus Thoma, Speaker of the Fraunhofer Defense and Security Research Alliance, Germany

An overview of the security research activities of the Fraunhofer Society

With the advent of security research in 2004 in the European Union the Fraunhofer-Gesellschaft has also started an internal process in order to get an overview of its security research portfolio. As a result of this process it became clear that roughly half of the Gesellschaft's Institutes are involved in security research activities. The activities span all Fraunhofer alliances with a focal point in the alliances microelectronics, information and communication, materials and components, and defense and security. They can be loosely grouped into the following key technology areas:

- **Security in information and communication** (IT for security; IT-security; communication to provide security)
- **Crisis and disaster management** (communication and monitoring systems for rescue and emergency teams; support and decision management tools, planning tools, situation awareness tools; simulation; logistics and traffic; search and recovery)
- **Multi-sensor detection and identification for surveillance and intelligence** (sensor networks; information/data fusion; surveillance; access control; authentification)
- **Detection and monitoring of CBRNE and dangerous goods** (stand-off detection of explosives; laser-spectroscopy and new laser sources; molecular imprinted polymers; teraherz to detect weapons and dangerous goods; bio-sensors for monitoring of drinking water; IR-sensors; NMR-Sensors)
- **Robotics** (special robot kinematics; flexible grabbing systems; robust and secure electronics to guarantee reliability; intelligent navigation functions; secure human machine interfaces; real time 3-D object recognition; tracing and interpretation; swarm intelligence)

- **Materials** (protection against blast and fragments; intelligent materials and embedded sensors; self healing materials; multifunctional explosion resistant materials; health monitoring of buildings; fire suppression with ceramic foams and special coatings

- **Risk analysis and risk management** (risk maps for cities, districts, countries, and Europe; threat analysis and vulnerability analysis; technology monitoring)

Fraunhofer innovation clusters: The cluster Future Security BW

The effectiveness of an innovation process depends decisively on efficient cooperation between development and production. For this reason, it is important for providers of research and development services to work in close collaboration with industry. The Fraunhofer-Gesellschaft is the largest provider of R&D services in Europe and as such strongly promotes this form of networking. In areas of technology with high innovation potential, companies and research institutions are brought together to form innovation clusters, with the support of the federal ministry of education and research (BMBF). The Fraunhofer-Gesellschaft’s political mandate for the sponsorship of regional clusters originates from resolutions adopted by the Bund-Länder Commission for Educational Planning and Research Promotion in November 2004 and June 2005 concerning the “Pact for Research and Innovation” and the initiative for excellence at institutions of higher education.

The Fraunhofer-Gesellschaft regards security research as an important and innovative topic and is thus currently in the process of setting up a security cluster. The regional focus of the cluster is in the state of Baden-Württemberg and involves 6 Fraunhofer Institutes from the cities of Karlsruhe and Freiburg, 20 Partners from Industry, 4 Universities (Freiburg, Karlsruhe, Stuttgart and Tübingen), and Institutes from Max-Planck and Hahn-Schickard-Gesellschaft.

At the moment the cluster has the following focal areas:

- Robust Sensing Walls: Development of mechanically robust sensor networks for the application in civil engineering materials and the development of innovative measures for the protection of critical infrastructure against explosions.
- Detection and identification of explosives and biological substances: Development of new technologies for the detection

of explosives, dangerous chemical substances as well as micro-organisms, viruses and toxins.

- System integration: Development of generic concepts for security systems architectures of the future.

These technical areas are accompanied by a fourth focal area "Security & Society" with the aim of investigating ethical, legal, socio-economic, psychological and societal effects of security technology on the public and the individual; demand and potentialities research.

Automation, Process Control and SCADA Systems in Critical Infrastructures – Future Threats and Requirements

Hans Honecker (Federal Office for Information Security BSI), Germany

Abstract:

Critical infrastructures provide indispensable and essential goods and services to society.

On the one hand complexity and interconnection of critical processes increase as requirements concerning their availability do – even with regard to extreme operating conditions. On the other hand these processes are put at risk by an increasing variety of threats within the full range from architectural caused technical or human failure to natural disasters or deliberate malicious acts.

To counter those threats appropriately, future technologies and their technical implementation in critical infrastructures have to meet new fundamental requirements. Future critical process infrastructures need to be more robust and flexible than they currently are.

This contribution will use the example of IT based automation and process control technology to show the increasing threats and name generic requirements to future automation and process control technology and systems. Generic requirements will be proposed for all technical layers of specialised IT-based automation and control systems as well as for control system network layer (architecture and technology), operating systems, database systems and other necessary applications. These have to be carefully integrated into an overall resilient infrastructure.

Critical Infrastructures and Critical Processes

Critical Infrastructures provide indispensable and essential goods and services to society.

Both our society and economy are increasingly depending on critical processes, which are also heavily interdependent. Thus critical processes in the future need to be built in an even more robust and resilient way than they already are today – at least in their critical core functionality. The risc of major or enduring impairment of society or economy through failure or severe malfunctions must be kept low, in spite of the growing technical complexity and new threats to critical infrastructures.

From the community perspective in the end there is no difference whether the necessary resilience of critical processes is achieved by a resilient design of the process itself or of the underlying critical process infrastructures. From the viewpoint of protecting critical infrastructures securing critical processes needs a holistic approach which will lead to a set of additional requirements.

This contribution will use the example of IT-supported automation technologies to discuss the challenges on the process layer as well as on the different layers of critical process infrastructures, and to derive proposals for future developments.

Critical Processes and IT-based Automation Technologies

Automation technologies including all types of process supervision, process control and grid control technologies are present in critical process infrastructures of electricity generation and distribution, gas and water supply, and process infrastructures of other critical infrastructures. They are used on virtually all layers of control of these processes. In most areas of automation the technologies cannot be thought of without the use of components based on information technology. This development will continue in the future.

As a general rule operational conditions for the use of IT-based automation technologies considerably differ from those of common information technology.

IT-based automation technology	**standard information technology**
continuous operation	operation during business hours.
top priority for availability	top priority for confidentiality and integrity
(physical) process has priority	information security has priority
specialised IT serves to control physical processes	standardised IT serves to process information

Since in this contribution for the *Future* Security we put the main focus on future challenges, we mainly consider requirements which up to now are not discussed to such an extent. As a base we presume that IT security according to today's state of the art standards is implemented.

Future Threats

To explain the future requirements we are going to set up we exemplarily list some threats for automation technology in critical process infrastructures. These are of ever-growing importance and it is necessary to take them into account for critical process infrastructures we currently build, rebuild, or plan to do so.

With regard to possible consequences of failures and malfunctions inter alia the more and more extending interconnection between critical process infrastructures of the same type (as in electricity distribution grids) and the increasing dependencies and interdependencies of different critical processes are of great relevance.

category	**threat (example)**
technical failure and human error	technical malfunction (Example: Programming errors in a distributed control system (DCS) were one cause, that necessary measures in the early stadium to mitigate the disaster of the US blackout 2003 were not taken)
natural disasters and phenomenons	increasing number and weight of natural disasters and weather phenomenons a “direct hit” by a solar storm may cause severe damages cooling problems in energy generation and operation of IT during long-lasting periods of heat and drought
attacks	risk of “cyber attacks” on critical infrastructures • hacking (Example: A penetration test of a US-based electricity provider led from the internet as far as into the process control network and the control system) • trojan horses: in case of an insufficient separation of automation networks, specific and dedicated malware may be placed in automation infrastructures and may put them at risk
breakdown or failure of other critical infrastructures	breakdown or failure of other critical infrastructures (e.g. basic infrastructures as supply of electricity or telecommunications) may impair other processes. This is no new threat, but due to the increased dependence has to be considered better.

Future Requirements

Particularly with regard to new or further development of technologies that are meant for use in critical infrastructures, we must take into account some additional aspects much more than today. At all layers of technology as well as when integrating technologies to create process infrastructures in the future the following aspects should be considered more carefully:

- necessary conditions for long term maintenance and service – keep open paths for system migration
- robustness and resilience as important design criteria
- options for minimisation – inbuilt graceful degradation to keep up core functionality even under crisis or disaster conditions
- minimised or minimisable energy consumption – inter alia as precondition for operation during blackouts or electricity shortages
- avoiding of functionalities that can endanger process infrastructures or do not contribute to the process
- explicit suitability for use in critical processes and automation infrastructures (qualified by manufacturers product specification)

The following table lists a few examples, that are more specific to different layers of process infrastructures:

layer	**requirement (example)**
process specific applications and application software	• largely platform independent (with regard to operating system and database layer) • robustness and resilience of sub-processes against failure and malfunction; modes for operation during crisis or extreme conditions (graceful degradation) • complete documentation of any communication relationships needed or used by the application • independent analysis of security, safety, correctness
standard software	• secure and/or minimisable installation • communication only to specified systems • offering standard functionality without security risks
operating systems	• minimisable functionality • feasible methods for system hardening • long term availability perspective (decades) • no functionality that could put infrastructures at risk
hardware	• physical robustness (e.g. industrial electro-magnetic environment; extreme solar activity)
network technology	• consequent restriction of communication to necessary connections (restrictive switching, port security, etc.) • feasible management of restrictive network operation

Transfer to other IT-supported Technology Areas

Many of the above requirements and findings can be transferred to other technology areas in which information technology is widely used for operating critical processes. As examples of particular importance we would like to emphasise the future requirements for process specific applications, operating systems in general and the special requirements for the network layer. Furthermore many of the future requirements are also valid for less critical processes.

Conclusions

Basically today’s process infrastructures using IT-based automation technology can be built as secure and safe as necessary. With regard to increasing threats on the one hand and to the ever growing complexity of the process infrastructures on the other hand, robustness, inbuilt resilience, and security characteristics of all concerned technology areas and layers need to be considerably enhanced. To achieve this all involved parties – be it process owners and operators, integrators of the different technology areas, or manufacturers, distributors and vendors of components – should collaborate in an intensive and consistent way, if necessary with support of public organisations.

New Research Dimensions for the Formal Analysis of Critical Information Infrastructures Security Requirements *

Dr. Syed Naqvi, Research Fellow, E-Science Systems Research Department, STFC Rutherford Appleton Laboratory
Chilton, Didcot, Oxfordshire OX11 0QX, United Kingdom

Abstract

Global connectivity of computing and storage resources opens up the possibility of sabotaging and misusing information to a degree never seen before. The exponential growth in the scale of distributed data management systems and corresponding increase in the amount of data being handled by these systems require efficient management by maintaining consistency, ensuring security, fault tolerance and good performance in terms of availability and security.

Achieving high confidence in security design requires the use of adequate modelling techniques. Goal-oriented requirements engineering methods such as KAOS support this by allowing the security analyst to capture of goals (in particular security properties), to model assets, to discover threats (or security anti-goals) and address them by operational security requirements enforced by responsible components. This analysis can be refined down to a formal level, supported by model-checking tools.

However, a comprehensive analysis of security requirements of critical information infrastructures (CII) requires additional parameters such as risk analysis, analysis of data isolation techniques, forensics, etc.

In this paper, we present our approach to integrate those new dimensions in KAOS for the formal analysis of security requirements. A Grid-based Data Management System (GDMS) is used as a case study in this work. Holistic view of the requirements model is presented to highlight the role of each new dimension in the comprehensive security requirements analysis of GDMS.

Formal Analysis of Security Requirements:

Formal analysis is based on the mathematical techniques for the specification, development, and verification of a system under consideration. This analysis though inflicts higher design costs yet it is desirable to enhance the reliability and robustness of any design in general and of high-integrity systems in particular. Security requirements are widely used in the modern system designs where resources are generally placed beyond the administrative control of the majority of the stakeholders. Moreover, the complexity of such highly scalable architectures makes it impossible to evaluate its security requirements by *simple examination*. This situation leads the security designers to opt for the formal techniques for the analysis of the security requirements of their designs.

Formal techniques widely used for security requirements analysis include KAOS [1], I-STAR [2], and TROPOS [3]. We have chosen KAOS for this work as it is comparatively more adaptive for the new dimensions without loosing its core methodology. We have employed Grid Data Management Systems (GDMS) as a case study to show the advantages of adding new dimensions in the existing ones.

KAOS:

KAOS treats requirements as a federation of four models namely goal model, responsibility model, operations model, and responsibility model. They collectively form a requirements model of the system under investigation. The desired system property (security in our case) is treated as *goal* in KAOS. Goals are structured into directed acyclic graphs, which ensure that analysts justify more strategic, high-level goals with at least one other goal that explains why the high-level goals are in the model. Goals can be refined as a collection of sub-goals that describe how to reach the refined goal. Verification, validation and conflicts resolution techniques for the goals have also been developed. The goal model also allows the analyst to capture and structure anti-goals which are the dual of goals, wished by malicious agent working against the achievement of system goals. The security related anti-goals are called threats. KAOS has been applied successfully to specify the goals and requirements in over 30 industrial projects in domains ranging from aerospace to publishing.

Grid Data Management System (GDMS):

Grid data management systems offer a common view of storage resources distributed over several administrative domains. The storage resources may be not only disks, but also higher-level abstractions such as files, or even file systems or databases. In this paper, we extend our previous work on modelling of security requirements of grid data management systems [4] where we addressed issues related to storage management policies by modelling security requirements at the application level, and the requirements on mechanisms for using storage semantic web services. In this paper, we extrapolate the existing

* This research work is supported by the European Network of Excellence CoreGRID (project reference number 004265). The network aims at strengthening and advancing scientific and technological excellence in the area of Grid and Peer-to-Peer technologies. The CoreGRID webpage is located at www.coregrid.net

dimensions [5] to effectively address the security requirements of critical information infrastructures.

New Research Dimensions:

This section elaborates the set of three new dimensions that we have identified and worked on their applicability in the formal security requirements analysis of critical information infrastructures.

Risk Assessment

We define risk assessment as a mandatory step for adequately addressing the threats within the critical information infrastructure [6]. Risk assessment includes the analysis of consequences and probability of occurrence. The former can be estimated using a priori knowledge about the presence of a vulnerability, the ease to exploit it and attack figures from honeypots. The later is related to the strategic importance of the broken goal. In the goal oriented approach, those figures can decorate the security requirements leaves and can be propagated up to more strategic goals for taking security design decisions among possible alternative (and the related costs) to address them. This second step involves considering a number of risk mitigation actions which in proper combination will reduce the risk to an acceptable level given possible drawbacks in terms of performance, usability and costs. Among other models, Defect Detection and Prevention (DDP) [7] developed by NASA can also be employed for risk analysis.

Data Isolation

Data confidentiality is an indispensable requirement of commercial organisations. However business also requires sharing data. Controlling the balance between those is critical and requires appropriate model depending on the context. The proven role-based access control can reach its limits in context where the conflict of interests plays significant role in the overall organisational datasets security strategy. Sound security assurances are sought by these organisations before even thinking of the *externalisation* of resources. Alternative models such as the Chinese wall [8] can help here to formalise dynamic data isolation as a security requirement of critical information infrastructure.

Forensics

We need to include this dimension to handle the post-attack scenarios. Forensics techniques should be powerful enough to trace the point(s) where security breach took place. We treat a security breach as a failure of dealing with the security requirements e.g. lack of envisioning a comprehensive set of security requirements; failure to properly address the envisaged security requirements, etc. We propose the use of events monitoring and distributed honeypot [9] to obtain information about the malicious entities.

Conclusions

This work presents our idea of extending the existing range of security requirements parameters to effectively address the security requirements of critical information infrastructures (CII). Due to its inherent large scale, dynamic and complex nature; CII security requirements analysis requires enrichment of the conventional set of security requirements parameters. In order to make CII dependable systems, we need to include reliability indicators to mitigate the risks. Likewise, we need to endow with confidentiality assurances by providing data isolation. Finally, security requirements model of CII should also encompass the post-attack scenario by providing the traces of events that lead to the accident.
This work is still in progress and a number of other issues for future research remain open.

References

1. Dardenne A., Lamsweerde A. and Fickas S., *Goal-Directed Requirements Acquisition*, Science of Computer Programming Vol. 20, North Holland, 1993, pp. 3-50
2. Yu E., ‘Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering’, Proceedings of the 3rd IEEE Int. Symp. on Requirements Engineering (RE'97) Jan. 6-8, 1997, Washington D.C., USA. pp. 226-235.
3. Bresciani P., Giorgini P., Giunchiglia F., Mylopoulos J., Perini A., ‘Modeling early requirements in Tropos: a transformation based approach’, Second International Workshop on Agent-Oriented Software Engineering (AOSE-2001). Montreal, Canada, May 29th 2001.
4. Naqvi S., Massonet P., Arenas A., 'Security Requirements Model for Grid Data Management Systems', Lecture Notes in Computer Science (LNCS 4347), pp 30-41, ISBN 9783540690832, 2006
5. van Lamsweerde A., *Elaborating Security Requirements by Construction of Intentional Anti-Models*, Proceedings of ICSE’04, 26th International Conference on Software Engineering, Edinburgh, May. 2004, ACM-IEEE, pp 148-157.
6. The European Project ASSESSGRID – www.assessgrid.eu
7. Feather M., Cornford S., Dunphy J., and Hicks K., ‘A Quantitative Risk Model for Early Lifecycle Decision Making’, *Proceedings of the Conference on Integrated Design and Process Technology*, Pasadena, California, June 2002.
8. Brewer D., Nash M., ‘The Chinese Wall security policy’, Proceedings of the IEEE Symposium on Security and Privacy 1989, 1-3 May 1989 pp 206 - 214
9. Yang G., Rong C., Dai Y., *A Distributed Honeypot System for Grid Security*, Proceeding of the Grid and Cooperative Computing 2003 (GCC2003), Shanghai, China, 2003, pp 1083-1086

Airport Security Management
Frankfurt Airport – An Overview

Volker Zintel (Executive Vice President Airport Security Management, Fraport AG)
Germany

Key information

Frankfurt Airport is Germany's biggest airport. In terms of cargo, it ranks on first place in Europe and on seventh place in the world. In terms of passengers, Frankfurt Airport ranks Europe wide on third place, worldwide on eights place. The airport is operated by Fraport AG. The majority of the airport operator's shares are held by the city of Frankfurt and the state of Hesse. The other shares are distributed among the Deutsche Lufthansa AG, Julius Bär, Capital Group, Artisan Partners and in free float. 129 airlines operate to and from Frankfurt Airport. They fly to 307 destinations in 109 countries. Additionally, Frankfurt Airport is the home base of Deutsche Lufthansa AG. The Lufthansa share in seat supply makes up 60%, together with its Star Alliance partners, it amounts to 70%. But not only air traffic is important at Frankfurt Airport. In order to give our customers the best connection alternatives, we have put our intermodality concept into practice: Our airport has two train stations, one for regional and one for long distance trains, and we are situated right beside two highways, A3 and A5.
As an employer, Frankfurt Airport is very important as well for the Rhein-Main-area. About 70.000 people are employed not only at the airport operator and airlines but also by logistic companies, shops, hotels, restaurants etc.

Airport Development

Currently there are considerable airport expansions being planned. The airport's expansion strategy envisions a fourth runway by 2011 and a third terminal by 2013. The investment volume for these expansion activities makes up 3,4 billion €. But Fraport AG does not only invest in the expansion program but also in renovation of the existing facilities, in security measures, fire prevention, retail and many more. Additionally, new sites are developed: For example, hangars for the newly developed Airbus A380 are being built, the building of the Airrail Center, a nine story office and commerce building on top of the long distance train station, has started and the Mönchhof Site will be developed into an office and cargo site.

Airport Security – Factual Environment

At Frankfurt Airport, each day, not only the aviation business but furthermore, a small town is to be managed: There are 145,000 passengers daily, 30,000 employees, 15.000 meeters and greeters as well as 3,000 visitors to be taken care of daily. Each day, 5,600 tons of cargo 265 tons of airmail are to be managed. All this is makes up 1,341 flight movements per day.
For all users, be it airlines, hotels, shops and their employees, passengers, visitors or others, the highest reasonable security level has to be guaranteed.

Airport Security – Legal and Commercial Environment

Our legal environment is mainly determined by the German Aviation Security Act. The act assigns specific tasks, such as passenger and baggage screening or reliability verifications, to the public authorities. Other security related tasks, such as access control to operation areas or employee screening prior to access to critical parts, are assigned to the airport operator. The airlines are responsible for the security of freight, airmail and catering that are in their sphere of influence.

The security measures in responsibility of the public authorities cost about 150 million €, the measures in responsibility of Fraport AG make up to 70 million € and others, such as airplane and building fire protection, make up to 20 million € per year.

Altogether, our processes at Frankfurt Airport are essentially dominated by numerous security regulations, frequent new requirements and difficulties in implementing them organizationally, constructionally and in educating our staff accordingly. Current examples are the separation of passengers or the new liquid regulations. Additionally there are strict audits by the authorities in order to supervise the proper enforcement of the security regulations.

Our Challenges

Security at Frankfurt Airport faces various challenges each day. These are not only relating to ever new regulations but also to the airport's size and complexity, to numerous companies working at the airport, crime and emergencies.

Size of and Access to Frankfurt Airport

The area of Frankfurt Airport amounts to 19.6 m², which compares to the size of downtown Frankfurt. This property is surrounded by a fence of 31 km in length. The airport's secured areas are additionally protected by a 20 km long fence. There are 48 controlled entrances to the secured areas, where vehicles and employees are controlled when accessing the secured areas. In the terminals there are currently 29 control posts for passengers and their hand baggage.

But not only airlines' and the airport's employees or passengers have access to the operational or the security areas. There are, as well, construction and other service companies whose staff need terminated or even unlimited access to the airport. So, there are currently 91,000 Airport Access Passes in circulation. Amongst them 73,000 personal Airport Access Passes, 8,500 driving permits for the operational area and/or on the tarmac, 1,500 key cards, 1,000 transferable Airport Access Passes and 7,000 transferable driving permits.

Crime and Emergencies

According to the huge number of people using and working at the airport, there are many risks resulting of crime, accidents, emergencies and other incidents resulting of human behaviour.

In 2006, 446 cases of cargo burglary, 209 cases of mail burglary, 1452 stolen bags and 15 bodily injuries were reported. Additionally, traffic accidents, injuries caused by dangerous goods, airplane accidents and even death are to be handled. Other harassments are acts of terrorism, such as airplane hijackings, explosive assaults (e.g. the Lockerbie assaults in 1985) and suicide assaults (e.g. the attacks on the former World Trade Center in 2001).

As a result of these and other incidences, Frankfurt Airport Security has had 131,451 alarms in 2006. The fire brigade has had 18,067 alarms and rescue services have been called 25,159 times.

Most challenging are still the humans lingering at the airport as each of them can be a potential victim of burglary or injuries or even be a potential criminal offender. Fraport AG, as the operator of Frankfurt Airport and provider of airport security, has to guarantee the highest reasonable security for all airport users. In this context, the conflict between highest possible customer satisfaction and highest security standards has to be handled each day.

Our Solution: Security Network

Altogether, 9,500 people work daily to guarantee security at Frankfurt Airport.

Together with all agencies and companies that are engaged in security matters at Frankfurt Airport, Fraport AG has established a security network which unites the competencies of all involved parties, be it the public authorities, the Airport Security department, the Fire Fighting Department and the rescue service of Fraport AG, the airlines or others under the roof of one Security Control Center. Here representatives of all partners are present in order to coordinate all significant security processes in a most ideal and effective way on behalf of all parties.

The key role of information systems for the security of critical infrastructures

José Esteban, Atos Origin sae – Albarracin 25, 28037 Madrid, Spain; jfernando.esteban@atosorigin.com
Thomas Usländer, Fraunhofer IITB – Fraunhoferstr. 1, 76131 Karlsruhe, Germany; uslaender@iitb.fraunhofer.de

Abstract

This paper focuses on the critical role of IT systems for the security of critical infrastructures. In particular, current paradigms for IT systems, such as service-oriented architectures, are considered, with special attention to the main requirements to be satisfied. Security planning and response phases are considered, distinguishing the specific requirements that they impose on an IT system.

Introduction

The improvement of European capabilities for securing critical infrastructures requires multidisciplinary research in several areas: sensor networks, data fusion, automated analyses of temporal and spatial changes, etc. The main objective is twofold: the increase of prevention capabilities and the improvement of response activities.

This involves the acquisition, processing, storage, retrieval, fusion and communication of large amounts of information at different temporal and spatial scales, with challenges like covering wide areas with the maximum possible resolution, combining airborne and satellite data with terrestrial data or combining basic information (infrastructures, topography) with detailed and more rapidly changing information (temperature, motion).

Such information is produced and owned by a wide range of organisations which need the necessary IT framework to achieve interoperability (successful exchange and use of information), while guaranteeing security and business requirements (i.e., ensure that the right information is delivered to the right person/institution for a specific use and for a given price).

The role of information systems for the security of critical infrastructures

As in many other application fields, information systems allow organisations to increase their efficacy and efficiency by providing the technological means to acquire, store, process, distribute and exploit all data and information which is core to their activities and objectives. In the following sections we develop on this key role of information systems as enablers, and focus on the requirements and criteria which are more relevant for the protection of critical infrastructures.

Information systems as enablers

In an era characterised – among others – by constant changes, uncertainty and what many consider an overflow of information, information systems play a key role as enablers. They allow organisations to optimise the acquisition of information (from external and internal sources), its maintenance and its exploitation according to the mission and objectives of the organisation. In a nutshell, organisations cannot fulfil their mandates and objectives without information systems.

In the domain of security, these systems have to play this role while satisfying a number of requirements and criteria which are, in general, quite more stringent than in other domains for obvious reasons.

General requirements and criteria

In this section we examine a number of important requirements and criteria which an IT system must satisfy in the security domain.

Coping with technological uncertainty

As we have already highlighted, an effective information system provides a solid foundation for an organisation, and in particular actors and stakeholders in the security domain, to meet its objectives, improve its performance and cope with an uncertain environment.

However, another important aspect is technological uncertainty itself. Technology shows increasingly short life cycles, so it is very important that modern information systems are designed for change so they can evolve and adapt to the changing technological environment. Otherwise, they would limit or hinder the performance of security actors and stakeholders, and also force them to invest significantly higher amounts in the replacement or adaptation of their information systems.

Flexibility and adaptivity

A recent and powerful paradigm for IT systems is that of Service-Oriented Architectures (SOA), which – among others – enables re-use of services, elimination of redundant work and investment, higher flexibility for designing, developing and modifying applications, and faster delivery.

These requirements, as well as others such as technological uncertainty, make it necessary to define architectures for IT systems which are technology- and policy-independent, so that the architectural principles that will enable the system to be flexible and adaptive are decoupled from current – and probably quickly changing – paradigms. This abstract architectural design can then be mapped and further defined to a given technology and/or organisational policy of choice for the design and development of the specific system.

An interesting architecture following this philosophy has been created for the European risk management domain in the ORCHESTRA Integrated Project, co-funded by the European Commission’s DG INFSO under FP6, and led by Atos Origin (http://www.eu-orchestra.org)

Interoperability

Not only considerable amounts of information are necessary to implement security activities for the protection of infrastructures, but this information originates from varied sources and has to be processed and distributed to a wide range of institutions. Therefore, interoperability – defined by IEEE as “*the ability of two or more systems or components to exchange information and to use the information that has been exchanged*” – is a fundamental requirement for information systems in the security field. Interoperability must be understood in a wide sense, comprising the organisational level (common or compatible objectives and procedures), technological level, syntactic level, semantic level, etc.

A basic starting point for interoperability is compliance to existing standards. Although it does not guarantee interoperability, it is a *sine* *qua non* condition to achieve it. A variety of standards must be considered in this framework: ISO, CEN, W3C (in case web services are used), OASIS (structured information standards), etc. In addition, in the field of security there are significant amounts of geospatial information, so OGC standards must be considered, as well as the INSPIRE European Directive for geospatial data harmonisation.

Security of IT systems

The security of IT systems themselves is of paramount importance for security applications. In addition to all security aspects related to the information managed by the system, IT systems must be robust, fault tolerant, resilient and at least partially redundant at physical and logical levels. Special attention must be paid to fast recovery mechanisms, which are particularly critical for security applications and for environments in which numerous institutions have to cooperate at international level.

Respecting stakeholders' missions

While satisfying all necessary requirements, an IT system must respect the mission and work processes of stakeholders. In the field of security, the protection and secure exchange of data and information are critical for the success of institutions and their operations. Apart from the considerations in the previous section, interoperability must be enabled for effective exchange of information while providing efficient mechanisms for security (user profiling, authentication, restricted access, data encryption). A current research area of interest to complement these measures is Digital Rights Management (DRM), which has originated in the commercial audiovisual domain but has important applications for security.

Prevention and response phases

From the perspective of IT systems, the distinction between the prevention and response phases has blurred due to the use of planning and assessment information during the response to crises and, conversely, to the use of response information in the prevention of future crises (for example, the update of prevention information and models or the post-mortem analysis of crises and response operations).

The key difference between phases resides however in the availability of IT systems during crises (power failures, communication breakdowns, etc.) and the need for real-time response. Contingency measures may be put in place in order to reduce the former, but the risk cannot be eliminated or neglected. Still, in a worst case scenario in which IT systems are locally inexistent or unavailable, neighbouring and remote IT systems may be used to produce relevant information that can be delivered through command and control centres and alternative communication means. Real-time response may be achieved by pre-processing of potentially relevant information during the prevention phase, or by optimising and prioritising requests and applications.

Conclusions

Effective IT systems lie at foundation of successful security applications and operations. Those based on the SOA paradigm may satisfy the main requirements posed by the security domain (and in particular for protecting critical infrastructures) if they are designed for change, flexible, interoperable and secure themselves (robust and resilient). If designed adequately, they can play a key role both in the prevention and response phases. Due to the amount of geospatial information in the security domain and its basic function in security applications, attention must be paid to the latest architectural developments, standards and regulations in this field.

Human Factor Aspects in Crisis Management and Critical Incident Management

Markus Bresinsky and Harald Schaub
{bresinksy | Schaub} @iabg.de, IABG mbH, Germany

Introduction

When one looks at some of the typical problems people have to deal with and often complain about in crisis and incident management one finds that these relate to the task of reducing complexity to comprehensible and operational dimensions. Namely, these refer to

- Finding and defining problems
- Choosing solvable problems among the host of existing problems to work on
- Combining "intuition" and "rationality" in decision making
- Tolerating ambiguity and coping with unexpected events
- Finding appropriate measures to handle novel situations
- Coping with stress and time pressure

The challenges people are facing are a result of the characteristics of their working environment. As a result of the internationalisation of formerly secluded national economies and in response to the stiff international competition these environments have changed considerably. In a broader sense, their general features can be described by using the following categories:

- Complexity: The environment consists of a large number of important aspects and "players" that influence each other in complicated ways. The environment thus constitutes a network of variables. One of the important consequences of this network-like feature is that there is no possibility "to press just one button". Each and every attempt to influence single variables causes waves in the whole network; each action may lead to the desired main effect but may also result in unexpected long-term and side effects.
- Novelty: One never knows all aspects of the environment; one never is able to learn about the motives and moves of all the

"players on the board". This means that the problem at hand remains at least partially intransparent and decisions must be taken under uncertainty. This also means that there are only small possibilities for the routinization of everyday work since new - and important - aspects will frequently require changes of routines.

- Dynamic: The working environment of the manager changes constantly. When one is solving chess puzzles, the situation on the board doesn't change and one thus is in the position to do as much analysis and ramification as seems necessary. Complex problems change on their own and not only the figures on the board move but also the rules of the game may be constantly redefined. One thus hasn't enough time for knowledge acquisition and analysis; one hasn't enough time for soberly calculating the risks and stakes of decisions which adds time pressure to uncertainty.
- Unclear goals: In many cases the goals one strives for are way too global to be used for planning. What exactly does it mean to create an "unpolluted environment" or a "sound company"? However, in complex working environments, it often turns out that it is difficult to decide on the concrete meaning of such goals because part goals may be contradictory and can not be achieved at the same time. For instance, it is not possible to reduce labour costs and create as many job opportunities as possible.
- Risky measures: Complex working environments know of few routinely available and safe measures. Since the situation changes constantly, what seemed right yesterday may lead to disaster today. Therefore, one has to repeatedly check the actual effects of implemented measures analyse desired main-effects and undesired long-term- and side-effects and should prefer such actions whose effects are reversible in the case of an unexpected emergency.

Basic Assumptions and Error Tendencies in Crisis Management and Critical Incident Management

Many of the inadequate features of overt behaviour in crisis and critical incident management are manifestations of a limited number of action patterns, basic assumptions and attribution tendencies that are critical psychological determinants of action regulation under conditions of uncertainty and complexity. They have a functional appeal for the problem solver in that they avoid uncertainty, convey a sense of mastery, and therefore make problems of apparently overwhelming difficulty manageable. These determinants sometime results in specific errors. Three basic error types are related to levels of performance. Slips and lapses are related to the skill-based level, mistakes to the rule-based and knowledge-based level of behaviour.

There are some psychological factors that characterise the difficulties people have in dealing with crisis and critical Incidents.

- There are no Contradictory Goals
- My View of the World is Correct
- Developments are Linear and Monotonic
- Demonstrate your Competence
- There is not Need for Self-Reflection
- All Important Issues are on my Control-Panel
- Consistently Keep to Your Plans
- Don’t Blame Me for Mistakes

The political dimension of crisis management

Processes of crisis management are also influenced by political interests, agenda, and power. In most cases of disasters political elites seek to influence the course of action in favour to their public support. This kind of decision making is not influenced by problem solving with regard to the urgent needs of consequence management but by the impression management of the political decision makers. Therefore, the analysis of the human factor in critical incident management needs also to take into account the political dimension of decision making.

Concluding remarks

We have shown some shortcomings people have in managing crisis and critical incidents. We have the impression that the often people lacked neither expertise nor motivation. Dealing with complexities in critical situations has a strong psychological component and that psychological factors should be taken into account. This means to be aware of the different traps of crisis and critical Incidents, and to recognise the different managerial dilemmas one has to find one's way through.

References

- Bresinsky, M. & Kluwe, R.H. (2003). The Political Actor Simulator (PAS). In: Detje, F., Dörner, D. & Schaub, H. (Eds), The Logic of Cognitive Systems. Proceedings of the Fifth International Conference on Cognitive Modeling, 33-38: Bamberg.
- Dörner,D. & Schaub,H. (1994). Errors in Planning and Decision-making and the Nature of Human Information Processing. Applied Psychology, 43, 433-453
- Ramnarayan,S. & Strohschneider,S. & Schaub,H. (1997). Trappings of Expertise and the Pursuit of Failure. Simulation & Gaming, 3 (in Press).
- Schaub,H. & Strohschneider,S. (1997). How Managers deal with Strategic Complexities. In: Ramnarayan,S.&Pandey,I.M.(Eds), Strategic Management of Public Enterprises in Developing Countries: New Delhi: Sage.

Situation Awareness – In Advance

Dr. Joachim Stamm (Plath GmbH)

Abstract

Lots of systems and techniques in security research deal with detection or observation of potential risks on site. In this presentation the aspect of effective information gathering and intelligent analysis of information is described to get hints for possible dangers in advance to "stay one step ahead".

Situation awareness on site and in time

For the security of critical infrastructures or security at public mass events in most of the discussions the aspect of explosives detection or effective access control is one of the main topics. Gas sniffing and/or automated video observation are only two of the possible techniques, which are taken into account. All these arrangements are disincentive to possible terrorists and try to detect the danger on site.

To protect every single element of critical infrastructures these systems have to be installed at every site at risk, which may result in an enormous amount of installations. For example there are about 5500 railway stations in Germany or 280 suburban railway stations in Hamburg. In addition these systems will provide increased security only against known threats, because only well known threats can be detected automatically (e.g. face recognition of known terrorists by automatic video analysis or sniffer for explosives of a special kind). Therefore manual control and an increased number of security personal are necessary to protect possible targets.

To manage the assignment of resources or initiate special provisions any indication of increasing risk potential in advance would help. This indication might be an abnormal behaviour in the surrounding area of events or observed sites or unusual activities of potential terrorists.

Situation awareness in economic system and intelligence services

For decision support in business environment the analysis of large amount of data with respect to different aspects can be summarized with the concept of business intelligence. Here business data - customer data,

buying patterns or information about stock turnover – are analysed to optimise business processes or predict customers buying behaviour.
In intelligence services or military reconnaissance organisations in our day methods according to business intelligence are adapted for communication intelligence. Here an analysis of the communications behaviour takes place. For example an indication for abnormal behaviour can be derived from detailed analysis of communication participants, statistical analysis or automated comparison to standard behaviours.

As long as this analysis is not based on the content of telephone calls or other recorded information, but based on the describing parameters of every single communication – the so called Meta Data - like e.g. place, date, time and method of communication, the methods of analysis and evaluation can be adapted as well to other fields like security.

And similar to the field of communication intelligence (COMINT) in military reconnaissance also in the security field with an increasing number of sensors and with the automation of information gathering the amount of data to be analysed increases every day.

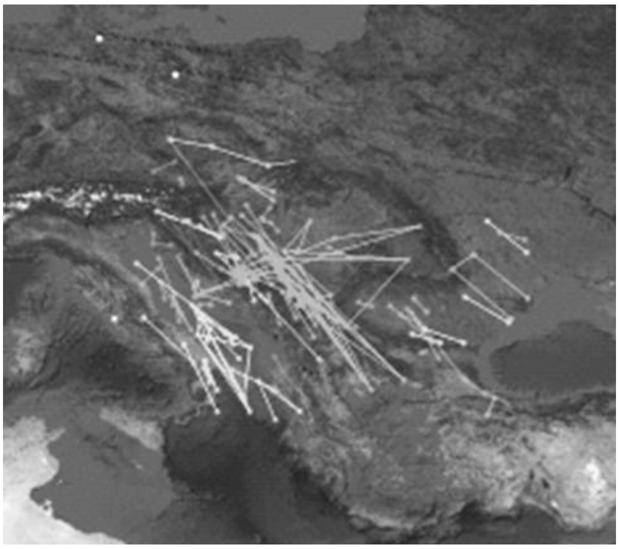
Automated mass data analysis with an explorative approach and interactive computing

To get any decision support to initiate special provisions this large amount of data and information has to be analysed in an efficient way. The main three aspects for an efficient analysis process are:

- Implementation of the analysis procedures in an automatic process
- User oriented visualisation with interactive computing and multidimensional graphical displays
- An explorative approach to integrate the operators experience

To analyse meta data not only with respect to statistical effects and conclusions new methods and algorithms were evaluated at Plath GmbH together with HITEC, a research centreof the university of Hamburg. Meta data analysis for automated procedures can be implemented with a model based system even for complex interrelationship of the analysed data. With this system the user can frame constraints which are then detected in the huge amount of data effectively and less time consuming. With such methods alarming and detection of known behaviour can be implemented for any kind of data based stored meta data.

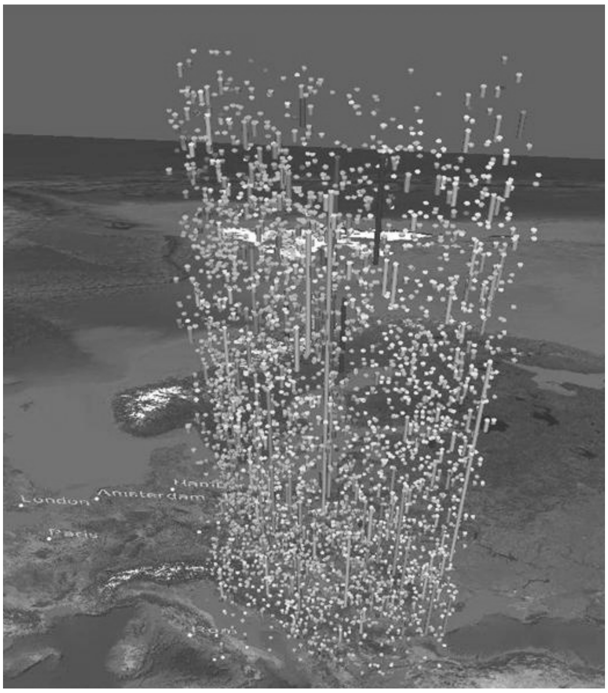
After analysing the large amount of data the visualisation of results is the next challenge for effective a user intuitive operation. Of course there are sometimes operators or analysts, who do prefer long listings and complex tables. But for most of the people a chart, a histogram or especially when a geographical background is given a map is much easier to "read" than any table.



Map display of communication structures

Therefore the right display for every special information is one of the key factors for a good decision support tool.

At least the possibility to analyse the mass data interactively with graphical tools and intuitive possibilities to manipulate and filter the displayed data is an important aspect to integrate the users experience into the computer assisted analysis. This intuitive way of data selection and display is the only way to let the specialists do the analysis work without being an expert of information technology.
Or in other words:
It must not be necessary any longer to write SQL database queries manually to do a good analysis job on mass data, with user friendly and interactive graphical user interfaces the specialist in content is the best operator to gain relevant information as soon as possible.



Interactive 3d display of radio communication

Summary

All three aspects are taken into account to improve the analysis of meta data from radio reconnaissance. With the model based system these methods can also be applied to any other field of analysis of technical data such as security applications. With the automation and the user driven exploration of the data the efficiency of the analysis will be speed up to get the situation awareness as soon as possible. By analysing the actual situation in detail indication for possible threats should be detected to initiate the right provisions and get situation awareness – in advance.

Security of Civil Air Transport. The projects CASAM, PALMA and PATIN

Dr. Klaus Scheerer, Diehl BGT Defence GmbH & Co. KG, Germany

Abstract

CASAM, PALMA and PATIN are EC supported projects which address the security of civilian aircraft in the face of terroristic threats. CASAM concentrates research on an innovative directed IR countermeasure (DIRCM) considering innovative laser systems especially designed for the use on commercial aircraft to counter MANPAD attacks. A prototype for validation purposes will be built and tested against an infrared seeker head.

PALMA investigates the threat by MANPADs in a broader context, especially the possibilities to transfer countermeasures well known inside the military community into a civilian environment.

The goal of PATIN is to design a system of systems for the protection of the entire air transportation chain against terrorist attacks. This comprises the detection and repelling of chemical, biological, radiological and explosive threats in the terminal buildings, hangars and the airport based defence against attacks by projectiles or missiles. For the overall protection concept the results of PALMA and CASAM will be considered.

Introduction

Commercial aircraft are a target of terrorists because they represent one of the best achievements of our society: an attack has a big psychological impact on population, and thus economical activity. If a multiple attack like the ones of Madrid railways were to occur in several airports spread over the globe, economy would be severely weakened.

This effect would be reinforced if terrorists underlined that after Madrid occurred London. Besides the 11th of September twin towers type of event exists another threat: 15000 disseminated shoulders launched IR guided missiles (MANPADS), which are in uncontrolled hands. Several attacks already occurred and evidence of MANPADS trafficking has been reported. The US are preparing regulations to force commercial aircraft to be equipped with onboard protection systems.

CASAM

Civil Aircraft Security Against MANPADS

CASAM is a project of the 6th framework programme and started on June 1, 2006. The duration is 26 months.

It is vital for Europe from a security and an economical point of view to be able to answer the requirement for a self-protections system against MANPADS for civilian airliners. Future protection systems must be competitive, i.e. they must be low-cost and are required to induce only minimal interference concerning aircraft performance. (low mass, low power consumption, low drag). A protection system comprises a missile approach warning system and missile deceiving device. CASAM research concentrates on the missile deceiving device: an innovative Directed InfraRed Countermeasure (DIRCM) equipment which represents the most expensive and bulky part of an aircraft self-defence system.

It will be specifically designed for civilian aircraft, keeping interferences with the aircraft and the airport environment minimal. As a two years' project in the 6th framework programme, CASAM explores several technological break throughs in laser technology, optics, electro-mechanics and signal processing that will be the core of the future competitive equipment. A technical validation prototype will be tested against an actual infrared seeker head. Specific effort will be put on threat analysis and simulation, economical analysis, aircraft installation constraints and overall impact. A specific study will be carried out on legal and regulation issues, which have a prominent position in the roadmap to an operational system.

PALMA

Protection of AirLiners against Manpads Attacks

PALMA is a project in the framework of the Preparatory Action on Security Research (PASR) and was started on February 1, 2006 with a duration of 18 months.

PALMA's main objective is to evaluate, on an European level, the efficiency and the impacts of on-board self-protection systems (certification, environment and population safety, air traffic, costs…).

Through the investigation of critical technologies for short, medium and long term solutions, future research needs will be identified and, if needed, requirements for a future operational system will be defined. Special attention will be given to the possibility to transfer already existing military technology into a civilian world.

The project is divided into three main items:

- Description of the threat in a qualitative and quantitative manner for typical airliners and typical MANPADS which are known to be in the hands of terrorist groups and identification of the functional and operational requirements,
- Technological analysis, including specific experimental investigations,
- Recommendation for future developments.

The main expected outputs of the project are:

- Recommendations for future regulations,
- Definition of intermediate solutions with existing technologies and a research programme for a fully compliant system,
- Roadmap for European technology developments.

PATIN

Protection of Air Transportation and Infrastructure

PATIN is a project in the framework of the Preparatory Action on Security Research (PASR) and was started on July 1, 2006 with a duration of 15 months.

PATIN aims to ensure the security of EU citizens by protecting the whole air transportation system against terrorist attacks, including airport, aircraft, critical ground infrastructure and the information system. The project will assess aspects of crisis management, interoperability and optimisation of security networks. PATIN will analyse all potentially relevant threats and technologies and will derive from these a set of viable future operational concepts. A conference and joint exercises with the stakeholder community (users and security organisations) will be organised to assess the operational concepts and the improved security provided. PATIN adapts a layered protection mechanism which forms a system-of-system interconnected through networks.

Essential work to be performed comprises:

- Analysis of the security measures of the existing Air Transportation system
- Definition of a security case
- Definition of a security assessment methodology
- Identification of technologies for protection of air transport and infrastructure
- Development of concepts for the protection of the critical infrastructure and the airport/aircraft protection system under consideration of the results of other relevant projects (PALMA, CASAM, SAFEE)

Analysing Critical Infrastructure Dependencies

H.A.M. Luiijf
ericluiijf@hcss.nl, The Hague Centre for Strategic Studies, Netherlands

A.H Nieuwenhuijs and M.H.A. Klaver
{albert.nieuwenhuijs | marieke.klaver}@tno.nl
TNO Defence, Security and Safety, Netherlands

Abstract

Critical Infrastructures are increasingly dependent and interdependent of each other. Various types of dependencies exist. An in-depth study on these types of dependencies has taken place based on modelling and on analysis of day-to-day dependencies found in our own database on international critical infrastructure outages. A new set of dependency dimensions for describing infrastructure dependencies is proposed in this paper.

Introduction

In 2001, [Rinaldi] proposed a set of dimensions for describing infrastructure dependencies and interdependencies. From the analysis of a large set of international critical (information) infrastructure failures, and analysis of the Dutch critical infrastructure, we gained more insight in (inter)dependencies of critical processes in critical infrastructures. Based on that experience we propose a different structuring of dependency dimensions disregarding any threats.

Definitions

A *critical infrastructure* (CI) consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments [EU].

Dependency is either a link or a connection between two products or services, through which the state of one influences or correlates to the state of the other. [Rinaldi] *Interdependency* is the mutual dependency of products or services. [ACIP].

Dependency dimension

[Rinaldi] described a set of dimensions for describing infrastructure dependencies. Growing experience with critical infrastructure and their dependencies brought us to revise the Rinaldi proposed structure. Our proposed structure covers new aspects and compacts some of the dimensions proposed by Rinaldi.

The 'type of dependency' dimension

Type 1: Service or product dependency (chain/cascading effect)

The undisturbed functioning of a critical process in a CI critically depends on the delivery of services and/or products produced by other CI. This type of dependency is split into the dependency of tangible products and of intangible products like services and information. Examples are fuel supply, financial services, and weather reports.

Type 2: Common vulnerabilities

Common weakness(es) create a vulnerability based dependency for critical processes within multiple CI. Such a vulnerability dependency may be revealed by a risk analysis per critical process. The right risk appreciation, however, depends on the understanding that the vulnerability is shared by more CI. This type of dependency is either caused by processes and components which are shared between infrastructures, or processes and components of different CI that share a common vulnerability.
The first type comprises for instance a single glass fibre or duct shared by multiple CI. The second type comprises for instance the sharing of the same geographic location (e.g., business park; road, rail, waterway, duct, pipeline, cable crossings) by multiple CI, every router running the same operating system with the same vulnerability, flooding of an area affecting more CI.

Type 3: Resilience dependency

Rather than the type 1 service or product dependency, a CI is dependent on other CI in order to maintain its proper state of resilience. For example, the control of power transmission and distribution requires the functioning of telecommunications. When the normal communication channels fail, the electric power control depends for its resilience upon other CI for its (alternate) communications.

The ‘reponse’ dimension

The response dimension falls apart into input-response and time-response. Input-response describes the output of a CI as a response function to the level (quality, quantity) in which its dependencies are satisfied. Time-response describes the output of a CI in terms of its temporal behaviour after failure or resumption in satisfying its dependencies.

Two aspects of input-response are distinguished: the way the output and inputs are related when the supply is deteriorating, and the way the output and inputs are related when the supply is recovering. Note that these input-response functions can be the same, but often are not.

The time-response falls apart in six aspects:

- the time period after failure in satisfying its dependencies before decay of the CI output starts,
- the time period between re-satisfaction of dependencies and restoration of the CI output starts,
- the extent to which output decays as a function of time,
- the extent to which output recovers as a function of time,
- differential aspect,
- integrating aspect.

The extent to which output decays as a function of time as well its recovery equivalent are often hard to determine due to their dependence on external circumstances such as weather, time of day, day of the week, water levels, etc.

The differential aspect describes the effect dependent on the degree or speed of (partial) disruption. An example is the level of stockpiling after a steep price increase of a critical commodity like petrol.

The integrating aspect describes the effect that a reduction in the level of satisfaction of dependencies on the input side causes a continuously increasing lack of service at the output side. For example, a minor decrease in responsiveness by the government leads to a steadily decreasing trust by the citizens.

The ‘quality’ dimension

Most of the dependencies discussed by [Rinaldi] implicitly presume either the availability or unavailability of a CI service or product. From incidents with CI (e.g., [RVTV]), we learned that the critical service availability is more than just on/off. CI products and services need to be supplied with the right quality. For example, the right quantity/time, speed of flow, temperature, pressure, mixture, frequency/voltage levels, purity, and data integrity.

Concluding remarks

We propose three dimensions for describing critical infrastructure dependencies as an alternate to [Rinaldi]. Our on-going dependency studies have to prove the completeness of our proposed set of dimensions.

References

- ACIP consortium, *Analysis and Assessment for Critical Infrastructure Protection (ACIP) final report*, EU/DG Information Society and Media, Brussels, Belgium, 2003.
- EU, *Critical Infrastructure Protection in the fight against terrorism, COM(2004) 702 final,* Communication from the Commission to the Council and the European Parliament, Brussels, 2004.
- Raad voor de Transportveiligheid (RVTV), *Storing gasmengstation*, report RVTV-CB-2-02.060, Den Haag, Netherlands, December 2002.
- Rinaldi, S.M., Peerenboom, J., Kelly, T., *Complexities in identifying, Understanding, and Analyzing Critical Infrastructure Dependencies*, Special issue IEEE Control Systems Magazine on “Complex Interactive Networks”, December 2001.

The ‘Secure Haven’ Concept: Living, Working and Recreation in an Inherently Secure Environment

Maud Groenberg (Ministry of the Interior and Kingdom Relation), Netherlands

The Hague. Not just a pleasant city by the sea, but above all a highly international town.

abstract:

The Hague ranks world wide fourth on the list of host towns for United Nations offices and agencies and is keen to expand the city's international position. One of the ways to do this is by the Secure haven project. This project combines security and comfort for both the city and its inhabitants and visitors.

The context: The Hague as a Secure Haven

On a global scale, The Hague ranks fourth on the list of host towns for United Nations offices and agencies. In addition, there are dozens of embassies and head offices of international corporations. The city is often referred to as "World Legal Capital" because justice, conflict prevention and security are core business of the international community in The Hague. The city hosts the International Court of Justice, the International Criminal Tribunal for the former Yugoslavia, the International Criminal Court and the Headquarters of Europol.

The city's international community serves as an important engine of the local economy. Not surprisingly, The Hague City Council is keen to expand the city's international position. One of the main projects to achieve this ambition is ‘Secure Haven’.

The Secure Haven project

This research project started in May 2007 and links innovation with infrastructure. Secure Haven will take shape over the next couple of years, with full support of the Dutch Ministry for Economic Affairs and the Ministry of the Interior and Kingdom relations. Knowledge available on the national level will be used to help The Hague in realizing its initiative.

The Hague, as World Legal Capital, will serve as an experimental testing ground for a whole new approach to security. High-performance yet inconspicuous, unobtrusive technology will guarantee security. No easy matter, because four contradictory perspectives have to be considered simultaneously and in relation to each other. The four perspectives are 1) how to preserve privacy, 2) optimization of security and vital infrastructure, 3) the quality of life and 4) the economy and services.

Through a series of try-outs and prototypes in The Hague, the partners aim to arrive at three products:

1. A blueprint for a Secure Haven; Eventually this should lead to an all encompassing design of how the city could look by 2015 – 2020;
2. Policy innovation; effectuated in several ways. There will be gaming, simulation and roundtable sessions with policymakers.
3. Knowledge transfer; in the shape of seminars and a dedicated website.

With these, The Hague will have the potential to transform (step-by-step) into a Secure Haven that can indeed continue to be a safe haven throughout the 21st century.

The conference will serve as an international and interdisciplinary communication platform for decision-makers, executive bodies, economic organisations and research and development partners. The conference defines the position of key organisations and demonstrates the potential of innovative technologies and preventative research for civil security on an international level.

Fraunhofer Verbund
Verteidigungs- und
Sicherheitsforschung

ISBN: 978-3-86644-147-7

www.uvka.de